Computer Forensics Analysis and Validation

Objectives

- Determine what data to analyze in a computer forensics investigation
- Explain tools used to validate data
- Explain common data-hiding techniques
- Describe methods of performing a remote acquisition

Determining What Data to Collect and Analyze

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
- Investigations often involve locating and recovering a few specific items, which simplifies and speeds processing

Determining What Data to Collect and Analyze

- **Scope creep**
  - Investigation expands beyond the original description
  - unexpected evidence prompt the attorney to ask investigator to examine other areas to recover more evidence
  - Scope creep increases the time and resources
  - Document any requests for additional investigation
    - Helps to explain why the investigation took longer than planned
- Right of full discovery of digital evidence
  - Helps prosecution teams to ensure that they have analyzed the evidence exhaustively before trial

Approaching Computer Forensics Cases

- Investigation begins by planning
  - investigation's goal and scope
  - the materials needed
  - the tasks to perform
- Some basic principles apply to almost all computer forensics cases
- The approach taken is case depends
  - Internal corporate investigation
    - Fairly easy and straightforward
    - Have ready access to the necessary records and files
  - Civil or criminal investigation
    - Need to contact the ISP and e-mail service
    - Need to set up a small camera to monitor
    - Plant a software or hardware
    - Network administrator's services to monitor

Approaching Computer Forensics Cases

- Basic steps for all computer forensics investigations
  - For target drives, use only *recently wiped media* that have been reformatted
  - Inspected for *computer viruses*
  - *Inventory* the hardware on the suspect's computer
  - 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 (bit stream , MD5)
  - Process the data methodically and logically

Approaching Computer Forensics Cases

- Basic steps for all computer forensics investigations
  - *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
  - For all *password-protected files* that might be related to the investigation, make your best effort to recover file contents
  - Identify the *function* of every executable (binary or .exe)
  - 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 - catalog all words
  - Live search – unallocated space, alphanumeric and hexadecimal values
  - Supports options and advanced searching techniques, such as stemming
- Analyzes compressed files
- Can generate reports - Using bookmarks

Validating Forensic Data

Validating Forensic Data

- One of the most critical aspects
- Ensuring the integrity of data
- Essential for presenting evidence in court
- Most computer forensic tools provide automated hashing of image files : ProDiscover, X-Ways Forensics, FTK, and EnCase

Validating with Hexadecimal Editors

- Advanced hexadecimal editors
  - is necessary to ensure data integrity
  - offer many features not available in computer forensics tools
    - Such as hashing specific files or sectors (Hex Workshop)
- Hex Workshop provides several hashing algorithms
  - Such as MD5 and SHA-1

