File Systems and Disk Forensics

Thomas Benos

MSc UniWA, Cisco CyberOps
GR CSIRT Incident Responder
thomasbenos1291@gmail.com

Agenda

- Introduction to File Systems
- Understanding File Systems
- NTFS File System
- Deleted Files and File Carving
- SANS Forensic Artifacts

Introduction to File Systems

What is a File System?

- A method and data structure that an operating system uses to manage and store files on a storage device (e.g. HDD or SSD).
- It provides a logical way for the operating system to organize and retrieve data, enabling users to create, access, and manage files efficiently.
- Key Components:
  - File Allocation Table (FAT)
  - Master File Table (MFT)
  - Inode Table (for some Unix-based file systems)
- File systems examples:
  - FAT32
  - NTFS/ReFS
  - ext4

Importance of File Systems

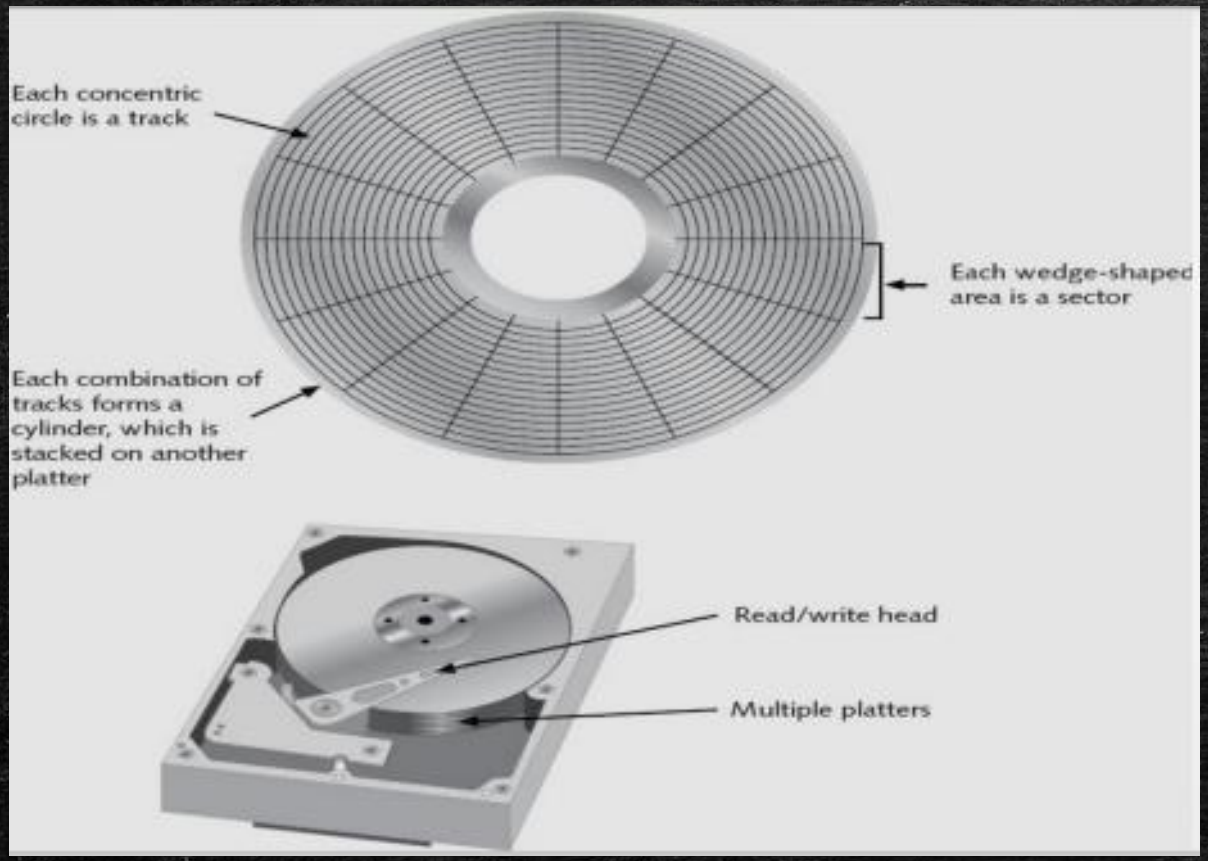
- Data Recovery
  - file locations and structures -> data recovery
- Timestamps
  - created, modified, accessed
- File Allocation
  - how files are allocated on storage
- Metadata and File Attributes
  - crucial in forensic analysis

Understanding File Systems

File System 5 Layers

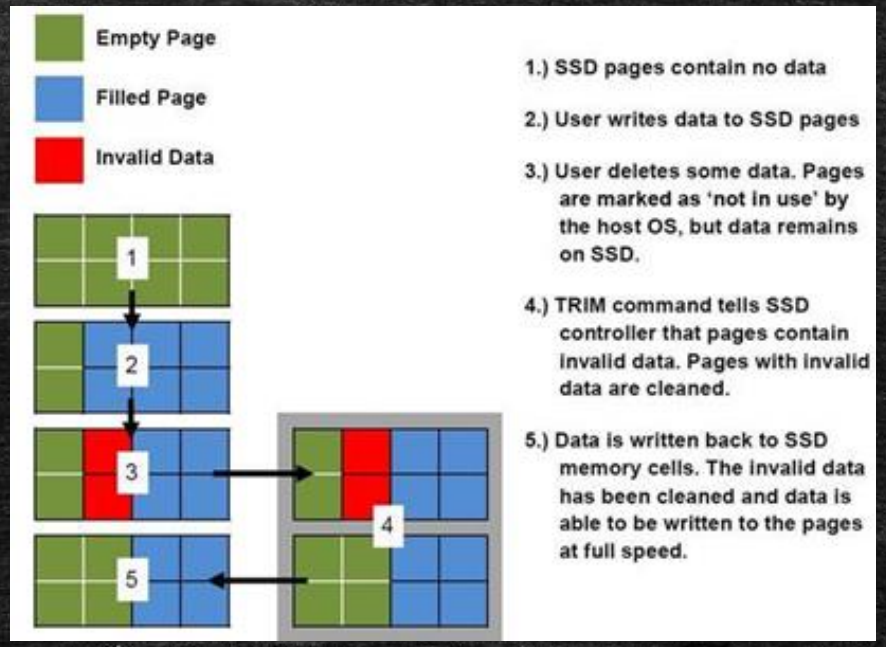
1. **Physical Layer** – The physical disk itself
2. **File System Layer** – Partition Information
3. **Data Layer** – Blocks and clusters (where the data are actually stored).
4. **Metadata Layer** – Structural information for the file system (FAT32, NTFS, etc.)
5. **File Name Layer** – The directory hierarchy and information that holds the files external name.

Physical Layer – HDDs & SSDs



Physical Layer – SSDs Considerations

- TRIM -> Garbage collection

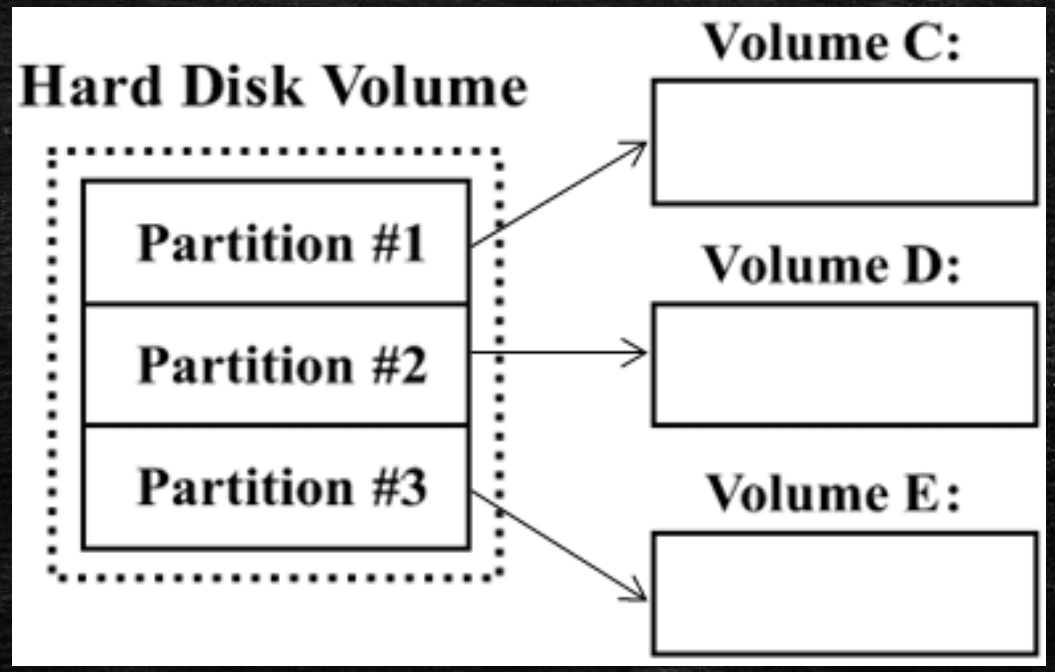


- Check if TRIM is enabled:
  - *fsutil behavior query disabledeleteNotify*

```
C:\Windows\System32>fsutil behavior query disabledeleteNotify
NTFS DisableDeleteNotify = 0  (Allows TRIM operations to be sent to the storage device)
ReFS DisableDeleteNotify = 0  (Allows TRIM operations to be sent to the storage device)
```

