Guide to Computer Forensics and Investigations Fourth Edition

Chapter 9

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

- 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

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)

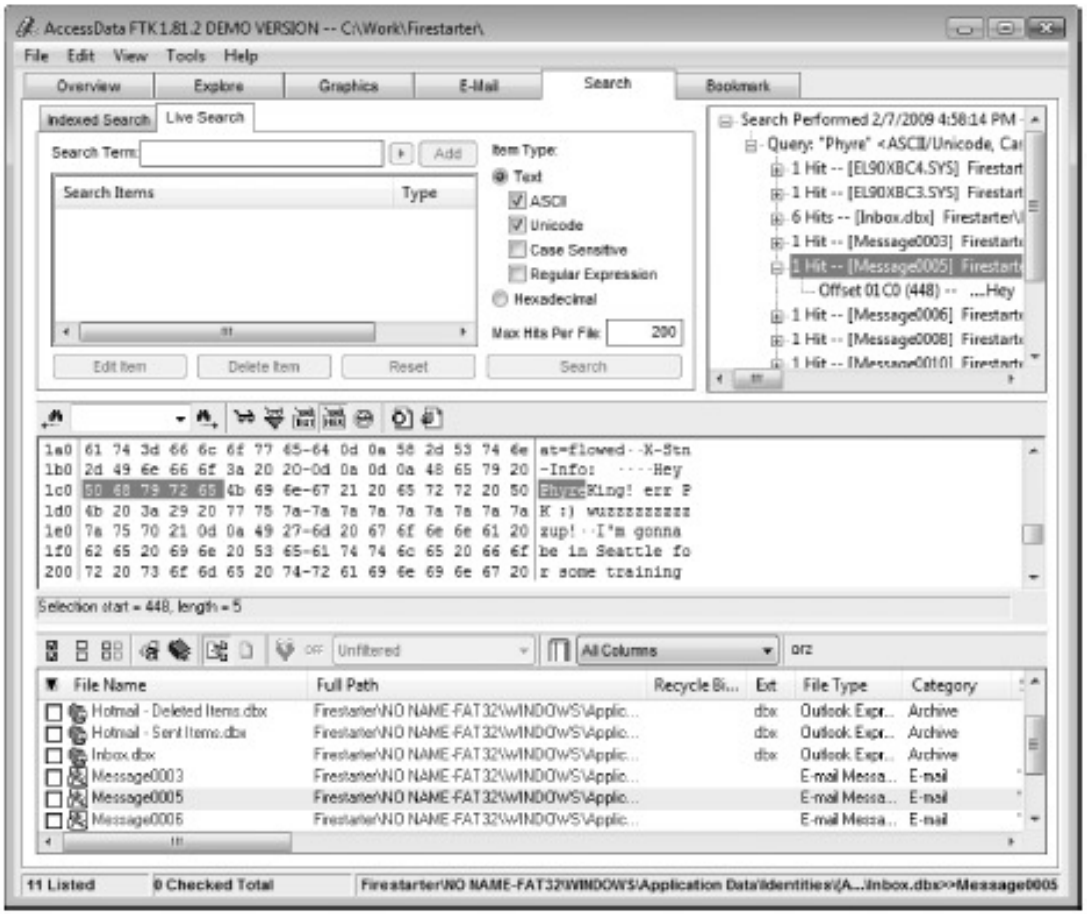

Figure 9-1 Viewing live search results in FTK

Using AccessData Forensic Toolkit to Analyze Data (continued)

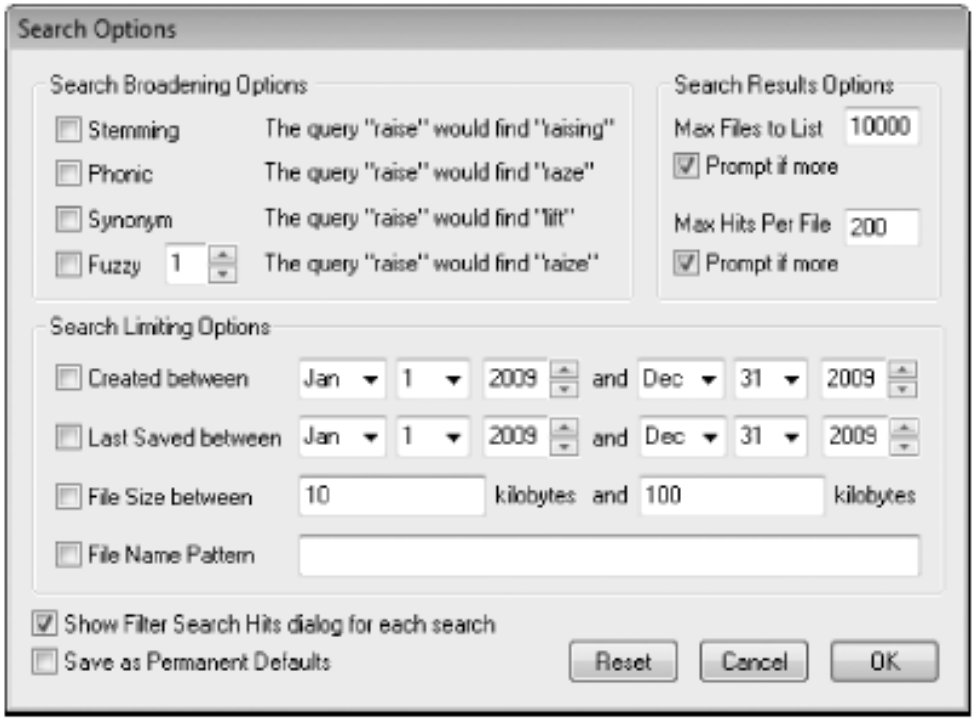

Figure 9-2 Selecting search options in FTK

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)

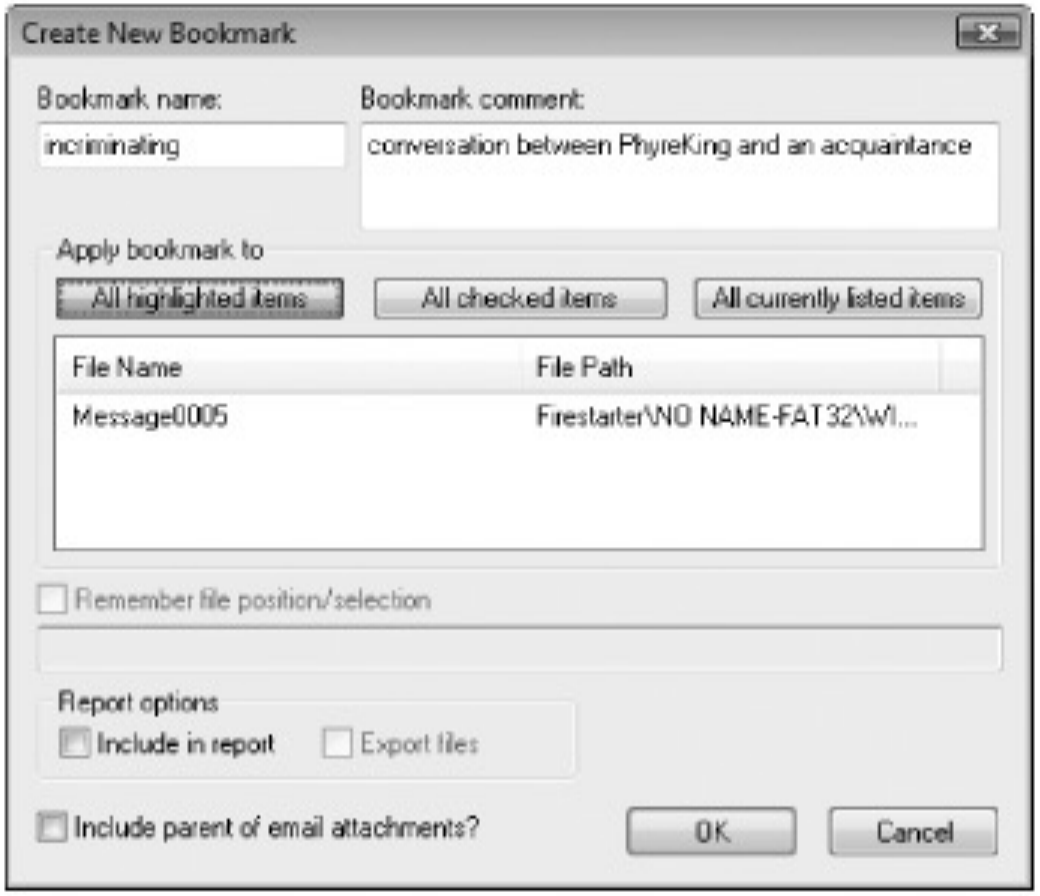

Figure 9-3 Creating a bookmark

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)

