Data Acquisition

Mostly Chapter 3 of Nelson

Also some of Chapter 3 of Carrier

Some More Information

Starting with class 05 next week (21 Sept) we will:

- *Start to use Carrier more and Nelson less*
- *Will discuss mass storage, then partitions and then file systems (FAT, NTFS and EXT)*

Will return to Nelson later in the course

In the past we used labs in which students were given drives and then took forensic images

- *For an online class this is not reasonable to do*
- *Would require that drives be distributed to online students*
- *Instead, I will give you forensic images where the data acquisition has already been performed*

Today's Lecture Overview

Introduction & Overview

Image Formats for Evidence

Acquisition Methods

Planning for Image Acquisitions

Acquisition Tools

Validating Data Acquisitions

RAID Acquisitions

Remote Network Acquisition Tools

Some Other Tools

Introduction & Overview

Forensic data acquisition is the process of accurately copying data from electronic storage media to preserve it for further forensic analysis

There are two types of data acquisition

- *Static acquisition*
  - The computer is off, and you take the drive out
- *Live acquisition*
  - The computer is running

Introduction & Overview

Live acquisition has become important because

- *Whole disk encryption is making it harder to extract and understand the contents of the disk*
- *The contents of RAM memory has become more important to digital investigations*
  - Tells if virtual machine(s) are running and being used
  - Can inform as to how networks were being used
  - Can find instantiated software that only exists in RAM

So today we need both

Introduction & Overview

Problems with live acquisition: What are they?

- *Can't perform repeatable acquisitions as is possible with static acquisition*
- *Each live acquisition is unique*
  - Acquire the contents of RAM
  - Acquire the contents of RAM again
  - The two acquisitions are likely to be different

Important forensic implication

- *Hashes can’t be used to verify image accuracy*

This rest of this lecture discusses static acquisition

- *Nelson Chap 10 partially devoted to live acquisition, which we’ll touch on later this semester*

Drive Image Formats for Evidence

Drive images, not logical/partition images

Image Formats for Evidence

Three classes of formats

- *Raw format (dd)*
- *Proprietary formats*
  - But competitors sometimes use them
- *Advanced Forensics Format (AFF)*
  - Open-source format

We will discuss this more in the context of images of logical (i.e., partition) images

- *Bit I'll discuss them a bit now*

Raw (dd) Format

Possible to write bit-stream data to files

Copies all bits in all drive sectors from *source* to *target*

- *All in correct order by sector*
- *Doesn't care what the content is. Might be empty, but still copies it.*

Advantages

- *Fast data transfers*
- *Can ignore minor data read errors on source drive*
- *Most (all?) computer forensics tools can read & write raw format*

Disadvantages

- *Requires as much storage as original disk or data*
- *Tools doing* **dd** *might not collect marginal (bad) sectors*
  - But most tools will identify & mark or skip bad sectors
    - *E.g., dd_rescue*

Proprietary Formats

Features offered

- *Option to compress or not compress drive image files*
- *Can split an image into smaller segmented files*
- *Can integrate metadata into the image file*

Examples

.e01	*EnCase*	*(sort of a de facto standard)*
.001	*FTK*	
.eve	*ProDiscover*	

Disadvantages

- *Inability to share an image between different tools*
- *File size limitation for each segmented volume*

Advanced Forensics Format
AFF

Developed by Simson Garfinkel of *Basis Technology Corp.*

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*

Advanced Forensics Format
AFF

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

AFF is open source

Several imaging tools now support the AFF formats

- *Autopsy/Sleuthkit*
- *OSFMount*
- *Xmount*
- *FTK/FTK Imager*

Acquisition Methods

Static vs. Live

Two types of acquisitions

- ***Static***
- *Live*

Static acquisitions

- *Might not be useful if drive is encrypted and readable only when computer is powered on and logged on*
- *Then live acquisition might be needed in order to read the drive*

Some Full Drive Encryption (FDE) Tools

- COMODO Disk Encryptor
- VeraCrypt
- DiskCryptor
- Bit Locker (really full file system encryption)
  - *Microsoft on Win2K and later OSs*
  - *Logical volume encryption*
- TrueCrypt
  - *Depreciated but v7.1a still available*
- Encrypted File System (EFS)
  - *Microsoft on Win2K and later OSs*
  - *Not completely full drive*

