

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.

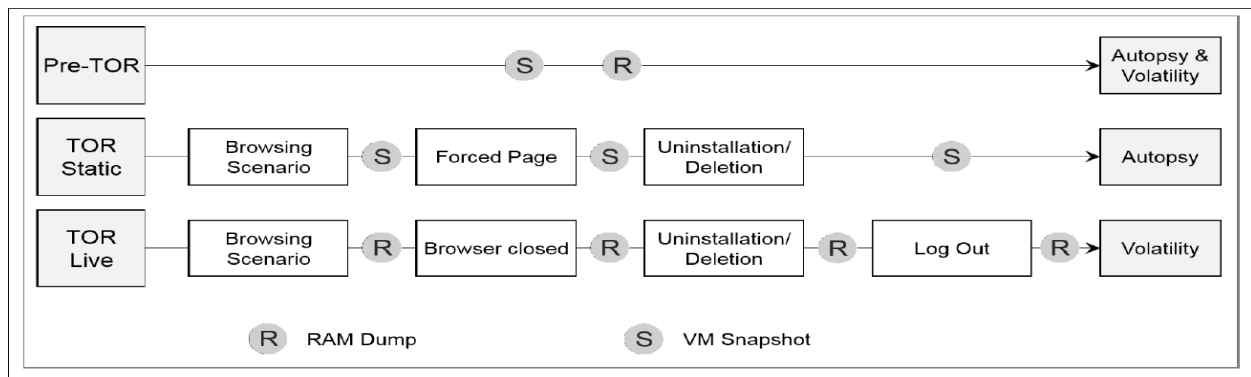
Live associate degree analysis of an application throughout runtime is especially beneficial so as to know however the host software package and application act. because the style e orts of the Tor project have centered on preventing writes to disk (Perry et al., 2018), a live analysis may probably yield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

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	02	00	00	00	DD	6D	E7	6B	55	CB	D3	01	00	00	00	00ŷmqkUEÓ....
00000010	43	42	01	00	CB	0A	0A	14	D2	14	39	43	00	3A	00	5C	CB...E...Ō.9C.t.:\\
00000020	00	55	00	73	00	65	00	72	00	73	00	5C	00	34	00	30	.U.s.e.r.s\\.4.0.30
00000030	00	31	00	38	00	37	00	30	00	37	00	30	00	5C	00	44	.l.s.7.0.7.0.\\D
00000040	00	65	00	73	00	6B	00	74	00	6F	00	70	00	5C	00	54	.e.s.k.t.o.p\\.T
00000050	00	6F	00	72	00	20	00	42	00	72	00	6F	00	77	00	73	.o.r\\.B.r.o.w.s
00000060	00	65	00	72	00	5C	00	42	00	72	00	6F	00	77	00	73	.e.r\\.B.r.o.w.s
00000070	00	65	00	72	00	5C	00	66	00	69	00	72	00	65	00	66	.e.r\\.f.i.r.e.f
00000080	00	6F	00	78	00	2E	00	65	00	78	00	65	00	C6	1F	D2	.o.x...e.x.e.E.Ō
00000090	83	10	D2	23	0B	66	00	69	00	72	00	65	00	66	00	6F	f.Ōf.F.i.r.e.f.c
000000A0	00	78	00	2E	00	65	00	78	00	65	00	D2	28	59	4E	00	.x...e.x.e.Ō(ŷN.
000000B0	69	00	6B	00	65	00	20	00	41	00	69	00	72	00	20	00	.i.k.e..A.i.r..
000000C0	46	00	6F	00	72	00	63	00	65	00	20	00	31	00	20	00	F.o.r.c.e..l..
000000D0	4C	00	75	00	6E	00	61	00	72	00	20	00	44	00	75	00	L.u.n.a.r..D.u.
000000E0	63	00	6B	00	62	00	6F	00	6F	00	74	00	2C	00	20	00	c.k.b.o.c.t...\\
000000F0	55	00	4B	00	20	00	37	00	2C	00	20	00	4D	00	6F	00	U.R..7...M.o.
00000100	72	00	65	00	20	00	43	00	6F	00	6C	00	6F	00	72	00	r.e..C.o.l.o.r..
00000110	73	00	20	00	26	00	20	00	53	00	69	00	7A	00	65	00	s..&..S.i.s.e.
00000120	73	00	20	00	41	00	76	00	61	00	69	00	6C	00	61	00	s..A.v.a.i.l.a.
00000130	62	00	6C	00	65	00	20	00	7C	00	20	00	65	00	42	00	b.l.e..l..e.B.
00000140	61	00	79	00	20	00	2D	00	20	00	54	00	6F	00	72	00	a.y..-..T.o.r.
00000150	20	00	42	00	72	00	6F	00	77	00	73	00	65	00	72	00	.B.r.o.w.s.e.r.
00000160	C6	32	BB	B5	8B	DC	D2	EA	F2	E9	01	C6	3C	8A	D6	81	æ2»µ<ŪŌææ.E<8Ū
00000170	D6	D3	EA	F2	E9	01	CA	50	00	00	D2	14	39	43	00	3A	ŌŌææ.Ėp...Ō.9C.i
00000180	00	5C	00	55	00	73	00	65	00	72	00	73	00	5C	00	34	.\\U.s.e.r.s\\.4
00000190	00	30	00	31	00	38	00	37	00	30	00	37	00	30	00	5C	.0.l.s.7.0.7.0.\\
000001A0	00	44	00	65	00	73	00	6B	00	74	00	6F	00	70	00	5C	.D.e.s.k.t.o.p\\.
000001B0	00	54	00	6F	00	72	00	20	00	42	00	72	00	6F	00	77	.T.o.r..B.r.o.w
000001C0	00	73	00	65	00	72	00	5C	00	42	00	72	00	6F	00	77	.s.e.r\\.B.r.o.w
000001D0	00	73	00	65	00	72	00	5C	00	66	00	69	00	72	00	65	.s.e.r\\.f.i.r.e
000001E0	00	66	00	6F	00	78	00	2E	00	65	00	78	00	65	00	C6	.f.o.x...e.x.e.E
000001F0	1F	D2	83	10	D2	23	0B	66	00	69	00	72	00	65	00	66	.Ōf.Ōf.F.i.r.e.f
00000200	00	6F	00	78	00	2E	00	65	00	78	00	65	00	D2	28	25	.o.x...e.x.e.Ō(t
00000210	6E	00	69	00	6B	00	65	00	20	00	61	00	69	00	72	00	n.i.k.e..a.i.r.
00000220	20	00	66	00	6F	00	72	00	63	00	65	00	20	00	31	00	.f.o.r.c.e..l..
00000230	20	00	7C	00	20	00	65	00	42	00	61	00	79	00	20	00	.l..e.B.a.y..
00000240	2D	00	20	00	54	00	6F	00	72	00	20	00	42	00	72	00	-..T.o.r..B.r.
00000250	6F	00	77	00	73	00	65	00	72	00	C6	32	AB	E7	D6	B2	o.w.s.e.r.æ2«gŪ²
00000260	D2	EA	F2	E9	01	C6	3C	BB	B5	8B	DC	D2	EA	F2	E9	01	Ōææ.E<»µ<ŪŌææ.
00000270	CA	50	00	00	D2	14	39	43	00	3A	00	5C	00	55	00	73	Ėp...Ō.9C.i.\\U.s
00000280	00	65	00	72	00	73	00	5C	00	34	00	30	00	31	00	38	.e.r.s\\.4.0.l.s
00000290	00	37	00	30	00	37	00	30	00	5C	00	44	00	65	00	73	.7.0.7.0.\\D.e.s

