UNIT - 2

Initial Response and Acquiring-Analyzing Digital evidence

What is Acquisition?

Acquisition is making a forensic copy of evidence, which could be any type of media

Data Acquisition is the process of taking an image from a machine.That image would be a copy from everything on the machine's storage device.

Why do we Acquire?

- You might end up damaging evidence while searching and working.
- You'll find that the client you're working for cannot afford to let you keep the machine till the end of your investigation
- With only one copy (which is the original machine) there is no way for multiple teams or investigators to work on the same case in parallel.

Volatility: Data volatility is defined as the rate or the likeliness for a change on a data set. A change could either be alteration or destruction.

Order of Volatility

Data is least volatile when stored on a secondary storage device such as a HDD

Types of Data Acquisition:

Static Acquisition is gathering non volatile data. In other words, gathering the data that remains intact after the system's reboots or goes down.Such acquisition is usually performed on hard disks and Flash

disks.

Dynamic Acquisition is gathering volatile data usually while the device is still running In this technique we are interested with the data that will get lost if the system goes down.

Dead acquisition refers to the attempt to acquire data from the suspect's machine without the operating system assistance. This is usually done with the help of the machine's hardware.

First Responder

- Investigation will send one or more individuals to investigate the case; this person is called the first Responder.
- He/she is responsible for conducting the initial investigation of the incident to determine its root cause, who from different backgrounds with official training
- The main role of the first responder is to identify, collect, preserve,transport digital evidence to the forensic lab in addition to identifying the root cause of an incident.
- He/she needs to identify their work scope clearly to avoid missing any detail related to the subject case.

The first responder needs to ask the reporting person/company some questions to determine the scope of work.

1. Does the reporting body need to investigate the case officially so they can move it to court later?
2. Do they just want to confirm that an attack was made against their computerized systems and ensure that no further damage can happen?

Key points in digital forensics investigations include:

1. **Search and Seizure:** Conducting searches and seizures of digital devices while adhering to legal standards, such as those outlined in the Fourth Amendment.
2. **Consent to Search:** When the owner of a device cooperates, allowing investigators to search and acquire digital evidence without an official warrant.
3. **Subpoena:** Obtaining court orders or permits to search and seize digital equipment when permission from the device owner is not granted. Care must be taken to prevent the destruction of digital evidence.
4. **Search Warrant:** The most powerful procedure allowing law enforcement to conduct searches without prior notice, particularly useful when there's a risk of evidence destruction.
5. **Electronic Storage Device Search Warrant:** Permitting the seizure of digital storage devices from suspect premises.
6. **Service Provider Search Warrant:** Allowing investigators to access information from external providers such as ISPs, cloud storage providers, and online merchants when relevant to the investigation.

General principles for the correct acquisition

The principle of correct acquisition in digital forensics involves several key steps to ensure the preservation of evidence and integrity of the investigation:

1. **Disable Surveillance Cameras:** Upon arrival at the scene, ensure any surveillance cameras are disconnected or covered to prevent interference with the investigation.

2. **Prevent Evidence Destruction:** If there are signs that the computer is actively destroying evidence, such as running specialized wiping software, immediately shut down the computer to prevent further data loss.
3. **Handling Powered Off Computers:** If the computer is already powered off, refrain from turning it on. Instead, seize it in an antistatic bag and transport it securely to the forensic lab.
4. **Handling Powered On Computers:** If the computer is powered on:
    - If a login window is displayed, power off the device and perform a hard shutdown.
    - If the screen is dark or showing a screensaver, move the mouse slowly to reveal the screen without interacting with the system. Photograph the screen to document running programs, opened files/folders, and system date/time.
5. **Acquire Volatile Memory (RAM):** Use specialized tools to capture the volatile memory (RAM) of the computer before powering it off, as it can contain valuable information crucial to the investigation.
6. **Acquire Networking Information:** If the computer was connected to a network device, gather networking information such as IP address, open sessions & ports, routing table, LAN addresses, broadcast address, and network interface card number.
7. **Document Seizure Steps:** Document all steps taken to seize the suspected computer device, ensuring that a record is available for future reference or inquiries.
8. **Secure Portable Devices:** When seizing portable devices with wireless communication capabilities, place them in impermeable bags to block wireless communications and prevent remote tampering.

Types of Shutting Down

1. **Hard Shutdown:**
    - This involves forcibly powering off the computer by removing the battery (for laptops) or unplugging the power cord (for desktops).
    - Advantages:
        - Preserves system files.
        - Prevents wiping programs from activating upon shutdown.
        - Prevents changes to files' timestamps and other attributes.
    - Disadvantages:
        - Removes unsaved open files, risking data loss.
        - May corrupt system files and the user's open documents.
2. **Graceful Shutdown:**
    - This method involves powering off the computer using the ordinary shutdown procedure, such as selecting "Shut Down" from the operating system's menu.
    - Advantages:
        - Discovers open files and programs upon shutting down.
        - Prevents corruption to system files.
        - Allows running applications to write any artifacts to the hard drive for potential recovery later.
    - Disadvantages:

- Risk of launching destructive programs configured to run at shutdown.
- Possibility of overwriting data on the hard drive.
- Activation of user-created scripts that may perform tasks like removing system logs or clearing system pagefile (if configured to do so upon normal shutdown).
- Potential changes to attributes of files.

Documenting the Digital Crime Scene

- Document how long you stayed there, and with whom.
- Name all people who accessed the crime scene and list each one's role
- The first responder must also document all items related to the case in hand that have been discovered at and acquired from the crime scene
- Photograph all areas of the crime scene; you can also use video for this purpose. Photography should be conducted twice, once upon entering the scene and the second before leaving

The evidence bag must include a detailed panel listing:

- Contents of the bag
- Names of investigators involved in seizing, photographing, sketching, and packaging the evidence
- Location of evidence seizure
- Suspect information and criminal record (if applicable)
- Date and time of seizure
- Passwords of seized devices (if known)
- Usage of Faraday bag for digital devices to prevent network signal interference.

Witness Signature

Sometimes a witness signature is required to verify the information collected from the crime scene

Storage Formats

1. Imaging

- When taking an image file, one of the important things to take into consideration is the file format which the image file will be stored in.
- Raw Format is the simplest format to save an image. As the name suggests, the data is read from the source device's disk and written on a file.
- That image file can be mounted later and analyzed for evidences.
- One popular tool to image a disc in raw format is the **DD tool**
  - DD allows the investigator to image a disk in raw format and split the file into multiple files for the ease of use.
  - dd if = [src] of=[dst]
  - It is possible to use the -b options to split the image into multiple parts

2. Proprietary

In digital forensics, proprietary storage formats are often utilized by commercial tools for imaging. These formats have specific characteristics and considerations:

1. **Characteristics:**
   - Proprietary formats contain original data encoded in a way unique to the tool.
   - They include a header with metadata such as hash values or CRC.
   - Compression is often used for space efficiency, although it may slow down imaging and analysis processes.
2. **Advantages:**
   - Space efficiency due to compression.
   - Integration of case-related metadata within a single file.
   - Convenience for investigators as proprietary tools typically offer imaging, analysis, and reporting modules within a single framework.
3. **Considerations:**
   - Slower processes due to compression and encoding.
   - Limited cross-platform compatibility, binding investigators to specific tools.
   - Some formats may have size limitations, requiring large disks to be split into smaller chunks for analysis.
4. **Famous Formats:**
   - Expert Witness Format (EWF) used by EnCase
   - IDIF,IRBF,IEIF used by ILook Investigator
   - sgzip used by PyFlag

   Old EWF's are limited in size to 2GB per image.

3. Advanced Forensics Format (AFF)

- It is an open image format developed by Basis Technology
- It also allows the investigator to either embed that metadata within the image or on a separate file.
- AFF based tools copy the data from the suspect's device in 16 MB blocks (usually called Pages).

4. Expert Witness (EnCase)

- This is a propriety file format created by Guidance Software (now OpenText) fortheir famous product “EnCase Forensic”
- Metadata can be associated with the same image file; however, the quantity and type of metadata are limited compared with the AFF file format.
- The EnCase file format has the extension “. E01” first chuck extension “.e01,” second chunk extension “.e02,” etc.

Data Acquistion va Copy

Aspect	Data Acquisition (Imaging)	Copying
Definition	Captures a complete replica of the source device, including both used and unused	Mirrors only the "useful" data from the source device, excluding unused or deleted data.

Aspect	Data Acquisition (Imaging)	Copying
	data.	
Scope of Data	Captures all data, including both active and inactive files, deleted files, and system areas.	Only mirrors active and intact data, excluding unused or deleted areas of the storage device.
Preservation	Preserves the entire contents of the source device, maintaining the integrity of the original data.	Preserves only the relevant and intact data, disregarding unused or deleted areas.
Chain of Custody	Helps establish the chain of custody by providing an exact replica of the original data for investigative purposes.	Assists in maintaining the chain of custody by preserving relevant data while excluding unnecessary or unused portions.
Investigative Process	Enables thorough analysis of all data on the source device, allowing investigators to examine both active and inactive information.	Facilitates analysis of relevant data without the need to process or examine unused or deleted areas, streamlining the investigative process.
Practical Consideration	Requires larger storage capacity and longer acquisition times due to capturing all data, including unused and deleted portions.	Requires less storage capacity and shorter processing times compared to data acquisition, as only active and relevant data are copied.
Purpose	Typically used for forensic investigations where a complete and unaltered copy of the source device is required for analysis.	Suitable for situations where only active and intact data need to be preserved or analyzed, such as data backup or data recovery scenarios.

Acquisition Issues

- First, when copying, make sure that the copy is an exact replica of the original image.
- Make sure that the original source is safe from tampering.
- Make sure that the copying process will not alter the original image or corrupt parts of it.

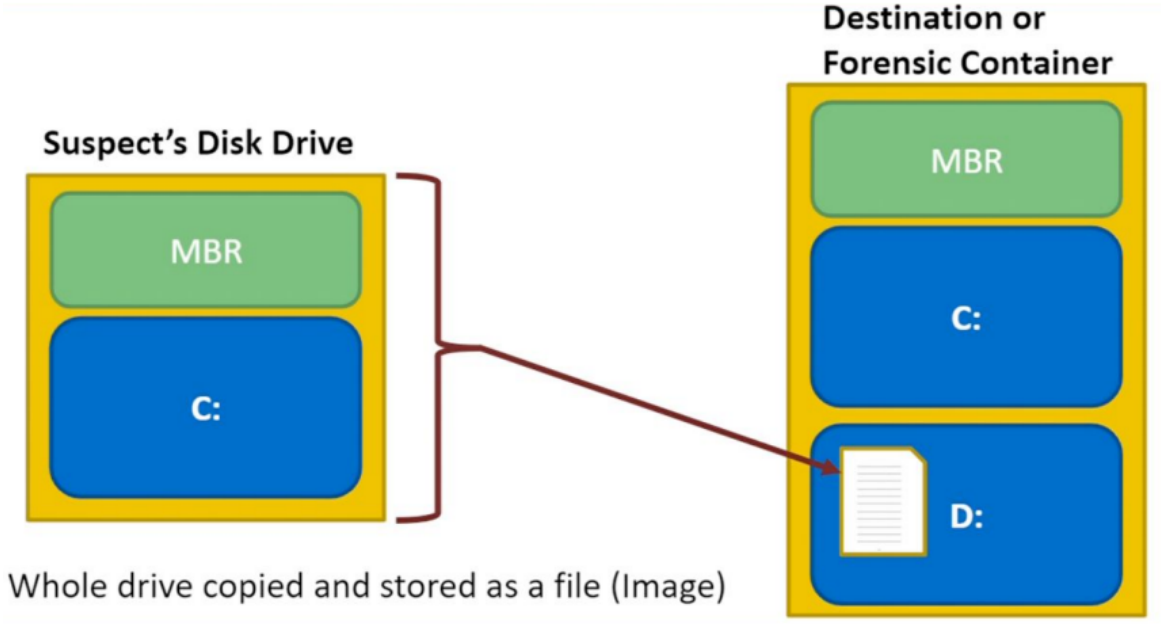
Acquisition Methods:

1. Two primary approaches: **disk drive to image file (imaging) and disk drive to disk drive (cloning).**
2. Multiple images can be created as needed, requiring sufficient storage space.

Disk Drive to Image File (Imaging):

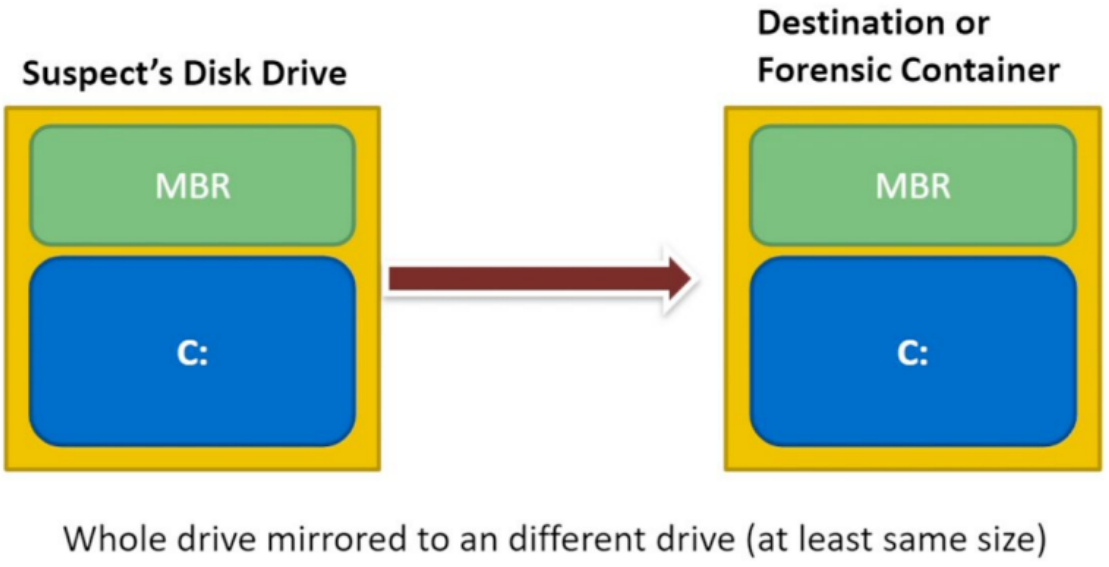
- Creating a forensic image does not have to be for a full disk drive, you might have a drive that has more than one partition, but as an investigator, you are only interested in a specific partition.
- In cases where the source disk consists of multiple partitions, imaging can be performed on individual partitions.
- If the investigator wants to image the D:\ partition only, then it is considered **Logical Disk Drive to Disk Drive acquisition.**
- Do not create only one and use it for your investigation, you never know if a faulty tool might interact with the image and either corrupt it or even jeopardize evidence stored on it.
- Forensic images can be stored in various locations, including:

- On the same disk (not recommended due to potential data integrity issues).
- On external disk drives.
- Sent through the network to a network share.



