Digital Forensic Investigation

Lecture 9

Malware Analysis and Digital Investigation

Objective

- Student will be able to :-
  - Understand the general Overview of Digital Forensic Investigation
  - Explain the important procedure in each of Digital Investigation Process
  - Identify the evidence in a digital incidents
  - Identify the suitable tools in gathering and analysing digital evidence
  - Demonstrate the ability to write a report in presenting digital evidence

Introduction

Overview Of Computer Forensics

- **Computer forensics**
  - Involves obtaining and analyzing digital information
    - As evidence in civil, criminal, or administrative cases
- FBI Computer Analysis and Response Team (CART)
  - Formed in 1984 to handle the increasing number of cases involving digital evidence
- In Malaysia
  - Digital forensics cases is handle by department of forensic (DFD) of CyberSecurity Malaysia
  - DFD has been providing digital forensics services to Law Enforcement Agency (LEA) and Regulatory Bodies(RBs) since 2005. As the vision of DFD in the Tenth Malaysia Plan is to continually become the National Centre of Reference and Excellence in Digital Forensics, DFD has strived to offer a quality service that continually meets the international standard, American Society of Crime Lab Directors Standard to the stakeholders.

Overview Of Computer Forensics (continued)

http://www.cybersecurity.my/en/services/digital_forensics/about/main/detail/14/index.html

Computer Forensics Versus Other Related Disciplines

- Computer forensics
  - Investigates data that can be retrieved from a computer's hard disk or other storage media
- Network forensics
  - Yields information about how a perpetrator or an attacker gained access to a network
- **Data recovery**
  - Recovering information that was deleted by mistake
    - Or lost during a power surge or server crash
  - Typically you know what you're looking for

Computer Forensics Versus Other Related Disciplines (continued)

- Computer forensics
  - Task of recovering data that users have hidden or deleted and using it as evidence
  - Evidence can be **inculpatory** (“incriminating”) or **exculpatory** (“innocence”)
- **Disaster recovery**
  - Uses computer forensics techniques to retrieve information their clients have lost
- Investigators often work as a team to make computers and networks secure in an organization

Computer Forensics Versus Other Related Disciplines (continued)

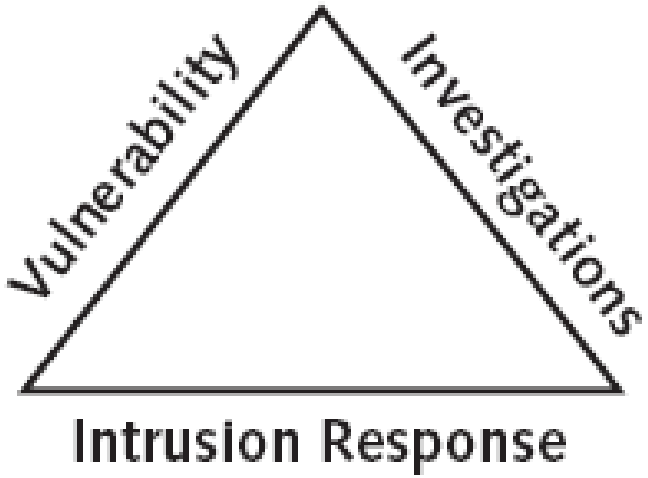


Figure 1-2 The investigations triad

Stage of Forensic Investigation in Tracking Computer Crime

- Identifying the crime
- Gathering the evidence
- Analyzing the evidence – use duplicate one
- Presenting the evidence
- Testifying
- Prosecution
  - In this stage, computer forensics investigator must act as an expert witness

Rules Of Computer Forensics

- Minimize the option of examining the original evidence
- Obey rules of evidence
- Never exceed the knowledge base
- Document any changes in evidence
- Handle evidence with care
- Always prepare chain of custody
- Do not tamper with the evidence

Computer Forensics Methodologies

The 3 A's

- ***Acquire*** evidence without modification or corruption
- ***Authenticate*** that the recovered evidence is same as the originally seized data
- ***Analyze*** data without any alterations

Identifying the crime

- Detecting/identifying the event/crime.
- Asses the case, ask people questions, and documenting the results in an effort to identify the crime and the location of the evidence

Preparing For Computer Investigations

- Computer investigations and forensics falls into two distinct categories
  - Public investigations
  - Private or corporate investigations
- Public investigations
  - Involve government agencies responsible for criminal investigations and prosecution
  - Organizations must observe legal guidelines
- Law of **search and seizure**
  - Protects rights of all people, including suspects

Preparing for Computer Investigations (continued)

- Private or corporate investigations
  - Deal with private companies, non-law-enforcement government agencies, and lawyers
  - Aren't governed directly by **criminal law** or Fourth Amendment issues
  - Governed by internal policies that define expected employee behavior and conduct in the workplace
- Private corporate investigations also involve litigation disputes
- Investigations are usually conducted in civil cases

Understanding Law Enforcements Agency Investigations

- In a **criminal case**, a suspect is tried for a criminal offense
  - Such as burglary, murder, or molestation
- Computers and networks are only tools that can be used to commit crimes
  - Many states have added specific language to criminal codes to define crimes involving computers
- Following the legal process
  - Legal processes depend on local custom, legislative standards, and rules of evidence

Understanding Corporate Investigations

- Private or corporate investigations
  - Involve private companies and lawyers who address company policy violations and litigation disputes
- Corporate computer crimes can involve:
  - E-mail harassment
  - Falsification of data
  - Gender and age discrimination
  - Embezzlement
  - Sabotage
  - **Industrial espionage**

Gathering the evidence

Identifying Digital Evidence

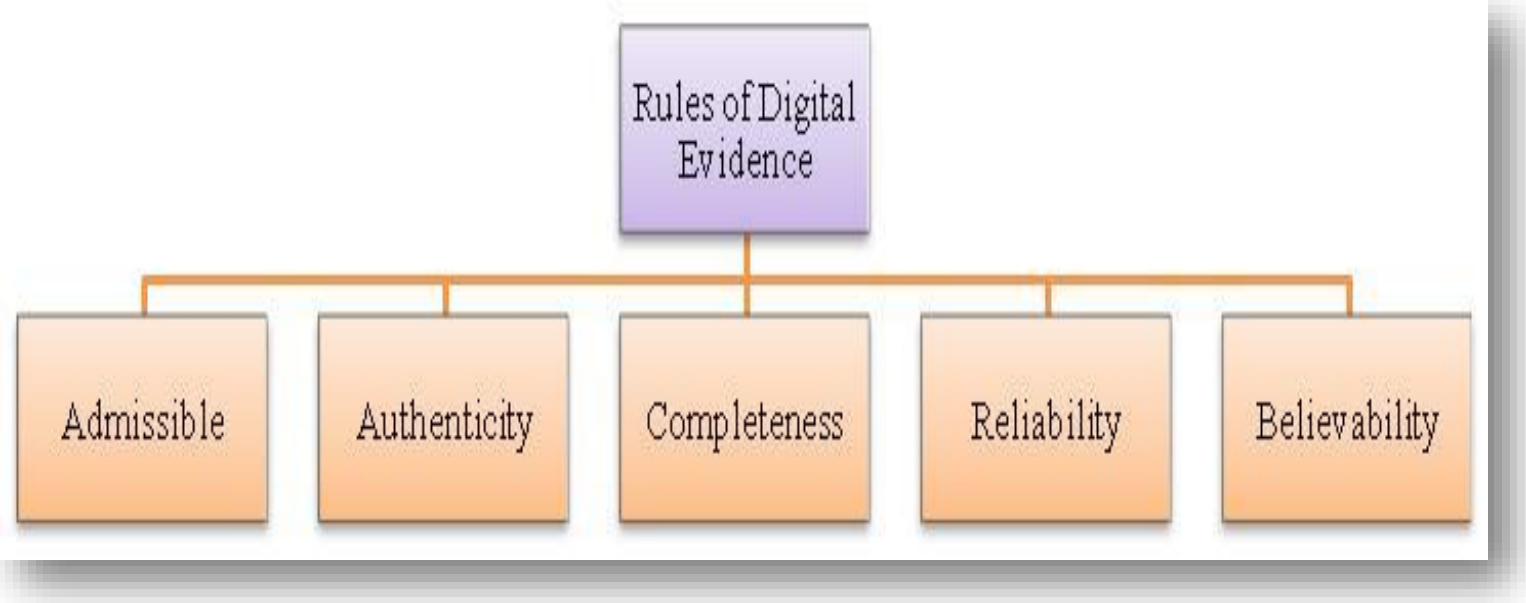
- **Digital evidence**
  - Can be any information stored or transmitted in digital form
- U.S. courts accept digital evidence as physical evidence
  - Digital data is a tangible object
- Some require that all digital evidence be printed out to be presented in court

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

Rules of Evidence

- Any data or information that is stored or transmitted in digital form can be accepted as digital evidence in a court of law if it passes the test of admissibility and weight which is known as digital evidence criteria discussed in Sommer (1999) and Kozushko (2003).



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

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

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

Number needed	Tools
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

Number needed	Tools
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

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)

4-mm DAT drive and tape

DLT tape drive

Figure 5-6 4-mm DAT and DLT tape drives

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)

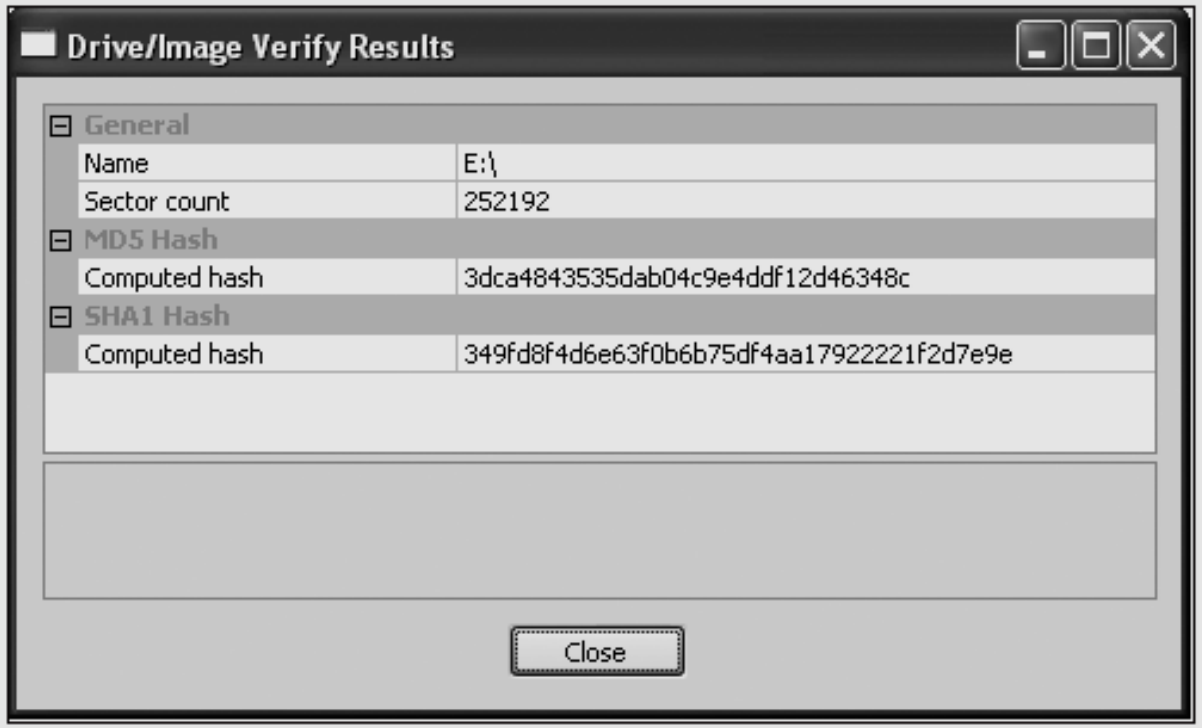


Figure 5-8 Using FTK Imager to verify hash values

Analyzing the evidence

Determining the Best Acquisition Method

- Types of acquisitions
  - **Static acquisitions** and **live acquisitions**
  - ***Static acquisition*** is the method used for retrieval of nonvolatile data. This type of acquisition is used to recover forensic data from hard drives, USB thumb drives, diskettes and discs.
  - ***Live acquisition*** is the examination of a system while it is running. Volatile computer forensic data is collected from RAM and during the live acquisition phase of the investigation.
- Four methods of acquisition
  - Bit-stream disk-to-image file
  - Bit-stream disk-to-disk
  - Logical disk-to-disk or disk-to-disk data
  - Sparse data copy of a file or folder

Determining the Best Acquisition Method (continued)

- Bit-stream disk-to-image file
  - Most common method
  - Can make more than one copy
  - Copies are bit-for-bit replications of the original drive
  - ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLook
- Bit-stream disk-to-disk
  - When disk-to-image copy is not possible
  - Consider disk's geometry configuration
  - EnCase, SafeBack, SnapCopy

Determining the Best Acquisition Method (continued)

- Logical acquisition or sparse acquisition
  - When your time is limited
  - Logical acquisition captures only specific files of interest to the case
  - Sparse acquisition also collects fragments of unallocated (deleted) data
  - For large disks
  - PST or OST mail files, RAID servers

Determining the Best Acquisition Method (continued)

- When making a copy, consider:
  - Size of the source disk
    - Lossless compression might be useful
    - Use digital signatures for verification
  - When working with large drives, an alternative is using tape backup systems
  - Whether you can retain the disk
  - Time allocation
  - Where the data/evidence is located

consideration to be taken in order to determine the data acquisition method

Contingency Planning for Image Acquisitions

- Create a duplicate copy of your evidence image file
- Make at least two images of digital evidence
  - Use different tools or techniques
- Copy host protected area of a disk drive as well
  - Consider using a hardware acquisition tool that can access the drive at the BIOS level
- Be prepared to deal with encrypted drives
  - **Whole disk encryption** feature in Windows Vista Ultimate and Enterprise editions

Using Acquisition Tools

- Acquisition tools for Windows
  - Advantages
    - Make acquiring evidence from a suspect drive more convenient
      - Especially when used with hot-swappable devices
  - Disadvantages
    - Must protect acquired data with a well-tested write-blocking hardware device
    - Tools can’t acquire data from a disk’s host protected area

- Data acquisition methods
  - Disk-to-image file
  - Disk-to-disk copy
  - Logical disk-to-disk or disk-to-data file
  - Sparse data copy
- Several tools available
  - Lossless compression is acceptable
- Plan your digital evidence contingencies
- Write-blocking devices or utilities must be used with GUI acquisition tools

