

# (WIP) Using Zimmerman Tools for Windows Forensics (WIP)

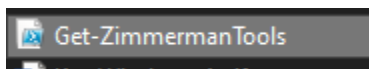


What are Zimmerman Tools? A suite of digital forensics tools developed by Eric Zimmerman. They are used by forensic examiners and investigators to analyze digital evidence. These tools are used for extracting and analyzing various types of data from Windows systems.

Download tools here:

<https://ericzimmerman.github.io/#!index.md>

To download all of his most recent tools, go to the above website and download his powershell script, Get-ZimmermanTools. Run this on the host you want to download the toolset to (you will need internet, also make sure your powershell is up to date and run as admin)



Once the script is run a folder will populate with the toolset (where the powershell script is ran, unless specified). Each tool has its own purpose and is used to examine certain windows artifacts.

Name	Date modified	Type	Size
EvtxCmd	5/23/2024 5:10 PM	File folder	
EZViewer	5/23/2024 5:10 PM	File folder	
iisGeolocate	5/23/2024 5:10 PM	File folder	
JumpListExplorer	5/23/2024 5:10 PM	File folder	
MFTExplorer	5/23/2024 5:10 PM	File folder	
RECmd	5/23/2024 5:10 PM	File folder	
RegistryExplorer	5/23/2024 5:10 PM	File folder	
SDBExplorer	5/23/2024 5:10 PM	File folder	
ShellBagsExplorer	5/23/2024 5:10 PM	File folder	
SQLCmd	5/23/2024 5:10 PM	File folder	
TimelineExplorer	5/23/2024 5:10 PM	File folder	
AmcacheParser.dll	5/21/2023 11:49 AM	Application exten...	2,397 KB
AmcacheParser	5/21/2023 11:49 AM	Application	338 KB
AmcacheParser.runtimeconfig	5/21/2023 11:48 AM	JSON Source File	1 KB
AppCompatCacheParser.dll	3/7/2023 3:13 PM	Application exten...	2,226 KB
AppCompatCacheParser	3/7/2023 3:13 PM	Application	263 KB
AppCompatCacheParser.runtimeconfig	3/7/2023 3:11 PM	JSON Source File	1 KB
bstrings.dll	5/20/2022 12:38 PM	Application exten...	1,697 KB
bstrings	5/20/2022 12:38 PM	Application	524 KB
bstrings.runtimeconfig	5/20/2022 12:38 PM	JSON Source File	1 KB
JLECmd.dll	10/16/2023 3:08 PM	Application exten...	3,227 KB

In the following pages we will go over commonly used Artifacts on a Windows host and how to use Zimmerman tools to analyze them.

You will need .net 6 to be installed on the host to run any GUI zimmerman tool! If not, you will need to go the the below link to download it.

<https://dotnet.microsoft.com/en-us/download/dotnet/6.0>



# ARTIFACTS

## Artifact: \$MFT

What is it: The \$MFT (Master File Table) is a special file used by the NTFS (New Technology File System) in Windows operating systems. It is a crucial component of the NTFS file system and serves as a central database that contains information about every file and directory on an NTFS volume.

For every file on the NTFS volume there are these dates

- (M) Data Content Change Time- this timestamp shows when the content of the file was last modified. It changes every time the file's data is altered.
- (A) Data Last Accessed Time- This timestamp indicates the last time the file was read or accessed. Simply viewing a file's contents will update this timestamp.
- (C) Metadata Change Time- In the NTFS file system, this is referred to as the MFT record modification timestamp. It indicates when the file's metadata or properties were last changed. Changes could include modifications to the file's name, attributes, or location (not the content itself).
- (B) Birth - Often also referred to as the creation timestamp, this records when the file was created on the file system.

Every time one of these events takes place an entry and timestamp will be placed in the \$MFT

Parsing the \$MFT is tremendously effective at creating a timeline of events that took place on a host.

**Windows 10 location:** C:\\$MFT (you will not be able to view it using file explore, but it's there)

**Tool:** MFTECmd.exe

**How to:** We must run MFTECmd.exe to parse the \$MFT into a csv file

```
c:\Users\Patrick\Desktop\Velociraptor\other\net6>MFTECmd.exe -f C:\$MFT --csv C:\Users\Patrick
MFTECmd version 1.2.2.1

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

Command line: -f C:\$MFT --csv C:\Users\Patrick

File type: Mft

C:\$MFT is in use. Rerouting...

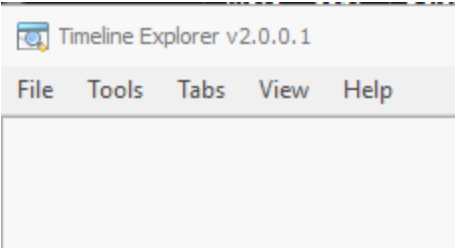
Processed C:\$MFT in 30.8635 seconds

C:\$MFT: FILE records found: 1,233,189 (Free records: 299,702) File size: 1.5GB
      CSV output will be saved to C:\Users\Patrick\20240523225301_MFTECmd_$MFT_Output.csv

c:\Users\Patrick\Desktop\Velociraptor\other\net6>
```

Now we can view the MFT using TimelineExplorer, lets try to search for a file (potential IOC):