Full Drive Encryption (FDE)

Some hard drive manufacturers are now selling devices with built-in drive encryption

FDE can prevent

- *Ability to create forensic images*
- *Recovery of information*

Some FDE software (e.g., SafeBoot) encrypt every sector on the hard drive including sector 0

You can still make an image, but the image will not have any structure or information

Full Drive Encryption (FDE)

SafeBoot puts the word “safeboot” in sector 0

PointSec puts the word “Protect” in sector 63

BitLocker encrypted drives can be decrypted by

- *Connecting the drive through a write blocker to a machine with BitLocker enabled*
- *Providing the passphrase when booting the system*

What about using a forensic boot CD or USB device?

- *All you will probably see is the FDE pre-boot authentication prompt*

Full Drive Encryption (FDE)

You can have an encrypted drive image in a virtual environment

Live View *(Java tool with GUI)*

- **Live View** *creates a VMware virtual machine from dd disk image or physical disk*
- *Supports encrypted images of most Windows OSs*

Using Live View, boot the VM using VMWare

Enter the passphrase (assuming that you know it)

Full Disk Encryption (FDE)

VMs are an interesting approach for forensics

- *Drive can be decrypted in a virtual environment*
    - A forensic duplicate of the decrypted disk can be acquired
    - Decrypted image can be examined
- *Examiner experiences the running environment*
- *Image is not modified*
    - All changes are written to a separate file
- *Examiner can take multiple snapshots*
- *Examiner can revert back to the original unmodified version*

Live Access of FDE Drives

Leave the target computer running

Use a tool running on a USB drive such as

- *X-Ways Capture*
- *FTK Imager Lite*

Or use a remote capture systems such as

- *ProDiscover IR*
- *EnCase Enterprise*
- *Must have a program running on the target system*

Can then recover an image of the decrypted drive

Live Access of FDE Drives

Live imaging will cause changes to the target drive such as

- *Registry changes*
- *Network connection changes*

But this is better than nothing

- *Extracted files can still be hashed to verify forensic integrity*

Best practices now include live imaging procedures

Live access can also get snapshots of RAM

But whatever you do, document.

Four Acquisition Methods

For either live or static acquisition, there are four methods of acquiring data

1. ***Bit-stream disk-to-image file***
2. *Bit-stream disk-to-disk*
3. *Logical disk-to-disk or disk-to-disk data*
4. *Sparse data copy of a file or folder*

Four Acquisition Methods

1. Bit-stream disk-to-image file

   Most common method

   Can easily make more than one copy

   Copies are bit-for-bit representations of the original drive

   Examples of software

   ProDiscover, EnCase, FTKimager, SMART,
   SleuthKit, X-Ways, iLook, Celebrite…

2. Bit-stream disk-to-disk

   Must consider disk's geometry configuration

   Examples of software

   EnCase, WinHex, SafeBack, SnapCopy

Four Acquisition Methods

3. & 4. Logical acquisition and sparse acquisition

- *Use with disk-to-image or when time is limited*
- *Logical acquisition captures only specific files of interest to the case*
- *Sparse acquisition also collects fragments of unallocated (deleted) data*
- *Use for very large disks or where structure is known*
  - e.g., Email files, RAID servers

It's a good idea make both a bit-stream and a logical acquisition.

- *Makes forensic examination easier.*

Other Acquisition Considerations

When making a forensic copy, consider:

- *Size of the source disk*
  - Lossless compression is useful if the disk is large
- *Use digital signatures (i.e., hashes) for verification of copy accuracy*
- *When working with very large drives, an alternative is to use tape backup systems or network attached storage (NAS)*

Planning Image Acquisitions

Two Verifiable Images*

Make at least two images

Use different tools or techniques

e.g., Use WinHex to make one image and Linux dd to make another

Verify that the two images represent exactly the same evidence.

How?

