Disk Forensics

Definitions

- Disk forensics is the study and analysis of storage volumes
- Keep in mind that in 2022 this isn’t all physical disks!
- Disk forensics is typically used when you:
  - Cannot access the running state of the system
  - Are investigating historical activity
  - Are working a Law Enforcement (LE) case

Types of Disks

Magnetic Disks

- Traditional “spinning disks”
- Spinning platter with a thin magnetic coating
- “Head” moves over the platter to write 1’s and 0’s
- Same head used to read data off of the disk
- Sometimes hard to find / access data that’s not sequential (seeking / fragmentation)

Solid State Drives

- No magnets
- Flash memory to store data
- Specifically uses NAND flash which is persistent without power (unlike RAM)
- Can write to a page level, erase at a block level
- Garbage collection

Types of Disks

VMWare Volumes

- A.k.a. “private cloud”
- Disk is a logical container on another disk.
- May be running on a non-traditional Operating System.
- We acquire through VMWare itself – virtual disk acquisition.
- Suspend the system > take a snapshot > analyze the vmdk.

AWS EBS Volumes

- Public cloud.
- Everything is abstracted.
- We again use the abstraction interface to capture the disk (AWS EBS Snapshot).
- Now we typically mount them on another instance to do the analysis (like a Magnet instance in AWS).

Common File System Formats

- NTFS New Technology File Allocation
- FAT File Allocation Table
- FAT32
- Apple File System (APFS)
  - Standard file system for macOS 10.12.4+
  - Also used for iOS, iPadOS, watchOS.
  - Optimized for SSDs

What is a file?

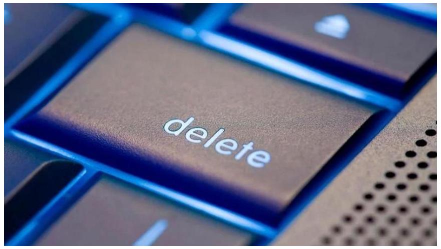
- Seems simple right?
- Short answer is that it depends on the file system.
- “indexed” file systems keep an index of every file on the disk
- On an indexed file system the file is a combination of:
  - Index entry (record) on MFT (Master File Table) for NTFS (metadata)
  - Points to a location(s) on disk where the actual bytes reside

File Deletion

- File deletion is not straightforward and can happen differently depending at an operating system and physical level
- This presents both challenges and opportunities for forensic investigators

File Delete – Operating System

- What happens when you “delete” a file in Windows?



- “Delete” -> moves file to recycle bin.
- “Permanently Delete” -> only removes the metadata / journal entry.
- “Slack Space” -> “empty” disk we can look to carve files from.

Physical Disk Capture

Capturing the physical contents of a drive.

- Pros:
  - May get deleted files.
  - Will be able to parse the entire “raw” disk and data structures.
- Cons:
  - Capture used and “unused” disk space
  - Time consuming.
  - Large output file.

Logical Disk Capture

Capturing the logical contents of a drive.

- Pros:
  - Gives us all of the files from the operating system's point of view.
  - Quick
  - Small(er) output files.
- Cons:
  - Won't get unused disk space.
  - No chance of recovering deleted files.

Disk Capture Formats

.RAW (DD)

- Literally the RAW disk formats

.E01 (EnCase Evidence File)

- Most common capture format for forensics.

MBR

- Master Boot Record
- Stored in the first sector of the hard disk.
- Contains the partition table.

GPT

- GUID Global Unique IDentifier Partition Table
- Used in most modern (non-Windows) operating systems.
- Typically used in 2022 unless there are hardware or other backwards-compatibility concerns.

Partition Tables

- Table that describes the logical segmentation and portioning of the physical disk.

Analysis of Disk Forensics

Investigation Options

- Critical to understand what Disk forensics is good at.
- Critical to understand what you’re doing in the disk image _before_ you get into it.

What is it good for?

