Guide to Computer Forensics and Investigations Fourth Edition

Chapter 4
Data Acquisition

Modified 9-23-10

Objectives

- List digital evidence storage formats
- Explain ways to determine the best acquisition method
- Describe contingency planning for data acquisitions
- Explain how to use acquisition tools

Objectives (continued)

- Explain how to validate data acquisitions
- Describe RAID acquisition methods
- Explain how to use remote network acquisition tools
- List other forensic tools available for data acquisitions

Understanding Storage Formats for Digital Evidence

Understanding Storage Formats for Digital Evidence

- Two types of data acquisition
  - Static acquisition
    - Copying a hard drive from a powered-off system
    - Used to be the standard
    - Does not alter the data, so it's repeatable
  - Live acquisition
    - Copying data from a running computer
    - Now the preferred type, because of hard disk encryption
    - Cannot be repeated exactly—alters the data
    - Also, collecting RAM data is becoming more important
      - But RAM data has no timestamp, which makes it much harder to use

Understanding Storage Formats for Digital Evidence

- Terms used for a file containing evidence data
  - Bit-stream copy
  - Bit-stream image
  - Image
  - Mirror
  - Sector copy
- They all mean the same thing

Understanding Storage Formats for Digital Evidence

- Three formats
  - Raw format
  - Proprietary formats
  - Advanced Forensics Format (AFF)

Raw Format

- This is what the Linux dd command makes
- Bit-by-bit copy of the drive to a file
- Advantages
  - Fast data transfers
  - Can ignore minor data read errors on source drive
  - Most computer forensics tools can read raw format

Raw Format

- Disadvantages
  - Requires as much storage as original disk or data
  - Tools might not collect marginal (bad) sectors
    - Low threshold of retry reads on weak media spots
    - Commercial tools use more retries than free tools
  - Validation check must be stored in a separate file
    - Message Digest 5 (MD5)
    - Secure Hash Algorithm (SHA-1 or newer)
    - Cyclic Redundancy Check (CRC-32)

Proprietary Formats

- Features offered
  - Option to compress or not compress image files
  - Can split an image into smaller segmented files
    - Such as to CDs or DVDs
    - With data integrity checks in each segment
  - Can integrate metadata into the image file
    - Hash data
    - Date & time of acquisition
    - Investigator name, case name, comments, etc.

Proprietary Formats

- Disadvantages
  - Inability to share an image between different tools
  - File size limitation for each segmented volume
    - Typical segmented file size is 650 MB or 2 GB
- Expert Witness format is the unofficial standard
  - Used by EnCase, FTK, X-Ways Forensics, and SMART
  - Can produce compressed or uncompressed files
  - File extensions **.E01**, **.E02**, **.E03**, …

Advanced Forensics Format

- Developed by Dr. Simson L. Garfinkel of Basis Technology Corporation
- Design goals
  - Provide compressed or uncompressed image files
  - No size restriction for disk-to-image files
  - Provide space in the image file or segmented files for metadata
  - Simple design with extensibility
  - Open source for multiple platforms and OSs

Advanced Forensics Format (continued)

- Design goals (continued)
  - Internal consistency checks for self-authentication
- File extensions include **.afd** for segmented image files and **.afm** for AFF metadata
- AFF is open source

Determining the Best Acquisition Method

Determining the Best Acquisition Method

- Types of acquisitions
  - **Static acquisitions** and **live acquisitions**
- Four methods
  - Bit-stream disk-to-image file
  - Bit-stream disk-to-disk
  - Logical
  - Sparse

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
- Tools: ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLook

Bit-stream disk-to-disk

- Used when disk-to-image copy is not possible
  - Because of hardware or software errors or incompatibilities
  - This problem is more common when acquiring older drives
- Adjusts target disk’s geometry (cylinder, head, and track configuration) to match the suspect's drive
- Tools: EnCase, SafeBack (MS-DOS), Snap Copy

Logical Acquisition and Sparse Acquisition

- When your time is limited, and evidence disk is large
- Logical acquisition captures only specific files of interest to the case
  - Such as Outlook **.pst** or **.ost** files
- Sparse acquisition collects only some of the data
  - I am finding contradictory claims about this—wait until we have a real example for clarity

Compressing Disk Images

- Lossless compression might compress a disk image by 50% or more
- But files that are already compressed, like ZIP files, won’t compress much more
  - Error in textbook: JPEGs use lossy compression and degrade image quality (p. 104)
- Use MD5 or SHA-1 hash to verify the image

Tape Backup

- When working with large drives, an alternative is using tape backup systems
- No limit to size of data acquisition
    - Just use many tapes
- But it’s slow

Returning Evidence Drives

- In civil litigation, a discovery order may require you to return the original disk after imaging it
- If you cannot retain the disk, make sure you make the correct type of copy (logical or bitstream)
  - Ask your client attorney or your supervisor what is required—you usually only have one chance

Contingency Planning for Image Acquisitions

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 (link Ch 4c)
- Be prepared to deal with encrypted drives
  - **Whole disk encryption** feature in Windows Vista Ultimate and Enterprise editions

Encrypted Hard Drives

- Windows BitLocker
- TrueCrypt
- If the machine is on, a live acquisition will capture the decrypted hard drive
- Otherwise, you will need the key or passphrase
  - The suspect may provide it
  - There are some exotic attacks
    - Cold Boot (link Ch 4e)
    - Passware (Ch 4f)
    - Electron microscope (Ch 4g)

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

Windows Write-Protection with USB Devices

- USB write-protection feature
  - Blocks any writing to USB devices
- Target drive needs to be connected to an internal PATA (IDE), SATA, or SCSI controller
- Works in Windows XP SP2, Vista, and Win 7

