Guide to Computer Forensics and Investigations Fourth Edition

Chapter 4
Data Acquisition

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

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

Raw Format

- Makes it possible to write bit-stream data to files
- Advantages
  - Fast data transfers
  - Can ignore minor data read errors on source drive
  - Most computer forensics tools can read raw format
- Disadvantages
  - Requires as much storage as original disk or data
  - Tools might not collect marginal (bad) sectors

Proprietary Formats

- Features offered
  - Option to compress or not compress image files
  - Can split an image into smaller segmented files
  - Can integrate metadata into the image file
- Disadvantages
  - Inability to share an image between different tools
  - File size limitation for each segmented volume

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

- Types of acquisitions
  - **Static acquisitions** and **live acquisitions**
- Four methods
  - 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

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

Windows XP 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
- Steps to update the Registry for Windows XP SP2
  - Back up the Registry
  - Modify the Registry with the write-protection feature
  - Create two desktop icons to automate switching between enabling and disabling writes to USB device

Windows XP Write-Protection with USB Devices (continued)

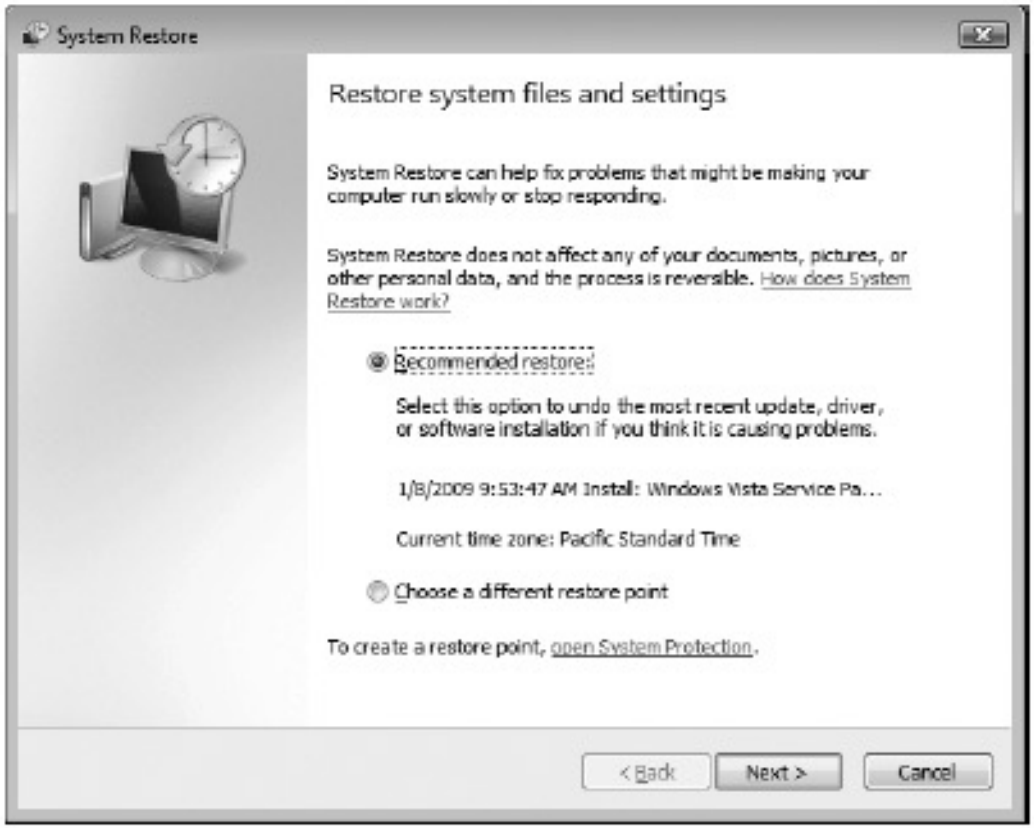

Figure 4-2 The System Restore Wizard

Acquiring Data with a Linux Boot CD

- Linux can access a drive that isn't mounted
- Windows OSs and newer Linux automatically mount and access a drive
- Forensic Linux Live CDs don't access media automatically
  - Which eliminates the need for a write-blocker
- Using Linux Live CD Distributions
  - Forensic Linux Live CDs
    - Contain additionally utilities

Acquiring Data with a Linux Boot CD (continued)