File System Layer

- Holds the data that describes the structural details of the file system.
- Boot Information (MBR, Superblock)
- Divides Physical Storage into manageable units
  - Partitions
  - Volumes



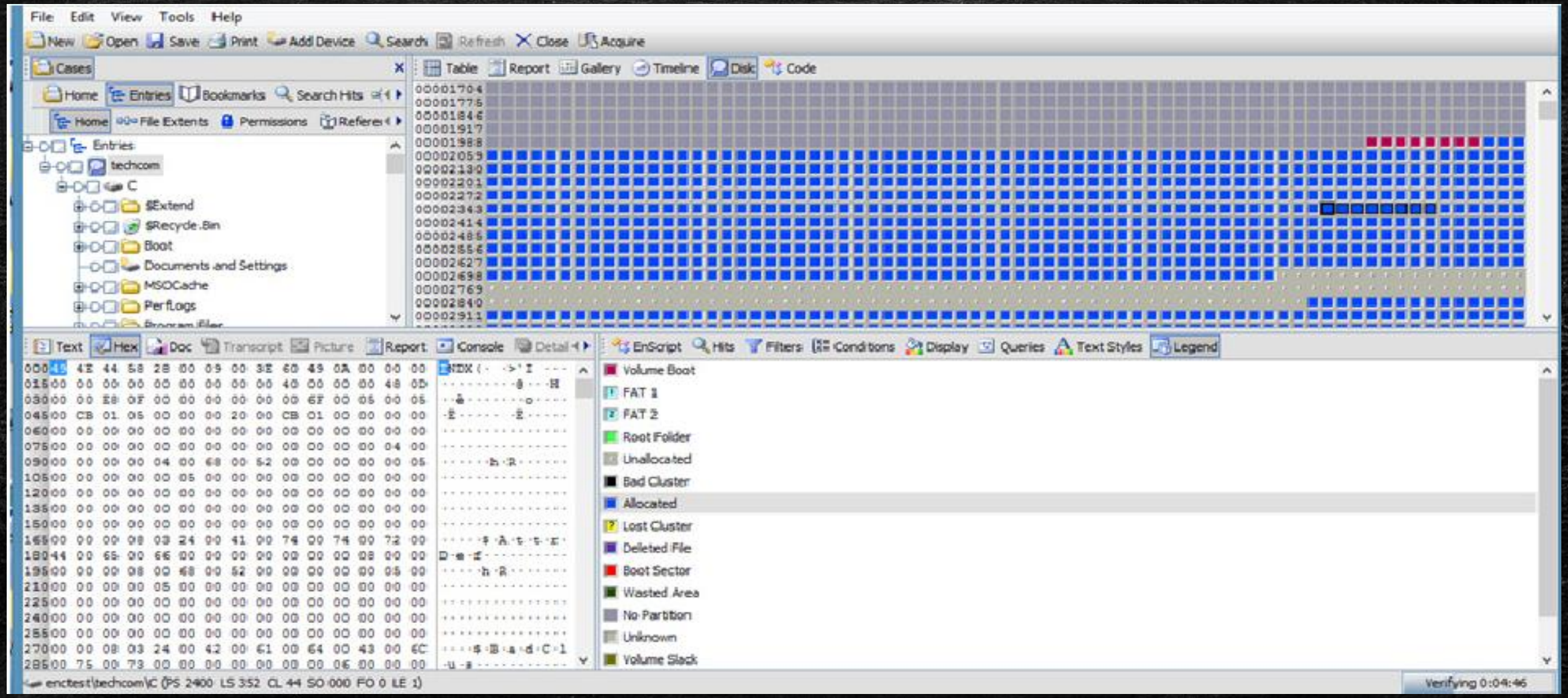
File System Types

- **NTFS** (New Technology File System)
- **FAT** (File Allocation Table)
- **exFAT** (Extended File Allocation Table)
- **ReFS** (Resilient File System)

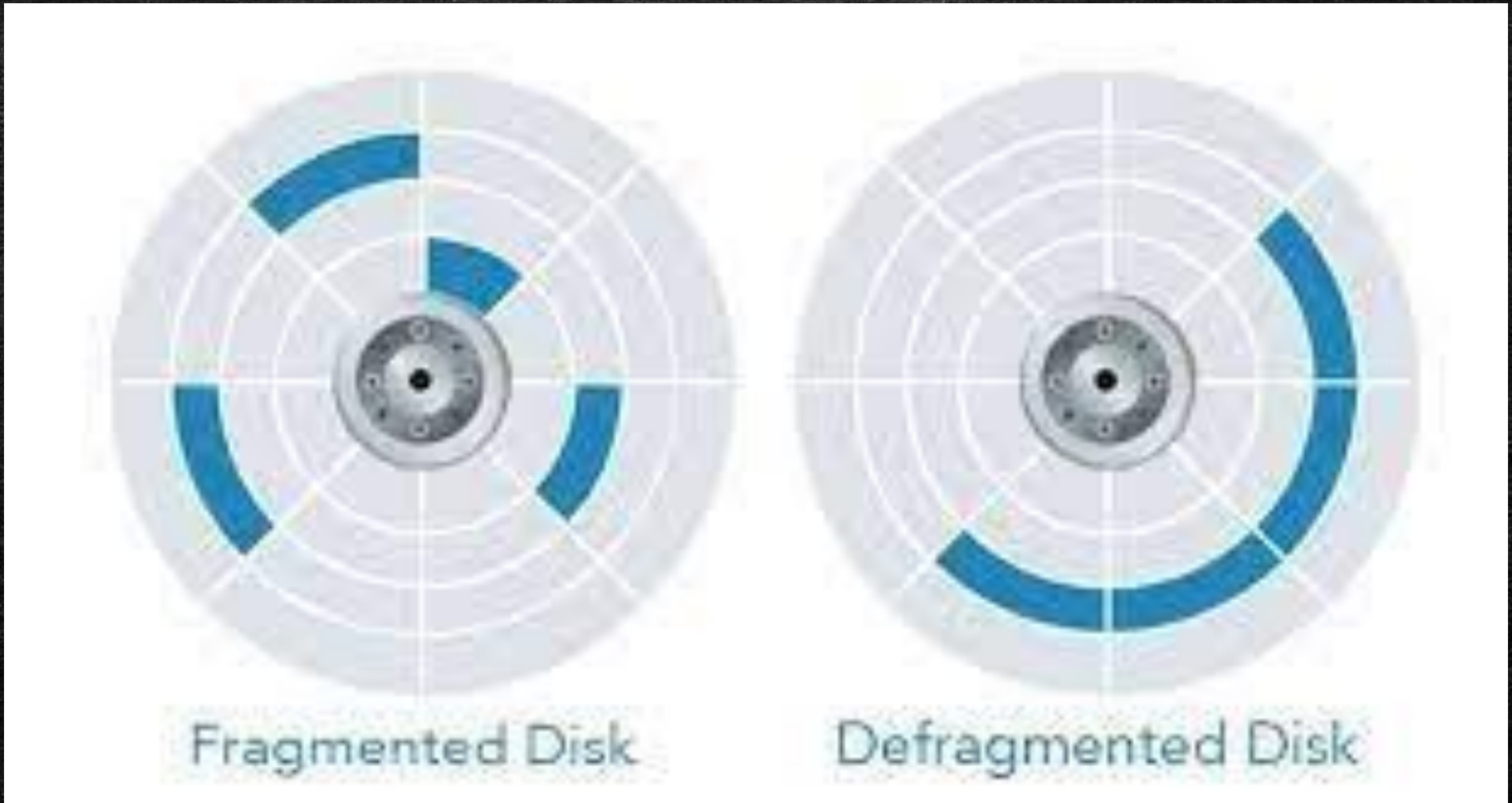
Data Layer

- Actual storage of digital information on a storage device.
- Organizes the physical drive into 512 byte sectors
  - Data is organized into blocks or clusters
- Allocation Methods
  - Sectors either “allocated” or “unallocated”.
- File Fragmentation
  - file data stored in non-contiguous blocks or clusters
- Impact on Forensic Analysis
  - reconstruct files, recover data, analyze storage patterns

