
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
TM
Capgemini
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 1

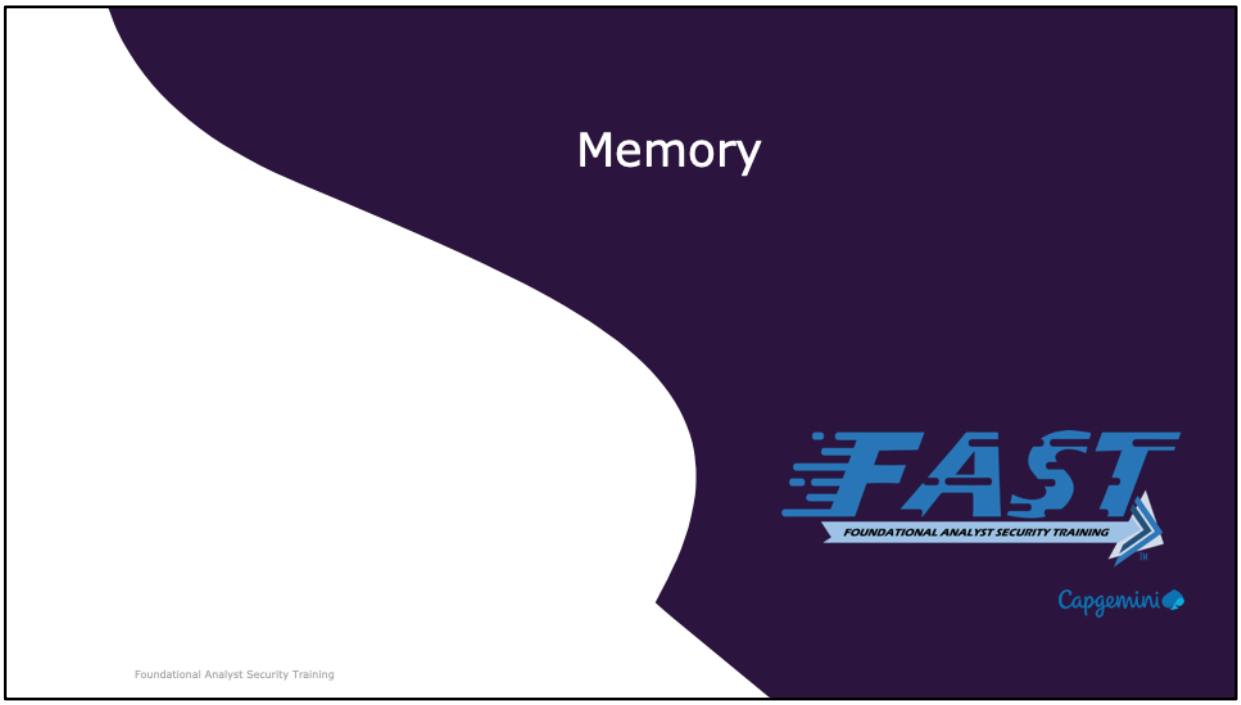
Module 7 – Hardware

Capgemini

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.



In this section, we will cover Memory and how volatile memory operates, and how information stored in memory can inform a forensics investigation.

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.

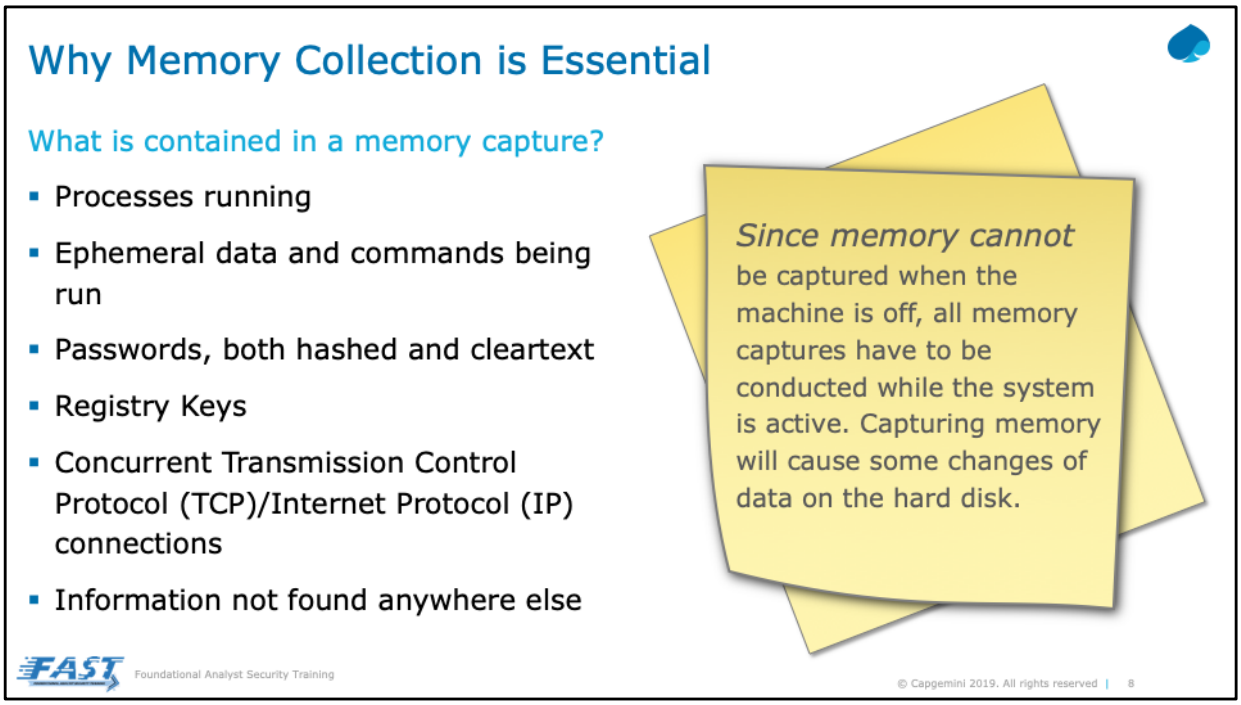
Forensic Collection of Information

- 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.

FAST Foundational Analyst Security Training

Memory collections should be done in the following order:

- Running Memory
- Network Connections and router information
- Any processes running on the processor
- System Logs and files
- Hard Disks



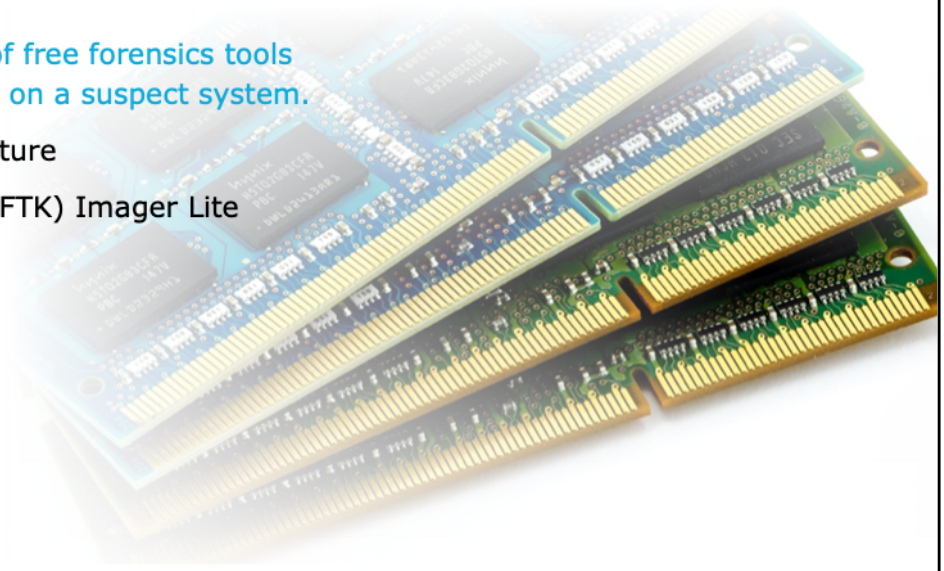
There is a lot of valuable information contained in a memory capture, including:

- Processes running
- Ephemeral data and commands being run
- Passwords both hashed and clear text
- Registry Keys
- Concurrent TCP/IP Connections
- Information not found anywhere else

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



FAST Foundational Analyst Security Training

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

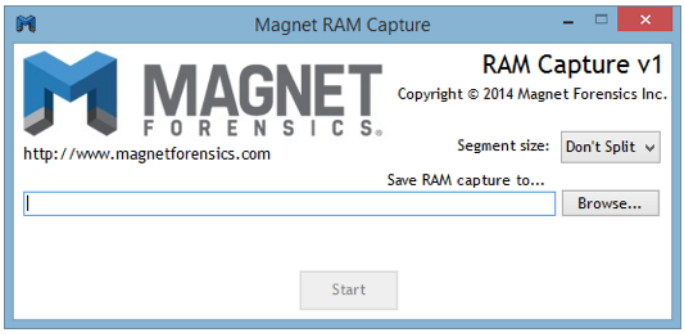
Magnet & FTK Imager Lite – Are both free memory capture tools that use a GUI interface to capture active memory on a suspect machine

dc3dd & Dumpit – Are both open-source forensic memory capture tools used to capture information from memory from a Linux Command line.

–

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.



FAST Foundational Analyst Security Training

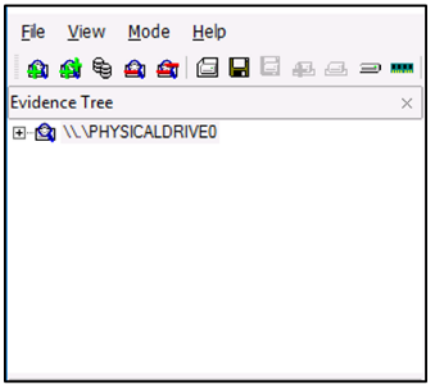
Magnet RAM Capture has a small memory footprint, meaning investigators can run the tool while minimizing the data that is overwritten in memory. Export captured memory data in Raw (.DMP/.RAW/.BIN) format and easily upload into leading analysis tools including, Magnet AXIOM and Internet Evidence Finder.

Evidence that can be found in RAM includes process and programs running on the system, network connections, evidence of malware intrusion, registry hives, username and passwords, decrypted files and keys, and evidence of activity not typically stored on the local hard disk.

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



FAST Foundational Analyst Security Training

FTK® Imager is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence. After you create an image of the data, use Forensic Toolkit® (FTK®) to perform a thorough forensic examination and create a report of your findings.

FTK imager does not compress memory, like other tools, if you have 8GB of memory then you need 8GB of space to store the memory. Using a usb formatted in FAT it will not be able to hold RAM bigger than 4GB you need to use FAT64, XFAT or NTFS. FTKImager can also be run from a USB device so you do not have to install it on a computer that you need to get the RAM from

Mention that FireEye HX, EnCase Enterprise, FTK Enterprise, and many End Point tools such as End Game can get memory images for analysis.

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.

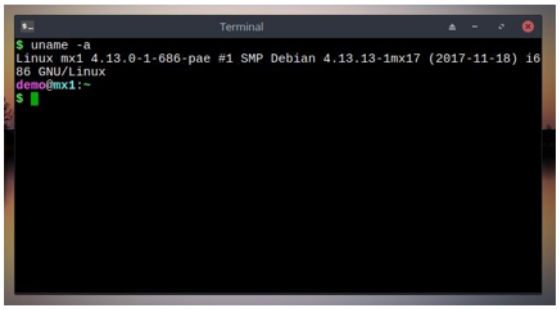
Now that we have our capture, what do we do with it?

There are several ways to get information from the capture, you can use "strings" and "grep" for analysis, or you can use tools to analyze the capture like Volatility.

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.



Some common items that are often searched for: host or machine names, specific commands, domain names, IP Addresses, email addresses, executed or running processes, usernames, etc.