Disk Drive to Disk Drive (Cloning):

- Disk Drive to Disk Drive (clone) mirrors the suspect's hard disk content into another hard disk.
- The tools which supports that type of data acquisition usually rebuilds the second disk so it becomes exactly similar to the source disk, and
  that is why it is also called a "clone".



Sparse Acquisition:

- Sparse acquisition involves selectively copying specific folders, files, or bytes residing within unused parts of the HDD, rather than mirroring all disk content.

- Useful when taking the suspect's system offline is not feasible or when imaging the entire HDD would be time-consuming.
- Ideal for cases with large HDD volumes that may require significant time for complete imaging or cloning.
- Can include targeted folders, files, or unallocated space where deleted or hidden data may reside.

Acquisition Method	Description	Pros	Cons
Disk to Image	Involves creating a digital image of the entire disk, storing it as a single file on another storage device.	- Efficient storage usage, as one storage device can hold multiple images. - Enables easy replication and distribution of images for analysis.	- Possibility of bugs or errors preventing successful image creation, leading to data loss.
Disk to Disk	Mirrors the contents of one hard disk onto another physical hard disk.	- Reliability in cases where image creation may fail due to technical issues. - Avoids reliance on software or tools for imaging, reducing the risk of errors.	- Requires a new physical hard disk for each data acquisition, potentially increasing costs.
Sparse Acquisition	Selectively copies specific folders, files, or bytes from the disk, excluding unused areas.	- Faster acquisition process compared to imaging the entire disk. - Useful when time is limited or when only specific data is relevant to the investigation.	- Risk of overlooking important evidence if not meticulously planned or documented. - Requires expertise to select and prioritize data for acquisition.
Logical Disk to Disk	Imaging method that mirrors the entire partition or logical drive onto another disk.	- Captures all data within the partition, ensuring completeness of evidence. - Avoids the risk of overlooking relevant data present in non-targeted areas.	- Longer acquisition time compared to sparse acquisition, especially for large volumes. - May result in unnecessary duplication of data if only specific files or folders are of interest.

Live Data Acquisition:

- Live Data acquisition is used to collect data while the machine is running.
- Usually an investigator looks for volatile data during live acquisition. Volatile data resides in a memory that can't hold the data after a reboot.
- Volatile data usually resides in RAM and cache.
- SYS Info is a generic term that describes Basic system information about the machine, the running OS, its configuration and the installed applications.
- RAM dump and running processes is Knowing what processes were running at the time of the acquisition might be crucial for the investigation.
- Sometimes, most of the investigation's time is spent looking for and in Logs.
- Logs could be Operating System event logs, specific process logs, login logs and network logs
- Time Stamps also play a major role in crime reconstruction

- Networking configurations are also important, especially when there is a network attack. Details such like number of NICs and their modes, MAC
  and IP addresses, could also help the investigator during the investigation.
- Full Disk Encryption, for example, is one case where memory forensic is the way to go. There are many security solutions which allow a user to
  encrypt his/her hard disk's content making normal disk imaging useless.

Tools: Write Blockers

Write Blockers are essential tools in digital forensics that prevent inadvertent alteration or damage to the original disk content during data acquisition. Here's an overview:

1. **Purpose:**
   - Write Blockers are used to perform data acquisition procedures while ensuring the integrity of the original disk content.
   - They prevent any write commands from being executed on the target disk, thus safeguarding against accidental changes or tampering.
2. **Functionality:**
   - Write Blockers work by filtering out write commands, effectively blocking the disk from writing any new data.
   - This ensures that only read operations are allowed, enabling safe and non-destructive data acquisition.
3. **Types:**
   - Write Blockers can be either hardware-based or software-based.
   - Hardware write blockers are physical devices that are connected between the suspect disk and the acquisition system.
   - Software write blockers are applications or utilities that run on the acquisition system and intercept write commands before they reach the suspect disk.
4. **Features:**
   - Some advanced write blockers allow investigators to customize the blocking behavior by specifying a list of commands to be blocked.
   - This additional control gives investigators flexibility in tailoring the write blocking process to suit the specific requirements of the investigation.
5. **Benefits:**
   - Ensures the preservation of the original disk content, maintaining its integrity for forensic analysis.
   - Mitigates the risk of inadvertently altering or damaging the disk during data acquisition, thereby ensuring the admissibility of evidence in legal proceedings.

Common write blockers

1. WiebeTech® Forensic UltraDock from CRU Inc.
2. Tableau Forensic Imager TD3 from Guidance Software

☞ **Non-Writable USB**

- In many cases, the investigator will have an acquisition tool acquiring data and dumping it onto an external storage, typically a disk with a USB connection.
- The problem is that this disk contains the evidence might be altered by Windows when connected to it; this would damage the evidence integrity.

☞ **Bootable Disks**

- Bootable Disks usually holds a self-contained fully functioning, bootable OS
- This allows the investigator to launch an OS on the suspect's machine without touching and modifying the device's main disk.

Non-Writable USB

- To maintain evidence integrity, it's essential to prevent any unauthorized writing on USB devices during forensic analysis.
- Microsoft introduced a USB-write blocking feature starting with Windows XP.
- This feature can be activated directly from the Windows registry, providing a built-in solution for preventing write access to USB devices.
- Type Regedit
  - HKLM/SYSTEM/CurrentControlSet/Control.
  - "StorageDevicePolicies."
  - WriteProtect

1. Live Forensic Tool : Ftk Imager

- FTK Imager enables investigators to acquire storage devices such as hard disks, USB drives, and memory cards.
- It supports acquiring images of both entire physical disks and specific partitions.

1. **Image Creation Process:**
   - To create an image of a storage device, users can select "Create Disk Image" from the File menu.
   - The tool allows users to specify the type of media to be imaged, such as a whole physical disk.
   - Users can select the specific physical disk from which they want to create the image.
2. **Image Format and Metadata:**
   - Users can choose the format in which the image file will be saved, ensuring compatibility with forensic analysis tools.
   - FTK Imager provides options for inserting metadata into the image file, including details about the acquisition process.
3. **Image Verification:**

- After the imaging process is complete, FTK Imager provides verification results to ensure the integrity of the acquired image.
- It is essential to save and document these verification results as part of the chain of custody.

4. **Analysis and Mounting:**
   - Users can analyze the acquired image by adding it as evidence in FTK Imager's analysis window.
   - Additionally, FTK Imager allows users to mount previously acquired forensic images for examination.
   - The mounted image appears as a virtual device in the system, facilitating easy access to its contents for analysis.
5. **Unmounting Images:**
   - Once analysis or examination is complete, users can unmount the image from within FTK Imager.

2. Live Forensic Tool: BriMor Labs Tools

BriMor Labs offers a powerful Live Response Collection framework, particularly from their Bambiraptor toolset, designed to facilitate efficient data collection from machines in digital forensic investigations. Here's an overview of their Live Response Tools:

1. **Versatile Data Collection:**
   - The Live Response Collection framework provides various acquisition types tailored to gather specific types of data relevant to the investigation.
2. **Ease of Use:**
   - Utilizing the Live Response Tools is straightforward, requiring users to simply select the desired acquisition type.
3. **Secure Data Handling:**
   - An added feature is the "secure" option, allowing investigators to safeguard acquired data with a password, ensuring its integrity and confidentiality.
4. **Folder Structure:**
   - Upon download, users will find a folder named after the machine in the tools directory.
   - This folder contains images captured, collected data, verification data, and a log file, organizing acquired information for easy access and management.
5. **Acquisition Actions:**
   - Users can view a sample of the actions performed by the Live Response Tools, providing transparency into the data collection process.
6. **File Integrity Verification:**
   - Each file obtained during the data collection process is accompanied by its hash value, enabling integrity verification and ensuring data authenticity.
7. **Forensics Images:**
   - Within the Forensics images folder, users will find hard disk and RAM images, essential components for comprehensive forensic analysis.

Memory Forensic Tool : Volatility Framework

- The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License for the extraction of digital artifacts from volatile memory (RAM) samples.

1. **Scope and Purpose:**
   - The framework is designed to facilitate the extraction of digital artifacts from volatile memory samples.
   - It operates independently of the system being investigated, allowing for the extraction of artifacts from various operating systems.
2. **Unprecedented Visibility:**
   - Volatility provides unparalleled visibility into the runtime state of a system, enabling forensic analysts to extract valuable digital artifacts for analysis.
3. **Compatibility and Support:**
   - Volatility supports memory dumps from a wide range of Windows versions, including both 32-bit and 64-bit architectures, spanning from XP SP2 to Windows 10 and Server 2003 to Server 2016.
   - Additionally, it extends support to Mac operating systems from version 10.5 (Leopard) to 10.12 (Sierra).
   - Memory dumps can be in various formats, including raw format, Microsoft crash dump, hibernation file, and virtual machine snapshot.
4. **Availability and Integration:**
   - Volatility is readily available, with pre-installed versions included in distributions such as Kali Linux.
   - It can also be installed and executed on Windows machines using executable files.

```
volatility --profile=Win7SP0x64 pslist -f img_mem.dmp
```

Bulk Extractor

Bulk Extractor is a powerful computer forensics tool designed to scan disk images, files, or directories of files to extract valuable information without parsing the file system or its structures. It provides a versatile and efficient means of extracting data, which can then be inspected, parsed, or processed using automated tools. Here's an overview of Bulk Extractor:

1. **Functionality and Purpose:**
   - Bulk Extractor is primarily used for extracting useful information from various sources, including disk images, files, and directories.
   - It bypasses the need to parse the file system or file system structures, enabling efficient extraction of data.
2. **Feature Analysis:**
   - The tool creates a histogram of features it finds during the extraction process. Features that appear more frequently are typically considered more important.

- This feature analysis aids in identifying and prioritizing significant data within the extracted information.

3. **Applications:**
   - Bulk Extractor finds applications in a wide range of fields, including law enforcement, defense, intelligence, and cyber-investigation.
   - Its versatility and effectiveness make it valuable for extracting insights and evidence from digital sources in various investigative contexts.
4. **Data Extraction:**
   - Bulk Extractor extracts a diverse range of data types, each stored in separate files within the output directory.
   - The extracted data can include information such as email addresses, credit card numbers, URLs, and more, depending on the content being analyzed.
5. **Usage and Output:**
   - To utilize Bulk Extractor, users provide it with an image or dump file, along with an output directory where the extracted data will be stored.
   - Upon completion, Bulk Extractor generates a summary report along with the hash value of the image, providing essential information for further analysis and validation.

Tool	Differences	Advantages	Disadvantages	When to Use
FTK Imager	- Acquires disk images and mounts them.	- User-friendly interface.	- Limited functionality compared to some tools.	- Creating disk images for analysis.
	- Supports various storage device types.	- Ability to create forensic images.	- May require additional tools for analysis.	- Mounting and analyzing disk images.
	- Provides metadata insertion for images.	- Verification of image integrity.		
Volatility Framework	- Focuses on extracting digital artifacts from volatile memory.	- Supports various Windows and Mac versions.	- Requires some technical expertise to use effectively.	- Analyzing memory dumps for forensic artifacts.
	- Offers visibility into runtime state of systems.	- Independent of system being investigated.	- May not support all memory dump formats.	- Extracting artifacts from volatile memory.
	- Open-source with active community support.	- Flexible and customizable.	- Learning curve for beginners.	- Analyzing memory dumps across different OS versions.
Bulk Extractor	- Extracts information from disk images, files, or directories.	- Efficient extraction of diverse data types.	- Requires understanding of data types and features.	- Extracting and analyzing data from digital sources.
	- Generates histograms of extracted features.	- Useful for law enforcement, defense, and cyber-investigation.	- May produce large amounts of data.	- Investigating digital evidence across various contexts.

Tool	Differences	Advantages	Disadvantages	When to Use
	- Provides detailed summary reports.	- Versatile applications in various fields.	- Requires appropriate storage for extracted data.	
BriMor Labs Tools	- Focuses on live response collection.	- Easy-to-use framework.	- Limited to live response data collection.	- Collecting live system data during investigations.
	- Provides secure data protection options.	- Organizes collected data efficiently.		- Conducting live system analysis in forensic investigations.
	- Offers detailed action logs for analysis.	- Suitable for a range of investigative applications.		

Capturing RAM Using the DumpIt Tool:

1. **Tool Description**: DumpIt is a portable tool designed for acquiring RAM memory from computers running Windows OS (32 or 64 bit).
2. **File Size**:
   - The captured image size is typically larger than the acquired RAM size. For example, capturing a PC with 8 GB of RAM may result in an image size of approximately 8.269 GB.
3. **Output Files**:
   - DumpIt produces two files after acquisition:
     - A file with the DMP extension, containing the RAM image.
     - A file with the JSON extension, containing technical information about the captured machine, including architecture type, machine name, maximum physical memory, username, OS version, and service information.

Belkasoft Live RAM Capturer:

1. **Tool Description**: Belkasoft Live RAM Capturer is a small, free tool designed to capture the entire contents of RAM memory, even if protected by active antidebugging or antidumping systems.
2. **Features**:
   - Ability to capture RAM contents regardless of anti-debugging or anti-dumping measures.
3. **Storage Requirement**:
   - The USB drive used for executing the tool should have more storage capacity than the RAM memory of the target computer.
4. **Advantages**:
   - Ability to bypass active antidebugging or antidumping systems.
   - Portable tool that can run from a USB thumb drive.
5. **Disadvantages**:
   - Limited information provided about specific technical features or capabilities.
   - Registration required to access the download section may be seen as an inconvenience by some users.

Capture RAM with Magnet:

1. **Tool Description**: Magnet is a portable tool designed for RAM capture, boasting a small footprint on the target machine and compatibility with various Windows OS versions.
2. **Features**:
    - Supports nearly all Windows OS versions, including Windows XP, Vista, 7, 8, 10, 2003, 2008, and 2012 (32 and 64 bit).
    - Portable and lightweight tool for capturing RAM.

Capture RAM with FTK Imager:

1. **Tool Description**: FTK Imager is a versatile data preview and imaging tool used in digital forensics. It allows for the creation of forensic images of target computer data without altering the original evidence.
2. **Features**:
    - Capable of creating forensic images of various data sources, including local hard drives, floppy diskettes, zip disks, CDs, DVDs, entire folders, or individual files.
    - Can be installed locally on a system or run from a USB thumb drive, making it suitable for use in the field during live forensics on running systems.
    - Offers additional functionalities beyond image acquisition, such as mounting an image for read-only access, previewing image contents, exporting files/folders from images, and acquiring Windows registry.

