Digital Mafia ~ Decrypted

Vismit Sudhir Rakhecha(Druk)
Department of Security Analyst
Orlox Security Labs

Abstract

The Onion Routing (TOR) project is a network of virtual tunnels that facilitates secure, private communications on the internet. A recent statics shows that TOR bundle browser usage has increased in recent years statistics show that in January 2016 there were approximately 1,400,000 users globally and now in January 2017 that figure is estimated to have reached 2,000,000 users. The statistics also shows that in India 1,500,000 are major contributors towards the massive increase in TOR usage. This research paper will be an introduction and identifies the need for research in this area, and provides a literature review on existing research. The objective of this paper is to discuss the existing methodologies for analyzing forensic artifacts from the use of the TOR browser bundle and to propose a synthesized forensic analysis framework that can be used for analyzing TOR artifacts.

Keywords- Tor Forensics, Onion Forensics, Digital Mafia, Dark Web Forensics, Digital Forensics

I. HISTORY AND INTRODUCTION

In Tor will probably permit free and anonymous communication over the Internet. Tor permits anybody to associate with sites that might be blocked by onerous governments, permits informants to speak with authorities secretly, and gives a methods for legitimate communication between organizations and people who yearning to keep their private discussions private.

TOR is based on the principle of "Onion Routing". TOR was developed by U.S Navy in 1990 for protecting the traffic analysis. The alpha version of TOR named the "TOR Project" developed by DARPA, launched on 20th Sep 2002. Under the financial roof of "Electronic Frontier Foundation".

Currently, the TOR is maintained and responsible for its development by a NGO named the "TOR Project Inc.". It is mainly funded by U.S Government further aid is provided by Swedish Government.

II. HOW DOES TOR WORK?

The Tor network runs through the computer servers of thousands of volunteers spread throughout the world. Your data is bundled into an encrypted packet when it enters the Tor network. At that point, dissimilar to the case with typical Internet connection, Tor strips away part of the packet header, which is a part of the addressing information that could be utilized to learn things about the sender.

Then, Tor encrypts whatever remains of the address information, called the packet wrapper.

The encrypted packet is then steered through many servers, called Relays, while in transit to its last destination.

Every relay decrypts sufficiently just of the data packet wrapper to know which relay the data is originated from, and which relay to send it to next. The transfer then rewraps the bundle in another wrapper and sends it on.

The layers of encrypted address information used to anonymize data packet sent through Tor are reminiscent of an onion, consequently the name. That way a data packet way through the Tor network can't be completely traced.

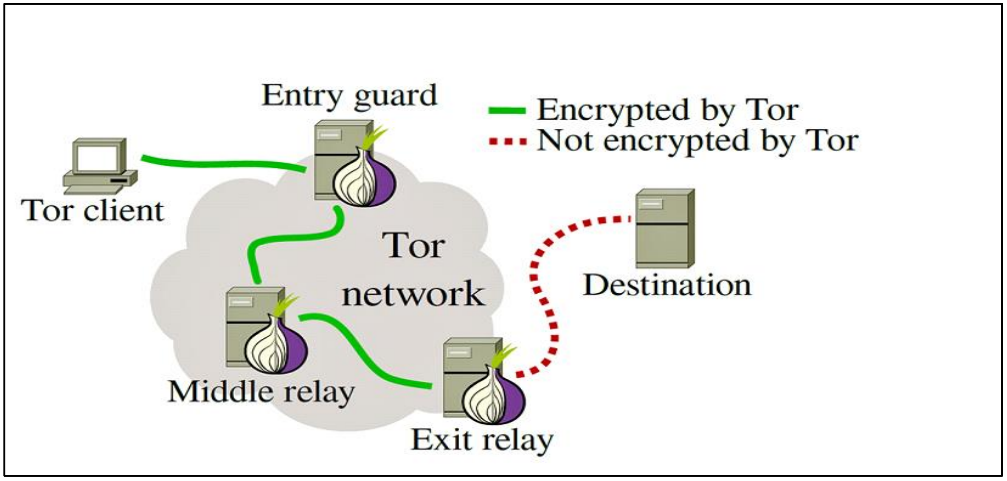


Fig. 1: Tor Working

III. TOR PRODUCTS

A. Tor Browser

Tor Browser contains everything you need to safely browse the Internet. This package requires no installation. Just extract it and run.

