

# **Guide to Computer Forensics and Investigations Fourth Edition**

## *Chapter 5 Processing Crime and Incident Scenes*

# Objectives

- Explain the rules for digital evidence
- Describe how to collect evidence at private-sector incident scenes
- Explain guidelines for processing law enforcement crime scenes
- List the steps in preparing for an evidence search
- Describe how to secure a computer incident or crime scene

# Objectives (continued)

- Explain guidelines for seizing digital evidence at the scene
- List procedures for storing digital evidence
- Explain how to obtain a digital hash
- Review a case to identify requirements and plan your investigation

# Identifying Digital Evidence

- **Digital evidence**
  - Can be any information stored or transmitted in digital form
- U.S. courts accept digital evidence as physical evidence
  - Digital data is a tangible object
- Some require that all digital evidence be printed out to be presented in court

# Identifying Digital Evidence (continued)

- General tasks investigators perform when working with digital evidence:
  - Identify digital information or artifacts that can be used as evidence
  - Collect, preserve, and document evidence
  - Analyze, identify, and organize evidence
  - Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably
- Collecting computers and processing a criminal or incident scene must be done systematically

# Understanding Rules of Evidence

- Consistent practices help verify your work and enhance your credibility
- Comply with your state's rules of evidence or with the Federal Rules of Evidence
- Evidence admitted in a criminal case can be used in a civil suit, and vice versa
- Keep current on the latest rulings and directives on collecting, processing, storing, and admitting digital evidence

# Understanding Rules of Evidence (continued)

- Data you discover from a forensic examination falls under your state's rules of evidence
  - Or the Federal Rules of Evidence
- Digital evidence is unlike other physical evidence because it can be changed more easily
  - The only way to detect these changes is to compare the original data with a duplicate
- Most federal courts have interpreted computer records as hearsay evidence
  - Hearsay is secondhand or indirect evidence

# Understanding Rules of Evidence (continued)

- Business-record exception
  - Allows “records of regularly conducted activity,” such as business memos, reports, records, or data compilations
- Generally, computer records are considered admissible if they qualify as a business record
- Computer records are usually divided into:
  - **Computer-generated records**
  - **Computer-stored records**

# Understanding Rules of Evidence (continued)

- Computer records must be shown to be authentic and trustworthy
  - To be admitted into court
- Computer-generated records are considered authentic
  - If the program that created the output is functioning correctly
- Collecting evidence according to the proper steps of evidence control helps ensure that the computer evidence is authentic

# Understanding Rules of Evidence (continued)

- When attorneys challenge digital evidence
  - Often they raise the issue of whether computer-generated records were altered
    - Or damaged after they were created
- One test to prove that computer-stored records are authentic is to demonstrate that a specific person created the records
  - The author of a Microsoft Word document can be identified by using file metadata