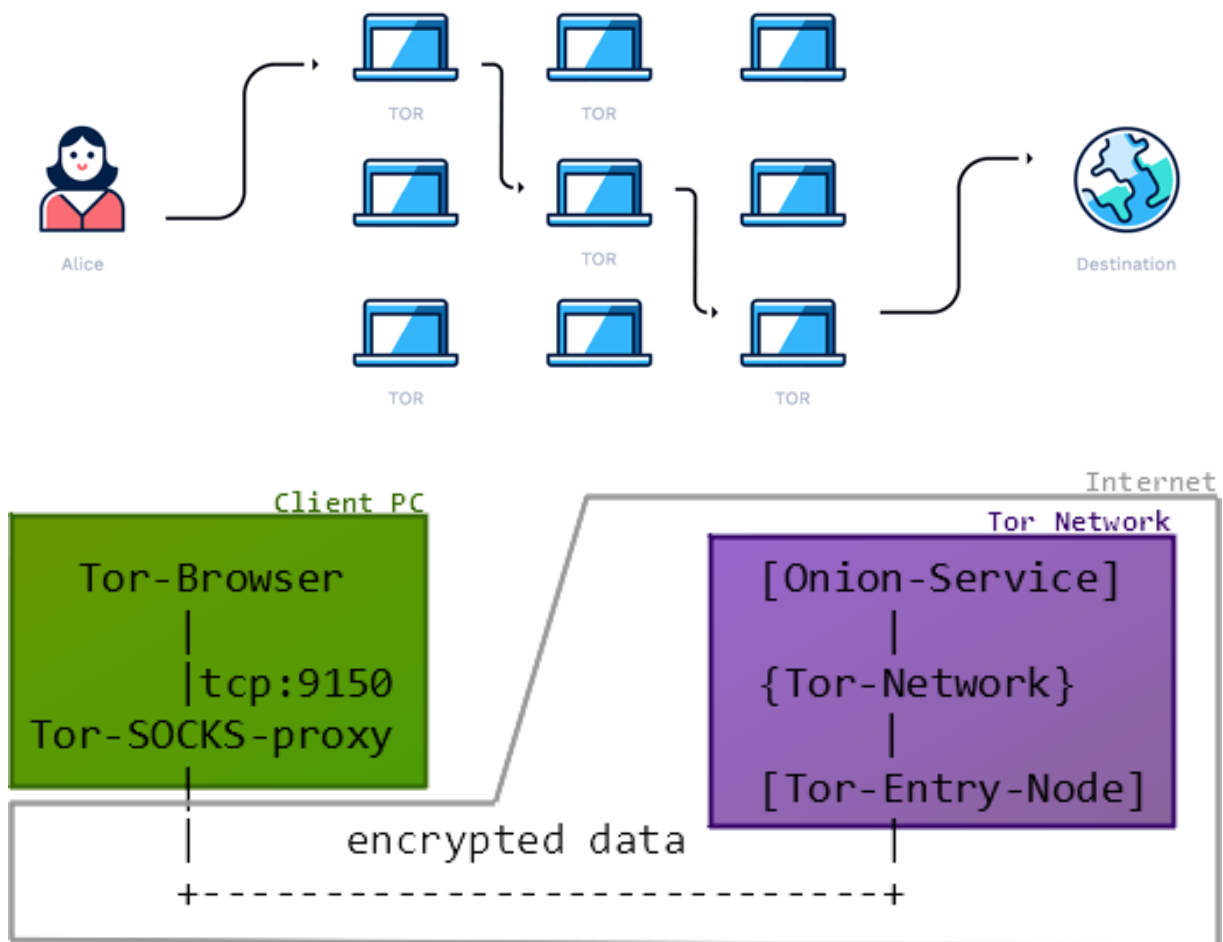
Memory Analysis with HexEditor:

HexEditor is an open source cross-platform hex editor written in C++ and Widgets. It will work as a 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:

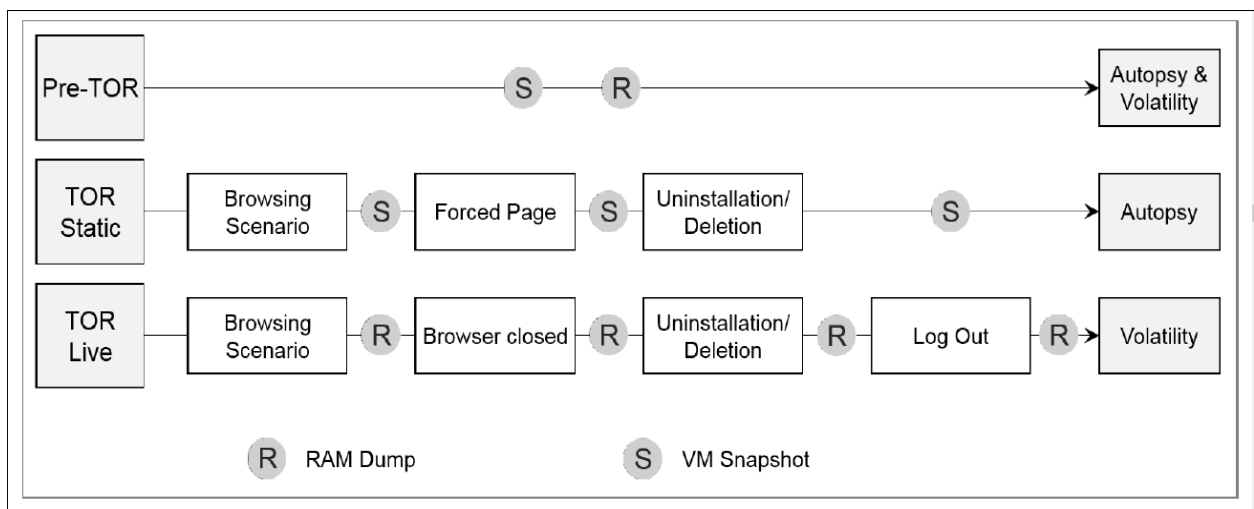
Real Time Data Extraction is focuses especially on the challenged by the character of a time period data extraction method. Whereas previous studies have collected knowledge from the ark web for analytical functions, they have been targeting a static setting. Time period capability may be a core demand 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 [\[1\]](#)