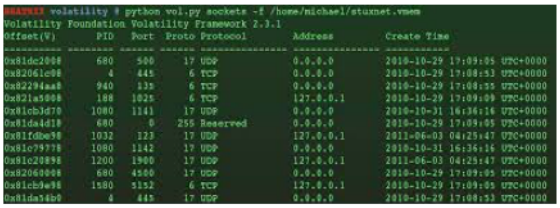
The problem with a manual analysis, is it lacks context to what the information referred too and may be unrelated, and many times attackers will encode or hash information to prevent its discovery.

This type of analysis is time intensive, and often ineffective without other tools.

Volatility Framework

Volatility

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



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

FAST Foundational Analyst Security Training

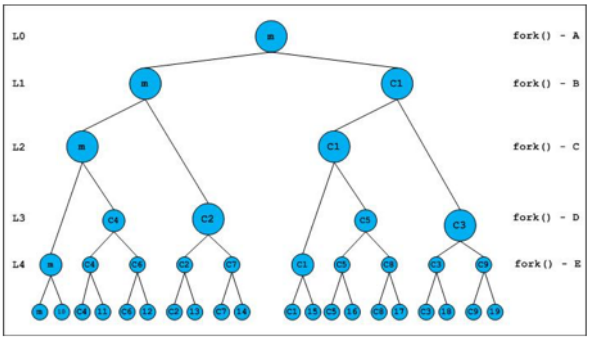
Volatility is a collection of python based tools that can be used to find artifacts in a memory capture.

Volatility can extract:

- Image properties / time
- Running processes
- Open network connections
- DLL's 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.

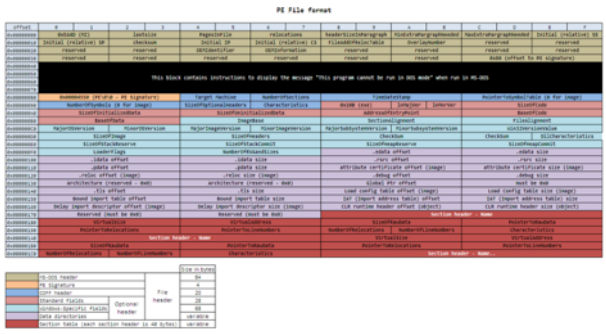


With Volatility the user can view memory content that is associated with specific process or child process. This allows the user to examine suspect process strings, and view the information as either ASCI text or UNICODE.

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.



FAST Foundational Analyst Security Training

 | 16

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

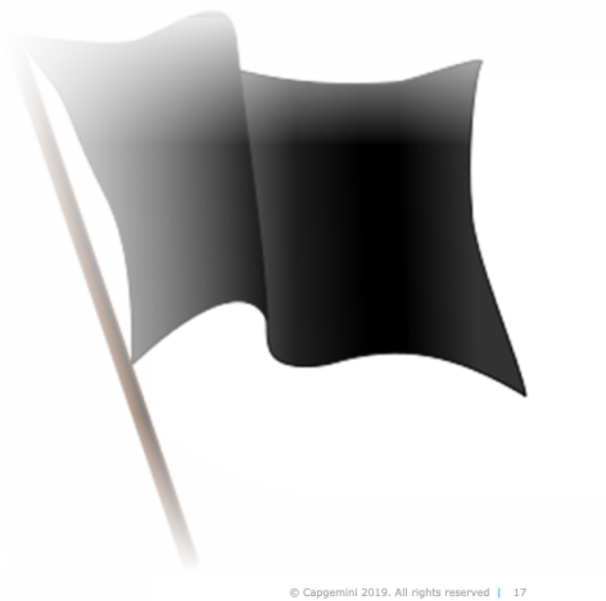
The header tells where to locate the information to reconstruct the file.

Also, note that the .exe may be altered during this process.

The exe files usually cannot be run when extracted, you have to use additional tools to alert the malware and make it run on a disk. It is using virtual addresses and you need to give it physical addressing and other things.

Process Images (cont.)

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



FAST Foundational Analyst Security Training

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

This is very useful for analysis of malware. Malware can be resident only in memory, and this process is the only way to find it. Always be aware of your security measures when pulling malware from memory.

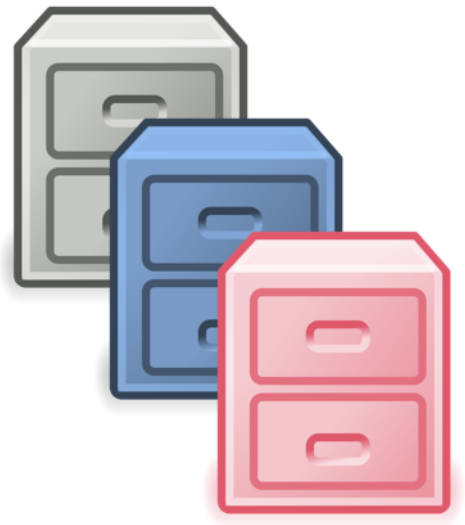
The exe files usually cannot be run when extracted, you have to use additional tools to alert the malware and make it run on a disk. It is using virtual addresses and you need to give it physical addressing and other things.

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.



FAST Foundational Analyst Security Training

There are other sources of information besides memory that can be analyzed, such as:

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

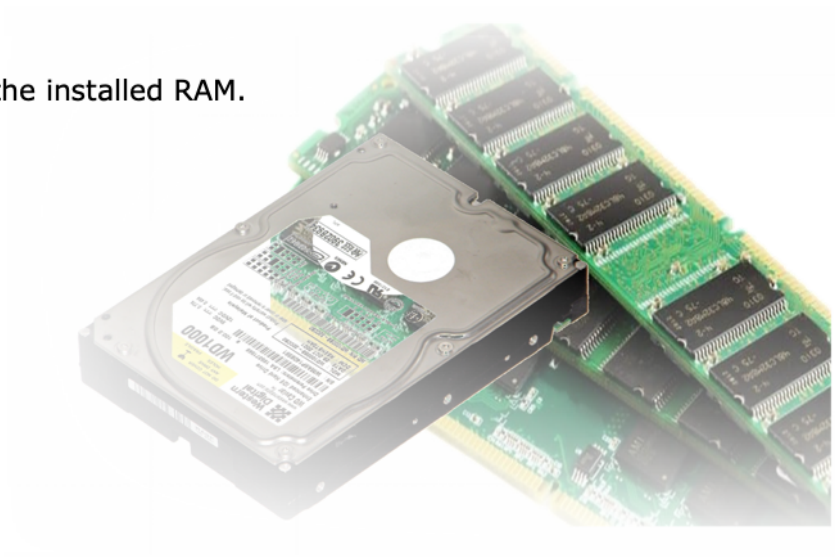
These can be analyzed, but should never replace memory.

You can use the same memory analysis tools to analyze these files either manually or using Volatility.

Paging File (Pagefile.sys)

Pagefile.sys

- Used to supplement the installed RAM.



FAST Foundational Analyst Security Training

The Paging file is used by windows as virtual memory to supplement the installed Ram. Consider a table (memory) in a large library (hard drive). If you had to go get one book at a time every time you wanted to do research it would be time consuming. It would be much easier to get all the books you need and bring them to the table (memory), the paging file is like a second table.

you are not allocating the virtual memory, it is allocated by the OS, you can only say how big you are willing to let it be, not where it is.

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.

FAST Foundational Analyst Security Training

Hiberfil.sys is used to take a snapshot of the active state of the system when it is placed in hibernation, or sleep.

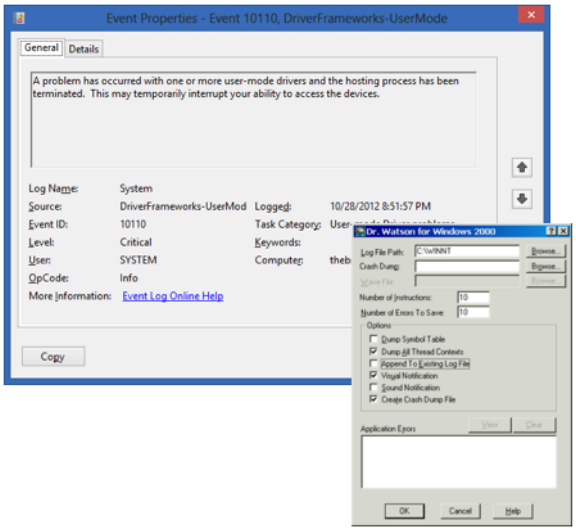
The Hiberfil.sys can be a treasure trove of forensic information.

hiberfil.sys is only memory not other things. It sets aside a specific space on the hard drive and it only uses that space, and nothing else does.

Dump Files (.dmp)

