Computers, Materials & Continua
DOI: 10.32604/cmc.2022.022475
Article

Tech Science Press

Windows 10's Browser Forensic Analysis for Tracing P2P Networks' Anonymous Attacks

Saima Kauser[1], Tauqeer Safdar Malik[1,*], Mohd Hilmi Hasan[2], Emelia Akashah P. Akhir[2] and Syed Muhammad Husnain Kazmi[3]

[1]Air University, Department of Computer Science, Multan, 60000, Pakistan
[2]Centre for Research in Data Science, Department of Computer and Information Sciences,
Universiti Teknologi PETRONAS, Seri Iskandar, Perak, 32610, Malaysia
[3]IAR Systems, Märsta, Stockholm, Station Gatan 23, 19542, Sweden
*Corresponding Author: Tauqeer Safdar Malik. Email: tauqeer.safdar@aumc.edu.pk

Received: 09 August 2021; Accepted: 29 September 2021

Abstract: A web browser is the most basic tool for accessing the internet from any of the machines/equipment. Recently, data breaches have been reported frequently from users who are concerned about their personal information, as well as threats from criminal actors. Giving loss of data and information to an innocent user comes under the jurisdiction of cyber-attack. These kinds of cyber-attacks are far more dangerous when it comes to the many types of devices employed in an internet of things (IoT) environment. Continuous surveillance of IoT devices and forensic tools are required to overcome the issues pertaining to secure data and assets. Peer to peer (P2P) applications have been utilized for criminal operations on the web. Therefore, it is a challenge for a forensic investigator to perform forensic analysis of the evolving hardware and software platforms for IoT. For identity concealment and privacy protection, the Onion Router (Tor) and Chrome with the Invisible Internet Project (I2P) as the foundation browser are often used. Confirmation is required to determine whether Tor is truly anonymous and private as they claim. Some people, on the other hand, utilize the Tor browser for evil reasons. Tools and techniques are available for the collection of artifacts, identifying problem areas, further processing and analysis of data on the computer and IoT. Present research tried to explore a few tools for the tracing of I2P activities over computer on windows 10 that reflects IoT devices. According to the results of this research, it leaves an excessive amount of important digital evidence on the operating system that can be exploited to attack the information of users. This research is based on windows operating system and does not support other operating systems.

Keywords: Cyber-security; peer-to-peer; invisible internet project (I2P); forensic analysis; the onion router (Tor)

1 Introduction

The Internet has become the inevitable part of our life today. According to datareportal.com, almost 4.66 billion people were active internet users as of Jan 2021, having 59.5% of the global population [1]. This tremendous increase in internet users has provided consumers with a variety of useful services, such as entertainment, social networking, e-commerce, live gaming, blogging, online tickets, banking, and so on. Furthermore, it is worth mentioning that approximately 8 million internet users use Tor to access the internet [2]. However, there are cyber-attacks escalation as well. In the field of computers, every activity is stored in digital form and can be retrieved by the process of forensic analysis. Today, many tools are available to obtain anonymity for the purpose of trackless browsing. In some countries, there is the possibility of having legal cover for anonymity, and in some areas, it could be a lethal weapon for cyber criminals [3]. There have been some major cyber-attacks that have prompted investigators to consider cybercrime, which is a growing problem in today's world. Cybercrime is defined as any fraudulent activities using a computer, digital device, or a network node.

The Tor project was started in 1995 by the US Naval Research Laboratories with the goal of separating the identity of a user as of routing and providing a military-friendly anonymous communication network [4]. No doubt, Tor was especially built for the military, but now, as per Tor metrics, about 3 million active users are available, having more than 7000 nodes for their traffic and 26 Gbps of bandwidth for the network. Tor is an advanced version of Mozilla Firefox that connects to the Tor overlay network to route users' communications anonymously, providing enhanced privacy and hidden identity capabilities.

Peer-to-Peer networks (P2P) are self-controlled overlay networks that are spread over Internet Protocol (IP) networks. P2P file-sharing networks are modelled after the Internet of Things (IoT), which features self-governing connected devices in dispersed and de-centralized systems [5]. The Scalability is facilitated by P2P overlays in a dynamic and de-centralized system. On the contrary toward the client-server architecture, the nodes in a P2P system are handled separately. These overlay networks can sometimes provide services those are not available through traditional client-server systems.

The most widely used open-source unidentified communication tool is the Invisible Internet Project (I2P) featuring identity hiding and maintaining privacy. The I2P is an unidentified peer to peer network layer over which enormous unidentified applications can work. I2P is mainly used for nameless browsing, file sharing, email, chat, blogs, online shopping and much more. To participate in an I2P network, an application software known as a router is required. The software does not know the endpoints or destinations linked to different applications. Thus, an end user would have several local destinations on their router. A separate tunnel is created for explicitly sending and receiving messages through a predefined list of routers. In I2P communication, inbound and outbound tunnels are used. I2P also uses garlic routing, a modified version of an onion router. It can encrypt multiple messages together and, hence, traffic analysis will be more complex and the data transfer speed would increase as shown in Fig. 1.

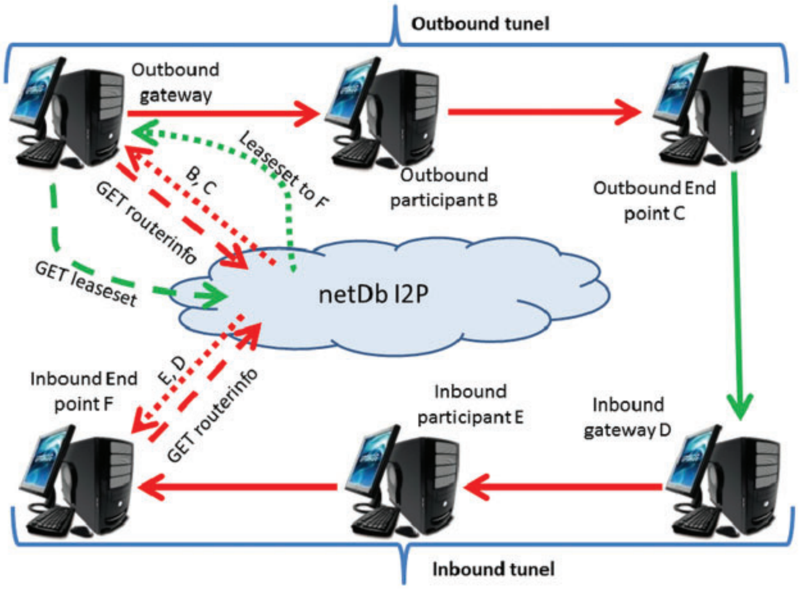


Figure 1: I2P connectivity in P2P networks for inbound and outbound users

In Fig. 1 virtual circuits B, C, E and D are created for sharing routing information of inbound and outbound participants E, F, D and B, C respectively. Tor client can get relay information from directory server netDb of I2P network. A "tunnel" is another crucial phrase to comprehend I2P. A tunnel is a path that is steered through a set of routers that has been carefully chosen. Each tunnel has a beginning and an end point (the first router, often known as the "gate"). There are two types of tunnels: "Outbound," which sends a message from the tunnel's maker, and "Inbound," which delivers a message to the tunnel's originator. We can convey messages from the sender to the recipient using the combination of these two tunnels. The I2P network database (netDb) is required to connect the two tunnels. This database contains the information needed to contact a certain router (public keys, transport addresses, and so on) as well as the information needed to reach the target recipient (the gateway, which enables a destination, the lifetime of the tunnel, a public key pair to encrypt messages).

The most difficult problem is addressing the misappropriations caused by the P2P network's capabilities in I2P. Many Law Enforcement Organizations (LEO) are struggling to cope with the new technologies and techniques that are being mistreated by P2P users who help facilitate and contribute to fraudulent activities online. There is a need to investigate the P2P networks for forensic analysis of I2P browsers on Windows 10 to recover some important artifacts in memory, registry and browsing activities on the hard disk. Moreover, it is pertinent to mention here that as far, no research is available for Law Enforcement Agencies (LEA) and with the help of proposed research forensic analysis of Windows 10 can be done speedily and easily. Therefore, our main focus is on cybercrime to benefit law enforcement agencies by providing a mechanism for forensic analysis. Furthermore, most of the time the network artefacts or Windows-based artefacts are under observations, hence, we are discovering the traces of dark web activity in criminal investigations on Windows 10. This is helping in P2P document sharing for organizations which are using the mirror for the Internet of Things (IoT) worldview with self-ruling arranged gadgets inside conveyed and decentralized framework [6].

The rest of the paper is organized as Section 2 presents the related work and shows the need of the presented work. Section 3 describes the methodology with its detailed tools and phases. Section 4 analyzes the results and compares with the previous research work. Finally, the conclusion section summarizes the current research with future work.

2 Literature Review

Studies of Tor and I2P forensics have previously motivated on memory forensics to recognize the source of dark web sites or to de-anonymize users. In [6], researchers presented a database containing domain link to present the reconstructed relations as graph and analyzed for interconnection with darknet. The results shows that main darknet service play important role in the communication paths of the darknet. As limitations, it is hard to find weaknesses if dataset contains services of TOR that are deployed securely. Several browsing tools are analyzed and presented a feature based comparison for analysis of browser running in normal, private and portable mode. Best forensic approaches are applied for the creation of digital artifacts [7]. A Case Study for Privacy and Anonymity on the Web has collected TOR artifacts from host machine and carried out a detail analysis of artifacts from registry, memory and hard disks [8]. The obtained results are supportive for LEA in cases where a Tor browser user is under investigation. It is performed on windows 8.1 with no support for latest operating systems. It is found that when the user used Incognito mode all the data of each event made by the user is traced like Login details, Email details, browsing details, etc. even after the browser closed or even open. The Universal Control (UC) Browser dealer said that by using Incognito mode of it, user history of events and other details will not be observable but using this forensics investigation it can be discoverable and the private browsing mode is still challenging according to user privacy [9]. The limitations for the research is that the research has been done on the incognito mode of the UC browser and finds some artifacts. But no forensic analysis on the onion browser.

A similar research on the forensic analysis of web browser is done in which the way to analyze the browser forensically is to take the image of the hard drive, select some user's search words from the history file, and use the Forensic Toolkit (FTK) Live Search option to search those keywords in the image drive. She revealed that no user can browse safely on the internet [10]. The researcher uses investigation based on the steps from live forensics method for acquisition of data on live media. The research is compatible to perform data acquisition process and background to the problem behind live forensic methods. For testing, Firefox browser is used in the research with privacy feature on and off. The result of the investigation shows that sufficient and valuable information is obtained after live memory forensic about suspicious activities [11]. These activities included traces of email and Facebook id even after the browser is closed, website visited, clear history and keywords on the internet. These artifacts are sufficient for the accusing of culprit.

The study of correlating message from multiple Instant Messaging (IM) networks to identify digital forensic artifacts, the suspect is communicating with correspondent relatedly through Digsby Instant Messaging (DIM) client. For the experimenting and conducting research, they have taken four IM protocols which include AIM, Windows Live Messenger protocols, Google Talk and Yahoo Messenger. The chat contents of each IM protocol either in complete or fractional form found at various locations found in Random Access Memory (RAM). Forensic Analyst can collect complete conversation contents from RAM as stored in Digsby logs. Additionally, the status updates (live, idle, away, etc.) can also gather from RAM using login ID of particular IM protocol and login ID of Digsby. Moreover, an automated tool should be developed to resolve the issue of using multiple IM protocols for a single conversation session [12]. In computer forensics, extraction of memory forensic artifacts are very important and provide basis for data acquisition. Thomas et al. have done memory forensic in different phases such as identification of Kernal Process Control Register (KPCR), extraction of running process list, identifying Process Environment Block (PEB) and its related structures and extracting process memory. They observed that the process of memory analysis is highly dependent on the operating system. In the given paper method for acquiring important information are KPCR, CR3 register value, process details, loaded Dynamic Link Libraries (DLLs) and process memory from windows 7 memory dump. However, as far as limitations are concerned this whole technique can be done on the latest window like windows 8.1 and windows 10 [13].

The researcher in [14] have proposed a system which extracts the physical memory dumps and local files of the system as input and processes it and then generates a report having I2P artifacts as output. The traces of I2P were successfully pointed out using in depth analysis of the memory dump and local system files. Furthermore, registry also contain I2P traces and HDD is also a place where traces of I2P can be find. No support for registry and HDD analysis is provided. Overall objectives in this research have been obtained but complex and updated application needs further improvements in research.