Validating Evidences

1. **Overview**:
    - Validating evidence is crucial in digital forensics to ensure the integrity and authenticity of collected data.
    - Hash functions play a vital role in validation, as they generate unique fingerprints for input data, enabling detection of any alterations.
2. **Hash Functions**:
    - Hash functions are one-way cryptographic functions that produce fixed-size output strings from variable-length input.
    - The resulting hash serves as a unique fingerprint for the input data, as even small changes to the source file result in completely different hash values.
    - Hashes are used to validate evidence by confirming that the file has not been tampered with, as any modifications would lead to changes in the hash value upon recomputation.
3. **Security Considerations**:
    - It's crucial to securely store the hash value to prevent tampering. If an attacker gains access to both the hash value and the disk, they could manipulate the disk, recalculate the hash, and create false evidence, compromising the investigation's integrity.
4. **Common Hash Functions**:
    - There are several hash functions used in the industry:

- SHA-1 and MD-5: Considered less secure due to collision vulnerabilities.
- SHA-2 and SHA-3: More robust and widely recommended for secure hashing purposes.

Exploring Evidence:

- After obtaining evidence forensically, the next step is to explore the evidence to understand its content before analysis.
- Different types of evidence may require different methods to connect them to the workstation.
- It's essential to establish a connection between the evidence and the analysis workstation to facilitate investigation.
- Evidence may use different filesystems, necessitating a way to connect these filesystems to the workstation's filesystem.
- Mounting the evidence is the primary approach, akin to attaching a USB thumb drive to a PC/Laptop.
- When mounting the forensic image or device, it's crucial to do so in Read-Only mode.
- Read-Only mode ensures that the evidence remains intact and prevents accidental corruption.
- Upon mounting the forensic image or device, users can explore its contents similar to browsing their computer files.
- However, Read-Only protection ensures that the evidence remains unaltered during exploration.

Some of the most commonly used are:

1. FTK Imager (yes the imager itself)
2. Mount Image Pro
3. OSFmount
4. Arsenal Image Mounter
5. P2 eXplorer Pro

TimeStamps

- **Definition**: Timestamps are sequences of characters or encoded data indicating when specific events occurred, typically including the date and time.
- **Importance in Evidence Acquisition**: Timestamps are crucial for maintaining the integrity of investigations by recording the date, time, and time zone of evidence acquisition.
- **Criticality in Digital Investigations**: Accurate timestamps help establish the presence or absence of suspects at specific locations and events, reducing the risk of wrongful accusations.
- **Role in Evidence Analysis**: Timestamps are essential for analyzing metadata from acquired evidence, providing information on file creation, modification, and access times.
- **Challenges in Timestamp Interpretation**: Interpretation of timestamps by analysis tools may sometimes be unreliable, leading to incorrect date and time information.
- **Impact of Incorrect Timestamps**: Incorrect timestamps can undermine the credibility of investigations, potentially resulting in wrongful prosecutions or accusations.

Decoder(Tool)

Decode is a tool which can convert the timestamps from various time formats to more human readable.

Virtual Memory (Swap Space)

- Pagefile.sys (also called virtual memory) is a file created by Windows to compensate for the limited capacity of RAM memory.
- Windows sets the initial virtual memory paging file equal to the amount of RAM installed; however, a user or system administrator can usually change its size.
- Parts of RAM files are moved from it into the virtual memory to free up more space.

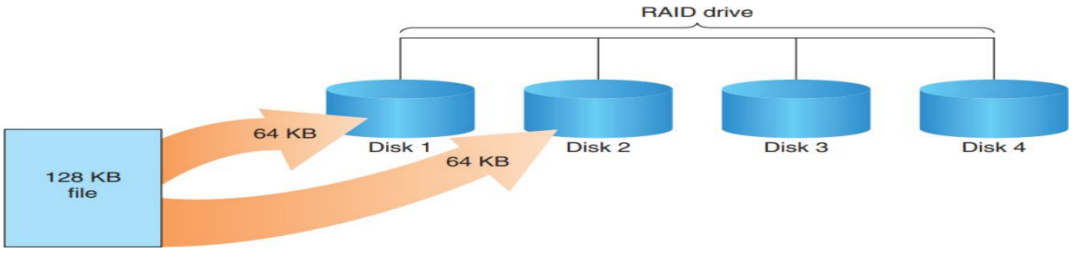
The Challenges of Acquiring RAM Memory

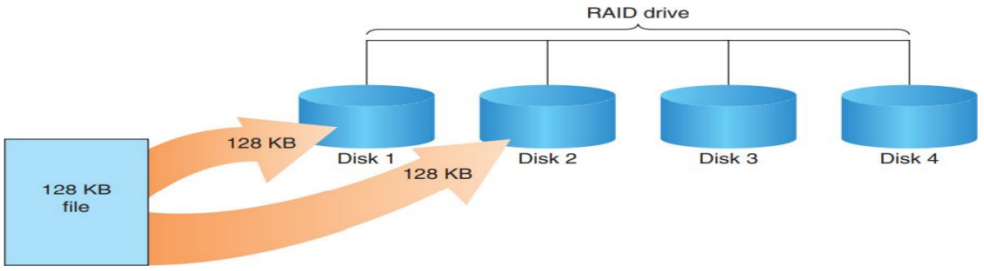
- **Windows Is Locked**:
  - Advisable to perform a hard shutdown to prevent loss of RAM contents.
  - Bypassing Windows login page without reboot using specialized tools or techniques.
  - Utilizing hardware accessories like CaptureGUARD and Phantom Probe to access live memory and encrypted disks without a password.
  - Performing direct memory access (DMA) attacks to extract passwords from RAM for system login.
  - Risk assessment needed to determine if forensic live acquisition is warranted due to potential traces left in RAM memory and varying success rates.
- **Administrative Privileges**:
  - Most RAM capture tools require administrative privileges to function properly.
  - In cases of limited user permissions, hardware acquisition tools or DMA attacks can be used to acquire RAM memory.
- **Capturing Tool Footprint**:
  - Capturing tools leave traces on the suspect machine, impacting evidence integrity.
  - Computer forensic software vendors claim minimal footprint, potentially overwriting data during live memory acquisition.
  - Hardware acquisition tools require a small driver installation on the target machine.
  - Documentation of changes made during acquisition crucial for admissibility of evidence in court.
- **Modifications from Live Acquisition**:
  - Live acquisition typically results in registry changes, memory entry overwrites, and minimal data writing to disk drives.
  - Courts may accept small footprints left by RAM capturing tools, but thorough documentation of interactions with suspect computers is essential.

RAID

- RAID stands for Redundant Array of Independent Disks, formerly known as "inexpensive" disks.
- It's a computer configuration or virtualization technology that enables multiple physical hard drives (two or more) to function in parallel, appearing as a single logical unit.
- **Usage in Computer Forensics**:

- Major computer forensic suites like AccessData FTK, ProDiscover, EnCase, and X-Ways Forensics are capable of acquiring RAID systems.
- **Importance**:
- RAID systems are common in enterprise environments and may contain crucial evidence in forensic investigations.
- Acquiring data from RAID setups requires specialized tools and expertise due to the complexity of the configuration.
- **Challenges**:
- Acquiring data from RAID systems may pose challenges due to the intricacies of RAID configurations and the need for compatibility with forensic tools.
- Understanding RAID levels and configurations is essential for effective acquisition and analysis in forensic investigations.





Challenges in Network Attached Storage (NAS):

- NAS units are increasingly popular in home environments for storing backups and multimedia content.
- NAS devices typically run their own dedicated operating systems, often Linux variants.
- Acquiring data from NAS devices requires bit-by-bit acquisition, including unallocated space, which necessitates Linux skills.
- The sheer volume of data stored on NAS devices can significantly increase the time required for acquisition and analysis.

Challenges in Encrypted Hard Drives:

- Live acquisition of volatile memory is preferable to recover encryption keys, but if not possible, encrypted hard drives must be acquired.
- Acquiring encrypted hard drives may require subsequent decryption, which may not always be successful without the correct password.

Challenges with Corrupted or Physically Damaged Hard Drives:

- Physical damage to hard drives may necessitate professional data recovery services to extract data forensically.
- Even in the case of damage, hard drives should not be abandoned as data recovery may still be possible with professional assistance.

Challenges in Cloud Data Acquisition:

- Cloud computing introduces legal, technical, and logistical challenges due to its dynamic nature and dependence on virtualization technology.
- Network acquisition involves handling large volumes of data, including RAID configurations and various device types.
- Forensic examiners need technical skills to navigate diverse network environments and acquire evidence.

Image Mount

- Image mounting allows investigators to browse the contents of forensic images as if they were accessing regular directories and files.
- Mounted images appear as virtual drives in the Windows operating system, enabling easy access to the image contents.
- Common forensic image formats include RAW, E01, AFF, etc., which can be mounted for analysis.

1. Arsenal Image Mounter:

- **Overview**:
  - Arsenal Image Mounter is a free, open-source program designed for mounting forensic images as complete disks in Windows.
- **Features**:
  - Enables investigators to browse image contents as if they were browsing any directory of files.
  - Supports both free and paid versions, with the paid version offering additional features.
  - Supports forensic images in RAW and EnCase file formats.
  - Compatible with all file systems used by Windows OS, such as NTFS and FAT32.

2. OSFMount:

- **Overview**:
  - OSFMount is another program used for mounting forensic drive images as local Windows drives.
- **Features**:
  - Supports mounting images of CDs in .ISO format and creation of RAM disks mounted into RAM.
  - Compatible with various image file formats, including AFF, Raw, split Raw, and EnCase.

3. Autopsy:

- **Overview**:

    - Autopsy is a graphical user interface (GUI) program designed to provide easy access to command-line tools and libraries included in the Sleuth Kit and other digital forensics tools.
- **Features**:
    - Automation of various forensics analysis tasks, such as recovering deleted files, analyzing Windows registry, investigating email messages, and examining unallocated disk space.
    - Additional features aimed at enhancing examiner productivity during analysis work.
    - Support for extending functionality with customized modules, known as "ingest modules," which can be developed using Python (Jython) or Java programming language.
- **Usage**:
    - Widely used by forensic professionals worldwide, with active support from both volunteer community and commercial support for paid users.
    - Provides a robust forensic platform for efficiently investigating cases and conducting digital forensic analysis tasks.

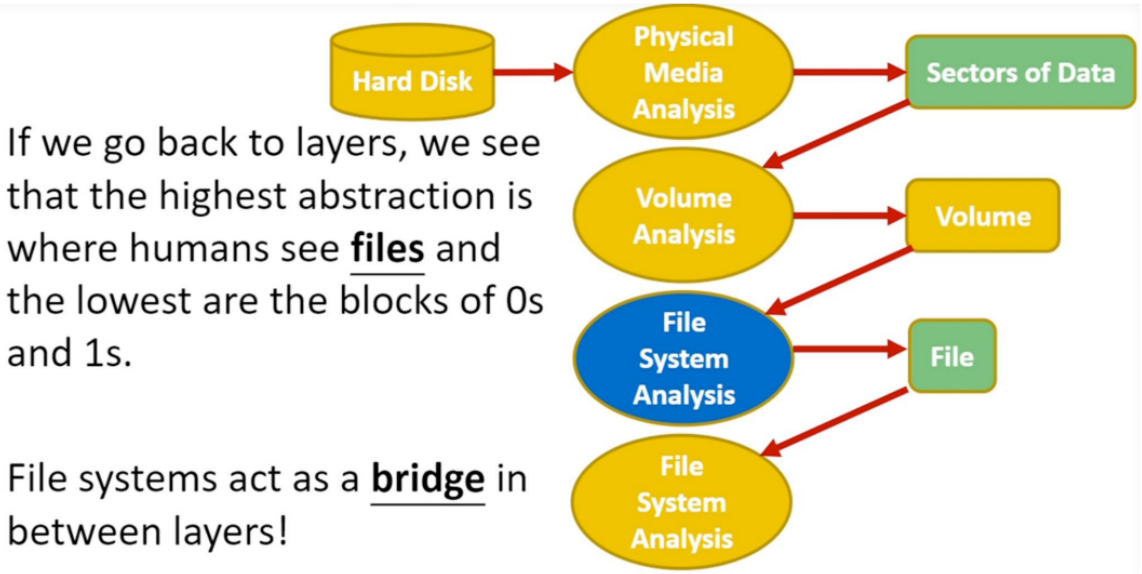
Analyzing RAM Forensic Image:

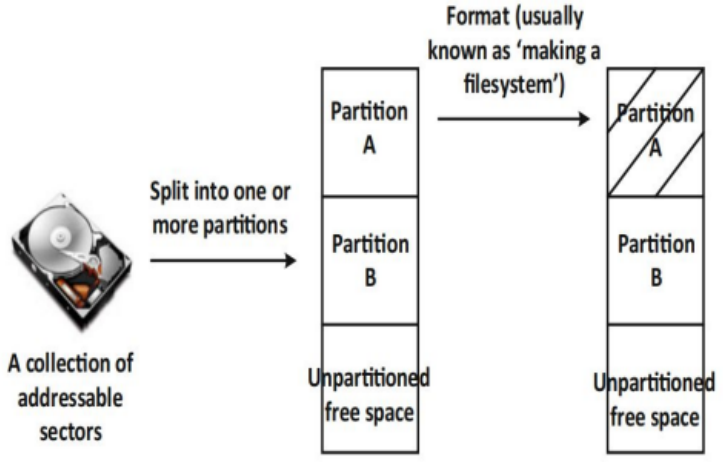
- **Major Computer Forensic Suites:**
    - EnCase
    - Belkasoft Evidence Center
    - X-Ways Forensics
- **Reputable and Popular Free Tools for RAM Forensic Analysis:**
    - Redline from FireEye
    - Volatility from the Volatility Foundation

Forensic Tools by FireEye:

- **Memoryze:**
    - Physical memory imaging and analysis command-line tool.
    - Can capture RAM images and perform advanced analysis of live memory while the computer is running.
    - Capable of analyzing memory image files acquired by Memoryze or any other forensic software (DD-format), although results may be more comprehensive when using Memoryze for acquisition.
- **Redline:**
    - Windows program for conducting memory investigation of malicious artifacts in Windows physical memory.
    - Capable of capturing memory images, running processes, opened files, and registry data.
    - Provides filtering options to narrow down results based on predefined criteria, such as timeframe of compromise events or precompiled MD5 hash values of known files.