.dmp (Dump) files

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

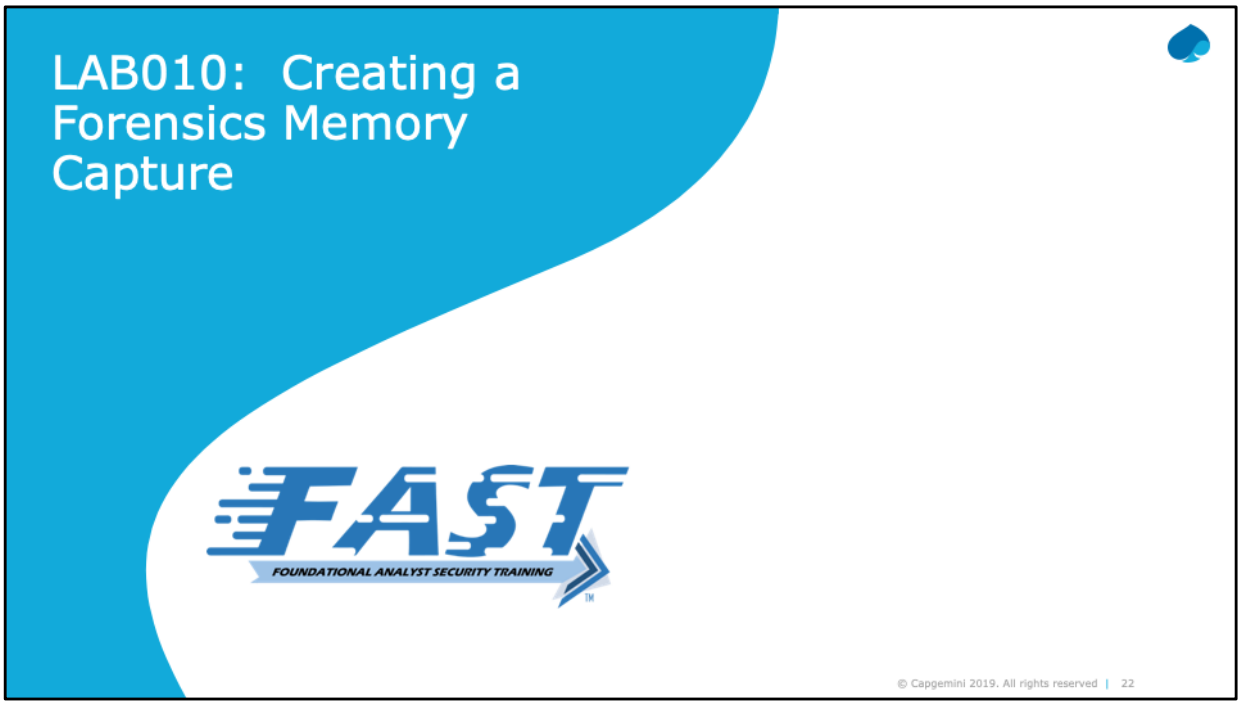


FAST Foundational Analyst Security Training

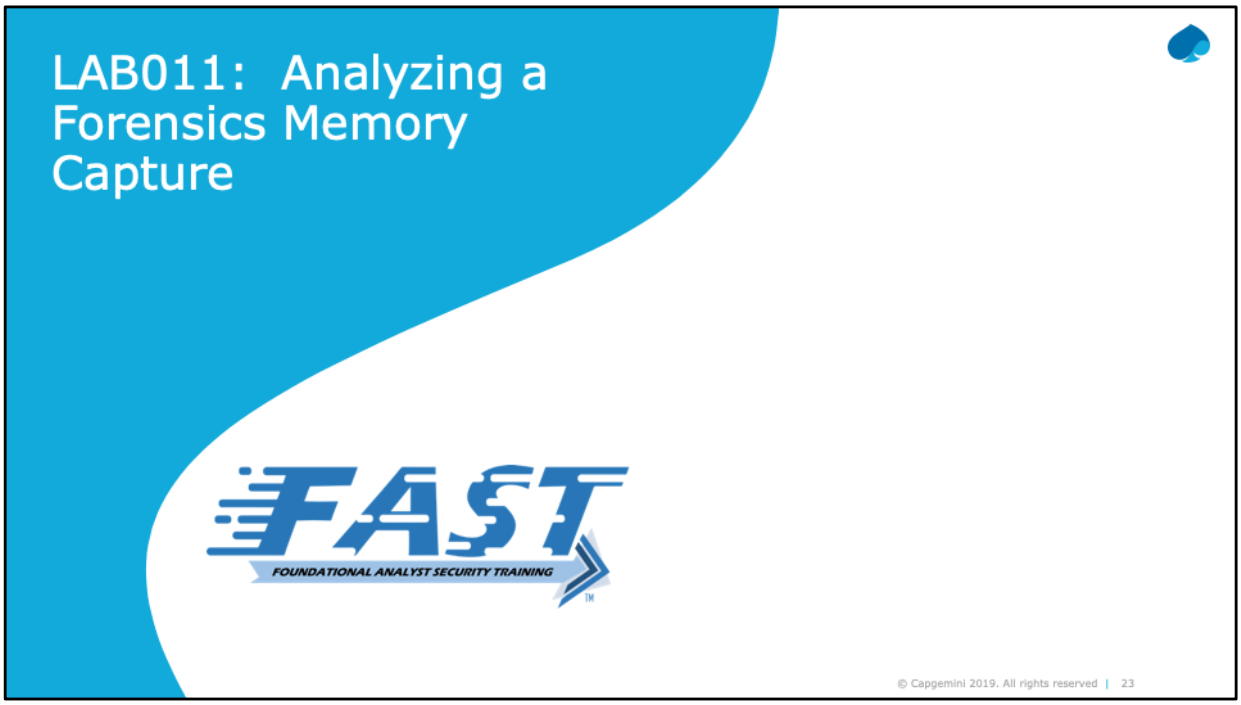
The .dmp (Dump) files are created upon application malfunction and crash.

These crashes can sometime be due to malicious code.

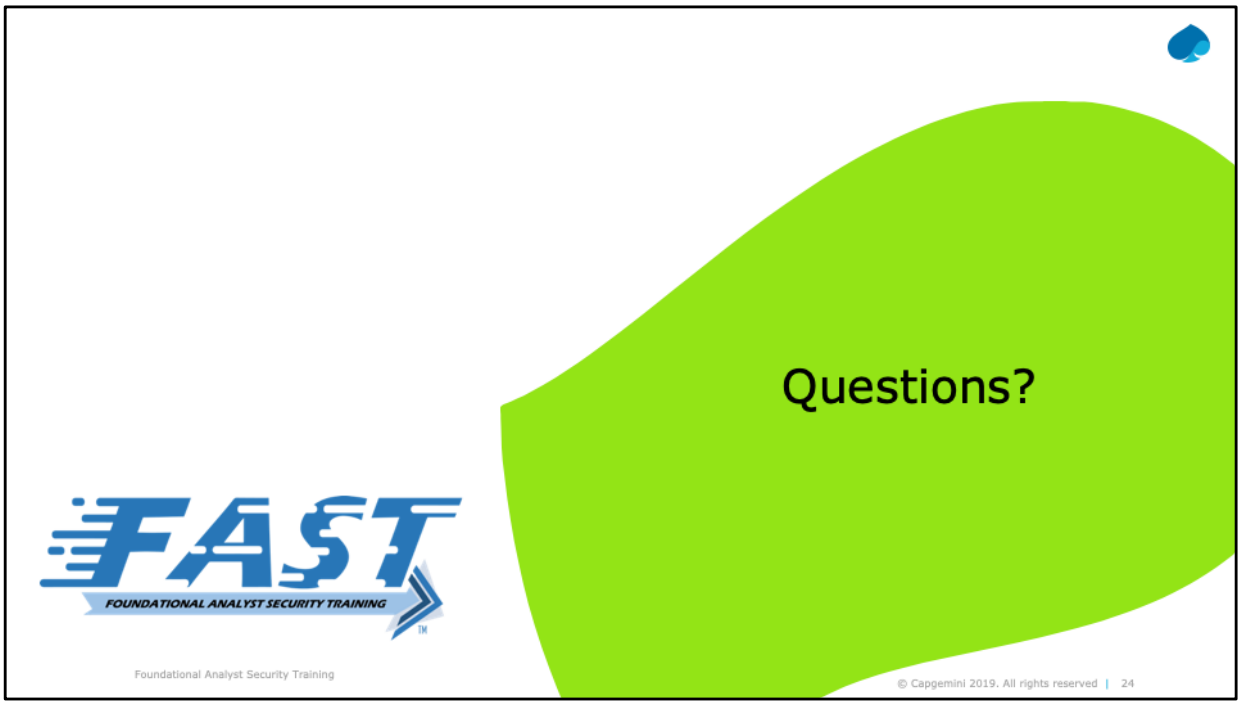
dr. watson usually creates these files. Now only process memory is captured instead of the entire memory of the system.

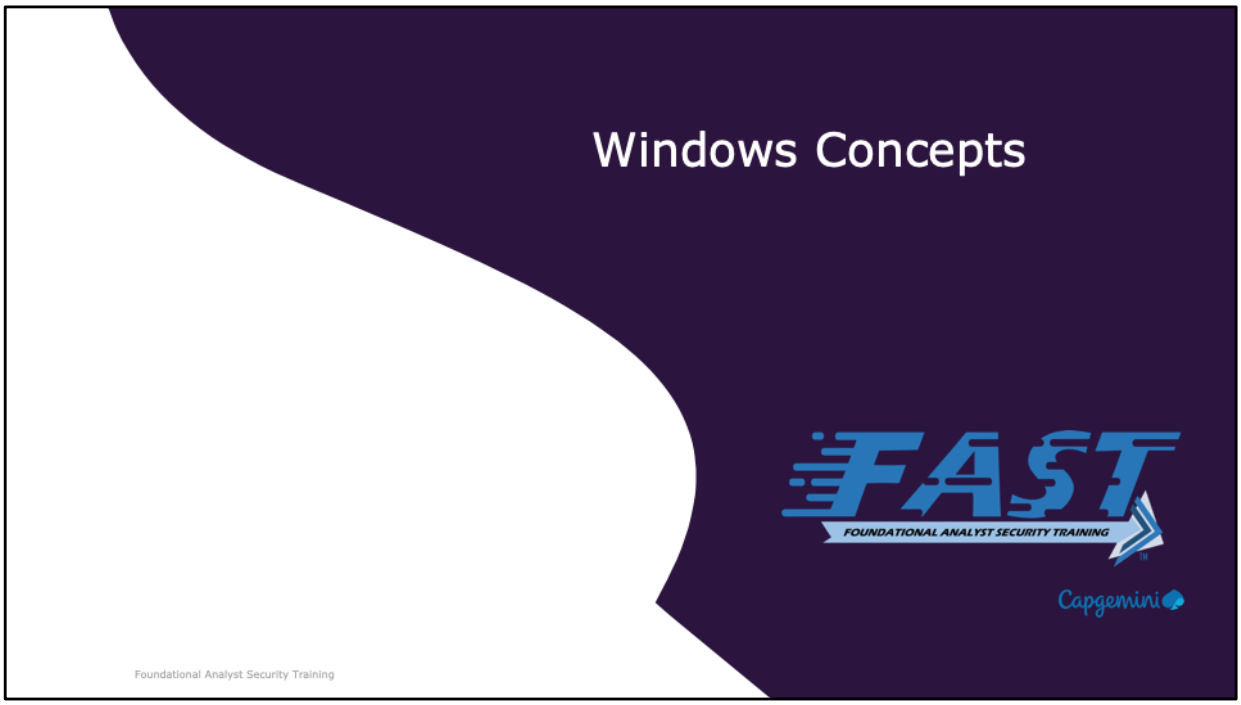


Content Source:



Content Source:


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 24



This section will cover basic Windows concepts and how the Microsoft Windows environment stores, retrieves and processes information, and how that information can be useful to a Tier 1 SOC Analyst.

Content Source:

https://www.lifewire.com/ntfs-file-system-2625948

https://www.free-online-training-courses.com/ntfs-security/

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.

FAST Foundational Analyst Security Training

Instructor Notes:

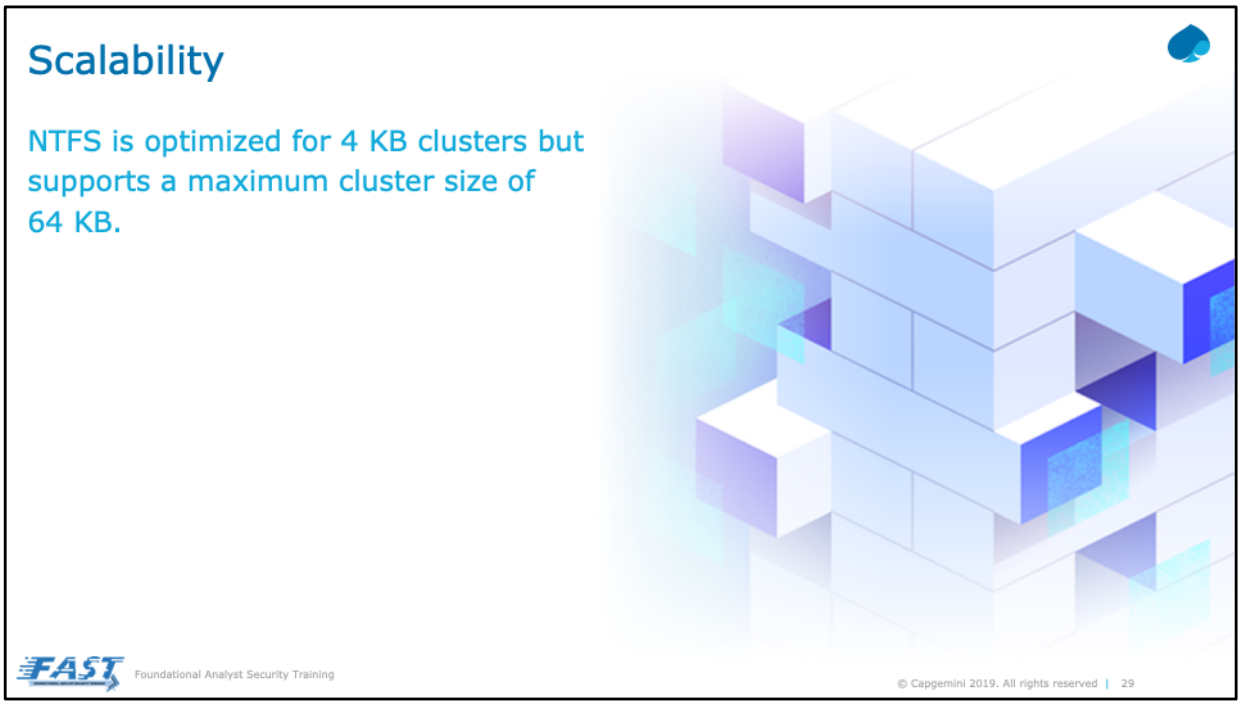
NTFS, an acronym that stands for *New Technology File System*, is a file system first introduced by Microsoft in 1993 with the release of Windows NT 3.1.

