Forensic Science International 299 (2019) 59–73

Contents lists available at ScienceDirect

Forensic Science International

journal homepage: www.elsevier.com/locate/forsciint

Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web

Abid Khan Jadoon, Waseem Iqbal, Muhammad Faisal Amjad, Hammad Afzal, Yawar Abbas Bangash

Department of Information Security, National University of Sciences and Technology (NUST), Islamabad 46000, Pakistan

ARTICLE INFO

Article history:
Received 24 November 2018
Received in revised form 15 March 2019
Accepted 18 March 2019
Available online 26 March 2019

Keywords:
Web browser forensics
Private BROWSING
Tor
Onion routing
Anonymity

ABSTRACT

Web browsers are among the most commonly used applications to access the web from any platform nowadays. With recent digital incidents involving breach of data, users are becoming more cognizant of the threat posed by malicious actors having access to personal data as well as vulnerable applications which may compromise their data. For this very reason, users are being offered privacy preserving solutions for trust maturity. The onion router (Tor) browser is one such application which not only ensures the privacy preservation goals but also provides promising anonymity. Due to this feature, majority of the users use Tor browser for normal use as well as malign activities. In order to validate the claims of Tor browser and help digital forensic investigators and researchers, we created different scenarios to forensically analyze the Tor browser privacy and anonymity. As a result of the findings, it can be concluded that the Tor browser leaves plethora of sensitive digital artifacts on host machine, which can be further used to compromise user data.

© 2019 Elsevier B.V. All rights reserved.

1. Introduction

Anonymity and privacy are two main elements to protect freedom of speech. Goal of anonymity is to protect all the information which can reveal real identity of user information like real name, location, IP address etc. The goal of privacy is to make sure that any organization or entity does not collect or store any personal or private information like user browser history, location information, account details etc without user's knowledge. Currently Tor project is working with the objective to protect user anonymity and privacy over the internet.

Tor project was initiated in 1995 by US Naval Research Laboratories [24]. The main goal of their project was to separate identification information from routing and to design an anonymous communication network for military communication. After public disclosure, it was deeply studied and extensive research has been carried out leading to different revisions of the project such as [47,23,46,14,51]. According to the latest report published by Tor metrics [50], there are more than 2.5 million active Tor users with 6000+ nodes carrying their traffic and providing 25.5 Gbps bandwidth for the Tor network. Tor browser is the easiest way to connect to the Tor overlay network to route users' traffic. Tor browser is a modified version of Mozilla Firefox with some extra features for anonymity and privacy. Some of these features are the *Tor launcher, Tor button, no script and HTTPS-Everywhere*. By default, browsing is configured for private mode with the option to clear browsing activity and its related artifacts such as cookies and other browsing related data after closing of the browser.

According to a study [2], local DNS resolver and swap partition used for memory swapping are two big challenges to private browsing. Private browsing may leave many artifacts on host machine [39,43] and it does not provide the level of privacy claimed by its vendors [31,8]. The research showed that artifacts can be recovered from memory if the browser which is used for private browsing is open at the time of acquisition [21]. In other cases, many useful artifacts were recovered from paged memory even after the browsing session was closed [45,16]. [19] shows that there is a lack of awareness and many misconceptions about private browsing. Current Browser forensic tools only target specific browsers or specific information files. In cases where a suspect used many browsers for criminal activities, these tools are not so effective because the evidence is spread across many files and locations so analyzing a single browser or specific information file does not provide all the artifacts about user activity. [38] proposed a new methodology to overcome these limitations and introduced a new tool (web browser forensic analyzer) which integrates forensic analysis of different browser.

E-mail addresses: abidjadoon.msis13@students.mcs.edu.pk (A.K. Jadoon), waseem.iqbal@mcs.edu.pk (W. Iqbal), faisal@nust.edu.pk (M.F. Amjad), hammad.afzal@mcs.edu.pk (H. Afzal), yawar@mcs.edu.pk (Y.A. Bangash).

https://doi.org/10.1016/j.forsciint.2019.03.030
0379-0738/© 2019 Elsevier B.V. All rights reserved.

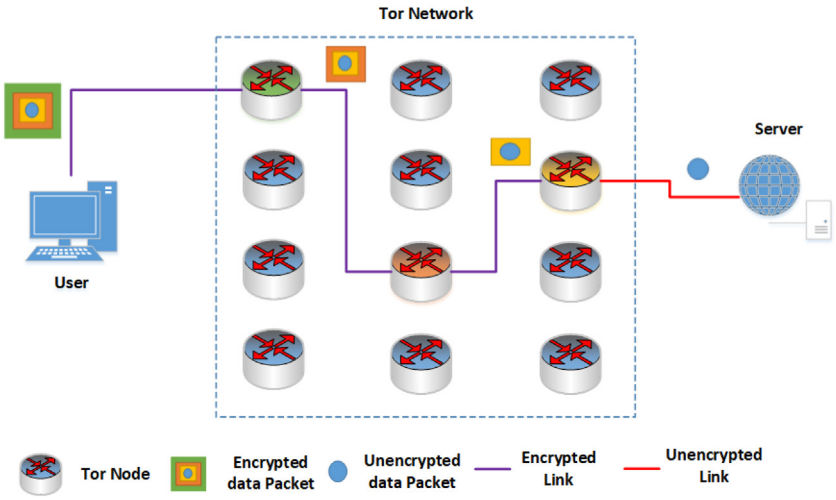

Fig. 1. Onion routing.

There have been studies with good analysis of Tor Browser [11,3,57], however, there are still some areas which are not comprehensively addressed. For instance, analysis of memory and hard disk for network[1] and browsing artifacts of Tor browser on Windows 8.1 is not performed. The presented research in this paper focuses on analyzing the Windows 8.1 memory and hard disk to recover all those artifacts which were not addressed in previous researches.

Rest of the paper is organized as follows: Introduction to Tor network and related research work in area of privacy and anonymity for browsing is discussed in Sections 2 and 3. followed by proposed methodology and experimental setup part. Whereas the results obtained from these experiments are discussed in Section 5. Comparison with existing research is done in Section 6 of the paper. Last part concludes the paper along with a brief discussion and future work.

2. Tor working methodology

Tor consists of a global overlay network of relays which helps in the achievement of privacy and anonymity for user Internet traffic. For every communication, the Tor network creates a virtual circuit comprising a minimum of three successive, randomly selected relays. Information about the relays is downloaded by the Tor client at source machine from a directory server. Encryption keys are exchanged with the selected relays using the Diffie–Hellman key exchange protocol. At the source node, the data packets are encrypted multiple times, once for every relay node using that relay's encryption key before forwarding the packets towards their destination. Therefore, the outer most layer of encryption is decrypted by the entry node whereas the inner most layer of encryption is meant for the exit node to decrypt. Every relay node decrypts the received packet using its own decryption key in order to discover the next hop address for the received packet. In this manner, every Tor node has the knowledge about relay nodes only one hop away from itself. At the exit node, the inner-most layer of encryption is decrypted and the un-encrypted data packet is forwarded towards its final destination. Thus, the privacy of users' data is preserved until last hop. In case of https over Tor network, data between last hop and destination is also encrypted. Furthermore, Tor browser change its path after every ten minute to ensure users anonymity. Routing of data through Tor network is depicted in Fig. 1.

Anonymity on the other hand, is provided by Tor network by ensuring that even the relay nodes of the overlay have knowledge about the predecessor and successor relay nodes in the entire virtual circuit. To further enhance the anonymity property, every new virtual circuit is established using a newly selected set of relay nodes.

3. Related work

In today's era of surveillance, online anonymity is very important, especially in the context of freedom of expression [15]. One of the earliest researches in the domain of anonymity was presented in [7] in which the mix-net was proposed. This work was later used to design many other anonymity solutions. Mix-net uses layers of encryption and series of mixes over the network. The first practical anonymity service provider was Remailer [22][29]. Similarly, the work in [26] demonstrated a remailer which replaced users' real ID with anonymous ID in messages using a mapping database. In this service, anonymity for users was better than the anonymity for service provider. This service was shut down in 1996 due to legal problems with the church of Scientology [27].

Cypherpunk remailer [30], also known as type I remailer, was based on Chaums mix-net [7]. It used public key cryptography for message encryption [42]. Mix master [35] was an upgraded version of Cypherpunk which used message splitting and padding techniques. This remailer was good in providing online anonymity but was vulnerable to tagging and blending attacks which were later patched in Mixminion remailer [10].

Later systems such as The Eternity service [4], Free Heaven [13] and Freenet [9] implemented the idea of online anonymous storage. The eternity service provided anonymous storage of a file for a long period of time [13]. It used Rabin's information dispersal Algorithm (IDA) [40] for dividing file into many parts before sharing with other servers. Another system, known as Freenet, was a peer to peer (P2P) network which offered storage and retrieval of data anonymously. Other systems such as Crowds [41] and Publius [56] provided services of anonymous web transactions and message publishing on World Wide Web (WWW). Tarzan [18] provided anonymity during web browsing. These systems provided adequate anonymity but at the same time, suffered from high latency.

