Capgemini

Module 7 – Hardware

Module Learning Objectives

Upon completion of this module, the student should be able to do the following:

- Understand how volatile memory works and how it can be used to benefit network forensics.
- Understand how the Windows file system and architecture works and what files and logs are provided for forensic analysis.
- Understand how both mechanical and solid-state hard drives work and how information can be captured and analyzed.
- Understand what tools are available to capture and analyze host information.

Memory

Capgemini

Agenda

Volatile Memory | Collection Tools | Virtual Memory

Topic Learning Objectives

Upon completion of this topic, the student should be able to do the following:

- Understand volatile memory.
- Understand the forensic importance of memory.
- List the tools that can be used to study memory artifacts.
- Understand how computers use memory and how it impacts the operation of a system.

Forensic Collection of Information

- Memory collections are forensically essential and should be conducted as quickly as possible.
- Other collections should be conducted in order of likelihood of being lost.
- Memory collection should be the primary priority of a forensics investigator.

Why Memory Collection is Essential

What is contained in a memory capture?

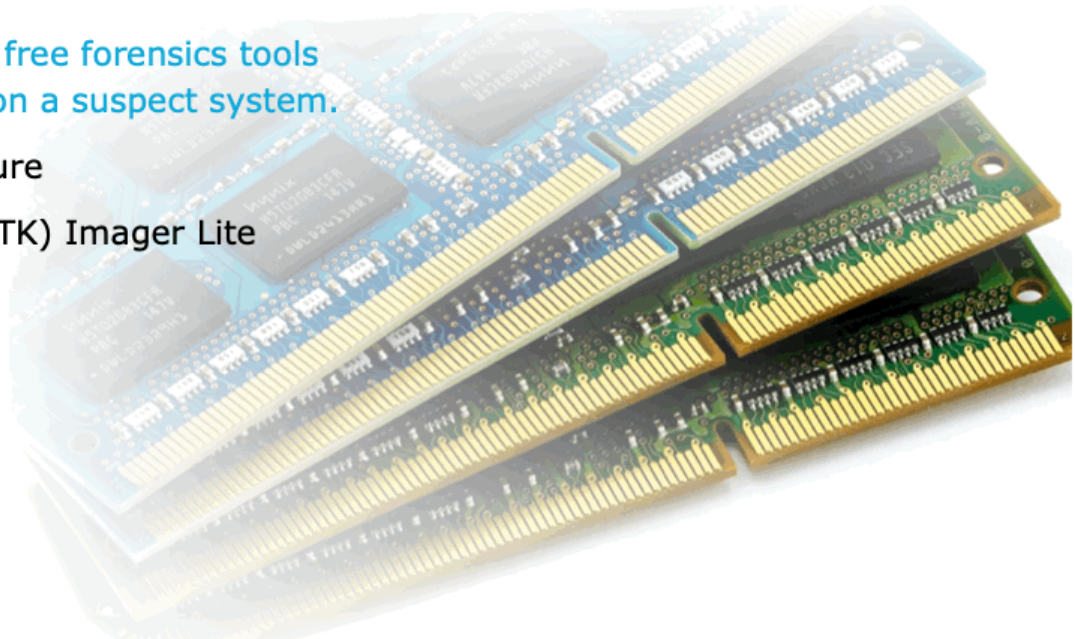
- Processes running
- Ephemeral data and commands being run
- Passwords, both hashed and cleartext
- Registry Keys
- Concurrent Transmission Control Protocol (TCP)/Internet Protocol (IP) connections
- Information not found anywhere else

Since memory cannot be captured when the machine is off, all memory captures have to be conducted while the system is active. Capturing memory will cause some changes of data on the hard disk.

Collection Tools

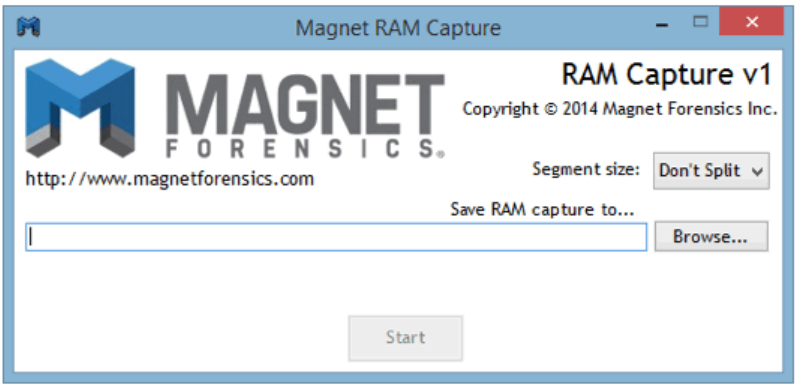
There are dozens of free forensics tools for examining data on a suspect system.

