



Master Thesis

Network Forensics, 60 credits

Dark Web Forensics

An Investigation of Tor and I2P Artifacts on Windows 11.

Thesis in Digital Forensics, 15 credits

Halmstad, 17th May 2024
Seyedhesam Abolghesami
Chukwudalu Chukwuneta



Abstract

With the rising use of the Internet by businesses and individuals for their regular activities and transactions, there has been increased attention to user privacy and data security on the web. While the adoption of dark web networks has ensured that users' privacy and anonymity concerns are being addressed, there has also been a consequential increase in illicit activities on the internet. The dark web remains a critical area for law enforcement investigations, providing a platform for criminal activities to thrive unchecked. This study evaluates the digital traces deposited by dark web browsers on the client side of user devices, providing a deep insight into the security features of Tor and I2P and outlining the potential areas where digital artifacts can be retrieved on a Windows 11 computer. By detailing the forensic acquisition process and subsequent artifact analysis, this research aims to enhance the capabilities of digital forensic examiners in tracking and prosecuting cybercriminals, thereby contributing to the broader field of digital forensics and cybersecurity.

Keywords: Digital Forensics, Tor, I2P, Dark Web, Privacy, Anonymity, Windows 11, Browser Forensics.

Abbreviations

Tor

The Onion Router

I2P

Invisible Internet Project

VM

Virtual Machine

FTK

Forensic Tool Kit

PID

Process Identity

IP

Internet Protocol

IPv4

Internet Protocol Version 4

IPv6

Internet Protocol Version 6

TCP

Transmission Control Protocol

TCPv4

Transmission Control Protocol Version 4

TCPv6

Transmission Control Protocol Version 6

UDP

User Datagram Protocol

UDPv4

User Datagram Protocol Version 4

UDPv6

User Datagram Protocol Version 6

URL

Uniform Resource Locator

Acknowledgment

The authors would like to thank Mark Sebastian Dougherty, Professor in information technology, for his excellent and extensive guidance. We also appreciate Pablo Picazo-Sanchez, Associate Senior Lecturer at Halmstad University, for his support and deep insight. Lastly, big thanks to our families for their understanding and support throughout the period of this research, most especially to Hassan Abolghasemi.

Table of Contents

1. Introduction.....	1
2. Literature Review.....	3
2.1. Forensic Investigation / Digital Forensics.....	3
2.2. Tor Overview	4
2.3. I2P Overview.....	5
2.4. Related Work.....	7
3. Problem Statement	1
3.1. Research Questions	2
3.2. Scope	2
4. Methodology	3
4.1. Tools.....	4
4.2. Data Acquisition.....	5
4.3. Browsing Activity	5
5. Results.....	10
5.1. Registry	10
5.1.1. Tor Registry	11
5.1.2. I2P Registry	13
5.2. Memory	15
5.2.1. Tor Browser Only	16
5.2.2. I2P Browser Only	17
5.2.3. Tor Browsing Open.....	17
5.2.4. I2P Browsing Open.....	18
5.2.5. Tor Browsing Closed	19
5.2.6. I2P Browsing Closed	20
5.3. Storage.....	23
5.3.1. Tor Browser Open.....	24
5.3.2. I2P Browser Open.....	25
5.3.3. Tor Browser Closed	26
5.3.4. I2P Browser Closed	26
5.3.5. Tor Browser Uninstalled.....	26
5.3.6. I2P Browser Uninstalled	27
6. Discussion	29
7. Conclusion	31

7.1. Future Work	31
References	32
Appendix	35

List of Figures

Fig 1. Illustration of the Tor Onion Routing.....	5
Fig 2. Illustration of the communication between I2P peers.	6
Fig 3. Forensic Acquisition and Analysis Process.....	4
Fig 4. Data acquisition workflow.....	8
Fig 5. Tor browser only public key artifact used by Tor for encrypted communication with nodes with the Tor network retrieved with Hex Workshop.....	44
Fig 6. Tor browser only relay node artifacts showing the IP address, ports, bandwidth, and other details used to build the Tor overlay network, retrieved with Hex Workshop.	44
Fig 7. Tor browser only Volatility netscan artifacts showing tor.exe process listening over ports 9150 and 9151	44
Fig 8. Tor browser only Volatility pstree artifacts showing tor.exe and firefox.exe processes, their parent PIDs, commands, and paths.	45
Fig 9. Tor browser only Volatility pslist artifacts listing tor.exe and firefox.exe processes, their Parent PIDs, and creation time.....	45
Fig 10. I2P browser only string-search for the inbound tunnel, which returned no artifact in Hex Workshop.	46
Fig 11. I2P browser only Volatility pslist artifacts showing i2p.exe, javaw.exe and firefox.exe processes.	46
Fig 12. I2P browser only Volatility pstree artifacts showing i2p.exe, javaw.exe, and firefox.exe processes, their parent PIDs, commands, and paths.	47
Fig 13. I2P browser-only Volatility netscan artifacts listing i2p.exe, javaw.exe, and firefox.exe processes, their Parent PIDs, and creation time.	48
Fig 14. tor.exe prefetch file showing the installation path, usage count, and timestamps from the Tor browser open scenario.	49
Fig 15. Tor installer prefetch file from the Tor browser open scenario showing the usage count, and timestamps but no information on the file path.....	50
Fig 16. The cached-cert file recovered from the slack storage in the Tor browser open scenario shows the encryption keys used by the Tor application.....	51
Fig 17. i2p.exe prefetch file showing the installation path, usage count, and timestamps from the I2P browser open scenario.	52
Fig 18. I2P installer prefetch file from the I2P browser open scenario showing the file path, usage count, and timestamps.....	53
Fig 19. I2psnark folder containing forensic artifacts from the browsing activities after the I2P uninstallation.....	53

List of Tables

Table 1. Summary of related works on dark web forensics.....	1
Table 2. Tools used for the experiment.....	5
Table 3. Summary of browsing activity.....	9
Table 4. Registry keys created by the Tor browser installation.....	12
Table 5. Existing registry keys affected by the Tor browser installation.	12
Table 6. Existing registry keys affected by the I2P installation.....	14
Table 7. Existing registry keys whose data were modified by the I2P installation.....	15
Table 8. Volatility plugins used for memory analysis.	16
Table 9. A summary of the forensic artifacts found in the memory.	22
Table 10. A summary of the forensic artifacts found in the storage.....	28
Table 11. A summary of forensic artifacts that can be retrieved from devices communicating over Tor/ I2P and where they can be found.	30
Table 12. All registry keys and value entries made by the installation of Tor	38
Table 13. All registry keys and value entries made by the installation and configuration of I2P.	43

1. Introduction

The Dark Web is a hidden part of the internet requiring specific software tools such as Tor (The Onion Router) and I2P (Invisible Internet Project) to access. By default, it is not indexed by traditional search engines. Tor and I2P provide privacy and anonymity to users and allow encrypted communications. Dark web users can access information under restrictive regimes or participate in activities such as trading illicit goods, cybercrime, and sharing illegal content [1, 2].

Given the malicious intentions of some users on these networks, there is a need to analyze what artifacts could be recovered after a user conducted typical browsing activity such as sending/receiving emails, using specialized search engines, or sharing files on websites. Several frameworks and research studies have been conducted in this area; however, given the constant evolution of technology, active monitoring of these networks can provide invaluable insights for forensic investigators. Before the advent of the dark web, the trail of evidence left by criminals was primarily physical, and traditional forensic methods sufficed for law enforcement to gather and analyze this evidence. However, the recent shift of criminal activities to the dark web has rendered conventional forensic techniques less effective [3].

This research aims to significantly enhance cybersecurity professionals' capabilities in newer environments like Windows 11 by detailing the forensic acquisition process and subsequent artifact analysis. This enhancement will not only aid in tracking and prosecuting cybercriminals but also contribute to the broader field of digital forensics and cybersecurity by:

- Improving the accuracy and speed of digital forensic investigations.
- Offering insights into the evolving tactics of cybercriminals on the dark web.
- Providing law enforcement agencies with the knowledge and tools necessary to combat the anonymity that dark web technologies provide to illegal operators.

The rest of the paper is organized in following sequence: Chapter 2 delves into the literature review, presenting an exhaustive examination of relevant existing studies and theories. In Chapter 3, the problem statement is articulated, identifying the specific issues and challenges the research aims to address. Chapter 4 describes the methodology used in the study, detailing the research design, data collection, and analytical techniques used. Chapter 5 presents the results obtained from the research, providing critical data and findings. Chapter 6 engages in a thorough discussion of these results, interpreting their implications in the context of the study. Finally, the thesis concludes with a summary in Chapter 7, where the main insights are synthesized, and the overall conclusions drawn from the research are outlined.

2. Literature Review

This chapter provides a foundation for understanding the current state of knowledge, identifying previous literature, and exploring key concepts, theories, methodologies, and findings from earlier studies on dark web forensics.

2.1. Forensic Investigation / Digital Forensics

Forensic science is crucial for law enforcement in collecting evidence in criminal investigations. This evidence, which may prove guilt or innocence, supports the prosecution of criminals. Forensic Investigation is critical when Law enforcement tries to determine whether an individual is guilty. With technological improvements, new tools and opportunities have come up to help law enforcement conduct their digital investigations. Digital forensics aims to use various tools to “Collect, examine, analyze, and report” evidence [3].

The utility of open-source and freeware forensic tools has become pivotal in contemporary digital forensics, offering both affordability and adaptability in investigative scenarios. Employing tools like FTK Imager, Regshot, Autopsy, and Volatility provides comprehensive capabilities in capturing and analyzing data from memory, registry, and storage [4]. The layered approach in using these tools enables extracting and comparing artifacts before and after using anonymity tools on Windows 11, revealing the modifications to system files and registry entries [5].

In forensic investigations, it is crucial to employ both static and live analysis techniques. Static analysis involves examining a digital copy of data from an inactive system, whereas live analysis involves collecting evidence from an operational system [6]. Forensic specialists focus on volatile and non-volatile memory data when analyzing a system suspected of conducting dark web activities. Memory holds essential information since the user can easily clean up a Hard drive. Analyzing volatile memory can unveil crucial details on browsing activities, active processes, and user interactions when the snapshot is taken [5].

As [5] describes, “The hard disk contains data from hardware and software that require examination and analysis. In the hard disk, the investigator can find evidence of the existence of a program, deleted files, and even hidden data”. In Windows systems, analyzing the registry can reveal operating systems' settings, configuration files, and installed applications and software [7].

Tor and I2P are prominent anonymity networks that are used to communicate over the Internet with enhanced privacy and security. Both networks mask the user's IP address and provide a degree of anonymity by routing traffic

through a series of volunteer-operated servers. However, they are significantly different in their design, implementation and functionality.

2.2. Tor Overview

Tor operates by routing internet traffic through global network of volunteer nodes known as relays or routers. Each user's data is encrypted multiple times, with each encryption layer corresponding to a network node. This setup is akin to the layers of an onion, which is why the process is called "onion routing" [8] [9].

Within the Tor network, data travels through a series of encrypted layers, similar to an onion. The number of layers corresponds to the number of relays the data passes through. Each relay removes one layer, revealing the address of the next relay in the chain. This layered approach Guarantees that no single relay can see both the origin and destination of the data, maintaining anonymity [10].

Tor utilizes a series of directory servers that provide a list of relays and their statuses. These servers help construct a path through the network that avoids non-operational or unreliable nodes, thus Preserving the efficiency and integrity of the network [11].

Each relay or node can only take one of the below-mentioned rules:

- **Entry Relay (Guard Node):** The first relay, where encrypted data enters the Tor network.
- **Middle Relays:** These nodes relay encrypted data across the Tor network.
- **Exit Relay:** The final relay that decrypts the innermost layer of encryption and sends data to its destination.

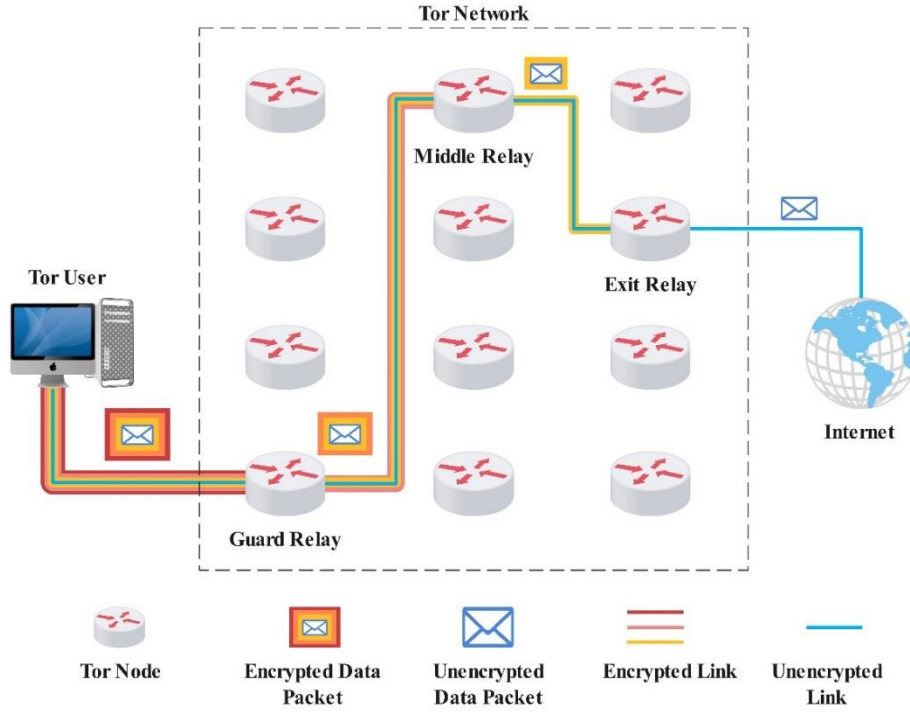


Fig 1. Illustration of the Tor Onion Routing.

2.3. I2P Overview

Unlike Tor, I2P is fully decentralized and does not rely on centralized directory servers. I2P establishes a peer-to-peer distributed network, employing a decentralized approach to avoid any single failure point and enhance privacy. Each node serves dual roles as a client and a server [12].

I2P employs garlic routing, where multiple messages are bundled together, enhancing anonymity beyond Tor's onion routing. Messages in I2P travel through unidirectional tunnels, i.e., separate inbound and outbound paths. The inbound tunnel is used for getting messages, whereas the outbound tunnel is used for sending messages. Tunnels are randomly reassigned at intervals to protect user privacy further [13].

I2P utilizes a distributed database known as NetDB, which stores network metadata and peer information. This database is spread across various nodes in the network and contains essential data such as routing information and tunnel addresses called RouterInfo and LeaseSets. A leaseset includes data for a particular destination, such as a web server or a BitTorrent client. However, RouterInfo has data for a specific router and the way to establish a connection, for example, router identity containing keys and a certificate or IP and Ports [12] [13] [14].

I2P Snark is a BitTorrent client designed for use within the I2P network. You have access to the I2P Browser when you install it. It supports anonymous downloading and uploading of files, providing users with a privacy-focused alternative to conventional BitTorrent clients. The benefit of using I2Psnark over P2P (BitTorrent) clients is that a forensic examiner does not know your

IP address and the location of the torrent creator, even if it was used on the regular internet [14] [15].

The I2P Addressbook is crucial for managing and translating human-readable addresses within the I2P network. It acts like a DNS service but for I2P sites, enabling users to connect to eepsites which are I2P-specific sites by using easy-to-remember names instead of complex cryptographic keys. I2P to update these Addressbooks uses a mechanism known as “subscriptions.” Through this mechanism, you do not need to modify the host files manually, and they routinely check for updating the addresses [15] [16].

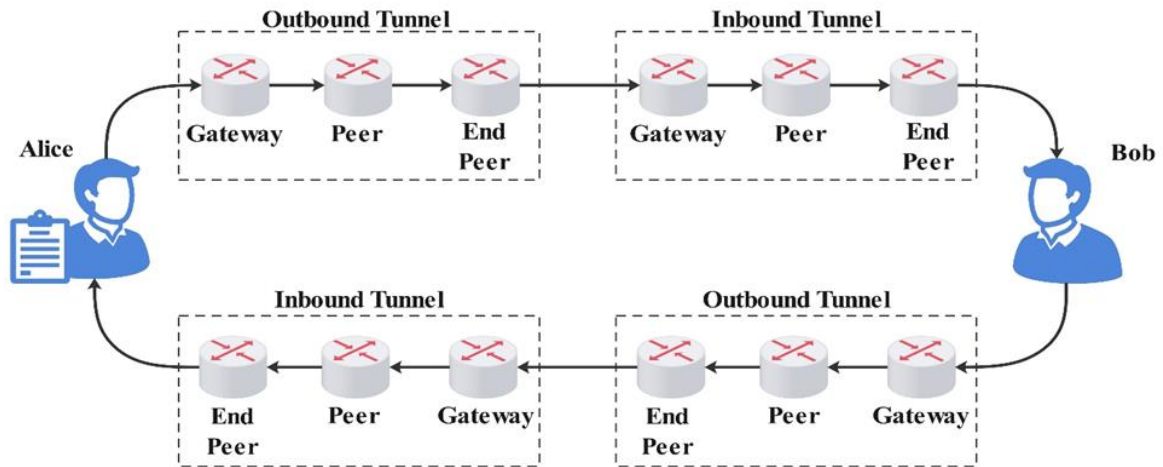


Fig 2. Illustration of the communication between I2P peers.