In 1995, US Naval research laboratory started a project to design anonymous network for military communication. This project was named as Onion routing [47,23]. It was a low latency network and used layer of encryption and onion network for anonymity. Later, the second

[1] Tor Relays detail, Public keys.

generation [14] of this project was named TOR (The Onion Router). Tor Browser is free software made by Tor project [51] to access Tor network. It routes user browser traffic through Tor network. For ensuring users privacy, it only runs in private browsing mode. It provides a high level of anonymity over the Internet. Due to the level of anonymity offered by this browser, soon it became a favorite tool of cyber criminals. Backtracking Tor user over the internet is very challenging and therefore, network and disk forensics is extremely important in cases where Tor browser is used for illegal activities [17].

There is a research gap in the area of Tor memory forensics. [12] highlights this issue and proposed a theoretical framework for Tor browser memory analysis. In [44], the authors showed many security issues present in this browser but these issues were resolved in later versions. Most artifacts from memory can be recovered when Tor browser is open during acquisition [3]. Authors of [11] presented a detailed analysis of Tor browser. They analyzed Windows 7 for pre- and post-Tor execution artifacts. Authors of [57] have shown the recovery of many artifacts of Tor browser from Windows 10 memory using volatility framework.

4. Proposed methodology

Objective of this research was to collect all the Tor artifacts from registry, memory and storage of host machine. For detail analysis different scenarios were also considered. In registry analysis artifacts add or removed during installation and uninstallation were collected. While for memory and storage analysis scenarios of browser open and closed were considered.

The overall methodology adopted in this work is illustrated in Fig. 2. An extensive literature review about the Tor paradigm is performed to define the objectives of research. Gap analysis is carried out with previous researches to further elaborate the objectives. A real environment is simulated for the proof of concept. Once the results are acquired, they are analyzed in detail and compared with existing works.

4.1. Experimental setup

In order to work in clean environment, a shredded storage is utilized for operating system installation and data storage. In order to analyze the registry, memory and storage artifacts, virtual environment is used. A list of tools used during this investigation are listed as:

- MiniTool Partition Wizard Free 9.1 [34]
- VMware Workstation 12 Pro (Version 12.5.7) [53]
- Window 8.1 (64 bit) [33]
- Tor Browser 7.0.2 (32 bit) [48]
- Google Chrome [25]
- Regshot 1.9.0 [6]
- Volatility 2.6 Windows Standalone Executable (x64) [54]
- Hex workshop v6.7 (64 bit) [5]
- AccessData FTK Imager v 4.1.1.1 [1]
- Magnet AXIOM v 1.2.0.6464 (Trial Version) [32]
- Bulk extractor 1.6.0 [20]

4.2. Browsing activity

In order to perform forensic analysis of the Tor browser, we simulate all the activities that a normal user performs using the browser. Two Gmail, one Yahoo mail, one Instagram, two Twitter, three Facebook accounts (including one account for Facebook onion website) and two Skype accounts are created. Some random contents are posted on these accounts before the start of our investigation. From these accounts one Gmail, one Facebook, one twitter and one Skype are used on Google Chrome for exchanging emails and messages with the rest of the accounts used for Tor browser. Details about all of the accounts used and activities performed using Tor browser are given in Table 1. After completing all these activities, all downloaded images and torrent files (.torrent files) are deleted from the system as well as

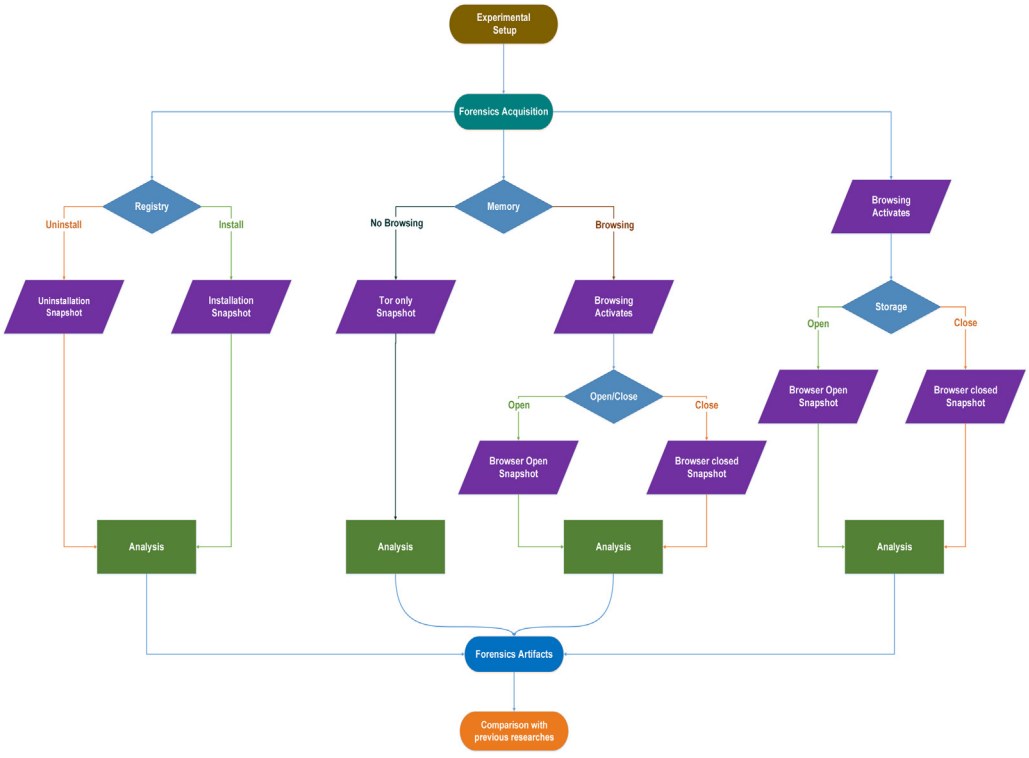

Fig. 2. The flowchart of research methodology.

Table 1
A summary of user browsing activities for simulation.

Website	Activities	Accounts used on Tor	Accounts used on Chrome
Search engine www.duckduckgo.com	• Browsing website • Key word search • Download/save images	–	–
Gmail www.accounts.google.com	• Browsing website • Login • Send emails to Gmail (for Chrome user) and Yahoo (for Tor user) • Receive emails from Gmail (for Chrome user) and Yahoo (for Tor user) • Read emails • Send email attachments • Receive email attachments • Online view MS Word &pdf document attachments	tor_user1@gmail.com	chrome_user1@gmail.com Exchange emails and attachments with Tor user Gmail account
Google Drive www.drive.google.com	• Browsing website • Save word &pdf email attachments to drive • view/read these attachments from drive online	tor_user1@gmail.com	Same account as used above Sent and receive attachments
Yahoo mail www.login.yahoo.com	• Browsing website • login • Sent mails to chrome user Gmail and Tor user Gmail accounts • Receive mails from chrome and Tor user Gmail accounts • Read emails • Sent email attachments • Receive email attachments • Download pdf attachment	tor_user2@yahoo.com	
tor_user1@gmail.com	Same account as used above Same activities as done with Gmail account		
Twitter www.twitter.com	• Browsing website • login • Tweet • Like tweet • Retweet • Comment • Visit accounts • follow • Chat with chrome user twitter account	user3_tor @user3_tor	user3_chrome @user3_chrome
Instagram www.instagram.com	• Browsing website • login • Visit accounts • Follow • Like pictures • comment	user4_tor @user4_tor	–
Facebook www.facebook.com	• Browsing website • login • like pages and posts • share posts • comments on posts • visit pages and user profiles • search accounts • receive friend request • chat with chrome user Facebook account	user5_tor	user5_chrome
Onion Facebook facebookcorewwwi.onion	Same as done above in Facebook	user6_tor	Same account as used above
Skype www.skype.com login.skype.com	• Browsing website • login • search accounts • chat with skype user on chrome	user7_tor	user7_chrome
YouTube www.youtube.com	• Browsing website • Search keyword/videos • Watch videos	–	–
Google maps maps.google.com	• Browsing website • Search places	–	–
Torrents academictorrents.com	• Browsing website • magnet links [a] • download.torrent file	_	_
Research papers www.garykessler.net www.blackhat.com http://icitech.org www.clarecomputer.com	• Browsing websites • open pdf research paper online • view/read 2 Anti-forensics papers &3 Ransomware papers	–	–
Mail2Tor email accounts mail2tor2zyjdctd.onion	• Browsing website • Create email account	Darkweb_user@mail2tor.com	–

[a] Downloading torrents using magnetic link did not work in Tor browser.

the recycle bin before taking the snapshots of the virtual machines.

Best effort has been made to cover all possible activities that can be performed using the Tor browser. Depending on the intention of user, similar activities can be performed by normal user for legitimate purpose or by a malicious user with some criminal intentions like cyberstalking, cyberbullying and sending hoax emails etc. Two such case studies where social media and email platforms on Tor browser were used for committing crime can be found here [36,37,52].