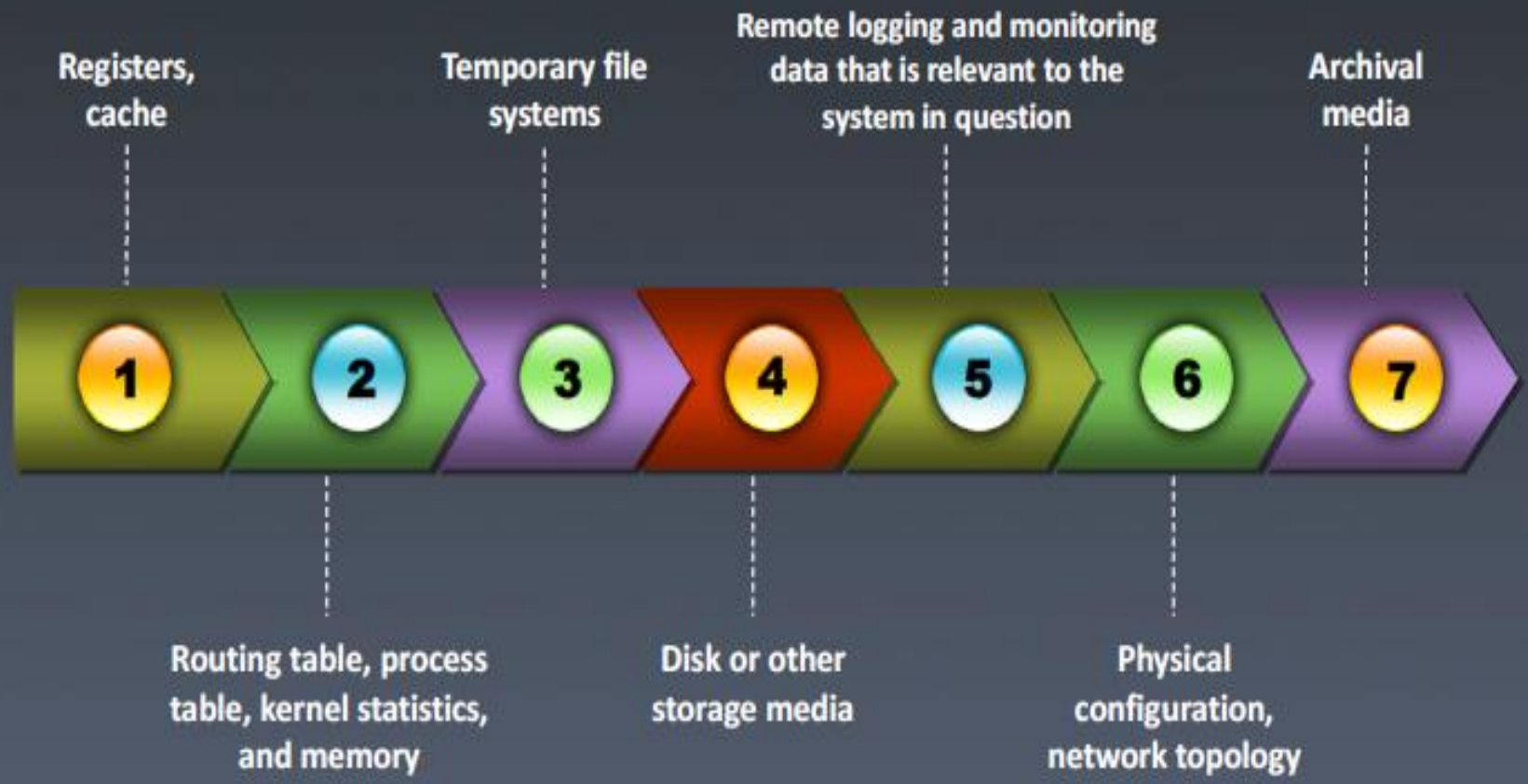
- Always validate acquisition
- A Linux Live CD, such as Helix, provides many useful tools for computer forensics acquisitions
- Preferred Linux acquisition tool is dcfldd (not dd)
- Use a physical write-blocker device for acquisitions
- To acquire RAID disks, determine the type of RAID
  - And then which acquisition tool to use

Determining What Data to Collect and Analyze

- Examining and analyzing digital evidence depends on:
  - Nature of the case
  - Amount of data to process
  - Search warrants and court orders
  - Company policies
- **Scope creep**
  - Investigation expands beyond the original description
- Right of full discovery of digital evidence

Order of Volatility

- When collecting evidence, the collection should proceed from the most volatile to the least volatile
- The list below is the order of volatility for a typical system:



Dealing with Powered On Computers (Cont'd)

The first step to take when approaching an active, powered on, and running computer is:

- Stop and Think
- Collect the RAM information of a running computer, which is occasionally vital in the case

- For example, data found on the hard disk may be encrypted, but the same data might be found in an unencrypted state in RAM, or a running process is to be identified and examined before power is removed
- All this kind of vital information in RAM will be lost when the computer is shut down or the power supply is removed to the device

Dealing with Powered On Computers

- If a computer is switched on and the screen is viewable:
  - Record the programs running on screen
  - Photograph the screen

- If a computer is on and the monitor shows some picture or screen saver:
  - Move the mouse slowly without depressing any mouse button
  - Take a photograph of the screen and record the information displayed

- If a monitor is powered on and the display is blank:
  - Move the mouse slowly without depressing any mouse button
  - Take a photograph

Dealing with Powered Off Computers

1. If computer is switched off – leave it off

2. If only monitor is switched off and the display is blank:
   - Turn the monitor on, move the mouse slightly, observe the changes from a blank screen to another screen and note the changes
   - Photograph the screen

3. If only monitor is switched off and the display is blank:
   - Turn the monitor on, move the mouse slightly
   - If the screen does not change, do not perform any other keystroke
   - Photograph the screen

Dealing with Networked Computer

Unplug the network cable from the router and modem

If computer is off, leave it off and if it is on, photograph the screen

If the computer is on and the screen is blank, move the mouse slowly and take a photograph of the screen

Label all the connected devices and cords for later identification

Unplug all the cords and devices connected to the computer

Dealing with Open Files and Startup Files

Malware attacks on the computer system create some files in the startup folder to run the malware program

1. Open the recently created document from startup or system32 folder for Window and rc.local file for Linux

2. Note down the date and time of the files

Procedures to find the evidence

4. Search for unusual MAC times on vital folders and startup files

3. Examine the open file for sensitive data such as password, image etc.

Approaching Computer Forensics Cases

- Some basic principles apply to almost all computer forensics cases
  - The approach you take depends largely on the specific type of case you're investigating
- Basic steps for all computer forensics investigations
  - For target drives, use only recently wiped media that have been reformatted
    - And inspected for computer viruses

Approaching Computer Forensics Cases (continued)

- Basic steps for all computer forensics investigations (continued)
  - Inventory the hardware on the suspect's computer and note the condition of the computer when seized
  - Remove the original drive from the computer
    - Check date and time values in the system's CMOS
  - Record how you acquired data from the suspect drive
  - Process the data methodically and logically

Approaching Computer Forensics Cases (continued)

- Basic steps for all computer forensics investigations (continued)
  - List all folders and files on the image or drive
  - If possible, examine the contents of all data files in all folders
    - Starting at the root directory of the volume partition
  - For all password-protected files that might be related to the investigation
    - Make your best effort to recover file contents

Approaching Computer Forensics Cases (continued)

- Basic steps for all computer forensics investigations (continued)
  - Identify the function of every executable (binary or .exe) file that doesn't match known hash values
  - Maintain control of all evidence and findings, and document everything as you progress through your examination

Refining and Modifying the Investigation Plan

- Considerations
  - Determine the scope of the investigation
  - Determine what the case requires
  - Whether you should collect all information
  - What to do in case of scope creep
- The key is to start with a plan but remain flexible in the face of new evidence

Using AccessData Forensic Toolkit to Analyze Data

- Supported file systems: FAT12/16/32, NTFS, Ext2fs, and Ext3fs
- FTK can analyze data from several sources, including image files from other vendors
- FTK produces a case log file
- Searching for keywords
  - Indexed search
  - Live search
  - Supports options and advanced searching techniques, such as stemming

Using AccessData Forensic Toolkit to Analyze Data (continued)

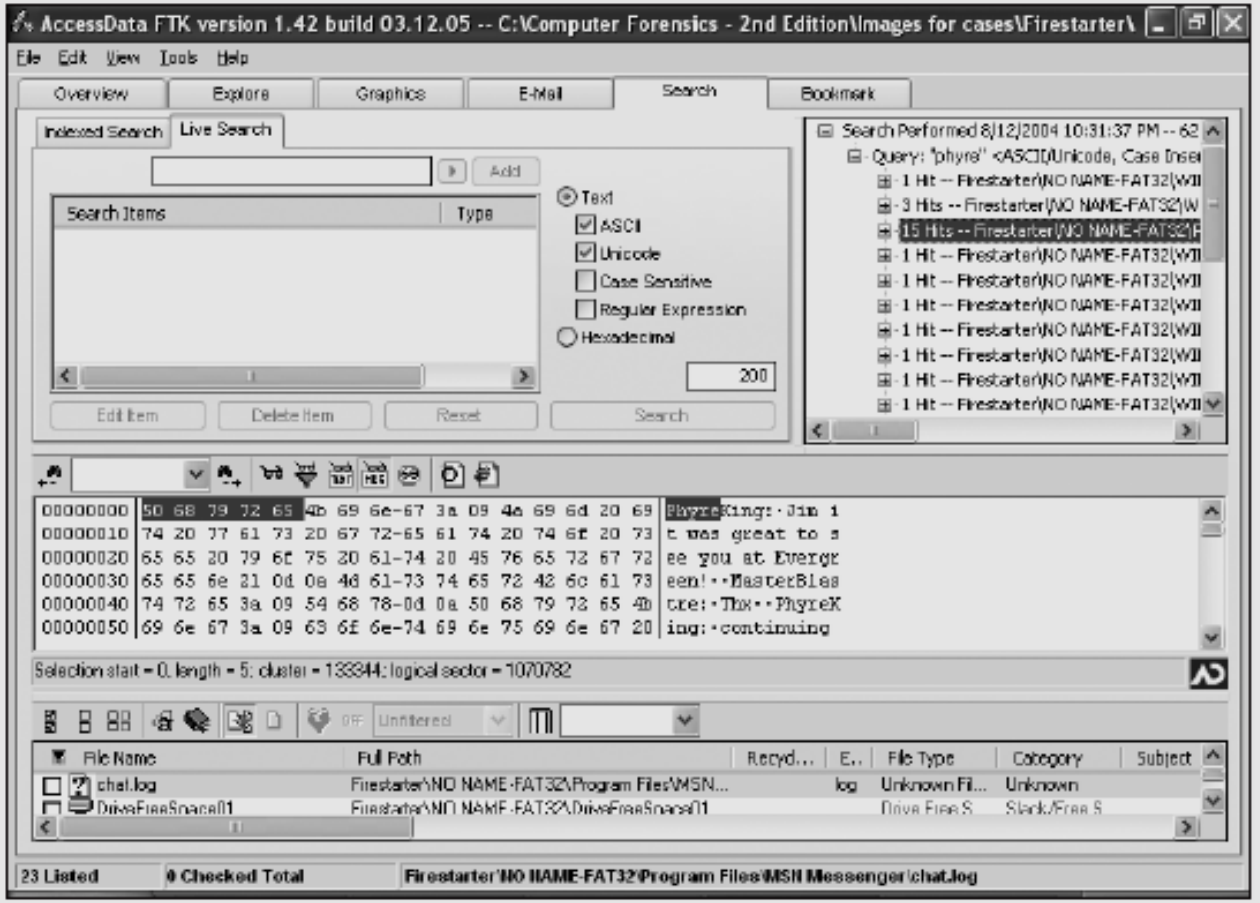


Figure 9-1 Viewing live search results in FTK

Using AccessData Forensic Toolkit to Analyze Data (continued)

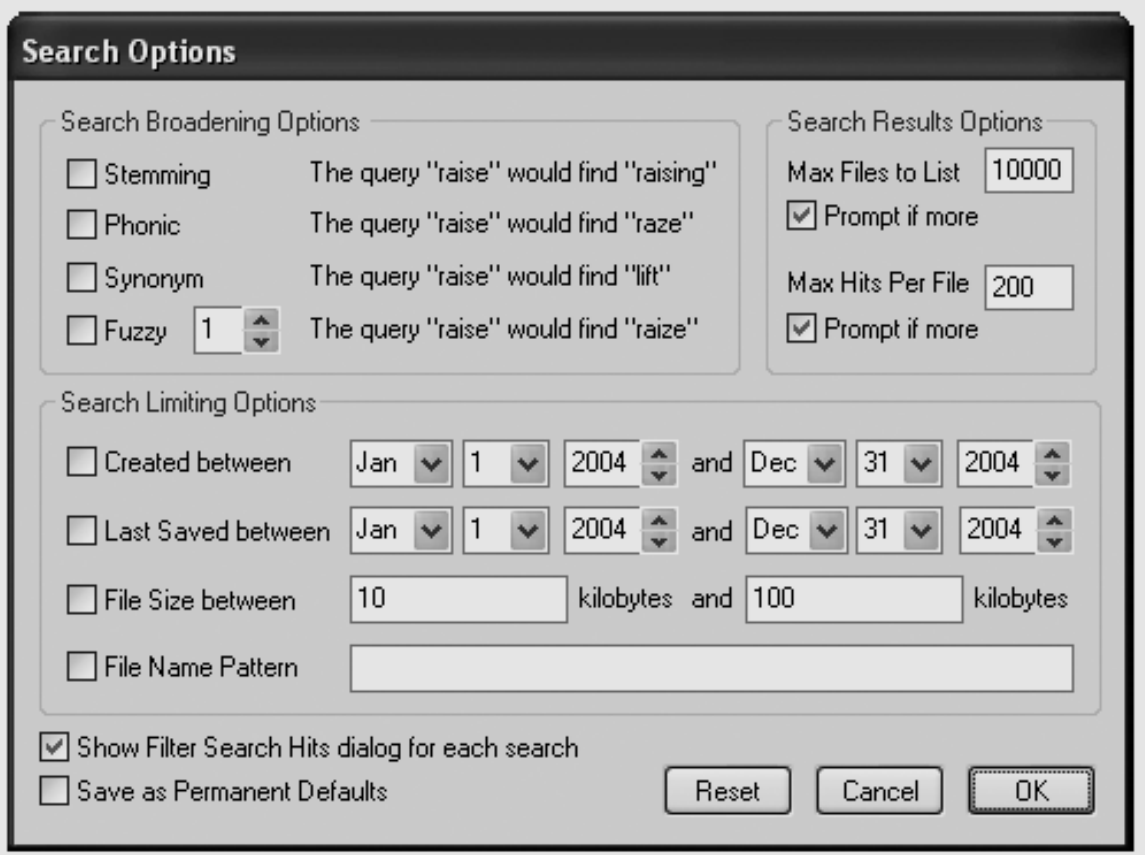


Figure 9-2 Selecting search options in FTK

Using AccessData Forensic Toolkit to Analyze Data (continued)

- Analyzes compressed files
- You can generate reports
  - Using bookmarks

Using AccessData Forensic Toolkit to Analyze Data (continued)

