Forensic Investigation : Prefetch File

October 15, 2020   By Raj Chandel

In this article, we are going to study an important artifact of Windows, i.e. prefetch files. Every time you do anything on your Windows system, a file is created. These files are called Prefetch files. Through this article, we will learn how these are important and why do we need them.

Table of Content

Introduction

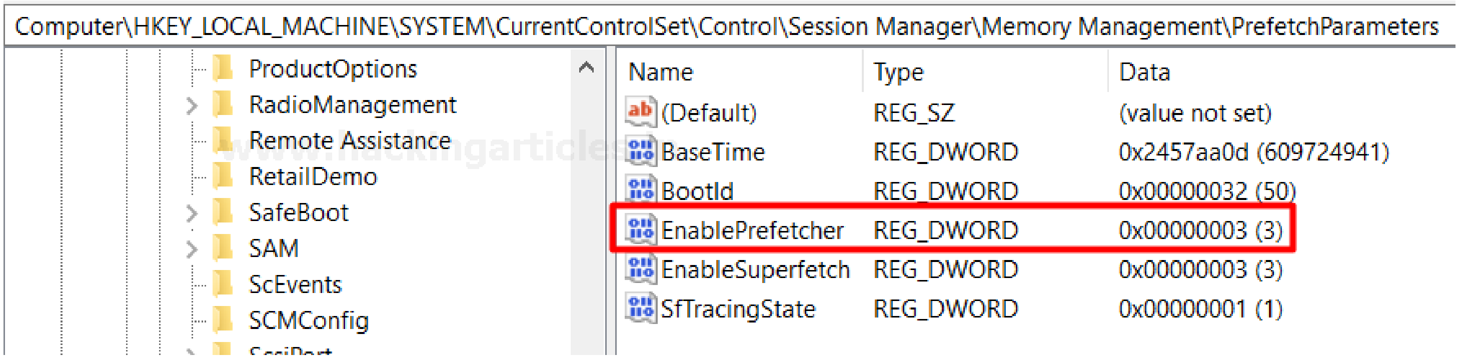
A Prefetch file is a file created when you open an application on your windows system. Windows makes a prefetch record when an application is run from a specific area for the absolute first time.

Prefetch files were introduced in Windows XP. Prefetch files are intended to accelerate the Windows boot process and applications' start-up process. In Windows XP, Vista, and 7 the number of prefetch files is limited to 128 whereas in Windows 8 and above it is up to 1024.

Proof of program execution can be a significant asset for a forensic investigator, they can prove that a certain executable was executed on the system to cover up the tracks. Before initiating the forensic analysis of the prefetch record as a forensic examiner you should check whether the prefetching process is enabled.

To check the status of prefetching, open the following location in Registry editor:

```
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memor
```



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

Name	Type	Data
(Default)	REG_SZ	(value not set)
BaseTime	REG_DWORD	0x2457aa0d (609724941)
BootId	REG_DWORD	0x00000032 (50)
EnablePrefetcher	REG_DWORD	0x00000003 (3)
EnableSuperfetch	REG_DWORD	0x00000003 (3)
SfTracingState	REG_DWORD	0x00000001 (1)

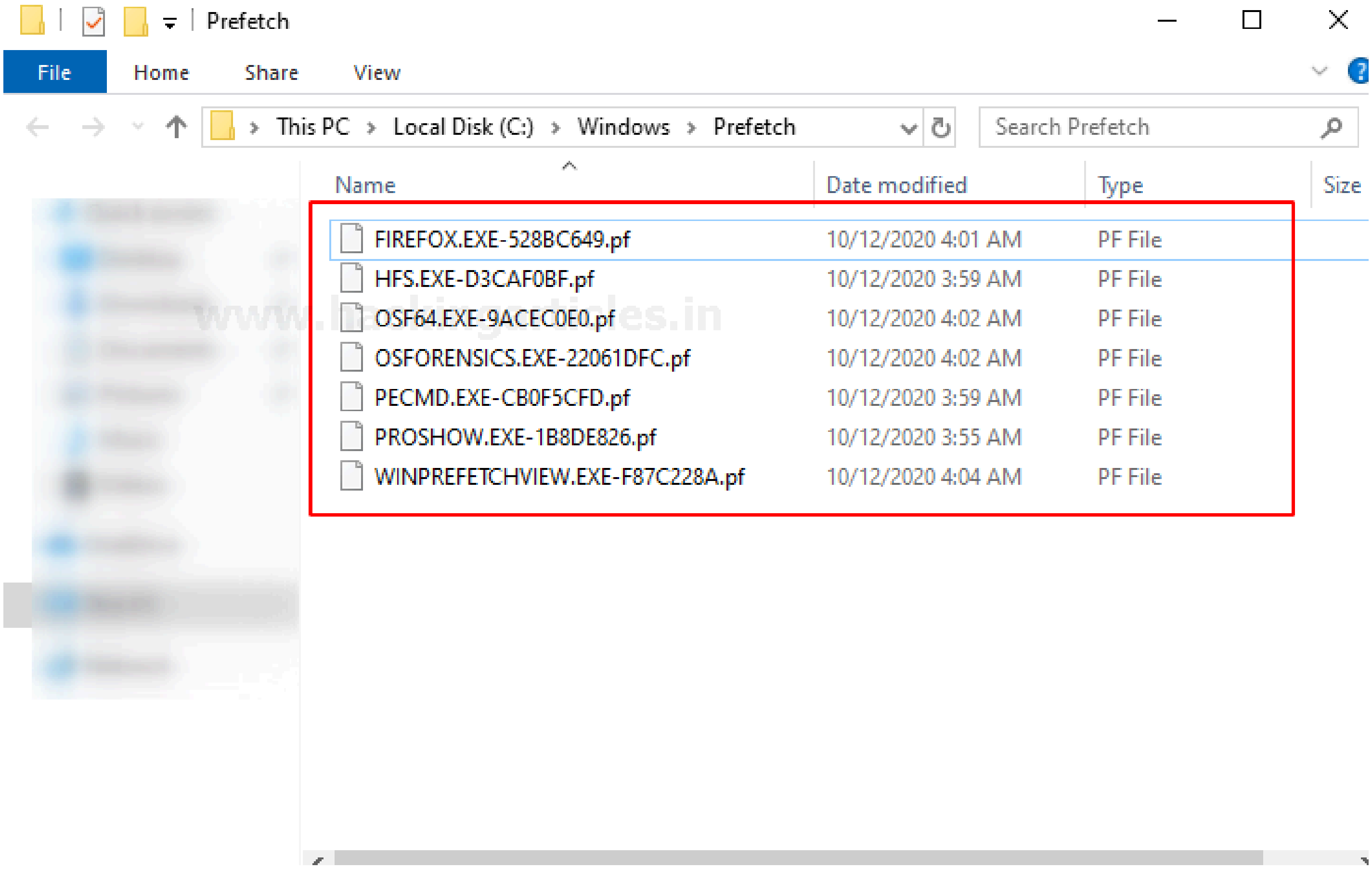
The value is set as 3 by default as shown in the image above. The following values can be changed according to your prefetching needs. All the options that windows provide us with in order to customize prefetching are explained below:

- 0:Prefetching Disabled
- 1:Application Prefetching Enabled
- 2: Boot Prefetching Enabled
- 3:Application and Boot both Enabled

The metadata that can be found in a single prefetch file is as following:

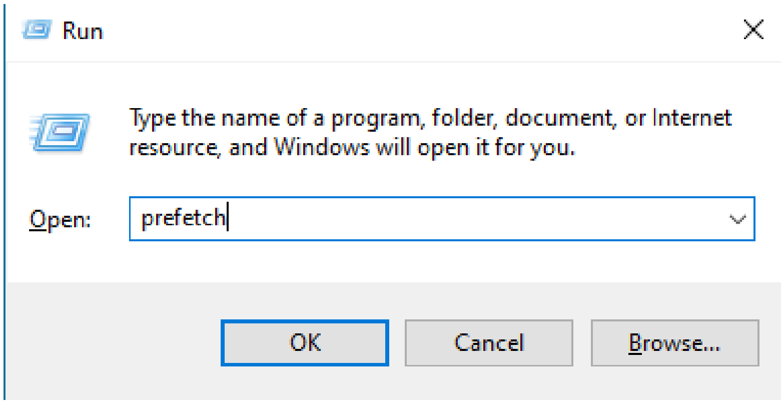
- Executable's name
- Eight character hash of the executable path.
- The path of the executable file
- Creation, modified, and accessed timestamp of executable
- Run count (Number of time the application has been executed)
- Last run time
- The timestamp for the last 8 run time (1 last run time and other 7 other last run times)
- Volume information
- File Referenced by the executable
- Directories referenced by the executable

The prefetch files are saved under %SystemRoot%\Prefetch (C:\Windows\Prefetch).



Name	Date modified	Type	Size
FIREFOX.EXE-528BC649.pf	10/12/2020 4:01 AM	PF File	
HFS.EXE-D3CAF0BF.pf	10/12/2020 3:59 AM	PF File	
OSF64.EXE-9ACEC0E0.pf	10/12/2020 4:02 AM	PF File	
OSFORENSICS.EXE-22061DFC.pf	10/12/2020 4:02 AM	PF File	
PECMD.EXE-CB0F5CFD.pf	10/12/2020 3:59 AM	PF File	
PROSHOW.EXE-1B8DE826.pf	10/12/2020 3:55 AM	PF File	
WINPREFETCHVIEW.EXE-F87C228A.pf	10/12/2020 4:04 AM	PF File	

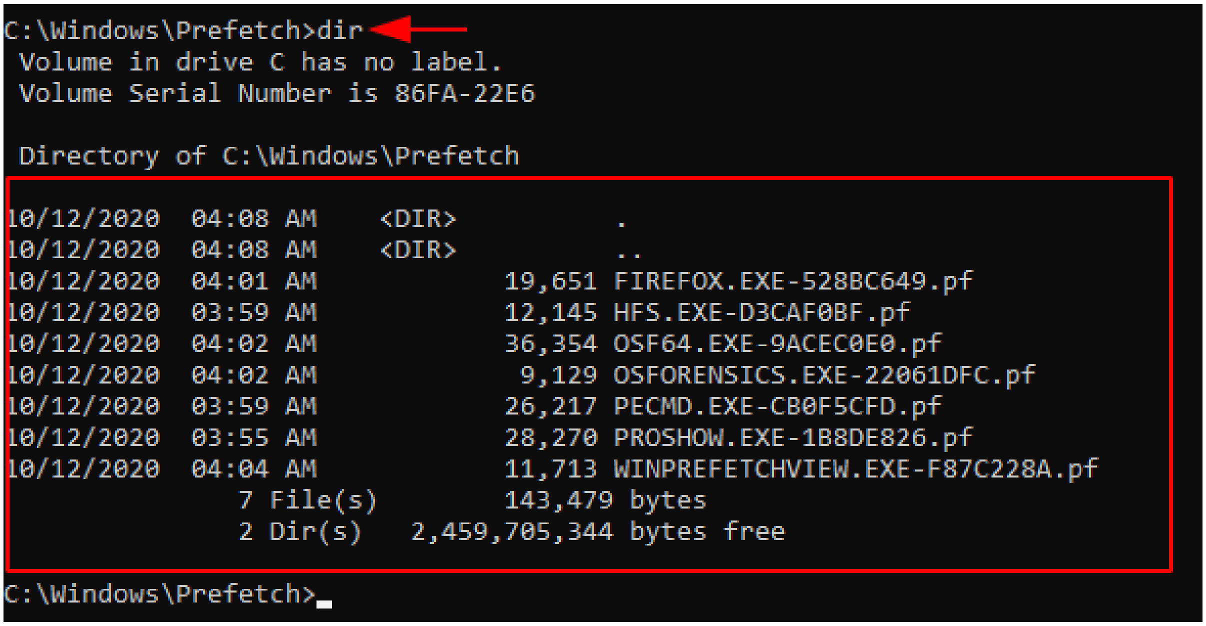
You can open the prefetch files location you can directly search for “prefetch “in the run command.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: prefetch

It can also be opened as a directory from the command prompt, which is a good news for all the command-line lovers.



