### **Chapter I**

#### INTRODUCTION

We live in the era of Information Technology, where data is everything. People wants to surf the internet without leaking their browsing data. They want anonymity and privacy. That is when people starts to turn their heads towards the Deepweb, instead of the surface web.

Deepweb/Darknet is a private network that is inaccessible to normal browsers and search engines. Their main purpose is to defend against network analysis, network surveillance and to provide anonymity and privacy in the network.<sup>[6]</sup>Because of these features many criminals use these to do malicious activities online. Freenet, Hornet and I2P are some of the popular browsers used by these criminals.

**Freenet** is a peer-to-peer platform for censorship-resistant communication. It uses a decentralized distributed data store to keep and deliver information and has a suite of free software for publishing and communicating on the web without fear of censorship. Both Freenet and some of its associated tools were originally designed by Ian Clarke in 1999, who defined Freenet's goal as providing freedom of speech on the internet with strong anonymity protection.<sup>[7]</sup>

**Hornet** is an anonymized and accelerated onion routing network. The name is an acronym for high speed onion routing network. It gives faster speeds to more efficient network design. Hornet claims to be much harder to crack than Tor. Both are called onion browsers for their layers of security. Instead of a direct link to places you've visited on the web, the browsers leave traces of your activity across the Internet, making it more difficult to track. In order for an outsider to gain access to someone using either browser, they'd have to control one of the layers of security.<sup>[8]</sup>

The **Invisible Internet Project (I2P)** is an anonymous network layer that allows for censorship-resistant, peer-to-peer communication. Anonymous connections are achieved by encrypting the user's traffic and sending it through

a volunteer run network of roughly 55,000 computers distributed around the world.Given the high number of possible paths the traffic can transit, a third party watching a full connection is unlikely.It was introduced in 2003.I2P has had a stable release every six to eight weeks.I2P has built in features including emailing,instant messaging and file sharing.<sup>[9]</sup>

**DB Browser for SQLite (DB4S)** is a high quality,visual,open source tool to create,design and edit database compatible with SQLite.DB4S uses a familiar spreadsheet like interface, and complicated SQL commands do not have to be learned.<sup>[10]</sup>

**SQLite Database Recovery** is a robust utility that effectively scans healthy or inaccessible SQLite2, SQLite3 and DB file and restores all its objects such as tables, views, triggers. This tool is offered by Systools group.<sup>[11]</sup>

Normal browsers will leave behind a lot of information like cookies, browsing histories etc.Cookies, more properly called HTTP cookies, are small bits of data stored as text files on a browser. Websites use those small bits of data to keep track of users and enable user-specific features.But in the case of these anonymous browsers it is very unlikely that they will contain any sort of cookie data.

However there are chances that they may leave some data regarding their online activities in the host machine.That's the kind of data which a cyber forensic investigator wants to get his hands on.That data can act as digital evidence against the criminal, it may even result in obtaining the identity of the criminal and his activities.

A previous study on the Tor browser artifacts resulted in obtaining some valuable data regarding browsing, from the host machine. Enlightened by that study, I was able to do a forensic analysis of Freenet, Hornet and I2P artifacts analysis in Windows and Linux operating systems. The Hornet browser was not available for download when I was doing this research, hence I could not conduct analysis on it. Nevertheless the process of installing the browser on the host machine and collecting the data are the same as of the other two browsers.

#### **Chapter II**

#### LITERATURE REVIEW

"A Forensic Audit of the Tor Browser Bundle" by Matt Muir, Petra Leimich and William J Buchanan (2019).<sup>[4]</sup> They simulated typical web browsing activity with Tor Usage of virtualisation and a predetermined browsing protocol allowed artefact recovery with static and live forensic techniques, such as process monitoring, keyword searching and file carving, with the aid of Autopsy and the Volatility Framework.Static analysis revealed significant leakage of user activity in the snapshots of machines used to perform the testing. This included HTTP header information, web page titles and an in-stance of a URL. Further, live analysis identified traces of Tor processes even after the user had closed and uninstalled the browser and logged out. The absolute path to the browser executable was seen in RAM on several occasions, including the username of the user running the browser and the device from which it was run. The research suggests to take a RAM dump, where possible. Analyse with Volatility's psscan, pstree and timeliner plugins to establish the use of TOR and find the username. This will also reveal timestamps and can be carried out even after the user has uninstalled TOR and logged out. Where they exist, pagefile.sys or hiberfile.sys can be used instead of a RAM dump. The analysis of all three of these data sources from the same system could result in the recovery of different, but nonetheless relevant and corroborative or complimentary evidence. In summary, Tor use can be easily detected using live forensics, particularly when the browsing session is still active. Ensuring that the browsing session is closed after use helps to conceal the fact that Tor was used. However, an artefact (firefox.exe) remains detectable in RAM after closure, deletion, and logout. It is likely that the traceable artefact is the result of an anomaly in Firefox's handling of running processes. This belief is strengthened by the fact that Tor manages to remove all evidence of the processes directly attributed to its browser, yet one Firefox process remains. Perhaps this abnormality was introduced in an update of Firefox's Extended

Support Release, or it may even be an unforeseen result of the interaction between Tor's plugins and the underlying browser. Nonetheless, it shows that reliance on a third-party browser can introduce problems which undermine user anonymity.Due to the volatile nature of RAM, acquisition of live memory is rarely possible in the field. This is applicable even in shared computing environments, as often the user can power cycle a shared computer without consequence. Considering that the intended audience for this project was both users of the browser and forensic investigators wishing to analyse it, the omission of a subsequent static analysis would constitute an in-complete methodology. This is especially true as a large number of Tor users will likely use their personal computer which could be subject to seizure by a forensic adversary. Therefore, the multifaceted experimental design was required. This proved successful in the end as many unexpected results were born from the static analysis, an aspect which may have been omitted if too much reliance had been placed on the results of previous research. The technique of indexing the hard drive and applying key-word searches based on known Tor artifacts and the browsing protocol was simple yet is something that the browser should protect against. This indicates that the Tor Browser does not adequately protect the user from a forensic adversary.

**"Tor Browser Artifacts in Windows 10" by Aron Warren (2017).**<sup>[2]</sup>The research gives an insight about the forensic approach which should be taken while looking for Tor browser artifacts in Windows 10 operating system.He used softwares like Regshot,X-ways forensics,Tor browser and RegRipper.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.Regshot was used 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.Using X-ways forensics filesystem artifacts was carved.X-Ways is compatible with VMDK files that are split into smaller file sizes. Among the artifacts, prefetch file will indicate the software's installation locationTo analyze the system and user registry hives, which contain artifacts about system and user activity, RegRipper was used. The researcher also obtained the memory artifacts like, dlllist,envars,cmdline,dumpfiles,vmem privs,vadtree,vadinfo etc.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.

**"Tor Forensics On Windows OS" by Mattia Epifani(2015).**<sup>[3]</sup>It examines the artifacts on a real case. The research points out the folders in which the data related to Tor is found. From the prefetch files the researcher was able to obtain details such as installation date, first execution date, last installation date, number of executions etc. By analyzing various NTUSER. DAT from VSS researcher identified the number and time of execution in a period of interest. Other artifacts from hard drive was separately obtained. Thumbnail Cache, USRCLASS. DAT registryfile, Windows Search Database etc. The researcher used these and applied to real life case and was able to successfully extract the desired data.

# **Chapter III**

# AIM AND OBJECTIVES

### AIM:

The aim of this research is to assist the cyber forensic investigators in obtaining the data associated with the installed privacy browsers in Windows and Linux operating systems.

## **OBJECTIVES:**

- Showcase a detailed overview of Freenet,Hornet,I2P browsers installation
- Find out the possible artifacts created by the browsers
- > Identify the file locations associated with the browsers

# **Chapter IV**

# MATERIALS AND METHODOLOGY

## MATERIALS:

Hornet,Freenet v1.4.8, I2P v0.9.44 (browsers),Windows OS v10, Linux OS v18.04.3, DB Browser for SQLite v3.11.2, SQLite Database Recovery v1.2

## **METHODOLOGY:**

The whole process consists of three phases,

- 1. Downloading and installation of all the softwares/browsers required
- 2. Launching of the browsers and performing certain tasks
- 3. Collection and analysis of artifacts

## 1. Downloading and installation

This is the phase where, all the steps in downloading the softwares and installing them in the host system will be shown. It is divided into two:

1.1 In Windows10

i) I2P browser

Open any search engine and type in "I2P browser".From the results obtained click on the first link.(Fig.1.1)





o = 🐂 e 🛍 🔳 ⊌ 🕼 O 📾 🗣 📴 👙

Fig.1.4

.