Acquiring Data with a Linux Boot CD

- Linux can read hard drives that are mounted as read-only
- Windows OSs and newer Linux automatically mount and access a drive
- Windows will write to the Recycle Bin, and sometimes to the NTFS Journal, just from booting up with a hard drive connected
- Linux kernel 2.6 and later write metadata to the drive, such as mount point configurations for an ext2 or ext3 drive
- All these changes corrupt the evidence

Acquiring Data with a Linux Boot CD

- Forensic Linux Live CDs mount all drives read-only
  - Which eliminates the need for a write-blocker
- Using Linux Live CD Distributions
  - Forensic Linux Live CDs
    - Contain additional utilities

Forensic Linux Live CDs

- Configured not to mount, or to mount as read-only, any connected storage media
- Well-designed Linux Live CDs for computer forensics
  - Helix
  - Penguin Sleuth
  - FCCU (French interface)
- Preparing a target drive for acquisition in Linux
  - Modern linux distributions can use Microsoft FAT and NTFS partitions

Acquiring Data with a Linux Boot CD (continued)

- Preparing a target drive for acquisition in Linux (continued)
  - **fdisk** command lists, creates, deletes, and verifies partitions in Linux
  - **mkfs.msdos** command formats a FAT file system from Linux
- Acquiring data with dd in Linux
  - dd (“data dump”) command
    - Can read and write from media device and data file
    - Creates raw format file that most computer forensics analysis tools can read

Acquiring data with dd in Linux

- Shortcomings of dd command
  - Requires more advanced skills than average user
  - Does not compress data
- dd command combined with the split command
  - Segments output into separate volumes
- dd command is intended as a data management tool
  - Not designed for forensics acquisitions

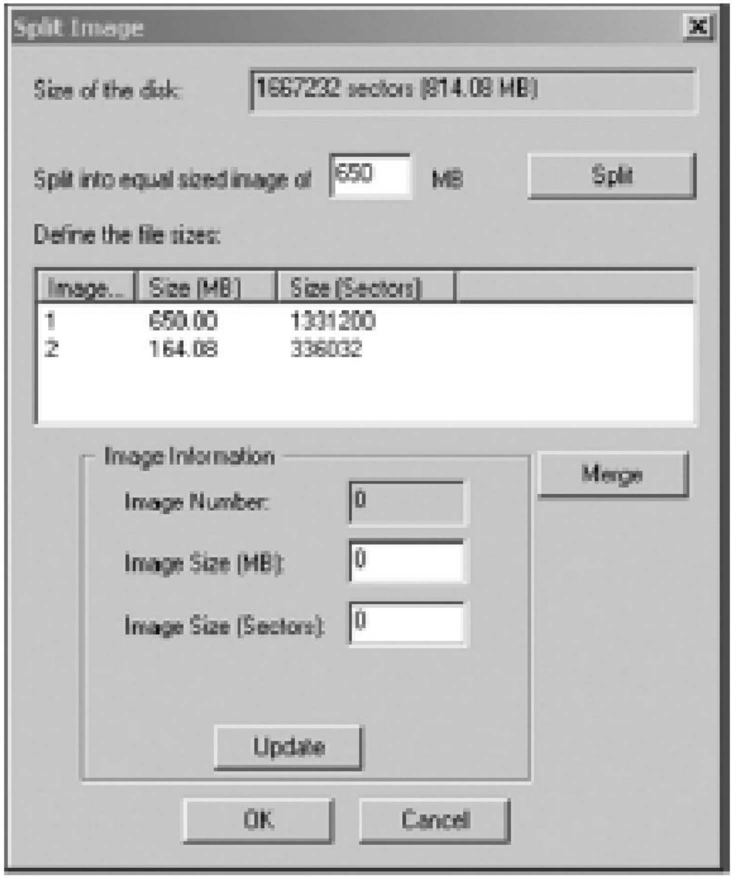
Acquiring data with dcfldd in Linux

- dcfldd additional functions
  - Specify hex patterns or text for clearing disk space
  - Log errors to an output file for analysis and review
  - Use several hashing options
  - Refer to a status display indicating the progress of the acquisition in bytes
  - Split data acquisitions into segmented volumes with numeric extensions
  - Verify acquired data with original disk or media data

Capturing an Image with ProDiscover Basic

- Connecting the suspect’s drive to your workstation
  - Document the chain of evidence for the drive
  - Remove the drive from the suspect’s computer
  - Configure the suspect drive’s jumpers as needed
  - Connect the suspect drive to a **write-blocker device**
  - Create a storage folder on the target drive
- Using ProDiscover’s Proprietary Acquisition Format
  - Image file will be split into segments of 650MB
  - Creates image files with an .eve extension, a log file (.log extension), and a special inventory file (.pds extension)

Capturing an Image with ProDiscover Basic (continued)



Size of the disk: 1667232 sectors (814.08 MB)

Split into equal sized image of 650 MB

Define the file sizes:

Image...	Size (MB)	Size (Sectors)
1	650.00	1331200
2	164.08	336032

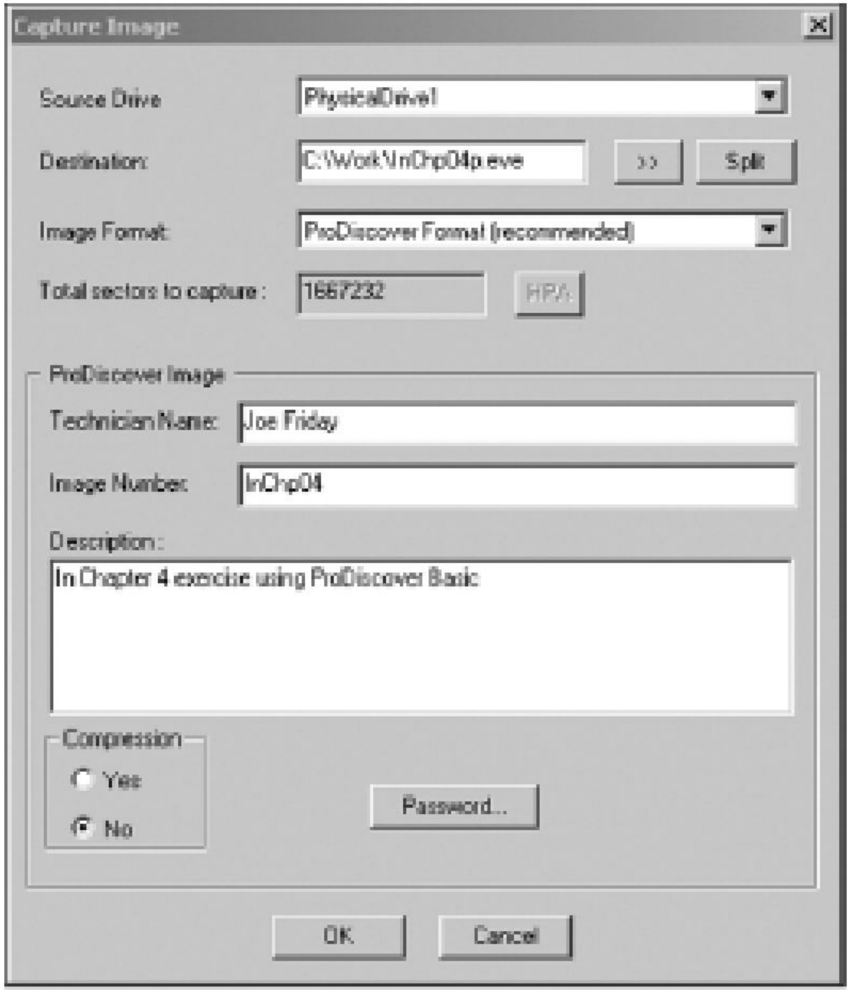
Image Information

Image Number: 0

Image Size (MB): 0

Image Size (Sectors): 0

Figure 4-4 The Split Image dialog box



Source Drive: PhysicalDrive1

Destination: C:\Work\InChp04p.eve

Image Format: ProDiscover Format (recommended)

Total sectors to capture : 1667232

Technician Name: Joe Friday

Image Number: InChp04

Description : In Chapter 4 exercise using ProDiscover Basic

○ Yes

● No

Figure 4-5 The Capture Image dialog box

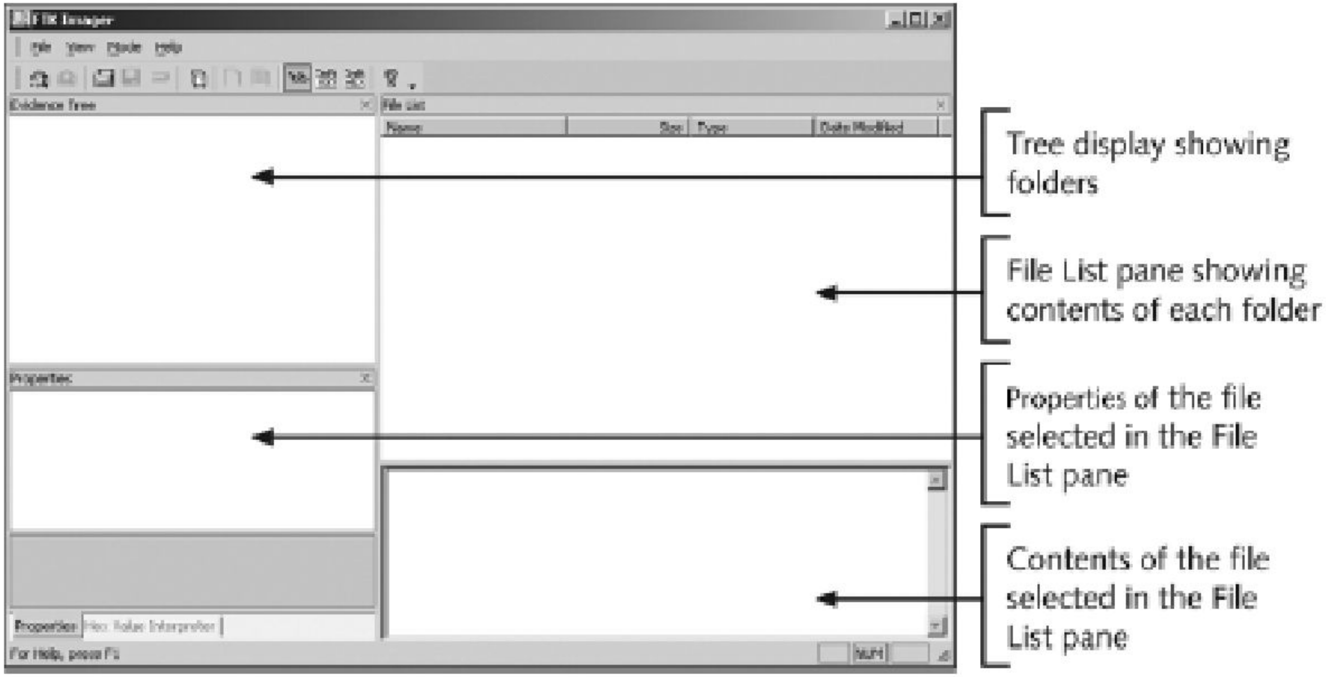
Capturing an Image with ProDiscover Basic (continued)