The implementation of classification of I2P network data traffic is performed on the basis of algorithms such as Baysnet, naivebays, Support Vector Machine (SVM) and random forest traffic [15]. The obtained results shows that for segmentation of data set, RandomForest is greatest having accuracy of 100%. As far as limitations are concerned no in-depth detailed analysis of the encryption principle and anonymous implementation of the I2P protocol. Whereas in [16], authors presented I2P characteristics to point out the security flaws and problems finding artifacts of the I2P. The results shows that the I2P artifacts collected and analyzed on the basis of vulnerabilities of I2P networks and specific security issues. The platform comprises on data acquisition module, forum information inquiry module and visualization module are analyzed in [17]. The obtained results help law enforcement agencies to analyze illegal and criminal activities over dark web. Research on Tor or onion routers is missing. In [18], a theoretical comparison of TOR and I2P is made from a variety of aspects, including community visibility, scalability, memory utilization, latency, bandwidth, documentation, vulnerability to DoS attacks, and the number of exit nodes. The authors attempted to characterize the file sharing environment within I2P, analyzing how it affects the network's anonymity. The majority of I2P's activities are focused on file sharing and anonymous site hosting, according to the findings. Furthermore, the nodes are found to be spatially scattered.

As per analysis of various literatures, comprehensive research on the latest windows 10 is missing as well as browser artifacts are mandatory in analysis. Various researches are also available on the topic but Tor left various browsing artifacts on memory and hard disk which is missing in previous research. The comparative analysis of some important research papers on the basis of above literature review is given as under see Tab. 1. Many structures for digital forensics already exist, demonstrating their relevance to the area. These current frameworks serve as a foundation for the suggested framework for this study. Tor memory forensics encompass huge research gap [19]. The present paper throws light on this issue and proposed a forensic platform for I2P and Tor browser memory, registry and hard disk analysis.

Table 1: Comparative analysis of literature review

Research paper	Area of forensic	Platform used	Browser artefacts	Network evidences
Tor browser artefacts in windows 10 (2021)	Memory and registry	Windows 10	No	No
Forensic analysis of tor browser bundle (2020)	Memory and registry	Windows 7	No	No
On the memory artefacts of the tor browser bundle (2019)	Memory	Windows 7	Yes	No

3 Methodology

With the invention of new hardware and software, as well as the rapid growth in internet users, many Peer-to-Peer (P2P) users are contributing to and facilitating illegal activities online, which should be addressed based on solid evidence. For the collection of these evidences, law enforcement agencies must be updated with new tools and techniques. The methodology that will be adopted in this work is shown in Fig. 2. In the first phase of methodology, a computer system having virtual machine with windows 10 operating system was setup for experimental purposes. The second phase comprises of acquisition of data for forensic analysis. In this phase artefacts were collected from registry, RAM and hard disk were taken. After acquisition, collected data was forensically analyzed in third phase for presentation of evidences. For the experimental purpose, the required platform and tools will be prepared on the host system. After installation of the required tools, data acquisition will be carried out. In the first phase, registry data artifacts will be collected and in second phase, memory data artifacts will be collected. Finally, browsing data artifacts will be collected as shown in Fig. 2. The mandatory investigational tools are tabulated in Tab. 2 to produce a fast and accurate result, a fresh Windows 10 installation was prepared in a virtual box. The tools used for the current investigations are totally free and easy to use.

Before the start of forensic analysis, some input is required to be given to the system. So that system could produce artifacts. In order to fulfill the requirement, experimental input was prepared in the form of performing activities over I2P and Tor browsers. One Instagram account, one Yahoo mail account, two Gmail accounts, two Skype accounts, two Twitter accounts, and three Facebook accounts are created for this purpose. The sample data is also shared between these accounts. Tab. 3 contains information on these activities. After these activities, all the downloaded images and files are removed from the system before the data acquisition.

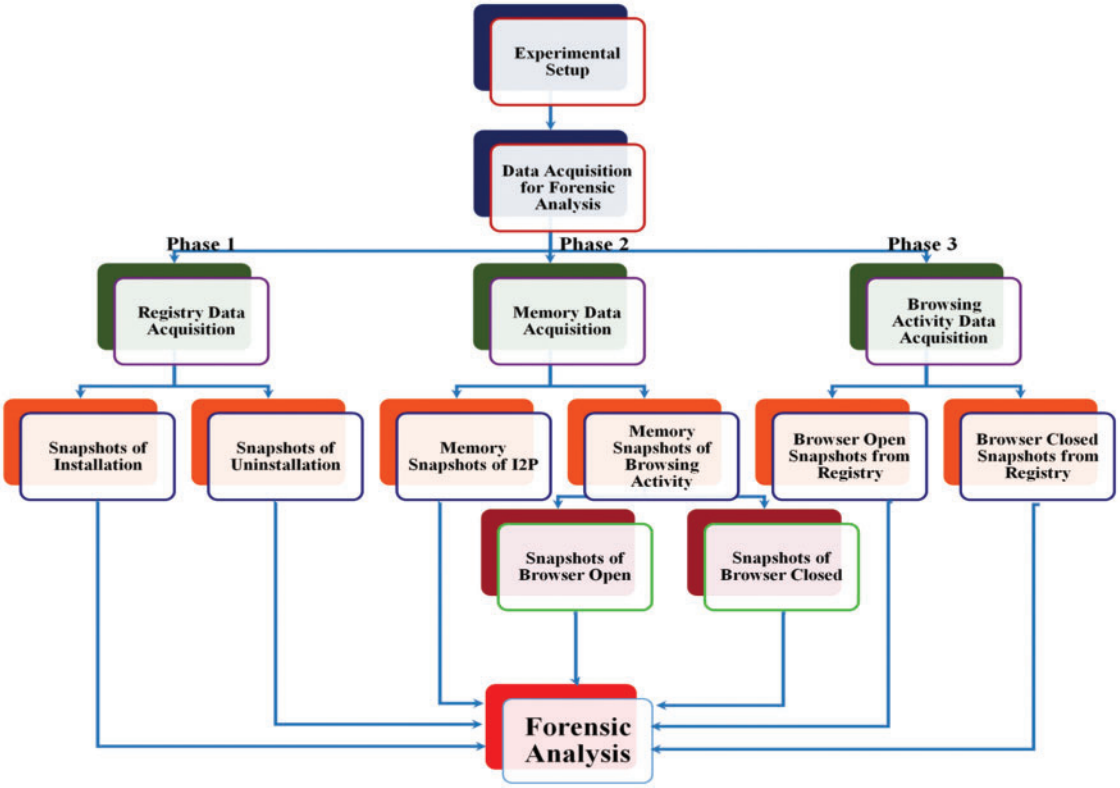

Experimental Setup
Data Acquisition for Forensic Analysis
Phase 1
Phase 2
Phase 3
Registry Data Acquisition
Memory Data Acquisition
Browsing Activity Data Acquisition
Snapshots of Installation
Snapshots of Uninstallation
Memory Snapshots of I2P
Memory Snapshots of Browsing Activity
Browser Open Snapshots from Registry
Browser Closed Snapshots from Registry
Snapshots of Browser Open
Snapshots of Browser Closed
Forensic Analysis

Figure 2: Proposed system design for forensic analysis

Table 2: Forensic analysis tools

Name of tool	Version	Used for
Oracle virtual box	6.1	Installation of OS
I2P browser	0.9.37	Anonymous browsing
Autopsy	4.18.0	HDD and memory analysis
Tor	7.0.2	Anonymous browsing
Firefox	89.0	Simple browsing
Bulk extractor [20]	1.6	Analysis
Hex workshop [21]	6.7	Analysis
Access data FTK imager	4.1	Memory data acquisition
Regshot [22]	1.9.0	Registry data acquisition

Table 3: Browsing activity over Tor and normal browser

Website	Activates performed on tor and chrome browsers	Tor accounts	Chrome accounts
Gmail	Sending, receiving email download attachment, view files online etc. were performed.	User1_Tor@gmail.com	User1_Chrome@gmail.com
Yahoo mail	Sending, receiving email download attachment, view files online etc. were performed.	User2_Tor@yahoo.com	User2_Tor@yahoo.com
Google Drive	Browsing, saving files to drive and reading from the drive online were completed.	User1_Tor@gmail.com	User1_Chrome@gmail.com
Twitter	Opening site, logging into the accounts, tweet, retweet, like tweet visit accounts follow were performed	User3_tor@User3_tor	User3_chrome@User3_chrome
Instagram	Activities on Instagram such as opening site, logging into the accounts, follow, like picture, comments were performed	User4_Tor@User4_Tor	User4_Tor@User4_Tor

(Continued)

Table 3: Continued

Website	Activates performed on tor and chrome browsers	Tor accounts	Chrome accounts
Facebook	Browsing the website, login, liked pages and post, sharing of posts, commenting on posts, pages visiting and user profiles, accounts searching, receive friend request, chatting with other users were the activities performed on facebook	User5_Tor User6_Tor	User5_Chrome
Skype	Browsing, login, searching accounts and chatting with other skype users.	User7_Tor	User7_Chrome
Youtube	Browsing the site, searching keywords and watching videos	–	
Google maps	Browsing the site and searching various places.	–	
Research papers	Website browsing, opening PDF research papers online.	–	

The data acquisition is completed in three phases. In the first phase, registry data is collected and in the second phase, I2P based Tor only memory data is collected. Finally in the third phase, artifacts of memory and storage are collected. After the data is collected from the three phases, the system is returned to a spotless state to confirm that no pieces from the preceding phase remained. The first phase entails gathering pre-installation data. The acquisition of post-installation data is part of the second phase. The third step is to collect post-uninstallation data. The Regshot tool is used for data acquisition of the registry [19]. Memory data acquisition is carried out in two portions. These parts are I2P based Tor only and I2P based Tor browsing. Whereas two scenarios are considered for I2P based Tor browsing open and closed.

4 Results and Analysis

Browsers are necessary for a productive work environment but they also serve as an ideal vector for cyber-attacks. Cyber-attacks and crimes are multi-faceted in today's world and they are on the rise [20]. With sophisticated tools, digital forensics is a great discipline for limiting and investigating such risks. The web browser is the most extensively used application for accessing content on the internet and serves as the user's interface to the rest of the world. Visit web pages, access email accounts, use social media, and upload and download various files are all common browsing activities. There are three stages to forensic analysis such as registry snapshots followed by memory and storage images in the second and third stages respectively.

The Regshot tool is used to take registry snapshots and to analyze them. During installation, this browser adds three registry keys, according to the research. After uninstallation, all of these keys remain in the registry, showing that it does not erase its registry artefacts. It is also revealed that in different instances that these keys are added in a different order as shown in Tab. 4. The browser is installed in this case with the option to "Open browser automatically after installation." The browser is automatically launched after installation. The first two keys were inserted into the registry. When the browser was reopened after being closed, the third key was added.

Table 4: Artifacts of registry

Sr. no.	Registry key location	Description
1	HKUnS-1-5-21-3610041324-1787688552-2397930110-1001nSoftwarenmicrosoftnwindowsNTnCurrentVersionnAppCompatFlagsnCompatibility AssistantnStorenSIGN.MEDIA = 31C3D37 torbrowser-install-7.0.2_enUS.exe: 51 41 42 50 01 00 00 00 00 00 00 00 07 00 00 00 27 00 00 00 38 3D 3C 03 B6 60 3C 03 01 00 00 00 00 00 00 00 00 00 00 00 00 00 01 06 00 01 00 00 97 3F D6 91 C4 9E CE 01 00 00 00 00 00 00 00 00	Setup file of tor browser was shown in registry key.
2	HKUnS-1-5-21-3610041324-1787688552-2397930110-1001nSoftwarenMicrosoftnInternetExplorernLowRegistrynAudionPolicyConfignPropertyStoren6ae17f4a_0n: "{2}.nn?nhdaudio#func_01&ven_15ad&dev_1975&subsys_15ad1975&rev_1001#{6994ad04-93ef-11d0-a3cc-00a0c9223196}nelineouttopo/00010001|nDevicenHarddiskVolume1nUsersnSaimaDesktopnTor BrowsernBrowsernfirefox.exe%b{00000000-0000-0000-0000-000000000000}"	Registry key show Sound setting and area of firefox.exe record

(Continued)