2.4. Related Work

[17] [18] analyzed Tor browser artifacts on Windows 7. In [19], The authors analyzed the Tor Browser on Windows 8.1, focusing on registry, memory, and disk, but did not cover network forensics. In [4] [5] [20] [21] [22] [23] [24], the investigations were conducted on Windows 10. In [20], the author analyzed remnants left by the Tor browser on a Windows 10 host, utilizing free and commercial tools to explore file systems and memory artifacts focused on pre- and post-Tor connections. In [21], The authors concentrate on Tor browser trace forensic analysis employing static and live analysis methods. To our knowledge, only in [5] did the authors integrate I2P into the investigation. Their forensic analysis of the Tor browser on Windows 10 aimed to identify artifacts across network, memory, hard disk, and registry components. In [23], the authors used an open-source tool kit and found artifacts regarding registry, memory, and storage.

Our methodology's idea of waiting for 15 minutes comes from [18], where researchers focused exclusively on memory forensics scenarios for the Tor browser. They evaluated the memory in different states: when a tab page was opened and then closed when the entire Tor browser was closed, and after the browser had been closed for 15 minutes. Their analysis indicated distinct memory traces for each state. The study in [17] found that despite Tor's anonymity claims, forensic techniques can still detect its usage. Live forensic methods were effective in documenting detailed user activities and network interactions. In contrast, dead-box forensics, which rely on registry and file path analysis, were less effective.

About the I2P forensic investigation, one study [15] focused on analyzing artifacts left by the I2P installer. The detailed techniques include comparing the address book with a reference database, assuming control of an address book registrar, and pinpointing an I2P node through network performance metrics. In [16], an in-depth analysis was conducted on the physical memory dump and local system files of a Windows 10 machine to detect the presence of I2P.

Paper	Year	Registry	Memory	Storage	Network	Operating System	Dark Web Version
A. Al-Khaleel [18]	2014	✗	✓	✗	✗	Windows 7	Tor
D. Winkler, et al. [17]	2015	✓	✓	✗	✓	Windows 7	Tor 3.6.1
B. Bazli, et al. [15]	2017	✗	✗	✓	✓	-	I2P 0.9.23
A. Warren [20]	2017	✓	✓	✓	✗	Windows 10	Tor 5.0
A. K. Jadoon, et al. [19]	2019	✓	✓	✓	✗	Windows 8.1	Tor 7.0.2
M. Muir, et al. [21]	2019	✓	✓	✓	✗	Windows 10	Tor 7.0.2, I2P 0.9.37
S. Soney et al. [16]	2020	✗	✓	✓	✗	Windows 10	I2P
M. Alfosail, et al. [24]	2021	✗	✓	✓	✗	Windows 10	Tor 9.0.7
M. R. Arshad, et al. [4]	2021	✓	✓	✓	✗	Windows 10, Android 10	Tor 10.0.7, Tor 68.7.0 (mobile)
T. Leng, et al. [23]	2021	✓	✓	✓	✓	Windows 10	Tor 10.5.5
V. M. Angeli, et al. [5]	2022	✓	✓	✓	✓	Windows 10	Tor 9.5

Table 1. Summary of related works on dark web forensics.

3. Problem Statement

Dark web forensics is an ever-evolving field marked by constant advancements in software and tools. Hence, research endeavors within this field must remain dynamic, adapting to emerging trends. As a result, there is a pressing need to explore dark-web forensics on Windows 11. This research investigates and compares the forensic artifacts extracted from Tor and I2P as they are utilized to access dark web services. The outcome will establish a systematic approach to address the gap in forensic acquisition and analysis on the Windows 11 platform, offering a procedure for future investigations within the dark web landscape. Such an endeavor will be valuable in tackling illicit activities by investigators within the digital underground. It will also enhance our understanding of the strengths and pitfalls of both networks, especially for users with privacy concerns.

3.1. Research Questions

Hence, our research questions are as follows:

- i. What forensic artifacts can be retrieved from a device communicating on the dark web?
- ii. What differences exist between the artifacts retrieved from I2P and Tor networks?
- iii. Which network is more secure from a forensic point of view?

3.2. Scope

This work is limited to Tor and I2P use on Windows 11. The acquisition of forensic artifacts would be limited to those found in the system registry, memory, and storage. The websites visited would be limited to sites on the dark web, and the activities performed would be restricted to those presented in Chapter Four.

This research will also be limited to using specific tools mentioned in Chapter Four. Hence, the results and analysis will only cover the output of the tools chosen for this experiment. Limiting the choice of tools only to open-source, demo, and free versions may result in certain tool functionalities being unavailable for the research. However, this decision enhances the reproducibility of the research work.

4. Methodology

This research aims to extract dark web browsing artifacts from the registry, memory, and storage of one host machine running on the Tor network and another on the I2P network. This research methodology is an adaptation from earlier work by [19] [5] with NIST SP 800-63 guidelines [25]. This exercise was carried out twice to ensure the repeatability of the results produced by the experiment. The phases of the acquisition process are shown in Fig 3. To achieve this objective, the artifacts added and removed during the installation and uninstallation are collected for registry analysis.

For memory analysis, three scenarios were considered. In the browser-only scenario, each browser is connected to its dark web network, but no browsing activity is performed. The second scenario considers the artifacts in the memory while each browser is open and the browsing activity is in progress. Lastly, in the third scenario, the state of the memory was examined after all browsing activity had been completed and the browsers were closed.

Storage analysis also involves three different scenarios. A browser open scenario where both browsers are open, connected to the dark web, and used for browsing activity. A browser-closed scenario where both browsers had been closed after being used for browsing activities on the dark web. In the browser uninstallation scenario, all downloaded files were deleted, and both browsers were uninstalled after all browsing activities had been completed.

The data collected from the acquisition process in Fig 3 will be analyzed for the presence of forensic artifacts that will provide answers to the research questions presented in Chapter Three.

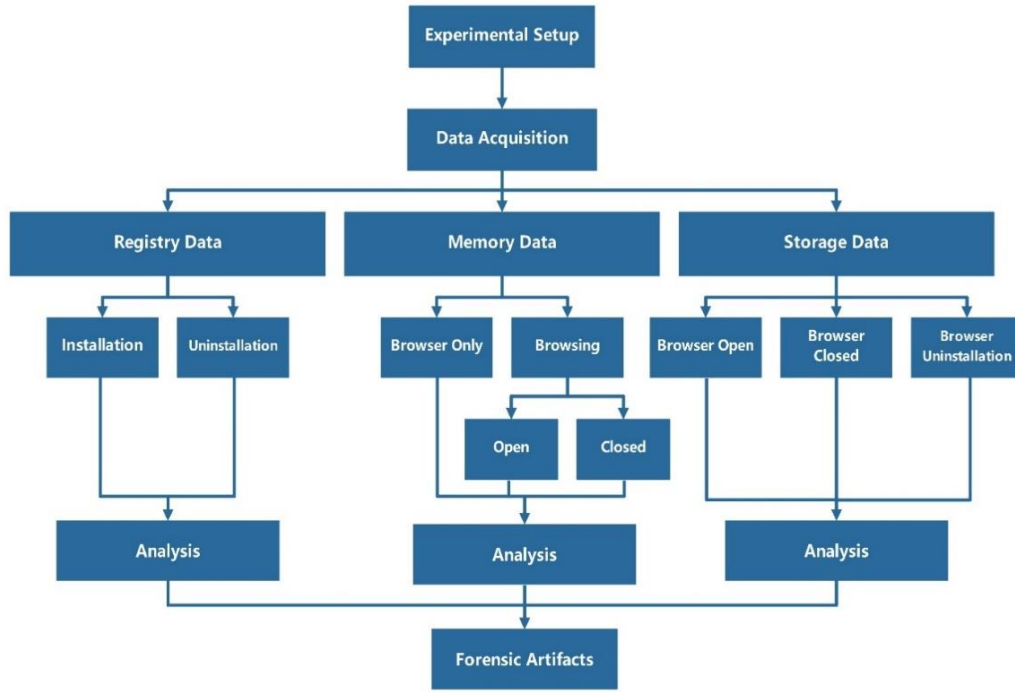


Fig 3. Forensic Acquisition and Analysis Process.

4.1. Tools

The forensic tools used for the activities in this research are given in Table 2. The tools used were chosen based on what was used by previous works, with a focus on open-source and freeware tools. For I2P deployment, Mozilla Firefox was installed and configured to work with I2P as the I2P installer does not provide a standalone browser like Tor. Mozilla Firefox was preferred to other browsers for I2P since Tor is built on the Firefox engine. This should provide a level playing ground in the performance of both browsers.

To have a clean and identical setup to conduct this experiment, two virtual machines were set up, one for Tor and the other for I2P. Both virtual machines were built to be identical in specification but isolated in operation. The storage space was pre-allocated when spinning each virtual machine to ensure that deleted items could be examined in the slack memory during the storage analysis phase. The specifications are listed below;

- Hypervisor: Virtual box
- Guest OS: Windows 11 (64-bit)
- CPU: 4 cores
- RAM: 4GB
- Storage: 30GB
- Network: NAT

Tool	Version	Use
Virtual box	7.0.8	Hypervisor and storage acquisition
Windows 11 (64-bit)	Build 22621	Guest OS
Tor Browser	13.0.9	Browser
I2P Browser	2.4.0	Browser
Mozilla Firefox	123.0	Browser
FTK Imager	4.0.1	Memory acquisition
Regshot	1.9.0	Registry acquisition and analysis
Autopsy	4.21.0	Storage analysis
Volatility 3	2.7.0	Memory analysis
Hex workshop	6.8	Memory analysis
Bulk extractor	2.0.0	Memory analysis
Python	3.12.0	Memory analysis

Table 2. Tools used for the experiment.

4.2. Data Acquisition

Following the forensic acquisition process presented in Fig 3, the data acquisition workflow given in Fig 4 shows the number of snapshots required to complete the data acquisition process and at what points they were taken.

For this research, we used two separate virtual machines (VMs) running Windows 11 with the specific configurations mentioned above. After installing Windows 11, the first step was to prepare the VMs for data acquisition. To minimize interactions with Windows, we decided to use an external hard drive for installing the Regshot and FTK Imager applications, and for saving the registry snapshots and memory snapshots taken from these applications. Additionally, we installed the Tor Browser on the Tor VM, while on the I2P VM, we installed the I2P software along with Java and Firefox.

The registry acquisition produced a total of three snapshots, three for each browser. The same goes for memory dumps and storage images captured for this experiment. The activity flow on the left in Fig 4 illustrates the acquisition procedure for the Tor browser. We started by taking a snapshot of a clean state of the registry with Regshot in a Windows 11 virtual machine environment, followed by the installation and immediate launch of the Tor browser. At this juncture, both the registry and the first memory snapshot are saved to document the initial impact made by launching and installing the browser in the registry and connecting to the Tor network in the memory. After browser activities, as detailed in Table 3, had been executed, a second memory snapshot was saved, and the first virtual storage snapshot was taken using VirtualBox’s snapshot feature. The browser is then closed, and after a 15-minute wait, a third memory snapshot and a second storage snapshot are recorded. The uninstallation process

follows the Tor Project's guidelines¹, which simply require deleting the browser's folder. The final registry and storage snapshots are then captured to document the system state post-uninstallation.

The right-hand side of Fig 4 details the acquisition procedure for the I2P browser. Before installing the I2P Bundle, we installed Java and Firefox; then, the initial registry snapshot was taken using Regshot. Installing the I2P bundle requires adjusting Firefox's network settings, specifically setting the manual proxy configuration to HTTP and SSL proxy at address 127.0.0.1, port 4444, as instructed on the I2P website. Once connected to the I2P network, the second registry snapshot and the first memory snapshot are saved. Browsing activities designed to mimic potential user interactions on the I2P network are then performed. Following these activities, a second memory snapshot and the first storage snapshot will be taken and saved. The browser is closed, and after waiting for 15 minutes, the final memory snapshot and the second storage snapshot are captured. Using the built-in uninstaller located in the I2P installation directory², the I2P browser was uninstalled, and the final snapshots of the registry and storage were taken to ensure comprehensive documentation of the final system state.

For each VirtualBox storage snapshot captured, we created a full-clone virtual machine, and then we used the Vboxmanage command-line interface to change the .vdi file to a raw image format. This was done to enable the analysis of these storage images with Autopsy.

4.1. Browsing Activity

The browsing activities simulated during our investigation play a crucial role in providing vital forensic information and potentially serving as evidence in legal proceedings when illegal activities are detected using the Tor browser and I2P browser [5]. We accessed several .onion websites uniquely structured for anonymity to investigate the Tor network. Conversely, for the I2P network, we exclusively visited .i2p sites. These activities are outlined in Table 3.

Email communication was another critical component of our simulation. We created four dark web email accounts to mirror typical user interactions: two for the Tor network using the Mail2Tor email service and two on Susimail for the I2P network. These platforms function similarly to conventional email services like Gmail but are designed for anonymous communication within the dark web. Email messages with attachments were sent and received between both email accounts.

¹ <https://tb-manual.torproject.org/uninstalling/>

² <https://eyedeekay.github.io/Install-Java-And-I2P-on-Windows/uninstall.html>

Our study also included searches using popular dark web search engines. We utilized Ahmia for the Tor network and Legwork for I2P, reflecting common tools users employ to navigate these hidden services. To access informational resources, we visited the Hidden Wiki for Tor and I2P-Wiki for I2P, both serving as directories analogous to Wikipedia but within their respective dark web environments.

File sharing was explored through FileHost, a specialized site that operates under separate domains for Tor and I2P, illustrating the distinct pathways for data exchange within these networks. We uploaded one file onto the file-sharing website, previewed a previously downloaded file directly through the web browser, and downloaded another to simulate the complete interaction with the file-sharing service on both networks.

Lastly, we engaged two services that are exclusive to both networks. On the Tor network, two instant messaging accounts were created on Chator, and messages were exchanged between both accounts to understand the dynamics of private communications. For I2P, we utilized I2P Snark, a built-in feature of the I2P network that facilitates torrent downloads, to analyze the remnants left on the system after such activity. A torrent file was created and seeded, while another file was downloaded using a magnet link sourced from the Postman website to assess further the forensic footprint of file-sharing activities within the I2P environment.

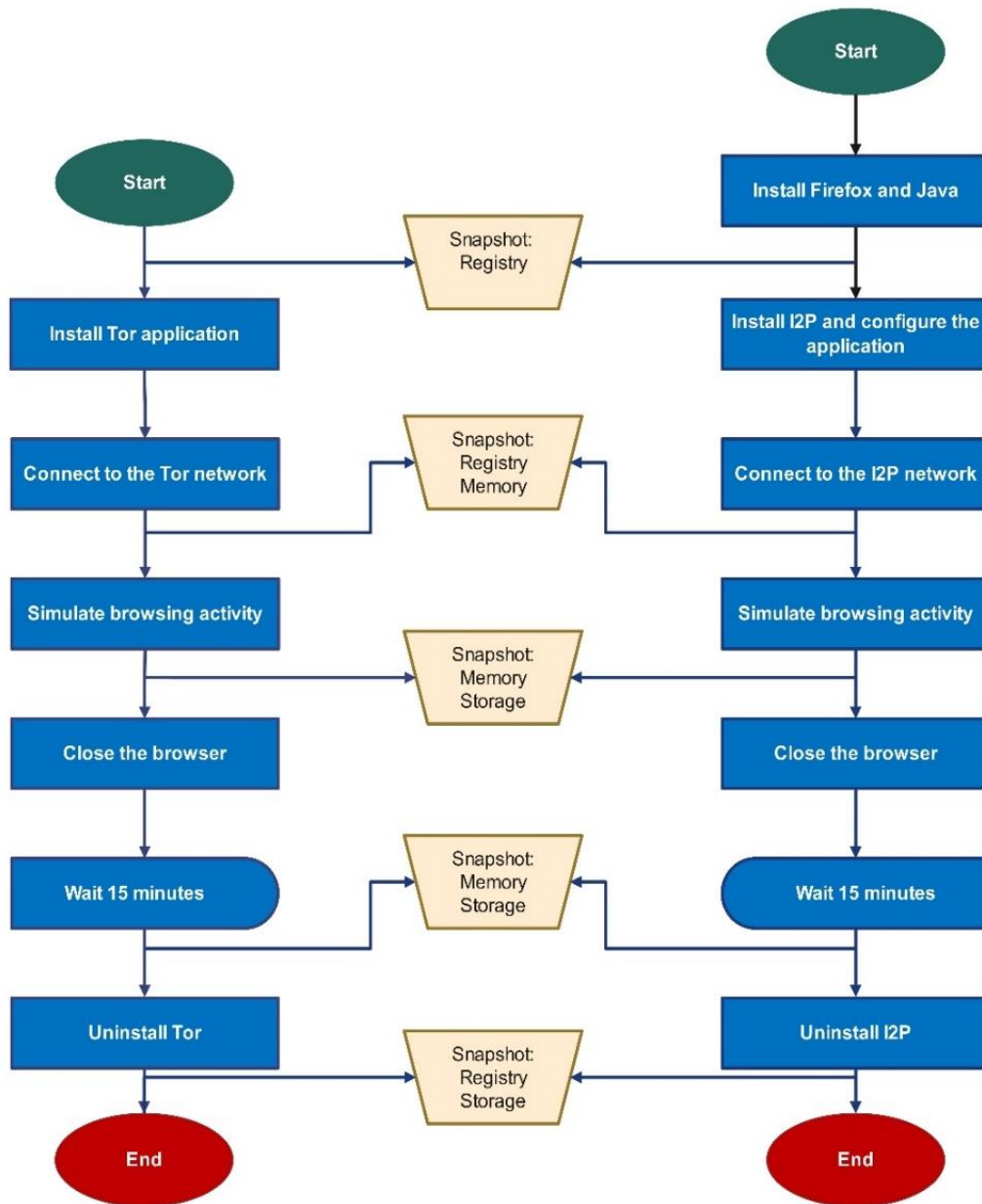


Fig 4. Data acquisition workflow.

