Online Anonymity: Forensic Analysis of the Tor Browser Bundle

Darcie Winkler*, B.S.[1]; Cpl. Robert Boggs[2]; John Sammons, M.S.[3]; Terry Fenger, Ph.D.[1]

[1]Marshall University Forensic Science Center, 1401 Forensic Science Drive, Huntington, WV 25701

[2]West Virginia State Police Digital Forensics Unit, 1401 Forensic Science Drive, Huntington, WV 25701

[3]Marshall University Department of Integrated Science and Technology, 1 John Marshall Drive, Huntington, WV 25755

Abstract

The Tor Browser Bundle (TBB) software uses a network of encrypted onion routers, known as the Tor network, that helps to increase the level of anonymity experienced by its users. The security and privacy provided by the Tor Browser was originally intended to protect the communication of the government, however, it also facilitates the participation in illicit activities. It is hoped that beneficial information will become evident by capturing packets while the Tor Browser is navigating to .onion and .com websites, dumping the Random-Access Memory (RAM), and comparing versions of the registry from various points of the installation process.

To test this theory, several virtual machines were used to monitor these key aspects in hopes of discovering evidence of the use or installation of the TBB. The results of this study will be of great use to the forensic science community in that it will provide necessary information for digital analysts in the event that they come across a suspect allegedly participating in illicit activities using the TBB.

Introduction

One way to protect online activity is by using an Onion Router (OR), which primarily hinders third parties from performing traffic analysis. The current OR technology has evolved into Tor, which stands for "the onion router." The layers surrounding the message establish a random, and therefore anonymous, communication circuit using the Diffie-Hellman Handshake Protocol.

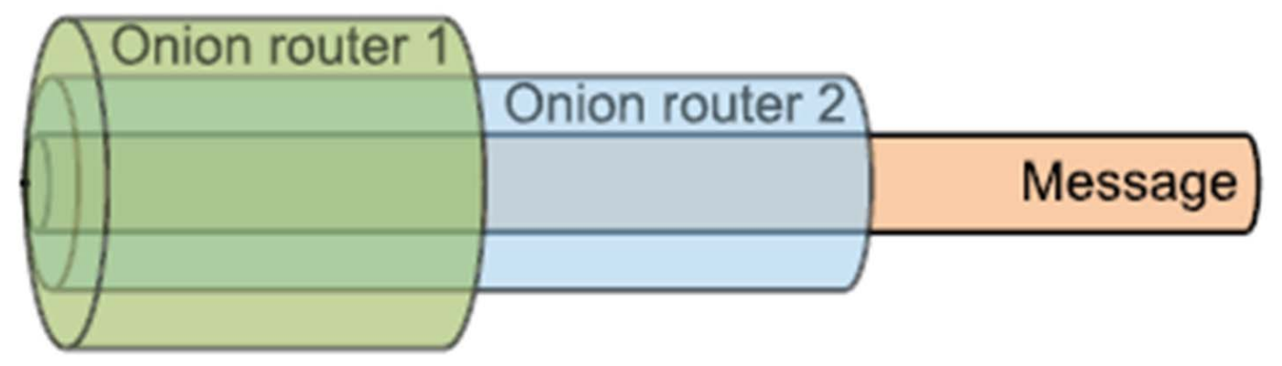


Figure 1. Several ORs encompass the message creating multiple layers of encryption.