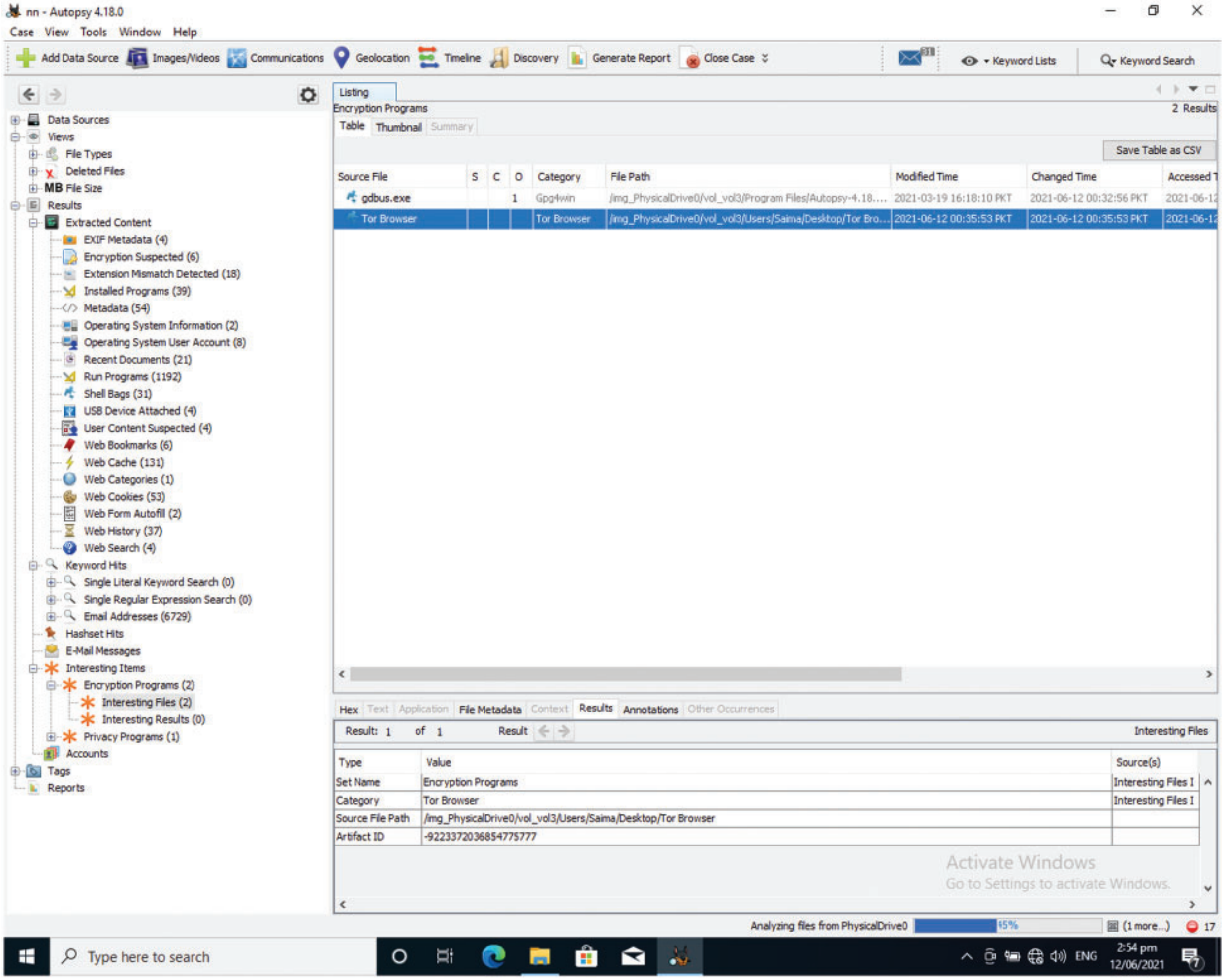
Table 4: Continued

Sr. no.	Registry key location	Description
3	HKUnS-1-5-21-3610041324-1787688552-2397930110-1001nSoftwarenMicrosoftnWindowsNTnCurrentVersionn AppCompatFlagsnCompatibility Assistantn-StorenC:nUsersnSaimaDesktopnTorBrowsernBrowsern firefox.exe: 51 41 42 50 01 00 00 00 00 00 00 07 00 00 00 27 00 00 00 38 3D 3C 03 B6 60 3C 03 01 00 00 00 00 00 00 00 00 00 00 00 00 00 01 06 00 01 00 00 97 3F D6 91 C4 9E CE 01 00 00 00 00 00 00 00 00	Location of tor shown in registry key. firefox.exe file is also located in the folder of tor browser.

The browser is installed in this case without the option to "Open browser automatically after installation." After the installation is complete, the first key is added. When the browser is opened, the second and third keys are added. These scenarios will be highly useful in circumstances when investigators want to determine if the individual only set up the Tor browser and if they used it after that. In respect to MS Word documents, various digital evidences can be recovered from memory. Al-Sharif et al. [21] developed a memory forensic technique based on the XML form utilized by MS Office internally. Different parts of MS Word can be recovered from memory to establish that the document was seen or modified by the user, according to their findings. Al-Saleh et al. [22] have investigated the effects of memory forensic methods on network reconnaissance detection. They made use of the data that can be retrieved from memory. Furthermore, they discovered that packets sent or received across the network can be stored in memory for a long time. Their findings revealed that memory analysis was useful in detecting assault artefacts. Primary artifacts recovered from Autopsy as shown in Fig. 3.

After installation, software leaves a large number of artifacts on the host machine. This section of the research focuses on recovering all of the artifact left on the host machine by Tor browser after installation and operation. For forensics analysis of obtained memory images, the Autopsy framework is employed. According to memory analysis, the Tor browser has two processes in memory: Firefox.exe and tor.exe. Other artifacts associated to these two processes are also recovered using their process ids. The key terms "Firefox" and "tor.exe" are used in obtaining information about Tor version artifacts for the two programs.

The third VMware snapshot was obtained for the "Open Browser" scenario, while the fourth was engaged for the "Closed Browser" scenario, as detailed in Data Acquisition. These two VMware snapshots' memory images (.mem files) are examined for surfing evidence. For analysis, the tool bulk extractor and a Hex workshop are utilized [23]. The bulk extractor is used for the majority of the analysis. Bulk extractor uses string search to locate links to user's social media account profiles, the profiles visited, videos watched and another artifact. The current strings are derived from the address of the site visited and user names that are used during the user's activity of browsing phase. Without utilizing strings searches, all of these artefacts can be found by analyzing all of the sites collected by Bulk Extractor, though this method is slower than string searches. Hex work-shops are used to search for email text in memory. To find these emails, the memory image was unwrapped using tool Hex workshop and various string explorations are conducted. During the user activities section, some strings from email text that are sent and received are also searched. The emails can also be recovered in memory without using string explorations by using hex workshop to display all strings present in memory completely. However, in the case of big memory images, this method is quite time consuming. All Gmail and Yahoo inbox emails, including unopened emails, are stored in memory when using Tor browser. Fig. 4 illustrates some of the emails found using string searches in the memory image of the third snapshot. Public keys and other relevant information of Tor relays used during communication by Tor browser for transmitting its traffic can be found using the strings "PUBLIC KEY" and "Relay=." IP address, Bandwidth, Ports, Name and Fingerprint, Tor version used, date and time of connection, and present status are among the other details (entry or exit) [24]. Figs. 5 and 6 show screenshots of public keys and some useful other information taken in the third VMware snapshot's memory picture.



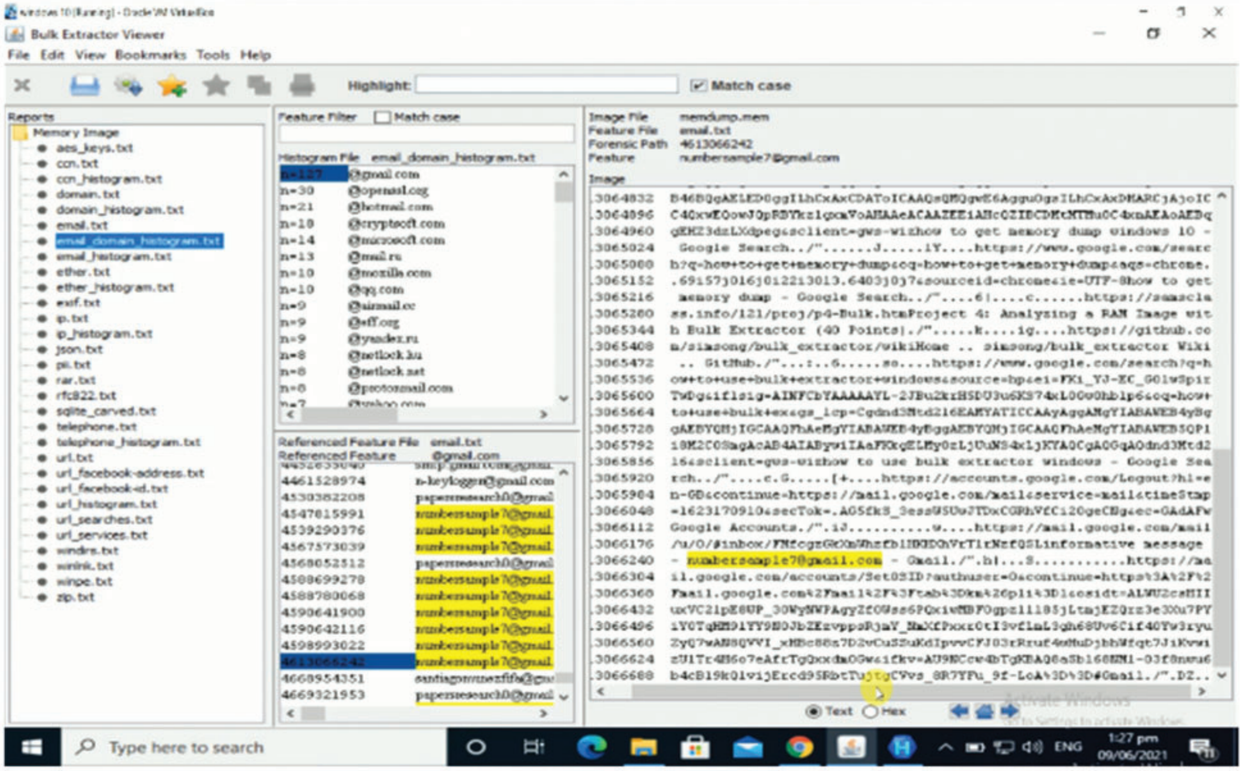
Encryption Programs 2 Results

Source File	S	C	O	Category	File Path	Modified Time	Changed Time	Accessed T
gdbus.exe			1	Gpg4win	/img_PhysicalDrive0/vol_vol3/Program Files/Autopsy-4.18....	2021-03-19 16:18:10 PKT	2021-06-12 00:32:56 PKT	2021-06-12
Tor Browser				Tor Browser	/img_PhysicalDrive0/vol_vol3/Users/Saima/Desktop/Tor Bro...	2021-06-12 00:35:53 PKT	2021-06-12 00:35:53 PKT	2021-06-12

Result: 1 of 1 Result Interesting Files

Type	Value	Source(s)
Set Name	Encryption Programs	Interesting Files I
Category	Tor Browser	Interesting Files I
Source File Path	/img_PhysicalDrive0/vol_vol3/Users/Saima/Desktop/Tor Browser	
Artifact ID	-9223372036854775777	

Figure 3: Tor artifacts recovered from autopsy



Histogram File email_domain_histogram.txt

n=127	@gmail.com
n=30	@openmail.org
n=21	@hotmail.com
n=18	@cryptoeft.com
n=14	@microsoft.com
n=13	@mail.ru
n=10	@mozilla.com
n=10	@qq.com
n=9	@airmail.cc
n=9	@eff.org
n=9	@yandex.ru
n=8	@netlock.hu
n=8	@netlock.net
n=8	@protonmail.com
n=7	@yahoo.com

Referenced Feature File email.txt
Referenced Feature @gmail.com

4452655040	smtp.gmail.com@gmail.
4461528974	n-keylogger@gmail.com
4530382208	paperresearch0@gmail
4547815991	numbersample7@gmail.
4539290376	numbersample7@gmail.
4567573039	numbersample7@gmail.
4568052512	paperresearch0@gmail
4588699278	numbersample7@gmail.
4588780068	numbersample7@gmail.
4590641900	numbersample7@gmail.
4590642116	numbersample7@gmail.
4598993022	numbersample7@gmail.
4613066242	numbersample7@gmail.
4668954351	santiagonunezfifa@gm
4669321953	paperresearch0@gmail