B. Arm

Arm is a terminal status monitor for Tor, intended for command-line aficionados and ssh connections. This functions much like top does for system usage, providing real time information on Tor's resource utilization and state.

C. Metrics Portal

Analytics for the Tor network, including graphs of its available bandwidth and estimated user base. This is a great resource for researchers interested in detailed statistics about Tor.

D. Tor Messenger

Tor Messenger is a cross-platform chat program that aims to be secure by default and sends all of its traffic over Tor.

E. Pluggable Transports

Pluggable Transports (PT) transform the Tor traffic flow between the client and the bridge. This way, censors who monitor traffic between the client and the bridge will see innocent-looking transformed traffic instead of the actual Tor traffic.

F. Onionoo

Web-based protocol to learn about currently running Tor relays and bridges.

G. Orbot

In collaboration with The Guardian Project, we're developing Tor on the Google Android mobile operating system. A related application is Orlib; a library for use by any Android application to route Internet traffic through Orbot/Tor.

H. Shadow

Shadow is a discrete-event network simulator that runs the real Tor software as a plug-in. Shadow is open-source software that enables accurate, efficient, controlled, and repeatable Tor experimentation.

I. Stem

Python library for applications and scripts that interact with Tor.

J. Tails

The Amnesic Incognito Live System is a live CD/USB distribution preconfigured so that everything is safely routed through Tor and leaves no trace on the local system.

K. TorBirdy

TorBirdy is Torbutton for Thunderbird and related *bird forks.

L. Tor2web

Tor2web allows Internet users to browse websites running in Tor hidden services. It trades user anonymity for usability by allowing anonymous content to be distributed to non-anonymous users.

M. Txtorcon

Python and Twisted event-based implementation of the Tor control protocol. Unit-tests, state and configuration abstractions, documentation. On PyPI and in Debian.

N. OONI

The Open Observatory of Network Interference, is a global observation network which aims is to collect high quality data using open methodologies, using Free and Open Source Software (FL/OSS) to share observations and data about the various types, methods, and amounts of network tampering in the world.

IV. TOR AND TECHNICAL FEATURES

The Tor arrange, made with support from the U.S. government, and is frequently utilized by writers, activists, and informants to secure their personalities and their correspondences. In any case, the secrecy system is likewise used by knowledge agents, cybercriminals and different malicious characters.

The utilization of Tor for malignant purposes has expanded over the past period with a great many noxious occasions beginning from Tor leave hubs consistently. According to a survey, roughly 345318 (19.87 %) events originate from U.S.A, 210990 (12.14 %) is from Russia, and 185647 (10.68 %) by Germany. Over 50 percent of malicious Tor traffic targets the information and communications, and manufacturing sectors. There has been a steady increase in the use of Tor for malicious purposes over the past years, with botnets that leverage the anonymity network being responsible for many of the traffic spikes.

V. Darknet

The part of the web that lies beyond a normal web browser's reach, and is an asylum for a shocking measure of criminal business - has never been less demanding, or better known.

Clients access the darknet by means of The Onion Router, or TOR, which masks a their identity by routing traffic through a complex network of servers (Relays).

Around 2 million individuals utilize TOR consistently, with 95 percent of that activity setting off to the general web and 5 percent to the darknet, said a representative for TOR.

Verifiably, the darknet is detonating in ubiquity among criminals. Cybercrime is huge business, and is anticipated to develop to $600 billion this year, outpacing whatever other type of crime including the drug trade, according to the United Nations Office on Drugs and Crime.

A boundless cluster of illegal products and services — from hit men to hackers — can be discovered practically on display. Helping with this bleak trade is bitcoin, which has made it less demanding than at any other time for anybody to do businesses anonymously.

"When you begin seeing advertisements for 'hard candy,' you are strolling into the peril zone," he said. "It escalates very quickly." ("Hard candy" in this setting is slang for child pornography.)

The criminal side of the darknet would stun to most normal people. A hit man can be enlisted for amongst $5,000 and $200,000. Purchasing a hit on CEOs and minor famous people costs $30,000, by and large, however there is a decent possibility some of these sites are fake, or could be government fronts hoping to catch criminals, by report.

"You can enlist people to hack diverse things, you can hire people to murder individuals, which is entirely frightening,"

An easygoing browser may think this all appears to be amazingly powerless against law requirement. But, as a user moves further into the underworld, they generally adopt measures to protect anonymity.