- Magnet RAM Capture
- Forensic Toolkit (FTK) Imager Lite
- Volatility



Magnet RAM Capture

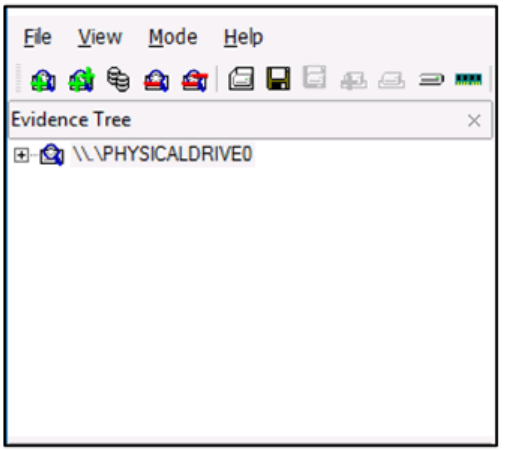
Magnet RAM Capture is a free imaging tool designed to capture the physical memory of a suspect's computer, allowing investigators to recover and analyze valuable artifacts that are often only found in memory.



FTK Imager Lite

Capabilities:

- Create Forensics Images
- Preview Files and Folders
- Preview File Contents
- View the Image (read-only or live)
- Export Files
- Create Hashes
- Generate Hash Reports



Memory Analysis

Now that we have a capture, how do we get information from it?

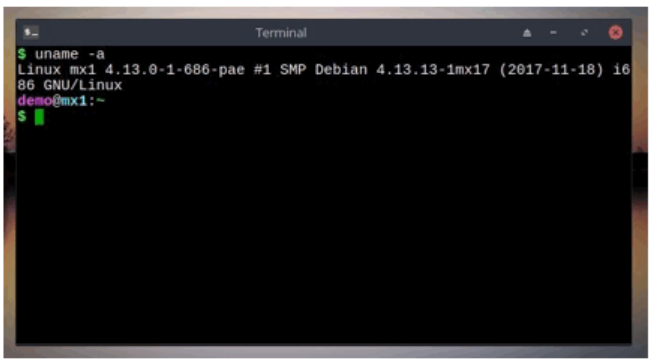
Following are ways to get information from the capture:

- Use "strings" and "grep" for analysis.
- Use tools, such as Volatility, to analyze the capture.

Manual Analysis

Linux command-line tools, such as strings and grep, can be used if there is specific information that is being gathered.

Also use proximity searches that will allow finding information that is close to the keyword in the file.



Volatility Framework

Volatility

Volatility is a collection of Python-based tools that can be used to find artifacts in a memory capture.

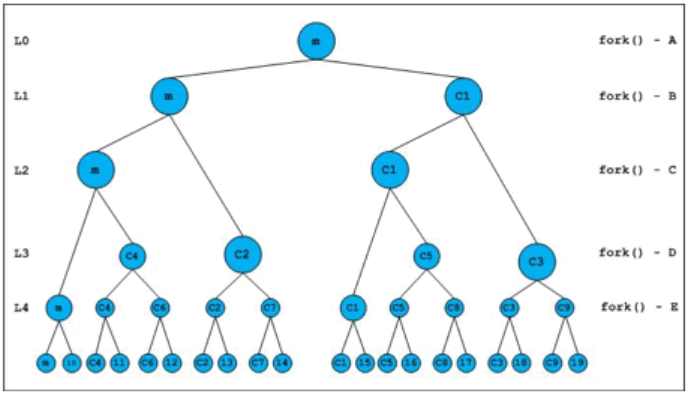
```
REMNUX volatility # python vol.py sockets -f /home/michael/stuxnet.vmem
Volatility Foundation Volatility Framework 2.3.1
Offset(V)     PID   Port  Proto Protocol        Address         Create Time
---------- ------ ------ ------ --------------- --------------- -----------
0x81dc2008    680    500     17 UDP             0.0.0.0         2010-10-29 17:09:05 UTC+0000
0x82061c08      4    445      6 TCP             0.0.0.0         2010-10-29 17:08:53 UTC+0000
0x82294aa8    940    135      6 TCP             0.0.0.0         2010-10-29 17:08:55 UTC+0000
0x821a5008    188   1025      6 TCP             127.0.0.1       2010-10-29 17:09:09 UTC+0000
0x81cbJd70   1080   1141     17 UDP             0.0.0.0         2010-10-31 16:36:16 UTC+0000
0x81da4d18    680      0    255 Reserved        0.0.0.0         2010-10-29 17:09:05 UTC+0000
0x81fdbe98   1032    123     17 UDP             127.0.0.1       2011-06-03 04:25:47 UTC+0000
0x81c79778   1080   1142     17 UDP             0.0.0.0         2010-10-31 16:36:16 UTC+0000
0x81e20898   1200   1900     17 UDP             127.0.0.1       2011-06-03 04:25:47 UTC+0000
0x82060008    680   4500     17 UDP             0.0.0.0         2010-10-29 17:09:05 UTC+0000
0x81cb9e98   1580   5152      6 TCP             127.0.0.1       2010-10-29 17:09:05 UTC+0000
0x81da34b0      4    445     17 UDP             0.0.0.0         2010-10-29 17:08:53 UTC+0000
```

