Global Information Assurance Certification Paper

Tor Browser Artifacts in Windows 10

GIAC GCFA Gold Certification

Author: Aron Warren, aronwarren@gmail.com
Advisor: Adam Kliarsky
Accepted: February 22nd, 2017

Abstract

The Tor network is a popular, encrypted, worldwide, anonymizing virtual network in existence since 2002 and is used by all facets of society such as privacy advocates, journalists, governments, and criminals. This paper will provide a forensic analysis of the Tor Browser version 5 client on a Windows 10 host for an individual or group interested in remnants left by the software. This paper will utilize various free and commercial tools to provide a detailed analysis of filesystem artifacts as well as a comparison between pre- and post- connection to the Tor network using memory analysis.

1. Introduction

The Tor project has been a worldwide collaborative effort for over twenty years with roots beginning in the United States Government. The Office of Naval Research funded a project in 1995 (Syverson, 2005b) with the goal of identifying a method "not specifically to provide anonymous communication, but, to separate identification from routing " (Syverson, 2005a, para. 5). The work was termed Onion Routing with the initial development milestone called "generation 0" (Syverson, 2005b, para. 4). The Onion Routing's initial public presentation was at the First Information Hiding Workshop on May 31, 1996 (Syverson, 2005b). In 1997 improvements moved development from generation 0 to generation 1 and Defense Advanced Research Projects Agency (DARPA) became a funding source (Syverson, 2005b). Generation 2 of the code is what is commonly named Tor (Syverson, 2005b). Tor is an acronym for "The onion routing" even though it does not follow acronym conventions in capitalization ("Tor FAQ," n.d.). In 2002 generation 2 was born as a fork of code "originally produced by Matej Pfajfar at Cambridge University for his undergraduate final-year project" (Syverson, 2005b, para. 24). Code development moved in 2003 to torproject.org and the Tor network was fully deployed (Syverson, 2005b).

Onion routing is a simple concept in that the end user, or *initiator* of network traffic, encrypts traffic with multiple layers. A layer of encryption exists for each hop inside the Tor network as denoted on the left in Figure 1. As the encrypted traffic moves through the Tor network, each node removes one layer of encryption, analogous to removing an onion layer. At the last Tor network node, the final layer of encryption is removed and the traffic proceeds out onto the Internet. The first node going into the Tor network, node A in Figure 1, is called the entry relay

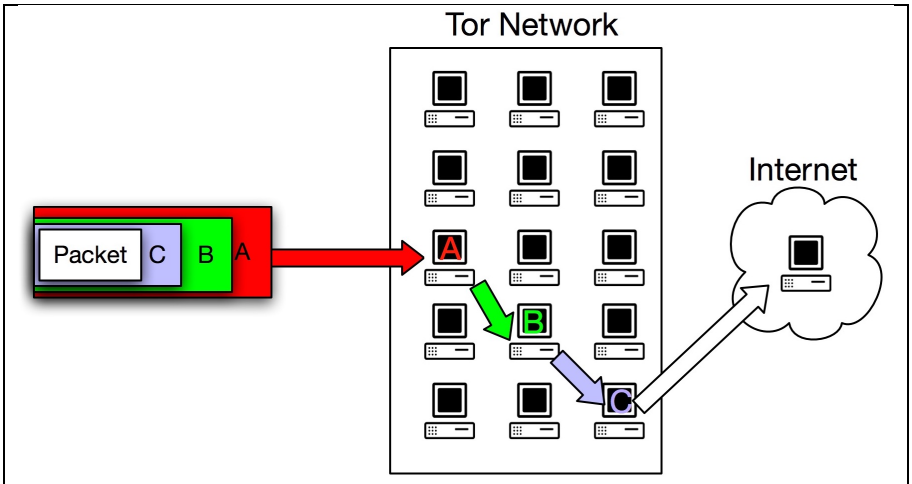


Figure 1. A packet is encrypted once for each hop in the Tor Network. At each Tor node, the outermost layer of encryption is removed.

or entry guard ("Tor FAQ," n.d.). The last node, node C in Figure 1, is called the exit relay or exit node ("Tor FAQ," n.d.).

The Tor Browser Bundle, currently called Tor Browser, attempts to achieve the simplest method for connecting users to Tor (Peery, 2014). In terms of software development, Tor dates back to at least a minimal version number of 1.0 as of March of 2008 (Phobos, 2008). The current version of 6.0.8 is based upon Mozilla's Firefox Extended Release Support (ESR) and includes "Torbutton, TorLauncher, NoScript, and HTTPS-Everywhere" ("What is Tor Browser," n.d.).

This paper will begin by giving an overview of steps taken in performing a Tor Browser installation and subsequent connection to the Tor network. The Tor Browser will be installed on a Windows 10 Virtual Machine (VM). Once the relevant image snapshots have been created, an in-depth look at the filesystem artifacts will be shown. Subsequently, an analysis of the in-memory artifacts will be performed. Lastly, the paper will be an overview of the Tor Browser's anti-forensics approach will be provided.

2. Forensic Approach

The disk images that will be used in the analysis are snapshots that were created using VMWare Fusion version 8.5.3. The Operating System (OS) used was a clean 64-bit installation of Windows 8.1 Pro, subsequently upgraded to a 64-bit Windows 10 Pro. The OS was patched to kernel version 10.0.10586.17. The user *warren* seen throughout this paper was a user account with administrative privileges.

To make the analysis easier, a full clone of the VM was made to have a clean starting point with the snapshots. The first snapshot of the clone was made immediately after the cloning was performed. The second snapshot was taken was after the Tor Browser software was installed. A third snapshot was made while a connection to the Tor network was active.

The computer used to perform the analysis was a Windows 7 Home Edition SIFT workstation provided in the SANS FOR408 class disc version 6.0, dated September 2012. The commercial X-Ways Forensics version 17.3 SR 4 was used along with open source tools that will be mentioned throughout this paper. The version of the Tor Browser installed was version 5.0_en-US.

The reason an older Tor Browser version was used for analysis in this paper is in following the Ethical Tor Research Guidelines whose general principle is that "experimentation

does not justify endangering people" (Ailanthus, 2015). By using an older version, it was this author's hope that any vulnerabilities have been mitigated allowing for end-user's time to upgrade to newer versions. The analysis done here was considered a basic template with the potential to be performed with the most current Tor Browser version.

3. Installation of Regshot

A basic Windows forensic step is to obtain the registry settings. The registry before and after installation of the Tor Browser software can yield an understanding of how the software installation changes the system. Regshot, shown in Figure 2, is open source software that performs registry snapshots (regshot, 2016). HAL9000 says that we "simply create the 1st shot, install the software or run the program you want to watch, and then press 2nd shot" (Hal9000, 2016).

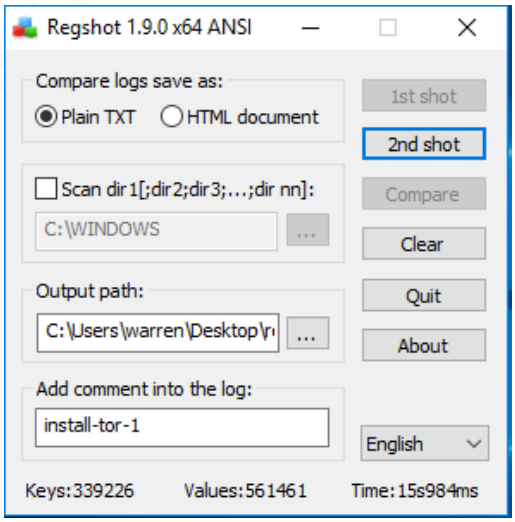


Figure 2. Regshot version 1.9.0 with the first shot already taken and the second shot ready to be taken.

4. Installation of Tor Browser

Older versions of the Tor Browser are difficult to find but can be obtained from https://archive.torproject.org/tor-package-archive/torbrowser/5.0/ . Pretty Good Privacy (PGP) was used, as shown in Figure 3 below, to verify the software signatures and ensure the version downloaded is a verified package ("How to verify signatures for packages," n.d.).

```
warren$ gpg --keyserver pool.sks-keyservers.net --recv-keys
0x4E2C6E8793298290
gpg: requesting key 93298290 from hkp server pool.sks-keyservers.net
gpg: key 93298290: public key "Tor Browser Developers (signing key)
<torbrowser@torproject.org>" imported
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: next trustdb check due at 2021-06-03
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

```
warren$ gpg --fingerprint 0x4E2C6E8793298290
pub   4096R/93298290 2014-12-15 [expires: 2020-08-24]
      Key fingerprint = EF6E 286D DA85 EA2A 4BA7  DE68 4E2C 6E87 9329 8290
uid                  Tor Browser Developers (signing key)
<torbrowser@torproject.org>
sub   4096R/F65C2036 2014-12-15 [expires: 2017-08-25]
sub   4096R/D40814E0 2014-12-15 [expires: 2017-08-25]
sub   4096R/C3C07136 2016-08-24 [expires: 2018-08-24]

warren$ gpg --verify torbrowser-install-5.0_en-US.exe{.asc*,}
gpg: Signature made Mon Aug 10 11:11:44 2015 MDT using RSA key ID D40814E0
gpg: Good signature from "Tor Browser Developers (signing key)
<torbrowser@torproject.org>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: EF6E 286D DA85 EA2A 4BA7  DE68 4E2C 6E87 9329 8290
     Subkey fingerprint: BA1E E421 BBB4 5263 180E  1FC7 2E1A C68E D408 14E0
```

Figure 3. PGP verifies a file's content against a signature signed by a key. This ensures that the file has not been altered.

Since the package has been verified, as shown with the words "Good signature" in Figure 3, the next step of installation was as easy as double-clicking the executable. For this installation, the user's desktop was chosen to make it easy to find forensically.

Regshot was used again and the second shot was taken. In comparing the differences between the first and second shots only one related entry was found, and it showed the location the installation binary was launched from was a VMware shared folder, as shown in Figure 4:

```
HKU\S-1-5-21-445630921-2900216602-2167668200-1001\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\\\vmware-
host\Shared Folders\shared-with-vm\torbrowser-install-5.0_en-US.exe:  53 41
43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 78 22 9C 02 34 6E 9C 02
01 00 00 00 00 00 00 00 00 00 01 06 00 01 00 00 19 B4 C5 29 E3 12 D1 01 00 00
00 00 00 00 00 00 02 00 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 54 48 00 00 00 00 00 00 02 00 00 00 02 00
00 00
```

Figure 4. The installation path of the Tor Browser installer.

5. Filesystem Artifacts

5.1 Carving in W-Ways

To perform the filesystem forensics, X-Ways was used to carve the files. X-Ways is compatible with VMDK files that are split into smaller file sizes. All that was needed to be done is "Create New Case" file from the "Case Data" window's File Menu, as shown in Figure 5.

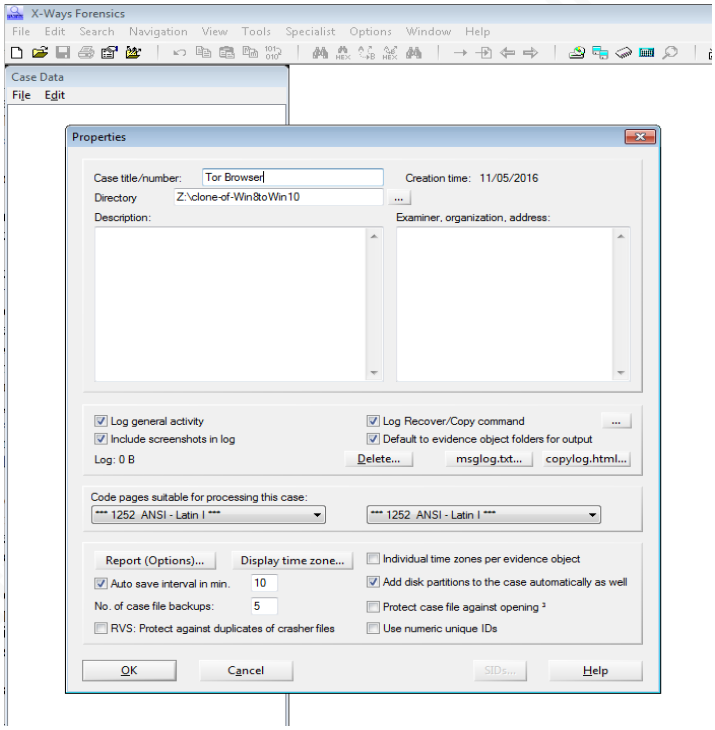


Figure 5. X-Ways default case properties when a new case is created.

Next, in the Case Data window selecting "Add Image" from the File menu was done to add the VMDK files. The next step was to select each VM snapshot's VMDK file.

As shown in Figure 6, each of the VM snapshots was added in with disk image "Virtual Disk-cl1-000003" which is the snapshot that is the post-Tor Browser installation snapshot when the Tor Browser was running and connected to the Tor network.

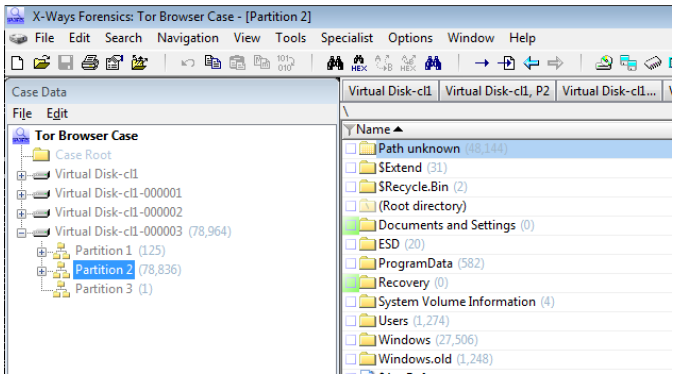
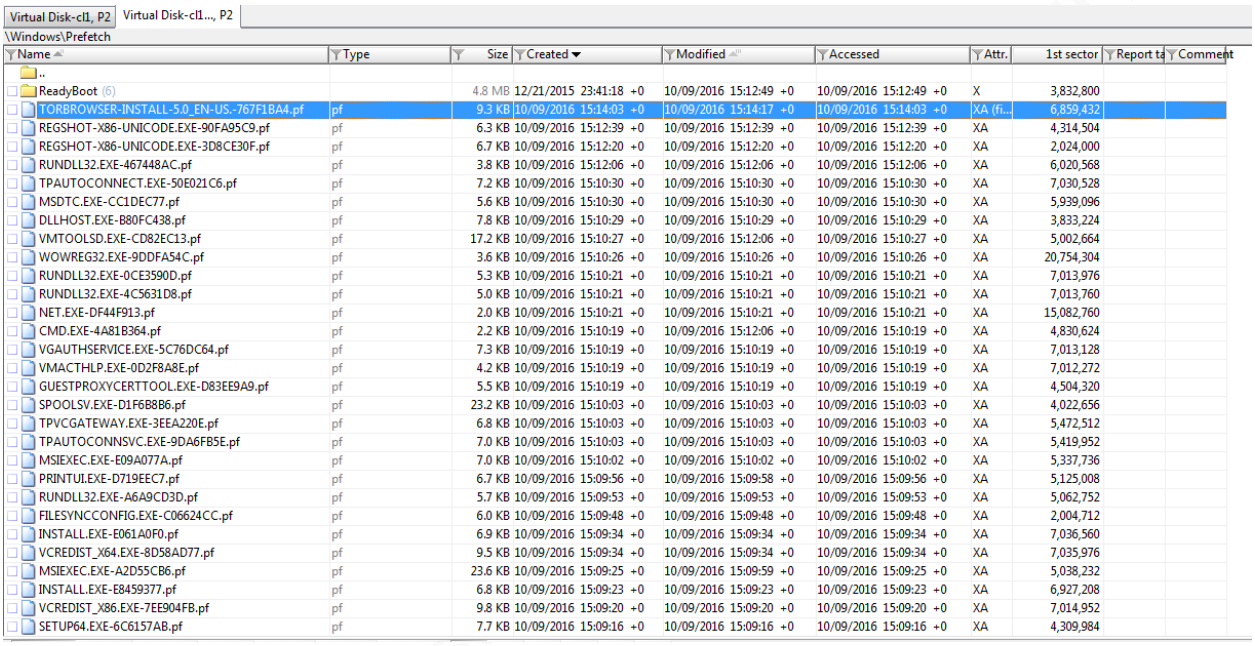


Figure 6. Adding each of the Virtual Machine disk images is necessary to gather pre- and post-filesystem artifacts.

5.2 Prefetch

One of the artifacts to look for on the filesystem is a prefetch file to indicate the software's installation location. To find prefetch files, one must traverse to %SystemRoot%\Prefetch. The contents are shown in Figure 7 below ("Prefetch," 2016).



Virtual Disk-cl1, P2 | Virtual Disk-cl1..., P2

\Windows\Prefetch

Name	Type	Size	Created	Modified	Accessed	Attr.	1st sector	Report ta	Comment
..									
ReadyBoot (6)		4.8 MB	12/21/2015 23:41:18 +0	10/09/2016 15:12:49 +0	10/09/2016 15:12:49 +0	X	3,832,800		
TORBROWSER-INSTALL-5.0_EN-US.-767F1BA4.pf	pf	9.3 KB	10/09/2016 15:14:03 +0	10/09/2016 15:14:17 +0	10/09/2016 15:14:03 +0	XA (fi...	6,859,432		
REGSHOT-X86-UNICODE.EXE-90FA95C9.pf	pf	6.3 KB	10/09/2016 15:12:39 +0	10/09/2016 15:12:39 +0	10/09/2016 15:12:39 +0	XA	4,314,504		
REGSHOT-X86-UNICODE.EXE-3D8CE30F.pf	pf	6.7 KB	10/09/2016 15:12:20 +0	10/09/2016 15:12:20 +0	10/09/2016 15:12:20 +0	XA	2,024,000		
RUNDLL32.EXE-467448AC.pf	pf	3.8 KB	10/09/2016 15:12:06 +0	10/09/2016 15:12:06 +0	10/09/2016 15:12:06 +0	XA	6,020,568		
TPAUTOCONNECT.EXE-50E021C6.pf	pf	7.2 KB	10/09/2016 15:10:30 +0	10/09/2016 15:10:30 +0	10/09/2016 15:10:30 +0	XA	7,030,528		
MSDTC.EXE-CC1DEC77.pf	pf	5.6 KB	10/09/2016 15:10:30 +0	10/09/2016 15:10:30 +0	10/09/2016 15:10:30 +0	XA	5,939,096		
DLLHOST.EXE-B80FC438.pf	pf	7.8 KB	10/09/2016 15:10:29 +0	10/09/2016 15:10:29 +0	10/09/2016 15:10:29 +0	XA	3,833,224		
VMTOOLSD.EXE-CD82EC13.pf	pf	17.2 KB	10/09/2016 15:10:27 +0	10/09/2016 15:12:06 +0	10/09/2016 15:10:27 +0	XA	5,002,664		
WOWREG32.EXE-9DDFA54C.pf	pf	3.6 KB	10/09/2016 15:10:26 +0	10/09/2016 15:10:26 +0	10/09/2016 15:10:26 +0	XA	20,754,304		
RUNDLL32.EXE-0CE3590D.pf	pf	5.3 KB	10/09/2016 15:10:21 +0	10/09/2016 15:10:21 +0	10/09/2016 15:10:21 +0	XA	7,013,976		
RUNDLL32.EXE-4C5631D8.pf	pf	5.0 KB	10/09/2016 15:10:21 +0	10/09/2016 15:10:21 +0	10/09/2016 15:10:21 +0	XA	7,013,760		
NET.EXE-DF44F913.pf	pf	2.0 KB	10/09/2016 15:10:21 +0	10/09/2016 15:10:21 +0	10/09/2016 15:10:21 +0	XA	15,082,760		
CMD.EXE-4A81B364.pf	pf	2.2 KB	10/09/2016 15:10:19 +0	10/09/2016 15:12:06 +0	10/09/2016 15:10:19 +0	XA	4,830,624		
VGAUTHSERVICE.EXE-5C76DC64.pf	pf	7.3 KB	10/09/2016 15:10:19 +0	10/09/2016 15:10:19 +0	10/09/2016 15:10:19 +0	XA	7,013,128		
VMACTHLP.EXE-0D2F8A8E.pf	pf	4.2 KB	10/09/2016 15:10:19 +0	10/09/2016 15:10:19 +0	10/09/2016 15:10:19 +0	XA	7,012,272		
GUESTPROXYCERTTOOL.EXE-D83EE9A9.pf	pf	5.5 KB	10/09/2016 15:10:19 +0	10/09/2016 15:10:19 +0	10/09/2016 15:10:19 +0	XA	4,504,320		
SPOOLSV.EXE-D1F6B8B6.pf	pf	23.2 KB	10/09/2016 15:10:03 +0	10/09/2016 15:10:03 +0	10/09/2016 15:10:03 +0	XA	4,022,656		
TPVCGATEWAY.EXE-3EEA220E.pf	pf	6.8 KB	10/09/2016 15:10:03 +0	10/09/2016 15:10:03 +0	10/09/2016 15:10:03 +0	XA	5,472,512		
TPAUTOCONNSVC.EXE-9DA6FB5E.pf	pf	7.0 KB	10/09/2016 15:10:03 +0	10/09/2016 15:10:03 +0	10/09/2016 15:10:03 +0	XA	5,419,952		
MSIEXEC.EXE-E09A077A.pf	pf	7.0 KB	10/09/2016 15:10:02 +0	10/09/2016 15:10:02 +0	10/09/2016 15:10:02 +0	XA	5,337,736		
PRINTUI.EXE-D719EEC7.pf	pf	6.7 KB	10/09/2016 15:09:56 +0	10/09/2016 15:09:58 +0	10/09/2016 15:09:56 +0	XA	5,125,008		
RUNDLL32.EXE-A6A9CD3D.pf	pf	5.7 KB	10/09/2016 15:09:53 +0	10/09/2016 15:09:53 +0	10/09/2016 15:09:53 +0	XA	5,062,752		
FILESYNCCONFIG.EXE-C06624CC.pf	pf	6.0 KB	10/09/2016 15:09:48 +0	10/09/2016 15:09:48 +0	10/09/2016 15:09:48 +0	XA	2,004,712		
INSTALL.EXE-E061A0F0.pf	pf	6.9 KB	10/09/2016 15:09:34 +0	10/09/2016 15:09:34 +0	10/09/2016 15:09:34 +0	XA	7,036,560		
VCREDIST_X64.EXE-8D58AD77.pf	pf	9.5 KB	10/09/2016 15:09:34 +0	10/09/2016 15:09:34 +0	10/09/2016 15:09:34 +0	XA	7,035,976		
MSIEXEC.EXE-A2D55CB6.pf	pf	23.6 KB	10/09/2016 15:09:25 +0	10/09/2016 15:09:59 +0	10/09/2016 15:09:25 +0	XA	5,038,232		
INSTALL.EXE-E8459377.pf	pf	6.8 KB	10/09/2016 15:09:23 +0	10/09/2016 15:09:23 +0	10/09/2016 15:09:23 +0	XA	6,927,208		
VCREDIST_X86.EXE-7EE904FB.pf	pf	9.8 KB	10/09/2016 15:09:20 +0	10/09/2016 15:09:20 +0	10/09/2016 15:09:20 +0	XA	7,014,952		
SETUP64.EXE-6C6157AB.pf	pf	7.7 KB	10/09/2016 15:09:16 +0	10/09/2016 15:09:16 +0	10/09/2016 15:09:16 +0	XA	4,309,984		

Figure 7. Prefetch files able to be carved from the VM snapshot taken after installation of the Tor Browser.

Right clicking on the prefetch file and selecting Recover/Copy from the context menu presents the option to export the prefetch file. Once the file is recovered decompression must be performed to view the contents of the prefetch file (Picasso, 2015a).

Windows 7 SIFT does not have the OS files for Windows 10 prefetch decompression necessary to run Picasso's regripper scripts (2015b). The scripts must instead be launched on a Windows 10 machine. The command used is shown in Figure 8:

```
$ python hotoloti/sas/w10pfdecomp.py TORBROWSER-INSTALL-5.0_EN-US.-767F1BA4.pf    TORBROWSER-INSTALL-5.0_EN-US.-767F1BA4-uncompressed
```

Figure 8. The command line arguments necessary to decompress the prefetch file on a Windows 10 host.

Running hexdump on the resultant uncompressed file produced the following first five lines shown in Figure 9:

```
0000000 1e 00 00 00 53 43 43 41 11 00 00 00 e2 ad 00 00
0000010 54 00 4f 00 52 00 42 00 52 00 4f 00 57 00 53 00
0000020 45 00 52 00 2d 00 49 00 4e 00 53 00 54 00 41 00
0000030 4c 00 4c 00 2d 00 35 00 2e 00 30 00 5f 00 45 00
0000040 4e 00 2d 00 55 00 53 00 2e 00 00 00 a4 1b 7f 76
0000050 00 00 00 00 30 01 00 00 53 00 00 00 90 0b 00 00
```

Figure 9. The first five lines of hex from the uncompressed file.

At offset 0x0000000 for four bytes and at offset 0x0000004 for four bytes the output shown in Figure 10 are the properties of the prefetch file ("Windows Prefetch File Format," 2016).

```
0x1e          = 30 (Windows 10)
0x53 43 43 41 = SCCA
```

Figure 10. The hex values converted.

Starting at location 0x0000010 for 60 bytes was the program identifier ("Windows Prefetch File Format," 2016) as shown in Figure 11:

```
54 00 4f 00 52 00 42 00 52 00 4f 00 57 00 53 00 45 00 52 00 2d 00 49 00 4e 00
53 00 54 00 41 00 4c 00 4c 00 2d 00 35 00 2e 00 30 00 5f 00 45 00 4e 00 2d 00
55 00 53 00 2e 00 00 00 a4 1b 7f 76 00 00 00 00 30 01 00 00 53 00 00 00 90 0b
00 00 0c 0c 00 00 f0 6b 00 00 12 2d 00 00 08 99 00 00
```

Figure 11. The program identifier expressed in hex.

Using a hex to ASCII converter of the hex in Figure 11 yielded the string shown in Figure 12:

```
TORBROWSER-INSTALL-5.0_EN-US.¤_□v0_S□ðk_-_™
```

Figure 12. The program identifier in ASCII.

The actual executable's location was not calculated nor considered in scope for this paper but could be obtained using Metz's instructions (2016). This information will instead be determined another way in a following section.

5.3 Hives and RegRipper

To analyze the system and user registry hives, which contain artifacts about system and user activity, RegRipper was used ("Registry Hives," n.d.). After installing RegRipper, the next step was to use X-Ways to carve out the System, SAM, and Security hives,

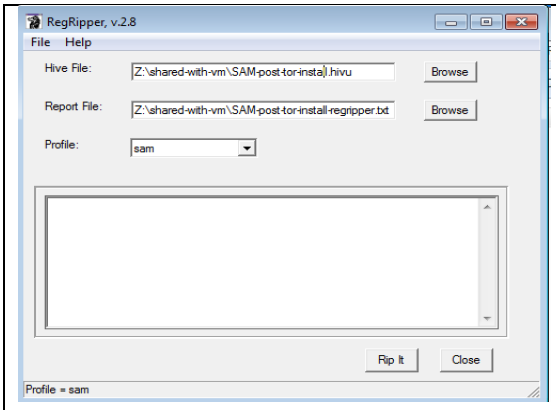


Figure 13. Regripper window showing the source hive file, the destination report location as well as the type of hive being analyzed.

both before and after installation of the Tor Browser. Running RegRipper on each hive (see Figure 13 above) then doing a Unix diff against both files, yielded that the SAM, System, Software, and Security hives had no relevant changes to indicate installation of the software.

One artifact from the SAM hive useful in correlating artifacts was the user *warren*'s Security IDentifier (SID) shown in Figure 14:

```
S-1-5-21-445630921-2900216602-2167668200-1001
```

Figure 14. warren's SID.

In analyzing the warren's NTUSER.dat the relevant entries are shown in Figure 15:

```
Fri Oct 30 07:18:23 2015 Z
     \\vmware-host\Shared Folders\shared-with-vm\torbrowser-install-5.0_en-
US.exe

Sun Oct  9 15:14:09 2016 Z
     \\vmware-host\Shared Folders\shared-with-vm\torbrowser-install-5.0_en-
US.exe (2)
```

Figure 15. NTUSER.dat entries pointing to the installer's location.

This indicated where the Tor Browser install executable was located. An analysis of the UsrClass.dat yielded nothing pertaining to the Tor Browser.

6. Memory Artifacts

At this point, a switch from filesystem artifacts is made to look at memory artifacts. Memory artifacts were obtained using the VM snapshot memory file and the Volatility suite. To perform that analysis the most current version of Volatility was obtained via the preferred installation instructions (iMHLv2, 2016). The commit ID of 33134a97 was the last committed change of the win10 profile for kernel 10586. Instead of using that kernel version, this example used commit ID of b3cde88 giving access to 0x64 tech preview 14968. The kernel version in that commit is a higher revision than the VM's version of 10586. Additionally, the volatility community plugins, used to gain access to additional tools ("Volatilityfoundation / community," 2017) were used at commit ID: 29b07e7

An example command line used for gathering the process tree using the pstree module is shown in figure 16.

```
mbp-2:volatility warren$ python2.7 vol.py \
   --plugins=~warren/Documents/community-plugins \
   --profile=Win10x64 \
   --filename=/Volumes/WD2TB/clone-of-Win8toWin10//Copy\ of\ all\ Full\
Clone\ Windows\ 8\ contents/Full\ Clone\ of\ Windows\ 8\ x86-Win8ToWin10-
Snapshot2.vmem pstree
```

Figure 16. Volatility command line options used to gather artifacts from memory images.

The following subsections show the artifacts relevant to the Tor Browser analysis captured from various modules:

6.1 getsids

Figure 17 depicts the SIDs associated with the two Process IDs (PIDs) used by the Tor Browser:

```
firefox.exe (4684): S-1-5-21-445630921-2900216602-2167668200-1001 (warren)
firefox.exe (4684): S-1-5-21-445630921-2900216602-2167668200-513 (Domain
Users)
firefox.exe (4684): S-1-1-0 (Everyone)
firefox.exe (4684): S-1-5-114 (Local Account (Member of Administrators))
firefox.exe (4684): S-1-5-21-445630921-2900216602-2167668200-1002
firefox.exe (4684): S-1-5-32-544 (Administrators)
firefox.exe (4684): S-1-5-32-545 (Users)
firefox.exe (4684): S-1-5-4 (Interactive)
firefox.exe (4684): S-1-2-1 (Console Logon (Users who are logged onto the
physical console))
firefox.exe (4684): S-1-5-11 (Authenticated Users)
firefox.exe (4684): S-1-5-15 (This Organization)
firefox.exe (4684): S-1-5-113 (Local Account)
firefox.exe (4684): S-1-5-5-0-199061 (Logon Session)
firefox.exe (4684): S-1-2-0 (Local (Users with the ability to log in
locally))
firefox.exe (4684): S-1-5-64-10 (NTLM Authentication)
firefox.exe (4684): S-1-16-8192 (Medium Mandatory Level)
tor.exe (4476): S-1-5-21-445630921-2900216602-2167668200-1001 (warren)
tor.exe (4476): S-1-5-21-445630921-2900216602-2167668200-513 (Domain Users)
tor.exe (4476): S-1-1-0 (Everyone)
tor.exe (4476): S-1-5-114 (Local Account (Member of Administrators))
tor.exe (4476): S-1-5-21-445630921-2900216602-2167668200-1002
tor.exe (4476): S-1-5-32-544 (Administrators)
tor.exe (4476): S-1-5-32-545 (Users)
tor.exe (4476): S-1-5-4 (Interactive)
tor.exe (4476): S-1-2-1 (Console Logon (Users who are logged onto the
physical console))
tor.exe (4476): S-1-5-11 (Authenticated Users)
tor.exe (4476): S-1-5-15 (This Organization)
tor.exe (4476): S-1-5-113 (Local Account)
tor.exe (4476): S-1-5-5-0-199061 (Logon Session)
tor.exe (4476): S-1-2-0 (Local (Users with the ability to log in locally))
tor.exe (4476): S-1-5-64-10 (NTLM Authentication)
tor.exe (4476): S-1-16-8192 (Medium Mandatory Level)
```

Figure 17. The SIDS used by both processes.

6.2 dlllist

Following, in Figure 18, are the DLL entries for the two known PIDs which also happen to show the installation location:

```
**********************************************************************
firefox.exe pid:   4684
Command line : "C:\Users\warren\Desktop\Tor Browser\Browser\firefox.exe"

Base                Size      LoadCount  Path
------------------  --------- ---------- ----
0x0000000000060000  0x55000   0x0        C:\Users\warren\Desktop\Tor
Browser\Browser\firefox.exe
0x00007ffc63f50000  0x1c1000  0x0        C:\WINDOWS\SYSTEM32\ntdll.dll
0x0000000057720000  0x50000   0x0        C:\WINDOWS\system32\wow64.dll
0x0000000057770000  0x7a000   0x0        C:\WINDOWS\system32\wow64win.dll
0x00000000577f0000  0x8000    0x0        C:\WINDOWS\system32\wow64cpu.dll

**********************************************************************
tor.exe pid:   4476
Command line :

Base                Size          LoadCount  Path
------------------  ------------- ---------- ----
0x0000000000880000  0x1fc000      0x0        C:\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\tor.exe
0x00007ffc63f50000  0x1c1000      0x0        C:\WINDOWS\SYSTEM32\ntdll.dll
0x0000000057720000  0x50000       0x0        C:\WINDOWS\system32\wow64.dll
0x0000000057770000  0x7a000       0x0        C:\WINDOWS\system32\wow64win.dll
0x00000000577f0000  0x8000        0x0        C:\WINDOWS\system32\wow64cpu.dll
**********************************************************************
```

Figure 18. The DLLs used in each process.

6.3 ports open from netscan

Shown in Figure 19 are the open network sockets related to the Tor activity. The Internet Protocol (IP) addresses that resolved to a name containing the word *tor* are represented as *torserver* below. The other IP addresses not directly attributable to Tor addresses are represented by *unknown*. The Tor SOCKS proxy is located on 9050/tcp and the Tor control port is located on 9051/tcp. Ports 9150 and 9151 are used by the Tor Browser Bundle (Crenshaw, 2014).

```
Offset(P)      Proto Local Address       Foreign Address  State       Pid Owner Created
0xe000177bd570 TCPv4 127.0.0.1:9151      127.0.0.1:49745  ESTABLISHED -         1
0xe000181e9d10 TCPv4 172.16.30.182:49775 unknown4:80      ESTABLISHED -         1
0xe00018892010 TCPv4 127.0.0.1:49700     127.0.0.1:9151   ESTABLISHED -         1
0xe00018c36600 TCPv4 127.0.0.1:9151      127.0.0.1:49700  ESTABLISHED -         1
0xe00018d05010 TCPv4 172.16.30.182:49756 unknown5:443     ESTABLISHED -         1
0xe00018e9ed10 TCPv4 127.0.0.1:49703     127.0.0.1:9151   ESTABLISHED -         1
0xe00019047b40 TCPv4 127.0.0.1:49754     127.0.0.1:9150   ESTABLISHED -         1
0xe000196054c0 TCPv4 127.0.0.1:49702     127.0.0.1:49701  ESTABLISHED -         1
```

```
0xe0001998a540 TCPv4 127.0.0.1:49778     127.0.0.1:9150   CLOSED      -        1
0xe000199abb00 TCPv4 127.0.0.1:49776     127.0.0.1:9150   CLOSED      -        1
0xe00019e904a0 TCPv4 127.0.0.1:49698     127.0.0.1:49697  ESTABLISHED -        1
0xe00019e99010 TCPv4 127.0.0.1:49697     127.0.0.1:49698  ESTABLISHED -        1
0xe00019edd120 TCPv4 172.16.30.182:49674 unknown6:443     ESTABLISHED -        1
0xe00019fbbd10 TCPv4 172.16.30.182:49692 unknown7:443     ESTABLISHED -        1
0xe0001a24dc00 TCPv4 127.0.0.1:9150      127.0.0.1:49754  ESTABLISHED -        1
0xe0001a2bc010 TCPv4 172.16.30.182:49725 torserver2:443   ESTABLISHED -        1
0xe0001a2c6aa0 TCPv4 127.0.0.1:9150      127.0.0.1:49778  CLOSED      -        1
0xe0001a376560 TCPv4 172.16.30.182:49734 unknown2:443     ESTABLISHED -        1
0xe0001a39e590 TCPv4 172.16.30.182:49740 unknown8:443     ESTABLISHED -        1
0xe0001a439d10 TCPv4 127.0.0.1:49753     127.0.0.1:9150   ESTABLISHED -        1
0xe0001a440c00 TCPv4 127.0.0.1:9150      127.0.0.1:49753  ESTABLISHED -        1
0xe0001a4d2160 TCPv4 127.0.0.1:9150      127.0.0.1:49776  CLOSED      -        1
0xe0001a50e850 TCPv4 172.16.30.182:49711 unknown1:443     ESTABLISHED -        1
0xe0001a529010 TCPv4 127.0.0.1:49701     127.0.0.1:49702  ESTABLISHED -        1
0xe0001a544310 TCPv4 127.0.0.1:9151      127.0.0.1:49703  ESTABLISHED -        1
0xe0001a5669e0 TCPv4 172.16.30.182:49709 torserver1:443   ESTABLISHED -        1
0xe0001a5de350 TCPv4 127.0.0.1:49745     127.0.0.1:9151   ESTABLISHED -        1
0xe0001ade1800 TCPv4 172.16.30.182:49779 unknown3:443     ESTABLISHED -        1
```

Figure 19. Ports listening on either the Tor Browser ports or the servers involved in the Tor browsing.

6.4 envars

Figure 20 shows the environment variables used by both processes. Environment variables are useful in that it will indicate where the process may look for information tailored for each system. The Path variable is particularly interesting in that for Tor, the path is the installation directory, whereas for Firefox it is not.

```
PID  Process      Block              Variable        Value
4684 firefox.exe  0x00000000001d0860 ALLUSERSPROFILE C:\ProgramData
4684 firefox.exe  0x00000000001d0860 APPDATA         C:\Users\warren\AppData\Roaming
4684 firefox.exe  0x00000000001d0860 CommonProgramFiles
       C:\Program Files\Common Files
4684 firefox.exe  0x00000000001d0860 CommonProgramFiles(x86)
       C:\Program Files (x86)\Common Files
4684 firefox.exe  0x00000000001d0860 CommonProgramW6432
       C:\Program Files\Common Files
4684 firefox.exe  0x00000000001d0860 COMPUTERNAME    WIN8-2
4684 firefox.exe  0x00000000001d0860 ComSpec         C:\WINDOWS\system32\cmd.exe
4684 firefox.exe  0x00000000001d0860 FPS_BROWSER_APP_PROFILE_STRING Internet Explorer
4684 firefox.exe  0x00000000001d0860 FPS_BROWSER_US...ROFILE_STRING Default
4684 firefox.exe  0x00000000001d0860 HOMEDRIVE       C:
4684 firefox.exe  0x00000000001d0860 HOMEPATH        \Users\warren
4684 firefox.exe  0x00000000001d0860 LOCALAPPDATA    C:\Users\warren\AppData\Local
4684 firefox.exe  0x00000000001d0860 LOGONSERVER     \\WIN8-2
4684 firefox.exe  0x00000000001d0860 NUMBER_OF_PROCESSORS          1
4684 firefox.exe  0x00000000001d0860 OS              Windows_NT
4684 firefox.exe  0x00000000001d0860 Path
       C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\Win
       dowsPowerShell\v1.0\
4684 firefox.exe  0x00000000001d0860 PATHEXT
       .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
4684 firefox.exe  0x00000000001d0860 PROCESSOR_ARCHITECTURE  AMD64
4684 firefox.exe  0x00000000001d0860 PROCESSOR_IDENTIFIER    Intel64 Family 6 Model 42
       Stepping 7, GenuineIntel
4684 firefox.exe  0x00000000001d0860 PROCESSOR_LEVEL         6
```

