Guide to Computer Forensics and Investigations
Sixth Edition

Chapter 1

Understanding The Digital Forensics Profession and Investigations

CENGAGE

Objectives

- Describe the field of digital forensics
- Explain how to prepare computer investigations and summarize the difference between public-sector and private-sector investigations
- Explain the importance of maintaining professional conduct
- Describe how to prepare a digital forensics investigation by taking a systematic approach
- Describe procedures for private-sector digital investigations
- Explain requirements for data recovery workstations and software
- Summarize how to conduct an investigation, including critiquing a case

An Overview of Digital Forensics (1 of 3)

- **Digital forensics**
  - The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation.
  - In October 2012, an ISO standard for digital forensics was ratified - ISO 27037 Information technology - Security techniques

An Overview of Digital Forensics (2 of 3)

- The Federal Rules of Evidence (FRE) was created to ensure consistency in federal proceedings
  - Signed into law in 1973
  - Many states’ rules map to the FRE
- FBI Computer Analysis and Response Team (CART) was formed in 1984 to handle cases involving digital evidence
- By late 1990s, CART teamed up with Department of Defense Computer Forensics Laboratory (DCFL)

An Overview of Digital Forensics (3 of 3)

- The **Fourth Amendment** to the U.S. Constitution protects everyone's right to be secure from search and seizure
  - Separate **search warrants** might not be necessary for digital evidence
- Every U.S. jurisdiction has case law related to the admissibility of evidence recovered from computers and other digital devices

Digital Forensics and Other Related Disciplines (1 of 3)

- Investigating digital devices includes:
  - Collecting data securely
  - Examining suspect data to determine details such as origin and content
  - Presenting digital information to courts
  - Applying laws to digital device practices
- Digital forensics is different from **data recovery**
  - Which involves retrieving information that was deleted by mistake or lost during a power surge or server crash
- Forensics investigators often work as part of a team, known as the investigations triad

Digital Forensics and Other Related Disciplines (2 of 3)

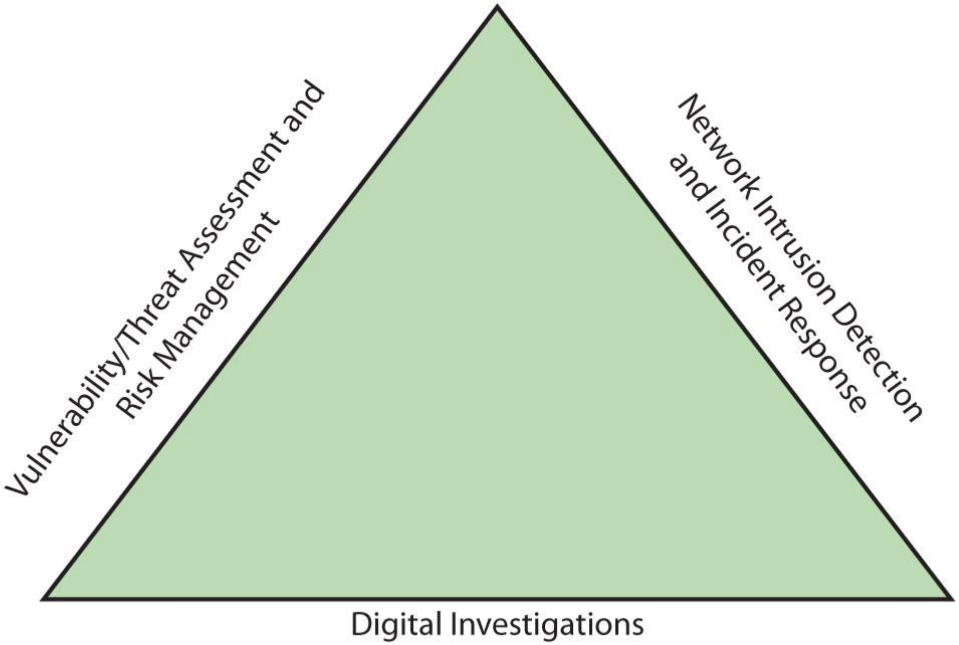

Vulnerability/Threat Assessment and Risk Management
Network Intrusion Detection and Incident Response
Digital Investigations

Figure 1-1 **The investigations triad**

Digital Forensics and Other Related Disciplines (3 of 3)

- Vulnerability/threat assessment and risk management
  - Tests and verifies the integrity of stand-along workstations and network servers
- Network intrusion detection and incident response
  - Detects intruder attacks by using automated tools and monitoring network firewall logs
- Digital investigations
  - Manages investigations and conducts forensics analysis of systems suspected of containing evidence

A Brief History of Digital Forensics

- By the early 1990s, the International Association of Computer Investigative Specialists (IACIS) introduced training on software for digital forensics
- IRS created search-warrant programs
- ASR Data created Expert Witness for Macintosh
- ILook is currently maintained by the IRS Criminal Investigation Division
- AccessData Forensic Toolkit (FTK) is a popular commercial product

Understanding Case Law

- Existing laws can’t keep up with the rate of technological change
- When statutes don’t exist, case law is used
  - Allows legal counsel to apply previous similar cases to current one in an effort to address ambiguity in laws
- Examiners must be familiar with recent court rulings on search and seizure in the electronic environment

Developing Digital Forensics Resources

- To supplement your knowledge:
  - Develop and maintain contact with computing, network, and investigative professionals
  - Join computer user groups in both the pubic and private sectors
    - Example: **Computer Technology Investigators Network (CTIN)** meets to discuss problems with digital forensics examiners encounter
  - Consult outside experts

Preparing for Digital Investigations (1 of 3)

- Digital investigations fall into two categories:
  - Public-sector investigations
  - Private-sector investigations

Preparing for Digital Investigations (2 of 3)

Government agencies
Article 8 in the Charter of Rights of Canada
U.S. Fourth Amendment search and seizure rules
Private organizations
Company policy violations
Litigation disputes

Figure 1-4 **Public-sector and private-sector investigations**

iStock.com/RobinsonBecquart, iStock.com/buzbuzzer

Preparing for Digital Investigations (3 of 3)