Table 3. Summary of browsing activity.

Web Service	Tor Account and Link	Tor Activity	I2P Account and Link	I2P Activity
Email	darkt2@mail2tor.com	<ul style="list-style-type: none"> Login Send an email with two attachments to darkt1@mail2tor.com 	darki2@mail.i2p	<ul style="list-style-type: none"> Login Send an email with two attachments to darki1@mail.i2p
	darkt1@mail2tor.com	<ul style="list-style-type: none"> Login Read an email with two attachments from darkt2@mail2tor.com 	darki1@mail.i2p	<ul style="list-style-type: none"> Login Read an email with two attachments from darki2@mail.i2p
	Mail2tor http://mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkw.yd.onion/	<ul style="list-style-type: none"> Open one attachment online Download one email attachment Send an email with an attachment to darkt2@mail2tor.com 	Susimail http://127.0.0.1:7657/susimail/	<ul style="list-style-type: none"> Open one attachment online Download one email attachment Send an email with an attachment to darki2@mail.i2p
Search Engine	Ahmia http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csy.d.onion/	<ul style="list-style-type: none"> Browsing Keyword search Open images online Download image file 	Legwork http://legwork.i2p/index.html?searchoptions= 1	<ul style="list-style-type: none"> Browsing Keyword search Open images online Download image file
Wiki	Hidden Wiki http://wiki2zkamfya6mnyvk4aom4yji2kwsz7et3e4wnikcrypqv63r.sskid.onion/	<ul style="list-style-type: none"> Browsing Keyword Search 	I2P Wiki http://wiki.i2p-projekt.i2p/	<ul style="list-style-type: none"> Browsing Keyword Search
File Sharing	Filehost http://uploaddd5rychb5mzvpycwr4c6pomy6ptr3gqbluivnig2jokirmf6qd.onion/	<ul style="list-style-type: none"> Upload View an image online Download Word document 	Filehost http://upload5futsclmsubidfe5wdvxs6smvd74to2snfrmnzbok5qxa.b32.i2p/	<ul style="list-style-type: none"> Upload View an image online Download Word document
Messenger	chator1	<ul style="list-style-type: none"> Login Send a message to chator2 		
	chator2 Chator http://chatorcfkrfdchasnaw7wverjlcj6j5jknwt.yulkyzpgle7ab7cnv2q.d.onion/	<ul style="list-style-type: none"> Login Send a message to chator1 		
Torrent			Postman http://tracker2.postman.i2p	<ul style="list-style-type: none"> Browsing Keyword search Download torrent Create torrent

5. Results

To discuss the results of the experiments, the artifacts retrieved from the analysis of data acquired from the registry, memory, and storage will be presented following the same sequence.

5.1. Registry

The Windows registry is a database, hierarchically organized and used by Windows Operating systems and applications to store necessary system and application information [26]. It is a good source of information when investigating installed applications within a Windows-based computer system. The Regshot tool captures the state of the system registry at a desired point in time. Two captured files can be compared to produce a result containing the added or deleted registry keys and values. This explains changes made in the registry by application(s) that were run or activities carried out between the time of the two snapshots.

A first snapshot was taken for the registry analysis while the system was at rest before the software installation commenced. The second snapshot was obtained after the application had been initialized after installation. This was compared with the first snapshot, which produced a result that included the registry keys and values affected by the software installation. A third snapshot was obtained after the software was uninstalled. This snapshot was compared with the second one to see if the software removal introduced any changes to the registry.

In the registry analysis, we retrieved artifacts that provided the installation source files for both Tor and I2P. The executable files' location, usage details, and Windows environment settings were also visible in the registry. The following sections further go into detail on the findings in the registry.

5.1.1. Tor Registry

Installation of the Tor browser bundle created four registry keys under the “HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\” registry path. These keys include DllPrefetchExperiment, Installer\D71232F1AB4CB903, Launcher and PreXULSkeletonUISettings. DllPrefetchExperiment stores the preference settings and has a value entry. Installer\D71232F1AB4CB903 stores installation settings but has no value entry. The Launcher registry key stores the path and configuration of the Firefox executable file that comes with the Tor bundle. PreXULSkeletonUISettings controls the visual design element. These results are summarized in Table 4.

The Tor browser also adds twelve values to existing keys in the Windows registry. The values control the Windows Block Access Manager settings, Access control rules and permission, audio output configuration, application compatibility, user permission, and user-environment data. These registry keys are summarized in Table 5.

The Tor project recommends deleting the Tor browser folder instead of using the Windows add/remove programs uninstaller. This is because the Tor browser bundle does not come with an uninstaller file, and the Tor application is not recognized as an installed program by the Windows add/remove programs feature. The registry data was unaffected after permanently deleting the Tor browser folder and all its content. Table 12 in the Appendix summarizes all the Tor registry values.

S/N	Registry Keys	Description
1	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\DllPrefetchExperiment	Preference setting related to the Tor Browser
2	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\Installer\D71232F1AB4CB903	Installation-related settings for the Tor Browser
3	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\Launcher	The Tor browser launcher path and configuration
4	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings	This key controls the visual design elements.

Table 4. Registry keys created by the Tor browser installation.

S/N	Registry Keys	Description
1	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-3314099954-1345764329-2790451392-1000	The Block Access Manager states settings for the Tor browser and the Tor browser installer
2	HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3314099954-1345764329-2790451392-1000	The current Block Access Manager states settings for the Tor browser and the Tor browser installer
3	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Microsoft\Internet Explorer\LowRegistry\Audio\PolicyConfig\PropertyStore\f3d3e487_0	Audio output configuration for the Tor Browser application
4	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store	Compatibility information for the Tor Browser installer
5	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	Stores user-permission data for both the Tor browser and the Tor browser installer executable files
6	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	Stores user-environment data for both the Tor browser and the Tor browser installer executable files

Table 5. Exiting registry keys affected by the Tor browser installation.

5.1.2. I2P Registry

Running the I2P installer executable file deployed the I2P router executable file (i2p.exe) and the I2P Windows service executable file (i2pSVC.exe) on the target computer system. It also changed the configuration of the Java executable/application file (javaw.exe). These changes gave rise to the registry changes described in this section. i2p.exe starts the I2P router with a GUI console through which a user can manage bandwidth, connections, routing, and other related tasks within the I2P network. i2psvc.exe is a Windows service program that runs the I2P router in the background without human interaction [16].

Unlike Tor, the I2P software installation was not seen to create any entry in the registry hive specific to itself. It, however, added some values to existing keys in the Windows registry. Under the Block Access Manager (BAM) user settings, entries were made for the Java application, the I2P installer file, the I2P router file, and the I2P Windows service executable file. Registry entries were made to alter the firewall policy to allow inbound TCP and UDP communication to the Java application over the network. Other entries made in the registry for the Java application were to control the User Model ID notification and Windows system tray notification settings. The registry keys holding the user permission and user-environment data also had values written into them for the Java application, I2P installer, and I2P router applications. These can be seen in Table 6.

I2P configuration also modified some existing registry values. The registry entries modified were for javaw.exe and firefox.exe under the current and the backup Windows Block Access Manager registry hive for the installed user account. The registry keys where the modifications were made can be seen in Table 7.

After the browsing activities had been completed, the browser was closed, and I2P uninstallation was done by launching the uninstaller executable file. This process removed the I2P application and files from the computer but did not affect the above registry keys and their associated values. Table 13 in the Appendix summarizes all the I2P registry values.

S/N	Registry Keys	Description
1	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\	The Block Access Manager states settings for the Java, I2P installer, router, and Windows service executable files
2	HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\	Windows firewall policy for the Java application
3	HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\	The current Block Access Manager states settings for the Java, I2P installer, router, and Windows service executable files
4	HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\	The current Windows firewall policy for the Java application
5	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Control Panel\NotifyIconSettings\12806010725221006127\	Windows system tray notification area icon settings for the Java application
6	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\	Compatibility information for the I2P installer, router, and Windows service executable files
7	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\	Stores user-permission data for the Java, I2P installer, and I2P router, executable files
8	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Software\Classes\AppUserModelId\NotifyIconGeneratedAumid_12806010725221006127\	User Model ID setting for the Java application
9	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\	Stores user-environment data for the Java, I2P installer, and I2P router, executable files
10	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000_Classes\AppUserModelId\NotifyIconGeneratedAumid_12806010725221006127\	User Model ID setting for the Java application

Table 6. Existing registry keys affected by the I2P installation

S/N	Registry Keys	Description
1	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\	The Block Access Manager states settings for the Java and Firefox executable files
2	HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\	The current Block Access Manager states settings for the Java and Firefox executable files

Table 7. Existing registry keys whose data were modified by the I2P installation.

5.2. Memory

Three memory dumps were collected for both Tor and I2P during the acquisition phase using FTK imager: Browser only with the browser connected, but no browsing activity was carried out; browsing – open, where all the simulation had been carried out, and the browser left open; and Browsing – closed, where the browser was closed after all the simulation was carried out.

Bulk extractor and Hex workshop were used to search for artifacts in the form of strings and keywords. Volatility was used to analyze the system processes and state during each acquisition phase to find relevant artifacts according to the phases of memory acquisition. We used mainly pslist, pstree, and pscan plugins, which retrieved the system processes and their related data, while netscan retrieved network processes, as seen in Table 8 below.

The memory analysis produced artifacts that show Tor and I2P usage. The installation destinations/locations of the executables were retrieved. The running and network processes and their network communication configuration were also in the memory. With an understanding of the browsing activities performed, we could retrieve relevant artifacts regarding the visited Tor and I2P sites and some of the data exchanged during the interaction process. The encryption keys for Tor were visible in clear text, while those of I2P could not be found. To further explain these findings, we have arranged the following subsection to explain the artifacts retrieved for each scenario and summarized these explanations in Table 9.

S/N	Plugin	Artifacts
1	Pslist	Processes, start and exit times
2	Pstree	Processes, start and exit times, commands, and file paths
3	Psscan	Processes, start and exit times (shows hidden and closed processes)
4	Netscan	Local Address, port, state, and network processes

Table 8. Volatility plugins used for memory analysis.

5.2.1. Tor Browser Only

In the browser-only scenario, the memory dump was analyzed for artifacts to prove the existence of connectivity between our device and the Tor network. Tor creates a bidirectional tunnel to the routers in its path to establish a communication channel for routing its traffic. Analysis with Hex Workshop and Bulk extractor tools showed the presence of public keys used to set up the tunnel in the memory (see Appendix, Fig 5). Additionally, IP addresses, listening ports, bandwidth, roles, and other details of multiple Tor nodes can be seen in the memory (see Appendix, Fig 6).

With the Volatility netscan plugin, the tor.exe process with PID=7252 can be seen listening on ports 9150 and 9151 over the loopback address 127.0.0.1 (see Appendix, Fig 7). These ports serve as ControlPort and SocksPort for the tor.exe process, over which the application listens to incoming communication messages from the network [24]. This output was further validated by the pstree plugin, which shows the commands used by the tor.exe process to listen on both ports and other commands executed by the tor.exe process and other firefox.exe processes linked to the Tor browser operation.

Viewing the outputs of the pstree and pslist plugins for tor.exe and firefox.exe processes, it can be seen that nine firefox.exe processes were running, of which the firefox.exe with PID=7712 served as the parent process for all firefox.exe processes, and the tor.exe process alike. Also, both the firefox.exe processes and the tor.exe processes made command line calls to folders and files in the “C:\Users\vboxuser\Desktop\Tor Browser\Browser\” path, which is the installation path of Tor (see Appendix, Fig 8 and Fig 9). This proves that the firefox.exe processes are part of the Tor Browser bundle and can be used to isolate firefox.exe processes relating to Tor operation from other firefox.exe processes in a device that has the default Firefox application installed alongside the Tor browser.

5.2.2. I2P Browser Only

The analysis of the I2P memory dump for artifacts that show connectivity with the I2P network was not as successful. I2P builds two unidirectional tunnels – one inbound and one outbound tunnel – to support network connectivity. Searching the memory dump with Hex Workshop and Bulk extractor for strings relating to the public keys used and inbound or outbound tunnel returned no exciting feedback (see Appendix, Fig 10).

The Volatility pslist plugin showed the I2P process, i2p.exe with PID=4208, as the parent process to a Java process, javaw.exe with PID=6784. It also showed ten firefox.exe processes running, of which the process with PID=7316 was the parent of the other firefox.exe processes (see Appendix, Fig 11).

During a forensic investigation, it will be challenging to determine the browser configured and used with I2P because I2P does not come bundled with any web browser software. As we have seen, the firefox.exe processes are independent of the i2p.exe and javaw.exe processes and cannot easily be linked together if the device under investigation runs multiple browsers simultaneously. This was validated from the output of the pstree plugin, which shows the command line executions of the firefox.exe processes (see Appendix, Fig 12). The commands were executed outside the I2P and Java installation paths.

The Volatility netscan plugin showed javaw.exe with PID= 6784, running over IPv4 and IPv6 simultaneously. In total, 18 ports were opened over TCPv6 (11), UDPv6 (3), TCPv4 (1), and UDPv4 (3). Port 27605 was open over TCPv6, UDPv6, TCPv4 and UDPv4. Port 1900 was open over UDPv6 and UDPv4. Ports 4444, 4445, 6668, 7652 – 7654, and 7657 – 7660 were open only on TCPv6 (see Appendix, Fig 13). This validates the firewall entries in the registry analysis, which allowed TCP and UDP connections to the Java application during the I2P software installation. This indicates that the I2P process does not handle its network communication process; the Java application (javaw.exe) handles such responsibility on its behalf.

5.2.3. Tor Browsing Open

With Hex Workshop and Bulk Extractor, the Tor Browsing – open scenario memory dump analysis contains the public key, as with the browser-open scenario. However, the information on the Tor network nodes was mostly overwritten in the memory dumps from the first iteration and was completely lost in the memory dumps from the second iteration.

For email artifacts, keyword searches retrieved the URL of mail2tor. The username used to log in to the email account (darkt1), and the content of the email sent. The name, storage location, and timestamps of the sent and the downloaded attachments were also in the memory. The name of the previewed

attachment was also found in the memory, but since it was not saved to the local storage, no location nor timestamp was attached to the name. Though the search for the login username had a positive match, the associated password could not be retrieved from the memory dump. This was also the case for the email address associated with the logged-in account.

The URL and search queries for both the search engine and Wiki browsing activity were found in the memory using their respective keywords to search for them. Other search engine artifacts like name, link, storage location, and timestamps of the downloaded image file could be retrieved, while only the link of the previewed file was retrieved. The artifacts related to file sharing retrieved from the memory include the URL of the file host onion site, the name, link, and storage location of the uploaded and downloaded files, and only the link to the previewed file.

The Chator messenger artifacts in the memory dump included the URL, username, and password used to log in to the messenger account. While the sent message could be found by keyword search, the received message could not be found in memory.

Using Volatility, the pslist plugin produces an output showing the same tor.exe process with PID=7252 and 23 firefox.exe processes with PID=7712 as the parent PID of the tor.exe and all the other firefox.exe processes. With the pstree plugin, the link between these processes and the Tor browser bundle can be further validated. As in the browser open scenario, the firefox.exe processes were launched from the Tor browse installation path. There were also commandline Interactions between the firefox.exe processes and files in the Tor browser bundle installation path. The output of the netscan plugin remained unchanged; the tor.exe process with PID=7252 was listened to on the control port 9150 and the socks port 9151 over the loopback address 127.0.0.1.

5.2.4. I2P Browsing Open

In the I2P browsing-open scenario, all the searches performed for forensic artifacts returned positive, except for the private-key information used for data encryption and the I2P network inbound and outbound tunnel details, which could not be found in the browser-open scenario.

Keyword searches using Hex Workshop for email artifacts found Susimail URL, login username and password, email addresses of both the sender and the receiver, and the body of the email. The names and storage locations of the sent and downloaded attachments with their respective timestamps and the name of the previewed attachment were also found in the memory.

The URL and search query for the Legwork search engine and the I2P Wiki browsing activities were found in the memory with their respective keyword

searches. The name, storage location, link, and timestamp of the downloaded image file, along with the link to the previewed file, were also found. All file-sharing artifacts were also found in the memory. These include the names of the downloaded and uploaded files, links, and storage locations. The link used to access the previewed file was also stored in the memory.

The URLs of Postman, I2P Snark, and torrents were found as artifacts from the torrent browsing activity. Other artifacts retrieved from the memory dump include the search query, the name and link to the seeding torrent, the name of the torrent downloaded, the downloaded file name, the storage location, and the magnet link of the downloaded torrent file.

With Volatility, the pslist plugin showed the I2P process, i2p.exe with PID=4208, as the parent process to a Java process, javaw.exe with PID=6784, similar to the browser-open memory dump output. This scenario showed twenty-one firefox.exe processes running, of which the process with PID=7316 was the parent of the other firefox.exe processes. The pstree plugin validates this finding and highlights the independence of the Firefox processes running in the memory from the I2P process, i2p.exe, and the Java process, javaw.exe. The output of the netscan plugin was unchanged from that of the I2P browser open scenario. The same 18 open ports were running over IPv4 and IPv6 by the javaw.exe process.

5.2.5. Tor Browsing Closed

After the browsing activities had been simulated, the browser was closed, and the memory dump was acquired after a 15-minute delay. Analysis of this memory dump revealed fewer artifacts than the browsing-open scenario. This was expected as computer memory is a volatile storage for running applications. Keyword search with Hex Workshop returned the onion encryption public keys, but the Tor relay node information produced the same results for both iterations as the Tor Browsing open scenario.