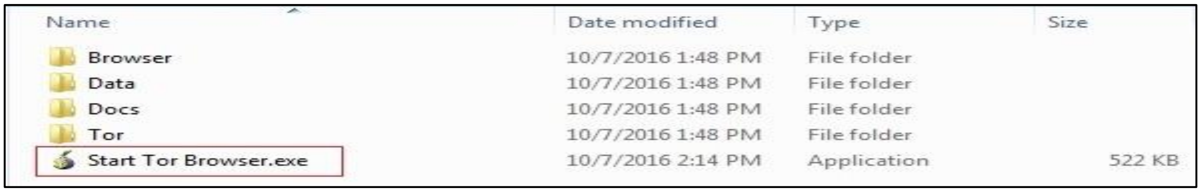
VI. Tor browser artifacts

Firstly, we install the Tor. You can get it.

Tools available at https://www.torproject.org

A. Files

1) \Browser
2) \Data
3) \Docs
4) \Tor
5) Start Tor Browser.exe

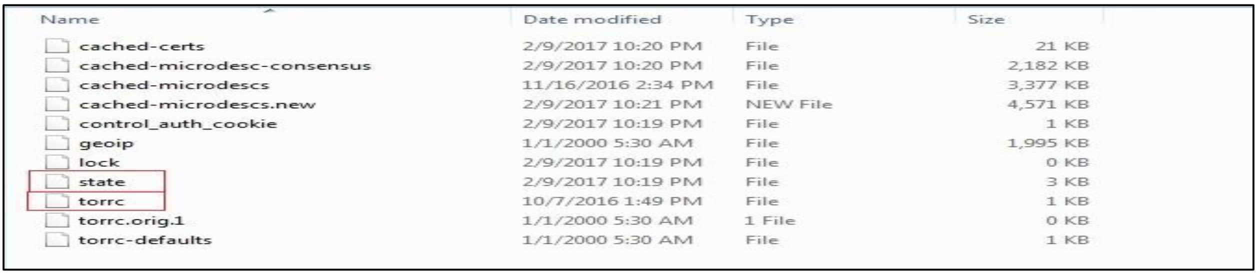


Name	Date modified	Type	Size
Browser	10/7/2016 1:48 PM	File folder	
Data	10/7/2016 1:48 PM	File folder	
Docs	10/7/2016 1:48 PM	File folder	
Tor	10/7/2016 1:48 PM	File folder	
Start Tor Browser.exe	10/7/2016 2:14 PM	Application	522 KB

Fig. 2: Tor Browser Folder

B. Interesting Folders

1) *\Data\Tor*

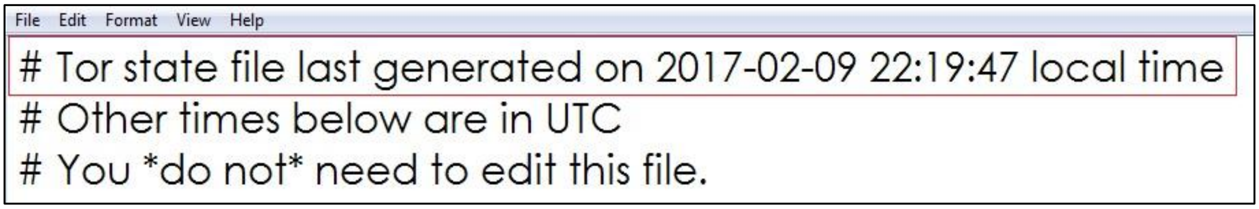


Name	Date modified	Type	Size
cached-certs	2/9/2017 10:20 PM	File	21 KB
cached-microdesc-consensus	2/9/2017 10:20 PM	File	2,182 KB
cached-microdescs	11/16/2016 2:34 PM	File	3,377 KB
cached-microdescs.new	2/9/2017 10:21 PM	NEW File	4,571 KB
control_auth_cookie	2/9/2017 10:19 PM	File	1 KB
geoip	1/1/2000 5:30 AM	File	1,995 KB
lock	2/9/2017 10:19 PM	File	0 KB
state	2/9/2017 10:19 PM	File	3 KB
torrc	10/7/2016 1:49 PM	File	1 KB
torrc.orig.1	1/1/2000 5:30 AM	1 File	0 KB
torrc-defaults	1/1/2000 5:30 AM	File	1 KB

Fig. 3: Tor Browser\Data\Tor

a) Folder: \Data\Tor\State

It contains the last execution date.