- Using Linux Live CD Distributions (continued)
  - Forensic Linux Live CDs (continued)
    - 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
- Preparing a target drive for acquisition in Linux
  - Linux distributions can create Microsoft FAT and NTFS partition tables

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 a Linux Boot CD (continued)

- Acquiring data with dd in Linux (continued)
  - 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
- Acquiring data with dcfldd in Linux
  - dd command is intended as a data management tool
    - Not designed for forensics acquisitions

Acquiring Data with a Linux Boot CD (continued)

- Acquiring data with dcfldd in Linux (continued)
  - 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
  - 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)

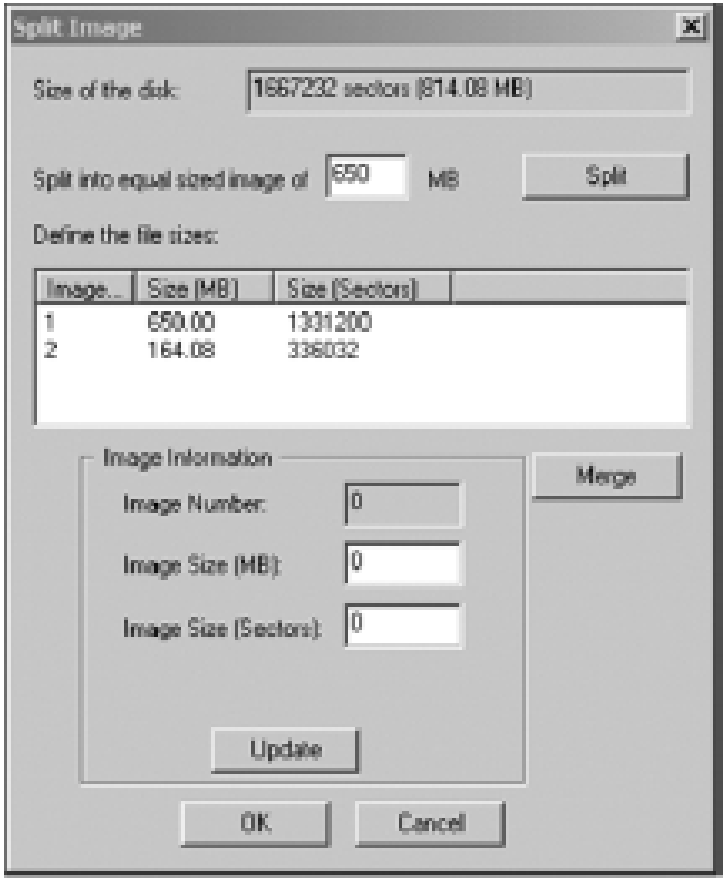

Figure 4-4 The Split Image dialog box

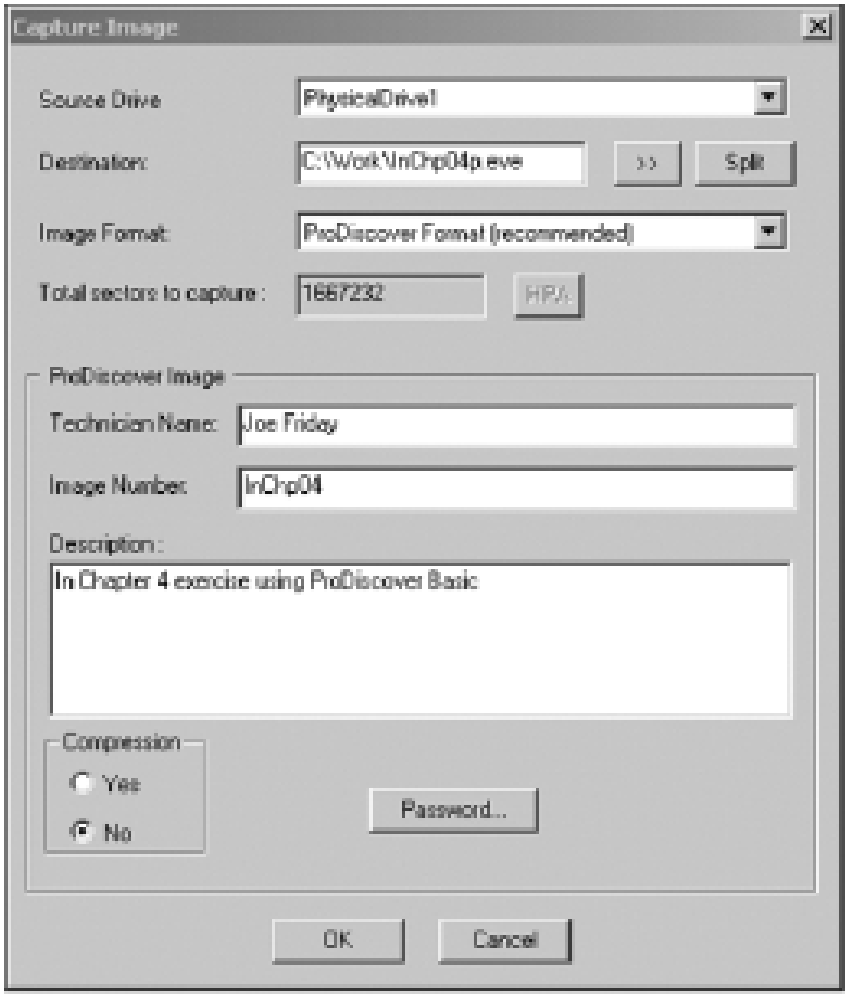

Figure 4-5 The Capture Image dialog box

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

Capturing an Image with AccessData FTK Imager (continued)

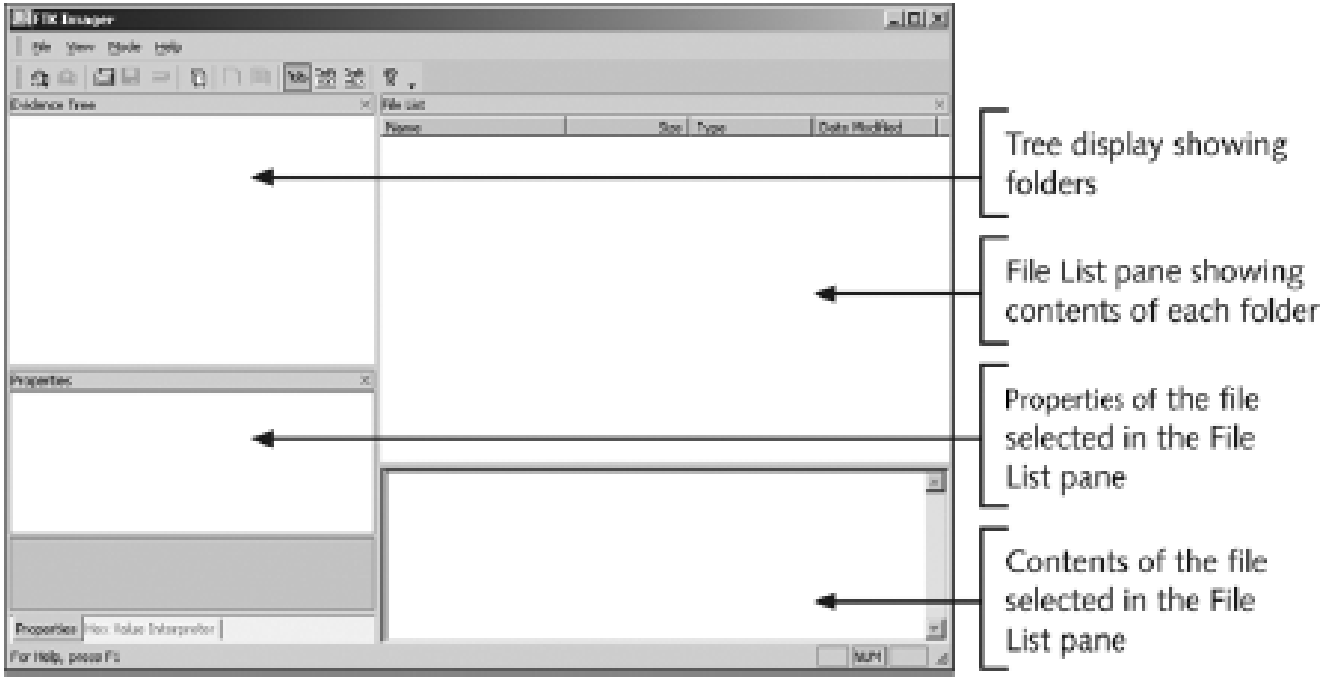

Figure 4-6 The FTK Imager main window

Capturing an Image with AccessData FTK Imager (continued)

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

Capturing an Image with AccessData FTK Imager (continued)