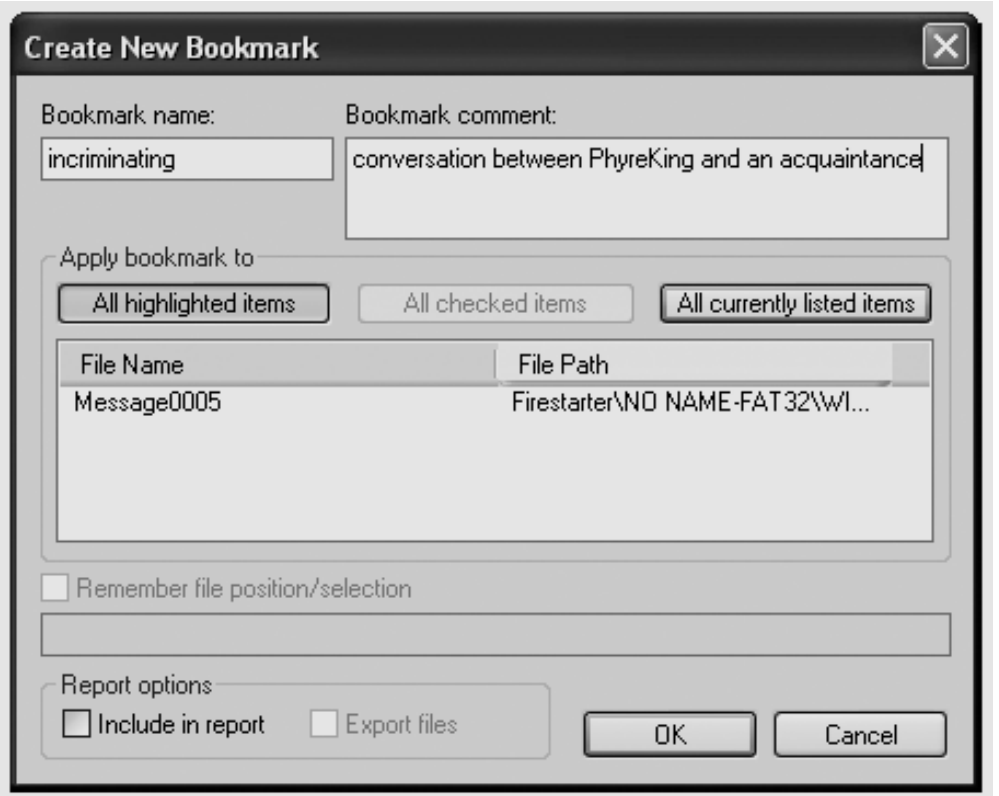


Figure 9-3 Creating a bookmark

Validating Forensic Data

- One of the most critical aspects of computer forensics
- Ensuring the integrity of data you collect is essential for presenting evidence in court
- Most computer forensic tools provide automated hashing of image files
- Computer forensics tools have some limitations in performing hashing
  - Learning how to use advanced hexadecimal editors is necessary to ensure data integrity

Validating with Hexadecimal Editors

- Advanced hexadecimal editors offer many features not available in computer forensics tools
  - Such as hashing specific files or sectors
- Hex Workshop provides several hashing algorithms
  - Such as MD5 and SHA-1
  - See Figures 9-4 through 9-6
- Hex Workshop also generates the hash value of selected data sets in a file or sector

Validating with Hexadecimal Editors (continued)

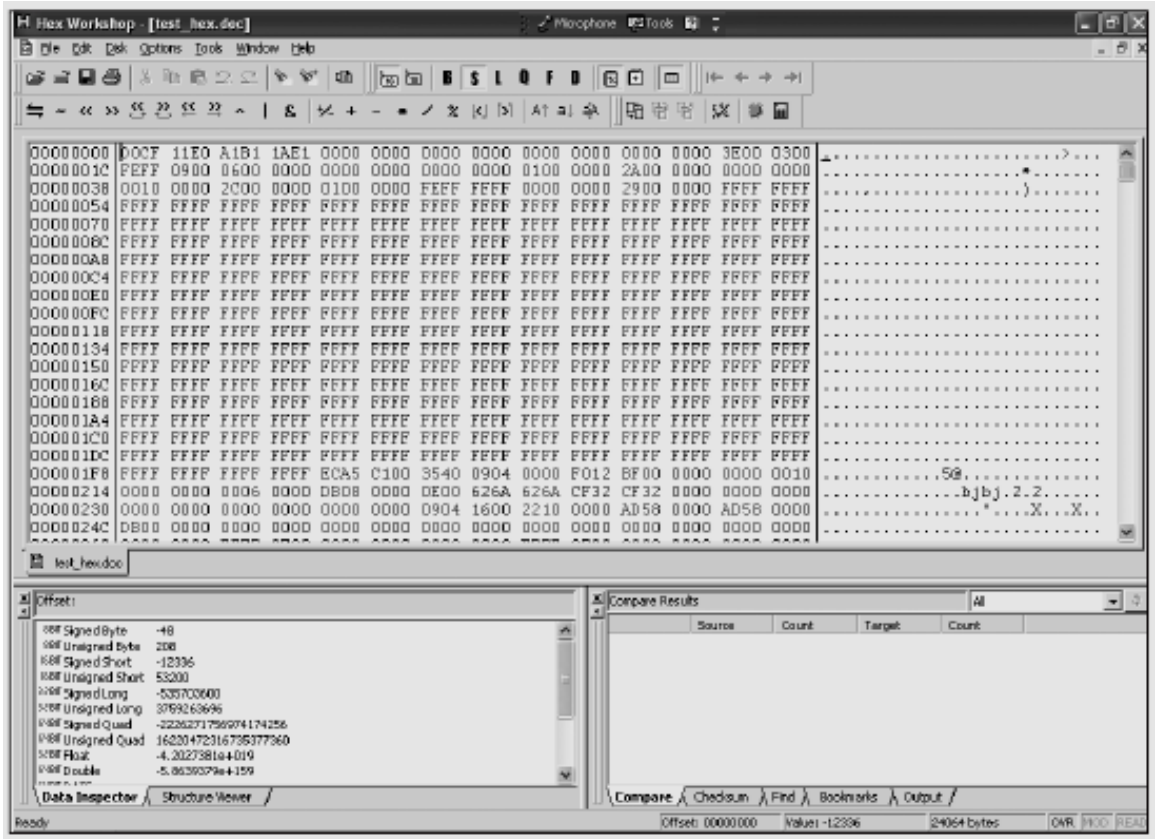


Figure 9-4 Viewing a file opened in Hex Workshop

Validating with Hexadecimal Editors (continued)

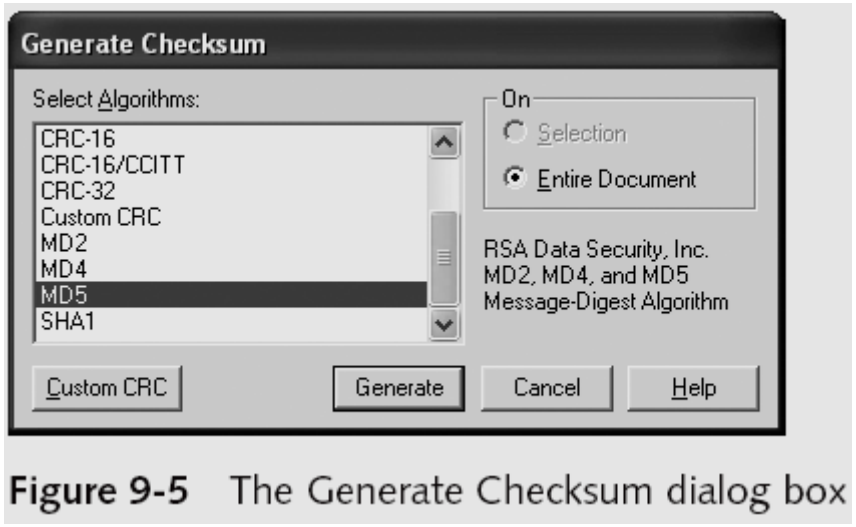


Figure 9-5 The Generate Checksum dialog box

Validating with Hexadecimal Editors (continued)

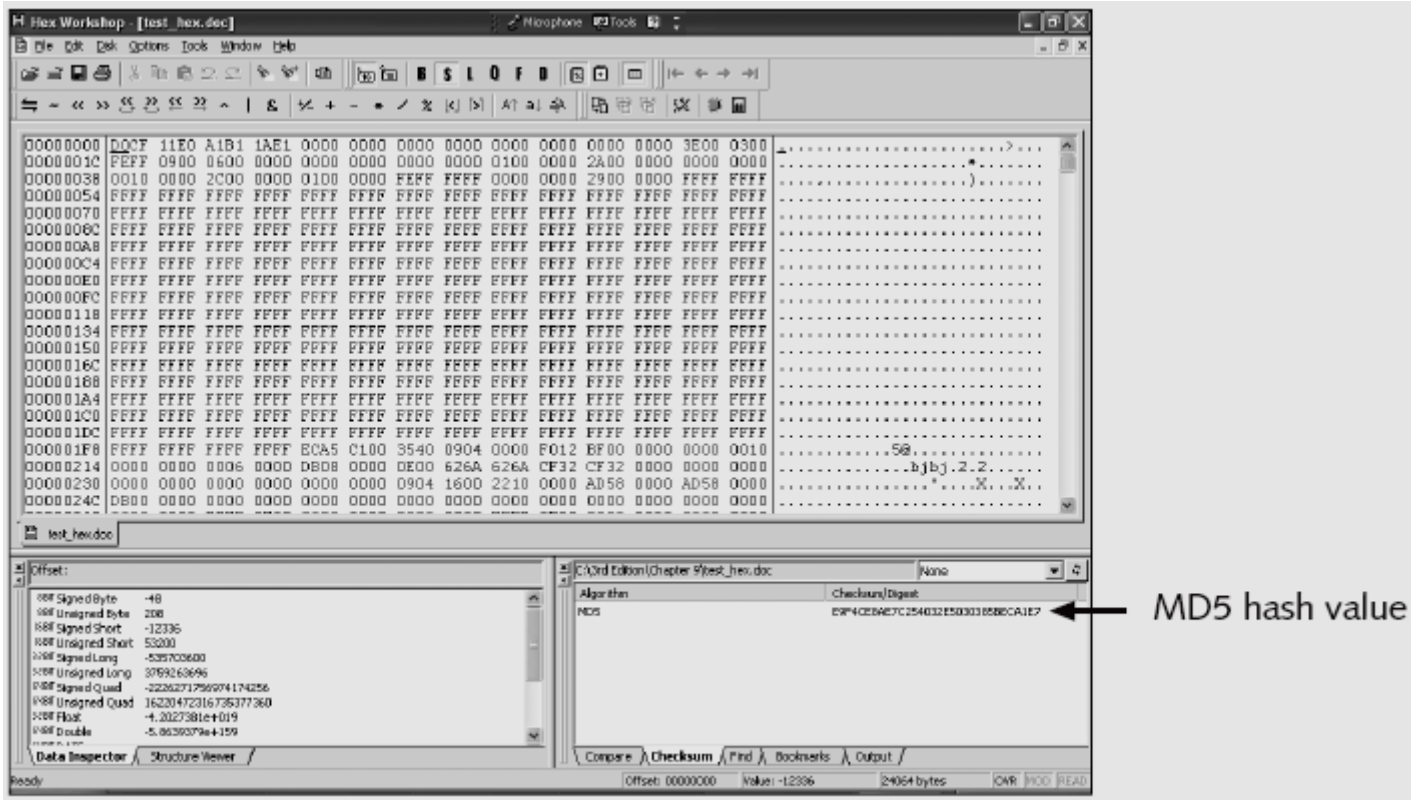


Figure 9-6 Hex Workshop displaying the MD5 hash value

Validating with Hexadecimal Editors (continued)

- Using hash values to discriminate data
  - AccessData has a separate database, the **Known File Filter (KFF)**
    - Filters known program files from view, such as MSWord.exe, and identifies known illegal files, such as child pornography
  - KFF compares known file hash values to files on your evidence drive or image files
  - Periodically, AccessData updates these known file hash values and posts an updated KFF

Validating with Computer Forensics Programs

- Commercial computer forensics programs have built-in validation features
- ProDiscover's .eve files contain metadata that includes the hash value
  - Validation is done automatically
- Raw format image files (.dd extension) don't contain metadata
  - So you must validate raw format image files manually to ensure the integrity of data

Validating with Computer Forensics Programs (continued)

- In AccessData FTK Imager
  - When you select the Expert Witness (.e01) or the SMART (.s01) format
    - Additional options for validating the acquisition are displayed
  - Validation report lists MD5 and SHA-1 hash values
- Figure 9-7 shows how ProDiscover's built-in validation feature works

Validating with Computer Forensics Programs (continued)

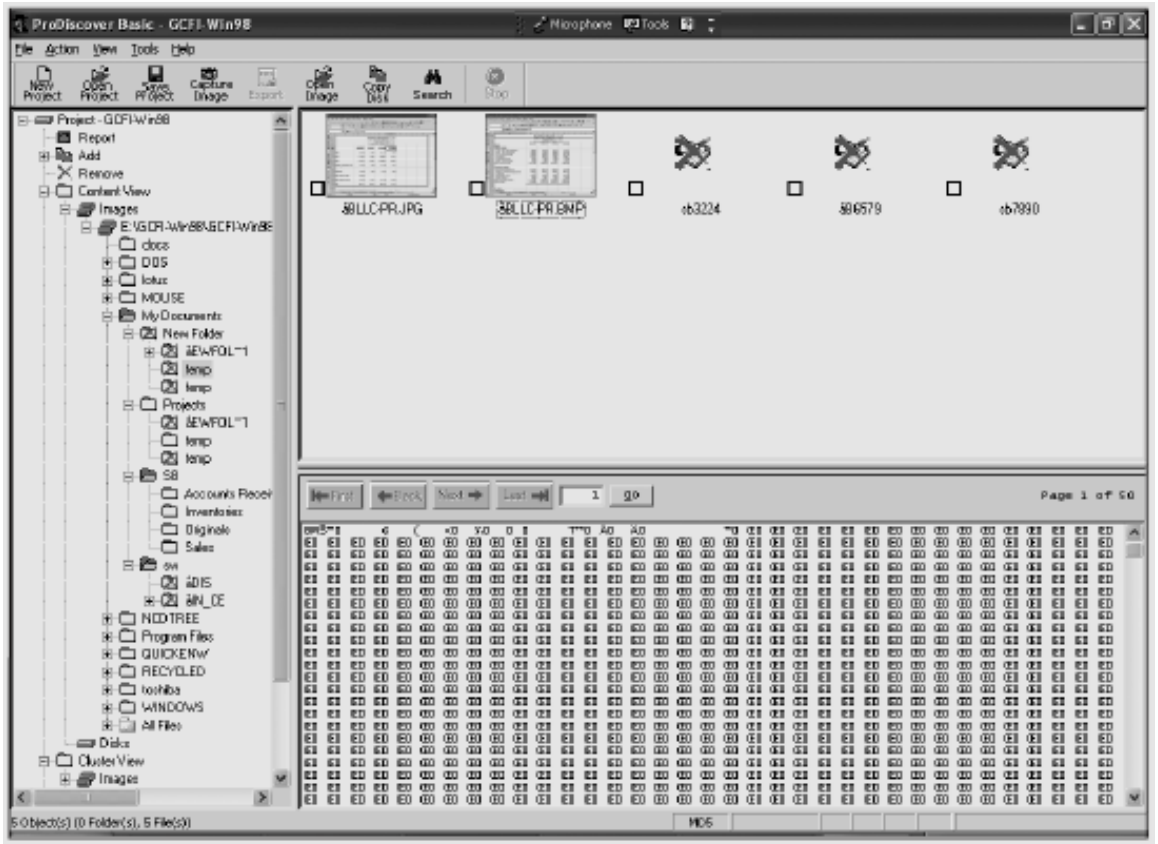


Figure 9-7 ProDiscover's Gallery view

Performing Computer Forensic Analysis: Forensic Workstations

- Carefully consider what you need
- Categories
  - Stationary
  - Portable
  - Lightweight
- Balance what you need and what your system can handle

