Prefetch: The Little Snitch That Tells on You

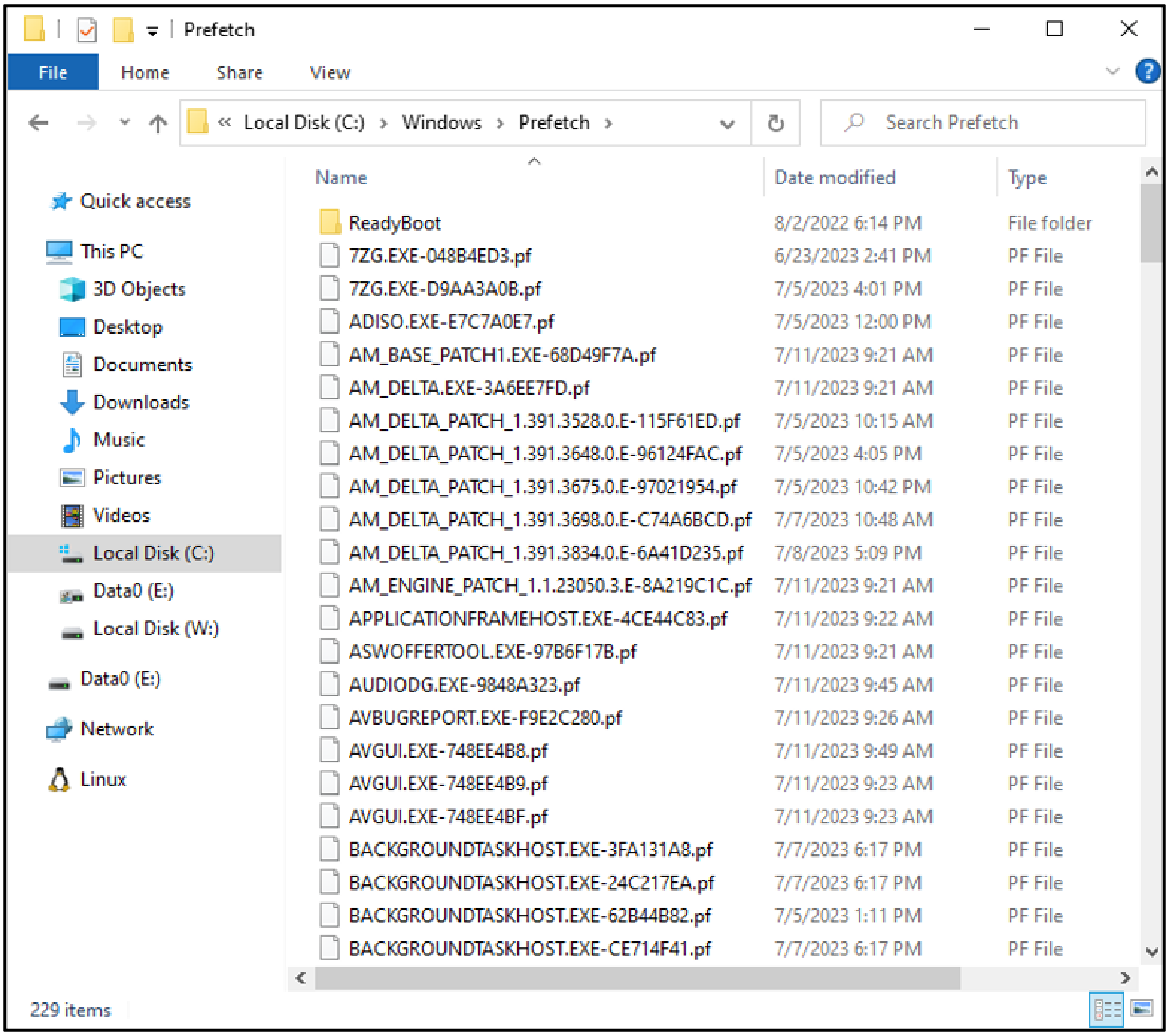
trustedsec.com/blog/prefetch-the-little-snitch-that-tells-on-you

By Shane Hartman in Incident Response, Incident Response & Forensics

July 25, 2023

Incident Response and forensic analysts use the contents of prefetch files in investigations to gather information, such as the source from which an executable was launched, how many times it was executed, what files it touched, and the date and time it was launched. A prefetch file is like the little brother that tells the parents who broke the lamp.

Prefetching is a Windows memory management process in which the operating system pre-loads resources from disk into memory as a means of speeding up the loading time for applications. As part of its process, a .pf file is created in the C:\Windows\Prefetch directory and updated each subsequent time the application is executed. The .pf file contains a list of resources, including files and directories that the executable referenced during execution, which is used to pre-load those resources the next time the application is executed.