- Using ProDiscover’s Raw Acquisition Format
  - Select the UNIX style dd format in the Image Format list box
  - Raw acquisition saves only the image data and hash value

Capturing an Image with AccessData FTK Imager

- Included on AccessData Forensic Toolkit
- View evidence disks and disk-to-image files
- Makes disk-to-image copies of evidence drives
  - At logical partition and physical drive level
  - Can segment the image file
- Evidence drive must have a **hardware write-blocking device**
  - Or the USB write-protection Registry feature enabled
- FTK Imager can’t acquire drive’s host protected area (but ProDiscover can)

Capturing an Image with AccessData FTK Imager (continued)



Tree display showing folders

File List pane showing contents of each folder

Properties of the file selected in the File List pane

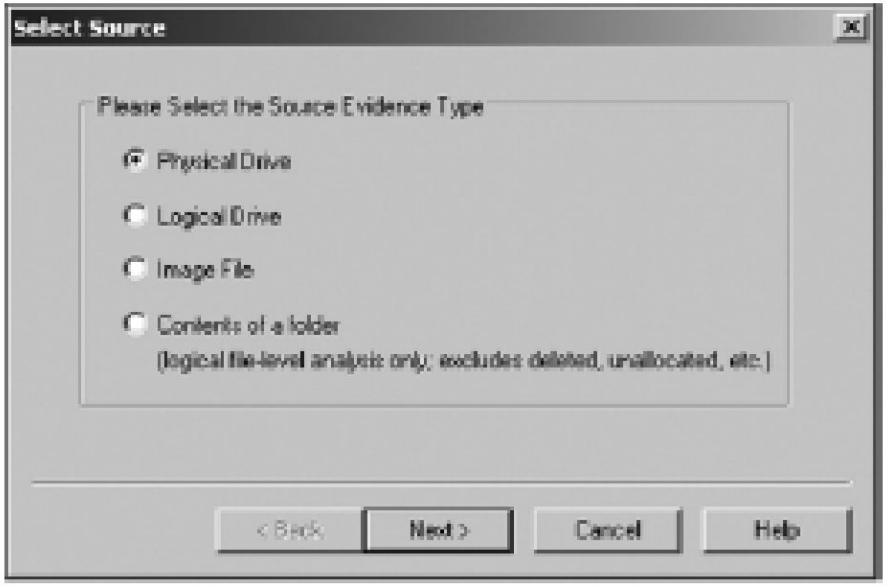
Contents of the file selected in the File List pane

Figure 4-6 The FTK Imager main window

Capturing an Image with AccessData FTK Imager (continued)

- Steps
  - Boot to Windows
  - Connect evidence disk to a write-blocker
  - Connect target disk
  - Start FTK Imager
  - Create Disk Image
    - Use Physical Drive option

Capturing an Image with AccessData FTK Imager (continued)



Select Source

Please Select the Source Evidence Type

● Physical Drive

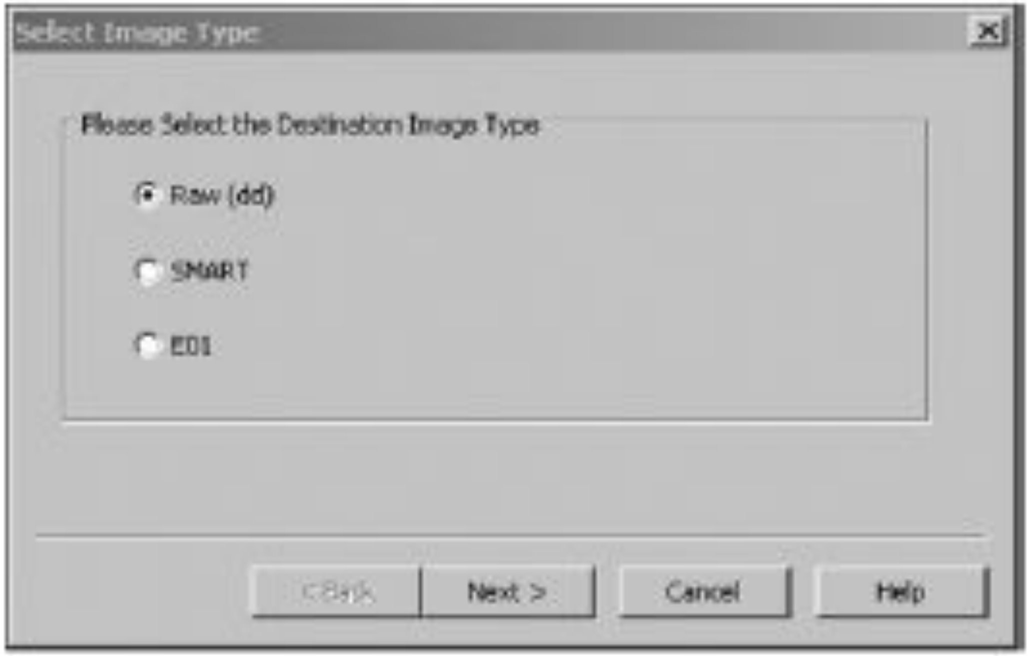
○ Logical Drive

○ Image File

○ Contents of a folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Figure 4-7 The Select Source dialog box

Capturing an Image with AccessData FTK Imager (continued)



