

Prepared by Dr. Nermin Ewais

CYB 770  
IT Forensics

## Lecture 04



# Media Analysis

## Lecture 04

CYB 770  
IT Forensics

Prepared by  
**Dr. Nermin Ewais**

- Media analysis
- Understanding the boot process
- Understanding filesystems
  - BIOS and UEFI
- Deleted Files
  - Recovery Tool
- Random access memory (RAM)
  - Exploring RAM capture tools

- Media analysis is where you are analyzing physical storage devices such as hard drives, SSD drives, or optical storage disks.
- The primary source of your digital investigation will be the forensic images of storage devices such as hard drives, SSD drives, USB devices, optical discs, and mobile devices such as smartphones.

- **The forensic image** is a bit for a bit of the source device. In most cases, you do not want to use a 'backup' as the source of your digital forensic investigation because a 'backup' will not contain all of the information that is contained on the storage device.
- **The goal of media analysis** in your digital forensic investigation is to find relevant artifacts that will either prove or disprove the allegations you are investigating.

The storage device may contain four different data types that you want to examine:

- **Allocated space:** This is the space on the storage device that a file occupies. The filesystem recognizes the storage space as being used.
- **Unallocated space:** This is the space on the storage device that is not occupied by a file. The filesystem recognizes the storage space as being available for use.

- **Slack space:** When the data is stored in a cluster; if the file does not completely fill a cluster, the remaining space not used by the file is referred to as slack space.
- **Bad blocks/sectors/clusters:** This is the space on the disk that has been marked bad by the filesystem because of a defect. It can also be used by a user to hide data from a casual inspection.

**Bad blocks** refer to **damaged areas on a storage device** (like a hard drive, SSD, or USB) that **cannot reliably store or retrieve data**.

| Term               | Commonly used for                    | Meaning                                                                                                     |
|--------------------|--------------------------------------|-------------------------------------------------------------------------------------------------------------|
| <b>Bad Block</b>   | General term (any storage)           | A unit of storage that is damaged or unreadable.                                                            |
| <b>Bad Sector</b>  | <b>Hard drives (HDDs)</b>            | A sector (usually 512 bytes or 4 KB) that cannot be read or written.                                        |
| <b>Bad Cluster</b> | <b>File systems (like FAT, NTFS)</b> | A group of sectors (the smallest allocation unit of the file system) that includes at least one bad sector. |

## Types

- **Physical (Hard) Bad Blocks**

- Caused by actual physical damage.
- Cannot be repaired — only marked as “unusable.”
- Example: Disk surface defect.

- **Logical (Soft) Bad Blocks**

- Caused by software or logical errors (like sudden shutdown).
- Can often be repaired by overwriting or reformatting.

- Because slack space is **not visible in the normal file view**, it can be **abused to hide data** secretly.
- **Example:**
- A malicious user saves a 2 KB text file in a 4 KB cluster.
- Then uses a special program to insert secret data (like messages, passwords, or malware) into the **remaining 2 KB slack space**.
- The operating system doesn't show this hidden content because it thinks the space belongs to the original file's cluster.
- So even if someone opens the text file, they'll only see the visible 2 KB — not the hidden data in the slack.
- This method is sometimes called **data hiding in file slack** or **slack space steganography**.

This technique is attractive for malicious actors because:

- It avoids detection by antivirus software.
- It doesn't change file sizes or timestamps.
- It can be used to hide malware, encryption keys, or confidential information

- Forensic investigators know that **hidden data** or **fragments of deleted files** can exist in slack space.  
So, during an investigation, they check it for:
- Hidden messages or files (steganography)
- Malicious code or scripts

# How Forensic Tools Detect Slack Space Data

- Forensic tools can **analyze the physical disk** (not just logical files) and examine **every cluster**, including unused parts.
- **Common Tools:**
- **EnCase**
  - Allows investigators to view cluster-level data.
  - Highlights file slack and unallocated space separately.
- **FTK (Forensic Toolkit)**
  - Can scan slack space for keywords, hidden content, or patterns.
- **Autopsy / Sleuth Kit**
  - Open-source tool that can extract and analyze slack space.
  - Investigators can compare file sizes vs. cluster sizes to locate slack areas.
- **Hex Editors (like WinHex or HxD)**
  - Used for manual inspection of cluster content.
  - Investigators can literally see raw bytes that don't belong to the main file.

