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.^[6]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.^[7]

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.^[8]

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.^[9]

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.^[10]

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.^[11]

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).^[4] 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).^[2]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).^[3]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)









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)

	A Real Stars	Mange Downtooth View application tools		- E X	0		-2
Amal A.S Driver Easy	Windowske 🗧 💉 🗎 🗋 🛔	Capypath Social Moles Copy Delete Reserve	New Class steps - Properties	Open * Select al Lite Select rome History Elliveri selectori	College of the local division of the local d		scanner,
(2)	H Detroit	Drgaven	New Idea	Select	<u></u>		
Firefax und-it	DreDrive A	Custom Setup Telect the way you sumt features to be initia		Sar	*	1.0	golang o
	This PC	Cleft the core in the tree below to change it	er way features will be installed.	tale. 1582.03	M		A Dec
Edgel	Brower Desitop Brower Dournests Cyberlisk WPS Office Stope	v	The complete participation of the complete participation of the complete co	25, 750 KB 70, 766 KB 80, 311 KB 19080- 1, 899 KB			Namiyo Achia Nanyo
VMware Windoarti.	Telegram Desk 8-jpeg-saarch 105-WNRT93W-* 105-WNRT93W-* 105-WNRT93W-*	unation: 20/Fragren Files(24 ikous	433 on your hard drive.	01/17 - 2013 pture 12,001 00 pture 100	-	×	Cybersec Analyst D
Recycle Bin McAlee®	amalapproj. admission iestawi						
LEDAY Monter	Mpriject TeamViewer			-	1		
100 C	to const	o 🗄 🐂 🙆 🖨 I	60			No no no no no	01106



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)

At natitation At natitation At samh again in * 10 Location	Py Kind * Image: Construction of the second controls * Dates Sates * Advected controls * Dates Other properties * Image: Construction of the second controls * Dates Other properties * Image: Construction of the second controls * Dates Other properties * Image: Construction of the second controls * Dates Other properties * Image: Construction of the second control of the second	Case seath			
Sean	th Results in prefetch			- D freeset	
Cuick access	FREENETTRAY, EXE-EE6058EE.pf	Type P\$ File	Date modified; 25-01-2020 16:19 Size: 27.2 XB		
Desktop Downloads Downloads	FREENETWRAPPER-64.EXE-20897E07.pf	Type: PF File	Date modified: 25-01-2020 14:29 - Side: 7,25 KB		
Pictures	FREENETINSTALLER-1484.TMP-6A677FE1.pf C/Windows/prefetch	Type: PF File	Data modified 25-01-2026 1409 Size 6.94 KB		
New Volume (F)	FREENETINSTALLER-1484.TMP-36635806.pf C:Windows/prefetch	Type: PF File	Clate modified: 25-01-2020 14.09 Size: 6.93 KB		
SUBMITHOW Display OneDrive	FREENETINSTALLER-1484.EXE-2C0CC056.pf	Type: PF File	Clate modified 26-01-2020 1409 Stor: 637 KB		
This PC 3D Objects Desktop					
Documents Downloads					
Pictures					
WINDOWS (C)					
> New Volume (E) > New Volume (F)					
RECOVERY (G)					
IPM .					E-8
			$\mathbf{E}_{i\alpha}$ 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.



