# Windows Forensics Analysis

**Mohammed AlHumaid**

**January 6, 2022**

**V 1.0**

# Introduction

Digital forensics is a branch of forensic science encompassing the recovery, investigation, examination and analysis of material found in digital devices, often in relation to mobile devices and computer crime.

In this project, I focused on Windows Forensic Analysis that contains all forensic artifacts in one simple PDF file that describing the Windows artifact, forensic value, location, required tool, and final output using only #open_source forensic tools. This will help DFIR investigators get better and faster evidence during Windows forensic investigations with #ZERO money cost instead of using commercial DFIR tools.

Scope in this release (v 1.0) are Windows artifacts on Windows 10 and Windows Servers only.

Highly recommend those working in DFIR to favorited it or print it out for use as a reference during digital forensic analysis or in cyber incidents.

# Covered Windows Forensic Artifacts

| Artifact | Artifact | Artifact |
|---|---|---|
| Thumbcache | Alternate Data Streams (ADS) | SYSTEM |
| Jump Lists | Link File – Shortcut (.lnk) | Windows Error Reporting (WER) |
| Recycle Bin | RDP Bitmap Cache (BMC) | EventTranscript.db |
| Prefetch Files | UserAssist | Volume Shadow Copy Service (VSS) |
| ShimCache | WordWheelQuery | User Access Logging (UAL) |
| Amcache | NTUSER.DAT | PowerShell |
| System Resource Usage Monitor (SRUM) | ShellBags | lsass.exe |
| Master File Table ($MFT) | Background Activity Moderator (BAM) / (DAM) | Windows.edb |
| Windows 10 Timeline (ActivitiesCache) | Security Account Manager (SAM) | sysmain.sdb |
| $J | SECURITY | Windows Registry Hive |
| $LogFile | SOFTWARE | Forensically interesting spots in Windows Registry |

# Thumbcache

**What is it?**

When the user views from the Windows folder viewing options, a small thumbnail version of the pictures will be created and stored in a single file. This file stores a thumbnail version of the existing and deleted pictures.
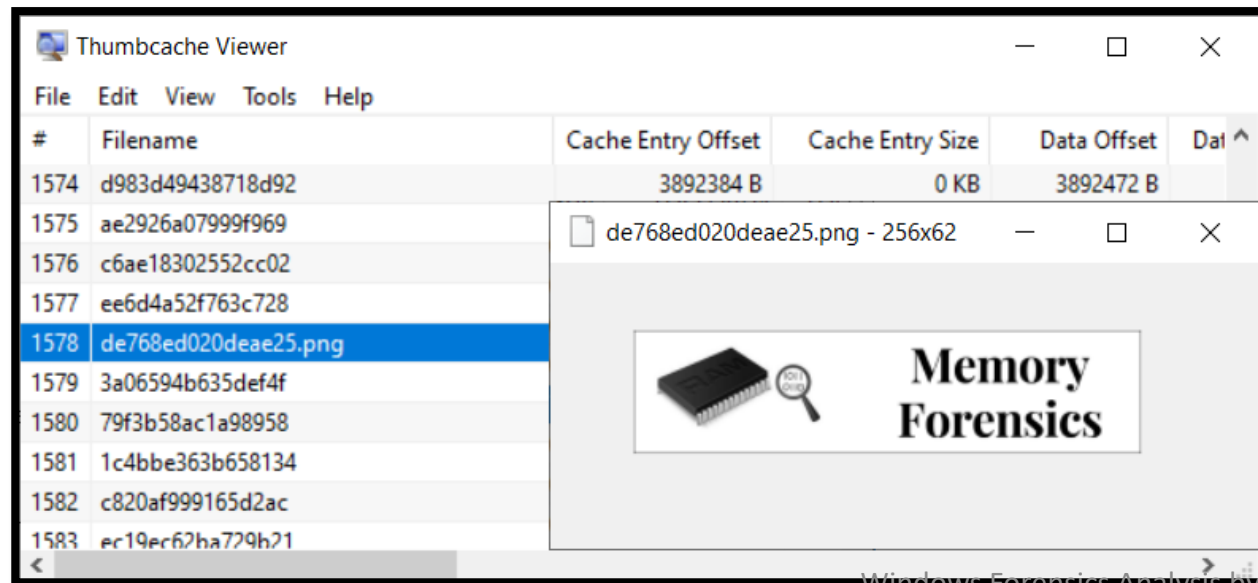
**Forensic Value:**

1. Evidences of deleted pictures
2. Recover deleted pictures
3. Good clue about the pictures contents that used

**Location:**

%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer

**Tool:**

thumbcache_viewer.exe , thumbs_viewer.exe

# Jump Lists

## What is it?

Provides the user with a graphical interface associated with each installed application which lists files that have been previously accessed by that application.

| SourceCreated | SourceModified | AppId | AppIdDescription | TargetIDAbsolutePath |
|---|---|---|---|---|
| 2/9/2021 20:29 | 9/28/2021 21:35 | 7e4dca80246863e3 | Control Panel - Settings | Control Panel\System and Security\System |
| 2/9/2021 20:29 | 9/28/2021 21:35 | 7e4dca80246863e3 | Control Panel - Settings | All Tasks\Uninstall a program |
| 2/9/2021 20:29 | 9/28/2021 21:35 | 7e4dca80246863e3 | Control Panel - Settings | Control Panel\Network and Internet\Network and Sharing Center |
| 2/9/2021 20:29 | 9/28/2021 21:35 | 7e4dca80246863e3 | Control Panel - Settings | Control Panel\Programs\Programs and Features |
| 2/9/2021 20:29 | 9/28/2021 21:35 | 7e4dca80246863e3 | Control Panel - Settings | Control Panel\Hardware and Sound\Power Options |

| TargetAccesse | AppIdDescription | LocalPath | TargetIDAbsolutePath | Arguments |
|---|---|---|---|---|
| 2/21/2021 21:11 | Remote Desktop Connection 6.1.7600 (Win7) | C:\Windows\System32\mstsc.exe | My Computer\C:\Windows\System32\mstsc.exe | /v:"172.16.151.50" |
| 5/5/2021 3:53 | Remote Desktop Connection 6.1.7600 (Win7) | C:\Windows\System32\mstsc.exe | My Computer\C:\Windows\System32\mstsc.exe | /v:"172.16.151.150" |
| 5/19/2021 23:51 | Remote Desktop Connection 6.1.7600 (Win7) | C:\Windows\System32\mstsc.exe | My Computer\C:\Windows\System32\mstsc.exe | /v:"172.16.85.104:65520" |
| 5/24/2021 7:20 | Remote Desktop Connection 6.1.7600 (Win7) | C:\Windows\System32\mstsc.exe | My Computer\C:\Windows\System32\mstsc.exe | /v:"172.16.85.103" |

## Forensic Value:

1. User activity who have interactively on system
2. Recover user's traces of recently accessed directories from the Windows Explorer jump list
3. History of attempted lateral movement by checking Remote Desktop jump lists, as they provide a list of recent connections
4. Destination IPs and ports via RDP

## Location:

%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

%USERPROFILE%\AppData\Microsoft\Windows\Recent\CustomDestinations (via Taskbar)

## Tool:

JLECmd.exe

# Recycle Bin

## What is it?

When the user deletes a file, the file is moved into a temporary storage location for deleted files named Recycle Bin. Windows creates two files each time a file is placed in the Recycle Bin **$I** and **$R** with string six character identifier generated for each file. **$R file is a renamed copy of the "deleted"** file. While the **$I file replaces the usage INFO2 file as the source of accompanying metadata**.
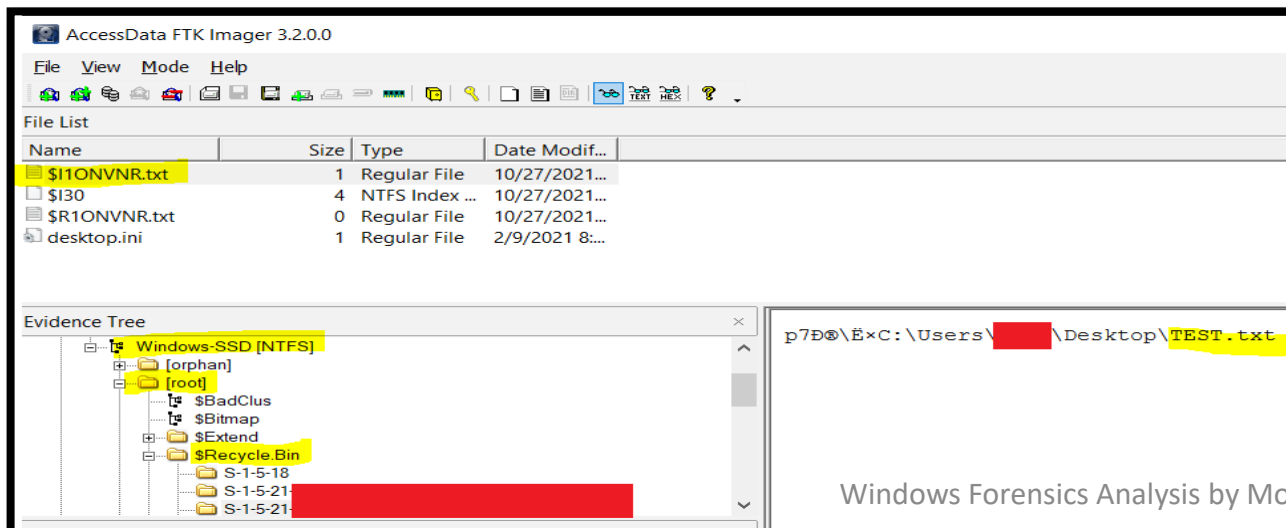
## Forensic Value:

1. The original file name and path
2. The deleted file size
3. The date and time of deletion

## Location:

$Recycle.Bin

## Tool:

RBCmd.exe , Rifiuti2, Recbin.exe, EnCase, FTK, Autopsy, RecycleDump.py , $I_Parse.exe

# Prefetch Files

## What is it?

They are a performance optimization mechanism to reduce boot and application loading times. The cache manager can use these prefetch files like a " cheat sheet " to speed up the loading process. Prefetch is not enabled by default on Windows servers.