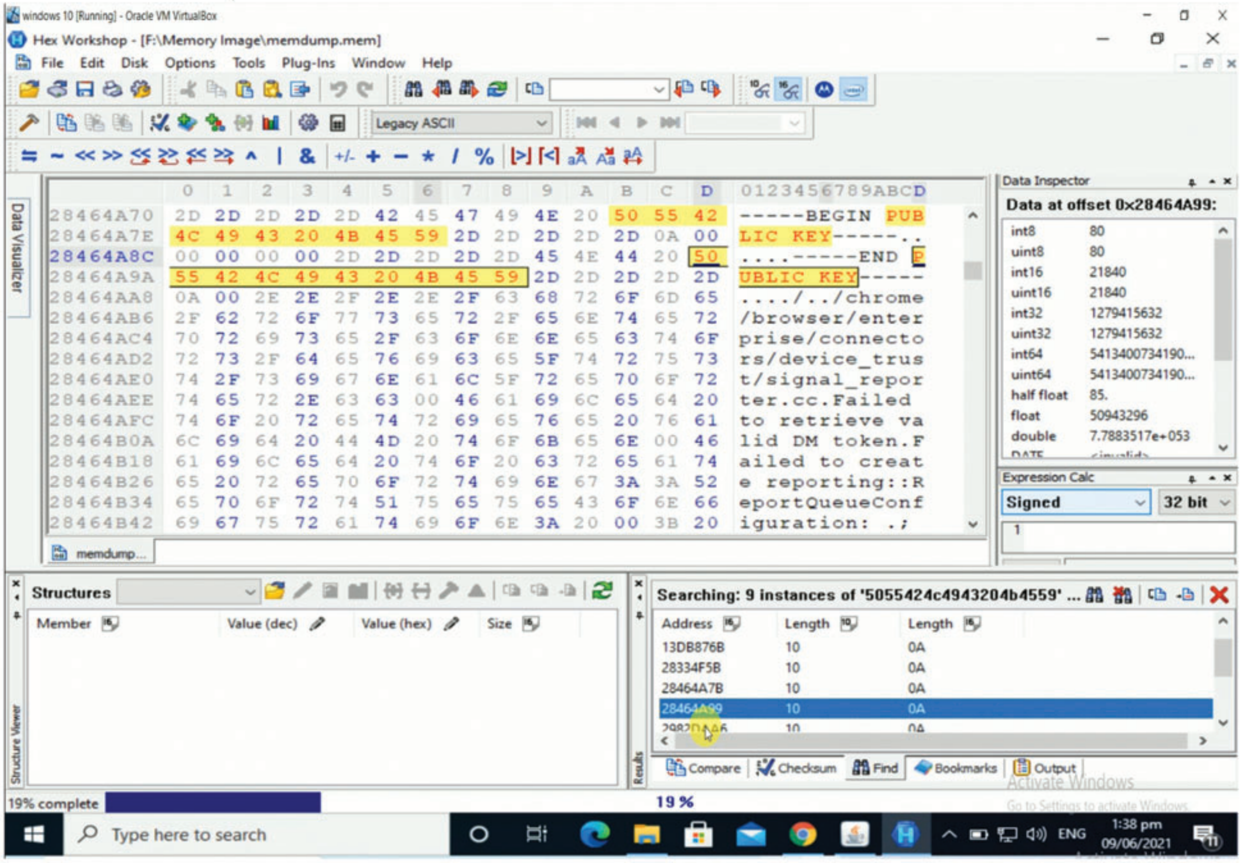
Image File memdump.mem
Feature File email.txt
Forensic Path 4613066242
Feature numbersample7@gmail.com

Image

```
.3064832  B46BQgAELED0ggIlhCxAxCDAToICAAQsGMQgwE6AgguOgsILhCxAxDMARCjAjoIC
.3064896  C40xwEQowJ0pRBYkz1gcmVoAHAAeACAAZEEiAHcOZIBCDMtMTMuOC4xnAEAoAEDq
.3064960  gEHZ3dzLXdpegcsclient=gws-wizhow to get memory dump windows 10 -
.3065024   Google Search../"......J.....lY....https://www.google.com/searc
.3065088  h?q=how+to+get+memory+dump&oq=how+to+get+memory+dump&aqs=chrome.
.3065152  .69i57j016j0122i3013.6403j0j7&sourceid=chrome&ie=UTF-8how to get
.3065216   memory dump - Google Search../"....6|....c......https://samscla
.3065280  ss.info/121/proj/p4-Bulk.htmProject 4: Analyzing a RAM Image wit
.3065344  h Bulk Extractor (40 Points)./"......k....ig....https://github.co
.3065408  m/simsong/bulk_extractor/wikiHome .. simsong/bulk_extractor Wiki
.3065472   .. GitHub./"...:..6.....so....https://www.google.com/search?q=h
.3065536  ow+to+use+bulk+extractor+windows&source=hp&ei=FKi_YJ-EC_G0lwSpir
.3065600  TwDg&iflsig=AINFCbYAAAAAYL-2JBu2krHSDU3u6KS74xL0Gv0hblp6&oq=how+
.3065664  to+use+bulk+ex&gs_lcp=Cgdnd3Mtd216EAMYATICCAAyAggAMgYIABAWEB4yBg
.3065728  gAEBYQHjIGCAAQFhAeMgYIABAWEB4yBggAEBYQHjIGCAAQFhAeMgYIABAWEB5QP1
.3065792  18M2C0SagAcAB4AIABywiIAaFKkgELMy0zLjUuNS4xLjKYAQCgAQGgAQdnd3Mtd2
.3065856  16&sclient=gws-wizhow to use bulk extractor windows - Google Sea
.3065920  rch../"....c.G.....[+....https://accounts.google.com/Logout?hl=e
.3065984  n-GB&continue=https://mail.google.com/mail&service=mail&timeStmp
.3066048  =1623170910&secTok=.AG5fkS_3essW5UwJTDxCGRhVfCi20geCNg&ec=GAdAFw
.3066112  Google Accounts./".iJ..........v....https://mail.google.com/mail
.3066176  /u/0/#inbox/FMfcgzGkXmWhzfblHDGDGhVrTlrNzfQSLinformative message
.3066240   - numbersample7@gmail.com - Gmail./".h|...S...........https://ma
.3066304  il.google.com/accounts/SetOSID?authuser=0&continue=https%3A%2F%2
.3066368  Fmail.google.com%2Fmail%2F%3Ftab%3Dkm%26pli%3D1&osidt=ALWU2csHII
.3066432  uxVC2lpE8UP_30WyNWPAgyZf0Wss6PQxiwMBFOgpz1118SjLtmjEZQrz3e30u7PY
.3066496  iY0TqHM91YY9H0JbZEzvppsRjmY_NaXfPxxz0tI3vflmL3gh68Uv6Cif40Yw3ryu
.3066560  ZyQ7wAN8QVVI_xMBc88s7D2vCuS2uKdIpvvCFJ03rRruf4mMuDjbbWfqt7JiKvwi
.3066624  zUlTr4N6o7eAfrTgQxxdmOGw&ifkv=AU9NCcw4bTgKBAQ8aSb168NMl-03f8nwu6
.3066688  b4cB19kQlvijErcd95RbtTujtgCVvs_8R7YFu_9f-LoA%3D%3D#Gmail./".DZ..
```

Figure 4: Recovered email artifacts using bulk extractor

The “cached-certs”, “cached-microdesc-consensus”, “cached-microdescs” and “cached-microdescs. new” folders in TorBrowser/Browser/TorBrowser/Data/Tor also contain the same artifact. As demonstrated in A, B, and C these files are evaluated in Hex Workshop. Various artifact can assist LEA in tracking down a person using Tor for any criminal behavior through gathering evidence about the user’s browsing activities from these relays. Both memory pictures contained identical traces, indicating that Tor did not remove browsing history of user from memory when the Tor is closed. Tab. 5 presents a detail of all the artifacts discovered in memory about user browsing behaviors. Fig. 7 show screenshots of several of these artefacts. All of these artifacts were discovered using bulk extractor, with the exception of Yahoo and Gmail inbox messages, those are discovered using Hex workshop.



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D   0123456789ABCD
28464A70  2D 2D 2D 2D 2D 42 45 47 49 4E 20 50 55 42  -----BEGIN PUB
28464A7E  4C 49 43 20 4B 45 59 2D 2D 2D 2D 2D 0A 00  LIC KEY-----..
28464A8C  00 00 00 00 2D 2D 2D 2D 2D 45 4E 44 20 50  ....-----END P
28464A9A  55 42 4C 49 43 20 4B 45 59 2D 2D 2D 2D 2D  UBLIC KEY-----
28464AA8  0A 00 2E 2E 2F 2E 2E 2F 63 68 72 6F 6D 65  ..../../chrome
28464AB6  2F 62 72 6F 77 73 65 72 2F 65 6E 74 65 72  /browser/enter
28464AC4  70 72 69 73 65 2F 63 6F 6E 6E 65 63 74 6F  prise/connecto
28464AD2  72 73 2F 64 65 76 69 63 65 5F 74 72 75 73  rs/device_trus
28464AE0  74 2F 73 69 67 6E 61 6C 5F 72 65 70 6F 72  t/signal_repor
28464AEE  74 65 72 2E 63 63 00 46 61 69 6C 65 64 20  ter.cc.Failed
28464AFC  74 6F 20 72 65 74 72 69 65 76 65 20 76 61  to retrieve va
28464B0A  6C 69 64 20 44 4D 20 74 6F 6B 65 6E 00 46  lid DM token.F
28464B18  61 69 6C 65 64 20 74 6F 20 63 72 65 61 74  ailed to creat
28464B26  65 20 72 65 70 6F 72 74 69 6E 67 3A 3A 52  e reporting::R
28464B34  65 70 6F 72 74 51 75 65 75 65 43 6F 6E 66  eportQueueConf
28464B42  69 67 75 72 61 74 69 6F 6E 3A 20 00 3B 20  iguration: .;
```

Data Inspector

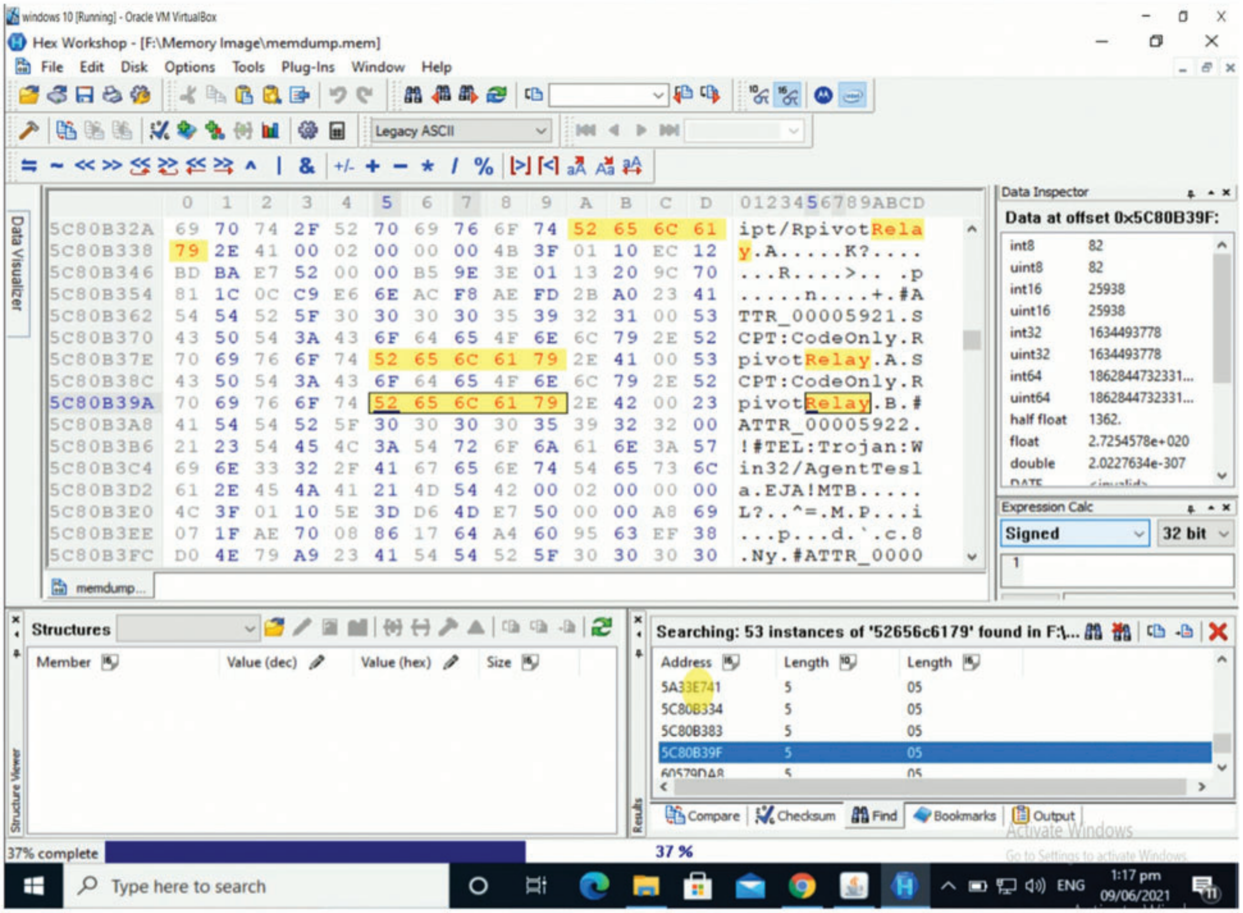
Data at offset 0x28464A99:

int8	80
uint8	80
int16	21840
uint16	21840
int32	1279415632
uint32	1279415632
int64	5413400734190...
uint64	5413400734190...
half float	85.
float	50943296
double	7.7883517e+053
DATE	<invalid>

Searching: 9 instances of '5055424c4943204b4559' ...

Address	Length	Length
13DB876B	10	0A
28334F5B	10	0A
28464A7B	10	0A
28464A99	10	0A
2982DAA6	10	0A

Figure 5: Memory showing public key of tor relay



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D   0123456789ABCD
5C80B32A  69 70 74 2F 52 70 69 76 6F 74 52 65 6C 61  ipt/RpivotRela
5C80B338  79 2E 41 00 02 00 00 00 4B 3F 01 10 EC 12  y.A.....K?....
5C80B346  BD BA E7 52 00 00 B5 9E 3E 01 13 20 9C 70  ...R....>.. .p
5C80B354  81 1C 0C C9 E6 6E AC F8 AE FD 2B A0 23 41  .....n....+.#A
5C80B362  54 54 52 5F 30 30 30 30 35 39 32 31 00 53  TTR_00005921.S
5C80B370  43 50 54 3A 43 6F 64 65 4F 6E 6C 79 2E 52  CPT:CodeOnly.R
5C80B37E  70 69 76 6F 74 52 65 6C 61 79 2E 41 00 53  pivotRelay.A.S
5C80B38C  43 50 54 3A 43 6F 64 65 4F 6E 6C 79 2E 52  CPT:CodeOnly.R
5C80B39A  70 69 76 6F 74 52 65 6C 61 79 2E 42 00 23  pivotRelay.B.#
5C80B3A8  41 54 54 52 5F 30 30 30 30 35 39 32 32 00  ATTR_00005922.
5C80B3B6  21 23 54 45 4C 3A 54 72 6F 6A 61 6E 3A 57  !#TEL:Trojan:W
5C80B3C4  69 6E 33 32 2F 41 67 65 6E 74 54 65 73 6C  in32/AgentTesl
5C80B3D2  61 2E 45 4A 41 21 4D 54 42 00 02 00 00 00  a.EJA!MTB.....
5C80B3E0  4C 3F 01 10 5E 3D D6 4D E7 50 00 00 A8 69  L?..^=.M.P...i
5C80B3EE  07 1F AE 70 08 86 17 64 A4 60 95 63 EF 38  ...p...d.`.c.8
5C80B3FC  D0 4E 79 A9 23 41 54 54 52 5F 30 30 30 30  .Ny.#ATTR_0000
```