NTFS is the primary file system used in Microsoft's Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, and Windows NT operating systems.

The Windows Server line of operating systems also primarily use NTFS.

Theoretically, NTFS can support hard drives up to just under 16 Exabytes. Individual file size is capped at just under 256 Terabytes, at least in Windows 8 and Windows 10, as well as in some newer Windows Server versions.

An EB would take **763 billion floppy disks** or **1.5 billion CD-ROM discs**



The maximum NTFS volume size that the specification can support is $2^{64} - 1$ clusters, but not all implementations achieve this theoretical maximum.

Every file must be allocated an integer number of clusters.
A cluster is the smallest unit of disk space that can be allocated to a file, which is why clusters are often called allocation units.
Wasted space is part of the process. If a volume uses clusters that contain 8,192 bytes, an 8,000 byte file will use one cluster, or 8,192 bytes on the disk. On the other hand, a 9,000 byte file will use two clusters, or 16,384 bytes on the disk.
Cluster size is an important consideration when setting up a hard disk so as to ensure that you maximizing the efficiency of the disk. Larger cluster sizes result in more wasted space because files are less likely to fill up an integer number of clusters.

Folder Permissions

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

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

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

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

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

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

FAST Foundational Analyst Security Training

Folder permission include:

- 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.
- 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.

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

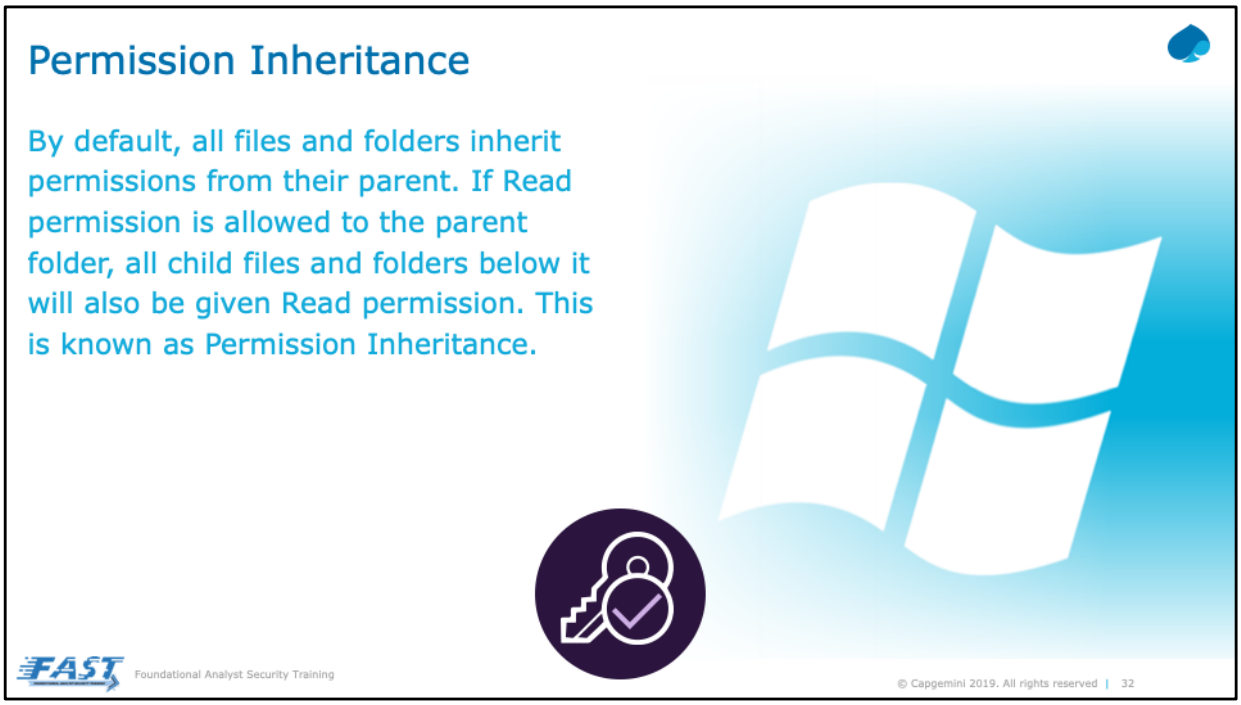
Write – Allows a user to overwrite a file, change attributes, and view ownership and permissions

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

FAST Foundational Analyst Security Training

File permission include:

- 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.
- 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.



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.

Windows also allows you to block Permission Inheritance, and assign permissions to files and folders individually.

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.

FAST Foundational Analyst Security Training

Additional extensions are a more elaborate security system based on access control lists (ACLs) and file system journaling.

NTFS is supported in other desktop and server operating systems as well. Linux and BSD have a free and open-source NTFS driver, called NTFS-3G, with both read and write functionality. macOS comes with read-only support for NTFS; its disabled-by-default write support for NTFS is unstable.

The current version is **v 5.1**: Released w/ Windows 10 in July of 2015 (test versions only), and July of 2016 (retail, and RTM versions). Allows for larger file sizes over 1TB, and has all the benefits of v. 3.1

when mentioning FAT be sure to note that if using USB to store memory image that most are in FAT32 for smaller drives.

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 is a feature that FAT does not provide and critical for NTFS to ensure that its complex internal data structures will remain consistent in case of system crashes or data moves performed by the defragmentation API, and allow easy rollback of uncommitted changes to these critical data structures when the volume is remounted.

Notably affected structures are the volume allocation bitmap, modifications to MFT records such as moves of some variable-length attributes stored in MFT records and attribute lists, and indices for directories and security descriptors.

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	

FAST Foundational Analyst Security Training

The journal is made available for applications to track changes to the volume.[18] This journal can be enabled or disabled on non-system volumes.[19]

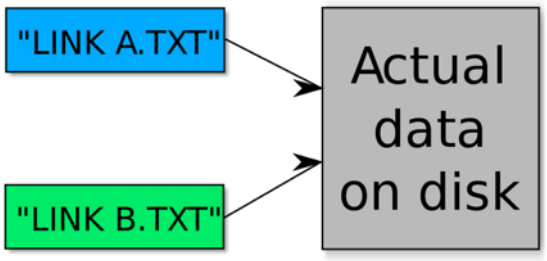
journaling is there so that if the computer is shut down before certain actions are completed that it can be completed when it is restarted, or completed before it is shut down, a usb removed etc… This is needed b/c of the lazy write system used by Hard Drives.

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.



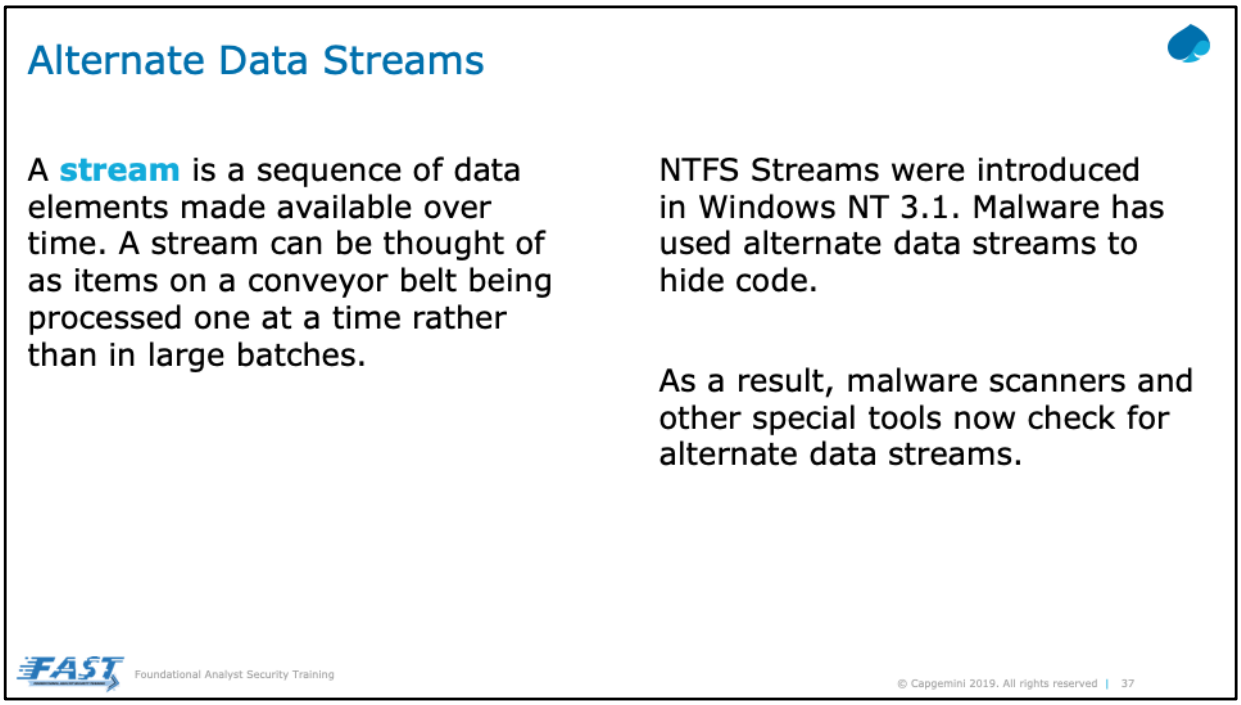
FAST Foundational Analyst Security Training

Hard links may link only to files in the same volume, because each volume has its own MFT. Hard links have their own file metadata, so a change in file size or attributes under one hard link may not update the others until they are opened.

Hard links were originally included to support the POSIX subsystem in Windows NT. Windows uses hard links to support short (8.3) filenames in NTFS.

Operating system support is needed because there are legacy applications that can work only with 8.3 filenames. In this case, an additional filename record and directory entry is added, but both 8.3 and long file name are linked and updated together, unlike a regular hard link.

The NTFS file system has a limit of 1024 hard links on a file.



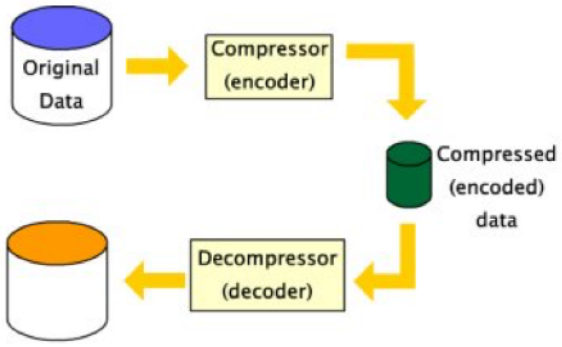
A stream is a sequence of data elements made available over time. A stream can be thought of as items on a conveyor belt being processed one at a time rather than in large batches.

Although current versions of Windows Server no longer include SFM, third-party Apple Filing Protocol (AFP) products (such as GroupLogic's ExtremeZ-IP) still use this feature of the file system.

ADS's are used naturally and most are not malicious. Also older APPLE devices and programs store the icon for a program in an ADS. When you download a file from a network or the internet an ADS is created on the Windows system.

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.



