

The background is a solid blue gradient. At the top, there are several wavy, horizontal lines in shades of light blue and cyan, creating a sense of movement or data flow.

# *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
- 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

# Data acquisition

- Data acquisition is the process of copying data
- it's the task of collecting digital evidence from electronic media

The background of the slide is a solid blue color. At the top, there are several wavy, horizontal lines in shades of blue and teal, creating a layered, wave-like effect.

# 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
- Three formats
  1. Raw format
  2. Proprietary formats
  3. Advanced Forensics Format (AFF)

# 1. Raw Format

- This is what the Linux dd command (**data duplicator**) 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

# 1. 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)



## 2. 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.

## 2. Proprietary Formats

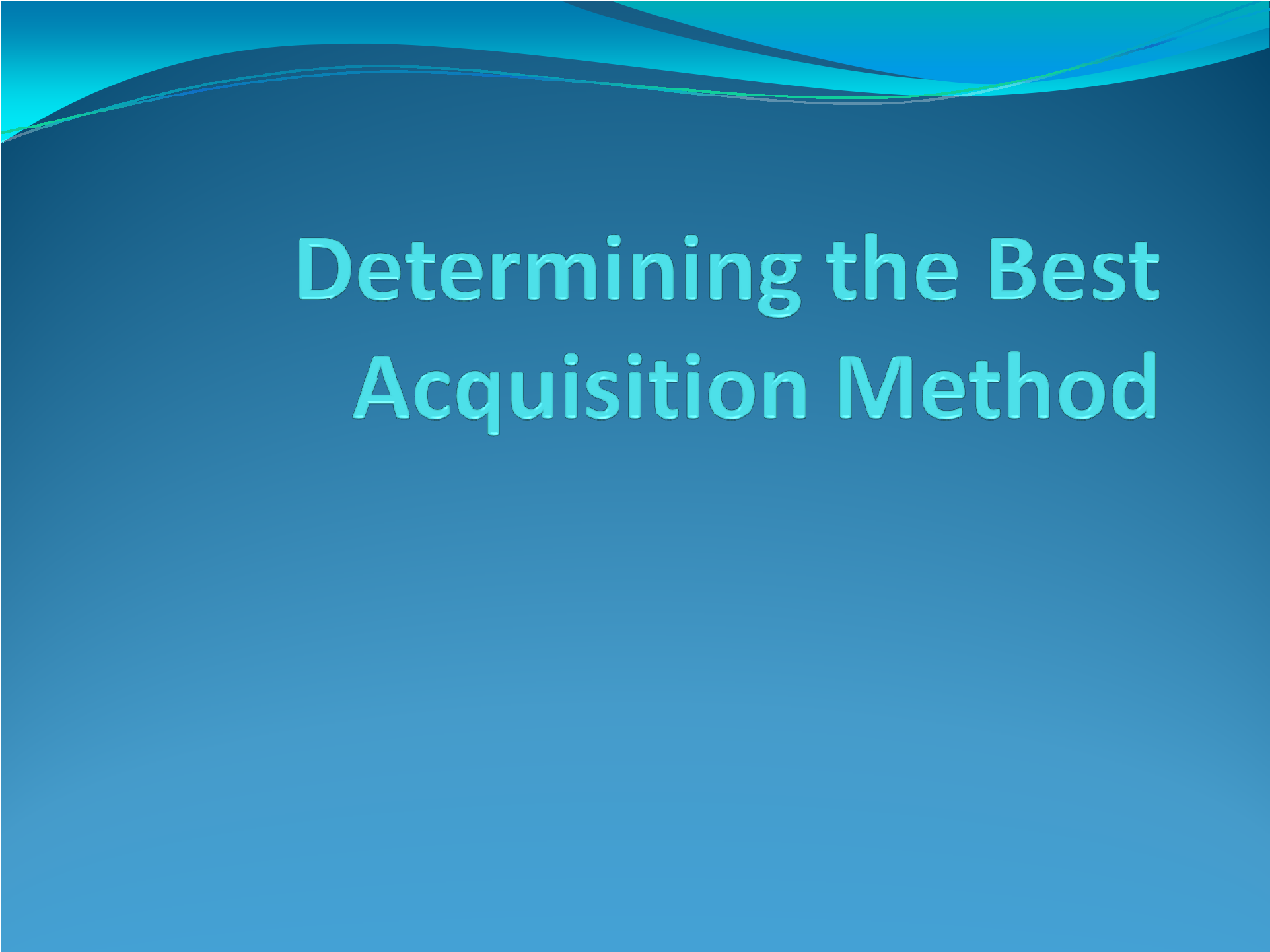
- Disadvantages
  - Inability to share an image between different tools
  - File size limitation for each segmented volume
    - Typical segmented file size is 650 MB or 2 GB
- Expert Witness format is the unofficial standard
  - Used by EnCase, FTK, X-Ways Forensics, and SMART
  - Can produce compressed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

### 3. Advanced Forensics Format

- Developed by Dr. Simson L. Garfinkel of Basis Technology Corporation
- File extensions include **.afd** for segmented image files and **.afm** for AFF metadata
- AFF is open source