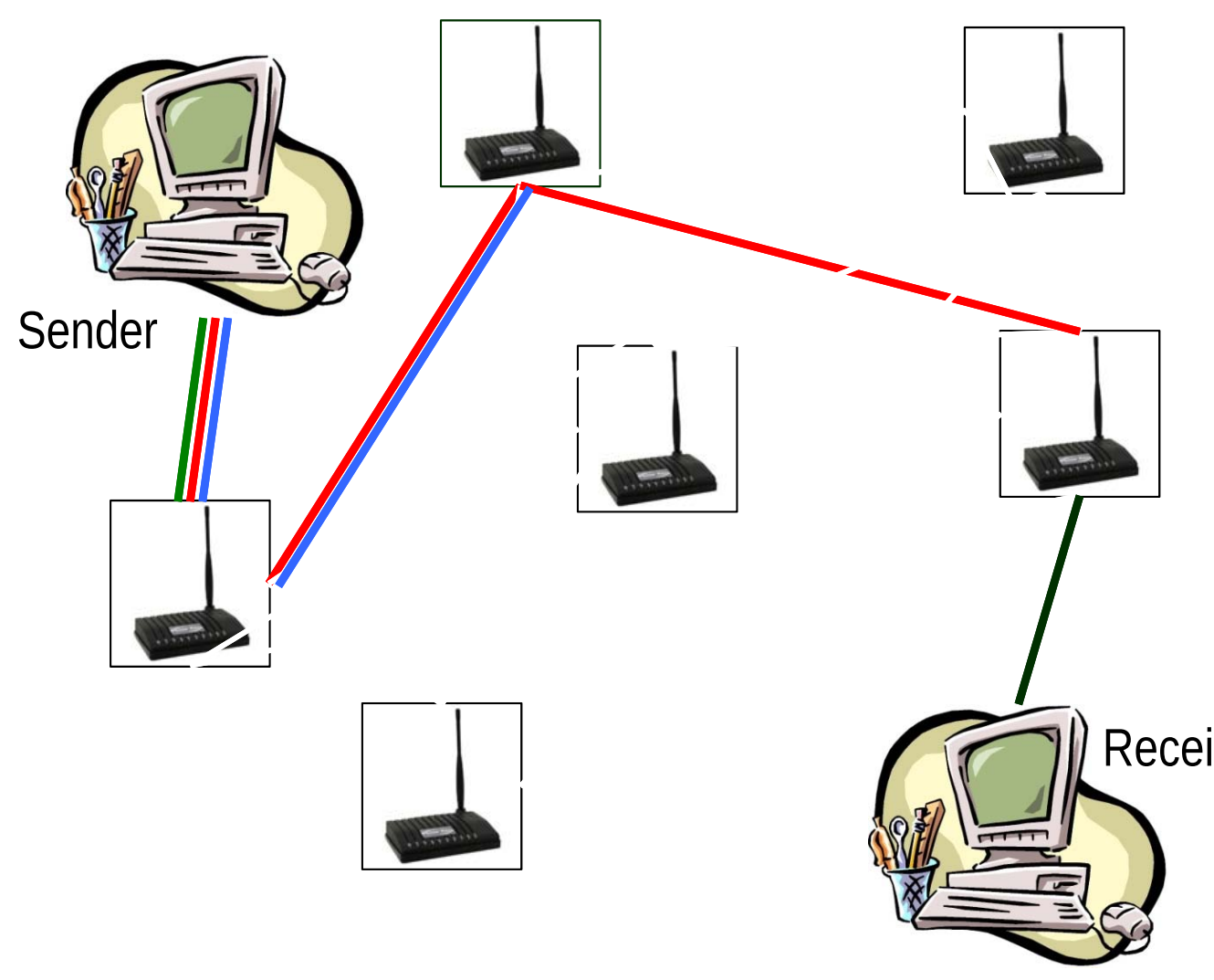


Figure 2. Peeling of the layers of encryption as the payload arrives at the target server.

The routing of encrypted traffic through several ORs has consequences such as:

- Enormous delay
- More users = greater anonymity

Materials and Methods

Virtual machines were constructed with identical parameters in order to test four possible scenarios: Windows Pre-Tor, Windows Tor Download, Windows Tor Active, Windows Post-Tor. An additional VM, Windows Registry, was created to track registry changes throughout the course of installing and uninstalling the TBB.