Open Timeline Explorer → File → Open → navigate to the parsed MFT is CSV format



Timeline Explorer v2.0.0.1

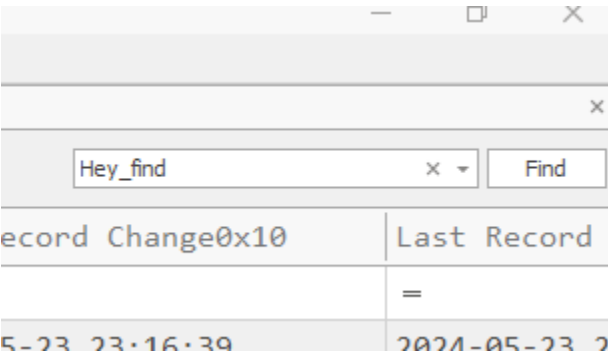
File Tools Tabs View Help

20240523231926\_MFTECmd\_\$MFT\_Output.csv

Drag a column header here to group by that column

	Line	Tag	Entry Number ▲	Sequence Number	Parent Entry Number	Parent Sequence Number	I
▼	=		=	=	=	=	
▶	132282		133039	72	90864	1	
	132283		133040	30	128891	38	
	132284		133041	43	133037	7	
	132285		133042	210	89114	2	

You can search for a file name



View NTFS time stamps, can pivot off the timestamps to see surrounding activity

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

20240523231926\_MFTECmd\_\$MFT\_Output.csv

Drag a column header here to group by that column

	File Name	Extension	Created0x10
▼			=
▶	ing\Microsoft\Window... Hey_find_this_ file.lnk	.lnk	2024-05-23 23:16:39
	Hey_find_this_ file.txt	.txt	2024-05-23 23:16:20

## Artifact: Windows Eventlogs

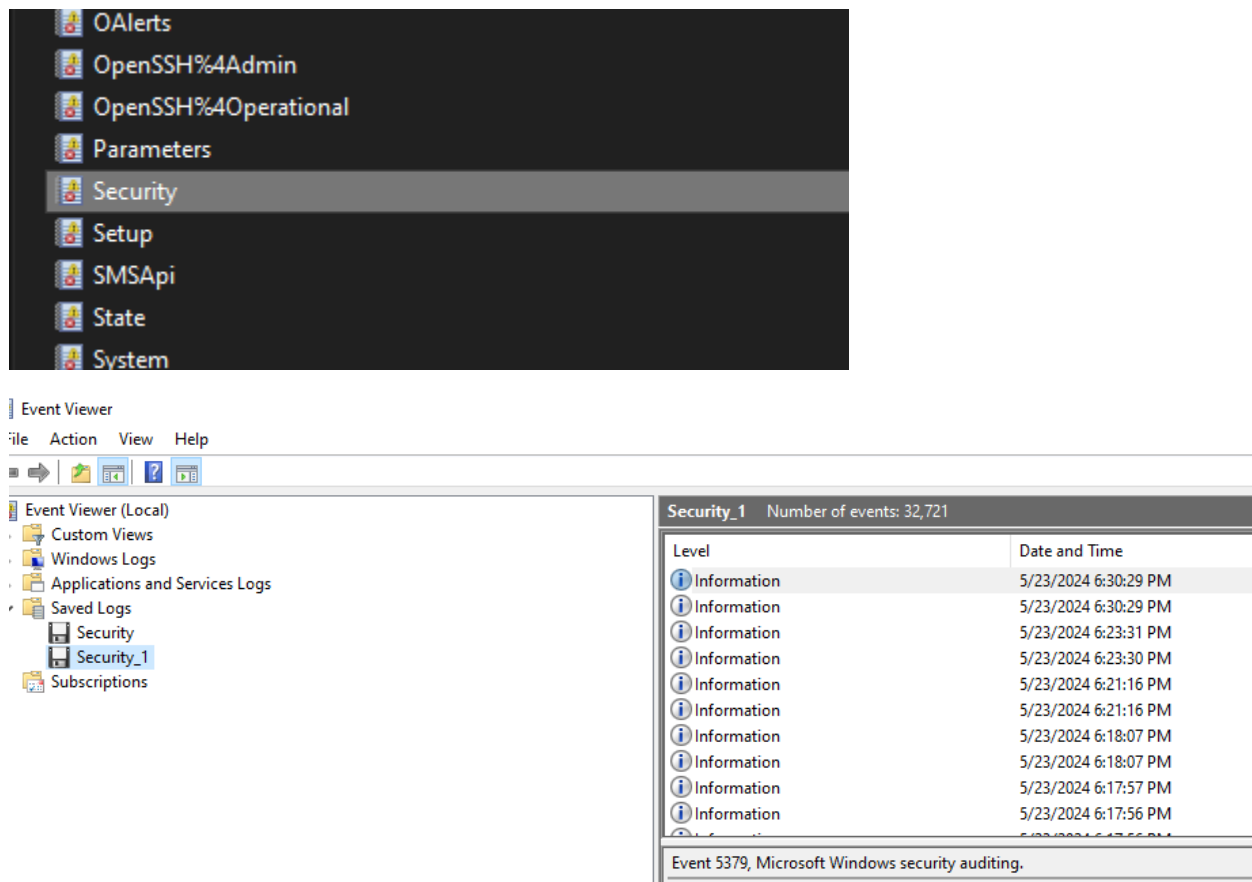
What is it: used to record detailed information about significant hardware, software, and system events on a computer. These logs are essential for system diagnostics, troubleshooting, security monitoring, and forensic investigations.