```
4684 firefox.exe  0x00000000001d0860 PROCESSOR_REVISION      2a07
4684 firefox.exe  0x00000000001d0860 ProgramData           C:\ProgramData
4684 firefox.exe  0x00000000001d0860 ProgramFiles          C:\Program Files
4684 firefox.exe  0x00000000001d0860 ProgramFiles(x86)     C:\Program Files (x86)
4684 firefox.exe  0x00000000001d0860 ProgramW6432          C:\Program Files
4684 firefox.exe  0x00000000001d0860 PSModulePath          C:\Program
      Files\WindowsPowerShell\Modules;C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modu
      les
4684 firefox.exe  0x00000000001d0860 PUBLIC                C:\Users\Public
4684 firefox.exe  0x00000000001d0860 SESSIONNAME           Console
4684 firefox.exe  0x00000000001d0860 SystemDrive           C:
4684 firefox.exe  0x00000000001d0860 SystemRoot            C:\WINDOWS
4684 firefox.exe  0x00000000001d0860 TEMP
      C:\Users\warren\AppData\Local\Temp
4684 firefox.exe  0x00000000001d0860 TMP
      C:\Users\warren\AppData\Local\Temp
4684 firefox.exe  0x00000000001d0860 USERDOMAIN                      win8-2
4684 firefox.exe  0x00000000001d0860 USERDOMAIN_ROAMINGPROFILE       win8-2
4684 firefox.exe  0x00000000001d0860 USERNAME                        warren
4684 firefox.exe  0x00000000001d0860 USERPROFILE                     C:\Users\warren
4684 firefox.exe  0x00000000001d0860 windir                          C:\WINDOWS
4476 tor.exe      0x00000000001e0860 ALLUSERSPROFILE                 C:\ProgramData
4476 tor.exe      0x00000000001e0860 APPDATA
      C:\Users\warren\AppData\Roaming
4476 tor.exe      0x00000000001e0860 CommonProgramFiles
      C:\Program Files\Common Files
4476 tor.exe      0x00000000001e0860 CommonProgramFiles(x86)
      C:\Program Files (x86)\Common Files
4476 tor.exe      0x00000000001e0860 CommonProgramW6432
      C:\Program Files\Common Files
4476 tor.exe      0x00000000001e0860 COMPUTERNAME                    WIN8-2
4476 tor.exe      0x00000000001e0860 ComSpec
      C:\WINDOWS\system32\cmd.exe
4476 tor.exe      0x00000000001e0860 FPS_BROWSER_APP_PROFILE_STRING Internet Explorer
4476 tor.exe      0x00000000001e0860 FPS_BROWSER_US...ROFILE_STRING Default
4476 tor.exe      0x00000000001e0860 HOMEDRIVE                       C:
4476 tor.exe      0x00000000001e0860 HOMEPATH                        \Users\warren
4476 tor.exe      0x00000000001e0860 LOCALAPPDATA
      C:\Users\warren\AppData\Local
4476 tor.exe      0x00000000001e0860 LOGONSERVER                     \\WIN8-2
4476 tor.exe      0x00000000001e0860 MOZ_NO_REMOTE                   1
4476 tor.exe      0x00000000001e0860 NUMBER_OF_PROCESSORS            1
4476 tor.exe      0x00000000001e0860 OS                              Windows_NT
4476 tor.exe      0x00000000001e0860 Path
      C:\Users\warren\Desktop\Tor
      Browser\Browser\TorBrowser\Tor;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System
      32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\
4476 tor.exe      0x00000000001e0860 PATHEXT
      .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
4476 tor.exe      0x00000000001e0860 PROCESSOR_ARCHITECTURE          AMD64
4476 tor.exe      0x00000000001e0860 PROCESSOR_IDENTIFIER            Intel64 Family 6
      Model 42 Stepping 7, GenuineIntel
4476 tor.exe      0x00000000001e0860 PROCESSOR_LEVEL                 6
4476 tor.exe      0x00000000001e0860 PROCESSOR_REVISION              2a07
4476 tor.exe      0x00000000001e0860 ProgramData                C:\ProgramData
4476 tor.exe      0x00000000001e0860 ProgramFiles               C:\Program Files
4476 tor.exe      0x00000000001e0860 ProgramFiles(x86)          C:\Program Files (x86)
4476 tor.exe      0x00000000001e0860 ProgramW6432               C:\Program Files
4476 tor.exe      0x00000000001e0860 PSModulePath
      C:\Program Files\WindowsPowerShell\Modules;
      C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules
4476 tor.exe      0x00000000001e0860 PUBLIC                      C:\Users\Public
4476 tor.exe      0x00000000001e0860 SESSIONNAME                 Console
4476 tor.exe      0x00000000001e0860 SystemDrive                 C:
```

```
4476 tor.exe      0x00000000001e0860 SystemRoot                  C:\WINDOWS
4476 tor.exe      0x00000000001e0860 TEMP
      C:\Users\warren\AppData\Local\Temp
4476 tor.exe      0x00000000001e0860 TMP
      C:\Users\warren\AppData\Local\Temp
4476 tor.exe      0x00000000001e0860 USERDOMAIN                  win8-2
4476 tor.exe      0x00000000001e0860 USERDOMAIN_ROAMINGPROFILE   win8-2
4476 tor.exe      0x00000000001e0860 USERNAME                    warren
4476 tor.exe      0x00000000001e0860 USERPROFILE                 C:\Users\warren
4476 tor.exe      0x00000000001e0860 windir                      C:\WINDOWS
```

Figure 20. The PATH environment variables where the process will look for executables. Also shown are other variables which may be of interest to the investigator.

6.5 cmdline

The command line for both processes assist in identifying the installation location, except for Tor in this case, is shown in Figure 21:

```
************************************************************************
firefox.exe pid:   4684
Command line : "C:\Users\warren\Desktop\Tor Browser\Browser\firefox.exe"
************************************************************************
tor.exe pid:   4476
Command line :
************************************************************************
```

Figure 21. The command line used by each process. Note that the tor executable is not displaying any command line.

6.6 dumpfiles

Unfortunately, due to time constraints it was not feasible to dump the individual files from the memory image to see what their contents were. The contents of the individual files possibly would show more artifacts about what was being browsed at the time of the snapshot. For completeness, they are listed in Appendix A.

6.7 vmem privs

The results from the Virtual Memory (vmem) privileges module are located in Appendix B due to the numerous entries.

6.8 vadtree

For both processes, the Virtual Address Descriptor (VAD) ranges can be seen in Figure 22:

```
**************************************************************************
Pid:   4476
 0x0000000057770000 - 0x00000000577e9fff
…
**************************************************************************
Pid:   4684
 0x0000000057720000 - 0x000000005776ffff
```

Figure 22. The VAD ranges in memory held by each process.

6.9 vadinfo

The vadinfo module produced information, specifically of interest is the starting and ending memory address range, of each VAD entry in the vadtree but due to the numerous entries, they are located in Appendix C.

6.10 Failed modules

Unfortunately, several volatility modules failed to parse the memory image and resulted in errors which returned with no useful output. The modules which failed were: psxview, shellbags, sockets, services, userassist, and devicetree. The apihooks module did not fail but instead returned no data, so the suspicion is that the module failed as well.

6 Anti-Forensics

Mike Peery outlines several design requirements for the Tor Browser which are "that [it] defends against both network and local forensic adversaries" (Perry, 2015, para. 8). For instance, "the browser MUST NOT write any information that is derived from or that reveals browsing activity to the disk" (Peery, 2015, para. 15). This statement was confirmed by the fact that while carving and performing cookie, history, and cache recover against Firefox's artifacts, nothing was found written to disk. An attempt using tools such as MZHistoryView, MZCacheView and MZCookieView from Nirsoft did not provide any results as the author could not get the tools to read the proper DLLs.

The only on-disk artifact found was when a VM snapshot was taken during a connection to Tor with the user surfing to google.com and bookmarking the site. The places.sqlite on-disk did contain the google.com location visited, as shown in Figure 23:

```
root# echo '.dump' | sqlite3 places.sqlite > places.txt
root# more places.txt
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
```

```
CREATE TABLE moz_places (   id INTEGER PRIMARY KEY, url LONGVARCHAR, title
LONGVARCHAR, rev_host LONGVARCHAR, visit_count INTEGER DEFAULT 0, hidden
INTEGER DEFAULT 0 NOT NULL, typed INTEGER DEFAULT 0 NOT NULL, favicon_id
INTEGER, frecency INTEGER DEFAULT -1 NOT NULL, last_visit_date INTEGER , guid
TEXT, foreign_count INTEGER DEFAULT 0 NOT NULL);
INSERT INTO "moz_places"
VALUES(1,'https://www.torproject.org/',NULL,'gro.tcejorprot.www.',0,0,0,1,140
,NULL,'sKr_fL_2R5qK',1);
INSERT INTO "moz_places"
VALUES(2,'https://blog.torproject.org/',NULL,'gro.tcejorprot.golb.',0,0,0,2,1
40,NULL,'FChOdf-VbdEN',1);
INSERT INTO "moz_places"
VALUES(3,'place:sort=8&maxResults=10',NULL,NULL,0,1,0,NULL,0,NULL,'yrr2EEMbCO
mE',1);
INSERT INTO "moz_places"
VALUES(4,'place:folder=BOOKMARKS_MENU&folder=UNFILED_BOOKMARKS&folder=TOOLBAR
&queryType=1&sort=12&maxResults=10&excludeQueries=1',NULL,NULL,0,1,0,NULL,0,N
ULL,'Gx39ziCQ-qgx',1);
INSERT INTO "moz_places"
VALUES(5,'place:type=6&sort=14&maxResults=10',NULL,NULL,0,1,0,NULL,0,NULL,'Bo
bBb4OVn6Ot',1);
INSERT INTO "moz_places"
VALUES(6,'https://www.google.com/',NULL,'moc.elgoog.www.',0,1,0,NULL,-
1,NULL,'ATecMqhOR884',1);
CREATE TABLE moz_historyvisits (  id INTEGER PRIMARY KEY, from_visit INTEGER,
place_id INTEGER, visit_date INTEGER, visit_type INTEGER, session INTEGER);
CREATE TABLE moz_inputhistory (  place_id INTEGER NOT NULL, input LONGVARCHAR
NOT NULL, use_count INTEGER, PRIMARY KEY (place_id, input));
/**** ERROR: (11) database disk image is malformed *****/
/**** ERROR: (11) database disk image is malformed *****/
CREATE TABLE moz_hosts (  id INTEGER PRIMARY KEY, host TEXT NOT NULL UNIQUE,
frecency INTEGER, typed INTEGER NOT NULL DEFAULT 0, prefix TEXT);
INSERT INTO "moz_hosts" VALUES(1,'torproject.org',140,0,NULL);
INSERT INTO "moz_hosts" VALUES(2,'blog.torproject.org',140,0,NULL);
INSERT INTO "moz_hosts" VALUES(3,'google.com',-1,0,NULL);
CREATE TABLE moz_bookmarks (  id INTEGER PRIMARY KEY, type INTEGER, fk
INTEGER DEFAULT NULL, parent INTEGER, position INTEGER, title LONGVARCHAR,
keyword_id INTEGER, folder_type TEXT, dateAdded INTEGER, lastModified
INTEGER, guid TEXT);
INSERT INTO "moz_bookmarks"
VALUES(1,2,NULL,0,0,'',NULL,NULL,1476026354653000,1476026354653000,'root_____
___');
INSERT INTO "moz_bookmarks" VALUES(2,2,NULL,1,0,'Bookmarks
Menu',NULL,NULL,1476026354653000,1483030789911000,'menu________');
INSERT INTO "moz_bookmarks" VALUES(3,2,NULL,1,1,'Bookmarks
Toolbar',NULL,NULL,1476026354653000,1476026355340000,'toolbar_____');
INSERT INTO "moz_bookmarks"
VALUES(4,2,NULL,1,2,'Tags',NULL,NULL,1476026354653000,1476026354653000,'tags_
_______');
INSERT INTO "moz_bookmarks" VALUES(5,2,NULL,1,3,'Unsorted
Bookmarks',NULL,NULL,1476026354653000,1476026355325000,'unfiled_____');
INSERT INTO "moz_bookmarks" VALUES(6,1,1,3,1,'Learn more about
Tor',NULL,NULL,1476026355340000,1476026355340000,'NaiD2PNu7Z89');
INSERT INTO "moz_bookmarks" VALUES(7,1,2,3,2,'The Tor
Blog',NULL,NULL,1476026355340000,1476026355340000,'IxpDbP40F0dD');
INSERT INTO "moz_bookmarks"
VALUES(8,3,NULL,2,2,NULL,NULL,NULL,1476026355340000,1476026355340000,'9ZBE3mo
BwrcJ');
```

Aron Warren, aronwarren@gmail.com