Volatility can extract the following:

- Image properties/time
- Running processes
- Open network connections
- Dynamic Link Libraries (DLLs) and registry processes
- Executable files
- Convert between different file formats
- Local password files

Process Memory (Parsing)

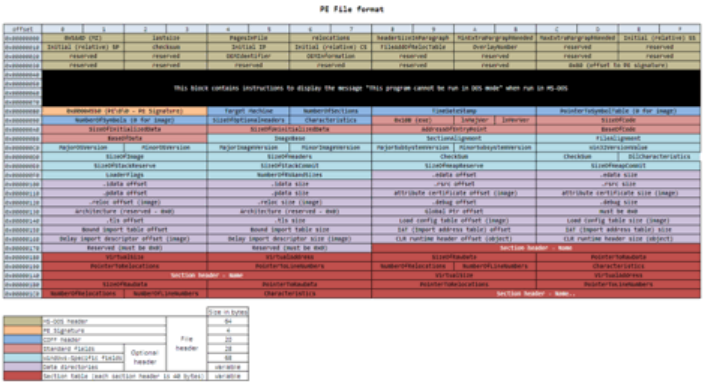
With Volatility, the user can view memory content that is associated with a specific process or child process.



Process Images

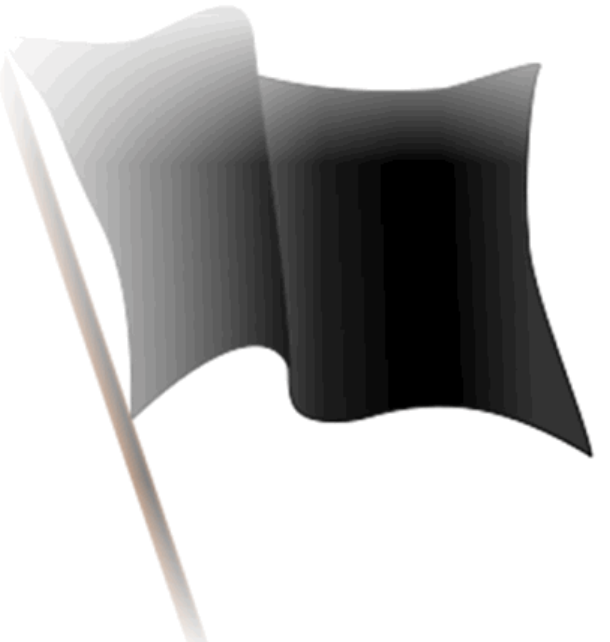
Volatility is capable of extracting .exe images from the memory capture by parsing the file header (Portable Executable [PE]).

The header tells where to locate the information to reconstruct the file.



Process Images (cont.)

Use the procexedump flag to accomplish a capture of malware that may only be resident in memory.

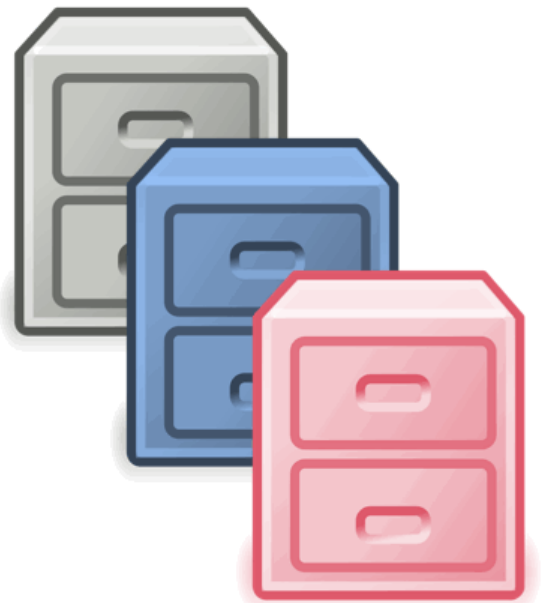


Other Sources of Information

There are other sources of information, besides memory, that can be analyzed.

- Pagefile.sys
- Hiberfil.sys
- Dump Files (.dmp)