Types of logs: Application, System, Security, PowerShell, Sysmon (if installed)

**Windows 10 location:** C:\Windows\System32\winevt\Logs\

**Tool:** Windows Event Viewer

**How to:** take .evtx file and open with Windows event viewer

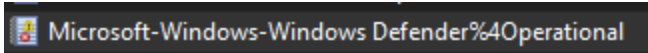


You will need to understand the type of logs you are reviewing and their corresponding Event IDs. I usually find myself in the Security Logs as a great place to start (Sysmon even better if that is installed).

Below is a link that lists Windows Security Log event IDs and what they mean (not official Microsoft documentation, but useful)

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>

Also, note that in the directory C:\Windows\System32\winevt\Logs\ contains Windows Defender logs. This could provide valuable information to see if HBSS successfully defeated a malicious program. If 3<sup>rd</sup> party antivirus is used you'll have to do research to see where the location for those logs are.



## Artifact: Prefetch

What is it: Prefetch files are files created by the Windows operating system to speed up the loading time of applications. They are part of the Windows Prefetcher, a component of the memory management system introduced in Windows XP and present in later versions. They are a key artifact to show potential execution of a program.

**Windows 10 location:** C:\Windows\Prefetch

**Tool:** PECmd

**How to:** You can view the directory to see all the prefetch files created, these should line up with a corresponding executable. Even better you can note a specific prefetch file and use the Zimmerman tool PECmd to provide detailed information about the execution of the application, including the files and directories it accessed, execution timestamps, and usage statistics

```
c:\Windows\Prefetch>dir
Volume in drive C has no label.
Volume Serial Number is 0283-E8ED

Directory of c:\Windows\Prefetch

05/23/2024  08:14 PM    <DIR>          .
05/23/2024  08:14 PM    <DIR>          ..
04/28/2024  12:43 AM             99,278  7ZG.EXE-0F8C4081.pf
05/23/2024  05:13 PM             63,572  ACROBAT.EXE-241192A7.pf
05/23/2024  05:13 PM             88,841  ACROBAT.EXE-241192A8.pf
05/23/2024  08:14 PM             29,314  ACRODIST.EXE-634B1B78.pf
05/23/2024  08:04 PM             14,914  ACROTRAY.EXE-9534F974.pf
09/20/2023  05:07 PM            149,134  ADOBE_DESKTOP_SERVICE.EXE-C3C0AD3C.pf
05/20/2024  01:43 PM             17,576  APPLICATIONFRAMEHOST.EXE-CCEE759.pf
05/09/2024  07:55 PM             50,830  ATMGR.EXE-5D4545CE.pf
05/23/2024  08:17 PM             13,163  BACKGROUNDTASKHOST.EXE-D61F7B44.pf
05/21/2024  10:52 PM              80  cadrespri.7db
```

```
>PECmd.exe -f "C:\Windows\Prefetch\notepad.exe-D8414F97.pf"
```

```
Command line: -f C:\Windows\Prefetch\NOTEPAD.EXE-D8414F97.pf
Keywords: temp, tmp
Processing C:\Windows\Prefetch\NOTEPAD.EXE-D8414F97.pf
Created on: 2021-03-20 04:33:18
Modified on: 2024-05-23 22:08:06
Last accessed on: 2024-05-24 01:20:15
Executable name: NOTEPAD.EXE
Hash: D8414F97
File size (bytes): 69,630
Version: Windows 10 or Windows 11
Run count: 223
Last run: 2024-05-23 22:07:55
Other run times: 2024-05-19 05:06:19, 2024-05-12 20:00:12, 2024-05-12 19:59:12, 2024-05-12 19:58:12, 2024-05-12 19:57:12, 2024-05-12 19:56:12, 2024-05-12 19:55:12, 2024-05-12 19:54:12, 2024-05-12 19:53:12, 2024-05-12 19:52:12, 2024-05-12 19:51:12, 2024-05-12 19:50:12, 2024-05-12 19:49:12, 2024-05-12 19:48:12, 2024-05-12 19:47:12, 2024-05-12 19:46:12, 2024-05-12 19:45:12, 2024-05-12 19:44:12, 2024-05-12 19:43:12, 2024-05-12 19:42:12, 2024-05-12 19:41:12, 2024-05-12 19:40:12, 2024-05-12 19:39:12, 2024-05-12 19:38:12, 2024-05-12 19:37:12, 2024-05-12 19:36:12, 2024-05-12 19:35:12, 2024-05-12 19:34:12, 2024-05-12 19:33:12, 2024-05-12 19:32:12, 2024-05-12 19:31:12, 2024-05-12 19:30:12, 2024-05-12 19:29:12, 2024-05-12 19:28:12, 2024-05-12 19:27:12, 2024-05-12 19:26:12, 2024-05-12 19:25:12, 2024-05-12 19:24:12, 2024-05-12 19:23:12, 2024-05-12 19:22:12, 2024-05-12 19:21:12, 2024-05-12 19:20:12, 2024-05-12 19:19:12, 2024-05-12 19:18:12, 2024-05-12 19:17:12, 2024-05-12 19:16:12, 2024-05-12 19:15:12, 2024-05-12 19:14:12, 2024-05-12 19:13:12, 2024-05-12 19:12:12, 2024-05-12 19:11:12, 2024-05-12 19:10:12, 2024-05-12 19:09:12, 2024-05-12 19:08:12, 2024-05-12 19:07:12, 2024-05-12 19:06:12, 2024-05-12 19:05:12, 2024-05-12 19:04:12, 2024-05-12 19:03:12, 2024-05-12 19:02:12, 2024-05-12 19:01:12, 2024-05-12 19:00:12, 2024-05-12 18:59:12, 2024-05-12 18:58:12, 2024-05-12 18:57:12, 2024-05-12 18:56:12, 2024-05-12 18:55:12, 2024-05-12 18:54:12, 2024-05-12 18:53:12, 2024-05-12 18:52:12, 2024-05-12 18:51:12, 2024-05-12 18:50:12, 2024-05-12 18:49:12, 2024-05-12 18:48:12, 2024-05-12 18:47:12, 2024-05-12 18:46:12, 2024-05-12 18:45:12, 2024-05-12 18:44:12, 2024-05-12 18:43:12, 2024-05-12 18:42:12, 2024-05-12 18:41:12, 2024-05-12 18:40:12, 2024-05-12 18:39:12, 2024-05-12 18:38:12, 2024-05-12 18:37:12, 2024-05-12 18:36:12, 2024-05-12 18:35:12, 2024-05-12 18:34:12, 2024-05-12 18:33:12, 2024-05-12 18:32:12, 2024-05-12 18:31:12, 2024-05-12 18:30:12, 2024-05-12 18:29:12, 2024-05-12 18:28:12, 2024-05-12 18:27:12, 2024-05-12 18:26:12, 2024-05-12 18:25:12, 2024-05-12 18:24:12, 2024-05-12 18:23:12, 2024-05-12 18:22:12, 2024-05-12 18:21:12, 2024-05-12 18:20:12, 2024-05-12 18:19:12, 2024-05-12 18:18:12, 2024-05-12 18:17:12, 2024-05-12 18:16:12, 2024-05-12 18:15:12, 2024-05-12 18:14:12, 2024-05-12 18:13:12, 2024-05-12 18:12:12, 2024-05-12 18:11:12, 2024-05-12 18:10:12, 2024-05-12 18:09:12, 2024-05-12 18:08:12, 2024-05-12 18:07:12, 2024-05-12 18:06:12, 2024-05-12 18:05:12, 2024-05-12 18:04:12, 2024-05-12 18:03:12, 2024-05-12 18:02:12, 2024-05-12 18:01:12, 2024-05-12 18:00:12, 2024-05-12 17:59:12, 2024-05-12 17:58:12, 2024-05-12 17:57:12, 2024-05-12 17:56:12, 2024-05-12 17:55:12, 2024-05-12 17:54:12, 2024-05-12 17:53:12, 2024-05-12 17:52:12, 2024-05-12 17:51:12, 2024-05-12 17:50:12, 2024-05-12 17:49:12, 2024-05-12 17:48:12, 2024-05-12 17:47:12, 2024-05-12 17:46:12, 2024-05-12 17:45:12, 2024-05-12 17:44:12, 2024-05-12 17:43:12, 2024-05-12 17:42:12, 2024-05-12 17:41:12, 2024-05-12 17:40:12, 2024-05-12 17:39:12, 2024-05-12 17:38:12, 2024-05-12 17:37:12, 2024-05-12 17:36:12, 2024-05-12 17:35:12, 2024-05-12 17:34:12, 2024-05-12 17:33:12, 2024-05-12 17:32:12, 2024-05-12 17:31:12, 2024-05-12 17:30:12, 2024-05-12 17:29:12, 2024-05-12 17:28:12, 2024-05-12 17:27:12, 2024-05-12 17:26:12, 2024-05-12 17:25:12, 2024-05-12 17:24:12, 2024-05-12 17:23:12, 2024-05-12 17:22:12, 2024-05-12 17:21:12, 2024-05-12 17:20:12, 2024-05-12 17:19:12, 2024-05-12 17:18:12, 2024-05-12 17:17:12, 2024-05-12 17:16:12, 2024-05-12 17:15:12, 2024-05-12 17:14:12, 2024-05-12 17:13:12, 2024-05-12 17:12:12, 2024-05-12 17:11:12, 2024-05-12 17:10:12, 2024-05-12 17:09:12, 2024-05-12 17:08:12, 2024-05-12 17:07:12, 2024-05-12 17:06:12, 2024-05-12 17:05:12, 2024-05-12 17:04:12, 2024-05-12 17:03:12, 2024-05-12 17:02:12, 2024-05-12 17:01:12, 2024-05-12 17:00:12, 2024-05-12 16:59:12, 2024-05-12 16:58:12, 2024-05-12 16:57:
```

