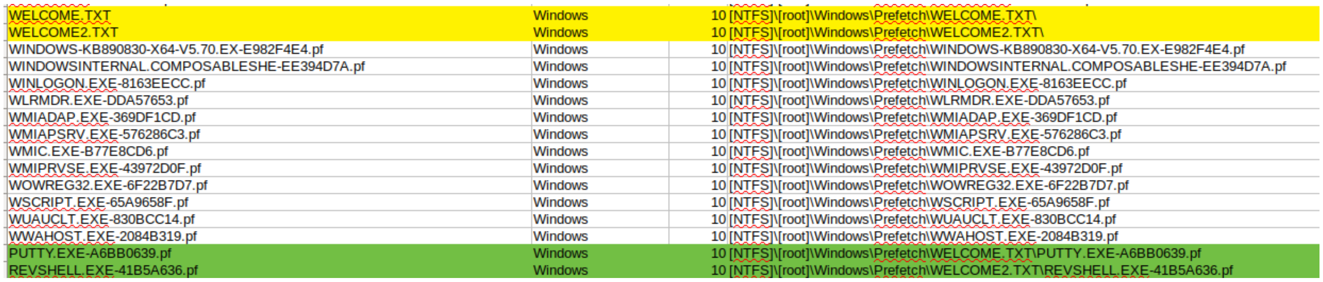
Creating a Hidden Prefetch File to Bypass Normal Forensic Analysis

binary-zone.com/2019/05/26/creating-a-hidden-prefetch-file-to-bypass-normal-forensic-analysis

View all posts by [email protected] → 26 May 2019

While doing more experiments of running EXEs and Malicious EXEs from ADS and Stealthy ADS to continue my previous work "Can We Say Farewell to Hiding Malicious EXEs in Stealth ADS", and in order to create a forensic image and share it with the community as I mentioned here, I found some unusual findings!

When creating a forensic image, I also create a list of files and directories within that image, as seen in Figure 1, just for further checking and verification purposes. So, as usual, was doing the image to share and I noticed the following:

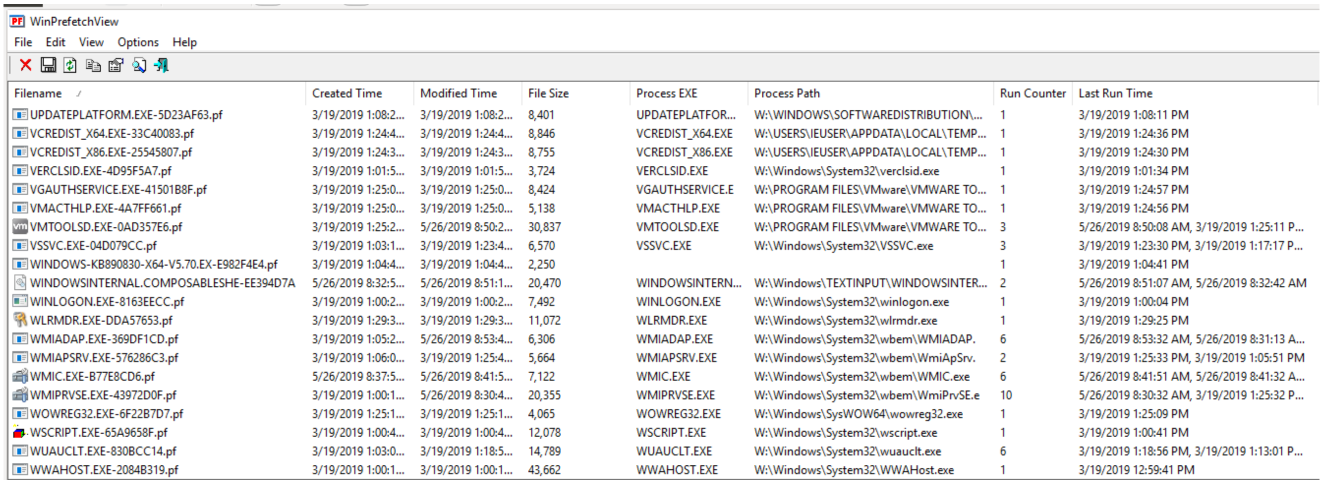


WELCOME.TXT	Windows	10	[NTFS]\[root]\Windows\Prefetch\WELCOME.TXT\
WELCOME2.TXT	Windows	10	[NTFS]\[root]\Windows\Prefetch\WELCOME2.TXT\
WINDOWS-KB890830-X64-V5.70.EX-E982F4E4.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WINDOWS-KB890830-X64-V5.70.EX-E982F4E4.pf
WINDOWSINTERNAL.COMPOSABLESHE-EE394D7A.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WINDOWSINTERNAL.COMPOSABLESHE-EE394D7A.pf
WINLOGON.EXE-8163EECC.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WINLOGON.EXE-8163EECC.pf
WLRMDR.EXE-DDA57653.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WLRMDR.EXE-DDA57653.pf
WMIADAP.EXE-369DF1CD.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WMIADAP.EXE-369DF1CD.pf
WMIAPSRV.EXE-576286C3.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WMIAPSRV.EXE-576286C3.pf
WMIC.EXE-B77E8CD6.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WMIC.EXE-B77E8CD6.pf
WMIPRVSE.EXE-43972D0F.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WMIPRVSE.EXE-43972D0F.pf
WOWREG32.EXE-6F22B7D7.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WOWREG32.EXE-6F22B7D7.pf
WSCRIPT.EXE-65A9658F.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WSCRIPT.EXE-65A9658F.pf
WUAUCLT.EXE-830BCC14.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WUAUCLT.EXE-830BCC14.pf
WWAHOST.EXE-2084B319.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WWAHOST.EXE-2084B319.pf
PUTTY.EXE-A6BB0639.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WELCOME.TXT\PUTTY.EXE-A6BB0639.pf
REVSHELL.EXE-41B5A636.pf	Windows	10	[NTFS]\[root]\Windows\Prefetch\WELCOME2.TXT\REVSHELL.EXE-41B5A636.pf

Figure 1: List of files found in a Forensic Image

I've highlighted the four entries which are totally weird. What does this mean? That is what we are going to find out in this post and prove too. Now from the screenshot above, it seems that there are two text files created WELCOME.TXT and WELCOME2.TXT. These are the files I created on the desktop inside a directory named "creepy" and used to hide putty (PUTTY.EXE) in the first and a reverse shell (REVSHELL.EXE) in the second. Therefore, I decided to run some Prefetch analysis against these two files and see what's going on.