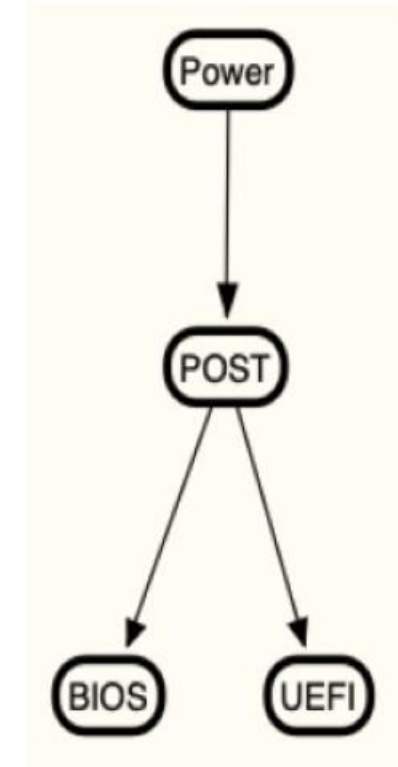
- **Disk:** Physical storage devices such as a hard disk drive, solid state disk drive, or flash media.
- **Data unit:** The smallest allocation unit available to the filesystem. In most cases, this will be clusters, or, in a UNIX-based system, it will be blocks.
- **Metadata:** This is the data about data. This includes the modified, accessed, and created date-time stamps, as well as any other information the filesystem will track about the file.

## Understanding the boot process

- **Computer System:**  
operating system, the filesystem, and the hardware bundled together to create a computer.
- To be effective, you must understand the physical media the data is stored on, the filesystem used on the storage device, and how that data is tracked and accessed while on the storage device.
- Once you understand the process, you can then implement controls to protect the integrity of the digital evidence.

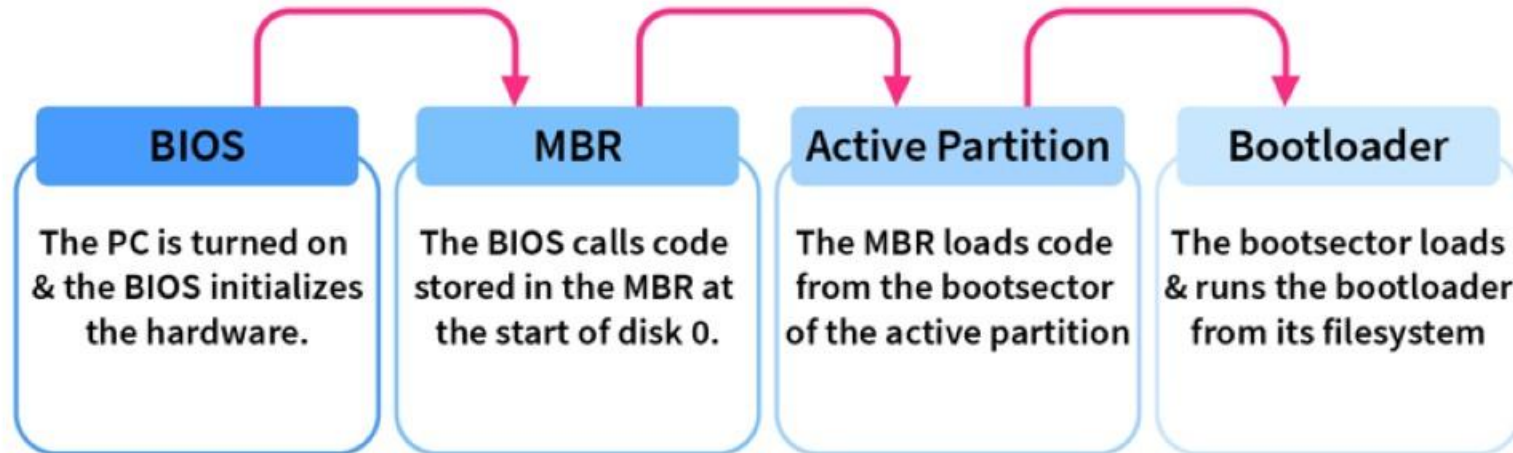
❑ The first step is the **Power-On Self-Test (POST)**;

- The CPU will access the **Read-Only Memory (ROM)** and the **Basic Input/Output System (BIOS)** and test essential motherboard functions.
- This is where you hear the beep sound when you turn the power on to the computer system.
- If there is an error : notify the error through the using of beep codes.
- The motherboard manual, to specific beep code.