Please Select the Destination Image Type

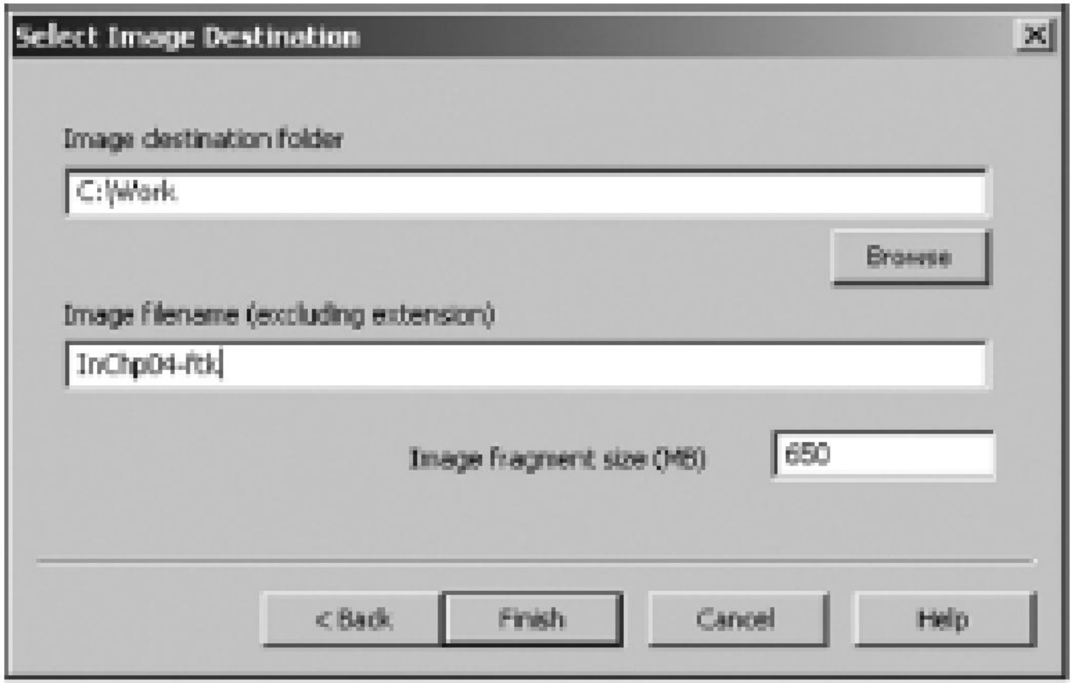
● Raw (dd)

○ SMART

○ E01

Figure 4-8 The Select Image Type dialog box

Capturing an Image with AccessData FTK Imager (continued)



Select Image Destination

Image destination folder: C:\Work

Image filename (excluding extension): InChp04-ftk

Image fragment size (MB): 650

Figure 4-9 Selecting where to save the image file

Capturing an Image with AccessData FTK Imager (continued)

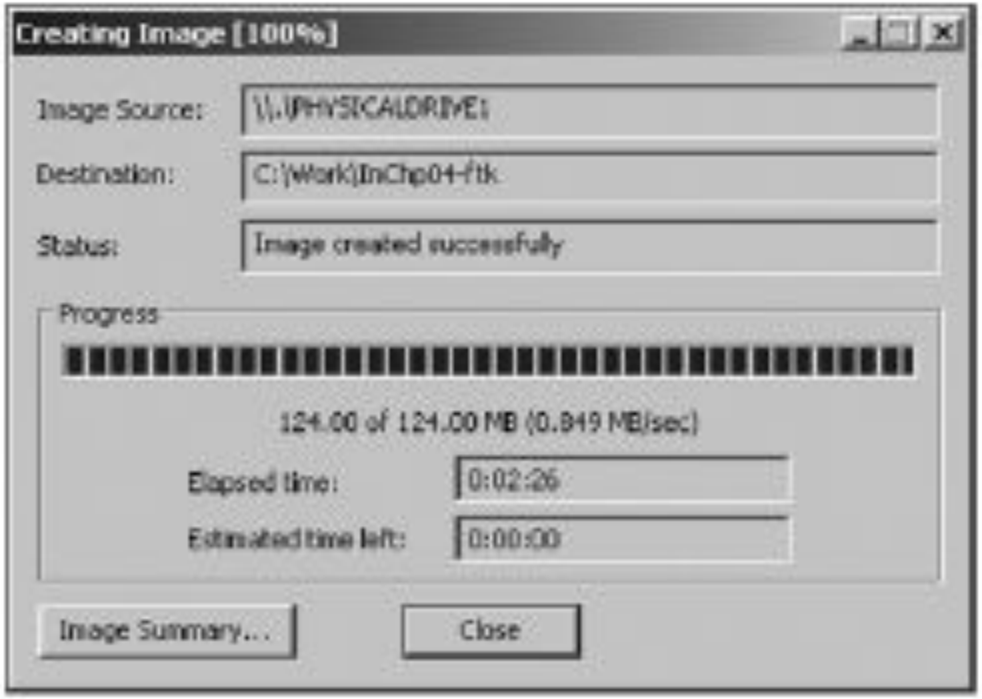


Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Work\InChp04-ftk

Status: Image created successfully

124.00 of 124.00 MB (0.849 MB/sec)

Elapsed time: 0:02:26

Estimated time left: 0:00:00

Figure 4-10 A completed image save

Validating Data Acquisitions

Validating Data Acquisitions

- Most critical aspect of computer forensics
- Requires using a hashing algorithm utility
- Validation techniques
  - CRC-32, MD5, and SHA-1 to SHA-512
- MD5 has collisions, so it is not perfect, but it’s still widely used
- SHA-1 has some collisions but it’s better than MD5
- A new hashing function will soon be chosen by NIST

Linux Validation Methods

- Validating dd acquired data
  - You can use md5sum or sha1sum utilities
  - md5sum or sha1sum utilities should be run on all suspect disks and volumes or segmented volumes
- Validating dcfldd acquired data
  - Use the hash option to designate a hashing algorithm of md5, sha1, sha256, sha384, or sha512
  - hashlog option outputs hash results to a text file that can be stored with the image files
  - vf (verify file) option compares the image file to the original medium