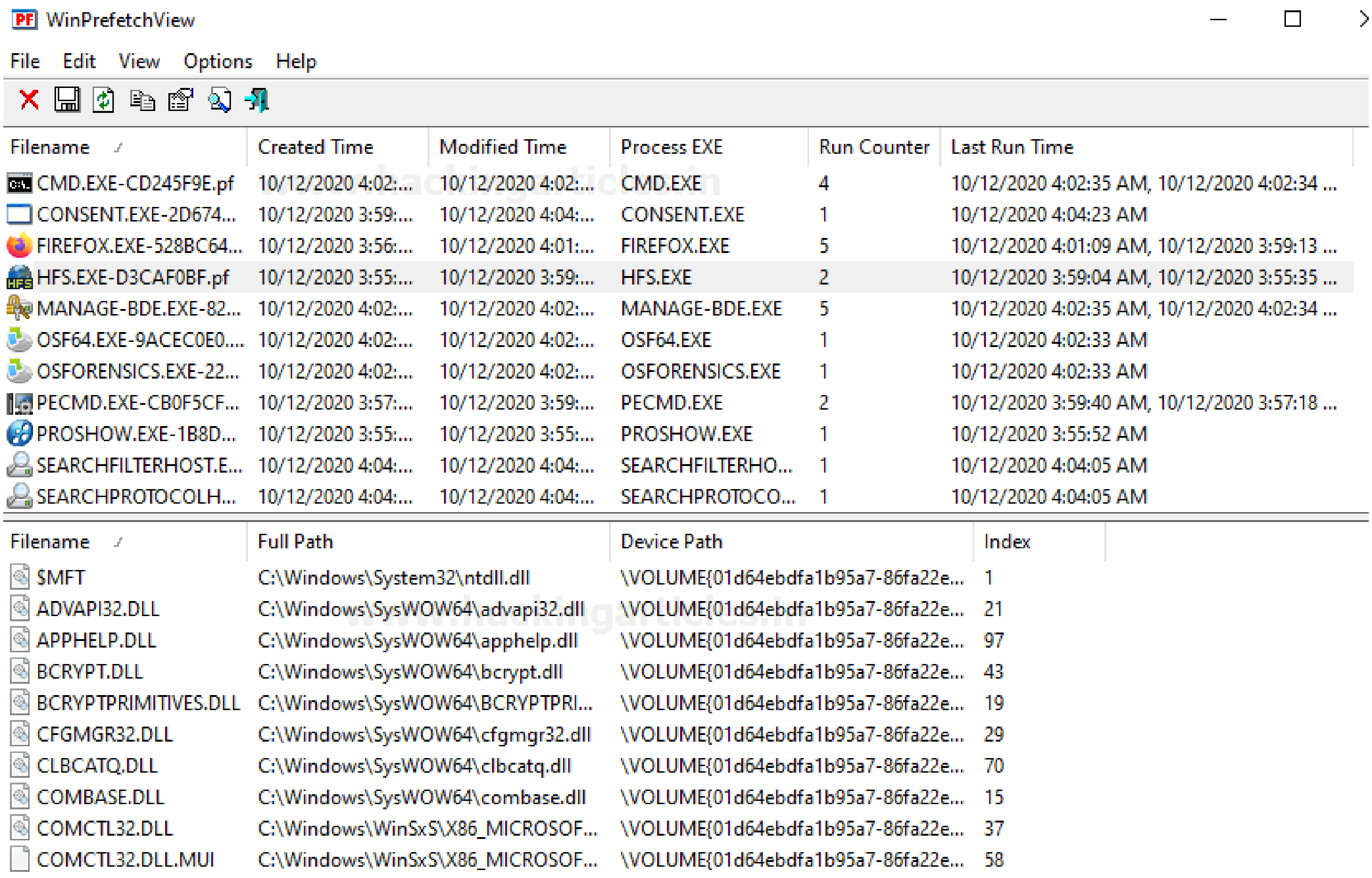
```
C:\Windows\Prefetch>dir
 Volume in drive C has no label.
 Volume Serial Number is 86FA-22E6

 Directory of C:\Windows\Prefetch

10/12/2020  04:08 AM    <DIR>          .
10/12/2020  04:08 AM    <DIR>          ..
10/12/2020  04:01 AM            19,651 FIREFOX.EXE-528BC649.pf
10/12/2020  03:59 AM            12,145 HFS.EXE-D3CAF0BF.pf
10/12/2020  04:02 AM            36,354 OSF64.EXE-9ACEC0E0.pf
10/12/2020  04:02 AM             9,129 OSFORENSICS.EXE-22061DFC.pf
10/12/2020  03:59 AM            26,217 PECMD.EXE-CB0F5CFD.pf
10/12/2020  03:55 AM            28,270 PROSHOW.EXE-1B8DE826.pf
10/12/2020  04:04 AM            11,713 WINPREFETCHVIEW.EXE-F87C228A.pf
               7 File(s)        143,479 bytes
               2 Dir(s)   2,459,705,344 bytes free

C:\Windows\Prefetch>_
```

Forensic Analysis of Prefetch Files

WinPrefetch View

WinPrefetch View is a tool to read and examine the prefetch files stored in your system. The tool was developed by **Nirsoft**. This utility deals with any variant of Windows, beginning from Windows XP to Windows 10.

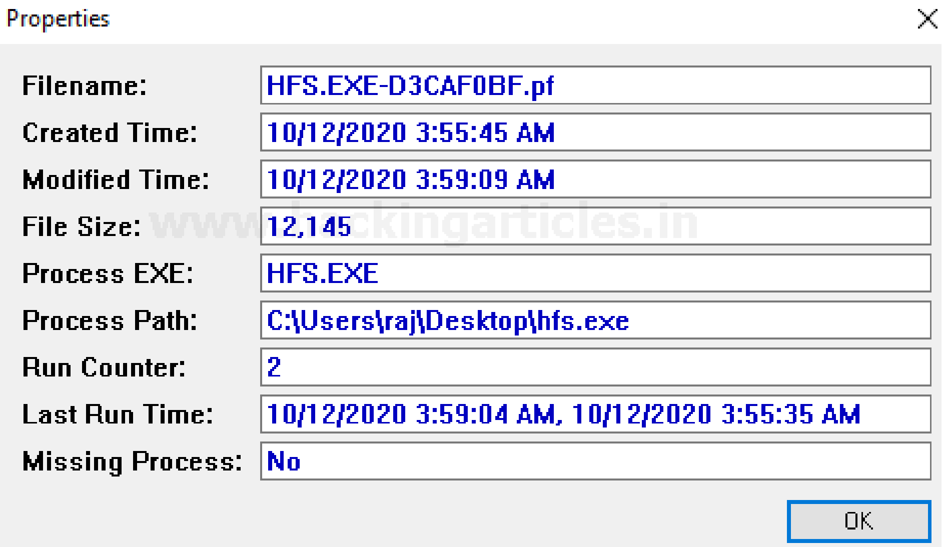
You can download the tool from **here**.



Filename	Created Time	Modified Time	Process EXE	Run Counter	Last Run Time
CMD.EXE-CD245F9E.pf	10/12/2020 4:02:...	10/12/2020 4:02:...	CMD.EXE	4	10/12/2020 4:02:35 AM, 10/12/2020 4:02:34 ...
CONSENT.EXE-2D674...	10/12/2020 3:59:...	10/12/2020 4:04:...	CONSENT.EXE	1	10/12/2020 4:04:23 AM
FIREFOX.EXE-528BC64...	10/12/2020 3:56:...	10/12/2020 4:01:...	FIREFOX.EXE	5	10/12/2020 4:01:09 AM, 10/12/2020 3:59:13 ...
HFS.EXE-D3CAF0BF.pf	10/12/2020 3:55:...	10/12/2020 3:59:...	HFS.EXE	2	10/12/2020 3:59:04 AM, 10/12/2020 3:55:35 ...
MANAGE-BDE.EXE-82...	10/12/2020 4:02:...	10/12/2020 4:02:...	MANAGE-BDE.EXE	5	10/12/2020 4:02:35 AM, 10/12/2020 4:02:34 ...
OSF64.EXE-9ACEC0E0....	10/12/2020 4:02:...	10/12/2020 4:02:...	OSF64.EXE	1	10/12/2020 4:02:33 AM
OSFORENSICS.EXE-22...	10/12/2020 4:02:...	10/12/2020 4:02:...	OSFORENSICS.EXE	1	10/12/2020 4:02:33 AM
PECMD.EXE-CB0F5CF...	10/12/2020 3:57:...	10/12/2020 3:59:...	PECMD.EXE	2	10/12/2020 3:59:40 AM, 10/12/2020 3:57:18 ...
PROSHOW.EXE-1B8D...	10/12/2020 3:55:...	10/12/2020 3:55:...	PROSHOW.EXE	1	10/12/2020 3:55:52 AM
SEARCHFILTERHOST.E...	10/12/2020 4:04:...	10/12/2020 4:04:...	SEARCHFILTERHO...	1	10/12/2020 4:04:05 AM
SEARCHPROTOCOLH...	10/12/2020 4:04:...	10/12/2020 4:04:...	SEARCHPROTOCO...	1	10/12/2020 4:04:05 AM