- **The BIOS (Basic Input/Output System)** will look for the Master Boot Record (MBR) of the boot device.
- The MBR is located at sector zero and holds information about the partitions, filesystems, and the boot loader code for the installed operating system.
- Once the MBR is found in the boot loader and has been activated, control is then passed over to the operating system to complete the booting process.

# Understanding the boot process



- **United Extensible Firmware Interface (UEFI).**
- It provides the same service as the BIOS, but has been enhanced.
- The UEFI will look for the GPT.
- A GPT disk can contain up to 128 partitions for a Windows operating system.
- Just like in the BIOS scheme, once the active partition and boot loader have been found, the operating system will take over the booting process.

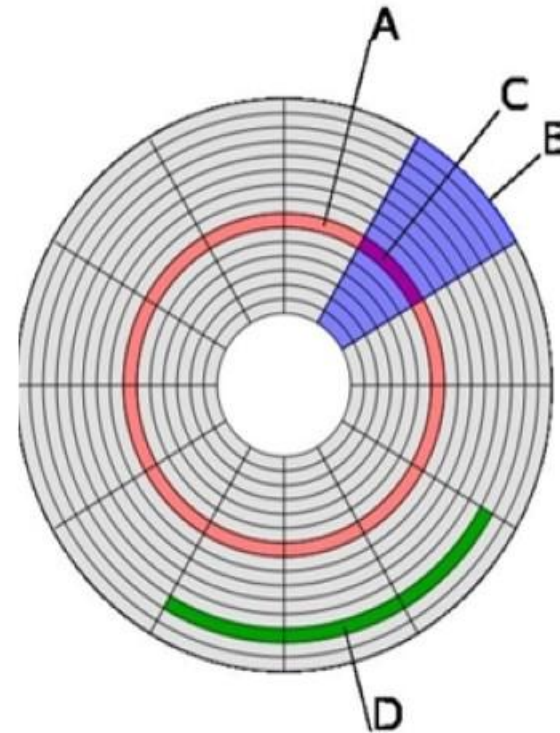
- We can find the MBR at sector zero.
- The MBR contains the information needed by the system to boot.
- The MBR will be contained in sector zero, so it will be no longer than 512 bytes.
- The first 440 bytes comprise the boot code,
- The next 64 bytes will be the partition table. The partition table will show us which partition is the active partition.

- Once the starting sector or the active partition is located, the boot process will continue.
- Partitioning occurs when we divide the physical device into logical segments called "volumes." With the MBR partitioning scheme

- **A GUID is a globally unique identifier**
- The GPT is a partitioning scheme that is used for newer storage devices and is part of the new UEFI standard.
- The UEFI standard replaces the BIOS, while the GPT replaces the MBR partitioning scheme

## Understanding filesystems

- Clusters are one or more sectors.
- A cluster is the smallest allocation unit the filesystem can write to.



Hard Drive Structure:

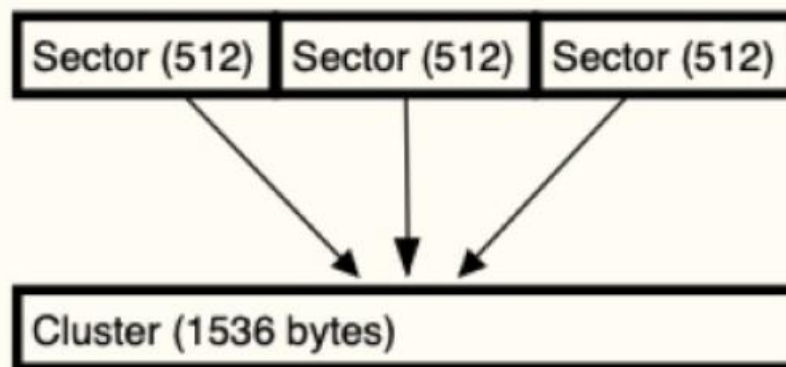
A = track

B = sector

C = sector of a track

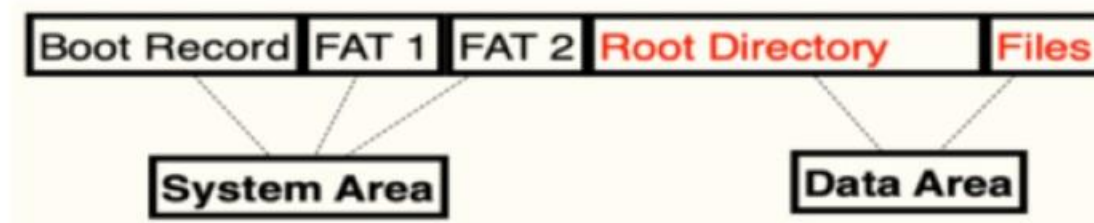
D = cluster

- A **cluster** is the smallest allocation unit the filesystem can address.
- A **sector** is the smallest allocation unit on the disk. A cluster is made up of one or more sectors.