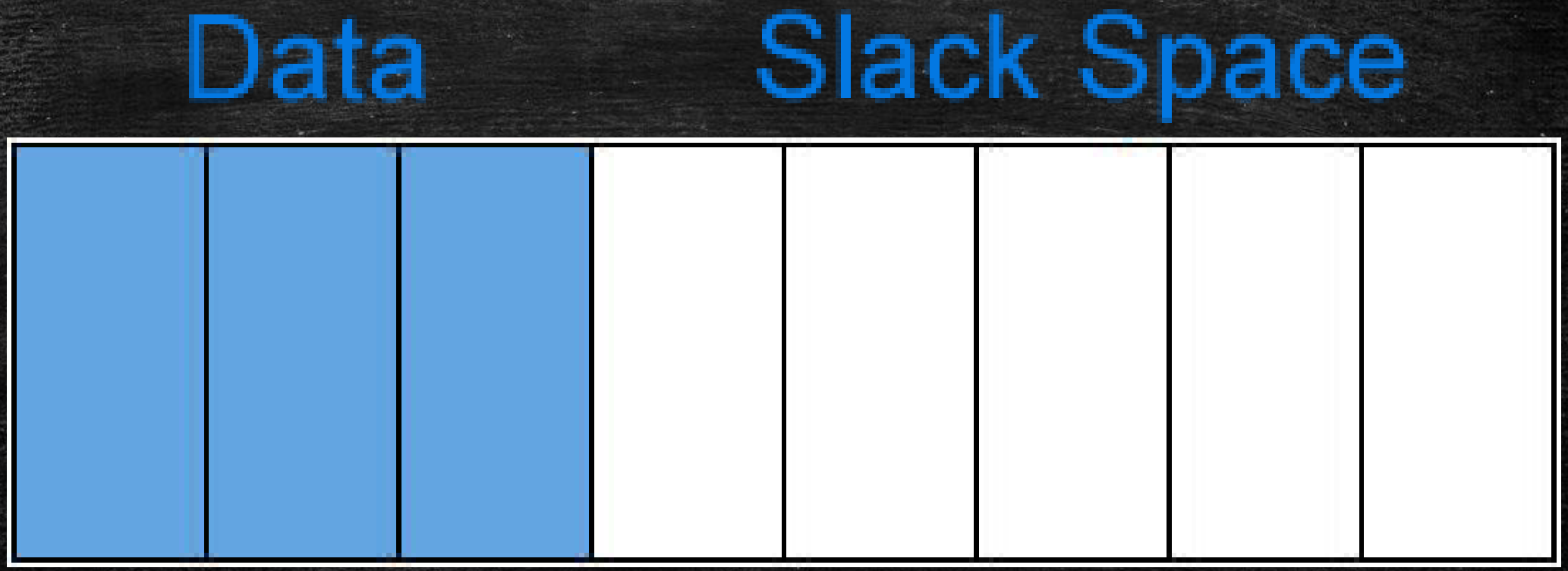
Data Layer - Allocated vs Unallocated Data



Data Layer - Fragmented vs. Non-Fragmented Data



Data Layer – Slack Space



Metadata Layer

- Structural information about files, directories, and the file system itself.
- Master File Table (MFT) (Windows NTFS)
  - maintains records for every file and directory on the volume
- Key Metadata Attributes
  - File Name
  - File Size
  - Timestamps
  - File Permissions
- Significance in Digital Forensics
  - identify ownership, establish digital evidence in investigations.

File Name Layer (1/2)

- Manages names and hierarchy of files and directories.
- Directory Hierarchy:
  - Organizes files and directories in a tree-like structure.
  - Allows for easy navigation and management.
  - Directories contain files and subdirectories, forming a hierarchical layout.
- External vs. Internal Names:
  - External Name: The name as it appears to users in the file system.
  - Internal Name: A unique identifier assigned by the file system for management.
- File Extensions:
  - Provide information about the type or format of a file.
  - Common examples include .txt for text files, .jpg for images, .docx for Word documents, etc.

File Name Layer (2/2)

- File Naming Conventions
  - Rules and restrictions for naming files, which may include character limits, allowed characters, and reserved keywords.
- Long File Names
  - Modern file systems support long file names, allowing for more descriptive and user-friendly naming conventions.
- File Attributes
  - Properties associated with files, such as read-only, hidden, system, archive, etc.
  - These attributes can impact how a file is accessed and managed.
- Importance in Digital Forensics
  - Locate, identify, and analyze files during an investigation.

NTFS File System

NTFS - Key Features (1/3)

- Scalability
  - NTFS supports Very large files
  - The maximum theoretical limit is practically unlimited (roughly 18.5 million Terrabytes)
  - There is no realistic file-size or partition size limits.
- Journaling
  - records file system changes before committing them
  - helps recover the file system quickly in case of unexpected shutdowns or crashes.
  - $Log File
    - Records metadata changes to the volume
    - Ensure that its complex internal data structures will remain consistent in case of system crashes or data moves and allow easy rollback of uncommitted changes to these critical data structures when the volume is remounted
  - $USN_Journal
    - Records changes to files, streams and directories

NTFS - Key Features (2/3)

- **Security and Permissions:**
  - Encryption options like BitLocker for data protection.
  - Advanced security features include granular file and folder permissions.
- **File and Folder Attributes:**
  - Supports various attributes (read-only, hidden, system, archive, etc.).
  - Provides additional control over file and folder behavior.
- **Recoverability:**
  - Features for file and volume recovery.
  - Previous versions and Shadow Copy enable recovery to previous states.
- **Compatibility:**
  - Compatible with operating systems back to Windows XP.

NTFS - Key Features (3/3)

- Unicode Support
  - NTFS supports Unicode, allowing for the use of a wide range of characters in file and folder names.
- Case Sensitivity
  - NTFS is case-insensitive but case-preserving, meaning it retains the case of file names for display purposes.
- Resilience to Fragmentation
  - NTFS employs strategies to reduce file fragmentation, improving overall system performance.
- Resizing and Quotas
  - Shrink or expand a partition
  - Allow the administrator of a computer that runs a version of Windows that supports NTFS to set a threshold of disk space that users may use

Security Descriptors & ACLs

- Security Descriptors:
  - contains information about an object's security
  - owner information, group membership, DACL
- Access Control Lists (ACLs):
  - part of the Security Descriptor
  - defines the permissions associated with an object
  - specifies which users or groups have access rights and the type of access allowed (e.g., read, write, execute).