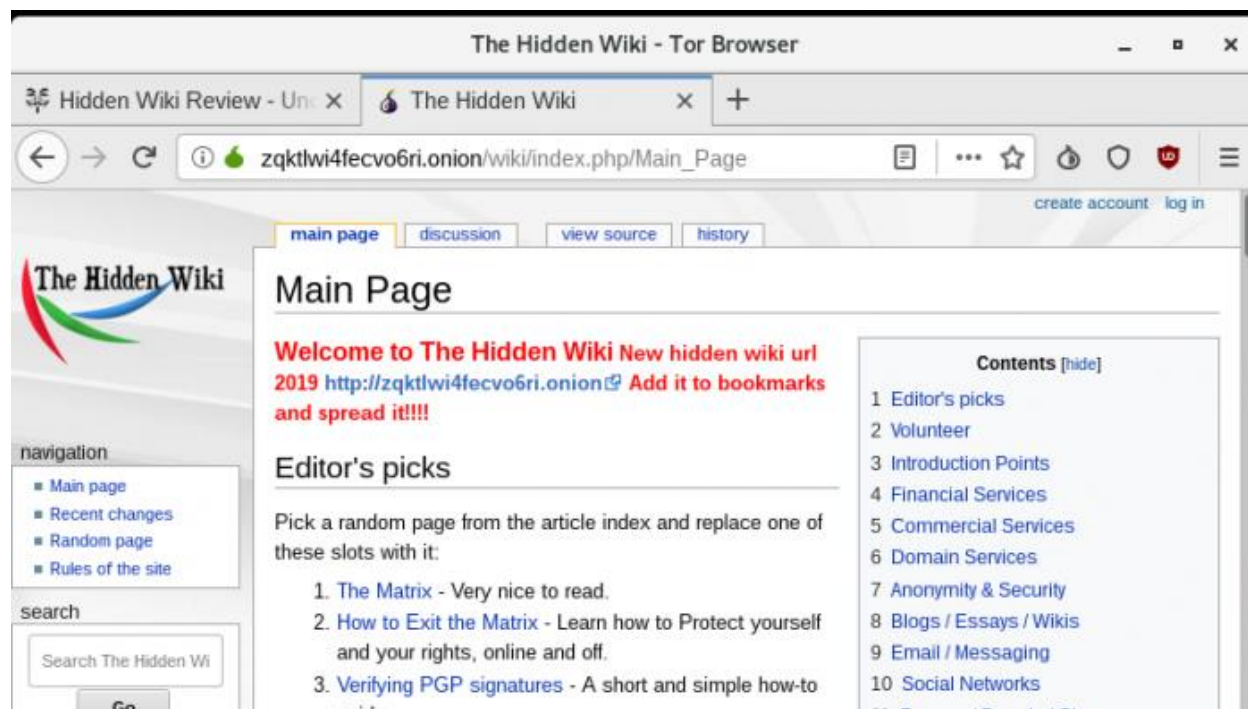
Dark webs with Tor Methodology

- 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.

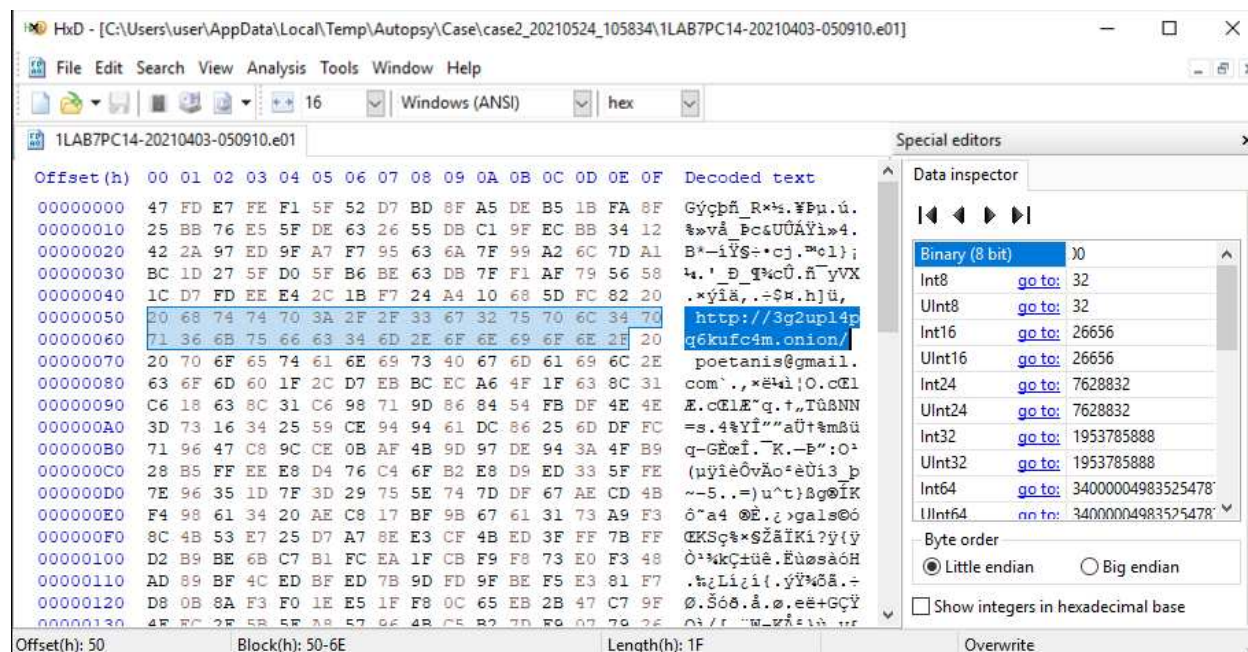


Case Study of Dark web monitoring in Tor Browser Forensics:

The hidden wiki: A dark web



Hex Analysis of The hidden wiki:



Email Address Found from the hidden wiki:

HxD - [C:\Users\user\AppData\Local\Temp\Autopsy\Case\case2_20210524_105834\1LAB7PC14-20210403-050910.e01]

