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)

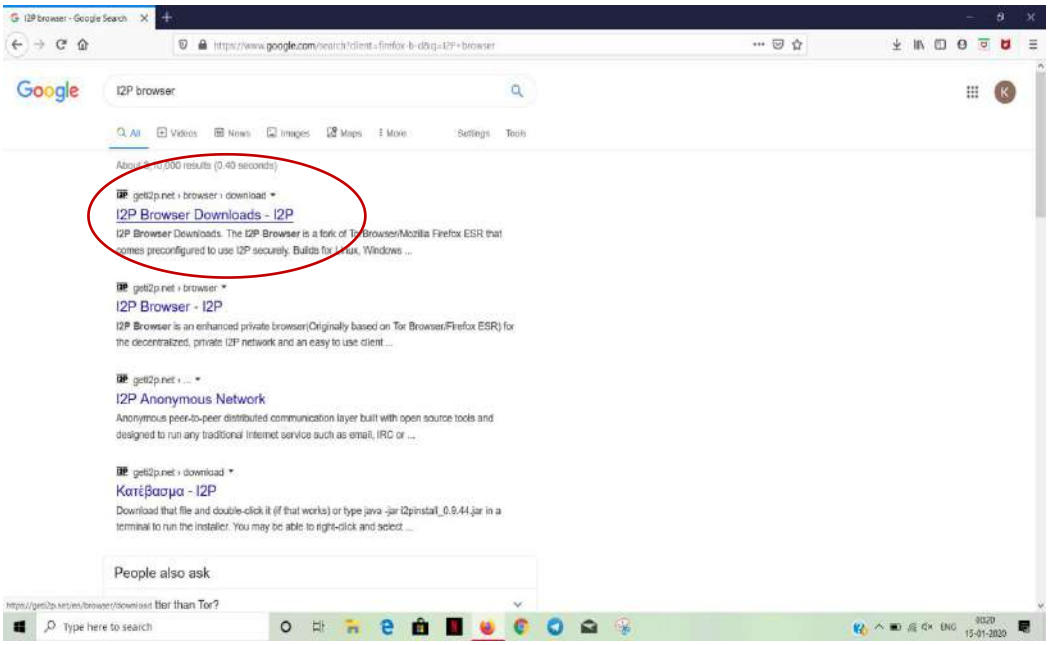


Fig.1.1

From the opening tab,click on the windows option.(Fig.1.2)

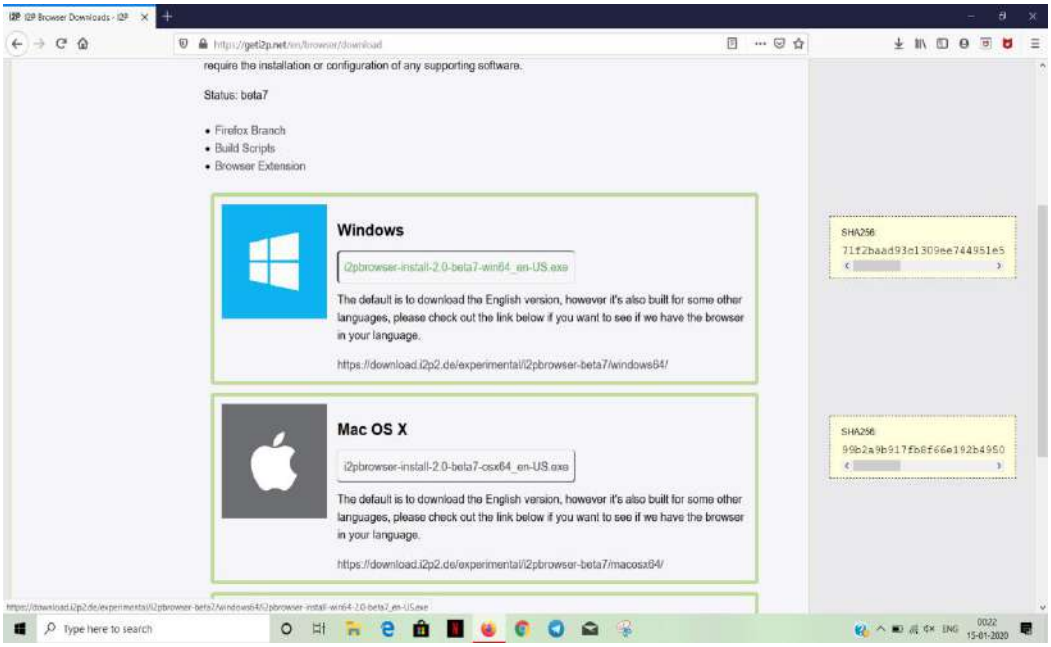


Fig.1.2

Click on “save file” option and the download will begin.(Fig.1.3)

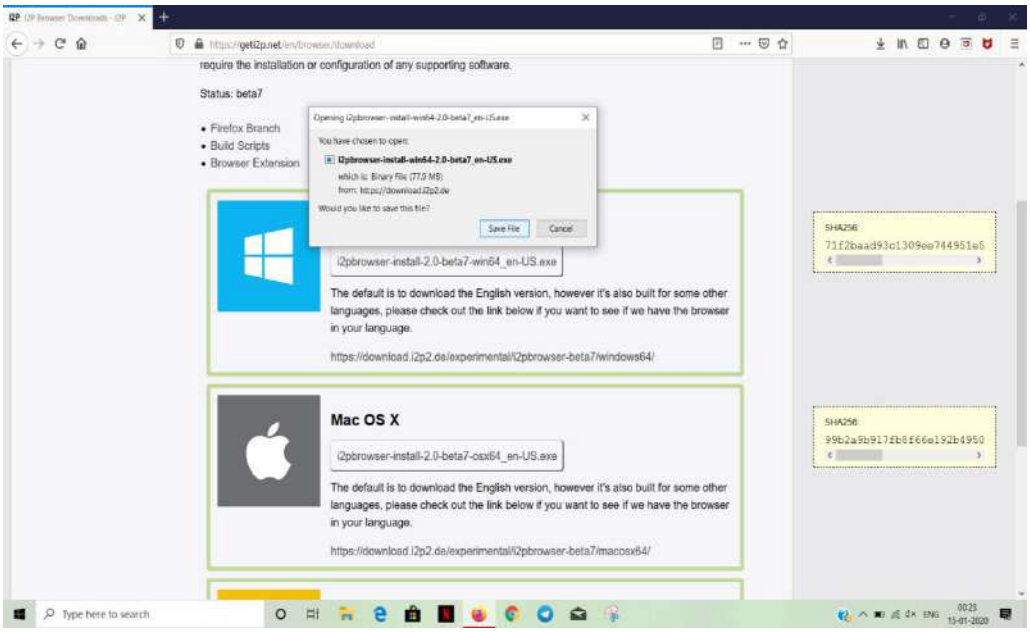


Fig.1.3

Click on the I2P browser installer and select language “English”,then click “OK” .(Fig.1.4)

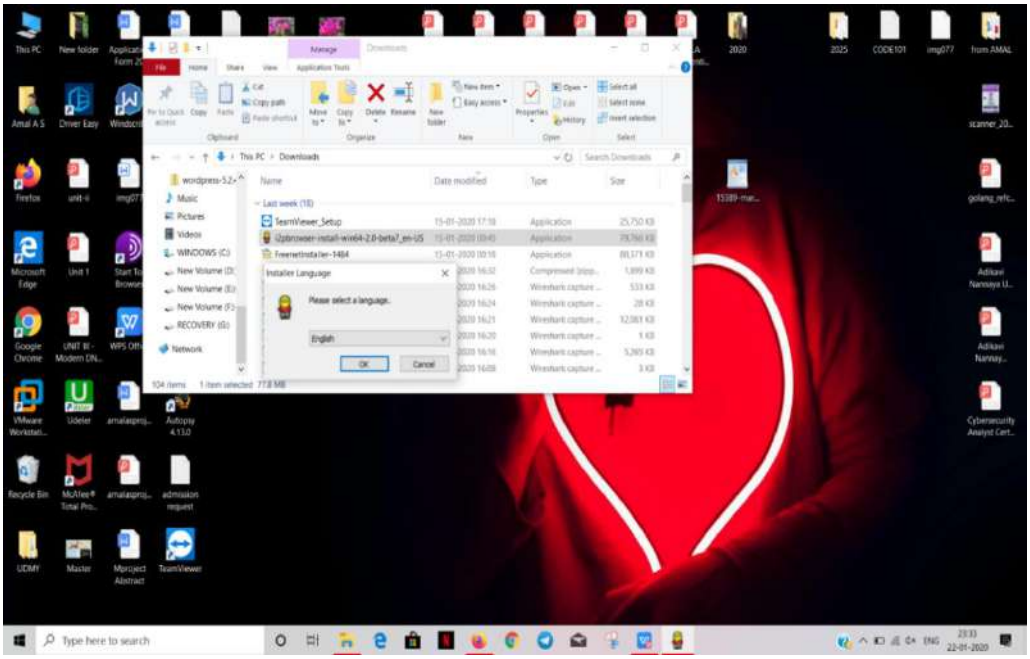


Fig.1.4

Choose the destination folder (in this case C:Drive) and click “Install”.(Fig.1.5)

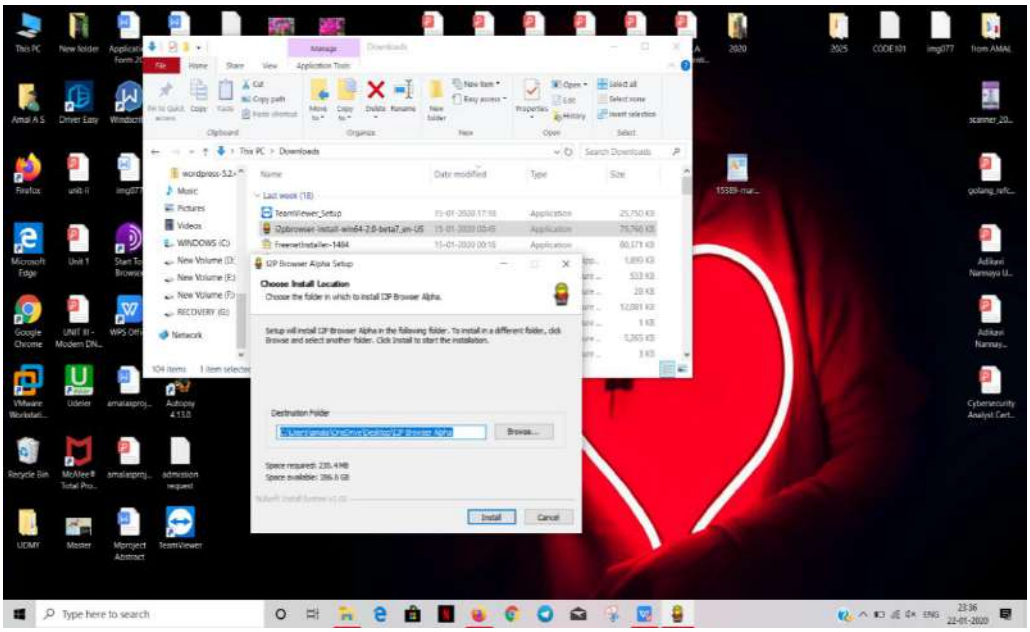


Fig.1.5

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

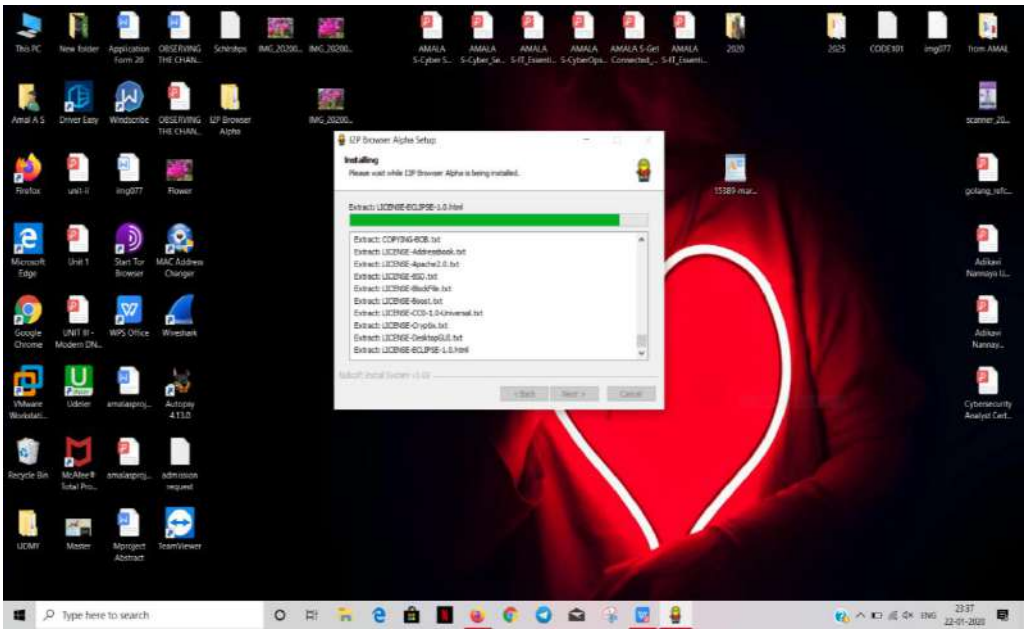


Fig.1.6

When the installation completes click “Finish”.(Fig1.7)