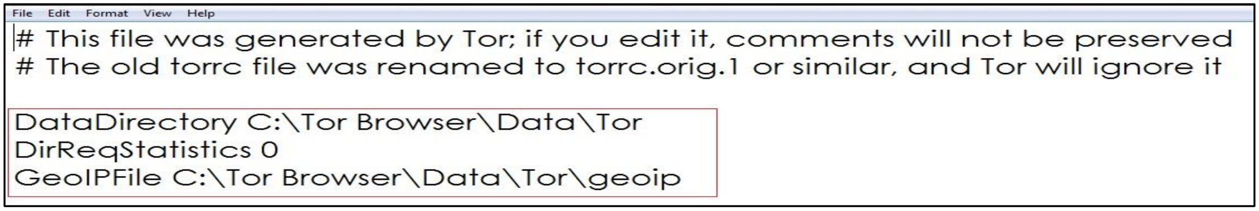


```
# Tor state file last generated on 2017-02-09 22:19:47 local time
# Other times below are in UTC
# You *do not* need to edit this file.
```

Fig. 4: Sate File

b) Folder: \Data\Tor\Torrc

It contains the path from where the Tor Browser was launched with the drive letter.

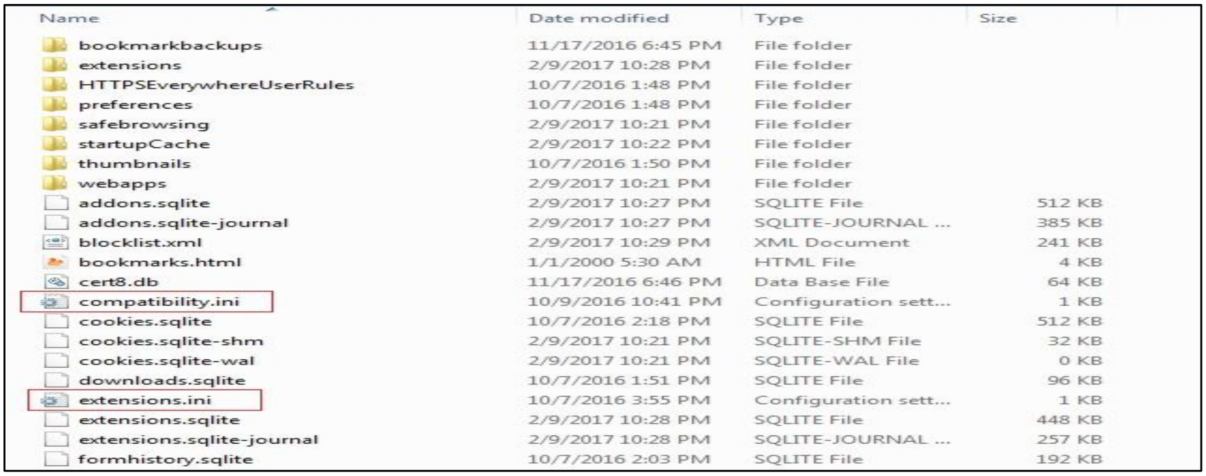


```
# This file was generated by Tor; if you edit it, comments will not be preserved
# The old torrc file was renamed to torrc.orig.1 or similar, and Tor will ignore it

DataDirectory C:\Tor Browser\Data\Tor
DirReqStatistics 0
GeoIPFile C:\Tor Browser\Data\Tor\geoip
```