HPAs, DCOs & Other Areas

Disk drives & SSDs can contain areas that are normally not seen or available to the operating system

- *HPA (Host Protected Area)*
- *DCO (Device Configuration Overlay)*

Some acquisition tools don't copy them

To copy:

- *The acquisition tool must bypass the OS to copy them*
- *It accesses the drive by going directly to the BIOS*

HPAs, DCOs & Other Areas

Not sure why…

It seems strange that a tool that claims to do bit-by-bit sector-by-sector images may not do it to the whole disk

HPAs, DCOs …
What gets or doesn't get everything

ProDiscoverBasic will capture HPAs

FTK Imager 3.4 and earlier did not capture HPA and DCO. Not sure about later versions

WinHex 16.3 & beyond and X-Ways Forensics will detect and capture both HPA and DCO partitions

EnCase 8.05 can detect both HPA and DCO

Raw (dd) copying of an entire disk <u>using a live Linux CD</u> will get everything

There are other products on the market that claim to capture everything

Encrypted Drives

In your future forensic work beyond this course

Be prepared to deal with whole disk encrypted drives

You can copy the encrypted disk, but then what?

You need the password or pass phrase

FDE Decryption Tools

There are FDE decryption tools available:

- *Passware*
- *Elcomsoft Forensic Disk Decryptor*
  - Attempts to extract keys from
    - *RAM captures*
    - *Hibernation or page files*

Using Acquisition Tools

Overview

Nelson Chapter 3 has a detailed section on doing forensic acquisition

- *Mini-WinFE boot CD or USB boot drive*
- *Linux and some Linux tools*
- *Windows using FTK Imager*

There are other forensic imaging tools such as WinHex

Using Acquisition Tools

Acquisition tools that run on Windows

- *Advantages*
  - Make acquiring evidence from a suspect drive more convenient if you're running Windows
    - *Especially when used with hot-swappable devices*
- *Disadvantages*
  - Must protect acquired data with a well-tested write-blocking hardware device
  - Tools sometimes can’t acquire data from a disk’s HPA or DCO

Acquiring Data with a Linux Live (Boot) Distribution

Linux Live CDs boot from the CD or USB

Forensic versions don't use the hard disk at all

Everything needed is contained on the CD or USB drive

Also, Linux can access a drive that isn't mounted

This makes it possible to read any drive without modifying it

All Windows and Linux OSs automatically mount and access a drive

But **forensic** Live CDs and USBs don't access media automatically

In theory eliminates the need for a write-blocker??

But legally this might be challenged

Acquiring Data with a Linux Live (Boot) Distribution

You can use a **forensic** Linux Live distribution to acquire images

Forensic Linux Live CDs and USBs are configured not to mount, or to mount as read-only, any connected storage media

Forensic Linux Live CDs also contain additional forensic utilities

Some well-designed Linux Live CD/USBs for computer forensics are ***Kali*, *CAINE*, *FIRE*, Penguin Sleuth**

Acquiring Data with Linux

Linux distributions can create Microsoft FAT and NTFS partition tables as well as EXT

The Linux ***fdisk*** command lists, creates, deletes, and verifies partitions for FAT, NTFS and EXT

The Linux ***parted*** command does what fdisk does

And handles GPT drives

Also the Linux **mkfs.msdos** command formats a FAT file system

Acquiring Data with Linux

Acquiring data with ***dd*** in Linux

- ***dd** (“data dump” or “disk dup”) command*
  - Can read and write from media device and data file
  - Creates raw format file that most computer forensics analysis tools can read

```
dd if=/dev/sdb of=./image
```

- *Comments regarding **dd** command*
  - Requires use of command line
  - You need to understand what you're doing
  - Does not compress data

Acquiring Data with Linux*

dd command combined with the ***split*** command segments output into separate volumes

This is desirable so that the image can be put on to several target storage devices that are smaller than the original

e.g., the image of a 100GB disk to a set of DVDs

Example command

```
dd if=/dev/hda2 | gzip -c | split -b 4000m -option
  /mnt/dvd/backup.img.gz
```

Acquiring Data with Linux

Acquiring data with ***dcfldd*** in Linux

- *Developed by Nicholas Harbor of Defense Computer Forensics Laboratory*
- ***dcfldd** provides additional functions beyond **dd***
  - 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

dd command is harder to use for forensic purposes

Validating Data Acquisitions Including Forensic Images

Validating Data Acquisitions

A critical aspect of computer forensic acquisition

Requires using a hashing algorithm utility

Some validation hashes

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

Linux Validation Methods

Validating ***dd*** acquired data in Linux

- *You can use **md5sum, sha1sum, sha256sum, sha384sum, sha512sum** or other hash utilities*
- *Hash 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*
- *Also Win10 has the Ubuntu Bash shell included as part of the Win10 distro*

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

- *Do separate manual validation for all raw acquisitions*

Suggested Lab Exercises

Suggested Lab Exercises

On your personal computer

Install a trial copy of WinHex

Install FTK Imager 4.7.1

Find a small USB flash drive

By small I mean much 500 MB or less – (Difficult to find).