Validating with Hexadecimal Editors

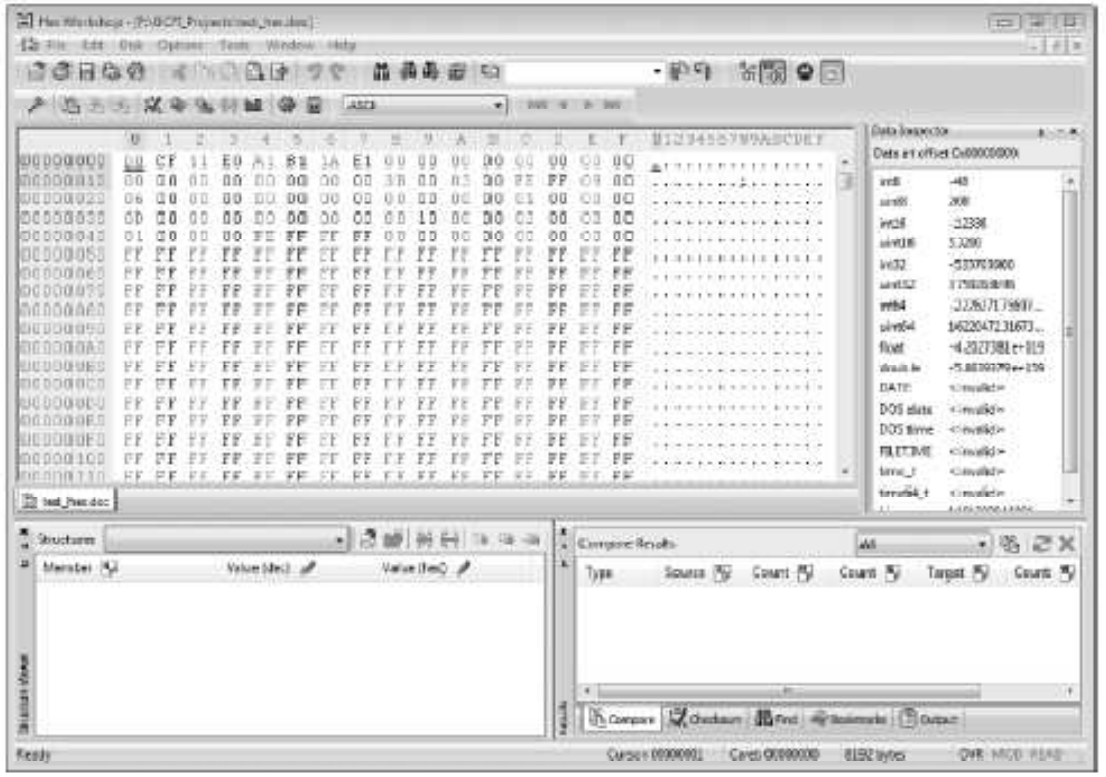

Figure 9-4 Viewing a file opened in Hex Workshop

Validating with Hexadecimal Editors

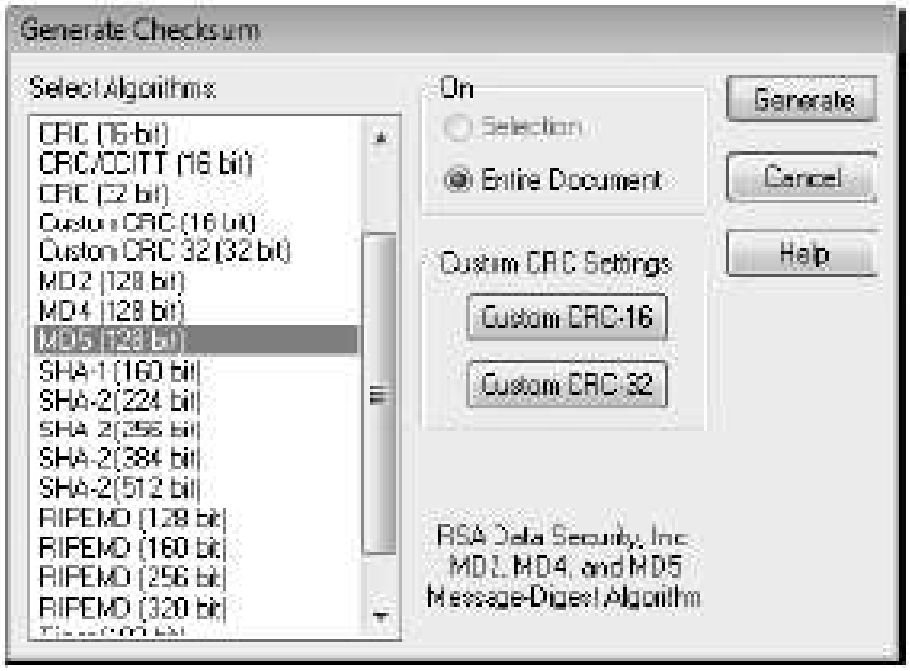

Figure 9-5 The Generate Checksum dialog box

Validating with Hexadecimal Editors

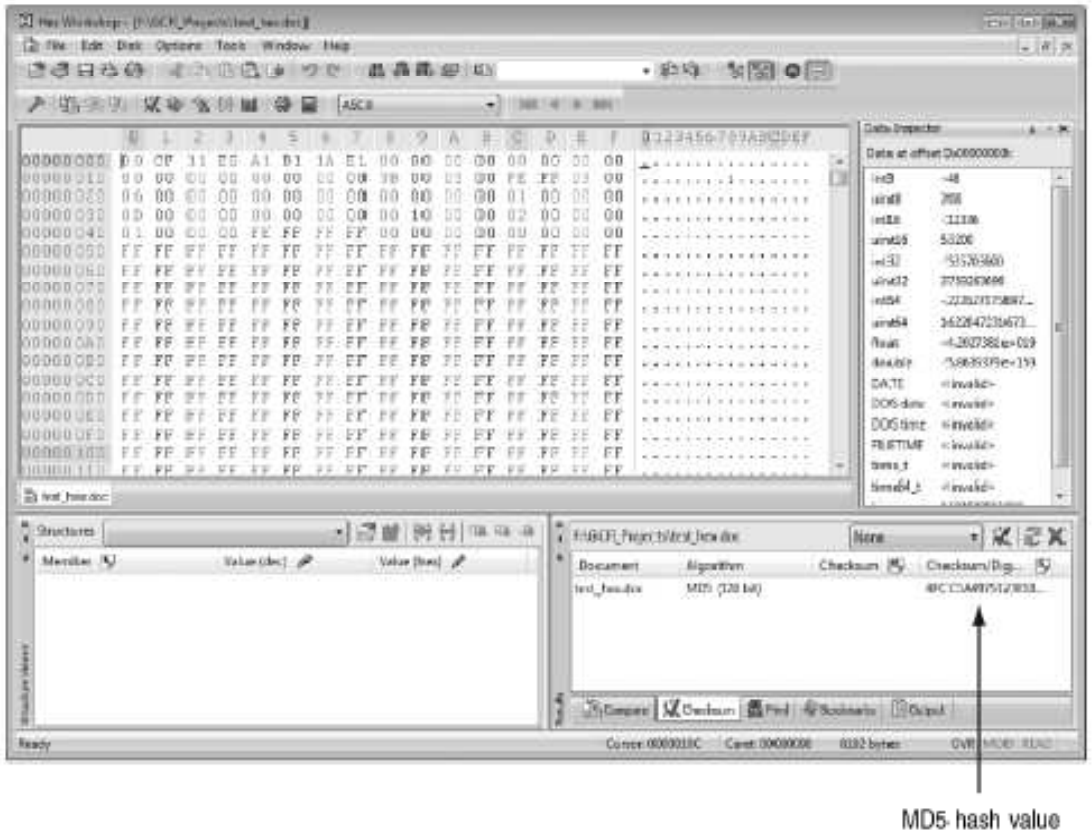

Figure 9-6 Hex Workshop displaying the MD5 hash value

Validating with Hexadecimal Editors

- **Using hash values to discriminate data**
  - AccessData has a separate database, the **Known File Filter (KFF)**
    - Filters known program files : MSWord.exe
    - Identifies known illegal files: 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 by generating and comparing hash
  - notifies you that the acquisition is corrupt and can't be considered reliable evidence
  - This feature is called *Auto Image Checksum Verification*

Validating with Computer Forensics Programs

- 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

Addressing Data-hiding Techniques

Addressing Data-hiding Techniques