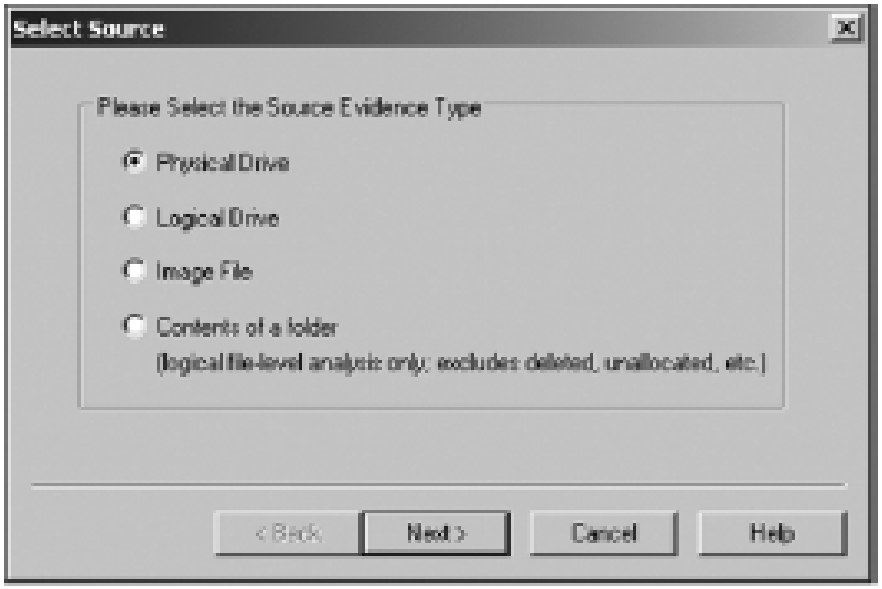

Figure 4-7 The Select Source dialog box

Capturing an Image with AccessData FTK Imager (continued)

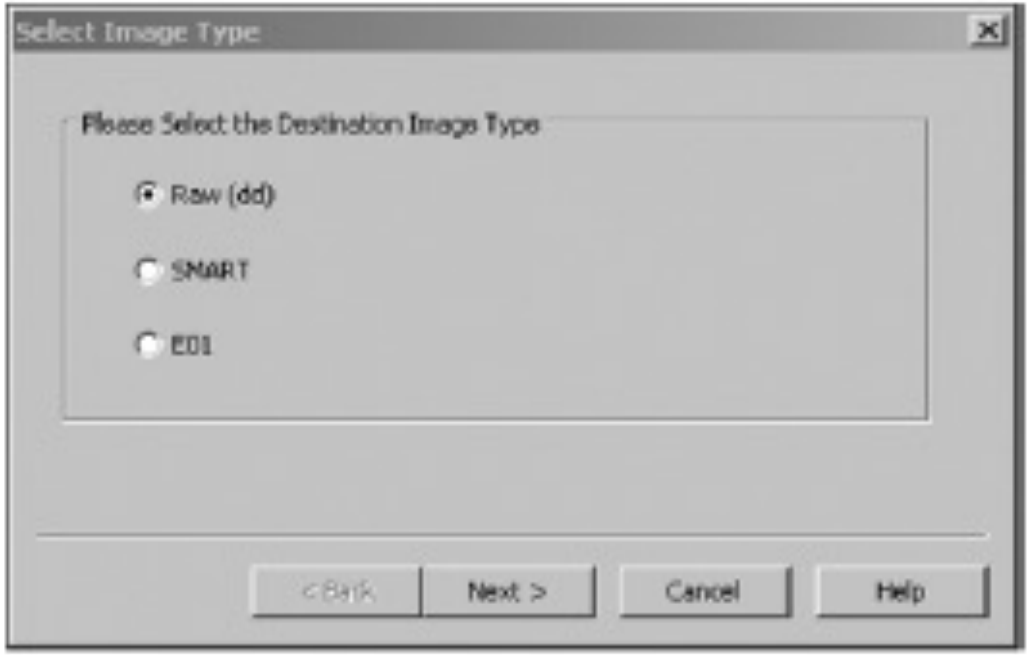

Figure 4-8 The Select Image Type dialog box

Capturing an Image with AccessData FTK Imager (continued)