| | A | B |
|---|---|---|
| 1 | RunTime | ExecutableName |
| 2 | 10/30/2021 20:21 | \VOLUME{01d4207de1e70a8f-58e49381}\USERS █████████████ \DFIR\PREFETCH\PECMD.EXE |
| 3 | 10/30/2021 20:21 | \VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\CMD.EXE |
| 4 | 10/30/2021 20:21 | \VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\CONHOST.EXE |
| 5 | 10/30/2021 20:21 | \VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\NOTEPAD.EXE |
| 6 | 10/30/2021 20:20 | \VOLUME{01d4207de1e70a8f-58e49381}\USERS█████\APPDATA\LOCAL\MICROSOFT\ONEDRIVE\21.196.0921.0007\FILECOAUTH.EXE |
| 7 | 10/30/2021 20:20 | \VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\SVCHOST.EXE |
| 8 | 10/30/2021 20:20 | \VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\SVCHOST.EXE |
| 9 | 10/30/2021 20:20 | \VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\SVCHOST.EXE |
| 10 | 10/30/2021 20:20 | \VOLUME{01d4207de1e70a8f-58e49381}\PROGRAM FILES\MICROSOFT OFFICE\ROOT\OFFICE16\EXCEL.EXE |
| 11 | 10/30/2021 20:20 | \VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\WBEM\WMIPRVSE.EXE |
| 12 | 10/30/2021 20:19 | \VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\BACKGROUNDTASKHOST.EXE |
| 13 | 10/30/2021 20:19 | \VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\RUNTIMEBROKER.EXE |
| 14 | 10/30/2021 20:15 | \VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\SNIPPINGTOOL.EXE |
| 15 | 10/30/2021 20:14 | \VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\BACKGROUNDTASKHOST.EXE |
| 16 | 10/30/2021 20:14 | \VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\RUNTIMEBROKER.EXE |

## Forensic Value:

1. The executable's name
2. The absolute Path to the executable
3. The number of times that the program ran within the system
4. The last time the application ran
5. A list of DLLs used by the program

## Location:

%SystemRoot%\prefetch

## Tool:

PECmd.exe , WinPrefetchView.exe

| | A | B | C | D | E | F | G | H | I | J | K | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ExecutableName | Size | RunCount | LastRun | PreviousRun0 | PreviousRun1 | PreviousRun2 | PreviousRun3 | PreviousRun4 | PreviousRun5 | PreviousRun6 | Directories |
| | ZOOM.EXE | 492350 | 54 | 8/26/2021 17:48 | 8/25/2021 9:56 | 8/25/2021 9:51 | 8/25/2021 9:34 | 8/25/2021 9:31 | 8/17/2021 9:22 | 8/17/2021 9:19 | 8/17/2021 9:17 | \VOLUME{01 |

# ShimCache

**What is it?**

Allows Windows to track executable files and scripts that may require special compatibility settings to properly run. It is maintained within kernel memory and serialized to the registry **upon system shutdown or restart.**

**Forensic Value:**

1. The executable or script file names and full paths
2. The standard information last modified date
3. The size of the binary
4. Finally, whether the file actually ran on the system (just browsed through explorer.exe)

**Location:**

HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache

**Tool:**

AppCompatCacheParser.exe

| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| | ControlSet | CacheEntryPosition | Path | LastModifiedTimeUTC | Executed | Duplicate | SourceFile |
| | 1 | 898 | C:\Program Files\Wireshark\extcap\USBPcapCMD.exe | 5/22/2020 9:01 | NA | FALSE | Live Registry |
| | 1 | 637 | C:\Users[    ]\Desktop\HxDSetup.exe | 2/28/2020 11:32 | NA | FALSE | Live Registry |
| | 1 | 634 | C:\Program Files\HxD\HxD.exe | 2/28/2020 9:25 | NA | FALSE | Live Registry |
| | 1 | 142 | C:\Users[    ]\DFIR\$J & $LogFile\sqlite3.exe | 1/1/2020 23:59 | NA | FALSE | Live Registry |
| | 1 | 143 | C:\Users[    ]\DFIR\$J & $LogFile\LogFileParser.exe | 1/1/2020 23:59 | NA | FALSE | Live Registry |
| | 1 | 157 | C:\Users[    ]sqlite3.exe | 1/1/2020 23:59 | NA | FALSE | Live Registry |
| | 1 | 160 | C:\Users[    ]LogFileParser.exe | 1/1/2020 23:59 | NA | FALSE | Live Registry |

# Amcache

**What is it?**

The Amcache.hve is a registry hive file stores information related to execution of programs when a user performs certain actions such as running host-based applications, installation of new applications, or running portable applications from external devices.

**Forensic Value:**
1. The executable names and full paths
2. Last executed time
3. The size of the binary and its version
4. The executable hash (SHA1)

**Location:**

C:\Windows\appcompat\Programs\Amcache.hve

**Tool:**

AmcacheParser.exe , RegRipper (rr.exe)

| | A | B | C | D | E | |
|---|---|---|---|---|---|---|
| 1 | ApplicationName | FileKeyLastWriteTim | SHA1 | FullPath | Name | ProductName |
| 46 | E0469640.LenovoUtility | 10/3/2021 2:02 | bf4a6a148bc020ababa121c0ead6b139fbfcbc6f | c:\program files\windowsapps\e0469640.lenovou | LenovoUtilityUI.exe | lenovo hotkeys |
| 47 | E0469640.LenovoUtility | 10/3/2021 2:02 | b638cf6f42ee38c8fbad13eece36190ce2748ecb | c:\program files\windowsapps\e0469640.lenovou | utility.exe | lenovo hotkeys |
| 48 | E046963F.LenovoCompanion | 8/29/2021 13:15 | 9891831aab7f629fc09232d0551b5fbbf6283f8a | c:\program files\windowsapps\e046963f.lenovoc | DeployAssistant.exe | deployassistant |
| 49 | E046963F.LenovoCompanion | 8/29/2021 13:15 | 6dc45ea51d7c66599500081ed35c82b999ddc884 | c:\program files\windowsapps\e046963f.lenovoc | LenovoVantage.exe | lenovovantageuwp |
| 50 | DolbyLaboratories.DolbyAudio | 2/14/2021 18:52 | d5ea2346a435b19b1e04098fc86a1f7589053341 | c:\program files\windowsapps\dolbylaboratories. | DAXUIDolbyAudio.exe | daxuidolbyaudio |
| 51 | Directory Snoop 5.11 (Trial Version) | 8/20/2021 18:40 | f4b830bd4c0430b05ea9479b25c32b2968eca470 | c:\program files (x86)\briggs softworks\directory s | DS_FAT.exe | |
| 52 | Directory Snoop 5.11 (Trial Version) | 8/20/2021 18:40 | 93e80a42873a173ba22f944577bea4c3c46eacd8 | c:\program files (x86)\briggs softworks\directory s | DS_NTFS.exe | |
| 53 | Directory Snoop 5.11 (Trial Version) | 8/20/2021 18:40 | bb7cb0c41f726fccb418ff95fc5a07823d28b6c4 | c:\program files (x86)\briggs softworks\directory s | elrawdsk32.sys | rawdisk |
| 54 | Directory Snoop 5.11 (Trial Version) | 8/20/2021 18:40 | d2c4fa05eb56d98acf5e08f0b2cbbcddeaf1c401 | c:\program files (x86)\briggs softworks\directory s | elrawdsk64.sys | rawdisk |
| 55 | Directory Snoop 5.11 (Trial Version) | 8/20/2021 18:40 | 08efa016657536d20844c550773b7b1a8568d1ad | c:\program files (x86)\briggs softworks\directory s | elrawdski64.sys | rawdisk |
| 56 | Directory Snoop 5.11 (Trial Version) | 8/20/2021 18:40 | e78b47322c26265de7206d2f23c07dd97c989c2f | c:\program files (x86)\briggs softworks\directory s | unins000.exe | |
| 57 | Digital Detective DCode v5.5 | 10/11/2021 15:02 | 32b7326cf6d99f15823dd86289a26076b0f7182f | c:\program files (x86)\digital detective\dcode v5\ | unins000.exe | dcode |
| 58 | Digital Detective DCode v5.5 | 10/11/2021 15:02 | a2a8758a196722c15d8beff7ec73d72944bcf959 | c:\program files (x86)\digital detective\dcode v5\ | DCode.exe | dcode |
| 59 | Autopsy | 10/6/2021 7:34 | afb7f7d1c52d3cc5a222d9b2e388c6bf4ef5c11a | c:\program files\autopsy-4.6.0\harness\launchers | app.exe | |
| 60 | Autopsy | 10/6/2021 7:34 | 62b10c0f74461cc77addf13064b8fddf0b85902c | c:\program files\autopsy-4.6.0\harness\launchers | app64.exe | |
| 61 | Autopsy | 10/6/2021 7:34 | e1363c24efc0a3ef242ae7e47cfc37c559ef9cdf | c:\program files\autopsy-4.6.0\autopsy\photorec | fidentify_win.exe | |
| 62 | Autopsy | 10/6/2021 7:34 | c5e13c67ed1f65b8329b570dfd390f78837fcad6 | c:\program files\autopsy-4.6.0\gstreamer\bin\gst-inspect.exe | gst-inspect.exe | |
| 63 | Autopsy | 10/6/2021 7:34 | a1489868b5a35ba18940b91b54a29e1a2259bdb9 | c:\program files\autopsy-4.6.0\gstreamer\bin\gst-launch.exe | gst-launch.exe | |
| 64 | Autopsy | 10/6/2021 7:34 | 7995c588f4985c5602db6d676e0ad4d80adddc7f | c:\program files\autopsy-4.6.0\gstreamer\bin\gst-player.exe | gst-player.exe | |
| 65 | AccessData FTK Imager | 8/29/2021 13:15 | 436a1d28aa0fd5a23d8a955d6c9eecf6c6d3e5fe | c:\program files (x86)\accessdata\ftk imager\ade | adencrypt_gui.exe | adencrypt exe |
| 66 | AccessData FTK Imager | 8/28/2021 20:16 | 31b158c61758dc81bc879432acedfd3d769b86df | c:\program files (x86)\accessdata\ftk imager\ftk i | FTK Imager.exe | accessdata® ftk® imager |
| 67 | | | | | | |

Hive (Amcache.hve) is dirty.
If you need to process hive transasction logs, please consider using yarp + registryFlush.py
(Maxim Suhanov) or rla.exe (Eric Zimmerman).

amcache v.20200515
(amcache) Parse AmCache.hve file

***InventoryApplicationFile***

c:\users _____ \amcacheparser.exe  LastWrite: 2021-09-25 01:11:11Z
hash: 13ab2021 7dff4932604 2d9a224e5405db00b3cc7

# System Resource Usage Monitor (SRUM)

**What is it?**

SRUM is considered a gold mine of forensic information, as it contains all the activities that occur on a particular Windows system. SRUM tracks and records program executions, power consumption, network activities, and much more information that can be retrieved even if the source has been deleted.