Forensic Workstations (continued)

- Police agency labs
  - Need many options
  - Use several PC configurations
- Private corporation labs
  - Handle only system types used in the organization
- Keep a hardware library in addition to your software library

Forensic Workstations (continued)

- Not as difficult as it sounds
- Advantages
  - Customized to your needs
  - Save money
- Disadvantages
  - Hard to find support for problems
  - Can become expensive if careless
- Also need to identify what you intend to analyze

Forensic Workstations (continued)

- You can buy one from a vendor as an alternative
- Examples
  - F.R.E.D.
  - F.I.R.E. IDE
- Having vendor support can save you time and frustration when you have problems
- Can mix and match components to get the capabilities you need for your forensic workstation

Addressing Data-hiding Techniques

- File manipulation
  - Filenames and extensions
  - Hidden property
- Disk manipulation
  - Hidden partitions
  - Bad clusters
- Encryption
  - Bit shifting
  - Steganography

Hiding Partitions

- Delete references to a partition using a disk editor
  - Re-create links for accessing it
- Use disk-partitioning utilities
  - GDisk
  - PartitionMagic
  - System Commander
  - LILO
- Account for all disk space when analyzing a disk

Hiding Partitions (continued)

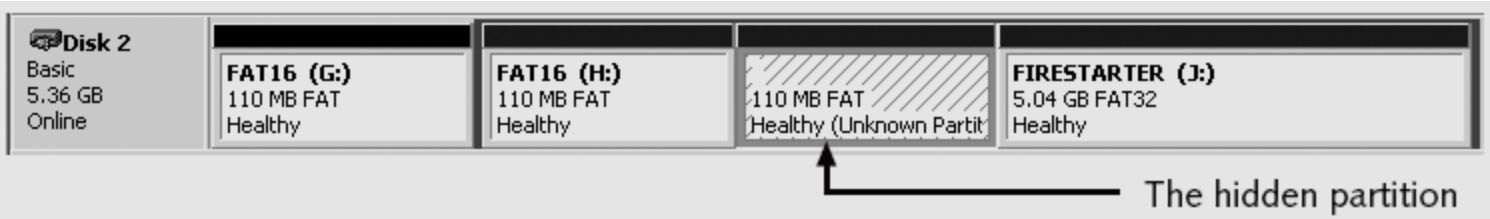


Figure 9-8 Viewing a hidden partition in Disk Manager

Hiding Partitions (continued)

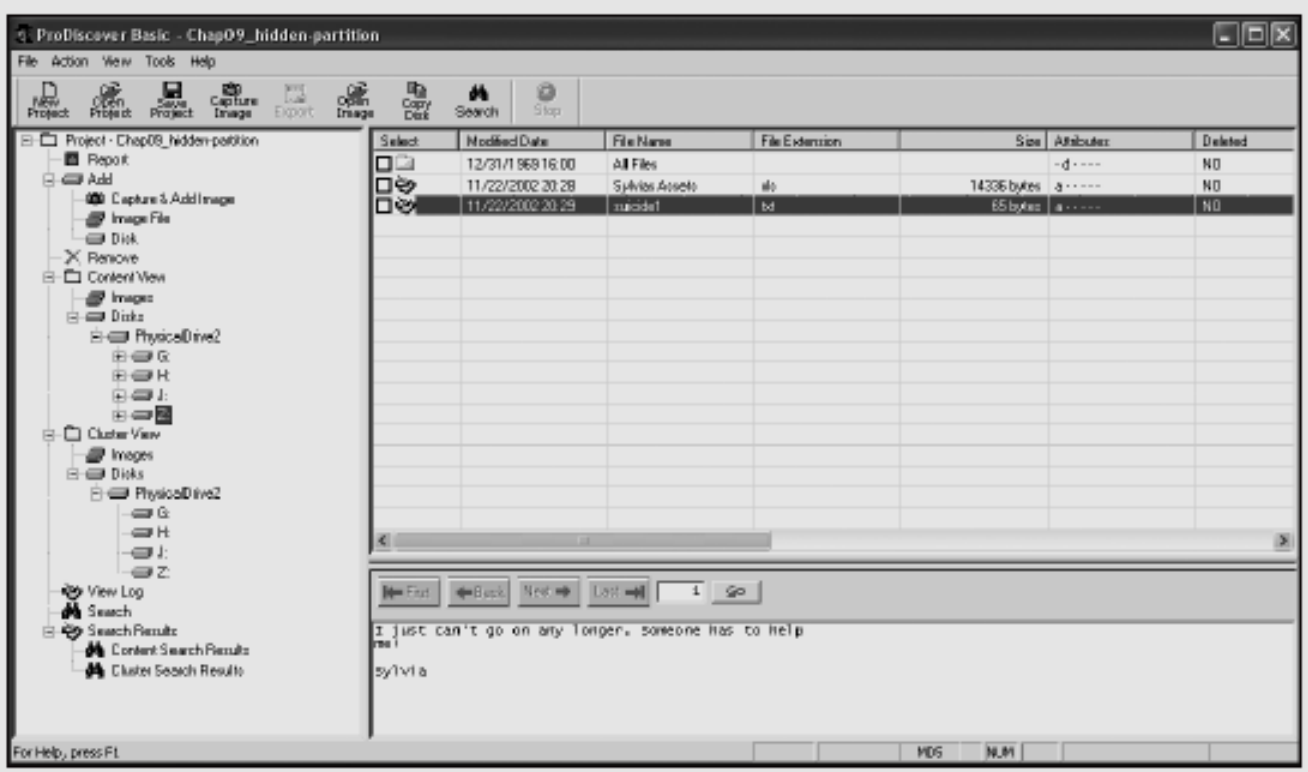


Figure 9-9 Viewing a hidden partition in ProDiscover

Marking Bad Clusters

- Common with FAT systems
- Place sensitive information on free space
- Use a disk editor to mark space as a bad cluster
- To mark a good cluster as bad using Norton Disk Edit
  - Type B in the FAT entry corresponding to that cluster

Bit-shifting

- Old technique
- Shift bit patterns to alter byte values of data
- Make files look like binary executable code
- Tool
  - Hex Workshop

Bit-shifting (continued)

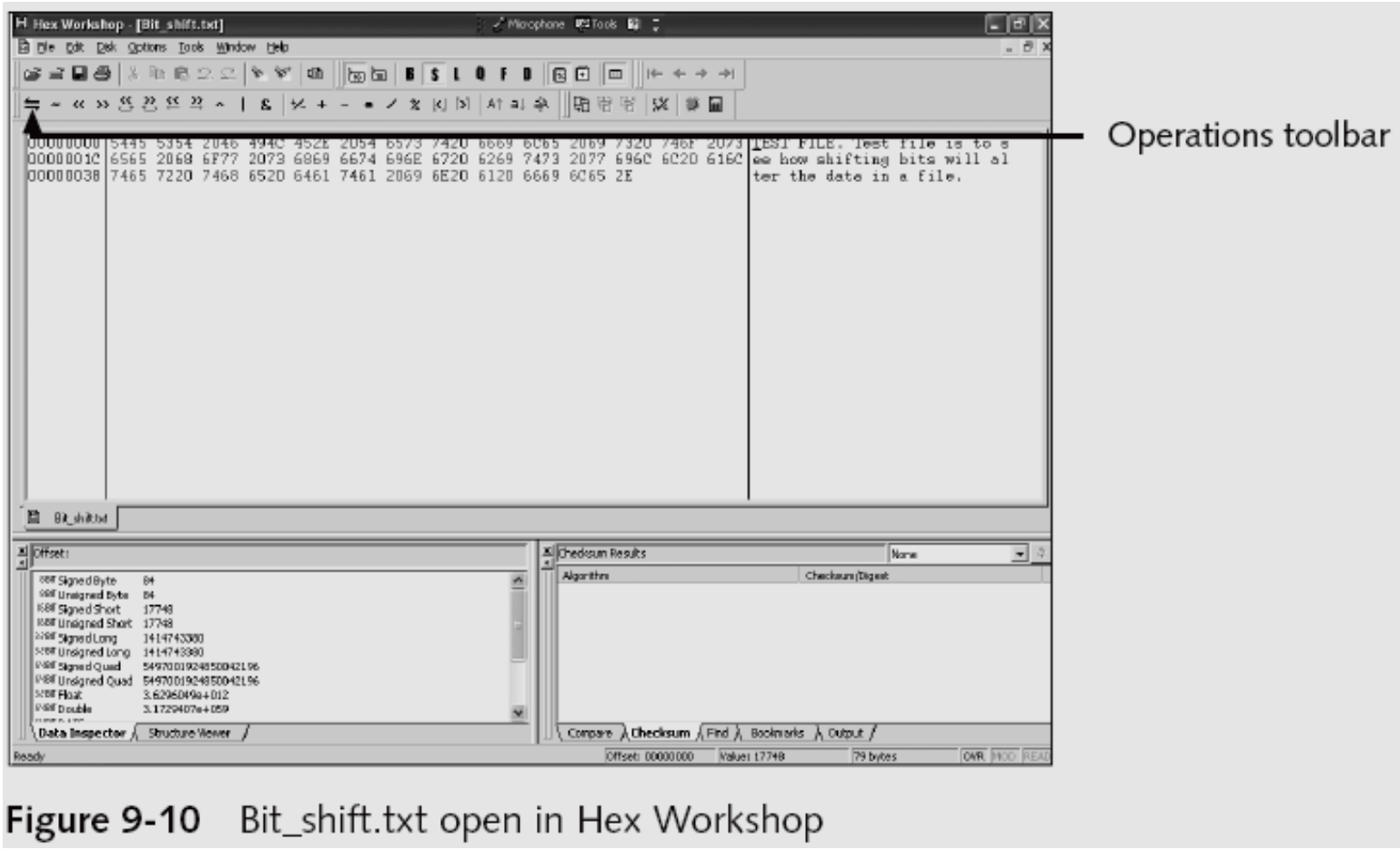


Figure 9-10 Bit_shift.txt open in Hex Workshop

Bit-shifting (continued)

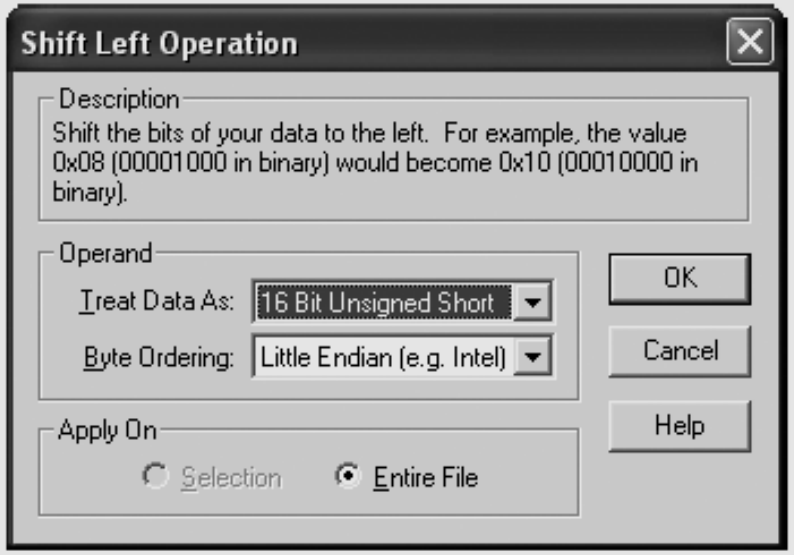


Figure 9-11 The Shift Left Operation dialog box

Bit-shifting (continued)

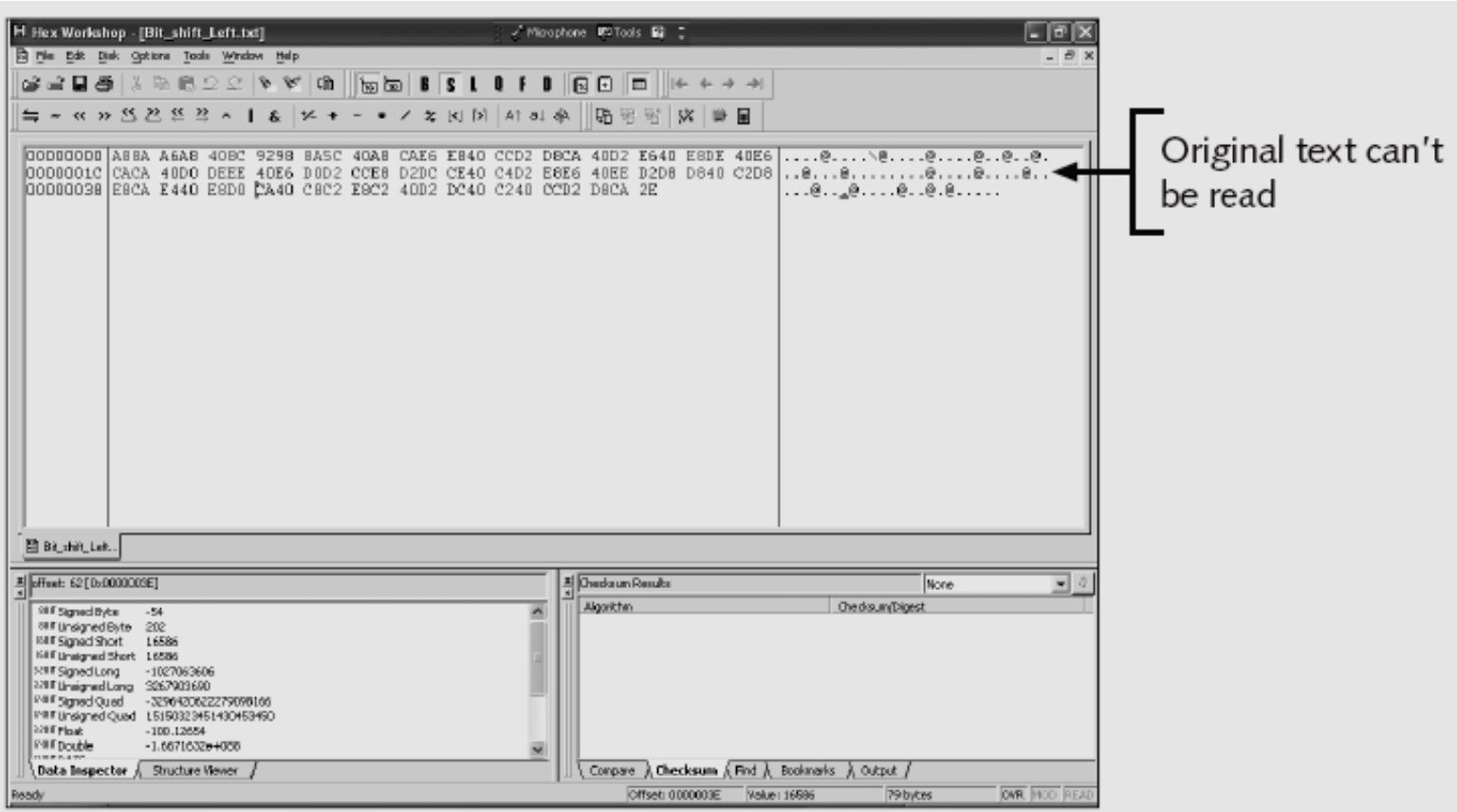


Figure 9-12 Viewing the shifted bits

Using Steganography to Hide Data

- Greek for “hidden writing”
- **Steganography** tools were created to protect copyrighted material
  - By inserting digital watermarks into a file
- Suspect can hide information on image or text document files
  - Most steganography programs can insert only small amounts of data into a file
- Very hard to spot without prior knowledge
- Tools: S-Tools, DPEnvelope, jpgx, and tte