# 3. Advanced Forensics 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



# Determining the Best Acquisition Method

# Determining the Best Acquisition Method

- Types of acquisitions
  - **Static acquisitions** and **live acquisitions**
- Four methods
  1. Bit-stream disk-to-image file
  2. Bit-stream disk-to-disk
  3. Logical
  4. Sparse
- Best acquisition method depends on the circumstances of the investigation

# 1. Bit-stream disk-to-image file

- Most common method
- offers the most flexibility
- Can make more than one copy
- Copies are bit-for-bit replications of the original drive
- Tools to read disk to image file created are:  
ProDiscover, EnCase, FTK, SMART,  
Sleuth Kit, X-W.ays, iLook

## 2. 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



### 3. Logical 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

### 4. Sparse Acquisition

- Sparse acquisition collects only some of the data
  - also collects fragments of unallocated (deleted) data

# Determining the Best Acquisition Method

- To determine which acquisition method to use for an investigation, consider
  - The size of the source (suspect) disk
  - Whether it is possible to retain the source disk as evidence or must return it to the owner
  - How much time you have to perform the acquisition
  - Where the evidence is located

# Compressing Disk Images

- If the source disk is very large, and there is no target disk of comparable size then reduce the size of data by compression
- Older Microsoft disk compression tools, such as DoubleSpace or DriveSpace, eliminate only slack disk space between files
- Other compression methods use an algorithm to reduce file size
  - Popular archiving tools, PKZip, WinZip, and WinRAR, use lossless compression

# Compressing Disk Images

- Lossless compression might compress a disk image by 50% or more
- Files that are already compressed, like ZIP files, won't compress much more
- Use MD5 or SHA-1 hash to verify the lossless compressed data
- Compression algorithms for graphics files use lossy compression, which can change data

# Tape Backup

- When working with large drives, an alternative is using tape backup systems
  - Super Digital Linear Tape (SDLT) or
  - Digital Audio Tape/Digital Data Storage (DAT/DDS)
  - Snap- Back and SafeBack
- No limit to size of data acquisition
  - Just use many tapes
- But it's slow and time consuming

# 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)
- Make sure you have a reliable forensics tool

The background of the slide is a solid blue color. At the top, there are several wavy, horizontal lines in shades of blue and cyan, creating a layered, wave-like effect.

# Contingency Planning for Image Acquisitions

# Contingency Planning for Image Acquisitions

- Take precautions to protect your digital evidence
- Create a duplicate copy of your evidence image file
- Make **at least two images of digital evidence**
  - Use different tools or techniques
  - imaging tool, such as ProDiscover, FTK, and X-Ways Forensics
  - If you have only one tool, make one copy with no compression and compress the other copy



# Contingency Planning for Image Acquisitions

- Copy host protected area (hidden) 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 – getting key is difficult
  - Making static acquisition is also difficult
  - Possible to recover passwords and passphrases from RAM

The background of the slide is a solid blue color. At the top, there are several wavy, horizontal lines in shades of blue and teal, creating a layered, wave-like effect. The text "Using Acquisition Tools" is centered in the middle of the slide in a light blue, sans-serif font.

# Using Acquisition Tools

# Using Acquisition Tools

- Acquisition tools for Windows
  - Advantages
    - Make acquiring evidence from a suspect drive more convenient
      - Especially when used with hot-swappable devices (USB, SATA, Fire wire)
  - Disadvantages
    - Windows can easily contaminate evidence drive
    - 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
- Modified the Windows Registry to enable write-protection
- Target drive needs to be connected to an internal PATA (IDE), SATA, or SCSI controller
- Works in Windows XP SP2, Vista
- To update the Registry - perform three tasks
  - First, back up the Registry in case something fails while you're modifying it
  - Second, modify the Registry with the write protection feature
  - Third, create two desktop icons to automate switching between enabling and disabling writes to the USB device

# Acquiring Data with a Linux Boot CD

- Linux can read hard drives that isn't mounted or mounted as read-only
- Windows OSs and newer Linux **automatically mount and access a drive**
  - Windows – access and alter the Recycle Bin
  - Linux – alter metadata to the drive, such as mount point configurations
- All these changes **corrupt the integrity** of evidence

# Acquiring Data with a Linux Boot CD

- While acquiring data
  - **Windows – use write blocking device**
  - **Linux –Forensic Live CD**
    - mount all drives read-only
    - Linux Live CD are generally for recovery
    - Few are specially designed for forensics

# Forensic Linux Live CDs

- Forensic Linux Live CDs
  - Configured not to mount or
  - To mount as read-only
    - Protects integrity
- Well-designed Linux Live CDs for computer forensics
  - Helix
  - Penguin Sleuth
  - FCCU
- These ISO images can be downloaded and a bootable CD can be created. It is then tested by booting a computer using the just burned Live CD

# Preparing a target drive for acquisition in Linux

- Use FAT and NTFS partitions
- **fdisk** command lists, creates, deletes, and verifies partitions in Linux
- **mkfs.msdos** command formats a FAT file system from Linux