FAST Foundational Analyst Security Training

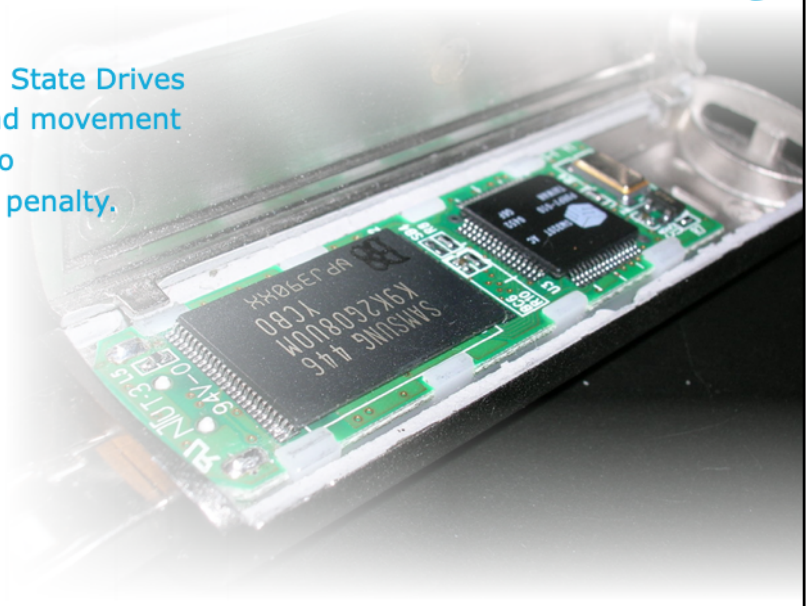
The compression algorithms in NTFS are designed to support cluster sizes of up to 4 KB. When the cluster size is greater than 4 KB on an NTFS volume, NTFS compression is not available.

If the compression reduces 64 KB of data to 60 KB or less, NTFS treats the unneeded 4 KB pages like empty sparse file clusters—they are not written. This allows for reasonable random-access times as the OS just has to follow the chain of fragments. However, large compressible files become highly fragmented since every chunk smaller than 64 KB becomes a fragment.

According to research by Microsoft's NTFS Development team, 50–60 GB is a reasonable maximum size for a compressed file on an NTFS volume with a 4 KB (default) cluster (block) size. This reasonable maximum size decreases sharply for volumes with smaller cluster sizes.

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.



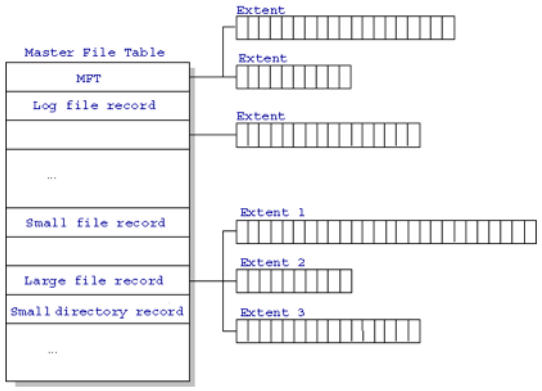
FAST Foundational Analyst Security Training

Users of fast multi-core processors will find improvements in application speed by compressing their applications and data as well as a reduction in space used.

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.

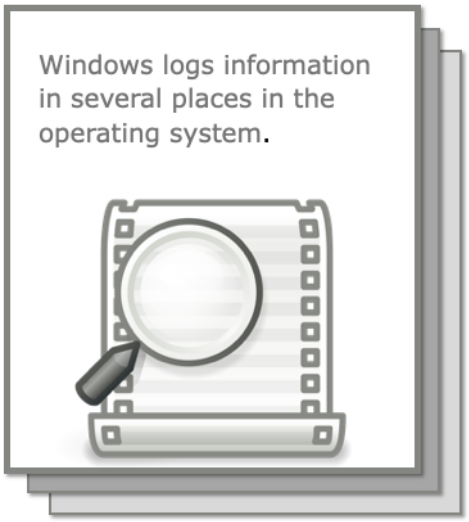


Each file on an NTFS volume is represented by a record in a special file called the master file table (MFT). NTFS reserves the first 16 records of the table for special information.
The first record of this table describes the master file table itself, followed by a MFT mirror record.
If the first MFT record is corrupted, NTFS reads the second record to find the MFT mirror file, whose first record is identical to the first record of the MFT. The locations of the data segments for both the MFT and MFT mirror file are recorded in the boot sector.

Windows Logs

Including the following:

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



FAST Foundational Analyst Security Training

Log files provide valuable information and is commonly used in investigations.

Windows logs information in several places in the operating system, including:

- 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.

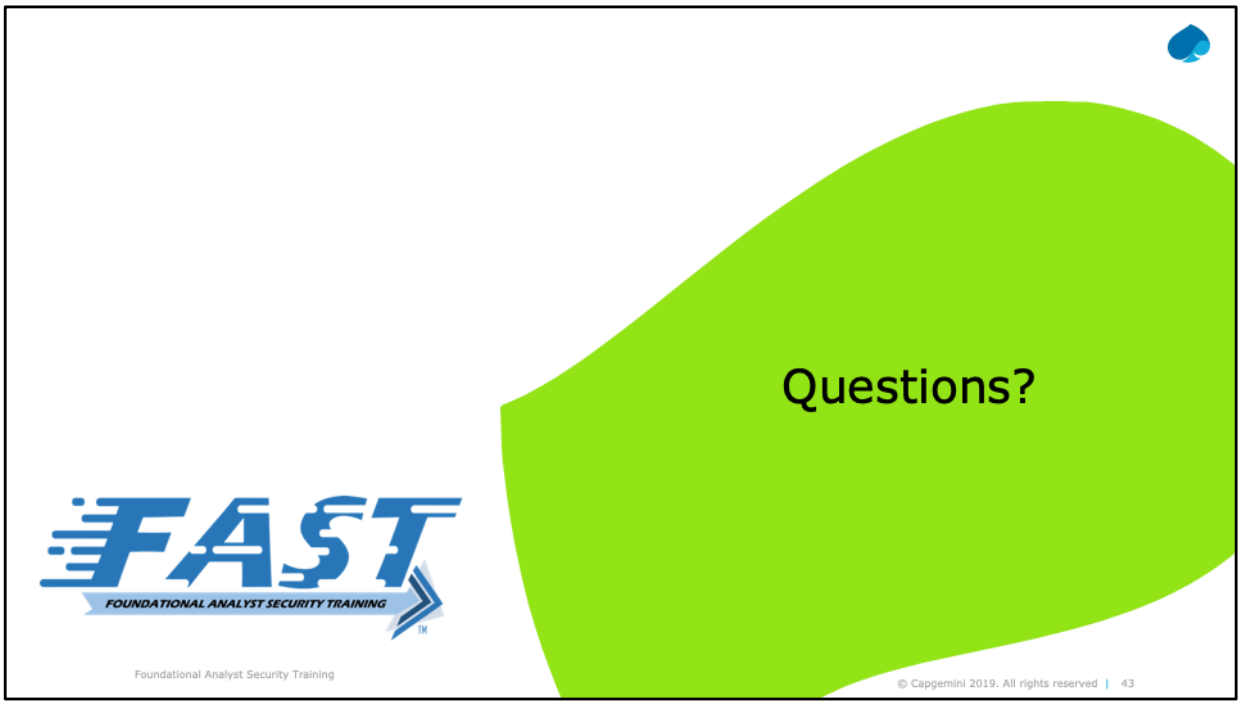
There are several tools used to view and parse logs.

- Autopsy
- TZWorks
- EnCase
- FTK Imager
- Log2timeline

FAST Foundational Analyst Security Training

log2timeline is designed as a framework for artifact timeline creation and analysis. The main purpose is to provide a single tool to parse various log files and artifacts found on suspect systems (and supporting systems, such as network equipment) and produce a body file that can be used to create a timeline

Event viewer can connect to remote computers and see their event logs. This can be useful if you do not have another way to get event logs from a remote system.


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 43

Content Source:

https://computer.howstuffworks.com/solid-state-drive.htm
https://www.stellarinfo.com/blog/myths-about-disk-wiping-and-solid-state-drives/
https://en.wikipedia.org/wiki/IBM_305_RAMAC

Module Overview:

When your computer is operating, it needs a place to put information that it uses regularly. This allows the computer to work faster, by removing the need to obtain information from the hard drive every time it is needed.

Data that is needed regularly is placed in volatile memory, or RAM in order to make it available faster. RAM is volatile memory, and does not retain information after power is removed.

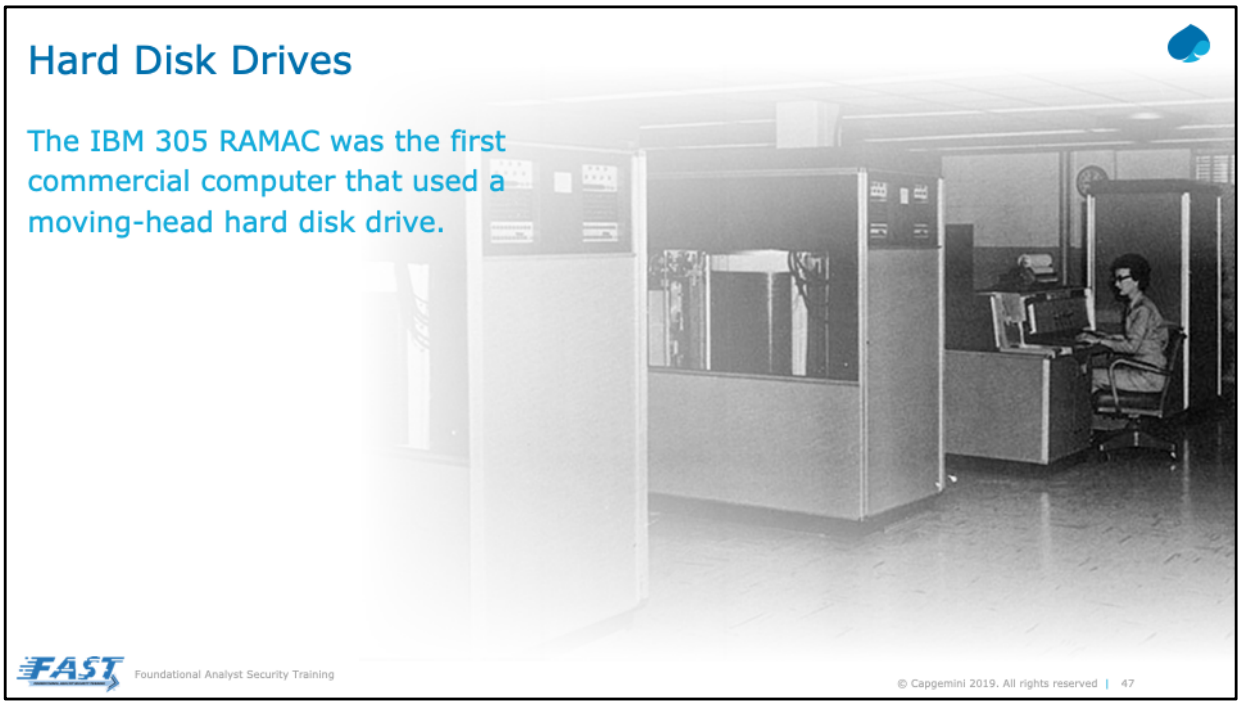
Agenda

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.



The **IBM 305 RAMAC** was the first commercial computer that used a moving-head hard disk drive (magnetic storage device).

The system was publicly announced on September 14, 1956 with test units already installed at the U.S. Navy and at private corporations.

The drive used 50 24-inch (61-centimeter) platters, stored a meager 5 megabytes of data and took up more room than two refrigerators. Oh, and the cost? Just $50,000, about $420,000 in todays money.

Since then, hard disk drives have grown smaller, will hold more data as well as become less expensive.

Hard Disks

Physical Data Storage

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

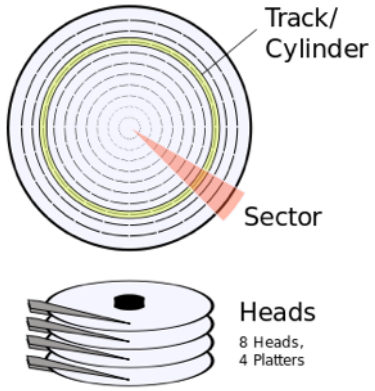
FAST Foundational Analyst Security Training

The largest representable value is 11111111, which is 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255.