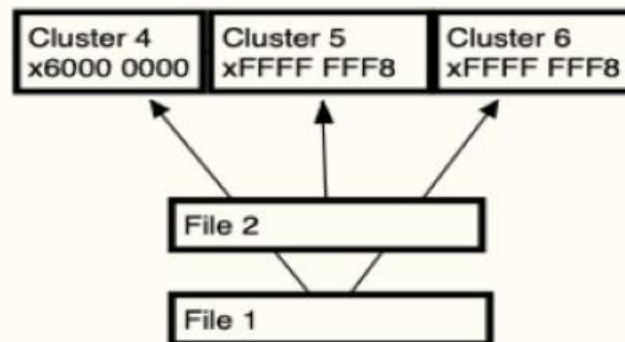
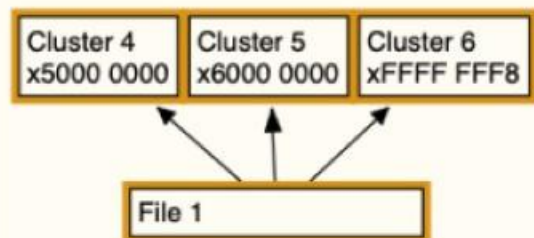


- A hard drive can have multiple partitions on it, and, in each partition, there will be (in most cases) a filesystem.
- There might be hundreds of thousands to millions of files contained within a partition.
- The filesystem tracks where every file is and how much space is available within the partition boundaries.
- The filesystem stores data based on clusters.
- We will now look at some of the common filesystems you may encounter: FAT and NTFS

- The File Allocation Table (FAT) filesystem
- FAT 12 – FAT 16 – FAT 32
- The FAT filesystem is laid out in two areas :
  - System Area: This stores the volume boot record and FAT tables.
  - Data Area: This stores the root directory and files.



- Unallocated: x0000 0000
- Allocated: The next cluster that is used by the file (for example, it represents cluster 7 as **x0700 0000**)
- Allocated: The last cluster that is used by the file (xFFFF FFF8)
- Bad cluster: Not available for use (xFFFF FFF7)



- The New Technology File System (NTFS) is the default filesystem for Microsoft Windows operating systems
- NTFS is far more complicated than the FAT filesystem; however, the overall purpose remains the same:
  - ❑ To record the metadata of a file, that is, the filename, the date timestamps, and the file size
  - ❑ To mark the clusters the file occupies
  - ❑ To record which clusters are allocated and which clusters are unallocated

Deleted Files

- Recycle Bin
- To give users a second chance to restore a file before permanently deleting it, a number of operating systems provide an easy-to-use method of restoring deleted files.
- A Recycle Bin or Trash Can is a repository where files are temporarily stored after they are deleted.

- If a file is deleted from a computer, the user can generally restore it him- or herself because it is usually sent to the Recycle Bin before actually being deleted.
- If the Recycle Bin has been emptied, the person held down Shift + DEL when deleting the file, or the person used a noncompliant program to delete the file (which bypassed the Recycle Bin), then the data may still be recoverable.

- The important point is that time isn't wasted before contacting someone to restore the data and nothing else is written to the hard disk (since this may overwrite the data).

## Recovering deleted data

- When a file is deleted in the FAT filesystem, the data itself does not get changed.
- The first character of the directory entry will have it changed to a xE5 and the file allocation table entries are reset to x00.
- When the filesystem reads the directory entries, and it encounters the xE5, it will skip that entry and start reading from the subsequent entries.

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |                  |     |      |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|-----|------|
| E5 | 48 | 4F | 52 | 54 | 20 | 20 | 20 | 54 | 58 | 54 | 20 | 18 | 6B | B0 | 6D | ãHORT            | TXT | .k°m |
| D3 | 4E | D4 | 4E | 00 | 00 | E9 | 5E | D4 | 4E | 08 | 00 | 27 | 00 | 00 | 00 | ÓNÔN..é^ÔN..'... |     |      |

- Data recovery tools are designed to restore data that has been deleted or corrupted from any number of sources, including hard disks, CDs, DVDs, Blu-ray, HD-DVD, floppy disks, memory cards used in digital cameras, and other storage media.