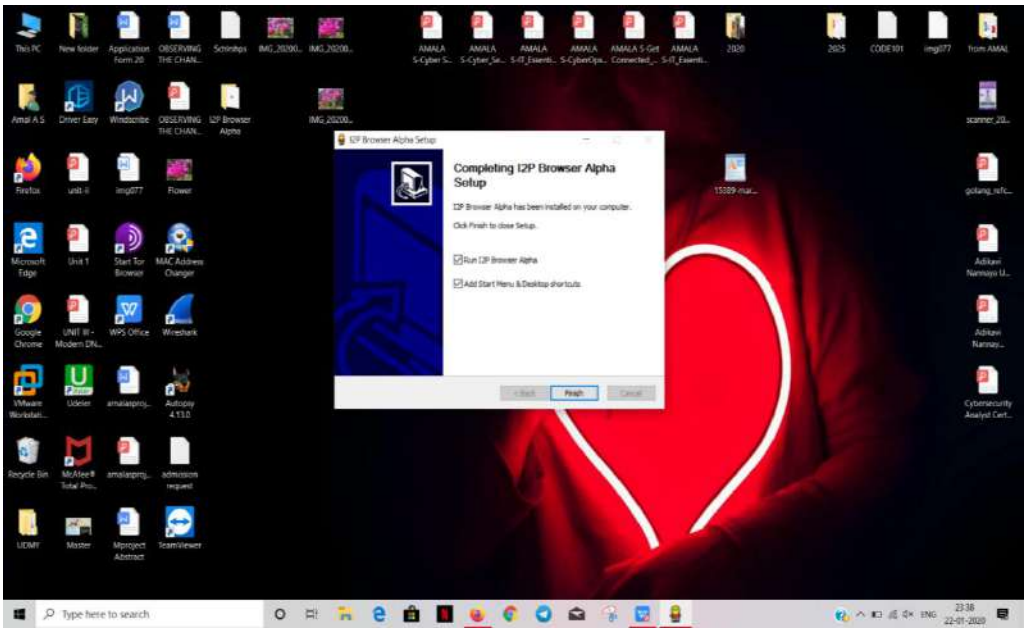


Fig.1.7

ii) Freenet browser

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

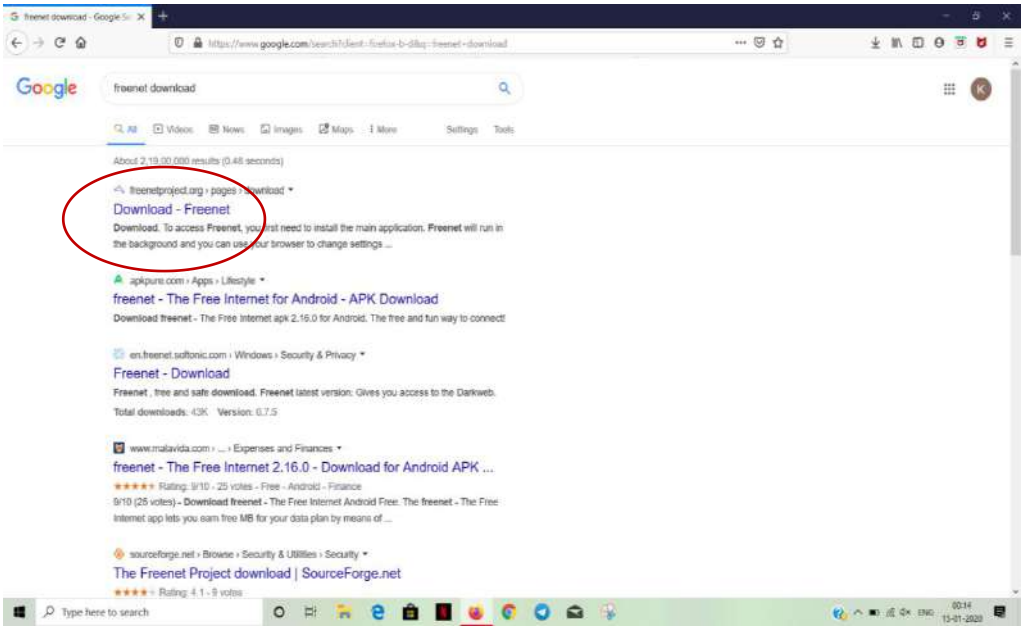


Fig.1.8

From the opening website click on the “For Windows” option.(Fig.1.9)

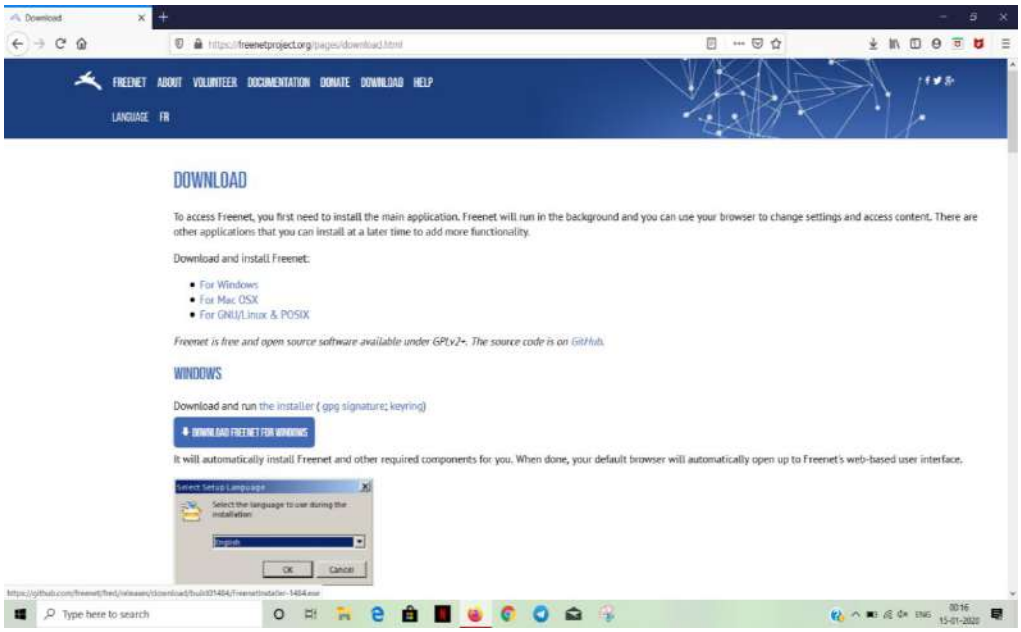


Fig.1.9

Click on “save file” option and the download will start.(Fig.1.10)

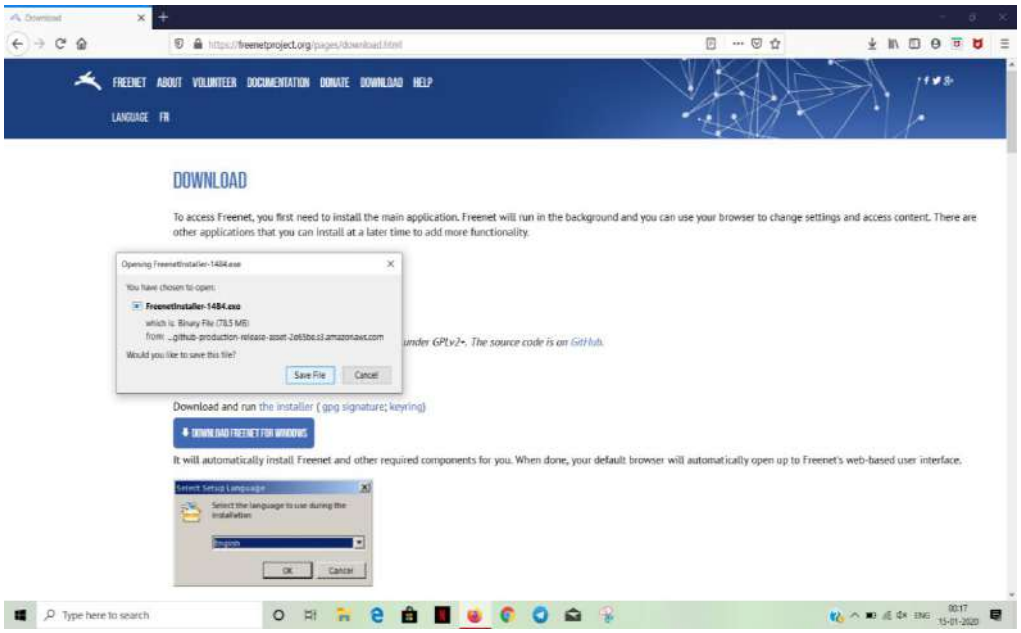


Fig.1.10

Click on the freenet installer and select “English” language and click “OK”. (Fig.1.11)

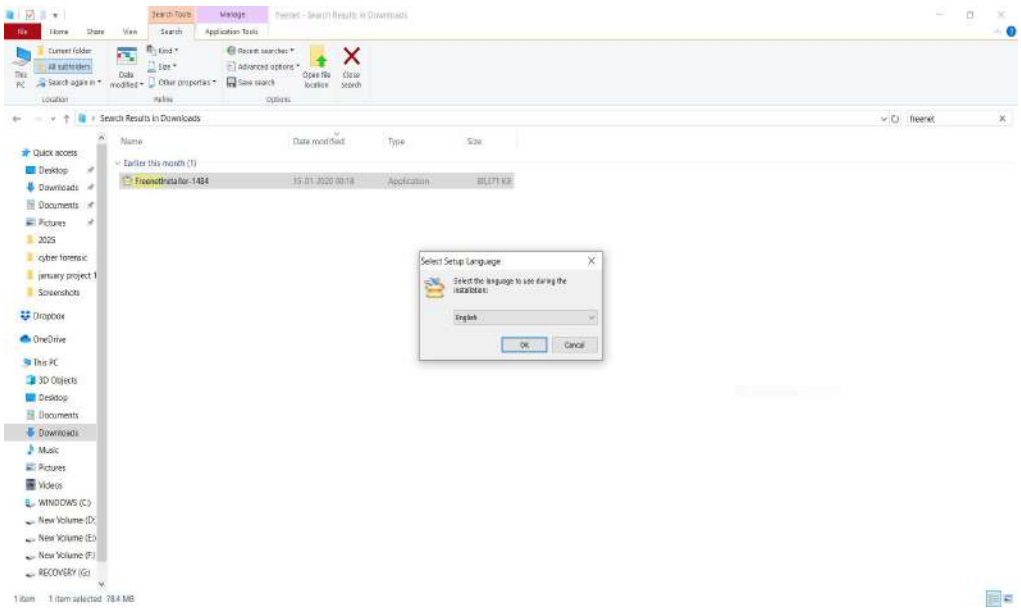


Fig.1.11

Choose the destination folder (in this case C:Drive) and click “Install”.(Fig.1.12)

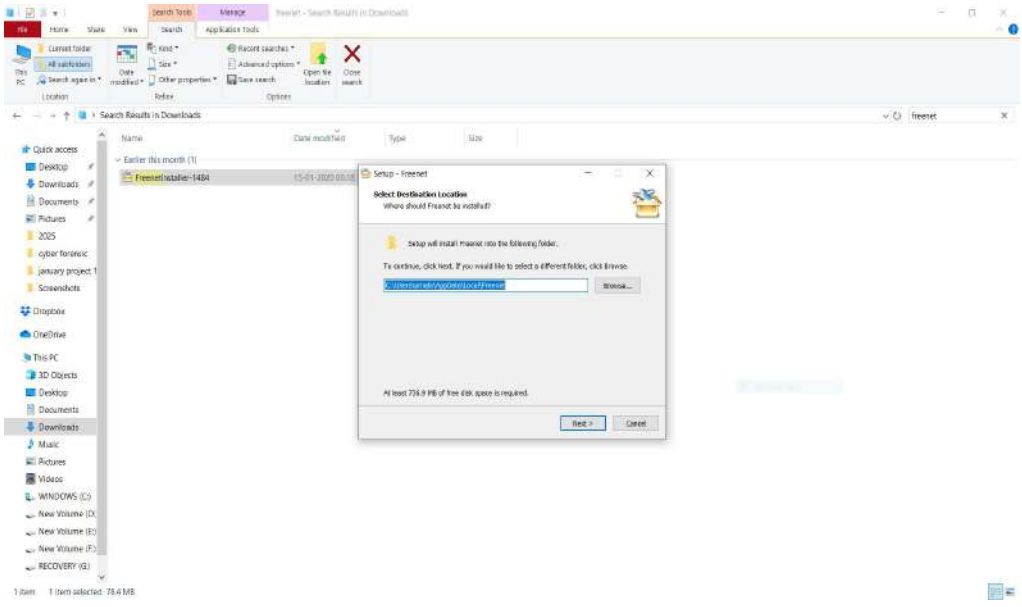


Fig.1.12

Click on “Finish” option to complete the installation.(Fig.1.13)