Mechanical Hard Disks

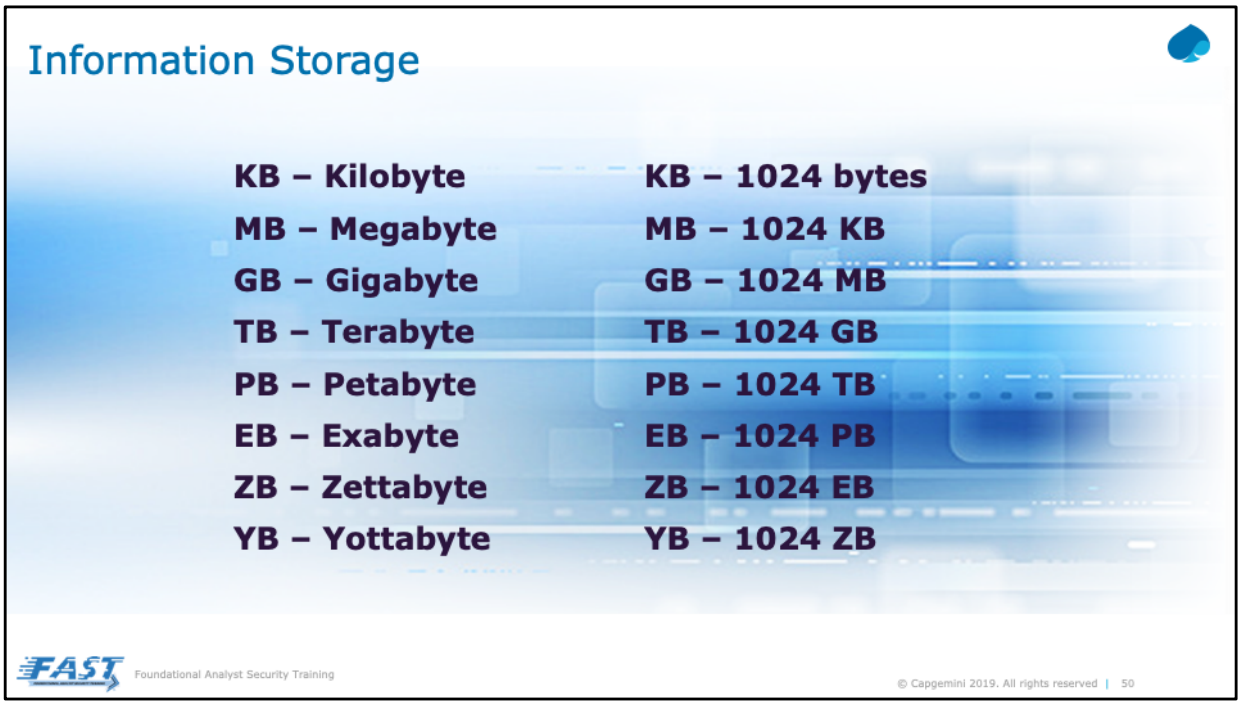
Hard disks are arranged into cylinders, heads, and sectors.

Each sector is typically 512 bytes.



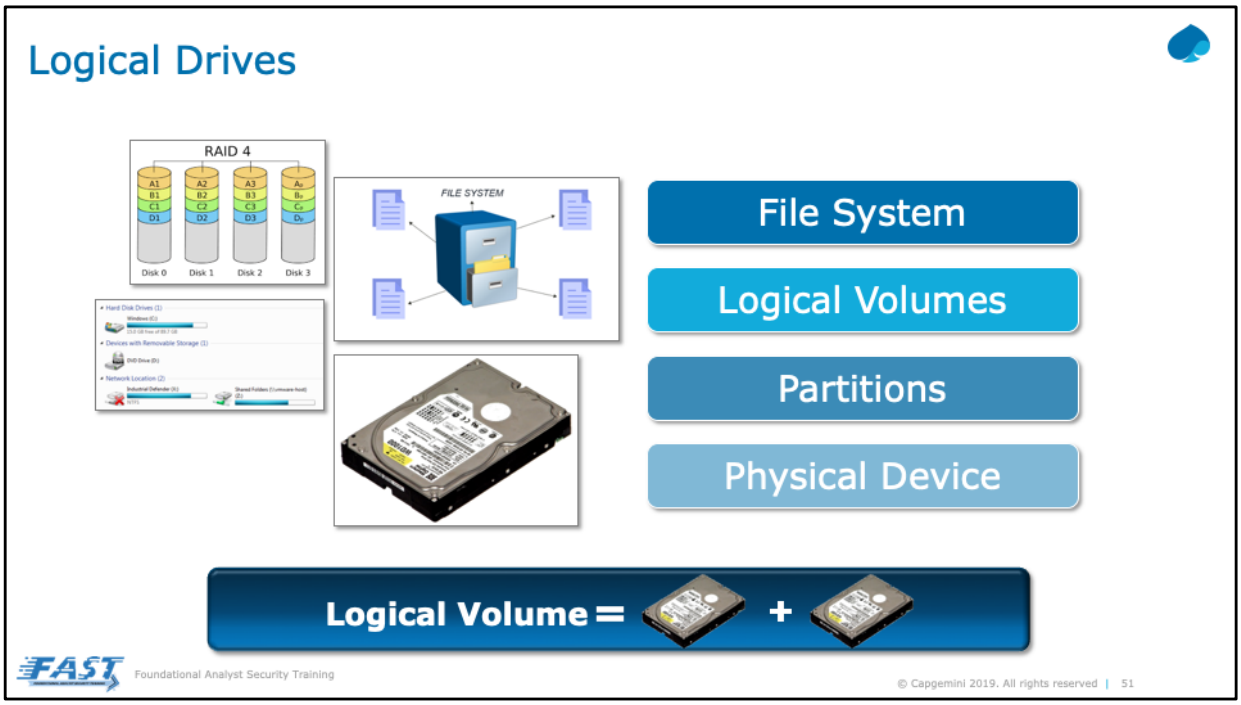
FAST Foundational Analyst Security Training

Hard Disks are arranged into cylinders, heads and sectors. Each sector is typically 512 bytes.



Each size depicted is a factor of 1024 bytes. A Kilobyte is 1024 bytes; a Megabyte is 1024 Kilobytes, or 1024*1024 bytes; a Gigabyte is 1024 Megabytes, or 1024*1024*1024 bytes; and so on…

note that computers use base 2 and when buying HD's they tell the space that is there in bytes. When they say 1 MB they mean 1,000,000 bytes not 1,048,576 bytes like the computer sees a MB.



Instructor Notes:

There are multiple layers of a physical mechanical hard drive

The lowest is they physical layer, then the logical, where volumes reside.

Volumes in Windows are typically assigned letters by the OS or the drive letter can be assigned by the user (for example C:\).

Physical – This layer consists of the actual physical disk that holds information, Hard disks are rigid platters, composed of a substrate and a magnetic medium. The substrate – the platter's base material – must be non-magnetic and capable of being machined to a smooth finish. It is made either of aluminum alloy or a mixture of glass and ceramic.

Partition - Disk partitioning or disk slicing is the creation of one or more regions on a hard disk or other secondary storage, so that an operating system can manage information in each region separately.[2] These regions are called partitions. It is typically the first step of preparing a newly manufactured disk, before any files

or directories have been created.

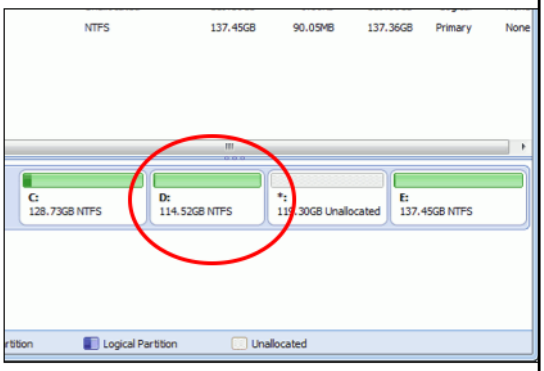
Logical Volume - A logical volume provides storage virtualization. With a logical volume, you are not restricted to physical disk sizes. In addition, the hardware storage configuration is hidden from the software so it can be resized and moved without stopping applications or unmounting file systems. This can reduce operational costs. These volumes can reside on separate physical disks, for example in a raid array.

File System - A file system can be thought of as an index or database containing the physical location of every piece of data on the hard drive or another storage device. The data is usually organized in folders called directories, which can contain other folders and files.

These physical drives can be some of the most valuable from a forensic perspective.

Unallocated Space

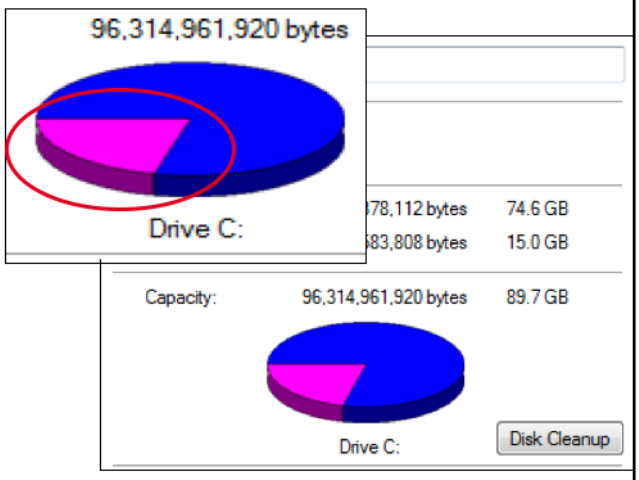
Unallocated space is different from unused space.



Unallocated Space, is space in the logical volume that has not be assigned to a partition.

Unused Space

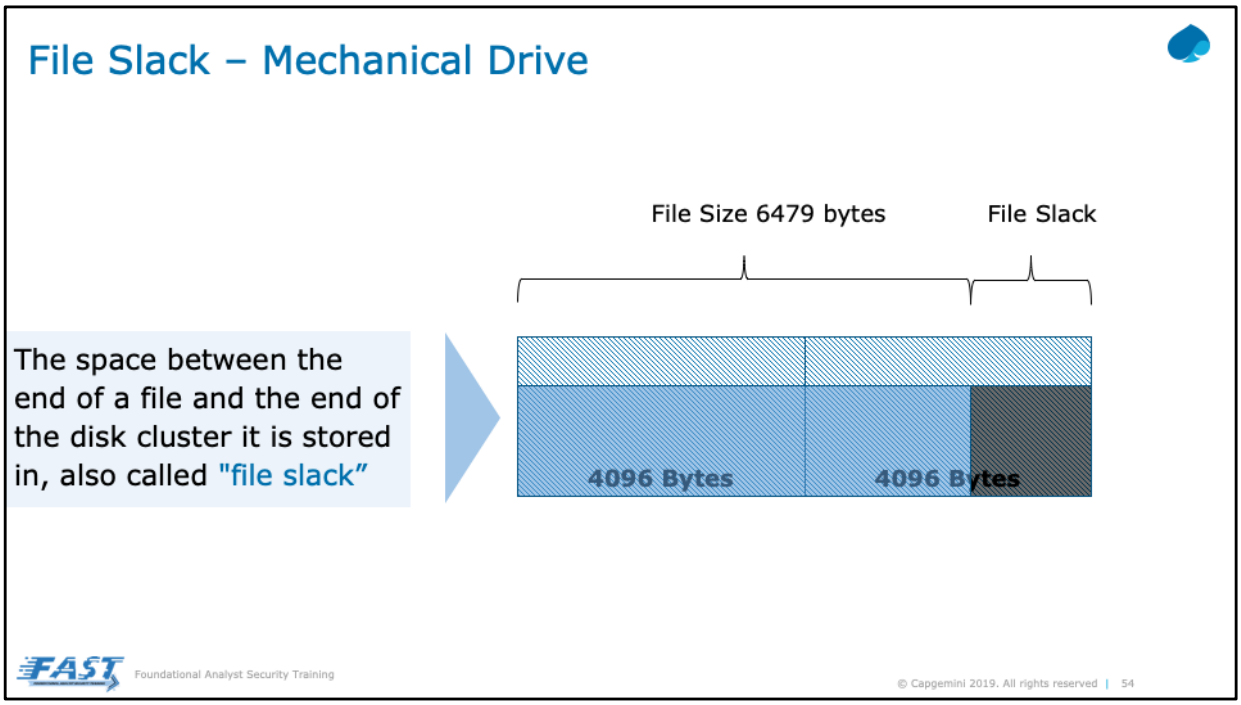
Unused space is an area of a volume that is not currently being used by the file system.