Ø Type here to search

😮 🗠 🖾 🕂 🗛 (NG 23:3) 関



Fig.1.5

The progress of the installation will be visible.(Fig.1.6)





ii) Freenet browser

Open any search engine and type in "freenet browser", from the results click on the first link.(Fig.1.8)













Fig.1.17

Choose the destination folder and click on "Next".(Fig.1.18)

2	(D)	M.	<ul> <li>Image: A state of the state of</li></ul>	Marage as the application too	Downitanda				0		-7
Amal A.S		Windsolbe	* 🔒 🗍	A Car A Car	D Criete Revene	any accest		Salatt none			scanner
			ann Ophae	17	Graner	New Dor		Invert selection Select	<b>N</b>		
Firefair		img077	+ <b>*</b> • •	Custom Setup	all allog	5			Bitter		golang s
	-	-	OneDrive		unt fedures in he insist	ы	3	528			
e			Ithis PC	Click the core in the	tree below to change th	e way feetures will be netailed.	faller .	15-89/43		4	California (California)
Edge		Browser	Desitop	E @ 100	General Contra	The complete parkage		23,750 KB			Namaya
		32	Cyberlink		🕘 • ] Meth			79,766 KH			2
Google	UNIT III-	WPS-Office	S Downicaete			This feature impaires 3996 on acar kand divid: 3 flass 1 of 1 subfactures	12 bits	80,371 KB 1,899 KE			Adika
Chrome	Modern DN_		Skype			sviettet. The subfeatures repare 4363 en yeur hard drive.	anter	533 KR	1000		Nancay
-			Teleptart Desk				421/1e -	20 KB 12,001 KD	1		
<b></b>	Castor of	(and the	K DS-WNRTSIN		Program Filest/Dê Brown	ar for SQLERA	attre -	1421	-		
Wiselestell.	Udeler	emalapproj	105 Atoma 1 dam sele	tend 1	Init things	led liet Canel	-		1		Cybersec Analyst C
-	-	-		them.	The Deep	103					
6								-			
Recycle Bin		amalasproj	admission.								
	total Pto.,		request								
			<b></b>								
UDMY	Master	Mproject	TeamViewer								
		Abstract						The second second		24	
									-		
4 3	D Type here	e to search		0 # 7	e 🔒 I	i i i i i i i i i i i i i i i i i i i		<b>3</b>		<b>12</b> ~ 10 d	4× ENG 01106
									1000		
•	D Type here	e to search		0 H 🔒	8 🗎	u c C f	3 8			<b>10</b> ~ 10 d	dx ENG 23-01-2020



Fig.1.19

To complete the installation click on "Finish" option. (Fig. 1.20)



#### iv) SQLite Data Base Recovery

Open any search engine and type in "sqlite database recovery".From the results click on the first link.(Fig.1.21)







Click on the sq lite database installer and click "Next".(Fig.1.24)



Choose the destination folder and click "Next". The installation will start. (Fig. 1.25)



Fig.1.25

Click on "Finish" option to complete the installation and launch the browser. (Fig.1.26)



### 1.2 In Linux Version 18.04.3

In Linux operating system the softwares are installed through Linux command line called the "Terminal".

Since there was no alternative download/install option available for Hornet browser for Linux OS, the browser could not be installed.

i) I2P browser

Open a terminal and enter: sudo apt-add-repository ppa:i2p-maintainers/i2p

This command will add the PPA to /etc/apt/sources.list.d and fetch the gpg key that the repository has been signed with. The GPG key ensures that the packages have not been tampered with since being built.(Fig.2.1)



Fig.2.1

Updating the system using: sudo apt-get update

This command will retrieve the latest list of software from each repository that is enabled in the system, including the I2P PPA that was added with the earlier command.(Fig.2.2)





Fig.2.5

The browser is launched using the following command: freenet\_installer (Fig.2.6)



Since SQLite Data Base Recovery and DB Browser for SQLite has the same features and functions, only DB Browser for SQLite was installed in the Linux system.Moreover SQLite Data Base Recovery had no alternative download for the Linux OS.

#### 2.Performing certain tasks

After the installation of the browsers, each browser was launched one after the other. Using each browsers I performed the following tasks.

- i. Visited the site "www.thehindu.com"
- ii. Downloaded an image file
- iii. Streamed an audio/downloaded an audio file
- iv. Searched for a specific product in Flipkart/Amazon

After performing the above tasks the browsers were closed and the system was turned off.

## 3. Collection and analysis of artifacts

The system was restarted. The directories and folders associated with the installed browsers were analyzed. The analysis was carried out using the installed DB Browser for SQLite application and other inbuilt application. Since the SQLite Data Base Recovery and DB Browser for SQLite has the same features and functions, only DB Browser for SQLite was used to analyse the data. The artifacts were documented by taking screen shots of each results.

# Chapter V

## **RESULTS AND CONCLUSION**

### **RESULTS**:

1. In Windows OS

The Prefetch files related to each browsers were analyzed by searching through the Prefetch directory.

i) Freenet

The regular search using the keyword "Freenet", inside the Windows C Drive gave five search results. All of them were in ".pf" format. (Fig. 1'.1)

Convert folder		date Seattle		
+ 🛯 + 54	earch Results in prefetch			- Di freeset
A Quick access	FREENETTRAY.EXE-EEGOSBEE.pf	Type: PF File	Class modified: 26-01-2020-16:15 Sine: 27.2 XB	
Desktop  Connicads  Conuments	FREENETWRAPPER-64,EXE-2D897E07.4 C\Windows\prefexts	of Type: PF File	Date modified 26-01-2020 14/29 Start 7.25 KB	
Pictures	FREENETINSTALLER-1484.TMP-6A677F	E1.pf type: PF File	Cate modified 26-01-2020 14:09 Size 0.94 KB	
New Volume (F)     Spreenchots	FREENETINSTALLER-1484.TMP-366358 C:\Windows\prefexch	06.pf Type: PF File	Date modified 25-01-2020 14.09 Stor: 6.93 KB	
SUBMITNOW	FREENETINSTALLER-1484.EXE-2C0CC0 C\Windows\prefexth	56.pf Type: PF File	Date modified: 26-01-2020 14:09 Stor: 6.37 KB	
Complete				
This PC				
3D Objects				
Decuments				
Downloads				
A Music				
Pictures				
Mdeos				
WINDOWS (C)				
- New Volume (D:				
New Volume (E)				
- New Volume (F)				
SECOVERY (G)				
tain.				E
			Fig.1'.1	

A view of the properties of each file showed the details like;File name, created time,modified time and the last run time etc.The file path,where the app data is stored was also seen.

Created time Indicates the date and time in which the browser was installed.Last run time gives the details like when the browser was last launched and used.It is shown in Fig.1'.2,Fig.1'.3 and Fig.1'.4 respectively.