Fig. 5: Torrc File

2) \Data\Browser

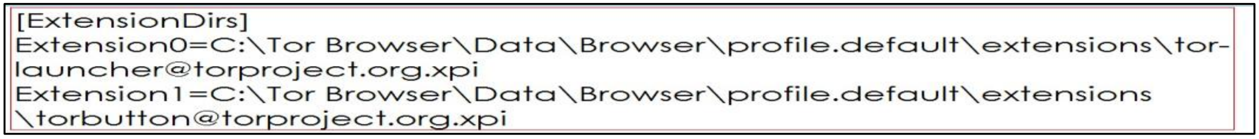


Name	Date modified	Type	Size
bookmarkbackups	11/17/2016 6:45 PM	File folder	
extensions	2/9/2017 10:28 PM	File folder	
HTTPSEverywhereUserRules	10/7/2016 1:48 PM	File folder	
preferences	10/7/2016 1:48 PM	File folder	
safebrowsing	2/9/2017 10:21 PM	File folder	
startupCache	2/9/2017 10:22 PM	File folder	
thumbnails	10/7/2016 1:50 PM	File folder	
webapps	2/9/2017 10:21 PM	File folder	
addons.sqlite	2/9/2017 10:27 PM	SQLITE File	512 KB
addons.sqlite-journal	2/9/2017 10:27 PM	SQLITE-JOURNAL ...	385 KB
blocklist.xml	2/9/2017 10:29 PM	XML Document	241 KB
bookmarks.html	1/1/2000 5:30 AM	HTML File	4 KB
cert8.db	11/17/2016 6:46 PM	Data Base File	64 KB
compatibility.ini	10/9/2016 10:41 PM	Configuration sett...	1 KB
cookies.sqlite	10/7/2016 2:18 PM	SQLITE File	512 KB
cookies.sqlite-shm	2/9/2017 10:21 PM	SQLITE-SHM File	32 KB
cookies.sqlite-wal	2/9/2017 10:21 PM	SQLITE-WAL File	0 KB
downloads.sqlite	10/7/2016 1:51 PM	SQLITE File	96 KB
extensions.ini	10/7/2016 3:55 PM	Configuration sett...	1 KB
extensions.sqlite	2/9/2017 10:28 PM	SQLITE File	448 KB
extensions.sqlite-journal	2/9/2017 10:28 PM	SQLITE-JOURNAL ...	257 KB
formhistory.sqlite	10/7/2016 2:03 PM	SQLITE File	192 KB

Fig. 6: Tor Browser\Data\Browser

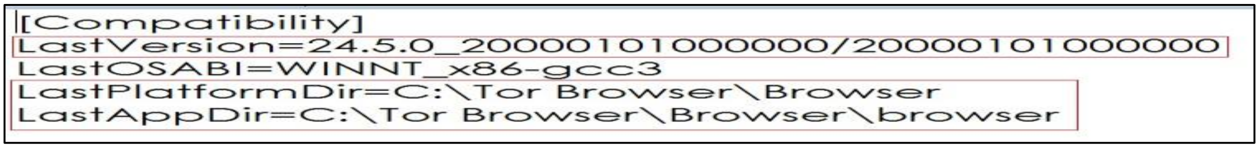
a) Folder: \Data\Browser\Compatibility.ini | Extension.ini

The most interesting files are Compatibility.ini and Extension.ini and contain the browser execution path.



```
[ExtensionDirs]
Extension0=C:\Tor Browser\Data\Browser\profile.default\extensions\tor-
launcher@torproject.org.xpi
Extension1=C:\Tor Browser\Data\Browser\profile.default\extensions
\torbutton@torproject.org.xpi
```

Fig. 7: Extension File



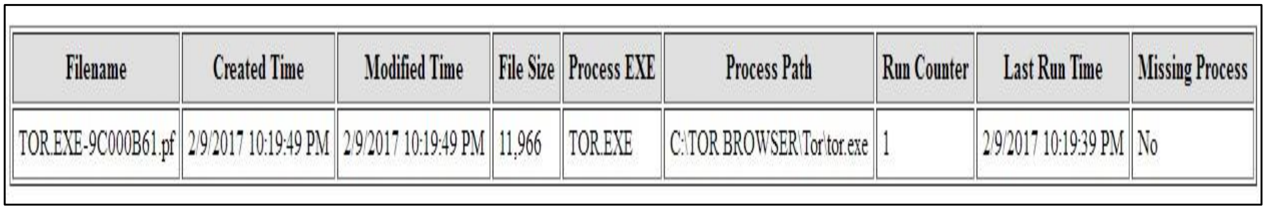
```
[Compatibility]
LastVersion=24.5.0_20000101000000/20000101000000
LastOSABI=WINNT_x86-gcc3
LastPlatformDir=C:\Tor Browser\Browser
LastAppDir=C:\Tor Browser\Browser\browser
```

Fig. 8: Compatibility File

C. Prefetch Files

1) Folder: C:\Windows\Prefetch

Prefetch file give details about tor ~ install date, first execution date, last execution date, and no. of executions.