4.3. Data acquisition

Acquisition is done in three phases; Registry, Tor only memory, memory and storage. In each phase Tor is installed from external storage. After completion of each phase, system is reverted to clean state to ensure that no artifacts from previous phase remain on the system. Some concepts which are used hereafter in this paper are explained below:

- **Tor Only memory** Tor browser is installed and executed. Browser is connected to the Tor network. No browsing activity is performed during this slot. VMware snapshot is taken during this state of the system referred as the second snapshot.
- **Browser Open** After completing browsing activates given in Table 1, browser is remained open on last opened tab of last visited site. During this time, VMware snapshot is taken, referred as the third snapshot.
- **Browser closed** Subsequent to the "Browser Open" scenario, browser is closed and snapshot is recorded, referred as the fourth snapshot.

4.3.1. Registry acquisition

Registry acquisition is accomplished in three steps i.e. pre-installation, post-installation and post uninstallation. Snapshots are dumped to the external storage to ensure the host integrity.

4.3.2. Memory acquisition

Memory acquisition has been categorized into two parts i.e. Tor only and Tor browsing stage. In Tor browsing stage there exists two scenarios i.e. browser open and closed.

4.3.3. Storage acquisition

Similar to the memory acquisition, "Browser Open" and "Browser Closed" are considered. To ensure that all artifacts from storage are recovered "vmdk files" of host system, third and fourth snapshot are acquired.

5. Analysis and results

Forensics analysis is done in three phases. In first phase, registry snapshots are analyzed while memory and storage images are done in next two phases.

5.1. Registry analysis

Registry snapshots are acquired and then analyzed using Regshot tool. The analysis shows that this browser add three registry keys during installation. All these keys remain in registry after uninstallation which indicates that it does not clear its registry artifacts during uninstallation[2] [49]. It was also noticed that these keys are added in different order under different scenarios which are explained below.

- **Install and Run** In this scenario, the browser is installed with selecting the "Open browser automatically after installation". After installation, browser is automatically opened. The first two keys got added to registry. Third key got added when browser was run next time after closing.
- **Install only** In this scenario, the browser is installed without selecting the "Open browser automatically after installation". First key is added after installation is completed. Second and third keys are added when browser is opened.

These scenarios will be very helpful in cases where investigator are interested to know that whether user just installed the Tor browser or used it as well after installation. For further details, refer to Table 2.

5.2. Memory analysis

Memory analysis is performed in two phases. In first phase, "Tor browser only artifacts" are searched for, whereas in second phase, "browsing artifacts" are also searched.

5.2.1. Tor only artifacts

Software leaves many artifacts on host machine after installation. This part of research focuses on recovering all these artifacts which Tor browser leaves on host machine after installation and execution. Volatility framework is used for forensics analysis of acquired memory image. List of all recovered artifacts and commands used are given in Table 3. The explanation about all commands and recovered artifacts are shown here [55]. Analysis of memory for running processes shows that Tor browser has two processes in memory, Firefox.exe (pid = 3548) and tor.exe (pid = 3668). Using process ids of these two processes, other artifacts linked to them are also recovered. In version information artifacts, key words "firefox" and "tor.exe"' are used to locate version information of these two processes. For processes tree, process list and virtual addresses, dot diagrams are also generated. Results given in Table 3 can be downloaded from here.[3] A similar analysis is also performed in [57]. They used Tor browser v5 on Windows 10 for the analysis.

5.2.2. Browsing artifacts

In this phase, the artifacts about user browsing activities in memory are searched. As explained in Data Acquisition, third snapshot of VMware is taken for "Browser Open" scenario while forth was taken for "Browser Closed" scenario. Memory images (.vmem files) of these two VMware snapshots are analyzed for browsing artifacts. Bulk extractor and Hex workshop are used for analysis. Most of analysis is performed using Bulk extractor. String search is used in Bulk extractor to find links of user social media account profiles, visited profiles watched videos, keywords searched and other artifacts. These strings are taken from visited sites addresses, user names which are used during user browsing activities phase. All these artifacts can be found without using strings searches by just analyzing all the sites extracted by Bulk extractor, however, this method is time consuming as compared to string searches. For searching email text in memory, Hex workshops is used. Memory image is opened in Hex workshop and different strings searches are performed to find these emails. Strings from email text which are sent and received during user

[2] According to the Tor project website, uninstallation of Tor browser simply deletes Tor browser folder and browser shortcut from system as well as recycle bin.

[3] https://www.dropbox.com/sh/06pmf2jml4muur6/AABfzbRZ2pYIlKRcJ-K0itHmna?dl=0.

Table 2
Registry artifacts.

S. No.	Location of registry keys	Description
1	HKU\S-1-5-21-3610041324-1787688552-2397930110-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\SIGN.MEDIA=33C3D38 torbrowser-install-7.0.2_en-US.exe: 53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 38 3D 3C 03 B6 60 3C 03 01 00 00 00 00 00 00 00 00 00 00 01 06 00 01 00 00 97 5F D8 91 C9 9E CE 01 00 00 00 00 00 00 00 00	Registry key shows name of Tor browser setup file used for installation
2	HKU\S-1-5-21-3610041324-1787688552-2397930110-1001\Software\Microsoft \Internet Explorer\LowRegistry\Audio\PolicyConfig \PropertyStore\6ae17f4a_0\: "{2}.\\?\ hdaudio#func_01&ven_15ad&dev_1975 &subsys_15ad1975&rev_1001#{6994ad04-93ef-11d0-a3cc-00a0c9223196}\ elineouttopo/00010001| \Device\HarddiskVolume1\Users\Abid Jadoon\Desktop\Tor Browser\Browser\firefox.exe%b {00000000-0000-0000-0000-000000000000}"	Registry key shows Audio settings and location of firefox.exe file
3	HKU\S-1-5-21-3610041324-1787688552-2397930110-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\Abid Jadoon\Desktop\Tor Browser\Browser\firefox.exe: 53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 00 28 05 00 94 FA 05 00 01 00 00 00 00 00 00 00 00 00 03 06 00 01 00 00 97 5F D8 91 C9 9E CE 01 00 00 00 00 00 00 00 00	Registry key shows location of installed Tor browser and firefox.exe file. It also shows that Firefox.exe file is located inside Tor Browser folder.

Table 3
Tor only artifacts.

S. No.	Artifacts recovered	Commands used
1	Processes list	Pslist, psscan
2	Process Tree	pstree
3	Dynamic-link library (Dlls)	dlllist, ldrmodules
4	Dll Dump	dlldump
5	handles	handles
6	Security Identifiers	getsids
7	process privileges	privs
8	process's environment variables	envars
9	version information embedded in PE files	verinfo
10	process's executable Dump	procdump
11	Files dump	dumpfiles
12	virtual addresses	Vadinfo, vadwalk, vadtree
13	ETHREAD objects	thrdscan
15	network artifacts	netscan
16	registry key	printkey

activities part are used. These emails can also be found in memory without using string searches by viewing all strings present in memory from start to the end using hex workshop. But this method is very time consuming in cases of large memory images. All inbox emails including unread emails of Gmail and Yahoo accounts used with Tor browser are present in memory. Some of the emails found in memory image of third snapshot using string searches are shown in Fig. 3.

Using string "PUBLIC KEY" and "Relay=" public keys and other useful information can also be found about Tor relays used by Tor browser for routing its traffic. Other information include IP address, Ports, Bandwidth, Name and Fingerprint, Tor version used by this relay, date and time of user browser connection and status (entry or exit). Figs. 4 and 5 are screenshot of public keys and other information in memory image of third VMware snapshot. Same artifacts can also be found in **"cached-certs", "cached-microdesc-consensus", "cached-microdescs" and "cached-microdescs.new"** files present at **TorBrowser/Browser/TorBrowser/Data/Tor**. These files are analyzed in Hex Workshop as shown in A, B, C and D. These artifacts can be helpful for law enforcement agencies in case of backtracking a Tor user for any illegal activity by collecting artifacts from these relays regarding browsing activity of the user. All the artifacts found in both memory images were identical which shows that Tor browser does not clear user browsing history from memory while closing the application. Summary of all the artifacts found in memory about user browsing activities are listed in Table 4. Screenshots of some of these artifacts are given in Fig. 6 and . All these artifacts are found using bulk extractor except inbox messages of Gmail and yahoo mail which were found using Hex workshop.

5.3. Hard disk analysis

In this part, analysis of virtual storage is performed. Four VMDK files are analyzed which include two VMDK file (OS,snapshot) for "Browser Open" scenario while two for "Browser Closed" scenario. Both Snapshot VMDK files are converted to EnCase image file format before starting of analysis.