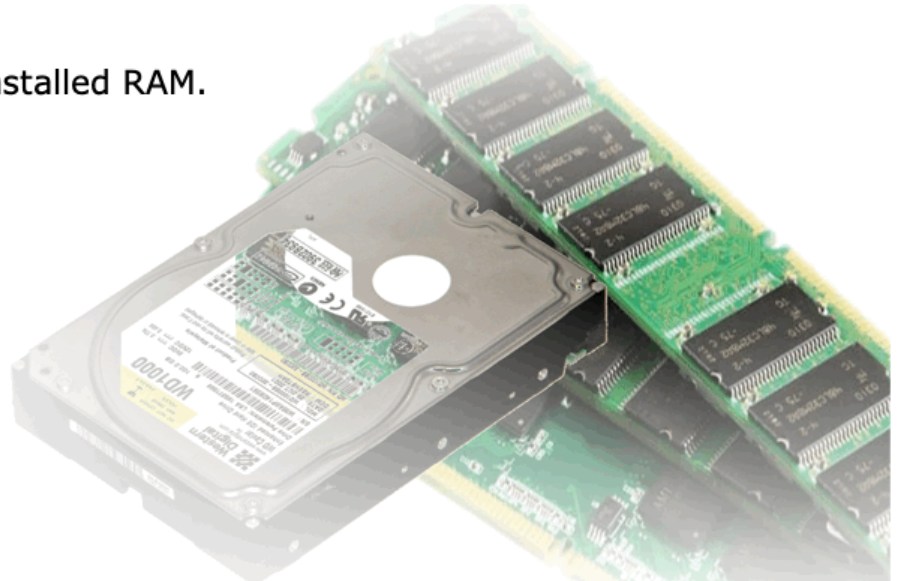
These can be analyzed but should never replace memory.



Paging File (Pagefile.sys)

Pagefile.sys

- Used to supplement the installed RAM.



Hibernation File (Hiberfil.sys)

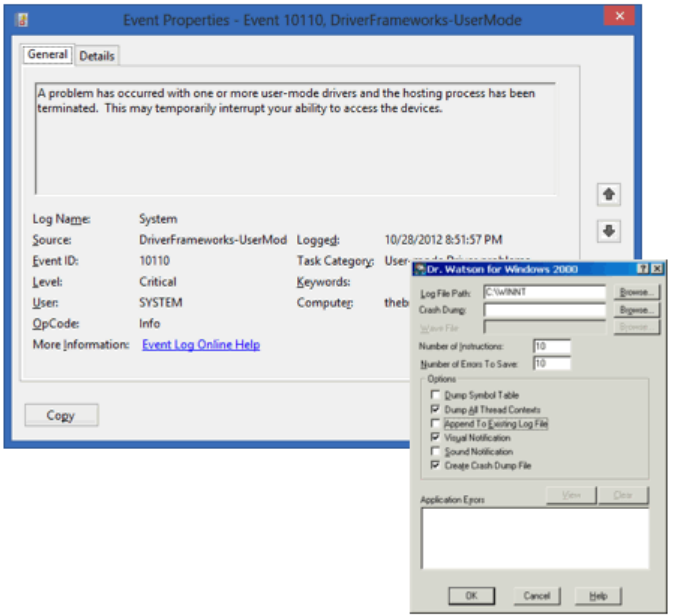
Hiberfil.sys

- Used to take a snapshot of the active state of the system when it is placed in hibernation, or sleep.
- The Hiberfil.sys can be a treasure trove of forensics information.

Dump Files (.dmp)

.dmp (Dump) files

- Created upon application malfunction and crash.
- These crashes can sometimes be due to malicious code.



LAB010: Creating a Forensics Memory Capture

LAB011: Analyzing a Forensics Memory Capture

Questions?

Windows Concepts

Capgemini

Agenda

New Technology File System (NTFS) | File Permissions | Windows Log Files

Topic Learning Objectives

Upon completion of this topic, the student should be able to do the following:

- Describe what the NTFS is and how it works.
- List the logs and system files that will benefit forensics analysis.
- Understand what Autopsy is and how it can be used in file analysis.

Windows NTFS

NTFS, an acronym for New Technology File System, is a file system first introduced by Microsoft in 1993 with the release of Windows NT 3.1.

Scalability

NTFS is optimized for 4 KB clusters but supports a maximum cluster size of 64 KB.

Folder Permissions

Read and Execute – Allows a user to read the contents of a folder and traverse folders

Modify – Allows a user to delete and modify the contents of a folder, and enables Read/Execute and Write permissions

Full Control – Allows a user to modify permissions and to take ownership

Read – Allows a user to see the files and subfolders in a folder and to view folder properties

Write – Allows a user to create new files and folders within the folder, change folder attributes, and view folder properties

List Folder Contents – Allows a user to view the contents of the folder

File Permissions

Modify – Allows a user to modify and delete a file and also allows **Read/Execute** and **Write** permissions

Full Control – Gives the user full control over a file, allowing the user to modify permissions and take ownership

Read – Allows a user to read a file and view its properties

Write – Allows a user to overwrite a file, change attributes, and view ownership and permissions

Read and Execute – Allows a user the right to run applications and read a file

Permission Inheritance

By default, all files and folders inherit permissions from their parent. If Read permission is allowed to the parent folder, all child files and folders below it will also be given Read permission. This is known as Permission Inheritance.

Improvements from Previous Systems

NTFS has several technical improvements over the file systems that it superseded – File Allocation Table (FAT) and High Performance File System (HPFS) – such as improved support for metadata and advanced data structures to improve performance, reliability, and disk space use.

Journaling

NTFS is a journaling file system and uses the NTFS Log ($LogFile) to record metadata changes to the volume.

This is a feature that, from a security standpoint, helps when doing a forensics study of a computer's file system.