**Forensic Value:**
1. Program executions
2. Power consumption
3. Network activities
4. Bytes Received & Sent

**Location:**
C:\Windows\System32\sru\SRUDB.dat

**Tool:**
SrumECmd.exe

| Timestamp | ExeInfo | BytesReceiv | BytesSen |
|---|---|---|---|
| 10/5/2021 1:16 | \device\harddiskvolume3\users\...\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe | 1765826 | 528180 |
| 10/5/2021 0:13 | \device\harddiskvolume3\users\...\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe | 41117327 | 1029971 |
| 10/2/2021 7:22 | \device\harddiskvolume3\users\...\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe | 1717790 | 437444 |
| 10/2/2021 5:59 | \device\harddiskvolume3\users\...\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe | 10948 | 9960 |
| 10/2/2021 5:36 | \device\harddiskvolume3\users\...\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe | 3744 | 3648 |
| 10/2/2021 5:32 | \device\harddiskvolume3\users\...\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe | 25092 | 5728 |
| 10/2/2021 5:27 | \device\harddiskvolume3\users\...\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe | 267854 | 16224 |
| 10/2/2021 5:26 | \device\harddiskvolume3\users\...\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe | 1007792 | 97860 |
| 9/27/2021 1:27 | \device\harddiskvolume3\users\...\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe | 892605 | 42818 |
| 9/27/2021 0:25 | \device\harddiskvolume3\users\...\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe | 4653862 | 108992 |
| 9/1/2021 16:02 | \device\harddiskvolume3\users\...\appdata\local\whatsapp\app-2.2132.6\whatsapp.exe | 1107334 | 357108 |

# Master File Table ($MFT)

**What is it?**

A master file table is a database in which information about every file and directory on an NT File System (NTFS) volume is kept. An MFT will have a minimum one record for every file and directory on the NTFS logical volume. Moreover, each record contains attributes that tell the operating system how to handle the file or directory associated with the record.

**Forensic Value:**

1. Timeline Analysis
2. Information about a file or directory
3. File Type, Size
4. Date/Time when created, modified and accessed

**Location:**

NTFS/root/$MFT (Extracted from FTK)

**Tool:**

MFTECmd.exe , MFTExplorer.exe



| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | EntryNumb | SequenceNumb | InU | ParentEntryNumb | ParentSequenceNumb | ParentPath | FileName | Extensic | FileSi | ReferenceCou | ReparseTarg | IsDirecto | HasA | IsAc | SI<F | uSe |
| 2 | 26206 | 62 | TRUE | 26193 | 58 | .\Users\■\Desktop\Mohammed\Others | Photograph of candidate.jpg | .jpg | 159125 | 1 | | FALSE | | FALSE | FALSE FALSE | FAL |

# Windows 10 Timeline (ActivitiesCache)

**What is it?**

Windows 10 Timeline info covering user activities is stored in the 'ActivitiesCache.db' file with the following path. The 'ActivitiesCache.db' file is an SQLite database. **StartTime** means the moment when an application was launched. **EndTime** means the moment when an application ceases to be used. **ExpirationTime** means the moment when the storage duration for a record covering a user activity expires in the database. **LastModifiedTime** means the moment when a record covering a PC user activity has been last modified (if such an activity has been repeated several times.

**Forensic Value:**

1. Timeline Analysis
2. Information about an application and file
3. Date/Time when started, created, modified and accessed

**Location:**

%USERPROFILE%\AppData\Local\ConnectedDevicesPlatform\<Profile ID>\ActivitiesCache.db

**Tool:**

WxTCmd.exe

| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | Executable | DisplayText | StartTime | LastModifiedTin | LastModifiedTimeOnClie | CreatedTime | ExpirationTime | OperationExpirationTim |
| 2 | System32\notepad.exe | File Carving_FROM_DISK.txt (Notepad) | 9/29/2021 20:40 | 9/29/2021 20:40 | 10/16/2021 1:57 | 9/29/2021 20:40 | 11/15/2021 1:57 | 11/15/2021 1:57 |
| 3 | Program Files x86\AccessData\FTK Imager\FTK Imager.exe | FTK Imager | 10/2/2021 23:11 | 10/2/2021 23:11 | 10/27/2021 18:01 | 10/2/2021 23:11 | 11/26/2021 18:01 | 11/26/2021 18:01 |
| 4 | System32\notepad.exe | test.txt (Notepad) | 10/2/2021 23:32 | 10/2/2021 23:32 | 10/18/2021 14:10 | 10/2/2021 23:32 | 11/17/2021 14:10 | 11/17/2021 14:10 |
| 5 | Program Files X64\Autopsy-4.6.0\bin\autopsy64.exe | Autopsy 4.6.0 | 10/5/2021 7:31 | 10/5/2021 7:31 | 10/27/2021 17:59 | 10/5/2021 7:31 | 11/26/2021 17:59 | 11/26/2021 17:59 |
| 6 | | | | | | | | |

# $J

## What is it?

The $J data stream contains the contents of the change journal and includes information such as the date and time of the change, the reason for the change, the MFT entry, the MFT parent entry and others. This information can be useful for an investigation, for example, in a scenario where the attacker is deleting files and directories while he moves inside an organization in order to hide his tracks.

## Forensic Value:

1. Timeline Analysis
2. File Activity Analysis (Open, Close and Update)
3. Evidence of renamed and deleted files

## Location:

NTFS/root/$Extend/$RmMetadata/$UsnJrnl/$J
(Extracted from FTK)

## Tool:

MFTECmd.exe

| Name | Extension | EntryNumber | SequenceNumber | ParentEntryNumber | ParentSequenceNumber | UpdateSequenceNumber | UpdateTimestamp | UpdateReasons | FileAttributes | OffsetToData | SourceFile |
|------|-----------|-------------|----------------|-------------------|----------------------|----------------------|-----------------|---------------|----------------|--------------|------------|
| ALHUMAID_TEST.txt | .txt | 15321 | 214 | 21249 | 17 | 12297437784 | 10/27/2021 19:55:05.2 | RenameNewName | Archive | 3707503192 | $J |
| ALHUMAID_TEST.txt | .txt | 15321 | 214 | 21249 | 17 | 12297437880 | 10/27/2021 19:55:05.2 | RenameNewName\|Close | Archive | 3707503288 | $J |
| ALHUMAID_TEST.txt | .txt | 15321 | 214 | 21249 | 17 | 12297438264 | 10/27/2021 19:55:05.3 | ObjectIdChange | Archive | 3707503672 | $J |
| ALHUMAID_TEST.txt | .txt | 15321 | 214 | 21249 | 17 | 12297438360 | 10/27/2021 19:55:05.3 | ObjectIdChange\|Close | Archive | 3707503768 | $J |
| ALHUMAID_TEST.txt | .txt | 15321 | 214 | 21249 | 17 | 12297441088 | 10/27/2021 19:55:08.8 | DataExtend | Archive | 3707506496 | $J |
| ALHUMAID_TEST.txt | .txt | 15321 | 214 | 21249 | 17 | 12297441184 | 10/27/2021 19:55:08.8 | DataExtend\|Close | Archive | 3707506592 | $J |
| ALHUMAID_TEST.txt | .txt | 15321 | 214 | 21249 | 17 | 12297442816 | 10/27/2021 19:56:19.3 | RenameOldName | Archive | 3707508224 | $J |
| ALHUMAID_CHANGE.txt | .txt | 15321 | 214 | 21249 | 17 | 12297442912 | 10/27/2021 19:56:19.3 | RenameNewName | Archive | 3707508320 | $J |
| ALHUMAID_CHANGE.txt | .txt | 15321 | 214 | 21249 | 17 | 12297443008 | 10/27/2021 19:56:19.3 | RenameNewName\|Close | Archive | 3707508416 | $J |
| ALHUMAID_CHANGE.txt | .txt | 15321 | 214 | 21249 | 17 | 12297443944 | 10/27/2021 19:56:22.6 | RenameOldName | Archive | 3707509352 | $J |

# $LogFile

**What is it?**

This file is stored in the MFT entry number 2 and every time there is a change in the NTFS Metadata, there is a transaction recorded in the $LogFile. These transactions are recorded to be possible to redo or undo file system operations. Why would $LogFile be important for investigation? Because the $LogFile keeps record of all operations that occurred in the NTFS volume such as file creation, deletion, renaming, copy.

**Forensic Value:**

1. Timeline Analysis
2. File Activity Analysis (Open, Close and Update)
3. Evidence of renamed and deleted files

**Location:**

NTFS/root/$LogFile (Extracted from FTK)

**Tool:**
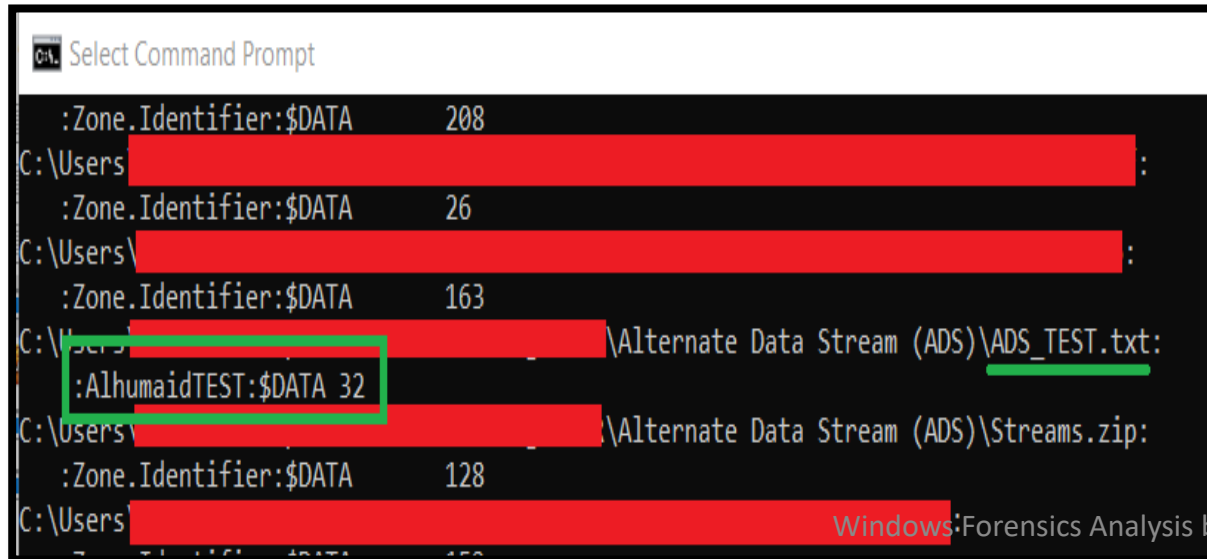
NTFS_Log_Tracker.exe , LogFileParser.exe

| LSN | EventTime(UTC+3) | Event | Detail | File/Directory Name | Redo | Target VCN | Cluster Index |
|-----|------------------|-------|--------|---------------------|------|------------|---------------|
| 58571421012 | 12/23/2021 03:12:18.0 | Renaming File | New Text Document.txt -> Alhumaid_Test.txt | Alhumaid_Test.txt | Create Attribute | 0x3B3E | 4 |
| 58571423061 | 12/23/2021 03:12:18.0 | File Creation | | Alhumaid_Test.txt.lnk | Initialize File Record Segment | 0x640 | 0 |
| 58571423281 | | Writing Content of Resident File | Writing Size : 584 | Alhumaid_Test.txt.lnk | Update Resident Value | 0x640 | 0 |
| 58571430272 | 12/23/2021 03:12:36.0 | Renaming File | Alhumaid_Test.txt -> Alhumaid_Renamed.txt | Alhumaid_Renamed.txt | Create Attribute | 0x3B3E | 4 |
| 58571432968 | 12/23/2021 03:12:38.0 | File Creation | | Alhumaid_Renamed.txt.lnk | Initialize File Record Segment | 0x39A9 | 0 |
| 58571433257 | | Writing Content of Non-Resident File | Data Runs(in Volume) : 10769738(1) | Alhumaid_Renamed.txt.lnk | Update Mapping Pairs | 0x39A9 | 0 |
| 58571438672 | | Move(Before) | | Alhumaid_Renamed.txt | Delete Attribute | 0x3B3E | 4 |