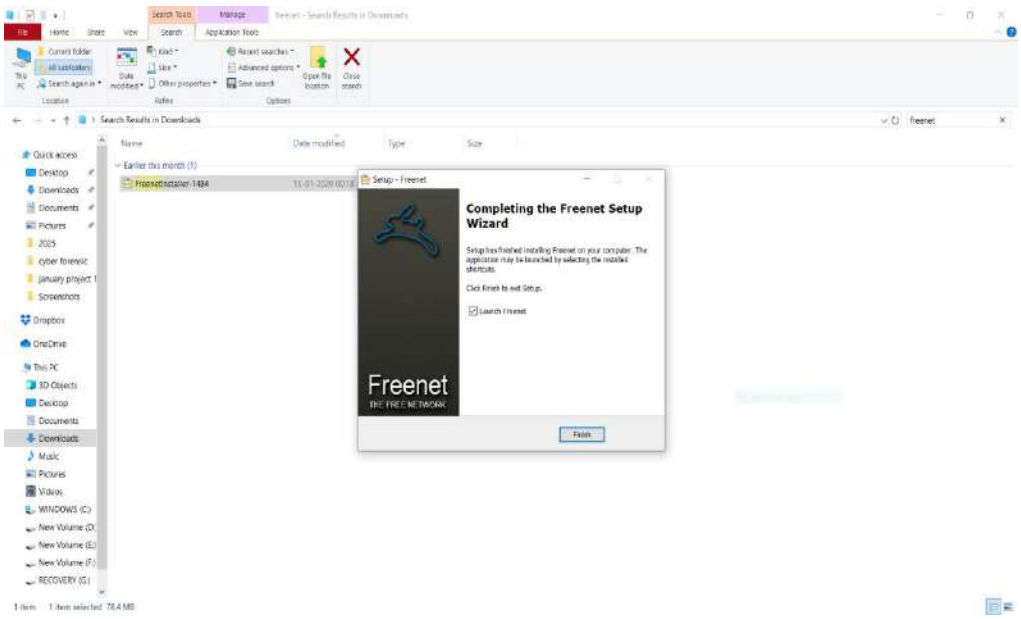


Fig.1.13

iii) DB Browser for SQLite

Open any search engine and type in “db browser for sqlite”.From the results click on the first link.(Fig.1.14)

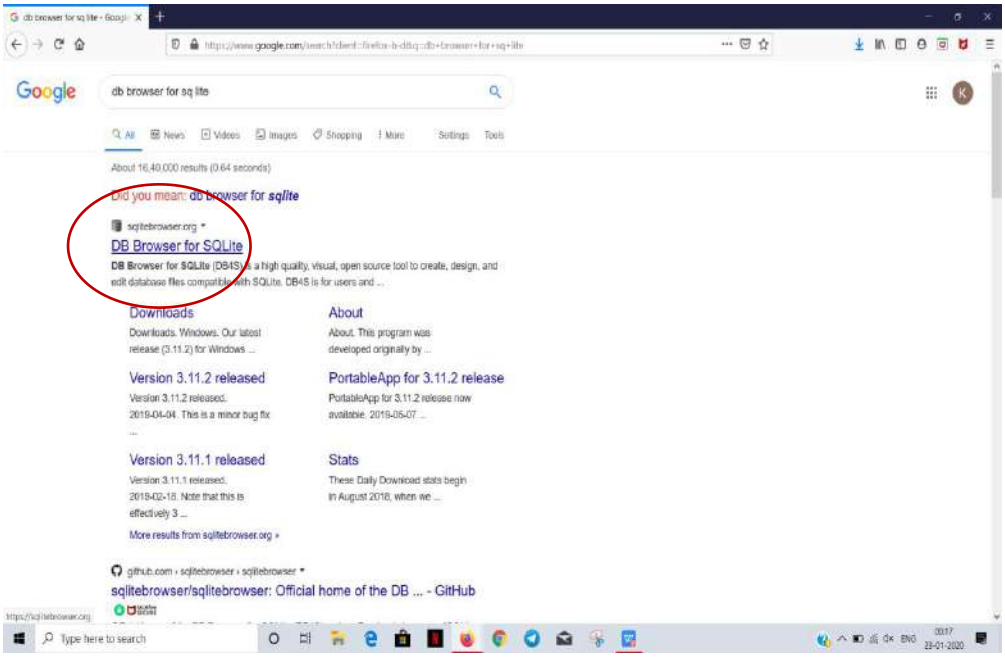


Fig.1.14

From the opening browser click on “standard installer for 64-bit Windows” option.(Fig.1.15)

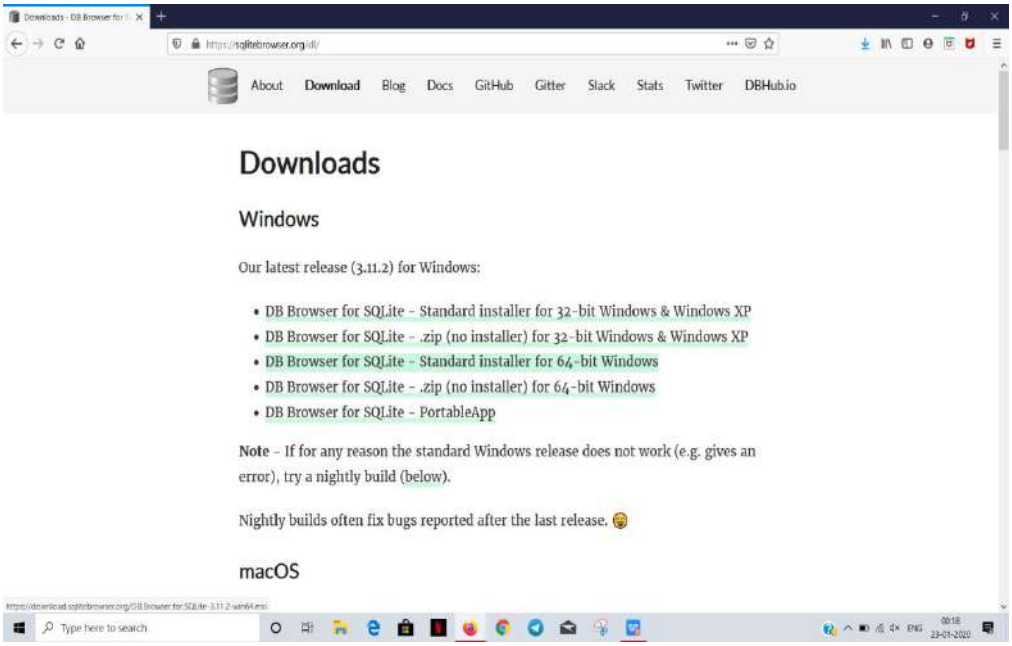


Fig.1.15

Click on the “Save file” option and the download will start.(Fig.1.16)

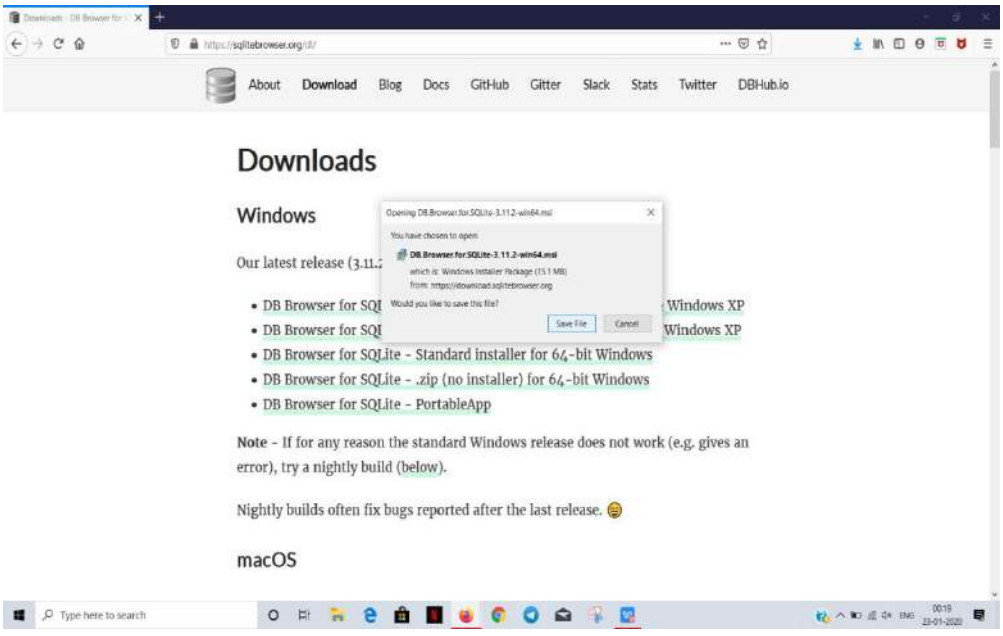


Fig.1.16

Click on the DB browser installer and click “Next”.(Fig.1.17)

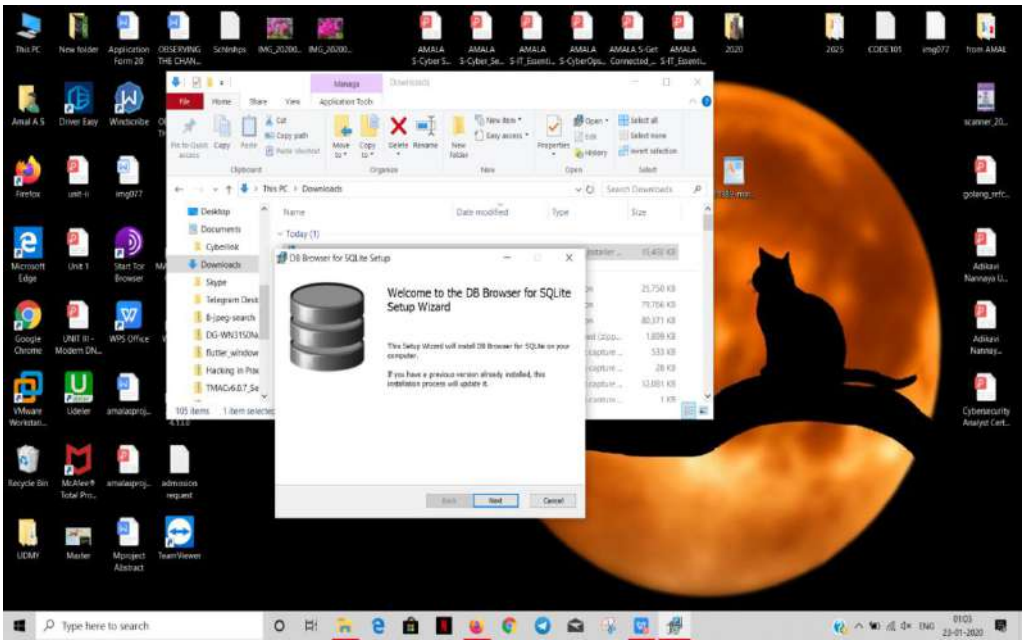


Fig.1.17

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

Fig.1.18

Now click “Install” to start the installation.(Fig.1.19)