A T Nother transmission			a n x	1		40) Fleetet
Desktop # X A Ra C	na Help		~ ~ ~				
Downloads / Filename , Propertie Documents / BREFOXEXE	-		× s	Find Brid shat: Treenet		×	
Pictures # FRENETAS Create	ome: ed Time:	FREENETTRAY.EXE-EE6050EE.pt 26-01-2020 14:19:30	EAST-TEC IV IADS/FREENE	Match shale word only	Dector.	Cancel	
New Yolane (F) FREENETING Modil Scientification (Comparison of Comparison of Compariso	lied Time: lize:	26-01-2028 16:19:15 27.908	IdeaLOCAL\II IdeaLOCAL\II IdeaLOCAL\II	U MACH Case	1947.940		
	us EXE:	FREENETTRAY.EXE	Local/Freene				
Receive Flerame / Proce	iss Path: Counter:	CSUserstamalajAppDatajLoca/Freenet/FHLENETTH&YIXE 0		1			
ans PC AdvAPIGEDL Last F 3D Objects AMSEDLL Missis	Run Time: ing Process;	26-01-2020 16:19:09, 26-01-2020 16:18:37, 26-01-2020 16:17:11, 26-01 No	2020				
Desktop APPHELP DL Documents DOLYFT.DLL		OK					
Downloads BCRVPTPRBMITNES.DU Mulic CFGMGR32.DU	L C\Windows C\Windows	System 32:BERVPTIPRIML VOLUME(21)41473746446cb-da 754b. 15 System 32:clgrog 32:all VOLUME(21)41473746446cb-da 754b. 55					
Videos							
WihiDOWS (C3 New Volume (D.							
New Volane (F)							
v v							
		F1g.1'.4					
n enlarged vi	ew c	Fig.1'.4	ow.				
n enlarged vi ^{perties}	ew c	Fig.1'.4	ow.				
n enlarged vi ^{perties} ilename:	ew c	Fig.1'.4 of Fig.1'.3 is given bel	ow. 6635806.	pf			
n enlarged vi ^{perties} ilename: created Time:	ew c	Fig. 1'.4 of Fig. 1'.3 is given bel ENETINSTALLER-1484.TMP-3	ow. 6635806.	pf			
n enlarged vi perties Tilename: Created Time: Modified Time:	ew c FRE 26-0 26-0	Fig.1'.4 of Fig.1'.3 is given bel EENETINSTALLER-1484.TMP-3 11-2020 14:09:50	ow. 6635806.	pf			
n enlarged vi ^{perties} ilename: Created Time: Modified Time: ile Size:	ew c FRE 26-1 7,09	Fig. 1'.4 of Fig. 1'.3 is given bel EENETINSTALLER-1484.TMP-3 01-2020 14:09:50 01-2020 14:09:50	ow. 6635806.	pf			
n enlarged vi perties ilename: Created Time: Modified Time: ile Size: Process EXE:	ew c FRE 26-1 7,09 FRE	Fig. 1'.4 of Fig. 1'.3 is given bel EENETINSTALLER-1484.TMP-3 01-2020 14:09:50 01-2020 14:09:50 09 EENETINSTALLER-1484.TMP	ow.	pf			
n enlarged vi perties ilename: created Time: dodified Time: ile Size: Process EXE: Process Path:	ew c FRE 26-1 7,09 FRE C:\L	Fig. 1'.4 of Fig. 1'.3 is given bel EENETINSTALLER-1484.TMP-3 D1-2020 14:09:50 D1-2020 14:09:50 D9 EENETINSTALLER-1484.TMP USERS\AMALA\APPDATA\LOCA	ow. 6635806. \TEMP\IS	pf S-UMMI4.TI	MP\FRE	ENET	INSTAL
n enlarged vi perties ilename: ireated Time: ile Size: Process EXE: Process Path: Run Counter:	ew c FRE 26-0 7,09 FRE C:\U 3	Fig. 1'.4 of Fig. 1'.3 is given bel ENETINSTALLER-1484.TMP-3 01-2020 14:09:50 01-2020 14:09:50 09 ENETINSTALLER-1484.TMP ISERS\AMALA\APPDATA\LOCA	оw. 5635806. \ТЕ МР\! !	pf S-UMMI4.TI	MP\FRE	ENET	INSTAL
n enlarged vi perties ilename: Created Time: Aodified Time: ile Size: Process EXE: Process Path: Aun Counter: ast Run Time:	ew c FRE 26-1 7,09 FRE C:\U 3 26-1	Fig. 1'.4 of Fig. 1'.3 is given bel EENETINSTALLER-1484.TMP-3 01-2020 14:09:50 01-2020 14:09:50 09 EENETINSTALLER-1484.TMP USERSYAMALAYAPPDATAYLOCA 01-2020 14:09:40	OW. 6635806. \TEMP\IS	pf S-UMMI4.TI	MP\FRE	ENET	INSTAL
n enlarged vi perties ilename: Created Time: Modified Time: ile Size: Process EXE: Process Path: Run Counter: ast Run Time: Missing Process:	ew c FRE 26-1 7,09 FRE C:\L 3 26-1 Yes	Fig. 1'.4 of Fig. 1'.3 is given bel EENETINSTALLER-1484.TMP-3 01-2020 14:09:50 01-2020 14:09:50 09 EENETINSTALLER-1484.TMP ISERS\AMALA\APPDATA\LOCAN 01-2020 14:09:40	OW. 6635806.	pf S-UMMI4.TI	MP\FRE	ENET	INSTAL
n enlarged vi perties ilename: reated Time: dodified Time: ile Size: Process EXE: Process Path: lun Counter: ast Run Time: fissing Process:	ew c FRE 26-1 7,09 FRE C:\L 3 26-1 Yes	Fig. 1'.4 of Fig. 1'.3 is given bel EENETINSTALLER-1484.TMP-3 D1-2020 14:09:50 D1-2020 14:09:50 D9 EENETINSTALLER-1484.TMP USERS\AMALA\APPDATA\LOCAL D1-2020 14:09:40	OW. 6635806.	pf S-UMMI4.TI	MP\FRE	ENETI	INSTAL
n enlarged vi perties ilename: reated Time: Aodified Time: ile Size: Process EXE: Process Path: Aun Counter: ast Run Time: dissing Process:	ew c FRE 26-1 7,09 FRE C:\L 3 26-1 Yes	Fig. 1'.4 of Fig. 1'.3 is given bel EENETINSTALLER-1484.TMP-3 01-2020 14:09:50 01-2020 14:09:50 09 EENETINSTALLER-1484.TMP USERSYAMALAYAPPDATAYLOCA 01-2020 14:09:40	OW. 6635806.	pf S-UMMI4.TI	MP\FRE	ENET	INSTAL
n enlarged vi perties ilename: Created Time: Aodified Time: ile Size: Process EXE: Process Path: Run Counter: ast Run Time: Aissing Process:	ew c FRE 26-1 7,09 FRE C:\U 3 26-1 Yes	Fig. 1'.4 of Fig. 1'.3 is given bel EENETINSTALLER-1484.TMP-3 11-2020 14:09:50 11-2020 14:09:50 19 EENETINSTALLER-1484.TMP USERS\AMALA\APPDATA\LOCA 11-2020 14:09:40	OW. 6635806. \TEMP\IS	pf S-UMMI4.TI	MP\FRE	ENET	INSTAL