- Data hiding involves changing or manipulating a file to conceal information
- Techniques
  - Hiding entire partitions
  - Changing file extensions
  - Setting file attributes to hidden
  - Bit-shifting
  - Using encryption
  - Setting up password protection

Addressing Data-hiding Techniques

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

Hiding Partitions

- **DISKMGMT.MSC**
- Right click on the partition you want to hide (dismount) and select *"Change Drive Letter and Paths“*
- In the *"Change Drive Letter and Paths"* window, click on the *Remove* button.
- In the *"Change Drive Letter and Paths"* window Click the *Add* button.

Hiding Partitions

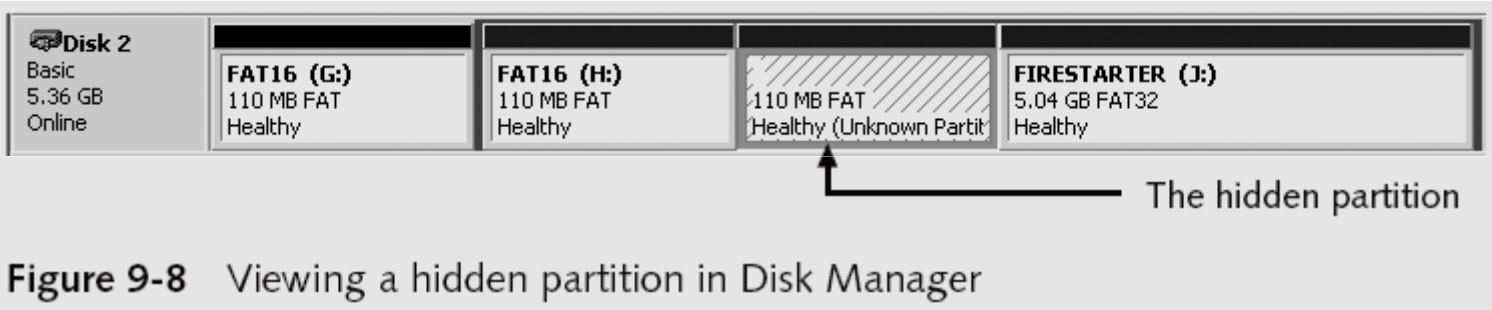

Figure 9-8 Viewing a hidden partition in Disk Manager

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

Marking Bad Clusters

- Common with FAT systems
- Place sensitive information on free or slack space
- Use a disk editor to mark space as a bad cluster
- Only way to access bad cluster from the OS is by changing to good clusters with a disk editor