Hardware:

- NCS Gemini (32-bit) Desktop Computer
- Western Digital 320GB External HD

Software:

- Windows 7 OS with 8GB RAM
- Internet Explorer version 11.0.9600.17107
- Tor Browser Bundle version 3.6.1
- Vmware® Workstation version 10.0.2
- AccessData FTK® version 5.4.0.37
- AccessData FTK® Imager Lite version 3.1.1
- AccessData Registry Viewer® version 1.7.4.2
- Process Monitor version 3.1
- RegShot version 1.9.0.0
- WireShark® versions 1.10.7 and 1.10.8
- NetworkMiner version 1.5

RAM Dump Results

Table 1. Windows Pre-Tor RAM Dump Data

Carved File	File Type	Evidence
1742724031	html	Keywords content from Marshall University Forensic Science Center
1999010751	html	Keywords content from Marshall University Forensic Science Center
282857993	html	Customer reviews from Amazon
300174271	html	Digital Forensics Graduate Program Emphasis & Certificate
1048027504	jpeg	WVSP Digital Forensics Lab
1274565160	jpeg	WVSP Digital Forensics Lab
219619824	jpeg	WVSP Digital Forensics Lab
244188438	jpeg	WVSP Digital Forensics Lab
302308856	jpeg	WVSP Digital Forensics Lab
308277800	jpeg	WVSP Digital Forensics Lab
395759984	jpeg	WVSP Digital Forensics Lab
415955584	jpeg	Forensic Science Book from Amazon
424508032	jpeg	Forensic Science Book from Amazon
7488104	jpeg	Criminalistics Book from Amazon
156696576	ole	URLs for MUFSC and FS graduate program
272224400	ole	"things to do in huntington wv" Google search
360423424	ole	URLs for MUFSC and FS graduate program
416923696	ole	WVSP ICAC Task Force
874856448	ole	URLs for MUFSC and FS graduate program
285597936	png	"Free Two-Day Shipping for College Students" from Amazon
307990152	png	Google

Prior to the use of Tor, several indications existed within the RAM dump that provided proof of websites visited, primarily in the form of images.

Table 2. Windows Tor Active RAM Dump Data

Carved File	File Type	Evidence
30843	html	Tor Browser Bundle for Windows Download
34320024	html	Index of/Library/English/Cryptography/
39555	html	Tor homepage
113135960	jpeg	WVSP Digital Forensics Lab
114992848	jpeg	WVSP Digital Forensics Lab
116777840	jpeg	WVSP Digital Forensics Lab
138543864	jpeg	Criminalistics Book from Amazon
1998049408	jpeg	Apple iPad from .onion site
2019227440	jpeg	YouTube from Silk Road
2024888964	jpeg	Instagram from Silk Road
2055586912	jpeg	Criminalistics Book from Amazon
2140398250	jpeg	Drugs from Silk Road
23107458	jpeg	Drugs from Silk Road
539082736	jpeg	Tor Onion image
8924056	jpeg	Drugs from Silk Road
2043916784	png	Apple iPhone from .onion site
2061738472	png	Apple iPad from .onion site

Evidence of Tor being downloaded was present. Once Tor was used for navigation, several images were recovered that was indicative of Silk Road in the navigation history.

Table 3. Windows Post-Tor RAM Dump Data

Carved File	File Type	Evidence
587228031	html	Tor homepage
510492752	jpeg	Tor Onion image
587254076	jpeg	Tor Orbot for Android Devices
587262788	jpeg	Tor Tails image
587214612	png	Tor Download image
134657420	lnk	Shortcut File: C:\Users\DFU-Research\Desktop\Tor Browser\Browser\firefox.exe
245874724	lnk	Shortcut File: C:\Users\DFU-Research\Desktop\Tor Browser\Browser\firefox.exe

Lastly, evidence of Tor was left behind in the form of a shortcut saved to the desktop after use and uninstallation.