Journaling (cont.)

The Update Sequence Number (USN) Journal is a system management feature that records (in $Extend\$UsnJrnl) changes to files, streams, and directories on the volume, as well as their various attributes and security settings.

This can be a great place to generate information on files and when they were changed (for example, by malware).

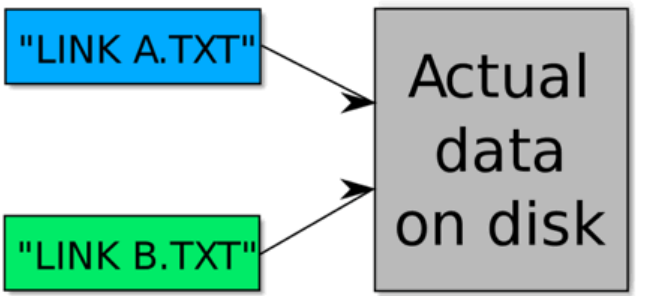
Mon Feb 23 02:32:47 2015	voice#5734223.zip	File_Create	
Mon Feb 23 02:32:58 2015	voice#5734223	File_Create	
Mon Feb 23 02:32:58 2015	voice.exe	File_Create	
Mon Feb 23 02:33:34 2015	testmem.exe	File_Create	
Mon Feb 23 02:33:34 2015	voice.exe	File_Delete	Close
Mon Feb 23 02:33:34 2015	VOICE.EXE-78467D55.pf	File_Create	
Mon Feb 23 02:33:34 2015	TESTMEM.EXE-309E8084.pf	File_Create	

Hard Links

The hard link feature allows different file names to refer directly to the same file contents.

Hard links are similar to directory junctions but refer to files instead.

An NTFS junction point is a symbolic link to a directory that acts as an alias of that directory.



Alternate Data Streams

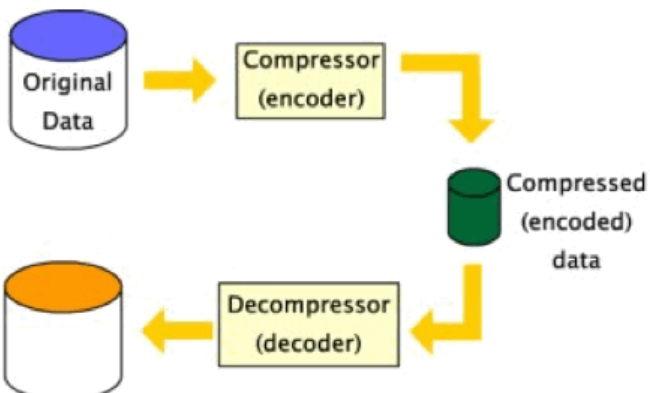
A **stream** is a sequence of data elements made available over time. A stream can be thought of as items on a conveyor belt being processed one at a time rather than in large batches.

NTFS Streams were introduced in Windows NT 3.1. Malware has used alternate data streams to hide code.

As a result, malware scanners and other special tools now check for alternate data streams.

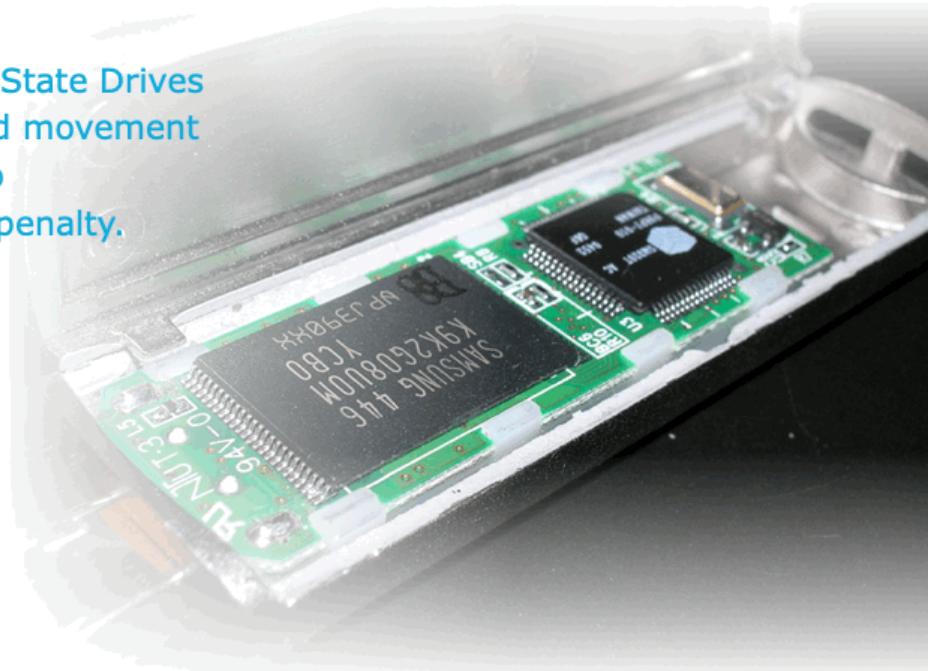
File Compression

NTFS can compress files using LZNT1 algorithm (a variant of LZ77). Files are compressed in 16 cluster chunks. With 4 KB clusters, files are compressed in 64 KB chunks.