Name	Date modified	Type
ReadyBoot	8/2/2022 6:14 PM	File folder
7ZG.EXE-048B4ED3.pf	6/23/2023 2:41 PM	PF File
7ZG.EXE-D9AA3A0B.pf	7/5/2023 4:01 PM	PF File
ADISO.EXE-E7C7A0E7.pf	7/5/2023 12:00 PM	PF File
AM_BASE_PATCH1.EXE-68D49F7A.pf	7/11/2023 9:21 AM	PF File
AM_DELTA.EXE-3A6EE7FD.pf	7/11/2023 9:21 AM	PF File
AM_DELTA_PATCH_1.391.3528.0.E-115F61ED.pf	7/5/2023 10:15 AM	PF File
AM_DELTA_PATCH_1.391.3648.0.E-96124FAC.pf	7/5/2023 4:05 PM	PF File
AM_DELTA_PATCH_1.391.3675.0.E-97021954.pf	7/5/2023 10:42 PM	PF File
AM_DELTA_PATCH_1.391.3698.0.E-C74A6BCD.pf	7/7/2023 10:48 AM	PF File
AM_DELTA_PATCH_1.391.3834.0.E-6A41D235.pf	7/8/2023 5:09 PM	PF File
AM_ENGINE_PATCH_1.1.23050.3.E-8A219C1C.pf	7/11/2023 9:21 AM	PF File
APPLICATIONFRAMEHOST.EXE-4CE44C83.pf	7/11/2023 9:22 AM	PF File
ASWOFFERTOOL.EXE-97B6F17B.pf	7/11/2023 9:21 AM	PF File
AUDIODG.EXE-9848A323.pf	7/11/2023 9:45 AM	PF File
AVBUGREPORT.EXE-F9E2C280.pf	7/11/2023 9:26 AM	PF File
AVGUI.EXE-748EE4B8.pf	7/11/2023 9:49 AM	PF File
AVGUI.EXE-748EE4B9.pf	7/11/2023 9:23 AM	PF File
AVGUI.EXE-748EE4BF.pf	7/11/2023 9:23 AM	PF File
BACKGROUNDTASKHOST.EXE-3FA131A8.pf	7/7/2023 6:17 PM	PF File
BACKGROUNDTASKHOST.EXE-24C217EA.pf	7/7/2023 6:17 PM	PF File
BACKGROUNDTASKHOST.EXE-62B44B82.pf	7/5/2023 1:11 PM	PF File
BACKGROUNDTASKHOST.EXE-CE714F41.pf	7/7/2023 6:17 PM	PF File

Figure 1- Example Prefetch Directory Listing

The .pf file naming convention is <executable name> in all caps, followed by a hyphen and a series of eight (8) letters and numbers (which is the hash value of the path where the executable is located on the filesystem), and lastly, a .pf extension. The astute observer will note from the previous figure that some of the executables have more than one (1) entry. There are two (2) reasons for this. The first is that certain executables such as svchost.exe and rundll32.exe can execute multiple times, spawning separate sub-processes. The operating system notes this and creates separate entries denoted by a different hash, which is the hash of the executable path and the command line used to start the application.

The second reason for the presence of an additional entry is that an application with the same name is executed from a different location. Attackers will sometimes use the names of common applications to hide their activities. This may get by some security systems; however, by reviewing the entries within the .pf file, the true path to the location of the executable is disclosed.

Another item to note is that there are two (2) instances when prefetch files may not be available on the system: when the Windows system is a server, or when the operating system drives are solid state drives (SSDs). This is because the Prefetch process doesn't offer the same benefits in finding and loading files from disk. The following registry key is used to determine whether the Prefetch process is configured.

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\Prefetech Parameters

Name: EnablePrefetcher

Type: REG_DWORD

Values:

0 – Disabled

1 – Application launch prefetching enabled

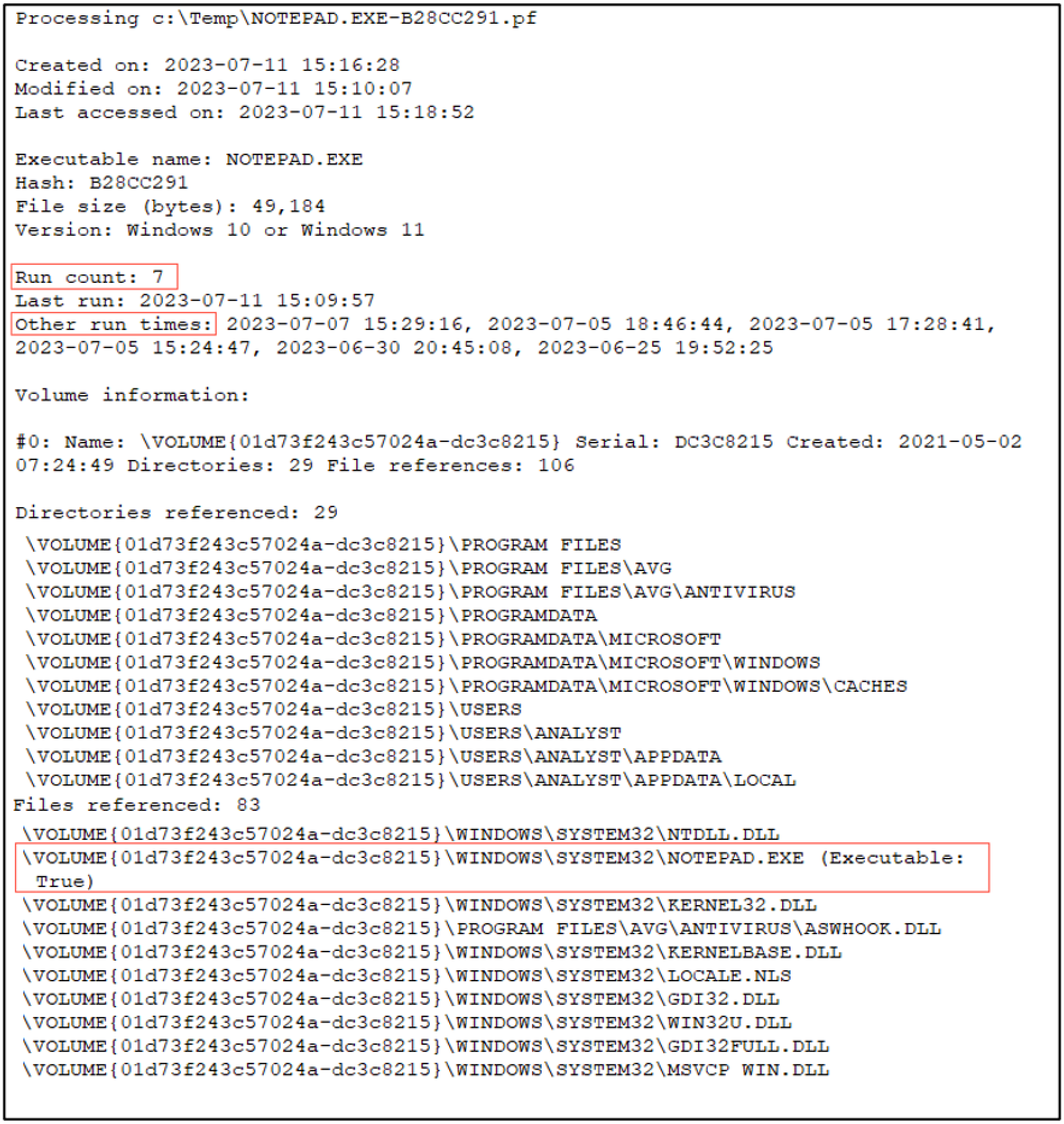
2 – Boot prefetching enabled

3 – Application launch and boot prefetching enabled

How Investigators Use Prefetch File Contents

The prefetch file, while not intended for analysis, can provide a wealth of information for an investigator. When opened, a prefetch file can show:

- Creation date – timestamped with the local time of the machine
- Date/time of last execution time – timestamped with the local time of the machine
- Run count – the number of times the executable has been launched
- Other run times – limited to the previous eight (8) executions
- Directories and files referenced – includes other executables
- Volumes and file paths – the location from which files were accessed