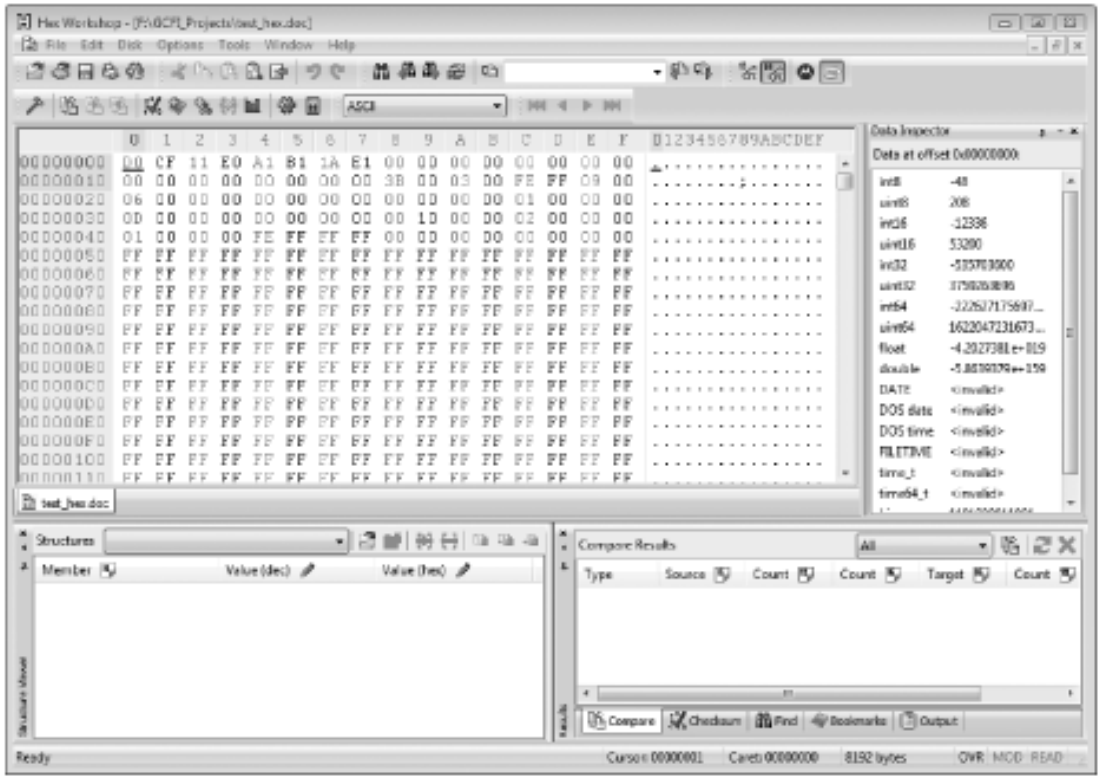

Figure 9-4 Viewing a file opened in Hex Workshop

Validating with Hexadecimal Editors (continued)

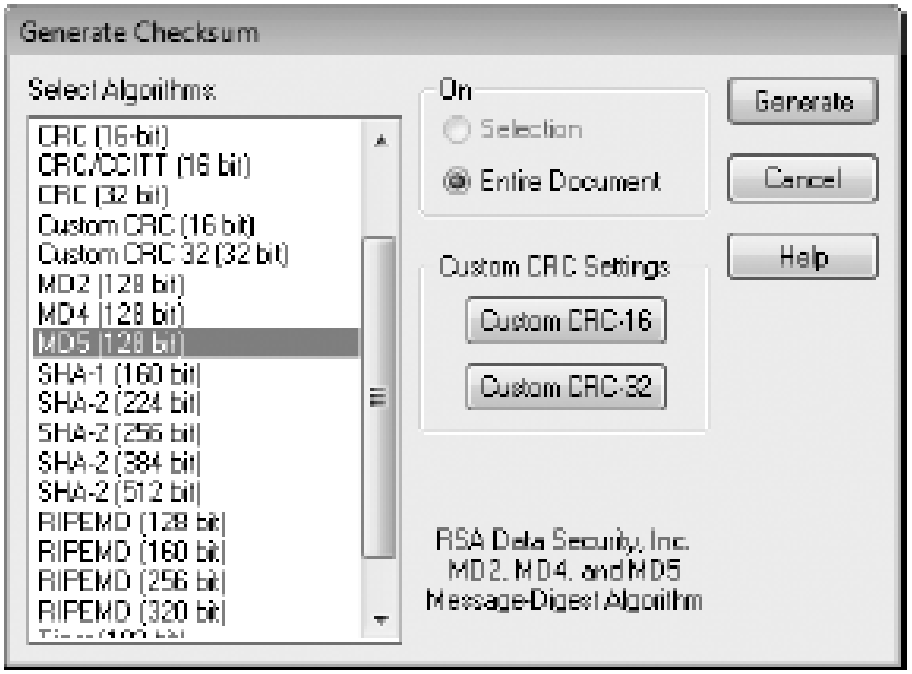

Figure 9-5 The Generate Checksum dialog box

Validating with Hexadecimal Editors (continued)

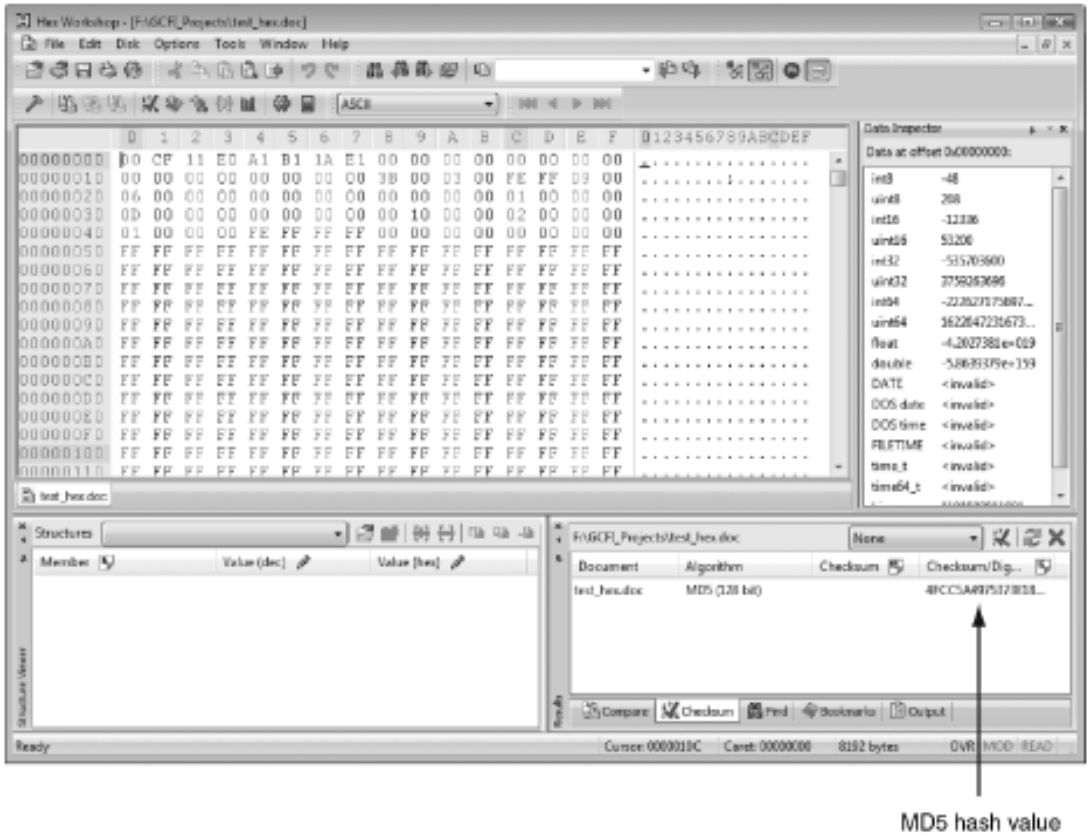

Figure 9-6 Hex Workshop displaying the MD5 hash value

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)

