Guide to Computer Forensics and Investigations
Sixth Edition

Chapter 3

Data Acquisition

Objectives (1 of 2)

- 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

CENGAGE

Objectives (2 of 2)

- 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

- Data in a forensics acquisition tool is stored as an image file

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

CENGAGE

Raw Format

- Makes it possible to write bit-stream data to files

- Advantages
  - Fast data transfers
  - Ignores 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

CENGAGE

Proprietary Formats

- Most forensics tools have their own 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

- The Expert Witness Compression format is unofficial standard

CENGAGE

Advanced Forensics Format

- Developed by Dr. Simson L. Garfinkel as an open-source acquisition format

- 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
  - Internal consistency checks for self-authentication

- File extensions include .afd for segmented image files and .afm for AFF metadata

- AFF is open source

CENGAGE

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

- Four methods of data collection
  - Creating a disk-to-image file
  - Creating a disk-to-disk
  - Creating a logical disk-to-disk or disk-to-data file
  - Creating a sparse data copy of a file or folder

- Determining the best method depends on the circumstances of the investigation

- Creating a disk-to-image file
  - Most common method and offers most flexibility
  - Can make more than one copy
  - Copies are bit-for-bit replications of the original drive
  - Compatible with many commercial forensics tools

- Creating a disk-to-disk
  - When disk-to-image copy is not possible
  - Tools can adjust disk's geometry configuration
  - Tools: EnCase and X-Ways

- **Logical acquisition** or **sparse acquisition**
  - Can take several hours; use when your time is limited
  - Logical acquisition captures only specific files of interest to the case
  - Sparse acquisition collects fragments of unallocated (deleted) data
  - For large disks
  - PST or OST mail files, RAID servers

CENGAGE

Determining the Best Acquisition Method (4 of 4)

- 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 lossless compression
  - Whether you can retain the disk
  - Time to perform the acquisition
  - Where the evidence is located

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 called BitLocker makes static acquisitions more difficult
  - May require user to provide decryption key

CENGAGE

Using Acquisition Tools

- Acquisition tools for Windows
    - Advantages
        - Make acquiring evidence from a suspect drive more convenient
    - 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
        - Some countries haven't accepted the use of write-blocking devices for data acquisitions

CENGAGE

Mini-WinFE Boot CDs and USB Drives

- Mini-WinFE
  - Enables you to build a Windows forensic boot CD/DVD or USB drive so that connected drives are mounted as read-only

- Before booting a suspect's computer:
  - Connect your target drive, such as a USB drive

- After Mini-WinFE is booted:
  - You can list all connected drives and alter your target USB drive to read-write mode so you can run an acquisition program

CENGAGE

- 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

CENGAGE

- Using Linux Live CD Distributions (cont'd)
  - Forensic Linux Live CDs (cont'd)
    - Configured not to mount, or to mount as read-only, any connected storage media
    - Well-designed Linux Live CDs for computer forensics
      - Penguin Sleuth Kit
      - CAINE
      - Deft
      - Kali Linux
      - Knoppix
      - SANS Investigative Forensic Toolkit (SIFT)

- Preparing a target drive for acquisition in Linux
  - Current Linux distributions can create Microsoft FAT and NTFS partition tables
  - **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
  - 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 `dd` in Linux (cont'd)

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

- Acquiring data with `dcfldd` in Linux (cont'd)
  - `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 AccessData FTK Imager Lite (1 of 8)

- Included with AccessData Forensic Toolkit

- Designed for viewing 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 run from a Live CD, such as Mini-WinFE