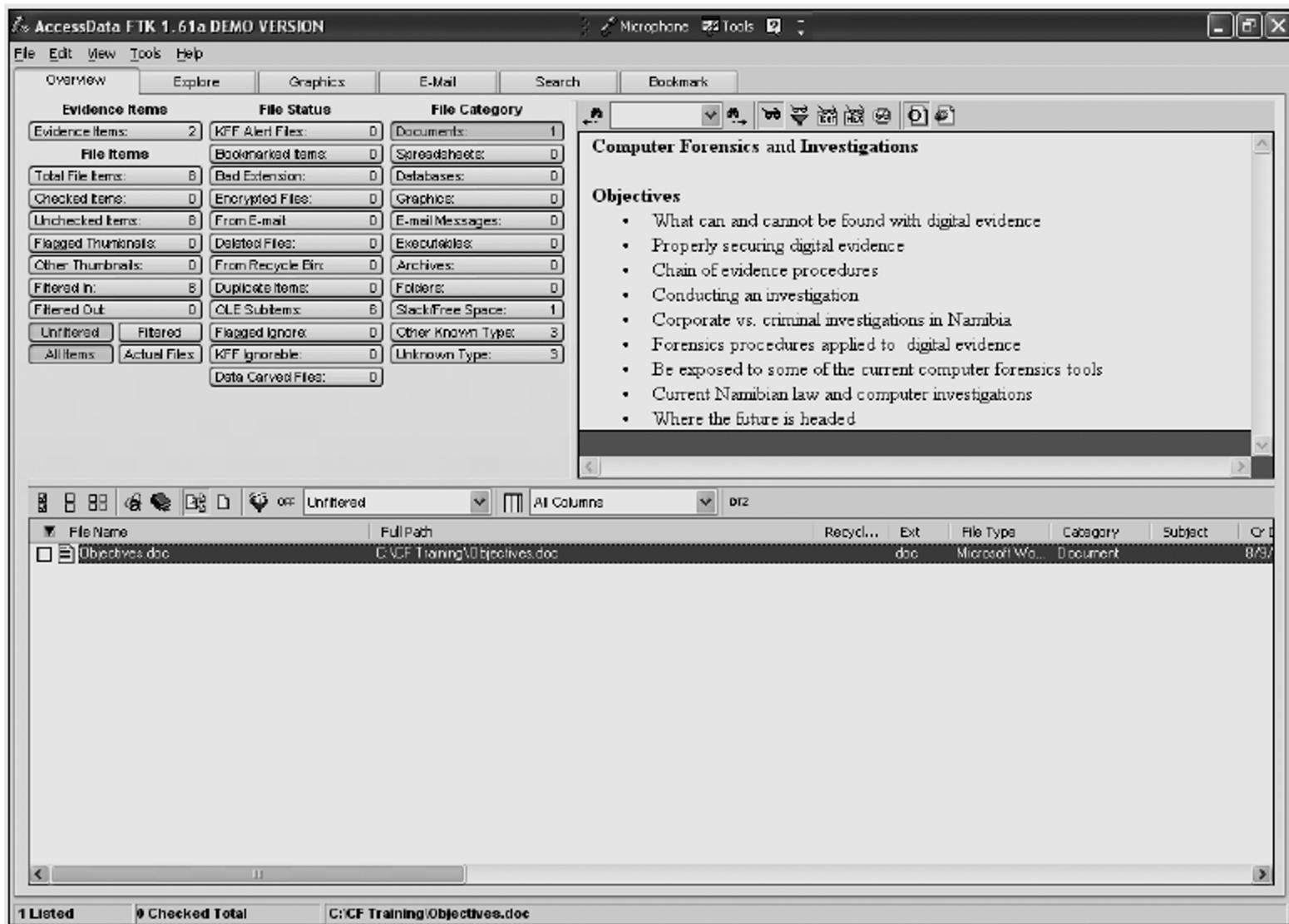


Figure 5-1 Selecting a document

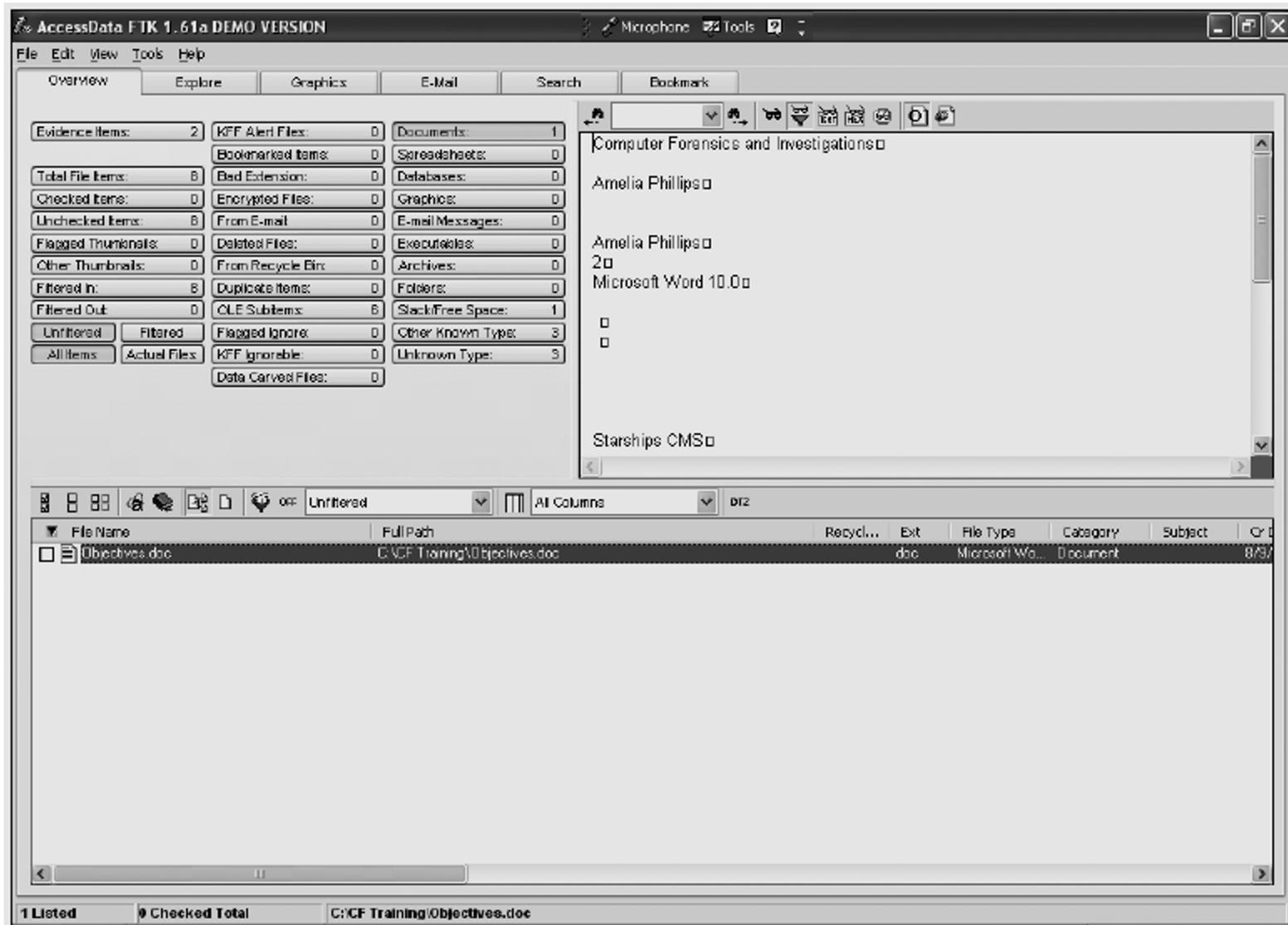


Figure 5-2 Viewing file metadata

# Understanding Rules of Evidence (continued)

- The process of establishing digital evidence's trustworthiness originated with written documents and the best evidence rule
- Best evidence rule states:
  - To prove the content of a written document, recording, or photograph, ordinarily the original writing, recording, or photograph is required
- Federal Rules of Evidence
  - Allow a duplicate instead of originals when it is produced by the same impression as the original

# Understanding Rules of Evidence (continued)

- As long as bit-stream copies of data are created and maintained properly
  - The copies can be admitted in court, although they aren't considered best evidence

# Collecting Evidence in Private-Sector Incident Scenes

- Private-sector organizations include:
  - Businesses and government agencies that aren't involved in law enforcement
- Agencies must comply with state public disclosure and federal Freedom of Information Act (FOIA) laws
  - And make certain documents available as public records
- FOIA allows citizens to request copies of public documents created by federal agencies

# Collecting Evidence in Private-Sector Incident Scenes (continued)

- A special category of private-sector businesses includes ISPs and other communication companies
- ISPs can investigate computer abuse committed by their employees, but not by customers
  - Except for activities that are deemed to create an emergency situation
- Investigating and controlling computer incident scenes in the corporate environment
  - Much easier than in the criminal environment
  - Incident scene is often a workplace

# Collecting Evidence in Private-Sector Incident Scenes (continued)

- Typically, businesses have inventory databases of computer hardware and software
  - Help identify the computer forensics tools needed to analyze a policy violation
    - And the best way to conduct the analysis
- Corporate policy statement about misuse of computing assets
  - Allows corporate investigators to conduct covert surveillance with little or no cause
  - And access company systems without a warrant

# Collecting Evidence in Private-Sector Incident Scenes (continued)

- Companies should display a warning banner or publish a policy
  - Stating that they reserve the right to inspect computing assets at will
- Corporate investigators should know under what circumstances they can examine an employee's computer
  - Every organization must have a well-defined process describing when an investigation can be initiated

# Collecting Evidence in Private-Sector Incident Scenes (continued)

- If a corporate investigator finds that an employee is committing or has committed a crime
  - Employer can file a criminal complaint with the police
- Employers are usually interested in enforcing company policy
  - Not seeking out and prosecuting employees
- Corporate investigators are, therefore, primarily concerned with protecting company assets

# Collecting Evidence in Private-Sector Incident Scenes (continued)

- If you discover evidence of a crime during a company policy investigation
  - Determine whether the incident meets the elements of criminal law
  - Inform management of the incident
  - Stop your investigation to make sure you don't violate Fourth Amendment restrictions on obtaining evidence
  - Work with the corporate attorney to write an affidavit confirming your findings

# Processing Law Enforcement Crime Scenes

- You must be familiar with criminal rules of search and seizure
- You should also understand how a search warrant works and what to do when you process one
- Law enforcement officer may search for and seize criminal evidence only with **probable cause**
  - Facts or circumstances that lead a reasonable person to believe a crime has been committed or is about to be committed

# Processing Law Enforcement Crime Scenes (continued)

- With probable cause, a police officer can obtain a search warrant from a judge
  - That authorizes a search and seizure of specific evidence related to the criminal complaint
- The Fourth Amendment states that only warrants “particularly describing the place to be searched, and the persons or things to be seized” can be issued

**Seize and examine, by persons qualified to do so, and in a laboratory setting, any and all electronic data processing and computer storage devices, including:** central processing units, internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, optical readers and scanning devices, CD Rom drives and Compact Disks and related hardware, digital cameras and digital storage media, operating logs, software and operating instructions or operating manuals, computer materials, software and programs used to communicate with other terminals via telephone or other means, and any computer modems, monitors, printers, etc., **that may have been used while engaging in [specify the illegal conduct], as defined in the Annotated Code of Maryland, amended and revised.**

**Figure 5-4** Sample search warrant wording for computer evidence

# Understanding Concepts and Terms Used in Warrants

- **Innocent information**
  - Unrelated information
  - Often included with the evidence you're trying to recover
- Judges often issue a **limiting phrase** to the warrant
  - Allows the police to separate innocent information from evidence

# Understanding Concepts and Terms Used in Warrants (continued)

- **Plain view doctrine**
  - Objects falling in plain view of an officer who has the right to be in position to have that view
    - Are subject to seizure without a warrant and may be introduced in evidence
- “Knock and announce”
  - With few exceptions, warrants require that officers knock and announce their identity
    - When executing a warrant

# Preparing for a Search

- Preparing for a computer search and seizure
  - Probably the most important step in computing investigations
- To perform these tasks
  - You might need to get answers from the victim and an informant
    - Who could be a police detective assigned to the case, a law enforcement witness, or a manager or coworker of the **person of interest** to the investigation

# Identifying the Nature of the Case

- When you're assigned a computing investigation case
  - Start by identifying the nature of the case
    - Including whether it involves the private or public sector
- The nature of the case dictates how you proceed
  - And what types of assets or resources you need to use in the investigation