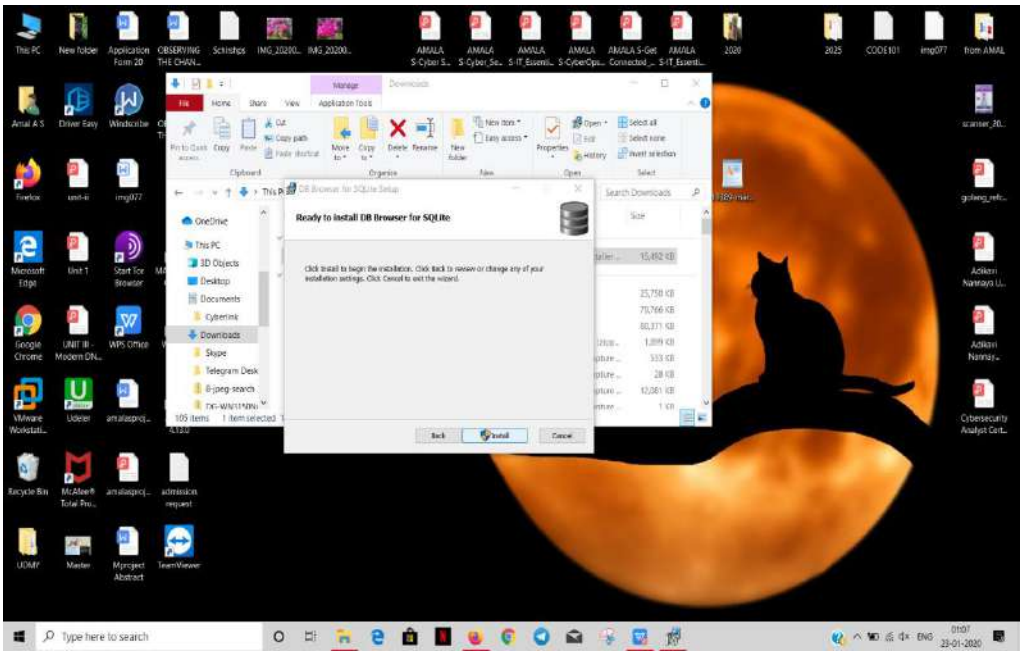


Fig.1.19

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

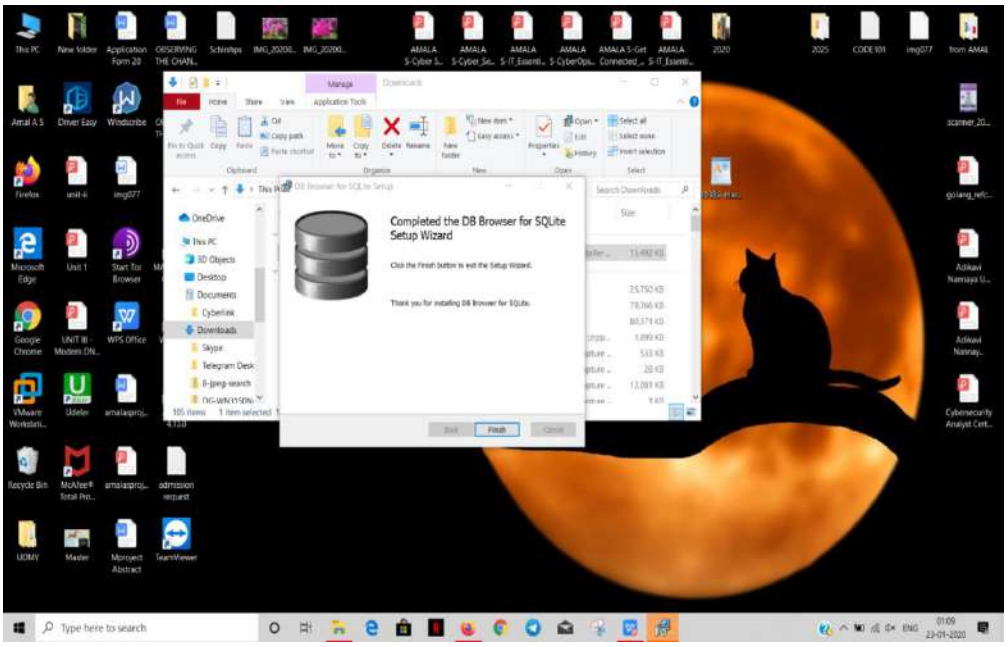


Fig.1.20

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)

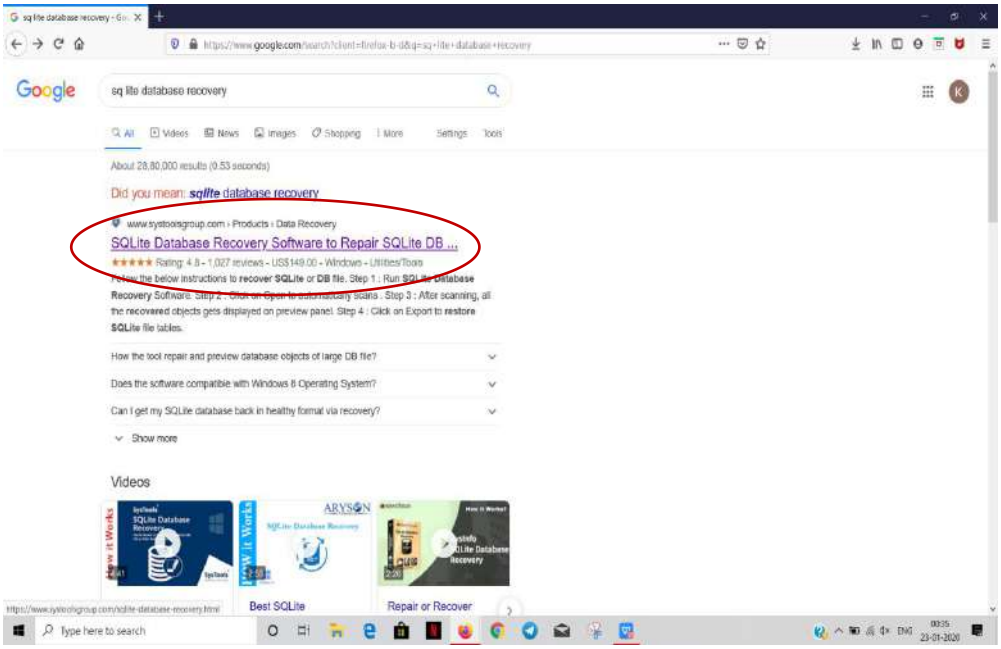


Fig.1.21

From the opening browser click on the “Download Now” option.(Fig.1.22)

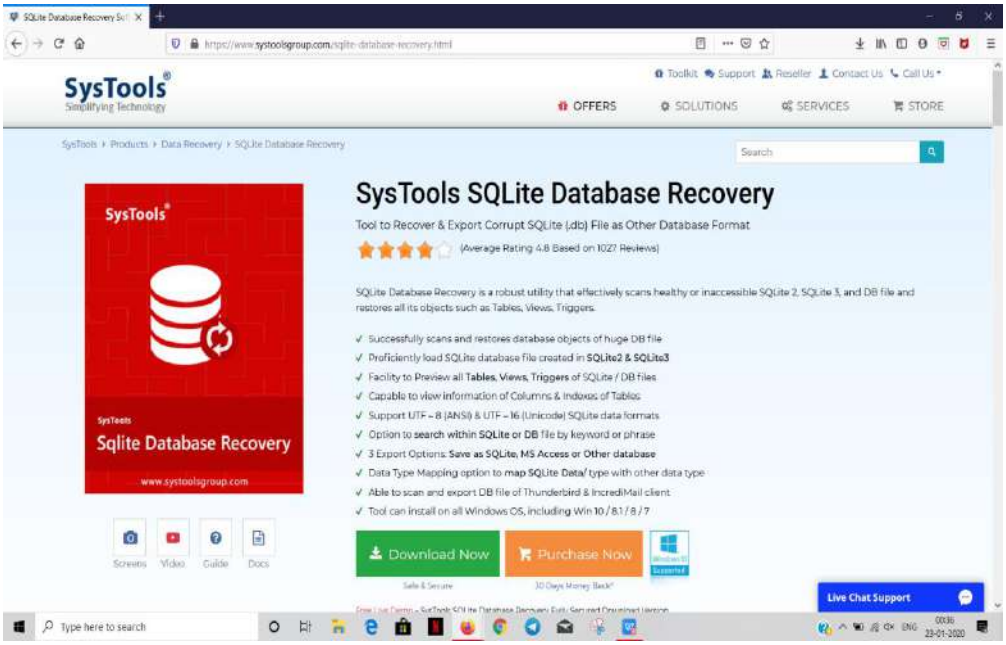


Fig.1.22

Click on the “Save file” option and the download will start.(Fig.1.23)