- Public-sector investigations involve government agencies responsible for criminal investigations and prosecution
- Fourth Amendment to the U.S. Constitution
  - Restrict government **search and seizure**
- The Department of Justice (DOJ) updates information on computer search and seizure regularly
- Private-sector investigations focus more on policy violations

Understanding Law Enforcement Agency Investigations

- When conducting public-sector investigations, you must understand laws on computer-related crimes including:
  - Standard legal processes
  - Guidelines on search and seizure
  - How to build a criminal case
- The Computer Fraud and Abuse Act was passed in 1986
  - Specific state laws were generally developed later

Following Legal Processes (1 of 2)

- A criminal investigation usually begins when someone finds evidence of or witnesses a crime
  - Witness or victim makes an **allegation** to the police
- Police interview the complainant and writes a report about the crime
- Report is processed and management decides to start an investigation or log the information in a police blotter
  - Blotter is a historical database of previous crimes

Following Legal Processes (2 of 2)

- **Digital Evidence First Responder (DEFR)**
  - Arrives on an incident scene, assesses the situation, and takes precautions to acquire and preserve evidence
- **Digital Evidence Specialist (DES)**
  - Has the skill to analyze the data and determine when another specialist should be called in to assist
- **Affidavit** - a sworn statement of support of facts about or evidence of a crime
  - Must include **exhibits** that support the allegation

Understanding Private-Sector Investigations (1 of 8)

- Private-sector investigations involve private companies and lawyers who address company policy violations and litigation disputes
  - Example: wrongful termination
- Businesses strive to minimize or eliminate litigation
- Private-sector crimes can involve:
  - E-mail harassment, falsification of data, gender and age discrimination, embezzlement, sabotage, and industrial espionage

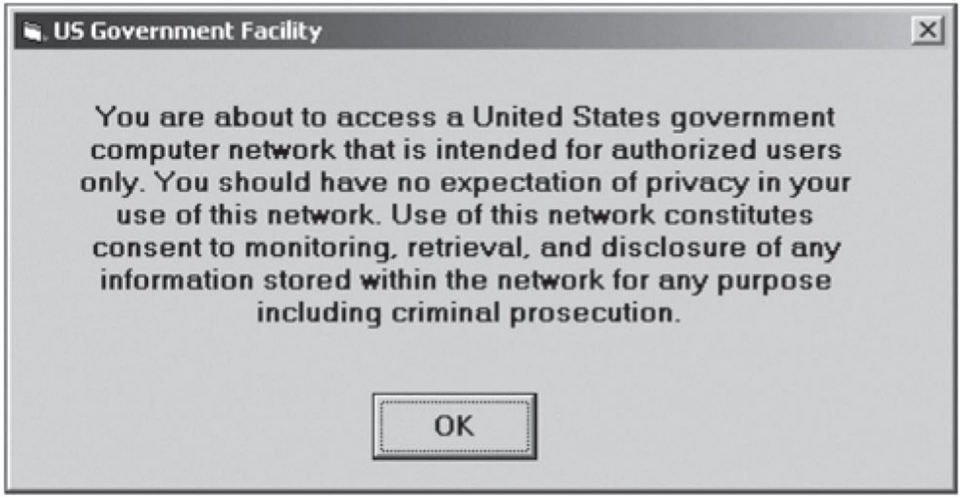
Understanding Private-Sector Investigations (2 of 8)

- Businesses can reduce the risk of litigation by publishing and maintaining policies that employees find easy to read and follow
- Most important policies define rules for using the company’s computers and networks
  - Known as an “Acceptable use policy”
- **Line of authority** - states who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to evidence

Understanding Private-Sector Investigations (3 of 8)

- Business can avoid litigation by displaying a **warning banner** on computer screens
  - Informs end users that the organization reserves the right to inspect computer systems and network traffic at will

Understanding Private-Sector Investigations (4 of 8)



You are about to access a United States government computer network that is intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose including criminal prosecution.

Figure 1-7 A sample warning banner

Understanding Private-Sector Investigations (5 of 8)

- Sample text that can be used in internal warning banners:
  - Use of this system and network is for official business only
  - Systems and networks are subject to monitoring at any time by the owner
  - Using this system implies consent to monitoring by the owner
  - Unauthorized or illegal users of this system or network will be subject to discipline or prosecution

Understanding Private-Sector Investigations (6 of 8)

- Businesses are advised to specify an **authorized requester** who has the power to initiate investigations
- Examples of groups with authority
  - Corporate security investigations
  - Corporate ethics office
  - Corporate equal employment opportunity office
  - Internal auditing
  - The general counsel or legal department

Understanding Private-Sector Investigations (7 of 8)

- During private investigations, you search for evidence to support allegations of violations of a company’s rules or an attack on its assets
- Three types of situations are common:
  - Abuse or misuse of computing assets
  - E-mail abuse
  - Internet abuse
- A private-sector investigator’s job is to minimize risk to the company

Understanding Private-Sector Investigations (8 of 8)

- The distinction between personal and company computer property can be difficult with cell phones, smartphones, personal notebooks, and tablet computers
- Bring your own device (BYOD) environment
    - Some companies state that if you connect a personal device to the business network, it falls under the same rules as company property

Maintaining Professional Conduct

- **Professional conduct** - includes ethics, morals, and standards of behavior
- An investigator must exhibit the highest level of professional behavior at all times
  - Maintain objectivity
  - Maintain credibility by maintaining confidentiality
- Investigators should also attend training to stay current with the latest technical changes in computer hardware and software, networking, and forensic tools

Preparing a Digital Forensics Investigation

- The role of digital forensics professional is to gather evidence to prove that a suspect committed a crime or violated a company policy
- Collect evidence that can be offered in court or at a corporate inquiry
  - Investigate the suspect’s computer
  - Preserve the evidence on a different computer
- **Chain of custody**
  - Route the evidence takes from the time you find it until the case is closed or goes to court