<ul> <li></li></ul>			e x			40	Figerief.
Nick access	Options Help		8.0				
Downloads / Filename / Pro	operties		X A	Find Find what Freenet		X Find flee	
ryber formuz	Filenome: Created Time:	FFIEENETTFIAY.EXE-EE6050EE.pt 26-01-2020 1 4:19:30	EAST-TEC IN IADS/FREENE	Match whole word only	Direction Orlia @Down	Garcel	
New Yolume (F) (F. FREENETINS' Screenshot) AFREENETINS I	Modified Time: File Size:	26-01-2020 16:19:15 27.908	MALOCAL/II HALOCAL/II Abcal/Freene	Match case	(Die Green		
SUBMITNOW	Process EXE:	FREENETTRAY, EXE	Ancel/Ferene w				
neDrive Filename /	Process Path: Run Counter:	CiUsersiamalajappDatajLocal/Freened/FREENETTRAY_EXE 0					
THE ALLOC THE	Last Run Time: Missing Process:	25-01-2020 16:19:09, 25-01-2020 16:18:37, 26-01-2020 16:17:11, 25-01-2020 No					
Desktop APPHELP.DL Documents BORVPT.DLL		ОК	1				
Music CEGMGR32.DUL	E:\Window	x15ydem228CTVPTPRMLVOLUME(01aH1d7374e446cb-da754b15 v15ydem22xdgmg122x81_VOLUME(01aH1d7374e446cb-da754b55 Wr5dtf Freeware_http://www.ntradf.avt		2			
Valen							
WINDOWS (C) New Volume (D)							
New Volume (E) New Volume (F)							
RECOVERY (G)							
		<b>F</b> : 17.4					
		Fig.1'.4					
-	view	of Fig.1'.3 is given below	W.				
n enlarged	view		w.				
-				pf			
perties	FR	of Fig.1'.3 is given below		pf			
perties <b>ilename:</b>	FR 26-	of Fig.1'.3 is given below EENETINSTALLER-1484.TMP-366		pf			
perties ilename: reated Time: fodified Time: ile Size:	FR 26- 26- 7,0	of Fig.1'.3 is given below EENETINSTALLER-1484.TMP-366 01-2020 14:09:50 01-2020 14:09:50 99		pf			
perties ilename: created Time: dodified Time: ile Size: Process EXE:	FR 26- 26- 7,0 FR	of Fig.1'.3 is given below EENETINSTALLER-1484.TMP-366 01-2020 14:09:50 01-2020 14:09:50 99 EENETINSTALLER-1484.TMP	35806.				
perties ilename: created Time: dodified Time: ile Size: Process EXE: Process Path:	FR 26- 7,0 FR C:\	of Fig.1'.3 is given below EENETINSTALLER-1484.TMP-366 01-2020 14:09:50 01-2020 14:09:50 99	35806.		MP\FRE	ENETI	INSTAL
perties ilename: created Time: dodified Time: ile Size: Process EXE: Process Path: Run Counter:	FR 26- 26- 7,0 FR C:\/ 3	of Fig. 1'.3 is given below EENETINSTALLER-1484.TMP-366 01-2020 14:09:50 01-2020 14:09:50 99 EENETINSTALLER-1484.TMP USERSYAMALAYAPPDATAYLOCALYT	35806.		MP\FRE	ENETI	INSTAL
perties ilename: created Time: dodified Time: ile Size: Process EXE: Process Path: tun Counter: ast Run Time:	FR 26- 7,0 FR C:\/ 3 26-	of Fig. 1'.3 is given below EENETINSTALLER-1484.TMP-366 01-2020 14:09:50 01-2020 14:09:50 99 EENETINSTALLER-1484.TMP USERSYAMALAYAPPDATAYLOCALYT 01-2020 14:09:40	35806.		MP\FRE	ENETI	INSTAL
perties ilename: created Time: dodified Time: ile Size: Process EXE: Process Path: Run Counter:	FR 26- 7,0 FR C:\/ 3 26-	of Fig. 1'.3 is given below EENETINSTALLER-1484.TMP-366 01-2020 14:09:50 01-2020 14:09:50 99 EENETINSTALLER-1484.TMP USERSYAMALAYAPPDATAYLOCALYT 01-2020 14:09:40	35806.		MP\FRE		
perties ilename: created Time: dodified Time: ile Size: Process EXE: Process Path: tun Counter: ast Run Time:	FR 26- 7,0 FR C:\/ 3 26-	of Fig. 1'.3 is given below EENETINSTALLER-1484.TMP-366 01-2020 14:09:50 01-2020 14:09:50 99 EENETINSTALLER-1484.TMP USERSYAMALAYAPPDATAYLOCALYT 01-2020 14:09:40	35806.		MP\FRE		INSTAL
perties ilename: created Time: dodified Time: ile Size: Process EXE: Process Path: tun Counter: ast Run Time:	FR 26- 7,0 FR C:\/ 3 26-	of Fig. 1'.3 is given below EENETINSTALLER-1484.TMP-366 01-2020 14:09:50 01-2020 14:09:50 99 EENETINSTALLER-1484.TMP USERSYAMALAYAPPDATAYLOCALYT 01-2020 14:09:40	35806.		MP\FRE		
perties ilename: created Time: dodified Time: ile Size: Process EXE: Process Path: tun Counter: ast Run Time:	FR 26- 7,0 FR C:\/ 3 26-	of Fig. 1'.3 is given below EENETINSTALLER-1484.TMP-366 01-2020 14:09:50 01-2020 14:09:50 99 EENETINSTALLER-1484.TMP USERSYAMALAYAPPDATAYLOCALYT 01-2020 14:09:40	35806.		MP\FRE		
perties ilename: created Time: dodified Time: ile Size: Process EXE: Process Path: tun Counter: ast Run Time:	FR 26- 7,0 FR C:\/ 3 26-	of Fig. 1'.3 is given below EENETINSTALLER-1484.TMP-366 01-2020 14:09:50 01-2020 14:09:50 99 EENETINSTALLER-1484.TMP USERSYAMALAYAPPDATAYLOCALYT 01-2020 14:09:40	35806.		MP\FRE		

only a single result. The document was in ".pf" format. (Fig. 1'.5)



An enlarged view of Fig.1'.6 is given below.

Filename:	I2PBROWSER-INSTALL-WIN64-2.0-9FDEEEE1.pf
Created Time:	22-01-2020 23:30:24
Modified Time:	22-01-2020 23:30:24
File Size:	38,705
Process EXE:	I2PBROWSER-INSTALL-WIN64-2.0-BETA7_EN-US.EXE
Process Path:	C:\Users\amala\DOWNLOADS\I2PBROWSER-INSTALL-WIN64-2.0-BETA7_E
Run Counter:	3
Last Run Time:	22-01-2020 23:30:14
Missing Process:	No

A search for the keyword "compatibility.ini" gave two results.Both of them had the same data, which is about the version of the browser installed in the system.(Fig.1'.7)

Risa BC BC BC BC BC BC BC BC BC BC BC BC BC	List         Extract and the set of the set o	
Laution	tole options	v D consetblitviri >
		+ C Consecution
🖈 Quick access	Compatibility Date mouth as: 24-01-2020 13:06 Crussed amost AppDiate/Reaming/Montial/Energies, Type: Configuration settings Size: 199 bytes	
🛄 Desktop 👒	Compatibility Date modified 23-01-2020 (605	
Documents	Culters/umais/OneDrive/Desktop/UP Browner Aph. Typic Cartiguration settings Son 279 bytes	
Pictures #	Composituity-Notepad – 🗆 X	
cyber forensic	Rie Edit Format Wew Help	
New Volume (F)	[Compatibility]	
Screenshots	LastVersion-60.7.0_20109703010101/20109703010101	
SUBMITNOW	Last12PBrowserVersion=2.1 Last0SA81=wINNT_x86_64-gcc3	
Coophex	LastPlatformDir=C:USersiamala\GneDrive\Desktop\I2P Browser Alpha\Browser LastAppDir=C:USersiamala\GneDrive\Desktop\I2P Browser Alpha\Browser/browser	
OneDrive	neuroblever Prease of agerna (raises row) preserved (ros. 19:00000). Arbuild (19:00000), (10:00000)	
This PC		
3D Objects		
Desitop	Ln 7, Eck 1 102% Windows (CRLF) UT7-8	
B Documents		
- Downloads		
A Music		
Patures		
Videos		
WINDOWS IET		
New Volume (D		
New Volume (E)		
New Volume (F)		
RECOVERY (G)		
and the second second		
2 items 1 item selected	a no topoli	E
	Fig.1'.7	
	118.1,	

2. In Linux OS

Due to some technical issues related to the storage directory of the Freenet browser, it's data couldn't be collected. Only the data related I2P browser could be obtained.

i.) I2P

The location "admin///var/log/i2p" contained a file named "log-router-0-txt".When I examined this file, it revealed data regarding the installation of the browser including the installation date, time and timestamps of the browser each time it was launched. It is displayed in Fig.2'.1, Fig.2'.2 and Fig.2'.3 below.





Fig.2'.3

The same location contained a second file named "wrapper.log".It revealed data like, when each file directory was created and it also indicated details regarding setting up a new user directory.It is shown Fig.2'.4



Fig.2'.4

The location "/var/lib/dpkg/info" contained a file named "i2p-router.md5sums".The file had different md5 hash values for each directories listed in that.It is shown in Fig.2'.5.