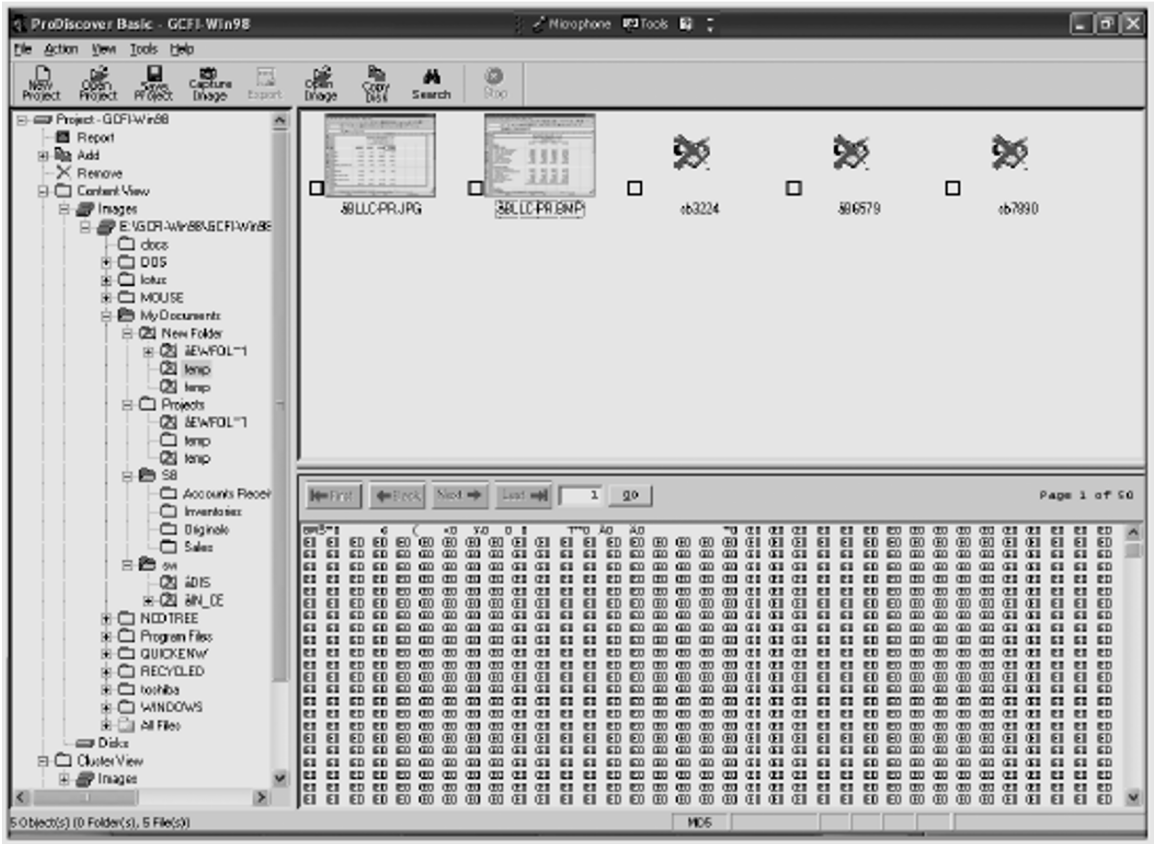

Figure 9-7 ProDiscover's Gallery view

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)

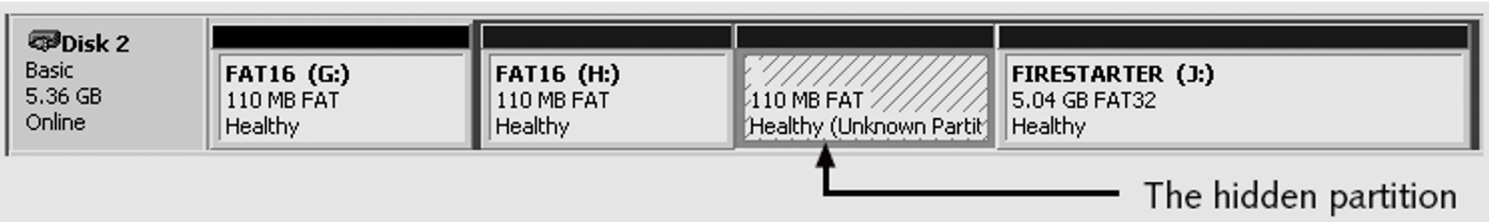

Figure 9-8 Viewing a hidden partition in Disk Manager

Hiding Partitions (continued)

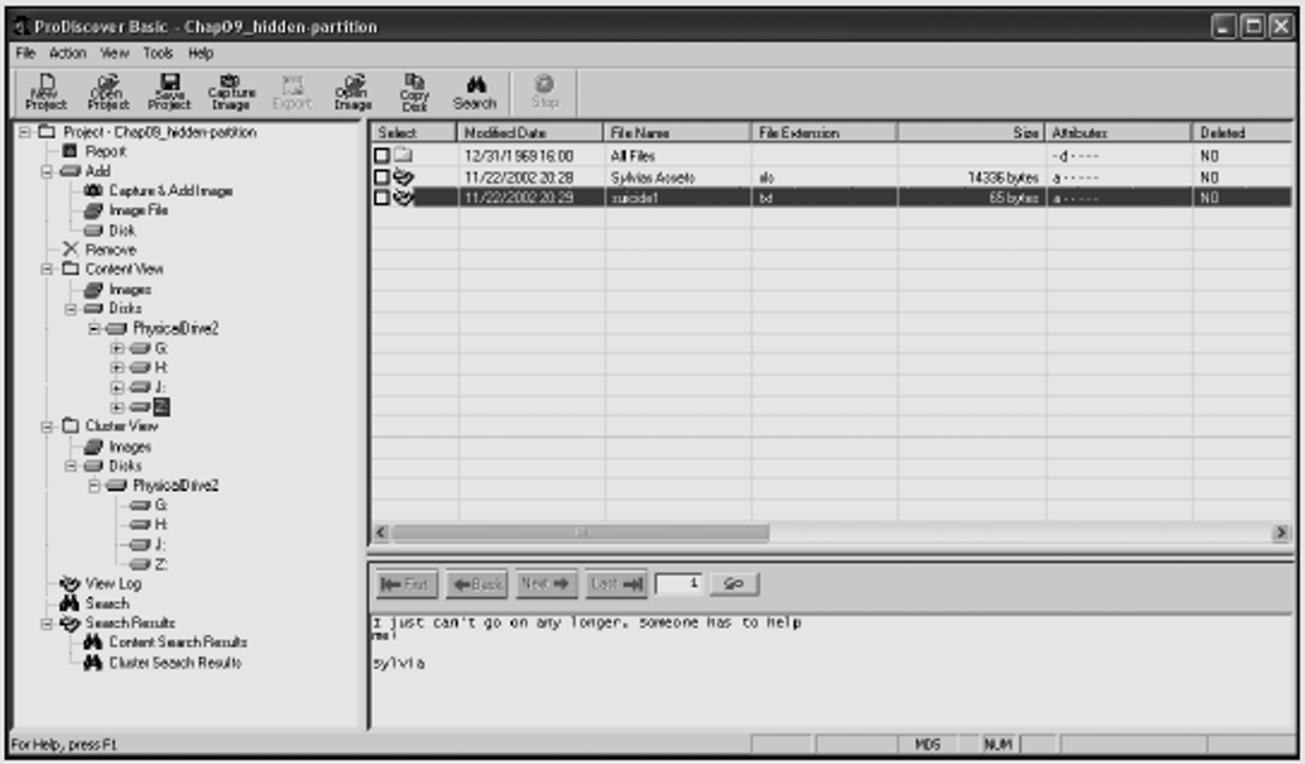

Figure 9-9 Viewing a hidden partition in ProDiscover

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)