An Overview of a Computer Crime

- Computers can contain information that helps law enforcement determine:
  - Chain of events leading to a crime
  - Evidence that can lead to a conviction
- Law enforcement officers should follow proper procedure when acquiring the evidence
  - Digital evidence can be easily altered by an overeager investigator
- A potential challenge: information on hard disks might be password protected so forensics tools may be need to be used in your investigation

An Overview of a Company Policy Violation

- Employees misusing resources can cost companies millions of dollars
- Misuse includes:
  - Surfing the Internet
  - Sending personal e-mails
  - Using company computers for personal tasks

Taking a Systematic Approach (1 of 2)

- Steps for problem solving
  - Make an initial assessment about the type of case you are investigating
  - Determine a preliminary design or approach to the case
  - Create a detailed checklist
  - Determine the resources you need
  - Obtain and copy an evidence drive

Taking a Systematic Approach (2 of 2)

- Steps for problem solving (cont’d)
  - Identify the risks
  - Mitigate or minimize the risks
  - Test the design
  - Analyze and recover the digital evidence
  - Investigate the data you recover
  - Complete the case report
  - Critique the case

Assessing the Case

- Systematically outline the case details
  - Situation
  - Nature of the case
  - Specifics of the case
  - Type of evidence
  - Known disk format
  - Location of evidence
- Based on these details, you can determine the case requirements

Planning Your Investigation (1 of 5)

- A basic investigation plan should include the following activities:
  - Acquire the evidence
  - Complete an evidence form and establish a chain of custody
  - Transport the evidence to a computer forensics lab
  - Secure evidence in an **approved secure container**

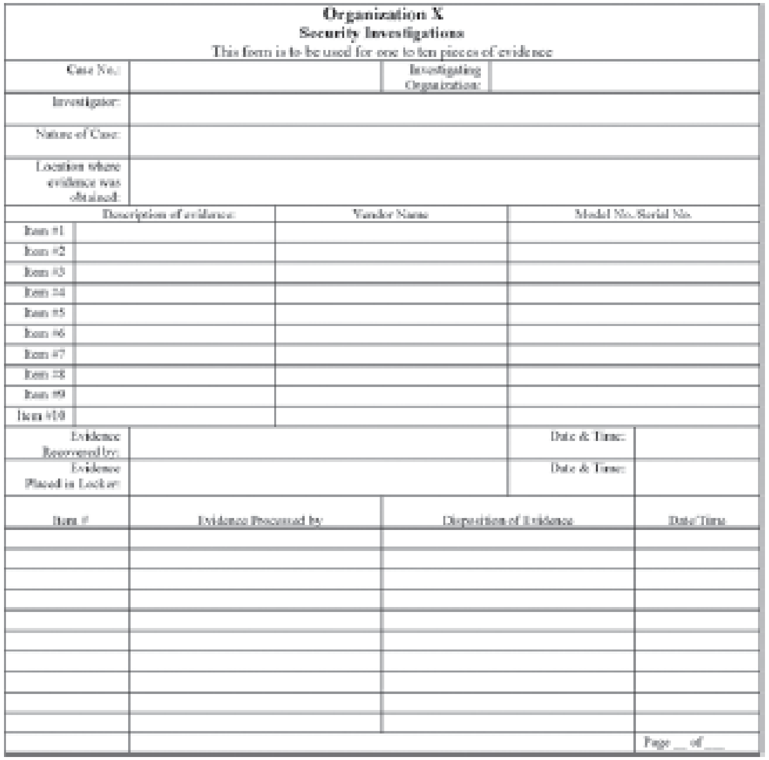
Planning Your Investigation (2 of 5)

- A basic investigation plan (cont’d):
  - Prepare your **forensics workstation**
  - Retrieve the evidence from the secure container
  - Make a forensic copy of the evidence
  - Return the evidence to the secure container
  - Process the copied evidence with computer forensics tools

Planning Your Investigation (3 of 5)

- An **evidence custody form** helps you document what has been done with the original evidence and its forensics copies
  - Also called a chain-of-evidence form
- Two types
  - **Single-evidence form**
    - Lists each piece of evidence on a separate page
  - **Multi-evidence form**

Planning Your Investigation (4 of 5)



Organization X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

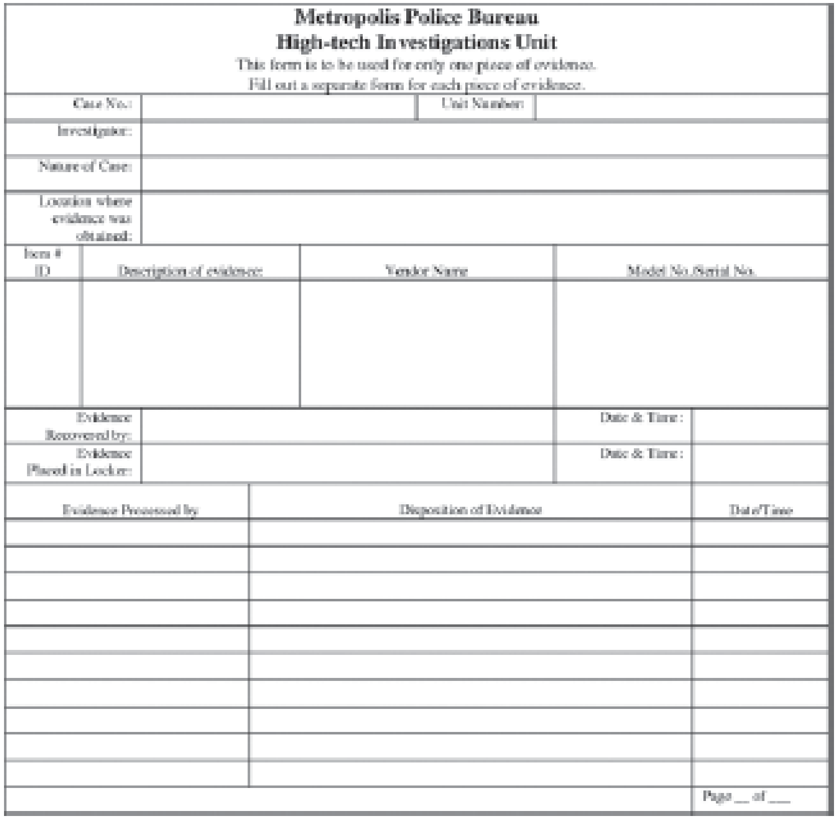
	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of ___