- **Easy-Undelete** ([www.easy-undelete.com](http://www.easy-undelete.com)) is a tool that will not only restore files from hard disks using FAT12, FAT16, FAT32, and NTFS file systems but also restore files from non-Microsoft partitions such as Linux and Macintosh OS X.
- **eData Unerase** is a free tool developed by Octanesoft and is available at [www.octanesoft.com](http://www.octanesoft.com). It allows you to restore any files that have been deleted from the Recycle Bin or using other methods that make it otherwise unrecoverable without data recovery software

- **VirtualLab** is data recovery software designed for use on Windows 9x or later, as well as Apple Macintosh computers running OS 9 or later.
- It is available at [www.binarybiz.com](http://www.binarybiz.com), and it allows you to recover files from drives using FAT12, FAT16, FAT32, NTFS, HFS, or HFS Plus partitions.

# Deleted File Recovery Tools

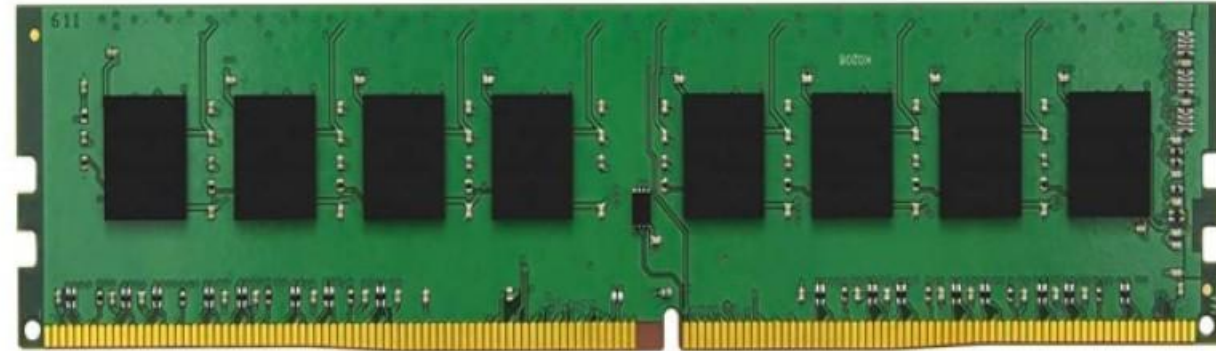
- **File Recover** is a tool developed by PC Tools Software that is available at [www.pctools.com/file-recover/](http://www.pctools.com/file-recover/). It supports FAT16, FAT32, and NTFS file systems and also IDE/ATA/SCSI hard drives, including drives larger than 8 GB.



## Random access memory

## Random access memory

- You may run into two different types of RAM: **static RAM (SRAM)** and **dynamic RAM (DRAM)**.
- SRAM is considered faster and more efficient with respect to energy use, whereas
- DRAM is cheaper to produce than SRAM.
- You will typically find **SRAM** being used as cache memory for the CPU,
- while **DRAM** chips being used for memory chips for the computer system.



RAM with read-only memory (ROM).

ROM permanently stores data within the memory chips and is not volatile

- ❑ The contents of RAM may include artifacts of what is or has occurred on the system. This can include the following:
- Configuration information
  - Typed commands
  - Passwords
  - Encryption keys
  - Unencrypted data
  - IP addresses
  - Internet history
  - Chat conversations
  - Emails
  - Malware

- What happens if you are not the investigator on the scene when the digital evidence is collected in the RAM, and they do not collect volatile data?
- Is it possible to still access the RAM, despite having the system shut down?
- While you cannot analyze the RAM, it is possible to examine other sources may contain the same data that was stored in the RAM.
- This option may not always be available, depending on the specific set of circumstances surrounding the seizure of the digital evidence.

- **Hibernation file (hiberfil.sys):** Hibernation is the process of powering down the computer while still maintaining the current state of the system.
- In Windows, the RAM is compressed and stored in a **hiberfil.sys** file.
- This will allow the system to power down completely, but when the system is reactivated, the contents of the **hiberfil.sys** file will be placed back into RAM.

- Depending on the size of the RAM installed on your PC, the hiberfil.sys file might consume from a few hundred MBs to GBs. Generally, the hiberfil.sys file's size is roughly about 30-70% of the size of the RAM on your PC.
- Hibernation is a fantastic feature as you can turn off your PC without actually shutting down your PC and closing all running programs. The hibernation feature is entirely different from the sleep mode.
- When analyzing the **hiberfil.sys** file, the last modification date/timestamp will show when the contents of RAM was added to the file.