CENGAGE
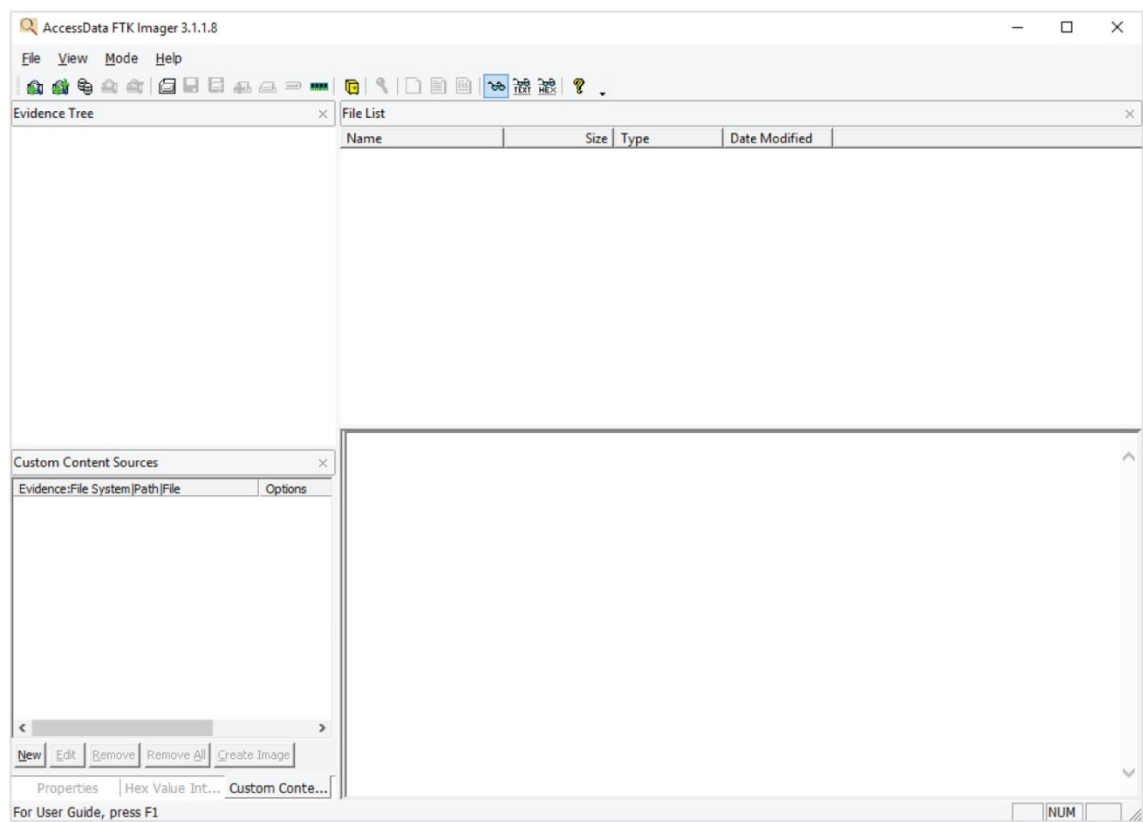
Figure 3-2 The FTK Imager main window

Source: AccessData Group, Inc.

Capturing an Image with AccessData FTK Imager Lite (3 of 8)

- FTK Imager can't acquire a drive's host protected area

- Use a write-blocking device and follow these steps
  - Boot to Windows
  - Connect evidence disk to a write-blocker
  - Connect target disk to write-blocker
  - Start FTK Imager Lite
  - Create Disk Image - use Physical Drive option
  - See Figures on the following slides for more steps

CENGAGE
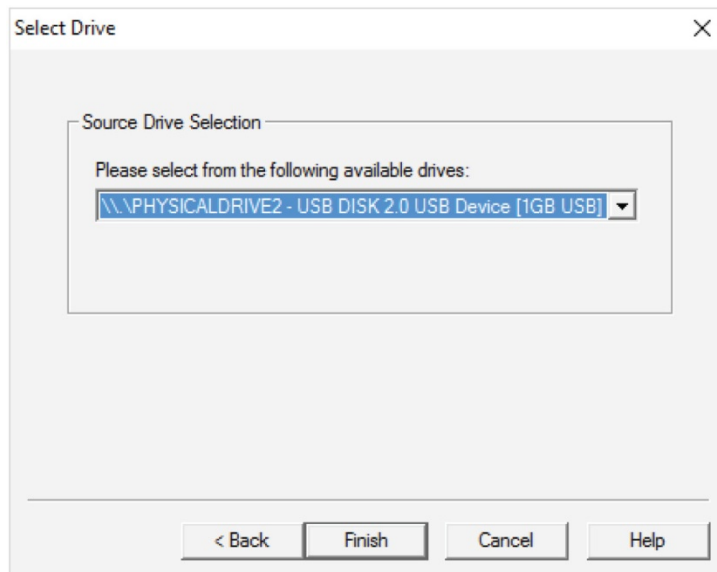
Figure 3-3 The Select Drive dialog box