Master File Table – MFT

```
7968c00 46 49 4c 45 30 00 03 00-36 e9 0e b4 37 00 00 00 FILE0···6é·´7···
7968c10 01 00 01 00 38 00 01 00-60 01 00 00 00 04 00 00 ····8···`·····
7968c20 00 00 00 00 00 00 00 00-05 00 00 00 a3 e5 01 00 ·····£å··
7968c30 1d 01 00 00 00 00 00 00-10 00 00 00 60 00 00 00 ·········`···
```

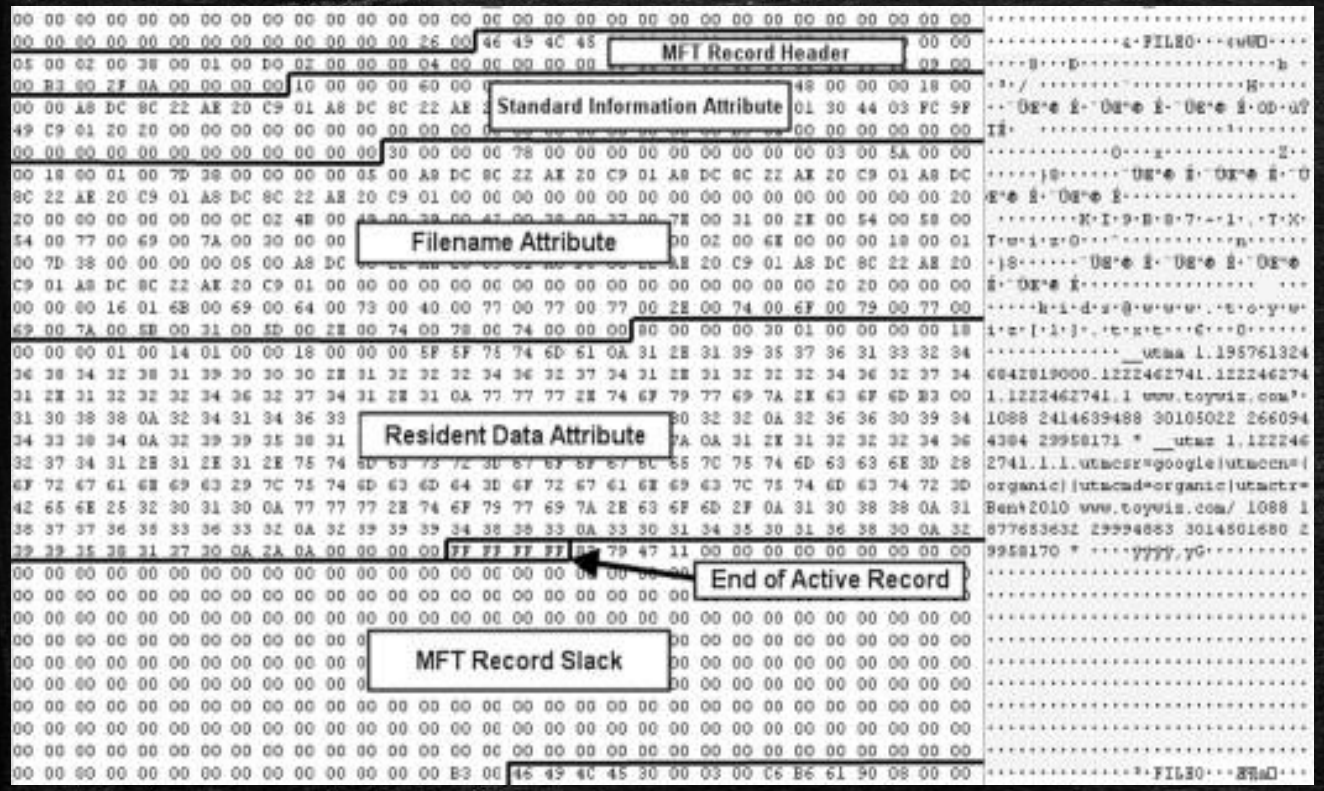
MFT Key Log Entries/Attributes

Record	Metadata	Function
0	$MFT	MFT table itself
1	$MFTMirr	Image of MFT in case the first record gets damaged
2	$LogFile	Log file, records important information that affects NTFS volume construction
3	$Volume	Volume file, contains volume label
4	$AttrDef	Attribute definition list
5	$Root	Root directory, saves index of all files and directories in root directory
6	$Bitmap	Bitmap file
7	$Boot	Boot file, stores boot commands; without it Windows cannot start
8	$BadClus	Store bad clusters of the volume so that Windows will not use them to store files

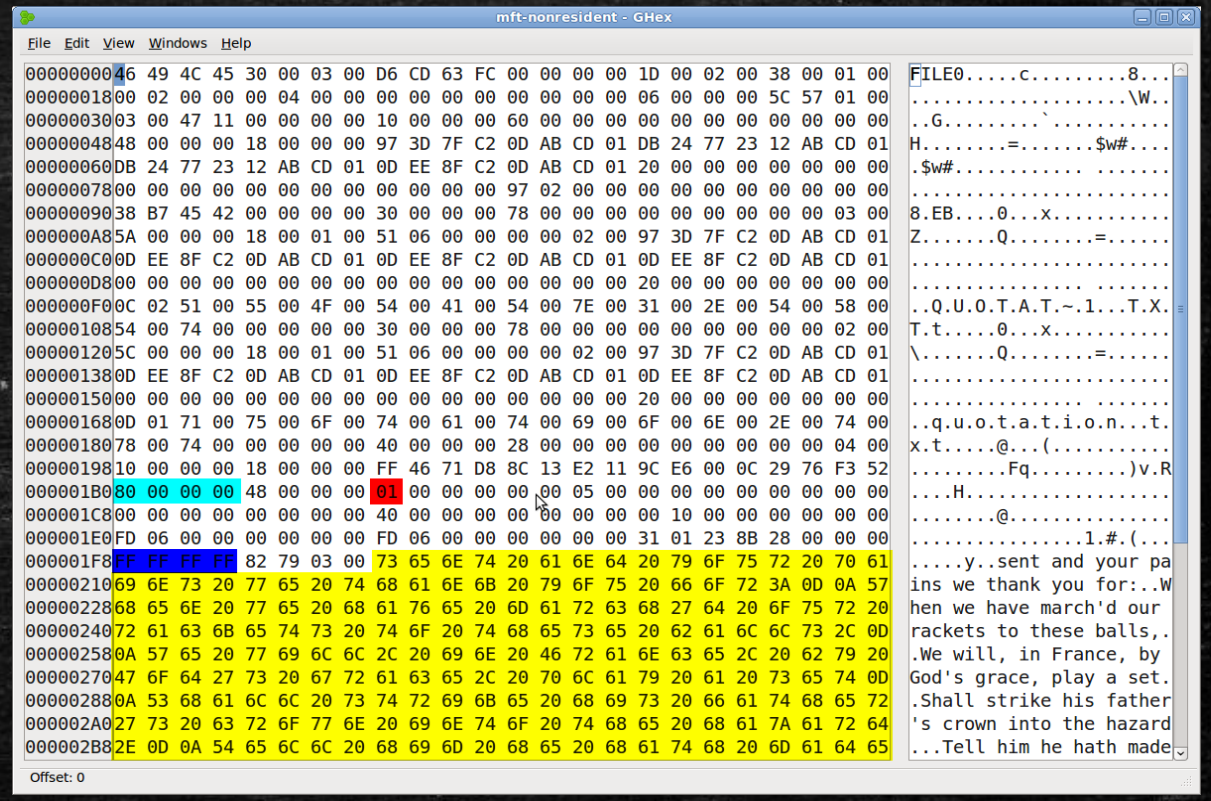
Record	Metadata	Function
9	$Secure	Secure file about the volume itself
10	$UpCase	Capitalized file
11	$Extended metadata directory	Extended metadata directory
12	$Extend\$Reparse	Reparse points file
13	$Extend\$UsnJrnl	Log changing file
14	$Extend\$Quota	Quota management file
15	$Extend\$ObjId	Object ID file
16		Reserved

Finding the Data – Resident/Non Resident

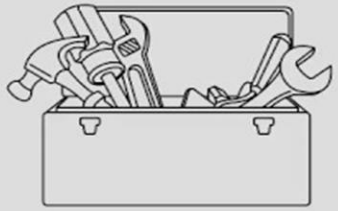
Resident



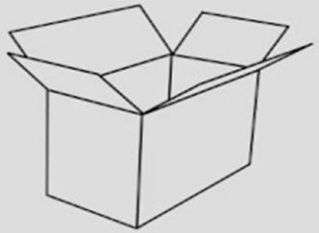
Non Resident



Timestamps



(M) Content Modified



(A) Accessed

(C) Metadata Changed

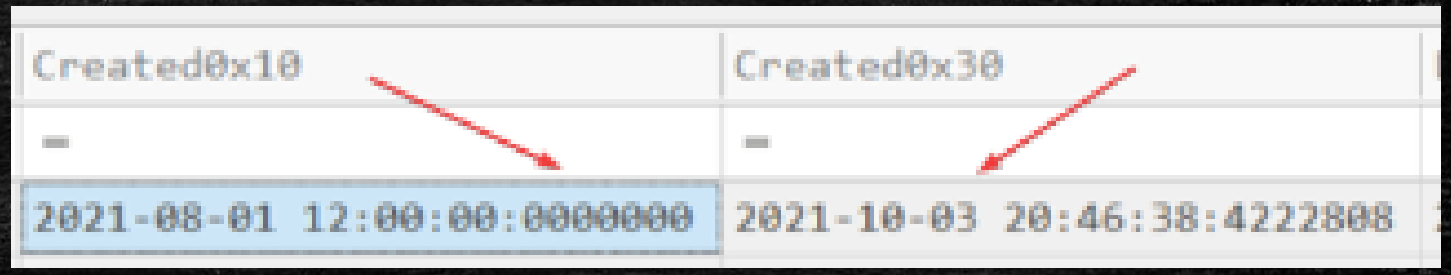
(B) Birth

Timestamps

- **Header – Identifies the attribute**:
  - file type, file size, and name (SI – Standard Information & FN - Filename).
  - It has flags to identify if the attribute is compressed or encrypted. Header is generic and standard to all attributes.