Part2: Windows File Systems





Disk Partitioning and Formatting

- **Partitioning:**
  - Partitioning involves dividing a physical disk into one or more separate areas known as partitions or logical drives.
  - Each partition functions as if it were a separate disk, with its own file system and directory structure.
  - Partitions are created to organize data, improve system performance, and facilitate data management.
- **Formatting:**
  - Before a partition can be used for data storage, it must be formatted.
  - Formatting initializes the file system on the partition and creates the necessary data structures to track files and directories.
  - During formatting, the disk or partition is divided into clusters, which are the smallest logical units used by file systems for file allocation.
  - Sectors, on the other hand, are the smallest physical units used with disk drives.

    - The number of sectors per cluster is determined during formatting and is typically based on the size of the disk or partition.
    - This information, including the number of sectors per cluster, is stored in the Boot Record of the file system.
- **Purpose:**
    - Partitioning and formatting prepare the disk for data storage and organization.
    - They create the necessary structures for file allocation, directory management, and data tracking on the disk.

Types of Formatting:

1. **High Level (Logical) Formatting:**
    - This process involves initializing the disk and setting up the file system structures.
    - High-level formatting prepares the disk for storing files and directories.
2. **Low-Level Formatting:**
    - Low-level formatting is typically performed at the manufacturer level.
    - It involves dividing the disk into sectors and preparing it for data storage.
    - Low-level formatting is not usually necessary for end-users as modern disks come pre-formatted from the factory.

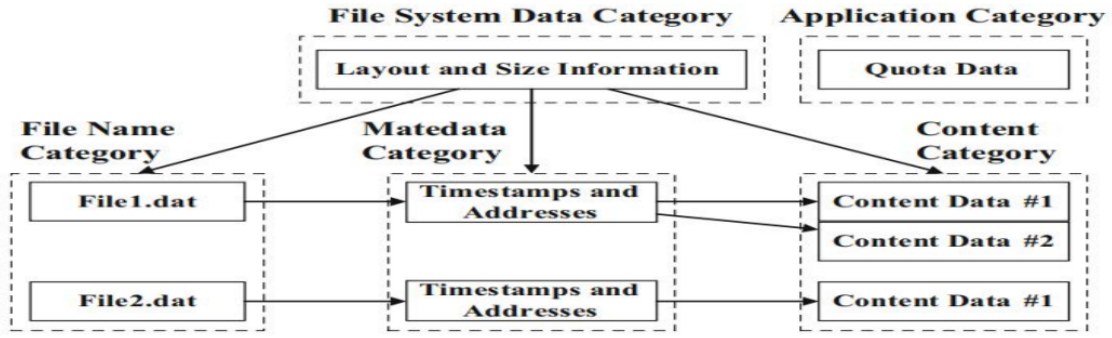
- **Cluster Allocation:**
    - When a file is created, the file system allocates a certain number of clusters to it.
    - The size of these clusters is determined during formatting and is crucial for disk performance and utilization.
    - The number of sectors per cluster affects both the performance and efficiency of the disk.
    - Choosing a large cluster size may result in wasted disk space, while selecting a small cluster size may lead to increased overhead.
- **Impact of Cluster Size:**
    - **Performance:** Larger cluster sizes can improve performance as there are fewer clusters to manage, reducing overhead.
    - **Disk Utilization:** Smaller cluster sizes can improve disk utilization as they reduce wasted space, especially for small files.
    - **Trade-offs:** Selecting an appropriate cluster size involves considering trade-offs between performance and disk utilization based on the types of files typically stored on the disk.

A File is a collection of data that has some relation, and most files have predefined organization.

File System

- File systems provide a mechanism (logical construction map) for the operating system to keep track of files in a partition.
- The file system tracks the drive's free space as well as the location of each file.
- Windows OS uses either the FAT or the NTFS file system to install itself on hard drives

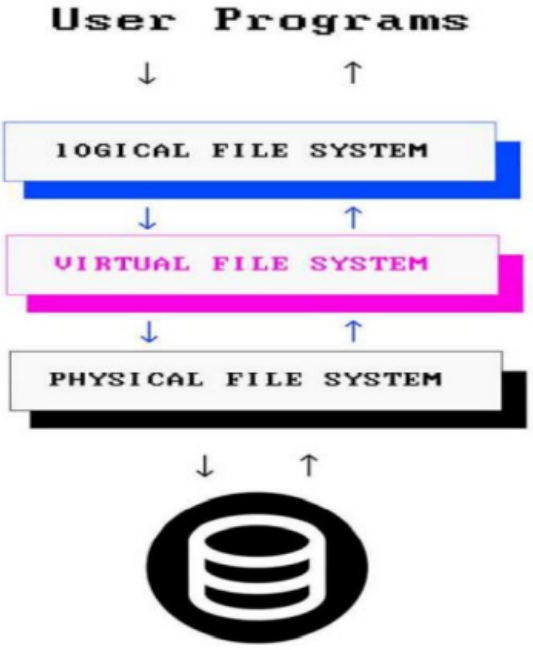
- responsibilities of a file system:
  - Space management
  - metadata, data encryption
  - file access control
  - data integrity



Data categories in file systems

- Extended file system (EXT), such as EXT2, EXT3, EXT4
- New Technology File System (NTFS)
- File Allocation Table (FAT), such as FAT12/16, FAT32
- Compact Disc File System (CDFS)
- High Performance File System (HPFS)

Architecture of File Systems



- **Three Layers:**
  1. **Physical File System:**

    - Responsible for data storage, retrieval, and space management on storage devices.
    - Interacts with storage hardware through device drivers.
  2. **Virtual File System (VFS):**
    - Provides a unified view of different file systems mounted on the same operating system.
    - Allows the operating system to use multiple file systems concurrently.
  3. **Logical File System:**
    - User-facing part of the file system.
    - Provides APIs for file operations (e.g., OPEN, READ, WRITE) to user programs.
- **Interaction Between Layers:**
  - **Physical Layer to VFS:** Provides a consistent interface to the VFS, allowing it to interact with different physical file systems.
  - **VFS to Logical Layer:** Acts as an intermediary, translating file system-specific commands into a unified API for user programs.
  - **Logical Layer to User Programs:** Enables user programs to perform file operations without needing to understand the underlying storage hardware.
- **Example:**
  - *Removable Storage on Windows:*
    - A flash drive formatted with exFAT or FAT32 can be used with a Windows system utilizing NTFS.
    - The VFS ensures compatibility and provides a unified interface for file operations regardless of the underlying file system.

File Allocation Mechanisms

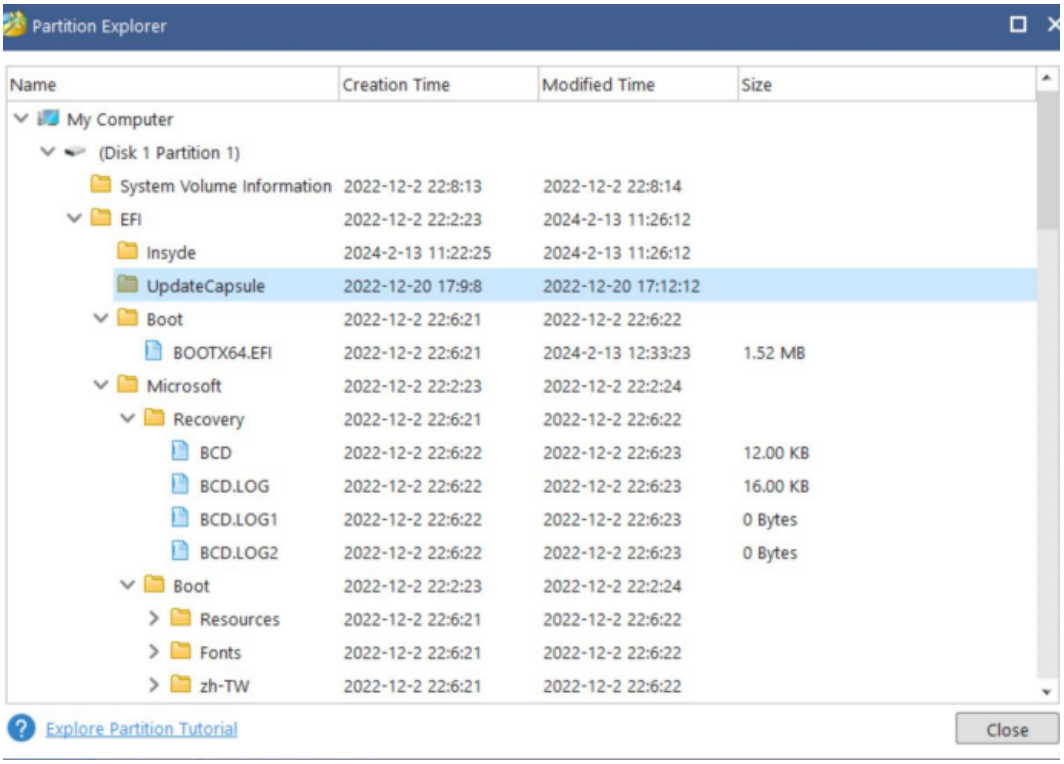
- **Cluster Definition:**
  - A cluster represents a logical grouping of sectors on a disk.
  - It's the minimum unit of disk space allocated for files or directories.
- **Need for File Allocation Mechanisms:**
  - Files often occupy multiple clusters.
  - Mechanism needed to track allocated clusters and their arrangement for each file.
- **Main Types:**
  1. **Contiguous Allocation:**
    - Files stored as contiguous blocks on disk.
    - Simple and efficient for sequential access.
    - Fragmentation can occur over time, leading to inefficient disk usage.
  2. **Linked Allocation:**
    - Each file is a linked list of disk blocks.
    - Allocation table stores pointers to the next block.
    - No fragmentation, but slower access due to non-contiguous storage.

3. **Indexed Allocation:**
    - Each file has an index block containing pointers to all its disk blocks.
    - Provides faster access than linked allocation.
    - Additional overhead for index block storage.

- **Operation:**
    - Allocation is done block by block until sufficient disk space is allocated for the entire file.
- **Considerations:**
    - Efficiency: Contiguous for sequential access, linked for dynamic size, indexed for faster access.
    - Fragmentation: Contiguous susceptible, linked and indexed less so.
    - Overhead: Linked and indexed have additional overhead compared to contiguous.

Sectors have a fixed size.

Inside Boot Partition



A surface test is a scan of a hard drive (HDD or SSD) for bad sectors. Disk surface test does what it implies - it scans the hard disk surface, checks bad sectors, and marks bad sectors so that the computer knows they will be not used in the future

FAT File System Analysis

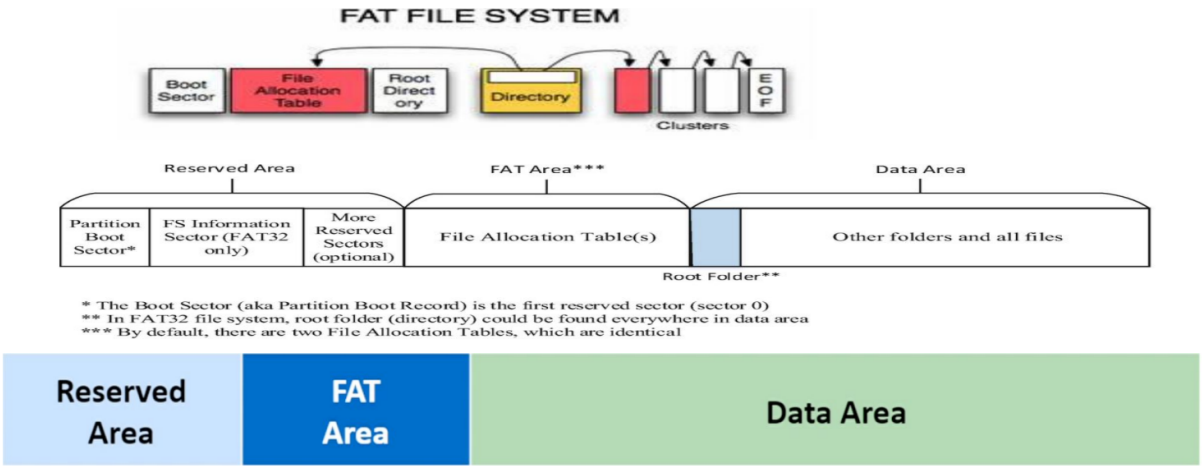
- **Introduction:**
    - Developed in 1977 for floppy disks, FAT (File Allocation Table) is a simple yet robust file system.
    - Used by MS-DOS and early Windows versions.
    - Still employed in modern devices like USB drives, memory cards, and EFI booting partitions.

- **Structure:**
  - Tracks files using a simple index table known as the File Allocation Table.
  - Implements linked allocation, where each allocated cluster contains a pointer to the next cluster.
- **Types of FAT:**
  1. FAT12
  2. FAT16
  3. FAT32
  4. exFAT (Extended File Allocation Table)
- **Cluster Representation:**
  - Each type of FAT file system can represent a different number of clusters.
  - For example, FAT32 utilizes 28 bits for cluster representation due to reserved bits.
- **Ease of Study:**
  - Remains relevant for study and understanding of file systems due to its simplicity.
  - Serves as a basis for comparison with more complex file systems like NTFS.
- **Cluster Sizes in FAT32:**
  - Default cluster sizes for FAT32 vary depending on the operating system used.
  - Example: Microsoft Windows 7, Windows Server 2008 R2, etc.