Files referenced (could be used to see an injected process, is it accessing any strange dlls?)

```
Files referenced: 97
00: \\VOLUME{01d61db383dc28d5-0283e8ed}\\WINDOWS\\SYSTEM32\\NOTEPAD.EXE (Executable: True)
01: \\VOLUME{01d61db383dc28d5-0283e8ed}\\WINDOWS\\SYSTEM32\\NTDLL.DLL
02: \\VOLUME{01d61db383dc28d5-0283e8ed}\\WINDOWS\\SYSTEM32\\KERNEL32.DLL
03: \\VOLUME{01d61db383dc28d5-0283e8ed}\\WINDOWS\\SYSTEM32\\KERNELBASE.DLL
04: \\VOLUME{01d61db383dc28d5-0283e8ed}\\WINDOWS\\SYSTEM32\\LOCALE.NLS
05: \\VOLUME{01d61db383dc28d5-0283e8ed}\\PROGRAM FILES\\NORTON SECURITY\\NORTONDATA\\22.21.3.
06: \\VOLUME{01d61db383dc28d5-0283e8ed}\\WINDOWS\\SYSTEM32\\ADVAPI32.DLL
07: \\VOLUME{01d61db383dc28d5-0283e8ed}\\WINDOWS\\SYSTEM32\\MSVCRT.DLL
08: \\VOLUME{01d61db383dc28d5-0283e8ed}\\WINDOWS\\SYSTEM32\\SECHOST.DLL
09: \\VOLUME{01d61db383dc28d5-0283e8ed}\\WINDOWS\\SYSTEM32\\RPCRT4.DLL
```

You can also run <PECmd.exe -d "C:\Windows\Prefetch"> To output the entire directory

## Artifact: Internet history files

What is it: Each browser will store a history file in it's default location that contains a user's browsing history. These are usually stored in an SQLite database.