File Edit Search View Analysis Tools Window Help

16 Windows (ANSI) hex

1LAB7PC14-20210403-050910.e01

Special editors

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000060	71	36	6B	75	66	63	34	6D	2E	6F	6E	69	6F	6E	2F	20	q6kufc4m.onion/
00000070	20	70	6F	65	74	61	6E	69	73	40	67	6D	61	69	6C	2E	poetanis@gmail.
00000080	63	6F	61	60	1F	2C	D7	EB	BC	EC	A6	4F	1F	63	8C	31	com`.,*e4i;O.cEl
00000090	C6	18	63	8C	31	C6	98	71	9D	86	84	54	FB	DF	4E	4E	E.cElE`q.†„TûßNN
000000A0	3D	73	16	34	25	59	CE	94	94	61	DC	86	25	6D	DF	FC	=s.4%YI`"aŮ†%mßü
000000B0	71	96	47	C8	9C	CE	0B	AF	4B	9D	97	DE	94	3A	4F	B9	q-GÊeİ.~K.-B":O:
000000C0	28	B5	FF	EE	E8	D4	76	C4	6F	B2	E8	D9	ED	33	5F	FE	(µyieÖvÄo°eÜi3_p
000000D0	7E	96	35	1D	7F	3D	29	75	5E	74	7D	DF	67	AE	CD	4B	~-5.,.=)u^t)ßg@İK
000000E0	F4	98	61	34	20	AE	C8	17	BF	9B	67	61	31	73	A9	F3	ô*a4 @Ê.¿>gals@ó
000000F0	8C	4B	53	E7	25	D7	A7	8E	E3	CF	4B	ED	3F	FF	7B	FF	QKSç*×\$ZâİKi?ý{ý
00000100	D2	B9	BE	6B	C7	B1	FC	EA	1F	CB	F9	F8	73	E0	F3	48	Ô°%kÇ±üê.ÊûesàóH
00000110	AD	89	BF	4C	ED	BF	ED	7B	9D	FD	9F	BE	F5	E3	81	F7	.%¿Li¿i{.ýY%ôâ.÷
00000120	D8	0B	8A	F3	F0	1E	E5	1F	F8	0C	65	EB	2B	47	C7	9F	Ø.Šóð.â.ø.eë+GÇY
00000130	4F	EC	2F	5B	5F	A8	57	96	4B	C5	B2	7D	F9	07	79	26	Oi/[_"W-KÄ°)ù.y&
00000140	57	E7	09	70	61	73	73	3A	33	35	35	32	33	32	30	30	Wç.pass:35523200
00000150	20	E7	A5	CE	73	AE	CC	75	CD	BF	D6	F8	9D	DF	66	31	çYis@İui¿Öø.ßfl
00000160	95	CB	F8	95	FE	D9	5B	BB	A5	EF	FC	F9	D7	F5	FA	60	•Êø•pŮ[»Yİüù×ôú`
00000170	EF	AD	F6	9F	FD	ED	D3	C7	18	63	8C	31	C6	18	63	8C	i.öYýiÓç.cElÆ.cœ
00000180	31	66	5C	A7	21	21	85	34	E1	D7	D3	9A	91	2C	68	4A	1f\Š!!...4â×ÓŠ',hJ
00000190	CA	B0	57	E4	8B	DE	EB	5F	7F	C6	2C	22	96	D2	15	84	ê°wß¿ßß çF "„À