Windows Validation Methods

- Windows has no built-in hashing algorithm tools for computer forensics
  - Third-party utilities can be used
- Commercial computer forensics programs also have built-in validation features
  - Each program has its own validation technique
- Raw format image files don’t contain metadata
  - Separate manual validation is recommended for all raw acquisitions

Performing RAID Data Acquisitions

Performing RAID Data Acquisitions

- Size is the biggest concern
  - Many RAID systems now have terabytes of data

Understanding RAID

- **Redundant array of independent** (formerly "inexpensive") **disks (RAID)**
  - Computer configuration involving two or more disks
  - Originally developed as a data-redundancy measure
- RAID 0 (Striped)
  - Provides rapid access and increased storage
  - Lack of redundancy
- RAID 1 (Mirrored)
  - Designed for data recovery
  - More expensive than RAID 0

Understanding RAID (continued)

- RAID 2
  - Similar to RAID 1
  - Data is written to a disk on a bit level
  - Has better data integrity checking than RAID 0
  - Slower than RAID 0
- RAID 3
  - Uses data striping and dedicated parity
- RAID 4
  - Data is written in blocks

Understanding RAID (continued)

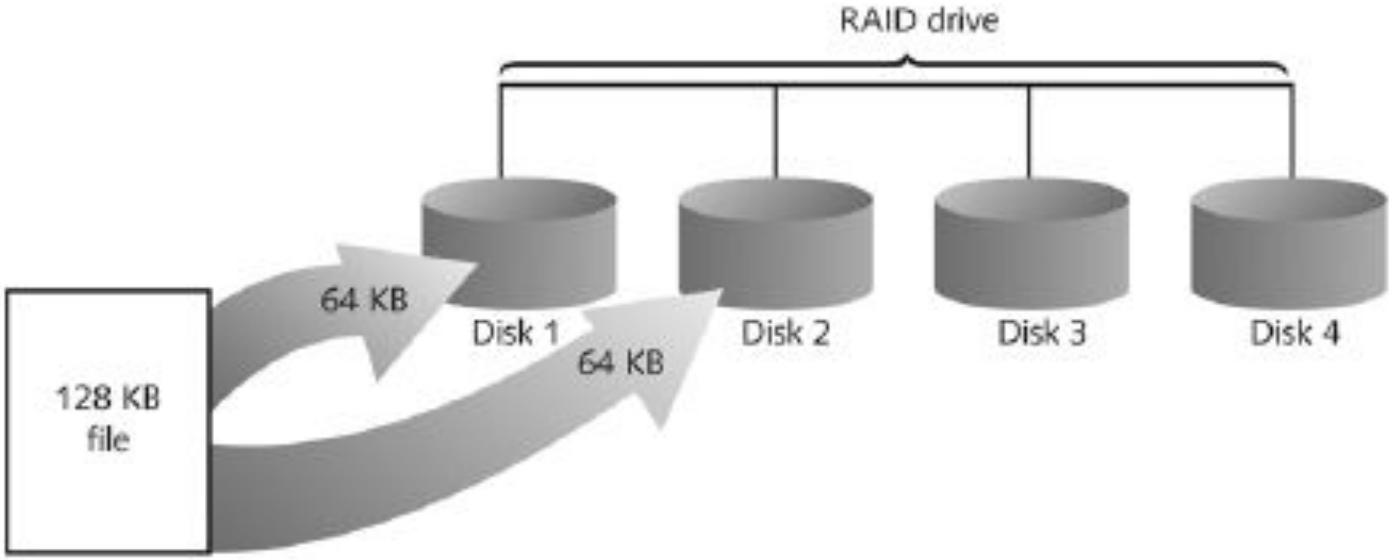


Figure 4-11 RAID 0: Striping

Understanding RAID (continued)