tivities 📑 Text Editor +	Mur (10)	(Christian Christian Chris
Open = B	(2provier.milisoms (Read-Only)	
8787914293740031ec364c2525172349		
06200350052909213023510193046578	wir/bin/l2prowler-nowlepper wir/share/bash-completion/completions/eesdet	
	asr/share/doc/lip-router/READHE.Debian	
	us//share/doc/l2p-route/changelog.Deblam.g2	
	usr/share/doc/12p-router/changelog.gz	
ec2c38e3e7cb7a84d4137290816375db	usr/share/doc/l2p-router/copyright	
	vsr/share/doc/l2p-router/examples/scrlpts/l2pProxy.pac.gz	
and a set in the set of the tweet of a set of the base of the	vsr/share/doc/lip-router/licenses/ABOUT-Jetty.html usr/share/doc/lip-router/licenses/COPYING-BOB.txt	
	usr/share/doc/12p-router/licenses/LICENSE-Addressbook.txt	
	usr/shere/doc/l2p-router/licenses/LICENSE-BlockFile.tst	
	wsr/share/doc/l2p-router/llcenses/LICENSE-Boost.txt	
	usr/share/doc/lip-router/licenses/LICENSE-CC8-1.8-Universal.txt.gz usr/share/doc/lip-router/licenses/LICENSE-Cryptix.txt	
	usr/share/doc/t2p-router/licenses/LICENSE-besktopU/L.txt	
	usr/share/doc/lip-router/licenses/LICENSE-ECLIPSE-5.8.html	
	usr/shere/doc/i2p-router/licenses/LICENSE-ElGamalDSA.txt	
	usr/share/doc/l2p-router/licenses/LICENSE-FatCowIcons.txt	
	usr/share/doc/lip-router/licenses/LICENSE-Feather.txt usr/share/doc/lip-router/licenses/LICENSE-roupercoms.txt	
	usr/share/doc/12p-router/licenses/LICENSE-GPLy3.txt.az	
	usr/share/doc/lip-router/licenses/LICENSE-GeoIP.txt	
	ssr/share/doc/lzp-router/licenses/LICENSE-HashCash.txt	
	usr/share/doc/12p-router/licenses/LICENSE-I2PTunnel.txt	
	esr/share/doc/lip-router/licenses/LICENSE-Identicon.txt usr/share/doc/lip-router/licenses/LICENSE-Installert.txt	
	usr/share/doc/t2p-router/licenses/LICENSE-LGPLv3.txt.az	
583940483f4f5e77bc95fd42fbda1636	usr/share/doc/lip-router/licenses/LICENSE-Hinistreaming.txt	
	usr/share/doc/l2p-router/ticenses/LICENSE-NDT.txt	
	usr/share/doc/l2p-router/licenses/LICENSE-Molse.txt usr/share/doc/l2p-router/licenses/LICENSE-SH4256.txt	
	wsr/share/doc/l2p-router/ilcenses/LICENSE-SNIP.txt	
	usr/shore/doc/l2p-router/licenses/LICENSE-Scale.nd	
	usr/share/doc/t2p-router/ticenses/LICENSE-Stikicons.tat	
	us//share/doc/lip-router/Elcenses/LICERSE-UPAP.txt	
	war/shere/doc/lzp-router/llcenses/LICENSE-Undrew.txt war/share/doc/lzp-router/llcenses/LICENSE-Wrapper.txt.uz	
	usr/share/doc/lip-router/licenses/LICENSE-forked-subprocess_svift.txt	
	usr/shere/doc/l2p-router/litenses/LICDNSL-iBCrypt.txt	
	usr/share/doc/l2p-router/licenses/LICENSE-sbt-wrapper.txt	
	esr/share/doc/lip-router/licenses/NOTICE-Corwons-Logging.ixt	
	usr/share/doc/lzp-router/licenses/NDTICE-Jetty.html usr/share/lzp/certificates/familu/gostcoin.crt	
	usr/share/l2p/certificates/family/l2p-dev.crt	
	usr/share/l2p/certlficates/family/l2pd-dev.crt	
	usr/share/i2p/certificates/family/volatile.crt	
	usr/share/l2p/certificates/news/ampernand_at_gmail.con.crt	
	<pre>usr/share/lzp/certificates/news/echelon_al_mail.lzp.crt usr/share/lzp/certificates/news/hankhill19580_at_pmail.com.crt</pre>	
	usr/share/l2p/certificates/news/str4d at #all.12p.crt	
51e3ee6aa0413898a1fafb2c48a93fc7	usr/share/i2p/cert(Ficates/news/222_at_natl./2p.crt	
	usr/share/l2p/certificates/plugin/backup_st_nail.i2p.crt	
	usr/share/L2p/certificates/plugin/cacapo at mail.L2p.crt usr/share/L2p/certificates/plugin/strid at mail.L2p.crt	
1837e24947a7c492706841b6e6c34fa8	usrysma dylzdycurtyriaatee(pongo)siyad ac marc.tap.irt	PlainText + Tabwidth: 8 + (n1, Col ) + (H)
	Fig.2'.5	

The location "admin:///var/log" contained a file named "syslog", which was the system log.System log contains details regarding details regarding the processes running in the system. A search through the system log resulted in finding the time stamps of I2P browser. It is shown in Fig.2'.6 and Fig.2'.7.

Contre E	sydag	
denied		
1.40 (distance picture) communications and the end of the end o	<pre>add Successfully activated service 'arg.goome.ternhout' ' 'itt: hild: ' itt: hild: ' itt: hild: ' itt: hild: ' itt: hild:' ' itt: hild:'</pre>	et: 2p;2022bockground eet-shadow: 0 fox tpx //deabboard.snapcraft.x //deabboard.snapcraft.x r/share/jawa/serviet- sr/share/jawa/jsp red_helper* pid=7168 srofile/user: Permissic firefox-00.0.1-buildi/ /firefox-00.0.1-buildi/





The location "admin:///var/log" contained another file named "kern.log", which is the kernel log.Kernel log keeps a record of all the kernel processes.It contained details regarding the kernel process of the I2P.It is shown in Fig.2'.8 and Fig.2'.9.