Figure 1-9 A sample multi-evidence form used in a private-sector environment

Planning Your Investigation (5 of 5)



Metropolis Police Bureau
High-tech Investigations Unit
This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Evidence Processed by	Disposition of Evidence	Date/Time
		Page __ of __

Figure 1-10 A single-evidence form

Securing Your Evidence (1 of 2)

- Use evidence bags to secure and catalog the evidence
- Use computer safe products when collecting computer evidence
    - Antistatic bags
    - Antistatic pads
- Use well padded containers
- Use evidence tape to seal all openings
    - CD drive bays
    - Insertion slots for power supply electrical cords and USB cables

Securing Your Evidence (2 of 2)

- Write your initials on tape to prove that evidence has not been tampered with
- Consider computer specific temperature and humidity ranges
  - Make sure you have a safe environment for transporting and storing it until a secure evidence container is available

Procedures for Private-Sector High-Tech Investigations

- As an investigator, you need to develop formal procedures and informal checklists
  - To cover all issues important to high-tech investigations
  - Ensures that correct techniques are used in an investigation

Employee Termination Cases

- The majority of investigative work for termination cases involves employee abuse of corporate assets
- Incidents that create a hostile work environment are the predominant types of cases investigated
  - Viewing pornography in the workplace
  - Sending inappropriate e-mails
- Organizations must have appropriate policies in place

Internet Abuse Investigations (1 of 2)

- To conduct an investigation you need:
  - Organization’s Internet proxy server logs
  - Suspect computer’s IP address
  - Suspect computer’s disk drive
  - Your preferred computer forensics analysis tool

Internet Abuse Investigations (2 of 2)

- Recommended steps
  - Use standard forensic analysis techniques and procedures
  - Use appropriate tools to extract all Web page URL information
  - Contact the network firewall administrator and request a proxy server log
  - Compare the data recovered from forensic analysis to the proxy server log
  - Continue analyzing the computer’s disk drive data

E-mail Abuse Investigations (1 of 2)

- To conduct an investigation you need:
    - An electronic copy of the offending e-mail that contains message header data
    - If available, e-mail server log records
    - For e-mail systems that store users’ messages on a central server, access to the server
    - Access to the computer so that you can perform a forensic analysis on it
    - Your preferred computer forensics analysis tool

E-mail Abuse Investigations (2 of 2)

- Recommended steps
  - Use the standard forensic analysis techniques
  - Obtain an electronic copy of the suspect’s and victim’s e-mail folder or data
  - For Web-based e-mail investigations, use tools such as FTK’s Internet Keyword Search option to extract all related e-mail address information
  - Examine header data of all messages of interest to the investigation

Attorney-Client Privilege Investigations (1 of 4)

- Under **attorney-client privilege (ACP)** rules for an attorney
  - You must keep all findings confidential
- Many attorneys like to have printouts of the data you have recovered
  - You need to persuade and educate many attorneys on how digital evidence can be viewed electronically
- You can also encounter problems if you find data in the form of binary files

Attorney-Client Privilege Investigations (2 of 4)

- Steps for conducting an ACP case
  - Request a memorandum from the attorney directing you to start the investigation
  - Request a list of keywords of interest to the investigation
  - Initiate the investigation and analysis
  - For disk drive examinations, make two bit-stream images using different tools for each image
  - Compare hash signatures on all files on the original and re-created disks

Attorney-Client Privilege Investigations (3 of 4)

- Steps for conducting an ACP case (cont’d)
  - Methodically examine every portion of the disk drive and extract all data
  - Run keyword searches on allocated and unallocated disk space
  - For Windows OSs, use specialty tools to analyze and extract data from the Registry
  - For binary data files such as CAD drawings, locate the correct software product
  - For unallocated data recovery, use a tool that removes or replaces nonprintable data

Attorney-Client Privilege Investigations (4 of 4)

- Steps for conducting an ACP case (cont'd)
  - Consolidate all recovered data from the evidence bit-stream image into folders and subfolders
- Other guidelines
  - Minimize written communications with the attorney
  - Any documentation written to the attorney must contain a header stating that it's "Privileged Legal Communication—Confidential Work Product"
  - Assist the attorney and paralegal in analyzing data

CENGAGE

Industrial Espionage Investigations (1 of 5)

- All suspected industrial espionage cases should be treated as criminal investigations
- Staff needed
  - Digital investigator who is responsible for disk forensic examinations
  - Technology specialist who is knowledgeable of the suspected compromised technical data
  - Network specialist who can perform log analysis and set up network sniffers
  - Threat assessment specialist (typically an attorney)

Industrial Espionage Investigations (2 of 5)

- Guidelines when initiating an investigation
  - Determine whether this investigation involves a possible industrial espionage incident
  - Consult with corporate attorneys and upper management
  - Determine what information is needed to substantiate the allegation
  - Generate a list of keywords for disk forensics and sniffer monitoring
  - List and collect resources for the investigation

Industrial Espionage Investigations (3 of 5)

- Guidelines (cont’d)
  - Determine goal and scope of the investigation
  - Initiate investigation after approval from management
- Planning considerations
  - Examine all e-mail of suspected employees
  - Search Internet newsgroups or message boards
  - Initiate physical surveillance
  - Examine facility physical access logs for sensitive areas

Industrial Espionage Investigations (4 of 5)

- Planning considerations (cont'd)
  - Determine suspect location in relation to the vulnerable asset
  - Study the suspect's work habits
  - Collect all incoming and outgoing phone logs
- Steps to conducting an industrial espionage case
  - Gather all personnel assigned to the investigation and brief them on the plan
  - Gather resources to conduct the investigation

Industrial Espionage Investigations (5 of 5)