Examining Encrypted Files

- Prevent unauthorized access
  - Employ a password or passphrase
- Recovering data is difficult without password
  - **Key escrow**
    - Designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system failure
  - Cracking password
    - Expert and powerful computers
  - Persuade suspect to reveal password

Recovering Passwords

- Techniques
  - Dictionary attack
  - Brute-force attack
  - Password guessing based on suspect’s profile
- Tools
  - AccessData PRTK
  - Advanced Password Recovery Software Toolkit
  - John the Ripper

Recovering Passwords (continued)

- Using AccessData tools with passworded and encrypted files
  - AccessData offers a tool called Password Recovery Toolkit (PRTK)
    - Can create possible password lists from many sources
  - Can create your own custom dictionary based on facts in the case
  - Can create a suspect profile and use biographical information to generate likely passwords

Recovering Passwords (continued)

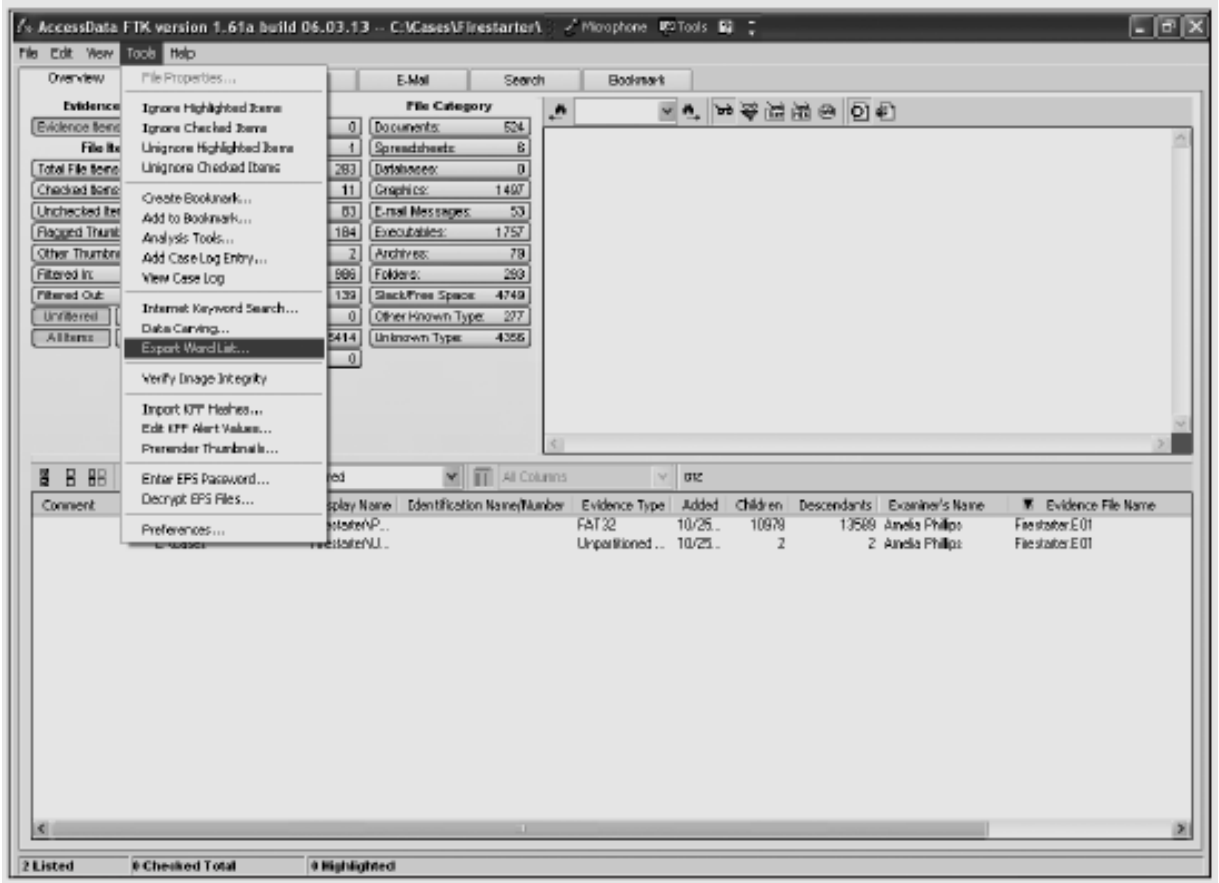


Figure 9-13 Using FTK to generate a password list

Recovering Passwords (continued)

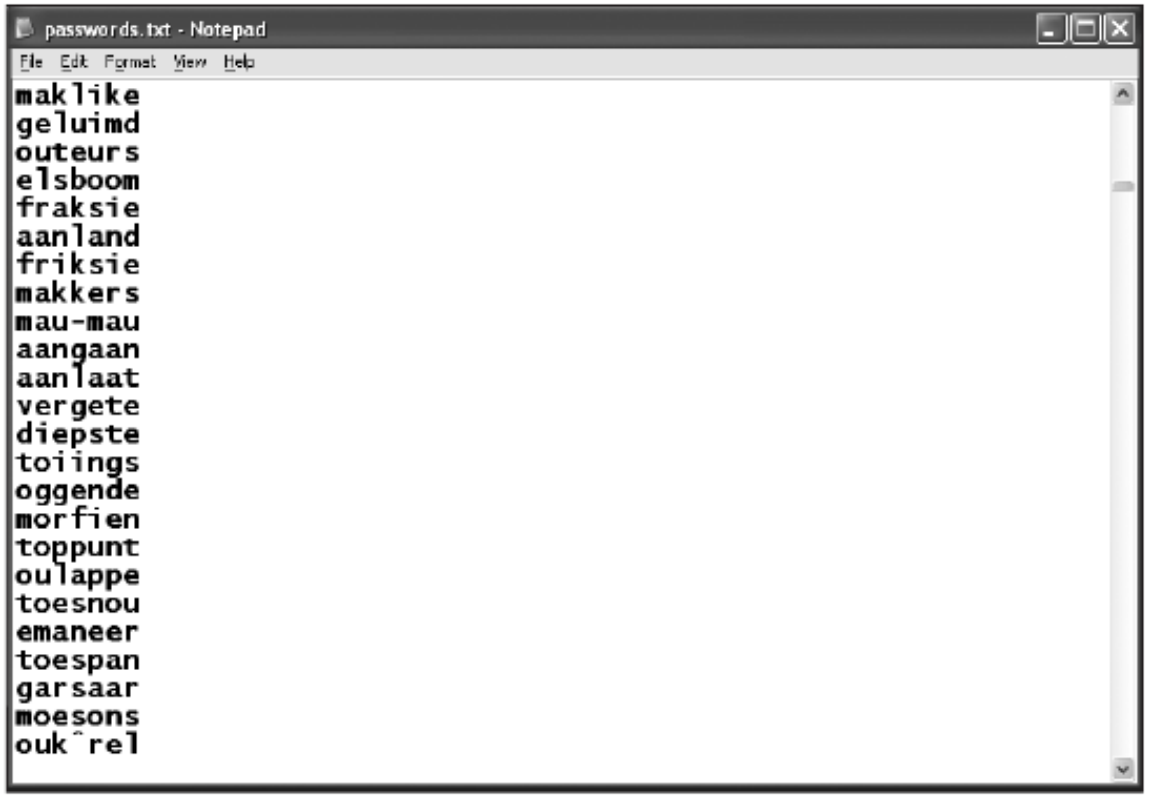


Figure 9-14 A partial list of possible passwords

Recovering Passwords (continued)

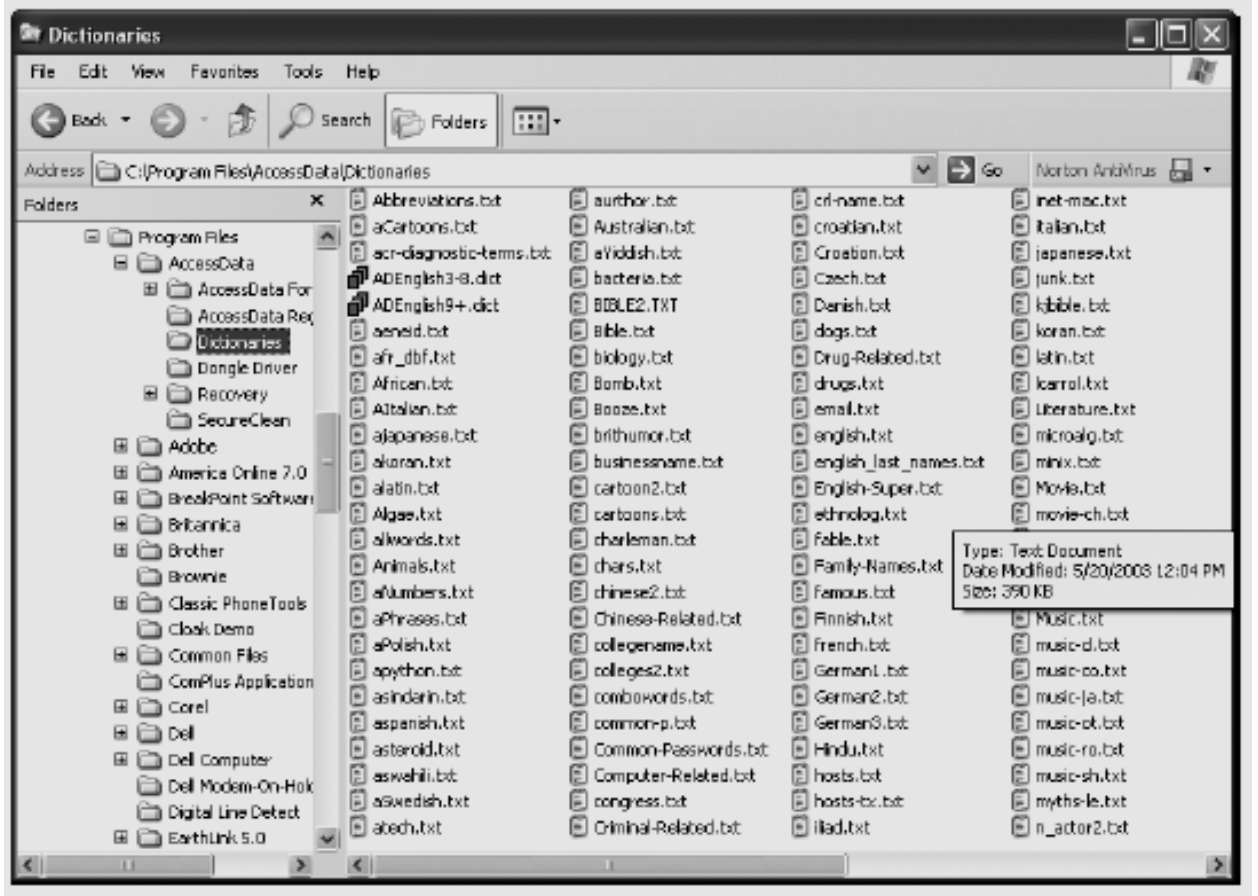


Figure 9-15 Dictionaries available for PRTK

Recovering Passwords (continued)

- Using AccessData tools with passworded and encrypted files (continued)
  - FTK can identify known encrypted files and those that seem to be encrypted
    - And export them
  - You can then import these files into PRTK and attempt to crack them

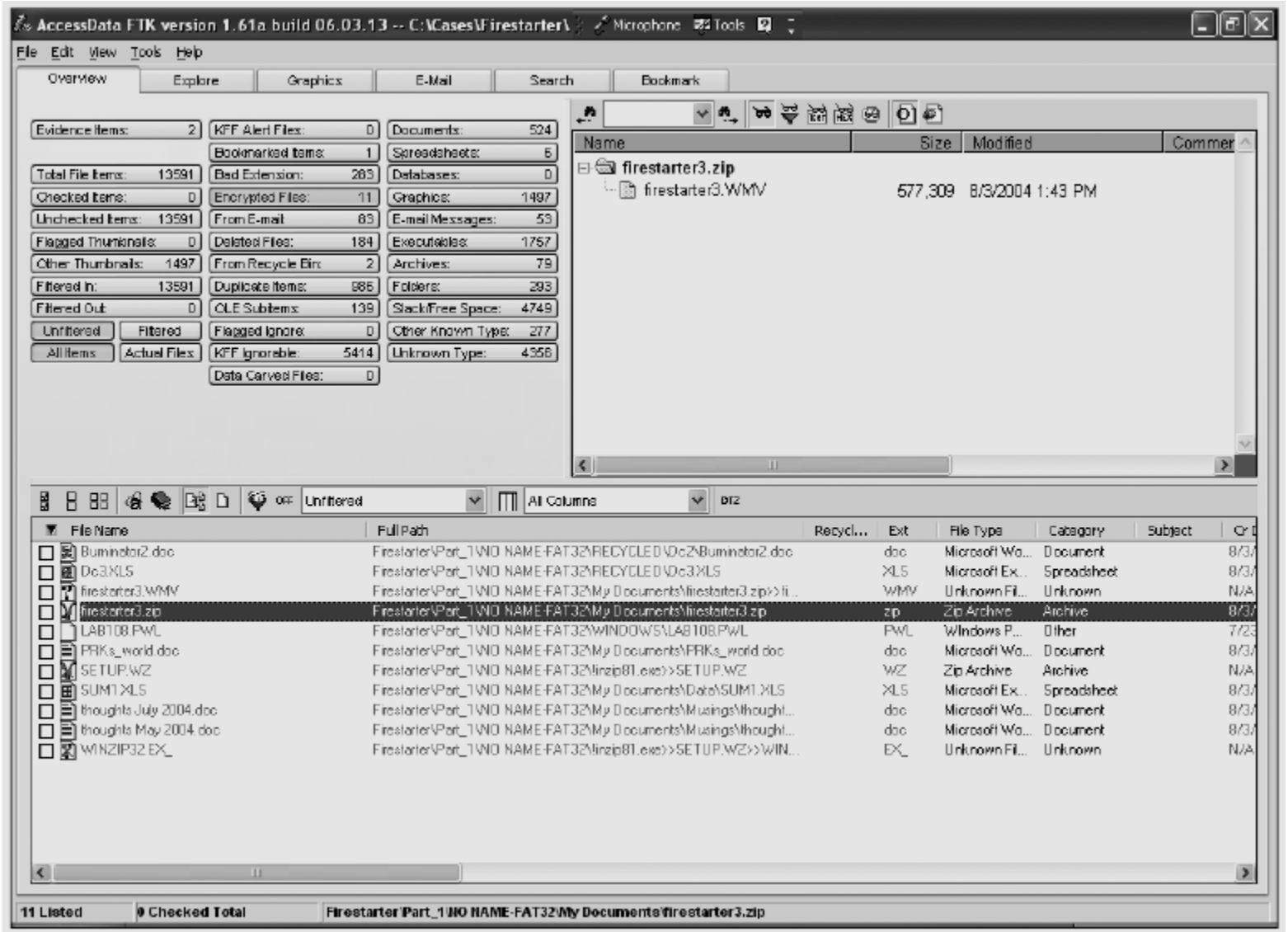


Figure 9-16 FTK displaying encrypted files

Recovering Passwords (continued)