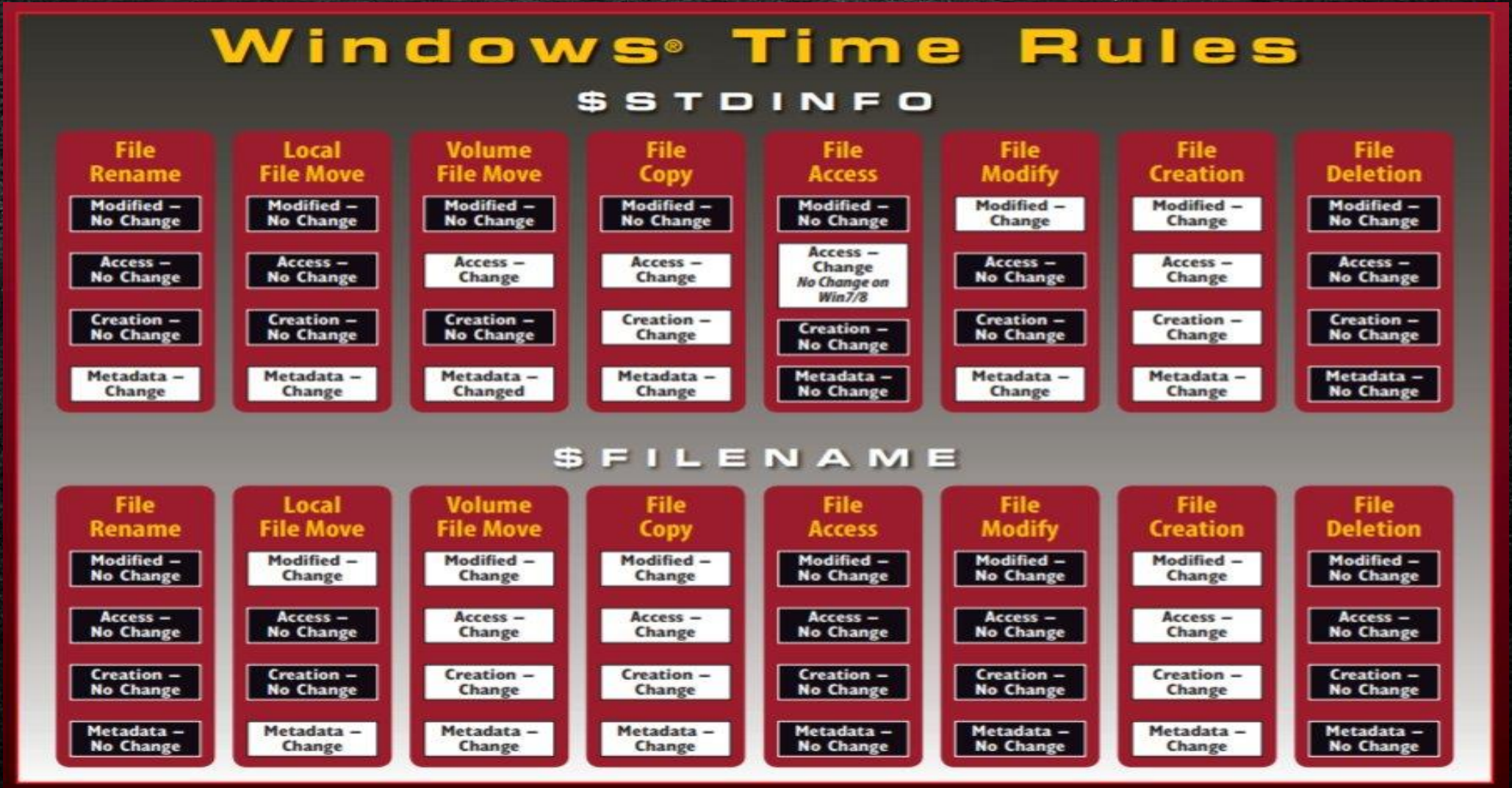
- **Content (Data)** :
  - The actual data of the file for a resident file.
  - Cluster location of file for nonresident files.

- **TIMESTOMP!!!**
  - $SI time is earlier than $FN
  - Nanosecond are all zeros



Created0x10	Created0x30
–	–
2021-08-01 12:00:00:0000000	2021-10-03 20:46:38:4222808

SANS $File_Name & $STANDARD_INFORMATION



MFT Analysis Tools

- **Analysis Tools Consideration:**
  - Choice of tools such as "TSK", "MFTECmd", “MFTExplorer”, “Timeline Explorer”or "AnalyzeMFT" depends on the case to be analyzed.
  - Understanding how tools interpret milliseconds and time formats is essential for accurate analysis.
  - Consideration of file names along with timestamp consistency is vital for a comprehensive analysis.

Volume Shadow Copy

- **Purpose:**
  - VSS enables the creation of shadow copies for backup and recovery purposes without disrupting ongoing operations on the volume.
- **Point-in-Time Snapshots:**
  - Shadow copies capture the state of the file system at a specific point in time, preserving the contents of files and directories.
  - A snapshot is taken by default once every 7 days.
  - 3% - 5% of disk, but can get up to 30%
  - VSS captures both file metadata and data at the time of the snapshot.
- **Usage:**
  - **Backup:** Shadow copies facilitate backup processes by providing a consistent and recoverable state of the file system.
  - **File Recovery:** Users can restore files, folders, volumes to previous states from shadow copies.
  - **System Restore:** Windows uses VSS for System Restore points, allowing users to revert the system to a previous state.
- **Storage Location:**
  - Shadow copies are stored in a hidden system volume information folder on each volume, typically as "System Volume Information" on the root.

Deleted Files and File Carving

Deleted Files and File Carving

- **Definition:**
  - Identifies and extracts file fragments based on known file signatures or header/footer patterns.
  - Particularly useful when file system metadata is damaged or missing.
- **Header/Footer Signatures:**
  - Each file type (e.g., JPEG, PDF, DOCX) has unique signatures at the beginning (header) and end (footer) of the file.
- **Fragmented Files:**
  - File carving can reconstruct fragmented files by identifying and combining related fragments.
- **Challenges:**
  - Carved files may lack meaningful filenames or directory structures, making it challenging to organize and interpret the recovered data.

How Deleted Files Leave Traces In The File System?

- **File System Metadata:**
  - In file systems like NTFS (New Technology File System) or FAT (File Allocation Table), information about files is stored in data structures like the Master File Table (MFT) or File Allocation Table. When a file is deleted, the associated metadata in these tables is often marked as available, but the actual data may remain intact until overwritten.
- **Directory Entries:**
  - Directory entries or file entries in directories may still contain references to the deleted file. These entries are not immediately removed but are marked as available for reuse.
- **Journaling:**
  - NTFS uses journaling mechanisms to log changes. Even after deletion, entries about the file deletion may exist in the journal until subsequent changes occur.

How Deleted Files Leave Traces In The File System?

- **File Slack:**
  - File slack refers to the space between the end of a file and the end of its allocated disk cluster. When a file is deleted, this slack space may still contain remnants of the file's data.
- **Unallocated Clusters:**
  - The clusters that once held the file's data are marked as unallocated, but until they are overwritten by new data, the original file content may still be recoverable.
- **System Restore Points and Shadow Copies:**
  - In systems with features like System Restore or Volume Shadow Copy, deleted files may be retained in these backups for a certain period, allowing potential recovery.