- Steps (cont’d)
  - Place surveillance systems at key locations
  - Discreetly gather any additional evidence
  - Collect all log data from networks and e-mail servers
  - Report regularly to management and corporate attorneys
  - Review the investigation’s scope with management and corporate attorneys

Interviews and Interrogations in High-Tech Investigations (1 of 2)

- Becoming a skilled interviewer and interrogator can take many years of experience
- **Interview**
  - Usually conducted to collect information from a witness or suspect
    - About specific facts related to an investigation
- **Interrogation**
  - Process of trying to get a suspect to confess

Interviews and Interrogations in High-Tech Investigations (2 of 2)

- Role as a digital investigator
  - To instruct the investigator conducting the interview on what questions to ask
    - And what the answers should be
- Ingredients for a successful interview or interrogation
  - Being patient throughout the session
  - Repeating or rephrasing questions to zero in on specific facts from a reluctant witness or suspect
  - Being tenacious

Understanding Data Recovery Workstations and Software

- Investigations are conducted on a computer forensics lab (or data-recovery lab)
  - In data recovery, the customer or your company just wants the data back
- Computer forensics workstation
  - A specially configured PC
  - Loaded with additional bays and forensics software
- To avoid altering the evidence use:
  - Write-blockers devices
    - Enable you to boot to Windows without writing data to the evidence drive

Setting Up Your Workstation for Digital Forensics (1 of 2)

- Basic requirements
  - A workstation running Windows 7 or later
  - A write-blocker device
  - Digital forensics acquisition tool
  - Digital forensics analysis tool
  - Target drive to receive the source or suspect disk data
  - Spare PATA or SATA ports
  - USB ports

Setting Up your Workstation for Digital Forensics (2 of 2)

- Additional useful items
  - Network interface card (NIC)
  - Extra USB ports
  - FireWire 400/800 ports
  - SCSI card
  - Disk editor tool
  - Text editor tool
  - Graphics viewer program
  - Other specialized viewing tools

Conducting an Investigation

- Gather resources identified in investigation plan
- Items needed
  - Original storage media
  - Evidence custody form
  - Evidence container for the storage media
  - Bit-stream imaging tool
  - Forensic workstation to copy and examine your evidence
  - Securable evidence locker, cabinet, or safe

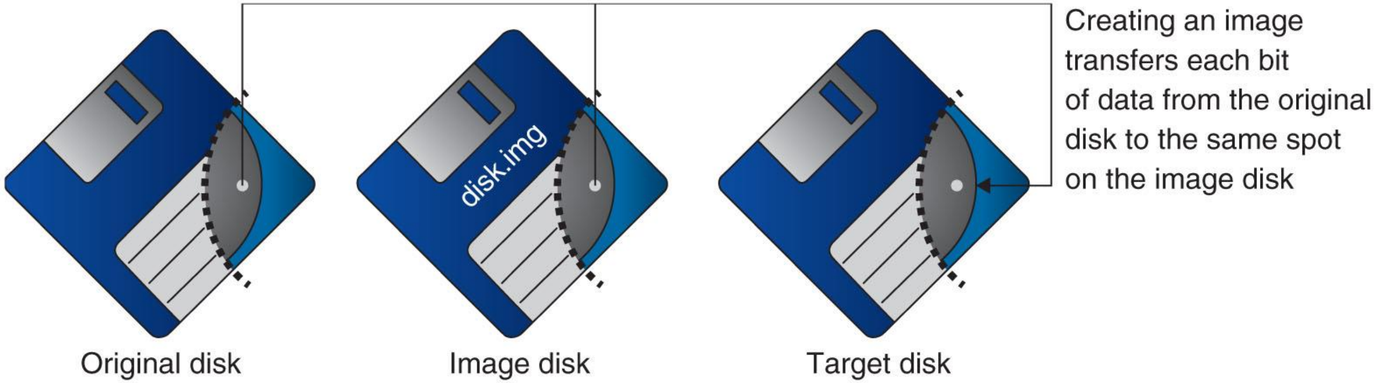
Gathering the Evidence

- Avoid damaging the evidence
- Steps
  - Meet the IT manager to interview him
  - Fill out the evidence form, have the IT manager sign
  - Place the evidence in a secure container
  - Carry the evidence to the computer forensics lab
  - Complete the evidence custody form
  - Secure evidence by locking the container

Understanding Bit-Stream Copies (1 of 2)

- Bit-stream copy
  - Bit-by-bit copy of the original storage medium
  - Exact copy of the original disk
  - Different from a simple backup copy
    - Backup software only copy known files
    - Backup software cannot copy deleted files, e-mail messages or recover file fragments
- Bit-stream image
  - File containing the bit-stream copy of all data on a disk or partition
  - Also known as “image” or “image file”
- Copy image file to a target disk that matches the original disk’s manufacturer, size and model

Understanding Bit-stream Copies (2 of 2)



Creating an image transfers each bit of data from the original disk to the same spot on the image disk

Figure 1-11 Transfer of data from original to image to target

Acquiring an Image of Evidence Media

- First rule of computer forensics
  - Preserve the original evidence
- Conduct your analysis only on a copy of the data
- Several vendors provide MS-DOS, Linux, and Windows acquisition tools
  - Windows tools require a write-blocking device when acquiring data from FAT or NTFS file systems

Analyzing Your Digital Evidence (1 of 8)

- Your job is to recover data from:
  - Deleted files
  - File fragments
  - Complete files
- Deleted files linger on the disk until new data is saved on the same physical location
- Tools can be used to retrieve deleted files
  - Autopsy