Data Inspector

Data at offset 0x5C80B39F:

int8	82
uint8	82
int16	25938
uint16	25938
int32	1634493778
uint32	1634493778
int64	1862844732331...
uint64	1862844732331...
half float	1362.
float	2.7254578e+020
double	2.0227634e-307

Searching: 53 instances of '52656c6179' found in F:\...

Address	Length	Length
5A33E741	5	05
5C80B334	5	05
5C80B383	5	05
5C80B39F	5	05
60579DA8	5	05

Figure 6: Memory showing relay information of Tor

Table 5: Browsing artifact recovered from memory

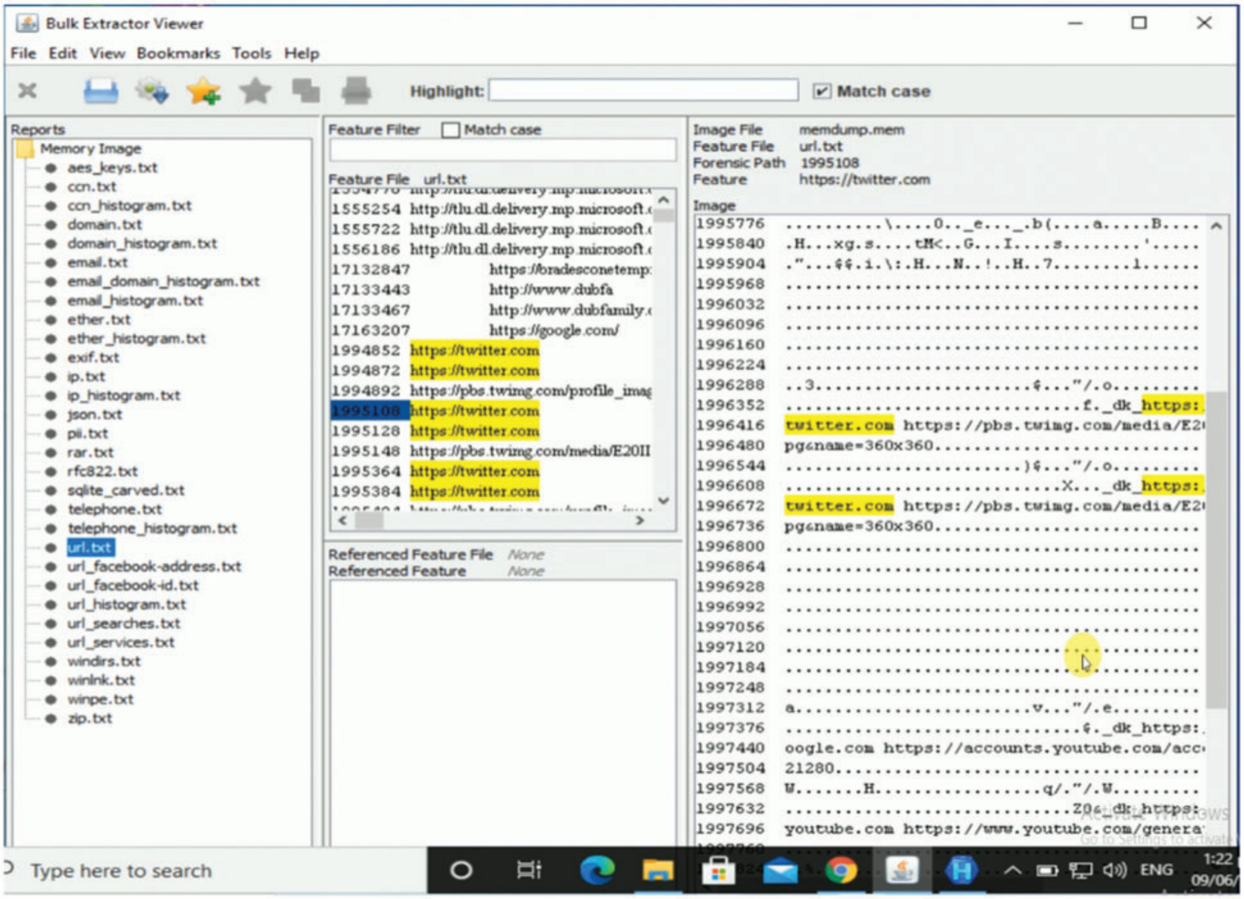
S. No.	Application/data searched	Artifacts found	No artifacts
1	Gmail	All email addresses o Inbox items. o Links to email attachment files	o Sent emails o Attached o Files
2	Google drive	Google drive links: o Links of online read documents o Links to email attachment files	Nil
3	Yahoo mail	All email addresses o Inbox items. o Links to email attachment files	Nil

(Continued)

Table 5: Continued

S. No.	Application/data searched	Artifacts found	No artifacts
4	Twitter	Links of all Twitter visited: o Profile of the user o Link of twitter account Profile	o Profile picture of the user o Followed Links of twitter accounts o Comments o Chat o Liked tweets o Shared tweets
5	Instagram	Links of all Instagram visited: o Profile of the user o Link of Instagram account Profile	o Profile picture of the user o Followed Links of Instagram accounts o Comments o Chat o Liked posts o Shared posts
6	Facebook	All Facebook links visited: o User profile o Profile link of Facebook account. o Keyword searched.	o User profile picture o Comments o Liked posts o Chat o Shared posts
7	Skype	Link of Skype visited.	o Profile picture of the user o Contacts o Chat
8	Youtube	Youtube links visited including o Keyword search o Watched videos	Nil
9	Google maps	Google maps visited o Keyword search o Viewed locations	Nil
10	Research papers	Research paper website visited o Online read pdf research papers.	Nil

The artifacts on the hard disk are analyzed when the browser is open using the Magnet Axiom to examine both the VMDK file of OS and the snapshot VMDK file of the third snapshot. The registry artifact found in these VMDK files are searched using Hex Workshop. The OS VMDK file is supported by Magnet Axiom, however the snapshot VMDK file is not. Using the image conversion method, we convert this VMDK file into EnCase Image File Format, which is supported by Axiom, using FTK imager. To confirm the integrity of converted snapshot VMDK files, hashes were calculated and matched before and after conversion using the FTK imager. FTK imager was also used to construct MD5 and SHA1 hashes for the OS virtual hard drive file. On the OS VMDK file, no Tor artifacts were discovered. This VMDK file was inspected in Hex Workshop for registry artifacts, and various string searches were conducted. In these searches, the strings "firefox.exe % b" and "SIGN.MEDIA = 31C3D37" were used. In the OS VMDK file, there were no registry artifacts. However, as shown in Tab. 6, various artifacts are discovered during the examination of the converted snapshot VMDK file.



☑ Match case

Memory Image
- aes_keys.txt
- ccn.txt
- ccn_histogram.txt
- domain.txt
- domain_histogram.txt
- email.txt
- email_domain_histogram.txt
- email_histogram.txt
- ether.txt
- ether_histogram.txt
- exif.txt
- ip.txt
- ip_histogram.txt
- json.txt
- pii.txt
- rar.txt
- rfc822.txt
- sqlite_carved.txt
- telephone.txt
- telephone_histogram.txt
- url.txt
- url_facebook-address.txt
- url_facebook-id.txt
- url_histogram.txt
- url_searches.txt
- url_services.txt
- windirs.txt
- winlnk.txt
- winpe.txt
- zip.txt

□ Match case

Feature File url.txt

```
1555254 http://tlu.dl.delivery.mp.microsoft.c
1555722 http://tlu.dl.delivery.mp.microsoft.c
1556186 http://tlu.dl.delivery.mp.microsoft.c
17132847          https://bradesconetemp:
17133443          http://www.dubfa
17133467          http://www.dubfamily.c
17163207          https://google.com/
1994852 https://twitter.com
1994872 https://twitter.com
1994892 https://pbs.twimg.com/profile_imag
1995108 https://twitter.com
1995128 https://twitter.com
1995148 https://pbs.twimg.com/media/E20II
1995364 https://twitter.com
1995384 https://twitter.com
```

Referenced Feature File *None*
Referenced Feature *None*

Image File memdump.mem
Feature File url.txt
Forensic Path 1995108
Feature https://twitter.com

Image

```
1995776  ..........\....0.._e..._.b(....a.....B....
1995840  .H...xg.s....tM<..G...I....s........'.....
1995904  ."...$$.i.\:.H...N..!..H..7........l......
1995968  ..........................................
1996032  ..........................................
1996096  ..........................................
1996160  ..........................................
1996224  ..........................................
1996288  ..3.....................$..."/.o.........
1996352  ...............................f._dk_https:
1996416  twitter.com https://pbs.twimg.com/media/E2
1996480  pg&name=360x360...........................
1996544  ........................)$..."/.o.........
1996608  ...........................X..._dk_https:
1996672  twitter.com https://pbs.twimg.com/media/E2
1996736  pg&name=360x360...........................
1996800  ..........................................
1996864  ..........................................
1996928  ..........................................
1996992  ..........................................
1997056  ..........................................
1997120  ..........................................
1997184  ..........................................
1997248  ..........................................
1997312  a.......................v..."/.e.........
1997376  ............................$._dk_https:
1997440  oogle.com https://accounts.youtube.com/acc
1997504  21280.....................................
1997568  W.......H.................q/."/.W.........
1997632  ............................Z0&_dk_https:
1997696  youtube.com https://www.youtube.com/genera
```

Figure 7: Twitter artifacts in memory

Table 6: Tor browser artifacts on Hard Disk

Item	Tor open scenario		Tor closed scenario	
	Vmdk file of OS	Snapshot of converted Vmdk file	Vmdk File of OS	Snapshot of converted Vmdk file
Browsing	No traces	No traces	No traces	No traces

(Continued)