Filename	Full Path	Device Path	Index
$MFT	C:\Windows\System32\ntdll.dll	\VOLUME{01d64ebdfa1b95a7-86fa22e...	1
ADVAPI32.DLL	C:\Windows\SysWOW64\advapi32.dll	\VOLUME{01d64ebdfa1b95a7-86fa22e...	21
APPHELP.DLL	C:\Windows\SysWOW64\apphelp.dll	\VOLUME{01d64ebdfa1b95a7-86fa22e...	97
BCRYPT.DLL	C:\Windows\SysWOW64\bcrypt.dll	\VOLUME{01d64ebdfa1b95a7-86fa22e...	43
BCRYPTPRIMITIVES.DLL	C:\Windows\SysWOW64\BCRYPTPRI...	\VOLUME{01d64ebdfa1b95a7-86fa22e...	19
CFGMGR32.DLL	C:\Windows\SysWOW64\cfgmgr32.dll	\VOLUME{01d64ebdfa1b95a7-86fa22e...	29
CLBCATQ.DLL	C:\Windows\SysWOW64\clbcatq.dll	\VOLUME{01d64ebdfa1b95a7-86fa22e...	70
COMBASE.DLL	C:\Windows\SysWOW64\combase.dll	\VOLUME{01d64ebdfa1b95a7-86fa22e...	15
COMCTL32.DLL	C:\Windows\WinSxS\X86_MICROSOF...	\VOLUME{01d64ebdfa1b95a7-86fa22e...	37
COMCTL32.DLL.MUI	C:\Windows\WinSxS\X86_MICROSOF...	\VOLUME{01d64ebdfa1b95a7-86fa22e...	58

You can easily open the details of a particular prefetch file by simply clicking on it. Here, I have opened HFS.EXE-D3CAF0BF.pf for a detailed view. It shows details such as created time, modified time, file size, the path of process run count, last run time, missing process.

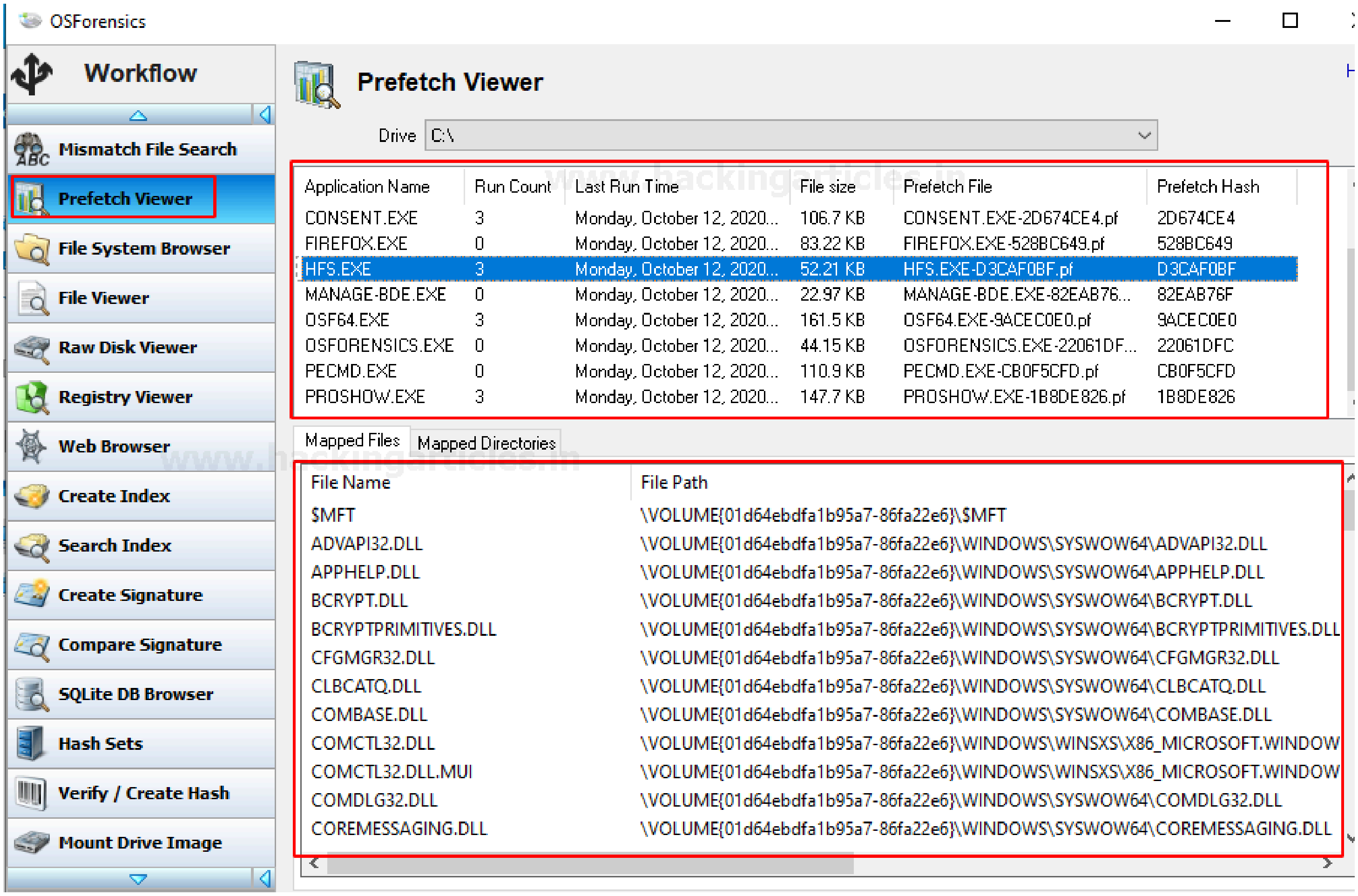


Filename:	HFS.EXE-D3CAF0BF.pf
Created Time:	10/12/2020 3:55:45 AM
Modified Time:	10/12/2020 3:59:09 AM
File Size:	12,145
Process EXE:	HFS.EXE
Process Path:	C:\Users\raj\Desktop\hfs.exe
Run Counter:	2
Last Run Time:	10/12/2020 3:59:04 AM, 10/12/2020 3:55:35 AM
Missing Process:	No

OS Forensics

OS Forensic is a digital forensic tool, a complete package for forensic investigation by Passmark software. It is used to extract, analyze data, search files, recover deleted passwords, and recover deleted evidence, much more.