# Alternate Data Streams (ADS)

## What is it?

Alternate Data Streams (ADS) are a file attribute only found on the NTFS file system to store different streams of data. The ability is to fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer. In addition to the default stream "**Zone.Identifier**" which is normally used for a file.

## Forensic Value:

1. Find the presence of a secret or malicious file inside the file record of an innocent file
2. Find hidden hacking toolkit
3. Find hidden files or information

## Location:

within the same file! There is no specified path.

## Tool:

streams.exe , powershell.exe (Get-Item) , AlternateStreamView.exe , cmd.exe (dir /R)



Windows Forensics Analysis by Mohammed Alhumaid (V 1.0)

# Link File – Shortcut (.lnk)

## What is it?

A shortcut file is a small file which has information used to access or point to another file. Windows operating system automatically creates LNK files when a user opens a non-executable file or document. Windows creates these LNK files on a frequent basis and their creation is performed in the background without the explicit knowledge of the user. Shortcut files are most often referred to Link files by forensic analysts based on their .lnk file extension.

## Forensic Value:

1. The path and size of target file
2. Timestamps for both the target file and LNK file
3. The attributes associated with the target file (i.e. read-only, hidden, archive, etc.)
4. The system name, volume name, volume serial number, and sometimes the MAC address of the system where the target is stored
5. Files opened from a specific removable USB device
6. Identification of files which no longer exist on a local machine

## Location:

%USERPROFILE%\Recent

%USERPROFILE%\Application Data\Microsoft\Office\Recent

## Tool:

LECmd.exe



```
C:\Windows\System32\cmd.exe
Processing 'C:\Users         \Application Data\Microsoft\Office\Recent Time_Line.xlsx.LNK'

Source file: C:\Users        \Application Data\Microsoft\Office\Recent\Time_Line.xlsx.LNK
  Source created:  2021-12-22 00:35:27
  Source modified: 2021-12-22 19:20:46
  Source accessed: 2021-12-29 23:20:27

--- Header ---
  Target created:  2021-10-05 07:01:48
  Target modified: 2021-10-05 07:01:15
  Target accessed: 2021-12-22 19:20:37

  File size: 43,625,731
  Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, IsUnicode
  File attributes: FileAttributeArchive
  Icon index: 0
  Show window: SwNormal (Activates and displays the window. The window is restored to its original size and position if the window is minimized or maximized.)

Relative Path: ..\..\..\..\..\Desktop\                           \TimelineExplorer\Time_Line.xlsx

--- Link information ---
Flags: VolumeIdAndLocalBasePath

>>Volume information
  Drive type: Fixed storage media (Hard drive)
  Serial number:
  Label: Windows-SSD
  Local path: C:\Users\                       \TimelineExplorer\Time_Line.xlsx
```

# RDP Bitmap Cache (BMC)

## What is it?

RDP is a known protocol developed by Microsoft that allows users to connect to other Windows operating systems with GUI. To enhance the RDP user experience and reduce the data throughput on the network, RDP Bitmap Cache was implemented. It stores bitmap-sized images of RDP sessions into a file so that session reuses these images and reduces the potential lag.

## Forensic Value:

1. RDP session photos, screenshots, images, captures
2. RDP activity evidences in case of the target system was completely damaged as the artifact is collected from the client side

## Location:

%USERPROFILE%\AppData\Local\Microsoft\Terminal Server Client\Cache\

## Tool:

bitmapcacheviewer.exe , bmc-tools.py
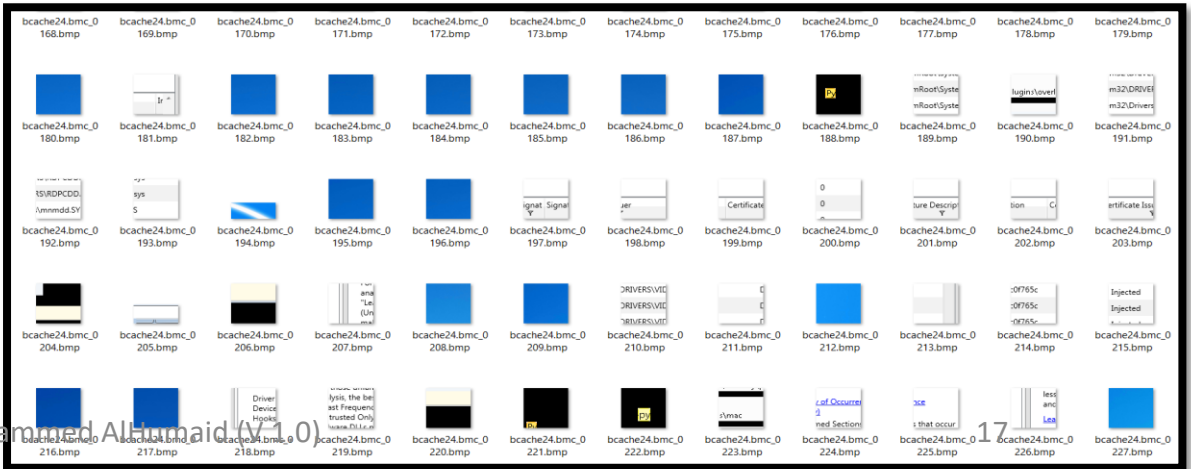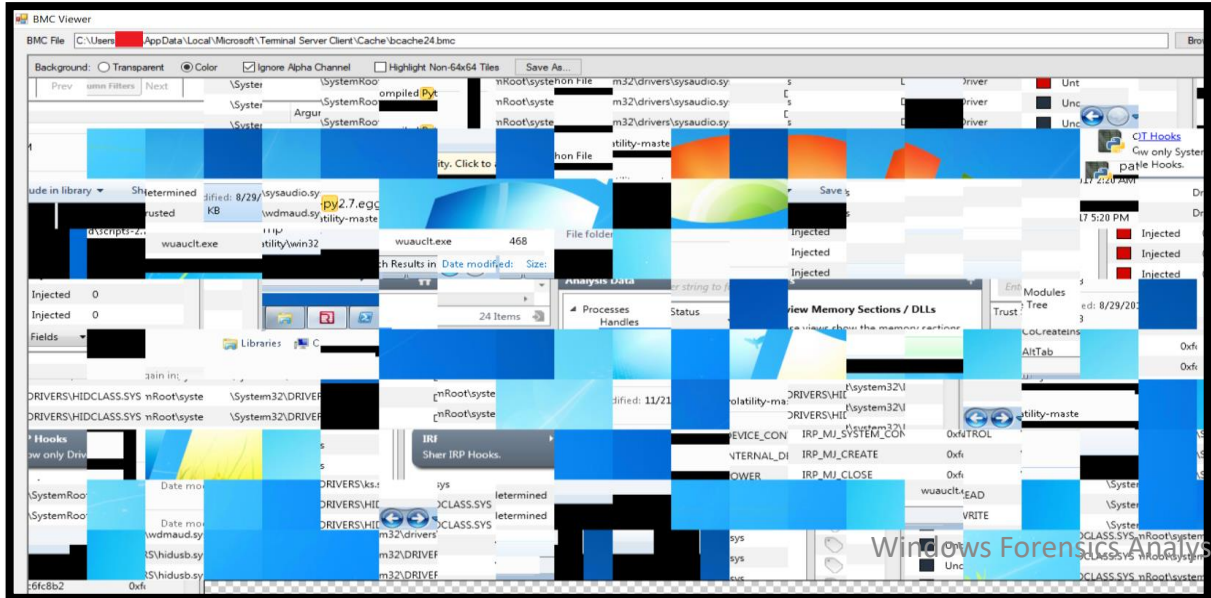
# UserAssist

## What is it?

UserAssist tracks every **GUI-based** programs launched are recorded in this registry key. This key contains two GUID subkeys (**CEBFF5CD** Executable File Execution, **F4E57C4B** Shortcut File Execution), each subkey maintains a list of system objects such as program, shortcut, and control panel applets that a user has accessed. Registry values under these subkeys are weakly encrypted using **ROT-13** algorithm which basically substitutes a character with another character 13 position away from it in the ASCII table.