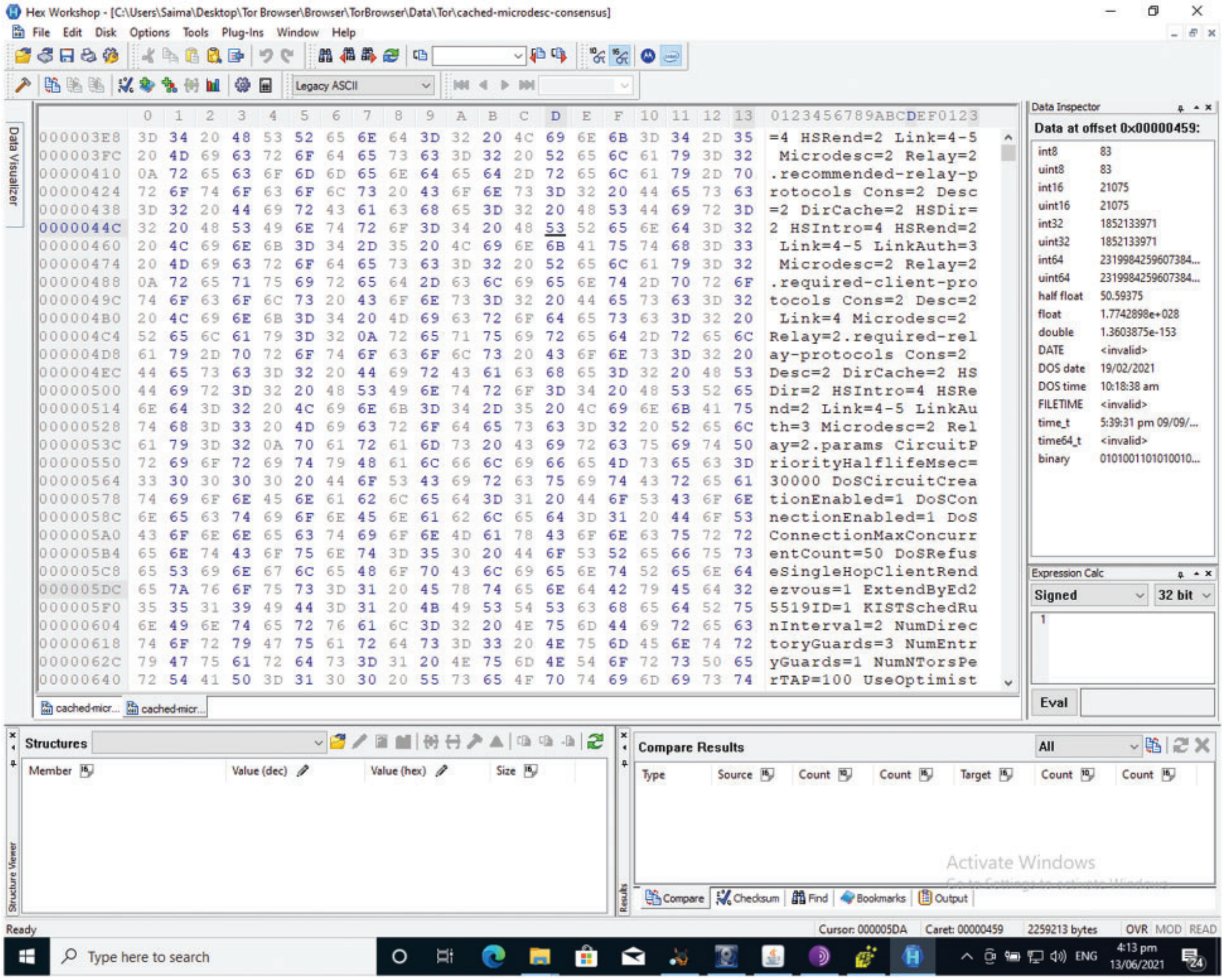
Table 6: Continued

Item	Tor open scenario		Tor closed scenario	
	Vmdk file of OS	Snapshot of converted Vmdk file	Vmdk File of OS	Snapshot of converted Vmdk file
Pictures	-	Icon of tor browser was available in recovered picture Artifacts of browsing activities did not provide any picture and videos	-	No artifacts
Downloads	-	All downloads like pictures, torrent file were available	-	No artifacts
Operating system	-	Only location of tor is available.	-	Only location of Tor is available.
Registry artifacts	-	Two registry key were recovered.	-	Two registry key were recovered.

Magnet Axiom discovered artifacts that contained all of the download data. Torrent files are displayed as peer-to-peer artefacts, whereas downloaded photos were displayed as media artefacts. Apart from downloaded images, Axiom found a plethora of other photographs from the OS's internal application. The Tor browser icon could also be seen in the photos, showing that Tor had been installed on the device. There was no other instance under the OS artefacts except for firefox.exe. During the collection of artifacts various artifacts of Tor browser regarding relays information has been recovered. This information is very useful in scenarios where back tracking is essentially required. This is done by obtaining the address of next node. Several artifacts recovered from Tor Browser are presented below as additional artifacts.

This artifact is collected when the Tor Browser is open. "**cached-cert**" file located in Tor browser folder at Desktop was loaded in Hex workshop. The file contains public key of Tor Browser. This artifact is collected when the Tor Browser is open. "**cached-microdesc.new**" file located in Tor browser folder at Desktop was loaded in Hex workshop. The file contains public key of Tor Relay as shown in Figs. 8–10. This artifact was collected when the Tor Browser is open. "**cached-microdesc-consensus**" file located in Tor browser folder at Desktop was loaded in Hex workshop. The file contains Relays information of Tor Browser.

Various researches have been performed for the analysis of security and privacy of Tor browser [25]. A few researches are found on the topic and detailed comparison of research is shown in Tab. 7. In a research where windows 7 platform is used for analysis of Tor browser [26]. Only memory was considered for obtaining artefacts for finding traces of Tor. Moreover, platform used was outdated. Whereas in our research many important artefacts were recovered from registry and hard disk as well as analysis performed on windows 10. Another research comprises on the analysis of user browsing artefacts from memory was presented [27]. Authors also confirmed that Tor remove all of its artefacts from memory when it is closed. Where our results shows that Tor leaves artefact while it is closed. Analysis of registry and hard disk is also missing. A research performed on windows 10 presented analysis over windows 10 [28]. But major drawback was no browser artefacts were collected and analysis performed [29]. Another major findings of our research is tracing relays information from hard disk and memory. The relays information will be useful in backtracking process. No previous research on recover relay information of Tor forensic. Browsing artefacts are also recovered in previous research from our dated windows. Our research is capable of collecting browsing artefacts from memory and hard disk running OS windows 10.