### Windows 10 location:

Chrome: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History

Edge: %USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\Default\History

Firefox: %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\places.sqlite

**Tool:** SQLite viewer. As of my knowledge Zimmerman doesn't have a tool to view browser history. An easy solution is to use SQLite viewer, just drag and drop the history file and export it to a csv (note, be cautious on what you upload. The github claims no file will be uploaded as it uses JavaScript HTML5 File Reader ).

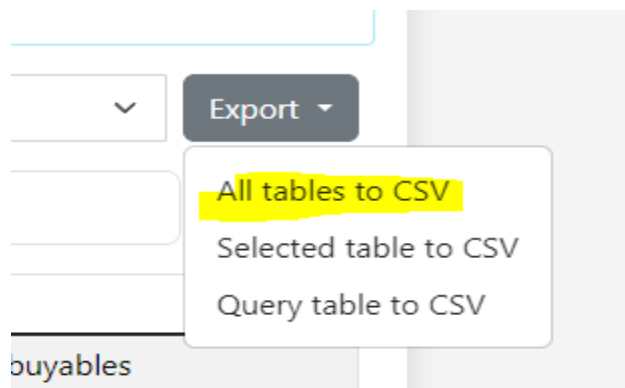
How to: upload one of the SQL lite databases to <https://inloop.github.io/sqlite-viewer/#>



**Drop file here** to load content or click on this box to open file dialog  
No file will be uploaded - uses only JavaScript HTML5 FileReader.

[... or download & try this sample file](#)

Export to csv



View in the tables you have downloaded, this is the parsed out history file



Name	Type
cluster_keywords	Microsoft Ex
cluster_visit_duplicates	Microsoft Ex
clusters	Microsoft Ex
clusters_and_visits	Microsoft Ex
content_annotations	Microsoft Ex
context_annotations	Microsoft Ex
downloads	Microsoft Ex
downloads_slices	Microsoft Ex
downloads_url_chains	Microsoft Ex
history_sync_metadata	Microsoft Ex
keyword_search_terms	Microsoft Ex
meta	Microsoft Ex
segment_usage	Microsoft Ex
segments	Microsoft Ex
sqlite_sequence	Microsoft Ex
urls	Microsoft Ex
visit_source	Microsoft Ex
visited_links	Microsoft Ex
visits	Microsoft Ex

I think the most useful tables are downloads and urls

Lets open the downloads up (of course we'll use Timeline explorer)

C:\Users\Patrick\Downloads\FY24 USAF Selective Retention Bonus Listing.pdf
C:\Users\Patrick\Downloads\SANS_DFPS_FOR500_v4.17_02-23.pdf
C:\Users\Patrick\Downloads\walkthrough.rtf
C:\Users\Patrick\Downloads\velociraptor-v0.72.3-windows-amd64.exe
C:\Users\Patrick\Downloads\velociraptor-v0.72.3-windows-amd64.exe
C:\Users\Patrick\Downloads\velociraptor-v0.72.3-windows-amd64.exe.sig
C:\Users\Patrick\Downloads\velociraptor-v0.72.3-windows-amd64.exe
C:\Users\Patrick\Downloads\velociraptor-v0.72.3-windows-amd64.exe
C:\Users\Patrick\Downloads\Get-ZimmermanTools.zip
C:\Users\Patrick\Downloads\dotnet-sdk-6.0.422-win-x64.exe

As you can see it stores what was downloaded from chrome. I was surprised how far the database goes back.

Lets take a look at the urls table. A column of urls visited will appear. Using timeline explorer we can filter for whatever we are searching for.

here to group by that column		foundry	x	Find
	url			
	url			
85	https://foundry.texnet1.net/console/vm/42292c5f-d43f-a356-2cae-366637747eb8/console?theme=dark-theme			
72	https://foundry.texnet1.net/player			
88	https://foundry.texnet1.net/vm/views/bcb160f8-2a9b-4cff-b70a-d2bad15203d9/map?theme=dark-theme			
89	https://foundry.texnet1.net/vm/views/bcb160f8-2a9b-4cff-b70a-d2bad15203d9?theme=dark-theme			
87	https://foundry.texnet1.net/player/view/bcb160f8-2a9b-4cff-b70a-d2bad15203d9?teamId=5a377375-9b0c-4c45-80e6-3393b5c			

## Artifact: Amcache.hve

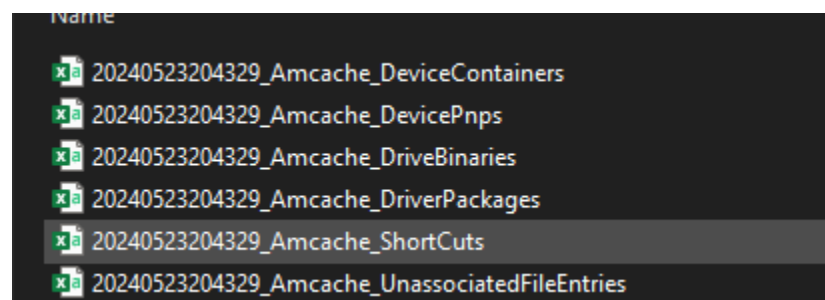
What is it: The Amcache.hve file in Windows is a part of the Windows Registry that stores important information related to the execution of applications.