The first quick tool I used was WinPrefetchView, just to have a visual idea of the entries. I was surprised that there is nothing about the two files we saw in the previous screenshot as you can see in Figure 2 below:



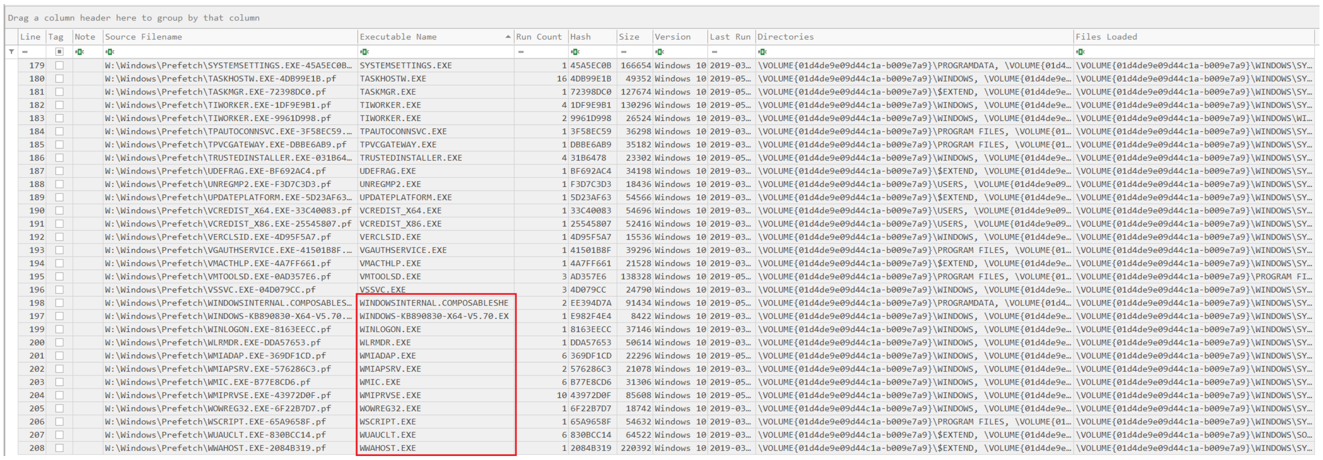
Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time
UPDATEPLATFORM.EXE-5D23AF63.pf	3/19/2019 1:08:2...	3/19/2019 1:08:2...	8,401	UPDATEPLATFOR...	W:\WINDOWS\SOFTWAREDISTRIBUTION\...	1	3/19/2019 1:08:11 PM
VCREDIST_X64.EXE-33C40083.pf	3/19/2019 1:24:4...	3/19/2019 1:24:4...	8,846	VCREDIST_X64.EXE	W:\USERS\IEUSER\APPDATA\LOCAL\TEMP...	1	3/19/2019 1:24:36 PM
VCREDIST_X86.EXE-25545807.pf	3/19/2019 1:24:3...	3/19/2019 1:24:3...	8,755	VCREDIST_X86.EXE	W:\USERS\IEUSER\APPDATA\LOCAL\TEMP...	1	3/19/2019 1:24:30 PM
VERCLSID.EXE-4D95F5A7.pf	3/19/2019 1:01:5...	3/19/2019 1:01:5...	3,724	VERCLSID.EXE	W:\Windows\System32\verclsid.exe	1	3/19/2019 1:01:34 PM
VGAUTHSERVICE.EXE-41501B8F.pf	3/19/2019 1:25:0...	3/19/2019 1:25:0...	8,424	VGAUTHSERVICE.E	W:\PROGRAM FILES\VMware\VMWARE TO...	1	3/19/2019 1:24:57 PM
VMACTHLP.EXE-4A7FF661.pf	3/19/2019 1:25:0...	3/19/2019 1:25:0...	5,138	VMACTHLP.EXE	W:\PROGRAM FILES\VMware\VMWARE TO...	1	3/19/2019 1:24:56 PM
VMTOOLSD.EXE-0AD357E6.pf	3/19/2019 1:25:2...	5/26/2019 8:50:2...	30,837	VMTOOLSD.EXE	W:\PROGRAM FILES\VMware\VMWARE TO...	3	5/26/2019 8:50:08 AM, 3/19/2019 1:25:11 P...
VSSVC.EXE-04D079CC.pf	3/19/2019 1:03:1...	3/19/2019 1:23:4...	6,570	VSSVC.EXE	W:\Windows\System32\VSSVC.exe	3	3/19/2019 1:23:30 PM, 3/19/2019 1:17:17 P...
WINDOWS-KB890830-X64-V5.70.EX-E982F4E4.pf	3/19/2019 1:04:4...	3/19/2019 1:04:4...	2,250			1	3/19/2019 1:04:41 PM
WINDOWSINTERNAL.COMPOSABLESHE-EE394D7A	5/26/2019 8:32:5...	5/26/2019 8:51:1...	20,470	WINDOWSINTERN...	W:\Windows\TEXTINPUT\WINDOWSINTER...	2	5/26/2019 8:51:07 AM, 5/26/2019 8:32:42 AM
WINLOGON.EXE-8163EECC.pf	3/19/2019 1:00:2...	3/19/2019 1:00:2...	7,492	WINLOGON.EXE	W:\Windows\System32\winlogon.exe	1	3/19/2019 1:00:04 PM
WLRMDR.EXE-DDA57653.pf	3/19/2019 1:29:3...	3/19/2019 1:29:3...	11,072	WLRMDR.EXE	W:\Windows\System32\wlrmdr.exe	1	3/19/2019 1:29:25 PM
WMIADAP.EXE-369DF1CD.pf	3/19/2019 1:05:2...	5/26/2019 8:53:4...	6,306	WMIADAP.EXE	W:\Windows\System32\wbem\WMIADAP.	6	5/26/2019 8:53:32 AM, 5/26/2019 8:31:13 A...
WMIAPSRV.EXE-576286C3.pf	3/19/2019 1:06:0...	3/19/2019 1:25:4...	5,664	WMIAPSRV.EXE	W:\Windows\System32\wbem\WmiApSrv.	2	3/19/2019 1:25:33 PM, 3/19/2019 1:05:51 PM
WMIC.EXE-B77E8CD6.pf	5/26/2019 8:37:5...	5/26/2019 8:41:5...	7,122	WMIC.EXE	W:\Windows\System32\wbem\WMIC.exe	6	5/26/2019 8:41:51 AM, 5/26/2019 8:41:32 A...
WMIPRVSE.EXE-43972D0F.pf	3/19/2019 1:00:1...	5/26/2019 8:30:4...	20,355	WMIPRVSE.EXE	W:\Windows\System32\wbem\WmiPrvSE.e	10	5/26/2019 8:30:32 AM, 3/19/2019 1:25:32 P...
WOWREG32.EXE-6F22B7D7.pf	3/19/2019 1:25:1...	3/19/2019 1:25:1...	4,065	WOWREG32.EXE	W:\Windows\SysWOW64\wowreg32.exe	1	3/19/2019 1:25:09 PM
WSCRIPT.EXE-65A9658F.pf	3/19/2019 1:00:4...	3/19/2019 1:00:4...	12,078	WSCRIPT.EXE	W:\Windows\System32\wscript.exe	1	3/19/2019 1:00:41 PM
WUAUCLT.EXE-830BCC14.pf	3/19/2019 1:03:0...	3/19/2019 1:18:5...	14,789	WUAUCLT.EXE	W:\Windows\System32\wuauclt.exe	6	3/19/2019 1:18:56 PM, 3/19/2019 1:13:01 P...
WWAHOST.EXE-2084B319.pf	3/19/2019 1:00:1...	3/19/2019 1:00:1...	43,662	WWAHOST.EXE	W:\Windows\System32\WWAHost.exe	1	3/19/2019 12:59:41 PM

Figure 2: WinPrefetch Results

But that's not enough, I went to use Eric Zimmerman's tool Prefetch Parser (PECmd) and run the test again. So ran the tool against the whole directory and generated a CSV file:

```
PECmd.exe -d W:\Windows\Prefetch --csv C:\Users\IEUser\Desktop\sleuthADS\
```

Then I loaded the CSV file generated into Eric's Time Line Explorer, as you can see in Figure 3:



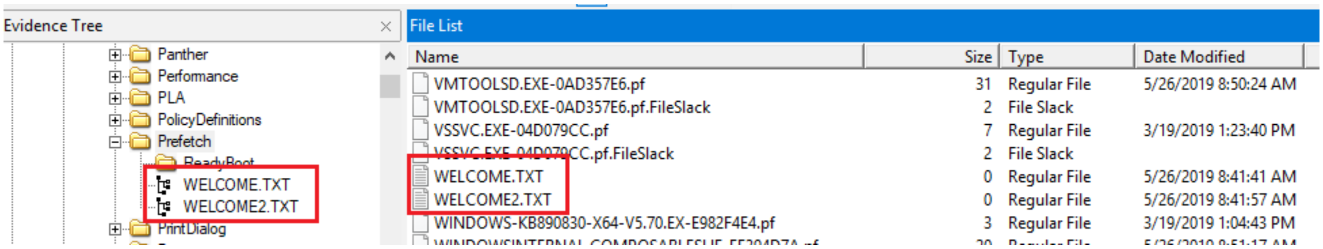
Drag a column header here to group by that column

Line	Tag	Note	Source Filename	Executable Name	Run Count	Hash	Size	Version	Last Run	Directories	Files Loaded
179	□		W:\Windows\Prefetch\SYSTEMSETTINGS.EXE-45A5EC0B…	SYSTEMSETTINGS.EXE	1	45A5EC0B	166654	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAMDATA, \VOLUME{01d4…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
180	□		W:\Windows\Prefetch\TASKHOSTW.EXE-4DB99E1B.pf	TASKHOSTW.EXE	16	4DB99E1B	49352	Windows 10	2019-05…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
181	□		W:\Windows\Prefetch\TASKMGR.EXE-72398DC0.pf	TASKMGR.EXE	1	72398DC0	127674	Windows 10	2019-05…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\$EXTEND, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
182	□		W:\Windows\Prefetch\TIWORKER.EXE-1DF9E9B1.pf	TIWORKER.EXE	4	1DF9E9B1	130296	Windows 10	2019-05…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
183	□		W:\Windows\Prefetch\TIWORKER.EXE-9961D998.pf	TIWORKER.EXE	2	9961D998	26524	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\WI…
184	□		W:\Windows\Prefetch\TPAUTOCONNSVC.EXE-3F58EC59.…	TPAUTOCONNSVC.EXE	1	3F58EC59	36298	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAM FILES, \VOLUME{01…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
185	□		W:\Windows\Prefetch\TPVCGATEWAY.EXE-DBBE6AB9.pf	TPVCGATEWAY.EXE	1	DBBE6AB9	35182	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAM FILES, \VOLUME{01…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
186	□		W:\Windows\Prefetch\TRUSTEDINSTALLER.EXE-031B64…	TRUSTEDINSTALLER.EXE	4	31B6478	23302	Windows 10	2019-05…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
187	□		W:\Windows\Prefetch\UDEFRAG.EXE-BF692AC4.pf	UDEFRAG.EXE	1	BF692AC4	34198	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\$EXTEND, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
188	□		W:\Windows\Prefetch\UNREGMP2.EXE-F3D7C3D3.pf	UNREGMP2.EXE	1	F3D7C3D3	18436	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\USERS, \VOLUME{01d4de9e09…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
189	□		W:\Windows\Prefetch\UPDATEPLATFORM.EXE-5D23AF63…	UPDATEPLATFORM.EXE	1	5D23AF63	54566	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\$EXTEND, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
190	□		W:\Windows\Prefetch\VCREDIST_X64.EXE-33C40083.pf	VCREDIST_X64.EXE	1	33C40083	54696	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\USERS, \VOLUME{01d4de9e09…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
191	□		W:\Windows\Prefetch\VCREDIST_X86.EXE-25545807.pf	VCREDIST_X86.EXE	1	25545807	52416	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\USERS, \VOLUME{01d4de9e09…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
192	□		W:\Windows\Prefetch\VERCLSID.EXE-4D95F5A7.pf	VERCLSID.EXE	1	4D95F5A7	15536	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
193	□		W:\Windows\Prefetch\VGAUTHSERVICE.EXE-41501B8F.…	VGAUTHSERVICE.EXE	1	41501B8F	39296	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAM FILES, \VOLUME{01…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
194	□		W:\Windows\Prefetch\VMACTHLP.EXE-4A7FF661.pf	VMACTHLP.EXE	1	4A7FF661	21528	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\$EXTEND, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
195	□		W:\Windows\Prefetch\VMTOOLSD.EXE-0AD357E6.pf	VMTOOLSD.EXE	3	AD357E6	138328	Windows 10	2019-05…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAM FILES, \VOLUME{01…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAM FI…
196	□		W:\Windows\Prefetch\VSSVC.EXE-04D079CC.pf	VSSVC.EXE	3	4D079CC	24790	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
198	□		W:\Windows\Prefetch\WINDOWSINTERNAL.COMPOSABLES…	WINDOWSINTERNAL.COMPOSABLESHE	2	EE394D7A	91434	Windows 10	2019-05…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAMDATA, \VOLUME{01d4…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
197	□		W:\Windows\Prefetch\WINDOWS-KB890830-X64-V5.70.…	WINDOWS-KB890830-X64-V5.70.EX	1	E982F4E4	8422	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
199	□		W:\Windows\Prefetch\WINLOGON.EXE-8163EECC.pf	WINLOGON.EXE	1	8163EECC	37146	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
200	□		W:\Windows\Prefetch\WLRMDR.EXE-DDA57653.pf	WLRMDR.EXE	1	DDA57653	50614	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
201	□		W:\Windows\Prefetch\WMIADAP.EXE-369DF1CD.pf	WMIADAP.EXE	6	369DF1CD	22296	Windows 10	2019-05…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
202	□		W:\Windows\Prefetch\WMIAPSRV.EXE-576286C3.pf	WMIAPSRV.EXE	2	576286C3	21078	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
203	□		W:\Windows\Prefetch\WMIC.EXE-B77E8CD6.pf	WMIC.EXE	6	B77E8CD6	31306	Windows 10	2019-05…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
204	□		W:\Windows\Prefetch\WMIPRVSE.EXE-43972D0F.pf	WMIPRVSE.EXE	10	43972D0F	85608	Windows 10	2019-05…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
205	□		W:\Windows\Prefetch\WOWREG32.EXE-6F22B7D7.pf	WOWREG32.EXE	1	6F22B7D7	18742	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
206	□		W:\Windows\Prefetch\WSCRIPT.EXE-65A9658F.pf	WSCRIPT.EXE	1	65A9658F	54632	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAM FILES, \VOLUME{01…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…
207	□		W:\Windows\Prefetch\WUAUCLT.EXE-830BCC14.pf	WUAUCLT.EXE	6	830BCC14	64522	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\$EXTEND, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SO…
208	□		W:\Windows\Prefetch\WWAHOST.EXE-2084B319.pf	WWAHOST.EXE	1	2084B319	220392	Windows 10	2019-03…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\$EXTEND, \VOLUME{01d4de9e…	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SY…

Figure 3: PECmd Results in Timeline Explorer

I was shocked that now I have two tools that are unable to see the two WELCOME.TXT and WELCOME2.TXT prefetch files or whatever these files are!!!.