Source: AccessData Group, Inc.

CENGAGE
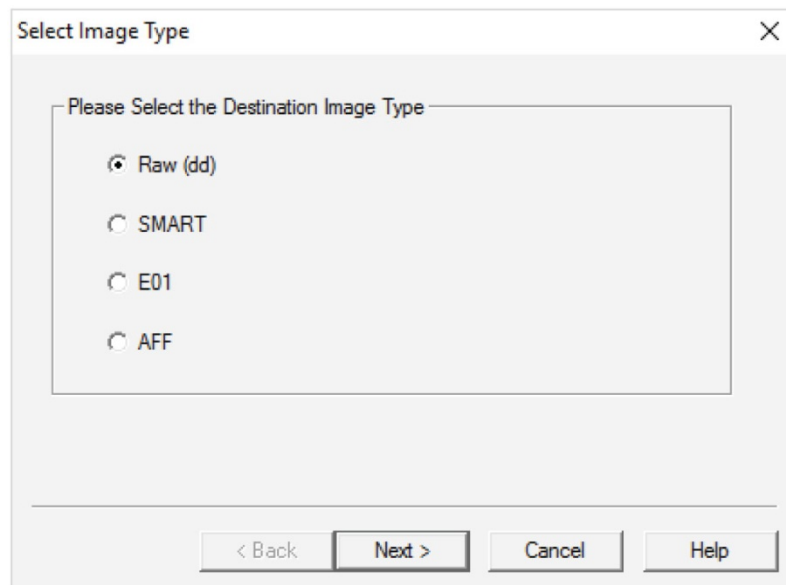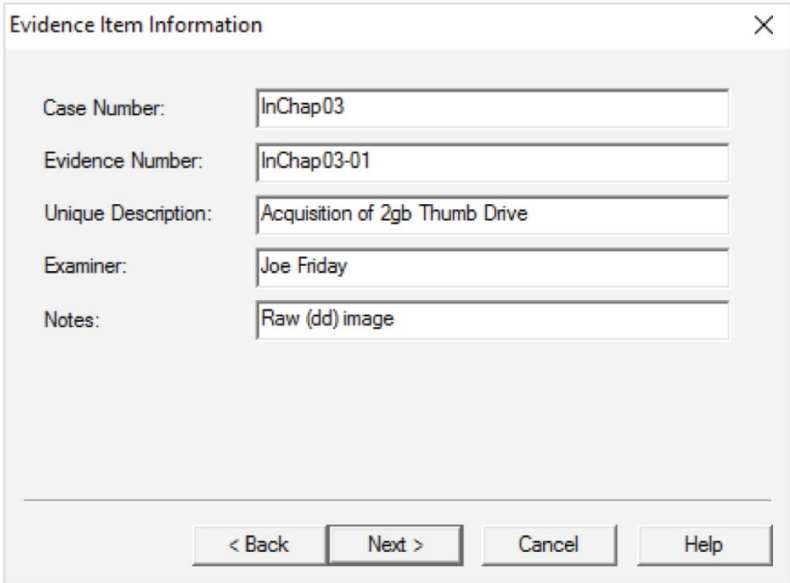
Figure 3-4 The Select Image Type dialog box

Source: AccessData Group, Inc.

Figure 3-5 The Evidence Item Information dialog box

Source: AccessData Group, Inc.