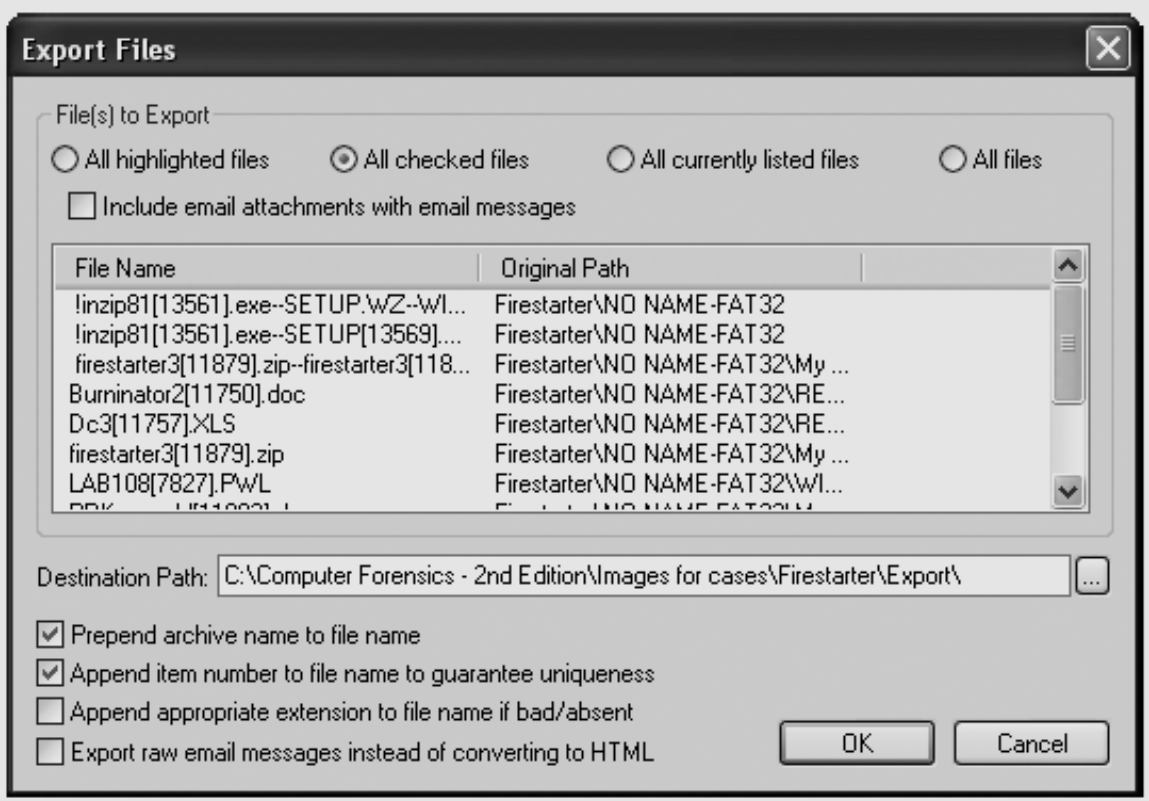


Figure 9-17 Exporting encrypted files

Performing Remote Acquisitions

- Remote acquisitions are handy when you need to image the drive of a computer far away from your location
  - Or when you don’t want a suspect to be aware of an ongoing investigation

Remote Acquisitions with Runtime Software

- Runtime Software offers the following shareware programs for remote acquisitions:
  - DiskExplorer for FAT
  - DiskExplorer for NTFS
  - HDHOST
    - a remote access program for communication between two computers
    - The connection is established by using the DiskExplorer program (FAT or NTFS) corresponding to the suspect (remote) computer's file system.
- Preparing DiskExplorer and HDHOST for remote acquisitions
  - Requires the Runtime Software, a portable media device (USB thumb drive or floppy disk), and two networked computers

Remote Acquisitions with Runtime Software (continued)

- Making a remote connection with DiskExplorer
  - Requires running HDHOST on a suspect's computer
  - To establish a connection with HDHOST, the suspect's computer must be:
    - Connected to the network
    - Powered on
    - Logged on to any user account with permission to run noninstalled applications
  - HDHOST can't be run surreptitiously
  - See Figures 9-18 through 9-24

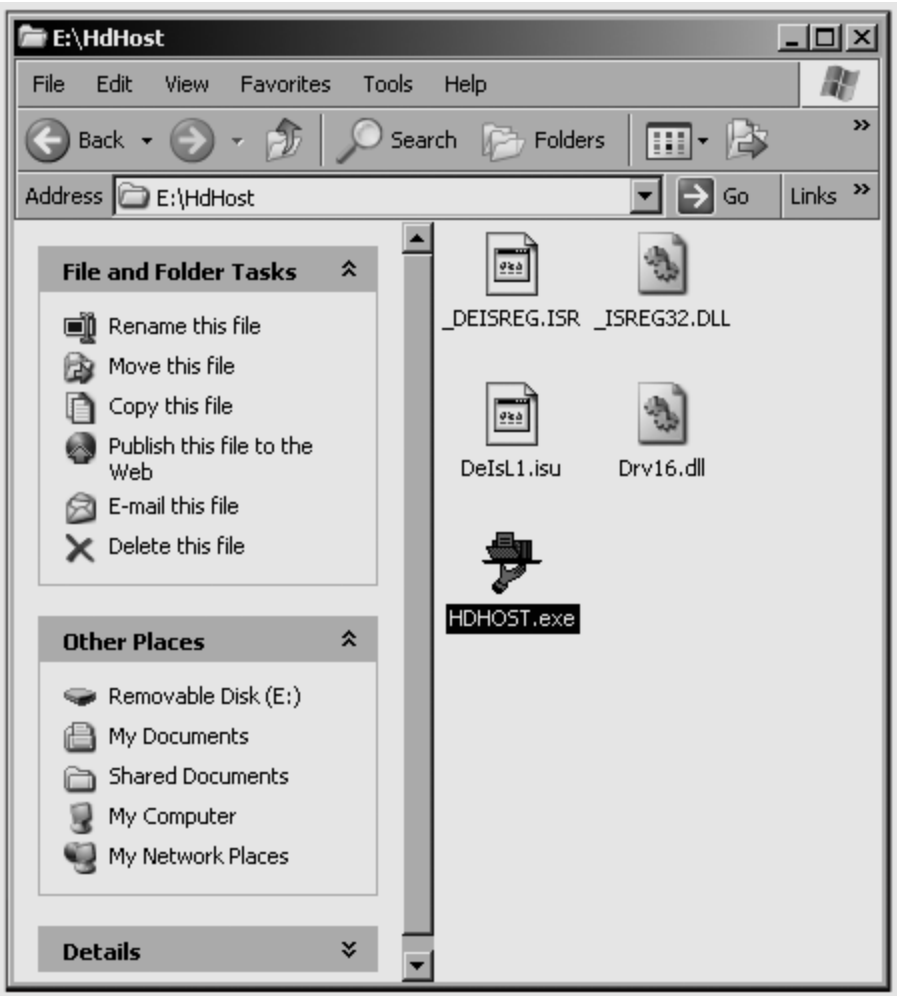


Figure 9-18 Displaying the contents of the HDHOST folder in Windows Explorer

Remote Acquisitions with Runtime Software (continued)

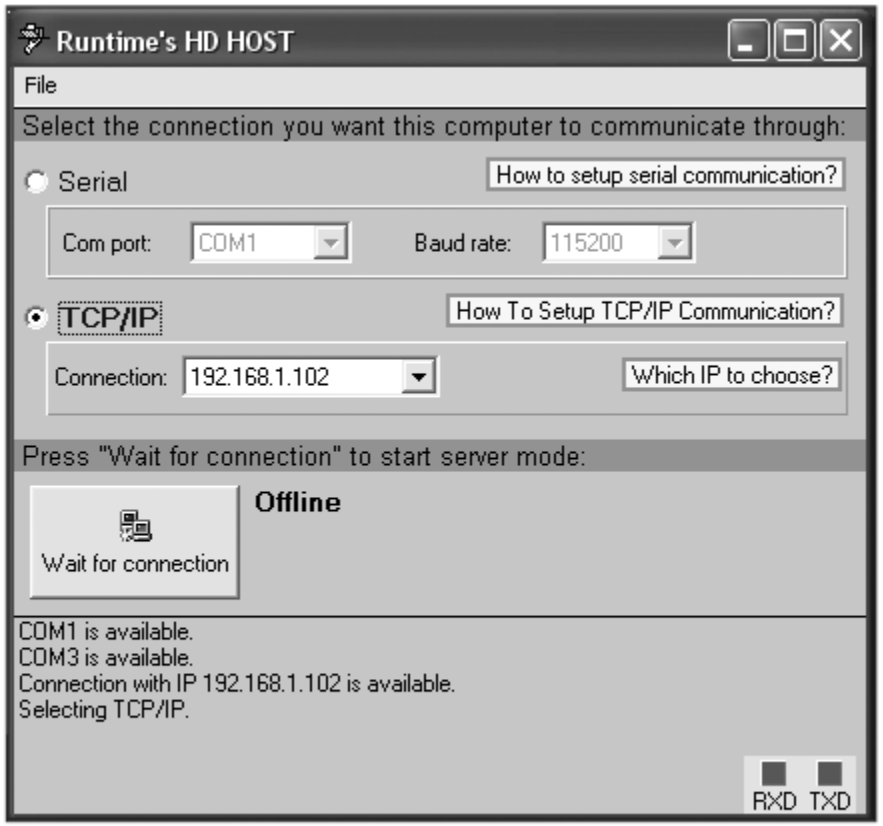


Figure 9-19 Selecting a connection type

Remote Acquisitions with Runtime Software (continued)

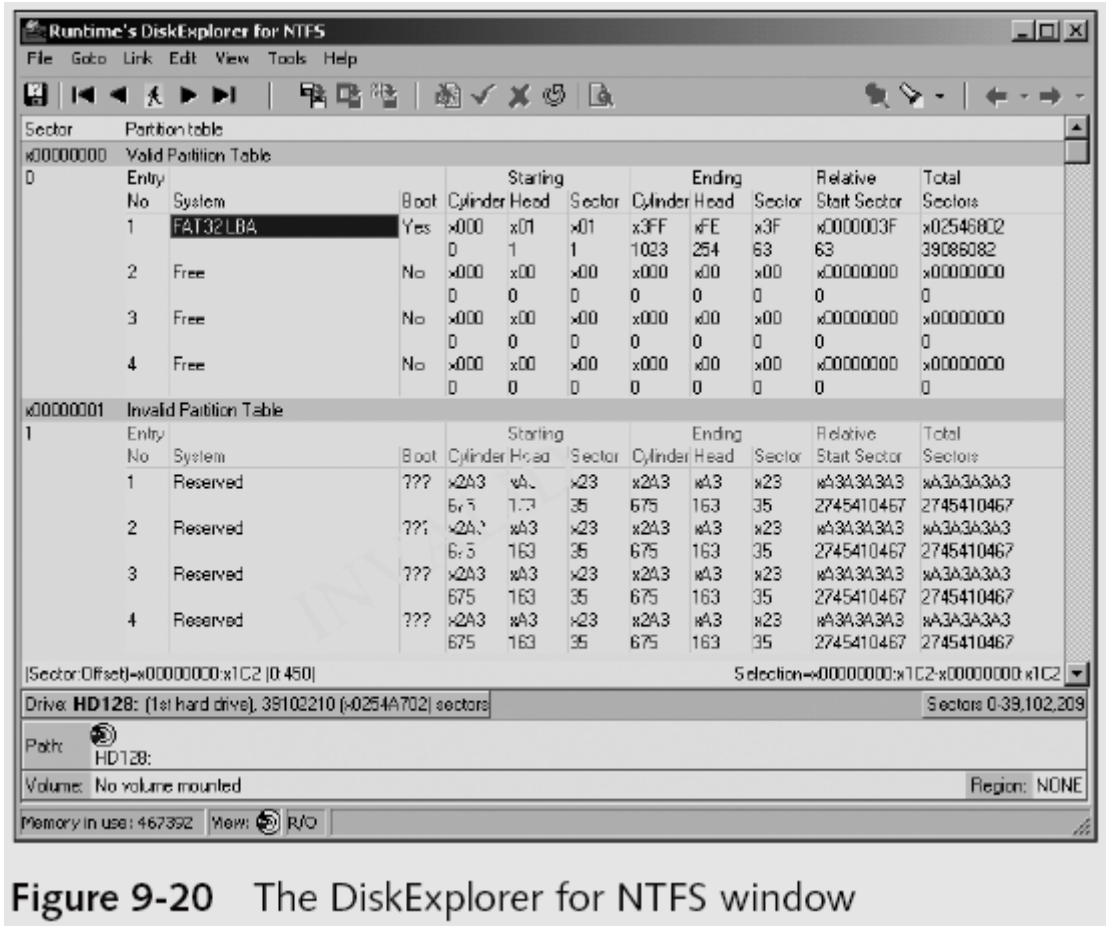


Figure 9-20 The DiskExplorer for NTFS window

Remote Acquisitions with Runtime Software (continued)