Therefore, time to do some manual sifting through the image and see what is going on. When browsing the Prefetch directory, I noticed the following in Figure 4:



Evidence Tree

Panther
Performance
PLA
PolicyDefinitions
Prefetch
ReadyBoot
WELCOME.TXT
WELCOME2.TXT
PrintDialog

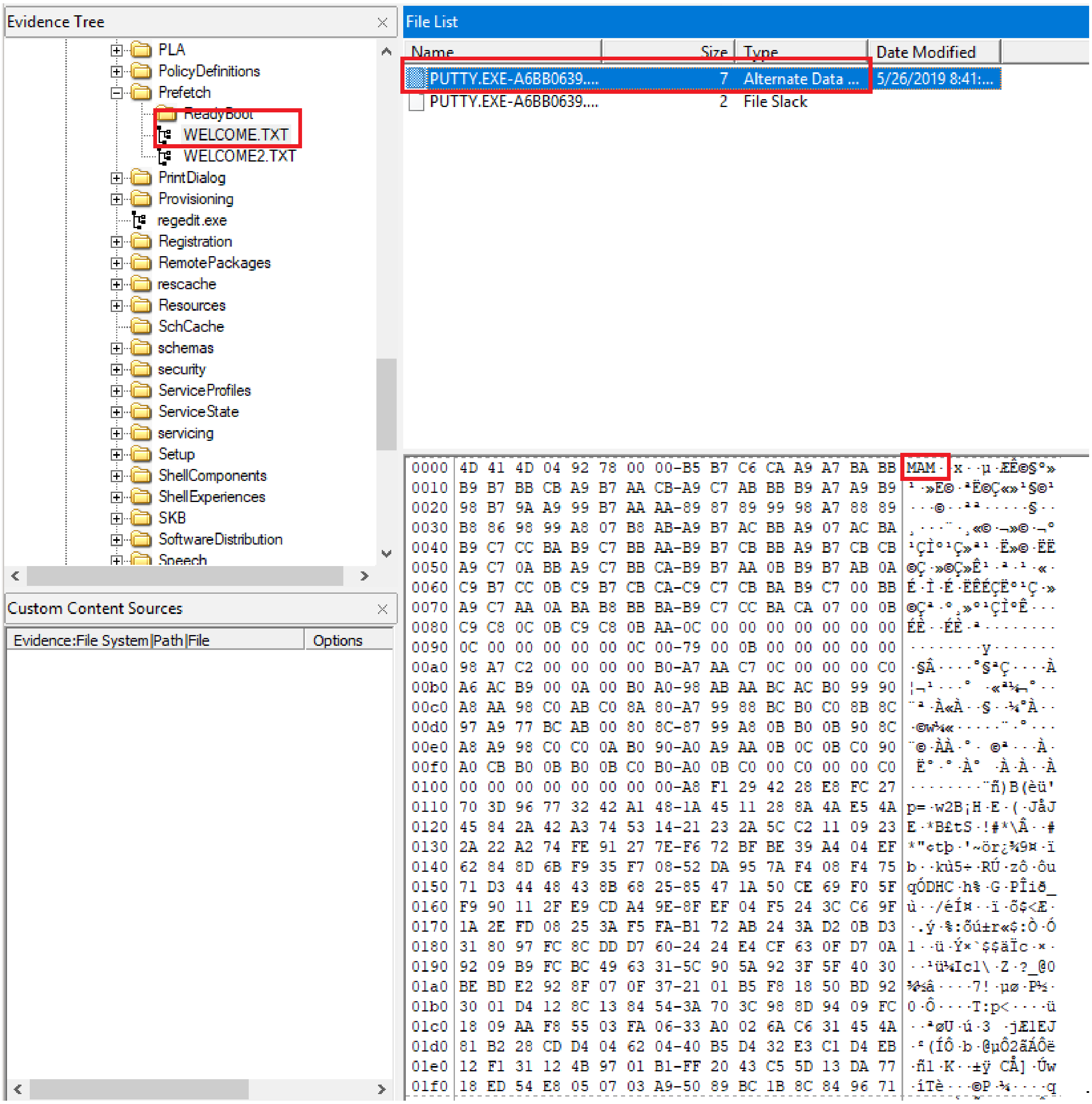
File List

Name	Size	Type	Date Modified
VMTOOLSD.EXE-0AD357E6.pf	31	Regular File	5/26/2019 8:50:24 AM
VMTOOLSD.EXE-0AD357E6.pf.FileSlack	2	File Slack	
VSSVC.EXE-04D079CC.pf	7	Regular File	3/19/2019 1:23:40 PM
VSSVC.EXE-04D079CC.pf.FileSlack	2	File Slack	
WELCOME.TXT	0	Regular File	5/26/2019 8:41:41 AM
WELCOME2.TXT	0	Regular File	5/26/2019 8:41:57 AM
WINDOWS-KB890830-X64-V5.70.EX-E982F4E4.pf	3	Regular File	3/19/2019 1:04:43 PM

Figure 4: Welcome Files in Prefetch Directory

Yes, we can see that they are listed exactly as normal files but with an ADS, as we saw in my previous post.

Let’s check each one of them. So, when accessing the first WELCOME.TXT file, we can see the details in Figure 5:

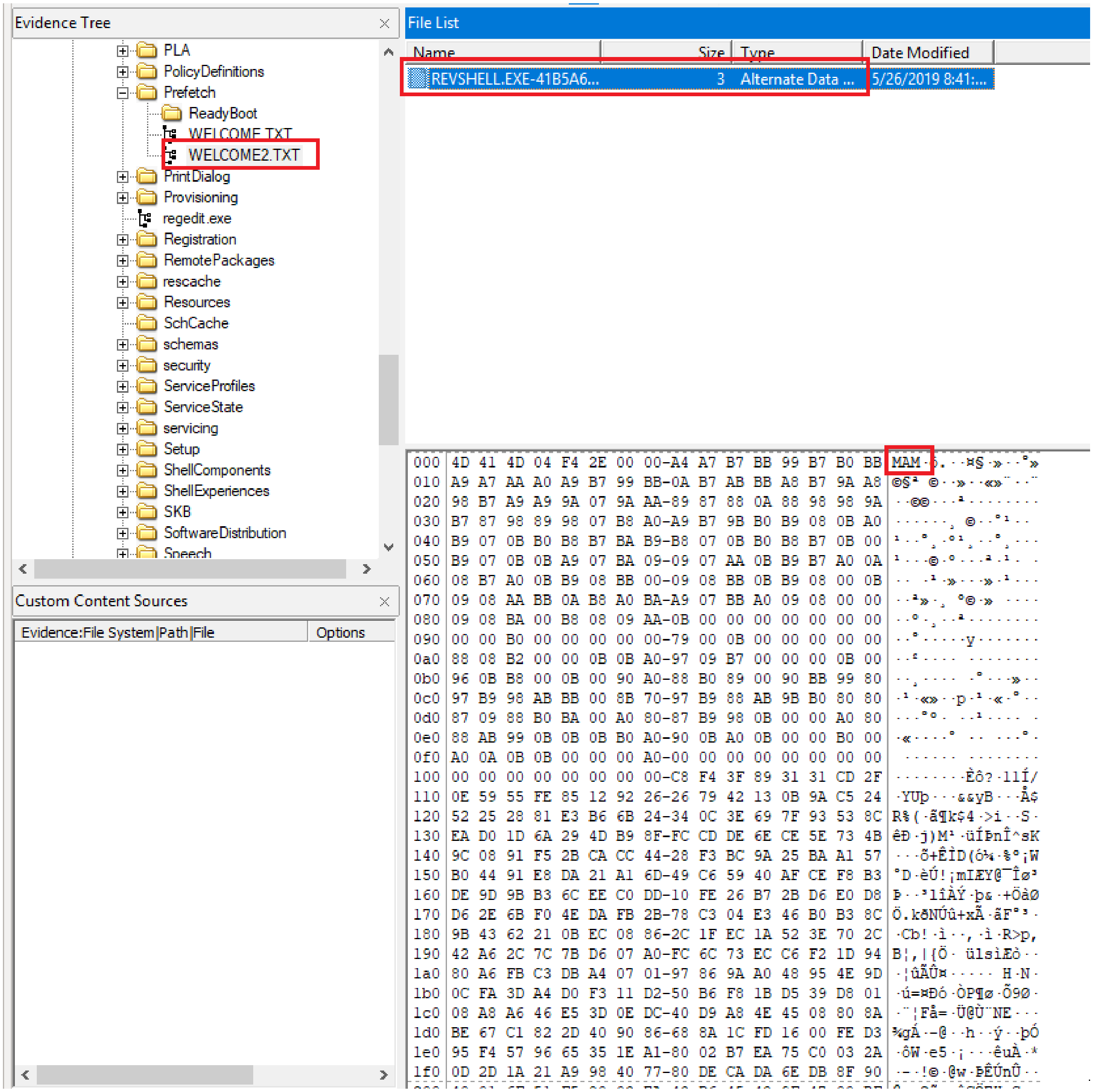


Name	Size	Type	Date Modified
PUTTY.EXE-A6BB0639....	7	Alternate Data ...	5/26/2019 8:41:...
PUTTY.EXE-A6BB0639....	2	File Slack	

```
0000 4D 41 4D 04 92 78 00 00-B5 B7 C6 CA A9 A7 BA BB MAM··x··µ·ÆÊ©§º»
0010 B9 B7 BB CB A9 B7 AA CB-A9 C7 AB BB B9 A7 A9 B9 ¹·»Ë©·ªË©Ç«»¹§©¹
0020 98 B7 9A A9 99 B7 AA AA-89 87 89 99 98 A7 88 89 ··©··ªª·····§··
0030 B8 86 98 99 A8 07 B8 AB-A9 B7 AC BB A9 07 AC BA ¸····¨·¸«©·¬»©·¬º
0040 B9 C7 CC BA B9 C7 BB AA-B9 B7 CB BB A9 B7 CB CB ¹ÇÌº¹Ç»ª¹·Ë»©·ËË
0050 A9 C7 0A BB A9 C7 BB CA-B9 B7 AA 0B B9 B7 AB 0A ©Ç·»©Ç»Ê¹·ª·¹·«·
0060 C9 B7 CC 0B C9 B7 CB CA-C9 C7 CB BA B9 C7 00 BB É·Ì·É·ËÊÉÇËº¹Ç·»
0070 A9 C7 AA 0A BA B8 BB BA-B9 C7 CC BA CA 07 00 0B ©Çª·º¸»º¹ÇÌºÊ···
0080 C9 C8 0C 0B C9 C8 0B AA-0C 00 00 00 00 00 00 00 ÉÈ··ÉÈ·ª········
0090 0C 00 00 00 00 00 0C 00-79 00 0B 00 00 00 00 00 ········y·······
00a0 98 A7 C2 00 00 00 00 B0-A7 AA C7 0C 00 00 00 C0 ·§Â····°§ªÇ····À
00b0 A6 AC B9 00 0A 00 B0 A0-98 AB AA BC AC B0 99 90 ¦¬¹···° ·«ª¼¬°··
00c0 A8 AA 98 C0 AB C0 8A 80-A7 99 88 BC B0 C0 8B 8C ¨ª·À«À··§··¼°À··
00d0 97 A9 77 BC AB 00 80 8C-87 99 A8 0B B0 0B 90 8C ·©w¼«·····¨·°···
00e0 A8 A9 98 C0 C0 0A B0 90-A0 A9 AA 0B 0C 0B C0 90 ¨©·ÀÀ·°· ©ª···À·
00f0 A0 CB B0 0B B0 0B C0 B0-A0 0B C0 00 C0 00 00 C0  Ë°·°·À° ·À·À··À
0100 00 00 00 00 00 00 00 00-A8 F1 29 42 28 E8 FC 27 ········¨ñ)B(èü'
0110 70 3D 96 77 32 42 A1 48-1A 45 11 28 8A 4A E5 4A p=·w2B¡H·E·(·JåJ
0120 45 84 2A 42 A3 74 53 14-21 23 2A 5C C2 11 09 23 E·*B£tS·!#*\Â··#
0130 2A 22 A2 74 FE 91 27 7E-F6 72 BF BE 39 A4 04 EF *"¢tþ·'~ör¿¾9¤·ï
0140 62 84 8D 6B F9 35 F7 08-52 DA 95 7A F4 08 F4 75 b··kù5÷·RÚ·zô·ôu
0150 71 D3 44 48 43 8B 68 25-85 47 1A 50 CE 69 F0 5F qÓDHC·h%·G·PÎið_
0160 F9 90 11 2F E9 CD A4 9E-8F EF 04 F5 24 3C C6 9F ù··/éÍ¤··ï·õ$<Æ·
0170 1A 2E FD 08 25 3A F5 FA-B1 72 AB 24 3A D2 0B D3 ·.ý·%:õú±r«$:Ò·Ó
0180 31 80 97 FC 8C DD D7 60-24 24 E4 CF 63 0F D7 0A 1··ü·Ý×`$$äÏc·×·
0190 92 09 B9 FC BC 49 63 31-5C 90 5A 92 3F 5F 40 30 ··¹ü¼Ic1\·Z·?_@0
01a0 BE BD E2 92 8F 07 0F 37-21 01 B5 F8 18 50 BD 92 ¾½â····7!·µø·P½·
01b0 30 01 D4 12 8C 13 84 54-3A 70 3C 98 8D 94 09 FC 0·Ô····T:p<····ü
01c0 18 09 AA F8 55 03 FA 06-33 A0 02 6A C6 31 45 4A ··ªøU·ú·3 ·jÆ1EJ
01d0 81 B2 28 CD D4 04 62 04-40 B5 D4 32 E3 C1 D4 EB ·²(ÍÔ·b·@µÔ2ãÁÔë
01e0 12 F1 31 12 4B 97 01 B1-FF 20 43 C5 5D 13 DA 77 ·ñ1·K··±ÿ CÅ]·Úw
01f0 18 ED 54 E8 05 07 03 A9-50 89 BC 1B 8C 84 96 71 ·íTè···©P·¼····q
```

Figure 5: Hidden Prefetch File for Putty using FTK

And the second file, WELCOME2.TXT resulted as seen in Figure 6:



Name	Size	Type	Date Modified
REVSHELL.EXE-41B5A6...	3	Alternate Data ...	5/26/2019 8:41:...

```
000 4D 41 4D 04 F4 2E 00 00-A4 A7 B7 BB 99 B7 B0 BB MAM·ô.··¤§·»···°»
010 A9 A7 AA A0 A9 B7 99 BB-0A B7 AB BB A8 B7 9A A8 ©§ª ©··»··«»¨··¨
020 98 B7 A9 A9 9A 07 9A AA-89 87 88 0A 88 98 98 9A ··©©···ª········
030 B7 87 98 89 98 07 B8 A0-A9 B7 9B B0 B9 08 0B A0 ·······¸ ©··°¹··
040 B9 07 0B B0 B8 B7 BA B9-B8 07 0B B0 B8 B7 0B 00 ¹··°¸·º¹¸··°¸···
050 B9 07 0B 0B A9 07 BA 09-09 07 AA 0B B9 B7 A0 0A ¹···©·º···ª·¹· ·
060 08 B7 A0 0B B9 08 BB 00-09 08 BB 0B B9 08 00 0B ·· ·¹·»···»·¹···
070 09 08 AA BB 0A B8 A0 BA-A9 07 BB A0 09 08 00 00 ··ª»·¸ º©·» ····
080 09 08 BA 00 B8 08 09 AA-0B 00 00 00 00 00 00 00 ··º·¸··ª········
090 00 00 B0 00 00 00 00 00-79 00 0B 00 00 00 00 00 ··°·····y·······
0a0 88 08 B2 00 00 0B 0B A0-97 09 B7 00 00 00 0B 00 ··²···· ········
0b0 96 0B B8 00 0B 00 90 A0-88 B0 89 00 90 BB 99 80 ··¸···· ·°···»··
0c0 97 B9 98 AB BB 00 8B 70-97 B9 88 AB 9B B0 80 80 ·¹·«»··p·¹·«·°··
0d0 87 09 88 B0 BA 00 A0 80-87 B9 98 0B 00 00 A0 80 ···°º· ··¹··· ·
0e0 88 AB 99 0B 0B 0B B0 A0-90 0B A0 0B 00 00 B0 00 ·«····° ·· ···°·
0f0 A0 0A 0B 0B 00 00 00 A0-00 00 00 00 00 00 00 00  ······ ········
100 00 00 00 00 00 00 00 00-C8 F4 3F 89 31 31 CD 2F ········Èô?·11Í/
110 0E 59 55 FE 85 12 92 26-26 79 42 13 0B 9A C5 24 ·YUþ···&&yB···Å$
120 52 25 28 81 E3 B6 6B 24-34 0C 3E 69 7F 93 53 8C R%(·ã¶k$4·>i··S·
130 EA D0 1D 6A 29 4D B9 8F-FC CD DE 6E CE 5E 73 4B êÐ·j)M¹·üÍÞnÎ^sK
140 9C 08 91 F5 2B CA CC 44-28 F3 BC 9A 25 BA A1 57 ···õ+ÊÌD(ó¼·%º¡W
150 B0 44 91 E8 DA 21 A1 6D-49 C6 59 40 AF CE F8 B3 °D·èÚ!¡mIÆY@¯Îø³
160 DE 9D 9B B3 6C EE C0 DD-10 FE 26 B7 2B D6 E0 D8 Þ··³lîÀÝ·þ&·+ÖàØ
170 D6 2E 6B F0 4E DA FB 2B-78 C3 04 E3 46 B0 B3 8C Ö.kðNÚû+xÃ·ãF°³·
180 9B 43 62 21 0B EC 08 86-2C 1F EC 1A 52 3E 70 2C ·Cb!·ì··,·ì·R>p,
190 42 A6 2C 7C 7B D6 07 A0-FC 6C 73 EC C6 F2 1D 94 B¦,|{Ö· ülsìÆò··
1a0 80 A6 FB C3 DB A4 07 01-97 86 9A A0 48 95 4E 9D ·¦ûÃÛ¤····· H·N·
1b0 0C FA 3D A4 D0 F3 11 D2-50 B6 F8 1B D5 39 D8 01 ·ú=¤Ðó·ÒP¶ø·Õ9Ø·
1c0 08 A8 A6 46 E5 3D 0E DC-40 D9 A8 4E 45 08 80 8A ·¨¦Få=·Ü@Ù¨NE···
1d0 BE 67 C1 82 2D 40 90 86-68 8A 1C FD 16 00 FE D3 ¾gÁ·-@··h··ý··þÓ
1e0 95 F4 57 96 65 35 1E A1-80 02 B7 EA 75 C0 03 2A ·ôW·e5·¡···êuÀ·*
1f0 0D 2D 1A 21 A9 98 40 77-80 DE CA DA 6E DB 8F 90 ·-·!©·@w·ÞÊÚnÛ··
```

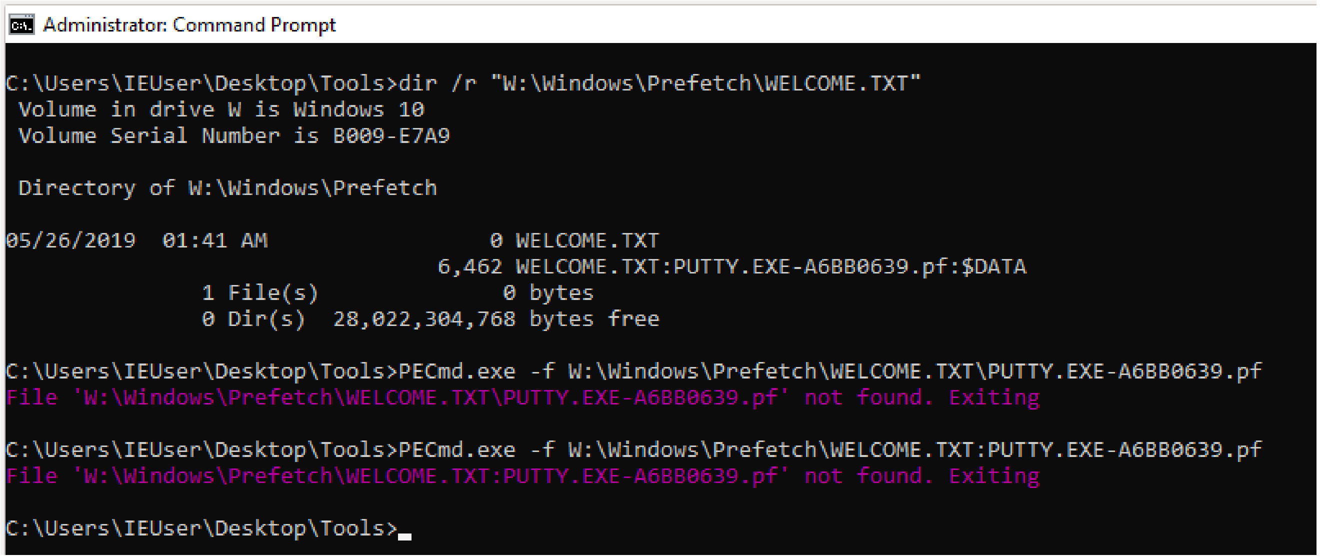
Figure 6: Hidden Prefetch File for Reverse Shell using FTK

They both have an alternate data stream (ADS), exactly how I created them, and the result of running these commands from within the ADS, resulted in creating a Prefetch file within an ADS too! We can prove that these are prefetch files, first by looking at the header (first 3 bytes), which shows the value is MAM. Based on the Prefetch File Format found here, we know that this is for a Windows 10 prefetch file:

> As of Windows 10 the PF is stored in compressed form in a MAM file similar to SuperFetch

Again, what happened is, when I ran the EXEs from the ADS of each text file, the system did not generate a normal Prefetch file, but created a file with the same name of the original, and the true prefetch file was inside the ADS of that file. That is the reason why the tools WinPrefetchView and PECmd, were unable to analyze those files, since they are not prefetch files and both of these tools were designed for analyzing prefetch files.