**Windows 10 location:** C:\Windows\AppCompat\Programs\Amcache.hve


**Tool:** AmcacheParser

**How to:** parse hive with the amcacheparser

```
>AmcacheParser.exe -f "c:\Windows\appcompat\Programs\Amcache.hve" --csv "c:\Users\Patrick"
```



Use timeline explorer to view the csv. We'll check out the unassociatedFileEntries csv output, most closely associated with program execution.

View	Help
File UnassociatedFileEntries.csv	
header here to group by that column	
	Name
	 c
122.77_124.0.6367.210_chrome_updater...	125.0.6422.77_124.0.6367.210_...
_8wekyb3d8bbwe\3dviewer.exe	3DViewer.exe
	7z.exe
ifier.exe	AAM Registration Notifier.exe
ifier.exe	AAM Registration Notifier.exe
.exe	AAM Updates Notifier.exe
	AAMCustomHook.exe
	AAMLauncher.exe
	AAMLauncherUtil.exe
	AASIapp.exe
	AddInUtil.exe
	addprinter.exe
anager (updater).exe	Adobe Application Manager (Up...
	AdobeIPCBroker.exe
rokercustomhook.exe	AdobeIPCBrokerCustomHook.exe

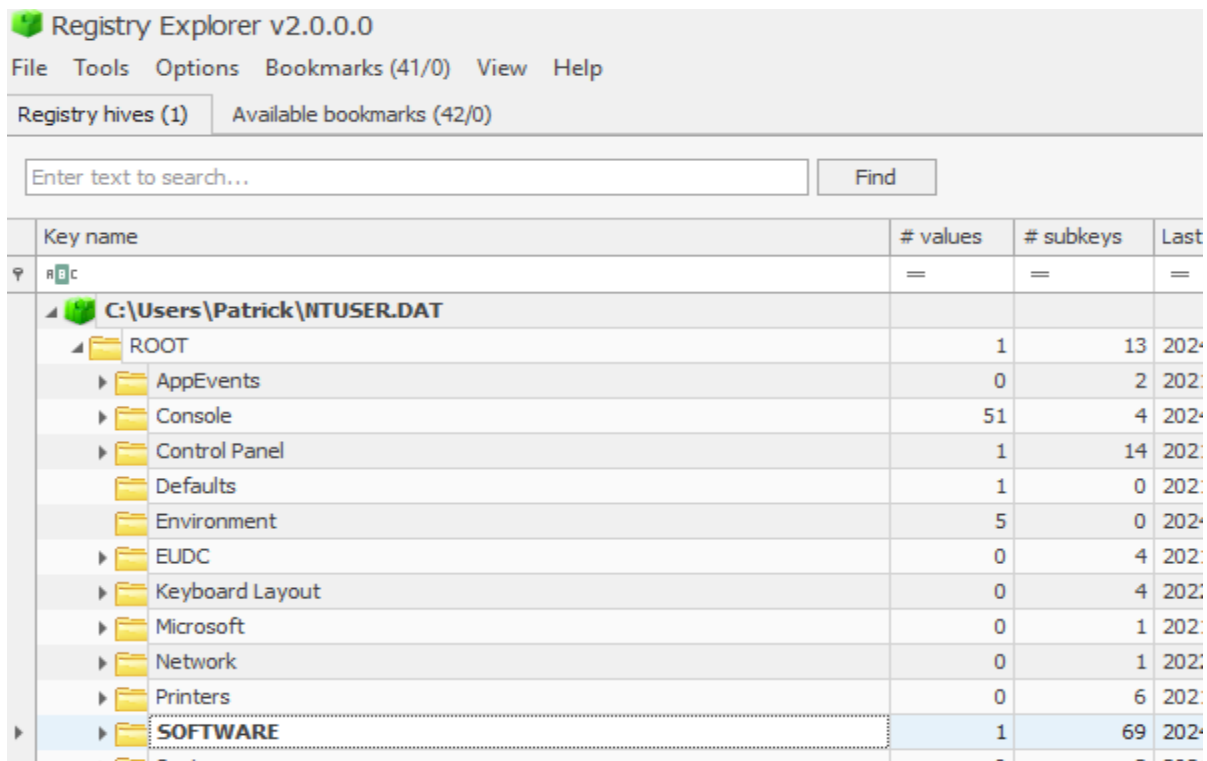
## Artifact: NTUSER.dat

What is it: is a registry file associated with a user profile on Windows. It contains user-specific registry settings that are loaded when a user logs into their Windows account. These settings help configure the user's environment according to their preferences and previous configurations.