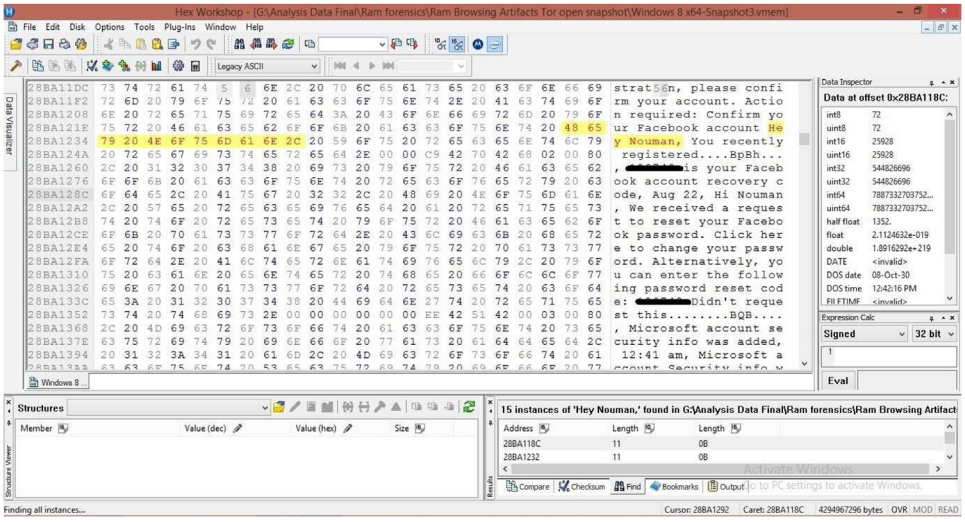

Fig. 3. Email text found in memory.

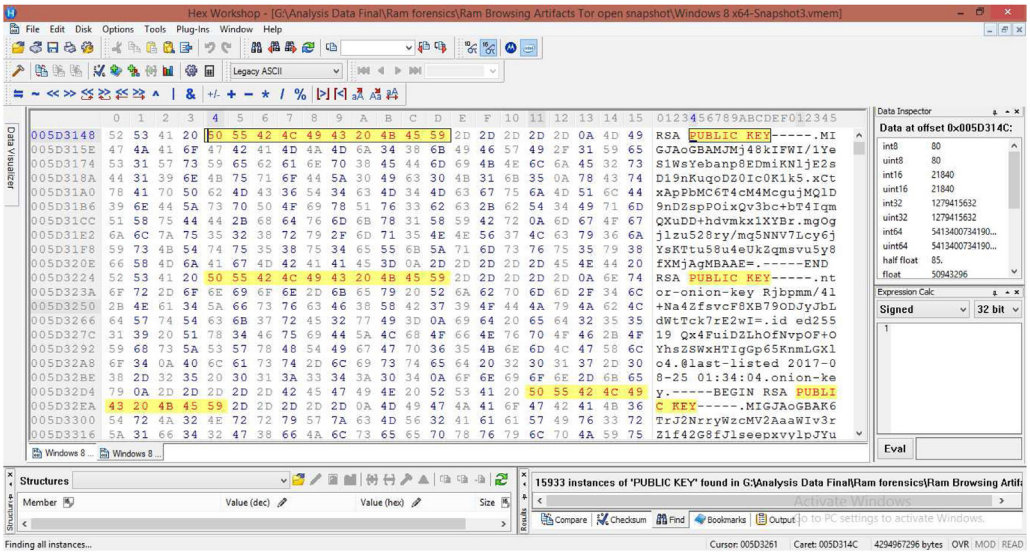

Fig. 4. Public keys of Tor relays in memory.

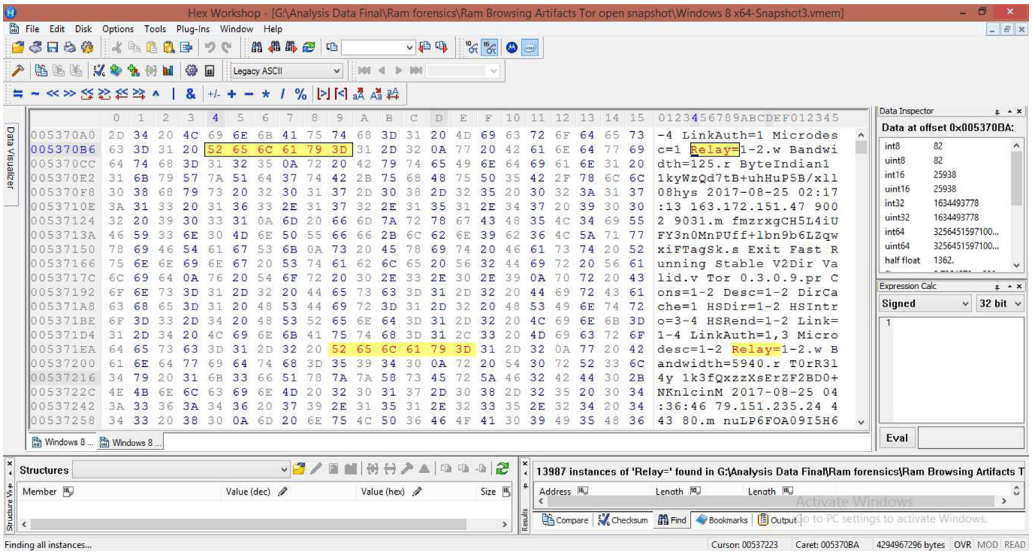

Fig. 5. Relays information present in memory.

5.3.1. Hard disk artifacts with open browser

Artifacts that are present in hard disk when browser is open were searched in this part of analysis. Both OS VMDK file and snapshot VMDK file of third snapshot were analyzed with Magnet Axiom [32]. Hex Workshop was used for searching registry artifacts present in these VMDK files. Magnet Axiom has support for OS VMDK file but no support for snapshot VMDK file. Using image conversion procedure adopted in [28] we use FTK imager to convert this VMDK file into EnCase Image File Format which is supported by Axiom. Using FTK imager MD5 and SHA1 hashes were computed and compared before and after conversion as shown in Appendix I to ensure integrity of converted snapshot VMDK files. MD5 and SHA1 hash were also computed for OS virtual hard disk file with FTK imager. No Tor browser artifacts were found on OS VMDK file. For registry artifacts this VMDK file is viewed in Hex Workshop and different strings searches were performed. Strings "firefox.exe%b" and "SIGN.MEDIA=33C3D38" were used in these searches. No registry artifacts were present in OS VMDK file. However many artifacts were recovered from analysis of converted snapshot VMDK file as shown in Table 5. Artifacts found by Magnet Axiom had all the download data. Downloaded images were show under media artifacts and downloaded torrent files were under peer to peer artifacts. Axiom also recovered many other images from OS internal application but none of them were from browsing activity except downloaded images. Tor browser icon was also present in recovered images which clearly indicate that Tor browser was installed on the system. No other instance was found under axiom OS artifacts Except location of firefox.exe as shown in Appendix H. All registry artifacts were present.[4]

5.3.2. Artifacts – hard disk with closed browser

In this part of analysis, all those Tor browser artifacts were searched which were present in hard disk after browser was closed. All steps performed in previous part of hard disk analysis for snapshot VMDK file, MD5 and SHA1 hashes computing for both converted snapshot VMDK file and OS VMDK file were also

[4] This is "Install and Run" scenario so only key 1 and 2 will be present as explained in Section 5.1.

Table 4
Browsing artifacts in memory.

S. No.	Application/data searched	Artifacts found while Tor browser was open	Artifacts found while Tor browser was closed	Artifacts found	Artifacts not found
1	Search Engine/ DuckDuckgo	Yes	Yes	All links visited by user including: • Links of viewed and download images • All searched key words	• Bulk extractor was unable to recover download images
2	Gmail	–	–	All email addresses of senders and receivers as shown in Appendix E • Inbox messages including unread messages • Links of all email attachment files	• Sent Messages • Attachment files(word and Pdf)
3	Google Drive	–	–	All Google drive links visited by user including: • Links of online viewed/read drive documents	Nil
4	Yahoo mail	–	–	• Same Artifacts as Gmail	• Same Artifacts Gmail
5	Twitter	–	–	All Twitter links visited by user including: • User profile link as shown in Fig. 6 • Profile links of viewed/visited twitter accounts • Links of all those twitter accounts which were visited/viewed before following them	• Liked tweets • Shared tweets • Comments • Chat • User Profile picture • Links of all those followed twitter accounts which were followed without visiting/viewing them
6	Instagram	–	–	All Instagram links visited by user including including: • User profile link as shown in Appendix F • Profile links of viewed/visited instagram accounts • Links of all those instagram accounts which were visited/viewed before following them	• Liked pictures • Comments • Chat • User Profile picture • Links of all those followed instagram accounts which were followed without visiting/viewing them
7	Facebook and Facebook Onion	–	–	All Facebook and Facebook Onion links visited by user including: • User profile link as shown in Appendix G • Profile links of viewed/visited facebook accounts and pages • keyword searched • Links of all those facebook accounts and pages which were visited/viewed before liking them[a]	• Liked posts • Comments • Shared posts • Chat • User Profile picture
8	Skype	–	–	• All Skype links visited by user which clearly shows that Skype account has been used by user on this browser[b]	• Chat • Contacts • User Profile picture
9	YouTube	–	–	All YouTube links visited by user including links of: • Keyword searched • Watched videos	Nil
10	Google Maps	–	–	All Google maps links visited by user including links of: • Keyword searched • Links of viewed location	Nil
11	Torrent/ Academictorrent site	–	–	All links of Academictorrents website visited by user including: • Links of viewed torrents • Magnetic links of downloaded torrent files	• Bulk Extractor was unable to recover downloaded torrent files
12	Research papers	–	–	Links of all research paper websites visited by user including: • Links of online viewed/read pdf research papers	Nil
13	Mail2tor	–	–	• All links of Mail2tor website visited by user • Email address of account created by user	Nil

[a] No such pages were liked which were not visited/viewed by user.
[b] Unlike Facebook and Twitter, Skype links does not provide any information about user's profile and keywords searched.

repeated in this section. For searching artifacts same tools and methods were used as in previous section of hard disk analysis. No Tor browser artifacts were present in OS VMDK file. In converted snapshot VMDK file we found some artifacts which are given in Table 5. Registry key[7] and location of firefox.exe were the only artifacts that were present in converted snapshot VMDK file.