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_EN
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)

Carriert lokker Rea PC Search again in * Location	Polist -		
	terch Results in WINDOWS (C)		v D consetbility ini >
* Quick access	Compatibility Collering anyon Application Real in proVidential Ferdian. Type: Configuration setting:	Date multifiest: 24-01-2020 13:06 Star: 199 bytes	
Desidop P Downloads	Compatibility ColumnianOneOner/Desktop/NZP Browser Alph_ Type: Configuration settings	Dane modified: 23-01-2020 1603 Son: 276 bytes	
Pictures #	Compatibility - Notepad	- 0 ×	
cyber forensic	Bie Erit Format West Help	ANN 47 922	
New Volume (F)	[Compatibility]	*	
Screenshots	LastVersion-60.7.0_20109703010101/20109703010101		
SUBMITNOW	LastOSABI=WINNT_X86_64-gcC3		
Urophox	LastPlatformDir=C:\Users\amala\OneDrive\Desktop\I2P Browser Alpha LastAppDir=C:\Users\amala\OneDrive\Desktop\I2P Browser Alpha\Brow	s\Browser ser\browser	
OneOrive	and address of a base of an and the provided of the second state o		
This BC			
T SDOMAGE			
Desiton	Ln 7, Gel 1 100%	Windows (CRLF) UTF-8	
Di Documents			
- Downioads			
A Music			
Patures			
Videos			
WINDOWS IET			
- New Volume (D			
👞 New Volume (E.)			
- New Volume (F)			
RECOVERY (G)			
A dama a dama a da a da	The largest		
and a start starting			1.0
	Fig.	17.7	
	8-		