# Acquiring Data with a Linux Boot CD

- To perform a data acquisition on a suspect computer, we need
  - A forensic Linux Live CD
  - A USB, FireWire, or SATA external drive with cables
  - Knowledge of how to alter the suspect computer's BIOS to boot from the Linux Live CD
  - Knowledge of which shell commands to use for the data acquisition

# Acquiring Data with a Linux Boot CD

- Writing the Data to an Image: Destination location
  1. Data can saved directly to a disk or to a file.
  2. To disc:
    - The destination disc must be wiped with zeros before the acquisition starts.
  3. To file (e.g. image.dd):
    - The file can be saved on a hard disc or other storage media.
    - Fragmentable in many smaller pieces to fit onto storage media.

# Acquiring Data with a Linux Boot CD

- 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

- Imported flags:
- Default block size: 512 bytes
- Source (file or drive) flag: 'if='
- Destination (file or drive) flag : 'of='
- Block size flag: 'bs='
- Conversion flag: 'conv='
- noerror: Do not stop when facing input / output errors
- sync: Pad input blocks with NULL (this keeps the offset within the image in presence of errors)
- notrunc: Do not truncate the output file
- e.g.: # dd if=file1.dat of=file1.dd bs=512 conv=noerror

# Acquiring data with dd in Linux

- Shortcomings of dd command
  - Requires more advanced skills than average user
  - Does not compress data
  - target drive needs to be equal to or larger than the suspect drive
- dd command + 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

- Developed by Nicholas Harbour of the Defense Computer Forensics Laboratory (DCFL)
- Tool that can be added to most UNIX/Linux OSs
- dcfldd command,
- Works similarly to the dd command but has many features designed for computer 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
  - 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



# Capturing an Image with ProDiscover Basic (continued)


- 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)
- 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

- 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)

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



# Validating Data Acquisitions

# Validating Data Acquisitions

- Most critical aspect of computer forensics
- Essential to check the integrity of evidence
- Requires hashing algorithm – digital fingerprint
- 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

# Linux Validation Methods

- Two linux commands dd and dcfldd combined with other commands validate the data
- two hashing algorithm utilities:
  - md5sum and sha1-sum
- compute hashes of a
  - single file
  - multiple files
  - individual or multiple disk partitions
  - an entire disk drive

# 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
- calculate the hash value
  - `md5sum/dev/sdb > md5_sdb.txt`
- To compute the MD5 hash value for the segmented volumes and append the output to the md5\_sdb.txt file,
  - `cat image_sdb. | md5sum >> md5_sdb.txt` and

# Linux Validation Methods

- 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
  - To create an MD5 hash output file
    - `dcfldd if=/dev/sda split=2M of=usbimg hash=md5 hashlog=usbhash.log`
  - vf (verify file) option compares the image file to the original medium
    - `dcfldd if=/dev/sda vf=sda_hash.img`



# 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
  - For example,
    - ProDiscover's .eve files contain metadata in the acquisition file including the hash value for the suspect drive or partition. Image data loaded into Pro-Discover is hashed and then compared to the hash value in the stored metadata. If the hashes don't match, ProDiscover notifies you that the acquisition is corrupt and can't be considered reliable evidence. This function is called **Auto Verify Image Checksum**.

