1.8. Data Acquisition

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)

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

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 format is unofficial standard

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

Determining the Best Acquisition Method

- 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
  - ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLookIX
- Creating a disk-to-disk
  - When disk-to-image copy is not possible
  - Tools can adjust disk's geometry configuration
  - EnCase, SafeBack, SnapCopy
- 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
    - 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 called BitLocker makes static acquisitions more difficult and May require user to provide decryption key

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

- Some countries haven't accepted the use of write-blocking devices for data acquisitions

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 readwrite mode so you can run an acquisition program

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
- 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
- F.I.R.E
- CAINE
- Deft

- Kali Linux
- Knoppix
- SANS Investigative Toolkit
- 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

– If you have a functioning Linux computer, follow steps starting on page 99 to learn how to prepare a target drive for acquisition

- 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)

– Follow the step starting on page 104 in the text to make an image of an NTFS disk on a FAT32 disk

- Acquiring data with dcfldd in Linux

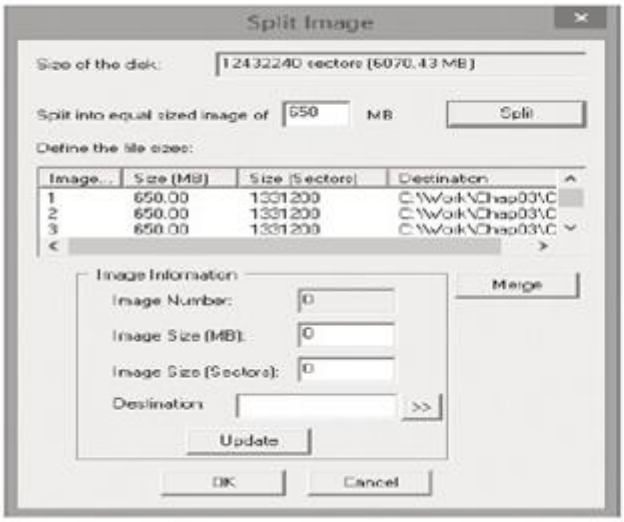
– The dd command is intended as a data management tool

- 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 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 write-blocker device
  - Create a storage folder on the target drive
- Using ProDiscover's Proprietary Acquisition Format
  - ProDiscover creates image files with an .eve extension, a log file (.log extension), and a special inventory file (.pds extension)
  - If the compression option was selected, ProDiscover uses a .cmp rather than an .eve extension on all segmented volumes
- Using ProDiscover's Raw Acquisition Format
  - Follow the same steps as for the proprietary format, but select the —UNIX style dd format in the Image Format list box
  - Raw acquisition saves only the image data and hash value
  - The raw format creates a log file (.pds extension) and segmented volume files