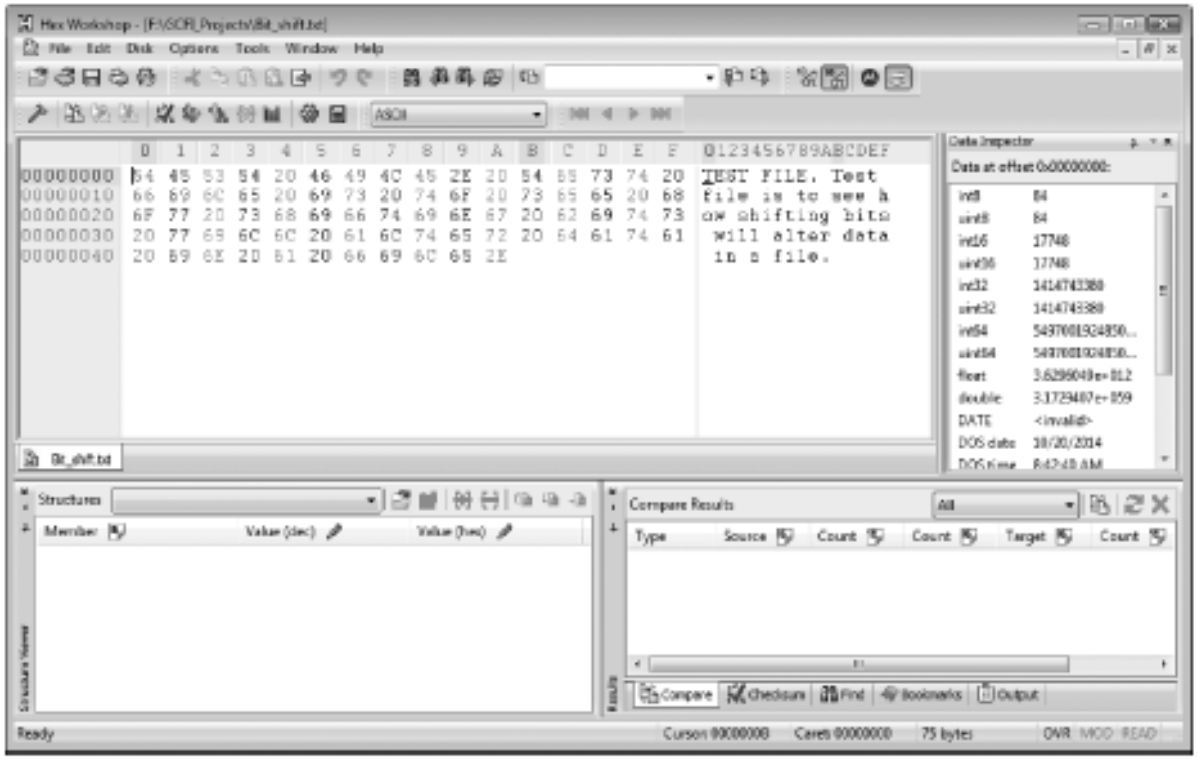

Figure 9-10 Bit_shift.txt open in Hex Workshop

Bit-shifting (continued)

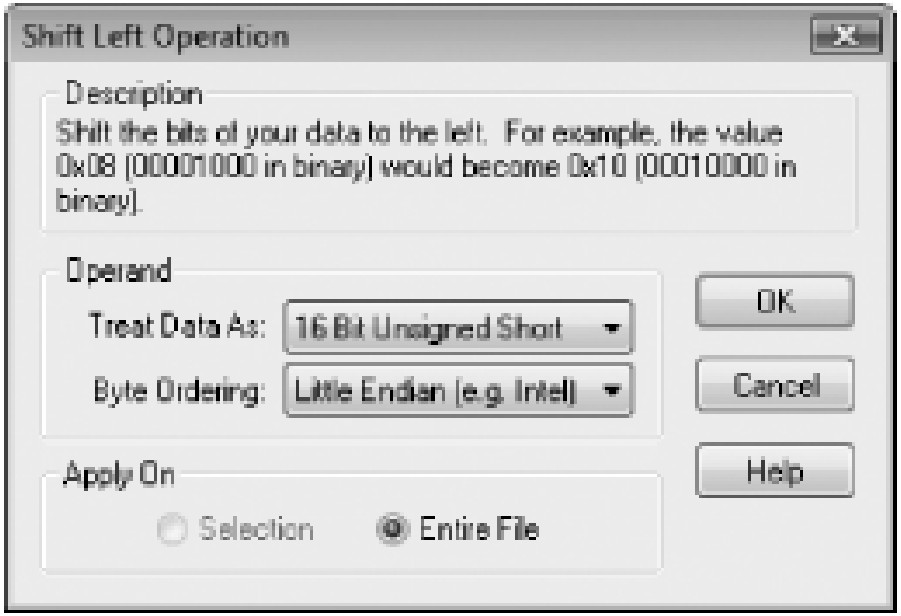

Figure 9-11 The Shift Left Operation dialog box

Bit-shifting (continued)

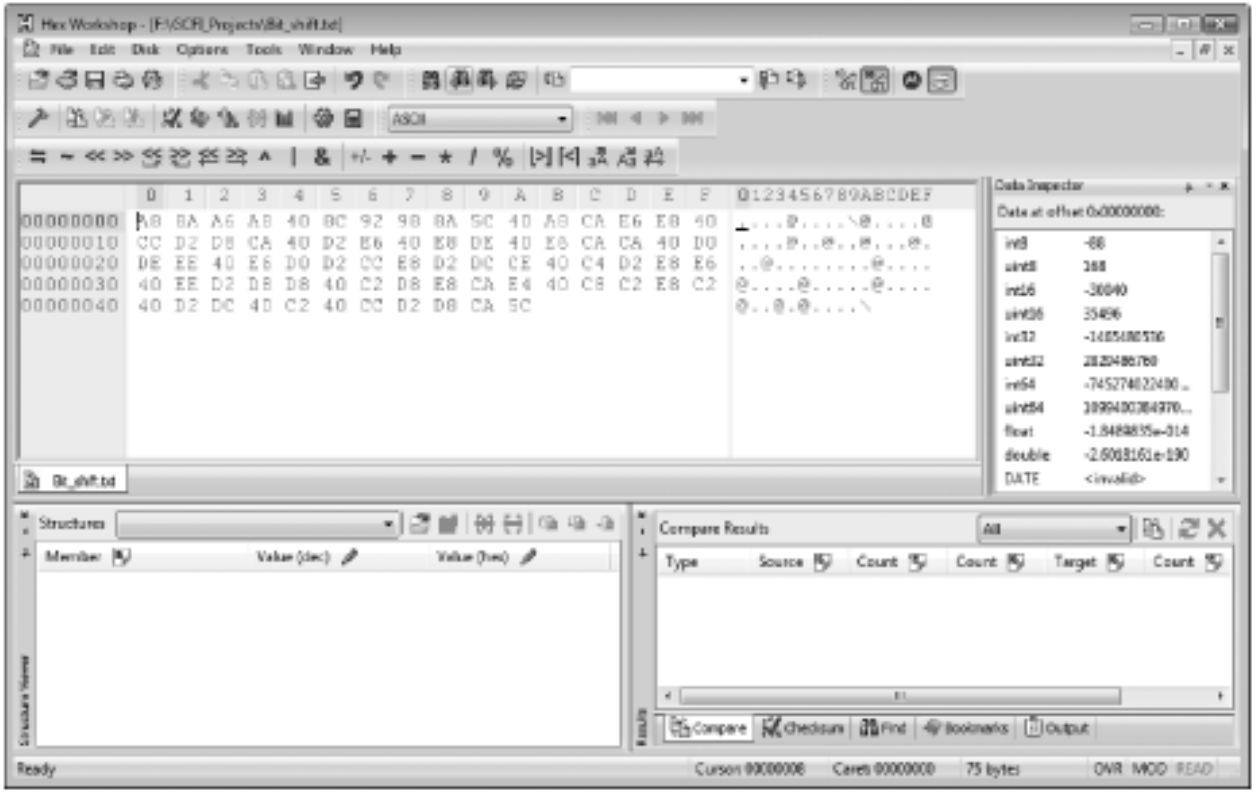

Figure 9-12 Viewing the shifted bits

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)