Figure 3-6 Selecting where to save the image file

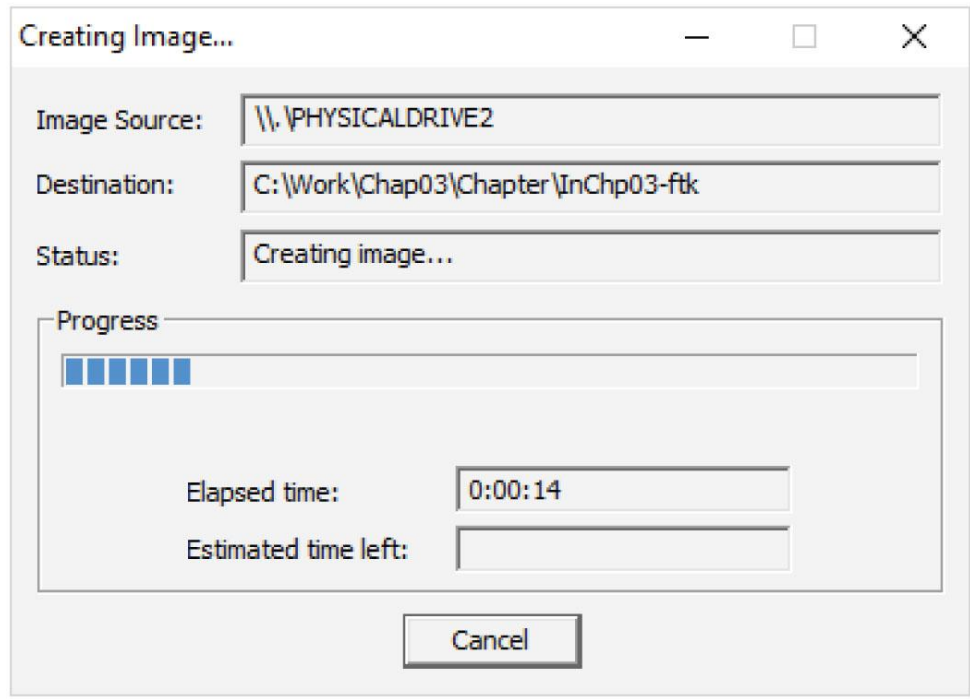Source: AccessData Group, Inc.

Figure 3-7   An image save in progress

Source: AccessData Group, Inc.

Validating Data Acquisitions

- Validating evidence may be the most critical aspect of computer forensics

- Requires using a hashing algorithm utility

- Validation techniques
  - CRC-32, MD5, and SHA-1 to SHA-512

CENGAGE

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

CENGAGE

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

CENGAGE

Performing RAID Data Acquisitions

- Acquisition of RAID drives can be challenging and frustrating because of how RAID systems are
  - Designed
  - Configured
  - Sized

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

CENGAGE

- **Redundant array of independent disks (RAID)**
  - Computer configuration involving two or more disks
  - Originally developed as a data-redundancy measure

- RAID 0
  - Provides rapid access and increased storage
  - Biggest disadvantage is lack of redundancy

- RAID 1
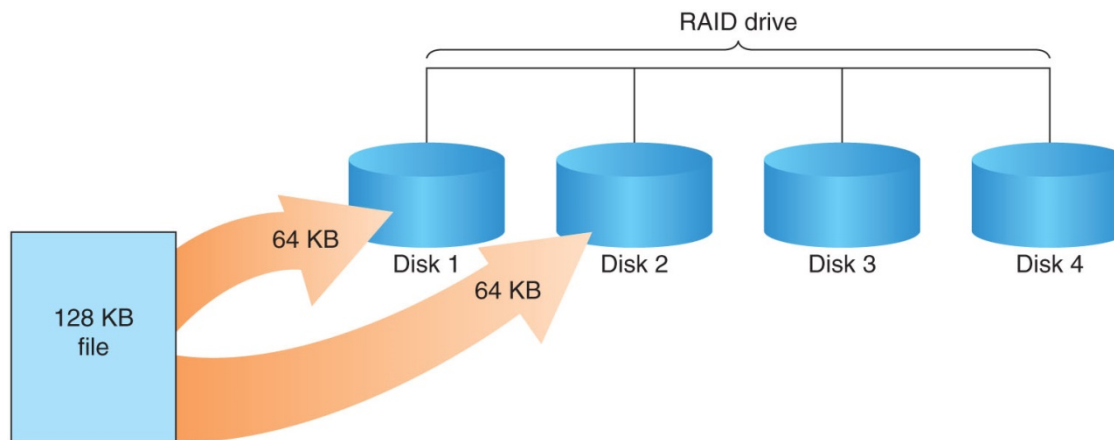 - Designed for data recovery
  - More expensive than RAID 0