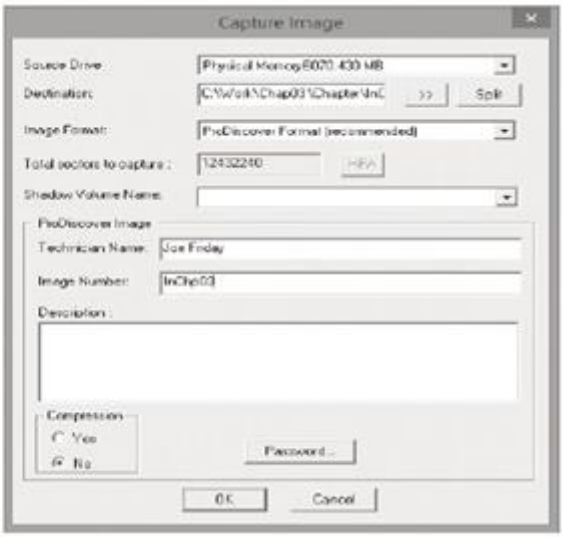


Fig: The split image dialog box **Fig: The Capture Image dialog box**

Capturing an Image with Access Data FTK Imager Lite

- 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

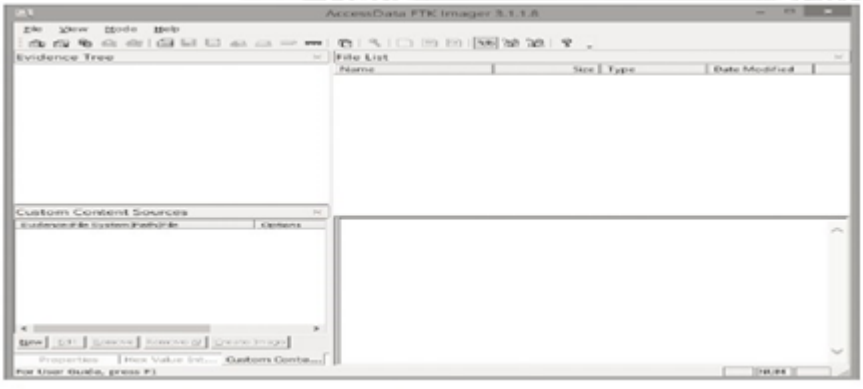


Fig: The FTK Imager main window

- 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

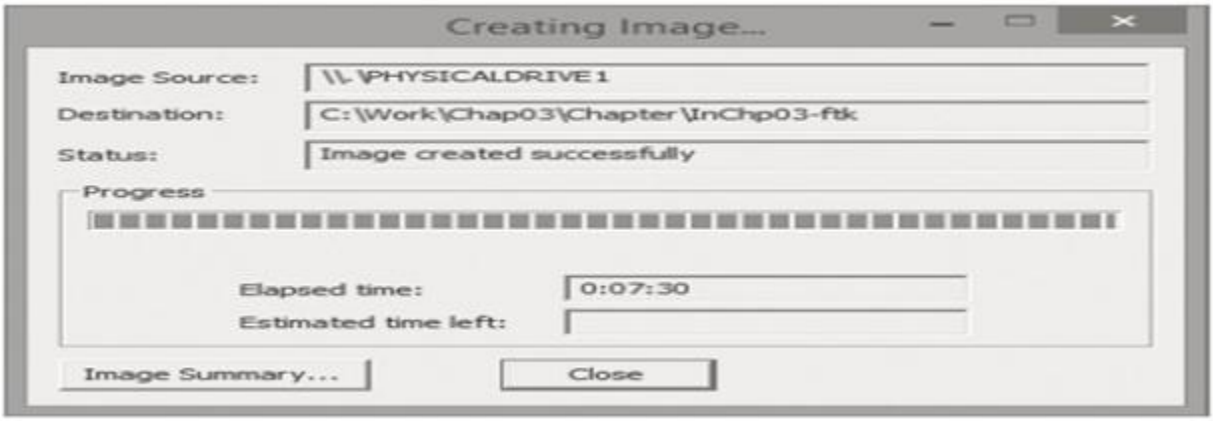


Fig: A complete image save

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

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

- 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 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
  - Biggest disadvantage is lack of redundancy

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

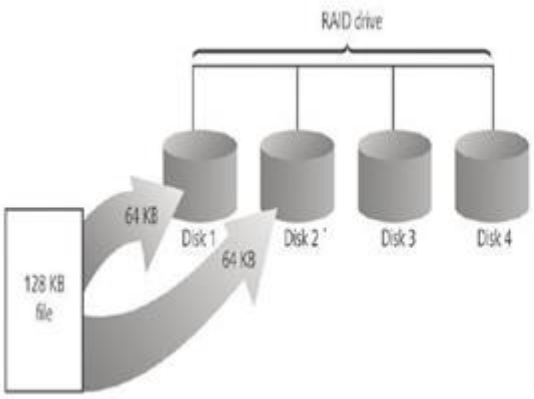


Fig: RAID 0-Striping

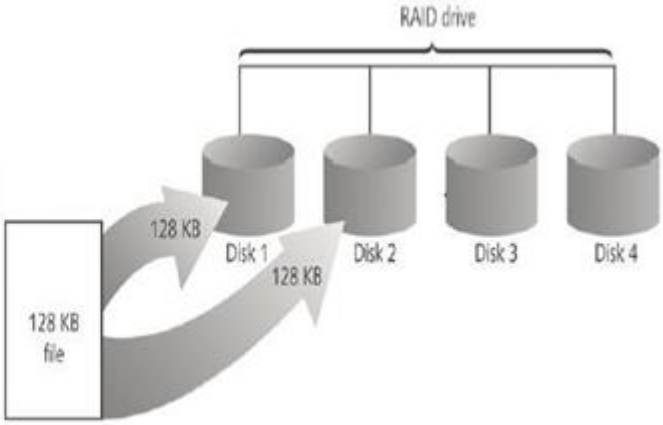


Fig: RAID 1-MIrroring

- 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
- RAID 4
  - Data is written in blocks