# Identifying the Type of Computing System

- For law enforcement
  - This step might be difficult because the crime scene isn't controlled
- If you can identify the computing system
  - Estimate the size of the drive on the suspect's computer
    - And how many computers to process at the scene
- Determine which OSs and hardware are involved

# Determining Whether You Can Seize a Computer

- The type of case and location of the evidence
  - Determine whether you can remove computers
- Law enforcement investigators need a warrant to remove computers from a crime scene
  - And transport them to a lab
- If removing the computers will irreparably harm a business
  - The computers should not be taken offsite

# Determining Whether You Can Seize a Computer (continued)

- An additional complication is files stored offsite that are accessed remotely
- If you aren't allowed to take the computers to your lab
  - Determine the resources you need to acquire digital evidence and which tools can speed data acquisition

# Obtaining a Detailed Description of the Location

- Get as much information as you can
- Identify potential hazards
  - Interact with your HAZMAT team
- HAZMAT guidelines
  - Put the target drive in a special HAZMAT bag
  - HAZMAT technician can decontaminate the bag
  - Check for high temperatures

# Determining Who Is in Charge

- Corporate computing investigations
  - Require only one person to respond
- Law enforcement agencies
  - Handle large-scale investigations
  - Designate lead investigators

# Using Additional Technical Expertise

- Look for specialists
  - OSs
  - RAID servers
  - Databases
- Finding the right person can be a challenge
- Educate specialists in investigative techniques
  - Prevent evidence damage

# Determining the Tools You Need

- Prepare tools using incident and crime scene information
- Initial-response field kit
  - Lightweight
  - Easy to transport
- Extensive-response field kit
  - Includes all tools you can afford



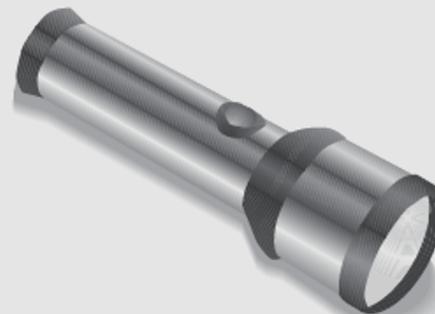
Computer forensics kit



Laptop computer



Digital camera



Flashlight

Figure 5-5 Items in an initial-response field kit

**Table 5-1** Tools in an initial-response field kit

<b>Number needed</b>	<b>Tools</b>
1	Small computer toolkit
1	Large-capacity drive
1	IDE ribbon cable (ATA-33 or ATA-100)
1	SATA cable
1	Forensic boot media containing your preferred acquisition utility
1	Laptop IDE 40- to 44-pin adapter, other adapter cables
1	Laptop computer
1	FireWire or USB dual write-protect external bay
1	Flashlight
1	Digital or 35mm camera with film and flash
10	Evidence log forms
1	Notebook or dictation recorder
10	Computer evidence bags (antistatic bags)
20	Evidence labels, tape, and tags
1	Permanent ink marker
10	External USB devices, such as a thumb drive, or a larger portable hard drive

**Table 5-2** Tools in an extensive-response field kit

<b>Number needed</b>	<b>Tools</b>
Varies	Assorted technical manuals, ranging from OS references to forensic analysis guides
1	Initial-response field kit
1	Portable PC with SCSI card for DLT tape drive or suspect's SCSI drive
2	Electrical power strips
1	Additional hand tools, including bolt cutters, pry bar, and hacksaw
1	Leather gloves and disposable latex gloves (assorted sizes)
1	Hand truck and luggage cart
10	Large garbage bags and large cardboard boxes with packaging tape
1	Rubber bands of assorted sizes
1	Magnifying glass
1	Ream of printer paper
1	Small brush for cleaning dust from suspect's interior CPU cabinet
10	USB thumb drives of varying sizes
2	External hard drives (200 GB or larger) with power cables
Assorted	Converter cables
5	Additional assorted hard drives for data acquisition

# Preparing the Investigation Team

- Review facts, plans, and objectives with the investigation team you have assembled
- Goals of scene processing
  - Collect evidence
  - Secure evidence
- Slow response can cause digital evidence to be lost

# Securing a Computer Incident or Crime Scene

- Goals
  - Preserve the evidence
  - Keep information confidential
- Define a secure perimeter
  - Use yellow barrier tape
  - Legal authority
- Professional curiosity can destroy evidence
  - Involves police officers and other professionals who aren't part of the crime scene processing team

# Seizing Digital Evidence at the Scene

- Law enforcement can seize evidence
  - With a proper warrant
- Corporate investigators rarely can seize evidence
- When seizing computer evidence in criminal investigations
  - Follow U.S. DoJ standards for seizing digital data
- Civil investigations follow same rules
  - Require less documentation though
- Consult with your attorney for extra guidelines

# Preparing to Acquire Digital Evidence

- The evidence you acquire at the scene depends on the nature of the case
  - And the alleged crime or violation
- Ask your supervisor or senior forensics examiner in your organization the following questions:
  - Do you need to take the entire computer and all peripherals and media in the immediate area?
  - How are you going to protect the computer and media while transporting them to your lab?
  - Is the computer powered on when you arrive?

# Preparing to Acquire Digital Evidence (continued)

- Ask your supervisor or senior forensics examiner in your organization the following questions (continued):
  - Is the suspect you're investigating in the immediate area of the computer?
  - Is it possible the suspect damaged or destroyed the computer, peripherals, or media?
  - Will you have to separate the suspect from the computer?

# Processing an Incident or Crime Scene

- Guidelines
  - Keep a journal to document your activities
  - Secure the scene
    - Be professional and courteous with onlookers
    - Remove people who are not part of the investigation
  - Take video and still recordings of the area around the computer
    - Pay attention to details
  - Sketch the incident or crime scene
  - Check computers as soon as possible

# Processing an Incident or Crime Scene (continued)

- Guidelines (continued)
  - Don't cut electrical power to a running system unless it's an older Windows 9x or MS-DOS system
  - Save data from current applications as safely as possible
  - Record all active windows or shell sessions
  - Make notes of everything you do when copying data from a live suspect computer
  - Close applications and shut down the computer

# Processing an Incident or Crime Scene (continued)

- Guidelines (continued)
  - Bag and tag the evidence, following these steps:
    - Assign one person to collect and log all evidence
    - Tag all evidence you collect with the current date and time, serial numbers or unique features, make and model, and the name of the person who collected it
    - Maintain two separate logs of collected evidence
    - Maintain constant control of the collected evidence and the crime or incident scene

# Processing an Incident or Crime Scene (continued)

- Guidelines (continued)
  - Look for information related to the investigation
    - Passwords, passphrases, PINs, bank accounts
  - Collect documentation and media related to the investigation
    - Hardware, software, backup media, documentation, manuals

# Processing Data Centers with RAID Systems

- Sparse acquisition
  - Technique for extracting evidence from large systems
  - Extracts only data related to evidence for your case from allocated files
    - And minimizes how much data you need to analyze
- Drawback of this technique
  - It doesn't recover data in free or slack space

# Using a Technical Advisor

- Technical advisor
  - Can help you list the tools you need to process the incident or crime scene
  - Person guiding you about where to locate data and helping you extract log records
    - Or other evidence from large RAID servers
  - Can help create the search warrant by itemizing what you need for the warrant

# Using a Technical Advisor (continued)

- Responsibilities
  - Know aspects of the seized system
  - Direct investigator handling sensitive material
  - Help secure the scene
  - Help document the planning strategy
  - Conduct ad hoc trainings
  - Document activities

# Documenting Evidence in the Lab

- Record your activities and findings as you work
  - Maintain a journal to record the steps you take as you process evidence
- Goal is to be able to reproduce the same results
  - When you or another investigator repeat the steps you took to collect evidence
- A journal serves as a reference that documents the methods you used to process digital evidence