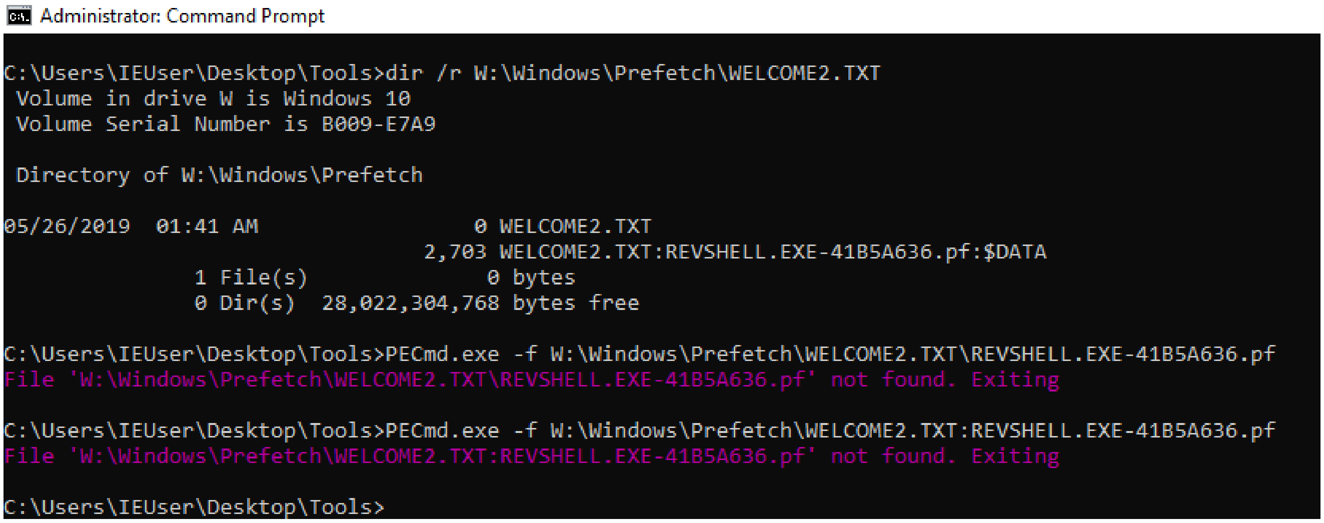
Let's try PECmd again, but by pointing to the file directly "WELCOME.TXT:PUTTY.EXE-A6BB0639.pf" and "WELCOME2.TXT:REVSHELL.EXE-41B5A636.pf". Unfortunately, while trying different ways to run PECmd directly as you can see in the Figure 7 below, I was unable to achieve my goal.



```
C:\Users\IEUser\Desktop\Tools>dir /r "W:\Windows\Prefetch\WELCOME.TXT"
 Volume in drive W is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of W:\Windows\Prefetch

05/26/2019  01:41 AM                 0 WELCOME.TXT
                             6,462 WELCOME.TXT:PUTTY.EXE-A6BB0639.pf:$DATA
               1 File(s)              0 bytes
               0 Dir(s)  28,022,304,768 bytes free

C:\Users\IEUser\Desktop\Tools>PECmd.exe -f W:\Windows\Prefetch\WELCOME.TXT\PUTTY.EXE-A6BB0639.pf
File 'W:\Windows\Prefetch\WELCOME.TXT\PUTTY.EXE-A6BB0639.pf' not found. Exiting

C:\Users\IEUser\Desktop\Tools>PECmd.exe -f W:\Windows\Prefetch\WELCOME.TXT:PUTTY.EXE-A6BB0639.pf
File 'W:\Windows\Prefetch\WELCOME.TXT:PUTTY.EXE-A6BB0639.pf' not found. Exiting

C:\Users\IEUser\Desktop\Tools>_
```

Figure 7: Failed Prefetch Analysis using PECmd "Test1"

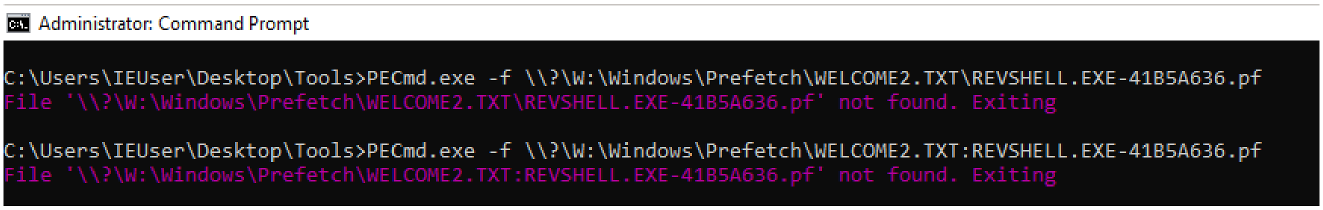
And the second file as seen in Figure 8:



```
C:\Users\IEUser\Desktop\Tools>dir /r W:\Windows\Prefetch\WELCOME2.TXT
 Volume in drive W is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of W:\Windows\Prefetch

05/26/2019  01:41 AM                 0 WELCOME2.TXT
                             2,703 WELCOME2.TXT:REVSHELL.EXE-41B5A636.pf:$DATA
               1 File(s)              0 bytes
               0 Dir(s)  28,022,304,768 bytes free

C:\Users\IEUser\Desktop\Tools>PECmd.exe -f W:\Windows\Prefetch\WELCOME2.TXT\REVSHELL.EXE-41B5A636.pf
File 'W:\Windows\Prefetch\WELCOME2.TXT\REVSHELL.EXE-41B5A636.pf' not found. Exiting

C:\Users\IEUser\Desktop\Tools>PECmd.exe -f W:\Windows\Prefetch\WELCOME2.TXT:REVSHELL.EXE-41B5A636.pf
File 'W:\Windows\Prefetch\WELCOME2.TXT:REVSHELL.EXE-41B5A636.pf' not found. Exiting

C:\Users\IEUser\Desktop\Tools>
```

Figure 8: Failed Prefetch Analysis using PECmd “Test2”