N open + B		Madi 23213 kemilag	
Jan 24 15:45:32 solo-HP-Laptop-15-bsDux kernel: Jan 24 15:45:32 solo-HP-Laptop-15-bsBux kernel:	1 442.014580	usb 1-2: Product: Cruzer Blade usb 1-2: Nanufacturer: Sanblok	Q, 12P G 1 (1 / 26
Jan 24 15:45:32 solo-HP-Laptop-15-botax kernel: Jan 24 15:45:32 solo-HP-Laptop-15-bstax kernel:	442.014592   442.816171	usb 1-2: SerialNumber: 200128452007713007#71 usb storage 1-2:1.8: USB Nass Storage device detected scsl host3: usb-storage 1-2:1.0	
Jan 24 15:45:33 solo-HP-Laptop-15-babax kernel: Jan 24 15:45:33 solo-HP-Laptop-25-babax kernel:	[ 441.816403 [ 441.022456	<pre>scst htstb: utb-storage 1-211.0 scst 3:0:00:Direct-Access SanDish Cruzer Blode 1.27 PQ: sd 3:0:00:Direct-Access SanDish Cruzer Blode 1.27 PQ: sd 3:0:0:Direct-Access SanDish Cruzer Blode 1.27 PQ: sd 3:0:Direct-Access SanDish Cruzer Blode 1.27 PQ: sd 3:Direct-Access SanDish Cruzer Blode 1.27 PQ: sd 3:Direct-Access SanDish Cruzer Blode 1.27 PQ: sd 3:Direct-Access SanDish Cruzer Blode 1.27 PQ: sd 3:Direct-Blode 1.27 PQ: sd 3:Dir</pre>	0 ANSI: 0
Jan 24 15:45:33 solo-HP-Laptop-15-bsBxx kernel: Jan 24 15:45:31 solo-HP-Laptop-15-bsbxx kernel:	443.824421	sd 3:8:0:05 Attached acst generic sg2 type 0 ad 3:8:0:16 [adb] 7821812 512-byte legical blocks: (4.88 GB/3.73 G ad 3:0:0:05 [adb] Hitle Protect is off ad 3:0:0:05 [adb] Node Sense: 43 06 06 00	(18)
Jan 14 15:45:33 solo-HP-Laptop-15-bsftxx kernel: Jan 24 15:45:33 solo-HP-Laptop-15-bsftxx kernel: Jan 24 15:45:33 solo-HP-Laptop-15-bsftxx kernel:	443.028588 443.028588 443.028588	ad 3:00:000 [sdo] Write rotect is off ad 3:00:000 [sdo] Node Sense: 43:06:00:00 ad 3:00:00:0: [sdb] Write cache: disabled, read cache: enabled, does	a'r suenert 700 or Fild
Jan 24 15:45:33 sələ-HP-Laptop-15-bətxx kernel Jan 24 15:45:33 sələ-HP-Laptop-15-bətxx kernel:	443.04130Z	adb: sdb1 sd 3:0:0:0: [sdb] Attached SCSI removable disk	and a support a series of a suspective state
Jan 24 15:47:84 coln-HP-Laptop-15-bsfix karnel: Jan 24 16:03:17 solu-HP-Laptop-15-bsfix kernel:	531.966150	ush 1-2: USB disconnect, device number 6	stion="profile_luad" profile="unconfined" mame="system 🕎" pld=9785
conn="appartor parser" Jan 34 16:03:17 solp-HP-Lapton-15-bstax kernel:	1 1586 605209	audit: tupe=1400 audit/1570061997 361:262): appartur="STATUS" oper	ations'profile load' profiles'unconfined' sames'saster 120//
Senitized_helper* pid=9705 comm="eppermor_perse Jan 24 16:03:18 solo-HP-Laptop-15-bsBax kernel:	er <sup>5</sup> [ 1587,340824	audit: type=1400 audit(1579801998.885:263): apparmor="STATU5" open	ation="profile_load" profile="unconfined" mame="/usr/bim/logrouter"
pid=9712 core='appareor_parsor' Jen 24 16:03:18 solo-MP-Laptop-15-bs0as kernel:	[ 1587.340800	aud(t: type=1400 aud(t(1579061995.005:254): eppermor="STATU5" oper	ation="profile_load" profile="unconfined" name="/usr/bin/liproster//
Jan 24 16:83:19 sele-HP-Lanten-15-boffex kernel:	T 1588 832368	audit: type=1488 audit(1570861900.407:265): angarmor="Alid#ED" ope	ration="open" profile="system_ <mark>lip</mark> " name="/usr/share/java/servlet-apl.jar
pid=9765 covm="jeva" requested_reska"r" denied Jan 24 16:83:19 solo-HP-Laptop-15-0sDxx kernel: pid=9765 covm="java" requested_resks"r" denied	1588.847674	sudit: type=1468 sudit(1579861999.513:266); apparmor="ALLOWED" ope	eration="open" profile="system_ <mark>12p</mark> " same="/usr/share/java/jsp-api.jar"
Jan 24 16:18:25 solo-HP-Laptop-15-bofax kernel:	[ 2415-140562	audit: type=1400 audit(1579062905.024:207): appartor="DENIED" oper aude_1:" denied marke_1:" found=1000	ation="open" profile="snap.gnome-system-monitor.gnome-system-monitor"
Jan 24 16:18:20 solp-HP-Laptop-15-bebax kernel:	F 2418.984968	audit: type=1488 audit:1579862989.584:288): anparmor="DEMIED" oper	ation="upen" profile="snap.nnowe-system-monitor.onone-system-monitor"
Jan 24 10:18:29 solo-HP-Laptop-15-bsBxx kernel: name="/var/Tlb/snapd/desktop/applications/grome	[ 2418.905309 -logs_gnore-log	<pre>sudit: type=1480 audit(1579862905.584:269): apparate="DeNIED" oper s.decktop" pld:11687 comm:"gnome-system.no" requested mack="r" deni</pre>	wpks"" dented_mesks"r" fauldal000 oxida0 atlen="open" profile="snap.gnome-system-monitor". ad_maiks"r" fauldal000 oxida0
Jan 24 10:16:29 solo-MP-Leptup-15-bsdxx kernel: name="/var/ltb/snapd/desktop/applications/gnome	- 1 2418-903373 - characters on	<pre>sudtt: type=1460 sudtt(1579062909.504:270): sppermor='DENIED' oper me-characters.desktop' ptd=11687 comm='gnome-system-mo" requested m</pre>	stion="upen" profile="snap.groke-system-nonitor.gnoke-system-monitor" wsk*"r" denied wsk="r" fould=1000 ouid=0
<pre>Jan 24 16:18:31 cstb-HP-Laptop-15-bsBsx kernel: neme="/run/nount/utab" pld=II007 comm="gsome-sy</pre>	:[ 2421.871252 /sten-mo" reque:	audit: type=1488 audit(1576062911.753:271); apparmor="DENIED" oper ted_mask="r" denied_mask="r" fouid=1000 ouid=0	ation:"open" profile="snap.gnoxe-system-monitor.gooxe-system-monitor"
Jan 24 10:18:31 solo-HP-Laptop-15-bsDax kernel: name="/proc/985/attr/current" pld=11687 commerg	[ 2421.254881 mome-system-no	<pre>sudtt: type=1400 sudtt(1579562911.945:272): apparror="DENIED" oper requested_mask="r" denied_masks"r" fsuid=1600 outd=1600</pre>	ation="open" profile="snap.goome-system-nonitor.goome-system-nonitor" ation="open" profile="snap.goome-system-nonitor.goome-system-nonitor"
<pre>inter:/proc/l/cgroup* pid=11007 cove-3gnove-sys lan 24 1618133 solp-HP-Lancom.Co.bella</pre>	ten-no" request	<pre>ed_mesk='r' denied_mesk='r' fsuid=1000 ouid=0 suid=1 type=1600 audt/1575662012 A00-27511 annaronr_"Distin" open audt/1 type=1600 audt/1575662012 A00-27511 annaronr_"Distin"</pre>	ation="upon" profile="snap.graws-system-monitor_gname-system-Wohild?"
hammer'/proc/l/cgroup' pld=lidB7 comer'gnowe-ave Jen 24 Jd(JB:32 solo-HP-Lanton-15-bsDax kernell	tem-Ho" request	ed mask:"r" demied mask:"r" fould:1886 outdem sudit: type:1400 sudit(1575062912.009:270): supernor:"DTMTD" oper	ation="uppn" grotile="imap.goome-system-monitor.goome-system-monitor" ation="oppn" profile="imap.goome-system-monitor.goome-system-monitor"
<pre>neme='/proc/1/cgroup' pid=11067 comm='gnorme-ays Jan 24 16:18:32 solo-HP-Laptop-15-bsDox kernel:</pre>	ten-so" reques [ 2421.329700	ed_nesk="r" desied_nesk="r" fsuid=1000 ouid=0 sudtt: type=1480 sudit(1579862912.013:278): apparmor="DEWIED" oper	ation="open" profile="snap.gnome-system-momiltor-gnome-system-momiltor"
<pre>names'/proc/1/cgroup' pid=11687 comm='gnome-sys Jan 24 16:18:32 solo=MP-Laptop=15-bstax kernel:</pre>	ten-Ro* reques: [ 2421.329742	ed_masks"r" demied_masks"r" fsuid=1008 ould=0 _gudit: type=1400_gud(t(1579062912.013:279): gpg=rmur="DENIED" oper	ation:"open" prof(le:"snap.gnome-system-mon(tor.gnome-system-mon(tor"
<pre>name='/proc/i/cgroup' pid=11887 comm='gnome-sys Jan 14 16:18:37 solo-HP-Laptop-15-babax kernel:</pre>	iten-no" request [ 3421.329866]	ed_mask="r" demied_mask="r" fsuid=1800_ouid=0 _audit: type=1408_audit(1570862012.813:208): apparmor="DEMIED" oper	ation="upen" profile="snap.gnowe-system-monitor.gnowe-system-monitor"
Jan 24 16:18:38 solo-HP-Laptop-15-bsBox kernel:	2427.644657	kaudiid_printk_skb: 1029 callbacks suppressed	Plain Test. + Teb Width: 8 + Lin 1729, Col 185 +
		Fig.2'.8	
DANS: 🕱 Yeel Balan -		Nun 2013	÷ 41 6
Darks ∎ Vert£ator * ∱ open* ≝		Non 2013 kem.log	∓44β ≲wa #⊜6
Орил - Д рал 20 60142157 2010-07-Laptop-15-байжи кеглец Дал 28 68143157 2010-07-Laptop-15-байжи кеглец	11.950129	Nun 13113 ken log Ingert Höh Heret Holl Hölf/d-porte av Jacobier problemskykolog nör Ingert Höh Heret Holl Hölf/d-porte av Jacobier Problemskykolog nörd	도 41 G L1-3/150m0/car10/Appt13 L1-3/150m0/car10/Appt13 L1-3/150m0/car10/Appt13
Cpin* E Inn 20 00142157 3010-0F-Laptop-15-508xs wernets Inn 28 00143157 3010-0F-Laptop-15-568xs wernets Inn 28 00143157 3010-0F-Laptop-15-568xs wernet Inn 28 00143157 3010-0F-Laptop-15-basks wernet	111.0580521	Ann 2013 Mar 2013 Mar 2013 Mar 2014 Mar 2014 Ma	T 41 G Com = Com =
Cpuin A 20 (01/21/27 301/0-01/2 (01/20)-21/201/01 Kerret 1 2011 72 01/01/21/27 301/0-01/2 (01/20)-21/201/01 Kerret 1 2011 72 01/01/21/37 10/0-01/2 (01/20)-21/201/01 Kerret 1 2011 72 01/21/37 10/0-01/2 (01/20)-21/201/01 Kerret 1	[ 11.058052] [ 12.115985] [ 12.115988] [ 12.115988] [ 12.115989]	Non 2013 ken Jog Tupots Hold Seret Roll Hold Jop Jose an Adorberty Jop 2000/10/2008/1001 Tupots Hold Janes Roll Hold Jop Joe an Adorberty Josef Seret Hold Jones Tubal Jones Ford Hold Jop Joe Adorbert Ser Adorbert Seret Tubal Jones Ford Hold Job Adorbert Joe Adorbert Tubal Jones Ford Hold Job Adorbert Jones	r 44 β cow = trajsona/cara0/topit) trajsona/cara0/topit) Cup Cizata ∧ trajsona/cara0/topit)
Oper   prove  pr	[ 11.058052] [ 12.115985] [ 12.115983] [ 12.115983] [ 12.115989] [ 12.115991] [ 12.350350]	Man 2013 Marine Mari	τ 48 β 17.3/19040/card0/loput3 17.3/19040/card0/loput3 17.3/cound/card0/loput3 17.3/cound/card0/loput3
Open         El           Im 20 00110137         1010-00112000         1010000000000000000000000000000000000	[ 12.058952] [ 12.115985] [ 12.115983] [ 12.115983] [ 12.115983] [ 12.115991] [ 12.550300] [ 12.554892] [ 12.554892] [ 12.554972]	tom 2013 kom.log toput: HAN Intel FAH HANI/D joord a joorderjop/0009100/0009100/ toput: HAN Intel FAH HANI/D joord a joorderjop/0009100/ toput: HAN Intel FAH HANI/D joorderjog joorderjop/0009100/ toput: Ani Intel FAH HANI/D joorderjop/0009100/ HANI/Joorderjop/000000000000000000000000000000000000	r d β com = 17.3/sound/cari0/input3 17.3/sound/cari0/input3 17.3/sound/cari0/input3 17.3/sound/cari0/input3 17.3/sound/cari0/input3
Course 22 Course 22	[ 11.058052] [ 12.113983] [ 12.115983] [ 12.115983] [ 12.115983] [ 12.115983] [ 12.55050] [ 12.554052] [ 12.554052] [ 12.555173] [ 12.773384] [ 16.040505]	Mar 1513 kerning toput: Hok inter for Hoki/de person in device/priodening/voosing/ toput: Hok inter for Hoki/de person in device/priodening/source toput: Hok intel for Hoki/de person is device/priodening/source topit/and common: Found BAR, device topit/and topit/and BAR, device in device in the source in the source in the source in the source in the source in the source interview of the source in the source in the source in the source interview of the source interview of the source in the source interview of the source interview of the source interview of the source interview of the source interview of the source interview of the source interview of the source interview of the source interview of the source interview of	t\$f.]//sound/cardb/laput16
Open         D           Im 20 00114157 1000-00-120000 11-00000 wered 0           Im 20 00114157 1000-00-120000 11-00000 wered 0           Im 20 001157 1000-00-120000 wered 0           Im 20 001157 1000-00-12000 11-0000 11-0000 wered 0           Im 20 001157 1000-00-12000 11-0000 11-0000 wered 0           Im 20 001157 1000-00-12000 11-0000 wered 0           Im 20 001157 1000-00-12000 11-0000 11-0000 wered 0           Im 20 001157 1000-00-12000 11-0000 11-0000 11-0000 wered 0           Im 20 001157 1000-00	[ 11.0548052] [ 12.115980] [ 12.115980] [ 12.115980] [ 12.115980] [ 12.1550050] [ 12.550050] [ 12.550050] [ 12.550050] [ 12.550050] [ 12.550050] [ 12.550050] [ 12.551073] [ 12.773094] [ 10.040005] [ 19.617614] [ 20.900144]	Mon 2013 kom.iog Input: HAN Intel FAH HANT/DP.pcn-H m /device/pct0400100/10001000 (hast: HAN Intel FAH HANT/DP.pcn-H m /device/pct0400100:00: Hast: HAN Intel FAH HANT/DP.pcn-H m /device/pct0400100:00: Hast: Jack Intel FAH HANT/DP.pcn-H m /device/pct0400100:00: Hast: Jack Intel FAH HANT/DP.pcn-HANT HANT HANT HANT Hast Intel FAH HANT/DP.pcn-HANT HANT HANT HANT Hast Intel FAH HANT HANT HANT HANT HANT HANT HANT Hast Intel FAH HANT HANT HANT HANT HANT HANT HANT Hast Intel FAH HANT HANT HANT HANT HANT HANT HANT HA	iff.]/round/cardb/laputiS 2003005k r5 Gaull) Gaulti_Tottl_loat" profUs-"unconfined" name="system <mark>307</mark> " pld=887.