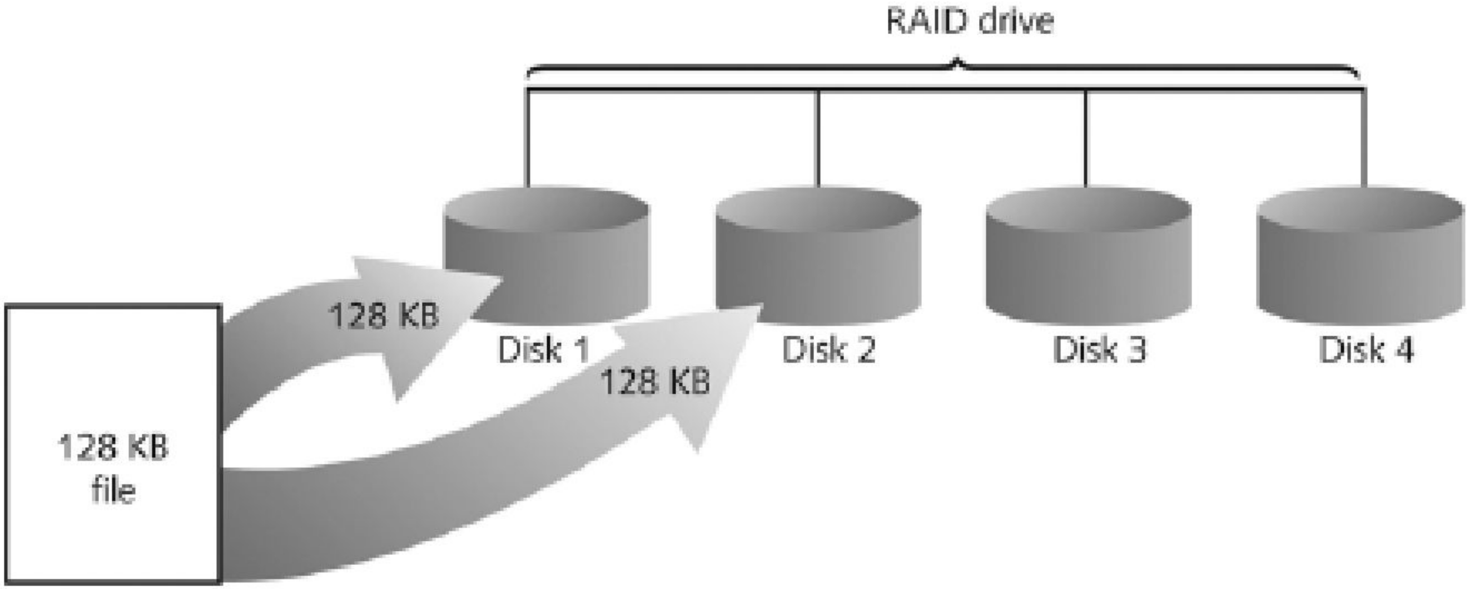


Figure 4-12 RAID 1: Mirroring

Understanding RAID (continued)

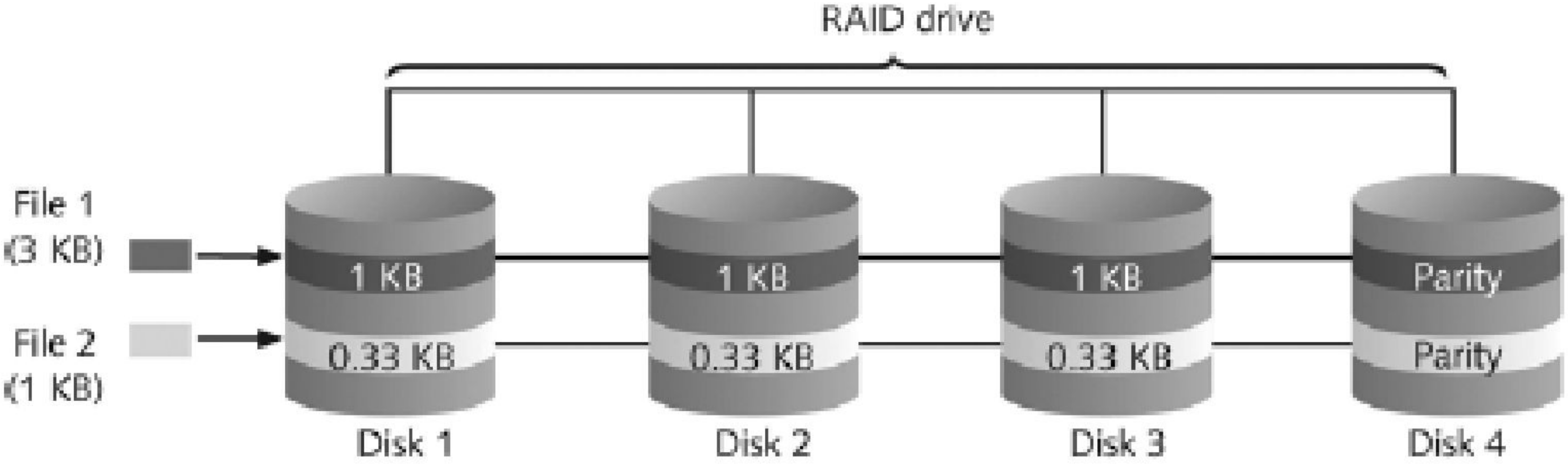


Figure 4-13 RAID 2: Striping (bit level)

Understanding RAID (continued)

- RAID 5
  - Similar to RAIDs 0 and 3
  - Places parity recovery data on each disk
- RAID 6
  - Redundant parity on each disk
- RAID 10, or mirrored striping
  - Also known as RAID 1+0
  - Combination of RAID 1 and RAID 0

Understanding RAID (continued)