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13  0123456789ABCDEF0123
000003E8  3D 34 20 48 53 52 65 6E 64 3D 32 20 4C 69 6E 6B 3D 34 2D 35  =4 HSRend=2 Link=4-5
000003FC  20 4D 69 63 72 6F 64 65 73 63 3D 32 20 52 65 6C 61 79 3D 32   Microdesc=2 Relay=2
00000410  0A 72 65 63 6F 6D 6D 65 6E 64 65 64 2D 72 65 6C 61 79 2D 70  .recommended-relay-p
00000424  72 6F 74 6F 63 6F 6C 73 20 43 6F 6E 73 3D 32 20 44 65 73 63  rotocols Cons=2 Desc
00000438  3D 32 20 44 69 72 43 61 63 68 65 3D 32 20 48 53 44 69 72 3D  =2 DirCache=2 HSDir=
0000044C  32 20 48 53 49 6E 74 72 6F 3D 34 20 48 53 52 65 6E 64 3D 32  2 HSIntro=4 HSRend=2
00000460  20 4C 69 6E 6B 3D 34 2D 35 20 4C 69 6E 6B 41 75 74 68 3D 33   Link=4-5 LinkAuth=3
00000474  20 4D 69 63 72 6F 64 65 73 63 3D 32 20 52 65 6C 61 79 3D 32   Microdesc=2 Relay=2
00000488  0A 72 65 71 75 69 72 65 64 2D 63 6C 69 65 6E 74 2D 70 72 6F  .required-client-pro
0000049C  74 6F 63 6F 6C 73 20 43 6F 6E 73 3D 32 20 44 65 73 63 3D 32  tocols Cons=2 Desc=2
000004B0  20 4C 69 6E 6B 3D 34 20 4D 69 63 72 6F 64 65 73 63 3D 32 20   Link=4 Microdesc=2
000004C4  52 65 6C 61 79 3D 32 0A 72 65 71 75 69 72 65 64 2D 72 65 6C  Relay=2.required-rel
000004D8  61 79 2D 70 72 6F 74 6F 63 6F 6C 73 20 43 6F 6E 73 3D 32 20  ay-protocols Cons=2
000004EC  44 65 73 63 3D 32 20 44 69 72 43 61 63 68 65 3D 32 20 48 53  Desc=2 DirCache=2 HS
00000500  44 69 72 3D 32 20 48 53 49 6E 74 72 6F 3D 34 20 48 53 52 65  Dir=2 HSIntro=4 HSRe
00000514  6E 64 3D 32 20 4C 69 6E 6B 3D 34 2D 35 20 4C 69 6E 6B 41 75  nd=2 Link=4-5 LinkAu
00000528  74 68 3D 33 20 4D 69 63 72 6F 64 65 73 63 3D 32 20 52 65 6C  th=3 Microdesc=2 Rel
0000053C  61 79 3D 32 0A 70 61 72 61 6D 73 20 43 69 72 63 75 69 74 50  ay=2.params CircuitP
00000550  72 69 6F 72 69 74 79 48 61 6C 66 6C 69 66 65 4D 73 65 63 3D  riorityHalflifeMsec=
00000564  33 30 30 30 30 20 44 6F 53 43 69 72 63 75 69 74 43 72 65 61  30000 DoSCircuitCrea
00000578  74 69 6F 6E 45 6E 61 62 6C 65 64 3D 31 20 44 6F 53 43 6F 6E  tionEnabled=1 DoSCon
0000058C  6E 65 63 74 69 6F 6E 45 6E 61 62 6C 65 64 3D 31 20 44 6F 53  nectionEnabled=1 DoS
000005A0  43 6F 6E 6E 65 63 74 69 6F 6E 4D 61 78 43 6F 6E 63 75 72 72  ConnectionMaxConcurr
000005B4  65 6E 74 43 6F 75 6E 74 3D 35 30 20 44 6F 53 52 65 66 75 73  entCount=50 DoSRefus
000005C8  65 53 69 6E 67 6C 65 48 6F 70 43 6C 69 65 6E 74 52 65 6E 64  eSingleHopClientRend
000005DC  65 7A 76 6F 75 73 3D 31 20 45 78 74 65 6E 64 42 79 45 64 32  ezvous=1 ExtendByEd2
000005F0  35 35 31 39 49 44 3D 31 20 4B 49 53 54 53 63 68 65 64 52 75  5519ID=1 KISTSchedRu
00000604  6E 49 6E 74 65 72 76 61 6C 3D 32 20 4E 75 6D 44 69 72 65 63  nInterval=2 NumDirec
00000618  74 6F 72 79 47 75 61 72 64 73 3D 33 20 4E 75 6D 45 6E 74 72  toryGuards=3 NumEntr
0000062C  79 47 75 61 72 64 73 3D 31 20 4E 75 6D 4E 54 6F 72 73 50 65  yGuards=1 NumNTorsPe
00000640  72 54 41 50 3D 31 30 30 20 55 73 65 4F 70 74 69 6D 69 73 74  rTAP=100 UseOptimist
```

Data Inspector

Data at offset 0x00000459:

int8	83
uint8	83
int16	21075
uint16	21075
int32	1852133971
uint32	1852133971
int64	2319984259607384...
uint64	2319984259607384...
half float	50.59375
float	1.7742898e+028
double	1.3603875e-153
DATE	<invalid>
DOS date	19/02/2021
DOS time	10:18:38 am
FILETIME	<invalid>
time_t	5:39:31 pm 09/09/...
time64_t	<invalid>
binary	0101001101010010...

Expression Calc

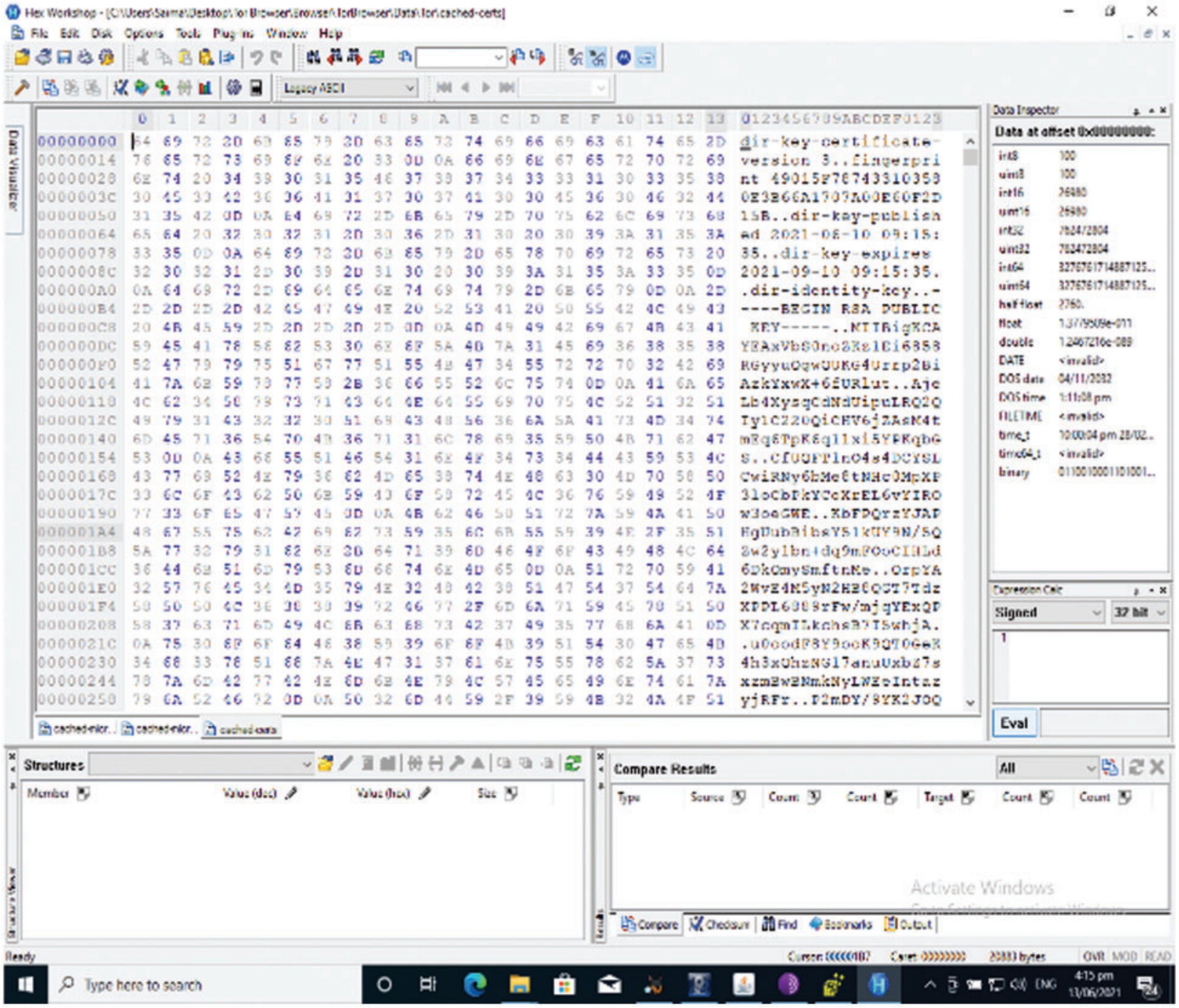
Signed 32 bit

1

Eval

Ready Cursor: 000005DA Caret: 00000459 2259213 bytes OVR MOD READ

Figure 8: Cached-microdesc-consensus file contains relay information


Hex Workshop - [C:\Users\Saima\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\cached-certs]
File Edit Disk Options Tools Plug-ins Window Help
Legacy ASCII
Data Visualizer
cached-micr... cached-micr... cached-certs
Structures
Member Value (dec) Value (hex) Size
Compare Results
All
Type Source Count Count Target Count Count
Compare Checksum Find Bookmarks Output
Ready
Type here to search
4:15 pm 13/06/2021

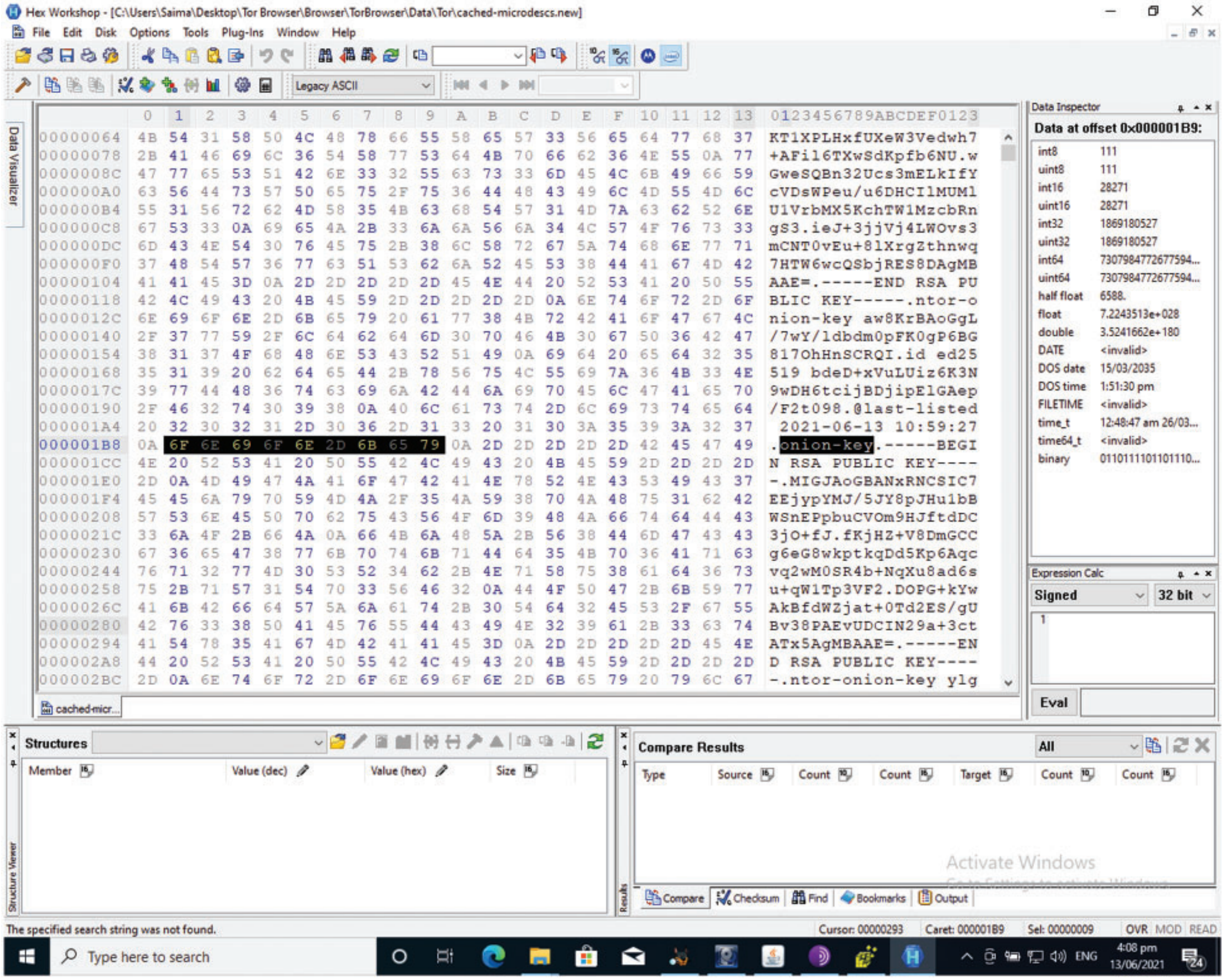
```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13  0123456789ABCDEF0123
00000000  64 69 72 2D 6B 65 79 2D 63 65 72 74 69 66 69 63 61 74 65 2D  dir-key-certificate-
00000014  76 65 72 73 69 6F 6E 20 33 0D 0A 66 69 6E 67 65 72 70 72 69  version 3..fingerpri
00000028  6E 74 20 34 39 30 31 35 46 37 38 37 34 33 33 31 30 33 35 38  nt 49015F78743310358
0000003C  30 45 33 42 36 36 41 31 37 30 37 41 30 30 45 36 30 46 32 44  0E3B66A1707A00E60F2D
00000050  31 35 42 0D 0A 64 69 72 2D 6B 65 79 2D 70 75 62 6C 69 73 68  15B..dir-key-publish
00000064  65 64 20 32 30 32 31 2D 30 36 2D 31 30 20 30 39 3A 31 35 3A  ed 2021-06-10 09:15:
00000078  33 35 0D 0A 64 69 72 2D 6B 65 79 2D 65 78 70 69 72 65 73 20  35..dir-key-expires 
0000008C  32 30 32 31 2D 30 39 2D 31 30 20 30 39 3A 31 35 3A 33 35 0D  2021-09-10 09:15:35.
000000A0  0A 64 69 72 2D 69 64 65 6E 74 69 74 79 2D 6B 65 79 0D 0A 2D  .dir-identity-key..-
000000B4  2D 2D 2D 2D 42 45 47 49 4E 20 52 53 41 20 50 55 42 4C 49 43  ----BEGIN RSA PUBLIC
000000C8  20 4B 45 59 2D 2D 2D 2D 2D 0D 0A 4D 49 49 42 69 67 4B 43 41   KEY-----..MIIBigKCA
000000DC  59 45 41 78 56 62 53 30 6E 6F 5A 4B 7A 31 45 69 36 38 35 38  YEAxVbS0noZKz1Ei6858
000000F0  52 47 79 79 75 51 67 77 51 55 4B 47 34 55 72 72 70 32 42 69  RGyyuQgwQUKG4Urrp2Bi
00000104  41 7A 6B 59 78 77 58 2B 36 66 55 52 6C 75 74 0D 0A 41 6A 65  AzkYxwX+6fURlut..Aje
00000118  4C 62 34 58 79 73 71 43 64 4E 64 55 69 70 75 4C 52 51 32 51  Lb4XysqCdNdUipuLRQ2Q
0000012C  54 79 31 43 32 32 30 51 69 43 48 56 36 6A 5A 41 73 4D 34 74  Ty1C220QiCHV6jZAsM4t
00000140  6D 45 71 36 54 70 4B 36 71 31 6C 78 69 35 59 50 4B 71 62 47  mEq6TpK6q1lxi5YPKqbG
00000154  53 0D 0A 43 66 55 51 46 54 31 6E 4F 34 73 34 44 43 59 53 4C  S..CfUQFT1nO4s4DCYSL
00000168  43 77 69 52 4E 79 36 62 4D 65 38 74 4E 48 63 30 4D 70 58 50  CwiRNy6bMe8tNHc0MpXP
0000017C  33 6C 6F 43 62 50 6B 59 43 6F 58 72 45 4C 36 76 59 49 52 4F  3loCbPkYCoXrEL6vYIRO
00000190  77 33 6F 65 47 57 45 0D 0A 4B 62 46 50 51 72 7A 59 4A 41 50  w3oeGWE..KbFPQrzYJAP
000001A4  48 67 55 75 62 42 69 62 73 59 35 6C 6B 55 59 39 4E 2F 35 51  HgUubBibsY5lkUY9N/5Q
000001B8  5A 77 32 79 31 62 6E 2B 64 71 39 6D 46 4F 6F 43 49 48 4C 64  Zw2y1bn+dq9mFOoCIHLd
000001CC  36 44 6B 51 6D 79 53 6D 66 74 6E 4D 65 0D 0A 51 72 70 59 41  6DkQmySmftnMe..QrpYA
000001E0  32 57 76 45 34 4D 35 79 4E 32 48 42 38 51 47 54 37 54 64 7A  2WvE4M5yN2HB8QGT7Tdz
000001F4  58 50 50 4C 36 38 38 39 72 46 77 2F 6D 6A 71 59 45 78 51 50  XPPL6889rFw/mjqYExQP
00000208  58 37 63 71 6D 49 4C 6B 63 68 73 42 37 49 35 77 68 6A 41 0D  X7cqmILkchsB7I5whjA.
0000021C  0A 75 30 6F 6F 64 46 38 59 39 6F 6F 4B 39 51 54 30 47 65 4D  .u0oodF8Y9ooK9QT0GeM
00000230  34 68 33 78 51 68 7A 4E 47 31 37 61 6E 75 55 78 62 5A 37 73  4h3xQhzNG17anuUxbZ7s
00000244  78 7A 6D 42 77 42 4E 6D 6B 4E 79 4C 57 45 65 49 6E 74 61 7A  xzmBwBNmkNyLWEeIntaz
00000258  79 6A 52 46 72 0D 0A 50 32 6D 44 59 2F 39 59 4B 32 4A 4F 51  yjRFr..P2mDY/9YK2JOQ
```

```
Data Inspector
Data at offset 0x00000000:
int8       100
uint8      100
int16      26980
uint16     26980
int32      762472804
uint32     762472804
int64      3276761714887125...
uint64     3276761714887125...
half float 2760.
float      1.3779598e-011
double     1.2467216e-089
DATE       <invalid>
DOS date   04/11/2032
DOS time   1:11:08 pm
FILETIME   <invalid>
time_t     10:00:04 pm 28/02...
time64_t   <invalid>
binary     0110010001101001...
```