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.

ectivities 🔚 Text Editor +		- 44 🔒 -
Open- 8	izp-router, edisums (Reed-Only)	
Image: State	<pre>inf / Dirty Taging inf / Dirty Taging i</pre>	

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.

Conver B cycle Statistics Science Addressing Science Science Science Science Science Science Science Science Science
<pre>detid 2.m 31 sign:22 clo.eP.lptop.15.dotx dbuc.daren[110]; [section 41d-1000 pid-tt0] Activating via systemd; service name-imp_group.Iertial' im 1.eP (idd:Domp pid:Dr); comm-swellin-obstep "lobe: sectors" 2.m 31 sign:22 clo.eP.lptop.15.dotx dbuc.daren[110]; [section 41d-1000 pid-tt0] 2.m 31 sign:22 clo.eP.lptop.15.dotx dbuc.daren[110]; [section 41d-1000 pid-tt0] sectors.fully activated service 'emp_group.Terninal' 2.m 31 sign:22 clo.eP.lptop.15.dotx dbuc.daren[110]; [section 41d-1000 pid-tt0] sectors.fully activated service 'emp_group.Terninal' 2.m 31 sign:22 clo.eP.lptop.15.dotx dbuc.dbuc.dbuc.dbuc.dbuc.dbuc.dbuc.dbuc.</pre>
<pre>Sun 25 155:12 Sole=P-14000:15-bank systemic-resolved[sml] Using degraded feature set (umr) for mos ierer 157:136.45.1. Bank 15 155:02 Sole=P-14000:15-bank org.gome.Ball.debx(0)1350]: [/mr/clM/ifrefM/ifrefM/iScS):Sole=P-14000:15:156:029.465: Usable to a datad Control (Streep Consecution) (Content Context, User 158 Context, Usable Context, Usabl</pre>





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.