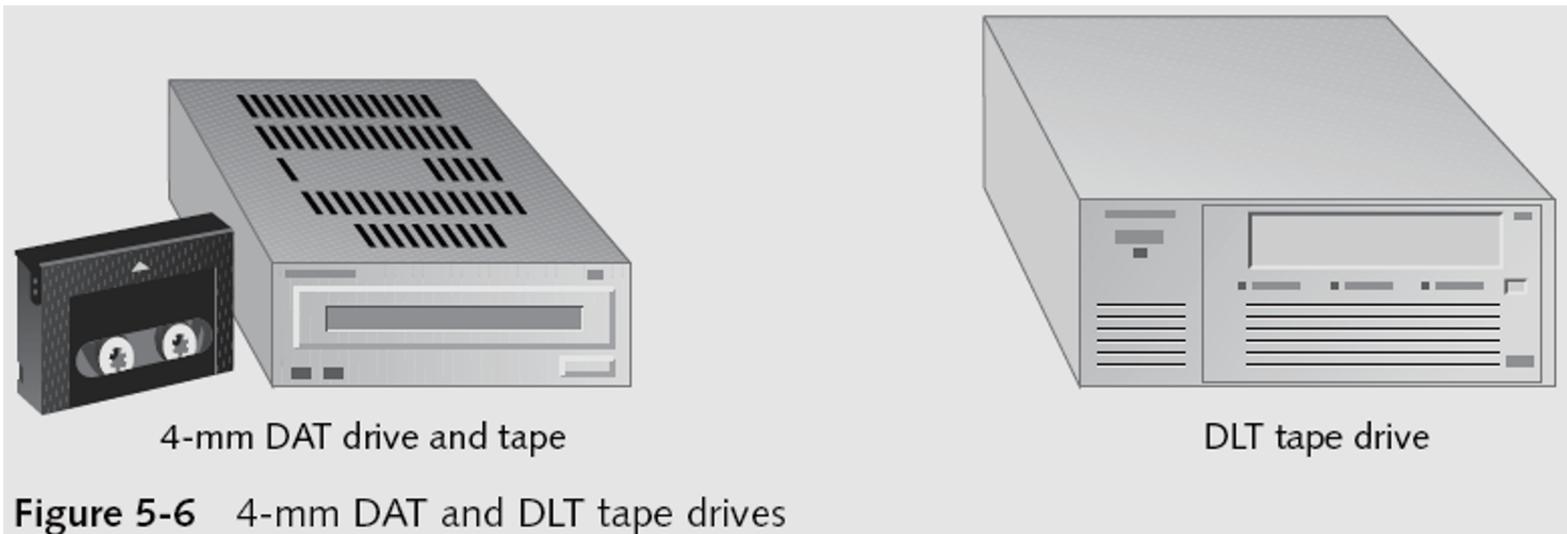
# Processing and Handling Digital Evidence

- Maintain the integrity of digital evidence in the lab
  - As you do when collecting it in the field
- Steps to create image files:
  - Copy all image files to a large drive
  - Start your forensics tool to analyze the evidence
  - Run an MD5 or SHA-1 hashing algorithm on the image files to get a digital hash
  - Secure the original media in an evidence locker

# Storing Digital Evidence

- The media you use to store digital evidence usually depends on how long you need to keep it
- CD-Rs or DVDs
  - The ideal media
  - Capacity: up to 17 GB
  - Lifespan: 2 to 5 years
- Magnetic tapes
  - Capacity: 40 to 72 GB
  - Lifespan: 30 years
  - Costs: drive: \$400 to \$800; tape: \$40

# Storing Digital Evidence (continued)



# Evidence Retention and Media Storage Needs

- To help maintain the chain of custody for digital evidence
  - Restrict access to lab and evidence storage area
- Lab should have a sign-in roster for all visitors
  - Maintain logs for a period based on legal requirements
- You might need to retain evidence indefinitely
  - Check with your local prosecuting attorney's office or state laws to make sure you're in compliance

# Evidence Retention and Media Storage Needs (continued)

Item description:				
Item tag number:				
Person	Date logged out	Time logged out	Date logged in	Time logged in

Figure 5-7 A sample log file

# Documenting Evidence

- Create or use an evidence custody form
- An evidence custody form serves the following functions:
  - Identifies the evidence
  - Identifies who has handled the evidence
  - Lists dates and times the evidence was handled
- You can add more information to your form
  - Such as a section listing MD5 and SHA-1 hash values

# Documenting Evidence (continued)

- Include any detailed information you might need to reference
- Evidence bags also include labels or evidence forms you can use to document your evidence

# Obtaining a Digital Hash

- **Cyclic Redundancy Check (CRC)**
  - Mathematical algorithm that determines whether a file's contents have changed
  - Most recent version is CRC-32
  - Not considered a forensic hashing algorithm
- **Message Digest 5 (MD5)**
  - Mathematical formula that translates a file into a hexadecimal code value, or a hash value
  - If a bit or byte in the file changes, it alters the **digital hash**

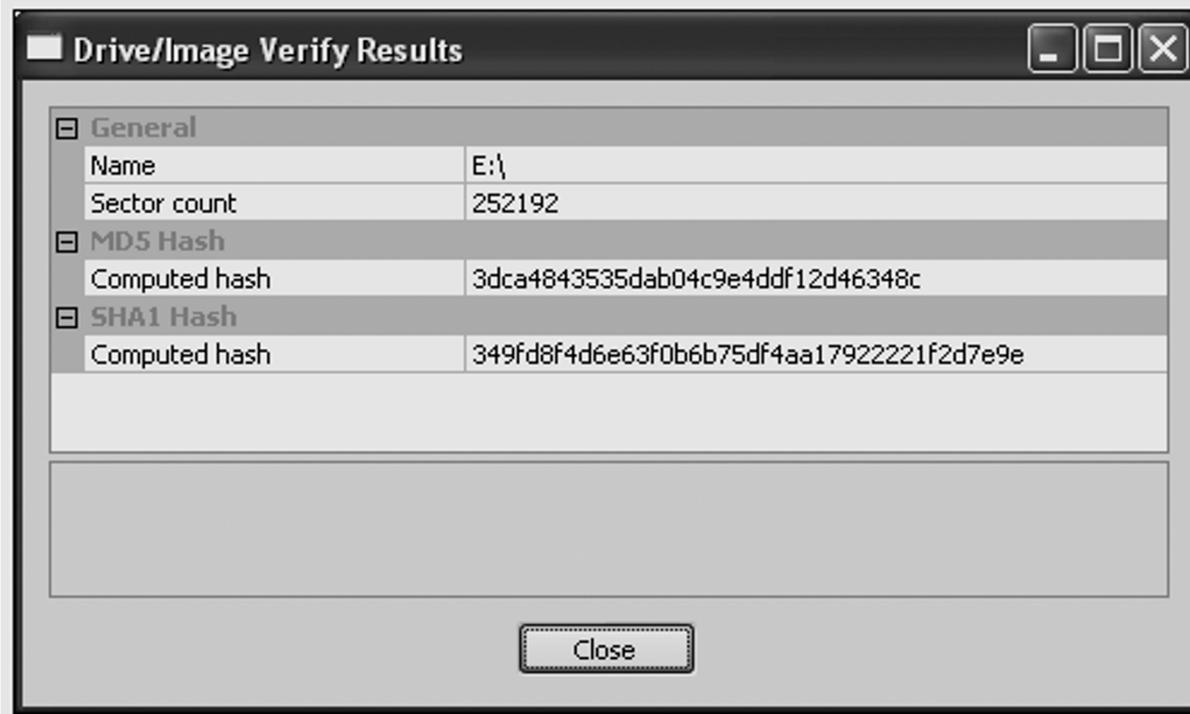
# Obtaining a Digital Hash (continued)