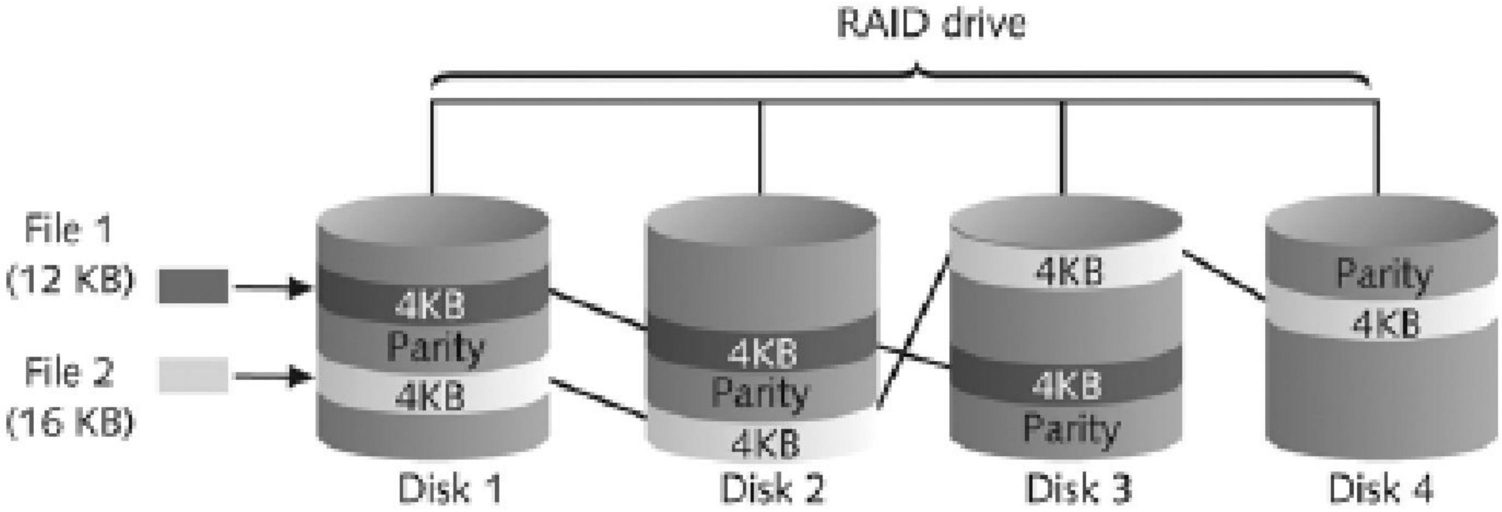


Figure 4-14 RAID 5: Block-level striping with distributed parity

Acquiring RAID Disks

- Concerns
  - How much data storage is needed?
  - What type of RAID is used?
  - Do you have the right acquisition tool?
  - Can the tool read a forensically copied RAID image?
  - Can the tool read split data saves of each RAID disk?
- Older hardware-firmware RAID systems can be a challenge when you’re making an image

Acquiring RAID Disks (continued)

- Vendors offering RAID acquisition functions
  - Technologies Pathways ProDiscover
  - Guidance Software EnCase
  - X-Ways Forensics
  - Runtime Software
  - R-Tools Technologies
- Occasionally, a RAID system is too large for a static acquisition
  - Retrieve only the data relevant to the investigation with the sparse or logical acquisition method

Using Remote Network Acquisition Tools

Using Remote Network Acquisition Tools

- You can remotely connect to a suspect computer via a network connection and copy data from it
- Remote acquisition tools vary in configurations and capabilities
- Drawbacks
  - LAN’s data transfer speeds and routing table conflicts could cause problems
  - Gaining the permissions needed to access more secure subnets
  - Heavy traffic could cause delays and errors
  - Remote access tool could be blocked by antivirus

Remote Acquisition with ProDiscover Investigator

- Preview a suspect’s drive remotely while it’s in use
- Perform a live acquisition
  - Also called a “smear” because data is being altered
- Encrypt the connection
- Copy the suspect computer’s RAM
- Use the optional stealth mode to hide the connection

Remote Acquisition with ProDiscover Incident Response

- All the functions of ProDiscover Investigator plus
  - Capture volatile system state information
  - Analyze current running processes
  - Locate unseen files and processes
  - Remotely view and listen to IP ports
  - Run hash comparisons to find Trojans and rootkits
  - Create a hash inventory of all files remotely

PDServer Remote Agent

- ProDiscover utility for remote access
- Needs to be loaded on the suspect computer
- PDServer installation modes
  - Trusted CD
  - Preinstallation
  - Pushing out and running remotely
- PDServer can run in a stealth mode
  - Can change process name to appear as OS function

Remote Connection Security Features

- Password Protection
- Encrypted communications
- Secure Communication Protocol
- Write Protected Trusted Binaries
- Digital Signatures

Remote Acquisition with EnCase Enterprise

- Remotely acquires media and RAM data
- Integration with intrusion detection system (IDS) tools
- Options to create an image of data from one or more systems
- Preview of systems
- A wide range of file system formats
- RAID support for both hardware and software

Other Remote Acquisition Tools

- R-Tools R-Studio
- WetStone LiveWire
- F-Response

Remote Acquisition with Runtime Software

- Compact Shareware Utilities
  - DiskExplorer for FAT
  - DiskExplorer for NTFS
  - HDHOST (Remote access program)
- Features for acquisition
  - Create a raw format image file
  - Segment the raw format or compressed image
  - Access network computers' drives

Using Other Forensics-Acquisition Tools

Using Other Forensics-Acquisition Tools

- Tools
  - SnapBack DatArrest
  - SafeBack
  - DIBS USA RAID
  - ILook Investigator IXimager
  - Vogon International SDi32
  - ASRData SMART
  - Australian Department of Defence PyFlag

SnapBack DatArrest

- Columbia Data Products
- Old MS-DOS tool
- Can make an image on three ways
  - Disk to SCSI drive
  - Disk to network drive
  - Disk to disk
- Fits on a forensic boot floppy
- SnapCopy adjusts disk geometry

NTI SafeBack

- Reliable MS-DOS tool
- Small enough to fit on a forensic boot floppy
- Performs an SHA-256 calculation per sector copied
- Creates a log file

NTI SafeBack (continued)

- Functions
  - Disk-to-image copy (image can be on tape)
  - Disk-to-disk copy (adjusts target geometry)
    - Parallel port laplink can be used
  - Copies a partition to an image file
  - Compresses image files

DIBS USA RAID

- Rapid Action Imaging Device (RAID)
  - Makes forensically sound disk copies
  - Portable computer system designed to make disk-to-disk images
  - Copied disk can then be attached to a write-blocker device

ILook Investigator IXimager

- Iximager
  - Runs from a bootable floppy or CD
  - Designed to work only with ILook Investigator
  - Can acquire single drives and RAID drives

ASRData SMART

- Linux forensics analysis tool that can make image files of a suspect drive
- Capabilities
  - Robust data reading of bad sectors on drives
  - Mounting suspect drives in write-protected mode
  - Mounting target drives in read/write mode
  - Optional compression schemes

Australian Department of Defence PyFlag

- PyFlag tool
  - Intended as a network forensics analysis tool
  - Can create proprietary format Expert Witness image files
  - Uses sgzip and gzip in Linux