CENGAGE

Figure 3-8 RAID 0: Striping

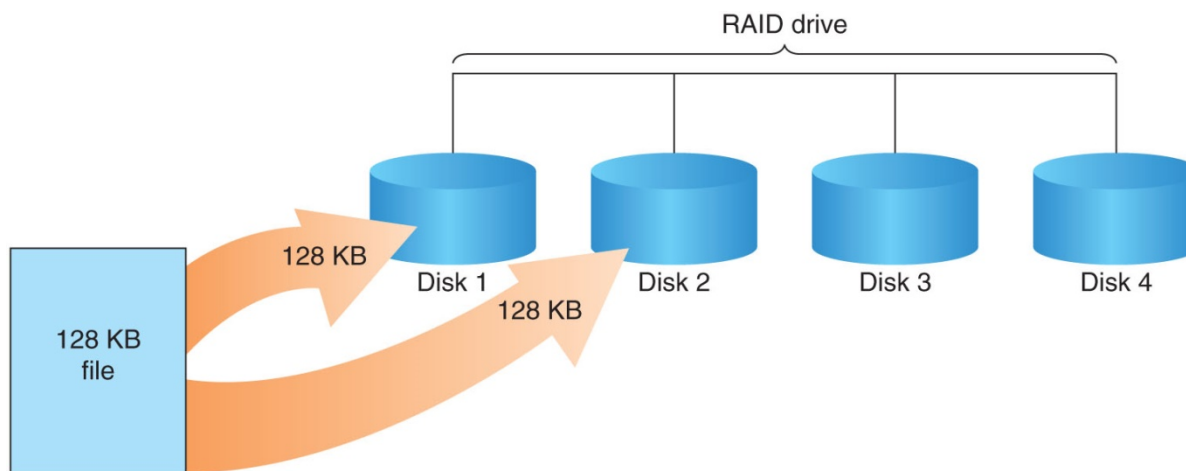**Figure 3-9**   RAID 1: Mirroring

- 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
  - Requires at least three disks

- RAID 4
  - Similar to RAID 3
  - Data is written in blocks
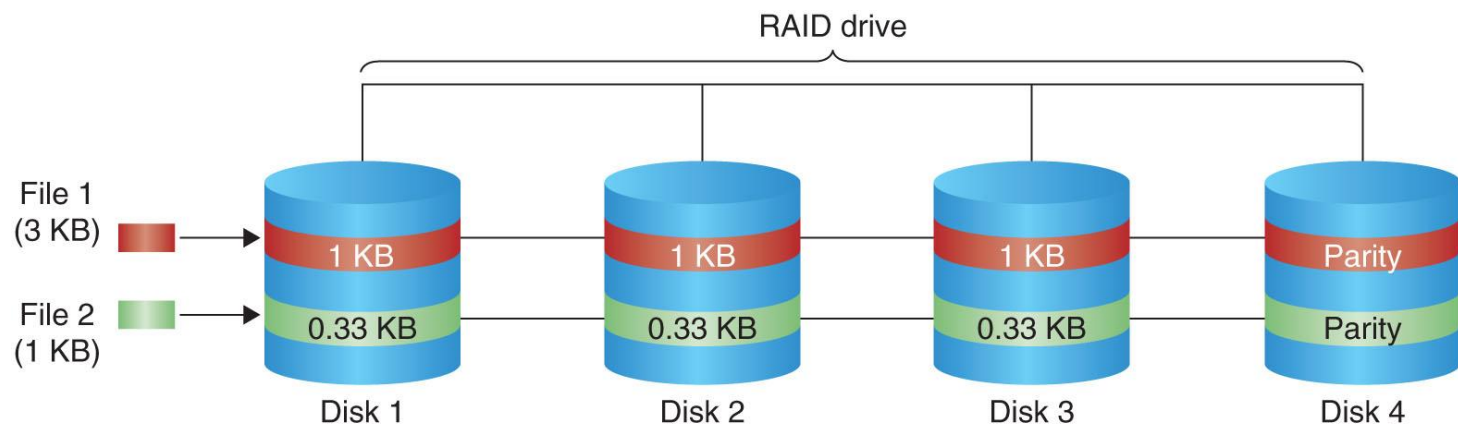
Figure 3-10   RAID 2: Striping (bit level)