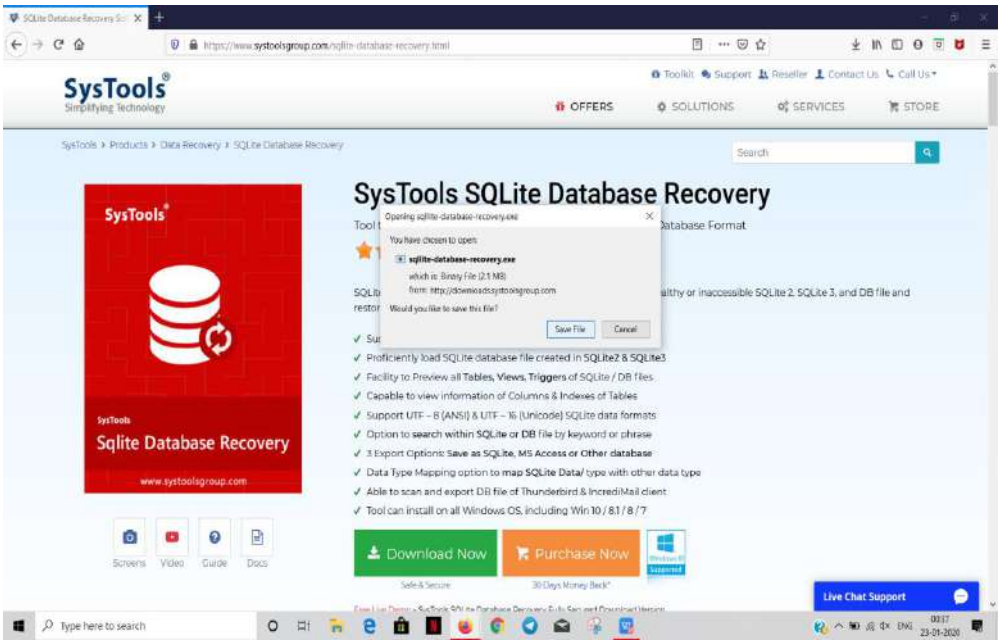


Fig.1.23

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

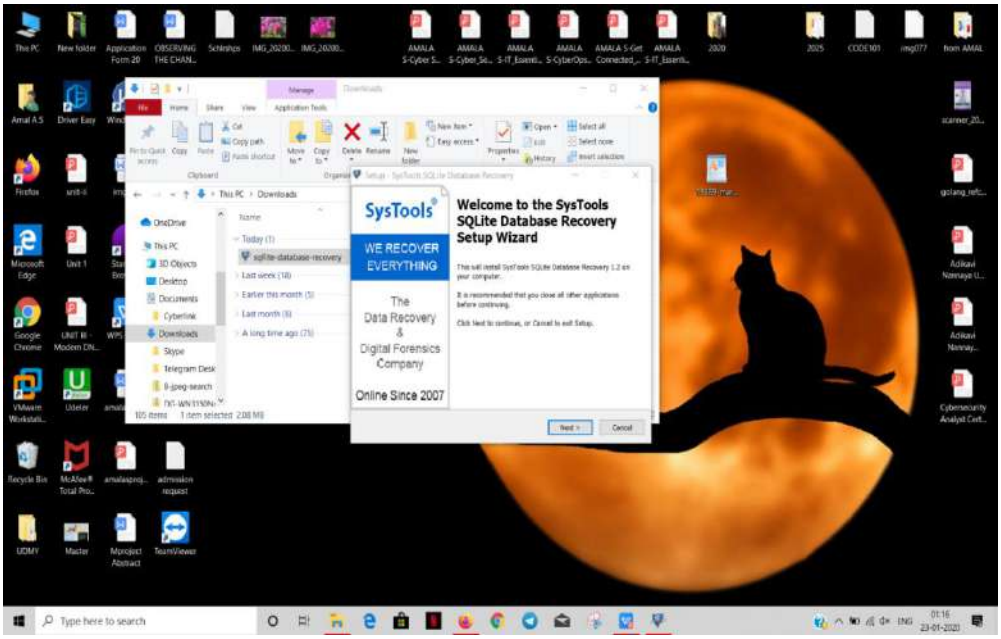


Fig.1.24

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

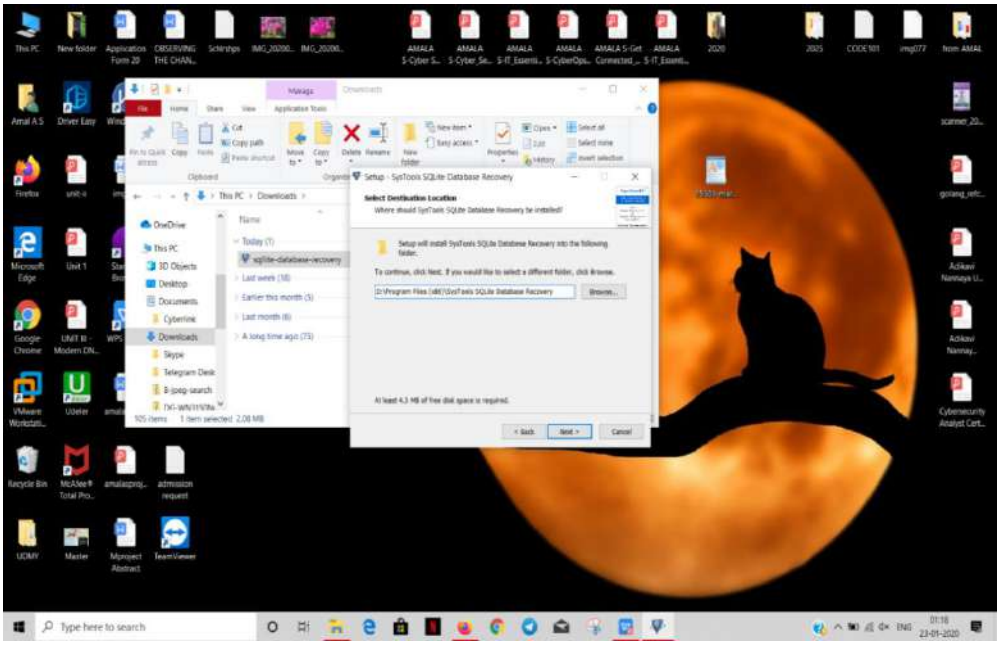


Fig.1.25

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

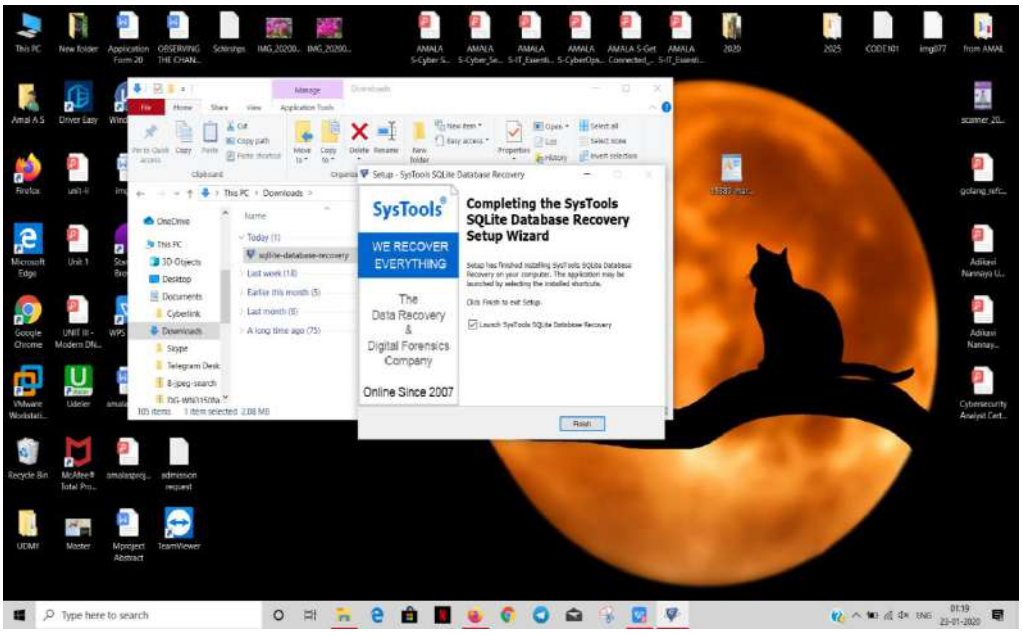


Fig.1.26

1.2 In Linux Version 18.04.3

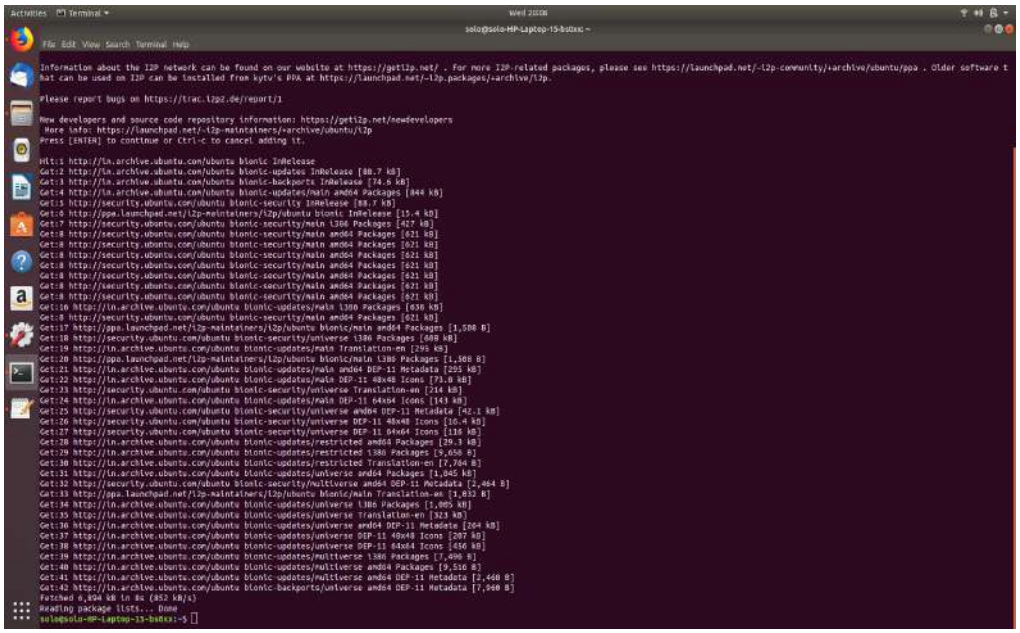
In Linux operating system the softwares are installed through Linux command line called the “Terminal”.

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)



```
Information about the I2P network can be found on our website at https://geti2p.net/ . For more I2P-related packages, please see https://launchpad.net/~i2p-community/+archive/ubuntu/ppa . Older software t
hat can be used on I2P can be installed from kytv's PPA at https://launchpad.net/~i2p.packages/+archive/i2p.

Please report bugs on https://trac.i2p2.de/report/1

New developers and source code repository information: https://geti2p.net/newdevelopers
 More info: https://launchpad.net/~i2p-maintainers/+archive/ubuntu/i2p
Press [ENTER] to continue or Ctrl-c to cancel adding it.

Hit:1 http://in.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://in.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [844 kB]
Get:5 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:6 http://ppa.launchpad.net/i2p-maintainers/i2p/ubuntu bionic InRelease [15.4 kB]
Get:7 http://security.ubuntu.com/ubuntu bionic-security/main i386 Packages [427 kB]
Get:8 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [621 kB]
Get:8 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [621 kB]
Get:8 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [621 kB]
Get:8 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [621 kB]
Get:8 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [621 kB]
Get:8 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [621 kB]
Get:8 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [621 kB]
Get:16 http://in.archive.ubuntu.com/ubuntu bionic-updates/main i386 Packages [636 kB]
Get:8 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [621 kB]
Get:17 http://ppa.launchpad.net/i2p-maintainers/i2p/ubuntu bionic/main amd64 Packages [1,508 B]
Get:18 http://security.ubuntu.com/ubuntu bionic-security/universe i386 Packages [608 kB]
Get:19 http://in.archive.ubuntu.com/ubuntu bionic-updates/main Translation-en [295 kB]
Get:20 http://ppa.launchpad.net/i2p-maintainers/i2p/ubuntu bionic/main i386 Packages [1,508 B]
Get:21 http://in.archive.ubuntu.com/ubuntu bionic-updates/main amd64 DEP-11 Metadata [295 kB]
Get:22 http://in.archive.ubuntu.com/ubuntu bionic-updates/main DEP-11 48x48 Icons [73.8 kB]
Get:23 http://security.ubuntu.com/ubuntu bionic-security/universe Translation-en [214 kB]
Get:24 http://in.archive.ubuntu.com/ubuntu bionic-updates/main DEP-11 64x64 Icons [143 kB]
Get:25 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11 Metadata [42.1 kB]
Get:26 http://security.ubuntu.com/ubuntu bionic-security/universe DEP-11 48x48 Icons [16.4 kB]
Get:27 http://security.ubuntu.com/ubuntu bionic-security/universe DEP-11 64x64 Icons [116 kB]
Get:28 http://in.archive.ubuntu.com/ubuntu bionic-updates/restricted amd64 Packages [29.3 kB]
Get:29 http://in.archive.ubuntu.com/ubuntu bionic-updates/restricted i386 Packages [9,658 B]
Get:30 http://in.archive.ubuntu.com/ubuntu bionic-updates/restricted Translation-en [7,704 B]
Get:31 http://in.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [1,045 kB]
Get:32 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-11 Metadata [2,464 B]
Get:33 http://ppa.launchpad.net/i2p-maintainers/i2p/ubuntu bionic/main Translation-en [1,832 B]
Get:34 http://in.archive.ubuntu.com/ubuntu bionic-updates/universe i386 Packages [1,005 kB]
Get:35 http://in.archive.ubuntu.com/ubuntu bionic-updates/universe Translation-en [323 kB]
Get:36 http://in.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 DEP-11 Metadata [264 kB]
Get:37 http://in.archive.ubuntu.com/ubuntu bionic-updates/universe DEP-11 48x48 Icons [207 kB]
Get:38 http://in.archive.ubuntu.com/ubuntu bionic-updates/universe DEP-11 64x64 Icons [456 kB]
Get:39 http://in.archive.ubuntu.com/ubuntu bionic-updates/multiverse i386 Packages [7,496 B]
Get:40 http://in.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 Packages [9,516 B]
Get:41 http://in.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 DEP-11 Metadata [2,468 B]
Get:42 http://in.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 DEP-11 Metadata [7,960 B]
Fetched 6,894 kB in 8s (852 kB/s)
Reading package lists... Done
solo@solo-HP-Laptop-15-bs0xx:~$
```

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)

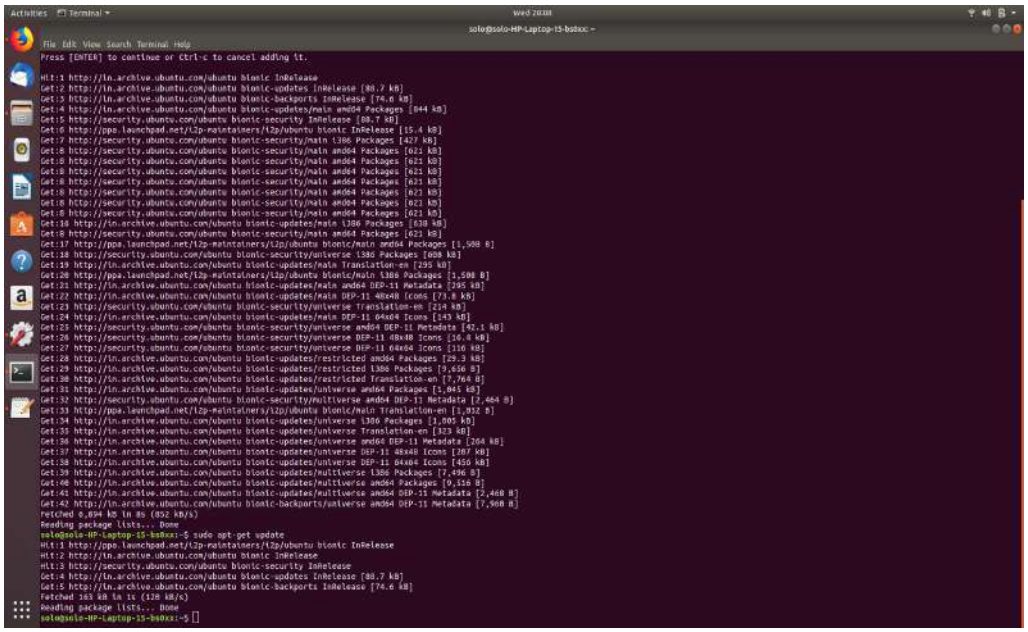


Fig.2.2

Install i2p using the following command: sudo apt-get install i2p (Fig.2.3)

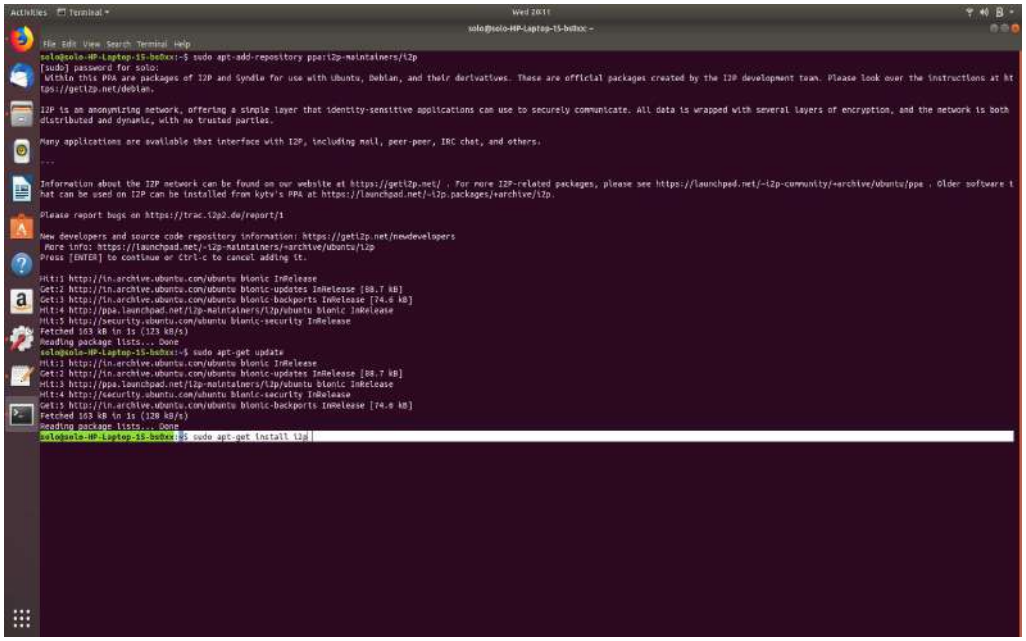


Fig.2.3

Start i2p: i2prouter start

This command will initiates the browser to open.(Fig.2.4)