File Carving Tools

- PhotoRec
- Scalpel
- Foremost
- ExifTool
- The Sleuth Kit (TSK)
- Autopsy

Sleuthkit (TSK)

Key Features:

- **File System Analysis:** TSK supports the analysis of various file systems, including FAT, NTFS, exFAT, Ext2/3/4, UFS, HFS+, and other file systems.
- **Metadata Extraction:** It allows forensic investigators to extract metadata information from files, such as timestamps, permissions, and ownership details.
- **Timeline Analysis:** Facilitates the creation of timelines, helping investigators understand the sequence of events on a system.
- **File Carving:** TSK includes tools for file carving, enabling the recovery of files from unallocated space or damaged file systems.
- **Hash Calculations:** TSK can compute hash values for files, aiding in data integrity verification.

Sleuthkit (TSK) & File System Layers

The Sleuthkit Tools are divide into 5 categories which loosely map to the file system layers.

- File system layer tools – prefixed by "fs"
- Data layer tools – prefixed by "blk"
- Metadata layer tools – prefixed by "i" (for inode)
- File Name layer tools – prefixed by "f"
- Misc. tools – no standard prefix, but relate to lower level sort and find operations in file system structure.

Autopsy

Key Features:

- User-Friendly Interface
- Cross-Platform Compatibility
- Integration with The Sleuth Kit (TSK)
- Automated Analysis
- Keyword Search and Filtering
- Timeline Analysis
- File Carving
- Artifact Analysis
- Report Generation

SANS Artifacts – Disk Forensics

SANS artifacts categorization

Category Name	Artifacts
System Information	OS Version, Computer Name, System Boot & Autoruns, System Last Shutdown Time
Application Execution	User Assist, Windows 10 Timeline, Shimcache, **Jump Lists**, Amcache.hve, **System Resource Usage Monitor (SRUM),** BAM/DAM, Last-Visited MRU, **Prefetch**, etc.
File/Folder Opening	Open/Save MRU, **Recent Files**, Jump Lists, Shell Bags, **Shortcut (LNK) Files**, Last-Visited MRU, IE|Edge file://
Deleted File or File Knowledge	**Windows Search Database**, **Thumbscache, Thumbs.db**, IE|Edge File://, Search–WordWheelQuery, **Recycle Bin**, User Typed Paths
Cloud Storage	OneDrive, Google Drive, Box Drive, Dropbox

Deleted File or File Knowledge

- Windows Search Database
- Thumbnails & Thumbcache
- Recycle Bin

Windows Search Database (windows.db/edb) (1/2)

- **Location:**
  - "C:\ProgramData\Microsoft\Search\Data\Applications\Windows" directory.
  - Size can vary based on the amount of indexed data.
- **Indexed Content:**
  - Contains information about files, emails, documents, and other user-specific data.
  - Indexing includes details like file names, metadata, and properties.
- **Windows Search Index Artifacts:**
  - **File Name**
  - **File Path**
  - **Created Date/Time**
  - **Modified Date/Time**
  - **Accessed Date/Time**
- **Database Format:**
  - Structured in a database format optimized for search operations.
  - Utilizes the Extensible Storage Engine (ESE) format for efficient data storage and retrieval.
  - The database is continuously updated by the Windows Search service.
  - Indexing occurs in the background to reflect changes in the file system.

Windows Search Database (windows.edb) (2/2)

ESEDatabaseView:

File Edit View Options Help

SystemIndex_PropertyStore [Table ID = 17, 598 Columns]

WorkID	4631F-System_Search_GatherTime	13F-System_Size	15F-System_DateModified	16F-System_DateCreated	4447-System_ItemPathDisplay	4625-System_Search_AutoSummary	4450-System_ItemType
1276	32 F7 4D 27 14 42 D9 01	2A 2A 2A 2A 2A 2A 2A 2A	2A 2A 2A 2A 2A 2A 2A 2A	2A 2A 2A 2A 2A 2A 2A ...	\\{S-1-5-21-29705265-400737687-482427116-1001}\LS\Desktop\Act...		ActivityHistoryItem
1275	76 3E 8F 26 14 42 D9 01	2A 2A 2A 2A 2A 2A 2A 2A	2A 2A 2A 2A 2A 2A 2A 2A	2A 2A 2A 2A 2A 2A 2A ...	\\{S-1-5-21-29705265-400737687-482427116-1001}\LS\Desktop\Act...		ActivityHistoryItem
1274	8B 73 32 0B 14 42 D9 01	32 00 00 00 00 00 00 00	BA 00 DC 05 14 42 D9 01	44 72 4D E7 13 42 D9 01	C:\Users\ \Desktop\StrozFriedberg-Example.txt	Example File from Stroz Friedberg.Happy Testing!	.txt
1273	9A 2C 72 06 14 42 D9 01	2A 2A 2A 2A 2A 2A 2A 2A	2A 2A 2A 2A 2A 2A 2A 2A	2A 2A 2A 2A 2A 2A 2A ...	\\{S-1-5-21-29705265-400737687-482427116-1001}\LS\Desktop\Act...		ActivityHistoryItem
1269	9E 0E 8B 67 88 40 D9 01	2A 2A 2A 2A 2A 2A 2A 2A	2A 2A 2A 2A 2A 2A 2A 2A	2A 2A 2A 2A 2A 2A 2A ...	\\{S-1-5-21-29705265-400737687-482427116-1001}\LS\Desktop\Act...		ActivityHistoryItem
1268	F1 56 8D 67 88 40 D9 01	2A 2A 2A 2A 2A 2A 2A 2A	2A 2A 2A 2A 2A 2A 2A 2A	2A 2A 2A 2A 2A 2A 2A ...	\\{S-1-5-21-29705265-400737687-482427116-1001}\LS\Desktop\Act...		ActivityHistoryItem

Thumbnails & Thumbcache

- **Definition:**
  - "Thumbnails" are small, reduced-size versions of images or videos used for quick identification and preview purposes.
  - "Thumbcache" refers to the cache or database that stores these thumbnail images to enhance system performance.
- **Purpose:**
  - Thumbnails provide a visual preview of image or video content, aiding users in quickly identifying files.
  - Thumbcache optimizes the retrieval and display of these thumbnails, improving overall system responsiveness.
- **Storage Location:**
  - Thumbnails are stored in the "Thumbs.db" hidden file in each directory containing images.
  - Thumbcache databases are typically located in the "C:\Users<Username>\AppData\Local\Microsoft\Windows\Explorer" directory.
- **File Types Supported:**
  - Thumbnails can be generated for a variety of image and video file formats, including JPEG, PNG, GIF, and others.
  - Thumbcache accommodates different file types and formats to provide a comprehensive preview experience.
- **Forensic Significance:**
  - Examination of "Thumbs.db" and thumbcache databases can reveal user interactions with image and video files.
  - Timestamps and file associations within these files can be of forensic interest during investigations.

Recycle Bin – Dumpster Diving Technique

C:\$Recycle.Bin

C:\Windows\System32\cmd.exe

```
C:\$Recycle.Bin>
```

```
C:\$Recycle.Bin>dir /a
 Volume in drive C has no label.
 Volume Serial Number is [redacted]

 Directory of C:\$Recycle.Bin

20. 02. 2019  19:44    <DIR>          .
06. 12. 2022  10:37    <DIR>          ..
20. 02. 2019  19:44    <DIR>          S-1-5-18
20. 02. 2019  18:45    <DIR>          S-1-5-21-[redacted]-1000
02. 12. 2022  12:07    <DIR>          S-1-5-21-[redacted]-1001
               0 File(s)              0 bytes
               5 Dir(s)  [redacted]
```

```
C:\$Recycle.Bin>wmic useraccount get name,sid
Name                 SID
Administrator        S-1-5-21-[redacted]-500
DefaultAccount       S-1-5-21-[redacted]-503
Guest                S-1-5-21-[redacted]-501
[redacted]           S-1-5-21-[redacted]-1001
WDAGUtilityAccount   S-1-5-21-[redacted]-504
```

```
06. 12. 2022  11:51                72 $IPOEO2Y.jpg
25. 02. 2019  10:23         1.258.261 $RPOEO2Y.jpg
```

