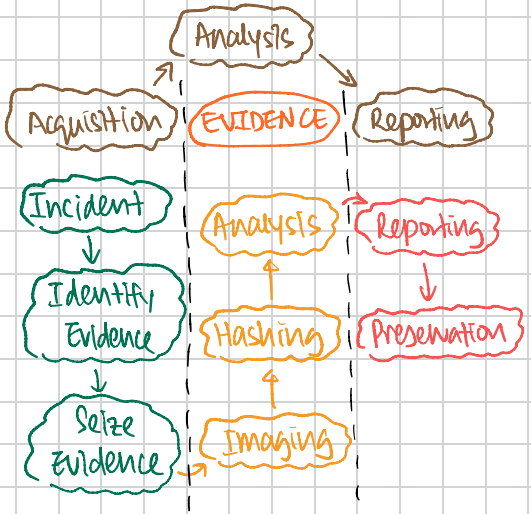
GitHub @deezombiedude612

IV. COMPUTER FORENSICS

Computer forensics

* application of scientifically-proven methods to gather, process & interpret [digital evidence] → any data that is preserved in a comsys that can be read or understood by ppl or computer systems\apps.
* process:



* answers the following questions (5W1H)
  - ↳ WHAT – Does it indicate potential digital evidence?
  - ↳ WHERE – Does it pinpoint location of event?
  - ↳ WHEN – Does it provide timeline of event?
  - ↳ WHO – Does it associate someone to an event?
  - ↳ WHY – Does it provide reasons why the event takes place?
  - ↳ HOW – Is it clear how you will use the evidence?

Data migration: process of moving data frm 1 location\format\app to another

Data Presentation

① preserve data frm most volatile first
② decide tradeoff btwn volatile vs non-volatile data
③ speed is of essence.
  ↳ manual collection: slow
  ↳ automatic collection: collects more data & more consistent

Data Volatility

Volatile Evidence

- RAM contents
- open\unsaved docs
- running processes
- pwds in clear text
- recent chat conversations
- network connections

Non-Volatile Evidence

* Master File Table (MFT)\ Master Boot Record (MBR)
* Registry
* Logs
* Config Files
* App Files
* SWAP Files
* Temp. Files
* Data Files
* unallocated space

File Systems

- NTFS
  - max. 256 TB (64KB format)
  - 8 PB (2MB format)
- EXT2\3\4
  - max. 4TB (1KB format)
  - 8TB (2KB format)
  - 16TB (4KB format)
  - 256 PB (64KB format)
- FAT32
  - max. 2TB (512 byte format)
  - 8TB (2KB format)
  - 16TB (4KB format)
- exFAT
  - max. 128PB

Refer: educaba.com/data-vs-metadata

DATA	METADATA
collection of info, but to add context to them	classified info; more detailed & defined in the system
provides info, but to all are necessarily relevant	provides detailed info abt the data & its instances
to description of resources	provides details abt resources
to responsible for managing users; unable to classify info required frm system	classifies kind of info required frm system; allows for user mgmt thru tracking user activities
to help in migration & desc. of data	helps in migration & discovering various instances of data
∴ to have other details that help in migration	⇒ system can know their working level & get info abt past performances
to always processed ⇒ discovering data for migration or checking facts became hectic	assured to be always processed
info abt data updated using Data Manipulation Language → makes them work in system when user needs info	metadata in data dictionary updated using Data Def^{n} Language → keeps metadata current ⇒ relevant in user's daily activities
to show location data, to be used in future before processing	shows location data, saves relevant data for future use
img or text in document is what is referred to as data.	metadata captures impt. details abt files (ex., timestamp of when saved)

NOTE: All disks, tapes & printouts are maintained for min. 10 years after data is reported.