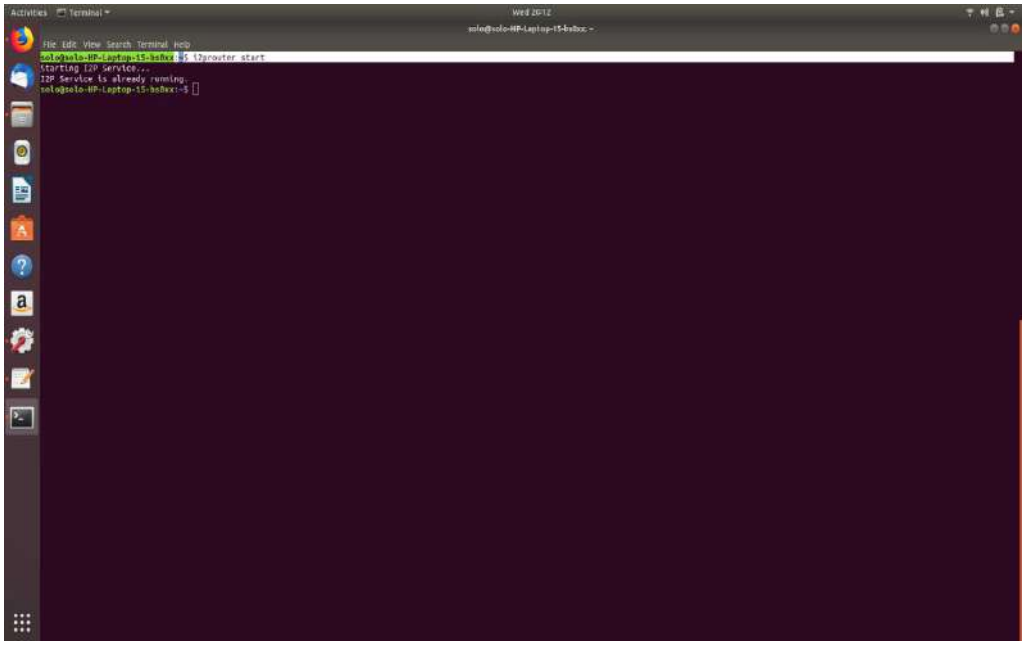


Fig.2.4

ii) Freenet

To install the browser, the following commands are used: (Fig.2.5)

sudo apt-get update

sudo apt-get install python3-setuptools build-essential python3-dev

sudo apt-get install openjdk-8-jre python3 cron git gnupg2

git clone https://github.com/datorrukis/freenet-installer.git.[5]

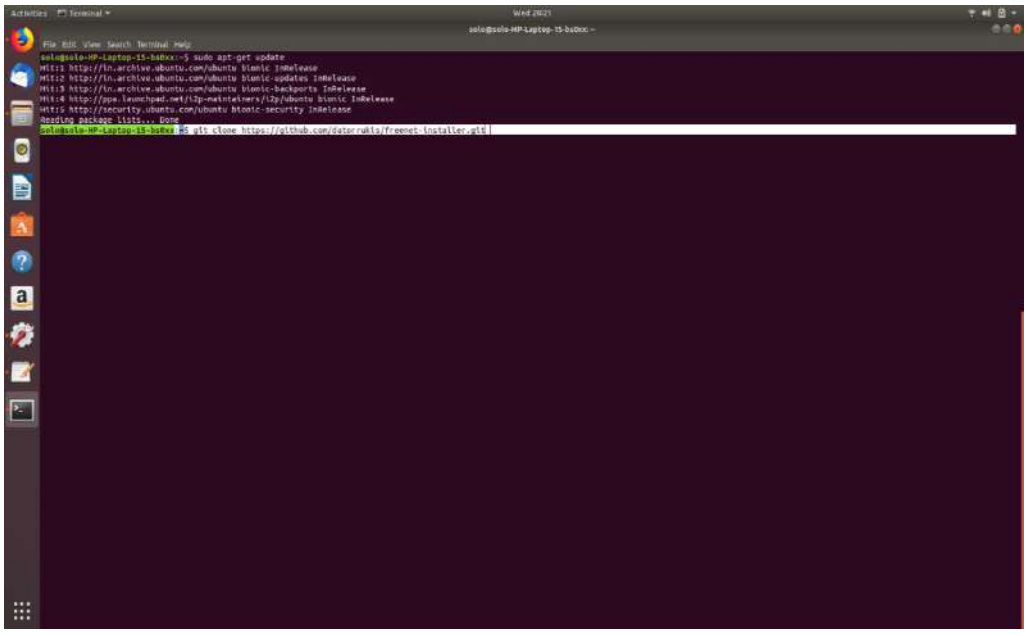


Fig.2.5

The browser is launched using the following command: freenet_installer (Fig.2.6)

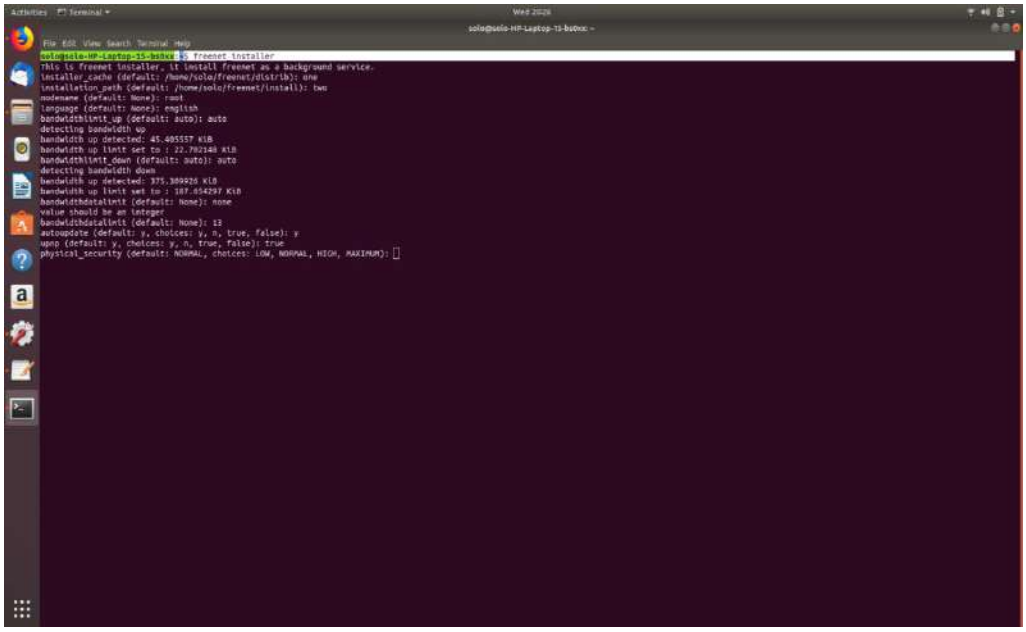


Fig.2.6

iii) DB Browser for SQLite

The browser is installed by using the following command:
sudo apt-get install sqlitebrowser (Fig.2.7)

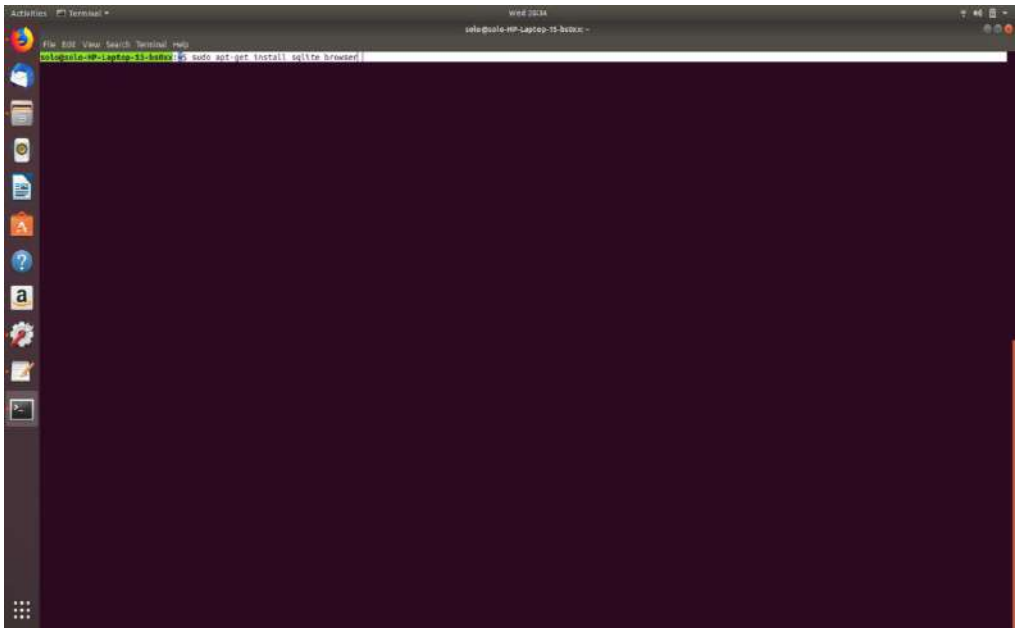


Fig.2.7

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)

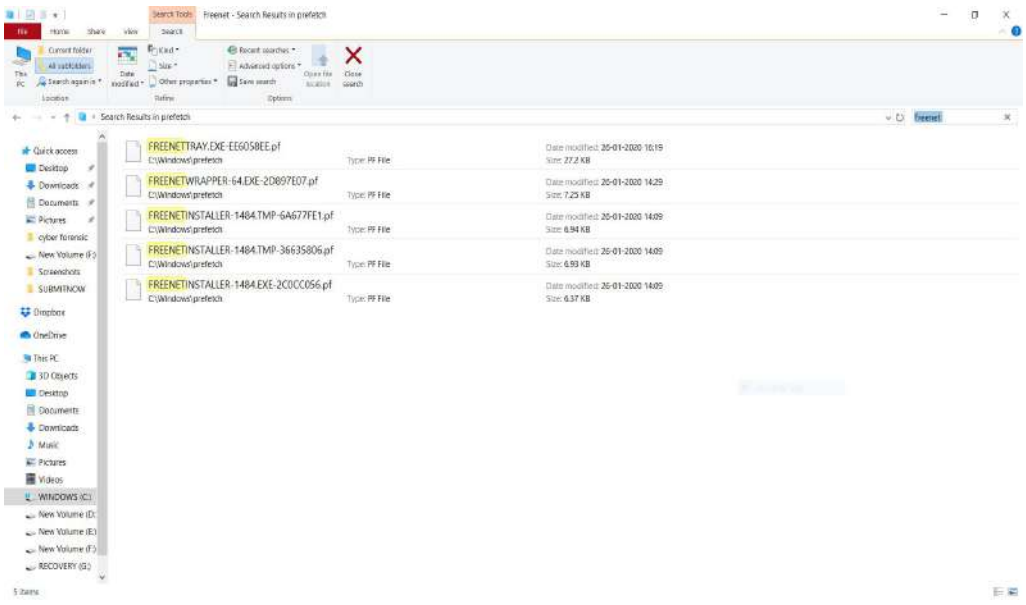


Fig.1’.1

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.