Put 6 to 10 files on it. The delete, some but not all, of the files.

Using WinHex and FTK Imager, take forensic images of the files.

You can use WinHex on RADIGSHng, but you will need to know how to have WinHex on RADISHng access your small USB drive when it is plugged into your personal computer.

This might present you with some problems

I'll now demo taking a physical and logical image using FTK Imager.

RAID Acquisitions

RAID

Redundant Array of Independent Drives (RAID)

- *Originally: "**Redundant Array of Inexpensive Disks**"*
- *Computer configuration involving two or more disks*
- *Originally developed as a data-redundancy measure*

There are a number of different RAID configurations

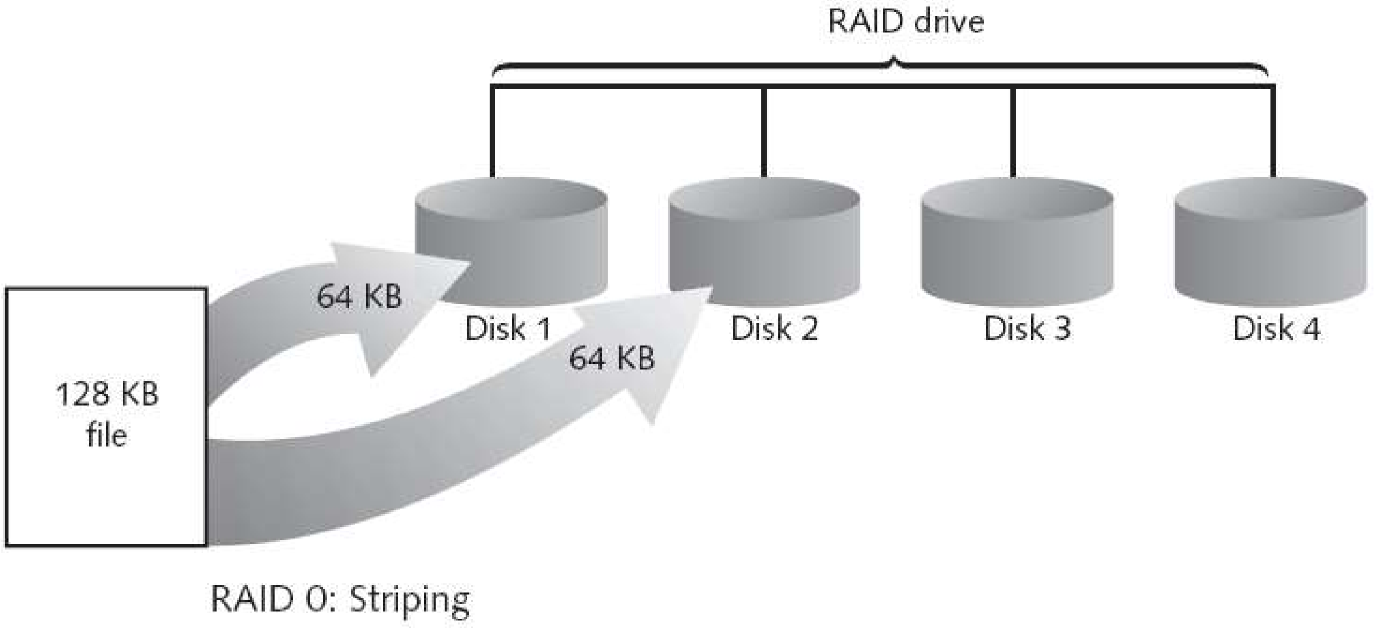
- *Each designated as "RAID x"*

RAID 0

Provides rapid access and increased storage

No redundancy

Two or more disks appear to the OS as a single volume



RAID 1

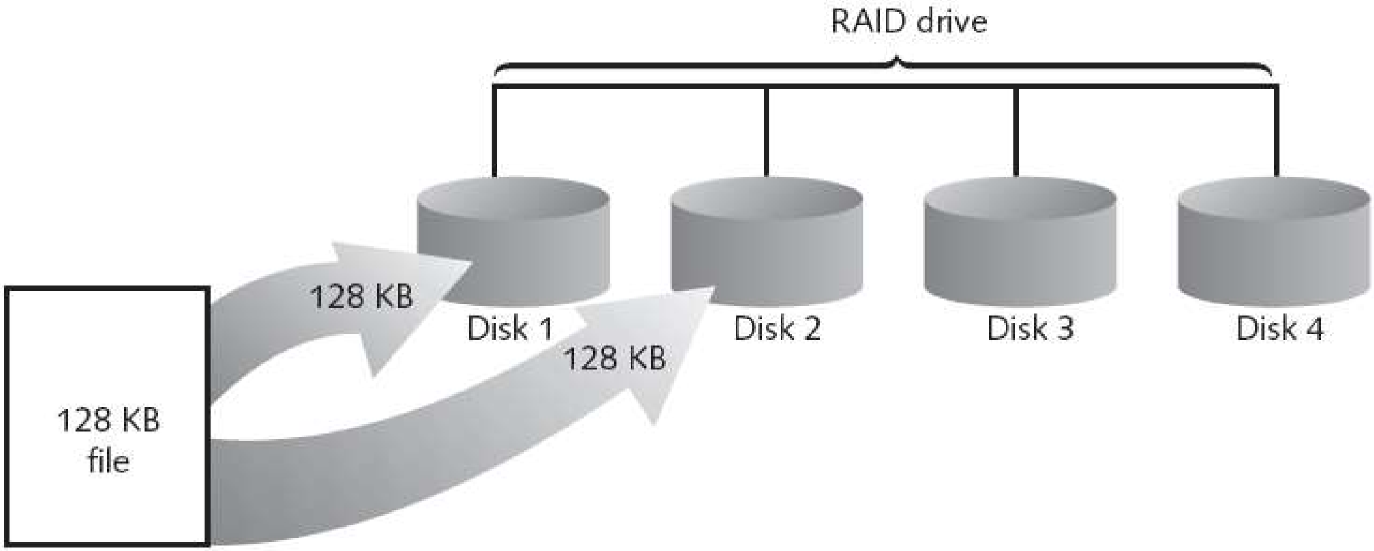
Designed for data recovery

More expensive than RAID 0

Usually uses two drives

Contents of the two drives is identical

Mirroring



RAID 1: Mirroring

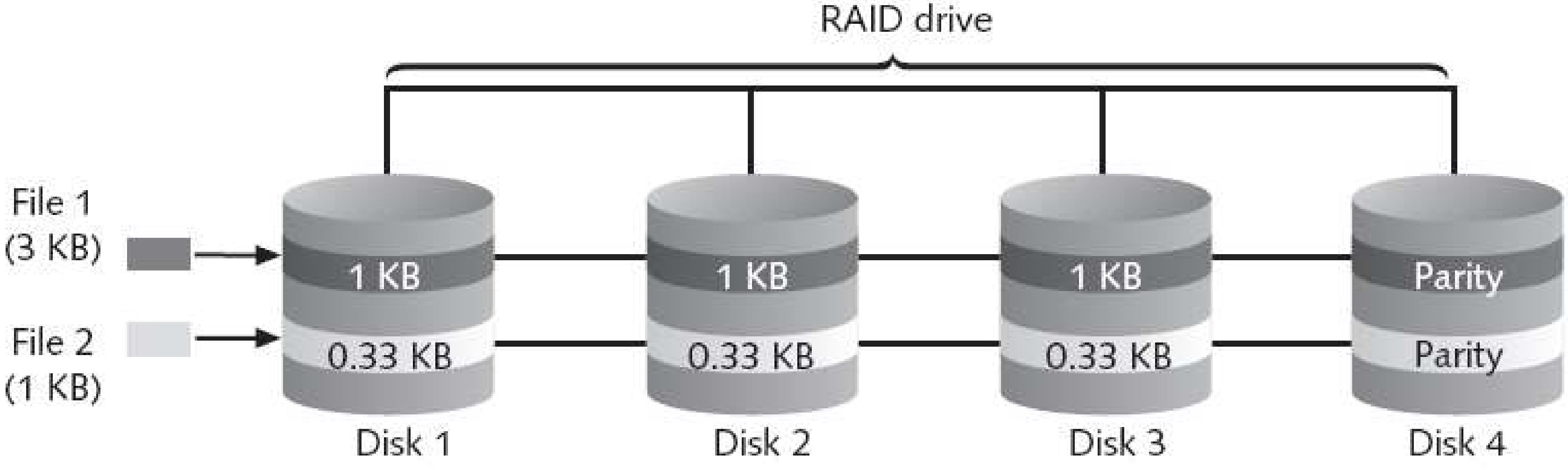
RAID 2

Data is written to a drive at the byte level

Has better data integrity checking than RAID 0

Parity is used on a separate drive

Slower than RAID 0 or 1



RAID 2: Striping (bit level)