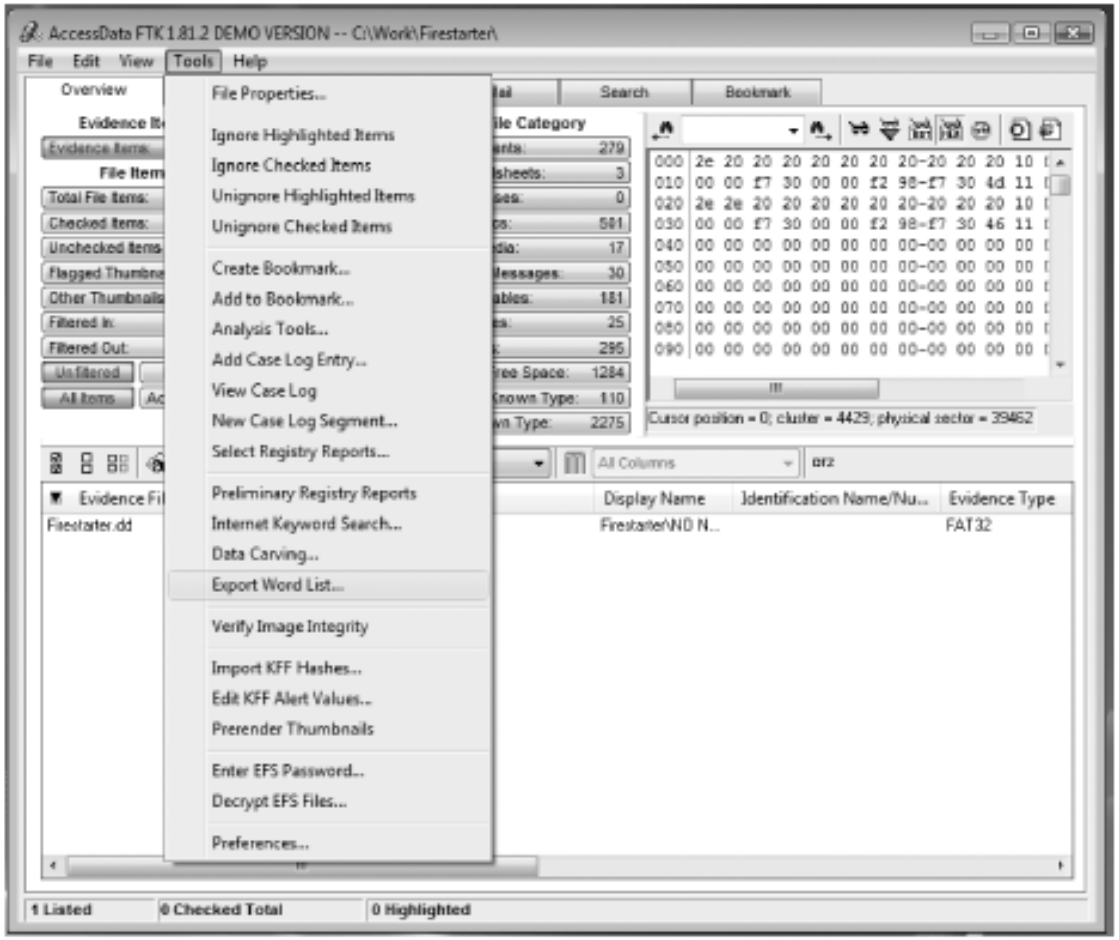

Figure 9-13 Using FTK to generate a password list

Recovering Passwords (continued)

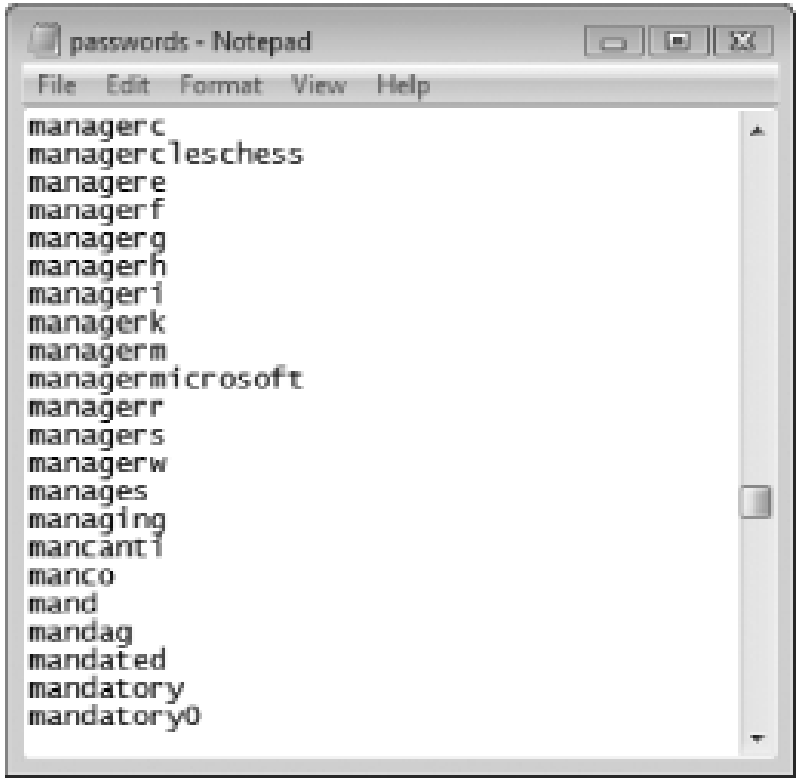

Figure 9-14 A partial list of possible passwords

Recovering Passwords (continued)