Volume Size	Cluster Size
64 MB – 128 MB	1 KB
128 MB – 256 MB	2 KB
256 MB – 8GB	4 KB
8GB – 16GB	8 KB
16GB – 32GB	16 KB
32GB – 2TB	32 KB

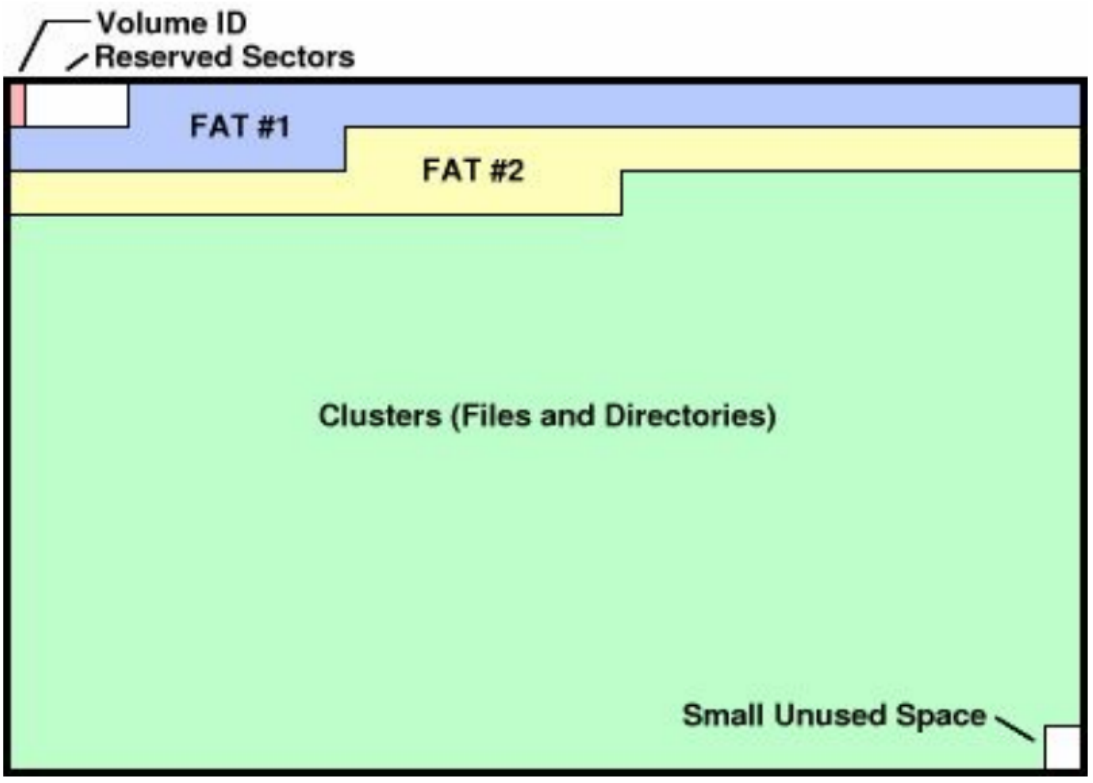
FAT Type	Max. No. of Clusters
FAT12	$(2^{12} - \#RC) \approx 4084$
FAT16	$(2^{16} - \#RC) \approx 65524$
FAT32	$(2^{28} - \#RC) \approx 268435444$
** assuming #RC equals 12 cluster	

FAT Structure

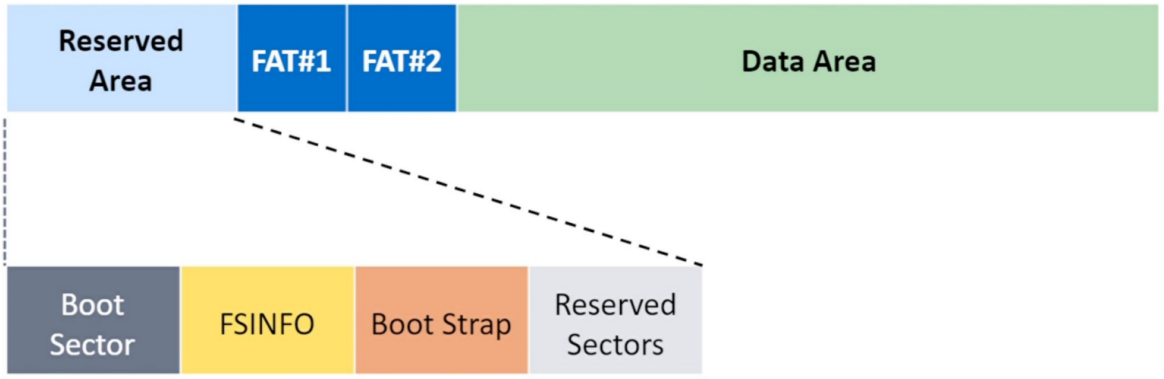


Disk Structure in FAT File System

- **Reserved Region:**
  - Includes the boot sector, extended boot sector, file system information sector, and other reserved sectors.
  - Critical for initializing and managing the file system.
- **FAT Region:**
  - Contains the File Allocation Table (FAT), which maps cluster locations to cluster locations.
  - Essential for tracking the allocation of clusters across the disk.
- **Data Region:**
  - Contains the actual file and directory data.
  - Utilizes addresses from the FAT region to locate and access file content.



FAT Area in a FAT32 file system has two parts and not one as in FAT12 and FAT16.

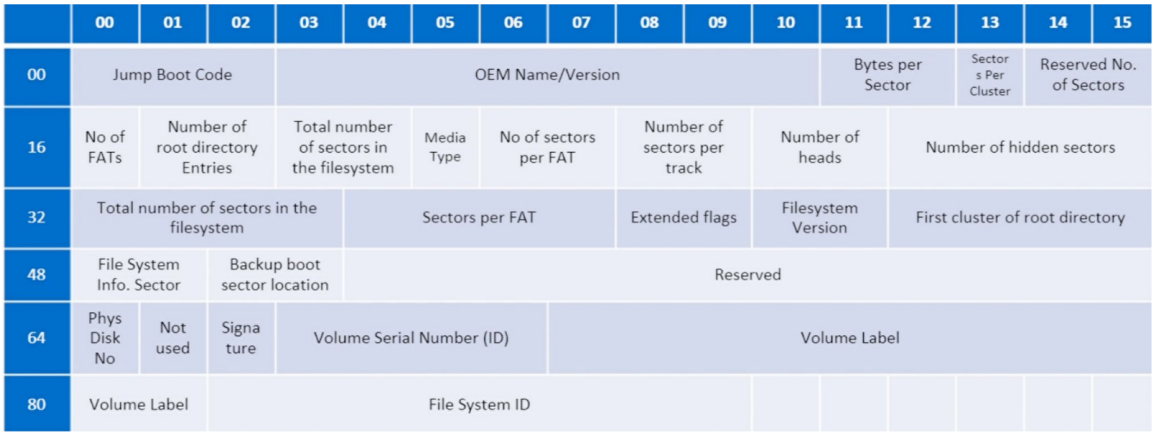


Reserved Area Structure in FAT File System

- **Volume Boot Sector:**
  - Sectors 0 and 6 for FAT12/16, containing critical boot information.
  - Sectors 0 and 7 for FAT32, also containing boot information.
- **File System Information (FSINFO) Structure:**
  - Sectors 1 and 7 for FAT12/16, storing file system metadata.
  - Sectors 1 and 8 for FAT32, containing file system metadata.
- **Bootstrap Code:**
  - Sectors 2 and 8 for FAT12/16, holding code for bootstrapping.

- Sectors 2 and 9 for FAT32, similarly containing bootstrapping code.

- **End of Sector Signature:**
  - All sectors, including bootstrap, end with the signature 0x55AA.
- **Reserved Sectors:**
  - Following the bootstrap sector, reserved sectors are usually empty or zeroed out.
  - There are typically 7 reserved sectors in FAT12/16 and 6 reserved sectors in FAT32.



FAT Area

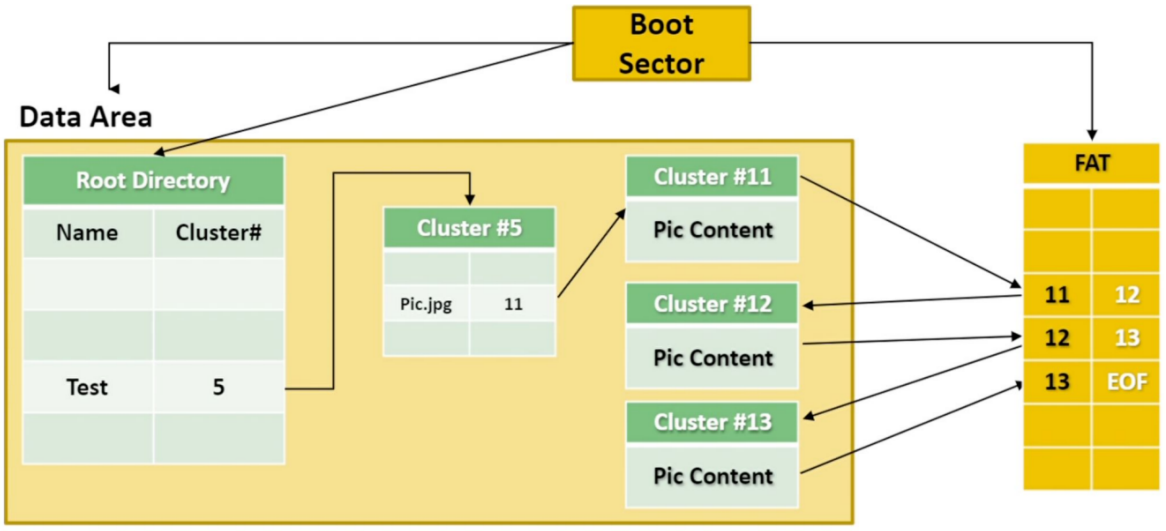
- **Mapping File Clusters:**
  - File systems are organized into clusters, and the FAT serves as a map to these clusters.
  - The size of each entry in the FAT depends on the type of FAT file system used:
    - FAT12: 12 bits per entry
    - FAT16: 16 bits per entry
    - FAT32: 28 bits per entry (top 4 bits reserved)
- **FAT32 Entry Structure:**
  - Each entry in the FAT32 corresponds to the next cluster in the chain of clusters for a file.
  - It operates like a linked-list: the first entry points to the next, and so on, until the end of the chain.
  - The last entry in the chain holds an end-of-cluster or end-of-chain value.
- **Reserved Clusters:**
  - Cluster #0: Contains the media descriptor and other bytes set to ones (1s).
  - Cluster #1: Used for dirty volume management, indicating the volume's status (dirty or clean).
    - A dirty state indicates improper volume unmounting, prompting the system to run disk recovery utilities upon next boot.
- **Dual FAT Structure:**
  - FAT32 utilizes two FATs (FAT#1 and FAT#2) instead of one for redundancy and integrity checking.

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
00	Media Type				Volume Status				Cluster #2				Cluster #3			
16	Cluster #4				Cluster #5				Cluster #6				Cluster #7			
32	Cluster #8				Cluster #9				Cluster #10				Cluster #11			
48	Cluster #12				Cluster #13				Cluster #14				Cluster #15			
64	Cluster #16				Cluster #17				Cluster #18				Cluster #19			
80	Cluster #20				Cluster #21				Cluster #22				Cluster #23			
96	Cluster #24				Cluster #25				Cluster #26				Cluster #27			
112	.....															

Data Area in FAT File System

- **Overview:**
  - The Data Area is the portion of the FAT volume that follows the System Area.
  - It comprises the remaining space on the volume and serves as the primary storage for file contents.
- **Content Storage:**
  - The Data Area contains the actual content of files stored in the file system.
  - Directories, which are special files, hold file names and metadata for the files.
  - File names adhere to the 8.3 naming convention, consisting of eight characters for the name and three for the file extension.
- **Significance for Forensics:**
  - Understanding directories and their metadata is crucial for digital forensics investigators analyzing FAT file systems.
  - It facilitates the extraction of file content and metadata, aiding in investigations and evidence collection.

File Allocation



1. **Boot Sector Analysis:**
   - Start from the boot sector to access key areas: Data Area, FATs, and the Root Directory.
   - Navigate to the Root Directory to locate the desired file or directory.
2. **Locating the Test Directory:**
   - Traverse through the Root Directory to locate the Test directory.
   - The Test directory's content is referenced by cluster #5.
3. **Finding the File Entry:**
   - Within the Test directory, locate the entry for the file Pic.jpg.
   - Retrieve the file's entry, which contains information about the file's location on the disk.
4. **Identifying the File's First Cluster:**
   - Determine that the file's first cluster is at cluster #11 based on the file's entry.
   - Refer to the FAT to understand the file's cluster allocation.
5. **Traversing through Clusters:**
   - Follow the FAT entries to access subsequent clusters allocated to the file.
   - For example, if the FAT entry for cluster #11 points to cluster #12, proceed to cluster #12.
6. **Reaching End of File (EOF):**
   - Continue traversing clusters until encountering the End-of-File (EOF) marker.
   - The EOF marker indicates the end of the file, signifying that no further clusters are allocated to the file.

Deleting a File

Deleting a File in FAT File System:

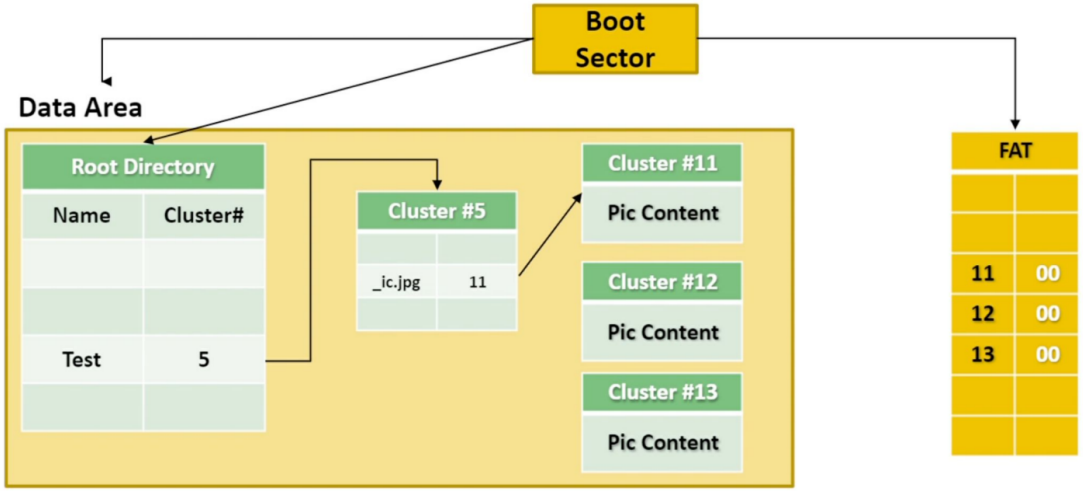
When a file within the FAT file system is deleted, the following changes occur:

1. **File Name Change:**
   - The first character in the file name is changed to `0xE5` to mark it as deleted.

2. **Cluster Entries Zeroed Out:**
    - All cluster entries for the file in the File Allocation Table (FAT) are zeroed out.
    - This indicates that the clusters previously allocated to the file are now available for reuse.
3. **Directory Entry:**
    - The starting cluster in the directory entry for the file remains unchanged.
    - This allows the file system to locate the starting cluster of the deleted file, although its content is no longer accessible.
4. **Contents Existence:**
    - The contents of the file (stored in clusters) still exist on the disk until their clusters are reallocated for storing new data.
    - The deleted file's clusters are considered free space and can be overwritten by new files.

Effect on Disk Illustration:

- Deleting the file Pic.jpg will reflect changes in the directory entry, FAT entries, and the file's name character, indicating its deletion.