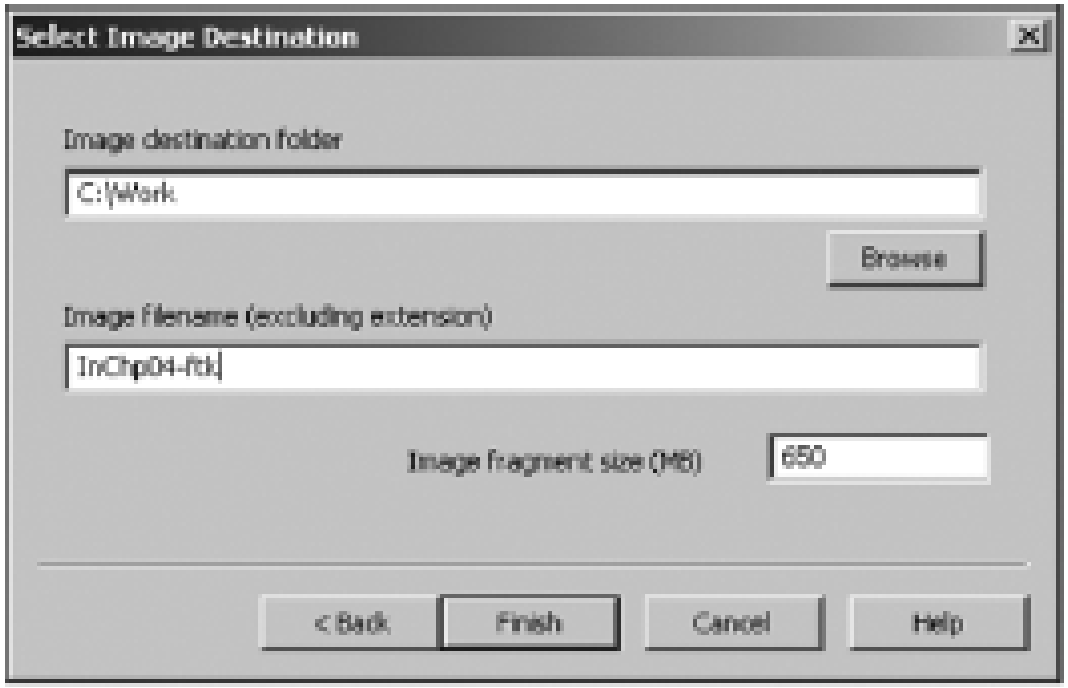

Figure 4-9 Selecting where to save the image file

Capturing an Image with AccessData FTK Imager (continued)

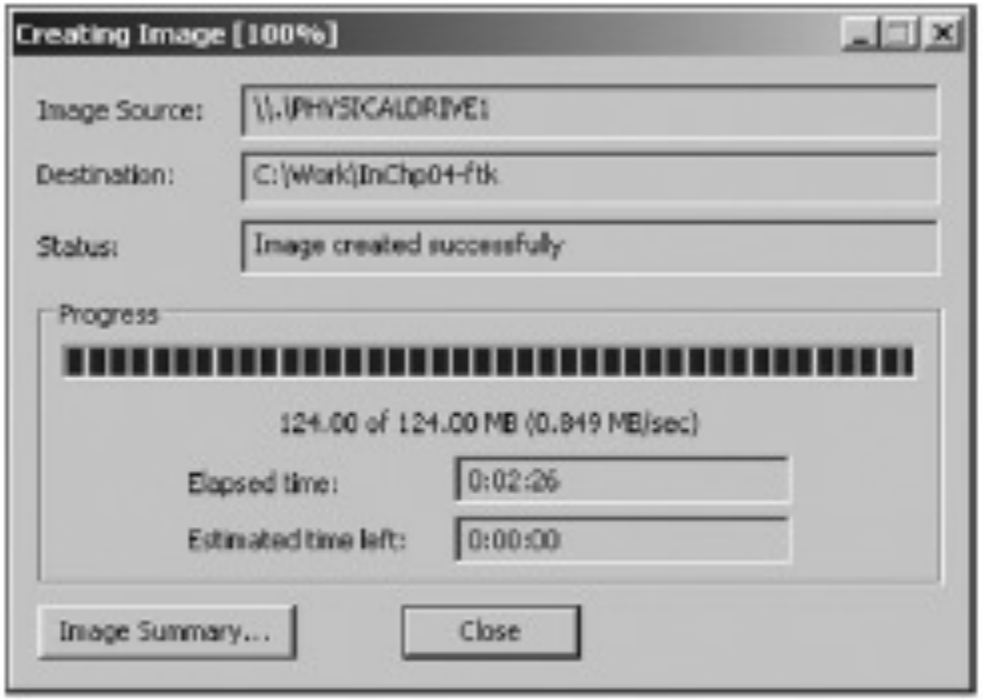

Figure 4-10 A completed image save

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

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

- 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
  - Provides rapid access and increased storage
  - Lack of redundancy
- RAID 1
  - 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 stripping and dedicated parity
- RAID 4
  - Data is written in blocks