Download the tool from **here**.



Application Name	Run Count	Last Run Time	File size	Prefetch File	Prefetch Hash
CONSENT.EXE	3	Monday, October 12, 2020...	106.7 KB	CONSENT.EXE-2D674CE4.pf	2D674CE4
FIREFOX.EXE	0	Monday, October 12, 2020...	83.22 KB	FIREFOX.EXE-528BC649.pf	528BC649
HFS.EXE	3	Monday, October 12, 2020...	52.21 KB	HFS.EXE-D3CAF0BF.pf	D3CAF0BF
MANAGE-BDE.EXE	0	Monday, October 12, 2020...	22.97 KB	MANAGE-BDE.EXE-82EAB76...	82EAB76F
OSF64.EXE	3	Monday, October 12, 2020...	161.5 KB	OSF64.EXE-9ACEC0E0.pf	9ACEC0E0
OSFORENSICS.EXE	0	Monday, October 12, 2020...	44.15 KB	OSFORENSICS.EXE-22061DF...	22061DFC
PECMD.EXE	0	Monday, October 12, 2020...	110.9 KB	PECMD.EXE-CB0F5CFD.pf	CB0F5CFD
PROSHOW.EXE	3	Monday, October 12, 2020...	147.7 KB	PROSHOW.EXE-1B8DE826.pf	1B8DE826

File Name	File Path
$MFT	\VOLUME{01d64ebdfa1b95a7-86fa22e6}\$MFT
ADVAPI32.DLL	\VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\ADVAPI32.DLL
APPHELP.DLL	\VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\APPHELP.DLL
BCRYPT.DLL	\VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\BCRYPT.DLL
BCRYPTPRIMITIVES.DLL	\VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\BCRYPTPRIMITIVES.DLL
CFGMGR32.DLL	\VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\CFGMGR32.DLL
CLBCATQ.DLL	\VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\CLBCATQ.DLL
COMBASE.DLL	\VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\COMBASE.DLL
COMCTL32.DLL	\VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\WINSXS\X86_MICROSOFT.WINDOW
COMCTL32.DLL.MUI	\VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\WINSXS\X86_MICROSOFT.WINDOW
COMDLG32.DLL	\VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\COMDLG32.DLL
COREMESSAGING.DLL	\VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\COREMESSAGING.DLL

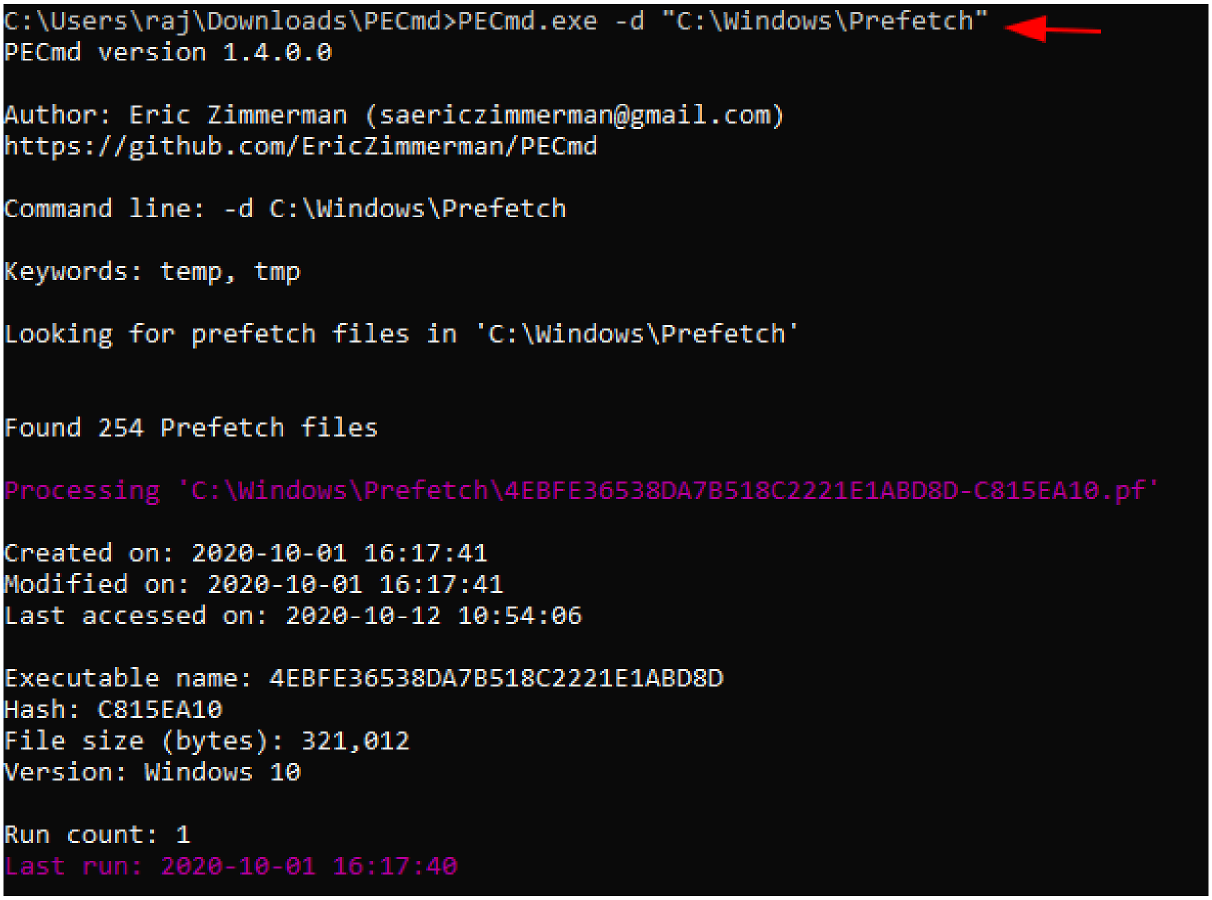
Prefetch Explorer Command Line (PECmd)

PECmd is a command-line tool by Eric Zimmerman, used for bulk analysis of prefetch files.This tool can also export your prefetch artifacts to **.csv** and **.css**.

You can download the tool from **here**.

