Dark Web Monitoring in Tor Browser Forensics

Md. Anisur Rahman

Id: 012202047

Email: mrahman202047@mscse.uiu.ac.bd

MSCSE, United International University.

Supervisor:

Mohammad Mamun Elahi

Assistant Professor, CSE, UIU

Abstract:

Dark webs are hidden websites in the internet, cloud or network sector. It plays an important role in our websites for privacy or data extracted in a hidden way. Dark webs are only accessed by specific web browsers. Deep webs are hidden sites but it isn't fully accessed through the Google, Yahoo, Bing or others search engines. Deep webs refer to pages to not indexed, private datasets, randomly parameters, inaccessible without specific systems and dark websites. The dark web was designed mainly to provide users with more privacy. But nowadays, most dark webs are built for crimes, illegal data extracted, hacking, breaking security and facing trouble into danger of human life. So we need to monitor the dark websites' threat analysis and detection for cyber security.

For this, I've selected this topic Tor browser forensics due to investigation, threat analysis, monitoring the dark websites. Tor (The Onion Router) browser is a specific browser which can be accessed by dark websites. It is free open source software, user friendly and protects our web privacy with safeguard.

For monitoring Dark webs, I've used some security tools such as-Tor Browser, Wireshark, HexEditor, Autopsy, SysTools SQL Recovery.

Keyword: *Tor Browser, Dark web, Forensics, threat analysis, Detection, Cyber Security and Privacy.*

Introduction:

The dark web was designed mainly to provide users with more privacy. Nowadays, most dark webs are built for crimes, illegal data extracted, hacking, breaking security and facing trouble into danger of human life. So we need for monitoring the dark websites' threat analysis and detection for cyber security.

TOR is an anonymous browser that browses webs, networks or clouds with their privacy. Websites privacy is provided by TOR. It accesses client to server in hidden ways. TOR encryption is provided by the application layer with destination network address. Each node during transmission decrypts only the other layer which the next node addresses about the data to be transmitted. TOR can protect and monitoring dark web and threat analysis and detection in cyber security like safeguard. TOR and Dark webs are carried out transactions through cryptographic algorithms with anonymous digital currency; client to server is accessed using cryptographic hash (data integrity), SQL queries and SQL data recovery, memory and network forensics.

So, I've motivated myself to select this topic **"The Dark Web Monitoring in TOR Browser Forensics"** for protecting and providing web privacy with the dark web threat analysis and detection in cyber security.

Related Works:

The Dark webs were created within the Middle 1990 century by Army researchers within the US. The technology that sealed the method for what's currently called the deep webs was employed by intelligence officers to share files anonymously. That initial platform was referred to as 'Tor', known as 'The Onion Router'.

Tor includes us in a cyber-security network that hides our identity as we browse the net, share contents, and have interaction in different on-line activities. It encrypts any information sent from our laptop so nobody will see UN agencies or wherever we are, even once we are logged into a website, Tor is included in hidden word clients are accessed destination using The Onion Router. It had been created by the U.S armed service laboratory within the nineties.

Literature Review:

Literature review is a part and parcel of research papers. It plays an important role in any research papers. All research papers depend on literature review for becoming valuable and acceptable research papers. So some secondary resources are included in my research paper. They are-

1. Evolution of the Dark Web Threat Analysis and Detection: A Symmetric Approach:

- Monitoring the dark webs.
- TOR Connectivity.
- Anomaly Detection.
- Threat Analysis and Detection Technique.
- Research Methodology.

2. Memory Forensics against Ransomware:

- Memory forensics with hash technique.
- RSA Hash key Analysis.
- Memory Investigation.

3. Network Forensics Investigation in TOR:

- TOR established.
- Networks Forensics using Wireshark.
- Anomaly Detection using Wireshark tools.

4. Digital Forensics-Wiley:

- Ram Imaging and Data Acquisition
- About forensics tools.

Research Methodology:

This part is a method of dark web monitoring in TOR Browser Forensics. Some experimental tests and we analyzed some approaches are included by methodology. [1]

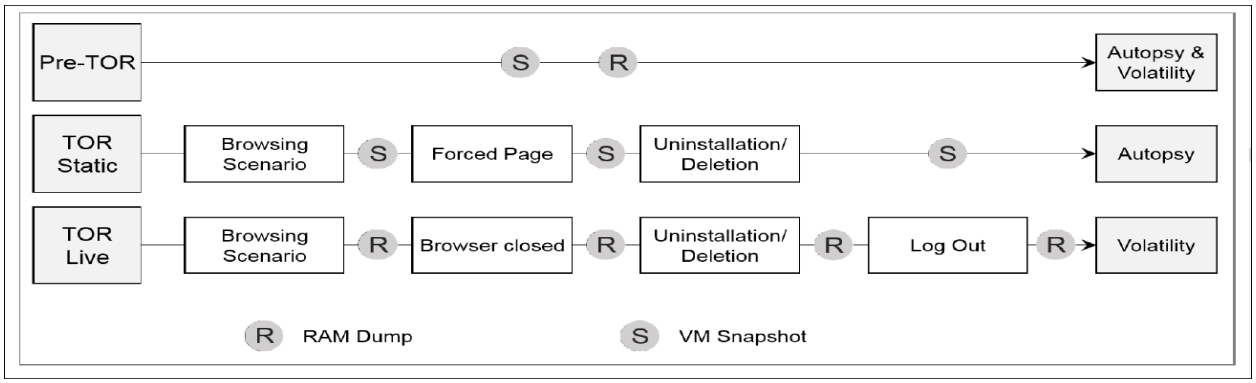
- Research Questions
- Extraction of the data.
- Search Strategy and Selection
- Threat Analysis and Detection
- TOR Forensics
- The dark web monitoring using Hash Tools.

Live associate degree analysis of an application throughout runtime is especially beneficial so as to know however the host software package and application act. because the style e orts of the Tor project have centered on preventing writes to disk (Perry et al., 2018), a live analysis may probably yield additional data pertaining to the browsing session.

Victimization associate degree earlier version of Tor (3.6.1), Darcie et al. (2014) found proof of net browsing in the form of JPEG and hypertext markup language files in live forensics however dead-box (static) forensics was unsuccessful. During a previous live forensics analysis of the Firefox browser, artifacts from a personal browsing session were recovered from memory while the browsing session was open and - to a lesser extent once the browsing session had closed (Findlay and Leimich, 2014). This showed that chrome was ready to terminate running processes,
effectively flushing memory of artifacts of the browsing protocol once the user closed the non-public Browsing window. However, whether or not this is often conjointly true for the TBB has not been established; this will be taken under consideration in our methodology. To build upon previous analysis, our approach has been designed to answer the questions:

- Will Tor Forensics manage to monitor the memory with forensics tools?
- Will the dark web threat analysis and detection how Tor represents?
- Are the dark web monitoring using hash tools how much live forensics victimization?