Source: forensicresources.org/wp-content/uploads/2020/4-13-1-Control-of-Records.pdf

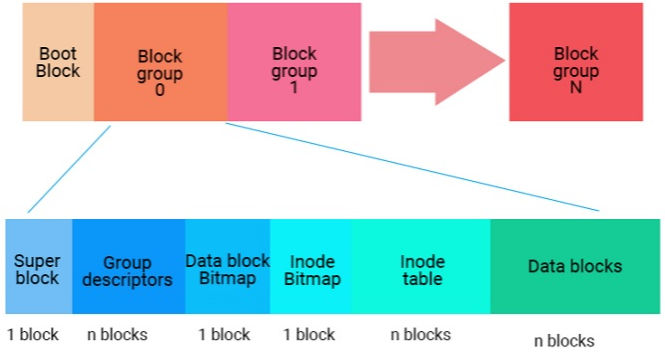
FAT File System Structure

FAT32 File System Structure

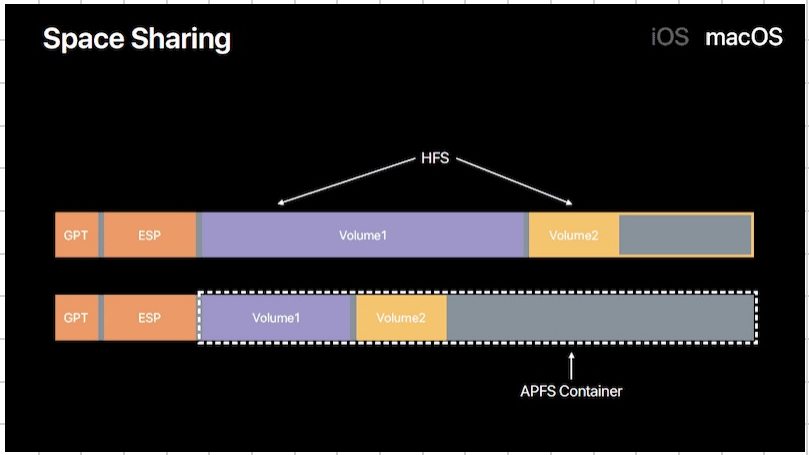
exFAT File System Structure

exFAT: Extensible File Allocation Table
* format primarily designed for removable storage devices
* 4 main sections
  - main boot region
  - backup boot region
  - FAT region
  - data region

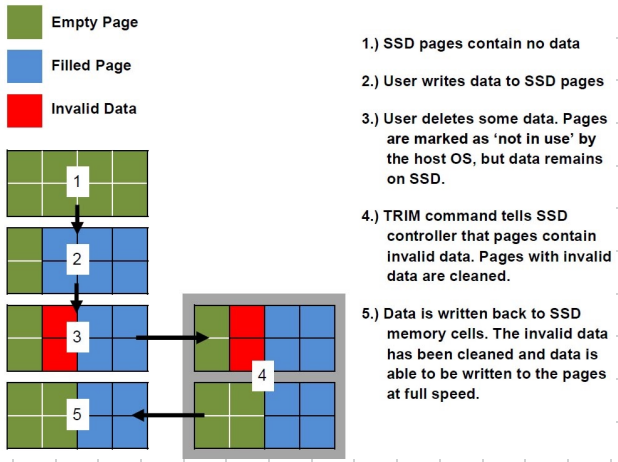
FAT: File Allocation Table
* contains data region map
* FAT area → table of contents for Data Area
* 4 major components
  - reserved sectors
  - FAT region
  - root directory region
  - data region



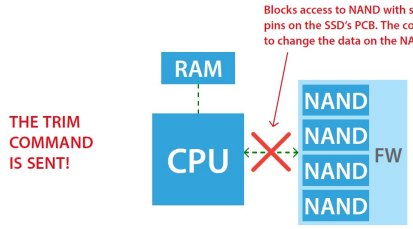
(for Linux)
EXT File System Structure



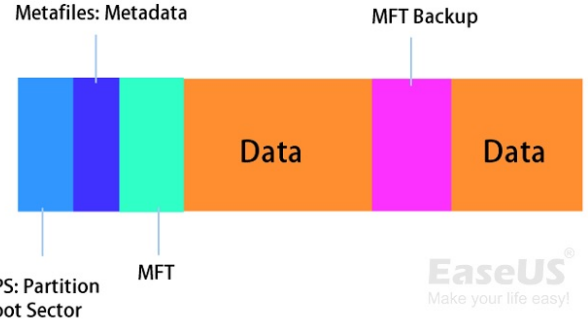
In HDD, new data can overwrite region that previously holds data marked as deleted.
↳ no the case for SSDs