# Windows Validation Methods

- 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

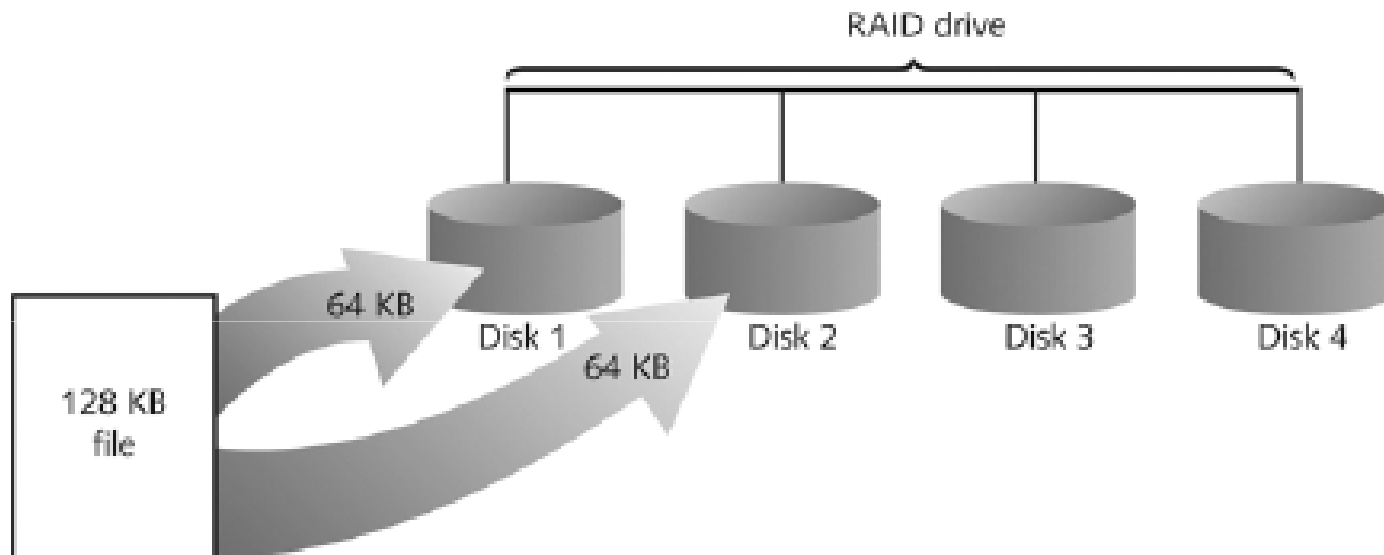
# Understanding RAID

- **Redundant array of independent** (formerly “inexpensive”) **disks (RAID)**
  - Is a Computer configuration involving two or more disks
  - Originally developed as a data-redundancy measure
  - to minimize data loss caused by a disk failure
  - technology - increased storage capabilities

# Understanding RAID

- RAID 0 (Striped)
  - Provides rapid access and increased storage
  - Two or more disk drives become one large volume
  - tracks of data on this mode of storage cross over to each disk
  - Advantage : increased speed and data storage capability
  - Disadvantage is lack of redundancy; if a disk fails, data isn't continuously available

# Understanding RAID (continued)



**Figure 4-11** RAID 0: Striping

# Understanding RAID

- RAID 1 (Mirrored)
  - Designed for data recovery
  - More expensive than RAID 0

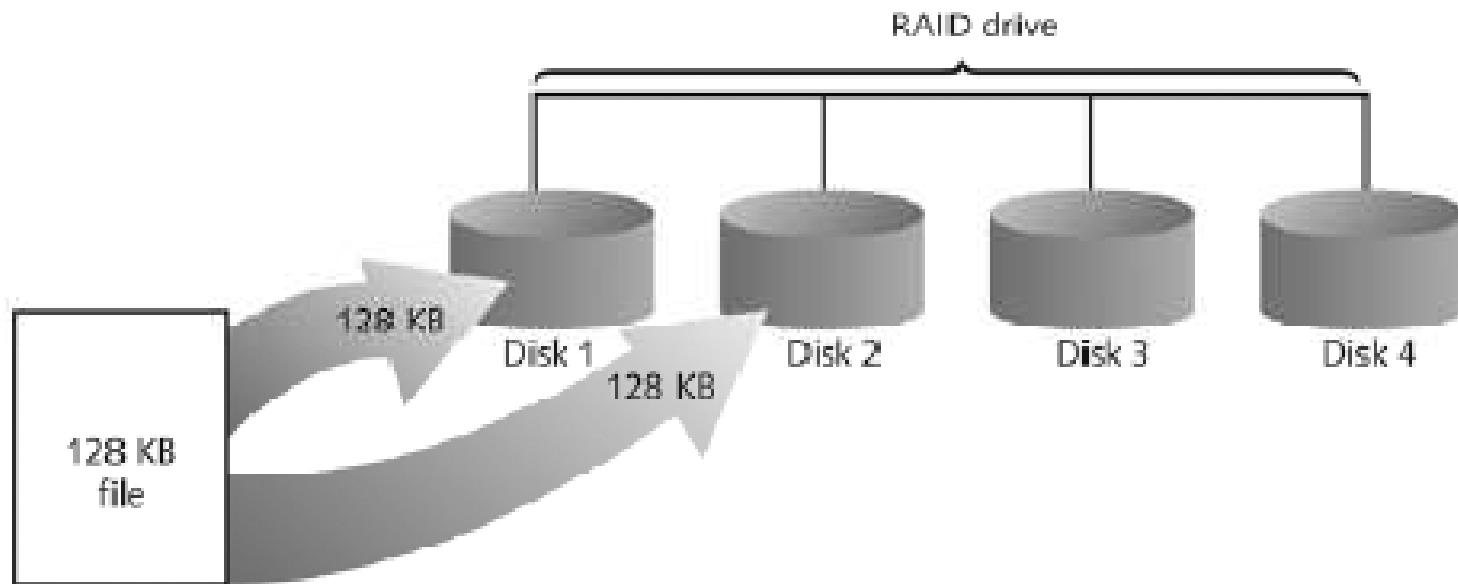


Figure 4-12 RAID 1: Mirroring



# Understanding RAID (continued)

- RAID 2
  - Similar to RAID 1
  - Uses bit level data striping
  - Has better data integrity checking than RAID 0
  - Slower than RAID 0
- RAID 3
  - Uses byte level data striping and dedicated parity
- RAID 4
  - Uses block level data striping and dedicated parity