## Forensic Value:

1. The executed GUI program name
2. The executed GUI program path
3. Last executed time
4. Run count

## Location:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count

## Tool:

RegRipper (rr.exe) , RegistryExplorer.exe

```
----------------------------------------
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2021-02-09 20:21:57Z

2022-01-01 00:18:10Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (180)
2022-01-01 00:09:14Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\AccessData\FTK Imager\FTK Imager.exe (11)
2021-12-31 23:56:11Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Adobe\Acrobat DC\Acrobat\Acrobat.exe (15)
2021-12-30 01:50:23Z
  C:\Users\Desktop\testdisk-7.2-WIP\photorec_win.exe (1)
```

| Program Name | Run Counter | Focus Count | Focus Time | Last Executed |
|---|---|---|---|---|
| {System32}\notepad.exe | 180 | 391 | 0d, 2h, 19m, 10s | 2022-01-01 00:18:10 |
| {System32}\WindowsPowerShell\v1.0\powershell.exe | 25 | 157 | 0d, 1h, 05m, 02s | 2021-12-30 00:51:32 |
| {System32}\cmd.exe | 19 | 209 | 0d, 1h, 33m, 04s | 2021-12-29 22:59:40 |
| {System32}\SnippingTool.exe | 16 | 55 | 0d, 0h, 14m, 40s | 2021-12-30 01:03:28 |
| {System32}\mspaint.exe | 12 | 21 | 0d, 0h, 14m, 47s | 2021-12-30 01:03:41 |
| {System32}\mmc.exe | 4 | 0 | 0d, 0h, 00m, 00s | 2021-12-14 21:54:54 |
| {System32}\eventvwr.exe | 2 | 0 | 0d, 0h, 00m, 00s | 2021-12-14 20:51:24 |
| {System32}\Fondue.exe | 0 | 2 | 0d, 0h, 00m, 15s | |

# WordWheelQuery

**What is it?**

WordWheelQuery is a registry key that stores keywords searched from the folder search menu bar. Keywords are added in Unicode and listed in temporal order in an MRUlist.

```
-----------------------------------------
wordwheelquery v.20200823
(NTUSER.DAT) Gets contents of user's WordWheelQuery key

Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
LastWrite Time 2021-12-22 20:31:36Z

Searches listed in MRUListEx order

19    security
18    python
17    .dmp
16    lsass
15    exe
14    ntuser.dat
13    ntuser
12    sru
11    shim
10    webexmta
9     webex
7     whatsapp
8     log
6     outlook
5     RecentFileCache.bcf
4     memory.dmp
2     memory
3     mem
1     gggg
0     openvpn
-----------------------------------------
```

| | Search DFIR |
|---|---|
| | security |
| | python |
| | .dmp |
| | lsass |
| | exe |
| | ntuser.dat |
| | ntuser |
| | sru |
| | shim |
| | webexmta |
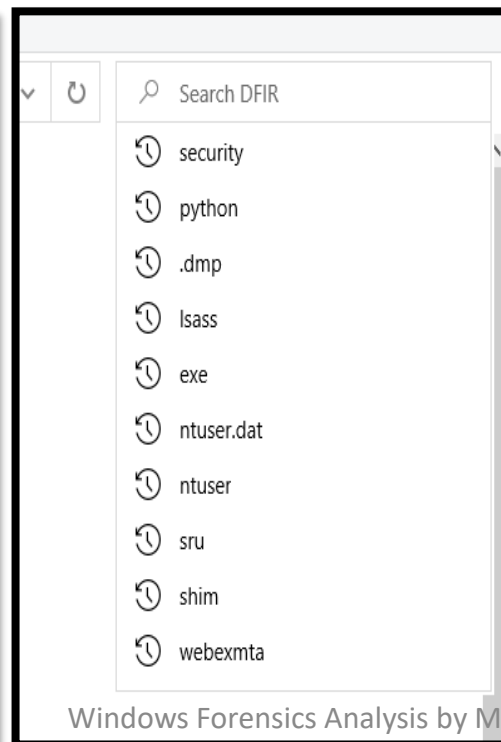
**Forensic Value:**

1. User Activity
2. Last folder search conducted (Last Write Time)
3. Keywords searched

**Location:**

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

=

NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

**Tool:**

RegRipper (rr.exe) , RegistryExplorer.exe

# NTUSER.DAT

**What is it?**

It's hidden file in every user profile and contains the settings and preferences for each user. Windows accomplishes this by first storing that information to the Registry in the **HKEY_CURRENT_USER** hive. Then when user sign out or shut down, Windows saves that information to the **NTUSER.DAT** file. The next time user sign in, Windows will load NTUSER.DAT to memory, and all preferences load to the Registry again.

**Forensic Value:**

1. Collecting registry hive (HKEY_CURRENT_USER) through its supporting file (NTUSER.DAT)
2. Forensicate user activity, setting via registry hive
3. Forensic artifacts (Recent Docs, Typed URLs, UserAssist, Recent Apps, Run and Run Once, ComDig32 Subkey, Typed Paths Subkey, Microsoft Office applications and the MRU subkey, RunMRU, Windows search function and the WordWheelQuery)

**Location:**

C:\Users\<username>\NTUSER.DAT

**Tool:**

RegRipper (rr.exe) , RECmd.exe , RegistryExplorer.exe

# ShellBags

**What is it?**

Windows tracks and records user's view settings and preferences while exploring folders. These view settings (size, view mode, position) of a folder window are stored in ShellBags registry keys. ShellBags keep track of the view settings of a folder window once the folder has been viewed through Windows Explorer. ShellBags does not only track the view settings of a folder on the local machine, but also on removable devices and network folders.

**Forensic Value:**

1. User's navigation activity on the system
2. Timestamps analysis
3. Deleted folders
4. Folders accessed within local machine
5. Folders accessed from removable devices
6. Folders accessed from network folders

**Location:**

NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU

NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags

USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags

**Tool:**

SBECmd.exe , ShellBagsExplorer.exe , sbag64.exe
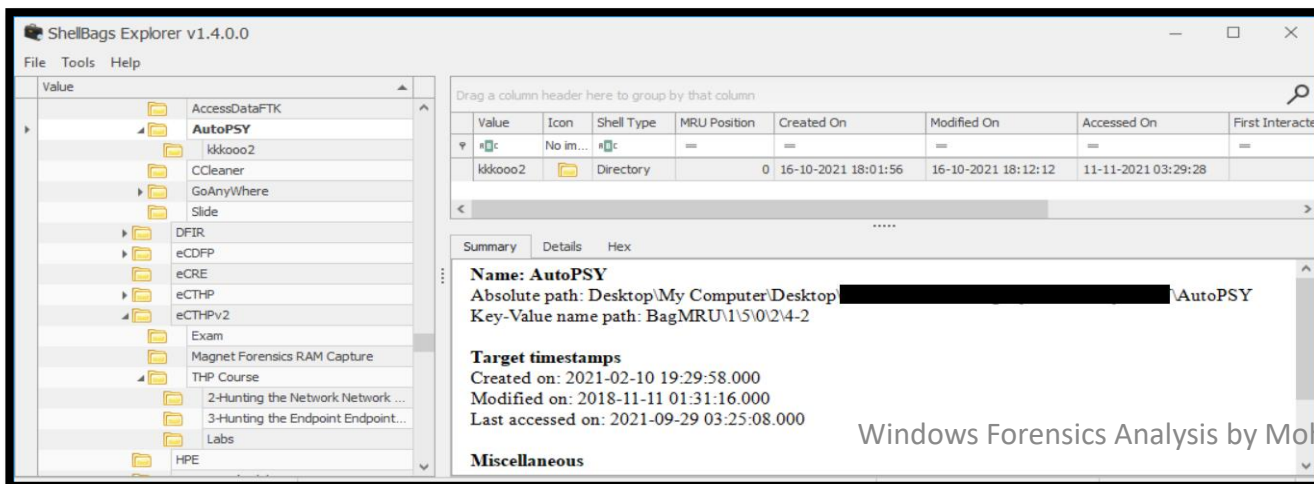
# Background Activity Moderator (BAM) / (DAM)

**What is it?**

BAM is a Windows service that controls activity of background applications. The BAM entries are updated when **Windows boots**. Also, there is dam\UserSettings Desktop Activity Monitor (DAM) and stores similar information to BAM.
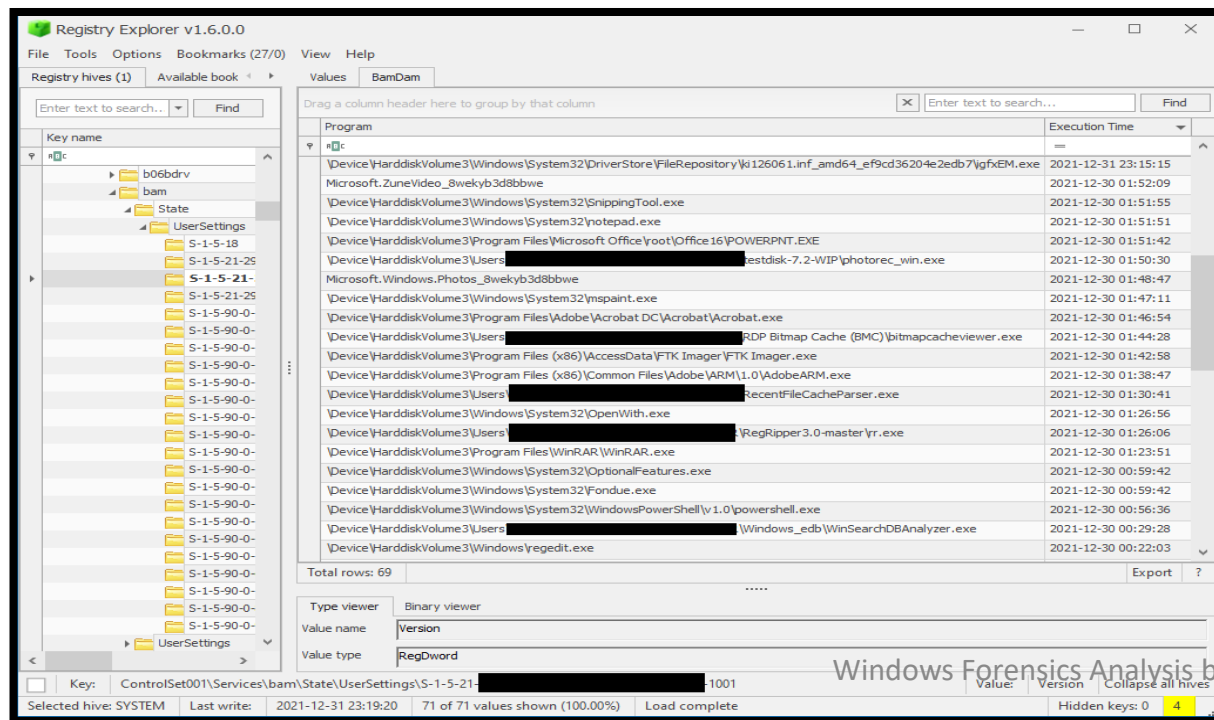
**Forensic Value:**

1. Evidence of execution
2. The executable's name
3. The absolute path to the executable
4. The last time the application ran

**Location:**

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet*\Services\bam\State\UserSettings\<SID>

**Tool:**

RegistryExplorer.exe , BamParser.py

# Security Account Manager (SAM)

**What is it?**

Security Account Manager (SAM) is a database file in Windows that stores users' passwords. It can be used to authenticate local and remote users. SAM uses cryptographic measures to prevent unauthenticated users accessing the system. The user passwords are stored in a hashed format in a registry hive either as an LM hash or as an NTLM hash.