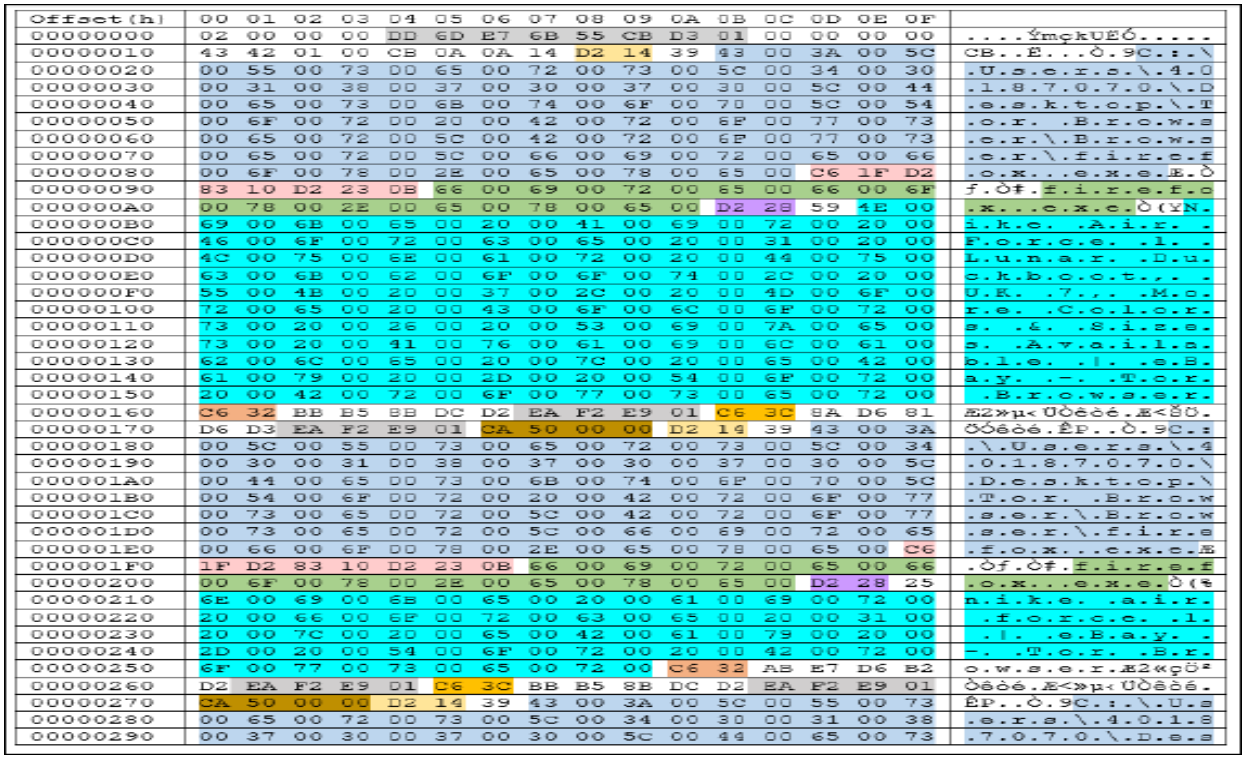
Tor analytical Analysis:



The Dark Web Analysis and Detection:

Hash Analysis:

Classification and assortment of digital proof is one among the main criteria to place criminals beneath enforcement in the cyber-crime as these forms of crimes square measure performed in computer based mostly systems. Hash functions play powerful role in cryptography to prove any proof is authentic during the investigation. Hash functions manufacture has values that represent the first message from that they need been computed. Some well-liked hash algorithms square measure MD5, SHA-1, SHA-256, and SHA-512. TOR contains a difficult structure with thousands of internal nodes and hash price computations that's untraceable however the exit node will be analyzed. Hash price analysis at the exit node layer of the onion routing will be enforced to the destination of the connecting servers. Many researches are done applying the hash price analysis for the detection of crime and digital forensics. These studies embrace analysis of crimes; approximate matching for digital forensically analysis of malware. Also steganography software package detection, fraud detection and financial crime detection. [2][4]



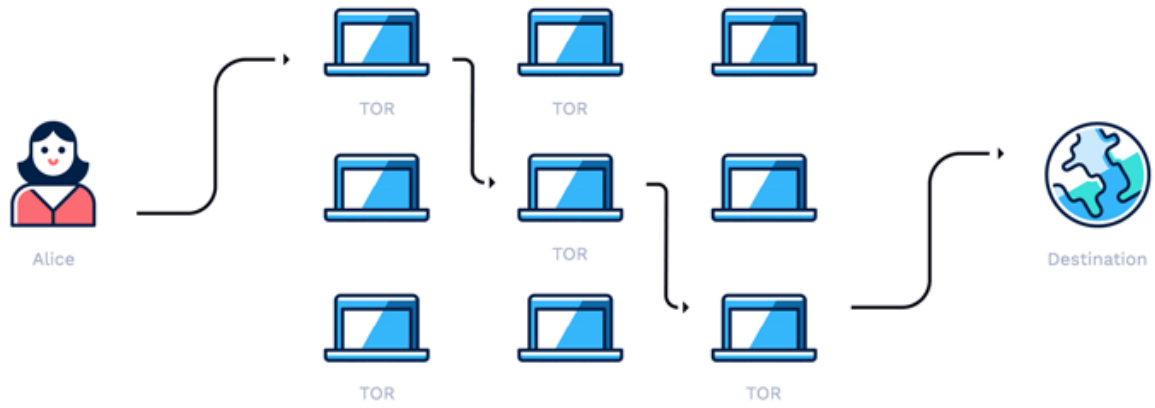
Memory Analysis with HexEditor:

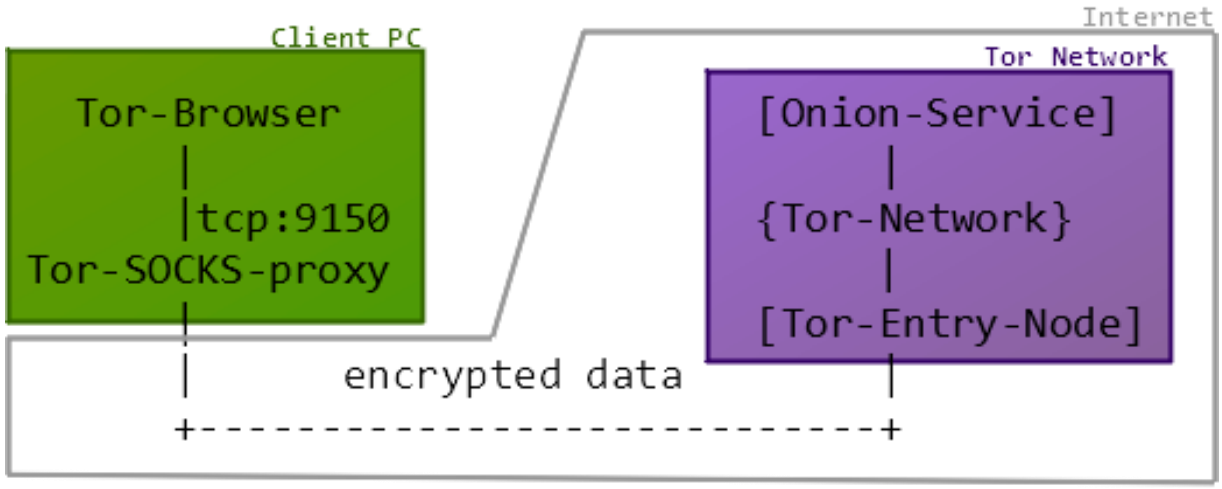
HexEditor is associate degree open supply cross-platform hex editor written in C++ and Widgets. It will work as low level disk editor too. It uses sixty four bytes file descriptors (supports files or devices up to 264 bytes). [2]

Memory Usage: presently 50 Megabytes whereas opened multiple 16GB files.

- May operate with file via XOR coding.
- Has a multiple views to point out multiple files in same time.
- Has an x86 dismantling support (via integrated udis86 library) to hack things very little quicker.
- Has a colorful tag to create reverse engineering easier and additional fun.
- Useful for rescue files/partitions by hand.
- Sector Indication on Disk devices, conjointly has visit Sector dialogue
- Formatted hash code it is simple to repeat a part of a go in HEX formatted.

Network Analysis in TOR:





Dark Web Monitoring Challenges:

1. Acquisition of target forums:

The first challenge is that the identification of target forums that square measure to our operation, i.e. people who contain users and content about cyber counter intelligence. Combined with the mentioned antecedently proven fact that eighty seven of dark internet sites don't link to the other sites, we will deduce that the dark internet is additional a collection of isolated short-lived silos than the classical internet, that encompasses a clear and stable graph structure. Instead of solely loose and sometimes out-of-date collections of URLs (both from the surface internet similarly as Tor Hidden Services) exist on the dark internet. A fully automated approach to beat this issue is unworkable and a semi-manual approach must at the start be used.

2. Resource of the Scalability:

Resource of Scalability a factor not difficult our resources was the habit of extensively sample variety of the most important on-line forums area unit accessible while not this observe, which enabled information assortment and analysis while not having to manually circumvent such protection measures. However, since we tend to did encounter a minimum of some such forums (or elements of forums), our approach might naturally be extended to them, though this would need vital manual resource investment.

3. Real Time Data Extraction:

Real Time Data Extraction is focuses especially on the challenged by the character of a time period data extraction method. Whereas previous studies have collected knowledge from the ark web for analytical functions, they have been targeting a static setting. Time period capability may be a core demand for the longer-term utility of the system, present to the customarily terribly restricted period of the target forums. To enable these functionalities, a high grade of automation is required, from the collection to the live analysis of the data. [5]

4. Data Collection and Processing:

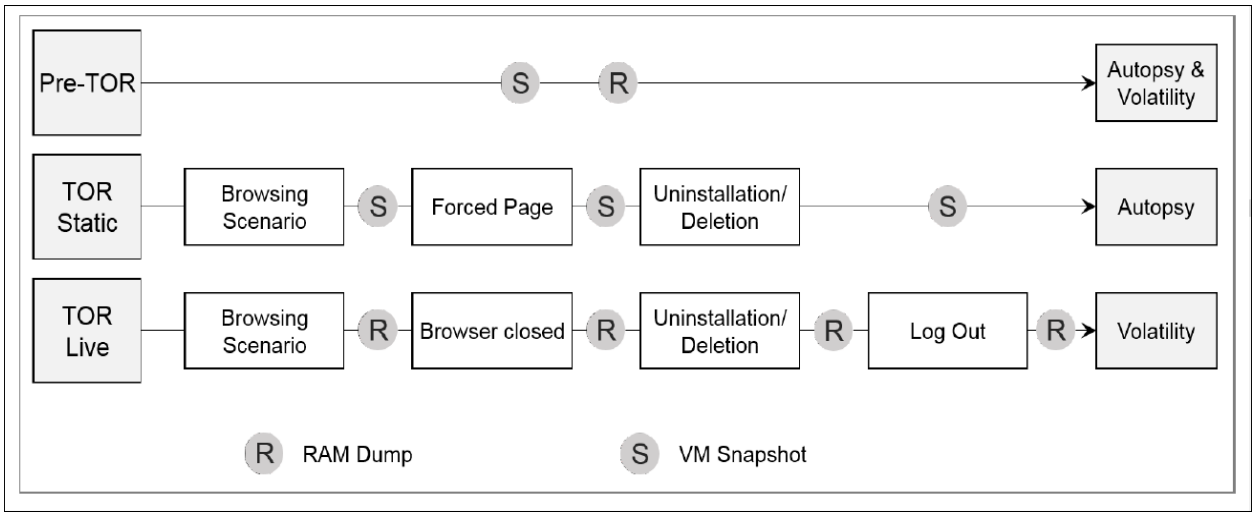
- Establishing anonymous access to forums
- Collection of raw data
- Parsing raw HTML data
- Translation of raw data
- Information Extraction [1]

Dark webs with Tor Methodology

- Tor Browser routes all of your net traffic through the Tor network. because the pictures below illustrate, Tor consists of a three-layer proxy, like layers of associate onion (Tor Browser connects haphazardly of the publically listed entry nodes, bounces that traffic through a at random chosen middle relay, and eventually spits out your traffic through the third and final exit node.