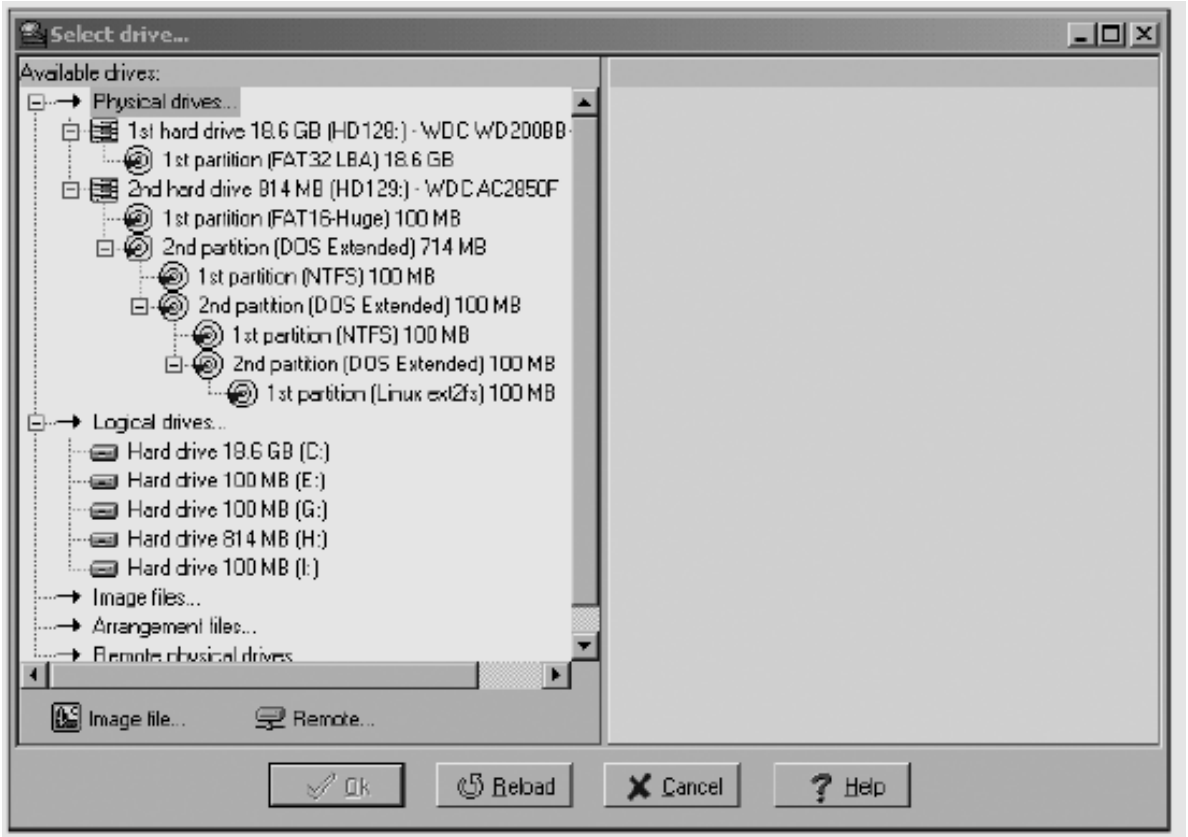


Figure 9-21 The Select drive dialog box

Remote Acquisitions with Runtime Software (continued)

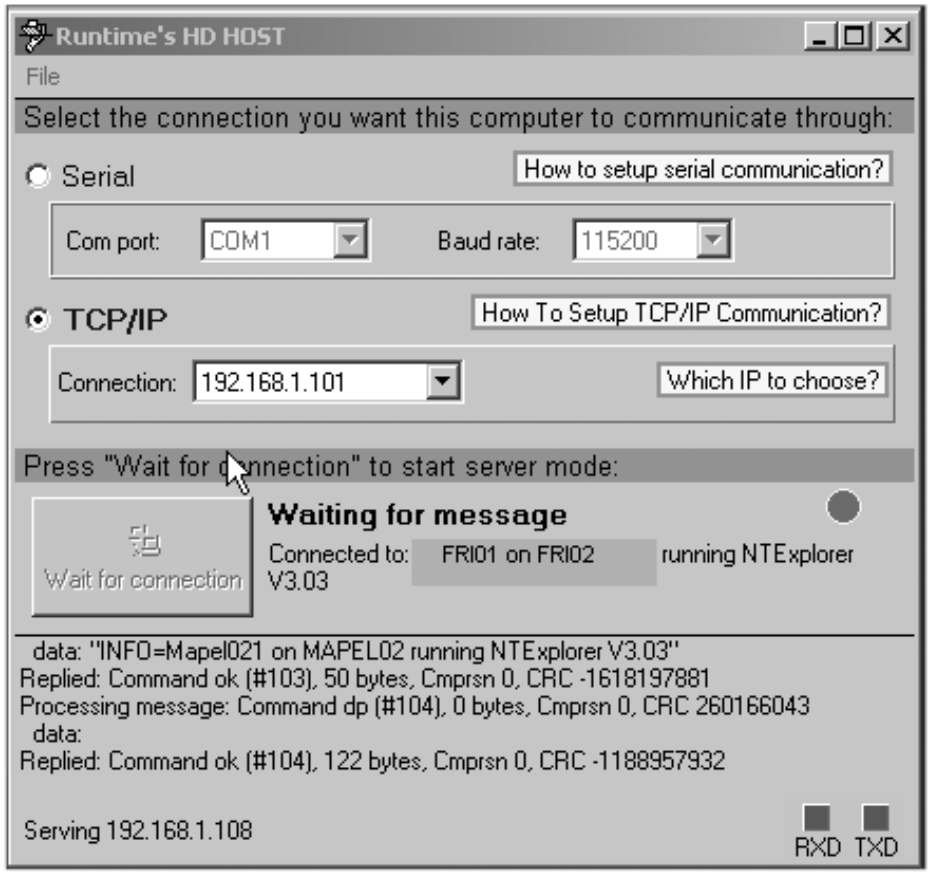


Figure 9-22 The HDHOST remote connection window

Remote Acquisitions with Runtime Software (continued)

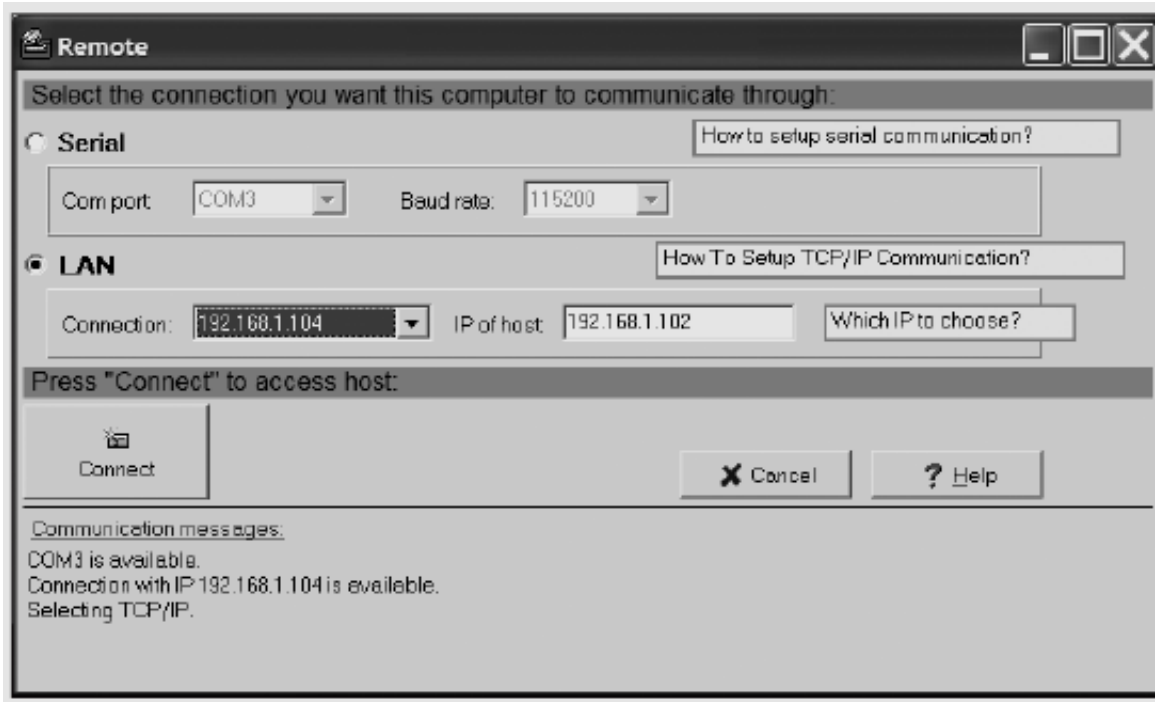


Figure 9-23 Connecting to the remote computer

Remote Acquisitions with Runtime Software (continued)

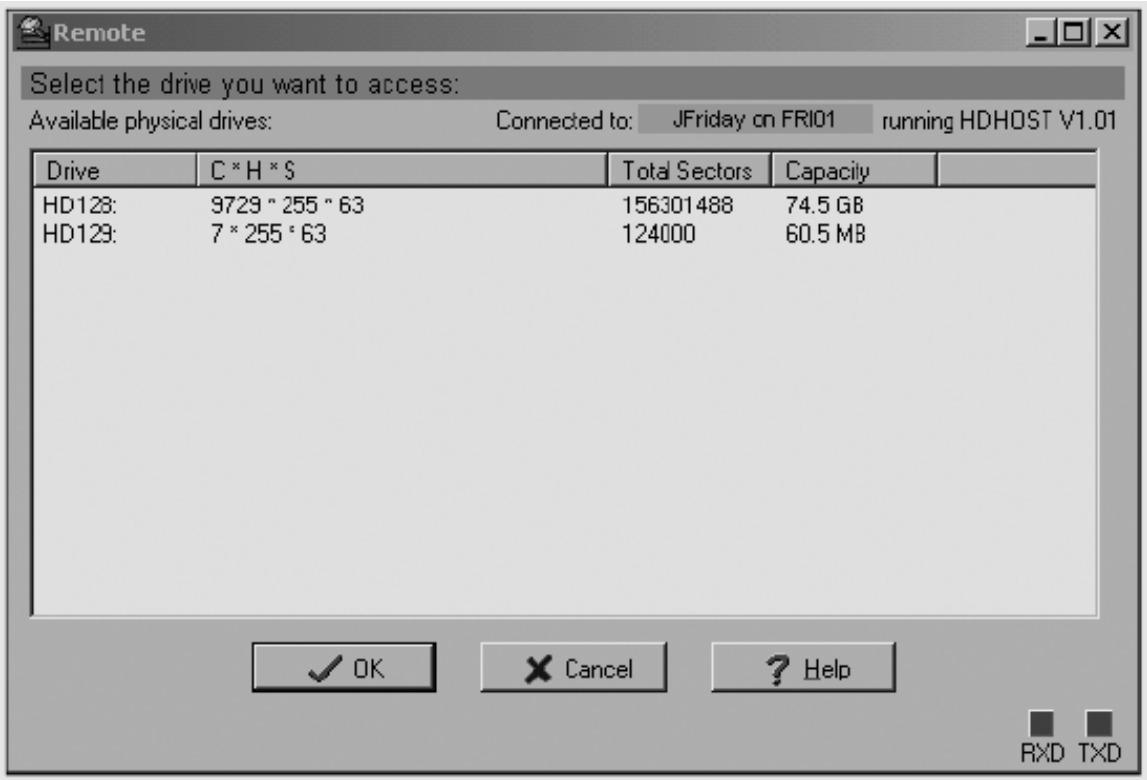


Figure 9-24 Select a drive to access

Remote Acquisitions with Runtime Software (continued)

- Making a remote acquisition with DiskExplorer
  - After you have established a connection with DiskExplorer from the acquisition workstation
    - You can navigate through the suspect computer's files and folders or copy data
  - The Runtime tools don't generate a hash for acquisitions

Remote Acquisitions with Runtime Software (continued)

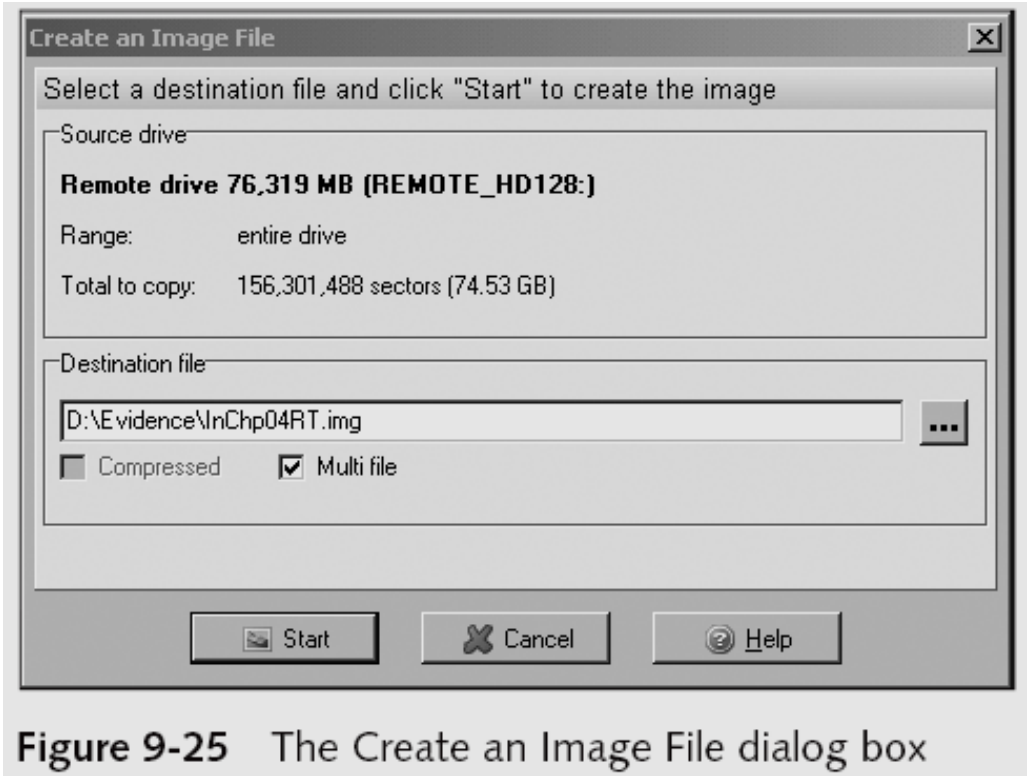


Figure 9-25 The Create an Image File dialog box

Presenting the evidence

Understanding the Importance of Reports

- Communicate the results of your investigation
  - Including expert opinion
- Courts require expert witness to submit written reports
- Written report must specify fees paid for the expert's services
  - And list all other civil or criminal cases in which the expert has testified
- **Deposition banks**
  - Examples of expert witness' previous testimonies

Limiting a Report to Specifics

- All reports to clients should start with the job mission or goal
  - Find information on a specific subject
  - Recover certain significant documents
  - Recover certain types of files
- Before you begin writing, identify your audience and the purpose of the report

Types of Reports

- Computer forensics examiners are required to create different types of reports
- **Examination plan**
  - What questions to expect when testifying
  - Attorney uses the examination plan to guide you in your testimony
  - You can propose changes to clarify or define information
  - Helps your attorney learn the terms and functions used in computer forensics

WITNESS EXAMINATION PLAN

WITNESS: Karen Stolz_____/Factors:_____Expert and Treating for P.