The only email artifact in the memory was the downloaded email attachment's name and storage location; the timestamp seen in the browsing-open scenario was not found. Artifacts seen in the browser-open scenario, such as mail2Tor URL, username, receiver's email address, email body, sent attachment, and previewed attachment, were not found. Also, the sender's email address and password, which were not seen in the browsing-open scenario, could not be found in the memory.

Search engine artifacts search returned the Ahmia URL, the search query, and the link to the previewed image file. Unlike in the browsing-open scenario, no trace of the downloaded image could be found in the memory. A search for Wiki artifacts returned only The Hidden Wiki URL, but the search query was not found in the memory. The file-sharing artifact retrieved only contained the downloaded

file's name and storage location. The Filehost URL, link to the previewed file, and the uploaded file's name, link, and storage location could not be retrieved from the memory dump.

A search for artifacts from Messenger returned only the Chator URL used to access the platform. Other artifacts retrieved from the browsing open, such as the Chator account username, password, and sent message, were not received from the memory dump. The received message could not be retrieved, similar to the browsing-open scenario.

Using Volatility, the pslist plugin returns only a firefox.exe process similar to the result obtained by [24]. The Firefox process returned is the firefox.exe with PID=7712, the parent process for tor.exe and other firefox.exe processes in the Tor browser-open and Tor browsing-open scenarios. However, an exit timestamp indicates that the process has been terminated. A similar result is obtained with the pstree plugin. With the psscan plugin, some recently closed processes can be investigated. The output shows the tor.exe process with PID=7252 and seven firefox.exe processes, of which the firefox.exe process with PID=7712 is the parent process of the other processes. All the processes have the same exit timestamp, indicating they are all linked to the Tor browser we closed before taking the memory dump. It also shows that the psscan plugin can be handy in retrieving process artifacts from memory dumps taken from devices that had the Tor browser closed just before the memory dump could be obtained. The Volatility netscan plugin returned no traces of Tor operations as the tor.exe process that was listening on ports 9050 and 9051 in the previous scenarios had been closed.

5.2.6. I2P Browsing Closed

The memory dump collected 15 minutes after the browser was closed contained fewer artifacts when compared with the browsing open scenario. Like the previous two scenarios, the Hex Workshop keyword search did not return any artifacts relating to the encryption keys and tunnel information used to set up the overlay network.

Email artifacts retrieved from the memory dump were the URL of Susimail and the name and storage location of the downloaded attachment. Other artifacts, like the username and password, email addresses, the email body, the sent attachment, and the previewed attachment, could not be found in the memory.

The search engine artifacts found in the memory were similar to the browsing-open scenario. The Legwork URL, search query, the downloaded image file name, link, storage location, and the link to the previewed image file were all found using keyword search. The I2P wiki URL was still in memory, but the Wiki search query was not found. Like the search engine results, the file-sharing

artifacts found in the memory were similar to the browsing-open scenario. These include the Filehost URL, the downloaded file's name, link, storage location, and the link used to access the previewed file.

Most of the artifacts of torrent browsing activity were still found in the memory. Postman, I2P Snark, and torrents URLs were retrieved from the memory dump. The search query, the name and link to the seeding torrent, the name of the torrent downloaded, the downloaded file name, and the storage location were also found. However, the magnet link of the downloaded torrent file was not found.

Volatility pslist and pstree plugins returned only one firefox.exe process. Like the Tor browsing closed scenario, this firefox.exe process was the parent process for all other Firefox processes with PID=7316. However, like in other I2P scenarios, linking this Firefox process to I2P might be difficult. The parent Firefox process also had an exit timestamp indicating that the process had ended. Running the psscan plugin to investigate some recently closed processes returned the parent Firefox process with two firefox.exe processes with PID=6612, 7980 and the javaw.exe process with PID=6784. The two firefox.exe processes are child processes of the parent process. The netscan plugin returned three ports running over the javaw.exe process. The three ports were two UDPv6 ports, 27605 and 6169, and UDPv4 port 27605. All four volatility plugins did not find the i2p.exe. This implies that after the I2P software has been terminated, it can be difficult to tell that I2P was used by looking at the list of processes in the memory.

Artifacts Category	Artifacts Found	Tor Browser Open	Tor Browsing Open	Tor Browsing Closed	I2P Browser Open	I2P Browsing Open	I2P Browsing Closed
Existence Artifacts	Public Key	✓	✓	✓	✗	✗	✗
	Overlay network	✓	✗	✗	✗	✗	✗
Email	URL		✓	✗		✓	✓
	Username		✓	✗		✓	✗
	Password		✗	✗		✓	✗
	Sender email address		✗	✗		✓	✗
	Receiver email address		✓	✗		✓	✗
	Email content		✓	✗		✓	✗
	Sent attachment		✓	✗		✓	✗
	Downloaded attachment		✓	✓		✓	✓
	Previewed attachment		✓	✗		✓	✗
Search engine	URL		✓	✓		✓	✓
	Search query		✓	✓		✓	✓
	Downloaded image		✓	✗		✓	✓
	Previewed image		✓	✓		✓	✓
Wiki	URL		✓	✓		✓	✓
	Search query		✓	✗		✓	✗
File sharing	URL		✓	✗		✓	✓
	Downloaded file		✓	✓		✓	✓
	Previewed image		✓	✗		✓	✓
	Uploaded file		✓	✗		✓	✗
Messenger	URL		✓	✓			
	Username		✓	✗			
	Password		✓	✗			
	Sent message		✓	✗			
	Received message		✗	✗			
Torrent	URL					✓	✓
	Search query					✓	✓
	Created torrent					✓	✓
	Downloaded file					✓	✓
	Name of torrent					✓	✓
	Magnet link					✓	✗

Table 9. A summary of the forensic artifacts found in the memory.

5.3. Storage

Storage artifacts were collected for three scenarios for both Tor and I2P. The first scenario –browser open – was captured while the browser was open after concluding all browsing activities. The browser closed snapshot was taken after the browser closed, while the third scenario was captured after the software uninstallation was completed and all downloaded files were deleted. The storage image files were acquired using the Virtual Box snapshot and were originally in VDI format. These files were converted to raw format using VboxManage – a command line tool that comes with Virtual Box to allow for flexible manipulation of virtual machines. The raw image files were then fed into Autopsy for forensic analysis.

I2P produced more storage artifacts when compared to Tor. The installation source and destination files were retrieved. Details such as the application usage statistics, network usage statistics, and configurations were retrieved. For Tor, the encryption keys were also retrieved from the storage images. While the encryption keys could not be retrieved for I2P, some cryptographic keys used by the I2P router were retrieved from the storage. The artifacts retrieved for each scenario are explained in the following subsections and summarized in Table 10.

The first step in the storage analysis of Tor and I2P for forensic artifacts is to examine the prefetch files for both applications. Windows operating system uses prefetch files to improve application startup performance. When the installation path of a dark web software is unknown during an investigation, the prefetch is an excellent source to retrieve such information. The prefetch files contain other information, such as the creation timestamp, utilization count, and timestamps [23]. The default location of prefetch in the Windows file system is “C:\Windows\Prefetch,” and these files have a .pf file extension. Beyond the prefetch for Tor and I2P, the prefetch files for Firefox and Java applications can also be examined for Tor and I2P, respectively.

Once the installation path has been retrieved, further investigation can be done at the Tor installation path to analyze the application files for some database and configuration information. Artifacts of interest are usually contained at “\Tor Browser\Browser\TorBrowser\Data\Tor.” Some helpful information that can be retrieved from this location includes public keys and relay node IDs, IP addresses, ports, bandwidth, nicknames, fingerprints, and version information for routing Tor traffic over the dark web [19]. These files of interest include;

- i. **state:** contains statistical information relating to Tor circuits and guards. Information such as the last time the application was used, guard RSA ID, nickname, version, Tor version, and circuit build time is contained in this file.

- ii. **cached-cert:** contains Tor directory authority descriptions like key publishing and expiry timestamps, fingerprints, identity keys, and signing keys.
- iii. **cached-microdesc.new:** contains cryptographic about Tor relays, such as encryption keys, accepted and rejected ports, and family membership.
- iv. **cached-microdesc-consensus:** this network status document contains relay descriptors, bandwidth, and consensus parameters.
- v. **geoip:** location database that maps IP address ranges to geographic locations.
- vi. **geoip6:** location database that maps IPv6 address ranges to geographic locations.

For I2P, most of the forensic artifacts of interest are in the AppData folder, “C:\Users\<username>\AppData\Local\I2P.” This folder contains I2P data and configuration [16]. Some of the items in this location are explained below;

- i. **router.config:** This file holds the local I2P router settings like the last used IP address, country, cryptographic keys, router version, update history, bandwidth, and language settings.
- ii. **hosts.txt:** This file stores the translation between I2P domain names and I2P network identifiers. An I2P network identifier serves as a replacement for an IP address in the I2P network.
- iii. **addressbook:** To improve simplicity and reduce the need for manual input into the host.txt file, I2P implements a subscription system and a name record update mechanism. The subscription.txt file and its log file (log.txt) are in the addressbook folder.
- iv. **clients.config.d:** This folder contains client-side settings of I2P, such as proxy settings and bandwidth limit.
- v. **logs:** This folder contains logs of I2P usage and activities. It is a good source for tracking the application activity.
- vi. **netDB:** This folder holds the database of I2P network routers. The entries are grouped by the letter r and the first character of the router hash – that is, if the hash starts with A, it is placed in the sub-folder rA, and so on.
- vii. **i2psnark:** I2PSnark comes as part of the I2P software as the default torrent client for I2P [15]. Torrent files data downloaded/uploaded with I2PSnark can be retrieved from this folder.
- viii. **susimail:** This is the default folder for the I2P susimail and contains the email message sent/received on the susimail platform.

5.3.1. Tor Browser Open

Analyzing the disc image for the Tor browser open scenario, the prefetch files for tor.exe and firefox.exe were found in the default location. In the Appendix, Fig 14, TOR.EXE-4672E5EF.pf is the prefetch file for the Tor application, while

the TOR-BROWSER-WINDOWS-x86_64-PO-05DE8DD8.pf is the prefetch file for the Tor Browser installer. The alphanumeric strings attached to the application's name differ for each experiment iteration. While the Tor application prefetch file contains the installation path, the Tor Browser installer prefetch file does not tell the path to the installer. Hence, the Tor Browser installer prefetch file has little forensic value as a forensic artifact. The firefox.exe prefetch file (FIREFOX.EXE-DD9E003F.pf) also provides a pointer to the installation path of Firefox, which is the same as that of tor.exe, indicating that this is the Firefox application used by the Tor browser (see Appendix, Fig 15).

Navigating through the Tor installation path, the tor.exe and the firefox.exe can be seen in the file system. Other Tor-existence artifacts were present, such as the Tor browser icon, DuckDuckGo icon, and other icons that come with Tor installation.

At “C:\Users\vboxuser\Tor Browser\Browser\TorBrowser\Data\Tor,” the forensic artifacts of interest, such as state, cached-cert, cached-microdesc.new, cached-microdesc-consensus, geoip, and geoip6 files, were present. Artifacts related to browsing activities, such as web links and browser history, icons of the visited websites, email addresses, sent and received emails and metadata, previewed files, search engine, and wiki search queries, could not be retrieved. However, the downloaded files from email, search engine, and file sharing were found in the download locations.

5.3.2. I2P Browser Open

Analyzing the I2P browser open scenario's forensic image, the prefetch files for i2p.exe and javaw.exe were found in the default location. As seen in the Appendix, Fig 17, I2P.EXE-9EFBD94E.pf is the prefetch file for i2p.exe, I2PINSTALL_2.4.0_WINDOWS.EXE-BBE1D20B0.pf is the prefetch file for the I2P installer and unlike the Tor Installer, it holds the source path information from which the installer was run. Of the four Java prefetch files, JAVAW.EXE-00FDF375.pf shares the same path with the javaw.exe process in the output of the volatility pstree in the Appendix, Fig 12.

In the AppData folder for I2P, the forensic artifacts of interest, like router.config and host.txt files, were present. Other artifacts in folders like the addressbook, clients.config.d, logs and netDB were found. In the i2psnark folder, both the downloaded and the uploaded files were all kept together with segregation, making it challenging to tell in which direction each file was utilized. However, reading the .torrent files associated with each artifact indicates how the artifacts were used. In the summary folder, a text copy of the sent and received emails were found. A text copy of the content of PDF files attached to the received email was also seen.

Under the Autopsy “Data Artifacts” section, the Web History, Web Search, Web Downloads, and Web Form Autofill contained artifacts relating to the browsing

activities. These artifacts include email addresses, sent and received email content, attachments, and metadata; downloaded files; previewed images both for search engine and file sharing; downloaded and uploaded torrents; magnet link and torrent metadata; search queries for both wiki and search engine and other visited URLs.

Other artifacts, such as the I2P icon, dashboard icons, and other icons like the national flags that come with the I2P installation, were retrieved from the file system. The downloaded files could also be located without going through the Autopsy “Data Artifacts” by navigating the file system to the download path.

5.3.3. Tor Browser Closed

The Tor browser closed scenario produced results identical to those of the Tor browser open scenario during the analysis. This is predominantly because the prefetch files, database, and configuration files relating to Tor in the file system remained unchanged after the browser was closed. The search for browsing activity artifacts also produced a negative result except for the downloaded files, as in the browser open scenario.

5.3.4. I2P Browser Closed

The I2P browser closed scenario results were identical to those of the I2P browser open scenario. The artifacts in the Prefetch and Appdata folders were still in their locations. The Data Artifacts were all present, and the downloaded files from the browsing activities in the file system remained in their various storage locations.

5.3.5. Tor Browser Uninstalled

In this scenario, the Tor, Firefox, and Tor browser installer prefetch files were still found in the default location, even after the removal of the application. Similar to the registry keys for Tor, these artifacts can tell if the application was previously installed and removed from a device. Investigators can also deduce when the application was last used, how often it was run, and the associated timestamps from these artifacts.

The installation path to the Tor application had been removed, and the forensic artifacts stored at “C:\Users\ vboxuser\Tor Browser\Browser\TorBrowser\Data\Tor” were not found in their default location. However, they were present in the slack storage. Slack storage refers to unused space within a file allocation system that can be used for data storage in the future. The cached-cert and cached-microdesc-consensus files were found in the slack storage for both iterations of the experiment, as seen in Fig 16. The state file was found in the slack storage in both iterations of the experiment, but its content was partially overwritten in one of the iterations.

The cached-microdesc.new, geoip, and geoip6 files were found in the slack storage in only one experiment iteration.

The downloaded files from email, search engine, and file sharing were also found in the Slack storage with the Tor browser icon. Other icons associated with Tor, like the DuckDuckGo icon, could not be retrieved from the Slack storage. Other artifacts related to browsing activities, such as web links and browser history, icons of the visited websites, email addresses, sent and received emails and metadata, previewed files, search engine, and wiki search queries, could not be retrieved.

5.3.6. I2P Browser Uninstalled

The I2P browser uninstalled scenario produced the same results as the I2P browser open and the I2P browser closed scenarios for the Prefetch and AppData folders analysis. This means that uninstallation of I2P does not change the artifacts in these locations. Fig 19 shows the content of the i2psnark folder with the torrent artifacts after the I2P uninstallation.

Under the Autopsy “Data Artifacts” section, the Web History, Web Search, Web Downloads, and Web Form Autofill still held the artifacts from the browsing activities performed, but all downloaded files had been removed from their storage locations. These artifacts were retrieved from the Firefox browser and not directly from the I2P router; hence, they were found after the I2P application had been uninstalled.

Other artifacts, such as the I2P icon, dashboard icons, other icons like the national flags that come with the I2P installation, and other files deleted from the I2P uninstallation process were retrieved from the Slack storage. The downloaded files were also found in Slack storage.

Artifacts Category	Artifacts Found	Tor Browser Open	Tor Browser Closed	Tor Browser Uninstalled	I2P Browser Open	I2P Browser Closed	I2P Browser Uninstalled
Existence Artifacts	Prefetch files	✓	✓	✓	✓	✓	✓
	Browser Icons	✓	✓	✓	✓	✓	✓
Interaction Artifacts	Network database and configuration files	✓	✓	✓	✓	✓	✓
	Encryption keys	✓	✓	✓	✗	✗	✗
	Browsing history	✗	✗	✗	✓	✓	✓
	Icons of the visited website	✗	✗	✗	✓	✓	✓
	Email addresses	✗	✗	✗	✓	✓	✓
	Sent email with content and metadata	✗	✗	✗	✓	✓	✓
	Received email with content and metadata	✗	✗	✗	✓	✓	✓
	Download files	✓	✓	✓	✓	✓	✓
	Previewed files	✗	✗	✗	✓	✓	✓
	Search engine search query	✗	✗	✗	✓	✓	✓
	Wiki search query	✗	✗	✗	✓	✓	✓

Table 10. A summary of the forensic artifacts found in the storage.

6. Discussion

The dark web comprises anonymizing networks that help protect users' privacy and freedom of speech by allowing them to communicate online without revealing their identities or locations. This anonymity makes it challenging for governments, ISPs, or other entities to censor or surveil users based on their online activities. This is primarily true in jurisdictions with strict censorship laws or surveillance measures. Encrypting and routing traffic through a decentralized network of volunteer-operated servers allows users to access restricted websites, and other online services like social media platforms without detection.

Law enforcement agencies also utilize the dark web for various purposes, including investigation, intelligence gathering, and combating criminal activities. Tor and I2P have facilitated the development of anonymous marketplaces on the dark web where the trade of illicit goods and services is commonplace. Criminals and threat actors exploit the privacy and anonymity features of the dark web to obfuscate their online activities, making it difficult for law enforcement agencies to track their communications, locations, and identities.