Jan 24 15145152 Solo-HF-Laptop-15-oblast Kernel	: 442.014583 uSD 1-2: Product: Lruier Blade
Jan 24 15:25:32 cale MD Lanton 15 holes have	- f dat mid-spill sch 1.2- Banufarturer: Sandisk
Jan 24 15:45:32 soln-HP-Laptop-15-bstax kernel	1 442.044501 300 1-2 Amulatian : Salota (442.04452) 300 1-2 Serial Manufer: 2002645200773301AF1
Jan J4 15:45:32 Selo-HP-Laptop-15-bstmx kernel Jan J4 15:45:33 selo-HP-Laptop-15-bstmx kernel	1 442.816273] HIGH THOMBE 1-211.01 LISE ALSS STOTAGE DEVICE DETECTED 2 [442.816403] HCSL htts: utb-storage 1-211.0
Jan 24 15:45:53 solo-HP-Laptop-15-bs8xx kernel Jan 24 15:45:33 solo-HP-Laptop-15-bs8xx kerne?	1 443.022455] xsci 3:0510:0: biret-Access :SanDish Cruzer Divide 1.27 PQ: 0 AKSI: 0 1 443.02242] xd 3:0500: bitached assi généric sgl Xype 0
Jan 24 13:45:31 soln-HP-Laptop-15-bstxx kernel Jan 24 13:45:33 solo-HP-Leptop-15-bstxx kernel	: [441.008340] x4 3:0:0:0: [x0] M21512 532-8y5e log(zal blocks: (4.86 68/3.73 GL8) : [443.00757] x4 2:0:0: [x0] M14: Protect is off
Jan 24 15:45:33 solo-HF-Laptop-15-bsBxx kernel Jan 24 15:45:31 solp-HF-Laptop-15-bsBxx kernel	1 441.023585 14 120:00:05 [14b] Node Sense: 43.00 00 00 1 441.02003 14 13:00:05 [14b] Node Sense: 43.00 00 nad caches english, doecn't support 200 or FUA
Jan 24 15:45:33 selo-HP-Leptop-15-betax kernel	1 449.045202] adds sdb1
Jan 24 15:47:84 coln-HP-Laptop-15-boffax kernel	1 531,866550) with 1-2: USB disconnect, device number 4
come "appartor parser"	: []au-asami andri (Ne-raw anor()):antai): effetuar- sixins offsterne hutif (nen hutif (nen num nen seme-sizin Tertia):
Jan 34 16:03:17 solo-HP-Laptop-15-bstbax kernel senitized_helper* pid=9705 comm="eppermor_perm	:[1586.005209] audit: type=1468 audit(1579H61097.381292): apparent="57ATHS" operation="profile_load" profile_"unconfined" same="system_log// er"
Jan 24 16:03:18 solo-HP-Laptop-15-bsBax kernel pid=9712 conv='apparent parser"	: [1507.340824] audil: type=1400 audit(1579801398.885:263): apparmor="STATUS" operation="profile_load" profile="unconfined" mame="/usr/bio/Labrouter"
Jen 24 16:03:18 solu-HF-Leptup-15-bs0ax kernel sanitized helper" sid+9712 comm="apparter part	: [1307.348000] audit: type=1400 audit(1577905398.009:254): epparmor="STATUS" operation="profile_load" profile_foad" ame="/usr/bin/L3prouter//
Jan 74 16:83:19 sole HP-Laptop-15-boltss kernel	1 1588.B03266j audit: type-1480 audit(1570061800.487:265): apparent="AilBuED" operation="open" profile="system_l3p" name="pur/share/java/serviet-api_j number=1" forund1373 methods.
Jan 24 16:03:19 solo-HP-Laptop-15-bsBxx kernel	(1988-1) (1988-1) (1997-1) (1997-1) (1997-1) (1998-1999-1) (1999-1) (1998-1998-1) (1998-1999-1) (1998-1998-1) (1998-19
Jen 24 10:18:25 solu-HP-Laptop-15-botax kernel	<pre>[1] [1] [1] [1] [1] [1] [1] [1] [1] [1]</pre>
hane="/home/solo/Documents/" pld=11790 comm="h Jan 34 16:18:20 solo-HP-Laptop-15-bsbsx kerne?	nad' requested mask+'r' denied pask+'r' fauld-1000 oud-1000 : [2416.94406] audh: Type-100a audh(137006/2006.544:243) apparnor="DBUED" operation="open" profile="snap.gnome-system-monitor". : [2416.94406] audh: Type-100a audh(137006/2006.544:243), apparnor="DBUED" operation="open" profile="snap.gnome-system-monitor".