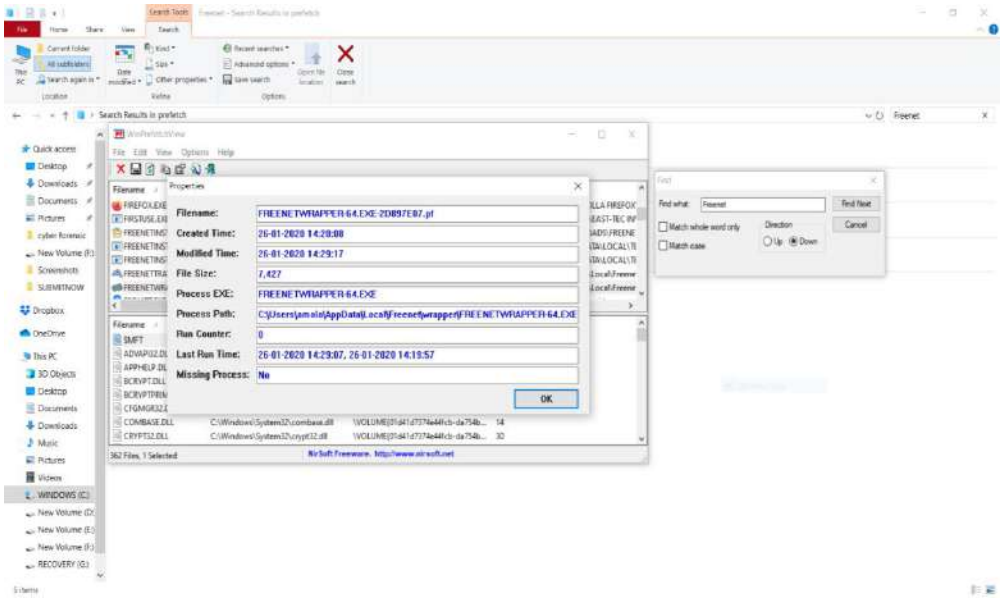


Fig.1'.2

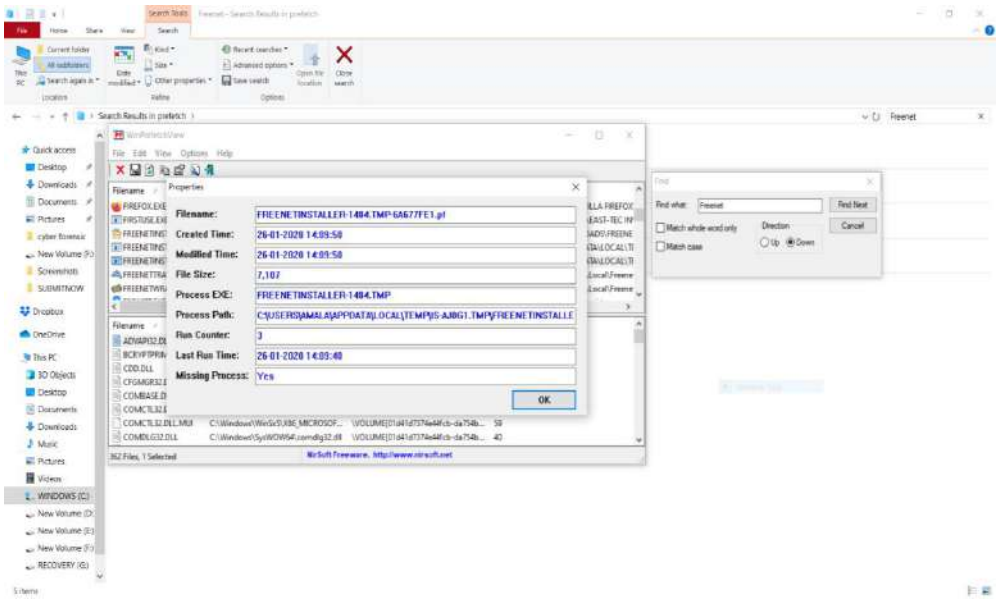


Fig.1'.3

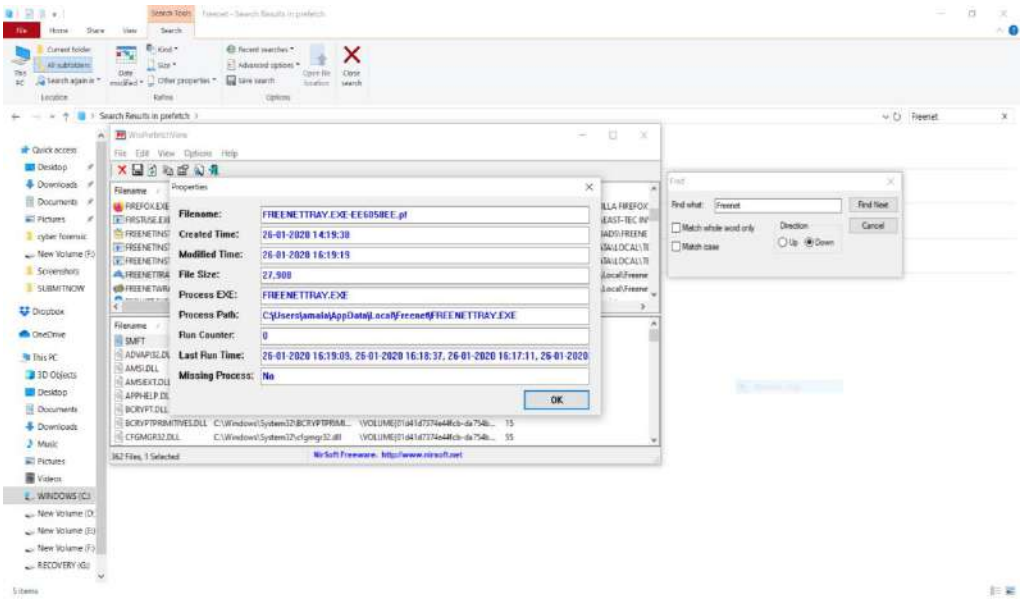


Fig.1'.4

An enlarged view of Fig.1'.3 is given below.

ii.) I2P

The regular search using the keyword "I2P",inside the Windows C Drive gave only a single result.The document was in ".pf" format.(Fig.1'.5)

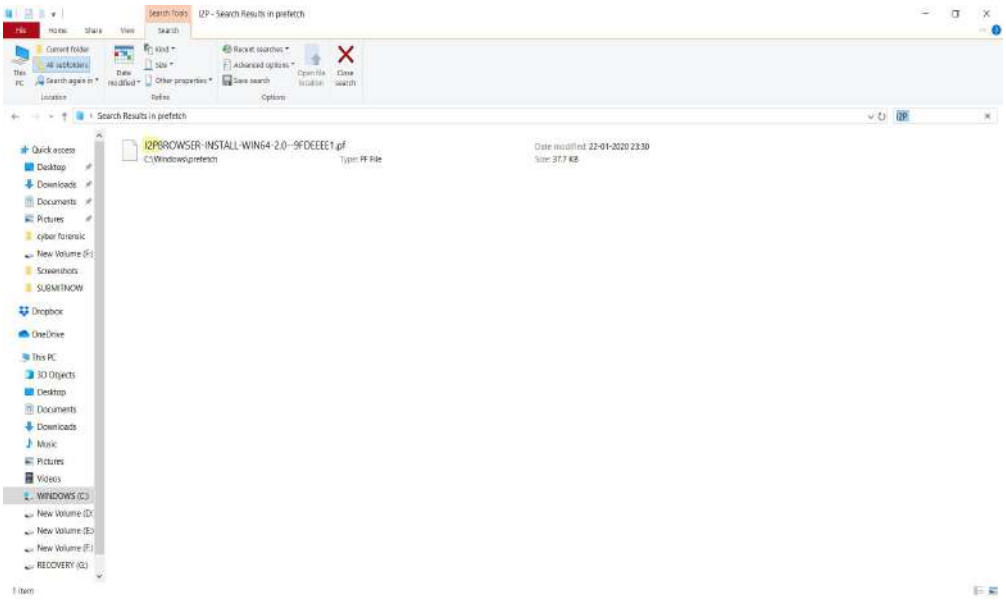


Fig.1'.5

By viewing the properties of the file,the created time,modified time,last used time etc. are known.It also shows the process path of the application.(Fig.1'.6)

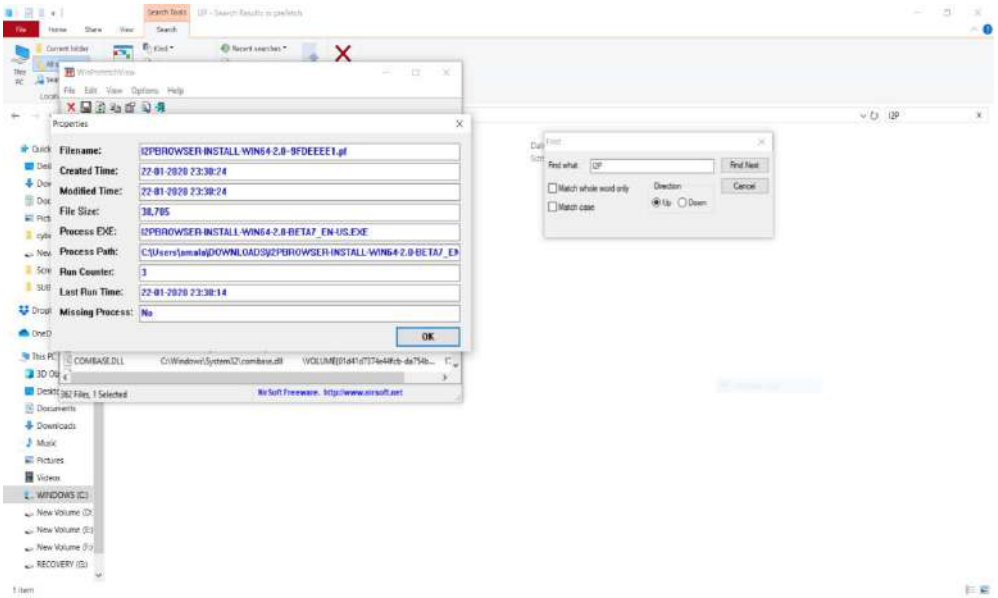
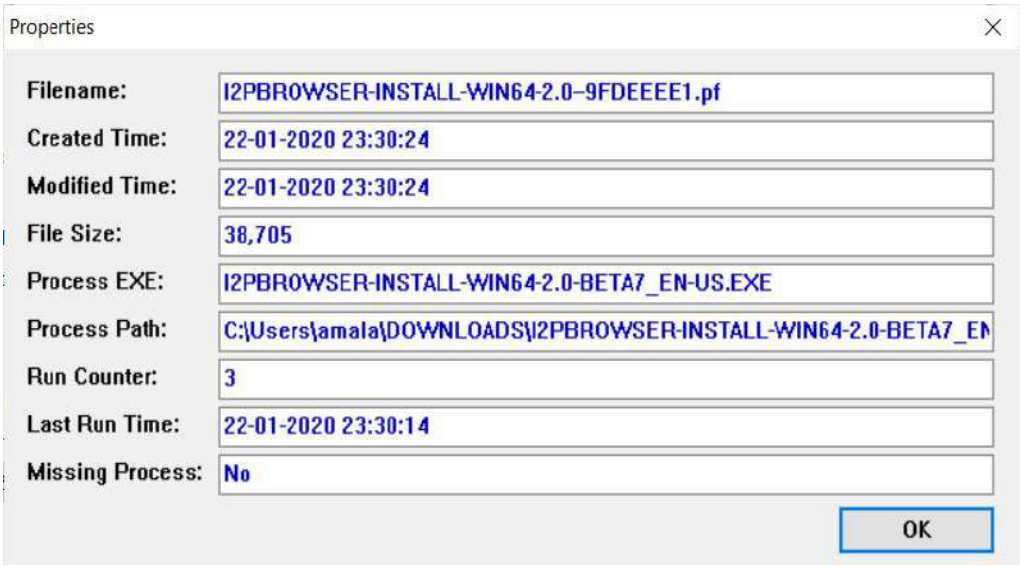


Fig.1'.6

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



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)