```
Expression Calc
Signed   32 bit
1
Eval
```

```
Cursor: 00000107   Caret: 00000000   20883 bytes   OVR MOD READ
```

Figure 9: Cached-cert file finds public keys of tor relay



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13  0123456789ABCDEF0123
00000064  4B 54 31 58 50 4C 48 78 66 55 58 65 57 33 56 65 64 77 68 37  KT1XPLHxfUXeW3Vedwh7
00000078  2B 41 46 69 6C 36 54 58 77 53 64 4B 70 66 62 36 4E 55 0A 77  +AFil6TXwSdKpfb6NU.w
0000008C  47 77 65 53 51 42 6E 33 32 55 63 73 33 6D 45 4C 6B 49 66 59  GweSQBn32Ucs3mELkIfY
000000A0  63 56 44 73 57 50 65 75 2F 75 36 44 48 43 49 6C 4D 55 4D 6C  cVDsWPeu/u6DHCIlMUMl
000000B4  55 31 56 72 62 4D 58 35 4B 63 68 54 57 31 4D 7A 63 62 52 6E  U1VrbMX5KchTW1MzcbRn
000000C8  67 53 33 0A 69 65 4A 2B 33 6A 6A 56 6A 34 4C 57 4F 76 73 33  gS3.ieJ+3jjVj4LWOvs3
000000DC  6D 43 4E 54 30 76 45 75 2B 38 6C 58 72 67 5A 74 68 6E 77 71  mCNT0vEu+8lXrgZthnwq
000000F0  37 48 54 57 36 77 63 51 53 62 6A 52 45 53 38 44 41 67 4D 42  7HTW6wcQSbjRES8DAgMB
00000104  41 41 45 3D 0A 2D 2D 2D 2D 2D 45 4E 44 20 52 53 41 20 50 55  AAE=.-----END RSA PU
00000118  42 4C 49 43 20 4B 45 59 2D 2D 2D 2D 2D 0A 6E 74 6F 72 2D 6F  BLIC KEY-----.ntor-o
0000012C  6E 69 6F 6E 2D 6B 65 79 20 61 77 38 4B 72 42 41 6F 47 67 4C  nion-key aw8KrBAoGgL
00000140  2F 37 77 59 2F 6C 64 62 64 6D 30 70 46 4B 30 67 50 36 42 47  /7wY/ldbdm0pFK0gP6BG
00000154  38 31 37 4F 68 48 6E 53 43 52 51 49 0A 69 64 20 65 64 32 35  817OhHnSCRQI.id ed25
00000168  35 31 39 20 62 64 65 44 2B 78 56 75 4C 55 69 7A 36 4B 33 4E  519 bdeD+xVuLUiz6K3N
0000017C  39 77 44 48 36 74 63 69 6A 42 44 6A 69 70 45 6C 47 41 65 70  9wDH6tcijBDjipElGAep
00000190  2F 46 32 74 30 39 38 0A 40 6C 61 73 74 2D 6C 69 73 74 65 64  /F2t098.@last-listed
000001A4  20 32 30 32 31 2D 30 36 2D 31 33 20 31 30 3A 35 39 3A 32 37   2021-06-13 10:59:27
000001B8  0A 6F 6E 69 6F 6E 2D 6B 65 79 0A 2D 2D 2D 2D 2D 42 45 47 49  .onion-key.-----BEGI
000001CC  4E 20 52 53 41 20 50 55 42 4C 49 43 20 4B 45 59 2D 2D 2D 2D  N RSA PUBLIC KEY----
000001E0  2D 0A 4D 49 47 4A 41 6F 47 42 41 4E 78 52 4E 43 53 49 43 37  -.MIGJAoGBANxRNCSIC7
000001F4  45 45 6A 79 70 59 4D 4A 2F 35 4A 59 38 70 4A 48 75 31 62 42  EEjypYMJ/5JY8pJHu1bB
00000208  57 53 6E 45 50 70 62 75 43 56 4F 6D 39 48 4A 66 74 64 44 43  WSnEPpbuCVOm9HJftdDC
0000021C  33 6A 4F 2B 66 4A 0A 66 4B 6A 48 5A 2B 56 38 44 6D 47 43 43  3jO+fJ.fKjHZ+V8DmGCC
00000230  67 36 65 47 38 77 6B 70 74 6B 71 44 64 35 4B 70 36 41 71 63  g6eG8wkptkqDd5Kp6Aqc
00000244  76 71 32 77 4D 30 53 52 34 62 2B 4E 71 58 75 38 61 64 36 73  vq2wM0SR4b+NqXu8ad6s
00000258  75 2B 71 57 31 54 70 33 56 46 32 0A 44 4F 50 47 2B 6B 59 77  u+qW1Tp3VF2.DOPG+kYw
0000026C  41 6B 42 66 64 57 5A 6A 61 74 2B 30 54 64 32 45 53 2F 67 55  AkBfdWZjat+0Td2ES/gU
00000280  42 76 33 38 50 41 45 76 55 44 43 49 4E 32 39 61 2B 33 63 74  Bv38PAEvUDCIN29a+3ct
00000294  41 54 78 35 41 67 4D 42 41 41 45 3D 0A 2D 2D 2D 2D 2D 45 4E  ATx5AgMBAAE=.-----EN
000002A8  44 20 52 53 41 20 50 55 42 4C 49 43 20 4B 45 59 2D 2D 2D 2D  D RSA PUBLIC KEY----
000002BC  2D 0A 6E 74 6F 72 2D 6F 6E 69 6F 6E 2D 6B 65 79 20 79 6C 67  -.ntor-onion-key ylg
```

Data Inspector

Data at offset 0x000001B9:

int8	111
uint8	111
int16	28271
uint16	28271
int32	1869180527
uint32	1869180527
int64	7307984772677594...
uint64	7307984772677594...
half float	6588.
float	7.2243513e+028
double	3.5241662e+180
DATE	<invalid>
DOS date	15/03/2035
DOS time	1:51:30 pm
FILETIME	<invalid>
time_t	12:48:47 am 26/03...
time64_t	<invalid>
binary	0110111101101110...

Expression Calc

Signed 32 bit

1

Eval

The specified search string was not found.

Cursor: 00000293 Caret: 000001B9 Sel: 00000009 OVR MOD READ

Figure 10: Cached-microdesc.new file searches public key of tor relay

Table 7: Research comparison

Research paper	Registry evidences	Memory evidences	Hard disk evidences	Network evidences
Forensic analysis of i2p browser on windows 10 to trace anonymous attacks of P2P networks reflecting IoT models	Yes	Yes	Yes	Partial evidence
Tor browser artefacts in windows 10 (2021)	Partial evidence	Partial evidence	Partial evidence	No

(Continued)

Table 7: Continued

Research paper	Registry evidences	Memory evidences	Hard disk evidences	Network evidences
Forensic analysis of tor browser bundle (2020)	Yes	Partial evidence	No	No
On the memory artefacts of the tor browser bundle (2019)	No	Partial evidence	No	No

5 Conclusion

The forensic study of the Tor browser on Windows 10 is presented in this study. We observed the registry of the system, RAM and HDD for any traces that the Tor left on the user's system when it's open and when it's closed. We were looking for evidence of installation of Tor, use, and browsing behaviors. The findings of the research reveal that the Tor leaves several artifacts on the user's computer, particularly in the system memory. By using different open source tools, all the necessary and sufficient available artifacts of the Tor browser were collected and analyzed. Network forensics is an essential component of any digital inquiry. The Tor browser's network forensics is an area of interest for future research. This will aid in understanding the browser's forensic behavior. We're especially curious about the forensics of Orfox, the browser used for Android devices. Another app runs on Android that acts as a Tor proxy is Orbot. Our future research aims also involve forensic investigation of this application.

Acknowledgement: This research is ongoing research supported by Yayasan Universiti Teknologi PETRONAS Grant Scheme; 015LC0029 and 015LC0277.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Mani, T. Wilson-Brown, R. Jansen and A. Jhonson, "Understanding tor usage with privacy-preserving measurement," *The Internet Measurement Conference (IMC'18)*, Boston MA USA, pp. 175–187, 2018.

[2] The Tor Project, 2021. [Online]. Available: https://metrics.torproject.org/userstats-relay-table.html.

[3] M. Wilson and B. Bazli, "Forensic analysis of I2P activities," in *22nd International Conference on Automation and Computing (ICAC)*, Colchester, UK, pp. 529–534, 2016.

[4] Digital Forensics: What Is It in 2021—2022?, 2021. [Online], Avialable: https://recfaces.com/articles/digital-forensics.

[5] C. Cilleruelo, L. de-Marcos, J. Junquera-Sanchez and J. Martinez-Herraiz, "Interconnection between darknets," *IEEE Internet Computing*, vol. 25, no. 3, pp. 61–70, 2021.

[6] S. Jo, J. Lee, J. Han and S. Ghose, "P2p computing for intelligence of things," *Peer-to-Peer Networking and Applications*, vol. 13, pp. 575–578, 2020.

[7] A. Rasool and Z. Jalil, "Review of web browser forensic analysis," *Researchpedia Journal of Computing*, vol. 1, no. 1, pp. 15–21, 2020.

[8] A. K. Jadoon, W. Iqbal, M. F. Amjad, H. Afzal and Y. A. Bangash, "Forensic analysis of tor browser: A case study for privacy and anonymity on the web," *Forensic Science International*, vol. 299, pp. 59–73, 2019.

[9] G. Horsman, B. Findlay, J. Edwick, A. Asquith, K. Swannell *et al.,* "A forensic examination of web browser privacy-modes," in *Forensic Science International: Reports*, vol. 1, pp. 100036, Elsevier, Netherlands, 2019.

[10] N. Shafqat, "Forensic investigation of user's web activity on Google chrome using various forensic tools," *International Journal of Computer Science and Network Security*, vol. 16, no. 9, pp. 123–132, 2016.

[11] R. Umar, A. Yudhana and M. N. Faiz, "Experimental analysis of web browser sessions using live forensics method," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 5, pp. 2951–2958, 2018.

[12] S. Soney, C. Balan, P. P. Sajan and E. R. Lalson, "I2p forensic analysis," *International Journal of Recent Technology and Engineering*, vol. 8, no. 6, pp. 1678–1682, 2020.

[13] E. Qawasmeh, M. I. AlSaleh and Z. A. AlSharif, "Towards a generic approach for memory forensic," in *IEEE 6th HCT Information Technology Trends (ITT)*, United Arab Emirates, 2019.

[14] H. Yin and Y. He, "I2p anonymous traffic detection and identification," in *5th Int. Conf. on Advanced Computing & Communication Systems (ICACCS)*, India, 2019.

[15] B. Bazli, M. Wilson and W. Hurst, "The dark side of I2P: A forensic analysis case study," *Systems Science & Control Engineering*, vol. 5, no. 1, pp. 278–286, 2017.

[16] Y. Yang, L. Yang, M. Yang, H. Yu, G. Zhu *et al.,* "Dark-web forum correlation analysis research," in *IEEE 8th Joint Int. Information Technology and Artificial Intelligence Conf. (ITAIC)*, China, 2019.

[17] B. D. Carrier and J. Grand, "A hardware–based memory acquisition procedure for digital investigations," *Digital Ivestigation*, vol. 1, no. 1, pp. 50–60, 2004.

[18] R. Magan-Carri, A. A. Galera, G. M. Fernandez and P. G. Teodoro, "Unveiling the I2P web structure: A connectivity analysis," *Computer Networks*, vol. 194, pp. 108158, 2021.

[19] D. Dayalamurthy, "Forensic memory dump analysis and recovery of the artefacts of using tor bundle browser–the need," in *11th Australian Conf. on Digital Forensic*, Australia, 2013.

[20] E. Erdin, C. Zachor and M. H. Gunes, "How to find hidden users: A survey of attacks on anonymity networks," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2296–2316, 2015.

[21] Z. A. Al Sharif, H. Bagci and A. Asad, "Towards the memory forensics of MS-Word documents," in *Advances in Intelligent Systems and Computing*, Springer, Singapore, pp. 179–185, 2018.

[22] M. I. Al Saleh, Z. A. Al Sharif and L. Alawneh, "Network reconnaissance investigation: A memory forensics approach," in *IEEE 10th Int. Conf. on Information and Communication Systems (ICICS)*, Jordan, pp. 36–40, 2019.

[23] A. Ali, M. Khan, M. Saddique, U. Pirzada, M. Zohaib *et al.,* "Tor vs I2P: A comparative study," in *IEEE Int. Conf. on Industrial Technology (ICIT)*, Taiwan, pp. 1748–1751, 2016.

[24] J. P. I. Chrisment and O. Festor, "A bird's eye view on the I2P anonymous file-sharing environment," in *Int. Conf. on Network and System Security*, Tianjin, China, Springer, pp. 135–148, 2012.

[25] W. Darcie, R. Boggs, J. Sammons and T. Fenger, "Online anonymity: Forensic analysis of the tor browser bundle," *Forensic Science International*, USA, 2014.

[26] S. Soltani and S. A. H. Seno, "A survey on digital evidence collection and analysis," in *7th Internation Conf. on Computer and Knowledge Engineering (ICCKE)*, Iran, 2017.

[27] T. Bakhshi, "Forensic of things: Revisiting digital forensic investigation in internet of things," in *IEEE Int. Conf. on Emerging Trends in Engineering, Sciences and Technology (ICEEST)*, Pakistan, 2019.

[28] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and K. Markakis, "A survey on the internet of things (IoT) forensics: Challenges, approaches and open issues," *IEEE Communicaation Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[29] G. Surange, Z. A. Al Sharif and P. Khatri, "IoT forensics: A review on current trends, approaches and foreseen challenges," in *8th Int. Conf. on Computing for Sustainable Global Development*, India, 2021.