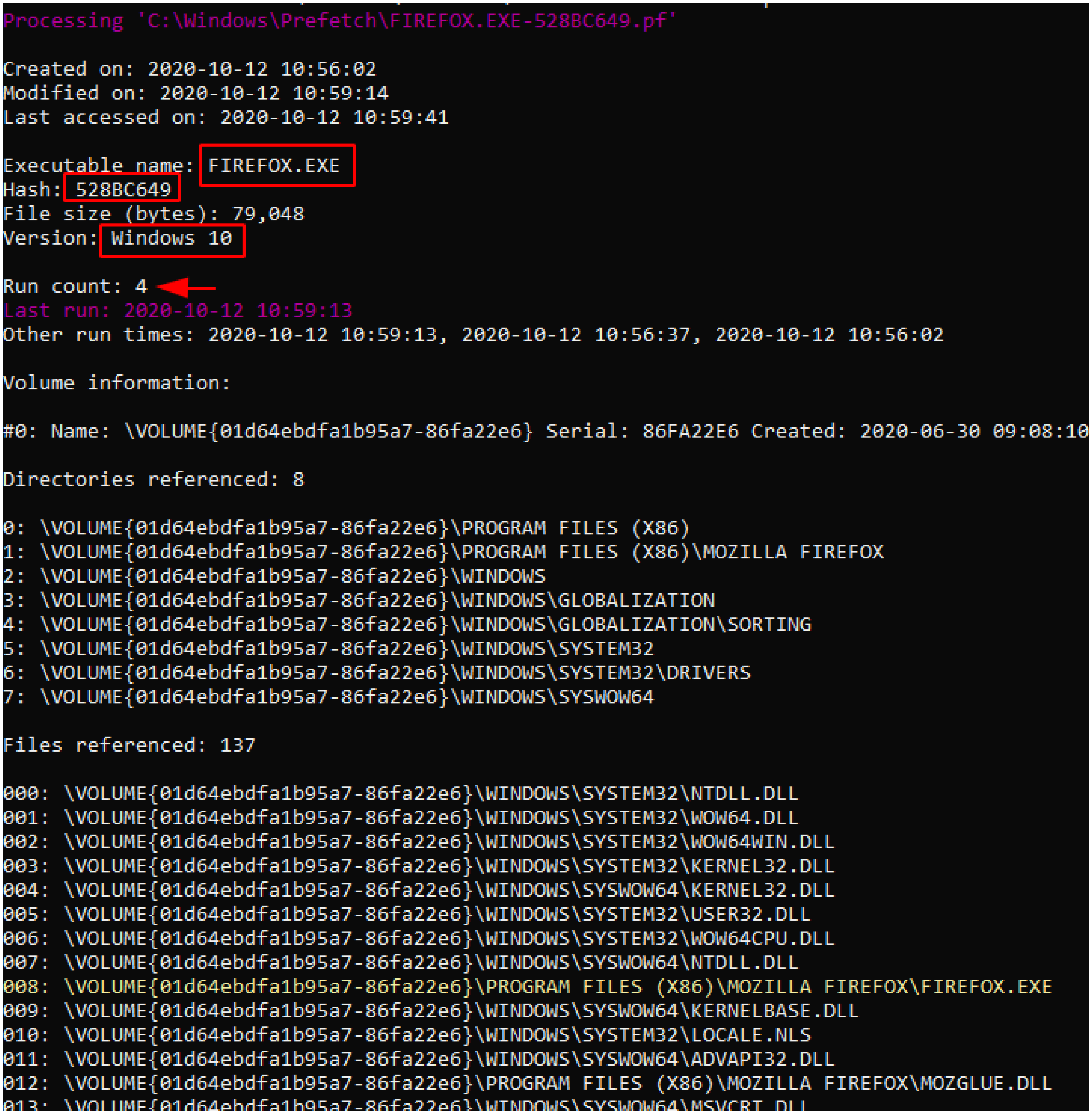
To begin with run the executable file. Let’s parse the prefetch file using this tool we will use the –d parameter to parse all the prefetch file.

```
PECmd.exe -d "C:\Windows\Prefetch"
```



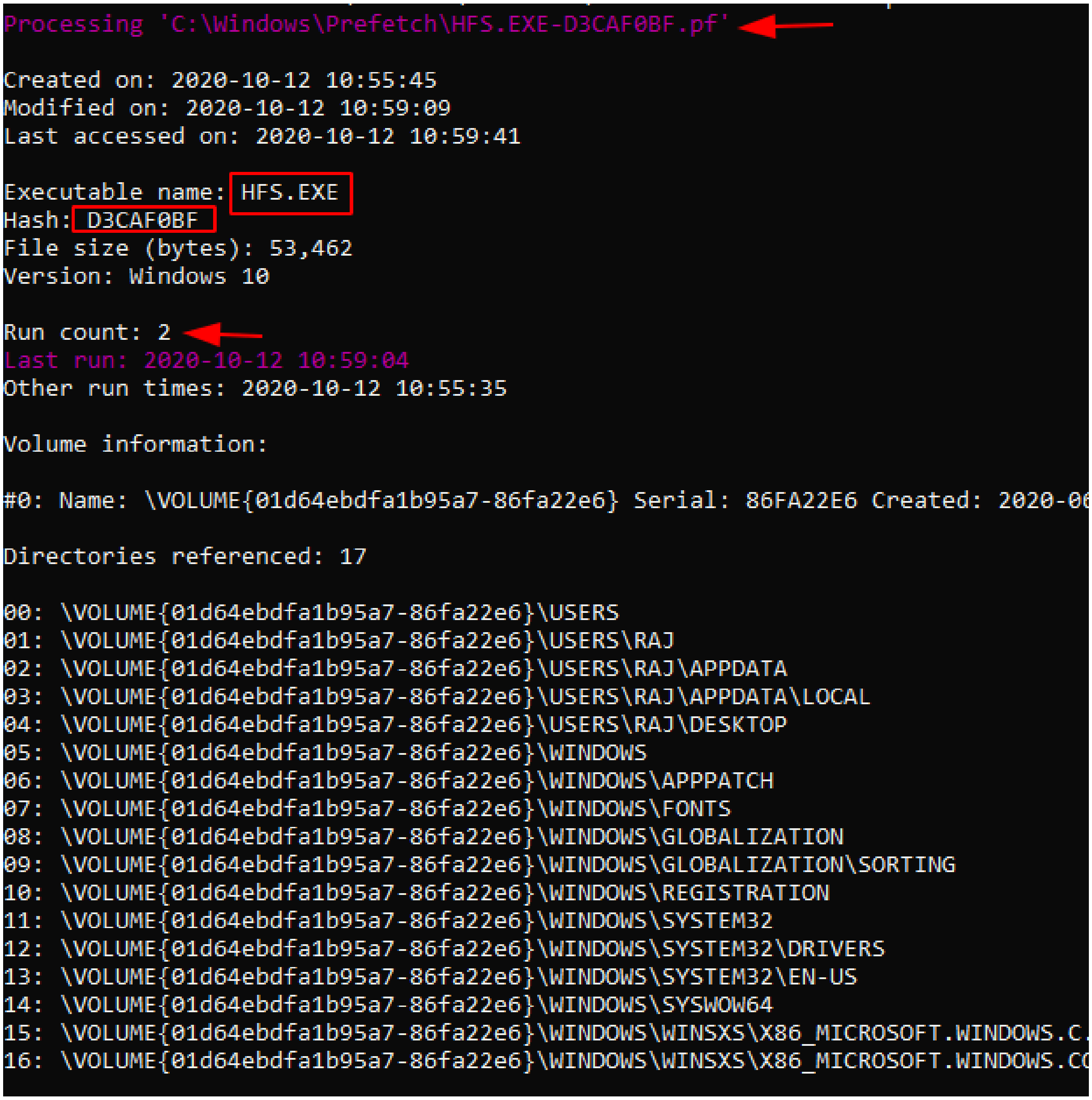
```
C:\Users\raj\Downloads\PECmd>PECmd.exe -d "C:\Windows\Prefetch"
PECmd version 1.4.0.0

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

Command line: -d C:\Windows\Prefetch

Keywords: temp, tmp

Looking for prefetch files in 'C:\Windows\Prefetch'


Found 254 Prefetch files

Processing 'C:\Windows\Prefetch\4EBFE36538DA7B518C2221E1ABD8D-C815EA10.pf'

Created on: 2020-10-01 16:17:41
Modified on: 2020-10-01 16:17:41
Last accessed on: 2020-10-12 10:54:06

Executable name: 4EBFE36538DA7B518C2221E1ABD8D
Hash: C815EA10
File size (bytes): 321,012
Version: Windows 10

Run count: 1
Last run: 2020-10-01 16:17:40
```