Flash Memory

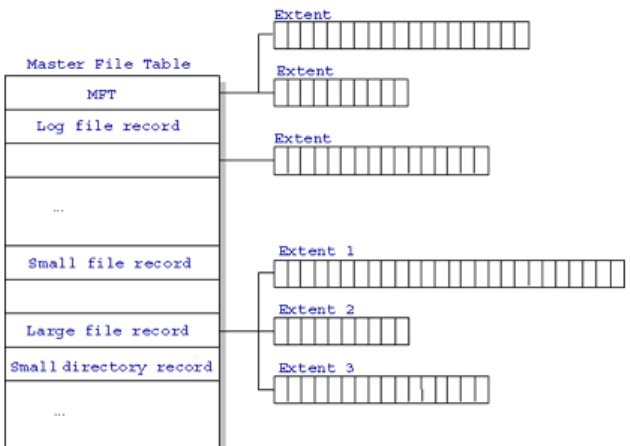
Flash memory, such as Solid State Drives (SSDs), do not have the head movement delays of hard disk drives; so fragmentation has a smaller penalty.



Master File Table (MFT)

The NTFS file system uses the MFT to organize the folders and files on the logical volume.

The MFT also keeps track of the file attributes and documents when the files are created, modified, or accessed.



Windows Logs

Including the following:

- Event Logs
- Browser Logs
- System Logs
- Security Logs

Viewing and Parsing Logs

However, in this class, we will be using an extremely effective tool called Autopsy.

There are several tools used to view and parse logs.

- Autopsy
- TZWorks
- EnCase
- FTK Imager
- Log2timeline

Windows has integrated tools for viewing logs (eventvwr), but there are also free ware and paid tools for doing analysis.

Questions?

Hard Disk Drives

Capgemini

Agenda

Mechanical Drives | Solid State Drives (SSDs) | File Storage Concepts | Information Storage

Topic Learning Objectives

Upon completion of this topic, the student should be able to do the following:

- Understand how mechanical and solid state hard drives operate.
- Understand how Windows uses the hard disk and how logical drives work.
- Understand how forensics analysis can benefit or suffer from the operational characteristics of different types of drives.

Hard Disk Drives

The IBM 305 RAMAC was the first commercial computer that used a moving-head hard disk drive.

Hard Disks

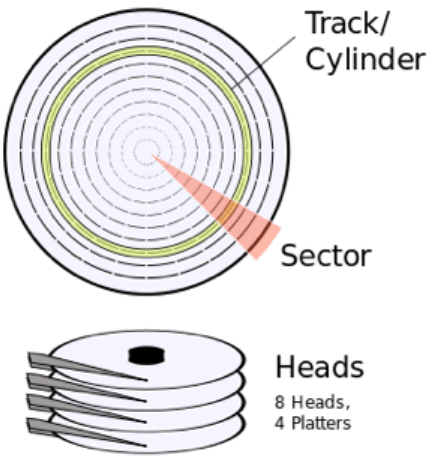
Physical Data Storage

- Store information in 1s and 0s, otherwise known as binary, each known as a bit

Mechanical Hard Disks

Hard disks are arranged into cylinders, heads, and sectors.

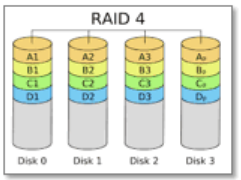
Each sector is typically 512 bytes.

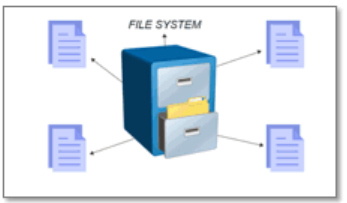


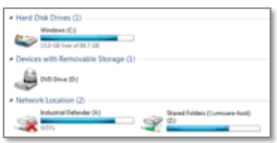
Information Storage

KB – Kilobyte	KB – 1024 bytes
MB – Megabyte	MB – 1024 KB
GB – Gigabyte	GB – 1024 MB
TB – Terabyte	TB – 1024 GB
PB – Petabyte	PB – 1024 TB
EB – Exabyte	EB – 1024 PB
ZB – Zettabyte	ZB – 1024 EB
YB – Yottabyte	YB – 1024 ZB