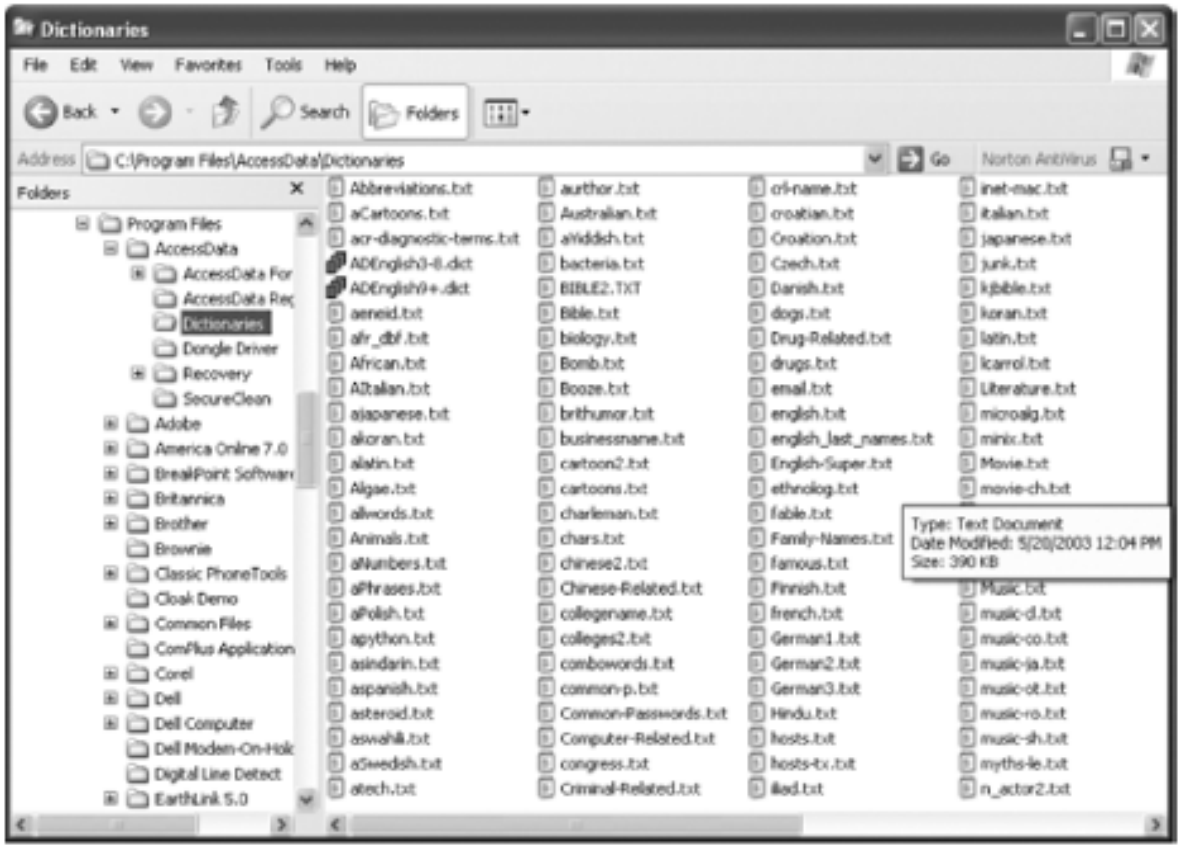

Figure 9-15 Dictionaries available in PRTK

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

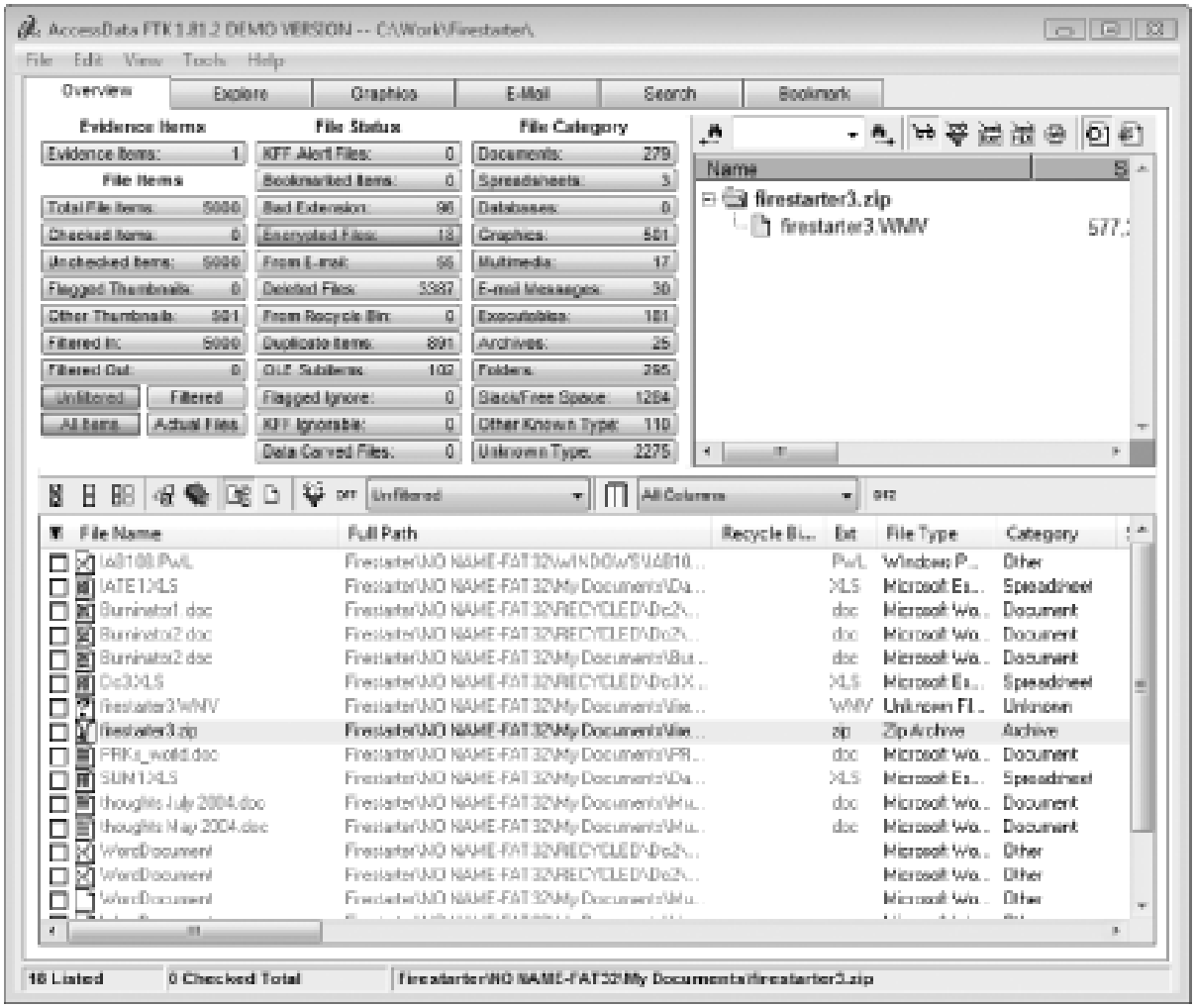

Figure 9-16 FTK displaying encrypted files

Recovering Passwords (continued)

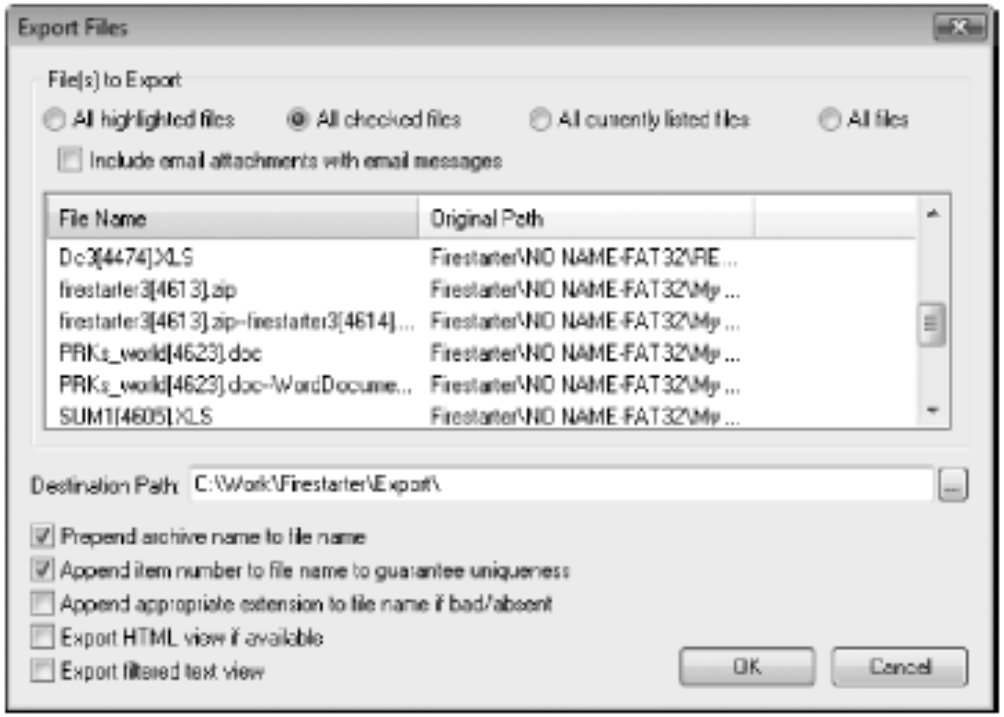

Figure 9-17 Exporting encrypted files

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
- 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)

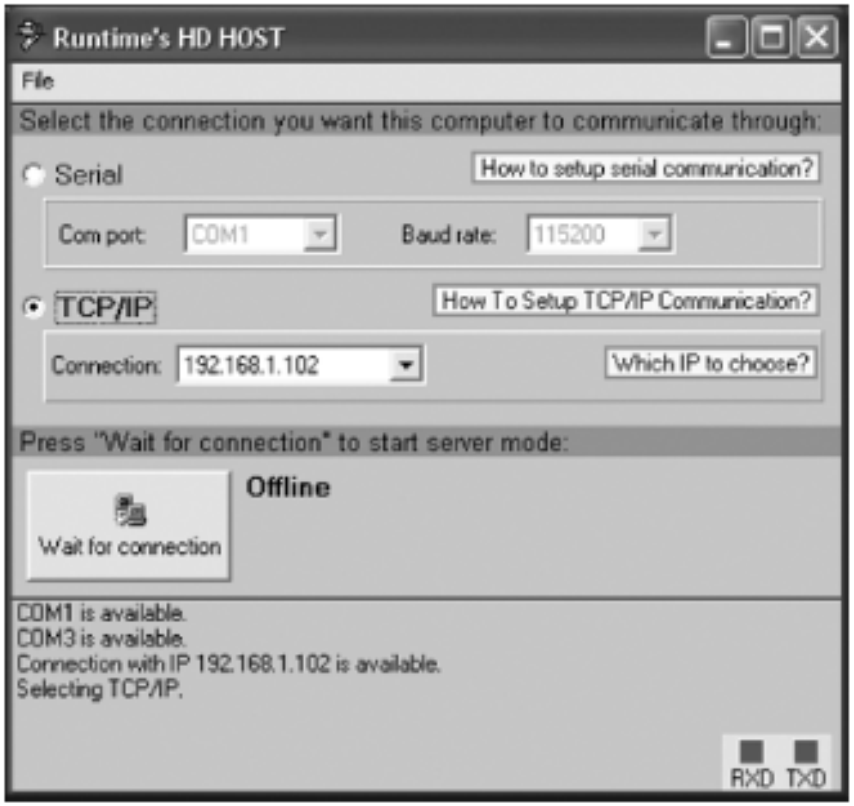

Figure 9-19 Selecting a connection type

Remote Acquisitions with Runtime Software (continued)