**Windows 10 location:** %USERPROFILE%\NTUSER.dat

**Tool:** Registry Explorer

**How to:** open registry Explorer → load hive and select the artifact NTUSER.dat



There is a plethora of information you can get about a user from this file

Example:

UserAssist – records GUI-based program execution

NTUSER.dat location –

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count

{System}\SnippingTool.exe	
{System}\WF.msc	
NortonLifeLock.Norton Security	
Microsoft.Windows.ControlPanel	
Microsoft.Windows.Explorer	
MSEdge	
Microsoft.Office.WINWORD.EXE.15	
{System}\notepad.exe	
{System}\WindowsPowerShell\v1.0\PowerShell_	
ISE.exe	
{ProgramFilesX86}\Adobe\Acrobat	
DC\Acrobat\Acrobat.exe	
C:\Users\Patrick\Desktop\Velociraptor\other\net	
6\EZViewer\EZViewer.exe	

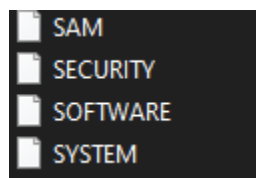
Also gives last execution time

Last Executed
=
2024-05-23 18:53:17
2024-05-23 19:09:44
2024-05-23 21:42:26
2024-05-23 21:43:09
2024-05-23 21:45:42
2024-05-23 21:45:44
2024-05-23 21:46:05
2024-05-23 21:55:45
2024-05-23 22:07:55
2024-05-23 22:08:14

## Artifact: Registry Hive

What is it: A registry hive is a group of keys, subkeys, and values in the Windows Registry that is stored in a respective file. Each hive contains a specific portion of the registry data and is loaded during system startup or user login. The hives represent different aspects of the configuration and are vital for the operation of the operating system and applications.

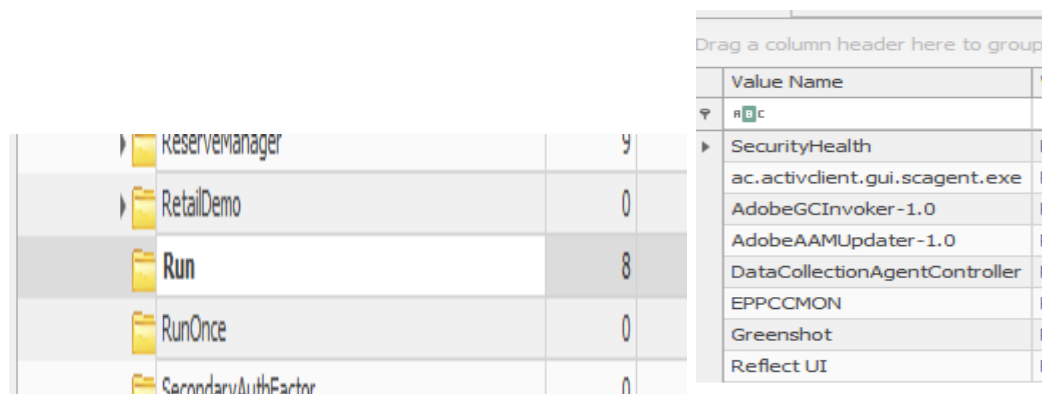
**Windows 10 location:** C:\Windows\System32\Config\



For forensics I generally will try to pull the Software hive, but the others may be useful as well.

**Tool:** registry explorer or reg editor

**How to:** pull one of the hives and open in either reg explorer (Zimmerman tool) or windows reg editor.



I opened the software hive and brought up the Run key. There are numerous artifacts in the registry that are useful. I'll list a few

---

**HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist**

We've talked about this before, it shows applications executed by gui

**HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Shell\BagMRU**

Stores information about folder settings, such as view preferences and size, which can reveal whether a user accessed a specific folder, even if the folder has been deleted.

**HKEY\_LOCAL\_MACHINE\SYSTEM\MountedDevices**

Contains information on all devices that have ever been mounted, providing insights into external drives, USB sticks, and other storage devices that were connected to the system.

**HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**

Lists recently opened documents, which can be used to determine recent user activities.

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall**

Contains details on installed software and any software that has been uninstalled, useful for identifying potentially malicious installations.

## Artifact: System Resource Usage Monitor (SRUM)

What is it: The System Resource Usage Monitor (SRUM) is a feature in Windows that collects system data related to resource usage, which can be useful in forensic analysis. SRUM tracks detailed information about resource usage by applications and users on a Windows machine, such as CPU usage, network usage, disk activity, and more, over time

**Windows 10 location:** C:\Windows\System32\sru\SRUDB.dat

**Tool:** ScumECmd

**How to:** first parse the data into a CSV

```
ScumECmd.exe -f C:\Users\Patrick\Desktop\Velociraptor\other\SRUDB.dat --csv C:\Users\Patrick
```

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

Command line: -f C:\Users\Patrick\Desktop\Velociraptor\other\SRUDB.dat --csv C:\Users\Patrick

Processing 'C:\Users\Patrick\Desktop\Velociraptor\other\SRUDB.dat'...

Processing complete!








Energy Usage count:          194
AppTimelineProvider count:   27,821
vfuprov count:              2,452
App Resource Usage count:    120,951
Network Connection count:    2,149
Network Usage count:         28911
Push Notification count:     631

CSV output will be saved to 'C:\Users\Patrick'