Understanding RAID (continued)

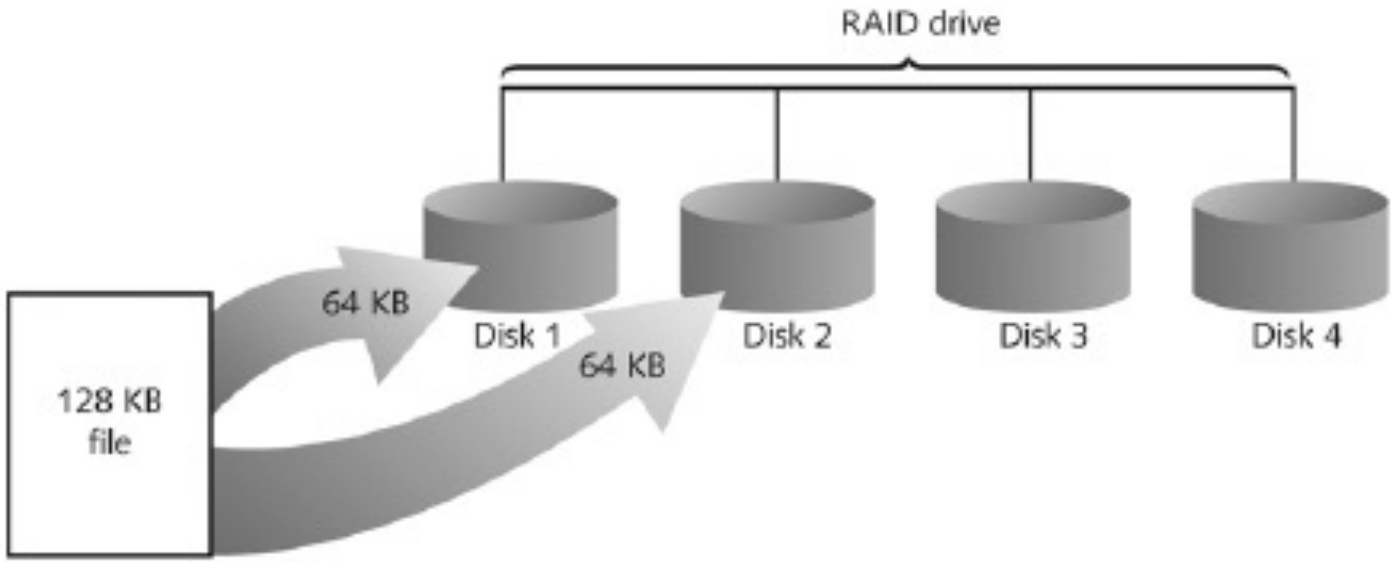

Figure 4-11 RAID 0: Striping

Understanding RAID (continued)