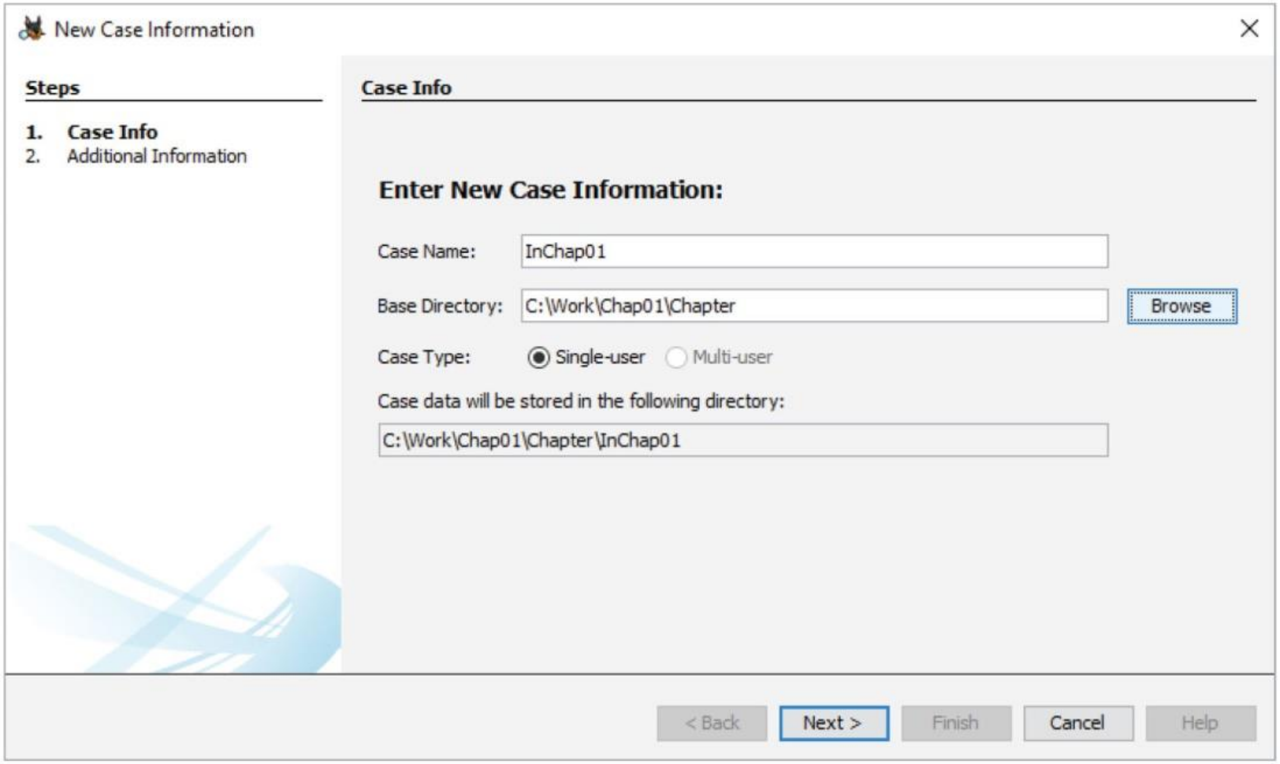
Analyzing Your Digital Evidence (2 of 8)

- Steps to analyze a USB drive
  - Start Autopsy
  - Create a new case
  - Type the case name
  - Select the working folder
- Steps to add source data
  - Select data source type
  - Select image file
  - Keep the default settings in the Configure Ingest Modules window

Analyzing Your Digital Evidence (3 of 8)

- Steps to display the contents of the acquired data
  - Click to expand **Views, File Types, By Extension, and Documents**
  - Select file to display
  - Click **Tag and Comment**
  - Click the **New Tag Name** button
- Analyze the data
  - Search for information related to the complaint
- Data analysis can be most time-consuming task

Analyzing Your Digital Evidence (4 of 8)



Enter New Case Information:

Case Name: InChap01

Base Directory: C:\Work\Chap01\Chapter

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

C:\Work\Chap01\Chapter\InChap01

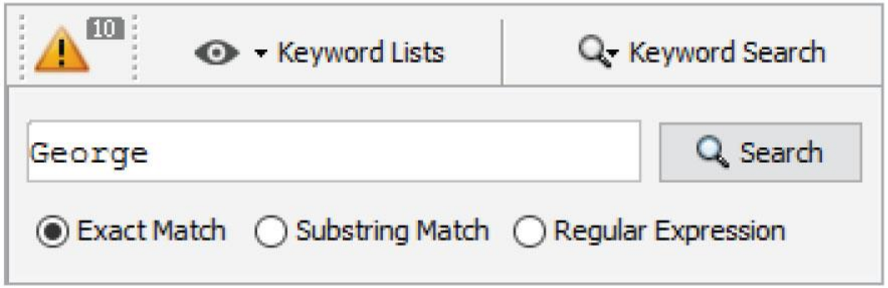
Figure 1-12 The New Case Information window

Source: *www.sleuthkit.org*

Analyzing Your Digital Evidence (5 of 8)

- With Autopsy you can:
  - Search for keywords of interest in the case
  - Display the results in a search results window
  - Click each file in the search results window and examine its content in the data area
  - Export the data to a folder of your choice
  - Search for specific filenames
  - Generate a report of your activities
- Additional features of Autopsy
  - Display binary (nonprintable) data in the Content Viewer

Analyzing Your Digital Evidence (6 of 8)