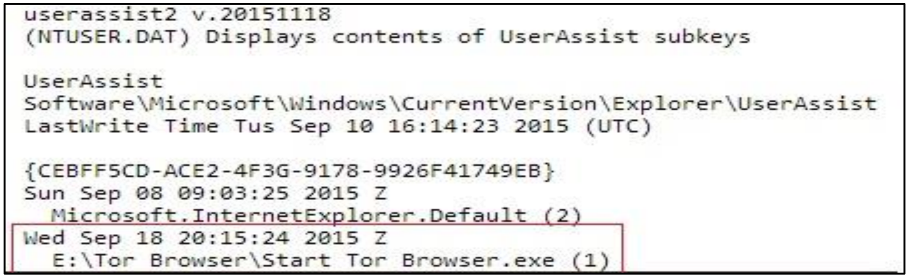
Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time	Missing Process
TOR.EXE-9C000B61.pf	2/9/2017 10:19:49 PM	2/9/2017 10:19:49 PM	11,966	TOR.EXE	C:\TOR BROWSER\Tor\tor.exe	1	2/9/2017 10:19:39 PM	No

Fig. 9: Prefetch File (.pf)

D. Ntuser

1) Folder: C:\Users\Druk\ntuser.dat

In Ntuser.dat file, you recover last Execution date, no. of execution, execution path.



```
userassist2 v.20151118
(NTUSER.DAT) Displays contents of UserAssist subkeys

UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Tus Sep 10 16:14:23 2015 (UTC)

{CEBFF5CD-ACE2-4F3G-9178-9926F41749EB}
Sun Sep 08 09:03:25 2015 Z
  Microsoft.InternetExplorer.Default (2)
Wed Sep 18 20:15:24 2015 Z
  E:\Tor Browser\Start Tor Browser.exe (1)
```

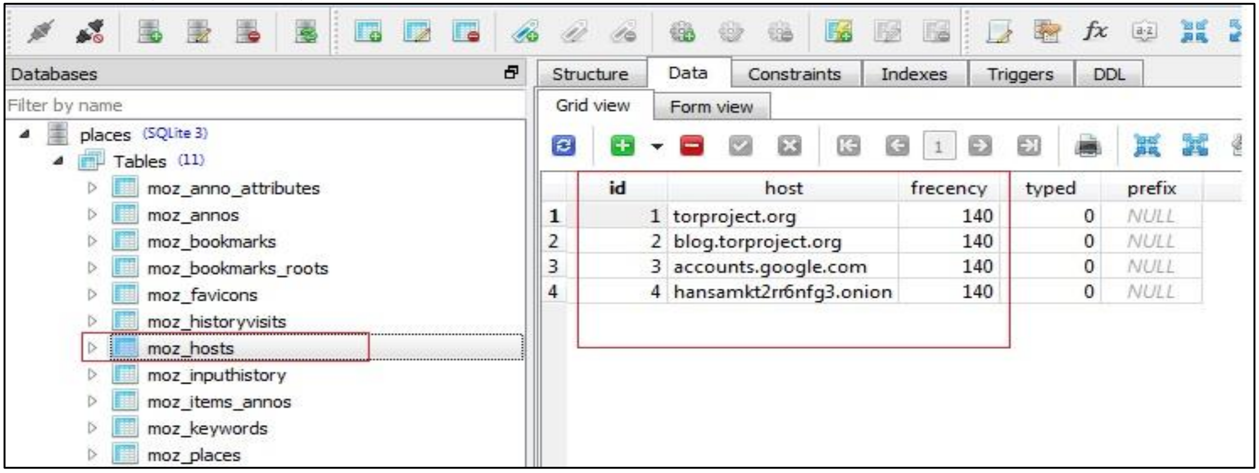
Fig. 10: Ntuser File (.dat)

Note: you can’t directly access Ntuser file in windows, I am using a software named Linux Reader and Hex Editor.

E. Places.sqlite

1) Folder: C:\Tor Browser\Data\Browser\profile.default\places.slite

In this file, we will get all the juicy information about site visited, bookmarks, places, etc.



	id	host	frecency	typed	prefix
1	1	torproject.org	140	0	NULL
2	2	blog.torproject.org	140	0	NULL
3	3	accounts.google.com	140	0	NULL
4	4	hansamkt2rr6nfg3.onion	140	0	NULL

Fig. 11: Places.sqlite

Note: you can open .sqlite files with Sqlite Studio.

VII. Conclusion

Given the results of the research, it would appear that Tor is not as anonymous as it advertises. However, most of the evidence acquired through the course of this research would otherwise be unattainable in dead-box forensic investigations.

References

[1] https://torproject.org/
[2] https://www.torproject.org/projects/projects.html.en
[3] http://www.tomsguide.com
[4] www.cnbc.com
[5] https://blog.torproject.org/blog/forensic-analysis-tor-linux