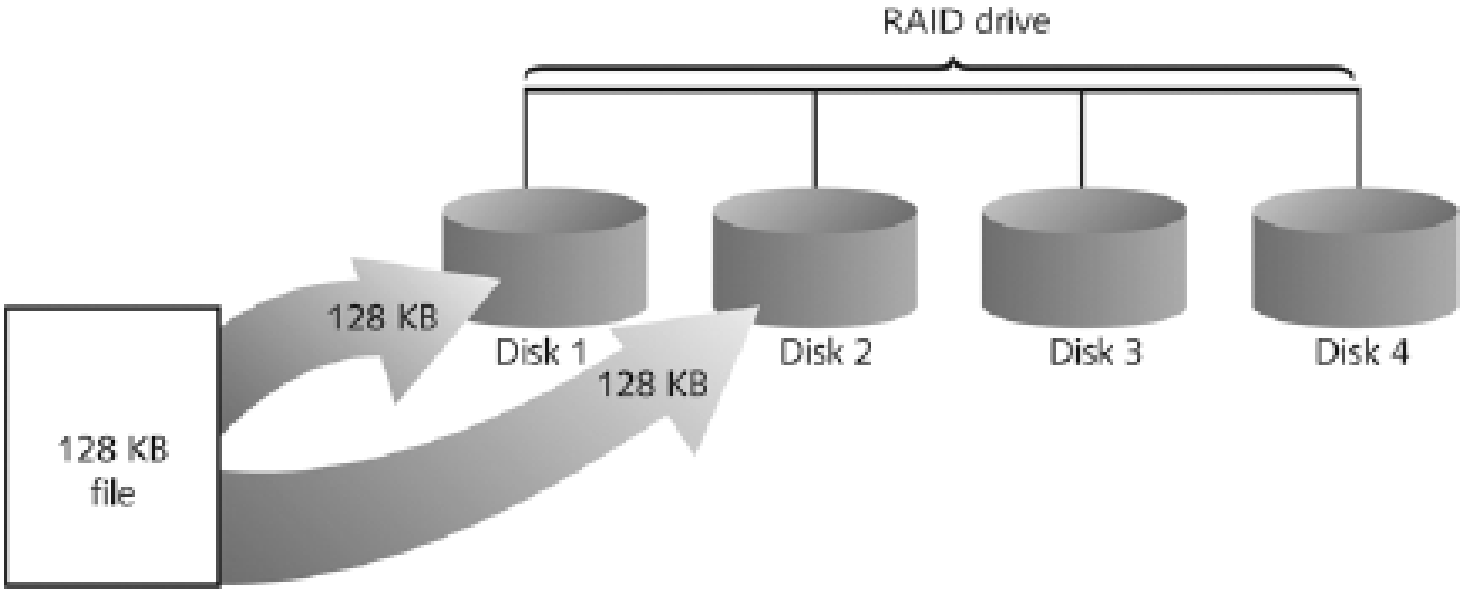

Figure 4-12 RAID 1: Mirroring

Understanding RAID (continued)

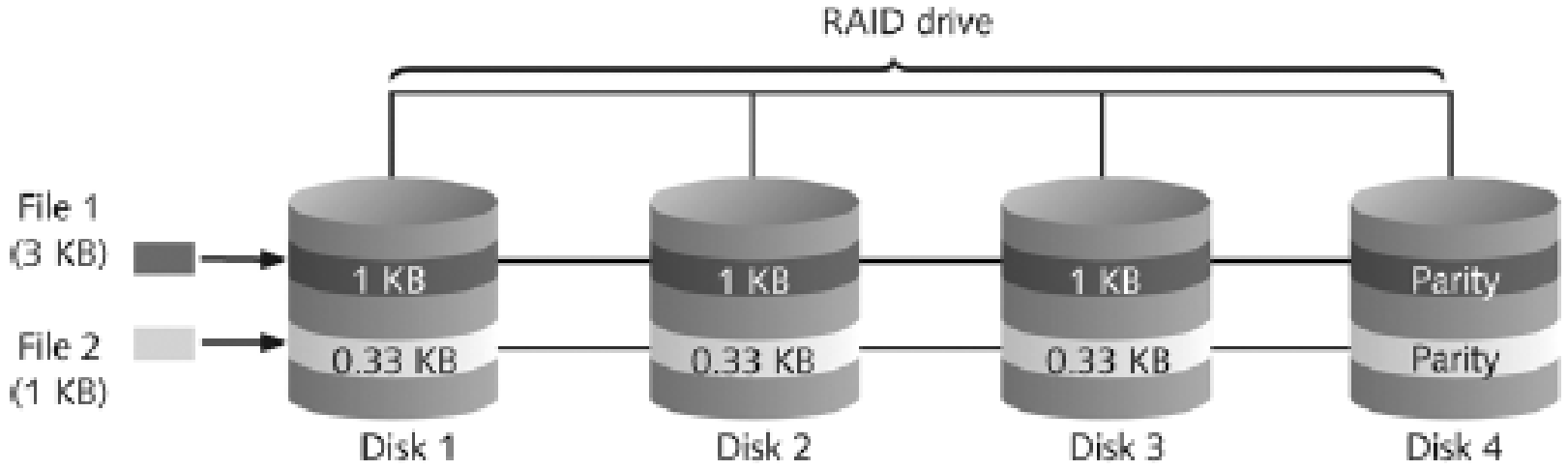

Figure 4-13 RAID 2: Striping (bit level)

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)