name="/var/lib/anapd/desktop/applications/gnom Jan 24 16:18:29 solo-HP-Laptop-15-bs8xx kernel	e-calculator_pone-celculator-idesktop' pid=11607 cons="gname-system-no" requested pasks"(" deried_masks"(" fauid=1000 ouid=0 : 1 / 2418-0953091 indit: type=1408 audit15379602408-58422497; socarror=PONIEF coeration="coer" open" certific="sna.come=system-nepitor".
name="/var/Tib/unapd/desktop/applications/goos	-logs_decktop* pill-11687 come*genese-represence* repeated packs*** deniad packs*** Fulld-1686 authors
name='/var/llb/unapd/desktop/applications/gnom	r characters goue characters deektop" pid-1667 come goues system to requested matk-"r" fented matk-"r" froid-1006 containers of the system to requested matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of matk-"r" fented matk-"r" froid-1006 containers of the system to request of the system to reque
name="/run/noust/wtab" pld=11067 comm="gsome-s	[variantza] autit (yerted autit): (sinducti.): (sinducti.): apartors units operations upon proties inde.gnow-system-estics.gnow-system-estic
Jan 24 10:18:31 solo-HP-Laptop-15-bs0ax kernel name="/proc/985/attr/current" pld=11687 com=="	: [1421.26400] audt: type-1400 audt:[157962311.965:272]: apparent="UBJED" operation="open" profile="snap.gnome-system-monitor" gnome-system-monitor" gnome-system-monitor" gnome-system-monitor" operation="system-monitor" profile="snap.gnome-system-monitor" operation="system-monitor" profile="snap.gnome-system-monitor" snap.gnome-system-monitor" snap.gnome-system-monitor
Jan 24 10:15:32 sola-HP-Laptop-15-bsDax kernel name='/proc/1/cgroup' pld=11087 come'rnome-sy	: [2421.329126] audit: type:1400 audit(1579862912.809;273): eppermor="DENIED" operation="open" profile="snap.grone-system-monitor" stem-mo" requested mask="r" denied mask="r" fsuid=1800 ouid=0
Jan J4 16:18:32 solo HP-Laptop-15-boBax kernel	: [3421.324161] audit: type:1488 audit(1579062912.889:274): apparent: "DERIED" operation: "open" profile: "inap.growe-system-monitor".gnowe-system-monitor" stem-mo" requested mesks"r" denied mesks"r" fauld:1000 peid:0
Jan 24 16:18:32 solp-HP-Laptop-15-bs8xx kernel	: [2421.329204] audit: type=1400 audit[1579602912.8091275]1 apparmor="DENIED" operation="apen" profile="imap.goome-system-monitor:gnome-system-monitor: tran.we" requested made-"r" (mild mode-"r" fould-500e cold-m
Jan 24 10:18:32 solo-HP-Leptop-15-bs0as kernel	i [421.3250] addit. yype-108 addit[15780621.009.270]; appartor="OENILO" operation="open" profile="anap.gnome-system-monitor".
Jan 34 16:18:32 solo-HP-Laptop-15-bifixs kernel	ystem-mo 'requested mask» (" oented Mask» (" fosto-joud odio-joud 1 [JdJ].30663] auftir type-1488 auftir[ST9866401.8111277]; apparent="DENTED" operation="open" profile="snap.growe-system-monitor", genme-system-monitor",
Jan 24 16:18:32 solo-HP-Laptop-15-bs(ox kerne)	stem.mo" requested_mesk="r" dented_mask="r" fauld-1000 outd-0 [2421.329700] sudtt: type=1408 sudtt(157966242.011:278); apparmar="DENIED" operation="open" profile="snap.gnome-system-monitor", gnome-system-monitor", gnome-system-monitor", gnome-system-monitor", apparmar="DENIED" operation="spatestem", apparmar="DENIED" operation="spatestem", apparmar="DENIED" operation="spatestem", apparmar="spatestem", apparmar="