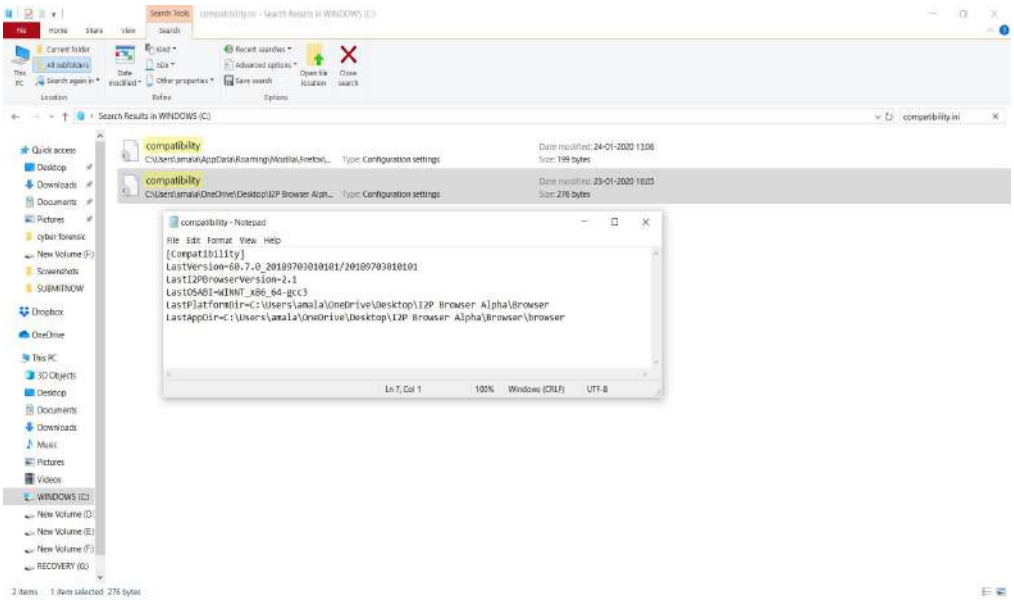


Fig.1'.7

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'.1

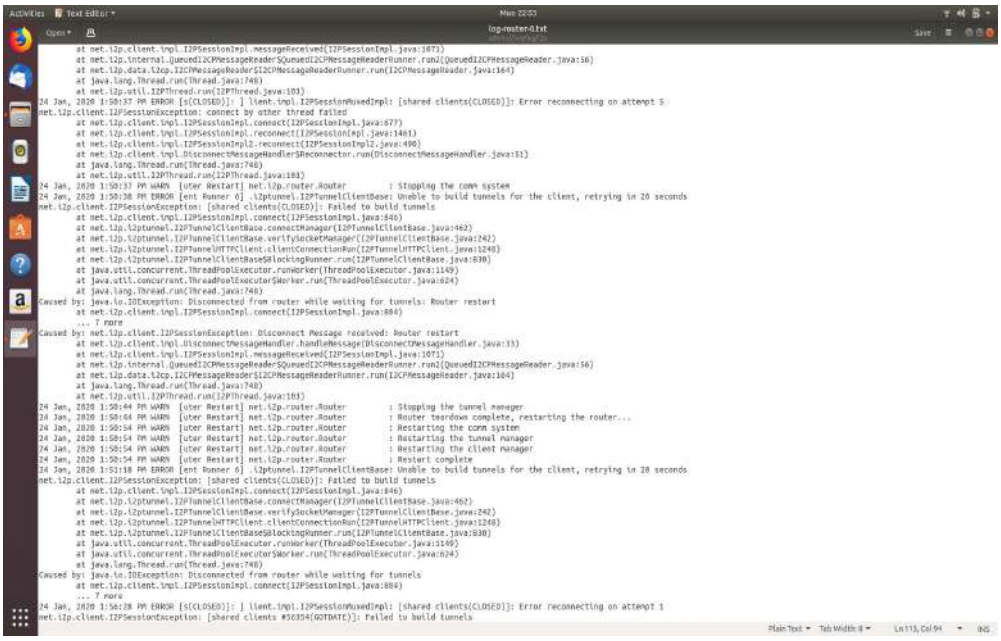


Fig.2'.2

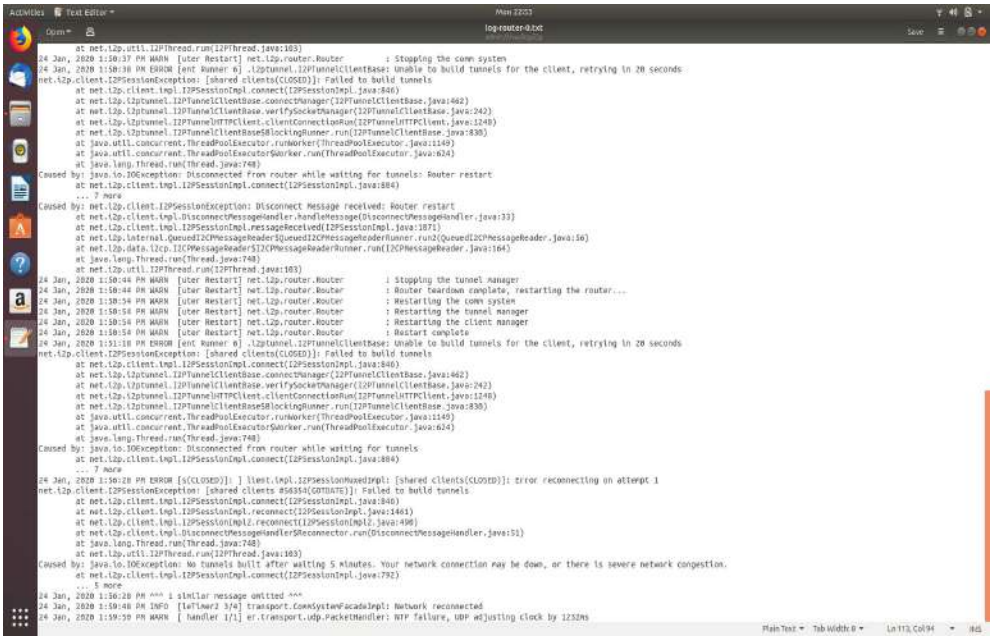


Fig.2'.3

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

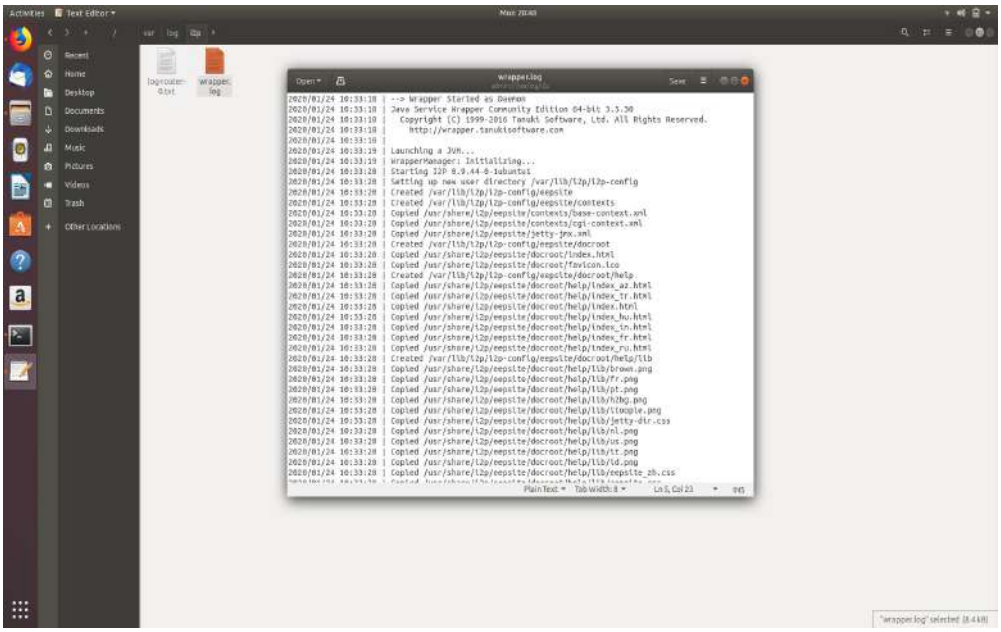


Fig.2'.4

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.

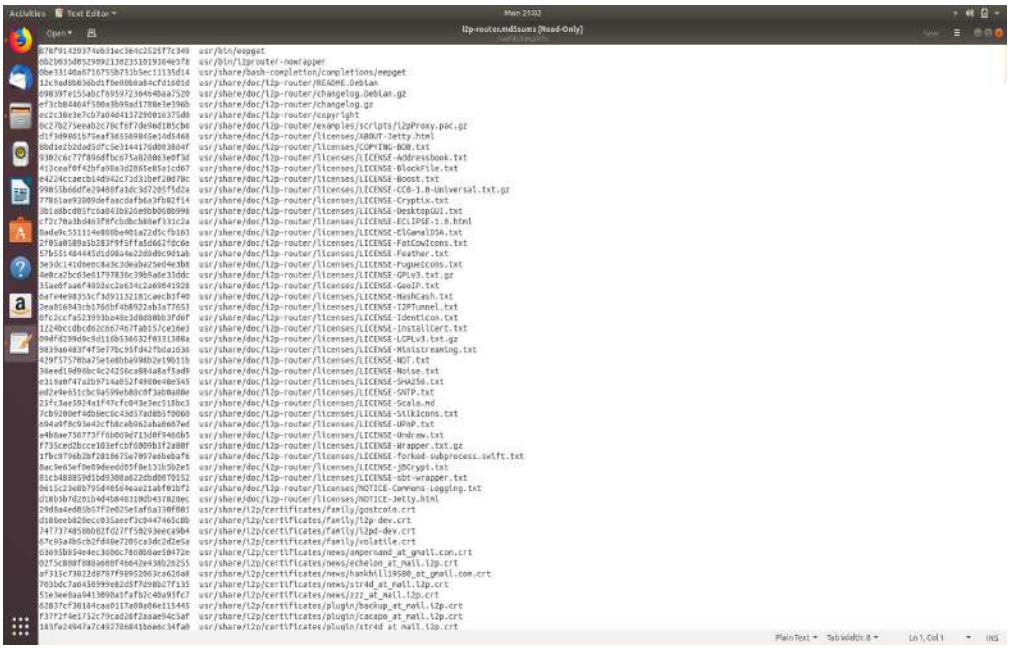


Fig.2'.5

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.

Fig.2’.6

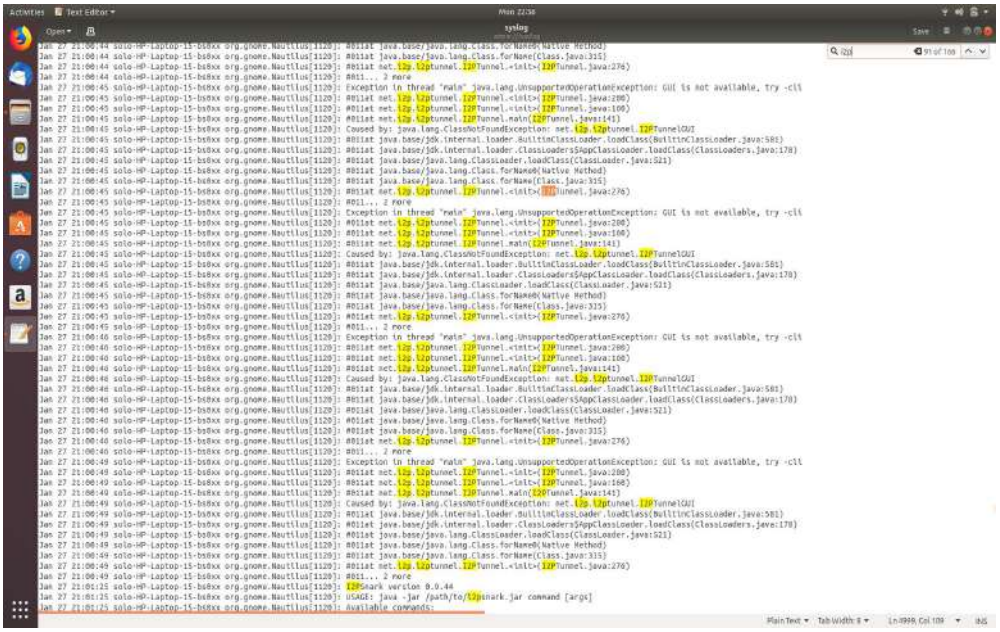


Fig.2’.7

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.

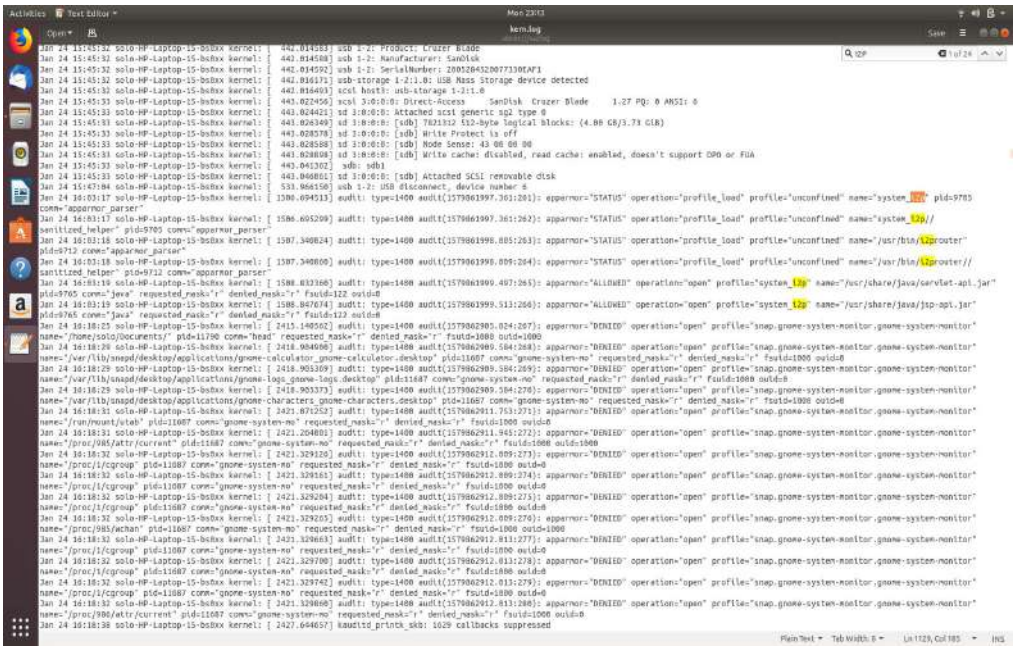


Fig.2’.8

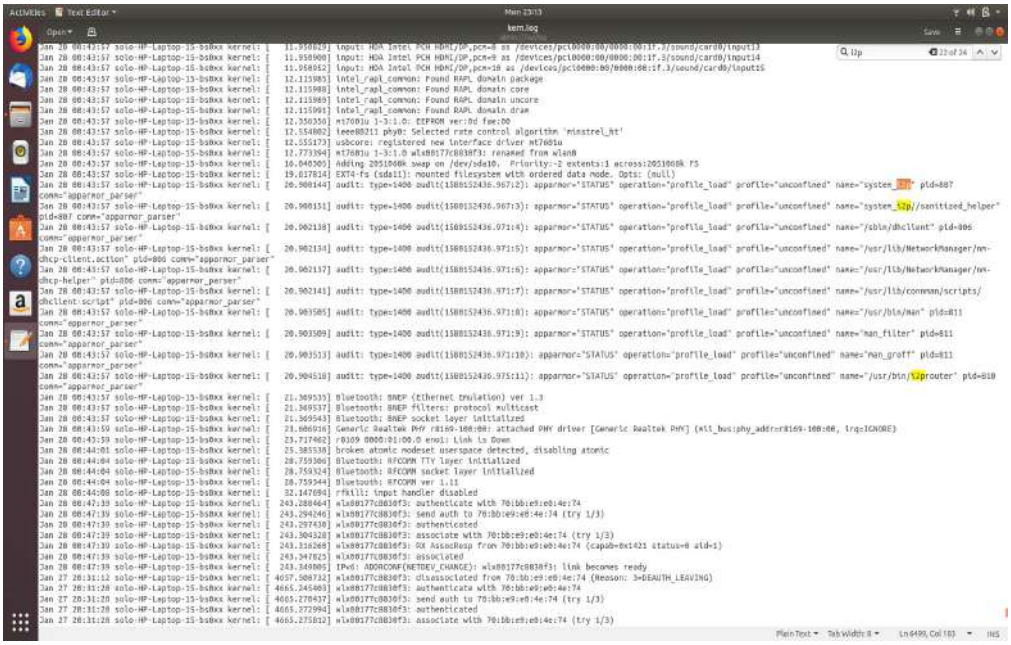


Fig.2’.9

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:

1. 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.

3. 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