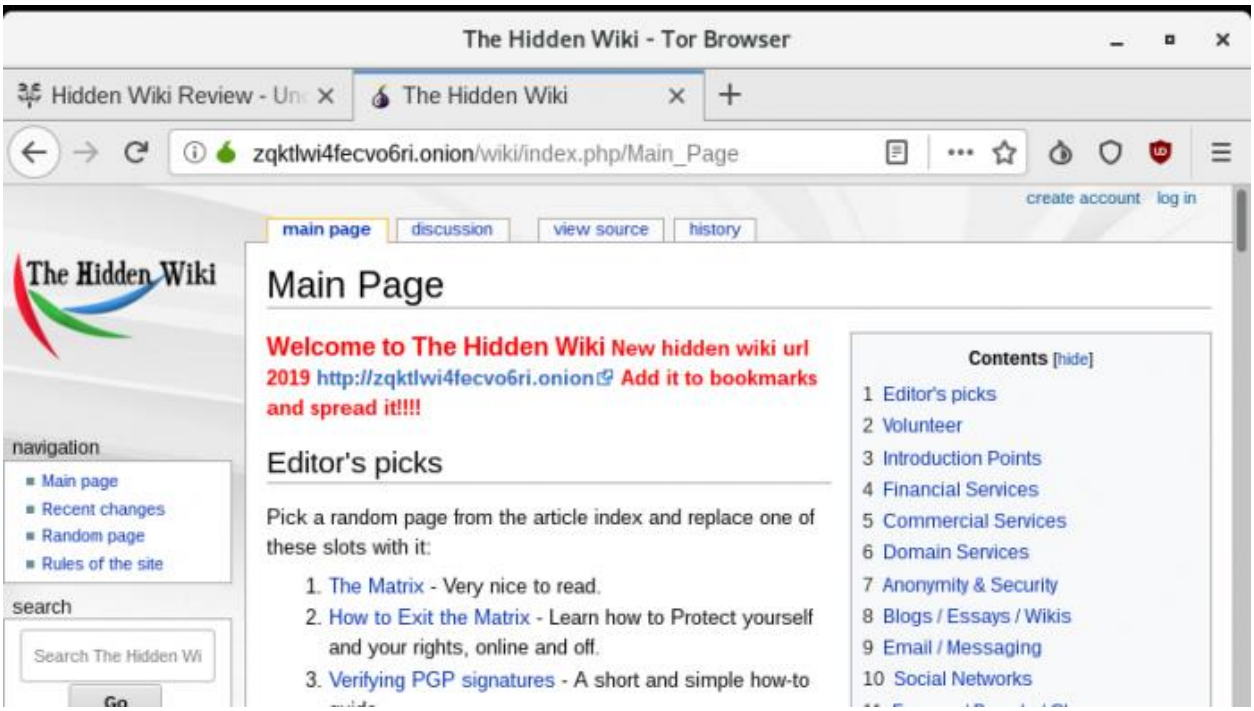
- As a result, do not be surprised if Google or another service greets you in an exceedingly foreign tongue. These services investigate our IP addresses and guesstimate your country and language, however once mistreatment Tor, We may usually seem to be in an exceedingly physical location halfway round the world.

- The Tor network routes TCP traffic of all kinds but is optimized for web browsing. Tor does not support UDP, so don't try to torrent free software ISOs, as it won't work.

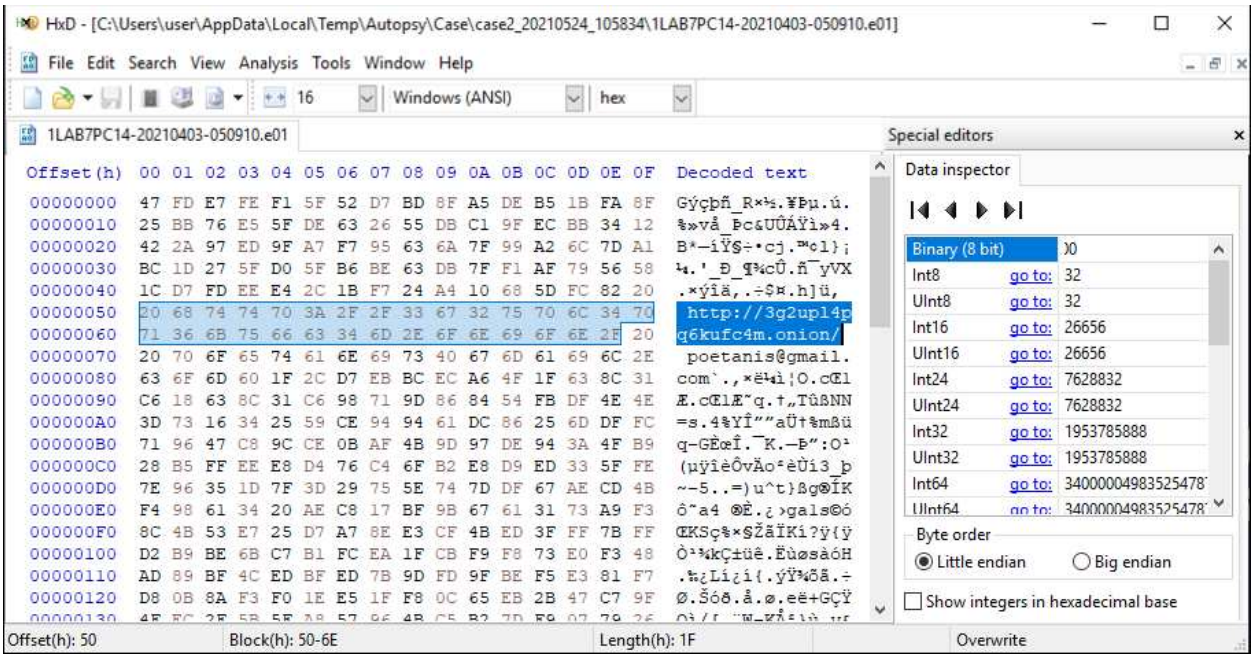


Case Study of Dark web monitoring in Tor Browser Forensics:

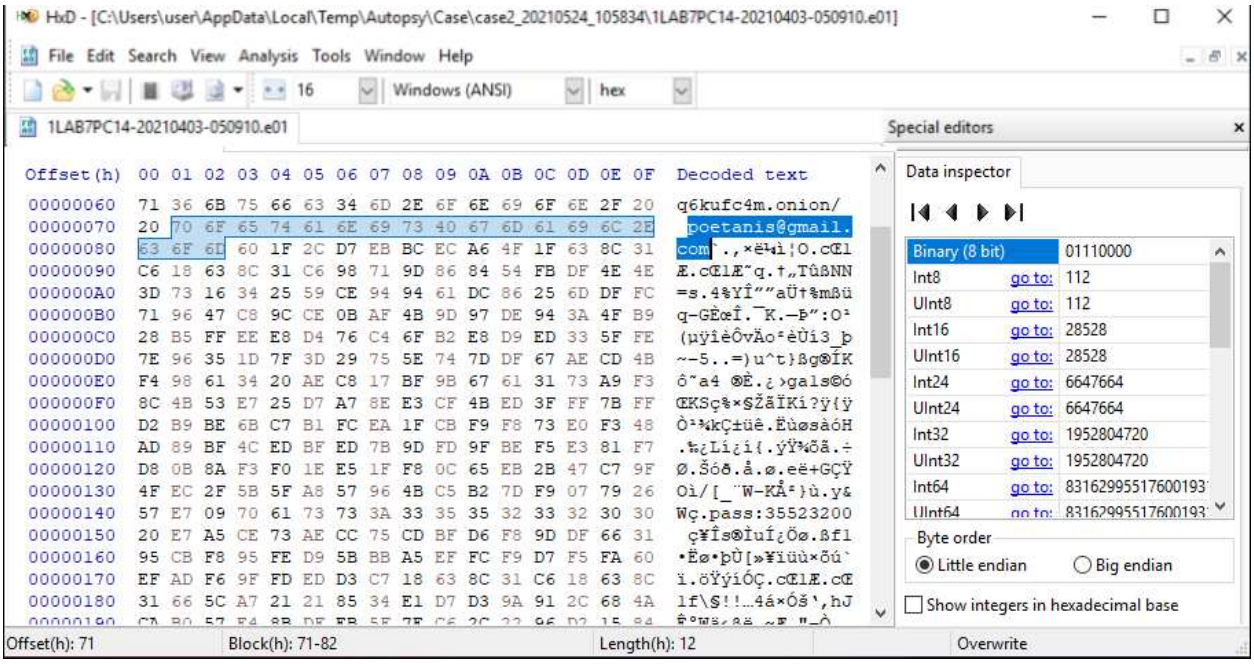
The hidden wiki: A dark web



Hex Analysis of The hidden wiki:

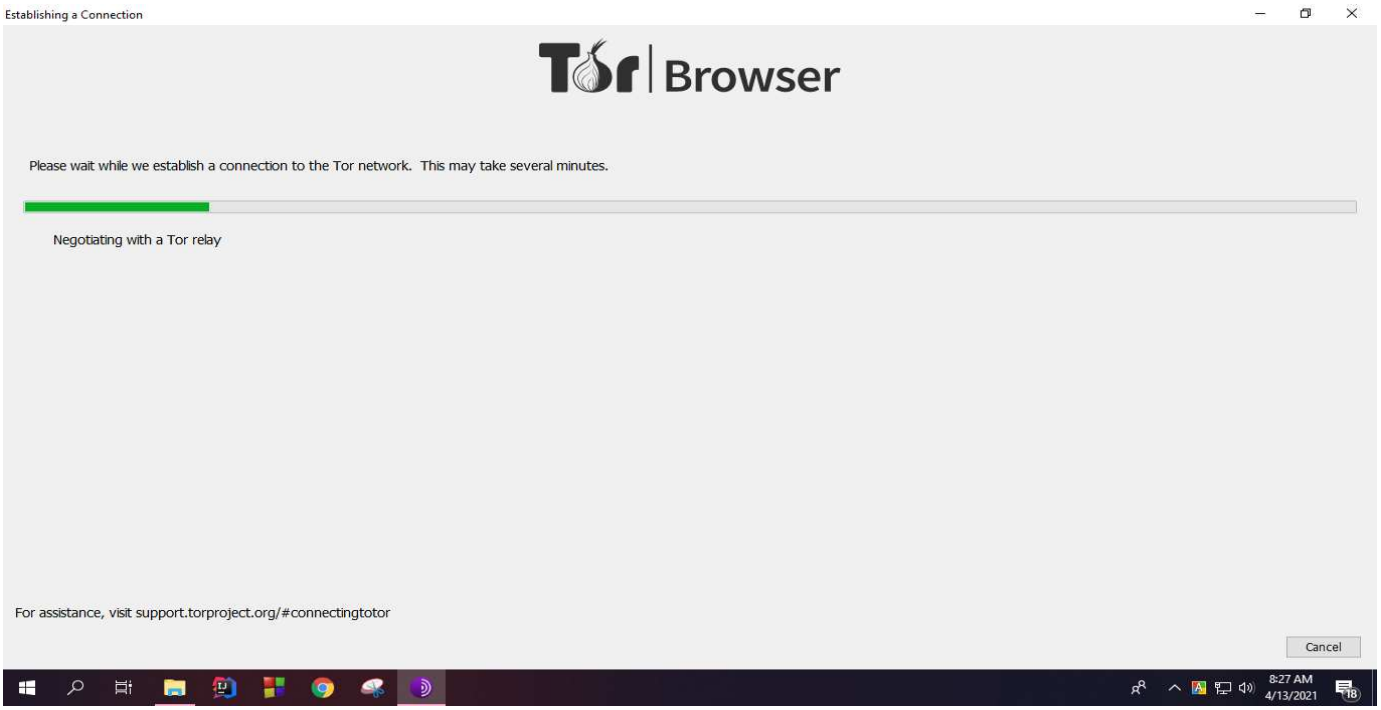


Email Address Found from the hidden wiki:

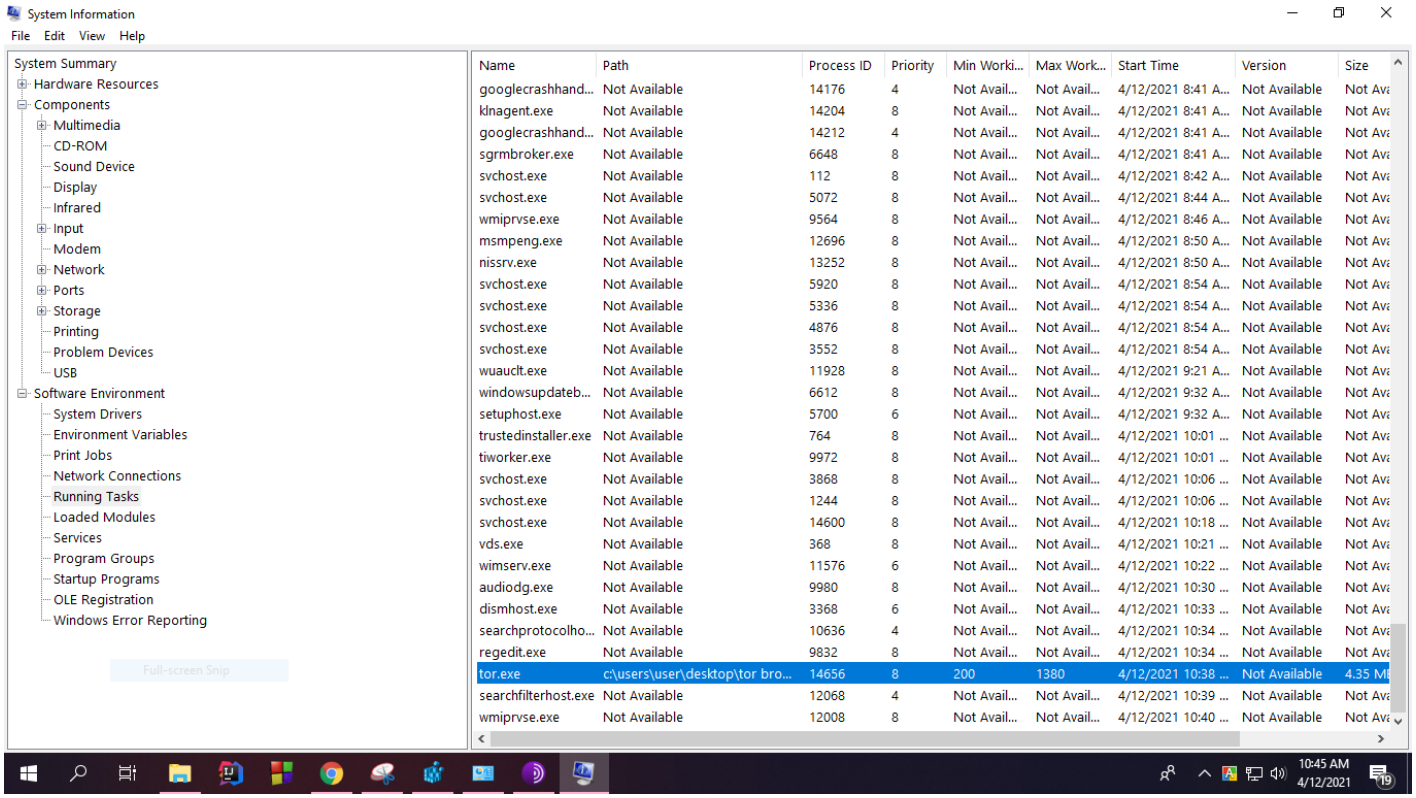


An observation of surface web in Tor:

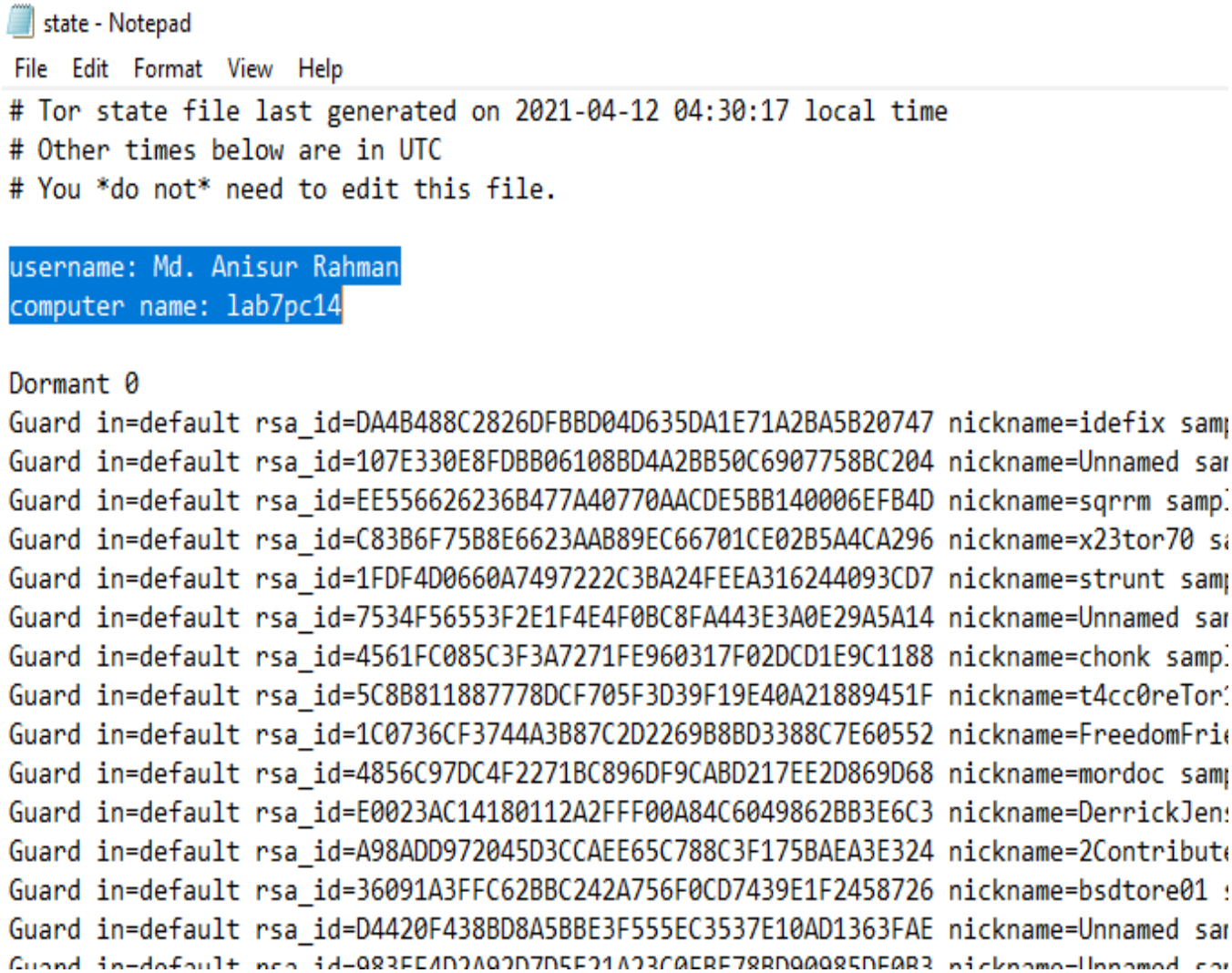
Establishing Tor:



System Information:



Tor State File:



Hex analysis of Surface web with my email which login: *poetanis@gmail.com*

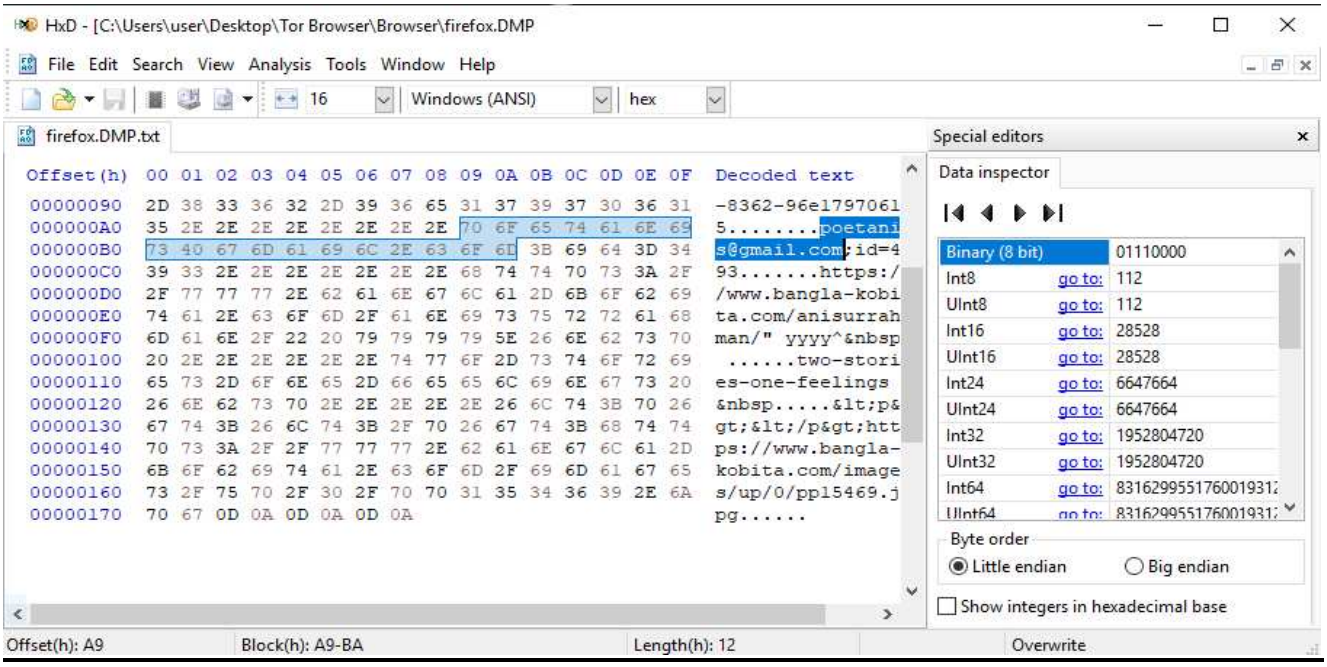
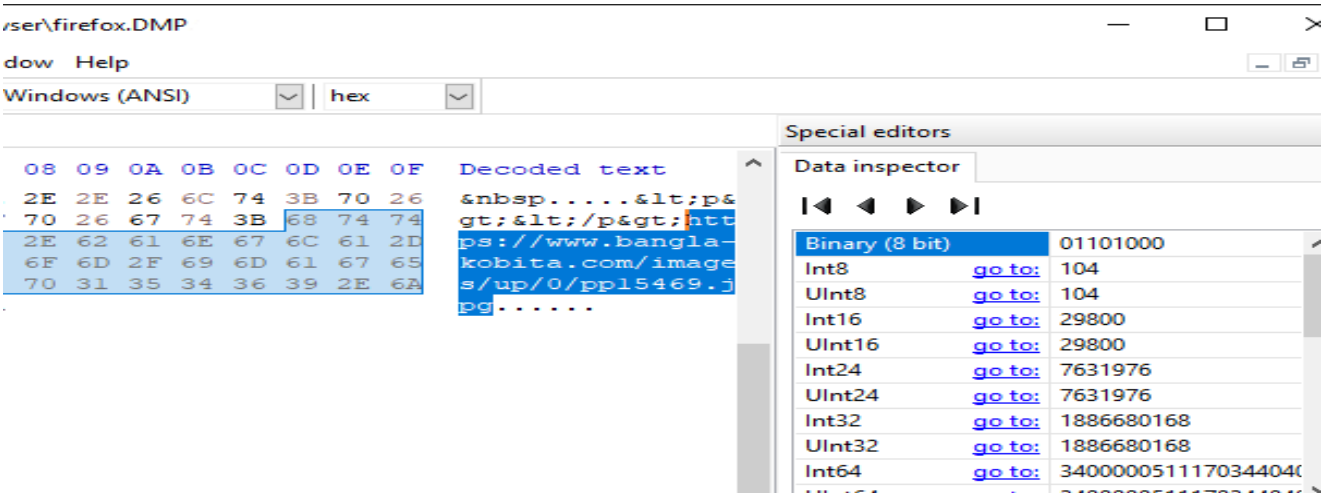
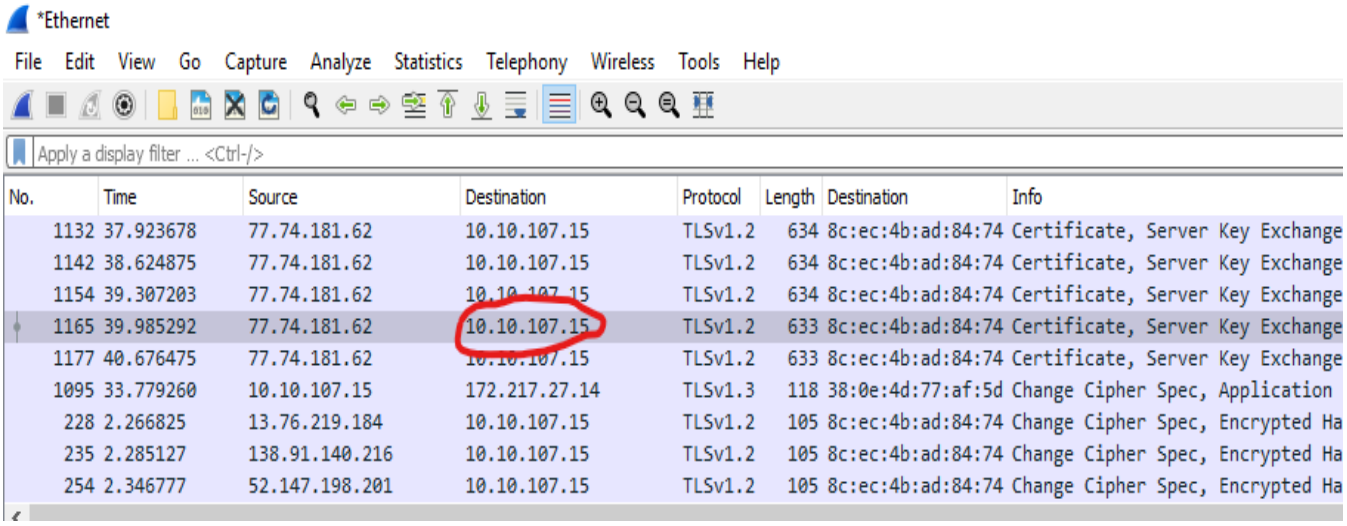