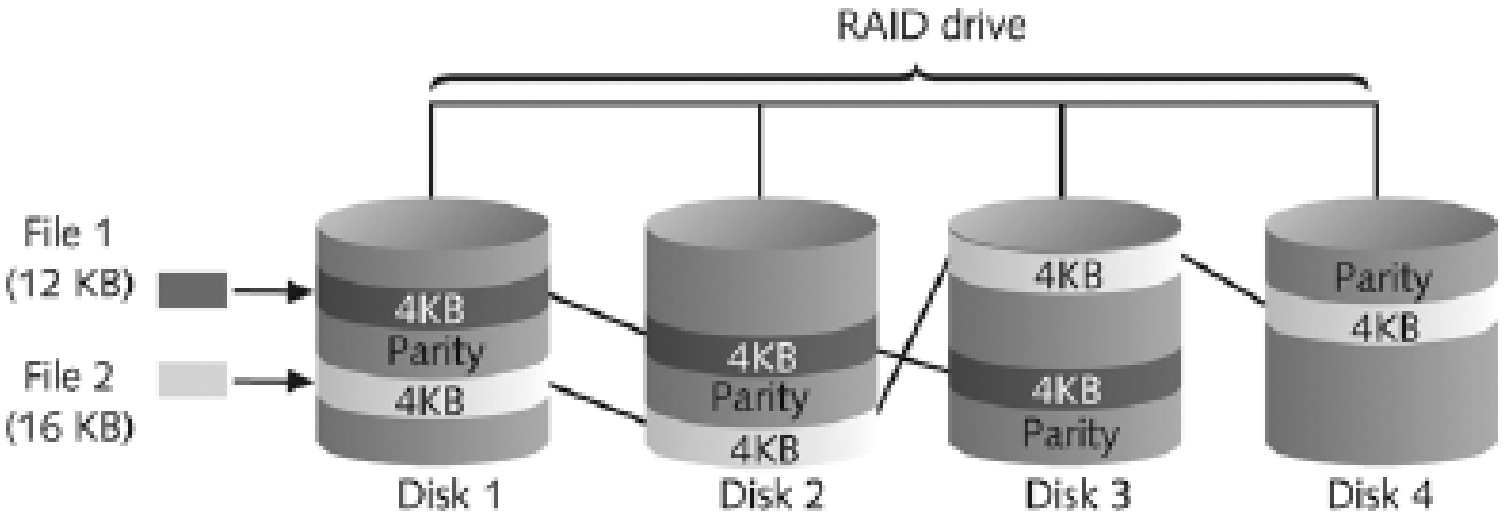

Figure 4-14 RAID 5: Block-level striping with distributed parity

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

- 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 Acquisition with ProDiscover

- With ProDiscover Investigator you can:
  - Preview a suspect's drive remotely while it's in use
  - Perform a live acquisition
  - Encrypt the connection
  - Copy the suspect computer's RAM
  - Use the optional stealth mode
- ProDiscover Incident Response additional functions
  - Capture volatile system state information
  - Analyze current running processes

Remote Acquisition with ProDiscover (continued)

- ProDiscover Incident Response additional functions (continued)
  - Locate unseen files and processes
  - Remotely view and listen to IP ports
  - Run hash comparisons
  - Create a hash inventory of all files remotely
- PDServer remote agent
  - ProDiscover utility for remote access
  - Needs to be loaded on the suspect

Remote Acquisition with ProDiscover (continued)

- 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 Acquisition with ProDiscover (continued)

- Remote connection security features
  - Password Protection
  - Encryption
  - Secure Communication Protocol
  - Write Protected Trusted Binaries
  - Digital Signatures

Remote Acquisition with EnCase Enterprise

- Remote acquisition features
  - Remote data acquisition of a computer's 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

Remote Acquisition with R-Tools R-Studio

- R-Tools suite of software is designed for data recovery
- Remote connection uses Triple Data Encryption Standard (3DES) encryption
- Creates raw format acquisitions
- Supports various file systems

Remote Acquisition with Runtime Software

- Utilities
  - DiskExplorer for FAT
  - DiskExplorer for NTFS
  - HDHOST
- 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

- 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

Vogon International SDi32

- Creates a raw format image of a drive
- Write-blocker is needed when using this tool
- Password Cracker POD
  - Device that removes the password on a drive's firmware card

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

Summary

- 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

Summary (continued)

- 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