- **Pagefile (pagefile.sys):** Paging is a method of storing/retrieving data being used in the RAM chips with a virtual memory file stored on a traditional storage device.
- **Swapfile (swapfile.sys):** The Swapfile was created so that the operating system can use it for paging operations with suspended Metro/modern Windows applications.
- **Crash dump (memory.dmp):** If you have used any version of Microsoft Windows, you might have experienced a system crash or a blue screen of death (BSOD). When that occurs, it may create a dump of memory to store information about the state of the system at the time of the crash.

- When the decision is made to capture the RAM from the system, several factors need to be considered before moving forward.
- The most significant issue is that you will be changing the state of the system when you collect the volatile data.

The Scientific Workgroup on Digital Evidence (SWGDE) has explored the collection of volatile data and offers the following considerations:

- The application used to collect the data in memory will overwrite some contents of the memory.
- The larger the tool and associated files are, the more data it overwrites.
- The system may load the USB device driver into memory.
- The system may load the USB device driver into the registry.

❑ To successfully image the RAM, you will need three things:

- A capturing device (such as a USB device)
- Access to the system
- Administrator privileges

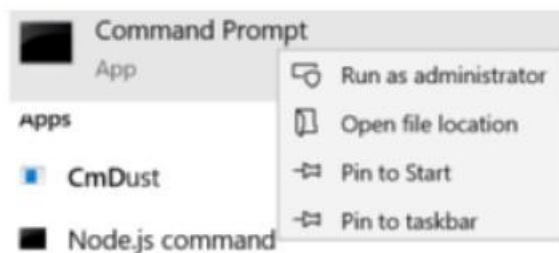
- The amount of RAM installed on the system will dictate the size of your external storage device.
- If the system has 16 GB of RAM, your external storage device will need to be greater than 16 GB.
- The memory dump will be the same size as the amount of installed RAM.

## Using **Dumplt** tool

1. Insert your thumb drive into the target host.
2. Type `cmd`



3. Right-click on **Command Prompt** so that you can run it as an administrator



## Exploring RAM capture tools

- 4. Once the Command Prompt comes up, navigate to the folder on your USB device that contains the executable. You will then type in the **cmd** command and execute it.
- 5. The system will then present you with a screen showing the amount of physical memory and the amount of space on the device. It will then ask you if you want to continue. Select **yes**

```
P:\Dumpit>dumpit
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      34883502080 bytes ( 33267 Mb)
Free space size:         125729640448 bytes ( 119905 Mb)

* Destination = \??\P:\Dumpit\FORENSIC-20190820-202139.raw

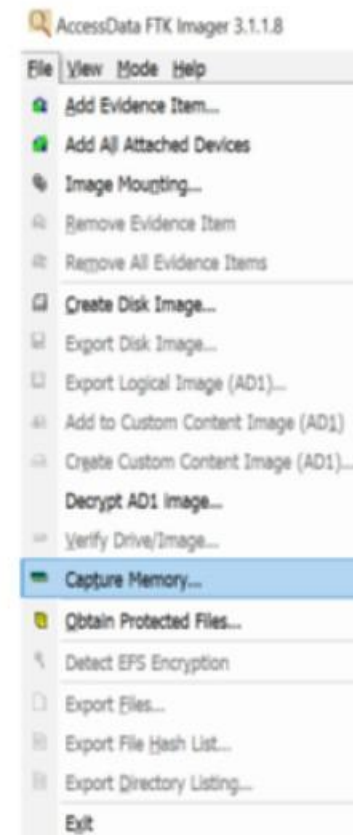
--> Are you sure you want to continue? [y/n] _
```

- 6. The amount of RAM installed will dictate the amount of time it will take to create the dump of the RAM. Once the process has been completed, the program will notify you that it was successful

```
* Destination = \\P:\Dumpit\FORENSIC-20190820-202139.raw  
--> Are you sure you want to continue? [y/n] y  
+ Processing... Success.
```

## FTK Imager

1. Insert your thumb drive into the target host.
2. If File Explorer does not automatically launch, use the Windows + E keyboard shortcut to open it.
3. Launch FTK Imager, left-click on File, and select Capture Memory..., as shown in the following screenshot



- Bulk Extractor
- Volix II



**Thank You**