FAST Foundational Analyst Security Training

When the user deletes a file, the operating system allows the space where the file was once stored to be unallocated, and labeled as ready to be used. Forensically this means that some file fragments still may be on the drive, even after they were deleted.

The larger the file is, the less likely you can recover the entire file.



Instructor Notes:

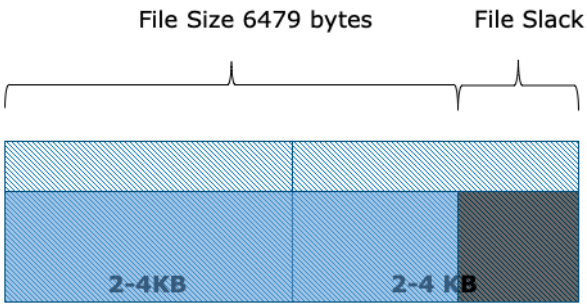
It occurs naturally because data rarely fill fixed storage locations exactly, and residual data occur when a smaller file is written into the same cluster as a previous larger file. In computer forensics, slack space is examined because it may contain meaningful data.

So if a file is 6479 bytes, it will allocated two 4096 byte file clusters, what is unused from that allocation is called file slack, and may contain information from a file previously using that space.

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**"

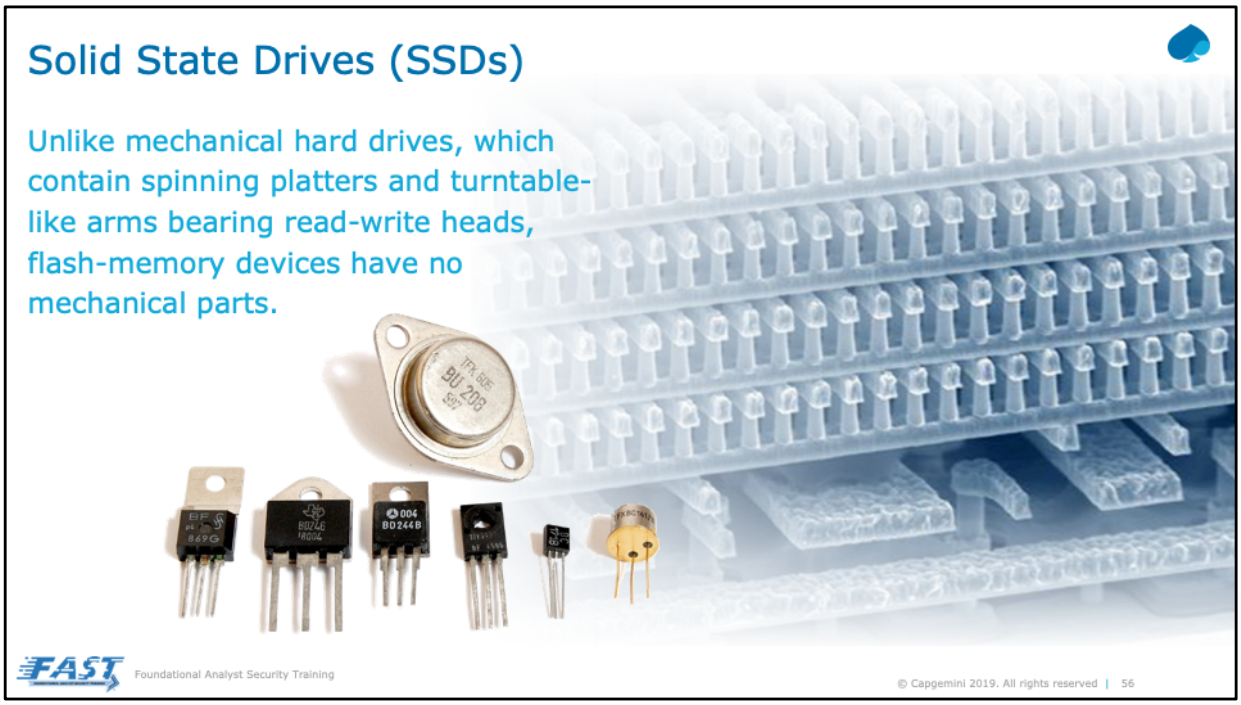
For SSDs, this is still true; but it is forensically useless…



FAST Foundational Analyst Security Training

File slack is the space between the end of a file and the end of the disk cluster it is stored in.

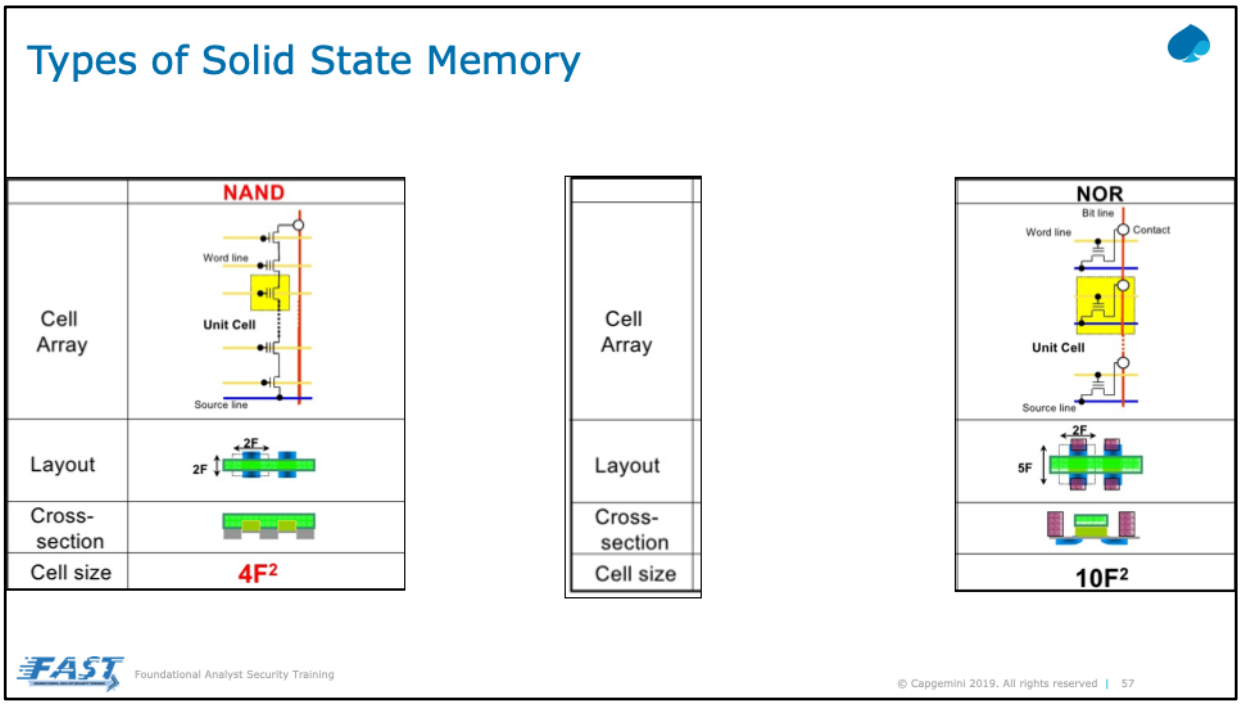
For Solid State Drives this is still true, but it is forensically problematic, we will talk about why in a moment.



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

They're built from transistors and other components you'd find on a computer chip.

As a result, they enjoy a label -- **solid state** -- reserved for devices that take advantage of semiconductor properties.



There are two types of flash memory: NOR and NAND. Both contain cells -- transistors -- in a grid, but the wiring between the cells differs. In **NOR flash**, the cells are wired in parallel. In NAND flash, the cells are wired in a series. Because NOR cells contain more wires, they're bigger and more complex. **NAND cells** require fewer wires and can be packed on a chip in greater density. As a result, NAND flash is less expensive, and it can read and write data much more rapidly. This makes NAND flash an ideal storage technology and explains why it's the predominant type of memory in solid-state drives. NOR flash is ideal for lower-density, high-speed, read-only applications, such as those in code-storage applications.