- To mark a good cluster as bad *using Norton Disk Edit*
  - Type B in the FAT entry corresponding to that cluster
  - Use any DOS disk editor to write and read data to this 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

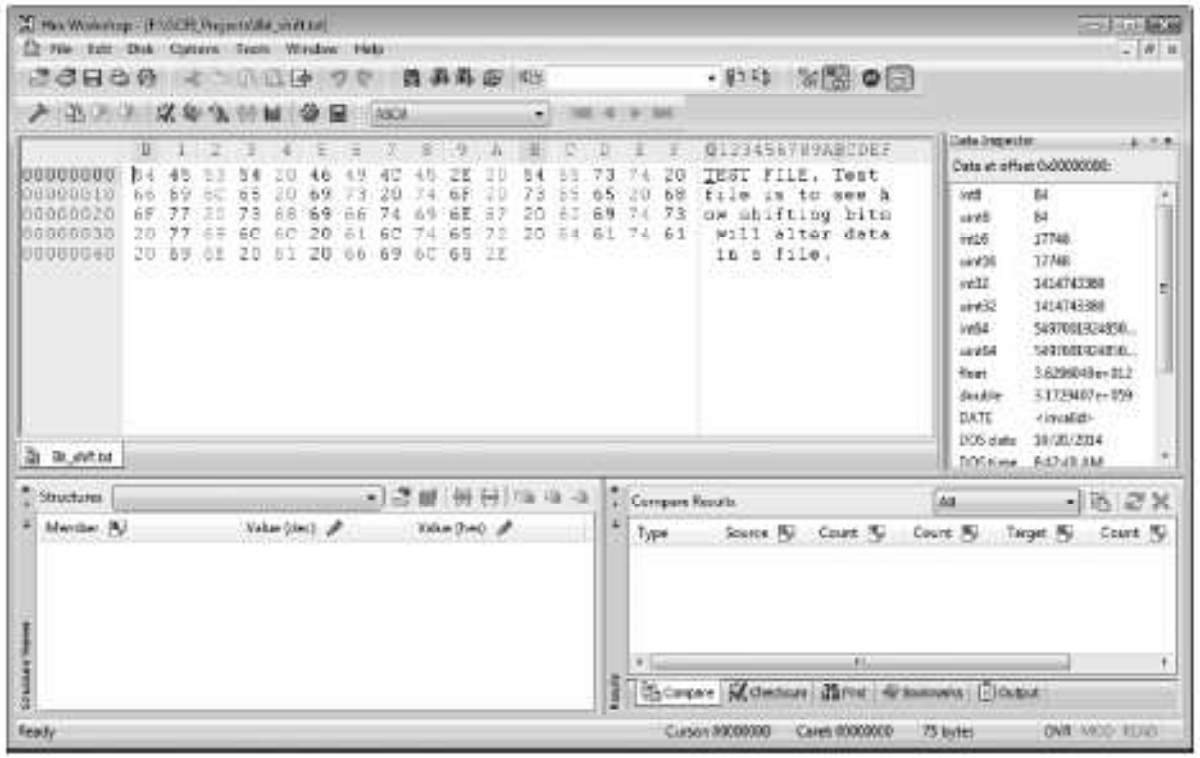

Figure 9-10 Bit_shift.txt open in Hex Workshop

Bit-shifting

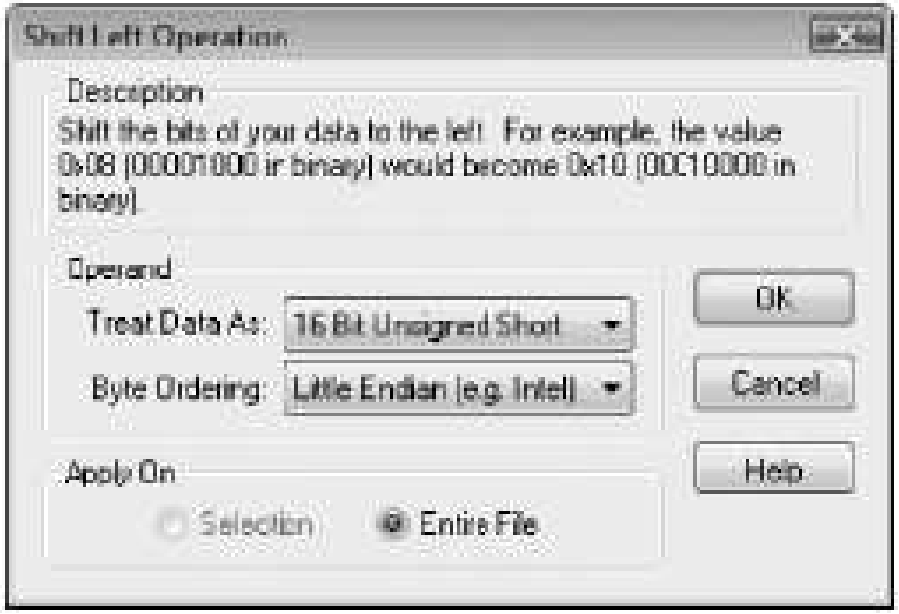

Figure 9-11 The Shift Left Operation dialog box

Bit-shifting

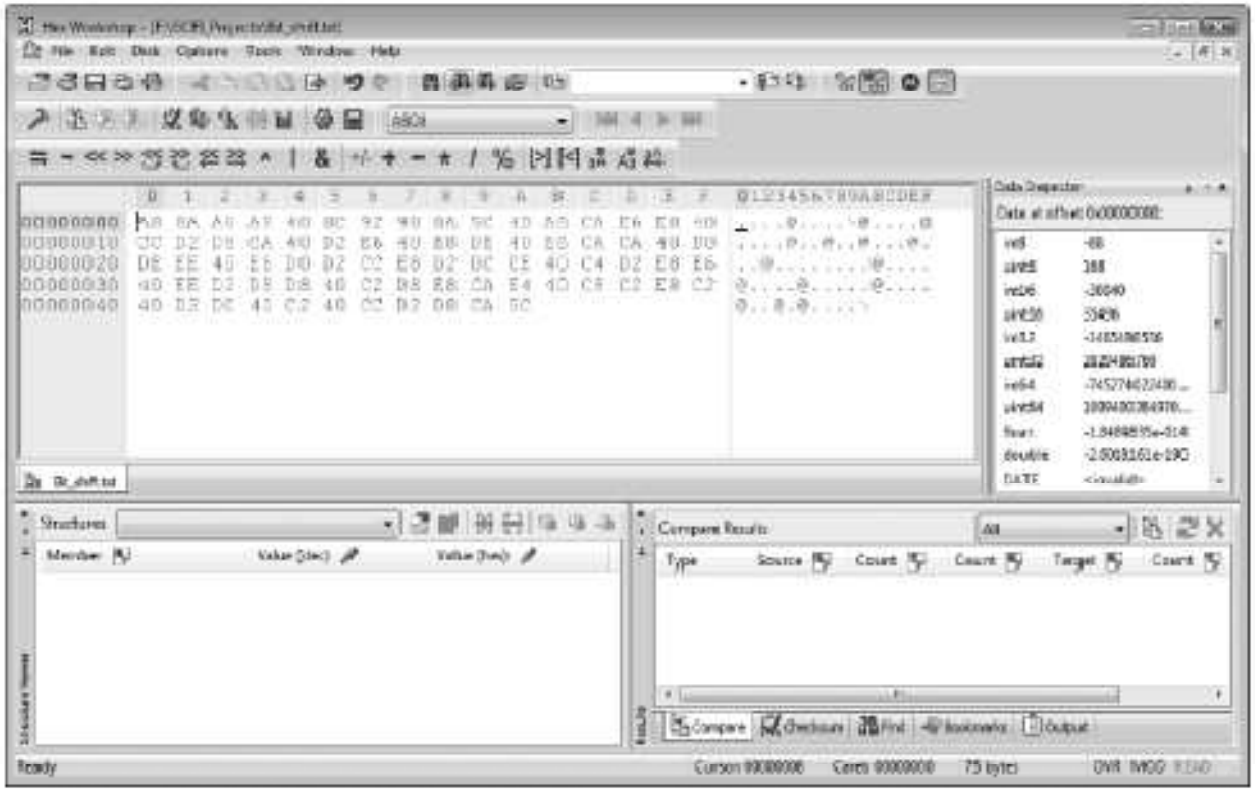

Figure 9-12 Viewing the shifted bits

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

- 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

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

Performing Remote Acquisitions

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
- Preparing for remote acquisitions
  - Requires the Runtime Software
  - A portable media device
  - two networked computers

Remote Acquisitions with Runtime Software

- 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
  - 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