Open         D           1m         20         2017         2010         -110	[ 11.080023 [ 12.113903] [ 12.113903 [ 12.115903] [ 12.115903] [ 12.115901] [ 12.550130] [ 12.555130] [ 12.555130] [ 12.555130] [ 12.555130] [ 12.555130] [ 12.556130] [ 12.556130] [ 12.556143] [ 12.6906144] [ 20.900151]	Non 2013 kom.602 Input: H0A Intel CAH H0H/20, pcx-8 as /devices/pc10000.000/100/ Unot: H0A Intel CAH H0H/20, pcx-8 as /devices/pc10000.00/ H0A/2000 CAH H0H/20, pcx-8 as /devices/pc10000.00/H0H/2000 Intel/real.common: Found BAH. downin upcx- Intel/real.common: Found BAH. downin. down H0H/2000 CAH H0H/2000 CAH H0H/2000 H0H/2000 CAH H0H/2000 CAH H0H/2000 CAH H0H/2000 H0H/2000 CAH H0H/2000 CAH H0H/2000 CAH H0H/2000 H0H/2000 CAH H0H/2000 CAH H0H/2000 H0H/2000 CAH H0H/2000 CAH H0H/2000 H0H/2000 CAH H0H/2000 CAH H0H/20	iff.]/roound/card8/laputis 20030008 rS [mull] ουσ:"portla_load" profile="unconfined" name="system_ <mark>log</mark> ;" pld=88? ion="profile_load" profile="unconfined" name="system_log;/romitleed_belpe
Opport         D           Im 20 0015117         3010-01177         3010-01177         3010-01177<	[ 11.080612; 12.113980] [ 12.113980] [ 12.113980] [ 12.113980] [ 12.135001] [ 12.350030] [ 12.551002] [ 12	Mar 2013 ken kg tapott 105 Setel FoH MOST/JD.post (most HA Jatel FoH MOST/JD.post (most HA JATE) MOST/JD.post (most HA JATEL FOH MOST/JD.post (most HA JATEL FOH MOST/JD.post (most HA JATEL FOH MOST/JD.post (most HA JATEL FOH MOST/JD.post (most HA JATEL FOH HA HA JATEL (most HA JATEL FOH HA HA HA JATEL (most HA JATEL FOH HA HA HA HA (most HA JATEL FOH HA HA HA HA (most HA JATEL FOH HA HA HA HA HA (most HA JATEL FOH HA HA HA HA (most HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA HA (most HA HA HA HA HA HA HA HA HA HA (most HA HA (most HA	ist.J/cound/cardb/inputis 1001005k f5 [mull] non-"profile_load" profile-"unconfined" name-"system_ <u>DF</u> pid-887 ion-"profile_load" profile-"unconfined" name-"system_ <u>DF</u> //confiled.jmlpe ion-"profile_load" profile-"unconfined" name-"system_ <u>DF</u> //confiled.jmlpe
Open         D           In 20 00110137 1010-011-101000 were (1 101000000000000000000000000000000000	[ 11.080612; 12.113980] [ 12.113980] [ 12.113980] [ 12.113980] [ 12.135001] [ 12.350030] [ 12.551002] [ 12	Mon 2013     Mon 2013     Mon 201     Mon 201     Mon 20	<pre>isf.J/cound/cardb/inputis NoiJogik fs (unil) NoiJogik fs (unil) Noimprotlle_load* profile="unconfined" name="system_lip/cantized_helps ton="profile_load* profile="unconfined" name="(sbin/doclimit" pid=des ion="profile_load* profile="unconfined" name="(sbin/doclimit" pid=des ion="profile_load* profile="unconfined" name="(sbin/doclimit" pid=des ion="profile_load* profile="unconfined" name="(sbin/doclimit"); pid=des</pre>
Current D 10.00000000000000000000000000000000000	[ 11.08062] [ 12.113980] [ 13.113980] [ 13.113989] [ 13.113989] [ 13.113989] [ 13.113989] [ 13.113989] [ 13.113989] [ 13.135010] [ 13.5550103] [ 13.550103] [ 13.5	Even 2013     Even 201	<pre>if.J/cound/cardb/loputis  provide a set of the set</pre>
Course 20 In 20 0001111 20100-1112000-1112000 correct 10 20 0001111 20100-1112000-1112000 correct 10 20 00011111 20100-1112000 correct 10 20 00011111 20100-1112000 10 20 000111111 20100-1112000 10 20 000111111 20100-1112000 10 20 0001111111 20100-1112000 10 20 00011111111 10 20 0001111111111 10 20 000111111111 10 20 000111111111 10 20 000111111111 10 20 000111111111 10 20 000111111111 10 20 00011111111 10 20 000111111111 10 20 00000 10 20 000000 10 20 00000 10 20 000000 10 20 0000000 10 20 0000000 10 20 00000000 10 20 0000000000000 10 20 000000000000000000000000000000000	1         1.0.869623           12.1135993         12.1135993           12.1135993         12.1135993           12.1135993         12.1135993           12.1135993         12.3135993           12.1135993         12.3135993           12.1355937         12.3551273           12.3551273         12.3551273           13.9.6778244         10.9696143           1         10.9696143           20.9695137         10.962137           20.9692134         20.9692143           20.9692143         20.9692143	Even 2013     Even 201     Even 20	<pre>ist.j/cound/cardb/inputis  poinogk rs mull com*profile_load* profile="unconfined* name="system_bf" pid-d8? nom*profile_load* profile="unconfined* name="system_bf" pid-d8? nom*profile_load* profile="unconfined* name="/stim/dbcilent* pid-d88 nom*profile_load* profile="unconfined* name="/stim/dbcilent* pid-d88 nom*profile_load* profile="unconfined* name="/stim/dbcilent*.pid-d88 nom*profile_load*.profile="unconfined* name="/stim/dbcilent*.pid-d88 nom*profile="/stim/dbcilent*.profile="/stim/dbcilent*.profile#.p</pre>
Conv. 2 10.0001111/0000000000000000000000000000	1         1.0.869623           12.1135993         12.1135993           12.1135993         12.1135993           12.1135993         12.1135993           12.1135993         12.3135993           12.1135993         12.3135993           12.1355937         12.3551273           12.3551273         12.3551273           13.9.6778244         10.9696143           1         10.9696143           20.9695137         10.962137           20.9692134         20.9692143           20.9692143         20.9692143	Mine 2013 kern.dog Input: Hok Intel, Poi Hoki, //o, pon-B an / devices/pc10000100/100010001 Input: Hok Intel, Poi Hoki, //o, pon-B an / devices/pc100001001001 Intel, //auk.common: Frond BAR, down a public //auk.common: Frond BAR, down and come Intel, //auk.common.come Intel, //auk.common.come Intel, //auk.come Intel, //auk.common.come Intel, //auk.come Intel, //auk.common Intel, //auk.come Intel, //au	<pre>ist.j/cound/cardb/inputis  poinogk rs mull com*profile_load* profile="unconfined* name="system_bf" pid-d8? nom*profile_load* profile="unconfined* name="system_bf" pid-d8? nom*profile_load* profile="unconfined* name="/stim/dbcilent* pid-d88 nom*profile_load* profile="unconfined* name="/stim/dbcilent* pid-d88 nom*profile_load* profile="unconfined* name="/stim/dbcilent*.pid-d88 nom*profile_load*.profile="unconfined* name="/stim/dbcilent*.pid-d88 nom*profile="/stim/dbcilent*.profile="/stim/dbcilent*.profile#.p</pre>
Open         Description           In 30 0000000000000000000000000000000000	1.0.08862           12.1.13981           12.1.13981           12.1.13981           12.1.13981           12.1.13981           12.1.13981           12.1.35091           12.1.35091           12.55130	Even 2013     Even 201     Even 20	<pre>stl.j/cound/cardb/inputis poiloof# r5 (null) non="profile_load" profile="unconfined" name="system_log" pid=d87 non="profile_load" profile="unconfined" name="rystem_log"/sontitued_relpe ion="profile_load" profile="unconfined" name="/cbla/dbclumt" pid=d86 non="profile_load" profile="unconfined" name="/cbla/dbclumt" pid=d86 non="profile_load" profile="unconfined" name="/cbla/dbclumt" non="profile_load" profile="unconfined" name="/cbla/dbclumt" input profile_load" profile="unconfined" name="/unclafted" input profile_load" profile="unconfined" name="/unclafted" input profile_load" profile="unconfined" name="/unclafted" input profile_load" input profile_load" profile="unconfined" name="/unclafted" input profile_load" input profile_load" input profile_load" input profile="/unconfined" name="/unclafted" input profile="/unclafted" input profile=</pre>
Current D 10.00000000000000000000000000000000000	11.00002           12.11398           12.11398           12.11398           12.11398           12.11398           12.11398           12.11398           12.11398           12.11398           12.11398           12.11398           12.11398           13.55673           13.55673           14.55673           15.67734           15.67844           15.67934           16.990513           17.990514           17.990514           18.990513           19.990513           19.990513           19.990513	Even 2013     Even 201     Even 20	<pre>if.J/cound/cardb/loputis  S0010080 r5 Call CardII. CardII.Card* profile="unconflued" name="system_BT* pid=d87 cardIi.card* profile="unconflued" name="system_BT* pid=d87 cardIi.card* profile="unconflued" name="system_BT* pid=d87 card*profile_lard* profile="unconflued" name="/our/Dis/DistanctNamager/nn- lons*profile_lard* profile="unconflued" name="/our/Dis/DistanctNamager/nn- cons*profile_lard* profile="unconflued" name="/our/Dis/Dis/DistanctNamager/nn- cons*profile_lard* profile="unconflued" name="/our/Dis/Dis/Dis* Totion* profile="/our/Dis/Dis* Totion* profile" name="/our/Dis/Dis* Totion* profile="/our/Dis* Totion* profile" name="/our/Dis* Totion* profile" name="/our/Dis* Totion* profile" name="/our/Dis* Totion* profile" profile="/our/Dis* Totion* profile" name="/our/Dis* Totion* prof</pre>
Course 20 12010 001111 2010 0111 2010 1112000 01100000000	1	Mar 2013 Mar 2014 Mar 20	<pre>if.J/cound/cardb/loputiS  Soliopia r5 Call CardII Car</pre>
Open         Description           1m         2m	1648652           115986           1.215986           1.215986           1.215986           1.215986           1.215986           1.215986           1.215986           1.215986           1.215986           1.215986           1.215986           1.215986           1.255173           1.255173           1.255173           1.255173           1.255173           1.255173           1.255173           1.255173           1.255173           1.255173           1.255173           1.255173           1.255173           1.259180           1.259180           1.259180           1.259180           1.259180           1.2591803           1.2591803           1.2591803           1.2591803           1.2591803           1.2591803           1.2591803           1.2591803           1.2591803           1.2591803           1.2591803	Mar 2013 km.0g Input: HoA intel for HoA/JA/Les a /doi/ap.com/a /doi/ap.com/ap	<pre>iff.J/cound/cardb/inputis boiloopk r5 (auil) ons"portle_load" profile="unconfined" name="system_me" pid=887 (auil) ons"portle_load" profile="unconfined" name="system_me" pid=887 (auin) ons"portle_load" profile="unconfined" name="/doi/little/loader/nm= configrentle_load" profile="unconfined" name="/unconfised" name="/unconfined" name="/unconfined" name="/unconfined" name="/unconfined" configrentle_load" profile="unconfined" name="/unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfigrentle_load" configrentle_load" profile="unconf</pre>