Image Extraction:



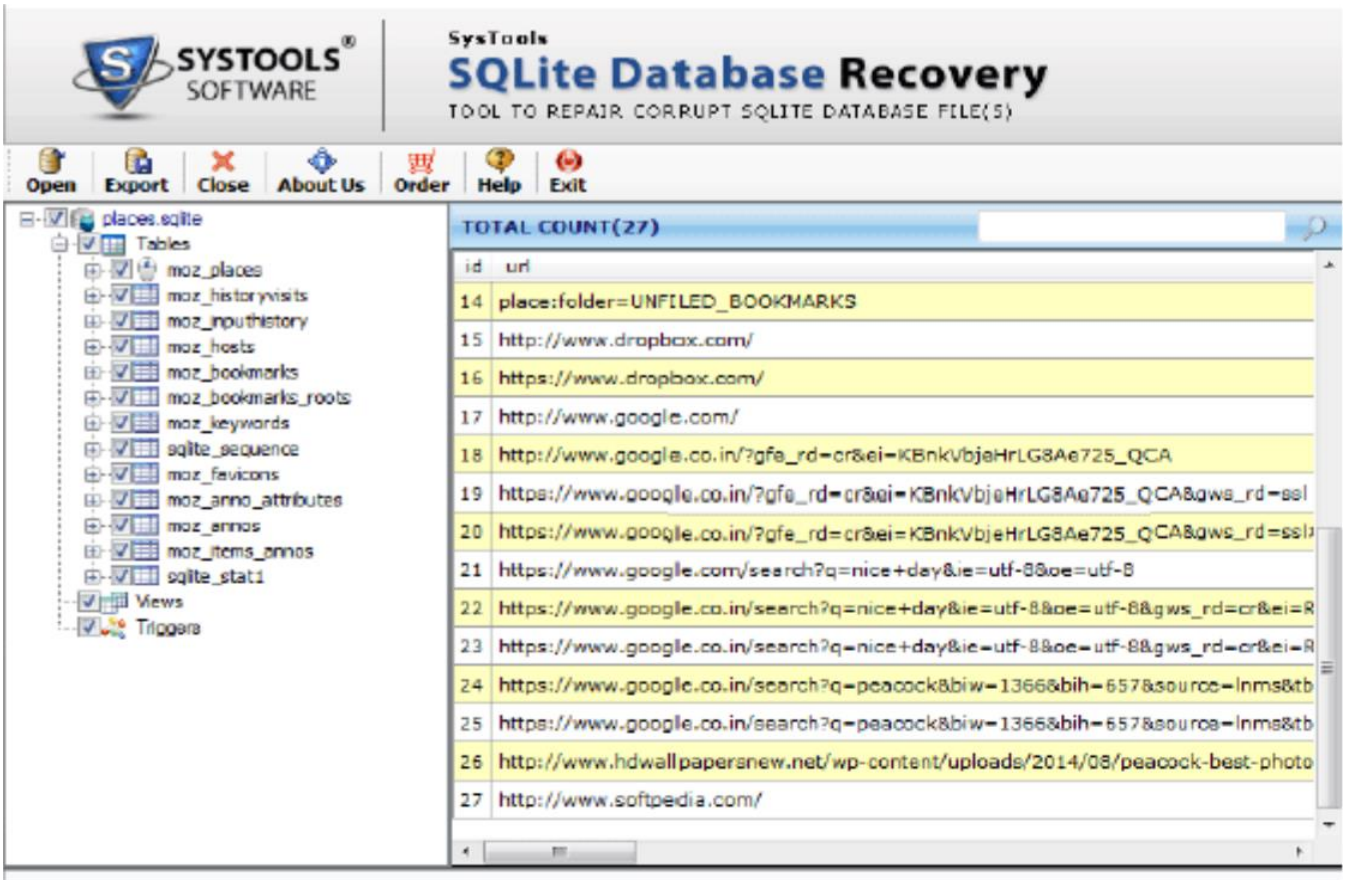
Extracted Image Found: Profile
Link: https://www.bangla-kobita.com/images/up/0/pp15469.jpg

IP address Found using Wireshark Tools in Tor Network Analysis: [3]



No.	Time	Source	Destination	Protocol	Length	Destination	Info
1132	37.923678	77.74.181.62	10.10.107.15	TLSv1.2	634	8c:ec:4b:ad:84:74	Certificate, Server Key Exchange
1142	38.624875	77.74.181.62	10.10.107.15	TLSv1.2	634	8c:ec:4b:ad:84:74	Certificate, Server Key Exchange
1154	39.307203	77.74.181.62	10.10.107.15	TLSv1.2	634	8c:ec:4b:ad:84:74	Certificate, Server Key Exchange
1165	39.985292	77.74.181.62	10.10.107.15	TLSv1.2	633	8c:ec:4b:ad:84:74	Certificate, Server Key Exchange
1177	40.676475	77.74.181.62	10.10.107.15	TLSv1.2	633	8c:ec:4b:ad:84:74	Certificate, Server Key Exchange
1095	33.779260	10.10.107.15	172.217.27.14	TLSv1.3	118	38:0e:4d:77:af:5d	Change Cipher Spec, Application
228	2.266825	13.76.219.184	10.10.107.15	TLSv1.2	105	8c:ec:4b:ad:84:74	Change Cipher Spec, Encrypted Ha
235	2.285127	138.91.140.216	10.10.107.15	TLSv1.2	105	8c:ec:4b:ad:84:74	Change Cipher Spec, Encrypted Ha
254	2.346777	52.147.198.201	10.10.107.15	TLSv1.2	105	8c:ec:4b:ad:84:74	Change Cipher Spec, Encrypted Ha

SysTools SQLite Database Recovery:



Conclusion:

Nowadays, most dark webs are built for crimes, illegal data extracted, hacking, breaking security and facing trouble into danger of human life. But the dark web was designed mainly to provide users with more privacy. So we need to monitor the dark websites' threat analysis and detection for cyber security. Through Tor appears to be a mechanism for secure communication, 1st appearance square measure deceiving. The paper has followed the Tor Project and discovered that the dark web monitoring threat analysis and detection in cyber security.

References:

- *Evolution of the Dark Web Threat Analysis and Detection: A Symmetric Approach; an IEEE Paper.[1]*
- *Memory Forensics against Ransomware; an IEEE Paper.[2]*
- *Network Forensics Investigation in TOR; Google scholar.[3]*
- *Digital Forensics: 3rd edition-Wiley; A text book.[4]*
- *Researchgate papers online [5]*