NTFS File System Analysis

Introduction:

- While the FAT file system served its purpose for a long time, evolving operating systems and user requirements necessitated the development of a new file system.
- The New Technology File System (NTFS) is a proprietary file system developed by Microsoft, first released in 1993 with Windows NT 3.1.
- NTFS became the default file system for the Windows NT family, including Windows XP, Server 2003, Vista, Server 2008, 7, 8, Server 2012, 10, Server 2016, and beyond.

Core NTFS Features:

1. **Journaling:**

- NTFS implements journaling, storing metadata changes in a log file ($LogFile) to ensure the file system can recover from uncommitted changes in case of system failures.

2. **Scalability:**
   - NTFS supports large volumes and files, offering scalability to meet the growing storage needs of modern computing environments.
3. **Hard Links:**
   - Users can create hard links to files, allowing multiple directory entries to point to the same file on disk, conserving storage space.
4. **Alternate Data Streams (ADS):**
   - NTFS supports alternate data streams, enabling files to contain additional data streams beyond the main file data.
5. **File Compression:**
   - NTFS offers file compression, allowing users to compress individual files or entire directories to save disk space.
6. **Sparse Files:**
   - NTFS supports sparse files, where only specific portions of a file are allocated on disk, reducing storage requirements for large, mostly empty files.
7. **Volume Shadow Copy:**
   - NTFS provides volume shadow copy capabilities, enabling users to create point-in-time snapshots of volumes for backup and recovery purposes.
8. **Transactions:**
   - NTFS supports transactions, allowing multiple file system operations to be grouped into atomic units to ensure data consistency.
9. **Security:**
   - NTFS offers robust security features, including file and folder permissions, access control lists (ACLs), and encryption capabilities.
10. **Encryption:**
    - NTFS supports file-level encryption, allowing users to encrypt individual files or directories for enhanced data security.

Additional Features:

- Quotas, Reparse Points, Resizing, and more.

NTFS Size Limit:

- NTFS does not have the same size limitations as FAT, allowing for much larger volumes and files to be supported.

Volume Size	Cluster Size
7 MB – 512 MB	4 KB
512 MB – 1 GB	4 KB
1 GB – 2 GB	4 KB
2 TB – 16 TB	4 KB
16 TB – 32 TB	8 KB
32 TB – 64 TB	16 KB
64 TB – 128 TB	32 KB
128 TB – 256 TB	64 KB
> 256 TB	Not supported

Description	Limit
Maximum file size	Architecturally = 16 Exabytes - 1 KB or (2^{64} bytes - 1 KB)
	Implementation = 16 Terabytes - 64 KB or (2^{44} bytes - 64 KB)
Maximum volume size	Architecturally = 2^{64} clusters - 1 cluster
	Implementation = 256 Terabytes minus 64 KB (232 clusters - 1 cluster)
Files per volume	4,294,967,295 (2^{32} - 1 file)

File System Structure:

- Unlike FAT, NTFS does not use a specific separation schema like Boot, FATs, and Data. Everything within NTFS is treated as a file.
- NTFS utilizes journaling, storing metadata changes in a log file to ensure system integrity in case of failures.

Journaling file system uses a log file ($LogFile) to store all metadata changes that happen to the volume.

NTFS start with $ character

NTFS Structure

Introduction:

- NTFS employs various metadata files to establish the structure of the file system, creating a robust framework for storing and organizing data.

Master File Table (MFT):

- The primary file in the NTFS file system is the Master File Table, denoted as $MFT.
- Conceptually, the MFT can be visualized as an array of records, each representing a file or directory within the file system.
- Every file, including the MFT itself, has one or more records in the MFT. The number of records allocated to a file depends on its size.

MFT Zone:

- To prevent fragmentation of the MFT (i.e., its records becoming non-contiguous on disk), NTFS reserves a portion of disk space specifically for the MFT.
- This reserved space, known as the MFT Zone, typically accounts for around 12.5% of the total disk space. However, users can adjust this setting to allocate 25%, 37.5%, 50%, or other percentages.
- If the MFT Zone becomes full, the MFT may become fragmented, impacting file system performance and integrity.

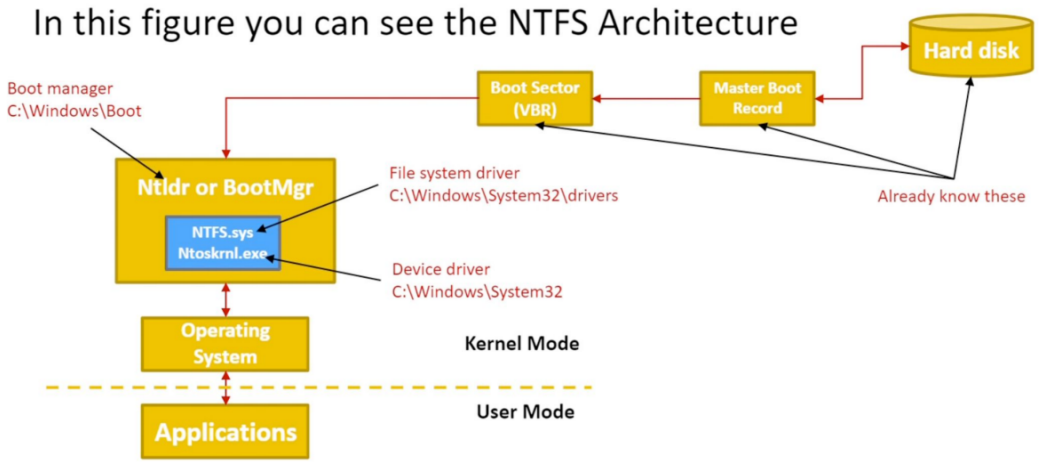
Reserved Disk Space:

- When formatting a hard disk drive with NTFS, a portion of disk space, equal to the size of the MFT Zone, is marked as reserved for the NTFS file system.
- For example, if a hard disk drive has a capacity of 100GB and the MFT Zone is set to 12.5%, approximately 12.5GB of disk space will be reserved and unavailable for user data.

System File	File Name	MFT Record #	Purpose
Master file table	$MFT	0	File holding a record for each file and directory on the volume
Master file table mirror	$MFTMirror	1	For recovery in case MFT failure
Log file	$LogFile	2	Holds information for file system metadata changes, and helps with recovery
Volume	$Volume	3	Information about the volume and its label
Attribute definition	$AttrDef	4	Holds info about all attributes used within the file system
Root file name index	.	5	The rood directory
Cluster bitmap	$Bitmap	6	Track free unused clusters within the volume
Boot sector	$Boot	7	Mount the volume and other bootstrap code when the volume is bootable
Bad cluster file	$BadClus	8	Track bad clusters within the volume
Security file	$Secure	9	Stores the security descriptors for all files in the volume
Upcase table	$Upcase	10	Convert lowercase chars to the matching Unicode uppercase chars
NTFS extension directory	$Extended	11	Holds optional and extended features such as quotas, reparse points, etc
		12 – 15	Reserved for future use

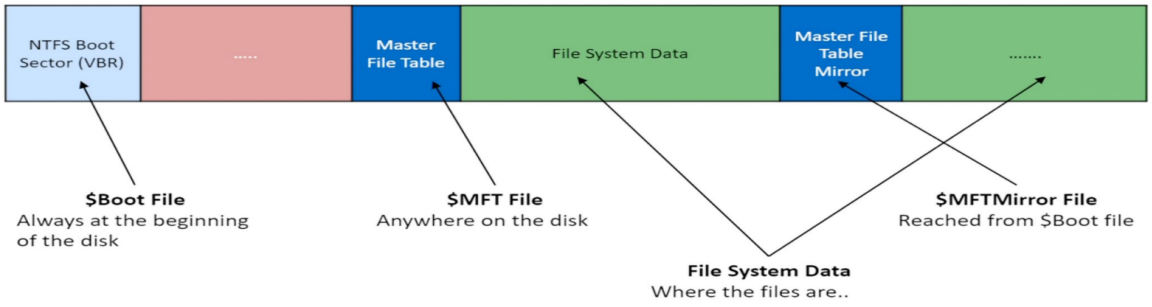
Reserved Entries in the MFT:

- The MFT, being the heart of the NTFS file system, dedicates the initial 15 entries to storing metadata files essential for file system operations.
- These metadata files include critical components necessary for the functioning and integrity of the NTFS volume.
- Details about the structure and contents of these metadata files will be explored further after analyzing the volume boot record (VBR).



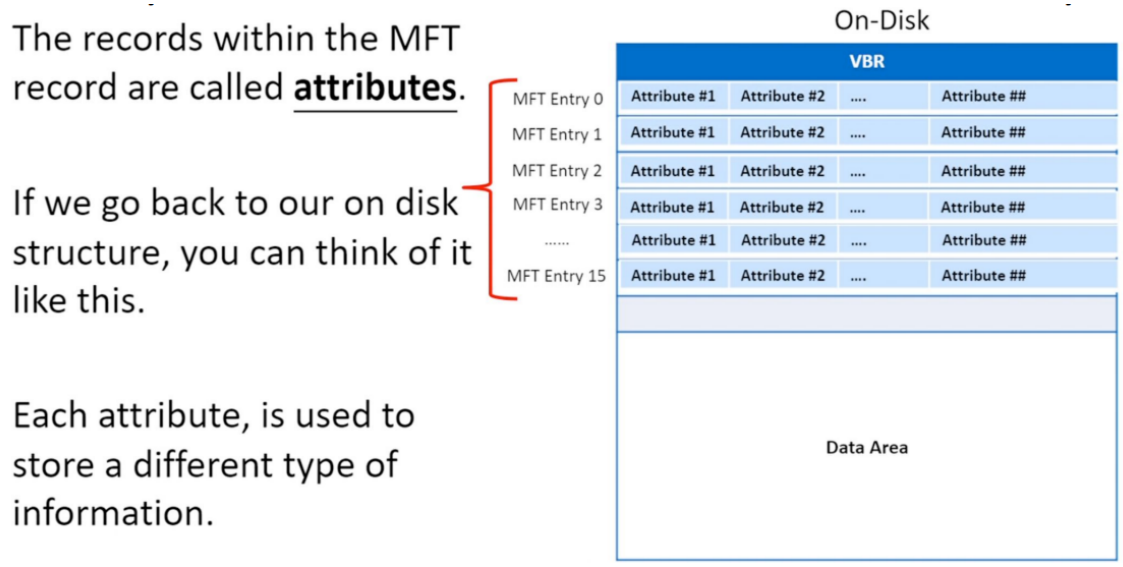
Significance of Metadata Files:

- Metadata files contained within the MFT facilitate various aspects of file system management, such as tracking file attributes, maintaining directory structures, and recording volume information.
- Proper allocation and management of these metadata files ensure the stability, reliability, and efficiency of the NTFS file system.



NTFS Structure - Volume Boot Record (VBR) - $Boot

- The Volume Boot Record (VBR), also known as $Boot, is a critical component of the NTFS file system, responsible for bootstrapping the operating system and providing essential details about the volume.
- Analyzing the VBR and its associated BIOS Parameter Block (BPB) provides valuable insights into the configuration and structure of the NTFS volume.



Master File Table (MFT):

- The MFT serves as an index to every file within the NTFS volume, with each MFT record containing a set of attributes.
- NTFS employs various attributes to store different types of information, with the number of attributes within each MFT record varying based on the nature of the file entry.

Contents of MFT Entry:

- Each MFT entry is constructed using a header, a series of variable-length attributes, and an end marker (typically 0xFFFFFFFF), reflecting the structure and organization of file entries within the MFT.

NTFS File System Analysis: File and RAM Slack

Introduction:

- In NTFS file systems, understanding the concepts of file and RAM slack is crucial for digital investigators as they play a significant role in forensic analysis.
- File slack refers to the unused space allocated to a file, while RAM slack involves residual data from previous files that may be present in unused sectors within allocated clusters.

File Slack:

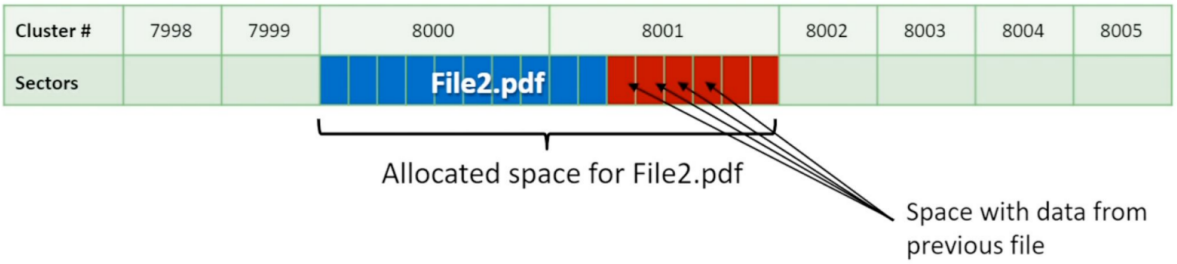
- When a file requires more disk space than the allocated clusters can accommodate, file slack occurs, resulting in unused space within sectors or entire sectors that have been allocated but remain unused by the file.
- Investigating file slack is essential for uncovering potential evidence left behind by previous file activities, making it a critical area for forensic examination.

Importance of Slack Space:

- Slack space serves as a vital location for digital investigators to search for valuable evidence.
- While unused bytes within an allocated sector are less useful, unused sectors within allocated clusters retain their original contents, potentially containing data from previous files.

Scenario: Utilization of Slack Space:

1. **Initial Configuration:**
    - Suppose a disk has a cluster size of 4KB, and a file named "file.txt" with a size of 8KB exists on the volume, occupying clusters 8000 and 8001.
2. **File Replacement:**
    - If "file.txt" is deleted and replaced with a new file named "file2.pdf" with a size of 5KB, it will occupy the same clusters (8000 and 8001) previously allocated to "file.txt."
3. **Analysis after Deletion:**
    - Even after the deletion of "file2.pdf," the space allocated to clusters 8000 and 8001 still contains the original contents of "file.txt," highlighting the persistence of data even after file deletion.



RAM Slack:

- RAM slack refers to the additional data added by the operating system to fill the last sector of a file entirely. It occurs when the size of the file is less than the sector size (usually 512 bytes on hard disk drives).

Explanation:

- When a file is written to a disk, the operating system typically writes data in complete sectors. If the file size is smaller than a sector, the system pads the remaining space with additional data to fill the sector.
- For example, if the volume uses a cluster size of 2048 bytes (four sectors), and a file of 1020 bytes is stored, the system would need to add padding to fill the last sector.

Evolution and Modern Practices:

- Modern operating systems have evolved to address security concerns related to RAM slack. Older systems used to fill RAM slack with data from memory, potentially exposing sensitive information. To mitigate this risk, modern systems pad RAM slack with random data, reducing the likelihood of exposing memory contents.
- As a result, RAM slack as a source of forensic evidence has become less common in modern operating systems.