Course 2 1. 20 001131 200-01 2000 10 2000 10 2000 10 2000 1. 20 001131 200-01 2000 10 2000 10 2000 1. 20 001131 200-01 2000 1. 20 001131 2000 1. 20 001131 2000 1. 20 0001	11.00002           12.11500           12.11500           12.11500           12.11500           12.11500           12.11500           12.15000           12.15000           12.15000           12.15000           12.15000           12.15000           12.55000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           13.0000           14.0000           13.00000           12.0000000           13.000000           13.0000000           14.0000000           13.00000000           13.00000000           14.0000000000           13.000000000000000000000000000000000000	Man 2013 Man 201 Jack Jones Add Mal/Jack Jones as /documents/pit/doinadocuments/ Tabue: Ibb Jines Jone Mal/Jack Jones as /documents/ Tabue: Ibb Jines Jone Mal/Jack Jones as /documents/ Tabue: Ibb Jines Jone Mal/Jack Jones as /documents/ Tabue: Ibb Jines Jones Jone	<pre>iff.J/cound/cardb/inputis boiloopk r5 (auil) ons"portle_load" profile="unconfined" name="system_me" pid=887 (auil) ons"portle_load" profile="unconfined" name="system_me" pid=887 (auin) ons"portle_load" profile="unconfined" name="/doi/little/loader/nm= configrentle_load" profile="unconfined" name="/unconfised" name="/unconfined" name="/unconfined" name="/unconfined" name="/unconfined" configrentle_load" profile="unconfined" name="/unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfigrentle_load" configrentle_load" profile="unconf</pre>
Courter         Description           10.00000000000000000000000000000000000	1         1.0.60822           1         1.2.1380           1         1.3.1380           1         1.3.1380           1         1.3.1380           1         1.3.55023           1         1.5.5522           1         1.5.5522           1         1.5.5522           1         1.5.5522           1         1.5.5522           1         1.5.5522           1         1.5.5522           1         1.5.5522           2         1.5.5522           3         1.5.5522           3         1.5.5522           4         1.5.5522           4         1.5.5522           5         1.5.5522           5         1.5.5522           6         1.5.5522           6         1.5.5522           7         1.5.5522           1         1.5.5522           2         1.5.5522           2         1.5.5522           2         1.5.5522           2         1.5.5522           2         1.5.5522           2         1.5.5522           2         1.5.5522	Sum 2013     Sum 2013     Sum 2013     Sum 201	<pre>iff.J/cound/cardb/inputis boiloopk r5 (auil) ons"portle_load" profile="unconfined" name="system_me" pid=887 (auil) ons"portle_load" profile="unconfined" name="system_me" pid=887 (auin) ons"portle_load" profile="unconfined" name="/doi/little/loader/nm= configrentle_load" profile="unconfined" name="/unconfised" name="/unconfined" name="/unconfined" name="/unconfined" name="/unconfined" configrentle_load" profile="unconfined" name="/unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfigrentle_load" configrentle_load" profile="unconf</pre>
Capure 10           In 10 0001117 solar in Luppo 11 solar served in 10 0001117 solar in 10 0001117 solar in Luppo 11 solar served in 10 0001117 solar in Luppo 11 solar served in 10 0001117 solar in Luppo 11 solar served in 10 0001117 solar in 10 0001117 solar in 10 0001117 solar in 10 0001117 solar in 10 000000000000000000000000000000000	1         1.0.60822           1         1.1.1580           1         1.1.1580           1         1.1.1580           1         1.1.1580           1         1.1.1580           1         1.1.1580           1         1.1.1580           1         1.1.1580           1         1.1.1580           1         1.0.64702           1         1.0.64702           1         1.0.64702           1         1.0.64702           1         1.0.64702           2         0.090131           1         20.900130           1         20.900130           1         20.900130           1         20.900130           1         20.900130           1         20.900130           1         20.900130           1         21.900030           1         21.900030           1         21.900030           1         21.900030           1         21.900030           1         21.900030           1         21.900030           1         21.9000303           1 <t< td=""><td>Mar 2013 km.log Input: HoA intel for HoA/J/D/cs.pcm4 as /device/pc10000.00/0000000 (moti HoA intel for HoA/J/D/cs.pcm4 as /device/pc100000.00/0000000 (moti HoA intel for HoA/J/D/cs.pcm4 as /device/pc10000000000000 (moti HoA intel for HoA/J/D/cs.pcm4 as /device/pc1000000000000000000000000000000000000</td><td><pre>isf.J/cound/cardb/inputis boiloopk r5 (auil) boiloopk r5 (auil) boiloopk r5 (auil) boin*portile_load* profile="unconfined* name="system_logi/cantited_helpe con*portile_load* profile="unconfined* name="/doi/logi/cantited_helpe con*portil_load* profile="unconfined* name="/doi/logi/cantited_helpe con*portile_load* profile="unconfined* name="/doi/logi/cantited#ili con*portile_load* profile="unconfined* name="/doi/logi/cantited#ili con*portile_load* profile="unconfined* name="/doi/logi/cantited*/doi/lo</pre></td></t<>	Mar 2013 km.log Input: HoA intel for HoA/J/D/cs.pcm4 as /device/pc10000.00/0000000 (moti HoA intel for HoA/J/D/cs.pcm4 as /device/pc100000.00/0000000 (moti HoA intel for HoA/J/D/cs.pcm4 as /device/pc10000000000000 (moti HoA intel for HoA/J/D/cs.pcm4 as /device/pc1000000000000000000000000000000000000	<pre>isf.J/cound/cardb/inputis boiloopk r5 (auil) boiloopk r5 (auil) boiloopk r5 (auil) boin*portile_load* profile="unconfined* name="system_logi/cantited_helpe con*portile_load* profile="unconfined* name="/doi/logi/cantited_helpe con*portil_load* profile="unconfined* name="/doi/logi/cantited_helpe con*portile_load* profile="unconfined* name="/doi/logi/cantited#ili con*portile_load* profile="unconfined* name="/doi/logi/cantited#ili con*portile_load* profile="unconfined* name="/doi/logi/cantited*/doi/lo</pre>
Current D 10.00000000000000000000000000000000000	11.04882           12.11380           12.11380           12.11380           12.11380           12.11380           12.11380           12.11380           12.11380           12.11380           12.11580           12.11580           12.11580           12.11580           12.11580           13.1580           13.0580           14.55520           15.5520           15.5520           14.55520           15.55620           15	Even 2013     Even 201	<pre>iff.J/cound/cardb/inputis boiloopk r5 (auil) ons"portle_load" profile="unconfined" name="system_me" pid=887 (auil) ons"portle_load" profile="unconfined" name="system_me" pid=887 (auin) ons"portle_load" profile="unconfined" name="/doi/little/loader/nm= configrentle_load" profile="unconfined" name="/unconfised" name="/unconfined" name="/unconfined" name="/unconfined" name="/unconfined" configrentle_load" profile="unconfined" name="/unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfined" name="/unconfigrentle_load" configrentle_load" profile="unconfigrentle_load" configrentle_load" profile="unconf</pre>
Control 2011 Control 2012 Control 2012 Co	11.04882           11.11589 <t< td=""><td>Man 2013 Man 20 Hanning Handrid Hanner (1997) Handrid Handrid Handr</td><td><pre>iff.J/cound/cardb/loput15 Seliops r5 Call SeniProfile_load" profile="unconflued" name="system_Eff" pid-d87 Call SeniProfile_load" profile="unconflued" name="system_Eff" pid-d87 Cann="profile_load" profile="unconflued" name="ysstem_Eff" pid-d81 Cann="profile_load" profile="unconflued" name="ysstem_Unit/DagFrouter" pid-d81 Cann="profile_load" profil</pre></td></t<>	Man 2013 Man 20 Hanning Handrid Hanner (1997) Handrid Handrid Handr	<pre>iff.J/cound/cardb/loput15 Seliops r5 Call SeniProfile_load" profile="unconflued" name="system_Eff" pid-d87 Call SeniProfile_load" profile="unconflued" name="system_Eff" pid-d87 Cann="profile_load" profile="unconflued" name="ysstem_Eff" pid-d81 Cann="profile_load" profile="unconflued" name="ysstem_Unit/DagFrouter" pid-d81 Cann="profile_load" profil</pre>
Courter         Description           11.1         20.00111317         20.001114117         20.00111417         20.00111417           11.1         20.00111317         20.00111417         20.00111417         20.00111417           11.1         20.00111417         20.00111417         20.00111417         20.00111417           11.1         20.001117         20.00111417         20.00111417         20.00111417         20.00111417           11.1         20.001117         20.00111417         20.00111417         20.00111417         20.00111417         20.00111417           11.1         20.001117         20.00111417         20.00111417         20.00111417         20.00111417         20.00111417           11.1         20.0011147         20.00111417         20.001	1         1.04862           1         1.04862           1         1.01980           1         1.01980           1         1.01980           1         1.01980           1         1.01980           1         1.01980           1         1.01980           1         1.01980           1         1.01980           1         1.01980           1         1.01980           1         1.01980           2         0.002181           1         0.002181           2         0.002181           1         0.002181           2         0.002181           1         0.002181           1         0.002181           1         0.002181           1         0.002181           1         0.002181           1         0.002181           1         0.002181           1         0.002181           1         0.002181           1         0.002181           1         0.002181           1         0.002181           1         0.002181	Mar 2019 Mar 20	<pre>iff.J/cound/cardb/loput15 Seliops r5 Call SeniProfile_load" profile="unconflued" name="system_Eff" pid-d87 Call SeniProfile_load" profile="unconflued" name="system_Eff" pid-d87 Cann="profile_load" profile="unconflued" name="ysstem_Eff" pid-d81 Cann="profile_load" profile="unconflued" name="ysstem_Unit/DagFrouter" pid-d81 Cann="profile_load" profil</pre>
Course 2 1. 2010 01313 2010 01 12100 12 5000 00 000000 1. 2010 01313 2010 01 12100 12 5000 00 00000 1. 2010 01313 2010 01 12000 12 5000 00000 1. 2010 01313 2010 01 12000 12 50000 00000 1. 2000 01313 2010 01 12000 12000000000000	1         1.0.60822           1         1.0.1080           1         1.0.1080           1         1.0.1080           1         1.0.1080           1         1.0.1080           1         1.0.1080           1         1.0.1080           1         1.0.0020     <	Mar 2013 tennog tenver 105 inter Coll BD///Disc. tenver 105 inter Coll	<pre>stf.l/sound/cardb/loputiS Doiloolk r5 (aull) Doim*portle_load* profile="unconfined* name="system_me" pid-dd? (aull) Doim*portle_load* profile="unconfined* name="routed_thetaet</pre>
Open         District State           100         <	1         1.0.60852           1         1.0.1080           1         1.0.1080           1         1.0.1080           1         1.0.1080           1         1.0.1080           1         1.0.1080           1         1.0.1080           1         1.0.0080           1         1.0.0080           1         1.0.0080           1         0.008010     <	Mar 2019 Mar 20	<pre>stf.j/second/cardBy/input15 boildock r5 (aull) boildock r5 (aull) boildock r5 boildoc</pre>