# Understanding RAID (continued)

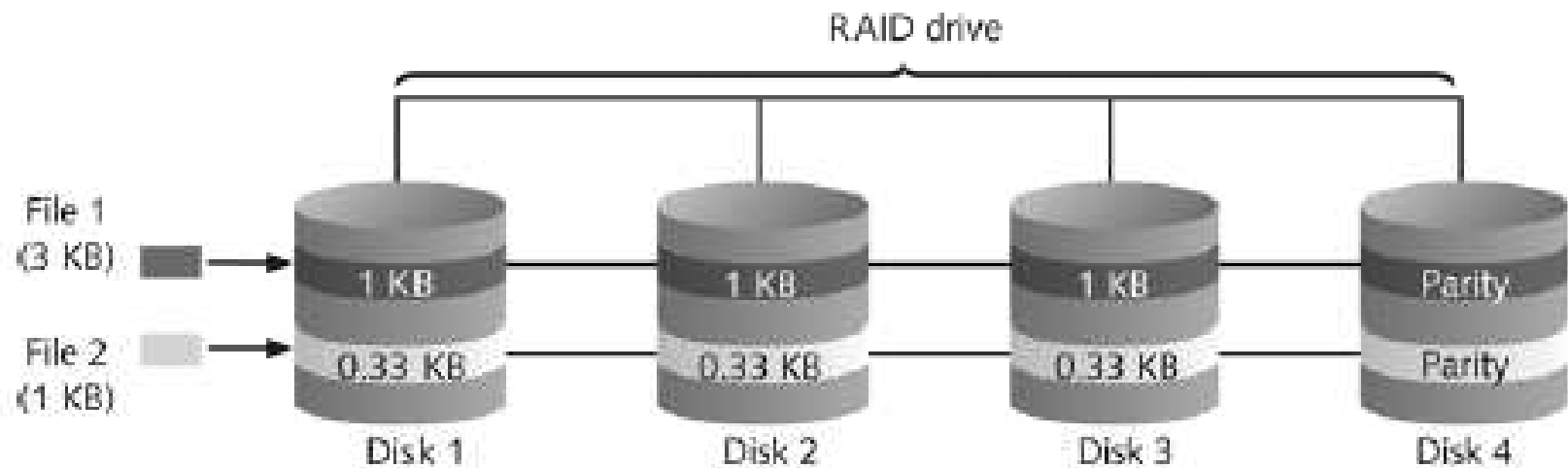


Figure 4-13 RAID 2: Striping (bit level)

# Understanding RAID (continued)

- RAID 5
  - Similar to RAID 0 and 3
  - Places parity recovery data on each disk - distributed parity
  - block-level striping
- 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)