```
INSERT INTO "moz_bookmarks" VALUES(9,1,3,3,0,'Most
Visited',NULL,NULL,1476026355340000,1476026355340000,'dhzdHmXxjAEq');
INSERT INTO "moz_bookmarks" VALUES(10,1,4,2,0,'Recently
Bookmarked',NULL,NULL,1476026355340000,1476026355340000,'5FNEurOmGncq');
INSERT INTO "moz_bookmarks" VALUES(11,1,5,2,1,'Recent
Tags',NULL,NULL,1476026355340000,1476026355340000,'V2zHNMYCX3Us');
INSERT INTO "moz_bookmarks"
VALUES(12,1,6,2,3,'Google',NULL,NULL,1483030789911000,1483030789911000,'at8i3
CDAFjAX');
CREATE TABLE moz_bookmarks_roots (  root_name VARCHAR(16) UNIQUE, folder_id
INTEGER);
```

Figure 23. The contents of places.sqlite showing locations browsed and bookmarks set.

Having the browsing history stored on-disk, albeit located solely inside the Tor installation directory, in and of itself is a trade-off between security and functionality. To mitigate this concern and others, tor_opsec (n.d.) gives a full list of steps for proper Operational Security (OPSEC) when using Tor too detailed and numerous to outline here. They are necessary if the end-user is going to maintain maximum anonymity while using Tor.

7 Conclusion

This paper began with an overview of The Onion Router (Tor) project and described the subsequent creation of the Tor Browser. A detailed overview of a Tor Browser installation and forensic methodology was provided so that the reader could recreate this analysis. After carving a prefetch file, system and user hives, as well as Mozilla on-disk files, the Tor project's goal of leaving a minimal footprint on-disk is confirmed by the above filesystem analysis. Memory analysis used provided various artifacts pointing to the installation location of the Tor Browser in addition to Internet locations the browser was connected to. In the end, using the above analysis, dozens of pointers to artifacts is provided to assist other investigators in identifying the location and use of the Tor Browser. Future research using reverse engineering techniques to dump memory locations may prove useful in identifying activity occurring when the third VM snapshot was taken.

References

Ailanthus. (2015, November 11). Ethical Tor Research: Guidelines. Retrieved from https://blog.torproject.org/blog/ethical-tor-research-guidelines

Crenshaw, A. (2014, December 29). Dropping Docs on Darknets: How People Got Caught [video]. Retrieved from https://www.youtube.com/watch?v=eQ2OZKitRwc

Hal9000. (2016). 8 Tools to Track Registry and File Changes by Comparing Before and After Snapshots. Retrieved from https://www.raymond.cc/blog/tracking-registry-and-files-changes-when-installing-software-in-windows/

How to verify signatures for packages. (n.d.). Retrieved from https://www.torproject.org/docs/verifying-signatures.html.en

iMHLv2. (2016, September 28). Installation. Retrieved from https://github.com/volatilityfoundation/volatility/wiki/Installation#_jmp0

Metz, J. (2016, November). Windows Prefetch File (PF) Format. Retrieved from https://github.com/libyal/libscca/blob/master/documentation/Windows%20Prefetch%20File%20(PF)%20format.asciidoc

Peery, M. (2014, Mar 12). Ticket 11193: Change Tor Browser Bundle to Tor Browser in package strings, download pages, and docs. Retrieved from https://trac.torproject.org/projects/tor/ticket/11193

Peery, M. (2015, May 6). The Design and Implementation of the Tor Browser [DRAFT]. Retrieved from https://www.torproject.org/projects/torbrowser/design/

Phobos. (2008, April 11). March 2008 Progress Report. Retrieved from https://blog.torproject.org/blog/march-2008-progress-report

Picasso, F. (2015a, June 22). A first look at Windows 10 prefetch files. Retrieved from http://blog.digital-forensics.it/2015/06/a-first-look-at-windows-10-prefetch.html

Picasso, F. (2015b, July 28). RealityNet / hotoloti. Retrieved from https://github.com/RealityNet/hotoloti

Prefetch. (2016, April 7). Retrieved from http://www.forensicswiki.org/wiki/Prefetch

Registry Hives. (n.d.). Retrieved from https://msdn.microsoft.com/en-us/library/windows/desktop/ms724877(v=vs.85).aspx

Regshot. (2016, November 4). Retrieved from https://sourceforge.net/projects/regshot/

Syverson, P. (2005a). Onion Routing Executive Summary. Retrieved from https://www.onion-router.net/Summary.html

Syverson, P. (2005b). Onion Routing Brief Selected History. Retrieved from https://www.onion-router.net/History.html

Tor FAQ. (n.d.). Retrieved from https://www.torproject.org/docs/faq

Tor_opsec. (n.d.) Here is a quick guide to using Tor + OPSEC. Retrieved from https://www.reddit.com/r/TOR/comments/3dq1pg/here_is_a_quick_guide_to_using_tor_opsec/

Volatilityfoundation / community. (n.d). Retrieved from https://github.com/volatilityfoundation/community.git

What is Tor Browser. (n.d.). Retrieved from https://www.torproject.org/projects/torbrowser.html.en#downloads

Windows Prefetch File Format. (2016, April 5). Retrieved from http://www.forensicswiki.org/wiki/Windows_Prefetch_File_Format

Appendix A:

The dumpfiles from subsection 6.6 are in Figure 24:

```
ImageSectionObject 0xffffe0001898d850   4684
\Device\HarddiskVolume2\Users\warren\Desktop\Tor Browser\Browser\firefox.exe
DataSectionObject
0xffffe0001898d850   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\firefox.exe
DataSectionObject
0xffffe00019b68720   4684   \Device\HarddiskVolume2\Windows\SysWOW64\en-
US\UIAutomationCore.dll.mui
DataSectionObject
0xffffe00017d41090   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite-shm
DataSectionObject
0xffffe0001a577090   4684   \Device\HarddiskVolume2\Windows\SysWOW64\en-
US\rasdlg.dll.mui
DataSectionObject 0xffffe0001728bbf0   4684   None
DataSectionObject 0xffffe00019001b90   4684   None
DataSectionObject
0xffffe000195a6ba0   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Data\Browser\profile.default\webappsstore.sqlite-shm
DataSectionObject 0xffffe0001a1b7a10   4684   None
DataSectionObject 0xffffe0001904d270   4684   None
DataSectionObject 0xffffe000191e3240   4684   None
DataSectionObject
0xffffe00019ecff20   4684   \Device\HarddiskVolume2\Windows\SysWOW64\en-
US\d2d1.dll.mui
ImageSectionObject
0xffffe0001a5aa090   4684   \Device\HarddiskVolume2\Windows\SysWOW64\rasman.dll
ImageSectionObject
0xffffe000191db520   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\softokn3.dll
DataSectionObject
0xffffe000191db520   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\softokn3.dll
ImageSectionObject
0xffffe0001a591090   4684   \Device\HarddiskVolume2\Windows\SysWOW64\pcacli.dll
ImageSectionObject
0xffffe00019571880   4684   \Device\HarddiskVolume2\Windows\SysWOW64\d3d10warp.dll
ImageSectionObject
0xffffe0001a590ac0   4684   \Device\HarddiskVolume2\Windows\SysWOW64\mscms.dll
ImageSectionObject 0xffffe00018a75200   4684   None
ImageSectionObject
0xffffe00018db2990   4684   \Device\HarddiskVolume2\Windows\SysWOW64\d2d1.dll
ImageSectionObject
0xffffe000189bef20   4684   \Device\HarddiskVolume2\Windows\SysWOW64\devrtl.dll
ImageSectionObject
0xffffe0001a1e4550   4684   \Device\HarddiskVolume2\Windows\SysWOW64\sfc_os.dll
ImageSectionObject
0xffffe000189f9f20   4684   \Device\HarddiskVolume2\Windows\SysWOW64\Wpc.dll
ImageSectionObject
0xffffe0001a189f20   4684   \Device\HarddiskVolume2\Windows\SysWOW64\ucrtbase.dll
ImageSectionObject
0xffffe0001a5a4b90   4684   \Device\HarddiskVolume2\Windows\SysWOW64\msvcp_win.dll
ImageSectionObject
0xffffe00017c949d0   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\nssckbi.dll
DataSectionObject
0xffffe00017c949d0   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\nssckbi.dll
```

```
ImageSectionObject
0xffffe00018919360   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\freebl3.dll
DataSectionObject
0xffffe00018919360   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\freebl3.dll
ImageSectionObject
0xffffe00019bfe710   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\xul.dll
ImageSectionObject
0xffffe0001a3c8f20   4684   \Device\HarddiskVolume2\Windows\SysWOW64\winrnr.dll
ImageSectionObject
0xffffe00017c8d3e0   4684   \Device\HarddiskVolume2\Windows\SysWOW64\ntmarta.dll
ImageSectionObject
0xffffe0001894da80   4684   \Device\HarddiskVolume2\Windows\SysWOW64\wshbth.dll
ImageSectionObject
0xffffe0001a5a5760   4684   \Device\HarddiskVolume2\Windows\SysWOW64\nlaapi.dll
ImageSectionObject
0xffffe0001a5a4090   4684   \Device\HarddiskVolume2\Windows\SysWOW64\DWrite.dll
ImageSectionObject
0xffffe0001892ed00   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\browser\components\browsercomps.dll
DataSectionObject
0xffffe0001892ed00   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\browser\components\browsercomps.dll
ImageSectionObject
0xffffe0001a53c090   4684   \Device\HarddiskVolume2\Windows\SysWOW64\NapiNSP.dll
ImageSectionObject
0xffffe0001a035ab0   4684   \Device\HarddiskVolume2\Windows\SysWOW64\pnrpnsp.dll
ImageSectionObject
0xffffe0001a5aba60   4684   \Device\HarddiskVolume2\Windows\SysWOW64\mprapi.dll
ImageSectionObject
0xffffe0001998c980   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\mozalloc.dll
DataSectionObject
0xffffe0001998c980   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\mozalloc.dll
ImageSectionObject
0xffffe000194ccf20   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\mozglue.dll
DataSectionObject
0xffffe000194ccf20   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\mozglue.dll
ImageSectionObject
0xffffe00019f54820   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\nss3.dll
DataSectionObject
0xffffe00019f54820   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\nss3.dll
ImageSectionObject
0xffffe0001a5a1300   4684   \Device\HarddiskVolume2\Windows\SysWOW64\rtutils.dll
ImageSectionObject
0xffffe0001a58ef20   4684   \Device\HarddiskVolume2\Windows\SysWOW64\dpapi.dll
ImageSectionObject
0xffffe0001a58d090   4684   \Device\HarddiskVolume2\Windows\SysWOW64\rasdlg.dll
ImageSectionObject
0xffffe00018f1a4b0   4684   \Device\HarddiskVolume2\Windows\SysWOW64\wtsapi32.dll
ImageSectionObject
0xffffe00017c7ecd0   4684   \Device\HarddiskVolume2\Windows\SysWOW64\rasapi32.dll
ImageSectionObject
0xffffe0001a3e0350   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\ssl3.dll
DataSectionObject
0xffffe0001a3e0350   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
```