In the image below, you can see the prefetch file for firefox.exe.The tool has parsed all the metadata as it has been explained in the introduction.



```
Processing 'C:\Windows\Prefetch\FIREFOX.EXE-528BC649.pf'

Created on: 2020-10-12 10:56:02
Modified on: 2020-10-12 10:59:14
Last accessed on: 2020-10-12 10:59:41

Executable name: FIREFOX.EXE
Hash: 528BC649
File size (bytes): 79,048
Version: Windows 10

Run count: 4
Last run: 2020-10-12 10:59:13
Other run times: 2020-10-12 10:59:13, 2020-10-12 10:56:37, 2020-10-12 10:56:02

Volume information:

#0: Name: \VOLUME{01d64ebdfa1b95a7-86fa22e6} Serial: 86FA22E6 Created: 2020-06-30 09:08:10

Directories referenced: 8

0: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\PROGRAM FILES (X86)
1: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\PROGRAM FILES (X86)\MOZILLA FIREFOX
2: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS
3: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\GLOBALIZATION
4: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\GLOBALIZATION\SORTING
5: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSTEM32
6: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSTEM32\DRIVERS
7: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64

Files referenced: 137

000: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSTEM32\NTDLL.DLL
001: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSTEM32\WOW64.DLL
002: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSTEM32\WOW64WIN.DLL
003: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSTEM32\KERNEL32.DLL
004: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\KERNEL32.DLL
005: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSTEM32\USER32.DLL
006: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSTEM32\WOW64CPU.DLL
007: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\NTDLL.DLL
008: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\PROGRAM FILES (X86)\MOZILLA FIREFOX\FIREFOX.EXE
009: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\KERNELBASE.DLL
010: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSTEM32\LOCALE.NLS
011: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\ADVAPI32.DLL
012: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\PROGRAM FILES (X86)\MOZILLA FIREFOX\MOZGLUE.DLL
013: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64\MSVCRT.DLL
```

Similarly, through the following image, you can observe the prefetch file for HFS.exe. Such files will be created for every application you access.

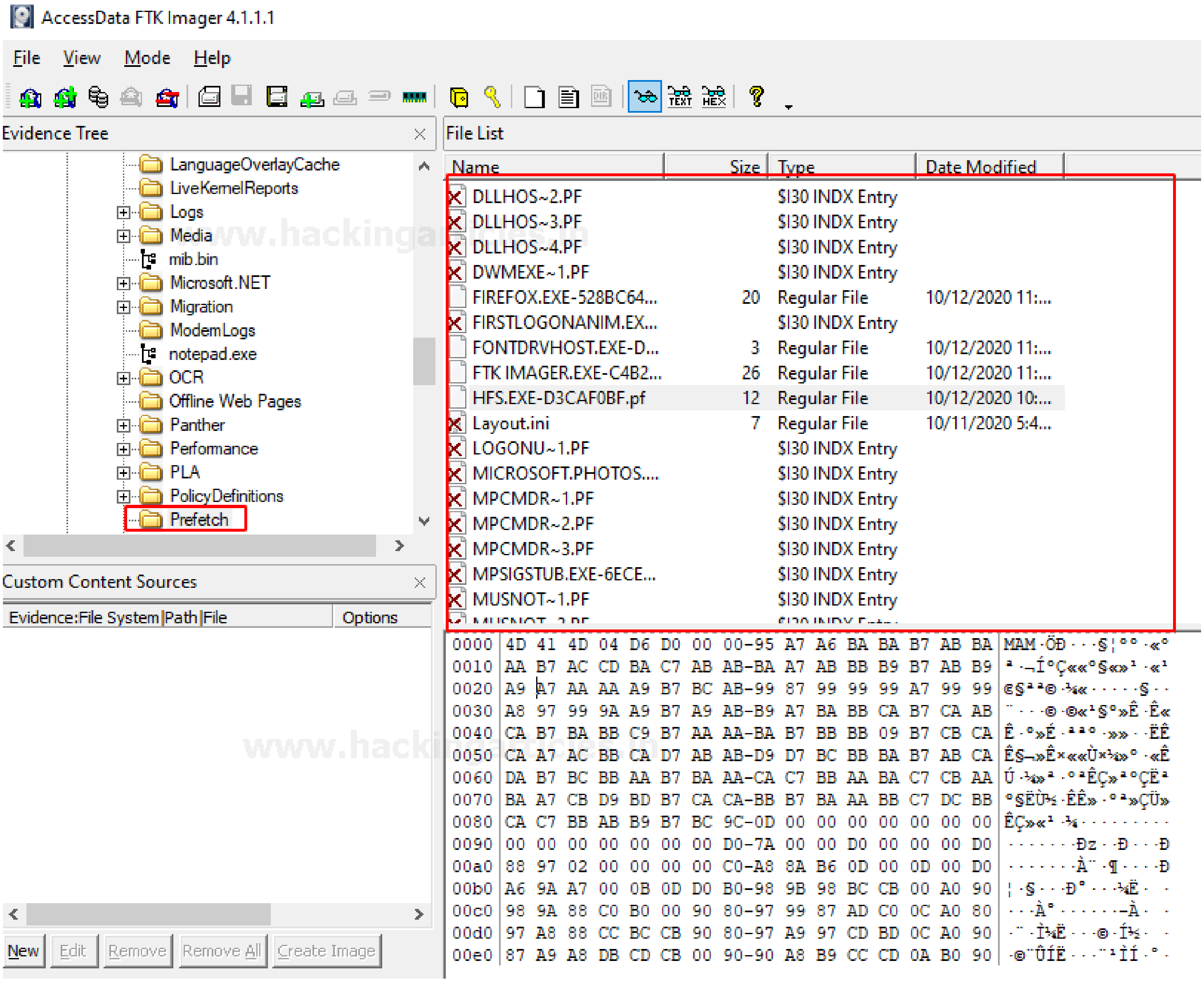


```
Processing 'C:\Windows\Prefetch\HFS.EXE-D3CAF0BF.pf'

Created on: 2020-10-12 10:55:45
Modified on: 2020-10-12 10:59:09
Last accessed on: 2020-10-12 10:59:41

Executable name: HFS.EXE
Hash: D3CAF0BF
File size (bytes): 53,462
Version: Windows 10

Run count: 2
Last run: 2020-10-12 10:59:04
Other run times: 2020-10-12 10:55:35

Volume information:

#0: Name: \VOLUME{01d64ebdfa1b95a7-86fa22e6} Serial: 86FA22E6 Created: 2020-06

Directories referenced: 17

00: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\USERS
01: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\USERS\RAJ
02: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\USERS\RAJ\APPDATA
03: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\USERS\RAJ\APPDATA\LOCAL
04: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\USERS\RAJ\DESKTOP
05: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS
06: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\APPPATCH
07: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\FONTS
08: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\GLOBALIZATION
09: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\GLOBALIZATION\SORTING
10: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\REGISTRATION
11: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSTEM32
12: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSTEM32\DRIVERS
13: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSTEM32\EN-US
14: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\SYSWOW64
15: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\WINSXS\X86_MICROSOFT.WINDOWS.C.
16: \VOLUME{01d64ebdfa1b95a7-86fa22e6}\WINDOWS\WINSXS\X86_MICROSOFT.WINDOWS.CO
```