- Three rules for forensic hashes:
  - You can't predict the hash value of a file or device
  - No two hash values can be the same
  - If anything changes in the file or device, the hash value must change
- **Secure Hash Algorithm version 1 (SHA-1)**
  - A newer hashing algorithm
  - Developed by the **National Institute of Standards and Technology (NIST)**

# Obtaining a Digital Hash (continued)

- In both MD5 and SHA-1, collisions have occurred
- Most computer forensics hashing needs can be satisfied with a **nonkeyed hash set**
  - A unique hash number generated by a software tool, such as the Linux md5sum command
- **Keyed hash set**
  - Created by an encryption utility's secret key
- You can use the MD5 function in FTK Imager to obtain the digital signature of a file
  - Or an entire drive

# Obtaining a Digital Hash (continued)



**Figure 5-8** Using FTK Imager to verify hash values

# Reviewing a Case

- General tasks you perform in any computer forensics case:
  - Identify the case requirements
  - Plan your investigation
  - Conduct the investigation
  - Complete the case report
  - Critique the case

# Sample Civil Investigation

- Most cases in the corporate environment are considered **low-level investigations**
  - Or noncriminal cases
- Common activities and practices
  - Recover specific evidence
    - Suspect's Outlook e-mail folder (PST file)
  - Covert surveillance
    - Its use must be well defined in the company policy
    - Risk of civil or criminal liability
  - **Sniffing** tools for data transmissions

# Sample Criminal Investigation

- Computer crimes examples
  - Fraud
  - Check fraud
  - Homicides
- Need a warrant to start seizing evidence
  - Limit searching area

# Sample Criminal Investigation (continued)

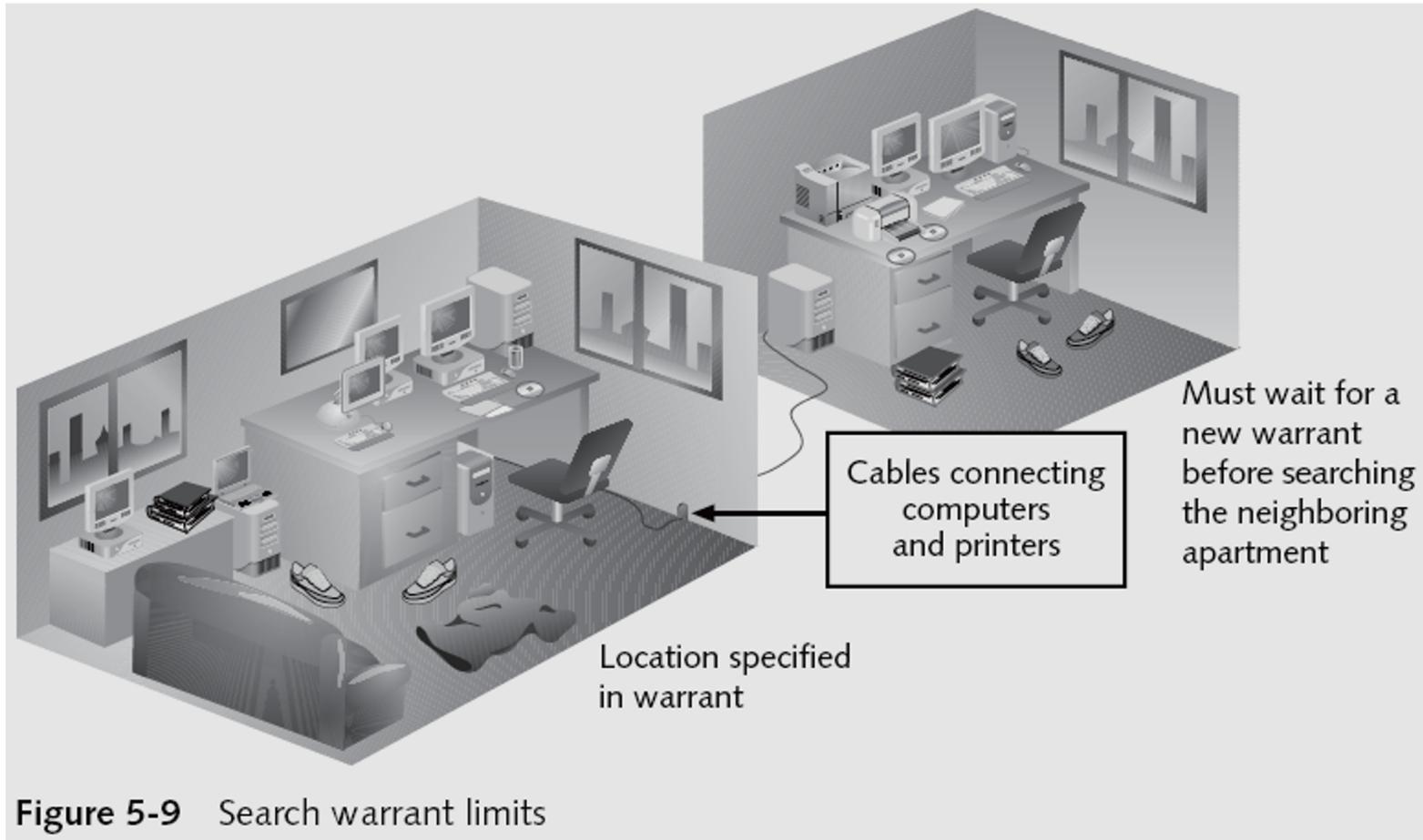


Figure 5-9 Search warrant limits

# Reviewing Background Information for a Case

- Company called Superior Bicycles
  - Specializes in creating new and inventive modes of human-driven transportation
- Two employees, Chris Murphy and Nau Tjeriko, have been missing for several days
- A USB thumb drive has been recovered from Chris's office with evidence that he had been conducting a side business using company computers

# Identifying the Case Requirements

- Identify requirements such as:
  - Nature of the case
  - Suspect's name
  - Suspect's activity
  - Suspect's hardware and software specifications

# Planning Your Investigation

- List what you can assume or know
  - Several incidents may or may not be related
  - Suspect's computer can contain information about the case
  - If someone else has used suspect's computer
- Make an image of suspect's computer disk drive
- Analyze forensics copy

# Conducting the Investigation: Acquiring Evidence with AccessData FTK

- Functions
  - Extract the image from a bit-stream image file
  - Analyze the image