6. Comparison with existing research

A lot of research has been done on security and privacy of Tor network but there is a research gap in the area of Tor Forensics. Limited research has been done in this field. We found only three researches in which forensics analysis of Tor browser was performed. Detail comparison between existing research and our experimentation is shown in Table 6.

Winkler et al. [11] performed analysis of Tor Browser on window 7. They considered three case scenarios namely Pre-tor,Tor active and Post-tor. They performed memory analysis in all these scenarios for finding Tor artifacts. Their research lacked in analysis of hard disk and Tor only artifacts in memory as shown in Table 6. These two areas are very important for forensics investigators. Many useful artifacts can be recovered from these areas as can be seen from our results. Another problem with this research was that it was done on Windows 7 which is old operating system and most of current user are shifted to window 8 or 10.

Atta et al. [3] also done similar analysis of Tor browser on Window 7. They analyzed system memory for Tor artifacts. There main focus was recovering artifacts about user browsing activities from memory. They consider only a limited set of browsing activities and these activities does not reflect browsing habits of a

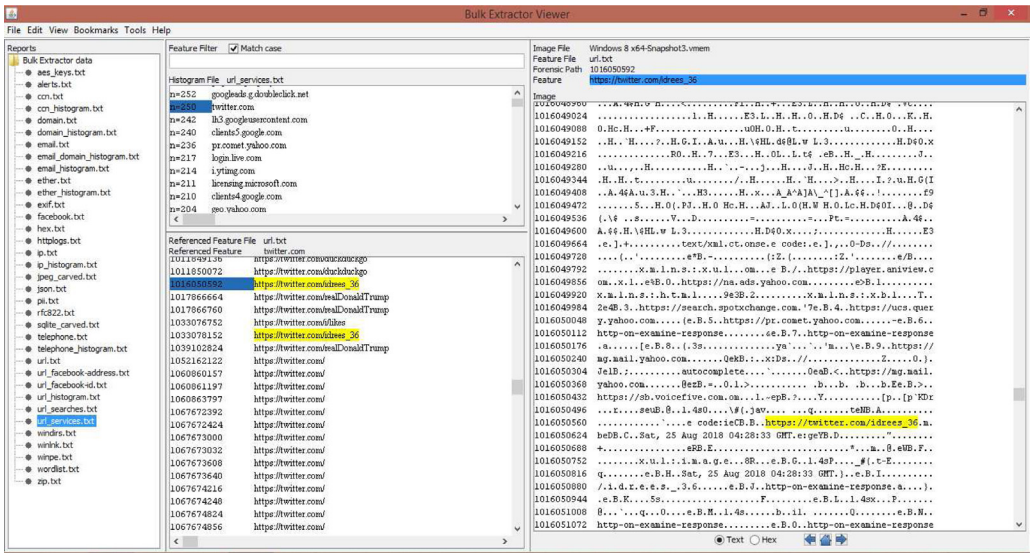

Fig. 6. Twitter artifacts recovered by bulk extractor from memory images.

Table 5
Summery of Tor browser hard disk artifacts.

Instance	Open Tor browser		Closed Tor browser	
	OS Vmdk File	Converted Snapshot Vmdk File	OS Vmdk File	Converted Snapshot Vmdk File
Browsing	• No artifacts	• No artifacts found	• No artifacts	• No artifacts found
Pictures	–	• Only Tor browser icon was present in recovered pictures • No picture and videos were present from browsing activities	–	• No artifacts found
Downloads	–	All downloads were present • Downloaded pictures • Downloaded torrent files(.torrent files)	–	• No artifacts found
Operating system	–	• Only location of firefox.exe was present • No other artifacts of Tor browser were present	–	• Only location of firefox.exe was present • No other artifacts of Tor browser were present
Registry artifacts	–	• Two registry keys 1 and 2 were present and third key was missing	–	• Two registry keys key 1 and key 2 were present and third key was missing

Table 6
Tor browser analysis and artifacts comparison.

Authors	Registry artifacts		Memory artifacts		Hard disk artifacts		Network artifacts
	Tor browser installation	Tor browser un-installation	Tor only	Browsing	Browser open	Browser closed	
Our work	✓	✓	✓	✓	✓	✓	×
Winkler et al. [11]	✓	✓	×	✓	×	×	✓
Atta et al. [3]	×	×	×	✓	×	×	×
Aron et al. [57]	✓	×	✓	×	✓	×	×

normal user.[5] Three important areas hard disk, registry and Tor only artifacts in memory were missing in their research. This paper also claim that Tor browser clear all its remnants after closing which is not true as can be seen from our analysis results.

Aron et al. [57] demonstrates the forensic analysis of Tor browser on Windows 10. Registry artifacts added during installation and Tor only artifacts in memory are analyzed. Authors used latest version of Windows and Tor browser for this research. However, authors did not analyze registry for artifacts that remain after uninstallation of Tor browser. Another missing part in this research was, no browsing activities were performed and no artifacts related to browsing activities were searched in system memory and hard disk.

In this research, all possible artifacts are recovered from host system. We also consider different test scenarios which a forensic investigator can face during investigation. Recovering relays information from memory and hard disk is very important. These information will be very helpful in backtracking Tor user. Specially information of exit node is most important because at exit node all data is in plain text. If any user or attacker share any personal information then by analyzing exit node and extracting those information will help law enforcement agencies to identify him. None of previous research recover relay information artifacts from memory and hard disk.

Browsing artifacts are very important because from these artifacts we can find out all the browsing activities perform by user.

[5] Use of social media, email etc. were not considered in these activities.

Our research is the only research that recover those artifacts from window 8.1 memory. In previous researches they only recover similar artifacts from window 7 memory but none of them recover it from window 8.1 or 10 memory.

Our focus was to use such tools which is either open source or available as demo version so that anyone can reproduce our results without purchasing commercial tools. This research will also be very help for researchers and investigator with limited budget.

7. Discussion

Censorship and surveillance are two biggest challenges to freedom of expression. To overcome these challenges more and more sites are shifting to onion domain so it is expected that in near future Tor browser will be among top five browsers in cyber market. Although this browser provide privacy but not as much as it can be seen from our results, especially from memory analysis results, that it leave many artifacts in memory even after closing the application. This browser is not perfect but still with all these weaknesses, it is good enough because it provides both privacy and anonymity at the same time. It offers features like tor button, no script and HTTPS-Everywhere which further improve its anonymity and privacy.

We can learn many things about user browsing activities from the memory analysis results. These results can be helpful for Law Enforcement Agencies in cases where a Tor browser user is under investigation. It will also be helpful for Tor browser developer to improve security and privacy of their browser in upcoming versions. Forensics tools are available for all major browser but there are no specific tools for this browser. Digital Forensics industry need to develop tool for this browser. Our research will be very helpful in designing and developing these tools. Backtracking Tor user on network is very challenges. Network artifacts we found in memory as shown in Fig. 5 will be very helpful for security and law enforcement agencies in cases were backtracking of Tor user is required.

8. Conclusions and future work

This paper presents a forensics analysis of Tor browser on Windows 8.1. We analyzed system registry, memory and hard disk for all the artifacts that Tor browser leaves on user system when browser is open and after it is closed. We looked for the artifacts about Tor installation, usage and browsing activities. Our results show that the Tor browser leaves many artifacts on user system especially in system memory.

Network forensics is very important part of digital investigation. In future research we are interested in network forensics of the Tor browser. This will help us to fully understand forensics behavior of this browser. We are also interested in forensics analysis of orfox which is android version of this browser. Orbot is another android app which work as Tor proxy. Forensics analysis of this app is also include in our future research goals.