FTK Imager

As a Forensic Investigator, you can always access the prefetch files to understand the case given to you. Because through these files, it can be determined that what was frequently used on the system that you are investigating. This can be easily done with FTK Imager. FTK imager allows one to view and analyze the prefetch file present in the drive. To access the prefetch file through FTK, just open the said tool and look for the **Prefetch** folder in the left panel as highlighted in the image below:

This is all on prefetch files. Now that we understand these files properly, we can customize it, access it, and use it as we need. The most important thing to know about prefetch files is that it a boon when comes to retracing a malware as any .exe file that has been run on the system, will be logged in prefetch files. Therefore, if a malicious file is executed; you can track it through this.



- LanguageOverlayCache
- LiveKernelReports
- Logs
- Media
- mib.bin
- Microsoft.NET
- Migration
- ModemLogs
- notepad.exe
- OCR
- Offline Web Pages
- Panther
- Performance
- PLA
- PolicyDefinitions
- Prefetch

Name	Size	Type	Date Modified
DLLHOS~2.PF		$I30 INDX Entry	
DLLHOS~3.PF		$I30 INDX Entry	
DLLHOS~4.PF		$I30 INDX Entry	
DWMEXE~1.PF		$I30 INDX Entry	
FIREFOX.EXE-528BC64...	20	Regular File	10/12/2020 11:...
FIRSTLOGONANIM.EX...		$I30 INDX Entry	
FONTDRVHOST.EXE-D...	3	Regular File	10/12/2020 11:...
FTK IMAGER.EXE-C4B2...	26	Regular File	10/12/2020 11:...
HFS.EXE-D3CAF0BF.pf	12	Regular File	10/12/2020 10:...
Layout.ini	7	Regular File	10/11/2020 5:4...
LOGONU~1.PF		$I30 INDX Entry	
MICROSOFT.PHOTOS....		$I30 INDX Entry	
MPCMDR~1.PF		$I30 INDX Entry	
MPCMDR~2.PF		$I30 INDX Entry	
MPCMDR~3.PF		$I30 INDX Entry	
MPSIGSTUB.EXE-6ECE...		$I30 INDX Entry	
MUSNOT~1.PF		$I30 INDX Entry	
MUSNOT~2.PF		$I30 INDX Entry	

```
0000  4D 41 4D 04 D6 D0 00 00-95 A7 A6 BA BA B7 AB BA  MAM·ÖÐ···§¦ºº·«º
0010  AA B7 AC CD BA C7 AB AB-BA A7 AB BB B9 B7 AB B9  ª·¬ÍºÇ««º§«»¹·«¹
0020  A9 A7 AA AA A9 B7 BC AB-99 87 99 99 99 A7 99 99  ©§ªª©·¼«·····§··
0030  A8 97 99 9A A9 B7 A9 AB-B9 A7 BA BB CA B7 CA AB  ¨···©·©«¹§º»Ê·Ê«
0040  CA B7 BA BB C9 B7 AA AA-BA B7 BB BB 09 B7 CB CA  Ê·º»É·ªªº·»»··ËÊ
0050  CA A7 AC BB CA D7 AB AB-D9 D7 BC BB BA B7 AB CA  Ê§¬»Ê×««Ù×¼»º·«Ê
0060  DA B7 BC BB AA B7 BA AA-CA C7 BB AA BA C7 CB AA  Ú·¼»ª·ºªÊÇ»ªºÇËª
0070  BA A7 CB D9 BD B7 CA CA-BB B7 BA AA BB C7 DC BB  º§ËÙ½·ÊÊ»·ºª»ÇÜ»
0080  CA C7 BB AB B9 B7 BC 9C-0D 00 00 00 00 00 00 00  ÊÇ»«¹·¼·········
0090  00 00 00 00 00 00 00 D0-7A 00 00 D0 00 00 00 D0  ·······Ðz··Ð···Ð
00a0  88 97 02 00 00 00 00 C0-A8 8A B6 0D 00 0D 00 D0  ·······À¨·¶····Ð
00b0  A6 9A A7 00 0B 0D D0 B0-98 9B 98 BC CB 00 A0 90  ¦·§···Ð°···¼Ë· ·
00c0  98 9A 88 C0 B0 00 90 80-97 99 87 AD C0 0C A0 80  ···À°·······À· ·
00d0  97 A8 88 CC BC CB 90 80-97 A9 97 CD BD 0C A0 90  ·¨·Ì¼Ë···©·Í½· ·
00e0  87 A9 A8 DB CD CB 00 90-90 A8 B9 CC CD 0A B0 90  ·©¨ÛÍË···¨¹ÌÍ·°·
```