Logical Drives







File System

Logical Volumes

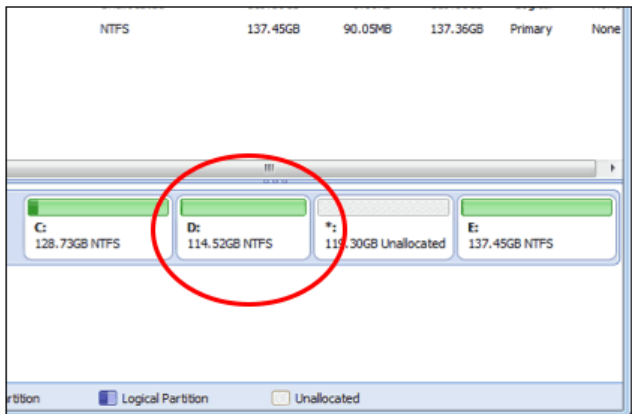
Partitions

Physical Device

Logical Volume =  **+** 

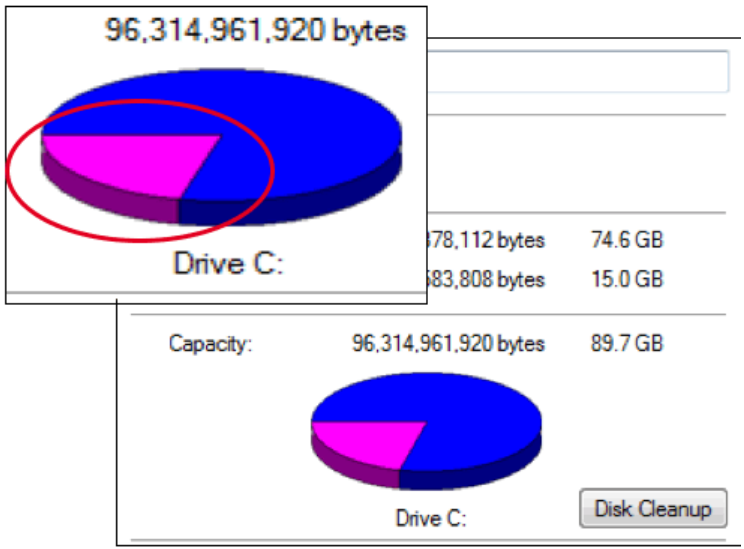
Unallocated Space

Unallocated space is different from unused space.



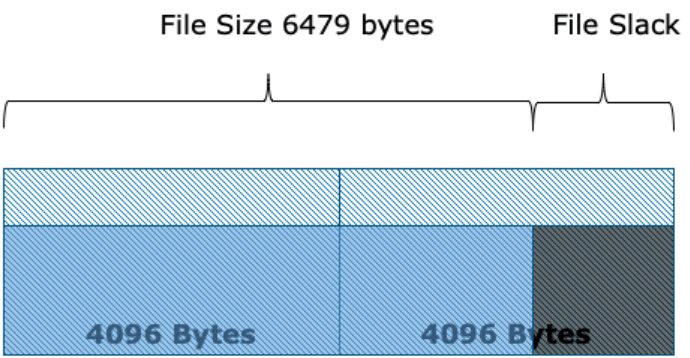
Unused Space

Unused space is an area of a volume that is not currently being used by the file system.



File Slack – Mechanical Drive

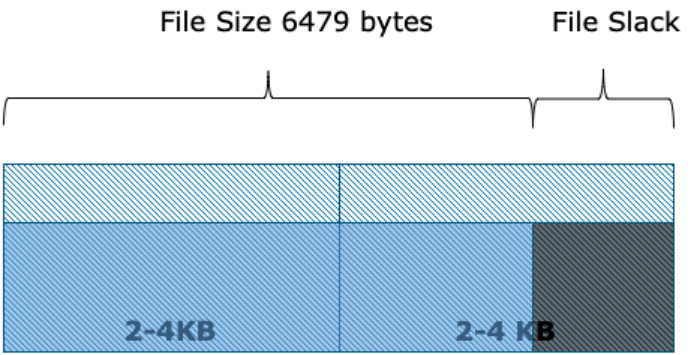
The space between the end of a file and the end of the disk cluster it is stored in, also called "file slack"



File Slack – Solid State

The space between the end of a file and the end of the disk cluster it is stored in, also called "**file slack**"

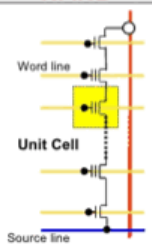
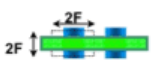
For SSDs, this is still true; but it is forensically useless…



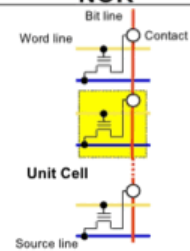
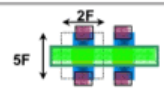
Solid State Drives (SSDs)

Unlike mechanical hard drives, which contain spinning platters and turntable-like arms bearing read-write heads, flash-memory devices have no mechanical parts.

Types of Solid State Memory

	NAND
Cell Array	
Layout	
Cross-section	
Cell size	$4F^2$

Cell Array
Layout
Cross-section
Cell size

NOR



$10F^2$

Mechanical vs. Solid State

As always… there is a downside…

SSDs will eventually "rot" into a read-only state.

Questions?