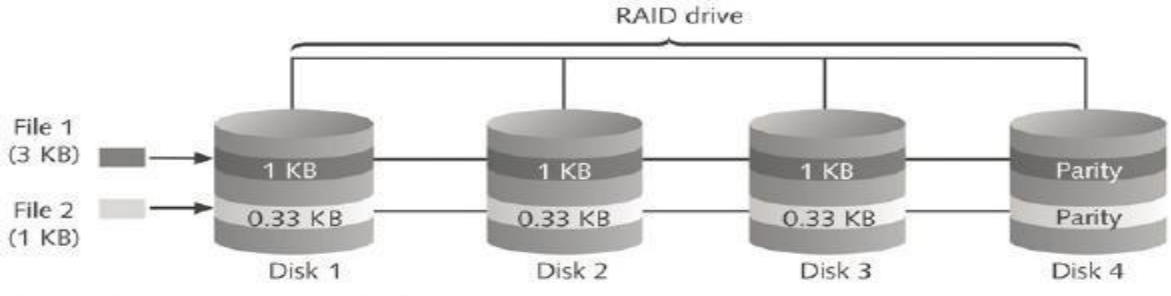


Fig: RAID 2-Striping (bit level)

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

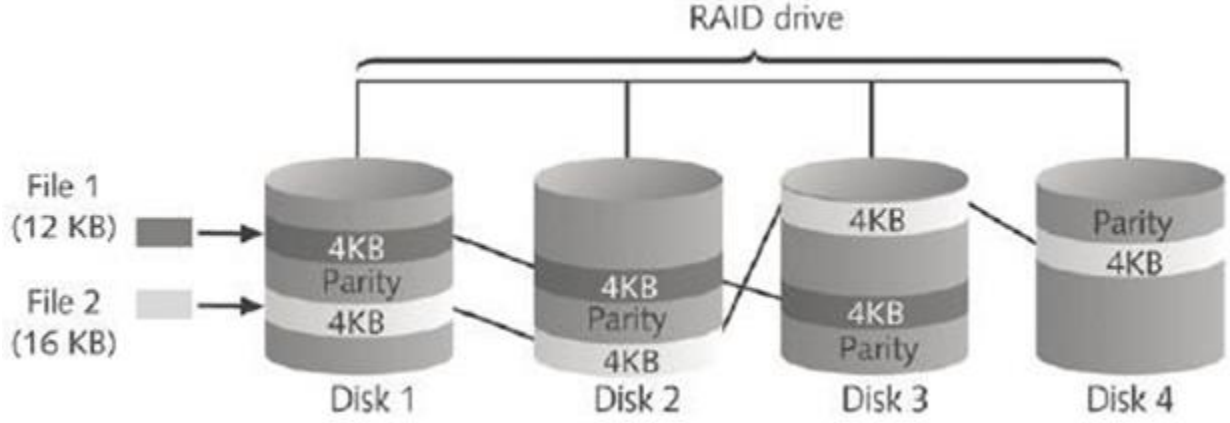


Fig: RAID 5:Block level striping with distributed parity

Acquiring RAID Disks

Address the following 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?

- Copying small RAID systems to one large disk is possible
- Vendors offering RAID acquisition functions
  - Technology Pathways ProDiscover
  - 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

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

Remote Acquisition with ProDiscover

- 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

  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

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 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

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

Using Other Forensics-Acquisition Tools

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

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

ASRData SMART

- ASRData 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

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 – Supports:

- IDE (PATA)
- SCSI
- USB
- FireWire