Appendix A. Tor public keys in storage

Fig. 7

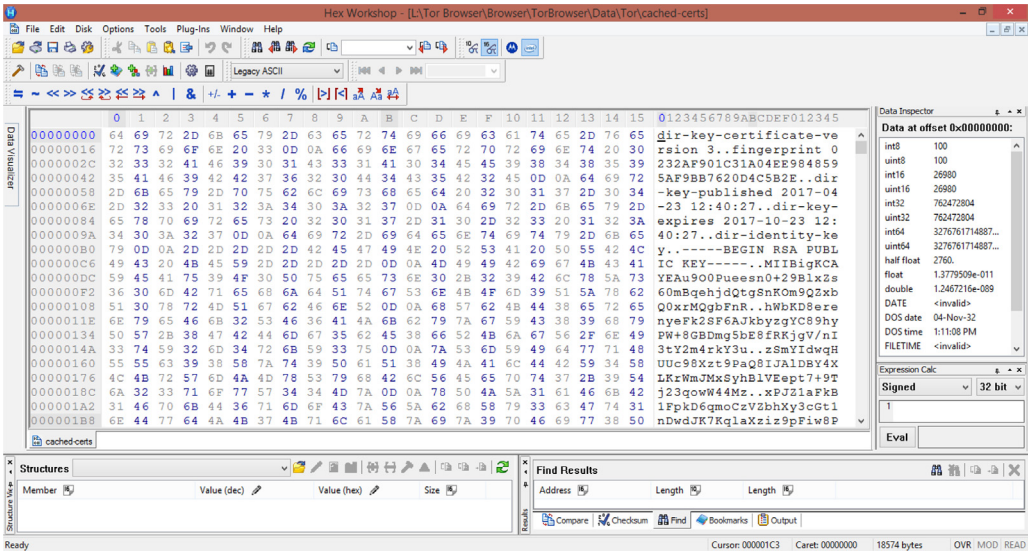

Fig. 7. Public keys of Tor relay in cached-certs file.

Appendix B. Relays information in storage

Fig. 8

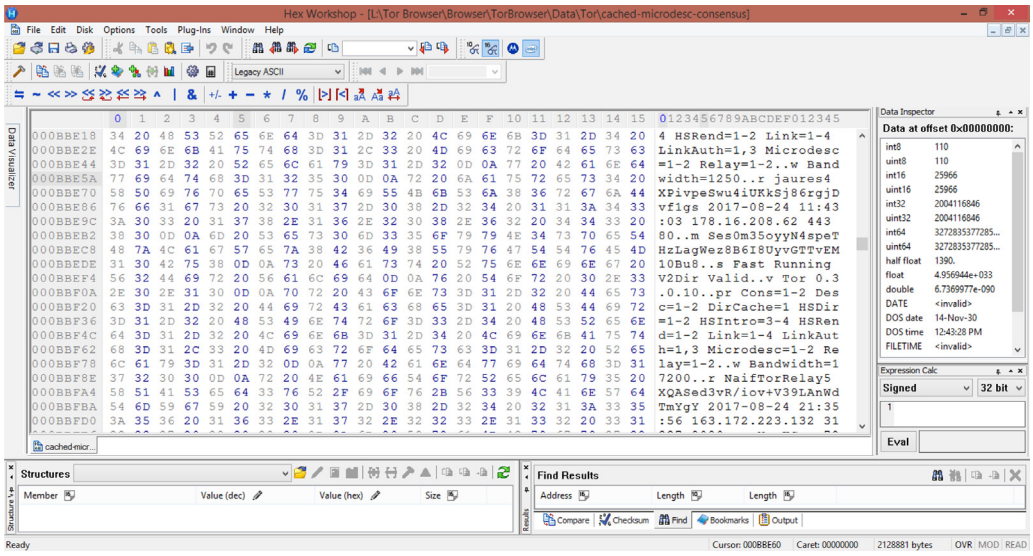

Fig. 8. Relays information present in cached-microdesc-consensus file.

Appendix C. Tor public keys in storage

Fig. 9

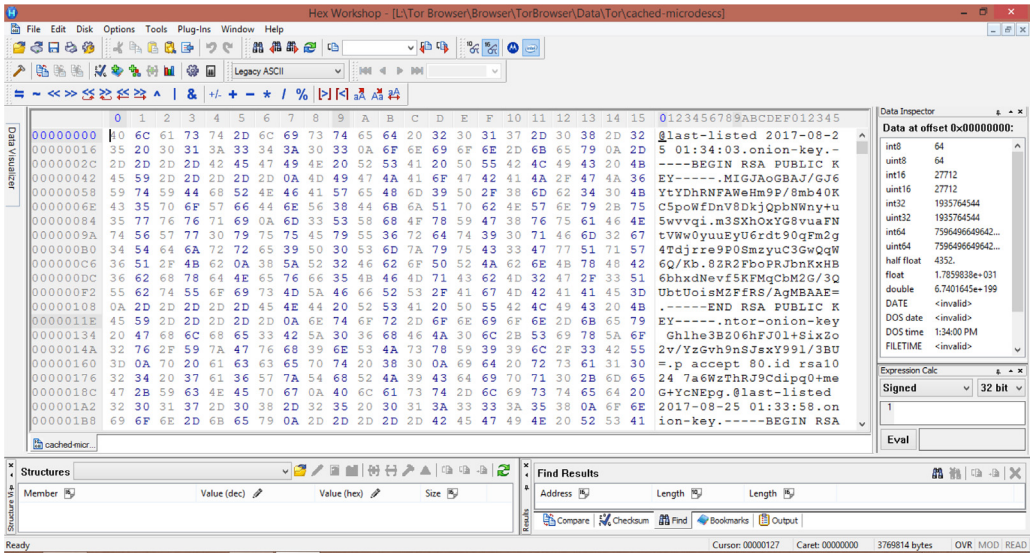

Fig. 9. Public keys of Tor relay in cached-microdescs file.

Appendix D. Tor public keys in storage

Fig. 10

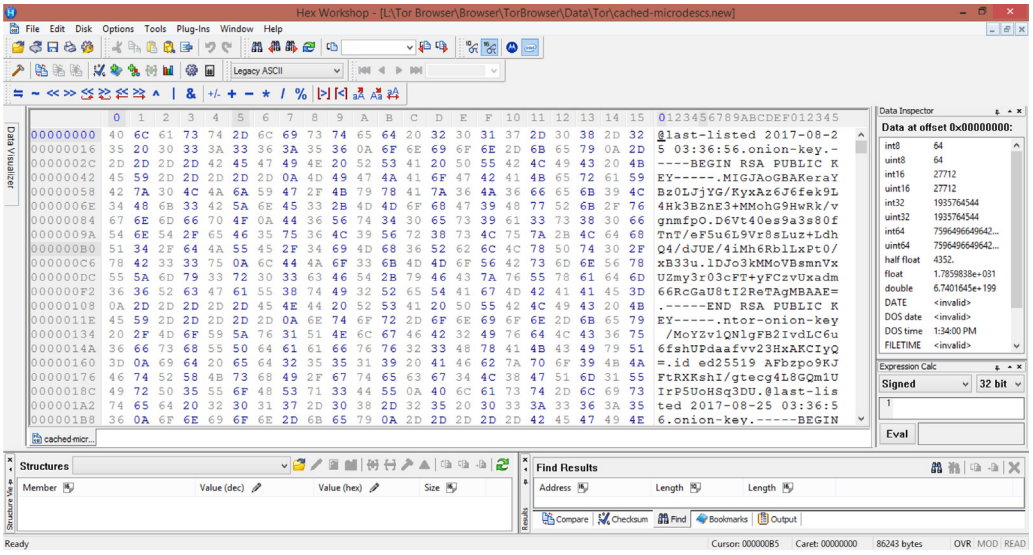

Fig. 10. Public keys of Tor relay in cached-microdescs.new file.

Appendix E. Email artifacts in memory

Fig. 11

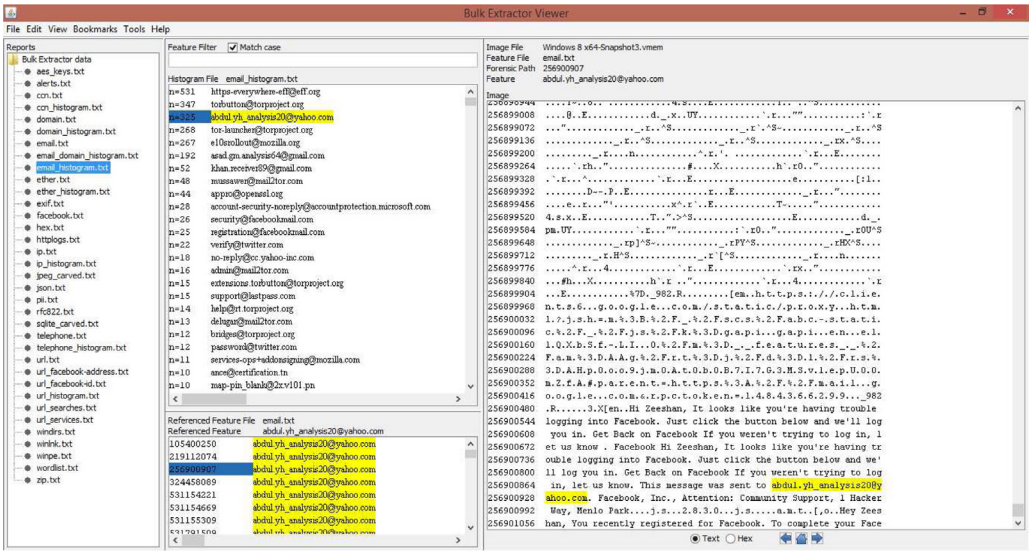

Fig. 11. Email artifacts recovered by bulk extractor from memory images.