name: '/proc/1/cgroup' pid=11687 corm='gnome-sy Jan 24 16:16:32 solo-6P-Lantop-15-bsfax kernel	stem.an' requested mask-'r' denied mask-'r' fauld:1886 ould-8 1: [42].32972] multi type:100 multi(157500212.013:279); enservor:"DENIED" overstion:"open" profile:"imso.grome-system-monitor.goome-system-monitor".
name='/proc/1/cgroup' pid=11887 come'gnome-sy Jan 34 16:18:32 soln_88-tantno.15.boftxx karnel	sten no" requested nesk-"/ deside nesk-"/ fauld-side osta-0 - 1 dai 100001 unit. Una-1400 unit/157000201.311 0014-0 - 1 dai 100001 unit. Una-1400 unit/157000201.311 0014-0000000-"DRTR" negation-"negation-"negation-"negation-"
name='/proc/900/attr/current' pid=11087 com="	gume-system-mo" requested_nesk="/" denied_nesk="/" fauid=1000_out=0
	Plain Test = Teb Walth B + La 1129, Col 185 =
	Fig.2'.8
	Fig.2'.8
Kins 📓 Teor Estlar *	Fig.2'.8
tiks ■ Teni Esilar + Opin + A	Fig.2'.8
kir; ∎ textsar+ орил – Да Балан сосан и посан и посан соса	Fig.2'.8
čes € 1646 £3160 ** фал 19 6014315 1930 ст.18,9 500 35-53,00 к.ет.ек Дал 28 60143157 зобсени - царор-13-53,00 к.ет.ек Дал 28 60143157 зобсени - царор-13-53,000 к.ет.ек дал 28 60143157 зобсени - царор-13-53,000 к.ет.ек	Fig.2'.8
ска: В Техт Байолт - Орийт В - Паради и состаници народа је за је и колисе - Паради и состанија и состаници народа је за је и колисе - Паради и состанија и состаници народа је за је и состани - Паради и состанија и состаници народа је за је и состани - Паради и состаници на радики и состаници на радики - Паради и состаници на радики и состаници на радики - Паради и состаници на радики и состаници на радики на радики - Паради и состаници на радики на радики - Паради и состаници на радики на радики - Паради и состаници на радики на радики - Паради на радики на - Паради на радики на - Паради на радики на р	Fig.2'.8
сна 🗑 Техе БоГолг * сремя — Д ран 20 Кан 1913 7 2016-00-14,20100-13-80100 метеол лан 20 Кан 1913 7 2016-00-14,20100-13-8010 метеол лан 20 Кан 1913 7 2016-00-14,20100-13-80100 метеол лан 20 Кан 1913 7 2016-00-14,20100-13-8020 метеол лан 20 Кан 1913 7 2016-00-14,20100-13-8020 метеол лан 20 Кан 1913 7 2016-00-14,20100-13-8020 метеол лан 20 Кан 1913 7 2016-00-14,20100-13-80100 метеол лан 20 Кан 1913 7 2016-00-14,20100-13-8000 метеол лан 20 Кан 1913 7 2016-00-14100-15-8000 метеол лан 20 Кан 1913 7 2016-00-14,20100-13-8000 метеол лан 20 Кан 1913 7 2016-00-14,20100-13-8000 метеол лан 20 Кан 1913 7 2016-00-1400 метеол лан 20 Кан 1913 7 2016-000 метеол лан 20 Кан 2016 7 2016 метеол лан 20 Кан 2000 метеол лан 20 Кан 2000 метеол лан 20 Кан 2000 метеол лан 2	Fig.2'.8
Eles ■ Text Ecfar* one 10 6017537 3300-010-Laptopn 35-53800 Merror Inn 20 6014317 2010-0114-2010 13-54800 Merror Inn 20 6014317 2010-0114-2010 13-54800 Merror Inn 20 6014317 1010-0114-2010-13-5800 Merror	Fig.2'.8
End Estar* Oprio B and 36 doi:31/2 solo=00-Lapeso-13-solica merror	Fig.2'.8