Registry Results

The following registry keys were examined for evidence of the TBB:

- NTUSER.DAT
- SOFTWARE
- SECURITY
- SYSTEM
- SAM

Table 4. Windows Pre-Tor Registry

SOFTWARE\Microsoft\Windows\CurrentVersion\AppPaths	Executable file for Internet Explorer
SOFTWARE\Wow6432Node\Microsoft\InternetExplorer	Installed applications
SOFTWARE\Clients\StartMenuInternet	Installed web browsers
NTUSER.DAT\Software\Microsoft\InternetExplorer\Typed URLs	Typed URLs within Internet Explorer

Table 5. Windows Tor Download Registry

NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags\1\Desktop	Tor Browser

Table 6. Windows Tor Active and Post-Tor Registries

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count	C:\Users\DFU-Research\Desktop\Tor Browser\Start Tor Browser.exe
NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags\1\Desktop	Tor Browser

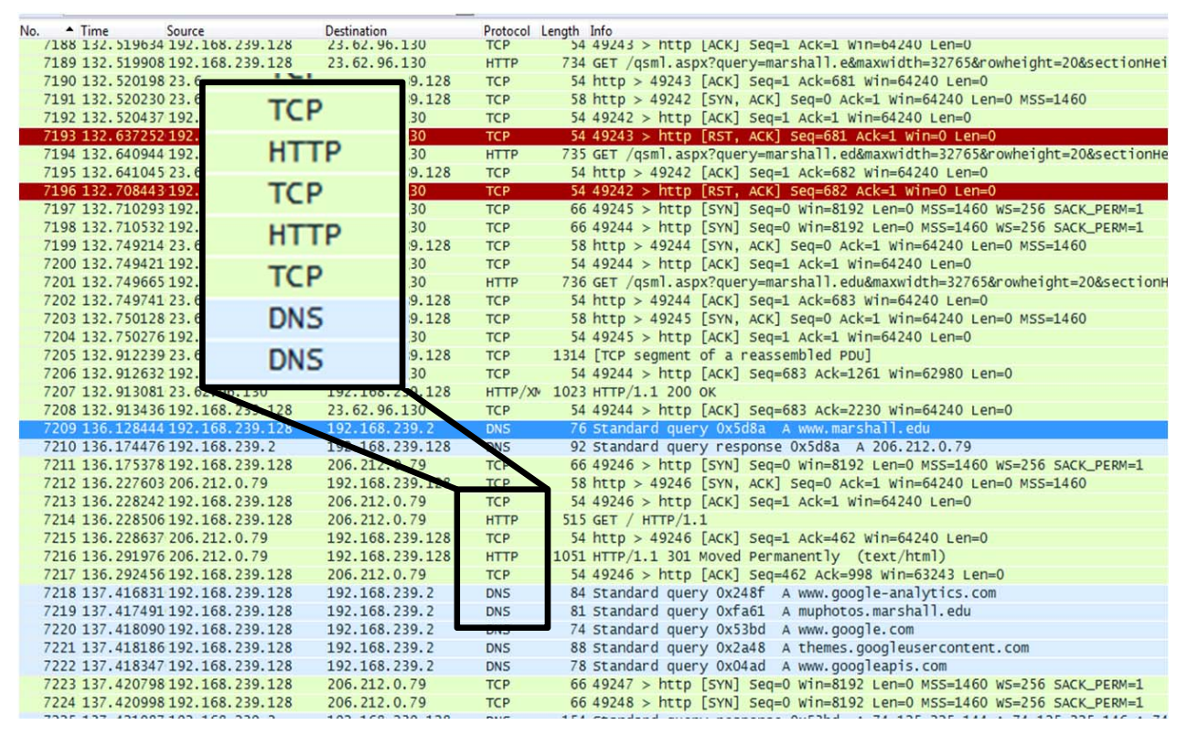
Table 7. RegShot – Changes in Registries with the Installation/Uninstallation of Tor

Action	Installation of Tor	Uninstallation of Tor
Keys Deleted	97	--
Keys Added	57	9
Values Deleted	173	--
Values Added	495	13
Values Modified	219	7
Files Added	566	--
Files Deleted	149	278
Files [Attributes?] Modified	57	10
Folders Added	153	--
Folders Deleted	3	74
Total Changes	1969	391

Process Monitor was also used to show changes made to the registry in real time during installation. It was incapable of acquiring any changes made after Tor was uninstalled.