As part of this research, the experiment results will aid law enforcement agencies in cases where Tor or I2P users are under investigation. Knowing what artifacts can be retrieved and where they can be found is vital in such investigations. The path to the source of installation files can be retrieved from the registry and storage. The installation destination can be retrieved from the registry, the storage, and the memory. Browsing activities and application processes can be retrieved only from memory, while the browser history can be found in the storage; however, this only applies to I2P. Network statistics and configuration details, such as overlay information, IP addresses, ports, cryptographic keys, etc., can be found in the memory and the storage. Artifacts relating to the application usage statistics can be found in the registry and the storage. In contrast, the application settings relating to GUI, audio, and other Windows user experience settings can be found in the storage. It is important to note that for all the artifacts that can be retrieved from the memory, a live acquisition must be conducted while the software runs on the target device. These findings are summarized in Table 11.

Even with the privacy and anonymity features of Tor and I2P, forensic artifacts can still be retrieved from devices that communicate over these networks. Knowing what artifacts can be found and where they may be found will increase efficiency and reduce the costs of digital investigation involving these dark web platforms. It would also help dark web users in jurisdictions with strict censorship or under high surveillance measures who seek to communicate

anonymously on the dark web to be aware of the nature of the artifacts that can be retrieved from their devices if they fall into the wrong hands.

Digital forensic investigation is indispensable in the fight against cybercrime, providing crucial evidence for prosecuting offenders and safeguarding digital infrastructures. However, such investigations must adhere meticulously to legal procedures and ethical standards. This entails obtaining proper authorization through warrants or legal processes before conducting searches or seizures of digital evidence, ensuring evidence integrity throughout the investigation, and respecting individuals' privacy rights. Moreover, ethical considerations demand that investigators maintain objectivity, impartiality, and transparency, avoiding any actions compromising the investigation's integrity or infringing upon the rights of suspects or other parties involved. Upholding these principles ensures the legitimacy and admissibility of evidence in legal proceedings. It fosters public trust in law enforcement agencies and the justice system's ability to combat cybercrime effectively while upholding fundamental rights and liberties.

Category of artifacts	Tor			I2P		
	Registry	Memory	Storage	Registry	Memory	Storage
Installation source	✓	✗	✓	✓	✗	✓
Installation destination	✓	✓	✓	✓	✓	✓
Running processes	✗	✓	✗	✗	✓	✗
Browsing activities	✗	✓	✗	✗	✓	✗
Browser history	✗	✗	✗	✗	✗	✓
Application usage	✓	✗	✓	✓	✗	✓
Network statistics and configuration	✗	✓	✓	✗	✓	✓
Application settings	✓	✗	✗	✓	✗	✗

Table 11. A summary of forensic artifacts that can be retrieved from devices communicating over Tor/ I2P and where they can be found.

7. Conclusion

The increase in illicit activities on the dark web has kept the eyes of law enforcement agencies and digital forensic examiners on its use and fostered discussions on curbing such interactions online. While substantial effort is being made in the digital forensic field to keep up with technological advancement, the dark web presents a unique set of challenges in cybersecurity.

This research investigated the forensic artifacts retrieved from a Windows 11 device for Tor and I2P. While both software are designed to provide users with increased privacy and anonymity on the web, our research proved that some digital traces created by using this software can leak valuable information about its use. Tor and I2P produced very similar results in the registry and memory analysis. The major outlier was the I2P encryption keys, which could not be retrieved from the memory. I2P's reliance on Java and lack of a dedicated browser in its software bundle also made the artifacts in the registry less obvious to locate when compared to Tor.

In the storage, the presence and use of both software could be deduced even after they had been uninstalled from the device. The results, however, varied largely because while Tor keeps no track of its browsing activity after use, I2P largely retains digital artifacts relating to its browsing history in the AppData folder even after it has been installed.

7.1. Future Work

Conducting dark web forensics on other operating systems like Linux and mobile operating systems like Android will be interesting. Research into I2P and its behavior when combined with Firefox in private browsing mode will also provide a better understanding of its functions.

References

- [1] A. S. Rajawat, K. Barhanpurkar, D. Mukhopadhyay and A. Ghosh, "A. S. Rajawat, K. Barhanpurkar, D. Mukhopadhyay and A. Ghosh," in *2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON)*, Kuala Lumpur, Malaysia, 2021.
- [2] C. Cilleruelo, L. de-Marcos, J. Junquera-Sánchez and J.-J. Martínez-Herráiz, "Interconnection Between Darknets," *IEEE Internet Computing*, vol. 25, no. 3, pp. 61-70, May-June 2021.
- [3] R. Brinson, H. Wimmer and L. Chen, "Dark Web Forensics: An Investigation of Tracking Dark Web Activity with Digital Forensics," in *2022 Interdisciplinary Research in Technology and Management (IRTM)*, Kolkata, India, 2022.
- [4] M. R. Arshad, M. Hussain, H. Tahir, S. Qadir, Y. Javed and F. I. Ahmed Memon, "Forensic Analysis of Tor Browser on Windows 10 and Android 10 Operating Systems," *IEEE Access*, vol. 9, pp. 141273-141294, 2021.
- [5] V.-M. Angeli, A. Atamli and E. Karafili, "Forensic analysis of Tor in Windows environment: A case study," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, Vienna, Austria, 2022.
- [6] M. Rafique and M. U. Khan, "Exploring Static and Live Digital Forensics: Methods, Practices and Tools," *International Journal of Scientific & Engineering Research*, vol. 4, pp. 1048-1056, 2013.
- [7] K. A. Alghafli, A. Jones and T. A. Martin, "Forensic Analysis of the Windows 7 Registry," *Journal of Digital Forensics, Security and Law*, vol. 5, no. 4, pp. 4-30, 2010.
- [8] M. AlSabah and I. Goldberg, "Performance and Security Improvements for Tor: A Survey," *ACM Computing Surveys*, vol. 49, no. 2, 2016.
- [9] L. Overlier and P. Syverson, "Locating hidden servers," in *2006 IEEE Symposium on Security and Privacy (S&P'06)*, Berkeley/Oakland, CA, USA, 2006.
- [10] R. Dingledine, N. Mathewson and P. Syverson, "Tor: The Second-Generation Onion Router," in *USENIX security symposium*, Berkeley, CA, 2004.

- [11] D. McCoy, K. Bauer, D. Grunwald, T. Kohno and D. Sicker, "Shining light in dark places: Understanding the Tor network," in *Privacy Enhancing Technologies: 8th International Symposium, PETS*, Leuven, Belgium, 2008.
- [12] H. Yin and Y. He, "I2P Anonymous Traffic Detection and Identification," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, Coimbatore, India, 2019.
- [13] R. Magán-Carrión, A. Abellán-Galera, G. Maciá-Fernández and P. García-Teodoro, "Unveiling the I2P web structure: a connectivity analysis," *Computer Networks*, vol. 194, 2021.
- [14] J. P. Timpanaro, I. Christment and O. Festor, "A Bird's Eye View on the I2P Anonymous File-Sharing Environment," in *International Conference on Network and System Security*, Berlin, Heidelberg, 2012.
- [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] S. Soney, C. Balan, P. P. Sajan and E. R. Lalson, "I2P Forensic Analysis," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 6, pp. 1678-1682, 30 March 2020.
- [17] D. L. Winkler, R. J. Boggs, J. E. Sammons and T. Fenger, "Online Anonymity: Forensic Analysis of The Onion Router (TOR) Browser Bundle," in *American Academy of Forensic Sciences: Digital and Multimedia Sciences Section*, 2015.
- [18] A. AL-Khaleel, D. Bani-Salameh and M. I. Al-Saleh, "On the memory artifacts of the tor browser bundle," in *The International Conference on Computing Technology and Information Management*, Dubai, UAE, 2014.
- [19] 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.
- [20] M. Alfosail and P. Norris, "Tor forensics: Proposed workflow for client memory artefacts," *Computers & Security*, vol. 106, p. 102311, 2021.
- [21] T. Leng and A. Yu, "A Framework of Darknet Forensics," in *Proceedings of the 3rd international conference on advanced information science and system*, 2021.

- [22] S. Kauser, T. S. Malik, M. H. Hasan, E. A. P. Akhir and S. M. H. Kazmi, "Windows 10's Browser Forensic Analysis for Tracing P2P Networks' Anonymous Attacks," *Computers, Materials and Continua*, vol. 72, no. 1, pp. 1251-1273, 2022.
- [23] M. Muir, P. Meimich and W. J. Buchanan, "A forensic audit of the tor browser bundle," *Digital Investigation*, vol. 29, pp. 118-128, 2019.
- [24] A. Warren, "Tor Browser Artifacts in Windows 10," The SANS Institute Infosec Read, Room, 2017.
- [25] P. Grassi, J. Fenton, N. Lefkovitz, J. Danker, Y.-Y. Choong, K. Greene and M. Theofanos, "Digital identity guidelines: enrollment and identity proofing," National Institute of Standards and Technology, 2017.
- [26] B. Dolan-Gavitt, "Forensic analysis of the Windows registry in memory," *Digital Investigation*, vol. 5, pp. S26-S32, 2008.

Appendix

A. All The Tor Registry Keys and Values

S/N	Registry Keys and Values
1	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-3314099954-1345764329-2790451392-1000\Device\HarddiskVolume4\Users\vboxuser\Downloads\tor-browser-windows-x86_64-portable-13.0.9.exe: 3C A1 C1 D2 87 6A DA 01 00 00 00 00 00 00 00 00 00 00 02 00 00 00
2	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-3314099954-1345764329-2790451392-1000\Device\HarddiskVolume4\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe: BE 0B 11 F0 87 6A DA 01 00 00 00 00 00 00 00 00 00 00 02 00 00 00
3	HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3314099954-1345764329-2790451392-1000\Device\HarddiskVolume4\Users\vboxuser\Downloads\tor-browser-windows-x86_64-portable-13.0.9.exe: 3C A1 C1 D2 87 6A DA 01 00 00 00 00 00 00 00 00 00 00 02 00 00 00
4	HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3314099954-1345764329-2790451392-1000\Device\HarddiskVolume4\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe: BE 0B 11 F0 87 6A DA 01 00 00 00 00 00 00 00 00 00 00 02 00 00 00
5	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Microsoft\Internet Explorer\LowRegistry\Audio\PolicyConfig\PropertyStore\f3d3e487_0\:{2}.\?hdaudio#func_01&ven_8384&dev_7680&subsys_83847680&rev_1034#{6994ad04-93ef-11d0-a3cc-00a0c9223196}\espeakertopo/00010001\Device\HarddiskVolume4\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe%b{00000000-0000-0000-0000-000000000000}"
6	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\vboxuser\Downloads\tor-browser-windows-x86_64-portable-13.0.9.exe: 53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 70 0C 23 06 8F B0 23 06 01 00 00 00 00 00 00 00 0A 00 21 00 00 A4 58 3D 09 D2 61 D8 01 00 00 00 00 00 00 00 00
7	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\vboxuser\Downloads\tor-browser-windows-x86_64-portable-13.0.9.exe.FriendlyAppName: "Tor Browser Installer"

8	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe.FriendlyAppName: "Tor Browser"
9	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe.ApplicationCompany: "Mozilla Corporation"
10	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\DllPrefetchExperiment\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe: 0x00000000
11	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\Launcher\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe Image: 0x00000000
12	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\Launcher\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe Blocklist: "C:\Users\vboxuser\AppData\Roaming\Tor Project\Firefox\blocklist-6B0C8EF1C2523FF8"
13	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\Launcher\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe Launcher: A2 AE 7E 59 07 00 00 00
14	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\Launcher\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe Browser: 64 2F 83 59 07 00 00 00
15	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\Launcher\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe Telemetry: 0x00000000
16	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe Progress: 0x00000001
17	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe Theme: 0x00000001
18	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe Enabled: 0x00000001

19	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe ScreenX: 0x00000004
20	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe ScreenY: 0x00000004
21	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe Width: 0x000003F4
22	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe Height: 0x000002B3
23	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe Maximized: 0x00000000
24	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe Flags: 0x00000002
25	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe CssToDevPixelScaling: 00 00 00 00 00 00 F0 3F
26	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe UrlbarCSSSpan: 00 00 00 00 00 C0 5D 40 00 00 00 00 00 88 8B 40
27	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe SearchbarCSSSpan: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
28	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000\Software\Tor Project\Firefox\PreXULSkeletonUISettings\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe SpringsCSSSpan: (NULL!)
29	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\vboxuser\Downloads\tor-browser-windows-x86_64-portable-13.0.9.exe.FriendlyAppName: "Tor Browser Installer"

30	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe.FriendlyAppName: "Tor Browser"
31	HKU\S-1-5-21-3314099954-1345764329-2790451392-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe.ApplicationCompany: "Mozilla Corporation"

Table 12. All registry keys and value entries made by the installation of Tor

B. All The I2P Registry Keys and Values

S/N	Registry Keys and Values
1	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\\Device\HarddiskVolume4\Users\ vboxuser\Downloads\i2pinstall_2.4.0_windows.exe: 56 FB DF 0A 33 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00
2	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\\Device\HarddiskVolume4\Program Files (x86)\Common Files\Oracle\Java\javapath_target_1272656\javaw.exe: CF 64 D6 0A 33 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00
3	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\\Device\HarddiskVolume4\Program Files\i2p\i2p.exe: 48 37 3F 90 33 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00
4	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\\Device\HarddiskVolume4\Program Files\i2p\I2Psvc.exe: DF 26 50 D8 33 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00
5	HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\TCP Query User{E462E535-5802-42AE-9EB1-3A6092E031EB}C:\program files\java\jre-1.8\bin\javaw.exe: "v2.10 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Public App=C:\program files\java\jre-1.8\bin\javaw.exe Name=Java(TM) Platform SE binary Desc=Java(TM) Platform SE binary Defer=User "
6	HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\UDP Query User{0E3BF80A-596A-4583-86B9-321FC5C5F13E}C:\program files\java\jre-1.8\bin\javaw.exe: "v2.10 Action=Allow Active=TRUE Dir=In Protocol=17 Profile=Public App=C:\program files\java\jre-1.8\bin\javaw.exe Name=Java(TM) Platform SE binary Desc=Java(TM) Platform SE binary Defer=User "
7	HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\\Device\HarddiskVolume4\Users\ vboxuser\Downloads\i2pinstall_2.4.0_windows.exe: 56 FB DF 0A 33 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00
8	HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\\Device\HarddiskVolume4\Program Files (x86)\Common

	Files\Oracle\Java\javapath_target_1272656\javaw.exe: CF 64 D6 0A 33 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00
9	HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\Device\HarddiskVolume4\Program Files\i2p\i2p.exe: 48 37 3F 90 33 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00
10	HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\Device\HarddiskVolume4\Program Files\i2p\I2Psvc.exe: DF 26 50 D8 33 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00
11	HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\Firewall Rules\TCP Query User{E462E535-5802-42AE-9EB1-3A6092E031EB}C:\program files\java\jre-1.8\bin\javaw.exe: "v2.10 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Public App=C:\program files\java\jre-1.8\bin\javaw.exe Name=Java(TM) Platform SE binary Desc=Java(TM) Platform SE binary Defer=User "
12	HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\Firewall Rules\UDP Query User{0E3BF80A-596A-4583-86B9-321FC5C5F13E}C:\program files\java\jre-1.8\bin\javaw.exe: "v2.10 Action=Allow Active=TRUE Dir=In Protocol=17 Profile=Public App=C:\program files\java\jre-1.8\bin\javaw.exe Name=Java(TM) Platform SE binary Desc=Java(TM) Platform SE binary Defer=User "
13	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Control Panel\NotifyIconSettings\12806010725221006127\UID: 0x00000001
14	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Control Panel\NotifyIconSettings\12806010725221006127\ExecutablePath: "{6D809377-6AF0-444B-8957-A3773F02200E}\Java\jre-1.8\bin\javaw.exe"
15	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Control Panel\NotifyIconSettings\12806010725221006127\InitialTooltip: ""
16	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Control Panel\NotifyIconSettings\12806010725221006127\IconSnapshot: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1F F3 FF 61 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 00 13 49 44 41 54 38 4F 63 18 05 A3 60 14 8C 02 30 60 60 00 00 04 10 00 01 A7 44 7C 63 00 00 00 00 49 45 4E 44 AE 42 60 82
17	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\vboxuser\Downloads\i2pinstall_2.4.0_windows.exe: 53 41 43 50 01 00 00 00 00 00 00 07 00 00 00 28 00 00 00 39 50 70 01 00 00 00 00 01 00 00 00 00 00 00 00

```
00 00 06 71 00 00 00 A4 58 3D 09 D2 61 D8 01 00 00 00 00 00 00 00 02 00 00 00 28 00 00 00
00 00 00 00 00 08 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 75 4C 01 00 00 00 00
00 01 00 00 00 01 00 00 00
```

18 HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Program
Files\i2p\i2p.exe: 53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 AA 32 01 00 A9
7F 01 00 01 00 00 00 00 00 00 00 00 00 0A 71 20 00 00 A4 58 3D 09 D2 61 D8 01 00 00 00 00
00 00 00 00

```

19 HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Software\Microsoft\Windows
   NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Program
   Files\i2p\I2Psvc.exe: 53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 00 94 06 00
   00 00 00 00 01 00 00 00 00 00 00 00 00 00 03 06 73 00 00 00 A4 58 3D 09 D2 61 D8 01 00 00 00
   00 00 00 00 02 00 00 00 28 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00
   00 00 00 00 00 00 1A 35 00 00 00 00 00 00 01 00 00 00 01 00 00 00

```

20 HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\vboxuser\Downloads\i2pinstall
_2.4.0_windows.exe.FriendlyAppName: "7z Setup SFX"