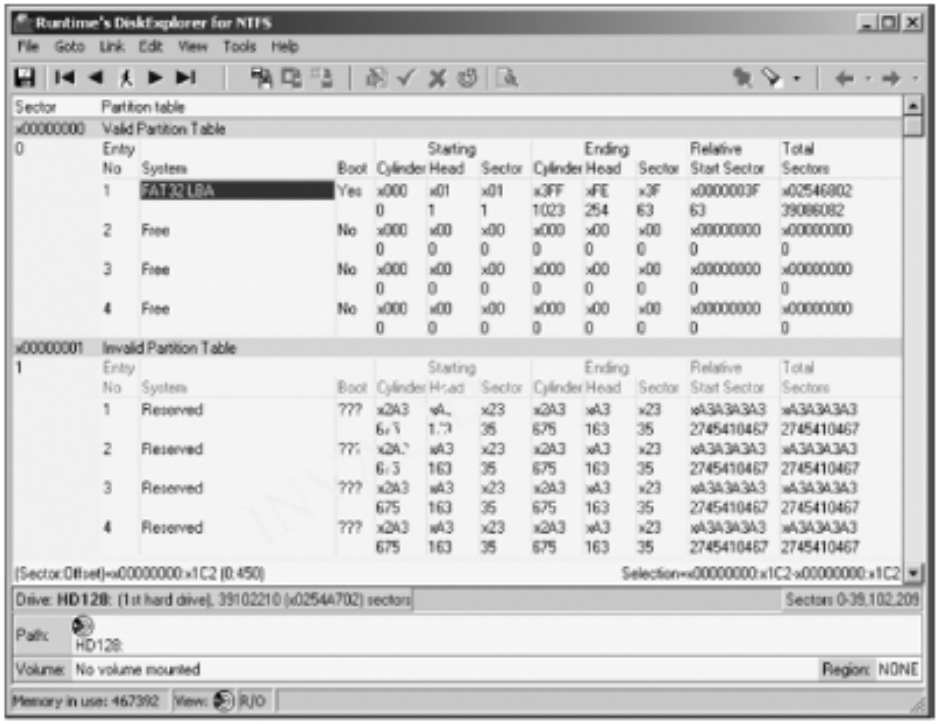

Figure 9-20 The DiskExplorer for NTFS window

Remote Acquisitions with Runtime Software (continued)

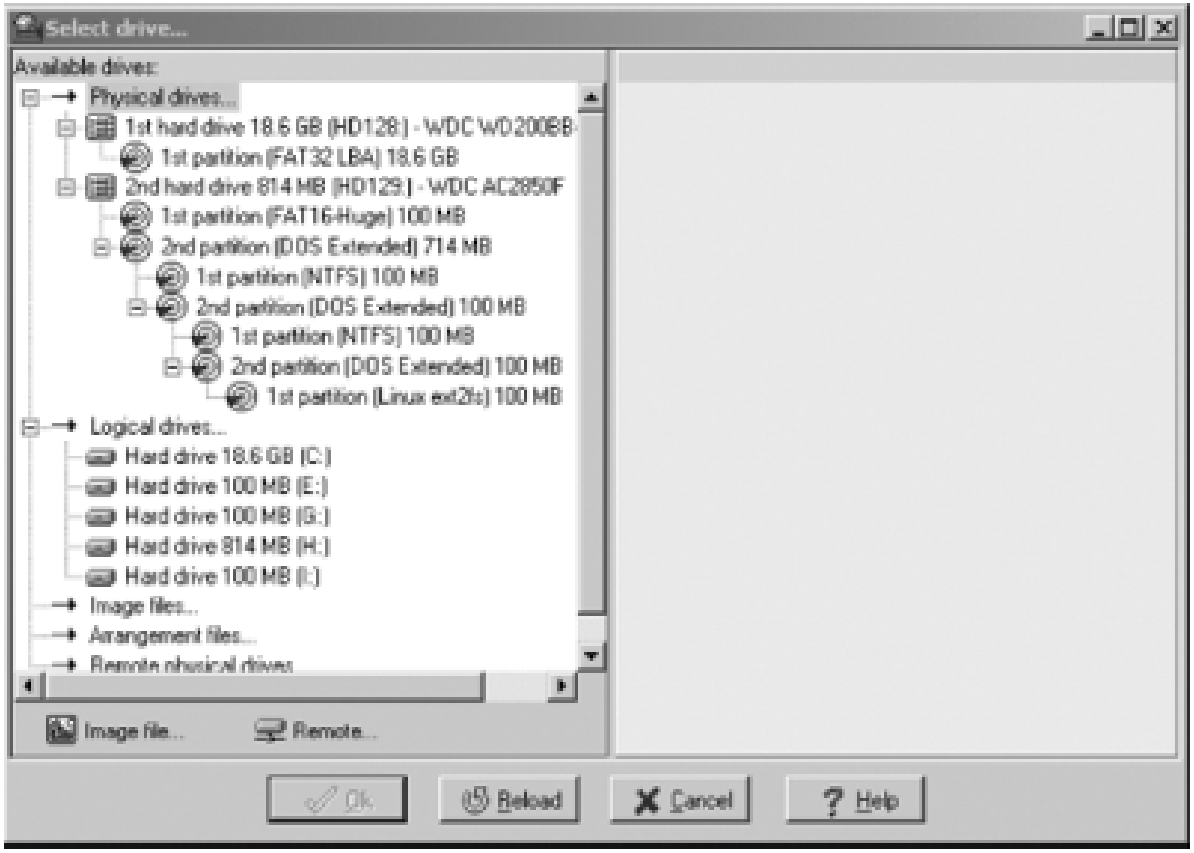

Figure 9-21 The Select drive dialog box

Remote Acquisitions with Runtime Software (continued)

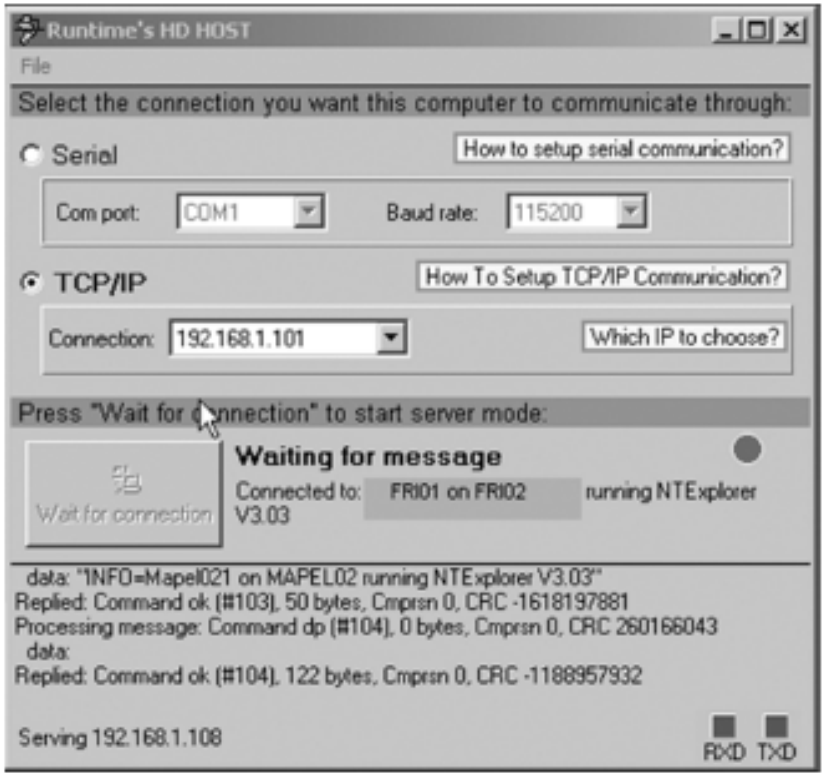

Figure 9-22 The HDHOST remote connection window

Remote Acquisitions with Runtime Software (continued)