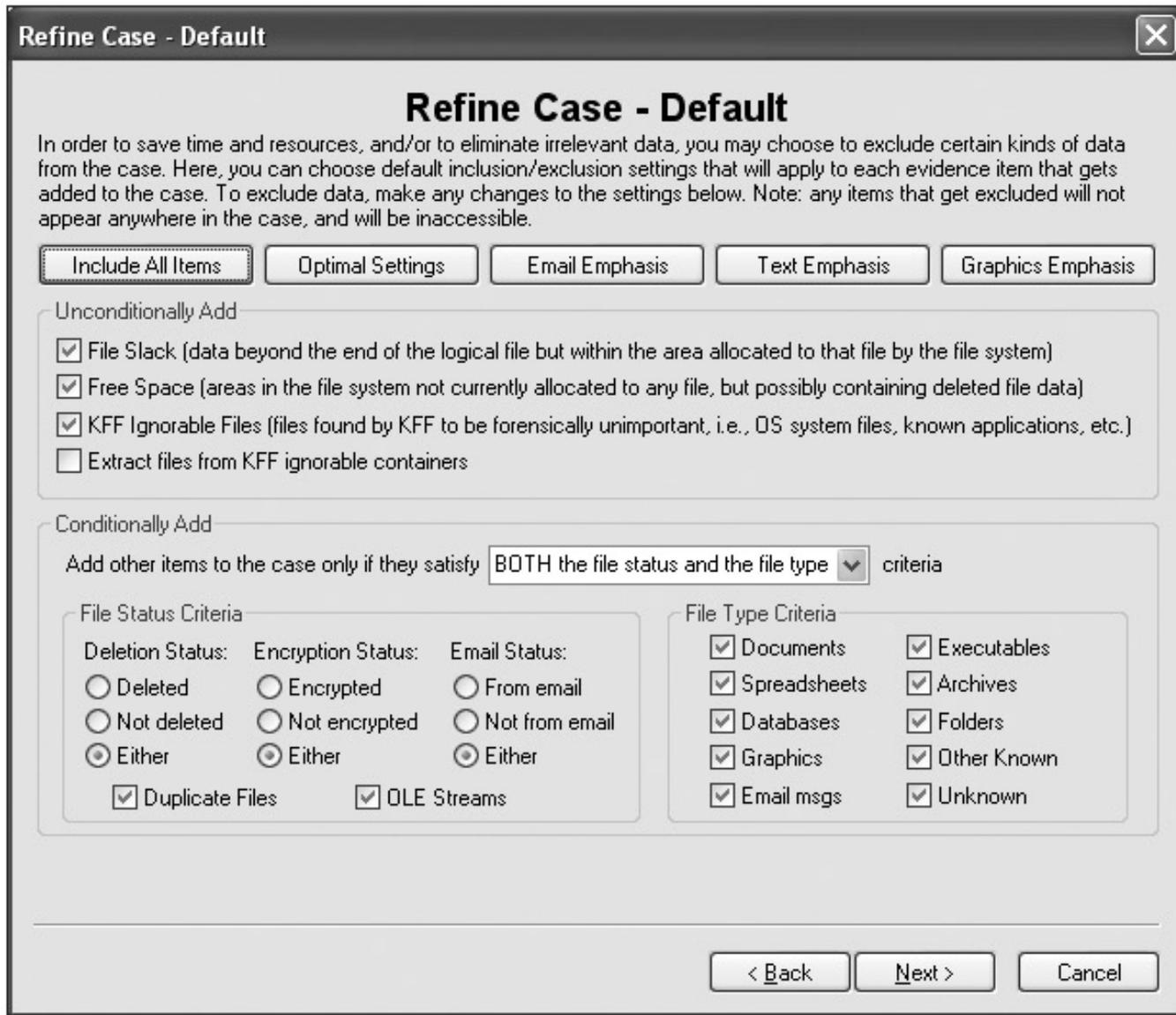
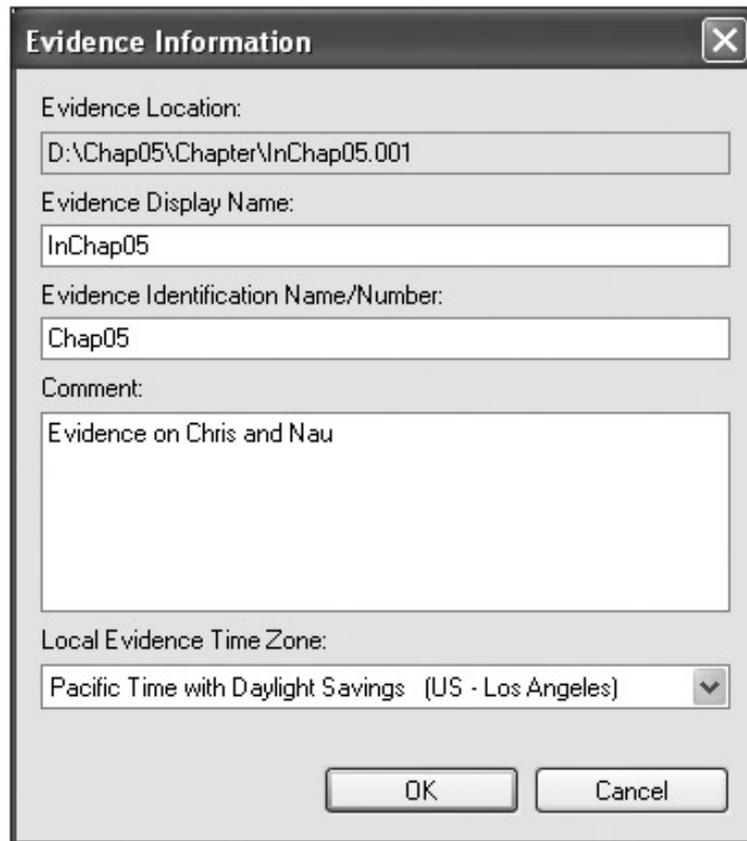
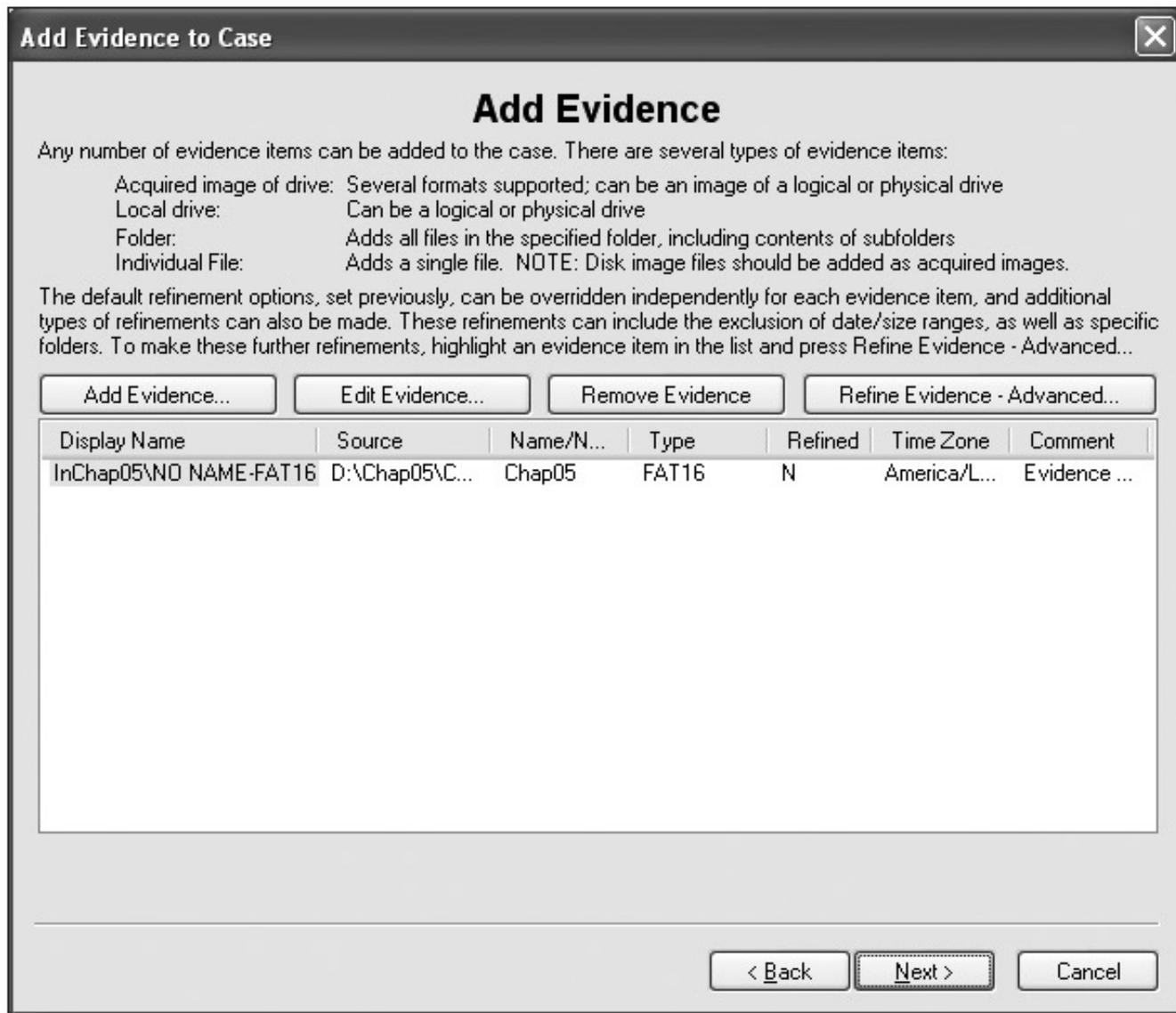