21 HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\vboxuser\Downloads\i2pinstall
_2.4.0_windows.exe.ApplicationCompany: "Igor Pavlov"

22 HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\program files\java\jre-
1.8\bin\javaw.exe.FriendlyAppName: "Java(TM) Platform SE binary"

23 HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\program files\java\jre-
1.8\bin\javaw.exe.ApplicationCompany: "Oracle Corporation"

24 HKU\S-1-5-21-1178577129-3943880853-2800665062-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program
Files\i2p\i2p.exe.FriendlyAppName: "i2p"

25 HKU\S-1-5-21-1178577129-3943880853-2800665062-
1000\Software\Classes\AppUserModelId\NotifyIconGeneratedAumid_12806010725221006127\
DisplayName: "Java(TM) Platform SE binary"

26 HKU\S-1-5-21-1178577129-3943880853-2800665062-
1000\Software\Classes\AppUserModelId\NotifyIconGeneratedAumid_12806010725221006127\I
conUri:
"C:\Users\vboxuser\AppData\Local\Temp\NotifyIconGeneratedAumid_12806010725221006127.
png"

27	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\vboxuser\Downloads\i2pinstall_2.4.0_windows.exe.FriendlyAppName: "7z Setup SFX"	
28	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\vboxuser\Downloads\i2pinstall_2.4.0_windows.exe.ApplicationCompany: "Igor Pavlov"	
29	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\program 1.8\bin\javaw.exe.FriendlyAppName: "Java(TM) Platform SE binary"	files\java\jre-
30	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\program 1.8\bin\javaw.exe.ApplicationCompany: "Oracle Corporation"	files\java\jre-
31	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files\i2p\i2p.exe.FriendlyAppName: "i2p"	
32	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000_Classes\AppData\Local\Temp\NotifyIconGeneratedAumid_12806010725221006127\DisplayN ame: "Java(TM) Platform SE binary"	
33	HKU\S-1-5-21-1178577129-3943880853-2800665062-1000_Classes\AppData\Local\Temp\NotifyIconGeneratedAumid_12806010725221006127\IconUri: "C:\Users\vboxuser\AppData\Local\Temp\NotifyIconGeneratedAumid_12806010725221006127.png"	
34	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\Device\HarddiskVolume4\Program Files\Mozilla Firefox\firefox.exe: 64 E3 C6 8A 2E 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00	
35	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\Device\HarddiskVolume4\Program Files\Mozilla Firefox\firefox.exe: 73 13 28 F2 33 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00	
36	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\Device\HarddiskVolume4\Program Files\Java\jre-1.8\bin\javaw.exe: 7F F6 D9 B2 2F 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00	
37	HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\Device\HarddiskVolume4\Program Files\Java\jre-1.8\bin\javaw.exe: 22 D1 AC 89 33 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00	

38	HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\\Device\HarddiskVolume4\Program Files\Mozilla Firefox\firefox.exe: 64 E3 C6 8A 2E 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00
39	HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\\Device\HarddiskVolume4\Program Files\Mozilla Firefox\firefox.exe: 73 13 28 F2 33 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00
40	HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\\Device\HarddiskVolume4\Program Files\Java\jre-1.8\bin\javaw.exe: 7F F6 D9 B2 2F 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00
41	HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1178577129-3943880853-2800665062-1000\\Device\HarddiskVolume4\Program Files\Java\jre-1.8\bin\javaw.exe: 22 D1 AC 89 33 88 DA 01 00 00 00 00 00 00 00 00 00 02 00 00 00

Table 13. All registry keys and value entries made by the installation and configuration of I2P.

C. Tor Memory Artifacts

```

00501212 00 00 00 00 00 00 B7 1C C7 9B 10 15 00 BF 6F 6E 69 6F 6E 2D 6B 65 .....onion-ke
00501228 79 0A 2D 2D 2D 2D 2D 42 45 47 49 4E 20 52 53 41 20 50 55 42 4C 49 y.-----BEGIN RSA PUBLI
0050123E 43 20 4B 45 59 2D 2D 2D 2D 2D 2D 0A 4D 49 47 4A 41 6F 47 42 41 4C 70 C KEY-----MIGJAoGBALp
00501254 4A 43 65 64 46 6E 68 6B 6A 74 45 69 31 4D 68 47 6A 50 58 35 55 31 JCedFnhkjtEiIMhGjPX5U1
0050126A 49 42 4C 64 73 4C 6B 6B 71 42 4A 61 31 6B 57 78 52 51 65 74 64 4D IBldsLkkqBJa1kWxRQetdM
00501280 57 5A 30 6B 6F 73 34 65 53 0A 4F 35 47 6E 47 67 76 42 51 62 41 4B WZ0kos4eS.O5GnGgvBQbAK
00501296 63 72 76 38 33 73 66 64 5A 6E 2B 2B 72 70 49 46 78 61 38 64 57 49 crv83sfdZn++rpIFxa8dWI
005012AC 31 51 68 69 57 35 58 36 74 30 76 30 76 39 72 39 76 4F 63 56 48 6E lQhiW5X6t0v0v9r9vOcVHn
005012C2 37 36 6B 4C 73 2B 6E 63 0A 4A 6F 59 63 6A 79 46 52 50 67 41 6B 53 76kLs+nc.JoYcjyFRPgAkS
005012D8 66 34 4A 6F 55 43 58 6B 59 41 68 41 38 6A 59 74 68 79 45 6A 52 6A f4JoUCXkyAhA8jYthyEjRj
005012EE 78 73 49 72 31 71 56 4E 78 2B 72 57 51 6F 6F 6F 54 41 67 4D 42 41 xsIr1qVNx+rWQoooTAgMBA
00501304 41 45 3D 0A 2D 2D 2D 2D 45 4E 44 20 52 53 41 20 50 55 42 4C 49 AE=-----END RSA PUBLI
0050131A 43 20 4B 45 59 2D 2D 2D 2D 2D 0A 6E 74 6F 72 2D 6F 6E 69 6F 6E 2D C KEY-----lntor-onion-

```

Fig 5. Tor browser only public key artifact used by Tor for encrypted communication with nodes with the Tor network retrieved with Hex Workshop.

```

03FB3ECA 79 47 52 78 6D 4C 65 4C 73 52 6E 79 43 67 30 0A 73 20 45 78 69 74 yGRxmLeLsRnyCg0.s Exit
03FB3EE0 20 46 61 73 74 20 48 53 44 69 72 20 52 75 6E 6E 69 6E 67 20 53 74 Fast HSDir Running St
03FB3EF6 61 62 6C 65 20 56 32 44 69 72 20 56 61 6C 69 64 0A 76 20 54 6F 72 able V2Dir Valid.v Tor
03FB3F0C 20 30 2E 34 2E 37 2E 31 33 0A 70 72 20 43 6F 6E 73 3D 31 2D 32 20 0.4.7.13.pr Cons=1-2
03FB3F22 44 65 73 63 3D 31 2D 32 20 44 69 72 43 61 63 68 65 3D 32 20 46 6C Desc=1-2 DirCache=2 Fl
03FB3F38 6F 77 43 74 72 6C 3D 31 2D 32 20 48 53 44 69 72 3D 32 20 48 53 49 owCtrl=1-2 HSDir=2 HSI
03FB3F4E 6E 74 72 6F 3D 34 2D 35 20 48 53 52 65 6E 64 3D 31 2D 32 20 4C 69 ntro=4-5 HSrend=1-2 Li
03FB3F64 6E 6B 3D 31 2D 35 20 4C 69 6E 6B 41 75 74 68 3D 31 2C 33 20 4D 69 nk=1-5 LinkAuth=1,3 Mi
03FB3F7A 63 72 6F 64 65 73 63 3D 31 2D 32 20 50 61 64 64 69 6E 67 3D 32 20 crodesc=1-2 Padding=2
03FB3F90 52 65 6C 61 79 3D 31 2D 34 0A 77 20 42 61 6E 64 77 69 64 74 68 3D Relay=1-4.w Bandwidth=
03FB3FA6 39 36 30 30 0A 72 20 52 65 73 65 74 54 68 65 57 6F 72 6C 64 20 41 9600.r ResetTheWorld A
03FB3FBC 79 48 41 77 2B 55 64 71 55 47 5A 63 47 79 6B 4C 31 65 55 74 67 66 yHaw+UdqUGZcGykLleUtgf
03FB3FD2 6A 6C 62 6B 20 32 30 33 38 2D 30 31 2D 30 31 20 30 30 3A 30 30 3A jlbk 2038-01-01 00:00:
03FB3FE8 30 30 20 38 39 2E 31 34 37 2E 31 31 30 2E 31 35 34 20 39 30 30 32 00 89.147.110.154 9002

```

Fig 6. Tor browser only relay node artifacts showing the IP address, ports, bandwidth, and other details used to build the Tor overlay network, retrieved with Hex Workshop.

```

0xb188beab6310 TCPv4 127.0.0.1 9151 0.0.0.0 0 LISTENING 7252 tor.exe 2024-02-25 13:15:38.000000
0xb188beab6890 TCPv4 127.0.0.1 9150 0.0.0.0 0 LISTENING 7252 tor.exe 2024-02-25 13:15:59.000000

```

Fig 7. Tor browser only Volatility netscan artifacts showing tor.exe process listening over ports 9150 and 9151

```
Administrator: Windows PowerShell
Volatility 3 Framework 2.7.0
Progress: 100.00
PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime Audit Cmd Path
7712 4844 firefox.exe 0xb188c06f3080 55 - 1 False 2024-02-25 13:15:34.000000 N/A \Device\HarddiskVolume4
\firefox.exe "C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe" C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe
* 4608 7712 firefox.exe 0xb188bfbf5080 6 - 1 False 2024-02-25 13:15:38.000000 N/A \Device\HarddiskVolume4
\firefox.exe "C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe" -contentproc --channel="7712.4.1965015778\41500912" -parentBuildID
ndle 3544 -prefsLen 22141 -prefMapSize 243588 -appDir "C:\Users\vboxuser\Desktop\Tor Browser\Browser\browser" - {0ec45728-f589-4f92-bf7d-5da2a3
Desktop\Tor Browser\Browser\firefox.exe
* 8160 7712 firefox.exe 0xb188b9b94080 14 - 1 False 2024-02-25 13:15:38.000000 N/A \Device\HarddiskVolume4
\firefox.exe "C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe" -contentproc --channel="7712.7.1413595107\423073369" -childID 6 -is
4192 -prefsLen 22426 -prefMapSize 243588 -jsInitHandle 1392 -jsInitLen 240916 -parentBuildID 20240115174022 -win32kLockedDown -appDir "C:\User
ser" - {2628afb4-d51f-4f19-bd0a-c03250d33225} 7712 tab C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe
* 1796 7712 firefox.exe 0xb188bf88a0c0 21 - 1 False 2024-02-25 13:15:37.000000 N/A \Device\HarddiskVolume4
\firefox.exe "C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe" -contentproc --channel="7712.0.1711020345\1065951767" -parentBuildID
Handle 1916 -prefsLen 19241 -prefMapSize 243588 -appDir "C:\Users\vboxuser\Desktop\Tor Browser\Browser\browser" - {69c24809-ff0e-4296-be47-ed79
Desktop\Tor Browser\Browser\firefox.exe
* 5764 7712 firefox.exe 0xb188bdf6a0c0 14 - 1 False 2024-02-25 13:15:38.000000 N/A \Device\HarddiskVolume4
\firefox.exe "C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe" -contentproc --channel="7712.6.1266394952\1398257315" -childID 5 -i
e 4056 -prefsLen 22426 -prefMapSize 243588 -jsInitHandle 1392 -jsInitLen 240916 -parentBuildID 20240115174022 -win32kLockedDown -appDir "C:\Use
r" - {d7e60f5d-d5c3-4299-a2a8-ed422f73e68d} 7712 tab C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe
* 7272 7712 firefox.exe 0xb188bfabb080 13 - 1 False 2024-02-25 13:16:08.000000 N/A \Device\HarddiskVolume4
\firefox.exe "C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe" -contentproc --channel="7712.8.2141838103\1820967677" -childID 7 -i
e 4372 -prefsLen 22640 -prefMapSize 243588 -jsInitHandle 1392 -jsInitLen 240916 -parentBuildID 20240115174022 -win32kLockedDown -appDir "C:\Use
r" - {ba0817c6-9b5b-4ea9-a7bd-8f6d29273837} 7712 tab C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe
* 7960 7712 firefox.exe 0xb188bdd6a080 22 - 1 False 2024-02-25 13:15:38.000000 N/A \Device\HarddiskVolume4
\firefox.exe "C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe" -contentproc --channel="7712.5.35818264\1116616270" -childID 4 -isF
2920 -prefsLen 22426 -prefMapSize 243588 -jsInitHandle 1392 -jsInitLen 240916 -parentBuildID 20240115174022 -win32kLockedDown -appDir "C:\Users
er" - {97ede4d2-6dec-440a-b79c-846d3b9b06a5} 7712 tab C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe
* 3284 7712 firefox.exe 0xb188becbc080 22 - 1 False 2024-02-25 13:15:37.000000 N/A \Device\HarddiskVolume4
\firefox.exe "C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe" -contentproc --channel="7712.2.1888541895\508212302" -childID 2 -is
2728 -prefsLen 20889 -prefMapSize 243588 -jsInitHandle 1392 -jsInitLen 240916 -parentBuildID 20240115174022 -win32kLockedDown -appDir "C:\User
ser" - {a13d76bd-70f2-4f97-b47d-7214e8ae37d1} 7712 tab C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe
* 7252 7712 tor.exe 0xb188bf88d080 6 - 1 False 2024-02-25 13:15:38.000000 N/A \Device\HarddiskVolume4\Users\v
ser\Tor\tor.exe "C:\Users\vboxuser\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe" --defaults-torrc "C:\Users\vboxuser\Desktop\Tor Browser\
-f "C:\Users\vboxuser\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\torrc" DataDirectory "C:\Users\vboxuser\Desktop\Tor Browser\Browser\TorB
rs\vboxuser\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\onion-auth" GeoIPFile "C:\Users\vboxuser\Desktop\Tor Browser\Browser\TorBrowser\Dat
\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\geoipt6" +__ControlPort 127.0.0.1:9151 HashedControlPasswd 16:b403daf481fb0eba60a6ce12dc90849
27.0.0.1:9150 ExtendedErrors IPv6Traffic PreferIPv6 KeepAliveIsolateSOCKSAuth" __OwningControllerProcess 7712 DisableNetwork 1 C:\Users\vboxus
or\tor.exe
** 4336 7252 conhost.exe 0xb188be0c8080 2 - 1 False 2024-02-25 13:15:38.000000 N/A \Device\HarddiskVolume4
dows\system32\conhost.exe 0x4 C:\Windows\system32\conhost.exe
* 3928 7712 firefox.exe 0xb188bfac3080 21 - 1 False 2024-02-25 13:15:37.000000 N/A \Device\HarddiskVolume4
\firefox.exe "C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe" -contentproc --channel="7712.3.1938941729\1006051796" -childID 3 -i
e 3200 -prefsLen 20966 -prefMapSize 243588 -jsInitHandle 1392 -jsInitLen 240916 -parentBuildID 20240115174022 -win32kLockedDown -appDir "C:\Use
r" - {a2bff3a0-e360-4a80-8afc-a14ef7026483} 7712 tab C:\Users\vboxuser\Desktop\Tor Browser\Browser\firefox.exe
PS C:\volatility3>
```

Fig 8. Tor browser only Volatility pstree artifacts showing tor.exe and firefox.exe processes, their parent PIDs, commands, and paths.

```
Administrator: Windows PowerShell
Volatility 3 Framework 2.7.0
Progress: 100.00
PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime
7712 4844 firefox.exe 0xb188c06f3080 55 - 1 False 2024-02-25 13:15:34.000000
1796 7712 firefox.exe 0xb188bf88a0c0 21 - 1 False 2024-02-25 13:15:37.000000
3284 7712 firefox.exe 0xb188becbc080 22 - 1 False 2024-02-25 13:15:37.000000
3928 7712 firefox.exe 0xb188bfac3080 21 - 1 False 2024-02-25 13:15:37.000000
7252 7712 tor.exe 0xb188bf88d080 6 - 1 False 2024-02-25 13:15:38.000000 N/A
4608 7712 firefox.exe 0xb188bfbf5080 6 - 1 False 2024-02-25 13:15:38.000000
7960 7712 firefox.exe 0xb188bdd6a080 22 - 1 False 2024-02-25 13:15:38.000000
5764 7712 firefox.exe 0xb188bdf6a0c0 14 - 1 False 2024-02-25 13:15:38.000000
8160 7712 firefox.exe 0xb188b9b94080 14 - 1 False 2024-02-25 13:15:38.000000
7272 7712 firefox.exe 0xb188bfabb080 13 - 1 False 2024-02-25 13:16:08.000000
PS C:\volatility3>
```

Fig 9. Tor browser only Volatility pslist artifacts listing tor.exe and firefox.exe processes, their Parent PIDs, and creation time.