Other Slack Spaces:

- Apart from file and RAM slack, forensic investigators should also consider other potential sources of slack space. Any data structure that does not fully occupy its storage location could potentially reveal data from previous structures.
- Therefore, forensic analysis should extend beyond traditional slack spaces to explore all areas where residual data might be present, enhancing the thoroughness and effectiveness of investigations.

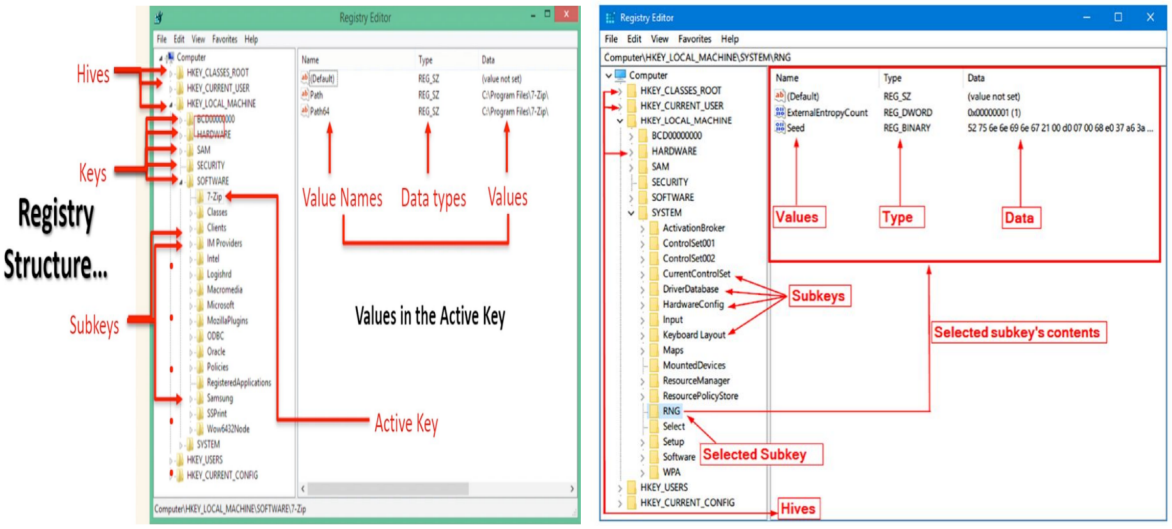
Windows Registry, Windows Artifacts and Windows Forensics

- System artifacts are for data that could be collected related to system activity in response to a stimuli
- User artifacts are those artifacts that are found related to user activity and/or files that have been used by the user himself/herself.
- Registry is computer's central nervous system

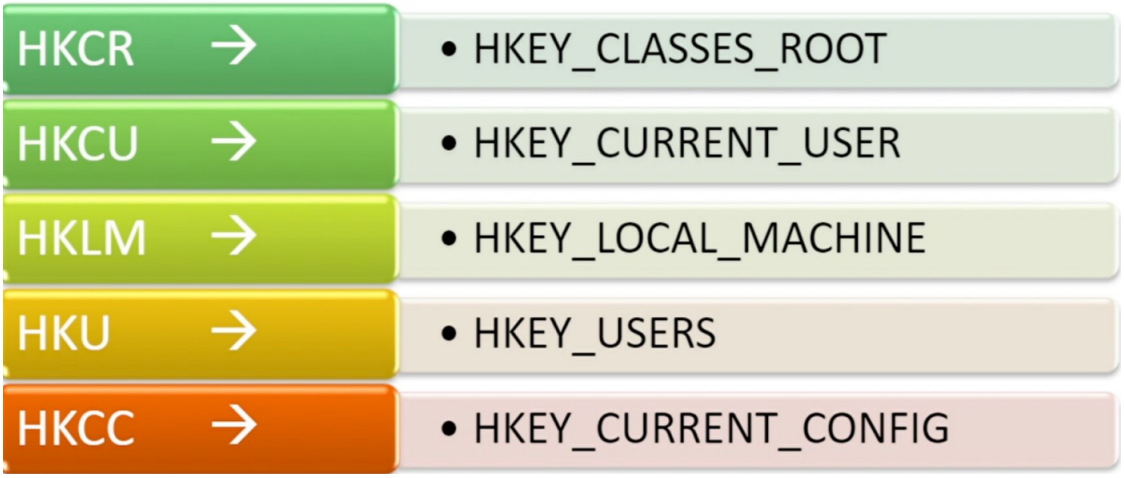
The Windows Registry is a crucial component of the Windows operating system, serving as a centralized database for storing system settings, configuration data, application settings, and user preferences. Digital forensic investigators often examine the Windows Registry during forensic examinations due to its wealth of information and potential to uncover valuable evidence. Here are some key points about inspecting the Windows Registry:

1. **Methods of Examination:**
    - Investigators can analyze the Windows Registry using two primary methods:
        - Examining registry files contained within a forensic image using forensic analysis software.
        - Conducting live analysis by booting up from the suspect forensic image and accessing the registry using the built-in Windows Registry Editor.
2. **Importance of Registry Examination:**
    - Inspecting the registry is a standard practice in forensic examinations because it contains critical system information and evidence.
    - Tools like EnCase and FTK are commonly used by forensic investigators to interpret registry data and extract valuable insights.
3. **Registry File Locations:**
    - The location and number of registry files depend on the Windows version:
        - In older Windows versions like Windows 9x/Me, the registry uses two files: User.dat and System.dat.
        - In newer Windows versions like Windows NT and later, there are six files: Ntuser.dat, System.dat, SAM.dat, Software.dat, Security.dat, and Default.dat.
4. **Significance of Registry Artifacts:**
    - Examining the registry can yield various artifacts with significant implications for the investigation, including:
        - System configurations and functionality settings.
        - Recycle Bin settings and Windows Firewall configurations.
        - User preferences, historical activity logs, and recently used files.
        - Autostart programs and applications configured to run during Windows startup.

Registry Structure:



1. **Hives:**
   - Hives are high-level containers or logical groupings within the Windows Registry that store related system and user configuration information. Each hive corresponds to a specific part of the registry and is represented by a file on the filesystem. The primary hives in the Windows Registry include:
     - `HKEY_CLASSES_ROOT` (HKCR)
     - `HKEY_CURRENT_USER` (HKCU)
     - `HKEY_LOCAL_MACHINE` (HKLM)
     - `HKEY_USERS`
     - `HKEY_CURRENT_CONFIG`

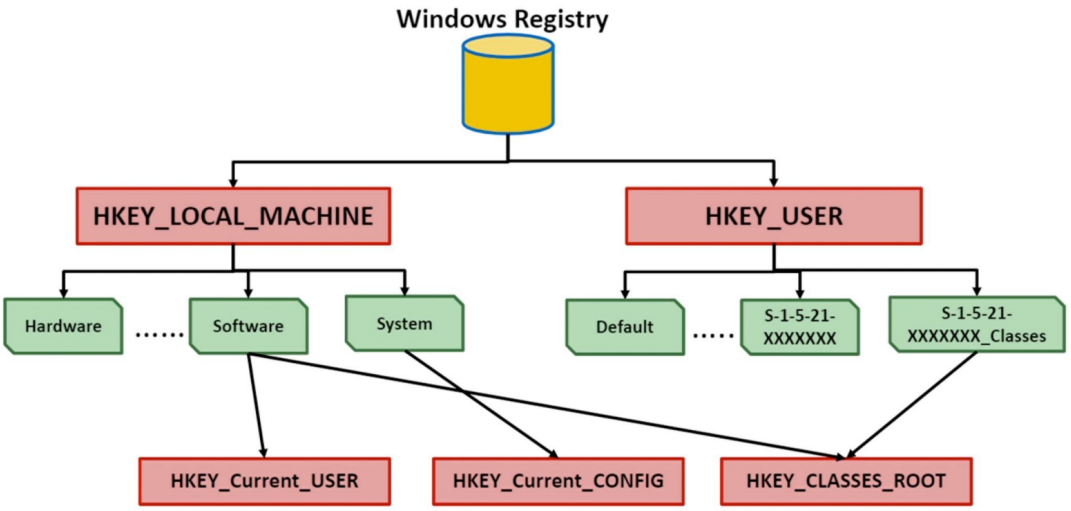


Hive	Abbreviation	Description
HKEY_CLASSES_ROOT	HKCR	Contains information about file associations and OLE object classes.
HKEY_CURRENT_USER	HKCU	Stores settings specific to the currently logged-in user, such as desktop configurations and preferences.

HKEY_LOCAL_MACHINE	HKLM	Holds configuration data for the local computer, including hardware settings and software information.
HKEY_USERS	N/A	Contains user profiles and settings for all users who have logged into the system.
HKEY_CURRENT_CONFIG	N/A	Provides a view of the current hardware configuration, derived from information in HKLM\System\Config.

These hives represent key areas of the Windows Registry where various system and user configuration settings are stored. Understanding their organization and contents is essential for managing system configuration and troubleshooting issues on Windows-based systems.

2. **Keys:**
   - Keys are the main organizational units within a hive and serve as containers for organizing related configuration settings or data. They are analogous to folders in a file system and help categorize information hierarchically. Keys are identified by unique paths within a hive, which specify their location in the registry hierarchy.
3. **Subkeys:**
   - Subkeys are keys that reside within other keys, forming a hierarchical structure within the registry. They are similar to nested folders within a directory structure, allowing for further organization and categorization of registry data. Subkeys can contain additional keys or values, enabling the registry to store a wide range of configuration settings and data.
4. **Values:**
   - Values are data elements stored within keys in the registry and represent the actual configuration settings, parameters, or data associated with a particular key. Each value is identified by a name and can contain various types of data, such as strings, integers, binary data, or multi-string data. Values provide the actual content or configuration information stored within the registry keys.
5. **Volatile Hives**:
   - These hives are stored in memory and are not permanently saved to disk.
   - They contain data that is volatile and may change frequently during system operation.
   - Examples include `HKEY_CURRENT_USER` and `HKEY_CURRENT_CONFIG`.
6. **Non-Volatile Hives**:
   - These hives are stored on disk and are persisted across system reboots.
   - They hold data that remains consistent between system restarts.
   - Examples include `HKEY_USERS`, `HKEY_CLASSES_ROOT`, and `HKEY_LOCAL_MACHINE`.



Filename and location	Purpose of file
Users*user-account*\Ntuser.dat	User-protected storage area; contains the list of most recently used files and desktop configuration settings
Windows\system32\config\Default.dat	Contains the computer's system settings
Windows\system32\config\SAM.dat	Contains user account management and security settings
Windows\system32\config\Security.dat	Contains the computer's security settings
Windows\system32\config\Software.dat	Contains installed programs' settings and associated usernames and passwords
Windows\system32\config\System.dat	Contains additional computer system settings
Windows\system32\config\systemprofile	Contains additional NTUSER information

Registry Keys

The registry key holds the following:

- A signature
  - Found at offset 0x0 and is 4 bytes long.
  - Holds the ASCII string **regf** and all hive files will start with this signature.
- The last write timestamp (*last time the key was written*)
- A major and minor version numbers
- The root cell offset

"NukeOnDelete" value set to "1" indicates that files are configured to bypass the Recycle Bin.

SID Subfolders: In Windows systems, the Recycle Bin contains SID (Security Identifier) subfolders, each corresponding to a specific user account. These subfolders store deleted files associated with each user.

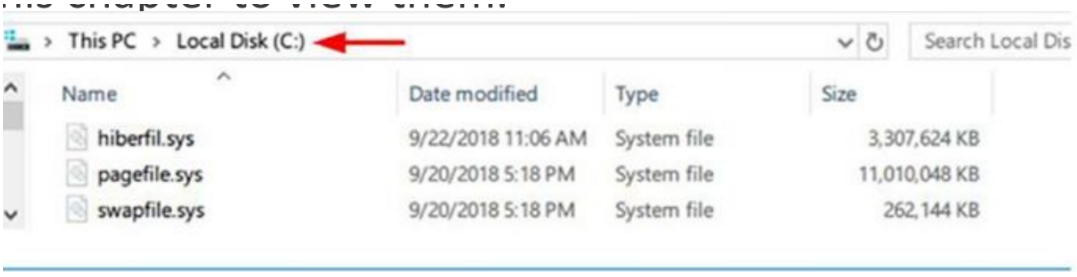
Metadata and Data Files: Deleted files in the Recycle Bin are stored as pairs of metadata files and actual data files. The metadata files provide information about the deleted files, while the data files contain the recoverable content of the deleted files.

File Carving

File carving is a forensic technique used to extract files or data fragments from unallocated space on storage devices, such as hard drives or memory cards.

Unallocated space refers to the portion of a storage device that does not contain any active file system data. This space may contain remnants of deleted files or fragments of data that are not associated with any specific file.

Windows Sleep



Hibernation File, often represented by the file "hiberfil.sys," plays a crucial role in the hibernation process of a computer.

The hibernation file is used by the computer to store a copy of the system's memory (RAM) on the hard disk when the hibernation or hybrid sleep setting is enabled. This allows the computer to quickly resume its previous state when it wakes from hibernation.