Figure 5-10 The Refine Case - Default dialog box

# Conducting the Investigation: Acquiring Evidence with AccessData FTK (continued)



**Figure 5-11** The Evidence Information dialog box



**Figure 5-12** The Add Evidence to Case dialog box with image file listed

Guide to Computer Forensics and Investigations

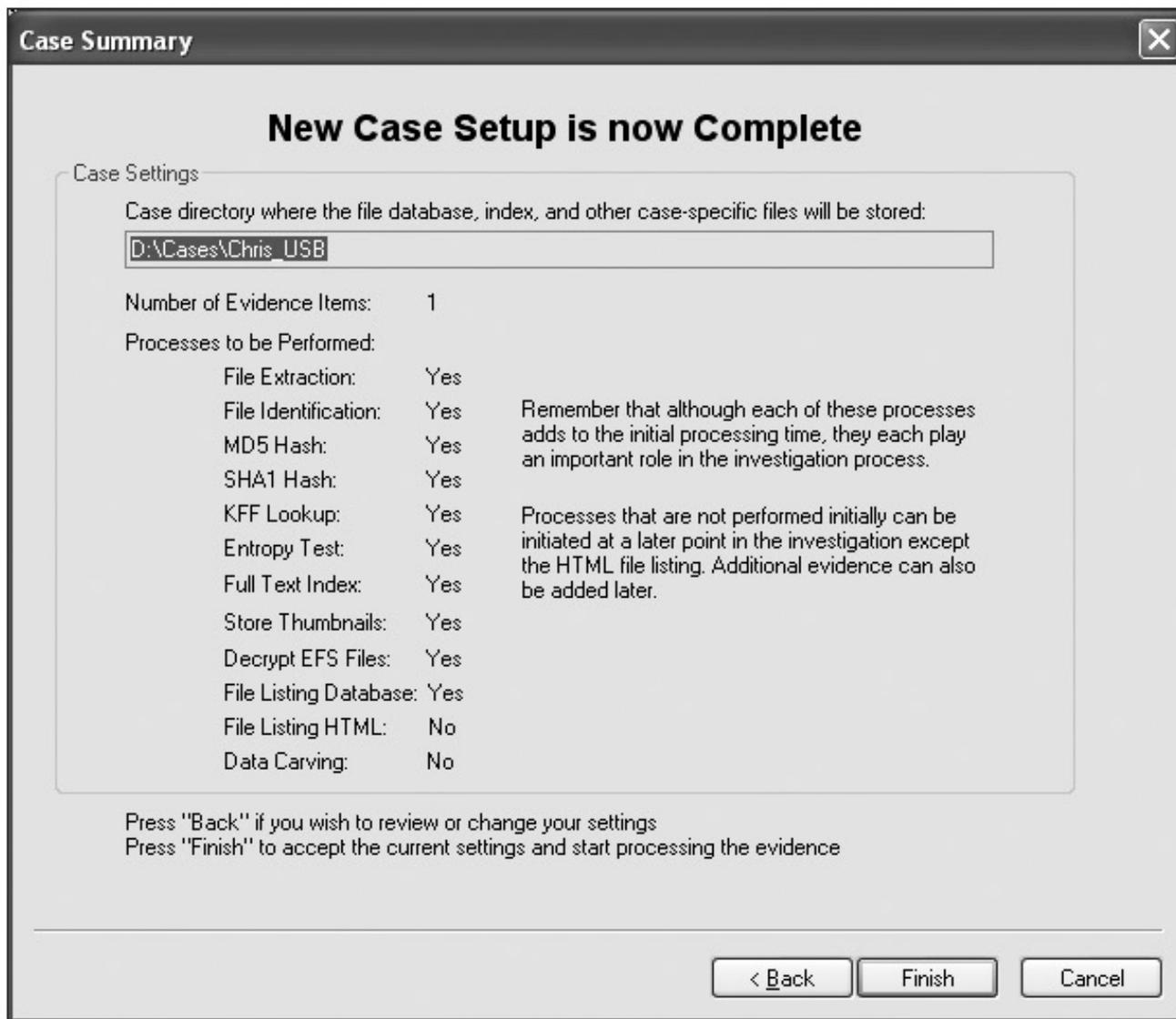
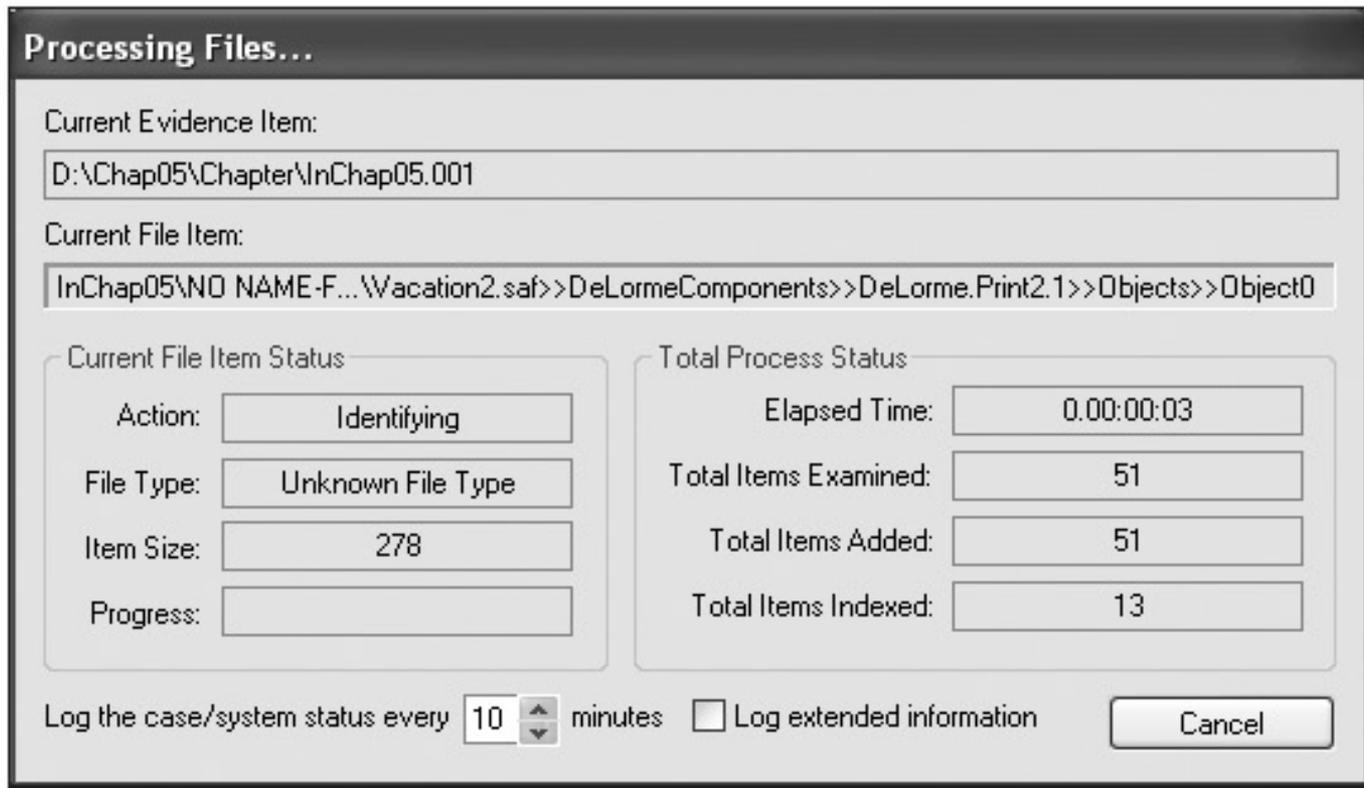