Application Execution - Evidence of Execution

- Prefetch
- SRUM
- ActivitiesCache.db
- Jumplists

Prefetch

- **Prefetch:**
  - *Windows feature storing data on program execution.*
  - Location: C:\Windows\Prefetch by default
- **Forensic Significance:**
  - *Detailed information on executed programs.*
  - *Reveals program execution times and frequency.*
  - *Assists in investigating security incidents.*
  - *Critical for understanding the timeline of malware execution.*
  - *Supports incident response, forensic investigations, and litigation.*

Name	Date created	Date modified
ZOOM_CM_FTOIGFK88Z9VVRZO4_M-F-B8542E79.pf	8/16/2022 2:01 PM	8/16/2022 2:01 PM
ZOOM.EXE-87652BD0.pf	8/18/2022 1:48 PM	8/18/2022 2:34 PM

Prefetch

- **Applications in Digital Forensics:**
  - *Determines user activities and program usage.*
  - *Identifies attempts to hide or delete evidence through tools like CCleaner.*
  - *Provides evidence of data transfer using cloud storage programs.*
- **Malware Detection:**
  - *Critical for detecting malicious software on a computer.*
  - *Reveals execution times and locations of malware.*
  - *Aids in understanding the source and arrival of malicious files.*
- **Useful Information:**
  - *Programs executed by the user.*
  - *Timestamps of program execution.*
  - *Insights into potential evidence tampering or spoliation.*

Prefetch Tools

- **Tools:**
  - Pecmd (Zimmerman)
  - WinPrefetchView (NirSoft Tools Suite)

```
PS C:\Users\SANSDFIR\Desktop\SANS Summit\ZimmermanTools> .\PECmd.exe -d E:\Windows\Prefetch\ --csv 'C:\Users\SANSDFIR\Desktop\SANS Summit\Prefetch' -q
PECmd version 1.5.0.0

Author: Eric Zimmerman (saueriz.zimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -d E:\Windows\Prefetch\ --csv C:\Users\SANSDFIR\Desktop\SANS Summit\Prefetch -q

Keywords: temp, tmp

Looking for prefetch files in E:\Windows\Prefetch\


Found 212 Prefetch files

---------- Processed E:\Windows\Prefetch\AM_DELTA.EXE-F5818816.pf in 0.03530010 seconds ----------
---------- Processed E:\Windows\Prefetch\AM_DELTA_PATCH_1.289.1184.0.E-2FF65020.pf in 0.00785820 seconds ----------
---------- Processed E:\Windows\Prefetch\AM_DELTA_PATCH_1.289.1368.0.E-357D79E4.pf in 0.00555800 seconds ----------
---------- Processed E:\Windows\Prefetch\AM_DELTA_PATCH_1.289.1380.0.E-DACAA516.pf in 0.03133030 seconds ----------
---------- Processed E:\Windows\Prefetch\APPLICATIONFRAMEHOST.EXE-8CF44CC4.pf in 0.02492180 seconds ----------
---------- Processed E:\Windows\Prefetch\AUDIODG.EXE-D0D776AC.pf in 0.00066740 seconds ----------
---------- Processed E:\Windows\Prefetch\AUTHHOST.EXE-B8024503.pf in 0.01631570 seconds ----------
---------- Processed E:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-0F542490.pf in 0.02383690 seconds ----------
---------- Processed E:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-1354AC27.pf in 0.00707280 seconds ----------
---------- Processed E:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-1D0C3899.pf in 0.01143630 seconds ----------
---------- Processed E:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-7F828CDF.pf in 0.00561540 seconds ----------
---------- Processed E:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-E5F71E86.pf in 0.02020920 seconds ----------
---------- Processed E:\Windows\Prefetch\BACKGROUNDTRANSFERHOST.EXE-EFD1BB7A.pf in 0.01954698 seconds ----------
---------- Processed E:\Windows\Prefetch\BDEUISRV.EXE-1E4955b7.pf in 0.01329730 seconds ----------
---------- Processed E:\Windows\Prefetch\BDEUNLOCK.EXE-C5D4009E.pf in 0.01309970 seconds ----------
---------- Processed E:\Windows\Prefetch\BITLOCKERWIZARDELEV.EXE-E4CCF1D7.pf in 0.00157350 seconds ----------
---------- Processed E:\Windows\Prefetch\BROWSER_BROKER.EXE-DDA21E2B.pf in 0.01133160 seconds ----------
---------- Processed E:\Windows\Prefetch\BYTECODEGENERATOR.EXE-883FEF7D.pf in 0.00133840 seconds ----------
```

System Resource Utilization Monitor (SRUM)

- **Overview:**
  - Tracks resource utilization by applications and processes.
  - SRUM is designed to collect and store data about resource usage, such as network, CPU, memory, and disk activity, providing insights into system behavior.
  - Path information to see what other binaries have executed from a location, giving us further indicators to pivot from.
- **Location:**
  - SRUM data is stored in a database in **%SystemRoot%\System32\sru\SRUDB.dat**
- **SRUM Artifacts:**
  - network data usage & network connectivity,
  - application execution,
  - other resource-related activities (Bytes send/received per application, user account, file read/write bytes, etc).
- **Tools:**
  - SrumEcmd (Zimmerman Tools)

System Resource Utilization Monitor (SRUM)

Artifacts

MATCHING RESULTS	1,312
OPERATING SYSTEM	1,312
SRUM Application Resource Usage	1,102
SRUM Network Usage	210

MATCHING RESULTS (1,102 of 1,189)

Column view

Entry...	Application Name	Full Path	Recorded Timest...	Secu
850	VGAuthService.exe	\Device\HarddiskVolume3\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthServ...	9/13/2022 3:25:00 PM	S-1-5-
913	VGAuthService.exe	\Device\HarddiskVolume3\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthServ...	9/13/2022 3:34:00 PM	S-1-5-
995	VGAuthService.exe	\Device\HarddiskVolume3\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthServ...	9/13/2022 4:46:00 PM	S-1-5-
1107	VGAuthService.exe	\Device\HarddiskVolume3\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthServ...	9/16/2022 6:22:00 PM	S-1-5-
1140	VMwareResolutionSet.exe	\Device\HarddiskVolume3\Program Files\VMware\VMware Tools\VMwareResolutionSet.exe	9/16/2022 6:22:00 PM	S-1-5-
1070	x32dbg.exe	\Device\HarddiskVolume3\Program Files\x64dbg\release\x32\x32dbg.exe	9/16/2022 6:22:00 PM	S-1-5-
1071	x64dbg.exe	\Device\HarddiskVolume3\Program Files\x64dbg\release\x64\x64dbg.exe	9/16/2022 6:22:00 PM	S-1-5-
676	py.exe	\Device\HarddiskVolume3\ProgramData\Package Cache\09F30201CB638C537D688461EC3A1B...	9/8/2022 3:22:00 PM	S-1-5-
1086	@WanaDecryptor@.exe	\Device\HarddiskVolume3\ProgramData\qchpkpkovx300\@WanaDecryptor@.exe	9/16/2022 6:22:00 PM	S-1-5-
1144	@WanaDecryptor@.exe	\Device\HarddiskVolume3\ProgramData\qchpkpkovx300\@WanaDecryptor@.exe	9/16/2022 6:22:00 PM	S-1-5-
1145	taskhsvc.exe	\Device\HarddiskVolume3\ProgramData\qchpkpkovx300\TaskData\Tor\taskhsvc.exe	9/16/2022 6:22:00 PM	S-1-5-
1164	taskdl.exe	\Device\HarddiskVolume3\ProgramData\qchpkpkovx300\taskdl.exe	9/16/2022 6:22:00 PM	S-1-5-

Artifacts

MATCHING RESULTS	6
OPERATING SYSTEM	6
SRUM Application Resource Usage	6

MATCHING RESULTS (6 of 1,189)

Column view

Entry...	Application Name	Full Path	Recorded Timesta...	S
1086	@WanaDecryptor@.exe	\Device\HarddiskVolume3\ProgramData\qchpkpkovx300\@WanaDecryptor@.exe	9/16/2022 6:22:00 PM	S-
1144	@WanaDecryptor@.exe	\Device\HarddiskVolume3\ProgramData\qchpkpkovx300\@WanaDecryptor@.exe	9/16/2022 6:22:00 PM	S-
1145	taskhsvc.exe	\Device\HarddiskVolume3\ProgramData\qchpkpkovx300\TaskData\Tor\taskhsvc.exe	9/16/2022 6:22:00 PM	S-
1164	taskdl.exe	\Device\HarddiskVolume3\ProgramData\qchpkpkovx300\taskdl.exe	9/16/2022 6:22:00 PM	S-
1143	tasksche.exe	\Device\HarddiskVolume3\ProgramData\qchpkpkovx300\tasksche.exe	9/16/2022 6:22:00 PM	S-
1148	taskse.exe	\Device\HarddiskVolume3\ProgramData\qchpkpkovx300\taskse.exe	9/16/2022 6:22:00 PM	S-

ActivitiesCache.db (1/2)

- **Definition:**
  - "ActivitiesCache.db" is a database file used by Windows to store information related to the Timeline feature.
  - The Timeline feature, introduced in Windows 10, allows users to review and resume past activities and open files across different devices.
  - Timestamps associated with each recorded activity allow for chronological tracking of user actions.
- **Location:**
  - **Data** from the Timeline are stored on disk in user profile directory – in folder %userprofile%\AppData\Local\ConnectedDevicesPlatform\.
  - **User´s activity** is stored in folder L.<username>, for example L.joe. Information is recorded in SQLite database ActivitiesCache.db.