Offset(h): 71 Block(h): 71-82 Length(h): 12 Overwrite

Data inspector

Binary (8 bit) 01110000

Int8 go to: 112

UInt8 go to: 112

Int16 go to: 28528

UInt16 go to: 28528

Int24 go to: 6647664

UInt24 go to: 6647664

Int32 go to: 1952804720

UInt32 go to: 1952804720

Int64 go to: 83162995517600193

UInt64 go to: 83162995517600193

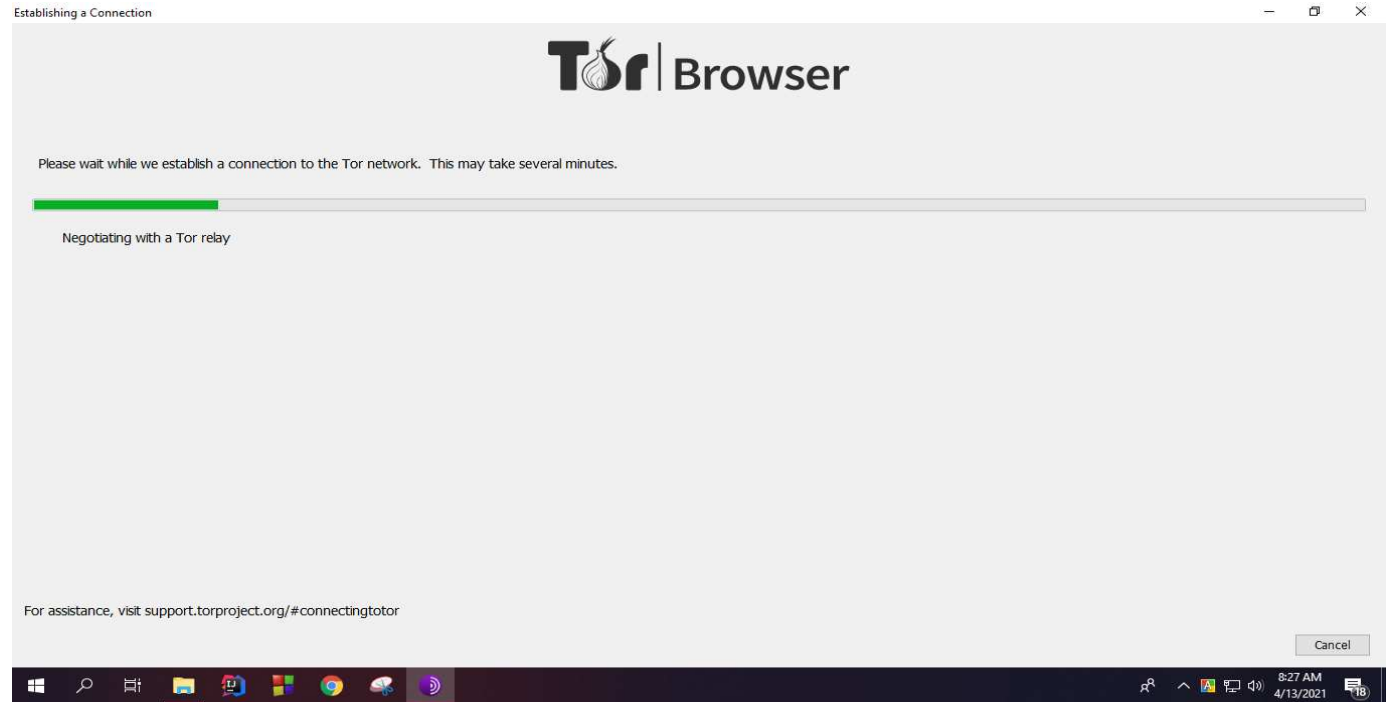
Byte order

☒ Little endian ☐ Big endian

☐ Show integers in hexadecimal base

An observation of surface web in Tor:

Establishing Tor:



System Information:

System Information

File Edit View Help

System Summary

- Hardware Resources
 - Components
 - Multimedia
 - CD-ROM
 - Sound Device
 - Display
 - Infrared
 - Input
 - Modem
 - Network
 - Ports
 - Storage
 - Printing
 - Problem Devices
 - USB
 - Software Environment
 - System Drivers
 - Environment Variables
 - Print Jobs
 - Network Connections
 - Running Tasks
 - Loaded Modules
 - Services
 - Program Groups
 - Startup Programs
 - OLE Registration
 - Windows Error Reporting

Full-screen Snip

Name	Path	Process ID	Priority	Min Worki...	Max Work...	Start Time	Version	Size
googlecrashhand...	Not Available	14176	4	Not Avail...	Not Avail...	4/12/2021 8:41 A...	Not Available	Not Av...
knagent.exe	Not Available	14204	8	Not Avail...	Not Avail...	4/12/2021 8:41 A...	Not Available	Not Av...
googlecrashhand...	Not Available	14212	4	Not Avail...	Not Avail...	4/12/2021 8:41 A...	Not Available	Not Av...
sgmbroker.exe	Not Available	6648	8	Not Avail...	Not Avail...	4/12/2021 8:41 A...	Not Available	Not Av...
svchost.exe	Not Available	112	8	Not Avail...	Not Avail...	4/12/2021 8:42 A...	Not Available	Not Av...
svchost.exe	Not Available	5072	8	Not Avail...	Not Avail...	4/12/2021 8:44 A...	Not Available	Not Av...
wmiprvse.exe	Not Available	9564	8	Not Avail...	Not Avail...	4/12/2021 8:46 A...	Not Available	Not Av...
mmpeng.exe	Not Available	12696	8	Not Avail...	Not Avail...	4/12/2021 8:50 A...	Not Available	Not Av...
nissrv.exe	Not Available	13252	8	Not Avail...	Not Avail...	4/12/2021 8:50 A...	Not Available	Not Av...
svchost.exe	Not Available	5920	8	Not Avail...	Not Avail...	4/12/2021 8:54 A...	Not Available	Not Av...
svchost.exe	Not Available	5336	8	Not Avail...	Not Avail...	4/12/2021 8:54 A...	Not Available	Not Av...
svchost.exe	Not Available	4876	8	Not Avail...	Not Avail...	4/12/2021 8:54 A...	Not Available	Not Av...
svchost.exe	Not Available	3552	8	Not Avail...	Not Avail...	4/12/2021 8:54 A...	Not Available	Not Av...
wuauclt.exe	Not Available	11928	8	Not Avail...	Not Avail...	4/12/2021 9:21 A...	Not Available	Not Av...
windowsupdateb...	Not Available	6612	8	Not Avail...	Not Avail...	4/12/2021 9:32 A...	Not Available	Not Av...
setuphost.exe	Not Available	5700	6	Not Avail...	Not Avail...	4/12/2021 9:32 A...	Not Available	Not Av...
trustedinstaller.exe	Not Available	764	8	Not Avail...	Not Avail...	4/12/2021 10:01 ...	Not Available	Not Av...
tiworker.exe	Not Available	9972	8	Not Avail...	Not Avail...	4/12/2021 10:01 ...	Not Available	Not Av...
svchost.exe	Not Available	3868	8	Not Avail...	Not Avail...	4/12/2021 10:06 ...	Not Available	Not Av...
svchost.exe	Not Available	1244	8	Not Avail...	Not Avail...	4/12/2021 10:06 ...	Not Available	Not Av...
svchost.exe	Not Available	14600	8	Not Avail...	Not Avail...	4/12/2021 10:18 ...	Not Available	Not Av...
vds.exe	Not Available	368	8	Not Avail...	Not Avail...	4/12/2021 10:21 ...	Not Available	Not Av...
wimserv.exe	Not Available	11576	6	Not Avail...	Not Avail...	4/12/2021 10:22 ...	Not Available	Not Av...
audiodg.exe	Not Available	9980	8	Not Avail...	Not Avail...	4/12/2021 10:30 ...	Not Available	Not Av...
dismhost.exe	Not Available	3368	6	Not Avail...	Not Avail...	4/12/2021 10:33 ...	Not Available	Not Av...
searchprotocolho...	Not Available	10636	4	Not Avail...	Not Avail...	4/12/2021 10:34 ...	Not Available	Not Av...
regedit.exe	Not Available	9832	8	Not Avail...	Not Avail...	4/12/2021 10:34 ...	Not Available	Not Av...
tor.exe	c:\users\user\desktop\tor bro...	14656	8	200	1380	4/12/2021 10:38 ...	Not Available	4.35 M...
searchfilterhost.exe	Not Available	12068	4	Not Avail...	Not Avail...	4/12/2021 10:39 ...	Not Available	Not Av...
wmiprvse.exe	Not Available	12008	8	Not Avail...	Not Avail...	4/12/2021 10:40 ...	Not Available	Not Av...