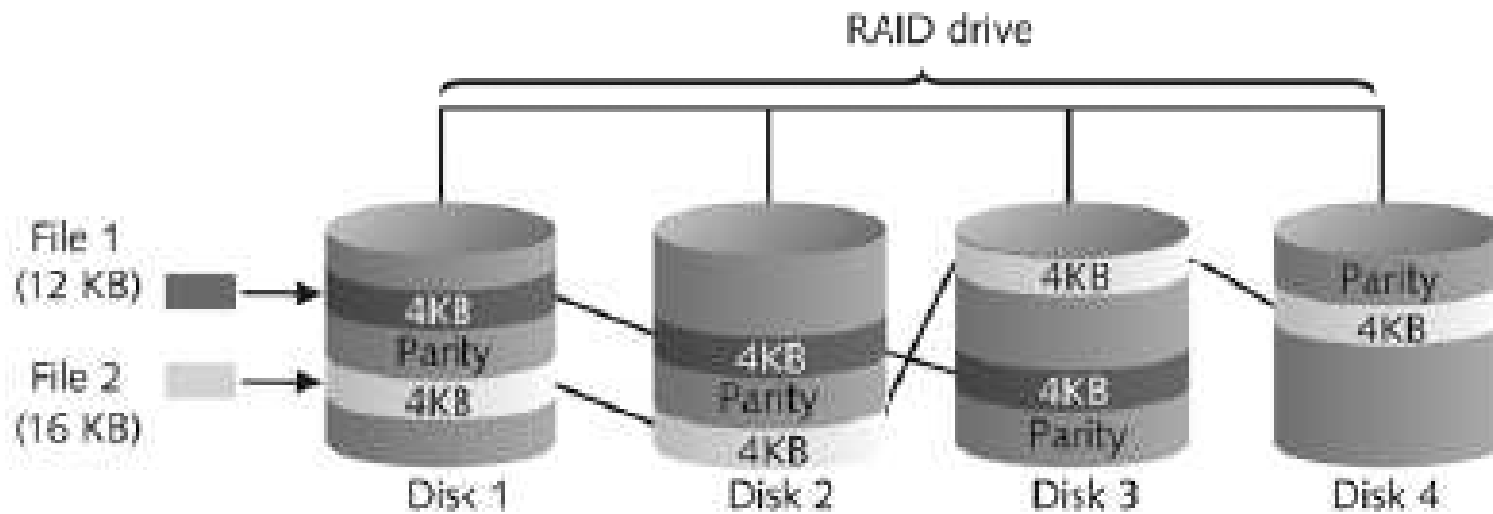
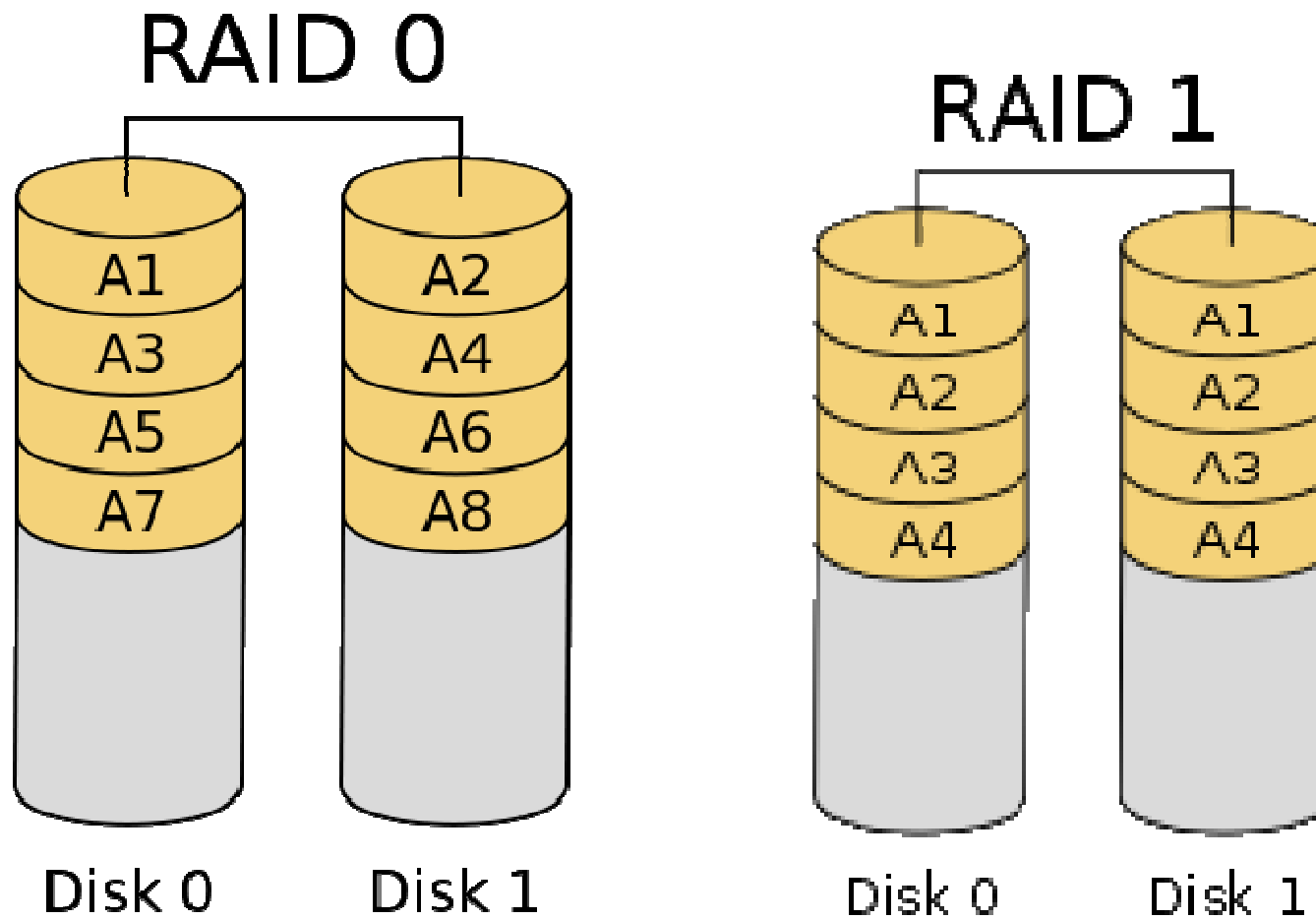