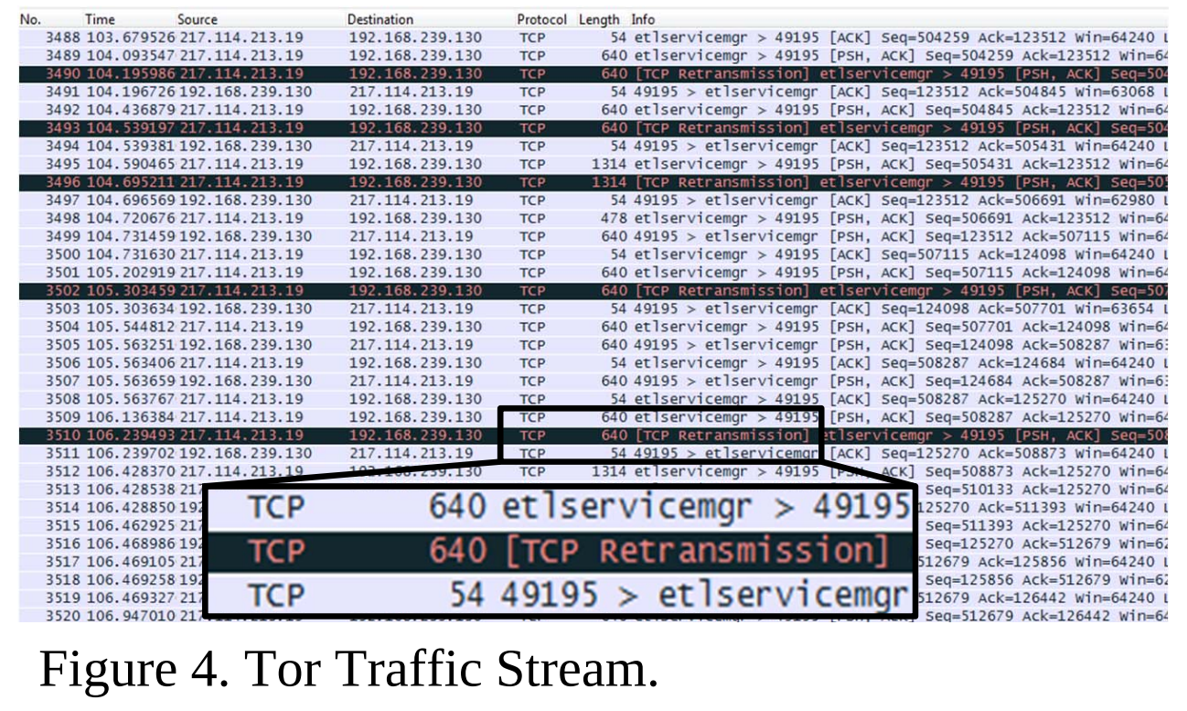
Packet Capture Results

WireShark® acquired information of the existence of Tor based on the way the packets traversed the network. The Protocol Hierarchy Statistics appeared vastly different. There tends to be more data packets using HTTP in Internet Explorer than in Tor. Additionally, some IP addresses with more frequent use within Tor may be indicative of entry ORs due to their location being in places such as France or Sweden.



```
No.   Time       Source          Destination     Protocol Length Info
7188 132.519634 192.168.239.128 23.62.96.130    TCP      54 49243 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
7189 132.519908 192.168.239.128 23.62.96.130    HTTP    734 GET /qsml.aspx?query=marshall.e&maxwidth=32765&rowheight=20&sectionHei
7190 132.520198 23.6                     9.128  TCP      54 http > 49243 [ACK] Seq=1 Ack=681 Win=64240 Len=0
7191 132.520230 23.6                     9.128  TCP      58 http > 49242 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
7192 132.520437 192.                     30     TCP      54 49242 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
7193 132.637252 192.                     30     TCP      54 49243 > http [RST, ACK] Seq=681 Ack=1 Win=0 Len=0
7194 132.640944 192.                     30     HTTP    735 GET /qsml.aspx?query=marshall.ed&maxwidth=32765&rowheight=20&sectionHe
7195 132.641045 23.6                     9.128  TCP      54 http > 49242 [ACK] Seq=1 Ack=682 Win=64240 Len=0
7196 132.708443 192.                     30     TCP      54 49242 > http [RST, ACK] Seq=682 Ack=1 Win=0 Len=0
7197 132.710293 192.                     30     TCP      66 49245 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7198 132.710532 192.                     30     TCP      66 49244 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7199 132.749214 23.6                     9.128  TCP      58 http > 49244 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
7200 132.749421 192.                     30     TCP      54 49244 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
7201 132.749665 192.                     30     HTTP    736 GET /qsml.aspx?query=marshall.edu&maxwidth=32765&rowheight=20&sectionH
7202 132.749741 23.6                     9.128  TCP      54 http > 49244 [ACK] Seq=1 Ack=683 Win=64240 Len=0
7203 132.750128 23.6                     9.128  TCP      58 http > 49245 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