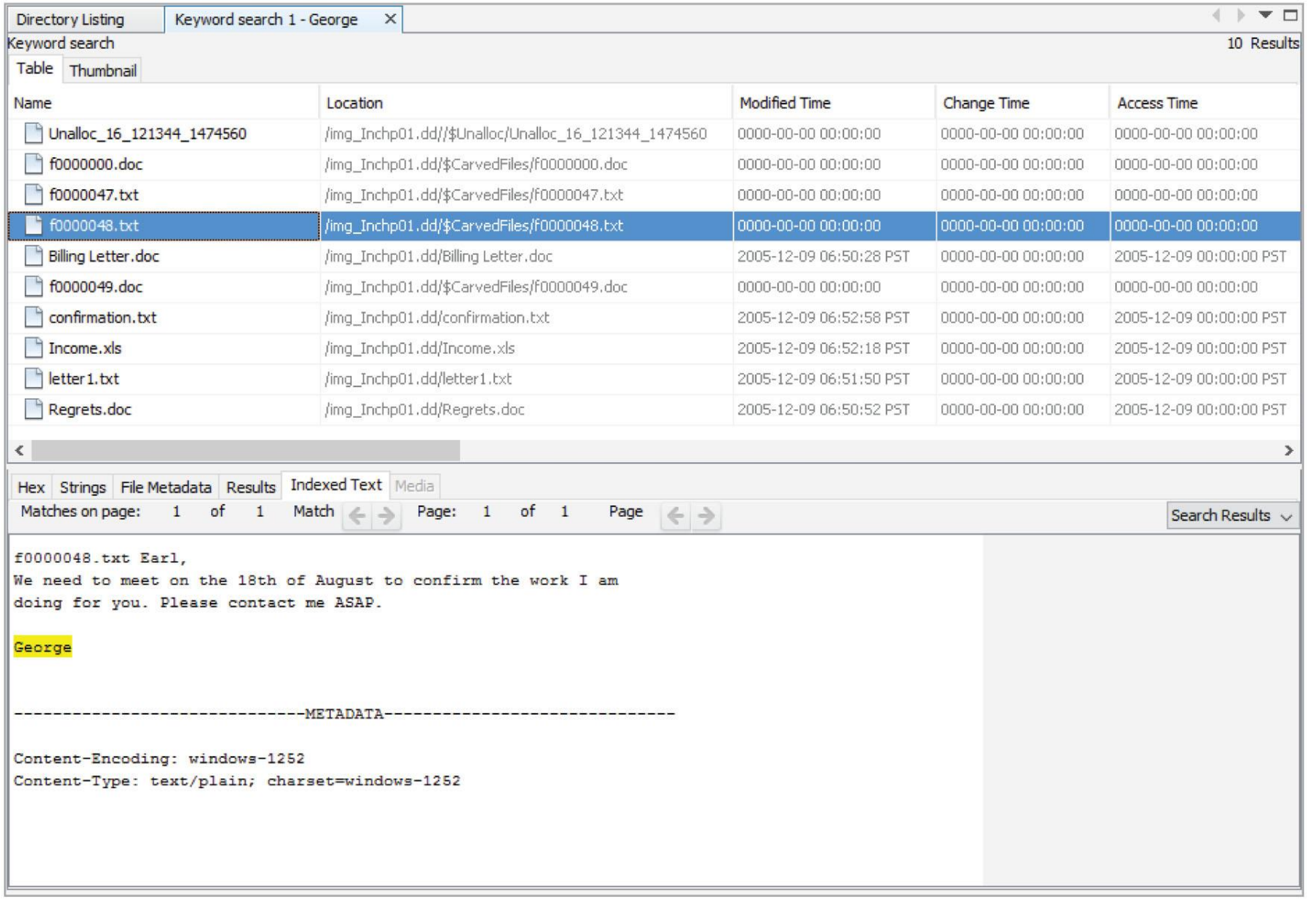
George

● Exact Match ○ Substring Match ○ Regular Expression

Figure 1-18 **Entering a keyword search term**

Source: *www.sleuthkit.org*

Analyzing Your Digital Evidence (7 of 8)



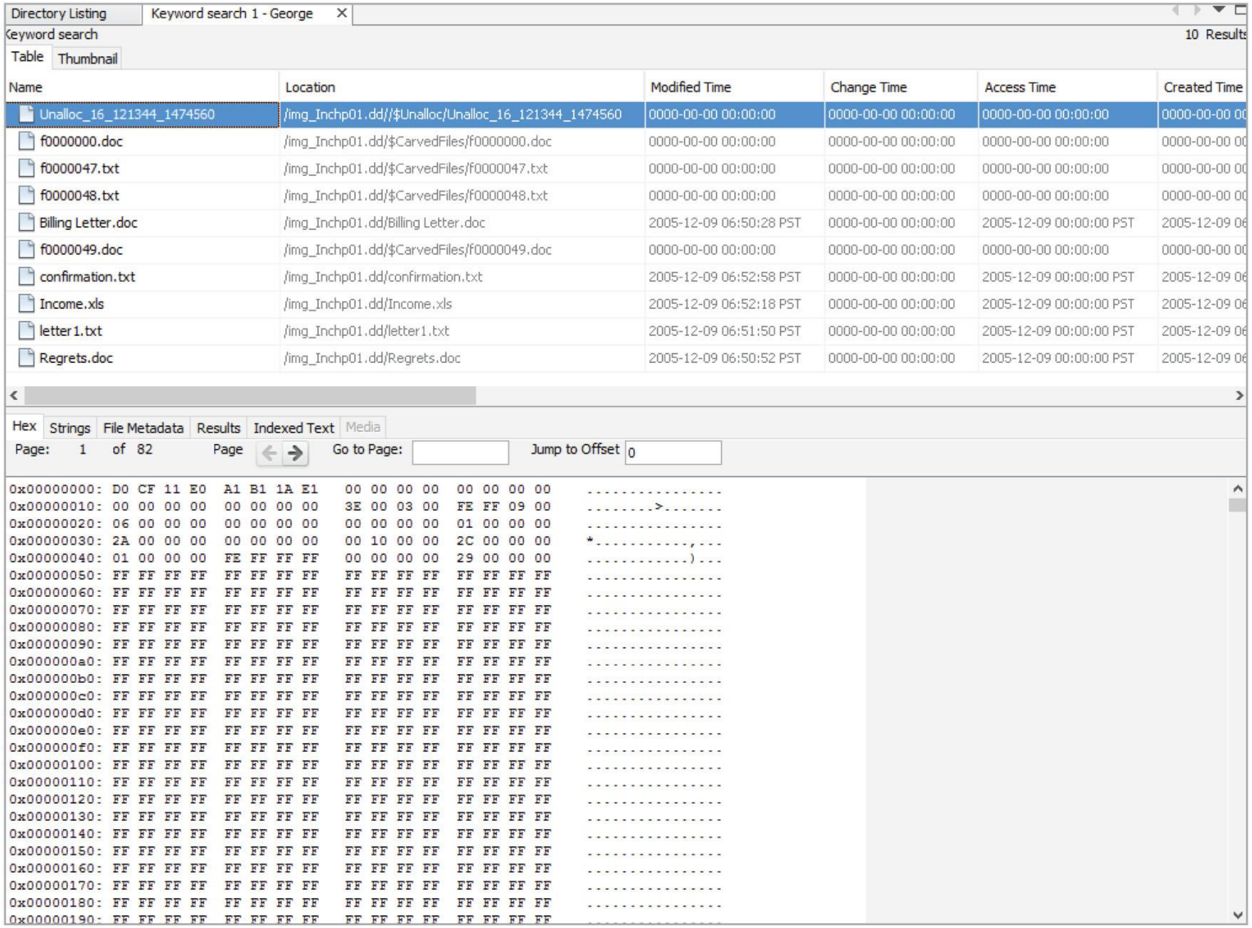
Name	Location	Modified Time	Change Time	Access Time
Unalloc_16_121344_1474560	/img_Inchp01.dd//$Unalloc/Unalloc_16_121344_1474560	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000000.doc	/img_Inchp01.dd/$CarvedFiles/f0000000.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000047.txt	/img_Inchp01.dd/$CarvedFiles/f0000047.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000048.txt	/img_Inchp01.dd/$CarvedFiles/f0000048.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Billing Letter.doc	/img_Inchp01.dd/Billing Letter.doc	2005-12-09 06:50:28 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
f0000049.doc	/img_Inchp01.dd/$CarvedFiles/f0000049.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
confirmation.txt	/img_Inchp01.dd/confirmation.txt	2005-12-09 06:52:58 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
Income.xls	/img_Inchp01.dd/Income.xls	2005-12-09 06:52:18 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
letter1.txt	/img_Inchp01.dd/letter1.txt	2005-12-09 06:51:50 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
Regrets.doc	/img_Inchp01.dd/Regrets.doc	2005-12-09 06:50:52 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST

```
f0000048.txt Earl,
We need to meet on the 18th of August to confirm the work I am
doing for you. Please contact me ASAP.

George


-----------------------------METADATA-----------------------------

Content-Encoding: windows-1252
Content-Type: text/plain; charset=windows-1252
```