D. I2P Memory Artifacts

```

3FE381AA D1 25 A9 87 01 88 1C 00 01 00 49 D4 89 75 57 61 6E 74 20 74 68 65 .%.I..uWant the
3FE381C0 20 69 6E 62 6F 75 6E 64 20 74 75 6E 6E 65 6C 20 66 6F 72 20 FF 00 inbound tunnel for ..
3FE381D6 07 01 1D 74 EE 25 01 88 01 90 17 00 01 00 51 C7 DD 2A 43 6F 6E 6E ...t.%.Q..*Conn

```

Fig 10. I2P browser only string-search for the inbound tunnel, which returned no artifact in Hex Workshop.

```

Administrator: Windows PowerShell
Volatility 3 Framework 2.7.0
Progress: 100.00 PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime
4208 4276 i2p.exe 0xb089143d50c0 0 - 1 True 2024-02-25 18:30:40.000000 2024-02-25 1
6784 4208 javaw.exe 0xb0890ddd5080 119 - 1 False 2024-02-25 18:30:41.000000 N/A
7316 7740 firefox.exe 0xb089144020c0 58 - 1 False 2024-02-25 18:31:18.000000 N/A
9168 7316 firefox.exe 0xb08914192080 17 - 1 False 2024-02-25 18:31:18.000000 N/A
4156 7316 firefox.exe 0xb08910a160c0 5 - 1 False 2024-02-25 18:31:18.000000 N/A
7556 7316 firefox.exe 0xb089144790c0 17 - 1 False 2024-02-25 18:31:19.000000 N/A
6612 7316 firefox.exe 0xb08910a1e080 16 - 1 False 2024-02-25 18:31:19.000000 N/A
8204 7316 firefox.exe 0xb089111600c0 6 - 1 False 2024-02-25 18:31:19.000000 N/A
7980 7316 firefox.exe 0xb08910f33080 18 - 1 False 2024-02-25 18:31:20.000000 N/A
8644 7316 firefox.exe 0xb0891106f080 13 - 1 False 2024-02-25 18:31:20.000000 N/A
856 7316 firefox.exe 0xb089149e8080 13 - 1 False 2024-02-25 18:31:20.000000 N/A
6708 7316 firefox.exe 0xb089141bc080 13 - 1 False 2024-02-25 18:31:24.000000 N/A
PS C:\volatility3>

```

Fig 11. I2P browser only Volatility pslist artifacts showing i2p.exe, javaw.exe and firefox.exe processes.


```
Administrator: Windows PowerShell
Volatility 3 Framework 2.7.0
Progress: 100.00
PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime Audit Cmd Path
732 624 winlogon.exe 0xb08911666080 5 - 1 False 2024-02-25 18:28:58.000000 N/A \Device\HarddiskVolume4\Window
s\System32\winlogon.exe winlogon.exe C:\Windows\system32\winlogon.exe
* 4228 732 userinit.exe 0xb089137b80c0 0 - 1 False 2024-02-25 18:29:06.000000 2024-02-25 18:29:32.000000 \Devic
e\HarddiskVolume4\Windows\System32\userinit.exe -
** 4276 4228 explorer.exe 0xb089137da0c0 98 - 1 False 2024-02-25 18:29:06.000000 N/A \Device\HarddiskVolume4\Window
s\explorer.exe C:\Windows\Explorer.EXE C:\Windows\Explorer.EXE
*** 4208 4276 i2p.exe 0xb089143d50c0 0 - 1 True 2024-02-25 18:30:40.000000 2024-02-25 18:30:52.000000 \Devic
e\HarddiskVolume4\Program Files\i2p\i2p.exe -
**** 6784 4208 javaw.exe 0xb0890ddd5080 119 - 1 False 2024-02-25 18:30:41.000000 N/A \Device\HarddiskVolume
4\Program Files\Java\jre-1.8\bin\javaw.exe "C:\Program Files\Java\jre-1.8\bin\javaw.exe" -Xmx128m -Djava.library.path=.;lib -DloggerFilenameOverr
ide=logs/log-router-@.txt -Dorg.mortbay.http.Version.paranoid=true -Dorg.mortbay.util.FileResource.checkAliases=false -jar "C:\Program Files\i2p\i2p.e
xe" C:\Program Files\Java\jre-1.8\bin\javaw.exe
7316 7740 firefox.exe 0xb089144020c0 58 - 1 False 2024-02-25 18:31:18.000000 N/A \Device\HarddiskVolume4\Progra
m Files\Mozilla Firefox\firefox.exe "C:\Program Files\Mozilla Firefox\firefox.exe" C:\Program Files\Mozilla Firefox\firefox.exe
* 7556 7316 firefox.exe 0xb089144790c0 17 - 1 False 2024-02-25 18:31:19.000000 N/A \Device\HarddiskVolume4\Progra
m Files\Mozilla Firefox\firefox.exe "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=1424 -childID 1 -isForBrowser -prefsHand
le 3152 -prefMapHandle 2880 -prefsLen 31591 -prefMapSize 244510 -jsInitHandle 1368 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -
appDir "C:\Program Files\Mozilla Firefox\browser" - {40a69163-9129-4208-a357-3cee5a1c152c} 7316 "\\.\pipe\gecko-crash-server-pipe.7316" 1e65cf78150 ta
b C:\Program Files\Mozilla Firefox\firefox.exe
* 8644 7316 firefox.exe 0xb0891106f080 13 - 1 False 2024-02-25 18:31:20.000000 N/A \Device\HarddiskVolume4\Progra
m Files\Mozilla Firefox\firefox.exe "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=5068 -childID 4 -isForBrowser -prefsHand
le 4988 -prefMapHandle 4992 -prefsLen 30542 -prefMapSize 244510 -jsInitHandle 1368 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -
appDir "C:\Program Files\Mozilla Firefox\browser" - {2550cf9e-dc9f-4067-a238-3f37031379a2} 7316 "\\.\pipe\gecko-crash-server-pipe.7316" 1e660d11d90 ta
b C:\Program Files\Mozilla Firefox\firefox.exe
* 8204 7316 firefox.exe 0xb089111600c0 6 - 1 False 2024-02-25 18:31:19.000000 N/A \Device\HarddiskVolume4\Progra
m Files\Mozilla Firefox\firefox.exe "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=4476 -parentBuildID 20240213221259 -sand
boxingKind 0 -prefsHandle 4008 -prefMapHandle 4456 -prefsLen 36891 -prefMapSize 244510 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\bro
wser" - {bdf77f14-e2cb-4fd9-8e9a-64b203d5b5a9} 7316 "\\.\pipe\gecko-crash-server-pipe.7316" 1e660388110 utility C:\Program Files\Mozilla Firefox\firef
ox.exe
* 7980 7316 firefox.exe 0xb08910f33080 18 - 1 False 2024-02-25 18:31:20.000000 N/A \Device\HarddiskVolume4\Progra
m Files\Mozilla Firefox\firefox.exe "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=4852 -childID 3 -isForBrowser -prefsHand
le 4744 -prefMapHandle 4748 -prefsLen 30542 -prefMapSize 244510 -jsInitHandle 1368 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -
appDir "C:\Program Files\Mozilla Firefox\browser" - {f8e2fd59-75cb-41dc-ade9-eae988be3957} 7316 "\\.\pipe\gecko-crash-server-pipe.7316" 1e660d11bd0 ta
b C:\Program Files\Mozilla Firefox\firefox.exe
* 9168 7316 firefox.exe 0xb08914192080 17 - 1 False 2024-02-25 18:31:18.000000 N/A \Device\HarddiskVolume4\Progra
m Files\Mozilla Firefox\firefox.exe "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=1820 -parentBuildID 20240213221259 -pref
sHandle 1736 -prefMapHandle 1728 -prefsLen 31450 -prefMapSize 244510 -appDir "C:\Program Files\Mozilla Firefox\browser" - {28f4305a-588a-4e09-b4ac-ea7
ce00e9e32} 7316 "\\.\pipe\gecko-crash-server-pipe.7316" 1e656fc9510 gpu C:\Program Files\Mozilla Firefox\firefox.exe
* 6612 7316 firefox.exe 0xb08910a1e080 16 - 1 False 2024-02-25 18:31:19.000000 N/A \Device\HarddiskVolume4\Progra
m Files\Mozilla Firefox\firefox.exe "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=4076 -childID 2 -isForBrowser -prefsHand
le 4092 -prefMapHandle 4084 -prefsLen 36019 -prefMapSize 244510 -jsInitHandle 1368 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -
appDir "C:\Program Files\Mozilla Firefox\browser" - {b0b2159e-bb44-455a-8f12-4f0b020d608c} 7316 "\\.\pipe\gecko-crash-server-pipe.7316" 1e65e449850 ta
b C:\Program Files\Mozilla Firefox\firefox.exe
* 6708 7316 firefox.exe 0xb089141bc080 13 - 1 False 2024-02-25 18:31:24.000000 N/A \Device\HarddiskVolume4\Progra
m Files\Mozilla Firefox\firefox.exe "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=5824 -childID 6 -isForBrowser -prefsHand
le 5840 -prefMapHandle 5836 -prefsLen 30542 -prefMapSize 244510 -jsInitHandle 1368 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -
appDir "C:\Program Files\Mozilla Firefox\browser" - {e0cd4556-375d-4805-925b-c558dbd5638b} 7316 "\\.\pipe\gecko-crash-server-pipe.7316" 1e66298cbd0 ta
b C:\Program Files\Mozilla Firefox\firefox.exe
* 856 7316 firefox.exe 0xb089149e8080 13 - 1 False 2024-02-25 18:31:20.000000 N/A \Device\HarddiskVolume4\Progra
m Files\Mozilla Firefox\firefox.exe "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=5176 -childID 5 -isForBrowser -prefsHand
le 5184 -prefMapHandle 5188 -prefsLen 30542 -prefMapSize 244510 -jsInitHandle 1368 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -
appDir "C:\Program Files\Mozilla Firefox\browser" - {ac5abc9a-eb06-4386-8723-fb644bfa30a3} 7316 "\\.\pipe\gecko-crash-server-pipe.7316" 1e660d11f50 ta
b C:\Program Files\Mozilla Firefox\firefox.exe
* 4156 7316 firefox.exe 0xb08910a160c0 5 - 1 False 2024-02-25 18:31:18.000000 N/A \Device\HarddiskVolume4\Progra
m Files\Mozilla Firefox\firefox.exe "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=2212 -parentBuildID 20240213221259 -pref
sHandle 2204 -prefMapHandle 2192 -prefsLen 31450 -prefMapSize 244510 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {6fbeb743-
22a5-4bd1-af96-d62267c0e5d1} 7316 "\\.\pipe\gecko-crash-server-pipe.7316" 1e64b180110 socket C:\Program Files\Mozilla Firefox\firefox.exe
PS C:\volatility3>
```

Fig 12. I2P browser only Volatility pstree artifacts showing i2p.exe, javaw.exe, and firefox.exe processes, their parent PIDs, commands, and paths.

Volatility 3 Framework 2.7.0											
Progress: 100.00											
PDB scanning finished											
Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Owner	Created		
0xb0890d4bdb50	TCPv6	7f00:1::402:496f:4362	7659	::	0	LISTENING	6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb0890d4bdc00	TCPv6	7f00:1::402:496f:4362	7657	::	0	LISTENING	6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb0890f0b45d0	TCPv6	a00:20f::402:4934:6169	7652	::	0	LISTENING	6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb0890f0c0890	TCPv6	7f00:1::402:496f:4362	4444	::	0	LISTENING	6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb0890f0c14f0	TCPv6	7f00:1::402:496f:4362	7658	::	0	LISTENING	6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb08911d021b0	TCPv6	7f00:1::402:496f:4362	4445	::	0	LISTENING	6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb08911d025d0	TCPv4	0.0.0.0	27605	0.0.0.0	0	LISTENING	6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb08911d025d0	TCPv6	::	27605	::	0	LISTENING	6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb08911d02cb0	TCPv6	::1	7657	::	0	LISTENING	6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb08911d02e10	TCPv6	7f00:1::402:496f:4362	7654	::	0	LISTENING	6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb08911d034f0	TCPv6	7f00:1::402:496f:4362	7660	::	0	LISTENING	6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb08911d03e90	TCPv6	7f00:1::402:496f:4362	6668	::	0	LISTENING	6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb089147a5910	UDPv4	0.0.0.0	1900	*	0		6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb089147a5dc0	UDPv4	0.0.0.0	1900	*	0		6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb089147a5dc0	UDPv6	::	1900	*	0		6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb08914888c70	UDPv6	a00:20f::402:4934:6169	7653	*	0		6784	javaw.exe	2024-02-25 18:30:43.000000		
0xb0891489abf0	UDPv4	0.0.0.0	27605	*	0		6784	javaw.exe	2024-02-25 18:30:46.000000		
0xb0891489abf0	UDPv6	::	27605	*	0		6784	javaw.exe	2024-02-25 18:30:46.000000		

Fig 13. I2P browser-only Volatility netscan artifacts listing i2p.exe, javaw.exe, and firefox.exe processes, their Parent PIDs, and creation time.

E. Tor Storage Artifacts

Listing								
/img_torOpen.img/vol_vol7/Windows/Prefetch								
Table	Thumbnail	Summary						
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
SYSTEMSETTINGSADMINFLOWS.EXE-B5F2FFDC.pf				2024-02-25 14:28:45 CET	2024-02-25 14:28:45 CET	2024-02-25 14:28:45 CET	2024-02-25 14:28:45 CET	7634
SYSTEMSETTINGSBROKER.EXE-4BB8D329.pf				2024-02-25 14:16:58 CET	2024-02-25 14:16:58 CET	2024-02-25 14:16:58 CET	2024-02-25 14:16:58 CET	14006
TASKHOSTW.EXE-1EAF2222.pf				2024-02-25 14:27:11 CET	2024-02-25 14:27:11 CET	2024-02-25 14:27:11 CET	2024-02-25 13:09:34 CET	19260
TIWORKER.EXE-26EFB80E.pf				2024-02-25 14:27:11 CET	2024-02-25 14:27:11 CET	2024-02-25 14:27:11 CET	2024-02-25 13:13:50 CET	18855
TOR-BROWSER-WINDOWS-X86_64-PO-05DE8DD8.pf				2024-02-25 14:15:14 CET	2024-02-25 14:15:14 CET	2024-02-25 14:15:14 CET	2024-02-25 14:15:14 CET	42350
TOR.EXE-4672E5EF.pf				2024-02-25 14:15:47 CET	2024-02-25 14:15:47 CET	2024-02-25 14:15:47 CET	2024-02-25 14:15:47 CET	8666
TRUSTEDINSTALLER.EXE-B018CCBF.pf				2024-02-25 14:27:11 CET	2024-02-25 14:27:11 CET	2024-02-25 14:27:11 CET	2024-02-25 13:13:49 CET	4334
VBOXCERTUTIL.EXE-8078CBAE.pf				2024-02-25 13:11:50 CET	2024-02-25 14:11:43 CET	2024-02-25 13:11:50 CET	2024-02-25 13:11:48 CET	3381
VBOXDRVINST.EXE-128B6CBA.pf				2024-02-25 13:11:56 CET	2024-02-25 14:11:43 CET	2024-02-25 13:11:56 CET	2024-02-25 13:11:52 CET	14669
VBOXTRAY.EXE-7AA2476D.pf				2024-02-25 14:12:27 CET	2024-02-25 14:12:27 CET	2024-02-25 14:12:27 CET	2024-02-25 14:12:27 CET	5689
VBOXWINDOWSADDITIONS-AMD64.EX-85C5A15E.pf				2024-02-25 13:11:46 CET	2024-02-25 14:11:43 CET	2024-02-25 13:11:46 CET	2024-02-25 13:11:46 CET	15034
VBOXWINDOWSADDITIONS.EXE-EE01DD11.pf				2024-02-25 13:11:43 CET	2024-02-25 14:11:43 CET	2024-02-25 13:11:43 CET	2024-02-25 13:11:43 CET	17429
VERCLSID.EXE-D9CCBE06.pf				2024-02-25 13:13:15 CET	2024-02-25 14:11:43 CET	2024-02-25 13:13:15 CET	2024-02-25 13:13:15 CET	3279
VSSVC.EXE-206E55B3.pf				2024-02-25 14:22:03 CET	2024-02-25 14:22:03 CET	2024-02-25 14:22:03 CET	2024-02-25 14:22:03 CET	4537
<								
Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations
Other Occurrences								
Result: 1 of 1 Result < >								
Type	Value							
Program Name	TOR.EXE							
Path	/USERS/VBOXUSER/DESKTOP/TOR BROWSER/BROWSER/TORBROWSER/TOR							
Date/Time	2024-02-25 14:15:38 CET							
Count	1							
Comment	Prefetch File							
Source File Path	/img_torOpen.img/vol_vol7/Windows/Prefetch/TOR.EXE-4672E5EF.pf							
Artifact ID	-9223372036854775004							

Fig 14. tor.exe prefetch file showing the installation path, usage count, and timestamps from the Tor browser open scenario.