Mechanical vs. Solid State

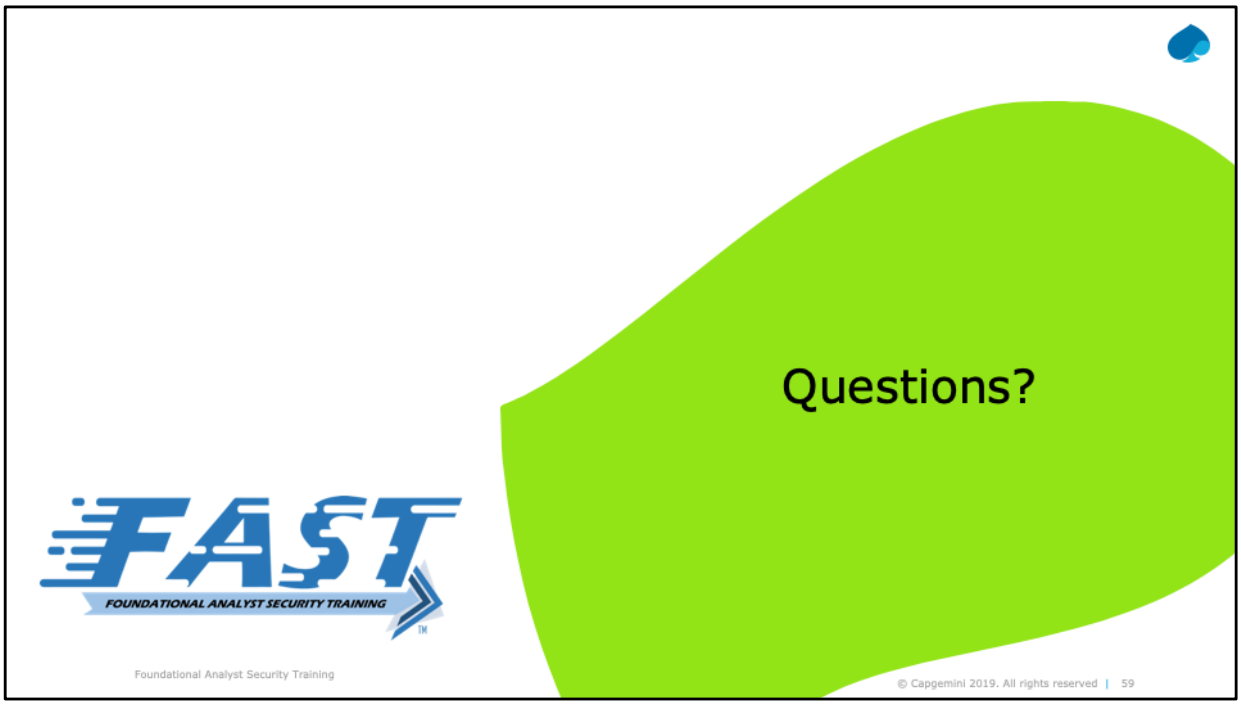
As always… there is a downside…

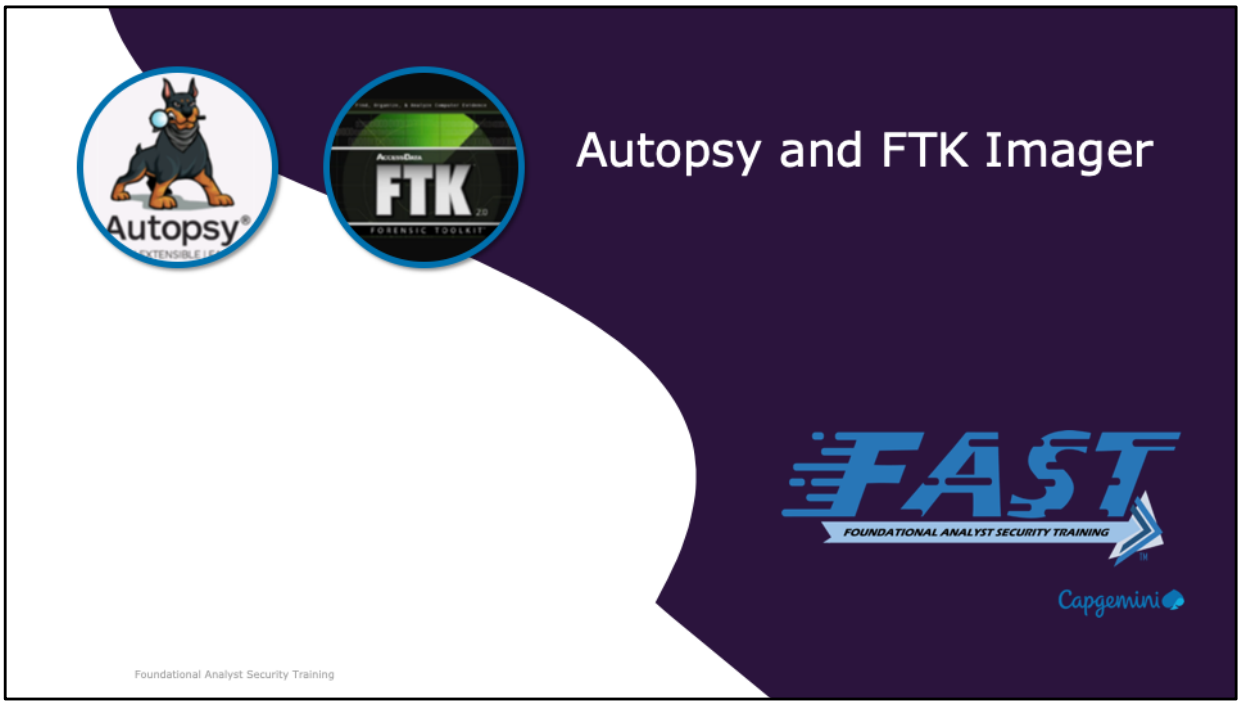
SSDs will eventually "rot" into a read-only state.

FAST Foundational Analyst Security Training

While SSD are 15 times faster at reading and writing data than their mechanical counter parts, there is a downside to slid state drives. SSD Drives will eventually "rot" into a read only state.

Mention that MAC's by default turn on a trim command that makes file slack analysis virtually useless, while windows does not generally enable this feature by default.


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 59



Content Source:

https://computer.howstuffworks.com/solid-state-drive.htm
https://www.stellarinfo.com/blog/myths-about-disk-wiping-and-solid-state-drives/
https://en.wikipedia.org/wiki/IBM_305_RAMAC

Module Overview:

When your computer is operating, it needs a place to put information that it uses regularly. This allows the computer to work faster, by removing the need to obtain information from the hard drive every time it is needed.

Data that is needed regularly is placed in volatile memory, or RAM in order to make it available faster. RAM is volatile memory, and does not retain information after power is removed.

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.

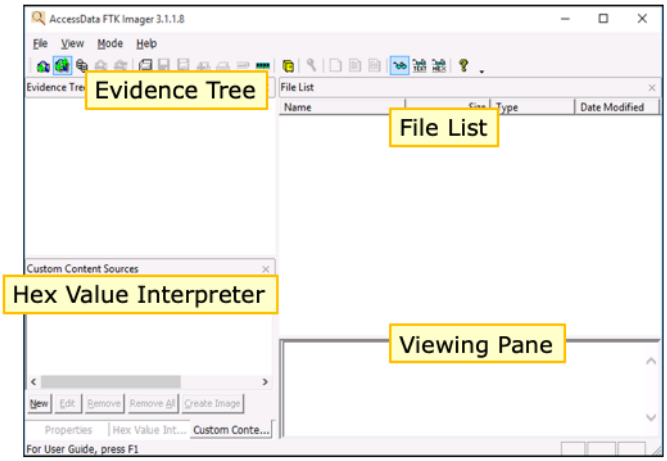
FTK imager (not lite) can be run from a USB if you copy the installed files from a computer to a USB drive. You do not have to install it on a computer and it can do Memory and Disk imaging.

FTK Imager (cont.)

FTK Imager Interface

There are four panes in the FTK Imager view.

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



mention that by default disk images are done in the Access Data format, you want to change this to either E01 or DD so that other tools can reed the image files, without having to do other steps to analyze them.

Autopsy by Sleuth Kit

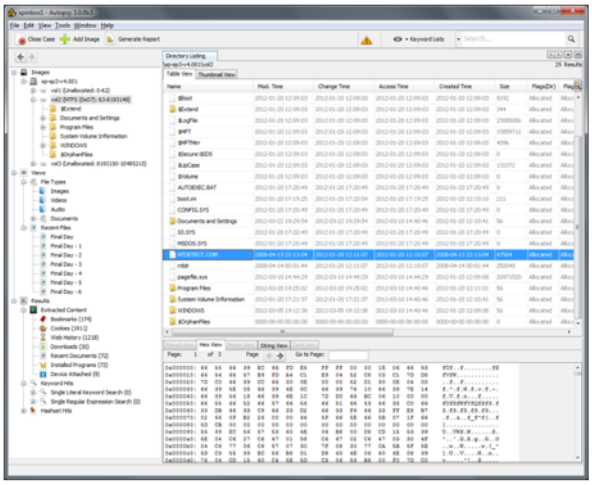
What is Autopsy?

- 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.



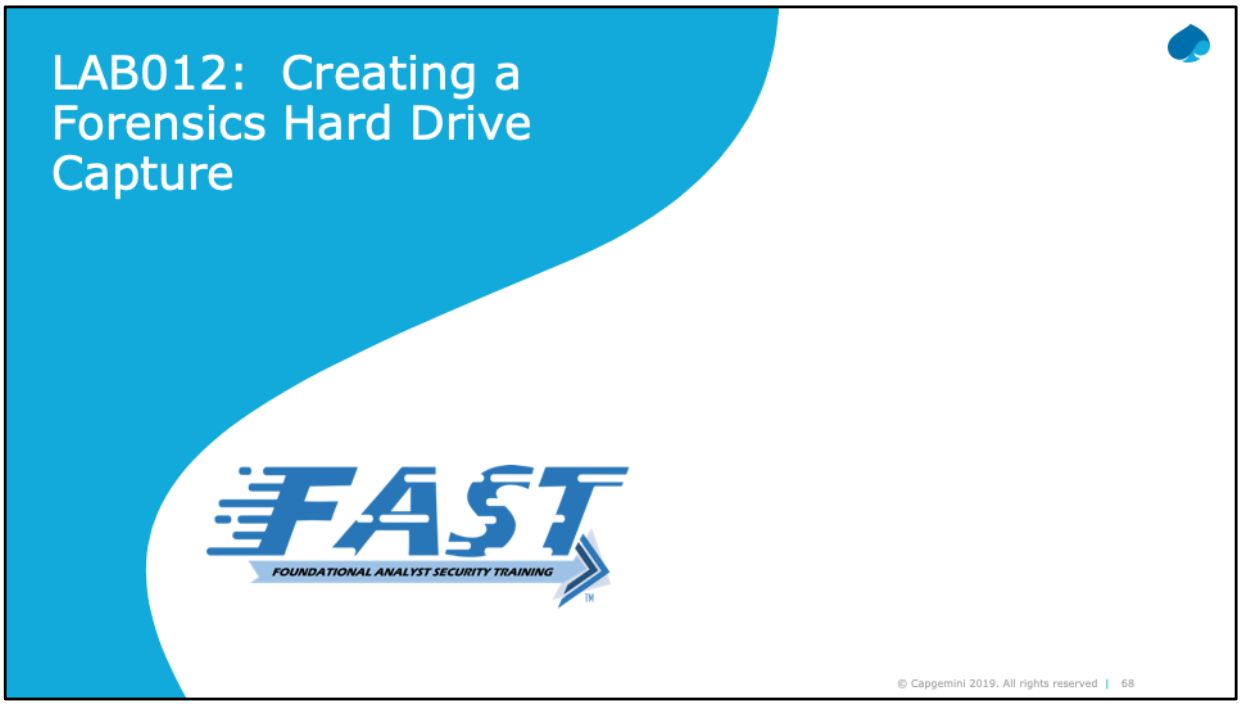
Autopsy by Sleuth Kit (cont.)

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.

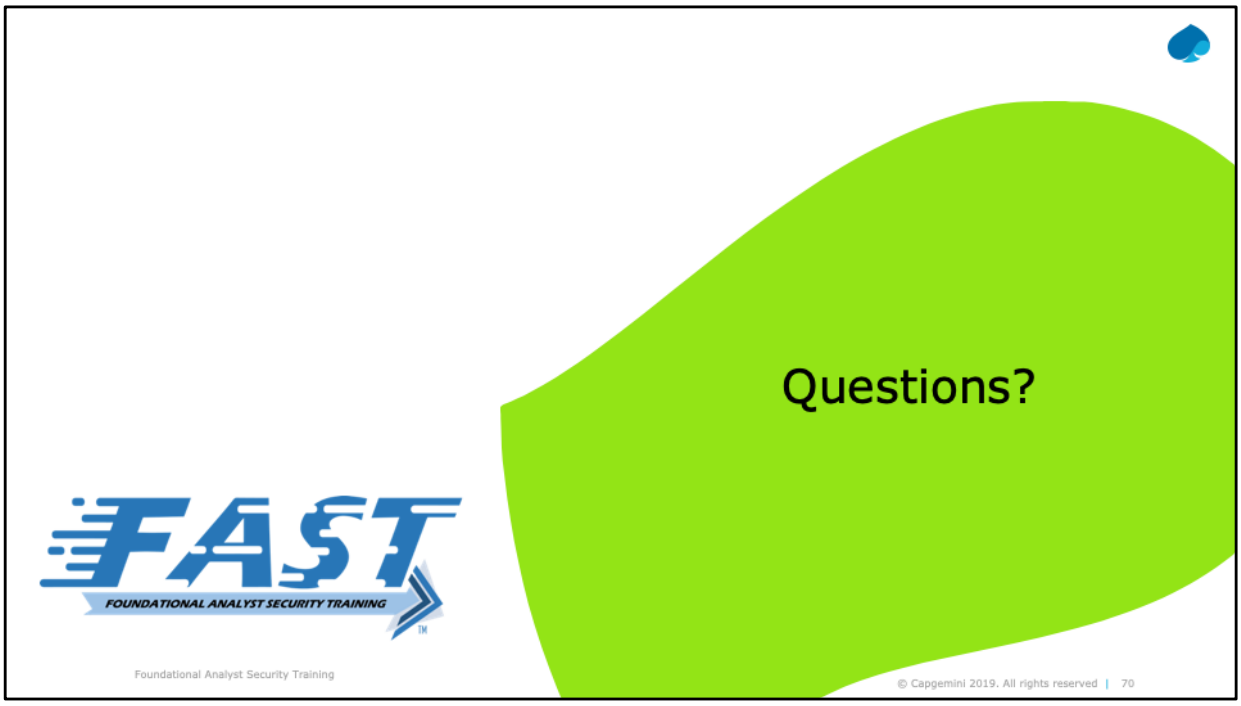
Some of the modules provide the following:

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)



Content Source:

Content Source:


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 70


FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
People matter, results count.
This presentation contains information that may be privileged or confidential and is the property of the CapGemini Group.
Copyright © 2019 CapGemini. All rights reserved.
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