**Forensic Value:**
1. User information
2. Group information
3. Authentication information
4. User's security settings
5. Login count

**Location:**
C:\Windows\System32\config\SAM

**Tool:**
RegRipper (rr.exe) , samparser.py

```
Hive (SAM) is not dirty.

samparse v.20200825
(SAM) Parse SAM file for user & group mbrshp info


User Information
------------------------
Username        : Administrator [500]
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    :
Account Created : 2021-02-10 07:08:57Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
Embedded RID    : 500
  --> Password does not expire
  --> Account Disabled
  --> Normal user account
```

# SECURITY

## What is it?

SECURITY hive helps us to understand the security measures of the needed Windows system in the Forensic Investigation process.

```
Hive (SECURITY) is dirty.
If you need to process hive transasction logs, please consider using yarp + registryFlush.py
(Maxim Suhanov) or rla.exe (Eric Zimmerman).

auditpol v.20200515
(Security) Get audit policy from the Security hive file

auditpol
Policy\PolAdtEv
LastWrite Time ███████████████████

Possible Win10(1607+)/Win2016
System:Security State Change
System:Security System Extension
System:System Integrity
System:IPsec Driver
System:Other System Events
Logon/Logoff:Logon
Logon/Logoff:Logoff
Logon/Logoff:Account Lockout
Logon/Logoff:IPsec Main Mode
Logon/Logoff:Special Logon
Logon/Logoff:IPsec Quick Mode
Logon/Logoff:IPsec Extended Mode
Logon/Logoff:Other Logon/Logoff Events
Logon/Logoff:Network Policy Server
Logon/Logoff:User/Device Claims
Logon/Logoff:Group Membership
Object Access:File System
Object Access:Registry
Object Access:Kernel Object
Object Access:SAM
Object Access:Other Object Access Events
Object Access:Certification Services
Object Access:Application Generated
Object Access:Handle Manipulation
Object Access:File Share
Object Access:Filtering Platform Packet Drop
Object Access:Filtering Platform Connection
Object Access:Detailed File Share
Object Access:Removable Storage
Object Access:Central Policy Staging
```

## Forensic Value:

1. Security settings
2. Disabled / Enabled audit logs
3. Last update on security settings

## Location:

C:\Windows\System32\config\SECURITY

## Tool:

RegRipper (rr.exe)

# SOFTWARE

**What is it?**

SOFTWARE hive file consists, all the information regarding the software installed in the needed Windows system.

```
--------------------------------------------------
Launching installer v.20200517
(Software) Determines product install information

Key      : 8BFDDD6597F70844985D521E5FA22BF8
LastWrite: 2021-10-29 09:06:38Z
20211029 - Bonjour 3.1.0.1 (Apple Inc.)

Key      : 902DD72566A8F28478977C3BABCC8A1F
LastWrite: 2021-10-29 09:10:05Z
20211029 - Apple Mobile Device Support 15.0.0.16 (Apple Inc.)

Key      : 9054B670F48A62740AD5B384EB92A8FA
LastWrite: 2021-02-23 23:05:17Z
20210224 - Mandiant IOCe for OpenIOC-1.1 3.2.0 (Mandiant)

Key      : 974690591A66B454398732D43F3B7172
LastWrite: 2021-02-10 16:56:23Z
20210210 - VMware Workstation 16.1.0 (VMware, Inc.)
```

```
--------------------------------------------------
audiodev v.20200525
(Software) Gets audio capture/render devices

Capture/Input Devices: GUID, Device
{45689cb3-ae4c-4631-a4a8-ab6639d360a4}, Device: Headset
{6b19fc5b-4a20-4824-9014-bf95fbcf5f10}, Device: Headset
{6fafe5bc-1a30-43f4-8fcc-6266eac05dc1}, Device: Microphone Array
{f3cb5bfd-94e8-4b86-922b-ee8eca549f4c}, Device: Stereo Mix

Render/Output Devices: GUID, Device
{042be894-d9a9-4553-9e74-d58b46f94be2}, Device: Headphones
{45bf603d-df10-4eab-8fb4-1681d81b902e}, Device: Headset
{6a859bca-f000-4462-a0da-b925198ec165}, Device: Headset
{94e3db05-714e-4f6d-88e6-9cf544afeced}, Device: Headphones
{9e0107c0-1cd9-4b65-bfa3-4690f16435cc}, Device: Speakers
{cbbcaa0b-f29e-4ab8-b6a2-4fcd17d7d2d1}, Device: SAMSUNG
{f13ee661-f587-4770-8a2e-14d2ef62af84}, Device: LG_TV
--------------------------------------------------
```

**Forensic Value:**

1. AppInit_DLLs
2. Last logged on user with its SID
3. Last logged on user with Time/Date
4. Network info (Network cards, type of connection whether wireless or wired, name of access point or product, default gateway MAC, time of first connection, time of last connection)
5. Input and output devices
6. Bluetooth drivers
7. Most Run Keys
8. User Account Control (UAC) information
9. Windows drivers with VolumeLabel
10. Windows version & build info

**Location:**

C:\Windows\System32\config\SOFTWARE

**Tool:**

RegRipper (rr.exe)

# SYSTEM

**What is it?**

The SYSTEM hive file consists of all basic information regarding the system information.

```
-------------------------------------------
bthport v.20200517
(System) Gets Bluetooth-connected devices from System hive

ControlSet001\services\BTHPORT\Parameters\Devices
LastWrite: 2021-12-22 20:23:24Z

Device Unique ID: 0021130c405c
Name              : HOCO E15
LastSeen          : 2021-04-13 23:05:19Z
LastConnected     : 2021-04-13 23:05:19Z

Device Unique ID: e807bfbdbea2
Name              : Soundcore Life Q10
LastSeen          : 2021-02-21 23:24:57Z
LastConnected     : 2021-02-21 23:24:57Z
```

```
-------------------------------------------
dafupnp v.20200525
(System) Parses data from networked media streaming devices

uuid:23456789-1234-1010-8000-104FA871CB93
DeviceDesc          : @c_swdevice.inf,%swd\genericraw.devicedesc%;Generic software device
CompatibleID        : UMB\urn:schemas-upnp-org:device:MediaRenderer:1 SWD\GenericRaw SWD\Gener
HardwareID          : UMB\Sony_Corporation/MediaRenderer/100/urn:schemas-upnp-org:device:Media
LocationInformation : http://192.168.100.5:52323/MediaRenderer.xml
MFG                 : Sony Corporation
FriendlyName        : KD-65X8500D

uuid:85b50b39-7a56-9ec2-501f-e4a0b03f3441
DeviceDesc          : @c_swdevice.inf,%swd\genericraw.devicedesc%;Generic software device
CompatibleID        : UMB\urn:dial-multiscreen-org:device:dial:1 SWD\GenericRaw SWD\Generic
HardwareID          : UMB\SkyworthDigital/JAWWY-TV-2.0/urn:dial-multiscreen-org:device:dial:1
LocationInformation : http://192.168.100.166:8008/ssdp/device-desc.xml
MFG                 : SkyworthDigital
FriendlyName        : JAWWY-TV-2.0

uuid:ab185dc1-ea40-022e-1d36-3ace3166fd27
DeviceDesc          : @c_swdevice.inf,%swd\genericraw.devicedesc%;Generic software device
CompatibleID        : UMB\urn:dial-multiscreen-org:device:dial:1 SWD\GenericRaw SWD\Generic
HardwareID          : UMB\Sony/BRAVIA_4K_2015/urn:dial-multiscreen-org:device:dial:1
LocationInformation : http://192.168.100.5:8008/ssdp/device-desc.xml
MFG                 : Sony
FriendlyName        : KD-65X8500D
-------------------------------------------
```

**Forensic Value:**
1. AppCompatCache (ShimCache) Info
2. Background Activity Moderator (BAM) Info
3. Bluetooth usage info (Device MAC Address, First Connected Time, Last Connected Time, Device Name)
4. Networked media streaming devices info
5. USB device info (FriendlyName, ClassGUID, HardwareID, Last Time Connected)
6. Lists services/drivers in Services key by LastWrite times
7. IP Addresses and domains (DHCP, Static)
8. Shutdown Time

**Location:**

C:\Windows\System32\config\SYSTEM

**Tool:**

RegRipper (rr.exe)

# Windows Error Reporting (WER)

## What is it?

The error reporting feature enables users to notify Microsoft of application faults, kernel faults, unresponsive applications, and other application specific problems. The crashes information is extracted from the .wer files created by the Windows Error Reporting (WER) component of the operating system every time that a crash is occurred.
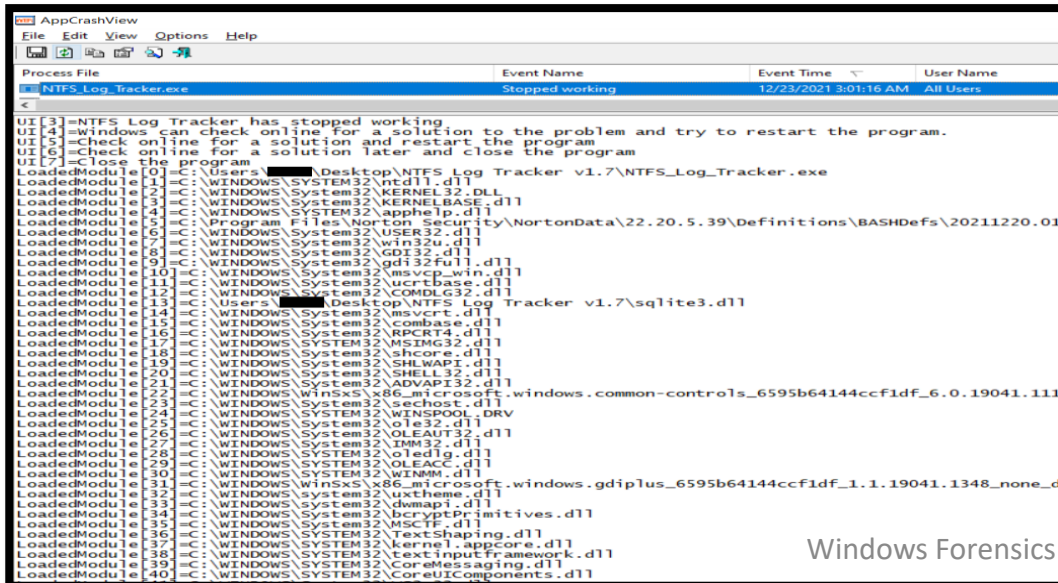
## Forensic Value:

1. Evidence of malware execution and crashes during its execution
2. The DLLs was loaded by malware during crashes
3. Absolut path of malware

## Location:

C:\ProgramData\Microsoft\Windows\WER
C:\Users\<username>\AppData\Local\Microsoft\Windows\WER