Direct Examination - Expected Testimony Objection/Rule/

Testimony on CV

Identity and Address Iowa Bureau of Criminal Investigation

Position (Current) Computer Forensic Examiner

Undergraduate Iowa State University summa cum laude 1990 BS Computer Engineering

Summer Internship 1989 Des Moines Police Department

Neurology residency, University of Massachusetts MC 86-89

Chief resident in neurology, UM MC 88-89____explain neurology

Fellowship in Electroencephalography and Clinical Neurophysiology, UWMC-Seattle 89-90

Fellowship in Sleep Disorders Medicine, Univ. Michigan MC, 90-91

Academic Appointments

Lecturer, Dept of Computer Science, University of Iowa 1998-Current

Instructor, Iowa Police Academy, 1999-Current

Professional Society Certifications

P.E. 1999

CISSP 2001

Membership

American Society for Industrial Security

Publications

Journal of the Iowa State Bar Association, May 1999, "Computer Forensics on Raid Servers-Testifying to a Reasonable Certainty"

How many systems have you conducted forensic examination on?

What is your relationship to the Plaintiff? Retained by his attorney to examine the hard drive of his computer for all financial records. I have never actually met or talked with Mr. Smith.

How long did it take you conduct this examination?

What types of files were you looking for? Why those file types? Where did you find those file types?

What condition were the files in?

What is your opinion as to the cause of that condition?

Can you say for a reasonable certainty that the financial data files were deleted intentionally? Yes.

Are you able to state to a reasonable certainty who deleted the financial data files? Yes.

What is your fee for examining the hard drive, preparing a report and testifying?

Cross Examination - Expected Testimony

How many times have you worked for Mr. Sawyer as an expert witness? I've had 16 contracts as consulting expert or expert witness.

Have you ever previously testified that overwrite utilities are not 100% reliable? Yes, but that was in 1994 and utilities are so far as I can tell 100% reliable today.

Figure 14-1 A sample examination plan

Types of Reports (continued)

- Verbal report
  - Less structured
  - Attorneys cannot be forced to release verbal reports
  - Preliminary report
  - Addresses areas of investigation yet to be completed
    - Tests that have not been concluded
    - Interrogatories
    - Document production
    - Depositions

Types of Reports (continued)

- Written report
  - Affidavit or declaration
  - Limit what you write and pay attention to details
    - Include thorough documentation and support of what you write

Guidelines for Writing Reports

- Hypothetical questions based on factual evidence
  - Less favored today
  - Guide and support your opinion
  - Can be abused and overly complex
- Opinions based on knowledge and experience
- Exclude from hypothetical questions
  - Facts that can change, cannot be used, or are not relevant to your opinion

Guidelines for Writing Reports (continued)

- As an expert witness, you may testify to an opinion, or conclusion, if four basic conditions are met:
  - Opinion, inferences, or conclusions depend on special knowledge or skills
  - Expert should qualify as a true expert
  - Expert must testify to a certain degree of certainty
  - Experts must describe facts on which their opinions are based, or they must testify to a hypothetical question

What to Include in Written Preliminary Reports

- Anything you write down as part of your examination for a report
  - Subject to **discovery** from the opposing attorney
- Considered **high-risk documents**
- **Spoliation**
  - Destroying the report could be considered destroying or concealing evidence
- Include the same information as in verbal reports

What to Include in Written Preliminary Reports (continued)

- Additional items to include in your report:
  - Summarize your billing to date and estimate costs to complete the effort
  - Identify the tentative conclusion (rather than the preliminary conclusion)
  - Identify areas for further investigation and obtain confirmation from the attorney on the scope of your examination

Report Structure

- Structure
  - Abstract
  - Table of contents
  - Body of report
  - Conclusion
  - References
  - Glossary
  - Acknowledgements
  - Appendixes

Writing Reports Clearly

- Consider
  - Communicative quality
  - Ideas and organization
  - Grammar and vocabulary
  - Punctuation and spelling
- Lay out ideas in logical order
- Build arguments piece by piece
- Group related ideas and sentences into paragraphs
  - Group paragraphs into sections

Writing Reports Clearly (continued)

- Avoid jargon, slang, and colloquial terms
- Define technical terms
  - Consider your audience
- Consider writing style
  - Use a natural language style
  - Avoid repetition and vague language
  - Be precise and specific
  - Use active rather than passive voice
  - Avoid presenting too many details and personal observations

Writing Reports Clearly (continued)

- Include signposts
  - Draw reader’s attention to a point

Designing the Layout and Presentation of Reports

- Decimal numbering structure
  - Divides material into sections
  - Readers can scan heading
  - Readers see how parts relate to each other
- Legal-sequential numbering
  - Used in pleadings
  - Roman numerals represent major aspects
  - Arabic numbers are supporting information

Designing the Layout and Presentation of Reports (continued)

- Providing supporting material
  - Use material such as figures, tables, data, and equations to help tell the story as it unfolds
- Formatting consistently
  - How you format text is less important than being consistent in applying formatting
- Explaining examination and data collection methods
  - Explain how you studied the problem, which should follow logically from the purpose of the report

Designing the Layout and Presentation of Reports (continued)

- Including calculations
  - If you use any hashing algorithms, be sure to give the common name
- Providing for uncertainty and error analysis
  - Protect your credibility
- Explaining results and conclusions
  - Explain your findings, using subheadings to divide the discussion into logical parts
  - Save broader generalizations and summaries for the report’s conclusion

Designing the Layout and Presentation of Reports (continued)

- Providing references
  - Cite references by author's last name and year of publication
  - Follow a standard format
- Including appendixes
  - You can include appendixes containing material such as raw data, figures not used in the body of the report, and anticipated exhibits
  - Arrange them in the order referred to in the report

Generating Report Findings with Forensics Software Tools

- Forensics tools generate reports when performing analysis
- Report formats
  - Plaintext
  - Word processor
  - HTML format

Testifying & Prosecution

Testifying in Court

- Procedures during a trial
  - Your attorney presents you as a competent expert
  - Opposing attorney might attempt to discredit you
  - Your attorney leads you through the evidence
  - Opposing attorney cross-examines you

Understanding the Trial Process

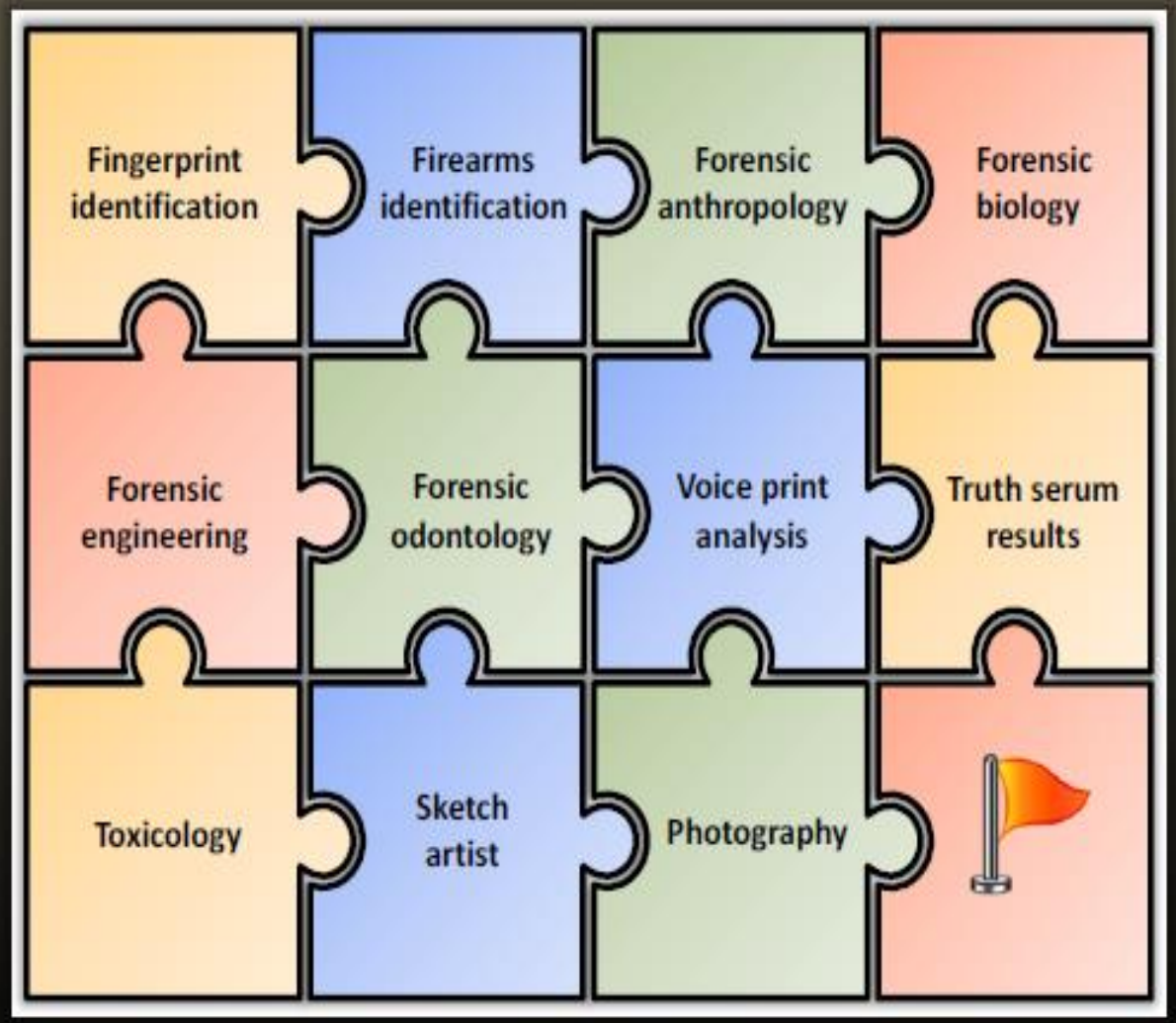
- Typical order of trial
  - Motion in limine
  - Empaneling the jury
  - Opening statements
  - Plaintiff
  - Defendant
  - Rebuttal
  - Closing arguments
  - Jury instructions

Providing Qualifications for Your Testimony

- Demonstrates you are an expert witness
  - This qualification is called **voir dire**
- Attorney asks the court to accept you as an expert on computer forensics
- Opposing attorney might try to disqualify you
  - Depends on your CV and experience

Scope of Expert Witness Testimony

The scope of the expert witness testimony includes the following areas of expertise:



Preparing for Testimony

While preparing for testimony:

Go through the documentation thoroughly

Determine the basic facts of the case before beginning and examining the evidence

Establish early communication with the attorney

Substantiate the findings:

- With documentation
- By collaborating with other computer forensics professionals

Avoid conflicting out (Practice of opposing attorneys who try to prevent investigator from testifying, claiming that investigator has discussed with them and therefore have a conflict of interest)

Detect conflicts of interest

General Guidelines on Testifying

- Be conscious of the jury, judge, and attorneys
- If asked something you cannot answer, say:
  - That is beyond the scope of my expertise
  - I was not requested to investigate that
- Be professional and polite
- Avoid overstating opinions
- Guidelines on delivery and presentation:
  - Always acknowledge the jury and direct your testimony to them

General Guidelines on Testifying (continued)

- Guidelines on delivery and presentation: (continued)
  - Movement
    - Turn towards the questioner when asked
    - Turn back to the jury when answering
  - Place microphone six to eight inches from you
  - Use simple, direct language to help the jury understand you
  - Avoid humor
  - Build repetition into your explanations

General Guidelines on Testifying (continued)

- Guidelines on delivery and presentation: (continued)
  - Use chronological order to describe events
  - If you're using technical terms, identify and define these terms for the jury
  - Cite the source of the evidence the opinion is based on
  - Make sure the chair's height is comfortable, and turn the chair so that it faces the jury

General Guidelines on Testifying (continued)

- Guidelines on delivery and presentation: (continued)
  - Dress in a manner that conforms to the community's dress code
  - Don't memorize your testimony
  - For direct examination
    - State your opinions
    - Identify evidence to support your opinions
    - Relate the method used to arrive to that opinion
    - Restate your opinion

General Guidelines on Testifying (continued)

- Prepare your testimony with the attorney who hired you
  - How is data (or evidence) stored on a hard drive?
  - What is an image or a bit-stream copy of a drive?
  - How is deleted data recovered from a drive?
  - What are Windows temporary files and how do they relate to data or evidence?
  - What are system or network log files?

General Guidelines on Testifying (continued)

- Using graphics during testimony
  - Graphical exhibits illustrate and clarify your findings
  - Your exhibits must be clear and easy to understand
  - Graphics should be big, bold, and simple
  - The goal of using graphics is to provide information the jury needs to know
  - Review all graphics with your attorney before trial
  - Make sure the jury can see your graphics, and face the jury during your presentation

General Guidelines on Testifying (continued)

- Avoiding testimony problems
  - Recognize when conflict-of-interest issues apply to your case
  - Avoid agreeing to review a case unless you're under contract with that person
  - Avoid conversations with opposing attorneys
  - You should receive payment before testifying
  - Don't talk to anyone during court recess
  - Make sure you conduct any conferences with your attorney in a private setting

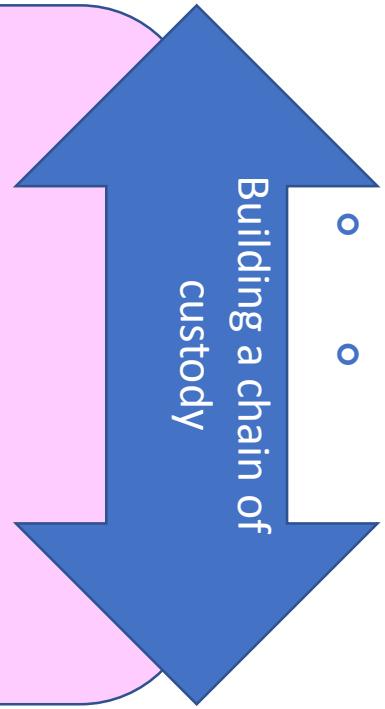
General Guidelines on Testifying (continued)

- Understanding prosecutorial misconduct
  - If you have found exculpatory evidence, you have an obligation to ensure that the evidence isn't concealed
  - Initially, you should report the evidence to the prosecutor handling the case
    - Be sure you document the communication
  - If this information isn't disclosed to the defense attorney in a reasonable time
    - You can report it to the prosecutor's supervisor or the judge

Summary

- Identifying the crime

- Gathering the evidence
- Analyzing the evidence – use duplicate one
- Presenting the evidence



- In this stage, data have been recovered
- Data once recovered must be duplicated or replicated.

- Testifying and Prosecution
  - In this stage, computer forensics investigator must act as an expert witness