```
Browser\Browser\ssl3.dll
ImageSectionObject
0xffffe0001a50b360   4684   \Device\HarddiskVolume2\Windows\SysWOW64\msimg32.dll
ImageSectionObject
0xffffe000172cdb10   4684   \Device\HarddiskVolume2\Windows\SysWOW64\usp10.dll
ImageSectionObject
0xffffe0001a434cd0   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\nssutil3.dll
DataSectionObject
0xffffe0001a434cd0   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\nssutil3.dll
ImageSectionObject
0xffffe000194abe80   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\smime3.dll
DataSectionObject
0xffffe000194abe80   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\smime3.dll
ImageSectionObject
0xffffe0001a2e1280   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\nspr4.dll
DataSectionObject
0xffffe0001a2e1280   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\nspr4.dll
ImageSectionObject
0xffffe00019bee090   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\msvcr100.dll
DataSectionObject
0xffffe00019bee090   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\msvcr100.dll
ImageSectionObject
0xffffe000191ee4b0   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\plds4.dll
DataSectionObject
0xffffe000191ee4b0   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\plds4.dll
ImageSectionObject
0xffffe0001a38a090   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\plc4.dll
DataSectionObject
0xffffe0001a38a090   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\plc4.dll
ImageSectionObject
0xffffe00019b58a20   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\mozsqlite3.dll
DataSectionObject
0xffffe00019b58a20   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\mozsqlite3.dll
ImageSectionObject
0xffffe0001947af20   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\libssp-0.dll
DataSectionObject
0xffffe0001947af20   4684   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\libssp-0.dll
ImageSectionObject
0xffffe000192fc460   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\tor.exe
DataSectionObject
0xffffe000192fc460   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\tor.exe
ImageSectionObject
0xffffe000193723b0   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\libssp-0.dll
DataSectionObject
0xffffe000193723b0   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
```

```
Browser\Browser\TorBrowser\Tor\libssp-0.dll
ImageSectionObject
0xffffe00019be2090   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\ssleay32.dll
DataSectionObject
0xffffe00019be2090   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\ssleay32.dll
ImageSectionObject
0xffffe00019353da0   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\libgcc_s_sjlj-1.dll
DataSectionObject
0xffffe00019353da0   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\libgcc_s_sjlj-1.dll
ImageSectionObject
0xffffe00018c6ab40   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\zlib1.dll
DataSectionObject
0xffffe00018c6ab40   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\zlib1.dll
ImageSectionObject
0xffffe00017c67bc0   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\libeay32.dll
DataSectionObject
0xffffe00017c67bc0   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\libeay32.dll
ImageSectionObject
0xffffe000198d0cf0   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\libevent-2-0-5.dll
DataSectionObject
0xffffe000198d0cf0   4476   \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\libevent-2-0-5.dll
```

Figure 24. The dump file locations are the locations of where the files in memory are located.

Appendix B:

Artifacts found from the vmem privs module from Volatility are shown in Figure 25.

```
4684 firefox.exe    2 SeCreateTokenPrivilege          Create a token object
4684 firefox.exe    3 SeAssignPrimaryTokenPrivilege   Replace a process-level token
4684 firefox.exe    4 SeLockMemoryPrivilege           Lock pages in memory
4684 firefox.exe    5 SeIncreaseQuotaPrivilege        Increase quotas
4684 firefox.exe    6 SeMachineAccountPrivilege       Add workstations to the domain
4684 firefox.exe    7 SeTcbPrivilege                  Act as part of the operating system
4684 firefox.exe    8 SeSecurityPrivilege             Manage auditing and security log
4684 firefox.exe    9 SeTakeOwnershipPrivilege        Take ownership of files/objects
4684 firefox.exe   10 SeLoadDriverPrivilege           Load and unload device drivers
4684 firefox.exe   11 SeSystemProfilePrivilege        Profile system performance
4684 firefox.exe   12 SeSystemtimePrivilege           Change the system time
4684 firefox.exe   13 SeProfileSingleProcessPrivilege Profile a single process
4684 firefox.exe   14 SeIncreaseBasePriorityPrivilege Increase scheduling priority
4684 firefox.exe   15 SeCreatePagefilePrivilege       Create a pagefile
4684 firefox.exe   16 SeCreatePermanentPrivilege      Create permanent shared objects
4684 firefox.exe   17 SeBackupPrivilege               Backup files and directories
4684 firefox.exe   18 SeRestorePrivilege              Restore files and directories
4684 firefox.exe   19 SeShutdownPrivilege    Present  Shut down the system
4684 firefox.exe   20 SeDebugPrivilege                Debug programs
4684 firefox.exe   21 SeAuditPrivilege                Generate security audits
4684 firefox.exe   22 SeSystemEnvironmentPrivilege    Edit firmware environment values
4684 firefox.exe   23 SeChangeNotifyPrivilege   Present,Enabled,Default  Receive notifications of
changes to files or directories
4684 firefox.exe   24 SeRemoteShutdownPrivilege       Force shutdown from a remote system
4684 firefox.exe   25 SeUndockPrivilege      Present  Remove computer from docking station
4684 firefox.exe   26 SeSyncAgentPrivilege            Synch directory service data
4684 firefox.exe   27 SeEnableDelegationPrivilege     Enable user accounts to be trusted for
delegation
4684 firefox.exe   28 SeManageVolumePrivilege         Manage the files on a volume
4684 firefox.exe   29 SeImpersonatePrivilege          Impersonate a client after authentication
4684 firefox.exe   30 SeCreateGlobalPrivilege        Create global objects
4684 firefox.exe   31 SeTrustedCredManAccessPrivilege Access Credential Manager as a trusted
caller
4684 firefox.exe   32 SeRelabelPrivilege              Modify the mandatory integrity level of an
object
4684 firefox.exe   33 SeIncreaseWorkingSetPrivilege  Present  Allocate more memory for user
applications
4684 firefox.exe   34 SeTimeZonePrivilege            Present  Adjust the time zone of the
computer's internal clock
4684 firefox.exe   35 SeCreateSymbolicLinkPrivilege   Required to create a symbolic link
4476 tor.exe        2 SeCreateTokenPrivilege          Create a token object
4476 tor.exe        3 SeAssignPrimaryTokenPrivilege   Replace a process-level token
4476 tor.exe        4 SeLockMemoryPrivilege           Lock pages in memory
4476 tor.exe        5 SeIncreaseQuotaPrivilege        Increase quotas
4476 tor.exe        6 SeMachineAccountPrivilege       Add workstations to the domain
4476 tor.exe        7 SeTcbPrivilege                  Act as part of the operating system
4476 tor.exe        8 SeSecurityPrivilege             Manage auditing and security log
4476 tor.exe        9 SeTakeOwnershipPrivilege        Take ownership of files/objects
4476 tor.exe       10 SeLoadDriverPrivilege           Load and unload device drivers
4476 tor.exe       11 SeSystemProfilePrivilege        Profile system performance
4476 tor.exe       12 SeSystemtimePrivilege           Change the system time
4476 tor.exe       13 SeProfileSingleProcessPrivilege Profile a single process
4476 tor.exe       14 SeIncreaseBasePriorityPrivilege Increase scheduling priority
4476 tor.exe       15 SeCreatePagefilePrivilege       Create a pagefile
4476 tor.exe       16 SeCreatePermanentPrivilege      Create permanent shared objects
4476 tor.exe       17 SeBackupPrivilege               Backup files and directories
4476 tor.exe       18 SeRestorePrivilege              Restore files and directories
4476 tor.exe       19 SeShutdownPrivilege            Present   Shut down the system
4476 tor.exe       20 SeDebugPrivilege                Debug programs
4476 tor.exe       21 SeAuditPrivilege                Generate security audits
4476 tor.exe       22 SeSystemEnvironmentPrivilege    Edit firmware environment values
4476 tor.exe       23 SeChangeNotifyPrivilege        Present,Enabled,Default  Receive
```

```
notifications of changes to files or directories
4476 tor.exe       24 SeRemoteShutdownPrivilege          Force shutdown from a remote system
4476 tor.exe       25 SeUndockPrivilege                 Present      Remove computer from docking
station
4476 tor.exe       26 SeSyncAgentPrivilege               Synch directory service data
4476 tor.exe       27 SeEnableDelegationPrivilege        Enable user accounts to be trusted for
delegation
4476 tor.exe       28 SeManageVolumePrivilege            Manage the files on a volume
4476 tor.exe       29 SeImpersonatePrivilege             Impersonate a client after
authentication
4476 tor.exe       30 SeCreateGlobalPrivilege            Create global objects
4476 tor.exe       31 SeTrustedCredManAccessPrivilege    Access Credential Manager as a trusted
caller
4476 tor.exe       32 SeRelabelPrivilege                 Modify the mandatory integrity level of
an object
4476 tor.exe       33 SeIncreaseWorkingSetPrivilege     Present  Allocate more memory for user
applications
4476 tor.exe       34 SeTimeZonePrivilege               Present     Adjust the time zone of the
computer's internal clock
4476 tor.exe       35 SeCreateSymbolicLinkPrivilege     Required to create a symbolic link
```

Figure 25. The privileges granted to each process.

Appendix C:

This section contains the relevant artifacts found from the vadinfo module of Volatility:

```
VAD node @ 0xffffe000189a78b0 Start 0x0000000000060000 End 0x00000000000b4fff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe000189f6830 Segment ffffc000f9636b90
NumberOfSectionReferences:          1 NumberOfPfnReferences:          39
NumberOfMappedViews:                1 NumberOfUserReferences:          2
Control Flags: File: 1, Image: 1
FileObject @ffffe0001898d850, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\firefox.exe
First prototype PTE: ffffc000f3f0c910 Last contiguous PTE: ffffc000f3f0cbb0
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe000175ba930 Start 0x0000000000b80000 End 0x0000000000b87fff Tag Vad
Flags: Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone
ControlArea @ffffe00018884490 Segment ffffc000fa3efce0
NumberOfSectionReferences:          1 NumberOfPfnReferences:           8
NumberOfMappedViews:                1 NumberOfUserReferences:          2
Control Flags: File: 1
FileObject @ffffe00017d41090, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Data\Browser\profile.default\places.sqlite-shm
First prototype PTE: ffffc000f0eff8d0 Last contiguous PTE: ffffc000f0eff908
Flags2: Inherit: 1, TrimBehind: 1

VAD node @ 0xffffe00019fcc750 Start 0x0000000007810000 End 0x0000000007817fff Tag Vad
Flags: Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone
ControlArea @ffffe00018e7ee00 Segment ffffc000fb6d9b00
NumberOfSectionReferences:          1 NumberOfPfnReferences:           8
NumberOfMappedViews:                1 NumberOfUserReferences:          2
Control Flags: File: 1
FileObject @ffffe000195a6ba0, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Data\Browser\profile.default\webappsstore.sqlite-shm
First prototype PTE: ffffc000f4d3e820 Last contiguous PTE: ffffc000f4d3e858
Flags2: Inherit: 1, TrimBehind: 1

(Note: X-Ways was not able to find this file in the disk image.)

VAD node @ 0xffffe00017d13930 Start 0x0000000069ad0000 End 0x0000000069b48fff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00019c18790 Segment ffffc000f306c740
NumberOfSectionReferences:          0 NumberOfPfnReferences:         114
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe00017c949d0, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\nssckbi.dll
First prototype PTE: ffffc000f4fe9ad0 Last contiguous PTE: ffffc000f4fe9e90
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe00019b30ab0 Start 0x0000000069b50000 End 0x0000000069bc0fff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00019c248a0 Segment ffffc000f4d07760
NumberOfSectionReferences:          0 NumberOfPfnReferences:          82
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe00018919360, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\freebl3.dll
```

```
First prototype PTE: ffffc000f50b6c70 Last contiguous PTE: ffffc000f50b6ff0
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe00019409170 Start 0x0000000069e90000 End 0x000000006cfdffff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00017de06e0 Segment ffffc000f9668290
NumberOfSectionReferences:          0 NumberOfPfnReferences:        6355
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe00019bfe710, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\xul.dll
First prototype PTE: ffffc000fbc76000 Last contiguous PTE: ffffc000fbc8ea78
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a08e960 Start 0x000000006e8a0000 End 0x000000006e8dafff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00018902d10 Segment ffffc000f4a5fb90
NumberOfSectionReferences:          0 NumberOfPfnReferences:          33
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe0001892ed00, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\browser\components\browsercomps.dll
First prototype PTE: ffffc000f4e3d920 Last contiguous PTE: ffffc000f4e3daf0
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a4d6280 Start 0x000000006fb30000 End 0x000000006fb3bfff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00019ef8ae0 Segment ffffc000f54135f0
NumberOfSectionReferences:          0 NumberOfPfnReferences:          10
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe0001998c980, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\mozalloc.dll
First prototype PTE: ffffc000f4e6a880 Last contiguous PTE: ffffc000f4e6a8d8
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe000177b5b20 Start 0x000000006ee00000 End 0x000000006eedcfff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe000194e2870 Segment ffffc000f98c0b20
NumberOfSectionReferences:          0 NumberOfPfnReferences:          27
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe000194ccf20, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\mozglue.dll
First prototype PTE: ffffc000f5020910 Last contiguous PTE: ffffc000f5020ff0
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a4c9190 Start 0x000000006eb40000 End 0x000000006ec2dfff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe000177b3010 Segment ffffc000f5928800
NumberOfSectionReferences:          0 NumberOfPfnReferences:         164
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe00019f54820, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\nss3.dll
First prototype PTE: ffffc000f4fec890 Last contiguous PTE: ffffc000f4fecff8
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a097100 Start 0x000000006ed20000 End 0x000000006ed54fff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
```

```
ControlArea @ffffe00017d2dbb0 Segment ffffc000f55311c0
NumberOfSectionReferences:          0 NumberOfPfnReferences:          46
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe0001a3e0350, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\ssl3.dll
First prototype PTE: ffffc000fbaa0e50 Last contiguous PTE: ffffc000fbaa0ff0
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a17f780 Start 0x000000006ed60000 End 0x000000006ed86fff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00019beb750 Segment ffffc000f94322a0
NumberOfSectionReferences:          0 NumberOfPfnReferences:          18
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe000194abe80, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\smime3.dll
First prototype PTE: ffffc000f4fbe960 Last contiguous PTE: ffffc000f4fbea90
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a58e6a0 Start 0x000000006edc0000 End 0x000000006edf5fff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00017dca470 Segment ffffc000f303b990
NumberOfSectionReferences:          0 NumberOfPfnReferences:          46
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe0001a2e1280, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\nspr4.dll
First prototype PTE: ffffc000f4fe9910 Last contiguous PTE: ffffc000f4fe9ab8
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a4c0b00 Start 0x000000006f510000 End 0x000000006f5cdfff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00019b82a00 Segment ffffc000f59f4a60
NumberOfSectionReferences:          0 NumberOfPfnReferences:          77
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe00019bee090, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\msvcr100.dll
First prototype PTE: ffffc000f4cf5a10 Last contiguous PTE: ffffc000f4cf5ff8
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a5a9190 Start 0x000000006f460000 End 0x000000006f46bfff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00017d38440 Segment ffffc000f4f61ae0
NumberOfSectionReferences:          0 NumberOfPfnReferences:          10
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe000191ee4b0, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\plds4.dll
First prototype PTE: ffffc000f4fb6820 Last contiguous PTE: ffffc000f4fb6878
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe00019625a70 Start 0x000000006f450000 End 0x000000006f45cfff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00019bfd9d0 Segment ffffc000f3070e10
NumberOfSectionReferences:          0 NumberOfPfnReferences:          11
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe0001a38a090, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\plc4.dll
First prototype PTE: ffffc000f4e4e920 Last contiguous PTE: ffffc000f4e4e980
```

```
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe00017570450 Start 0x000000006f470000 End 0x000000006f505fff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00019beb450 Segment ffffc000f396da60
NumberOfSectionReferences:          0 NumberOfPfnReferences:         129
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe00019b58a20, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\mozsqlite3.dll
First prototype PTE: ffffc000f4d05b50 Last contiguous PTE: ffffc000f4d05ff8
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a3b5190 Start 0x000000006fb10000 End 0x000000006fb2bfff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe0001a187350 Segment ffffc000faefe2c0
NumberOfSectionReferences:          0 NumberOfPfnReferences:           9
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe0001947af20, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\libssp-0.dll
First prototype PTE: ffffc000f4fe9820 Last contiguous PTE: ffffc000f4fe98f8
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe00017cb71f0 Start 0x0000000000880000 End 0x0000000000a7bfff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00017c73010 Segment ffffc000f31ba0f0
NumberOfSectionReferences:          1 NumberOfPfnReferences:         458
NumberOfMappedViews:                1 NumberOfUserReferences:          2
Control Flags: File: 1, Image: 1
FileObject @ffffe000192fc460, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\tor.exe
First prototype PTE: ffffc000f980e010 Last contiguous PTE: ffffc000f980efe8
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a583b80 Start 0x0000000069650000 End 0x000000006966bfff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00019c0a430 Segment ffffc000f3221c20
NumberOfSectionReferences:          0 NumberOfPfnReferences:           9
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe000193723b0, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\libssp-0.dll
First prototype PTE: ffffc000f4e3b8e0 Last contiguous PTE: ffffc000f4e3b9b8
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a59f720 Start 0x00000000693f0000 End 0x000000006945ffff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe0001898ad10 Segment ffffc000f3221a00
NumberOfSectionReferences:          0 NumberOfPfnReferences:         103
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe00019be2090, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\ssleay32.dll
First prototype PTE: ffffc000f4e3b9d0 Last contiguous PTE: ffffc000f4e3bd48
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe000196084c0 Start 0x0000000069340000 End 0x00000000693b6fff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe00017c39010 Segment ffffc000f321d880
```

```
NumberOfSectionReferences:          0 NumberOfPfnReferences:          12
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe00019353da0, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\libgcc_s_sjlj-1.dll
First prototype PTE: ffffc000f4e4bc40 Last contiguous PTE: ffffc000f4e4bff0
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a59f680 Start 0x00000000693c0000 End 0x00000000693e1fff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe0001a72f120 Segment ffffc000f30d00d0
NumberOfSectionReferences:          0 NumberOfPfnReferences:          29
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe00018c6ab40, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\zlib1.dll
First prototype PTE: ffffc000f97f7ef0 Last contiguous PTE: ffffc000f97f7ff8
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a583ae0 Start 0x0000000069460000 End 0x000000006964efff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe0001893cd10 Segment ffffc000f481daf0
NumberOfSectionReferences:          0 NumberOfPfnReferences:         448
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe00017c67bc0, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\libeay32.dll
First prototype PTE: ffffc000f97bb010 Last contiguous PTE: ffffc000f97bbf80
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a59f680 Start 0x00000000693c0000 End 0x00000000693e1fff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe0001a72f120 Segment ffffc000f30d00d0
NumberOfSectionReferences:          0 NumberOfPfnReferences:          29
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe00018c6ab40, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\zlib1.dll
First prototype PTE: ffffc000f97f7ef0 Last contiguous PTE: ffffc000f97f7ff8
Flags2: Inherit: 1, NoValidationNeeded: 1

VAD node @ 0xffffe0001a583ae0 Start 0x0000000069460000 End 0x000000006964efff Tag Vad
Flags: Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @ffffe0001893cd10 Segment ffffc000f481daf0
NumberOfSectionReferences:          0 NumberOfPfnReferences:         448
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: File: 1, Image: 1
FileObject @ffffe00017c67bc0, Name: \Device\HarddiskVolume2\Users\warren\Desktop\Tor
Browser\Browser\TorBrowser\Tor\libeay32.dll
First prototype PTE: ffffc000f97bb010 Last contiguous PTE: ffffc000f97bbf80
Flags2: Inherit: 1, NoValidationNeeded: 1
```

Figure 26. The VAD node's description.