Print Spooling

Location of Installed Printers' Keys in Windows Registry: To view the properties of currently installed printers on a Windows system, navigate to the following registry path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers\
```

- In forensic investigations, a suspect's printing activities may be relevant and can leave traces in the system.
- Print spooling is a process where print jobs are temporarily stored until they can be printed.
- During the spooling process, Windows creates two complementary files for each print job: an Enhanced Meta File (EMF) and a spool file (.spl).
- The EMF file contains an image of the document to be printed, while the spool file contains information about the print job itself, including the printer name, computer name, and user account that sent the job to the printer.

- Both the EMF and spool files may have evidentiary value in forensic investigations.
- Normally, these files are deleted automatically after the print job is completed, but exceptions occur if there are problems with printing or if the computer is configured to retain copies of print jobs.
- Spool and EMF files can potentially contain valuable evidence, such as copies of documents, contracts, client lists, or other incriminating materials sent to the printer.

Metadata

There are two flavors of metadata : application and file system.

The file system keeps track of our files and folders as well as some information about them. File system metadata include the date and time
a file or folder was created, accessed, or modified

1. **Created**:
   - Indicates the timestamp when a file or folder was initially placed on a storage device.
   - It provides insight into the origin of the file, showing how it was introduced into the system, whether through saving, copying, cutting and pasting, or dragging and dropping.
   - Understanding the creation timestamp is crucial for determining the file's provenance and potential relevance to an investigation.
2. **Modified**:
   - Reflects the date and time when a file was last altered and saved.
   - Modifications encompass any changes made to the file's content, attributes, or metadata.
   - This timestamp is essential for tracking the evolution of a file over time and identifying when significant alterations occurred.
3. **Accessed**:
   - Updated whenever a file is interacted with by the file system, indicating instances where the file is accessed or queried by system processes.
   - Unlike the "opened" status, which requires user interaction, "accessed" includes automated interactions such as antivirus scans, indexing operations, or backup routines.
   - It provides insights into system-level interactions with the file, beyond user actions, which can be valuable for understanding the file's usage patterns.
4. **Importance**:
   - Metadata serves as a vital source of information in digital investigations, providing contextual details about files and folders.
   - However, the reliability of metadata may be compromised by factors such as user manipulation of system clocks or differences in time zones.
   - Investigators must verify the accuracy of metadata timestamps and consider potential discrepancies during analysis.
5. **Application Metadata**:
   - Applications can generate and store metadata related to file attributes and usage patterns.
   - In addition to basic timestamps, application-specific metadata may include details such as author names, organizational affiliations, document properties, and version history.

- This application-level metadata offers deeper insights into the context and purpose of files, enhancing their relevance in forensic examinations.

6. **Metadata Removal**:
   - Concerns about privacy and data integrity have prompted efforts to remove metadata from files before sharing or publishing.
   - Various tools and software solutions facilitate the scrubbing of metadata, ensuring sensitive information is not inadvertently disclosed.
   - Organizations, including law firms and government agencies, often employ metadata removal procedures to mitigate the risk of unintentional data exposure.
7. **Role in Investigations**:
   - Recovered metadata can play a crucial role in forensic investigations, providing corroborating evidence and establishing timelines of events.
   - Timestamps associated with file creation, modification, and access can be used to reconstruct sequences of actions and attribute accountability.
   - By analyzing metadata, investigators can refute claims of file manipulation or ignorance, leveraging timestamp discrepancies to uncover inconsistencies in narratives.

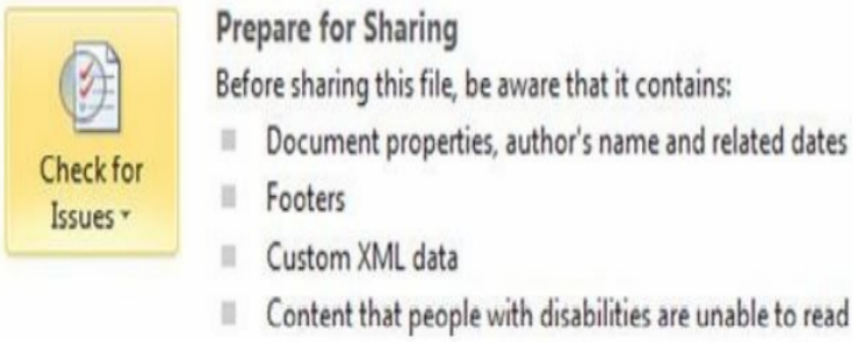


Figure Menu item to choose scrubbing inside of Microsoft Word 2010.

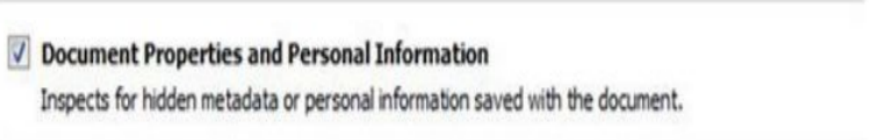


Figure The option to scan for metadata in Microsoft Word 2010.

Thumbnail Cache:

1. **Purpose**:
    - Thumbnails are small, miniature versions of images created by Windows to facilitate easier browsing of pictures on a computer.
    - They provide a visual preview of images, allowing users to quickly identify and select files without opening them individually.
2. **Creation Process**:
    - Windows generates thumbnails automatically when the user selects "Thumbnail" view in Windows Explorer.
    - These thumbnails are smaller versions of the original images, enabling faster browsing and navigation through folders containing numerous pictures.
3. **Types of Thumbnail Files**:
    - Depending on the Windows version, different thumbnail cache files are created:
        - **Windows XP**: thumbs.db
        - **Microsoft Vista and Windows 7**: thumbcache.db
    - These files store information about the thumbnails generated by Windows Explorer.
4. **Visibility**:
    - Many users are unaware of the existence of thumbnail cache files because they are created and managed by the operating system in the background.
    - Unlike regular image files, thumbnail cache files are not typically visible to users during regular file navigation.
5. **Persistence**:
    - An important aspect of thumbnail cache files is that they persist even after the original images have been deleted.
    - This means that even if the original images are removed from the system, the thumbnail cache files may still contain visual representations of those images.
6. **Forensic Significance**:
    - Thumbnail cache files can be valuable sources of evidence in forensic investigations.
    - Even if the original images are no longer accessible, recovering thumbnail cache files can provide insights into the types of images that were previously present on the system.
    - Investigators can use thumbnail cache files to reconstruct the user's browsing history and identify potentially relevant images, even if the originals have been deleted or hidden.

Most Recently Used (MRU):

- The Most Recently Used (MRU) list is a feature designed by Windows to enhance user experience by providing quick access to recently used applications or files.
- MRU entries serve as shortcuts or links to files and applications that have been accessed or used recently by the user.
- Windows maintains a log of the most recently accessed files, recording instances where users open files using Windows File Explorer, standard open/save dialog boxes, or execute commands through

the MS-DOS prompt.

- Many applications running on Windows also maintain their own MRU lists, such as recently opened Microsoft Office files or recently visited web pages in web browsers.

No	Registry key
1	HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs
2	HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word*\File MRU
3	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU
4	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU**
5	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
6	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
7	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit

> LastVisitedPidlMRU

Restore Points:

1. **Definition**:
   - Restore points are snapshots of crucial system settings and configurations captured at specific moments in time, serving as checkpoints for system recovery (Microsoft Corporation).
   - These snapshots enable users to restore their systems to a previous working state in case of system errors, failures, or undesired changes.

   Examining restore points may reveal evidence that is not present in other system artifacts or locations.

   Shadow copies provide the source data for restore points.

Prefetch

1. **Introduction**:
   - Prefetching is a technique used by operating systems, such as Windows, to optimize system performance by predicting and loading data into memory before it is actually needed.
   - Microsoft developers utilize prefetching to enhance system responsiveness by reducing program loading times.
   - Detecting prefetch files associated with applications like "Evidence Eliminator" can indicate their past presence on the system.
   - Even if the original evidence has been wiped or deleted, the existence of prefetch files can serve as indirect evidence of the application's usage.
   - Investigating the Prefetcher's configuration stored in the Windows registry can provide insights into system settings related to prefetching.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Ma
```

The configuration settings for the Prefetcher are stored in the Windows registry under the following

Link Files:

1. **Overview**:
   - Link files, commonly known as shortcuts, are pointers or references to other files or folders.
   - They facilitate quick access to files or applications without navigating through the entire file system.
   - Link files can be manually created by users or automatically generated by the computer.
2. **Creation**:
   - Users often create shortcuts on their desktops or in specific folders for easy access to frequently used files or programs.
   - Computers automatically generate link files in various locations. For example, recent documents lists in applications like Microsoft Word consist of link files.
3. **Forensic Significance**:
   - Each link file possesses its own metadata, including creation and last access timestamps.
   - The presence of a link file can indicate that a particular file or application was accessed or used at some point in time.
   - Link files can be crucial in establishing the existence of certain files or folders, refuting claims of non-existence.
   - They may retain the full file path, even if the associated storage device, such as a USB thumb drive, is no longer connected.
4. **Importance**:
   - Investigators can analyze link files to reconstruct user activities, identify frequently accessed files or applications, and determine usage patterns.
   - Link files serve as valuable forensic artifacts, aiding in the reconstruction of digital events and user behavior.

USB Device Forensics:

1. **Windows USB History Log**:
   - Windows maintains a history log of all previously connected USB devices.
   - This log includes details such as connection times and the associated user account that installed the devices.
2. **Registry Information**:
   - The Windows registry stores technical information for each connected USB device.
   - Key details stored include vendor ID, product ID, revision, and serial number.
   - USB history-related information is stored in five registry keys, each providing different insights into connected devices.
3. **Registry Keys**:

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR**: Contains a record of all USB devices plugged into the system since its installation.
- **HKEY_LOCAL_MACHINE\SYSTEM\Currentcontrolset\Enum\Usb**: Holds technical data about connected USB devices and their last connection times.
- **HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices**: Stores drive letter allocations related to USB devices.
- **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2**: Records user information and last connection times for USB devices.

4. **Investigative Insights**:
   - By analyzing this information, investigators can understand how individuals have used USB devices to conduct or facilitate actions.
   - The gathered data provides insights into device connections, users associated with those connections, and technical details of the connected devices.
5. **Automation Tools**:
   - Tools like USBDeview by Nirsoft automate the process of retrieving information about current and previous USB devices connected to a system.
   - USBDeview provides extended details such as device name, description, type, and serial number for each connected USB device.

Windows Shutdown Time:

1. **Registry Key**:
   - The shutdown time of a Windows system is recorded in the registry key:

     ```
     HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Windows
     ```

   - This information is stored in the value named `ShutdownTime`.
2. **Data Format**:
   - The shutdown time value is stored in binary format.
   - To decode this binary value into a human-readable format, a tool called DCode from Digital Detective can be utilized.

- DCode will then decode the binary data and present the shutdown time in a readable format, providing investigators with precise information about the last shutdown event of the Windows system.

Timeline analysis

1. **Holistic View of Events**: Timeline analysis provides investigators with a chronological overview of activities that occurred on a system. This helps in understanding the progression of events leading up to an incident, aiding in the investigation process.
2. **Determining Activity Timing**: One of the primary goals of timeline analysis is to pinpoint when specific activities occurred on the system. This information is vital for establishing the timeline of events and identifying any suspicious or malicious actions.

3. **Focus Investigation Efforts**: By narrowing down the timeframe of interest, timeline analysis allows investigators to focus their efforts on examining relevant data. This can significantly reduce the volume of data that needs to be analyzed, saving time and resources.
4. **Malware Detection and Analysis**: Timeline analysis is particularly important in malware investigations. It helps identify when a system's state changed due to a malware attack, allowing investigators to trace the malware's behavior and its impact on the system.
5. **File Timestamps**: Timestamp information associated with files, such as creation, modification, and access times, serves as the foundation for timeline analysis. Each file in a forensic image contains these attributes, which provide valuable insights into file-related activities.
6. **Operating System Differences**: It's essential to note that different operating systems treat file timestamps differently. For example, in Windows, creation and change times indicate content modifications, whereas UNIX systems focus on metadata changes. Investigators must understand these differences when analyzing file timestamps.

Network Analysis

Network analysis in digital forensics involves examining various aspects of network connections made by a system. Here's how Windows registry plays a crucial role in network analysis:

1. **Logging Network Connections**: Windows logs all network connections, whether to the Internet or an intranet, in the registry. This includes both wired and wireless connections.
2. **Identification of Network Cards**: The registry stores information about all network cards used on the system, including built-in cards and those connected via USB ports. This information can help identify the hardware used for network communication.
3. **Wireless Connection Profiles**: For wireless connections, the registry contains details of connection profiles, including the network name (SSID), IP address, subnet mask, and DHCP settings. This information provides insights into the wireless networks the system has connected to.
4. **Timestamps**: Each network connection entry in the registry includes timestamps indicating when the connection was first established and when it was last used. These timestamps can be crucial for establishing timelines of network activity.

Common Windows Registry Keys for Storing Network Connections

No	Registry key
1	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards
2	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Nla\Cache\Intranet
3	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Wireless*
4	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Signatures\Unmanaged**
5	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles***

**Holds the identifier of all wireless networks to which the system was connected.*

***Holds detailed information about each wireless connection on the target machine. Links the identifier of the previous key to this key to provide comprehensive information about the target connection*

****Holds the "Creation date" and "Last connected date" of the selected wireless connection. The values of these dates are of binary type*

UserAssist Forensics

1. **Record of Executable Programs**: UserAssist maintains a log of all executable programs launched by users on a Windows system. This log includes details such as the name of the program and the frequency of its usage, measured by the number of executions.
2. **Registry Location**: The information collected by UserAssist is stored in the Windows registry, specifically in the following key: `HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\UserAssist`.
3. **Limitation**: It's important to note that UserAssist records only those programs launched via Windows Explorer. Programs launched through the command line interface (CLI) won't be recorded in the UserAssist registry keys.
4. **Data Encoding**: Information stored in the UserAssist registry keys is encoded using ROT-13 encoding, a simple letter substitution cipher. This encoding scheme obfuscates the data to some extent. However, it can be decoded using tools like UserAssist-View developed by Nirsoft.

Jump Lists

Jump Lists Forensics is a valuable technique in digital forensics for investigating user activity on Windows systems. Here's an overview:

1. **Introduction to Jump Lists**: Jump Lists is a feature introduced by Microsoft in Windows 7, allowing users to quickly access recently viewed or accessed files for each installed application. This feature provides insights into the user's computer habits and recently accessed files, which can be crucial in forensic investigations, particularly when focusing on user activities.
2. **Forensic Value**: Investigating Jump Lists provides deep insight into user behavior and recently accessed files, aiding in reconstructing timelines of events and identifying relevant evidence in criminal investigations.
3. **Configuration**: Jump Lists are enabled by default in Windows 10. Users can configure this feature through Windows Settings by navigating to Start ➔ Personalization ➔ Start.
4. **Location of Jump List Files**: Jump List files are stored for each user on a Windows system and can be found at the following directory path: `\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent\`.
5. **Types of Jump Lists**:
   - **AUTOMATICDESTINATIONS-MS**: These files are automatically created by Windows in the directory when a user opens an application or accesses a file. Jump Lists are contained within OLE containers and are named according to the application that has opened the relevant file.

     ```
     \Users\<username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinat
     ```

   - **CUSTOMDESTINATIONS-MS**: These files are created in the directory when a user pins a file to the Start menu or taskbar. `\Users<username>\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations-ms`

Windows Minidump File Forensics:

When a Windows machine crashes with a Blue Screen of Death (BSOD), a copy of the computer memory at the time of the crash is stored in the `\Windows\minidump or \Winnt\minidump` directory, depending on the Windows version. Minidump files from Windows 10 typically contain information about the programs running or installed at the time of the crash.

Minidump files can be valuable for digital forensic examiners, as they may contain information about the programs and activities occurring at the time of the crash

Deleted Registry Key Recovery:

Recovering deleted Windows registry keys can be important in forensic investigations. The Register Explorer tool, developed by Eric Zimmerman, is a simple and portable tool that can handle this task and more. It allows forensic examiners to recover deleted registry keys, providing valuable insights into system activities and changes.