Appendix F. Instagram artifacts in memory

Fig. 12

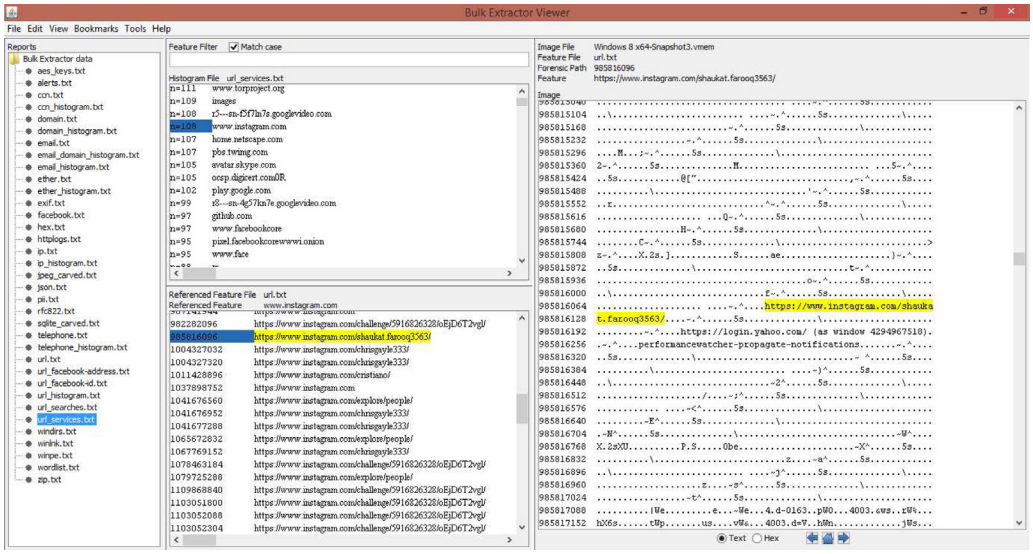

Fig. 12. Instagram artifacts recovered by bulk extractor from memory images.

Appendix G. Facebook artifacts in memory

Fig. 13

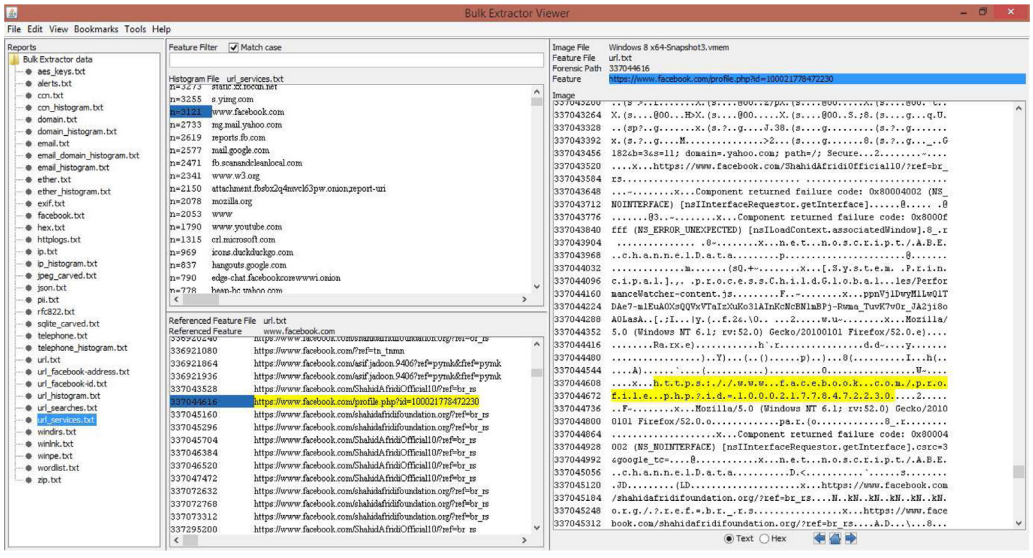

Fig. 13. Facebook artifacts recovered by bulk extractor from memory images.

Appendix H. Tor browser artifacts in storage

Fig. 14

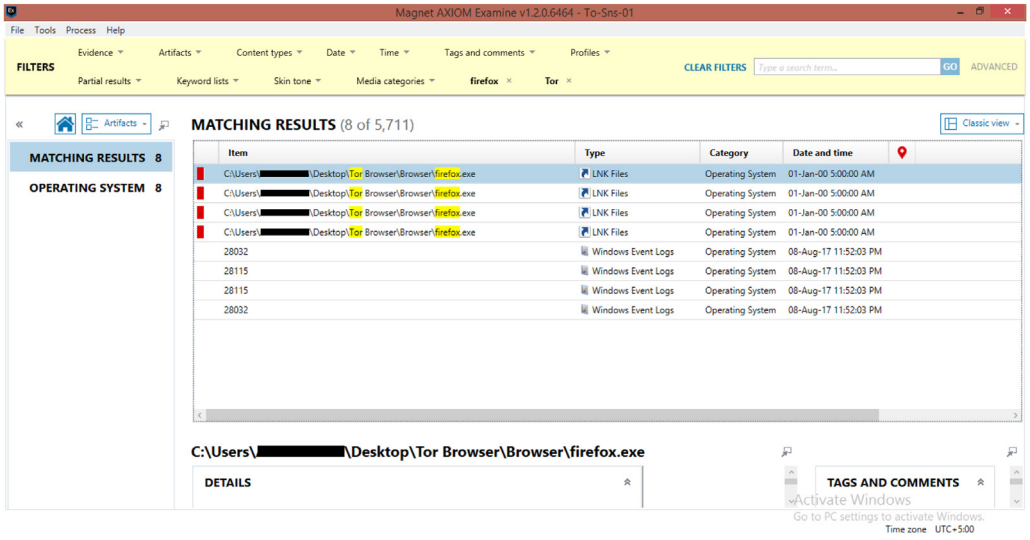

Fig. 14. Tor browser artifacts in storage.

Appendix I. Forensics hashes

Fig. 15

```
Created By AccessData® FTK® Imager 4.1.1.1

Case Information:
Acquired using: ADI4.1.1.1
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:
---------------------------------------------------------|
Information for G:\Analysis Data Final\Hard disk Analysis\Tor open\Snapshot disk\ToSn:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 29,360,128
[Image]
 Image Type: VMWare Virtual Disk
 Source data size: 14336 MB
 Sector count:    29360128
[Computed Hashes]
 MD5 checksum:    57f7e29a381f8aede9037c738472c348
 SHA1 checksum:   77f484ad2e9152d472f643b8a45e6fefad16e49a

Image Information:
 Acquisition started:   Thu Oct 19 23:57:08 2017
 Acquisition finished:  Fri Oct 20 00:02:57 2017
 Segment list:
  G:\Analysis Data Final\Hard disk Analysis\Tor open\Snapshot disk\ToSn.E01

Image Verification Results:
 Verification started:  Fri Oct 20 00:03:03 2017
 Verification finished: Fri Oct 20 00:09:29 2017
 MD5 checksum:    57f7e29a381f8aede9037c738472c348 : verified
 SHA1 checksum:   77f484ad2e9152d472f643b8a45e6fefad16e49a : verified
```

```
Created By AccessData® FTK® Imager 4.1.1.1

Case Information:
Acquired using: ADI4.1.1.1
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:
---------------------------------------------------------|
Information for G:\Analysis Data Final\Hard disk Analysis\Tor closed\Snapshot Disk\TcSns:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 29,360,128
[Image]
 Image Type: VMWare Virtual Disk
 Source data size: 14336 MB
 Sector count:    29360128
[Computed Hashes]
 MD5 checksum:    9cd6b6fd9cbee13ccaf46ef35b890ff7
 SHA1 checksum:   b0b8b10e22e1cf0fda10e3a106c157af157b3181

Image Information:
 Acquisition started:   Sun Oct 22 01:11:12 2017
 Acquisition finished:  Sun Oct 22 01:14:28 2017
 Segment list:
  G:\Analysis Data Final\Hard disk Analysis\Tor closed\Snapshot Disk\TcSns.E01

Image Verification Results:
 Verification started:  Sun Oct 22 01:14:34 2017
 Verification finished: Sun Oct 22 01:19:21 2017
 MD5 checksum:    9cd6b6fd9cbee13ccaf46ef35b890ff7 : verified
 SHA1 checksum:   b0b8b10e22e1cf0fda10e3a106c157af157b3181 : verified
```

Fig. 15. Hashes of hard disk image files for Tor browser open and closed status.