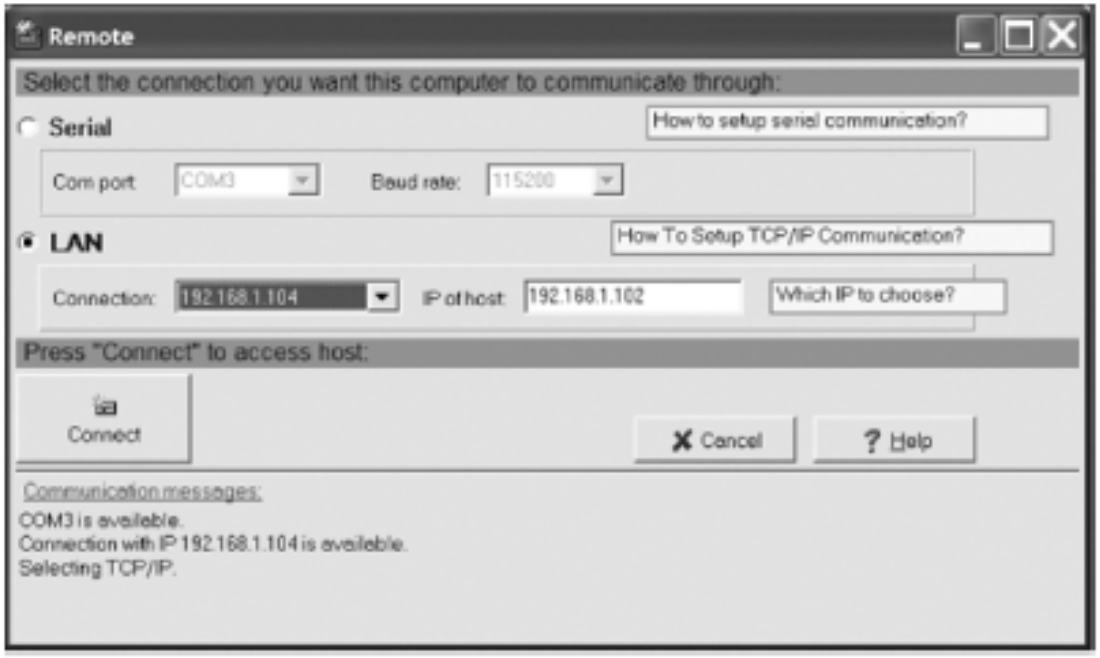

Figure 9-23 Connecting to the remote computer

Remote Acquisitions with Runtime Software (continued)

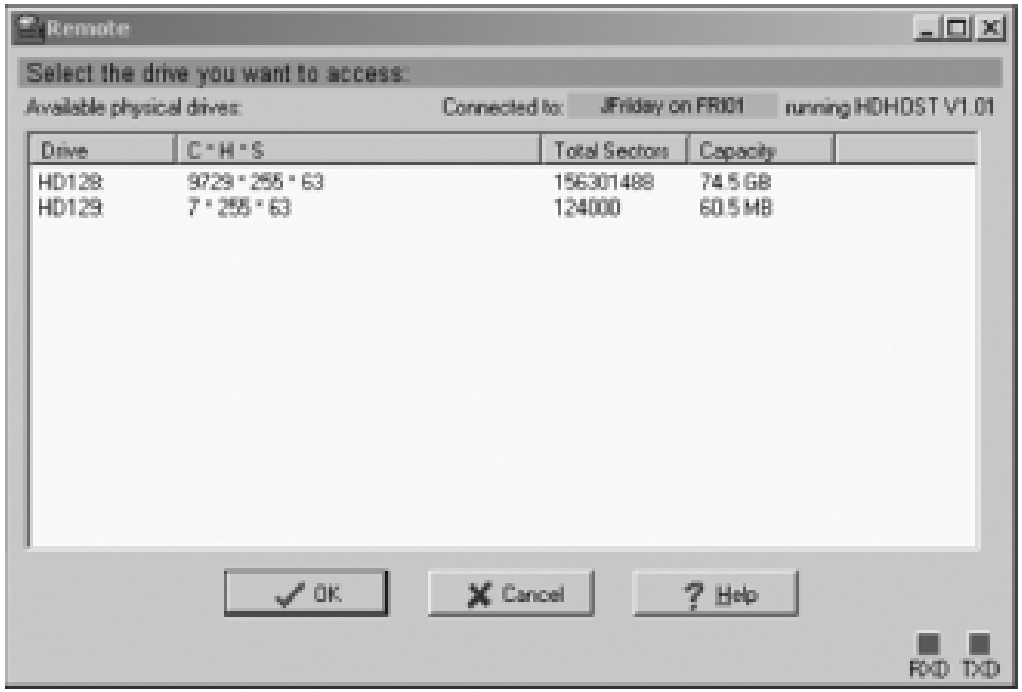

Figure 9-24 Select a drive to access

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)

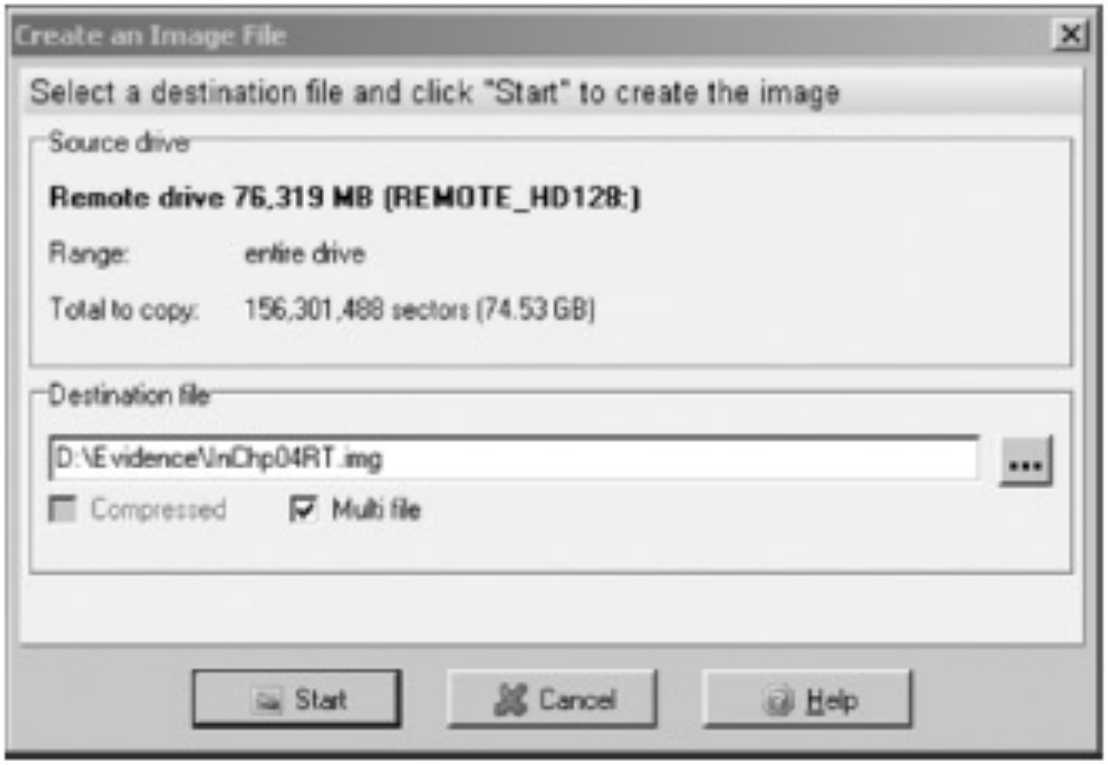

Figure 9-25 The Create an Image File dialog box

Summary

- Examining and analyzing digital evidence depends on the nature of the investigation and the amount of data you have to process
- For most computer forensics investigations, you follow the same general procedures
- One of the most critical aspects of computer forensics is validating digital evidence

Summary (continued)

- Data hiding involves changing or manipulating a file to conceal information
- Remote acquisitions are useful for making an image of a drive when the computer is far away from your location or when you don’t want a suspect to be aware of an ongoing investigation