## Tool:

AppCrashView.exe

# EventTranscript.db

## What is it?

EventTranscript.db is a SQLite database that appears to record lots of diagnostic-related information about events that occur on the Windows operating system in real-time. This database is **NOT** enabled by default and, if enabled, can be enormous in size and potentially serve as a treasure trove of data.

```
PS D:\EventTranscriptParser> .\EventTranscriptParser.exe -f .\EventTranscript.db -o .\CSV-Output\
 _____                 _     _____                           _       _   ____
| ____|_   _____ _ __ | |_  |_   _| __ __ _ _ __  ___  ___ _ __(_)_ __ | |_|  _ \ __ _ _ __ ___  ___ _ __
|  _| \ \ / / _ \ '_ \| __|   | || '__/ _` | '_ \/ __|/ __| '__| | '_ \| __| |_) / _` | '__/ __|/ _ \ '__|
| |___ \ V /  __/ | | | |_    | || | | (_| | | | \__ \ (__| |  | | |_) | |_|  __/ (_| | |  \__ \  __/ |
|_____| \_/ \___|_| |_|\__|   |_||_|  \__,_|_| |_|___/\___|_|  |_| .__/ \__|_|   \__,_|_|  |___/\___|_|
                                                                 |_|

Author: Abhiram Kumar (Twitter: @_abhiramkumar)
Github: https://github.com/stuxnet999/EventTranscriptParser
_____
Output written to D:\EventTranscriptParser\CSV-Output\BrowserHistory.csv
Output written to D:\EventTranscriptParser\CSV-Output\SoftwareInventory.csv
Output written to D:\EventTranscriptParser\CSV-Output\WlanScan.csv
Output written to D:\EventTranscriptParser\CSV-Output\PnpDeviceInstall.csv
Output written to D:\EventTranscriptParser\CSV-Output\WiFiConnectedEvents.csv
Output written to D:\EventTranscriptParser\CSV-Output\UserDefaults.txt
Output written to D:\EventTranscriptParser\CSV-Output\PhysicalDiskInfo.txt
PS D:\EventTranscriptParser> ls .\CSV-Output\

    Directory: D:\EventTranscriptParser\CSV-Output


Mode                 LastWriteTime         Length Name
-a---          16-09-2021     22:15          49037 BrowserHistory.csv
-a---          16-09-2021     22:15            197 PhysicalDiskInfo.txt
-a---          16-09-2021     22:15          31214 PnpDeviceInstall.csv
-a---          16-09-2021     22:15          17497 SoftwareInventory.csv
-a---          16-09-2021     22:15            522 UserDefaults.txt
-a---          16-09-2021     22:15            111 WiFiConnectedEvents.csv
-a---          16-09-2021     22:15             27 WlanScan.csv
```

## Forensic Value:

1. MS Edge browser history
2. List of software installed on the host system
3. Wireless Scan results
4. WiFi connection details (SSIDs, device manufacturers etc...)
5. Physical Disk information (Disk size, No. of partitions etc...)
6. nP device installation information (Install time, Model, Manufacturer etc...)

## Location:

C:\ProgramData\Microsoft\Diagnosis\EventTranscript\EventTranscript.db

## Tool:

EventTranscriptParser.py , EventTranscriptParser.exe

# Volume Shadow Copy Service (VSS)

**What is it?**

Volume Shadow Copy Service (VSS) is a set of Component Object Model (COM) interfaces in Microsoft Windows that provide the framework for doing volume backups and for creating consistent, point-in-time copies of data (known as shadow copies).
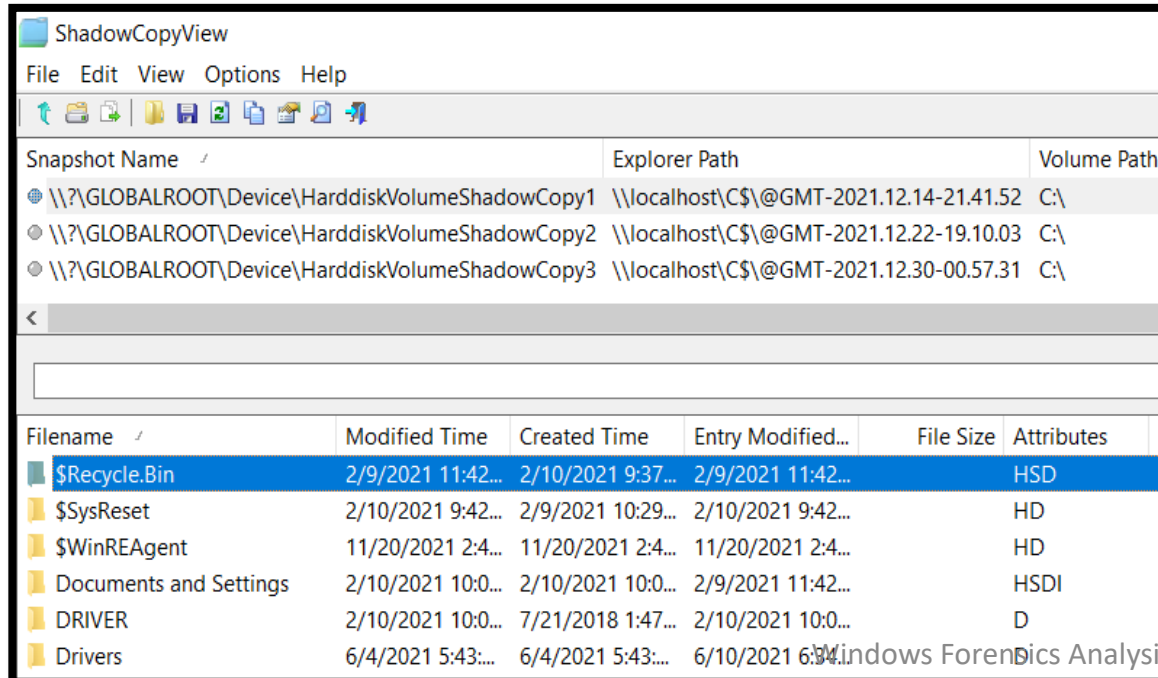
**Forensic Value:**

1. Recover corrupted files
2. Restore deleted files
3. Examine registry hives

**Location:**

C:\

**Tool:**

VSCMount.exe (Mounting) , ShadowCopyView.exe
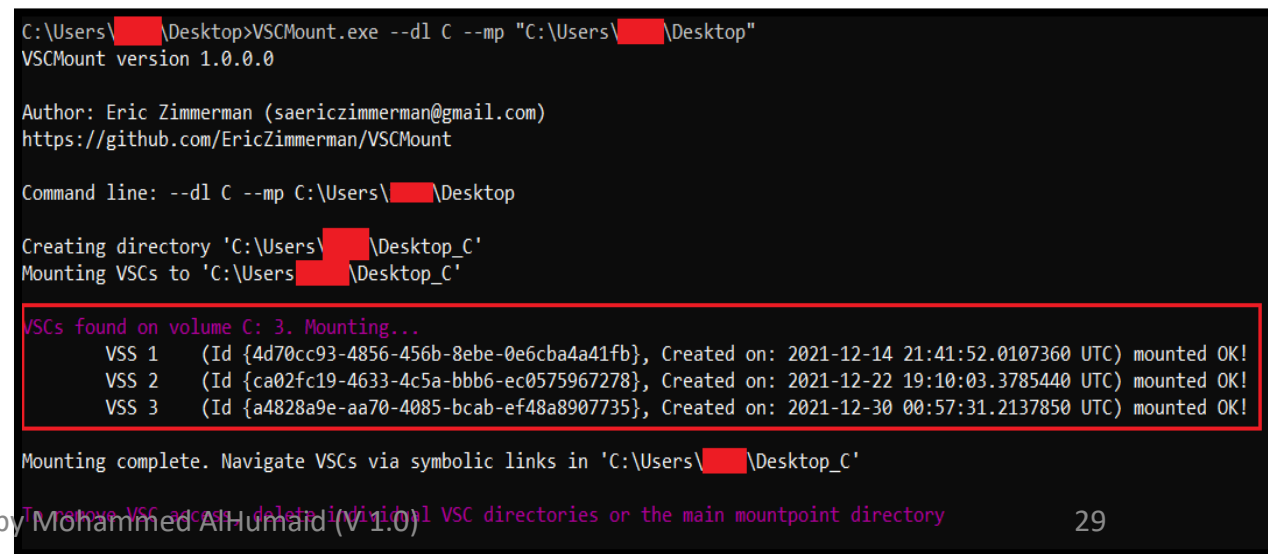
# User Access Logging (UAL)

**What is it?**

UAL is a feature included by default in **Server editions of Microsoft Windows only**, starting with Server 2012. As defined by Microsoft, UAL is a feature that logs unique client access requests, in the form of IP addresses and usernames, of installed products and roles on the local server.

**Forensic Value:**

1. Service accessed
2. User account that performed the access
3. User's source IP
4. Last Access Time
5. Total Accesses
6. Type of authentication access

**Location:**

C:\Windows\System32\LogFiles\Sum\*.mdb

**Tool:**

SumECmd.exe , KStrike.py

# PowerShell

**What is it?**

PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework.
PowerShell in Windows 10 saves the last 4096 commands that are stored in a plain text file located in the profile of each user.
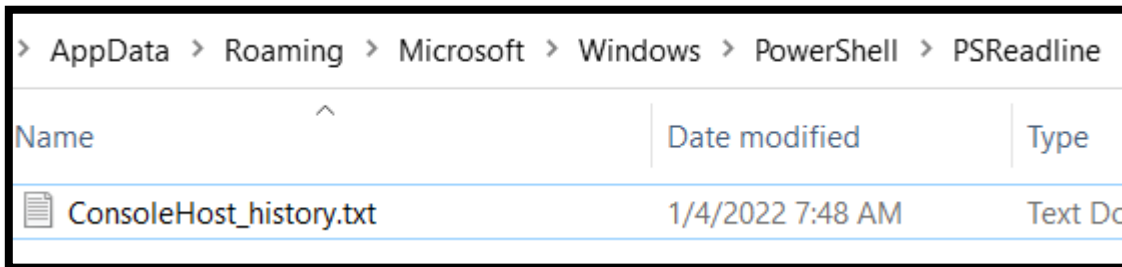
**Forensic Value:**

1.  Evidence of PowerShell commands executed by the user

**Location:**

C:\Users\<username>\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

**Tool:**

notepad.exe

# lsass.exe

**What is it?**

Local Security Authority Subsystem Service (LSASS) is a process in Microsoft Windows operating systems that is responsible for enforcing the security policy on the system. It verifies users logging on to a Windows computer or server, handles password changes, and creates access tokens. It also writes to the Windows Security Log.