TRIM Command
* works in Garbage Collection to clean up & organize SSD
  ↳ SSD efficiency & lifespan ↑
  ↳ downside: bane for data recovery for SSD
* Garbage Collection
  ↳ goal: periodically optimize drive to ↑ drive's efficiency & lifespan
* to prevent TRIM: disable access to CPU & NAND chips
  ↳ short circuit drive into SAFE mode



NTFS File System Structure (for Windows)



belkasoft.com/why-ssd-destroy-court-evidence
kingston.com/en/blog/pc-performance/ssd-garbage-collection-trim-explained
blog.acelab.eu.com/pc-3000-ssd-how-to-bypass-the-trim.html

Windows Forensics

* Core Windows services → C:\Windows\System32
  (ex., svchost.exe, winnt.exe, lsass.exe)
* Windows Prefetch → C:\Windows\Prefetch
  ↳ maintains a list of used programs
    to ↓ time taken to open program
  ↳ a method to identify evidence of execution
  ↳ proprietary format ⇒ ✗ built-in tool to parse data
* Process Explorer \ Task Manager
  ↳ use to examine props. of sus. files
    → running fm uncommon location
    → missing company name
    → missing digital signatures
    → open TCP connections
    → compressed \ packed files

learn.microsoft.com/en-us/sysinternals/downloads/sigcheck

* Sigcheck (part of Sysinternals suite of tools)
  ↳ checks digital signatures of exes against Microsoft certificates
  ↳ helps identify files trying to hide inside Windows $PATH
  ↳ useful cmd line switches: sigcheck [switch] <file\dir>
    - -e scans for exes regardless of listed extension
    - -c generates csv output
    - -u only display unknown files
    - -v performs lookup in VirusTotal for assoc. hash of suspected file
    - -vt used w above to agree to VirusTotal's ToS

⚠ Tool correlation based on findings

pecmd.exe (3rd party tool)
* presents content of .pf files in human-readable format
  ↳ created at, modified at, last accessed at
* keeps track of last 8 times a program is run
* highlights lives of potential interest — assoc. dirs\files

⚠ upload sus. file to VirusTotal

↱ can help clearly identify what happened

Timeline Analysis gathers input fm multiple srcs, places them in chronological order

↳ NTFS Timestamps:
- M → last modified (content of file)
- A → last accessed
- C → metadata changes
- B → when was file born\created

File Creation	File Deletion	File Modification	File Access	File Copy	Local File Move	Volume File Move	File Rename
Modified – Time of File Creation	Modified – No Change	Modified – Time of Data Modification	Modified – No Change	Modified – Inherited from Original	Modified – No Change	Modified – Inherited from Original	Modified – No Change
Access – Time of File Creation	Access – No Change	Access – No Change	Access – No Change NTFS Win7<	Access – Time of File Copy	Access – No Change	Access – Time of File Move	Access – No Change
Metadata – Time of File Creation	Metadata – No Change	Time of Data Modification	Metadata – No Change	Metadata – Time of File Copy	Metadata – Time of Local File Move	Metadata – Inherited from Original	Metadata – Time of File Rename
Creation – Time of File Creation	Creation – No Change	Creation – No Change	Creation – No Change	Creation – Time of File Copy	Creation – No Change	Creation – Time of File Move by CLI*	Creation – No Change

MUICache
* shows software which has been executed on a system
* ✗ timestamp info, but have descriptive comments

user assist file
contains list of programs executed on system
(incl. filename, run count, last execution timestamps)

MRU (Most Recently Used)
many apps have MRU list detailing which files were recently opened by the app

NTUSER.DAT
* settings specific to indv. users; tracks user activity & preferences
* stored in root of user profile, moves btwn systems w roaming profiles

Windows Registry Analysis

Security Accts. Manager (SAM)
(only local \ domain admins)
contains username, SID, encrypted pswd hash ∀ users in a domain

System
contains Windows OS setup, mounted devices, hardware settings & services

Security
* contains security permissions for admins
* used by sys. to enforce security policy
* limited usefulness for forensics

Software
contains programs & Windows settings ∀ software on system