Tor State File:

state - Notepad

File Edit Format View Help

```
# Tor state file last generated on 2021-04-12 04:30:17 local time
# Other times below are in UTC
# You *do not* need to edit this file.
```

```
username: Md. Anisur Rahman
computer name: lab7pc14
```

Dormant 0

```
Guard in=default rsa_id=DA4B488C2826DFBBD04D635DA1E71A2BA5B20747 nickname=idefix samp
Guard in=default rsa_id=107E330E8FDBB06108BD4A2BB50C6907758BC204 nickname=Unnamed sar
Guard in=default rsa_id=EE556626236B477A40770AACDE5BB140006EFB4D nickname=sqrrm samp.
Guard in=default rsa_id=C83B6F75B8E6623AAB89EC66701CE02B5A4CA296 nickname=x23tor70 si
Guard in=default rsa_id=1FDF4D0660A7497222C3BA24FEEA316244093CD7 nickname=strunt samp
Guard in=default rsa_id=7534F56553F2E1F4E4F0BC8FA443E3A0E29A5A14 nickname=Unnamed sar
Guard in=default rsa_id=4561FC085C3F3A7271FE960317F02DCD1E9C1188 nickname=chonk samp.
Guard in=default rsa_id=5C8B811887778DCF705F3D39F19E40A21889451F nickname=t4cc0reTor:
Guard in=default rsa_id=1C0736CF3744A3B87C2D2269B8BD3388C7E60552 nickname=FreedomFri
Guard in=default rsa_id=4856C97DC4F2271BC896DF9CABD217EE2D869D68 nickname=mordoc samp
Guard in=default rsa_id=E0023AC14180112A2FFF00A84C6049862BB3E6C3 nickname=DerrickJen:
Guard in=default rsa_id=A98ADD972045D3CCAEE65C788C3F175BAEA3E324 nickname=2Contribut
Guard in=default rsa_id=36091A3FFC62BBC242A756F0CD7439E1F2458726 nickname=bsdtore01 :
Guard in=default rsa_id=D4420F438BD8A5BBE3F555EC3537E10AD1363FAE nickname=Unnamed sar
Guard in=default rsa_id=083FE4D2A92D7D5E21A23C0E7878D90085DE0B3 nickname=Unnamed sar
```