Processing completed in 6.3042 seconds

c:\Users\Patrick\Desktop\Velociraptor\other\net6>
```

7 csv's are created

Name	Date modified
 20240523235026_SrumECmd_AppResourceUseInfo_Output	5/23/2024 6:50 PM
 20240523235026_SrumECmd_AppTimelineProvider_Output	5/23/2024 6:50 PM
 20240523235026_SrumECmd_NetworkConnections_Output	5/23/2024 6:50 PM
 20240523235026_SrumECmd_NetworkUsages_Output	5/23/2024 6:50 PM
 20240523235026_SrumECmd_PushNotifications_Output	5/23/2024 6:50 PM
 20240523235026_SrumECmd_vfuprov_Output	5/23/2024 6:50 PM
 20240523235026_SrumECmd_EnergyUsage_Output	5/23/2024 6:50 PM

Now we can view the csv with Timeline explorer. Lets look at the AppResourceUseInfo, this potentially can be used as evidence of file execution.

120898	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	\Device\HarddiskVolume2\Program Files\Microsoft Office\root\Office16\WINWORD.EXE
120897	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	\Device\HarddiskVolume2\Program Files (x86)\VMware\VMware Horizon View Client\x64\vmware-print-redir-c
120896	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	\Device\HarddiskVolume2\Program Files (x86)\VMware\VMware Horizon View Client\x64\vmware-remotemks.exe
120895	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	\Device\HarddiskVolume2\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe
120894	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	\Device\HarddiskVolume2\Users\Patrick\AppData\Local\Microsoft\OneDrive\24.086.0428.0003\FileCoAuth.exe
120893	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	\Device\HarddiskVolume2\Program Files (x86)\Webull Desktop\wb_crashpad_handler.exe
120892	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	\Device\HarddiskVolume2\Program Files (x86)\Webull Desktop\Webull Desktop.exe
120891	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	\Device\HarddiskVolume2\Users\Patrick\AppData\Local\Microsoft\OneDrive\24.086.0428.0003\Microsoft.Shar
120890	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	\Device\HarddiskVolume2\Program Files\Proton\VPN\v3.2.11\ProtonVPN.exe
120889	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	\Device\HarddiskVolume2\Windows\System32\SnippingTool.exe
120888	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	\Device\HarddiskVolume2\Program Files (x86)\GeoComply\PlayerLocationCheck\PlayerLocationIcon.exe
120887	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	\Device\HarddiskVolume2\Windows\System32\notepad.exe
120886	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	Microsoft.MicrosoftOfficeHub_18.2405.1121.0_x64__8wekyb3d8bbwe
120885	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	AdobeAcrobatDCCoreApp_23.0.0.0_x64__pc75e8sa7ep4e
120884	<input type="checkbox"/>	27649...	2024-05-23 23:15:00	\Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

## Artifact: Windows 10 Timeline

What is it: This is a newer artifact in windows 10. Windows 10 records recently used applications and files in a “timeline” database in SQLite format.

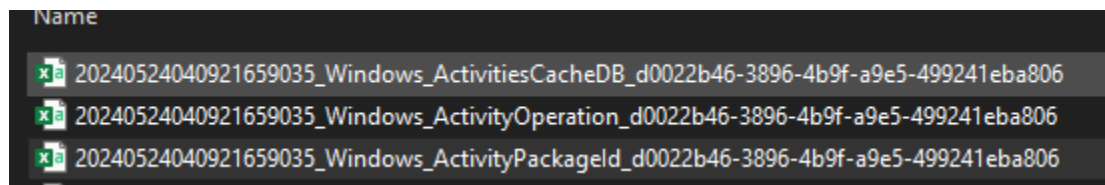
**Location:** %USERPROFILE%\AppData\Local\ConnectedDevicesPlatform\\ActivitiesCache.db

Tool: SQLECmd.exe

## How to: parse the db file with SQLECmd.exe.

```
>SQLCmd.exe -f c:\Users\Patrick\Desktop\ActivitiesCache.db --csv C:\Users\Patrick
```

3 CSVs should be produced. I found the most useful to be the Windows\_ActivityOperation



Lets use timeline explorer to open the CSV and see the timeline windows 10 has in the database. Looking through the results I see a familiar list of recent applications I have used. The database went back about two months.

```
[{"application": "Chrome", "platform": "windows_win32"}, {"application": "Chrome", "platform": "packageId"}, {"application": "Chrome", "platform": "packageId"}, {"application": "Microsoft.Office.EXCEL.EXE.15", "platform": "windows_win32"}, {"application": "excel.activity.windows", "platform": "windows_universal"}, {"application": "Microsoft.WindowsCamera_8wekyb3d8bbwe!App", "platform": "windows_universal"}, {"application": "Microsoft.WindowsCamera_8wekyb3d8bbwe!App", "platform": "packageId"}, {"application": "Chrome", "platform": "windows_win32"}, {"application": "Chrome", "platform": "packageId"}, {"application": "Chrome", "platform": "packageId"}, {"application": "Norton.Secure VPN", "platform": "x_exe_path"}, {"application": "Norton.Secure VPN", "platform": "packageId"}, {"application": "C:\\Users\\Patrick\\Downloads\\Draftkings Non Live Gaming Player Location Check.exe", "platform": "windows_win32"}, {"application": "C:\\Users\\Patrick\\Downloads\\Draftkings Non Live Gaming Player Location Check.exe", "platform": "packageId"}, {"application": "C:\\Users\\Patrick\\Downloads\\Draftkings Non Live Gaming Player Location Check.exe", "platform": "packageId"}, {"application": "C:\\Users\\Patrick\\Downloads\\Draftkings Non Live Gaming Player Location Check.exe", "platform": "packageId"}, {"application": "C:\\Users\\Patrick\\Downloads\\Draftkings Non Live Gaming Player Location Check.exe", "platform": "packageId"}, {"application": "Norton.Secure VPN", "platform": "x_exe_path"}, {"application": "Norton.Secure VPN", "platform": "packageId"}, {"application": "Norton.Secure VPN", "platform": "packageId"}, {"application": "Chrome", "platform": "windows_win32"}, {"application": "Chrome", "platform": "packageId"}, {"application": "Chrome", "platform": "packageId"}]
```