7204 132.750276 192.                     30     TCP      54 49245 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
7205 132.912239 23.6                     9.128  TCP    1314 [TCP segment of a reassembled PDU]
7206 132.912632 192.                     30     TCP      54 49244 > http [ACK] Seq=683 Ack=1261 Win=62980 Len=0
7207 132.913081 23.6                     .128   HTTP/XM 1023 HTTP/1.1 200 OK
7208 132.913436 192.168.2    128 23.62.96.130    TCP      54 49244 > http [ACK] Seq=683 Ack=2230 Win=64240 Len=0
7209 136.128444 192.168.239.128 192.168.239.2   DNS      76 Standard query 0x5d8a  A www.marshall.edu
7210 136.174476 192.168.239.2   1   168.239.128  NS      92 Standard query response 0x5d8a  A 206.212.0.79
7211 136.175378 192.168.239.128 206.21   79     TC       66 49246 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7212 136.227603 206.212.0.79    192.168.239.1           58 http > 49246 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
7213 136.228242 192.168.239.128 206.212.0.79    TCP      54 49246 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
7214 136.228506 192.168.239.128 206.212.0.79    HTTP    515 GET / HTTP/1.1
7215 136.228637 206.212.0.79    192.168.239.128 TCP      54 http > 49246 [ACK] Seq=1 Ack=462 Win=64240 Len=0
7216 136.291976 206.212.0.79    192.168.239.128 HTTP   1051 HTTP/1.1 301 Moved Permanently  (text/html)
7217 136.292456 192.168.239.128 206.212.0.79    TCP      54 49246 > http [ACK] Seq=462 Ack=998 Win=63243 Len=0
7218 137.416831 192.168.239.128 192.168.239.2   DNS      84 Standard query 0x248f  A www.google-analytics.com
7219 137.417491 192.168.239.128 192.168.239.2   DNS      81 Standard query 0xfa61  A muphotos.marshall.edu
7220 137.418090 192.168.239.128 192.168.239.2            74 Standard query 0x53bd  A www.google.com
7221 137.418186 192.168.239.128 192.168.239.2   DNS      88 Standard query 0x2a48  A themes.googleusercontent.com
7222 137.418347 192.168.239.128 192.168.239.2   DNS      78 Standard query 0x04ad  A www.googleapis.com
7223 137.420798 192.168.239.128 206.212.0.79    TCP      66 49247 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7224 137.420998 192.168.239.128 206.212.0.79    TCP      66 49248 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

Figure 3. Internet Explorer Traffic Stream.



TCP 640 etlservicemgr > 49195
TCP 640 [TCP Retransmission]
TCP 54 49195 > etlservicemgr