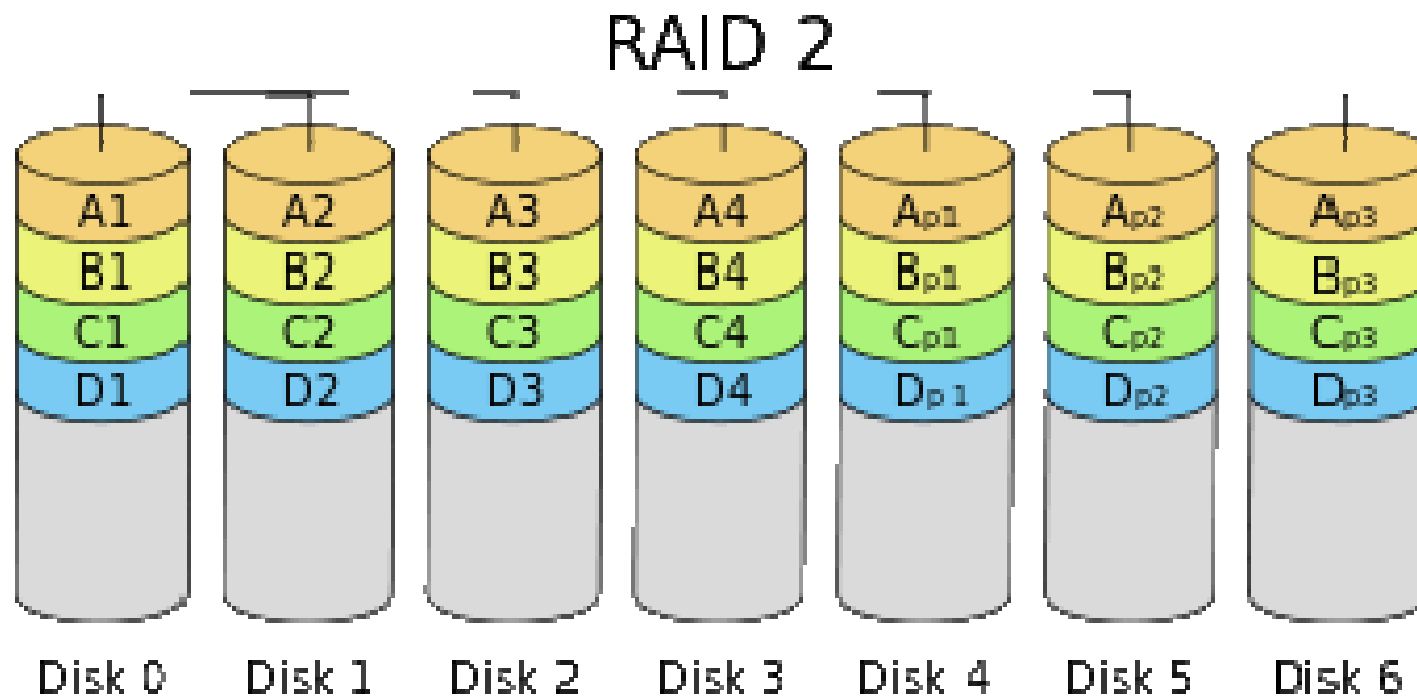