RAID 3

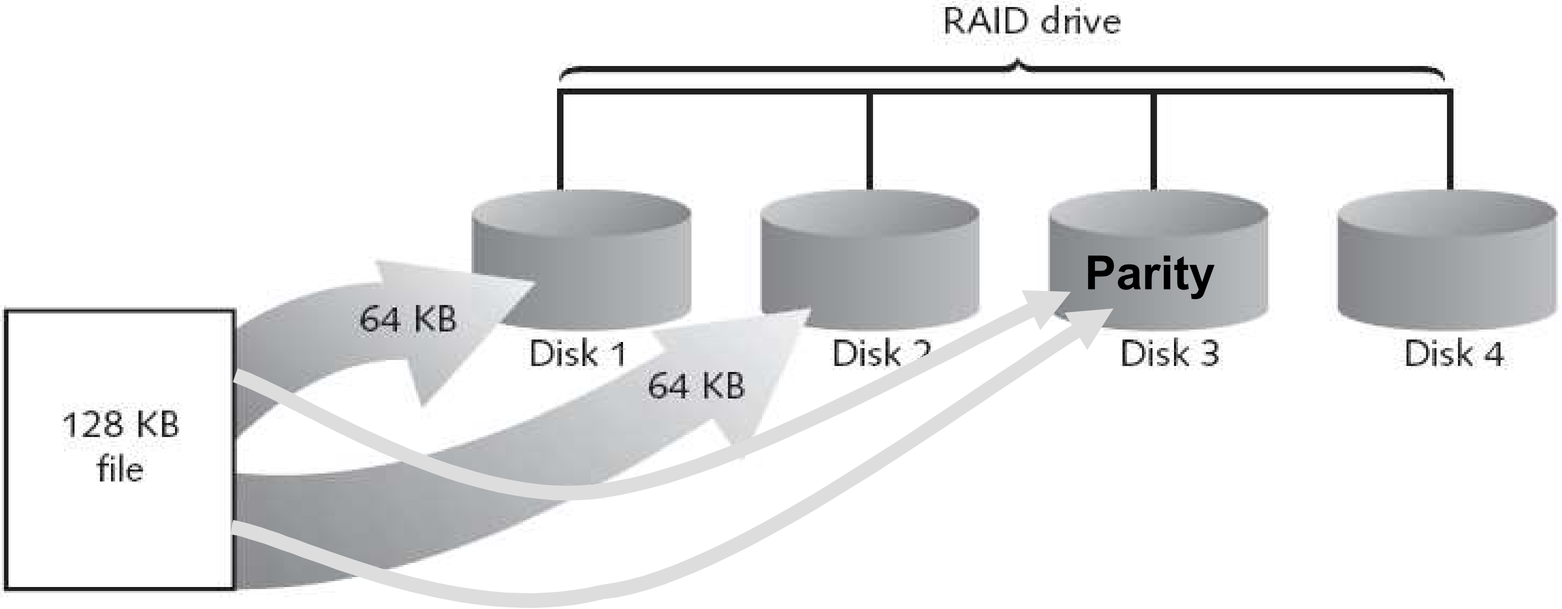
Uses data striping and dedicated parity

Must have 3 or more drives

Two for RAID 0 – for data

A third for parity

Like RAID 0 but adds a separate drive for parity



RAID 4

RAID 4

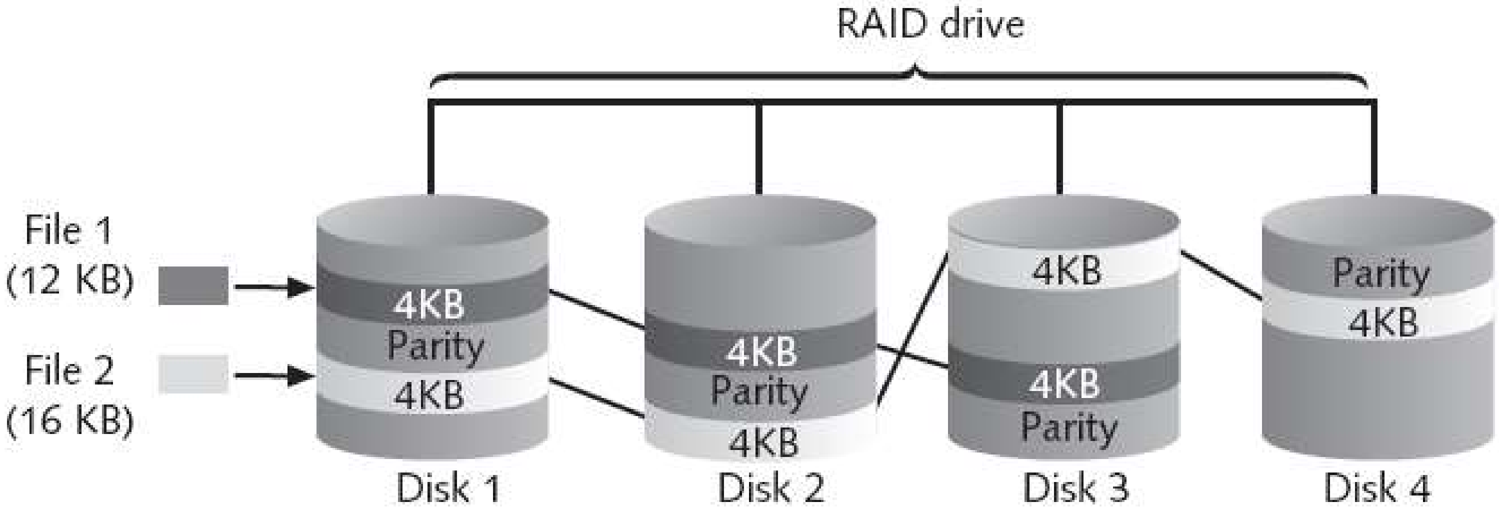
- *Similar to RAID 3*
- *Data is written in block, not bytes*
- *Blocks are interleaved*

RAID 5

RAID 5

Similar to RAID 0 and 3

But places parity recovery data on each drive



RAID 5: Block-level striping with distributed parity

RAID 6 & 10

RAID 6

Redundant parity on each drive

RAID 10, or mirrored striping

Also known as RAID 1+0

Combination of RAID 1 and RAID 0

Stripes a file onto a pair of drives

Requires 4 or more drives

Mirrors the drive pair on another drive pair

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 drive?*

Nelson says that older hardware-firmware RAID systems can be a challenge when you're making an image

- *Due to the fact that early RAID systems used proprietary formats*

Acquiring RAID Disks

Vendors offering RAID acquisition functions

- *Technologies Pathways ProDiscover*
- *Guidance Software EnCase*
- *X-Ways Forensics*
- *Runtime Software*
- *R-Tools Technologies*
- *FTK 2 & 3*

Occasionally, a RAID system is deemed to be too large for a full static acquisition

- *Retrieve only the data relevant to the investigation with the sparse or logical acquisition method*

Remote Acquisition

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 will slow down the process 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* (not Basic) 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*
- *Has an optional stealth mode*

ProDiscover Incident Response 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*
- *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*

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*
- *Potentially malicious?*

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

Runtime Utilities

- *DiskExplorer for FAT*
- *DiskExplorer for NTFS*
- *RAID Reconstructor*
- *DriveImage*
- *ShadowCopy*
- *GetDataBack for FAT*
- *GetDataBack for NTFS*

Features for acquisition

- *Create a raw format image file*
- *Segment the raw format or compressed image*
- *Access network computers' drives*

Some Other Acquisition Tools

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 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*

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*

PyFlag
Australian Department of Defence

PyFlag tool

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