```
No.  Time       Source          Destination     Protocol Length Info
3488 103.679526 217.114.213.19  192.168.239.130 TCP      54 etlservicemgr > 49195 [ACK] Seq=504259 Ack=123512 Win=64240 L
3489 104.093547 217.114.213.19  192.168.239.130 TCP     640 etlservicemgr > 49195 [PSH, ACK] Seq=504259 Ack=123512 Win=64
3490 104.195986 217.114.213.19  192.168.239.130 TCP     640 [TCP Retransmission] etlservicemgr > 49195 [PSH, ACK] Seq=504
3491 104.196726 192.168.239.130 217.114.213.19  TCP      54 49195 > etlservicemgr [ACK] Seq=123512 Ack=504845 Win=63068 L
3492 104.436879 217.114.213.19  192.168.239.130 TCP     640 etlservicemgr > 49195 [PSH, ACK] Seq=504845 Ack=123512 Win=64
3493 104.539197 217.114.213.19  192.168.239.130 TCP     640 [TCP Retransmission] etlservicemgr > 49195 [PSH, ACK] Seq=504
3494 104.539381 192.168.239.130 217.114.213.19  TCP      54 49195 > etlservicemgr [ACK] Seq=123512 Ack=505431 Win=64240 L
3495 104.590465 217.114.213.19  192.168.239.130 TCP    1314 etlservicemgr > 49195 [PSH, ACK] Seq=505431 Ack=123512 Win=64
3496 104.695211 217.114.213.19  192.168.239.130 TCP    1314 [TCP Retransmission] etlservicemgr > 49195 [PSH, ACK] Seq=505
3497 104.696569 192.168.239.130 217.114.213.19  TCP      54 49195 > etlservicemgr [ACK] Seq=123512 Ack=506691 Win=62980 L
3498 104.720676 217.114.213.19  192.168.239.130 TCP     478 etlservicemgr > 49195 [PSH, ACK] Seq=506691 Ack=123512 Win=64
3499 104.731459 192.168.239.130 217.114.213.19  TCP     640 49195 > etlservicemgr [PSH, ACK] Seq=123512 Ack=507115 Win=64
3500 104.731630 217.114.213.19  192.168.239.130 TCP      54 etlservicemgr > 49195 [ACK] Seq=507115 Ack=124098 Win=64240 L
3501 105.202919 217.114.213.19  192.168.239.130 TCP     640 etlservicemgr > 49195 [PSH, ACK] Seq=507115 Ack=124098 Win=64
3502 105.303459 217.114.213.19  192.168.239.130 TCP     640 [TCP Retransmission] etlservicemgr > 49195 [PSH, ACK] Seq=507
3503 105.303634 192.168.239.130 217.114.213.19  TCP      54 49195 > etlservicemgr [ACK] Seq=124098 Ack=507701 Win=63654 L
3504 105.544812 217.114.213.19  192.168.239.130 TCP     640 etlservicemgr > 49195 [PSH, ACK] Seq=507701 Ack=124098 Win=64
3505 105.563251 192.168.239.130 217.114.213.19  TCP     640 49195 > etlservicemgr [PSH, ACK] Seq=124098 Ack=508287 Win=63
3506 105.563406 217.114.213.19  192.168.239.130 TCP      54 etlservicemgr > 49195 [ACK] Seq=508287 Ack=124684 Win=64240 L
3507 105.563659 192.168.239.130 217.114.213.19  TCP     640 49195 > etlservicemgr [PSH, ACK] Seq=124684 Ack=508287 Win=63
3508 105.563767 217.114.213.19  192.168.239.130 TCP      54 etlservicemgr > 49195 [ACK] Seq=508287 Ack=125270 Win=64240 L
3509 106.136384 217.114.213.19  192.168.239.130 TCP     640 etlservicemgr > 49195 [PSH, ACK] Seq=508287 Ack=125270 Win=64
3510 106.239493 217.114.213.19  192.168.239.130 TCP     640 [TCP Retransmission] etlservicemgr > 49195 [PSH, ACK] Seq=508
3511 106.239702 192.168.239.130 217.114.213.19  TCP      54 49195 > etlservicemgr [ACK] Seq=125270 Ack=508873 Win=64240 L
3512 106.428370 217.114.213.19                  TCP    1314 etlservicemgr > 49195        ACK] Seq=508873 Ack=125270 Win=64
3513 106.428538 217                                                                            Seq=510133 Ack=125270 Win=64
3514 106.428850 192                                                                            125270 Ack=511393 Win=64240 L
3515 106.462925 217                                                                            Seq=511393 Ack=125270 Win=64
3516 106.468986 192                                                                            Seq=125270 Ack=512679 Win=62
3517 106.469105 217                                                                            512679 Ack=125856 Win=64240 L
3518 106.469258 192                                                                            Seq=125856 Ack=512679 Win=62
3519 106.469327 217                                                                            512679 Ack=126442 Win=64240 L