- RAID 5
  - Similar to RAIDs 0 and 3
  - Places parity recovery data on each disk

- RAID 6
  - Redundant parity on each disk

- RAID 10 (1+0), or mirrored striping
  - Combination of RAID 1 and RAID 0
  - Provides fast access and redundancy

- RAID 15 (1+5)
  - Combination of RAID 1 and RAID 5
  - More costly option

CENGAGE
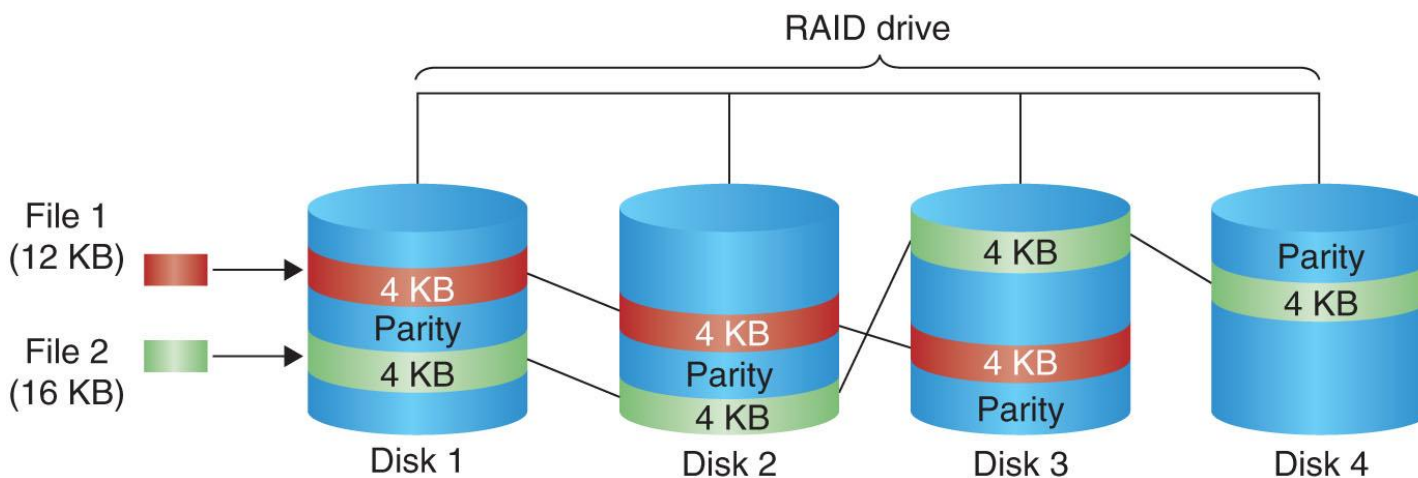
Figure 3-11 RAID 5: Block-level striping with distributed parity

Acquiring RAID Disks (1 of 2)

- Address the following concerns:
  - How much data storage is needed?
  - What type of RAID is used?
  - Do you need to have all drives connected?
  - 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?