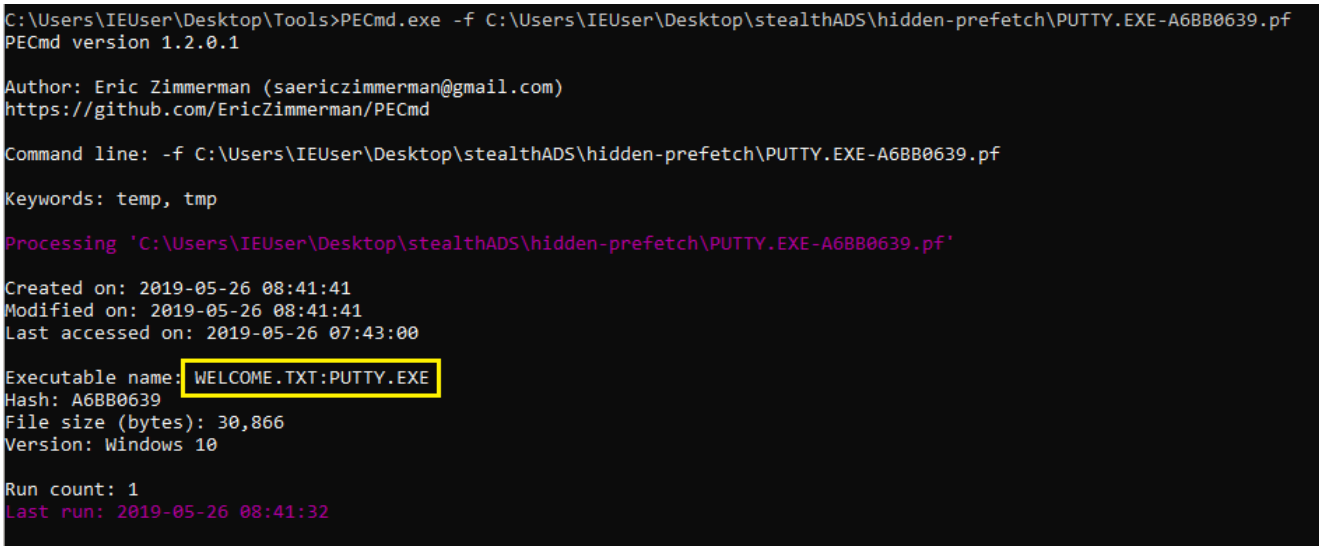
Not even approaching it as in Figure 9:



```
C:\Users\IEUser\Desktop\Tools>PECmd.exe -f \\?\W:\Windows\Prefetch\WELCOME2.TXT\REVSHELL.EXE-41B5A636.pf
File '\\?\W:\Windows\Prefetch\WELCOME2.TXT\REVSHELL.EXE-41B5A636.pf' not found. Exiting

C:\Users\IEUser\Desktop\Tools>PECmd.exe -f \\?\W:\Windows\Prefetch\WELCOME2.TXT:REVSHELL.EXE-41B5A636.pf
File '\\?\W:\Windows\Prefetch\WELCOME2.TXT:REVSHELL.EXE-41B5A636.pf' not found. Exiting
```

Figure 9: Failed Prefetch Analysis using PECmd “Test3”

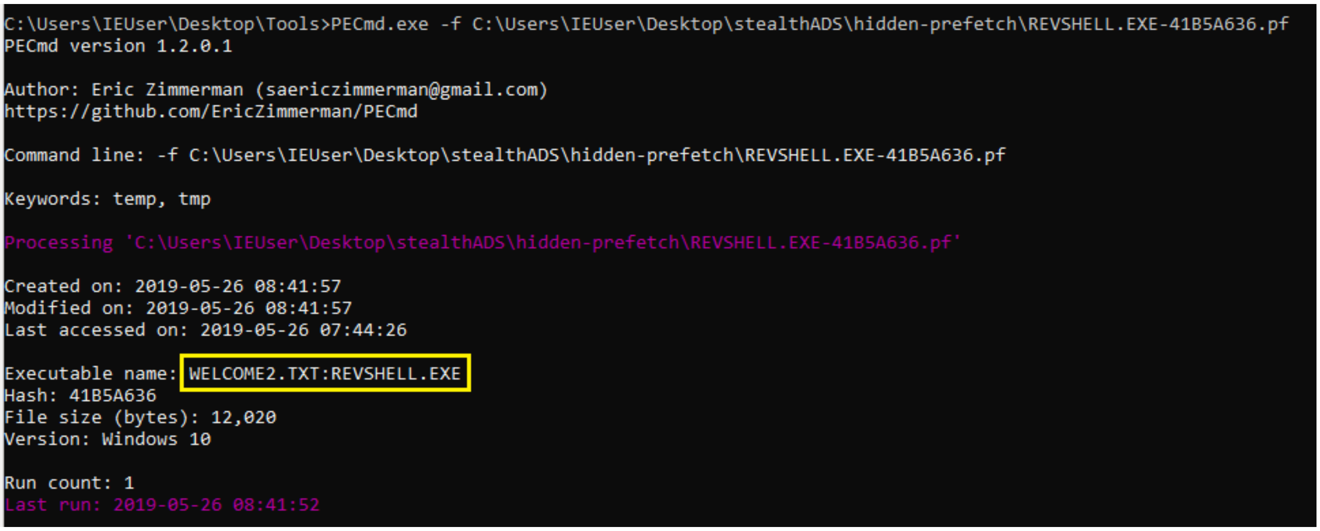
The solution was to extract the alternate data stream from each welcome file and run the tool again. This time, we managed to get the results we expected, as you can see in Figure 10 below:



```
C:\Users\IEUser\Desktop\Tools>PECmd.exe -f C:\Users\IEUser\Desktop\stealthADS\hidden-prefetch\PUTTY.EXE-A6BB0639.pf
PECmd version 1.2.0.1

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

Command line: -f C:\Users\IEUser\Desktop\stealthADS\hidden-prefetch\PUTTY.EXE-A6BB0639.pf

Keywords: temp, tmp

Processing 'C:\Users\IEUser\Desktop\stealthADS\hidden-prefetch\PUTTY.EXE-A6BB0639.pf'

Created on: 2019-05-26 08:41:41
Modified on: 2019-05-26 08:41:41
Last accessed on: 2019-05-26 07:43:00

Executable name: WELCOME.TXT:PUTTY.EXE
Hash: A6BB0639
File size (bytes): 30,866
Version: Windows 10

Run count: 1
Last run: 2019-05-26 08:41:32
```

Figure 10: PECmd Results for Hidden Putty Prefetch File (Putty)

And the second hidden prefetch file as seen in Figure 11:



```
C:\Users\IEUser\Desktop\Tools>PECmd.exe -f C:\Users\IEUser\Desktop\stealthADS\hidden-prefetch\REVSHELL.EXE-41B5A636.pf
PECmd version 1.2.0.1

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

Command line: -f C:\Users\IEUser\Desktop\stealthADS\hidden-prefetch\REVSHELL.EXE-41B5A636.pf

Keywords: temp, tmp

Processing 'C:\Users\IEUser\Desktop\stealthADS\hidden-prefetch\REVSHELL.EXE-41B5A636.pf'

Created on: 2019-05-26 08:41:57
Modified on: 2019-05-26 08:41:57
Last accessed on: 2019-05-26 07:44:26

Executable name: WELCOME2.TXT:REVSHELL.EXE
Hash: 41B5A636
File size (bytes): 12,020
Version: Windows 10

Run count: 1
Last run: 2019-05-26 08:41:52
```

Figure 11: PECmd Results for Hidden Putty Prefetch File (RevShell)

As you can see, if you just depend on running your tools, then you might miss something, it is always good to sift through the data you have, check stuff manually. I know this takes time, but it will help you make sure you did not miss something. Oh, and before I forget, I'm going to write another post showing how we can detect executables that were launched from alternate data streams could be detected, even if you did not have any event logs configured! More on that later…

So there you go, the post covered how to go under the radar and also how to find this sort of unusual activity.

See you in the next post…

Note(s):
1. Both Putty.exe and RevShell.exe were hidden in a normal ADS and stealth ADS (more on the later in the next post).
2. Both were executed from normal and stealth ADS
3. Putty has a manually injected payload, while RevShell.exe is a normal reverse shell meterpreter.

Good readings:
1. Forensic Riddle #3 – Answer
2. "Hidden" Prefetch File Analysis and Alternate Data Sources
3. Prefetch folder is empty