Figure 1-19 Viewing the results of searching for the keyword "George"

Source: *www.sleuthkit.org*

Analyzing Your Digital Evidence (8 of 8)



Name	Location	Modified Time	Change Time	Access Time	Created Time
Unalloc_16_121344_1474560	/img_Inchp01.dd//$Unalloc/Unalloc_16_121344_1474560	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00
f0000000.doc	/img_Inchp01.dd/$CarvedFiles/f0000000.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00
f0000047.txt	/img_Inchp01.dd/$CarvedFiles/f0000047.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00
f0000048.txt	/img_Inchp01.dd/$CarvedFiles/f0000048.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00
Billing Letter.doc	/img_Inchp01.dd/Billing Letter.doc	2005-12-09 06:50:28 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06
f0000049.doc	/img_Inchp01.dd/$CarvedFiles/f0000049.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00
confirmation.txt	/img_Inchp01.dd/confirmation.txt	2005-12-09 06:52:58 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06
Income.xls	/img_Inchp01.dd/Income.xls	2005-12-09 06:52:18 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06
letter1.txt	/img_Inchp01.dd/letter1.txt	2005-12-09 06:51:50 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06
Regrets.doc	/img_Inchp01.dd/Regrets.doc	2005-12-09 06:50:52 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06

```
0x00000000: D0 CF 11 E0  A1 B1 1A E1  00 00 00 00  00 00 00 00   ................
0x00000010: 00 00 00 00  00 00 00 00  3E 00 03 00  FE FF 09 00   ........>.......
0x00000020: 06 00 00 00  00 00 00 00  00 00 00 00  01 00 00 00   ................
0x00000030: 2A 00 00 00  00 00 00 00  00 10 00 00  2C 00 00 00   *...........,...
0x00000040: 01 00 00 00  FE FF FF FF  00 00 00 00  29 00 00 00   ............)...
0x00000050: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000060: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000070: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000080: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000090: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x000000a0: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x000000b0: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x000000c0: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x000000d0: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x000000e0: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x000000f0: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000100: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000110: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000120: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000130: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000140: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000150: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000160: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000170: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000180: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
0x00000190: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF   ................
```

Figure 1-20 Viewing search results found in unallocated drive space

Source: *www.sleuthkit.org*

Completing the Case (1 of 2)

- You need to produce a final report
  - State what you did and what you found
- Include Autopsy report to document your work
- **Repeatable findings**
  - Repeat the steps and produce the same result
- If required, use a report template
- Report should show conclusive evidence
  - Suspect did or did not commit a crime or violate a company policy

Completing the Case (2 of 2)

- Keep a written journal of everything you do
  - Your notes can be used in court
- Answer the six Ws:
  - Who, what, when, where, why, and how
- You must also explain computer and network processes
- Autopsy Report Generator
  - Can generate reports in different styles: plain text, HTML and Excel

Critiquing the Case

- Ask yourself the following questions:
  - How could you improve your performance in the case?
  - Did you expect the results you found? Did the case develop in ways you did not expect?
  - Was the documentation as thorough as it could have been?
  - What feedback has been received from the requesting source?
  - Did you discover any new problems? If so, what are they?
  - Did you use new techniques during the case or during research?

Summary (1 of 3)

- Digital forensics involves systematically accumulating and analyzing digital information for use as evidence in civil, criminal, and administrative cases
- Investigators need specialized workstations to examine digital evidence
- Public-sector and private-sector investigations differ; public-sector typically require search warrants before seizing digital evidence

Summary (2 of 3)

- Always use a systematic approach to your investigations
- Always plan a case taking into account the nature of the case, case requirements, and gathering evidence techniques
- Both criminal cases and corporate-policy violations can go to court
- Plan for contingencies for any problems you might encounter
- Keep track of the chain of custody of your evidence

Summary (3 of 3)

- Internet abuse investigations require examining server log data
- For attorney-client privilege cases, all written communication should remain confidential
- A bit-stream copy is a bit-by-bit duplicate of the original disk
- Always maintain a journal to keep notes on exactly what you did
- You should always critique your own work