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

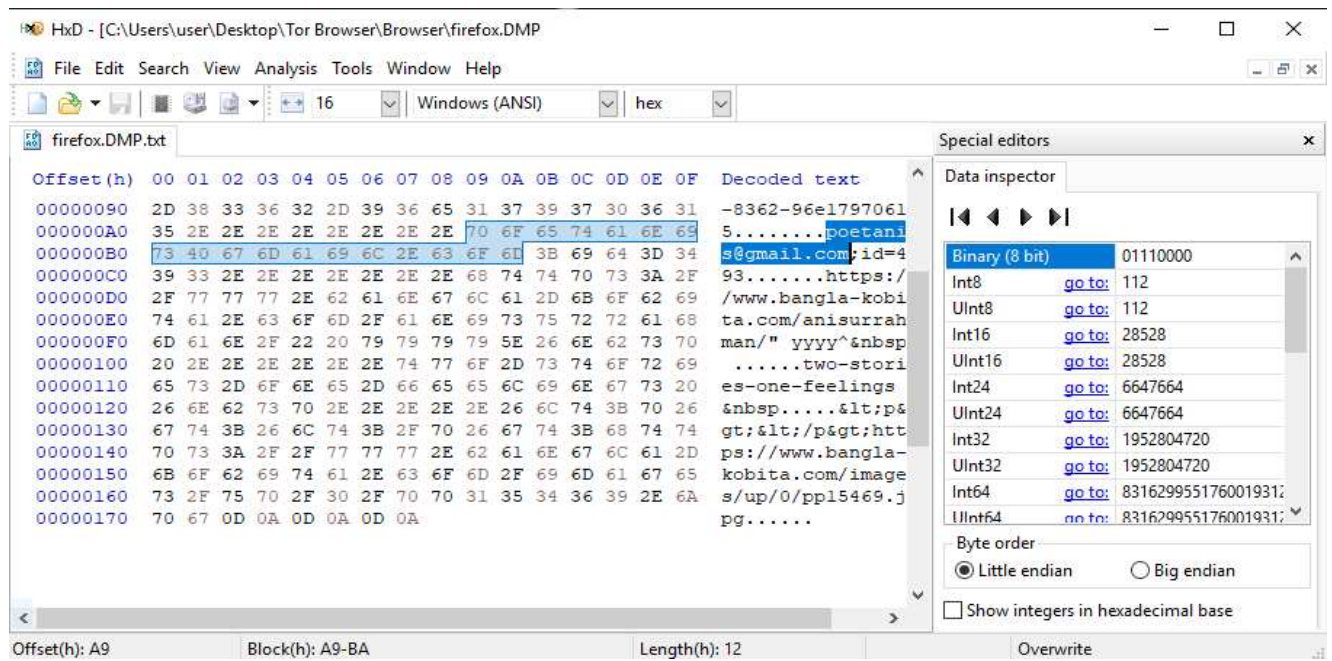
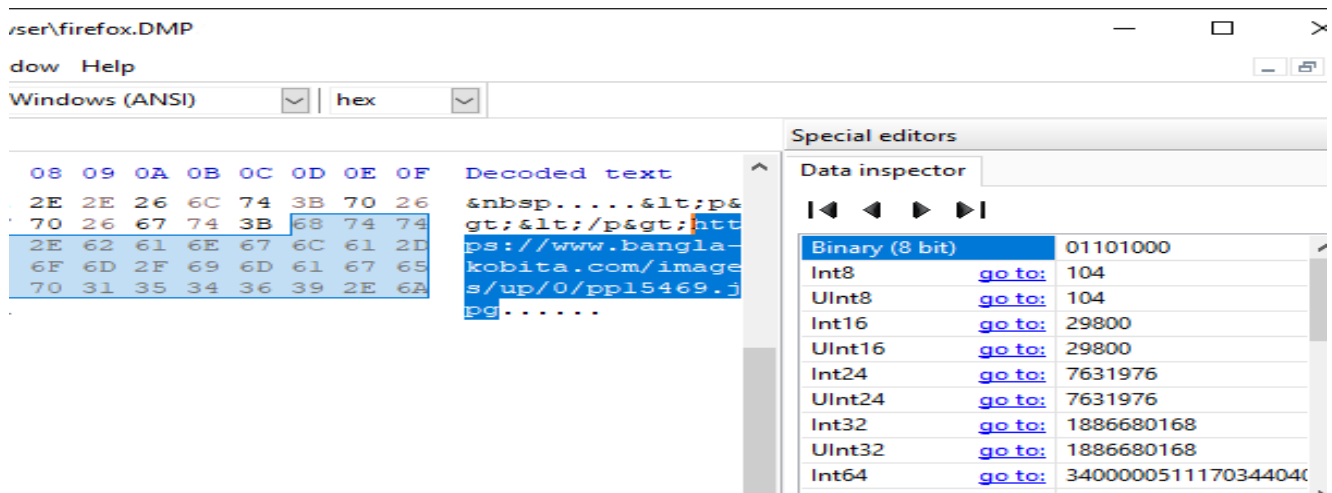


Image Extraction:



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]

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

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:

SYSTOOLS® SOFTWARE

SysTools SQLite Database Recovery
TOOL TO REPAIR CORRUPT SQLITE DATABASE FILE(S)

Open Export Close About Us Order Help Exit

places.sqlite

Tables

- moz_places
- moz_historyvisits
- moz_inputhistory
- moz_hosts
- moz_bookmarks
- moz_bookmarks_roots
- moz_keywords
- sqlite_sequence
- moz_favicons
- moz_anno_attributes
- moz_ennos
- moz_items_annos
- sqlite_stat1

Views

Triggers

TOTAL COUNT(27)

id	url
14	place:folder=UNFILED_BOOKMARKS
15	http://www.dropbox.com/
16	https://www.dropbox.com/
17	http://www.google.com/
18	http://www.google.co.in/?gfe_rd=cr&ei=KBnkVbjeHrLG8Ae725_QCA
19	https://www.google.co.in/?gfe_rd=cr&ei=KBnkVbjeHrLG8Ae725_QCA&gws_rd=ssl
20	https://www.google.co.in/?gfe_rd=cr&ei=KBnkVbjeHrLG8Ae725_QCA&gws_rd=ssl
21	https://www.google.com/search?q=nice+day&ie=utf-8&oe=utf-8
22	https://www.google.co.in/search?q=nice+day&ie=utf-8&oe=utf-8&gws_rd=cr&ei=R
23	https://www.google.co.in/search?q=nice+day&ie=utf-8&oe=utf-8&gws_rd=cr&ei=R
24	https://www.google.co.in/search?q=peacock&biw=1366&bih=657&source=lnms&tb
25	https://www.google.co.in/search?q=peacock&biw=1366&bih=657&source=lnms&tb
26	http://www.hdwallpapersnew.net/wp-content/uploads/2014/08/peacock-best-photo
27	http://www.softpedia.com/

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]*