Contents:

- The database contains information about user activities, including opened files, applications, and timestamps, details about document openings, application launches, and other user interactions.

- **Tools:**
  - WxTCMD (Zimmerman Tools)

ActivitiesCache.db (2/2)

ActivityTyp	ActivityType	Executable	DisplayText	ContentInfo	Payload	ClipboardPayload	StartTime	EndTime	Duration	LastMod
5	ExecuteOpen	System32\notepad.exe	Notepad		{"displayText":"Notepad","activationUri":"ms-shellactivity:","appDisplayName":"Notepad","backgroundColor":"black"}		9/6/2021 11:25			9/6/2
5	ExecuteOpen	System32\notepad.exe	pshashes.txt (Notepad)	C:\Users\ar	{"displayText":"pshashes.txt","activationUri":"ms-shellactivity:","appDisplayName":"Notepad","description":"C:\\Users\\amy.LAB\\Desktop\\pshashes.txt","backgroundColor":"black","contentUri":"file:///C:/Users/amy.LAB/Desktop/pshashes.txt?VolumeId={054B9B6F-9AAE-4C36-8B6E-96EB74351608}&ObjectId={AF887C99-0B06-11EC-955C-000C297B9B88}&KnownFolderId=ThisPCDesktopFolder&KnownFolderLength=24"}		9/6/2021 11:25			9/6/2
6	InFocus	System32\notepad.exe			{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":3,"shellContentDescription":{"MergedGap":600,"ActivityEngagementFlags":3},"userTimezone":"Europe/Budapest"}		9/6/2021 11:25	9/6/2021 11:25	0:00:03	9/6/2
6	InFocus	System32\cmd.exe			{"type":"UserEngaged","reportingApp":"ShellActivityMonitor","activeDurationSeconds":93274,"shellContentDescription":{"MergedGap":600,"ActivityEngagementFlags":0},"userTimezone":"Europe/Budapest"}		8/25/2021 9:50	9/7/2021 13:29	13.03:39:1	9/7/2

Jumplists

- **Definition:**
  - Allow users to "jump" or access items they have frequently or recently. This can include files, applications, and directories to name the major items of significance for forensic investigations.
  - The data stored in the AutomaticDestinations directory contains a unique file for each application prepended with a unique Application ID.
- **Location:**
  - C:%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
- **Forensic Significance:**
  - The Jump List files contain information relating to program execution times, execution count and local file paths of the application being investigated.
  - Proof that an application existed in the system.
- **Tools:**
  - JLEcmd & JumpListExplorer (Zimmerman Tools)

Jumplists

```
C:\Users\lrocha\Desktop\JLECmd>JLECmd.exe -f E:\LAB\BackupExecProfile\Recent\
AutomaticDestinations\9b9cdc69c1c24e2b.automaticDestinations-ms --fd | more
JLECmd version 0.9.9.0

(..)

--- AppId information ---
  AppID: 9b9cdc69c1c24e2b
  Description: Notepad (64-bit)

--- DestList information ---
  Expected DestList entries:  5
  Actual DestList entries: 5
  DestList version: 1

--- DestList entries ---
Entry #: 5
  MRU: 0
  Path: C:\Windows\Temp\tmp.txt
  Pinned: False
  Created on: 2017-11-12 12:47:15
  Last modified: 2017-11-12 12:58:17
  Hostname: chesrv002
  Mac Address: 00:0c:29:69:b5:10

--- Lnk information ---

  Lnk target created: 2017-11-12 12:53:29
  Lnk target modified: 2017-11-12 12:53:29
  Lnk target accessed: 2017-11-12 12:53:29

--- Header ---
  Target created:  2017-11-12 12:53:29
  Target modified: 2017-11-12 12:53:29
  Target accessed: 2017-11-12 12:53:29

  File size: 6,287
  Flags: HasTargetIdList, HasLinkInfo, IsUnicode, DisableKnownFolderTracking,
AllowLinkToLink
  File attributes: FileAttri[illegible]hive
  Icon index: 0
  Show window: SwNormal (Activates and displays the window. The window is restored to
its original s
ize and position if the window is minimized or maximized.)

(..)

  -File ==> tmp.txt
    Short name: tmp.txt
    Modified: 2017-11-12 12:53:30
    Extension block count: 2

    --------- Block 0 (Beef0004) ---------
    Long name: tmp.txt
    Created: 2017-11-12 12:53:30
    Last access: 2017-11-12 12:53:30
    MFT entry/sequence #: 77153,5 (0x12D61/0x5)
    --------- Block 1 (Beef001a) ---------
    File document type: txtfile

(..)
```

AppID 9b9cdc69c1c24e2b is associated with Notepad

Entry that shows this file was opened with Notepad

Standart Information timestamps about the .lnk file

Standart Information timestamps about the target file.

File size

$MFT Entry number for tmp.txt. Usefull if the file was deleted and we want to attempt it to recover

File / Folder Opening

- Shortcut (.lnk) files

Shortcut (.lnk) files

- **Definition:**
  - Shortcut files automatically created by windows when accessing recent items and opening local and remote data files and documents.
  - Windows 11 contains a shortcut (.LNK) files that direct to the application, file, or directory.
- **Location:**
  - C:%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\
- **Forensic Significance:**
  - In digital forensics, examining .lnk files can reveal user behavior, recent activities, and frequently accessed programs or files.
  - LNKTarget File (Internal LNK file details) Details:
    - Modified, Accessed and creation times of target file
    - Volume information
    - Network Share information
    - Original location
    - Name of system
- **Tools:**
  - Lecmd (Zimmerman Tools)

Shortcut (.lnk) files

```
PS C:\Temp> .\LECmd.exe -f "C:\Users\eric\Desktop\X-Ways Forensics 32-bit.lnk"
LECmd version 0.9.5.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

Command line: -f C:\Users\eric\Desktop\X-Ways Forensics 32-bit.lnk

Processing 'C:\Users\eric\Desktop\X-Ways Forensics 32-bit.lnk'

Source file: C:\Users\eric\Desktop\X-Ways Forensics 32-bit.lnk
  Source created:  2016-09-15 13:59:01
  Source modified: 2017-04-05 13:04:18
  Source accessed: 2016-09-15 13:59:01

--- Header ---
  Target created:  2016-08-31 15:21:50
  Target modified: 2016-09-15 22:09:02
  Target accessed: 2016-08-31 15:21:50

  File size: 3,820,672
  Flags: HasTargetIdList, HasLinkInfo, HasName, HasRelativePath, IsUnicode, RunAsUser
  File attributes: FileAttributeArchive
  Icon index: 0
  Show window: SwNormal (Activates and displays the window. The window is restored to

Name: X-Ways Forensics 32-bit
Relative Path: ..\..\..\xwf\xwforensics.exe

--- Link information ---
Flags: VolumeIDAndLocalBasePath

--- Volume information ---
  Drive type: Fixed storage media (Hard drive)
  Serial number: FC72BA1F
  Label: (No label)
  Local path: C:\xwf\xwforensics.exe

--- Target ID information (Format: Type ==> Value) ---

  Absolute path: My Computer\C:\xwf\xwforensics.exe

  -Root folder: GUID ==> My Computer
```

Labs

- Lab #4 - Use Autopsy

Thank you for your patience!