Autopsy and FTK Imager

FAST
FOUNDATIONAL ANALYST SECURITY TRAINING

Capgemini

Agenda

Autopsy Purpose | FTK Imager Purpose

Topic Learning Objectives

Upon completion of this topic, the student should be able to do the following:

- Understand how FTK Imager is used to capture an image of a hard drive.
- Understand how Autopsy is used to perform drive analysis.

FTK Imager

What is FTK Imager?

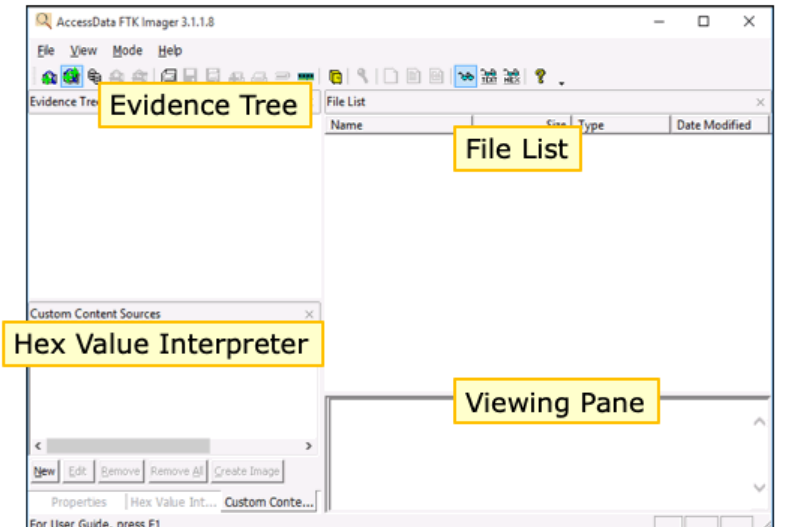
- The AccessData Forensic Toolkit (FTK) includes a stand-alone disk imaging program called FTK Imager, which we will be using in this class.
- FTK Imager is a simple tool but a powerful one. It saves an image of a hard disk in one file or in segments that may be reconstructed later.
- It calculates Message Digest 5 (MD5) hash values and confirms the integrity of the data before closing the files. The result is an image file(s) that can be saved in several formats, including DirectDraw (DD) raw.

FTK Imager (cont.)

FTK Imager Interface

There are four panes in the FTK Imager view.

- Evidence Tree
- Hex Value Interpreter
- File List
- Viewing Pane



Autopsy by Sleuth Kit

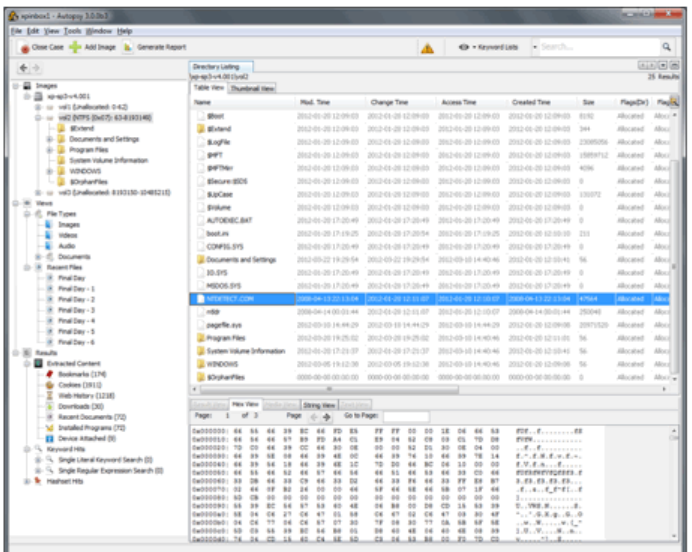
What is Autopsy?

- Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools.
- It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer.
- It can even be used to recover photographs from a camera's memory card.

Autopsy by Sleuth Kit (cont.)

Easy to Use

- Autopsy was designed to be intuitive out of the box.
- Installation is easy, and wizards guide every step.
- All results are found in a single tree.



Autopsy by Sleuth Kit (cont.)

Extensible

Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from third parties.

Some of the modules provide the following:

Timeline Analysis	Advanced graphical event viewing interface (video tutorial included)
Hash Filtering	Flag known bad files, and ignore known good
Keyword Search	Indexed keyword search to find files that mention relevant terms
Web Artifacts	Extract history, bookmarks, and cookies from Firefox, Chrome, and Internet Explorer (IE)
Data Carving	Recover deleted files from unallocated space using PhotoRec
Multimedia	Extract Exchangeable Image File (EXIF) from pictures and watch videos
Indicators of Compromise	Scan a computer using Structured Threat Information Expression (STIX)

LAB012: Creating a Forensics Hard Drive Capture

LAB013: Analyzing a Forensics Hard Drive Capture

Questions?

People matter, results count.

About CapGemini

A global leader in consulting, technology services and digital transformation, CapGemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, CapGemini enables organizations to realize their business ambitions through an array of services from strategy to operations. CapGemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.

Learn more about us at

www.capgemini.com