References

[1] ACCESSDATA GROUP, Inc, Ftk Imager, (2017) Available at: https://accessdata.com/product-download/ftk-imager-version-4.1.1.
[2] G. Aggarwal, E. Bursztein, C. Jackson, D. Boneh, An analysis of private browsing modes in modern browsers, Proceedings of the 19th USENIX Conference on Security, USENIX Association, 2010, pp. 6.
[3] A. Al-Khaleel, D. Bani-Salameh, M.I. Al-Saleh, On the memory artifacts of the tor browser bundle, The International Conference on Computing Technology and Information Management (ICCTIM), Society of Digital Information and Wireless Communication, 2014, pp. 41.
[4] R. Anderson, et al., The eternity service, Proceedings of PRAGOCRYPT (1996) 242–252.
[5] BreakPoint Software, Inc, Hex workshop, (2017) Available at: http://www.bpsoft.com/downloads/.
[6] M. Buecher, XhmikosR, TiANWEi, Regshot, (2017) Available at: https://sourceforge.net/projects/regshot/files/latest/download.
[7] D.L. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, CACM 24 (1981) 84–90.
[8] H. Chivers, Private browsing: a window of forensic opportunity, Digital Invest. 11 (2014) 20–29.
[9] I. Clarke, O. Sandberg, B. Wiley, T.W. Hong, Freenet: a distributed anonymous information storage and retrieval system, Designing Privacy Enhancing Technologies, Springer, 2001, pp. 46–66.
[10] G. Danezis, R. Dingledine, N. Mathewson, Mixminion: design of a type iii anonymous remailer protocol, Proceedings 2003 Symposium on Security and Privacy, IEEE, 2003, pp. 2–15.
[11] W. Darcie, R. Boggs, J. Sammons, T. Fenger, Online Anonymity: Forensic Analysis of the tor Browser Bundle, (2014) .
[12] D. Dayalamurthy, Forensic Memory Dump Analysis and Recovery of the Artefacts of Using tor Bundle Browser – The Need, (2013) .
[13] R. Dingledine, M.J. Freedman, D. Molnar, The free haven project: distributed anonymous storage service, Designing Privacy Enhancing Technologies, Springer, 2001, pp. 67–95.
[14] R. Dingledine, N. Mathewson, P. Syverson, Tor: The Second-Generation Onion Router. Technical Report, Naval Research Lab, Washington, DC, 2004.
[15] M. Edman, B. Yener, On anonymity in an electronic society: a survey of anonymous communication systems, ACM Comput. Surv. 42 (2009) 5.
[16] J. Filleau, M. Zizyte, What Private Browsing Leaves Behind, (2016) 12 Dec.
[17] D. Forte, Advances in onion routing: description and backtracing/investigation problems, Digital Invest. 3 (2006) 85–88.
[18] M.J. Freedman, R. Morris, Tarzan: a peer-to-peer anonymizing network layer, Proceedings of the 9th ACM Conference on Computer and Communications Security, ACM, 2002, pp. 193–206.
[19] X. Gao, Y. Yang, H. Fu, J. Lindqvist, Y. Wang, Private browsing: an inquiry on usability and privacy protection, Proceedings of the 13th Workshop on Privacy in the Electronic Society, ACM, 2014, pp. 97–106.
[20] S. Garfinkel, A. Bruce, Bulk extractor, (2017) Available at: http://downloads.digitalcorpora.org/downloads/bulk_extractor/newer_dev/.
[21] A. Ghafarian, S.A.H. Seno, Analysis of privacy of private browsing mode through memory forensics, Int. J. Comput. Appl. 132 (2015).
[22] I. Goldberg, D. Wagner, E. Brewer, Privacy-enhancing technologies for the internet, Proceedings of Compcon'97, IEEE, 1997, pp. 103–109.
[23] D. Goldschlag, M. Reed, P. Syverson, Onion routing, CACM 42 (1999) 39–41.
[24] D.M. Goldschlag, M.G. Reed, P.F. Syverson, Hiding routing information, International Workshop on Information Hiding, Springer, 1996, pp. 137–150.
[25] Google, Google Chrome, (2017) Available at: https://www.google.com/chrome/browser/desktop/index.html.
[26] S. Helmers, A brief history of anon.penet.fi – the legendary anonymous remailer, Comput Mediated Commun. Mag. 4 (1997) 9.
[27] J. Helsingius, Johan Helsingius gets Injunction in Scientology Case Privacy Protection of Anonymous Messages still Unclear, (1996) .
[28] M. Hirwani, Y. Pan, B. Stackpole, D. Johnson, Forensic acquisition and analysis of vmware virtual hard disks, Proceedings of the International Conference on Security and Management (SAM), The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2012, pp. 1.
[29] D.J. Kelly, A Taxonomy for and Analysis of Anonymous Communications Networks, Air Force Institute of Technology, 2009.
[30] S. Levy, Crypto Rebels. High Noon on the Electronic Frontier, (1996) , pp. 185–205.
[31] J.C. Liou, M. Logapriyan, T.W. Lai, D. Pareja, S. Sewell, A study of the internet privacy in private browsing mode, Proceedings of the 3rd Multidisciplinary International Social Networks Conference on SocialInformatics, Data Science 2016, ACM, 2016, pp. 3.
[32] Magnet Forensics Inc, Magnet Axiom, (2017) Available at: https://www.magnetforensics.com/try-magnet-axiom-free-30-days/.
[33] Microsoft, Window 8.1, (2017) Available at: https://www.microsoft.com/en-us/software-download/windows8.
[34] MiniTool Solution Ltd, Minitool Partition Wizard, (2017) Available at: https://www.partitionwizard.com/download.html.
[35] U. Möller, L. Cottrell, P. Palfrader, L. Sassaman, Mixmaster Protocol-Version 2, (2003) Available at: www.abditum.com/mixmaster-spec.txt.
[36] Office of Public Affairs, D.o.J, Massachusetts Man Arrested and Charged with Cyberstalking Former Roommate, (2017) Available at: https://www.justice.gov/opa/pr/massachusetts-man-arrested-and-charged-cyberstalking-former-roommate.
[37] Office of Public Affairs, D.o.J, Massachusetts Man Sentenced to More than 17 years in Prison for Cyberstalking Former Housemate and Others, Computer Hacking, Sending Child Pornography and Making over 100 Hoax Bomb Threats, (2018) Available at: https://www.justice.gov/opa/pr/massachusetts-man-sentenced-more-17-years-prison-cyberstalking-former-housemate-and-others.
[38] J. Oh, S. Lee, S. Lee, Advanced evidence collection and analysis of web browser activity, Digital Invest. 8 (2011) S62–S70.
[39] D.J. Ohana, N. Shashidhar, Do private and portable web browsers leave incriminating evidence?: a forensic analysis of residual artifacts from private and portable web browsing sessions, EURASIP J. Inform. Security 2013 (2013) 6.
[40] M.O. Rabin, Efficient dispersal of information for security, load balancing, and fault tolerance, J. ACM 36 (1989) 335–348.
[41] M.K. Reiter, A.D. Rubin, Crowds: anonymity for web transactions, ACM Trans. Inform. Syst. Security 1 (1998) 66–92.
[42] T. Rid, The Cypherpunk Revolution, (2017) . (accessed on 1.25.2017) http://projects.csmonitor.com/cypherpunk.
[43] H. Said, N. Al Mutawa, I. Al Awadhi, M. Guimaraes, Forensic analysis of private browsing artifacts, 2011 International Conference on Innovations in Information Technology (IIT), IEEE, 2011, pp. 197–202.
[44] R.A. Sandvik, Forensic Analysis of the tor Browser Bundle on os x, linux, and Windows, (2013) .
[45] K. Satvat, M. Forshaw, F. Hao, E. Toreini, On the privacy of private browsing – a forensic approach, Data Privacy Management and Autonomous Spontaneous Security, Springer, 2014, pp. 380–389.
[46] P. Syverson, A peel of onion, Proceedings of the 27th Annual Computer Security Applications Conference, ACM, 2011, pp. 123–137.
[47] P.F. Syverson, D.M. Goldschlag, M.G. Reed, Proceedings of 1997 IEEE Symposium on Anonymous Connections and Onion Routing, Security and Privacy, 1997, IEEE, 1997, pp. 44–54.
[48] TOR Project, Tor Browser, (2017) Available at: https://www.torproject.org/projects/torbrowser.html.en.
[49] TOR Project, Tor Faq, (2017) Available at: https://www.torproject.org/docs/faq.html.en#HowUninstallTor.
[50] TOR Project, Tor Metrics, (2017) Available at: https://metrics.torproject.org.
[51] TOR Project, The tor Project: Anonymity Online, (2017) Available at: https://www.torproject.org.
[52] U.S. Attorney's Office District of Massachusetts, D.o.J, Harvard Student Charged with Bomb Hoax, (2013) Available at: https://www.justice.gov/usao-ma/pr/harvard-student-charged-bomb-hoax.
[53] VMware, Vmware Workstation Pro, (2017) Available at: https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html.
[54] Volatility Foundation, An Advanced Memory Forensics Framework, (2017) Available at: http://www.volatilityfoundation.org.
[55] Volatility Foundation, Command Reference, (2017) Available at: https://github.com/volatilityfoundation/volatility/wiki/Command-Reference.
[56] M. Waldman, A.D. Rubin, L.F. Cranor, Publius: a robust, tamper-evident censorship-resistant web publishing system, USENIX Security Symposium (2000) 59–72.
[57] A. Warren, Tor Browser Artifacts in Windows 10, (2017) Retrieved from SANS Institute website: https://www.sans.org/reading-room/whitepapers/forensics/tor-browser-artifacts-windows-10-37642.