Figure 4-14 RAID 5: Block-level striping with distributed parity

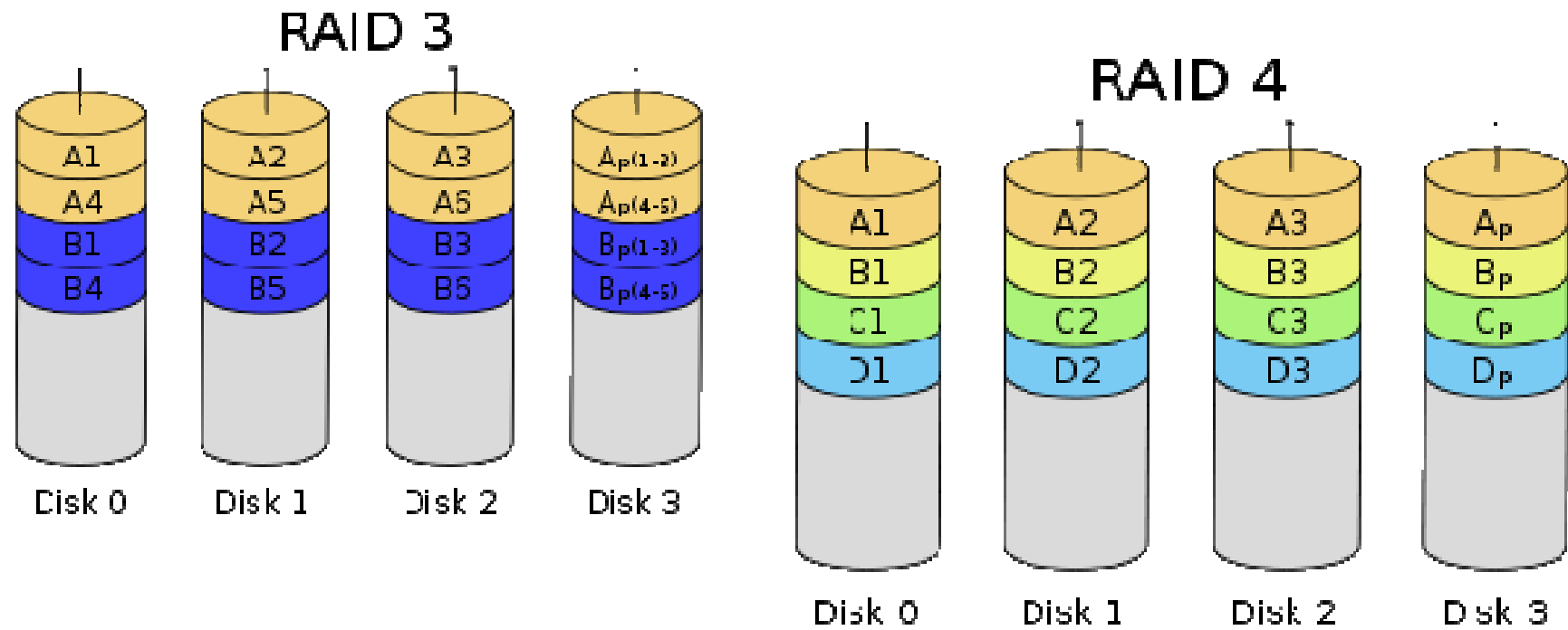
# RAID LEVEL



# RAID LEVEL

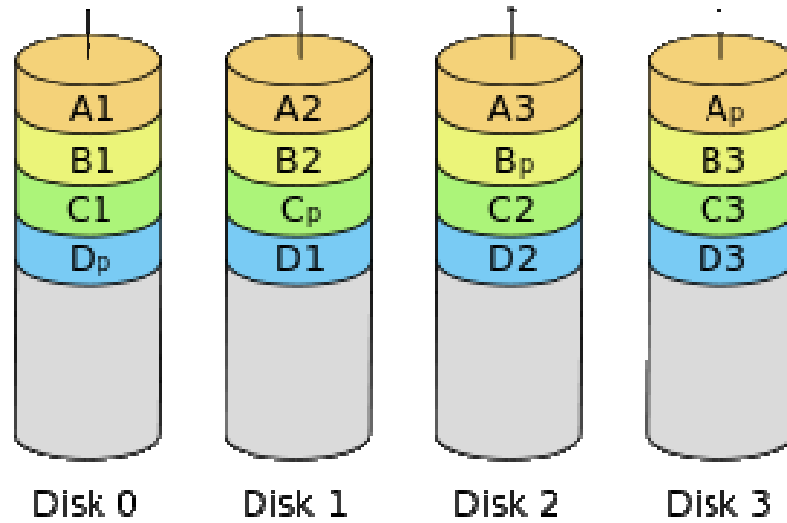


# RAID LEVEL

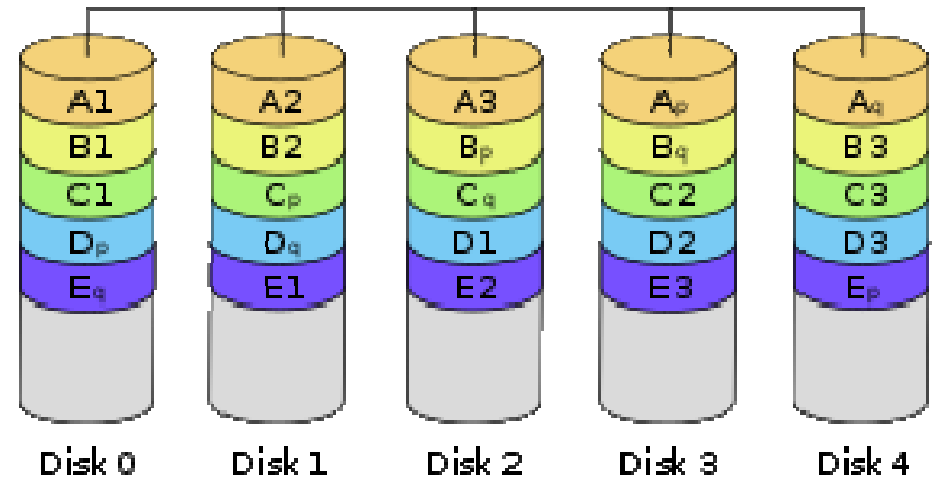


# RAID LEVEL

## RAID 5



## RAID 6






# 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

The background of the slide is a solid blue color. At the top, there are several wavy, horizontal lines in shades of blue and teal, creating a layered, wave-like effect.

# 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

- Two versions
  - ProDiscover Investigator
  - ProDiscover Incident Response
- ProDiscover Investigator
  - Preview a suspect's drive remotely
  - Perform Live acquisition
  - Encrypt the connection between the suspect's and examiner's computers
  - Copy the suspect computer's RAM
  - Use the optional stealth mode to hide the remote connection from the suspect while data is previewed or acquired

# Remote Acquisition with ProDiscover

- ProDiscover Incident Response
  - Network intrusion analysis tool
  - Perform all functions of ProDiscover Investigator
  - Additional 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 to find Trojans and rootkits
    - Create a hash inventory of all files remotely

# Remote Acquisition with ProDiscover

- 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

# PDServer Remote Agent

- 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
  - R-Tools for data recovery
  - R-Studio - network edition - can remotely access networked computer systems
- WetStone LiveWire
  - can connect to a networked computer remotely and perform a live acquisition of all drives connected to it
  - format is raw (.dd)
  - capture RAM data from remote systems
- F-Response
  - installed on a remote computer, it sets up a security read-only connection that allows the computer forensics examiner to access it

# 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

The background of the slide is a solid blue color with a gradient. At the top, there are several wavy, horizontal lines in shades of blue and cyan, creating a sense of movement or a stylized horizon. The text is centered in the upper half of the slide.

# Using Other Forensics- Acquisition Tools

# Using Other Forensics-Acquisition Tools

- Tools
  - SnapBack DatArrest
  - SafeBack
  - DIBS USA RAID
  - ILook Investigator IXimager
  - Vagon 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
- 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