- Historical investigation.
- Timelines.
- Timelines.
- Timelines.
- Recovering deleted files.

Timelining

- Leverage tools and automation to help process timelines (like Autopsy or Magnet).
- Remove / filter baseline OS actions and behavior that’s not relevant to the current investigation.
- Find the key event.
- Bookend your investigation as soon as possible.
- Know your local (computer) timezones – use UTC

MAGNET FORENSICS

AUTOPSY DIGITAL FORENSICS

Key Filesystem Locations

- Temporary files
- Browser temp / artifacts
- Browser downloads cache
- Email attachments
- Prefetch
- Windows registry
- Jump lists
- Common log directories

Environment Variable Shortcuts

- %USERPROFILE%
  - C:\Users\<USERNAME>
- %TEMP%
  - C:\Users\<USERNAME>AppData\Local\Temp
- %SYSTEMROOT%
  - C:\Windows\
- %USERPROFILE%
  - C:\Users\<USERNAME>

Temporary Files

Attackers will often stage out of temporary directories, can often find useful artifacts.

- C:\Windows\Temp
- C:\Users\<USERNAME>AppData\Local\Temp\
- %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat
- %USERPROFILE%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\places.sqlite
  - Table:moz_annos
- %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History

Browser Downloads Cache

Downloads managers in modern browsers will track files downloaded from the Internet.

- Firefox
  - %userprofile%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\downloads.sqlite
- Chrome (also sqlite)
  - C:UsersUSER_NAMEAppDataLocalGoogleChromeUserDataDefaultHistory
  - C:UsersUSER_NAMEAppDataLocalGoogleChromeUserDataChromeDefaultDataHistory
- Edge
  - C:\Users\%USERNAME%\AppData\Local\Microsoft\Edge\User Data\Default

Email Attachments

Lots of malware comes from email attachments.

- %USERPROFILE%\AppData\Local\Microsoft\Outlook

Prefetch

“Increases performance”

- Limited number of files that get effectively pre-cached.
- Get the date / time file by the name and path it was first executed and last executed.
- C:\Windows\Prefetch

AMCACHE

AMCACHE

- Application Experience Service Cache
- Win7+
- C:\Windows\AppCompat\Programs\Amcache.hve
- Entry for every application executed:
  - Full path information.
  - Last modification time.
  - SHA1 hash of the executable

Registry

One of the ways we can get access to the registry is on disk. The registry is effectively its own filesystem and a forensically rich source of information.

- %SYSTEMROOT%\System32\config
- %USERPROFILE%\Ntuser.dat

Jump Lists

Related to recent items in the task bar.

- Data is stored in the AutomaticDestinations folder
- C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recnet\AutomaticDestinations

Logon Activity

Attempted and actual system logons.

- Data is stored in Windows Event Logs (winEVT)
- %SYSTEMROOT%\System32\winevt\logs\Security.evtx
  - EVT 4624 – successful logon
  - EVT 4625 – failed logon
  - EVT 4634|4647 – successful logoff
  - EVT 4684 – Runas Logon
  - EVT 4672 – Administrator logon
  - EVT 4720 – Account created

Common Log Directories

Attackers will often stage out of temporary directories, can often find useful artifacts.

- Apache Tomcat
  - <install_dir>\logs
  - C:\Program Files\Apache Software Foundation\Tomcat 10.0\logs
- Weblogic logs
  - DOMAIN_NAME\servers\ADMIN_SERVER_NAME\logs\DOMAIN_NAME.log
- Exchange
  - C:\Program Files\Microsoft\Exchange Server\V15\Logging
  - C:\inetpub\logs
  - Keep in mind that there are 2 web servers on an OWA box (front / back)
  - ECP specifically (often exploited component) - c:\Program Files\Microsoft\Exchange Server\V15\Logging\ECP\ServerException\
- VSphere
  - C:\ProgramData\VMware\VCenterServer\runtime\VmwareServiceSTS\logs\