**Forensic Value:**

1. Parse user's NTLM hash (If needed ONLY)

**Location:**

C:\WINDOWS\System32\lsass.exe

**Tool:**

Pypykatz , mimikatz



```
└$ pypykatz lsa minidump lsass.DMP
INFO:root:Parsing file lsass.DMP
FILE: ======== lsass.DMP =======
== LogonSession ==
authentication_id 173062 (2a406)
session_id 1
username testadmin
domainname TEST
logon_server WIN-KRVVC7KSTU7
logon_time 2021-07-22T15:10:04.118449+00:00
sid S-1-5-21-2788876189-2294947777-1464636003-1603
luid 173062
        == MSV ==
                Username: testadmin
                Domain: TEST
                LM: NA
                NT: 58a478135a93ac3bf058a5ea0e8fdb71
                SHA1: 0d7d930ac3b1322c8a1142f9b22169d4eef9e855
                DPAPI: NA
        == MSV ==
                Username: NA
                Domain: NA
                LM: NA
                NT: 58a478135a93ac3bf058a5ea0e8fdb71
                SHA1: 0d7d930ac3b1322c8a1142f9b22169d4eef9e855
                DPAPI: NA
        == WDIGEST [2a406]==
                username testadmin
                domainname TEST
                password None
                password (hex)
```

# Windows.edb

**What is it?**

Windows.edb is the Windows Search index database. A search index allows users to quickly search for data and files in the file system due to indexing of files, e-mails in PST files and other content. Indexing is performed in the background by the **SearchIndexer.exe** process. Obviously, the more files there are in the system, the larger the size of the Windows.edb file. In some cases, it can grow up to tens or even hundreds of GB, taking up all the free space on the system drive. The Windows.edb file can be found in all modern client and server Microsoft OSs.
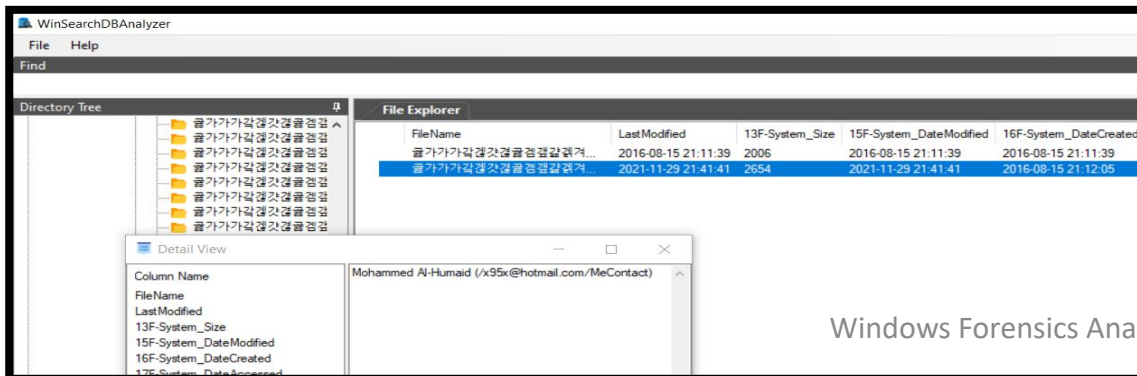


**Forensic Value:**

1. Parse normal records
2. Recover deleted records
3. Outlook Mail Data (Time ,Contents, Contact)
4. OneNote Title
5. Internet History (URLs, Last visit time)
6. Lnk list
7. Network Drive (When adding offline)
8. File, Folder Information (Time, Contents(2KB))
9. Activity History (Recently used programs, Windows Timeline)

**Location:**

C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

**Tool:**

WinSearchDBAnalyzer.exe

# sysmain.sdb

## What is it?

When an application creates a process, WindowsLoader (mostly shimeng.dll and apphelp.dll — which is the Application Compatibility Interface) checks sysmain.sdb and determines whether the program needs to be repaired which will perform lookups in the system compatibility database, recovering various information. The compatibility database is named sysmain.sdb and contains information how the target operating system should handle the application.
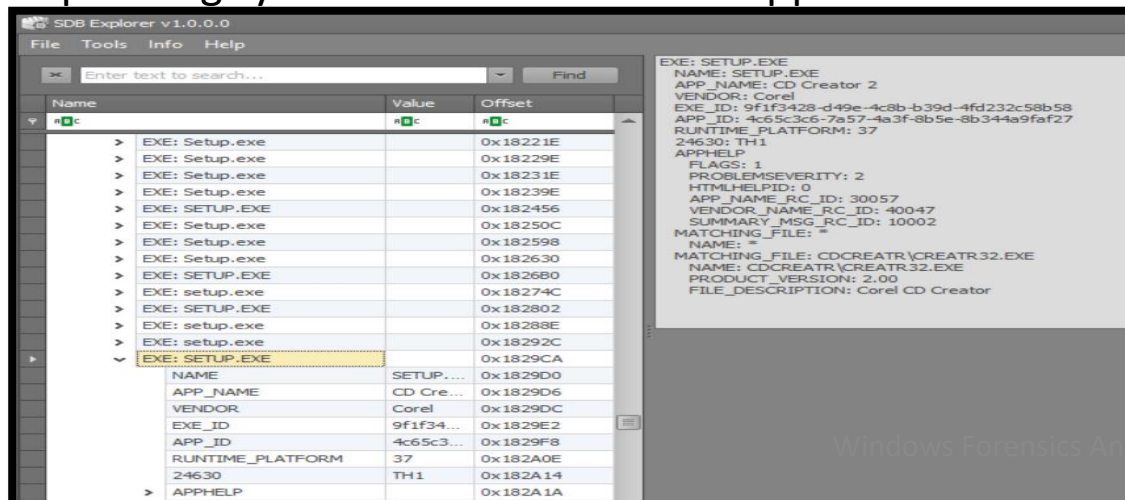
## Forensic Value:

1. Show shims
2. Show executables
3. Show layers
4. Show flags
5. Show patches
6. Use Blocked Driver Database
7. Use Application Compatibility Database

## Location:

C:\Windows\apppatch\sysmain.sdb

## Tool:

SDBExplorer.exe

# Windows Registry Hive

The Windows registry is stored in a collection of hive files. Hives are binary files containing a simple filesystem with a set of cells used to store keys, values, data, and related metadata.

The registry can provide a wealth of data for a forensic investigator. With numerous sources of deleted and historical data, a more complete picture of attacker activity can be assembled during an investigation. As attackers continue to gain sophistication and improve their tradecraft, investigators will have to adapt to discover and defend against them.

The following table lists the standard hives and their supporting files.

| Registry Hive | Supporting Files |
| --- | --- |
| HKEY_CURRENT_CONFIG | System, System.alt, System.log, System.sav |
| HKEY_CURRENT_USER | Ntuser.dat, Ntuser.dat.log |
| HKEY_LOCAL_MACHINE\SAM | Sam, Sam.log, Sam.sav, Userclass.dat |
| HKEY_LOCAL_MACHINE\Security | Security, Security.log, Security.sav |
| HKEY_LOCAL_MACHINE\Software | Software, Software.log, Software.sav |
| HKEY_LOCAL_MACHINE\System | System, System.alt, System.log, System.sav |
| HKEY_USERS\.DEFAULT | Default, Default.log, Default.sav |

# Forensically interesting spots in Windows Registry

| Forensic Value | Registry Key Path |
|---|---|
| Time Zone Information | SYSTEM\ControlSet00#\Control\TimeZoneInformation |
| Windows Product Info. | SOFTWARE\Microsoft\Windows NT\CurrentVersion |
| Windows Computer Name | SYSTEM\ControlSet00#\Control\ComputerName\ComputerName |
| Windows Services | SYSTEM\ControlSet00#\Service |
| Windows DHCP Config | SYSTEM\ControlSet00#\Services\Tcpip\Parameters\Interfaces\\\{\DhcpIPAddress |
| Legal Notice & Text | SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System |
| NTFS Last Accessed | SYSTEM\ControlSet\Control\FileSystem |
| Autoruns | Highly recommended to use AutoRuns tool which is from the Microsoft's SysInternals Suite. |
| Installed Applications | HKLM\SOFTWARE\Microsoft\Windows\C.V.\App\Paths |
|  | HKLM\SOFTWARE\Microsoft\Windows\C.V.\Uninstall |
| Windows Firewall | SYSTEM\ControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\EnableFirewall |
|  | SYSTEM\ControlSet\Services\SharedAccess\Parameters\FirewallPolicy\PublicProfile\EnableFirewall |
|  | SYSTEM\ControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\EnableFirewall |
| Remote Desktop | SYSTEM\ControlSet\Control\TerminalServer\fDenyTSConnections |
| Network History | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache |
|  | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed |
|  | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged |
| Network Types (Wired is 0x06 , Broadband is 0x17 , Wireless is 0x47) | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles |
| Shutdown Details | HKLM\SYSTEM\ControlSet001\Control\Windows |
| AppInit_DLLs | HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs |
|  | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs |
| Windows Recycle Bin | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{GUID}\NukeOnDelete |
| Last User Logged In | SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUser |
| User Sessions | SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\SessionData\<#>\LastLoggedOnSamUser |

# Continued to previous slide

| Forensic Value | Registry Key Path |
|---|---|
| Local Users | SAM\Domains\Users |
| UserPasswordHint | SAM\SAM\Domains\Account\Users\\\<32\bithexvalue>\UserPasswordHint |
| Graphic Login Tile | SAM\Domains\Account\Users\\\<32\bit\hexvalue>\UserTile |
| UAL Setting | SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA |
| User Assist Key | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist |
| Last Registry Subkey that was viewed by the user | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\LastKey |
| Hidden Files Settings | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden |
| Hiding File Extensions | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt |
| Start Menu Run MRUs | HKEY_USERS\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU |
| RecentDocs MRUs | HKEY_USERS\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs |
| Remote Desktop MRU | HKEY_USERS\{SID}\Software\Microsoft\Terminal\Server\Client\Servers<br>HKEY_USERS\{SID}\Software\Microsoft\Terminal\Server\Client\Default |
| IE TypedURLs | NTUSER.DAT\Software\Microsoft\Internet Explorer |
| IE Browser Settings | NTUSER.DAT\Software\Microsoft\Internet Explorer\Main |
| MUICache | NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\MUICache |

# Contact Me!

Seriously, don't be a stranger. Ask me anything. I will do my best to help you get your answer or to add something new or correct something that I did not manage to explain correctly. Good luck :)

➢ **Mohammed AlHumaid**

➢ **info@mohammedalhumaid.com**

➢ **https://www.linkedin.com/in/maalhumaid**

➢ **https://twitter.com/ma_alhumaid**