#### CONCLUSION:

Acknowledging the above results, a forensic investigator could find/prove:

- i. The use of the browsers by the criminal.
- ii. The time/date of installation of the browsers.
- iii. The last execution time/date.
- iv. Configuration files
- v. Installation directory

The fact that details regarding :

- i. Downloaded files,
- ii. Titles of webpages visited,
- iii. HTTP header information
- iv. Any URL,etc.

were not found points out the high level of security that these browsers provide for their users. The browser does not write any browsing data permanently to the hard drive. Right after closing the browser, all the data regarding browsing are deleted by the browser itself. The investigator will have to further more rely on more advanced tools/software to acquire more useful kind of information, even though the chances of obtaining such useful information are very narrow. The increase in crimes using such browsers have also increased the demand for an effective and reliable tool and methodology for collection and analysis of these browsing data. This research fulfilled its aim and have provided the promised results, including a detailed overview on how to install and launch the mentioned privacy browsers.

# **Chapter VI**

### **REFERENCES:**

- John Doe (2016), TOR Browser Forensics-Introduction to Darknet. URL: htts://www.dataforensics.org/tor-browser-forensics
- 2. Aron Warren (2017), Tor Browser Artifacts in Windows 10. SANS Institute.
- Mattia Epifani,Marco Scarito and Francesco Picasso(2015),Tor Forensics on Windows OS. URL:http://dfrws.org

4. Matt Muir,Petra Leimich and William J Buchanan (2019), A Forensic Audit of Tor Browser Bundle. URL:https://arxiv.org

- 5. https://github.com/datorrukis/freenet
- 6. https://en.m.wikipedia.org/wiki/Deep\_web
- 7. https://freenet.org

8. https://whatis.techtarget.com/definition/HORNET-high-speed-onion-routing-network.

- 9. https://geti2p.net/en/
- 10. https://sqlitebrowser.org
- 11. https://www.systoolsgroup.com/sqlite-database-recovery.html