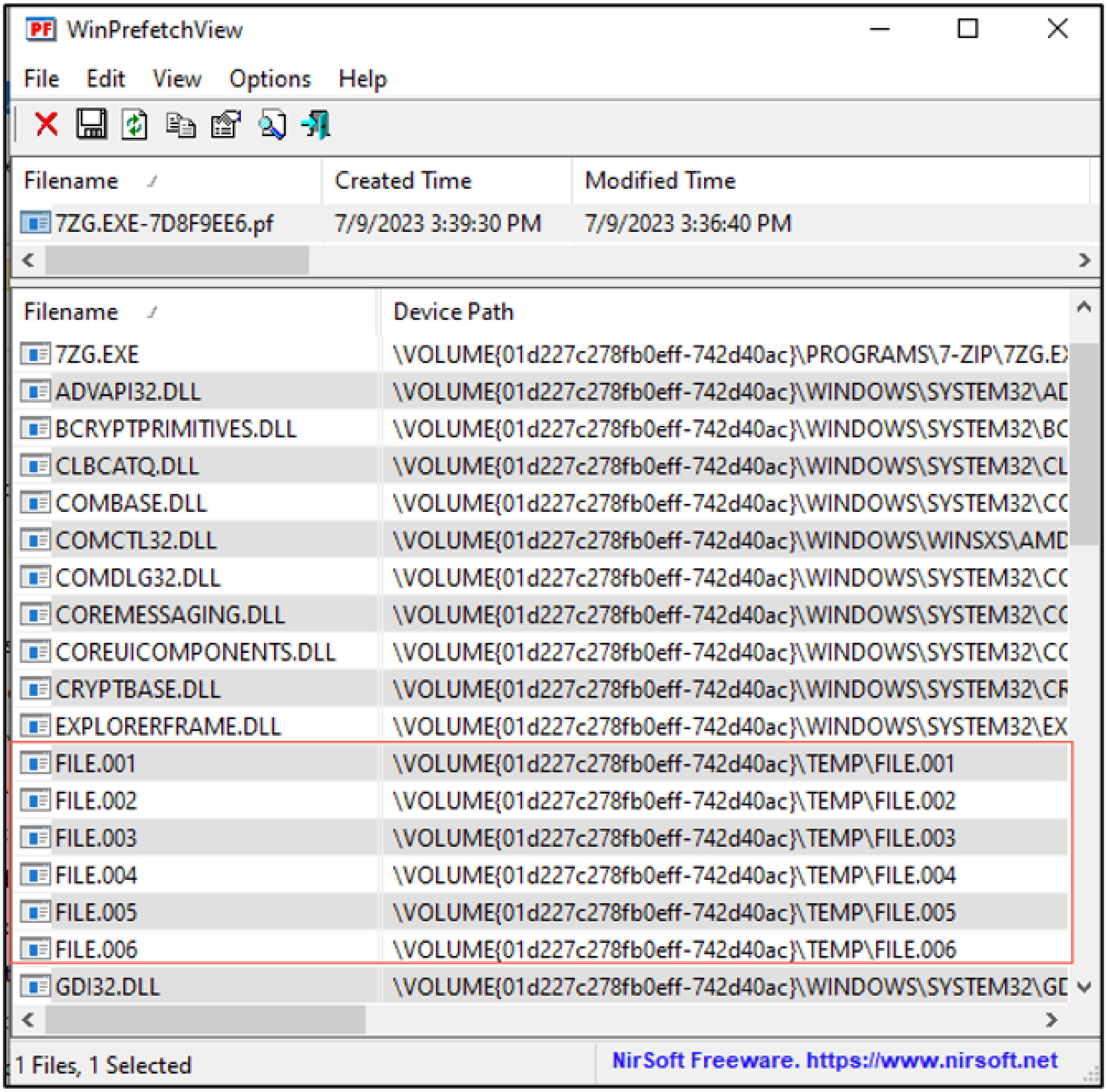


```
Processing c:\Temp\NOTEPAD.EXE-B28CC291.pf

Created on: 2023-07-11 15:16:28
Modified on: 2023-07-11 15:10:07
Last accessed on: 2023-07-11 15:18:52

Executable name: NOTEPAD.EXE
Hash: B28CC291
File size (bytes): 49,184
Version: Windows 10 or Windows 11

Run count: 7
Last run: 2023-07-11 15:09:57
Other run times: 2023-07-07 15:29:16, 2023-07-05 18:46:44, 2023-07-05 17:28:41,
2023-07-05 15:24:47, 2023-06-30 20:45:08, 2023-06-25 19:52:25

Volume information:

#0: Name: \VOLUME{01d73f243c57024a-dc3c8215} Serial: DC3C8215 Created: 2021-05-02
07:24:49 Directories: 29 File references: 106

Directories referenced: 29
 \VOLUME{01d73f243c57024a-dc3c8215}\PROGRAM FILES
 \VOLUME{01d73f243c57024a-dc3c8215}\PROGRAM FILES\AVG
 \VOLUME{01d73f243c57024a-dc3c8215}\PROGRAM FILES\AVG\ANTIVIRUS
 \VOLUME{01d73f243c57024a-dc3c8215}\PROGRAMDATA
 \VOLUME{01d73f243c57024a-dc3c8215}\PROGRAMDATA\MICROSOFT
 \VOLUME{01d73f243c57024a-dc3c8215}\PROGRAMDATA\MICROSOFT\WINDOWS
 \VOLUME{01d73f243c57024a-dc3c8215}\PROGRAMDATA\MICROSOFT\WINDOWS\CACHES
 \VOLUME{01d73f243c57024a-dc3c8215}\USERS
 \VOLUME{01d73f243c57024a-dc3c8215}\USERS\ANALYST
 \VOLUME{01d73f243c57024a-dc3c8215}\USERS\ANALYST\APPDATA
 \VOLUME{01d73f243c57024a-dc3c8215}\USERS\ANALYST\APPDATA\LOCAL
Files referenced: 83
 \VOLUME{01d73f243c57024a-dc3c8215}\WINDOWS\SYSTEM32\NTDLL.DLL
 \VOLUME{01d73f243c57024a-dc3c8215}\WINDOWS\SYSTEM32\NOTEPAD.EXE (Executable:
  True)
 \VOLUME{01d73f243c57024a-dc3c8215}\WINDOWS\SYSTEM32\KERNEL32.DLL
 \VOLUME{01d73f243c57024a-dc3c8215}\PROGRAM FILES\AVG\ANTIVIRUS\ASWHOOK.DLL
 \VOLUME{01d73f243c57024a-dc3c8215}\WINDOWS\SYSTEM32\KERNELBASE.DLL
 \VOLUME{01d73f243c57024a-dc3c8215}\WINDOWS\SYSTEM32\LOCALE.NLS
 \VOLUME{01d73f243c57024a-dc3c8215}\WINDOWS\SYSTEM32\GDI32.DLL
 \VOLUME{01d73f243c57024a-dc3c8215}\WINDOWS\SYSTEM32\WIN32U.DLL
 \VOLUME{01d73f243c57024a-dc3c8215}\WINDOWS\SYSTEM32\GDI32FULL.DLL
 \VOLUME{01d73f243c57024a-dc3c8215}\WINDOWS\SYSTEM32\MSVCP WIN.DLL
```

Figure 2 – Example Prefetch Tool PECmd Output

Note the Prefetch process is not a tracer or monitor program for applications; the data contained within each .pf file is only a snapshot of the executable and the files with which it interacts for the purpose of speeding up loading. As such, the Prefetch process snapshot is created ten (10) seconds after application execution to capture library and file references for subsequent loads. When reviewed, these records can be helpful to investigators in identifying potentially malicious directory paths, binaries, and data files with which an executable might be coded to interact.

In the figure below, a threat actor was attempting to use 7-Zip to compress files before exfiltration. The figure helps to illustrate that the application is interacting with data files named **FILE01, FILE02,** etc. from the **TEMP** directory within the first (10) seconds of execution. This information could be used to determine what kind of data might have been exfiltrated and where the files were on the file system for potential recovery.



Filename	Created Time	Modified Time
7ZG.EXE-7D8F9EE6.pf	7/9/2023 3:39:30 PM	7/9/2023 3:36:40 PM

Filename	Device Path
7ZG.EXE	\VOLUME{01d227c278fb0eff-742d40ac}\PROGRAMS\7-ZIP\7ZG.E
ADVAPI32.DLL	\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSTEM32\AD
BCRYPTPRIMITIVES.DLL	\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSTEM32\BC
CLBCATQ.DLL	\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSTEM32\CL
COMBASE.DLL	\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSTEM32\CC
COMCTL32.DLL	\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\WINSXS\AMD
COMDLG32.DLL	\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSTEM32\CC
COREMESSAGING.DLL	\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSTEM32\CC
COREUICOMPONENTS.DLL	\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSTEM32\CC
CRYPTBASE.DLL	\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSTEM32\CR
EXPLORERFRAME.DLL	\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSTEM32\EX
FILE.001	\VOLUME{01d227c278fb0eff-742d40ac}\TEMP\FILE.001
FILE.002	\VOLUME{01d227c278fb0eff-742d40ac}\TEMP\FILE.002
FILE.003	\VOLUME{01d227c278fb0eff-742d40ac}\TEMP\FILE.003
FILE.004	\VOLUME{01d227c278fb0eff-742d40ac}\TEMP\FILE.004
FILE.005	\VOLUME{01d227c278fb0eff-742d40ac}\TEMP\FILE.005
FILE.006	\VOLUME{01d227c278fb0eff-742d40ac}\TEMP\FILE.006
GDI32.DLL	\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSTEM32\GD

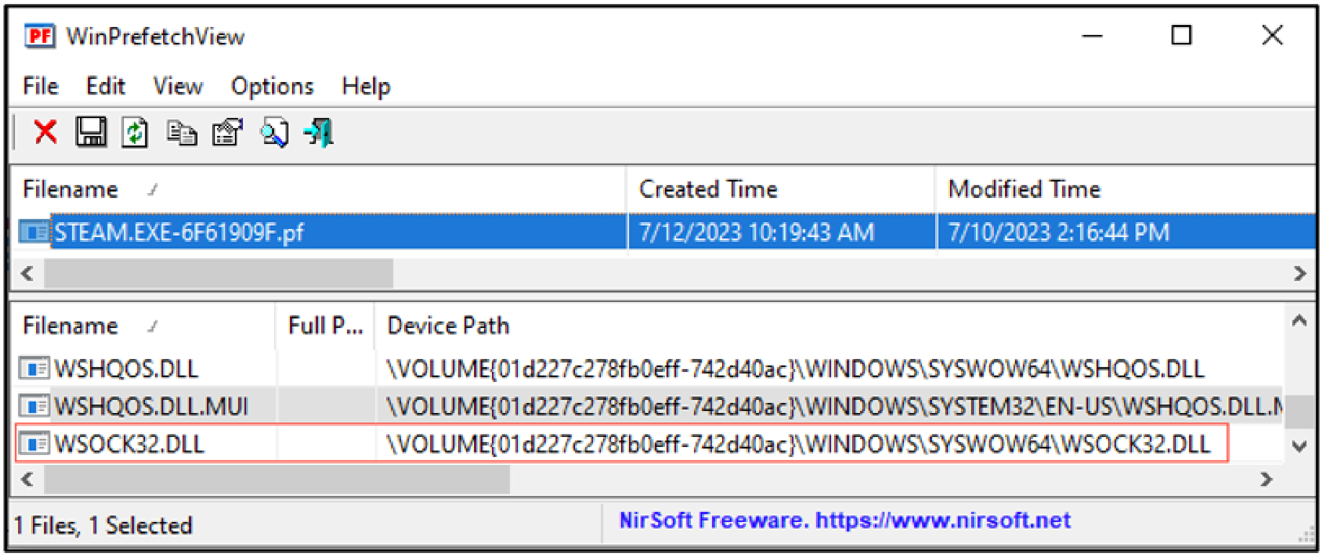
1 Files, 1 Selected

NirSoft Freeware. https://www.nirsoft.net

Figure 3 – Example of File Interaction Captured Within 10 Second Snapshot

Another area where prefetch analysis can be helpful is in malware analysis. As already noted, the prefetch file contains information about the files and directories with which an executable interacts. This can not only identify files that might be downloaded but can also identify other malicious activities, such as accessing files located in unusual locations. This can be particularly helpful when tracing down the file(s) responsible for the malicious activity. Take, for instance, a search order hijacking attack, in which the attacker places a malicious .DLL file in a location where it is loaded before the legitimate file (more details on the attack here: https://malwareandstuff.com/the-dll-search-order-and-hijacking-it/).

To demonstrate how prefetch file analysis can uncover this type of attack, let's look at the following example. The Steam application uses the **WSOCK32.DLL**, finding it on the test machine under C:\Windows\SYSWOW64\, using the systems search order to find it.



Filename	Created Time	Modified Time
STEAM.EXE-6F61909F.pf	7/12/2023 10:19:43 AM	7/10/2023 2:16:44 PM

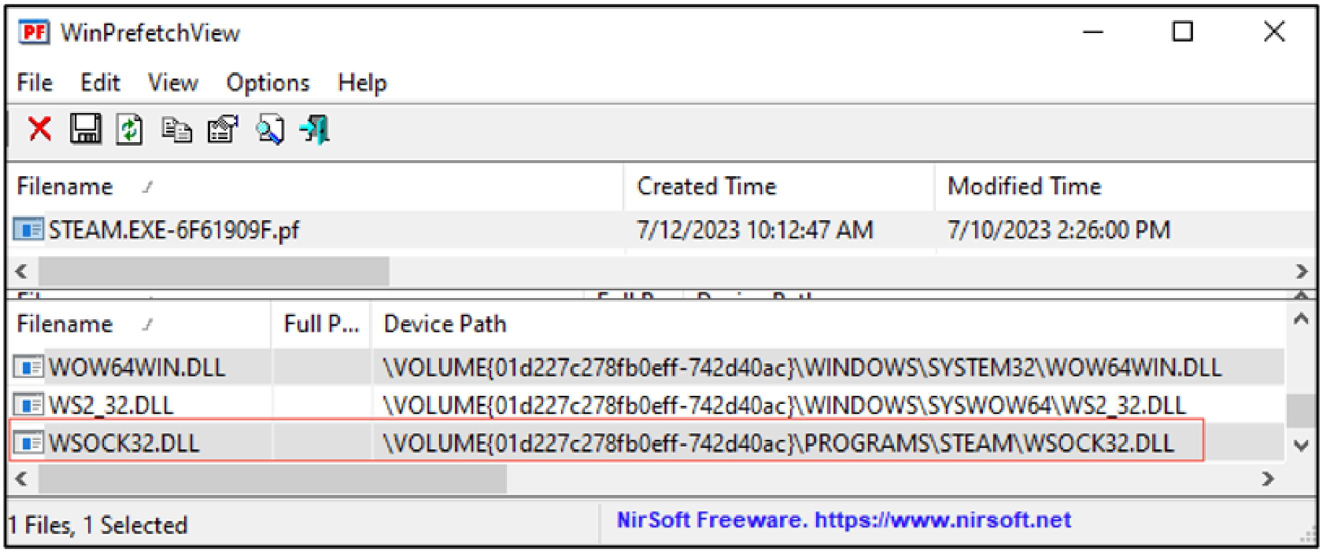
Filename	Full P...	Device Path
WSHQOS.DLL		\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSWOW64\WSHQOS.DLL
WSHQOS.DLL.MUI		\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSTEM32\EN-US\WSHQOS.DLL.M
WSOCK32.DLL		\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSWOW64\WSOCK32.DLL

1 Files, 1 Selected

NirSoft Freeware. https://www.nirsoft.net

Figure 4 – Steam Using WSOCK32.DLL from SYSWOW64

Noting this, the attacker knows that the default search order will look in the directory where the application is launched first. The attacker places their version of the DLL higher in the search order path, to be executed before the real DLL. The figure below shows the malicious DLL being executed from the application directory, which is searched before the system directories, thus compromising the system.



Filename	Created Time	Modified Time
STEAM.EXE-6F61909F.pf	7/12/2023 10:12:47 AM	7/10/2023 2:26:00 PM

Filename	Full P...	Device Path
WOW64WIN.DLL		\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSTEM32\WOW64WIN.DLL
WS2_32.DLL		\VOLUME{01d227c278fb0eff-742d40ac}\WINDOWS\SYSWOW64\WS2_32.DLL
WSOCK32.DLL		\VOLUME{01d227c278fb0eff-742d40ac}\PROGRAMS\STEAM\WSOCK32.DLL

1 Files, 1 Selected

NirSoft Freeware. https://www.nirsoft.net

Figure 5 – Steam Using Malicious WSOCK32.DLL Using Search Order

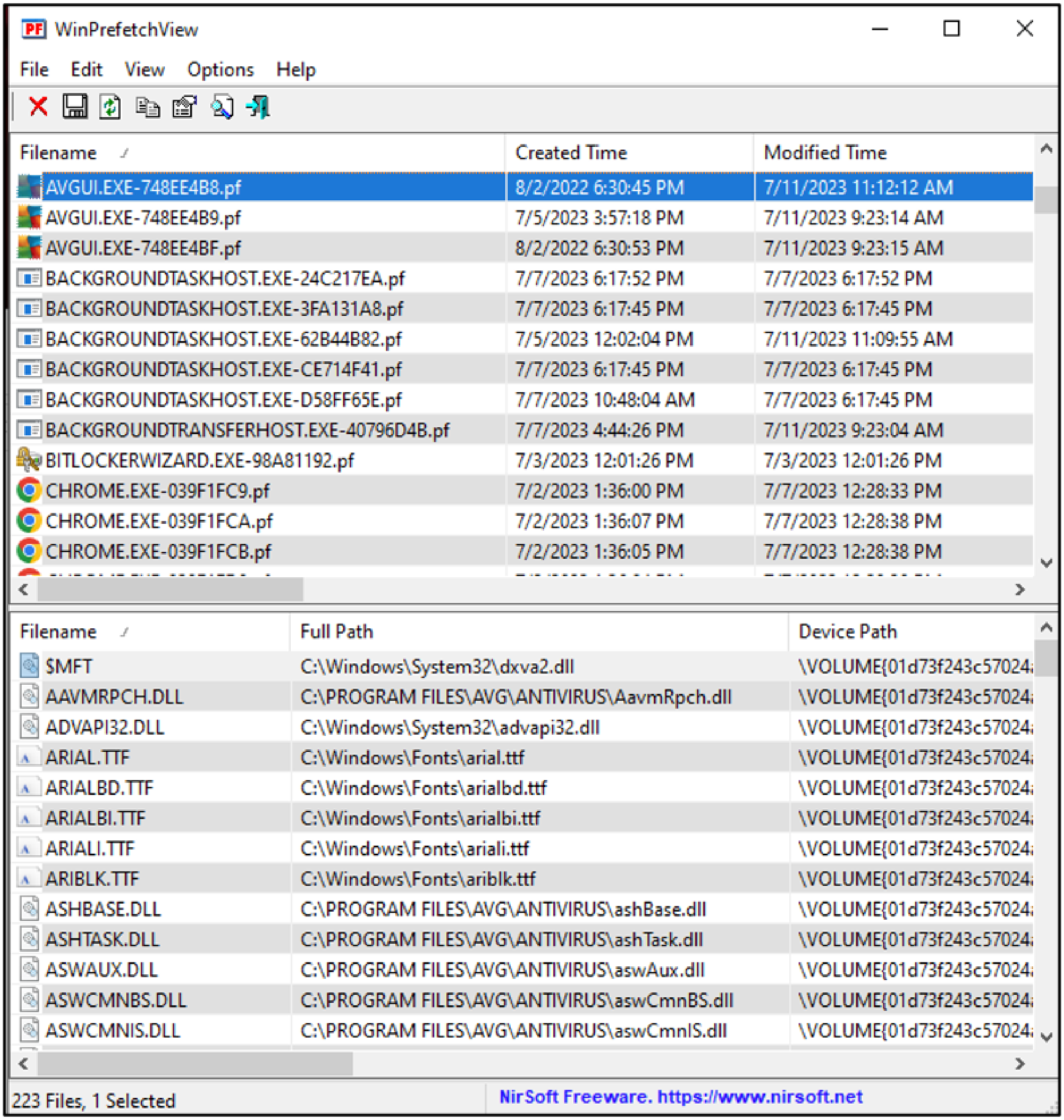
Prefetch analysis is one (1) of the few ways that security analysts can gain understanding of application interactions in the absence of more robust EDR tools that map out process flows.

Prefetch Analysis Tools

There are several tools available for reviewing the contents of prefetch files, including Eric Zimmerman's PECmd command line tool and NirSoft's WinPrefetchView.

PECmd is used for opening and reviewing the contents of .pf files. It supports several functions, including processing a single file or a directory of prefetch files. It can also output the .pf file information in a number of formats, including JSON, CSV, and HTML, as well as standard out. Zimmerman's tool can be downloaded from GitHub at https://github.com/EricZimmerman/PECmd.

Like PECmd, WinPrefetchView can open and review the individual contents of a .pf or pull in an entire prefetch directory.



Filename	Created Time	Modified Time
AVGUI.EXE-748EE4B8.pf	8/2/2022 6:30:45 PM	7/11/2023 11:12:12 AM
AVGUI.EXE-748EE4B9.pf	7/5/2023 3:57:18 PM	7/11/2023 9:23:14 AM
AVGUI.EXE-748EE4BF.pf	8/2/2022 6:30:53 PM	7/11/2023 9:23:15 AM
BACKGROUNDTASKHOST.EXE-24C217EA.pf	7/7/2023 6:17:52 PM	7/7/2023 6:17:52 PM
BACKGROUNDTASKHOST.EXE-3FA131A8.pf	7/7/2023 6:17:45 PM	7/7/2023 6:17:45 PM
BACKGROUNDTASKHOST.EXE-62B44B82.pf	7/5/2023 12:02:04 PM	7/11/2023 11:09:55 AM
BACKGROUNDTASKHOST.EXE-CE714F41.pf	7/7/2023 6:17:45 PM	7/7/2023 6:17:45 PM
BACKGROUNDTASKHOST.EXE-D58FF65E.pf	7/7/2023 10:48:04 AM	7/7/2023 6:17:45 PM
BACKGROUNDTRANSFERHOST.EXE-40796D4B.pf	7/7/2023 4:44:26 PM	7/11/2023 9:23:04 AM
BITLOCKERWIZARD.EXE-98A81192.pf	7/3/2023 12:01:26 PM	7/3/2023 12:01:26 PM
CHROME.EXE-039F1FC9.pf	7/2/2023 1:36:00 PM	7/7/2023 12:28:33 PM
CHROME.EXE-039F1FCA.pf	7/2/2023 1:36:07 PM	7/7/2023 12:28:38 PM
CHROME.EXE-039F1FCB.pf	7/2/2023 1:36:05 PM	7/7/2023 12:28:38 PM

Filename	Full Path	Device Path
$MFT	C:\Windows\System32\dxva2.dll	\VOLUME{01d73f243c57024
AAVMRPCH.DLL	C:\PROGRAM FILES\AVG\ANTIVIRUS\AavmRpch.dll	\VOLUME{01d73f243c57024
ADVAPI32.DLL	C:\Windows\System32\advapi32.dll	\VOLUME{01d73f243c57024
ARIAL.TTF	C:\Windows\Fonts\arial.ttf	\VOLUME{01d73f243c57024
ARIALBD.TTF	C:\Windows\Fonts\arialbd.ttf	\VOLUME{01d73f243c57024
ARIALBI.TTF	C:\Windows\Fonts\arialbi.ttf	\VOLUME{01d73f243c57024
ARIALI.TTF	C:\Windows\Fonts\ariali.ttf	\VOLUME{01d73f243c57024
ARIBLK.TTF	C:\Windows\Fonts\ariblk.ttf	\VOLUME{01d73f243c57024
ASHBASE.DLL	C:\PROGRAM FILES\AVG\ANTIVIRUS\ashBase.dll	\VOLUME{01d73f243c57024
ASHTASK.DLL	C:\PROGRAM FILES\AVG\ANTIVIRUS\ashTask.dll	\VOLUME{01d73f243c57024
ASWAUX.DLL	C:\PROGRAM FILES\AVG\ANTIVIRUS\aswAux.dll	\VOLUME{01d73f243c57024
ASWCMNBS.DLL	C:\PROGRAM FILES\AVG\ANTIVIRUS\aswCmnBS.dll	\VOLUME{01d73f243c57024
ASWCMNIS.DLL	C:\PROGRAM FILES\AVG\ANTIVIRUS\aswCmnIS.dll	\VOLUME{01d73f243c57024

223 Files, 1 Selected

NirSoft Freeware. https://www.nirsoft.net

Figure 6 – WinPrefetchView from NirSoft

WinPrefetchView allows for the quick location and review of specific .pf files. However, it is limited in its report export functions allowing only HTML output. WinPrefetchView can be downloaded at https://www.nirsoft.net/utils/win_prefetch_view.html.

In closing, prefetch files are little snitches spilling their contents, providing information that may not otherwise be available in an investigation. Additionally, information derived from files can provide critical information that management, legal, and cyber insurance might need, such as what files were accessed, when they were accessed, and what kind of information might be in those files, laying the groundwork for communications, disclosure, and exposure. Lastly, analysts can use the information derived from prefetch data to corroborate and validate other forensic artifact data, further solidifying the timeline of events.

References

- https://isc.sans.edu/diary/rss/29168
- https://www.forensicfocus.com/articles/hunting-for-attackers-tactics-and-techniques-with-prefetch-files/
- https://or10nlabs.tech/prefetch-forensics/

DM questions or comments: @H3xxEdit