- Copying small RAID systems to one large disk is possible

CENGAGE

Acquiring RAID Disks (2 of 2)

- Vendors offering RAID acquisition functions
  - Guidance Software EnCase
  - X-Ways Forensics
  - AccessData FTK
  - 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

CENGAGE

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
  - Antivirus, antispyware, and firewall tools can be configured to ignore remote access programs
  - Suspects could easily install their own security tools that trigger an alarm to notify them of remote access intrusions

CENGAGE

- ProDiscover Incident Response functions:
    - Capture volatile system state information
    - Analyze current running processes
    - 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

- 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
  - Encryption
  - Secure communication protocol
  - Write-protected trusted binaries
  - Digital signatures

CENGAGE

Remote Acquisition with EnCase Enterprise

- Remote acquisition features
  - Search and collect internal and external network systems over a wide geographical area
  - Support multiple Oss and file systems
  - Triage to help determine system's relevance to an investigation
  - Perform simultaneous searches of up to five systems at a time

CENGAGE

Remote Acquisition with R-Tools R-Studio

- R-Tools suite of software is designed for data recovery

- Can remotely access networked computer systems

- Creates raw format acquisitions

- Supports various file systems

CENGAGE

Remote Acquisition with WetStone US-LATT PRO

- US-LATT PRO
  - Part of a suite of tools developed by WetStone
  - Can connect to a networked computer remotely and perform a live acquisition of all drives connected to it

CENGAGE

Remote Acquisition with F-Response

- F-Response
  - A vendor-neutral remote access utility
  - Designed to work with any digital forensics program
  - Sets up a security read-only connection
    - Allows forensics examiners to access it

- Four different version of F-Response
  - Enterprise Edition, Consultant + Convert Edition, Consultant Edition, and TACTICAL Edition

CENGAGE

Using Other Forensics-Acquisition Tools

- Other commercial acquisition tools
  - PassMark Software ImageUSB
  - ASRData SMART
  - Runtime Software
  - ILookIX Investigator IXimager
  - SourceForge

CENGAGE

PassMark Software ImageUSB

- PassMark Software has an acquisition tool called ImageUSB for its OSForensics analysis product

- To create a bootable flash drive, you need:
  - Windows XP or later
  - ImageUSB downloaded from the OSForensics Web site

ASR Data SMART

- ASR Data SMART
  - A Linux forensics analysis tool that can make image files of a suspect drive
  - Can produce proprietary or raw format images

- Capabilities:
  - Data reading of bad sectors
  - Can mount drives in write-protected mode
  - Can mount target drives in read/write mode
  - Compression schemes to speed up acquisition or reduce amount of storage needed

Runtime Software

- Runtime Software offers shareware programs for data acquisition and recovery:
  - DiskExplorer for FAT and NTFS

- Features:
  - Create a raw format image file
  - Segment the raw format or compressed image for archiving purposes
  - Access network computers' drives

CENGAGE

ILook Investigator IXimager

- IXimager
  - Runs from a bootable floppy or CD
  - Designed to work only with ILookIX
  - Can acquire single drives and RAID drives
  - Supports:
    -IDE (PATA)
    -SCSI
    -USB
    -FireWire

SourceForge

- SourceForge provides several applications for security, analysis, and investigations

- For a list of current tools, see:
  - SourceForge-Tools

- Windows version of `dcfldd`
  - SourceForge-dcfldd

- Forensics data acquisitions are stored in three different formats:
  - Raw, proprietary, and AFF

- Data acquisition methods
  - Disk-to-image file
  - Disk-to-disk copy
  - Logical disk-to-disk or disk-to-data file
  - Sparse data copy

Summary (2 of 3)

- Several tools available
  - Lossless compression is acceptable
- Plan your digital evidence contingencies
  - Make a copy of each acquisition
- Write-blocking devices or utilities must be used with GUI acquisition tools
- Always validate acquisition
- A Linux Live CD, such as SIFT, Kali Linux, or Deft, provides many useful tools for digital forensics acquisitions

CENGAGE

- 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

- Remote network acquisition tools require installing a remote agent on the suspect computer