Figure 5-13 The Case Summary dialog box

# Conducting the Investigation: Acquiring Evidence with AccessData FTK (continued)



**Figure 5-14** The Processing Files dialog box

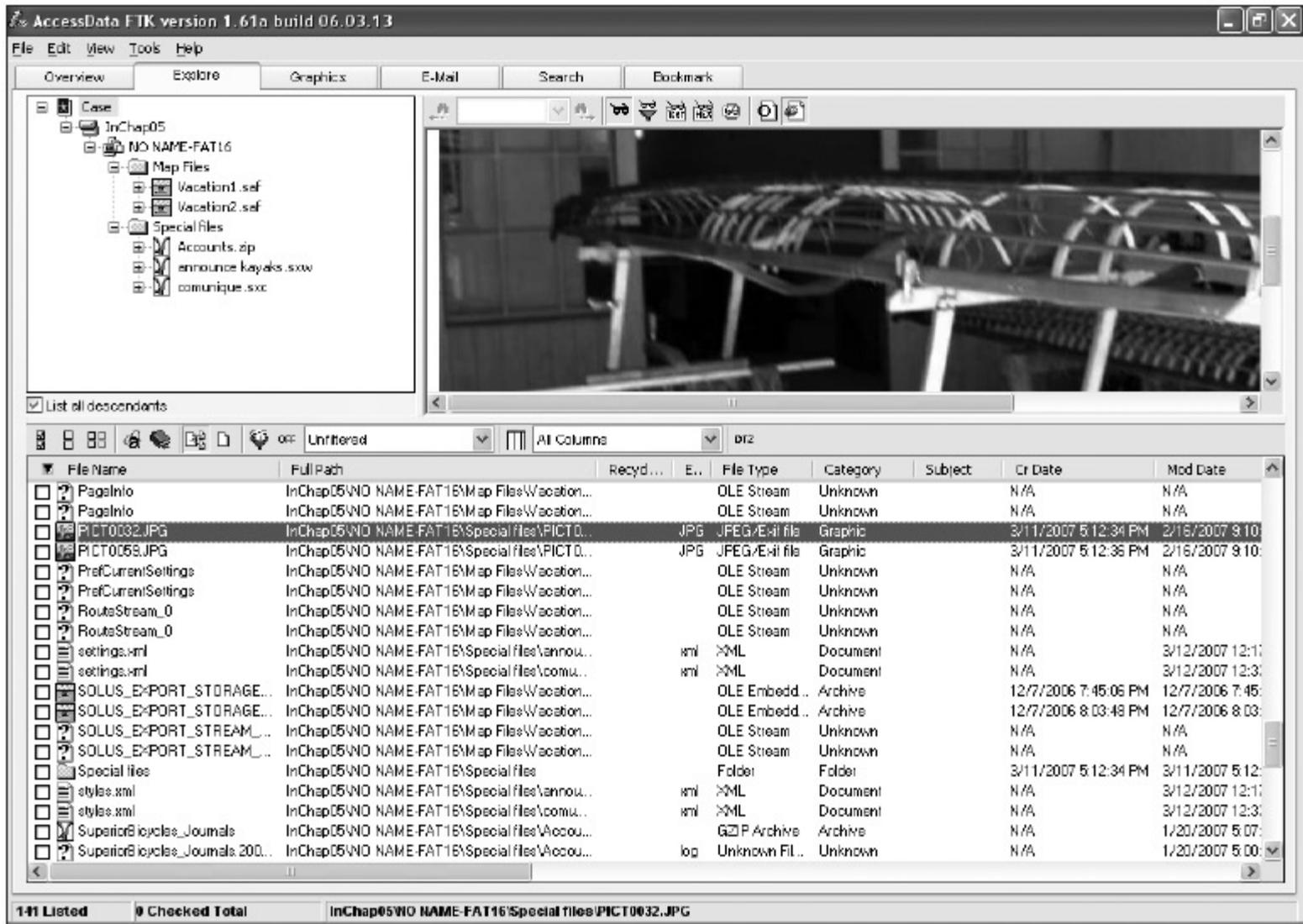


Figure 5-15 Selecting files of interest

# Conducting the Investigation: Acquiring Evidence with AccessData FTK (continued)

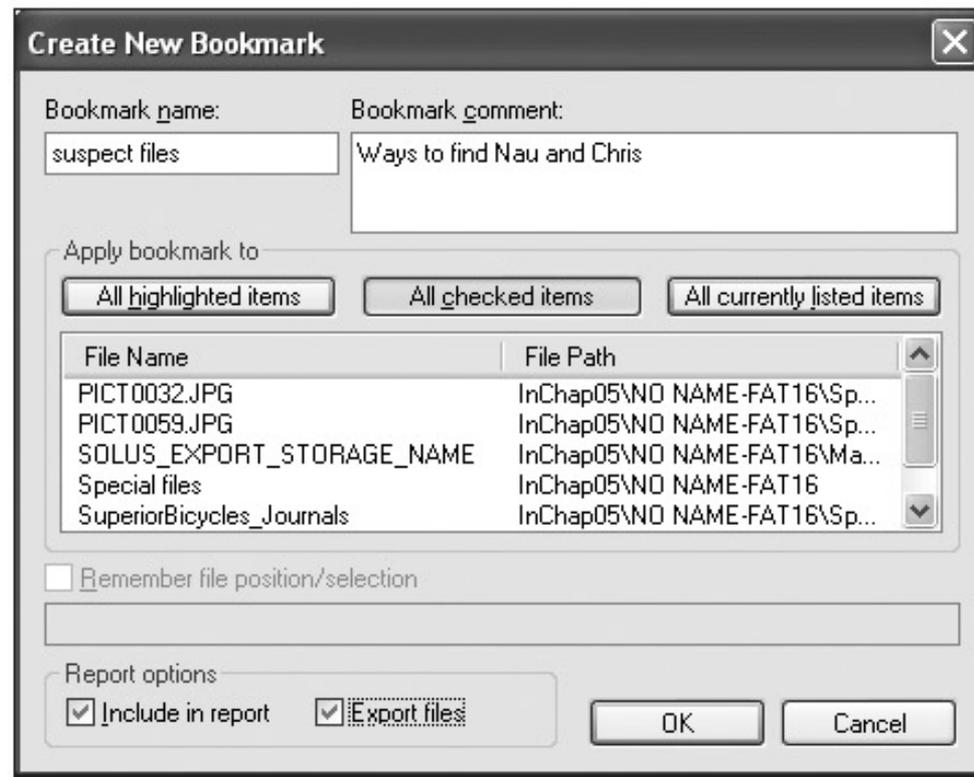


Figure 5-16 The Create New Bookmark dialog box

# Summary

- Digital evidence is anything stored or transmitted on electronic or optical media
- Private sector
  - Contained and controlled area
- Publish right to inspect computer assets policy
- Private and public sectors follow same computing investigation rules
- Criminal cases
  - Require warrants

# Summary (continued)

- Protect your safety and health as well as the integrity of the evidence
- Follow guidelines when processing an incident or crime scene
  - Security perimeter
  - Video recording
- As you collect digital evidence, guard against physically destroying or contaminating it
- Forensic hash values verify that data or storage media have not been altered

# Summary (continued)

- To analyze computer forensics data, learn to use more than one vendor tool
- You must handle all evidence the same way every time you handle it
- After you determine that an incident scene has digital evidence, identify the digital information or artifacts that can be used as evidence