Intel Est/or+ Capacity Ell Dir JM (0014):151 close-state close-state Dir JM (0014):151 close-state close-state close-state Dir JM (0014):151 close-state close-state close-state close-state Dir JM (0014):151 close-state close-state <thclosestate< th=""> closestate <thcl< td=""><td>Fig.2'.8</td></thcl<></thclosestate<>	Fig.2'.8
E: ■ Tool 5510 *** Span*	Fig.2'.8
Let ■ Text Estur* Opur* ① Text 20 402157 also: HP-Laptop-15-balks works Text 20 402157 also: HP-Laptop-15-balks works Text 20 402157 also: H-Laptop-15-balks works Text 20 4021577 also: H-Laptop-	Fig.2'.8
E Text Editor* Oprim* Display and 35 distants solar-W-Lapson-13-solara warmed and 35 distants solar-W-Lapson-13-solara warmed and 35 distants solar-W-Lapson-13-solara warmed and 36 distants solar-W-Lapson-13-solara warmed and 36 distants solar-W-Lapson-13-solara warmed and 38 distants solar-W-Lapson-13-sola	Fig.2'.8
E: ■ Tool Siton ** Source B Source Siton 11: 1: 1: 1: 1: 1: 1: 1: 1: 1: 1: 1: 1:	Fig.2'.8
bis ■ Text Ecllor*	Fig.2'.8
Ken Latar* (proc 2)	Fig.2'.8
Contine	Fig.2'.8
bits ■ Text 6.510×** Optimize B <	Fig.2'.8
Les ■ text Solor* opport	Fig.2'.8
Is: ● Tool Safar = Open ● Ison S for http://www.isonary.op/is/safar events in 18 declars? cole=H-Lappo-15-safar events in 18 declars? cole=H-Lappo-15-bask events decaster.exten* sole=H-Lappo-15-bask events decaster.exten* sole=H-Lappo-15-bask events in 18 declars? cole=H-Lappo-15-bask events in 18 declars?	Fig.2'.8
Ener Editor* Capir* D Stra 30 Mail 101 social in 4 (a) 101 size in the second	Fig.2.*8
 bis € Text Ecilar* cpure Ecilar* cp	Fig.2.8
Contin Exec 6210x** Contin EX	Fig.2:A8
Constant - A Constant - A Consta	Fig.2.8
bis ■ Text £c16x *	Fig.2.8
Lits C text Estar * C pir/ A an 20 de1:417 yolo-11 - Liptop-13 - Salka kernel Lin 20 de1:4157 yolo-11 - Liptop-13 - Salka kernel Liptop-10 - Liptop-15 - Salka kernel Liptop-10 - Liptop-15 - Salka kernel Liptop-15 yolo-11 - Liptop-15 - Salka kernel Lin 20 de1:4157 yolo-11 - Liptop-15 - Salka kernel Lin 20 de1:4155 yolo-11 - Liptop-15 - Salka kernel Lin 20 de1:4158 yolo-11	Fig.2:A8
Image The set dofter * Cypin* Display Sam 200 Display Display Sam 200 Display Display Display Sam 200 Display Display Display Sam 200 Display Display Display Display Sam 200 Display Display Display Display Display Sam 200 Display Display <thdisplay< th=""> Display<td>Fig.2.8</td></thdisplay<>	Fig.2.8
Dies Text Exifer* Oper* Die Am 20 60:131/2 20:00-00-12-0000 Merror Am 20 60:131/2	Fig.2 : As
Desi Solar* Open Desi 100 200 100	Fig.2.*.8
Dies Totel Enform Capitre Bit Dies Bit Bit Dies Bit Bit Bit Bit Dies Bit Bit <td>Fig.2.*.8</td>	Fig.2.*.8
Contention Open Description Open Description Description Description	Fig.2.*.8
Dies Text ESTer* Oper* Ab Oper* Ab Dies Statistics Dies Dies Dies Dies Dies Dies Dies Dies Dies Dies Dies Dies Di	Fig.2.*.8
Image: Section - Contine Elements Contine Elements Elements Contine Elements Elements Elements Contine Elements Elements Elements Contine Contine Elements Elements Contine Contine Contine Elements Contine Contine Contine Contine Contine Contine Contine Contine Contine Contine Contine Contine Contine Contine Contine Contine Contine Contine Contine Contine Contine Contine	Fig.2.4.8

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