Listing								
/img_torOpen.img/vol_vol7/Windows/Prefetch								
Table	Thumbnail	Summary						
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
SYSTEMSETTINGSADMINFLOWS.EXE-B5F2FFDC.pf				2024-02-25 14:28:45 CET	2024-02-25 14:28:45 CET	2024-02-25 14:28:45 CET	2024-02-25 14:28:45 CET	7634
SYSTEMSETTINGSBROKER.EXE-4BB8D329.pf				2024-02-25 14:16:58 CET	2024-02-25 14:16:58 CET	2024-02-25 14:16:58 CET	2024-02-25 14:16:58 CET	14006
TASKHOSTW.EXE-1EAF2222.pf				2024-02-25 14:27:11 CET	2024-02-25 14:27:11 CET	2024-02-25 14:27:11 CET	2024-02-25 13:09:34 CET	19260
TIWORKER.EXE-26EFB80E.pf				2024-02-25 14:27:11 CET	2024-02-25 14:27:11 CET	2024-02-25 14:27:11 CET	2024-02-25 13:13:50 CET	18855
TOR-BROWSER-WINDOWS-X86_64-PO-05DE8DD8.pf				2024-02-25 14:15:14 CET	2024-02-25 14:15:14 CET	2024-02-25 14:15:14 CET	2024-02-25 14:15:14 CET	42350
TOR.EXE-4672E5EF.pf				2024-02-25 14:15:47 CET	2024-02-25 14:15:47 CET	2024-02-25 14:15:47 CET	2024-02-25 14:15:47 CET	8666
TRUSTEDINSTALLER.EXE-B018CCBF.pf				2024-02-25 14:27:11 CET	2024-02-25 14:27:11 CET	2024-02-25 14:27:11 CET	2024-02-25 13:13:49 CET	4334
VBOXCERTUTIL.EXE-8078CBAE.pf				2024-02-25 13:11:50 CET	2024-02-25 14:11:43 CET	2024-02-25 13:11:50 CET	2024-02-25 13:11:48 CET	3381
VBOXDRVINST.EXE-128B6CBA.pf				2024-02-25 13:11:56 CET	2024-02-25 14:11:43 CET	2024-02-25 13:11:56 CET	2024-02-25 13:11:52 CET	14669
VBOXTRAY.EXE-7AA2476D.pf				2024-02-25 14:12:27 CET	2024-02-25 14:12:27 CET	2024-02-25 14:12:27 CET	2024-02-25 14:12:27 CET	5689
VBOXWINDOWSADDITIONS-AMD64.EX-85C5A15E.pf				2024-02-25 13:11:46 CET	2024-02-25 14:11:43 CET	2024-02-25 13:11:46 CET	2024-02-25 13:11:46 CET	15034
VBOXWINDOWSADDITIONS.EXE-EE01DD11.pf				2024-02-25 13:11:43 CET	2024-02-25 14:11:43 CET	2024-02-25 13:11:43 CET	2024-02-25 13:11:43 CET	17429
VERCLSID.EXE-D9CCBE06.pf				2024-02-25 13:13:15 CET	2024-02-25 14:11:43 CET	2024-02-25 13:13:15 CET	2024-02-25 13:13:15 CET	3279
VSSVC.EXE-206E55B3.pf				2024-02-25 14:22:03 CET	2024-02-25 14:22:03 CET	2024-02-25 14:22:03 CET	2024-02-25 14:22:03 CET	4537
<								
Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations
Other Occurrences	Result: 1 of 1 Result < >							
Type	Value							
Program Name	TOR-BROWSER-WINDOWS-X86_64-PO							
Path								
Date/Time	2024-02-25 14:15:04 CET							
Count	1							
Comment	Prefetch File							
Source File Path	/img_torOpen.img/vol_vol7/Windows/Prefetch/TOR-BROWSER-WINDOWS-X86_64-PO-05DE8DD8.pf							
Artifact ID	-9223372036854775005							

Fig 15. Tor installer prefetch file from the Tor browser open scenario showing the usage count, and timestamps but no information on the file path.

Listing

File System

Table

Thumbnail

Summary

Page: 1 of 10

Pages: ↩ →

Go to Page:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2024-02-25 14:15:38 CET	2024-02-25 14:15:38 CET	2024-02-25 14:31:45 CET	2024-02-25 14:15:38 CET	48
[parent folder]				2024-02-25 15:04:03 CET	2024-02-25 15:04:03 CET	2024-02-25 15:04:03 CET	2024-02-25 14:15:38 CET	48
search.json.mozlz4				2024-02-25 14:15:39 CET	2024-02-25 14:15:39 CET	2024-02-25 14:15:39 CET	2024-02-25 14:15:39 CET	337
extended_PFL_Package_for_RollupFix~~amd64~~2				2024-02-25 14:30:15 CET	2024-02-25 14:33:15 CET	2024-02-25 14:30:15 CET	2024-02-25 14:30:15 CET	1211
containers.json				2024-02-25 14:15:39 CET	2024-02-25 14:15:39 CET	2024-02-25 14:15:39 CET	2024-02-25 14:15:39 CET	875
handlers.json				2024-02-25 14:15:40 CET	2024-02-25 14:15:40 CET	2024-02-25 14:15:40 CET	2024-02-25 14:15:40 CET	410
cached-microdesc-consensus				2024-02-25 14:16:01 CET	2024-02-25 14:16:01 CET	2024-02-25 14:16:01 CET	2024-02-25 14:16:01 CET	2686291
cached-certs				2024-02-25 14:16:02 CET	2024-02-25 14:16:02 CET	2024-02-25 14:16:02 CET	2024-02-25 14:16:01 CET	18574
UpdateInfo				2024-02-25 15:04:03 CET	2024-02-25 15:04:03 CET	2024-02-25 15:04:03 CET	2024-02-25 14:16:06 CET	48
[current folder]				2024-02-25 15:04:03 CET	2024-02-25 15:04:03 CET	2024-02-25 15:04:03 CET	2024-02-25 14:16:06 CET	48
[parent folder]				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
updates				2024-02-25 15:04:03 CET	2024-02-25 15:04:03 CET	2024-02-25 15:04:03 CET	2024-02-25 14:16:09 CET	48
[current folder]				2024-02-25 15:04:03 CET	2024-02-25 15:04:03 CET	2024-02-25 15:04:03 CET	2024-02-25 14:16:09 CET	48
[parent folder]				2024-02-25 15:04:03 CET	2024-02-25 15:04:03 CET	2024-02-25 15:04:03 CET	2024-02-25 14:16:06 CET	48

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 1 of - Page

Matches on page: - of - Match

100%

Reset

```

dir-key-certificate-version 3
fingerprint 49015F787433103580E3B66A1707A00E60F2D15B
dir-key-published 2023-12-12 07:10:31
dir-key-expires 2024-03-12 07:10:31
dir-identity-key
-----BEGIN RSA PUBLIC KEY-----
MIIBigKCAyEAxVbS0noZKz1Ei6858RGyyuQgwQUKG4Urrp2BiAzkYxwX+6fUrlut
AjeLb4YsqCdNdUipuLRQ2Qly1C220QiCHV6jZAsM4tmEq6TpK6q1Xi5YPKqbGS
CfUQT1nO4s4DCYSLCwiRny6bMe8tNHc0MpXP3loCbPkYCoXrEL6vYIOW3oeGWE
KbFPQrzYJAPhUgUubBib5Y5IkUY9N/5QZw2y1bn+ dq9mFOoCIHLd6DkQmySmftnMe
QrpYA2WvE4M5yN2HB8QG7T7dzXPPL6889fW/mjqYExQPX7cqmlKchsB7l5whjA
u0oodF8Y9ooK9QT0GeK4h3xQhzNG17anuUxbZ7sxzmBwBNmkNylWEEIntazyRFR
P2mDY/9YK2JOQKkh3tKI1whcCG9ZtAhKmm/ijG7OrhqtusdGKBXlgALf4f11AK1
gNcacDx2fJzRHuNK8zkiORAZStxKdLbAbBNELenk1zBjSkxCOJH4mBpr8TXULq1
ThLI/8OzZq4LAgMBAAE=
-----END RSA PUBLIC KEY-----
dir-signing-key
-----BEGIN RSA PUBLIC KEY-----
MIIBBgKCAQEAr25jmxqSAa4JGzVKY9jCWFe35IQWv/8Xf9wigoGPfvhSSx0KgiR
3GPKs9qnpdMpy9RfNF0/nugCMFIE7M5M5sqfWvltMm5Fa91zGjaLs5okWfuiED3g
Q/Az8zoxBJUcs70e6Lxf1zvJ3FoMR0xc99aYkkl00qcH0+ ZsUK+ dSnXKrmGNxDqK
AEzUIGQj/LPJqAr3+ QKFdUs4gehd6dtyG1OITrqcEt1M5fj8X6ejd1A1Vd4nq4AH
f97r8kwbQfbp+ XFB0/YTNqOT5ymttL9bgLuCmg3FeZQ3jf35RHoE4R8Dv74n2nq7
RjF6LWN12kfZ+ zwG1oRmX9WDCLVgBq3eQIDAQAB
-----END RSA PUBLIC KEY-----
dir-key-crosscert
-----BEGIN ID SIGNATURE-----
eDQK5kloCtF3ZV7mwbD0C/KiuauLCicMxvo4Ds8M5buVwLAaGG7IkXdpC1xUI+ v
Y0paCGZJUKA9GMTHfdQDZr4Qc8Ljm7VsroYUuLLxELJhmVDOsRniFFRnqSkqpl9x
m/0gpWmvuWMGXnzOOJLI520bV+ fmSAka9RT0BzDKN580GxlgF/EyBsGXzp6XZpE9
IIFZZWnqLqui5oPPsVL0OP57dh+ lvzNd2FA2UFIXnm5ECMcllcXffpC/Czf2H5Da















```

Fig 16. The cached-cert file recovered from the slack storage in the Tor browser open scenario shows the encryption keys used by the Tor application.

F. I2P Storage Artifacts

Listing

/img_i2pClosed.img/vol_vol7/Windows/Prefetch

Table	Thumbnail	Summary							
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	
 GRPCONV.EXE-926E9525.pf			0	2024-02-25 19:12:23 CET	2024-02-25 19:29:03 CET	2024-02-25 20:32:16 CET	2024-02-25 19:12:23 CET	3411	
 I2P.EXE-9EFBD94E.pf			0	2024-02-25 19:30:51 CET	2024-02-25 19:30:51 CET	2024-02-25 20:32:16 CET	2024-02-25 19:30:51 CET	5937	
 I2PINSTALL_2.4.0_WINDOWS.EXE-BBE1D2B0.pf			0	2024-02-25 19:24:08 CET	2024-02-25 19:29:03 CET	2024-02-25 20:32:16 CET	2024-02-25 19:24:08 CET	31853	
 ICACLS.EXE-B1BB271D.pf			0	2024-02-25 19:24:13 CET	2024-02-25 19:29:03 CET	2024-02-25 20:32:16 CET	2024-02-25 19:24:01 CET	2367	
 IDENTITY_HELPER.EXE-03BA1B6E.pf			0	2024-02-25 19:31:27 CET	2024-02-25 19:31:27 CET	2024-02-25 20:32:16 CET	2024-02-25 19:31:16 CET	17318	
 IEXPLORE.EXE-7A9337F2.pf			0	2024-02-25 19:30:48 CET	2024-02-25 19:30:48 CET	2024-02-25 20:32:16 CET	2024-02-25 19:26:18 CET	17660	
 INSTALLER.EXE-9069A145.pf			0	2024-02-25 19:09:11 CET	2024-02-25 19:29:03 CET	2024-02-25 20:32:16 CET	2024-02-25 19:09:11 CET	15126	
 JAVA.EXE-FBFEC892.pf			0	2024-02-25 19:24:20 CET	2024-02-25 19:29:03 CET	2024-02-25 20:32:16 CET	2024-02-25 19:24:12 CET	11882	
 JAVAW.EXE-00FDF375.pf			0	2024-02-25 19:30:51 CET	2024-02-25 19:30:51 CET	2024-02-25 20:32:16 CET	2024-02-25 19:09:02 CET	54606	
 JAVAW.EXE-87BBC398.pf			0	2024-02-25 19:24:09 CET	2024-02-25 19:29:03 CET	2024-02-25 20:32:16 CET	2024-02-25 19:24:09 CET	28509	
 JAVAWS.EXE-6C33614C.pf			0	2024-02-25 19:09:12 CET	2024-02-25 19:29:03 CET	2024-02-25 20:32:16 CET	2024-02-25 19:09:11 CET	5510	
 JRE-8U401-WINDOWS-X64.EXE-35A1E1CD.pf			0	2024-02-25 19:08:52 CET	2024-02-25 19:29:03 CET	2024-02-25 20:32:16 CET	2024-02-25 19:08:52 CET	47702	
 JRE-8U401-WINDOWS-X64.EXE-C5743275.pf			0	2024-02-25 19:08:51 CET	2024-02-25 19:29:03 CET	2024-02-25 20:32:16 CET	2024-02-25 19:08:51 CET	45884	
 JUSCHED.EXE-4B303C70.pf			0	2024-02-25 19:29:44 CET	2024-02-25 19:29:44 CET	2024-02-25 20:32:16 CET	2024-02-25 19:14:24 CET	5425	

<

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Result: 1 of 1

Result

<

>

Type	Value
Program Name	I2P.EXE
Path	/PROGRAM FILES/I2P
Date/Time	2024-02-25 19:30:41 CET
Count	1
Comment	Prefetch File
Source File Path	/img_i2pClosed.img/vol_vol7/Windows/Prefetch/I2P.EXE-9EFBD94E.pf
Artifact ID	-9223372036854775179

Fig 17. i2p.exe prefetch file showing the installation path, usage count, and timestamps from the I2P browser open scenario.















Listing

/img_i2pOpen.img/vol_vol7/Windows/Prefetch

Table

Thumbnail

Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
 I2P.EXE-9EFBD94E.pf				2024-02-25 19:30:51 CET	2024-02-25 19:30:51 CET	2024-02-25 19:30:51 CET	2024-02-25 19:30:51 CET	5937
 I2PINSTALL_2.4.0_WINDOWS.EXE-BBE1D2B0.pf				2024-02-25 19:24:08 CET	2024-02-25 19:29:03 CET	2024-02-25 19:24:08 CET	2024-02-25 19:24:08 CET	31853
 ICACLS.EXE-B1BB271D.pf				2024-02-25 19:24:13 CET	2024-02-25 19:29:03 CET	2024-02-25 19:24:13 CET	2024-02-25 19:24:01 CET	2367
 IDENTITY_HELPER.EXE-03BA1B6E.pf				2024-02-25 19:31:27 CET	2024-02-25 19:31:27 CET	2024-02-25 19:31:27 CET	2024-02-25 19:31:16 CET	17318
 IEXPLORE.EXE-7A9337F2.pf				2024-02-25 19:30:48 CET	2024-02-25 19:30:48 CET	2024-02-25 19:30:48 CET	2024-02-25 19:26:18 CET	17660
 INSTALLER.EXE-9069A145.pf				2024-02-25 19:09:11 CET	2024-02-25 19:29:03 CET	2024-02-25 19:09:11 CET	2024-02-25 19:09:11 CET	15126
 JAVA.EXE-FBFEC892.pf				2024-02-25 19:24:20 CET	2024-02-25 19:29:03 CET	2024-02-25 19:24:20 CET	2024-02-25 19:24:12 CET	11882
 JAVAW.EXE-00FDF375.pf				2024-02-25 19:30:51 CET	2024-02-25 19:30:51 CET	2024-02-25 19:30:51 CET	2024-02-25 19:09:02 CET	54606
 JAVAW.EXE-87BBC398.pf				2024-02-25 19:24:09 CET	2024-02-25 19:29:03 CET	2024-02-25 19:24:09 CET	2024-02-25 19:24:09 CET	28509
 JAVAWS.EXE-6C33614C.pf				2024-02-25 19:09:12 CET	2024-02-25 19:29:03 CET	2024-02-25 19:09:12 CET	2024-02-25 19:09:11 CET	5510
 JRE-8U401-WINDOWS-X64.EXE-35A1E1CD.pf				2024-02-25 19:08:52 CET	2024-02-25 19:29:03 CET	2024-02-25 19:08:52 CET	2024-02-25 19:08:52 CET	47702
 JRE-8U401-WINDOWS-X64.EXE-C5743275.pf				2024-02-25 19:08:51 CET	2024-02-25 19:29:03 CET	2024-02-25 19:08:51 CET	2024-02-25 19:08:51 CET	45884
 JUSCHED.EXE-4B303C70.pf				2024-02-25 19:29:44 CET	2024-02-25 19:29:44 CET	2024-02-25 19:29:44 CET	2024-02-25 19:14:24 CET	5425
 MAINTENANCESERVICE.EXE-3122AC73.pf				2024-02-25 19:07:32 CET	2024-02-25 19:29:03 CET	2024-02-25 19:07:32 CET	2024-02-25 19:07:32 CET	4170
<								

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Result: 1 of 1

Result

<

>

Type	Value
Program Name	I2PINSTALL_2.4.0_WINDOWS.EXE
Path	/THESIS
Date/Time	2024-02-25 19:23:57 CET
Count	1
Comment	Prefetch File
Source File Path	/img_i2pOpen.img/vol_vol7/Windows/Prefetch/I2PINSTALL_2.4.0_WINDOWS.EXE-BBE1D2B0.pf
Artifact ID	-9223372036854775184

Fig 18. I2P installer prefetch file from the I2P browser open scenario showing the file path, usage count, and timestamps.

Listing									
/img_i2pClosed.img/vol_vol7/Users/vboxuser/AppData/Local/I2P/i2psnark									
Table	Thumbnail	Summary							
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	
[current folder]				2024-02-25 20:18:11 CET	2024-02-25 20:18:11 CET	2024-02-25 20:18:11 CET	2024-02-25 19:26:14 CET	56	
[parent folder]				2024-02-25 20:26:56 CET	2024-02-25 20:26:56 CET	2024-02-25 20:26:56 CET	2024-02-25 19:26:12 CET	168	
Epycs.zip			0	2024-02-25 20:15:30 CET	2024-02-25 20:15:30 CET	2024-02-25 20:15:30 CET	2024-02-25 20:14:16 CET	1731330	
Epycs.zip.torrent			0	2024-02-25 20:14:16 CET	2024-02-25 20:14:16 CET	2024-02-25 20:14:16 CET	2024-02-25 20:14:16 CET	272	
Progress_Report_3.pdf			0	2024-02-25 18:47:15 CET	2024-02-25 19:29:54 CET	2024-02-25 20:18:11 CET	2024-02-25 20:17:30 CET	653033	
Progress_Report_3.pdf.torrent			0	2024-02-25 20:18:11 CET	2024-02-25 20:18:11 CET	2024-02-25 20:18:11 CET	2024-02-25 20:18:11 CET	318	

Fig 19. I2psnark folder containing forensic artifacts from the browsing activities after the I2P uninstallation.