3520 106.947010 21                                                                             Seq=512679 Ack=126442 Win=64
```

Figure 4. Tor Traffic Stream.

Table 8. Network Miner comparison between Pre-Tor and Tor Active

Category	Pre-Tor	Tor Active
Hosts	253	39
Frames	19xxx	10xxx
Files	722	60
Images	224	0
Messages	0	0
Credentials	112	0
Sessions	377	19
DNS	636	72
Parameters	9234	201
Keywords	0	0
Cleartext	0	0
Anomalies	0	0

Network Miner was able to condense the packets captured from WireShark® and easily display the activity. Tor is capable of decreasing activity that can be monitored with a packet capture.

Discussion and Conclusions

RAM Dump

- Beneficial in network forensics
- Provides images from browsing activity
- Cannot determine from which websites images originated

Registry

- Beneficial in dead-box forensics
- Presence on desktop
- Uninstallation of Tor was not complete

Packet Capture

- Beneficial in network forensics
- Tor usage determined by traffic appearance
- Potential location of entry node

Based on the aforementioned methods and results, it can be determined that the Tor Browser Bundle does not appear to be as anonymous as it advertises. There may be a chance of de-anonymizing Tor if digital forensic laboratories had access to resources similar to FoxAcid. However, it appears that digital analysts will be hard pressed to find a reliable method of breaking through the anonymity provided by the TBB software.

In the future, it would be beneficial to use the information gathered from RegShot to determine where the data was stored that failed to be uninstalled. Additionally, it may be helpful to use a patch for WireShark® called Tor Dissector that will theoretically decrypt traffic.

References

Ball J, Schneier B, Greenwald G. NSA and GCHQ target Tor network that protects anonymity of web users, 2013; http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption (accessed June 5, 2014).

Dayalamurthy D. Forensic Memory Dump Analysis and Recovery of the Artefacts of Using Tor Bundle Browser - The Need. Proceedings of the 11th Australian Digital Forensics Conference 2013 December 2-4;Edith Cowan University, Perth, Western Australia.

Forte D. Advances in Onion Routing: Description and backtracing/investigation problems. Digit Invest 2006;3(2):85-8.

Ling Z, Luo J, Yu W, Fu X, Jia W, Zhao W. Protocol-level attacks against Tor. Comput Netw 2013;57(4):869-86.

Liška T, Sochor T, Sochorová H. Comparison between normal and Tor-Anonymized Web Client Traffic. Procedia Comput Sci 2011;3:888-92.

Norcie G, Blythe J, Caine K, Camp L.J. Why Johnny Can't Blow the Whistle: Identify and Reducing Usability Issues in Anonymity Systems. Proceedings of the NDSS Workshop on Usability Security 2014 February 23;San Diego, CA, USA.

Owen M. Fun with onion routing. Netw Secur 2007;(4):8-12.

Ren J, Wu J. Survey on anonymous communications in computer networks. Comput Commun 2010;33(4):420-31.

Schneier B. Attacking Tor: how the NSA targets users' online anonymity. 2013; http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity (accessed June 5, 2014).

Tor. Project: Overview. https://www.torproject.org/about/overview.html.en (accessed June 21, 2014).

Zhou P, Luo X, Chang R.K.C. Interference attacks against trust-based onion routing: Trust degree to the rescue. Comput & Secur 2013;39(B):431-46.

Acknowledgements

I thank Dr. Terry Fenger, Dr. Pamela Staton, Josh Brunty, and Ian Levstein from Marshall University Forensic Science Center for their assistance throughout the course of this research. Additionally, I thank Corporal Robert Boggs from the West Virginia State Police Digital Forensics Unit as well as John Sammons from the Department of Integrated Science and Technology at Marshall University for their instruction and expertise. This project was supported by Award No. 2010-IJ-CX-K025 awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice.