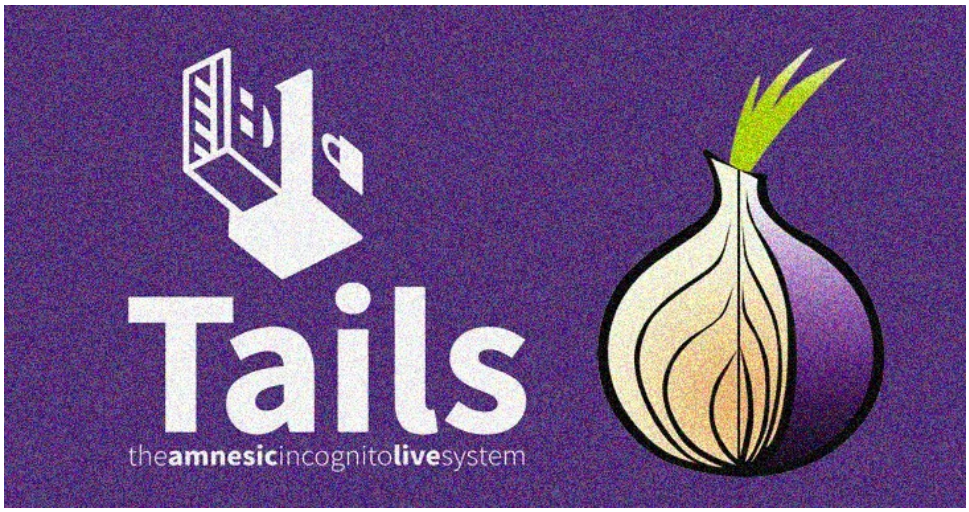
Centre for Development of Advanced Computing, Thiruvananthapuram

2024

A Forensic Analysis of the Tor Network in Tails Operating System



SUBMITTED BY

Prashant Kumar Moroliya (240360940024)

Pooja Suresh Kakade (240360940022)

Pritesh Vishwas Barela (240360940025)

Poorva Dalvi (240360940023)

Kunal Rajendra Patil (240360940021)

UNDER THE GUIDANCE OF

Mr. Hiron Bose

(Scientist E)

CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING, THIRUVANANTHAPURAM

2024

CERTIFICATE

We hereby declare that the work presented in this report entitled "VULNERABILITY ASSESSMENT AND PENETRATION TESTING ON METASPLOITABLE2" in partial fulfilment of the requirements for the award of the Post Graduation Diploma in Cybersecurity and Forensics submitted to CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING, THIRUVANANTHAPURAM is an authentic record of my own work carried out over a period from 15th July 2024 to 15th August 2024 under the supervision of Mr Hiron Bose (Scientist E), Centre for Development of Advanced Computing, Thiruvananthapuram.

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

(Student Signature)

This is to certify that the above statement made by the candidates is true to the best of my knowledge.

Date:

Project Supervisor HOD Principal

TABLE CONTENTS

ACKNOWLEDGEMENT

We wish to express our deep appreciation to Mr Hiron Bose (Scientist E), Centre for Development of Advanced Computing, Thiruvananthapuram, for providing his uncanny guidance, invaluable support and encouragement throughout the Project work, without which the work would have been an exercise in vainness.

We would like to thank all our colleagues, who have given us moral support and their relentless advice throughout the completion of this work.

Prashant Kumar Moroliya (240360940024)

Pooja Suresh Kakade (240360940022)

Pritesh Vishwas Barela (240360940025)

Poorva Dalvi (240360940023)

A Forensic Analysis of the Tor Network in Tails Operating system

Abstract— The Tor network is a widely recognized and utilized platform for ensuring online privacy and security, offering users the ability to browse the internet, communicate, and access information without revealing their identities. By routing traffic through a series of volunteer-operated servers, Tor effectively anonymizes users, making it difficult to trace their online activities. This feature has made Tor indispensable for those seeking to protect their privacy, including journalists, activists, and individuals living under repressive regimes. However, the very attributes that make Tor a powerful tool for safeguarding privacy also create significant challenges for Law Enforcement Agencies (LEAs) attempting to monitor, investigate, and mitigate criminal activities that take place within the dark web—a part of the internet accessible only through specialized software like Tor.

This study is centred on conducting a comprehensive forensic analysis of the unencrypted layer of the Tor network, with the objective of assessing the extent to which network traffic analysis can reveal detailed information about a user's online activities. Such analysis is crucial for criminal investigations, as it may enable LEAs to identify and track individuals engaged in illegal activities despite the anonymity provided by Tor. The methodology employed in this study involves the capture and thorough examination of network traffic generated by the Tor Browser operating within the Tails operating system, a security-focused OS known for preserving user anonymity. Particular attention is paid to the data transmitted in the unencrypted segments of the network, as these may contain critical information that could potentially compromise user anonymity.

The findings of this study are significant, revealing that it is indeed possible to de-anonymize Tor users and ascertain their online behaviours by carefully analysing the unencrypted headers of the network packets they transmit. This de-anonymization process involves scrutinizing specific aspects of the network traffic that remain exposed despite the overall encrypted nature of the Tor network. These findings carry profound implications for LEAs and cybersecurity professionals, as they suggest that even within a network designed to offer robust privacy protections, there are vulnerabilities that can be exploited to uncover user identities and activities.

Furthermore, the study's results underscore the importance of awareness among Tor users regarding the limitations and potential risks associated with the network. While Tor is undoubtedly a valuable resource for maintaining online privacy, the research highlights that it is not foolproof. Users must adopt additional security measures, such as ensuring that all layers of their communication are encrypted and remaining vigilant about the types of data they transmit, to enhance their protection against potential exposure.

In conclusion, this study provides critical insights into the capabilities of network traffic analysis in the context of the Tor network and highlights the dual-edged nature of tools designed to protect privacy. While Tor remains an essential tool for those requiring online anonymity, this research illustrates the need for continuous vigilance and improvement in both user practices and the network's architecture to address and mitigate the risks and limitations inherent in its use.

Keywords— *Tor network, digital forensics, unencrypted layer, network traffic analysis, de-anonymization, privacy, dark web, deep web, Tor browser.*

INTRODUCTION

With the growth of the Internet and the increasing use of technology in our daily lives, cybercrime has become a pressing issue for both law enforcement agencies and Internet users [1]. Cybercriminals take advantage of the anonymity and privacy provided by the Internet to carry out their illegal activities, making it increasingly difficult to identify and prosecute these criminals [2]. The Tor network and the Tails operating system are two popular privacy tools that have gained significant attention in recent years because they provide users with a secure and private environment that leaves no trace of their online activities on the host computer, allowing criminals to hide and evade detection [3].

Cybercriminals have become more sophisticated and agile, taking advantage of the anonymity and privacy protections the Internet provides to carry out their illegal activities [4]. The dark web has been and remains a target of exploitation by various harmful entities, such as criminal organizations, terrorists, cybercriminals, and actors supported by governments [5]. This has created a major problem for law enforcement agencies, who find it difficult to identify and prosecute cybercriminals because they can hide their identities and actions online using advanced privacy tools such as the Tor network [6]. The Tor network is free software that allows anonymous communication and browsing by routing Internet traffic through a global network of volunteer servers [7].

Tails is a live operating system that can be booted from a USB stick, DVD, or SD card. It comes pre-installed with the Tor browser and other privacy and encryption tools to provide users with a secure and private environment that leaves no trace of their activities on the host computer [8]. The Tor browser transmits encrypted traffic through a layered network overlay. Digitally hijacking the Tor network is a complex and time-consuming process. However, examining a seized device, whether it's a cell phone or a computer, can make it easier to find evidence of illegal online activity. Given the critical role of Tor Browser forensics in investigating cybercrime, it is essential to study the latest versions of Tor Browser on the latest operating systems. This can enable investigators to effectively profile the application's evidence and conduct successful forensic investigations.

The objective of this study is to conduct a forensic analysis of the latest version of Tor Browser on the latest Tails operating system under a hypothetical cybercrime scenario involving dark web activity. Specifically, we aim to identify the areas of the Tails network at the local host layer that a forensic investigator could scrutinize for evidence related to the Tor privacy browser. The findings of this study can potentially enhance the effectiveness and accuracy of Tor Browser forensics in real-world investigations.

The first section provides background and a literature review of Tor Browser forensics. The second section presents different types of crimes taking place on the dark web. The third section presents the research methodology, including the analysis of unencrypted headers of network packets and the identification of patterns and characteristics in the evidence and traces left by the Tor Browser running on the Tails operating system. The fourth section discusses the findings of the study, including the de-anonymization of users and the identification of online criminal activities. The final section summarizes the conclusions and implications for the field of digital forensics and offers suggestions for future research.

LITERATURE SURVEY

Various studies have been conducted to analyse the forensics of the Tor Browser using different virtual scenarios and methodologies. In [9], the researchers conducted a forensic investigation of the Tor Browser installed on a Windows 8.1 platform, covering aspects such as memory registry and hard disk footprint. However, the study did not include any network forensics, and the researchers rarely connected to dark websites. Teng and Wen [10] investigated seven different web browsers, including Tor on the Windows operating system. The other six browsers tested were Comodo Dragon, Epic Browser, SRWare Iron, Secure Browser, Maxthon, and Dooble. The researchers investigated different types of evidence, including system, registry, network packets, memory, and unallocated space. Although these methods can be used to analyze Tor browsers on Tails OS, the methodology should be slightly adjusted.

Warren [11] performed forensics on 64-bit Windows 10 from Tor Browser version 5.0. Their research included a before-and-after study of registry settings installation as well as other file system and memory artifacts of the system. After analysing the data, the researchers concluded that the Tor Browser leaves very little evidence on the system disk. In [12], Nelson et al. compared the forensic evidence obtained from normal and private browsing modes of Google Chrome and Mozilla Firefox with the Tor v7.0.5 Browser on Windows 7 (64-bit). The researchers collected artifacts using AccessData FTK as the primary tool. The study found that the Tor Browser revealed very few artifacts of user browsing activities compared to the experimental virtual machines' storage and the private browsing modes in Firefox and Chrome. These results suggest that the Tor Browser may be more effective at protecting user privacy by minimizing the digital footprint of user activity.

Muir [13] presented a Tor privacy browser artifact extraction framework from memory. However, their research was aimed only at the memory aspect of the study and Windows 10 build 10586. The researchers did not analyse other components of the operating system, including the registry or file system, to discover their associated artifacts connected to the Tor Browser. Also, their research was limited to revealing information about the user-related data.

In [14], the researchers discussed memory forensics related to Tor and investigated the open/closed state of tab pages and the browser's closed state after 15 minutes. The report found that the lack of well-established research-driven approaches for extracting and recovering Tor artifacts from a memory dump is a significant barrier to progress in Tor Browser bundle detection. Industries and researchers have not produced any literature or undertaken tests on extracting and analysing artifacts from a Tor Browser's memory dump. Kulm [15] conducted a forensic investigation on Tor Browser traces left on Windows and Mac OS X and also created a framework to analyse the traces.

Arshad et al. [16] subjected the Tor Browser to a forensic study using a virtual computer running Windows 10. Several traces in the computer's memory led researchers to the Tor Browser's installation directory and the websites to which it was linked. However, the authors did not provide any reverse engineering tools that could have been used to dump memory locations. In [17], blockchain data and OSINT were combined to evaluate Bitcoin transactions, and the researchers discovered that by connecting 125 distinct users to dark web services, it is possible to identify Bitcoin users on dark web marketplaces.

Sandvik [18] performed a forensic investigation of the Tor Browser installed on Windows and Linux. Three snapshots of artifacts, including prefetch, hives, and memory objects, were examined. Huang et al. [19] investigated the traces the browser leaves behind when the Tor Browser is used without administrative rights or knowledge of how to delete the browser. The investigation was restricted to three virtual computers and only took into account traces left behind after the system was shut down and the browser was erased.

The studies discussed above primarily focused on examining basic Tor browsing activities, such as website browsing and opening and closing the browser. However, these studies were conducted on older versions of the Tor Browser and operating system builds, which may no longer provide useful insights into the latest versions of applications. As applications and platforms evolve, updates to their internal structures can make the results of previous studies obsolete and irrelevant for further forensic investigations. Hence, it is crucial to investigate the latest versions of Tor Browser on the latest operating system versions to effectively profile the application's evidence.

INCURSION OF CRIMES IN THE DARK WEB

The Internet is divided into 3 components: surface web, deep web, and dark web [20]. Figure 1 shows these layers of the Internet.

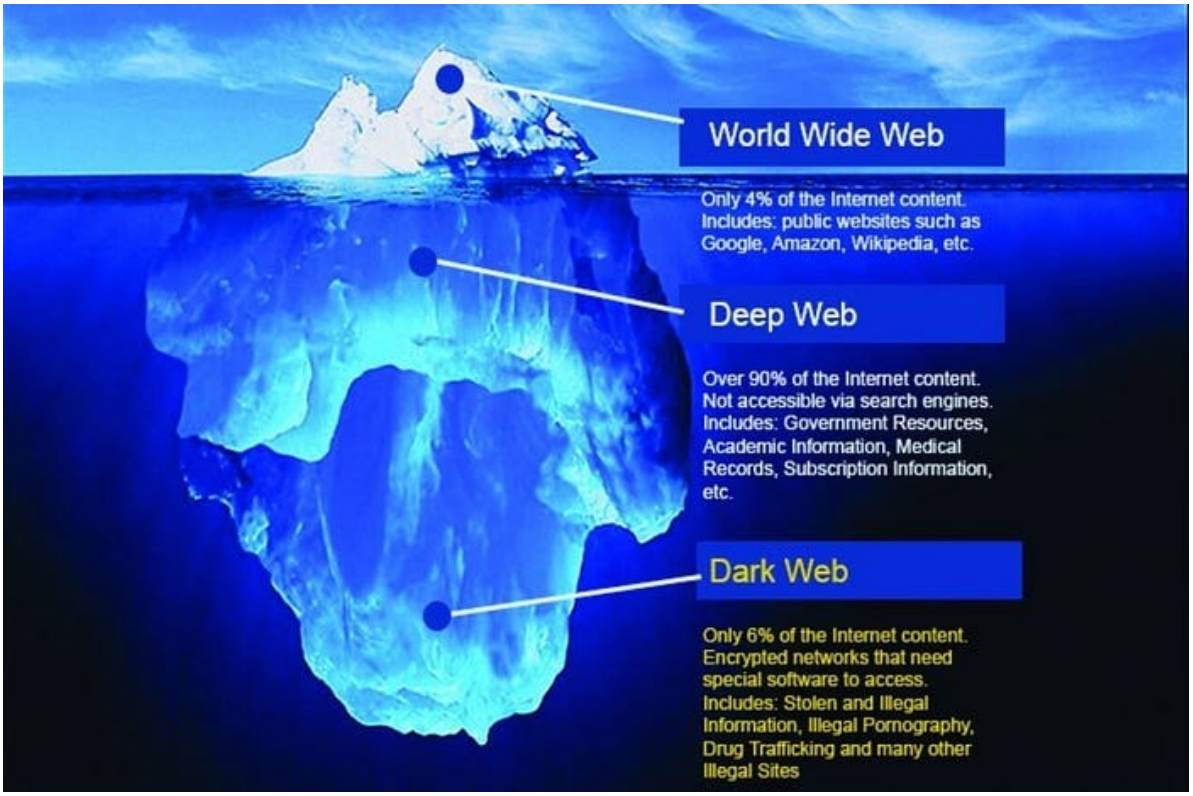


Figure 1 Internet Layers [5]

The dark web is a network of websites that are hidden from search engines and are only accessible through specialized tools such as the Tor browser. The dark web uses encryption and multi-point relay obfuscation to provide users with anonymous internet access [21]. It is characterized by its strong privacy and security features, making it popular among criminals for committing financial fraud and other illegal activities. Bitcoin provides a powerful tool for the dark web and has helped realize the function of secret transactions [22]. Currently, there are more than a dozen encrypted digital currencies used for transactions on the dark web with varying prices [23].

Some of the most notable crimes that take place on the dark web include:

A. Fraud and Financial Crimes

In the current digital era, fraud and financial crimes are major issues, and the dark web plays a significant role in their facilitation. One of the primary ways in which the dark web is used for financial crimes is through the sale and exchange of stolen financial data. This can include login credentials for bank accounts, credit card information, and other personal financial information. Hackers can use this information to open new credit accounts in the victim's name or make unauthorized purchases [24].

B. Child Exploitation and Human Trafficking

Some dehumanized criminals control innocent children and earn money by selling images and videos of sexual assault and abuse on the dark web. They even provide perverted services beyond the imagination of ordinary people, such as live broadcasts of sexual assault, torture, and maiming of children in ways requested by the payer, as long as someone is willing to pay [24]. Child exploitation on the dark web includes the production, distribution, and possession of child pornography. Due to the secrecy of the dark web, it is extremely difficult for the police to detect it. It often takes a lot of hard work to destroy a pornographic website, but criminals can easily build another one. According to statistics from Wikipedia in recent years, the number of visits to pornographic websites on the dark web is second only to drugs [25], and it is already a growing cancer.

C. Sale of Stolen Data

In the Internet era, data has become an important resource. While people are mining the huge value of data and making it serve economic and social development, a black industry chain that profits through the reselling of illegally obtained data is rapidly forming, with most illegal data transactions moving to the dark web [25].

D. Computer Hacking Platform

The dark web provides an excellent place for hackers to communicate and trade. There are various hacker forums on the dark web where hackers can not only learn new skills but also trade exploits and sell various malware. The dark web has accelerated the proliferation of hacking technology, expanding the threat to network security and spawning new types of crime such as cyber extortion [26].

E. Terrorism

The dark web provides terrorists with a secure internal communication tool, enabling them to covertly exchange information and connect more broadly to plan, organize, deploy, and carry out terrorist activities [26]. Terrorist organizations also use the dark web to promote extremist ideas, recruit new members, and provide skilled training for followers around the world, such as setting up training centres on how to make bombs and carry out terrorist attacks. This includes training "lone wolf" attackers, who are difficult to detect [27]. The dark web has also been used by terrorists to raise money and transfer funds. The dark web black market has long been an "arsenal" for terrorists, making it relatively easy to buy guns and ammunition on illegal trading sites such as "Silk Road" [28]. Fig. 2 shows the sale of guns.

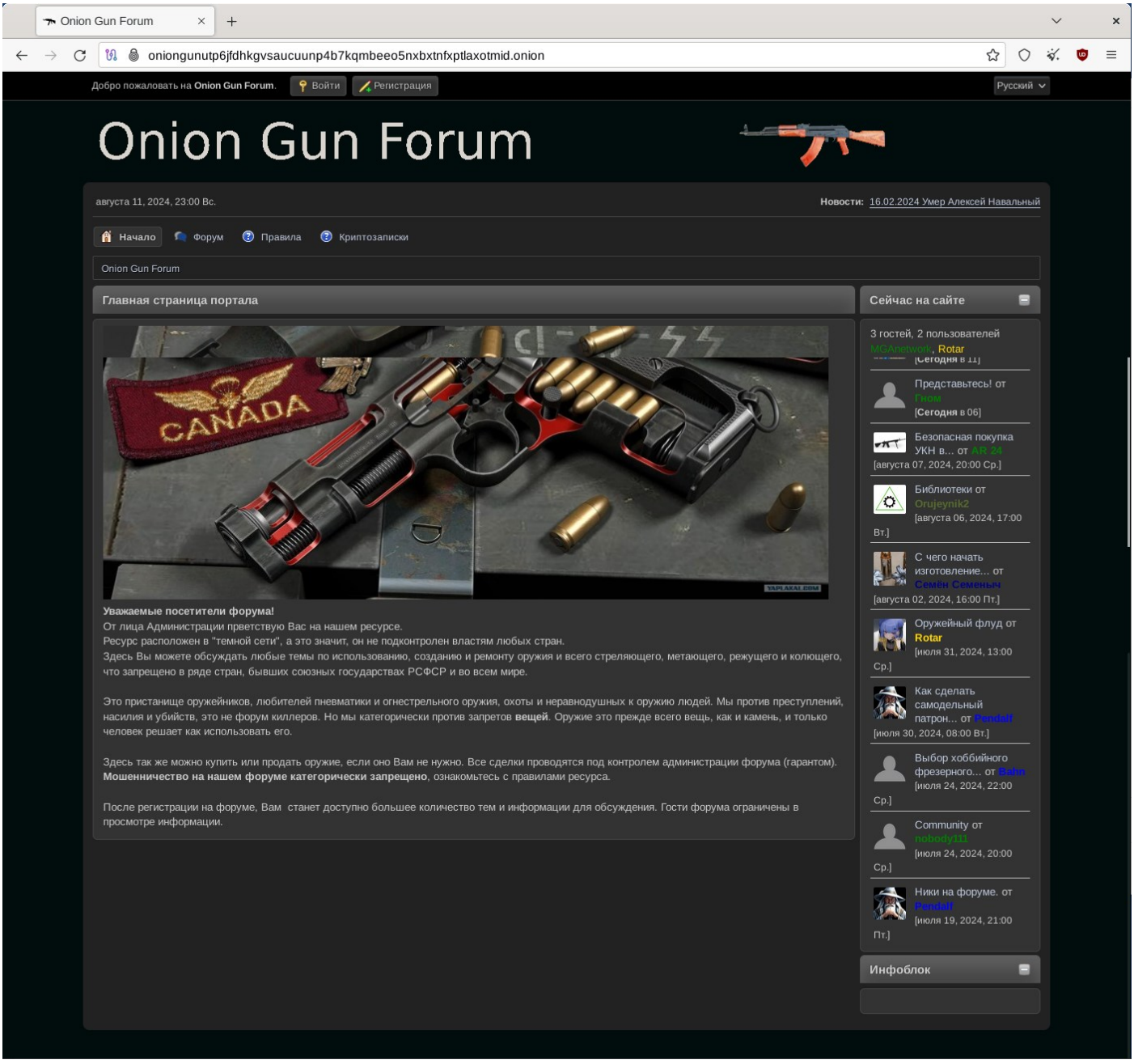


Figure 2Sale of Guns on a Website

F. Illicit Goods and Services

One of the primary ways in which the dark web is used for the sale of illicit goods and services is through the use of anonymous marketplaces [28]. These marketplaces, often referred to as "darknet markets," allow individuals to buy and sell a range of illegal items, including drugs, weapons, and stolen credit card information. Fig. 3 shows the sale of fake currency on the dark web.

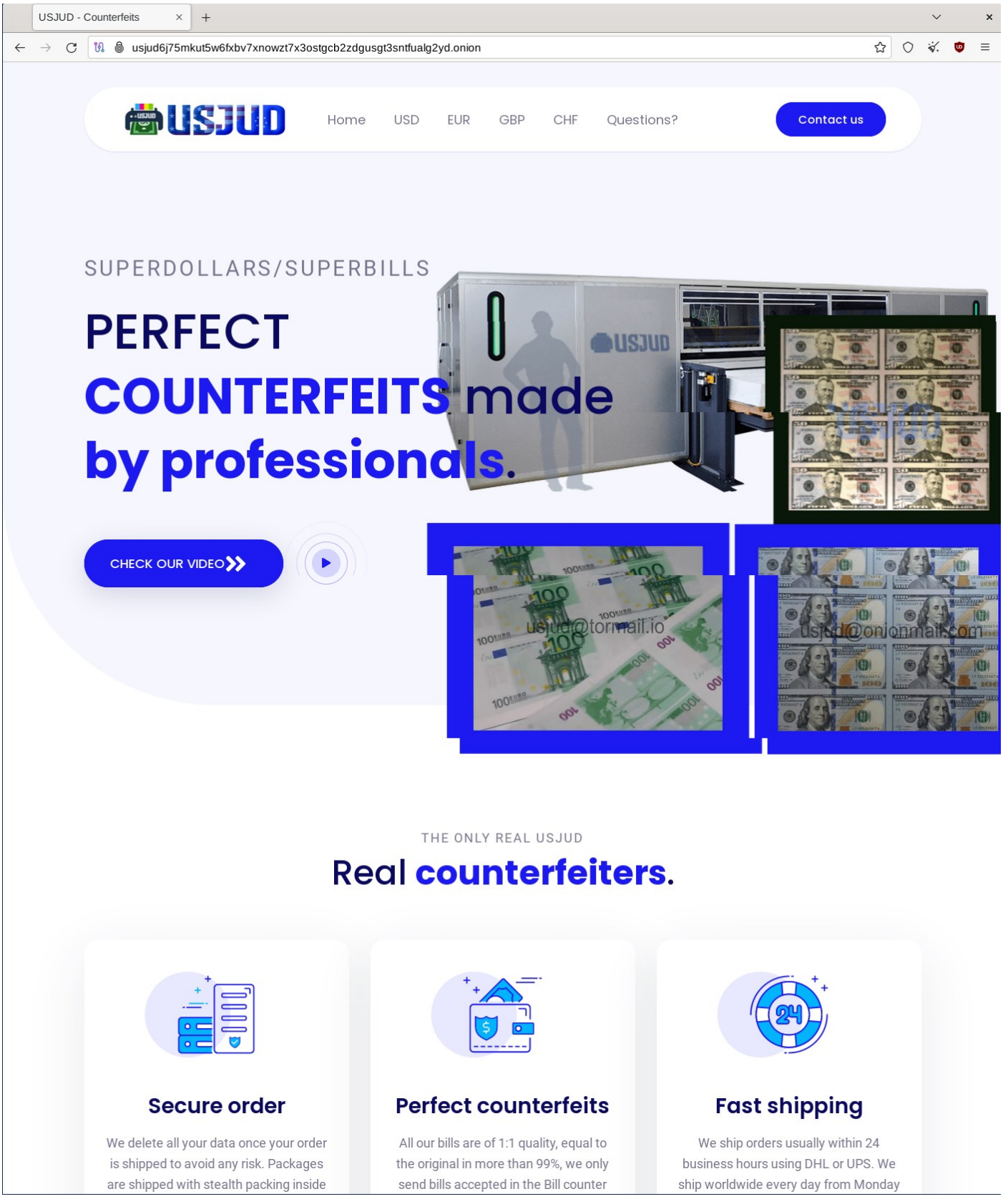


Figure 3Sale of Counterfeit Currency on a Website

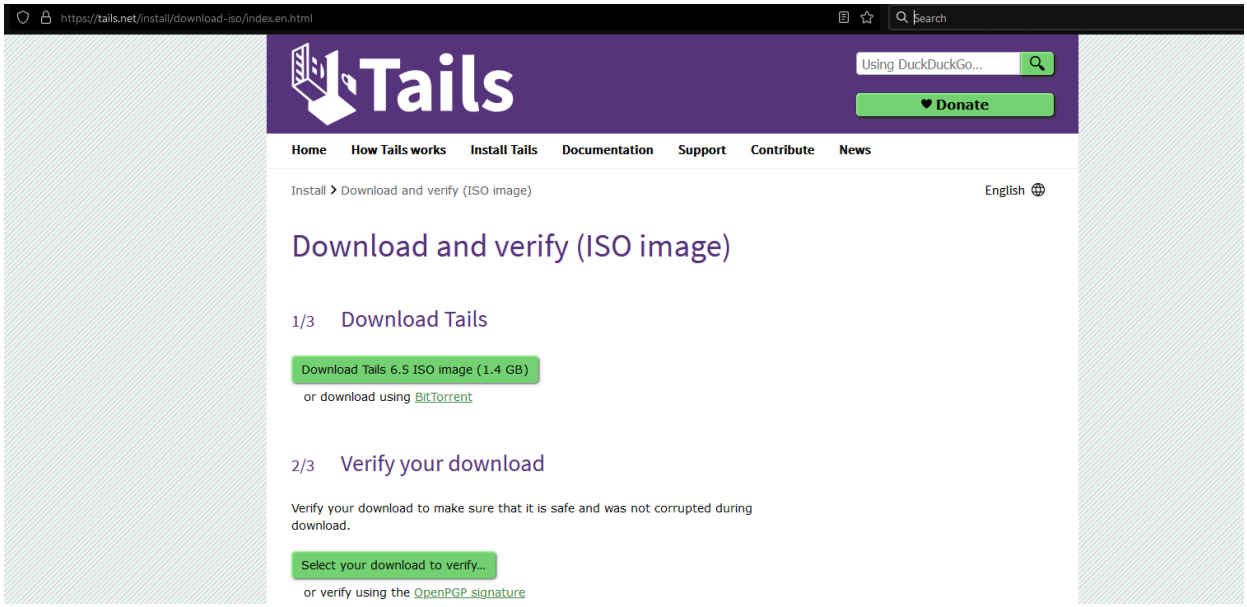
METHODOLOGY

The methodology involved several steps in setting up the test environment, using network forensic capture tools, and analysing unencrypted traffic at the local host layer over the Tor network.

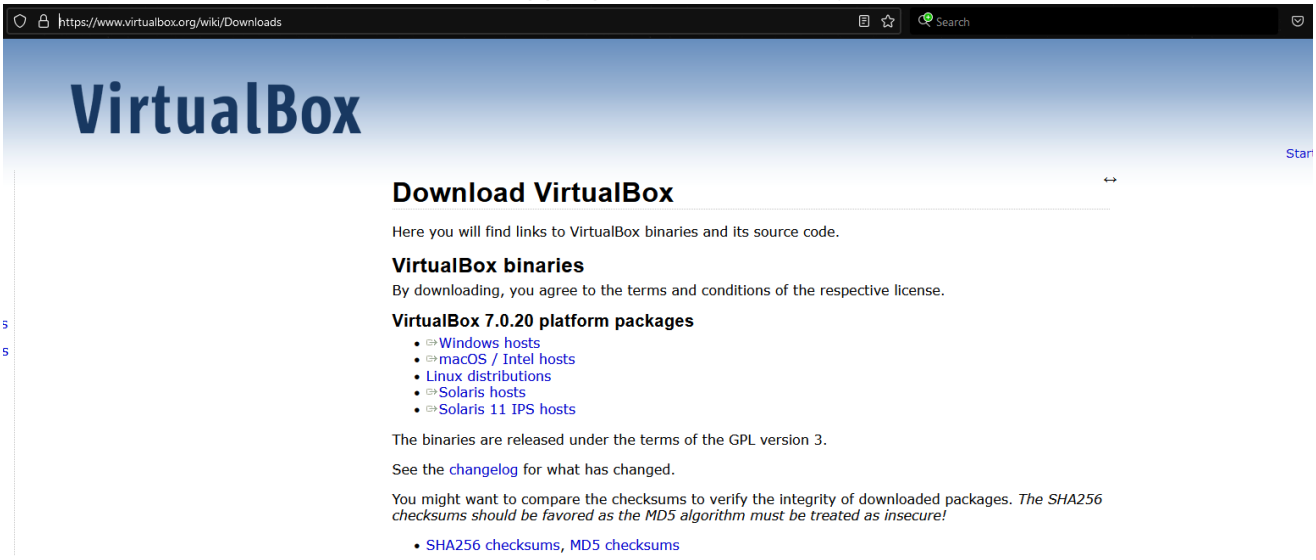
A. Environment Setup
   The Tails operating system was installed in VirtualBox. Tails was chosen because it comes with the Tor browser preinstalled and is designed with a focus on privacy and security, aligning with the objectives of this research.

Installing Tail OS in VirtualBox.

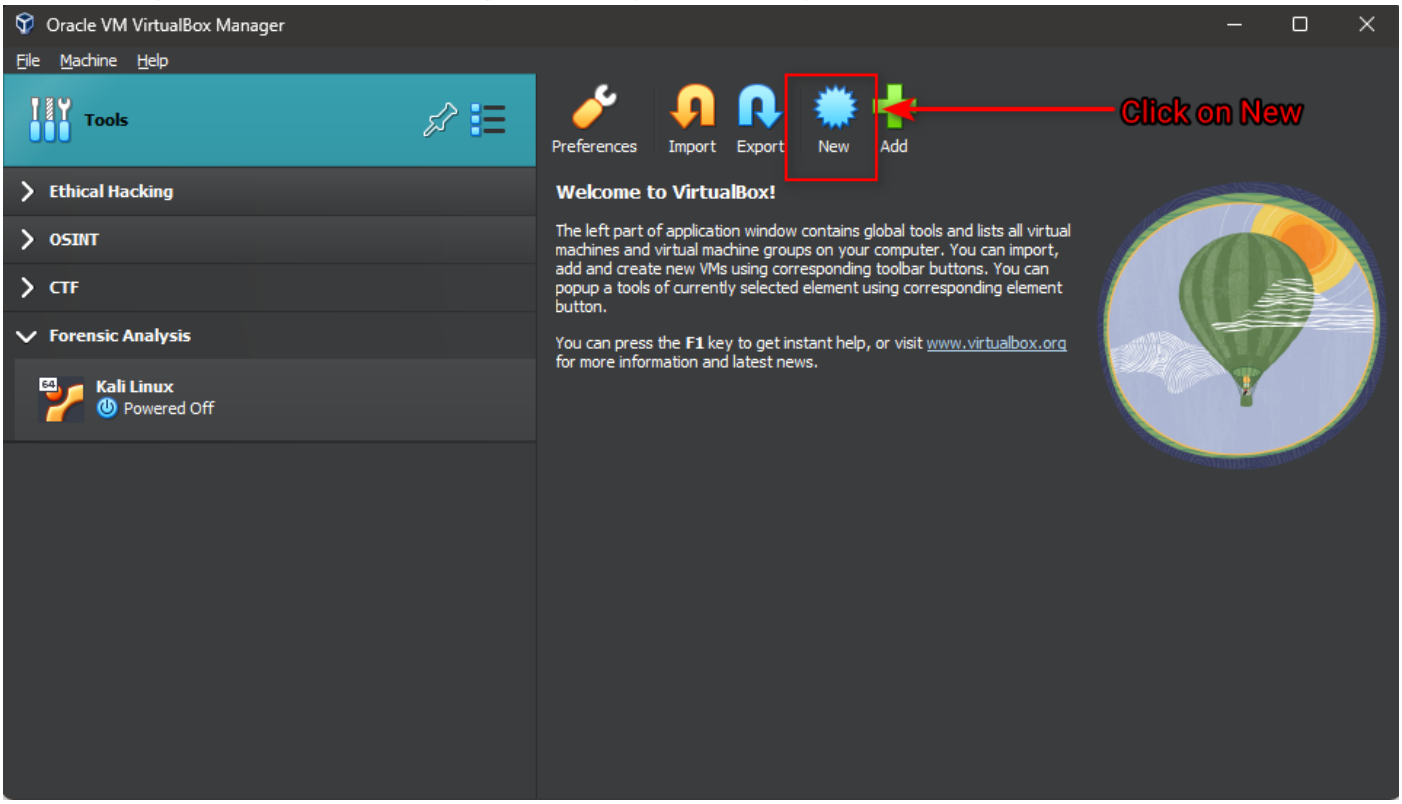
1. Download ISO file from here and also verify it:
https://tails.net/install/download-iso/index.en.html

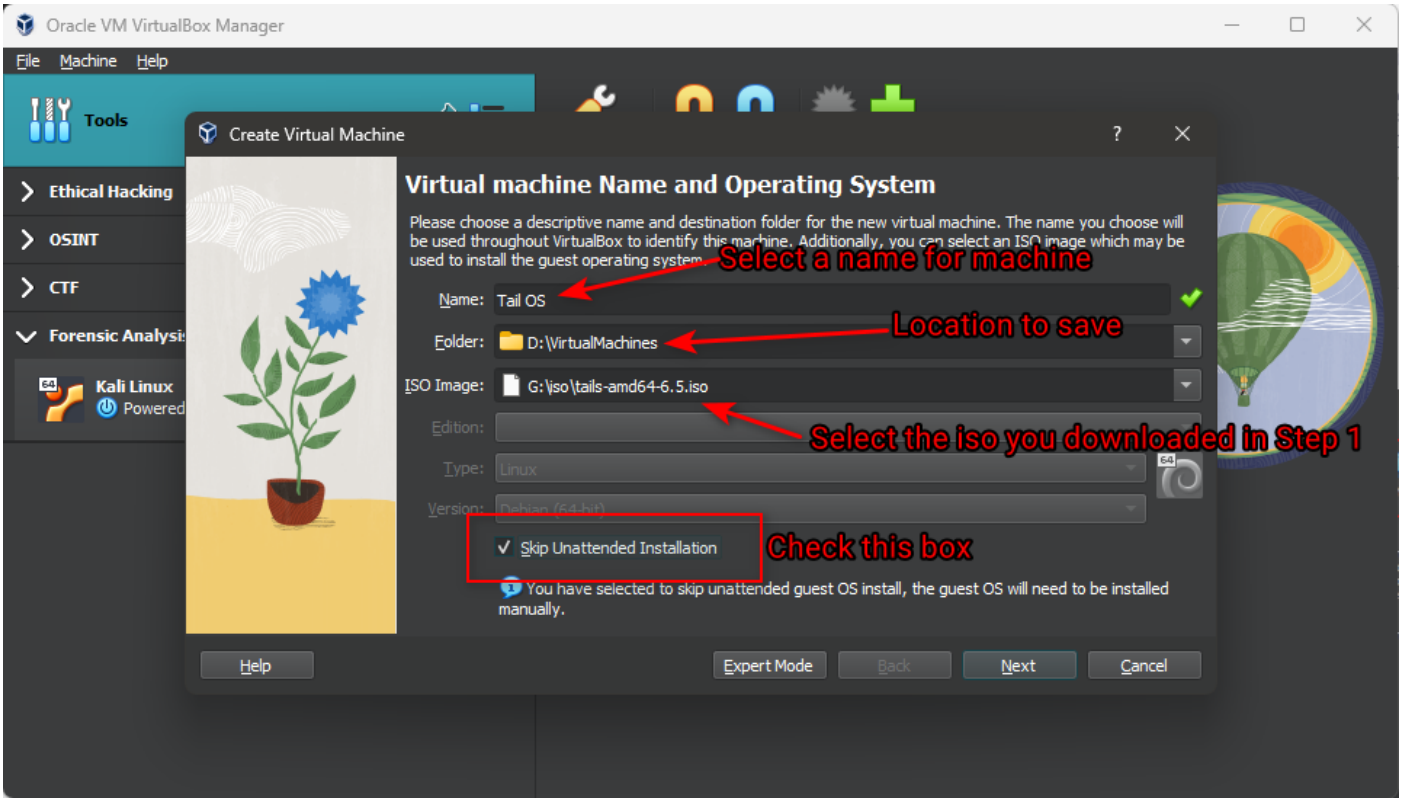


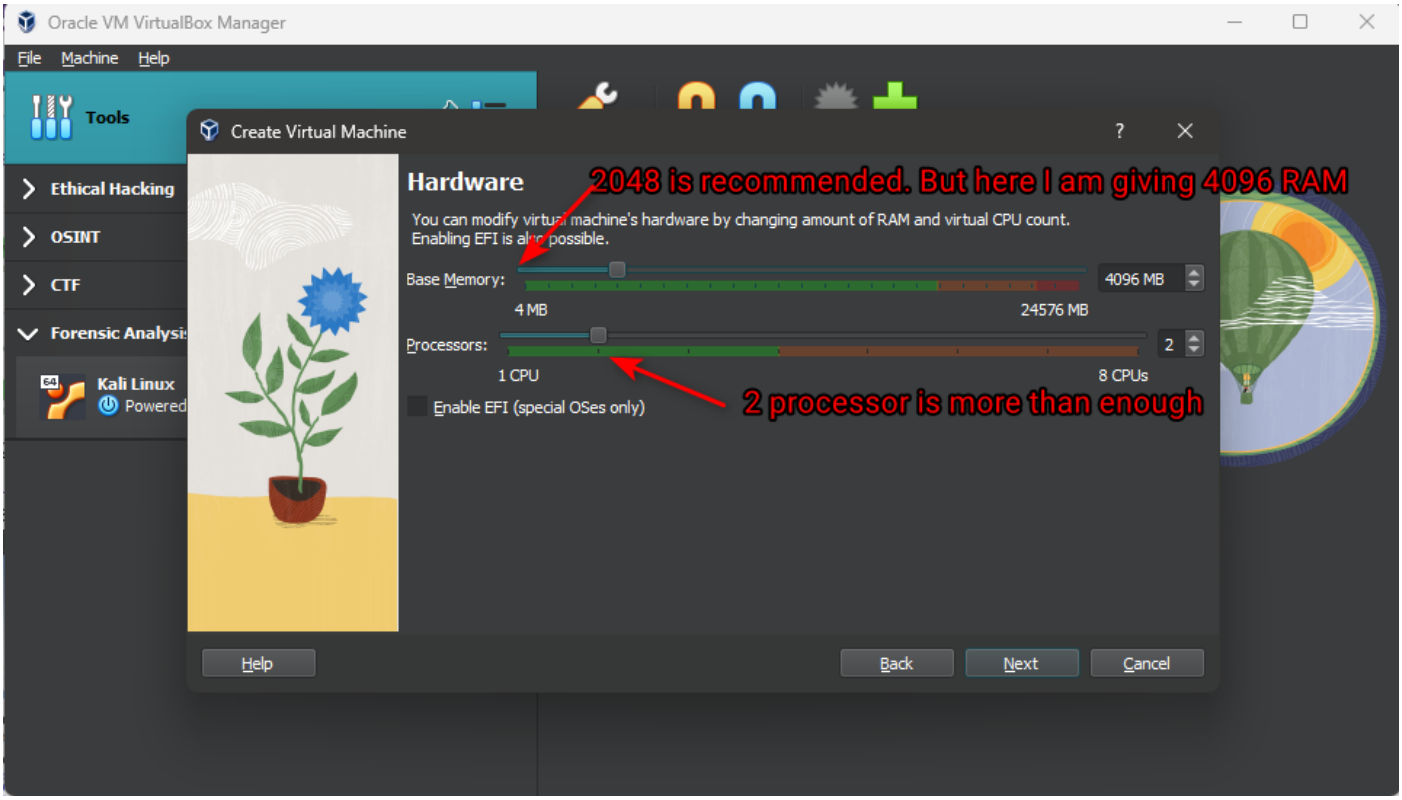
2. Download VirtualBox from here:
https://www.virtualbox.org/wiki/Downloads
Choose appropriate version for your system.

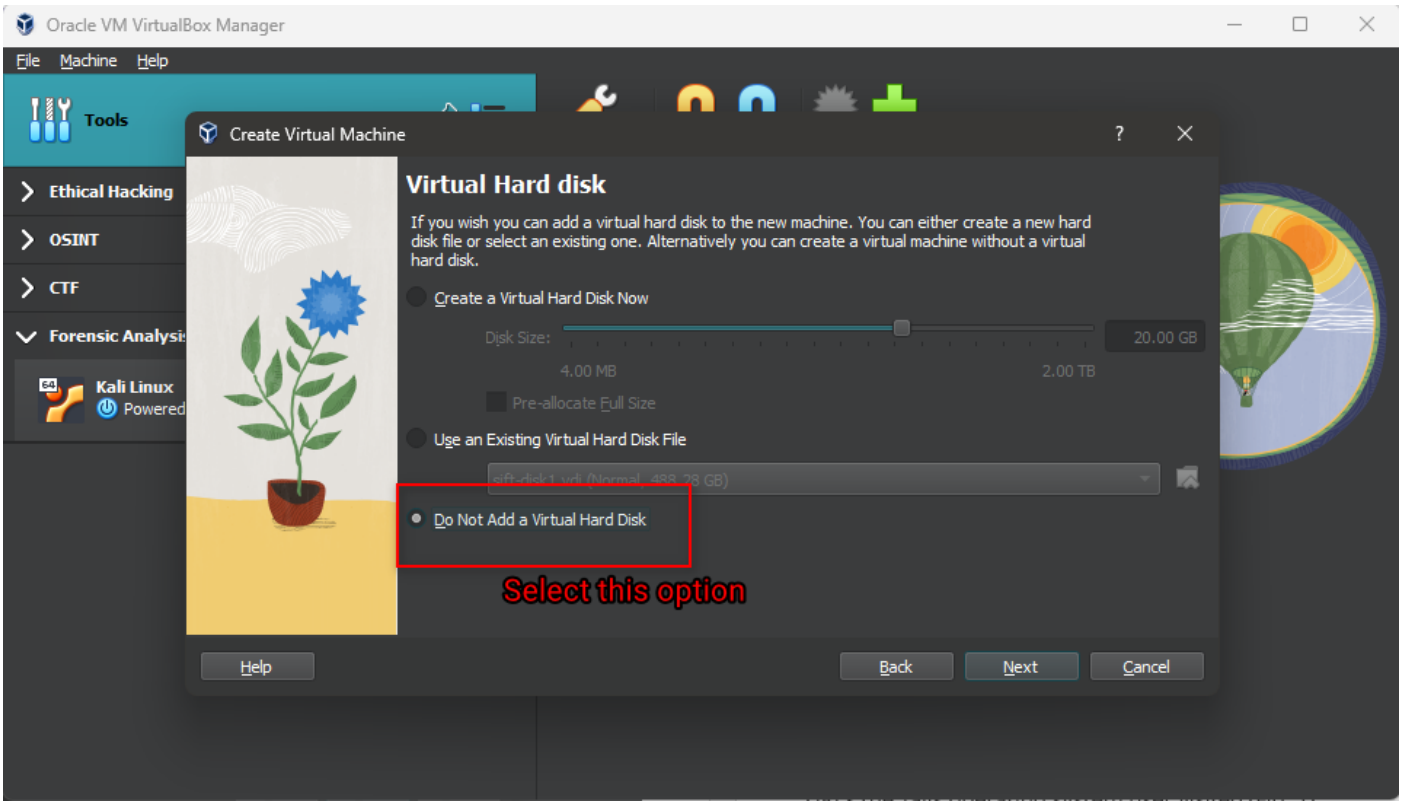


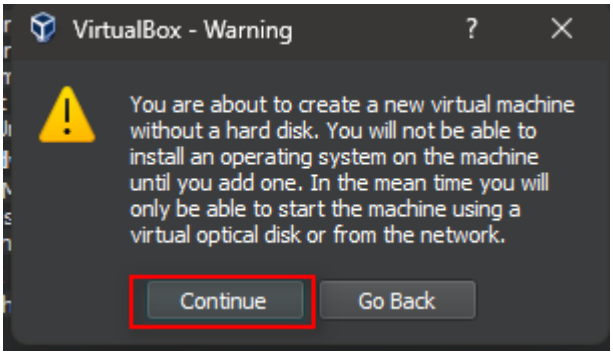
3. Open VirtualBox and setup according to following screenshots.

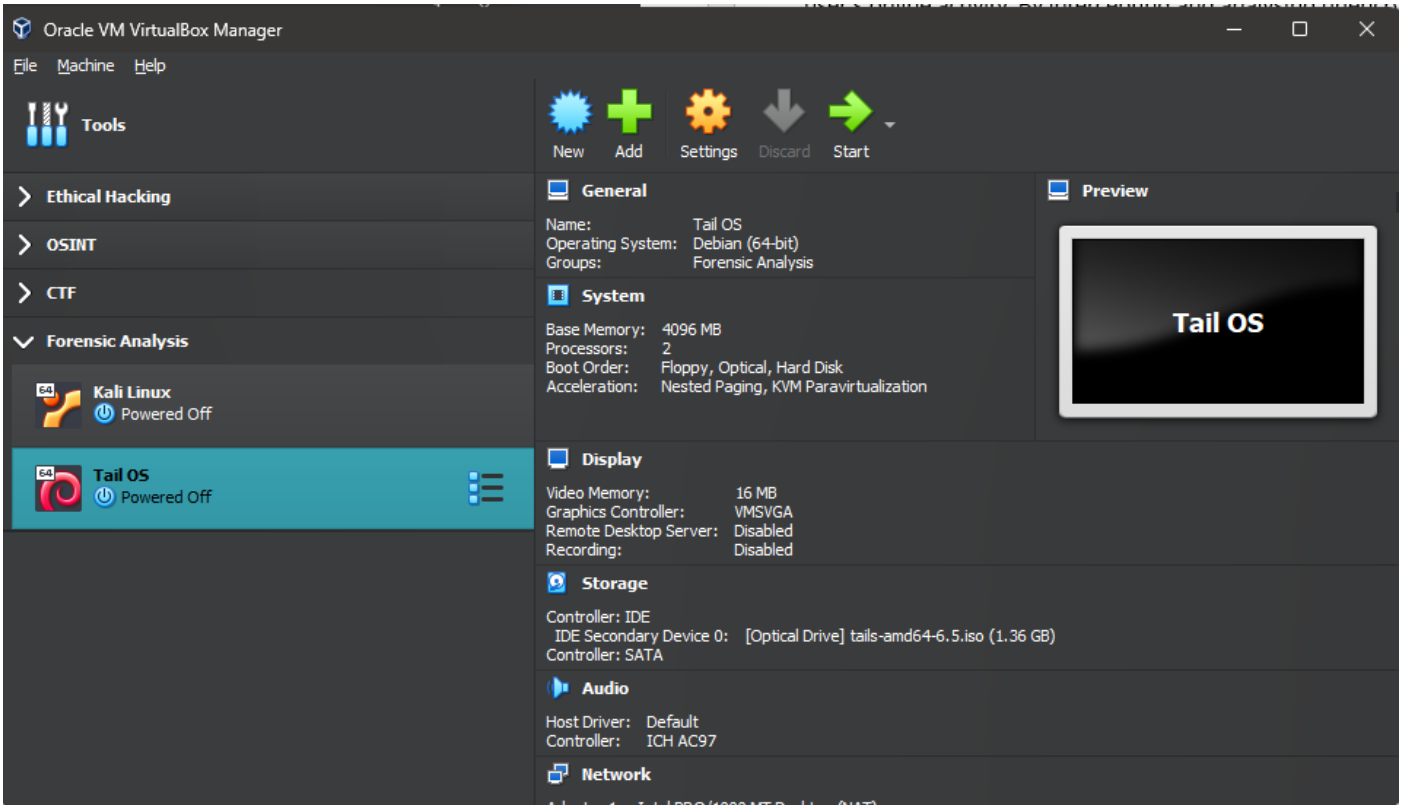




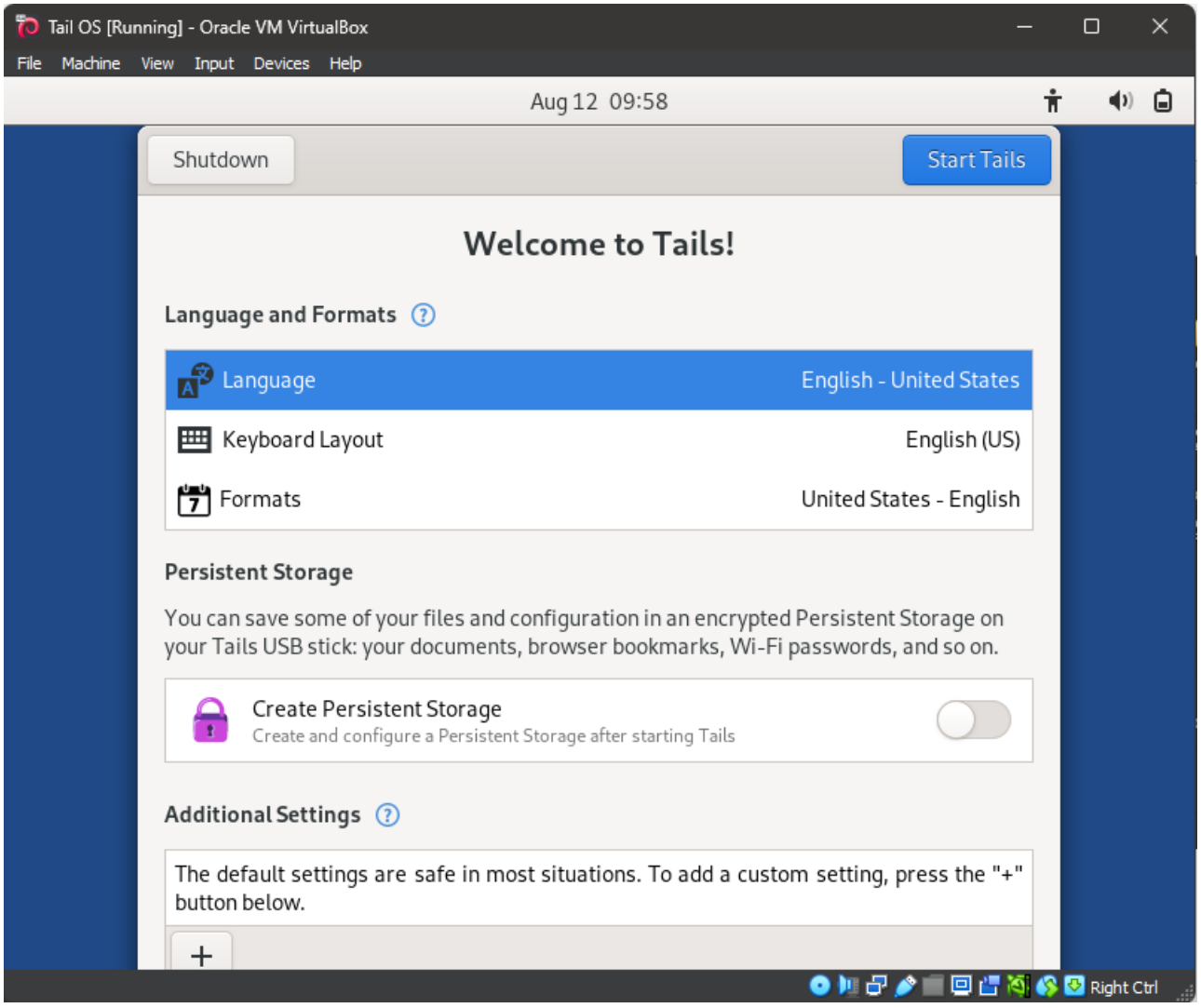

Oracle VM VirtualBox Manager
File Machine Help
Tools
Ethical Hacking
OSINT
CTF
Forensic Analysis
Kali Linux
Powered
Create Virtual Machine
Hardware
2048 is recommended. But here I am giving 4096 RAM
You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count.
Enabling EFI is also possible.
Base Memory:
4096 MB
4 MB
24576 MB
Processors:
2
1 CPU
8 CPUs
Enable EFI (special OSes only)
2 processor is more than enough
Help
Back
Next
Cancel

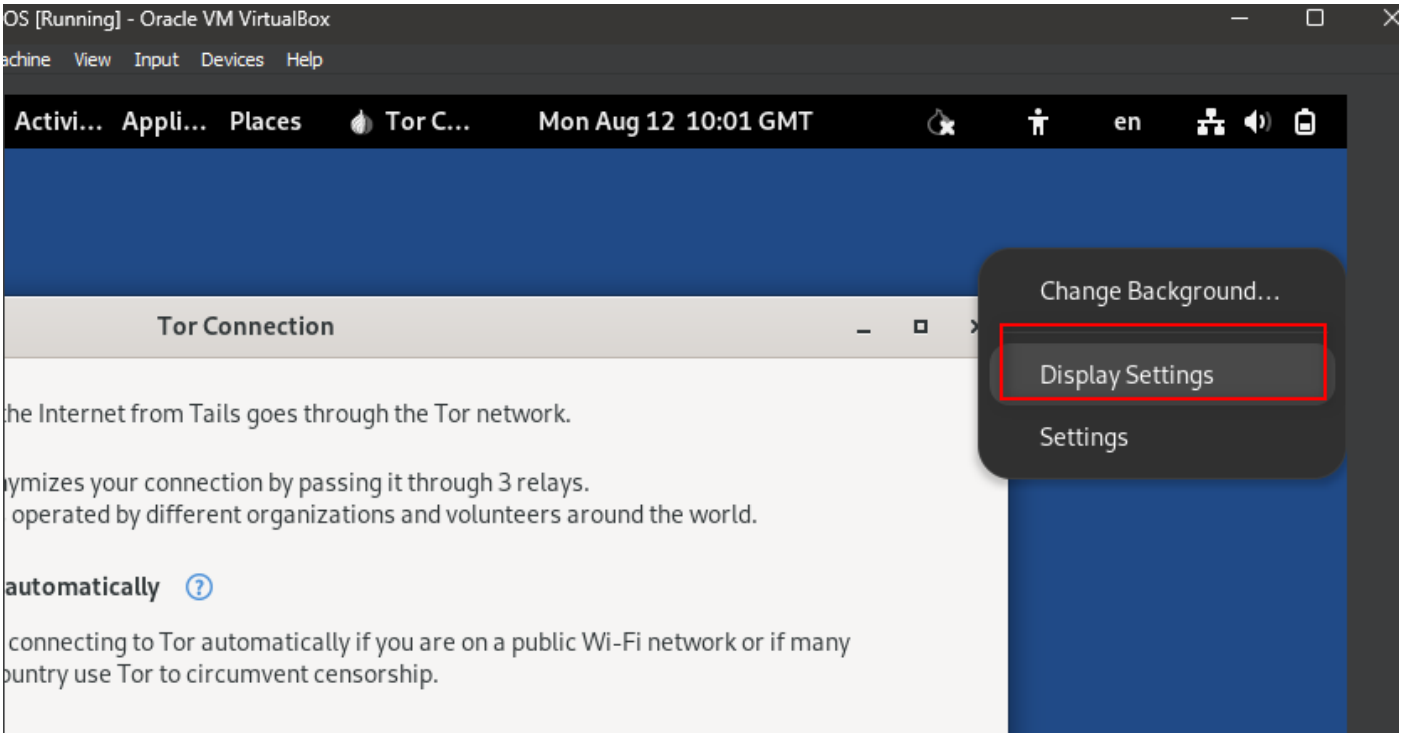

Oracle VM VirtualBox Manager
File Machine Help
Tools
Ethical Hacking
OSINT
CTF
Forensic Analysis
Kali Linux
Powered
Create Virtual Machine
Virtual Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.
Create a Virtual Hard Disk Now
Disk Size:
20.00 GB
4.00 MB
2.00 TB
Pre-allocate Full Size
Use an Existing Virtual Hard Disk File
Do Not Add a Virtual Hard Disk
Select this option
Help
Back
Next
Cancel

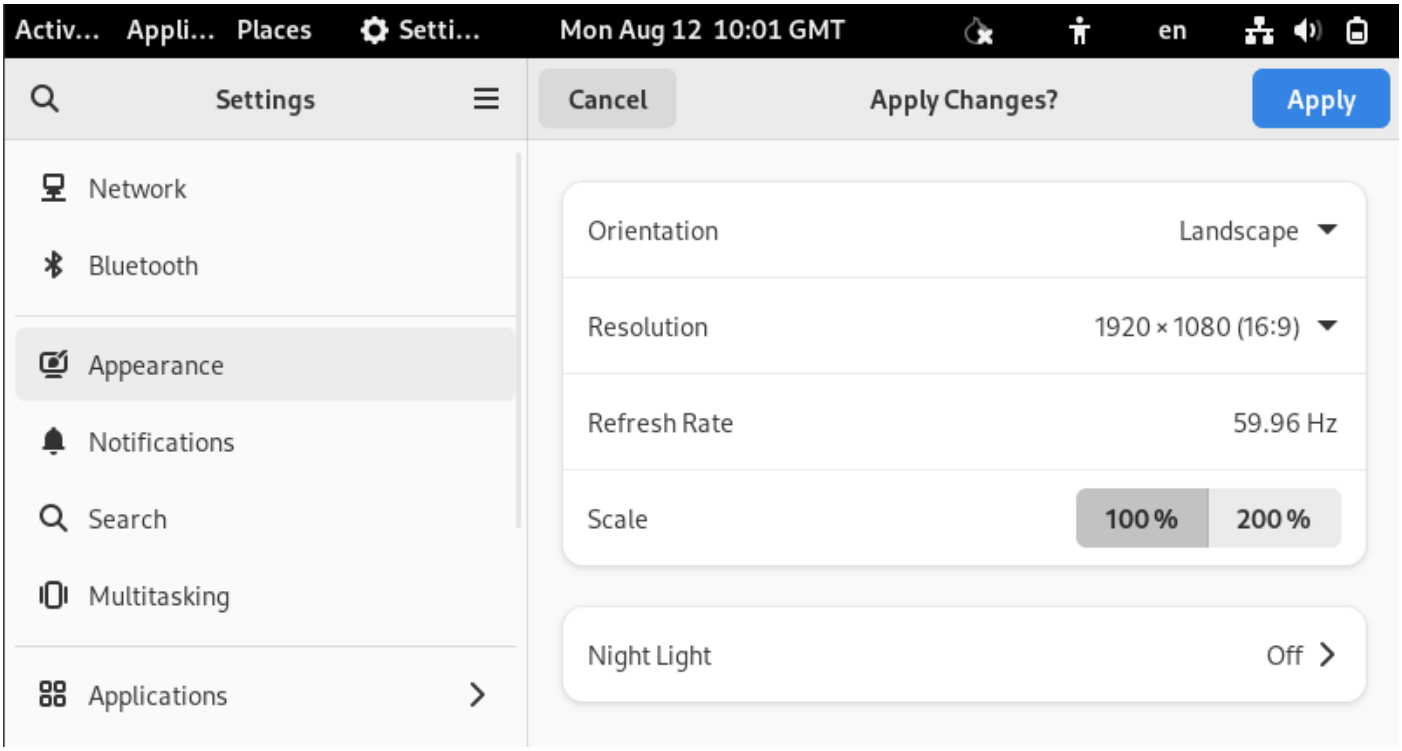

VirtualBox - Warning
You are about to create a new virtual machine without a hard disk. You will not be able to install an operating system on the machine until you add one. In the mean time you will only be able to start the machine using a virtual optical disk or from the network.
Continue
Go Back

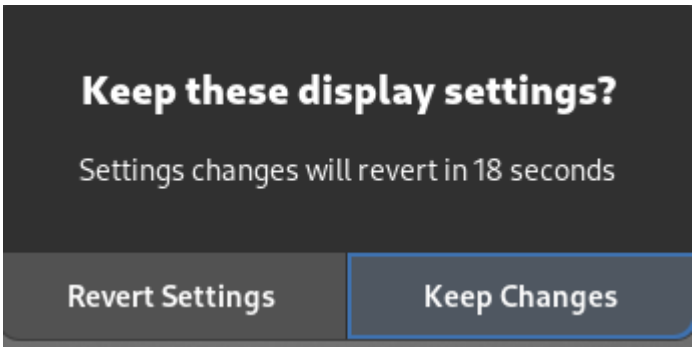


4. Now we will Start Tail OS




OS [Running] - Oracle VM VirtualBox
achine View Input Devices Help
Activi... Appli... Places Tor C... Mon Aug 12 10:01 GMT en
Change Background...
Display Settings
Settings
Tor Connection
he Internet from Tails goes through the Tor network.
ymizes your connection by passing it through 3 relays.
operated by different organizations and volunteers around the world.
automatically
connecting to Tor automatically if you are on a public Wi-Fi network or if many
untry use Tor to circumvent censorship.


Activ... Appli... Places Setti... Mon Aug 12 10:01 GMT en
Settings
Cancel
Apply Changes?
Apply
Network
Bluetooth
Appearance
Notifications
Search
Multitasking
Applications
Orientation
Landscape
Resolution
1920 × 1080 (16:9)
Refresh Rate
59.96 Hz
Scale
100 %
200 %
Night Light
Off


Keep these display settings?
Settings changes will revert in 18 seconds
Revert Settings
Keep Changes

Tor Connection

Everything you do on the Internet from Tails goes through the Tor network.

Tor encrypts and anonymizes your connection by passing it through 3 relays.
Tor relays are servers operated by different organizations and volunteers around the world.

Connect to Tor automatically

We recommend connecting to Tor automatically if you are on a public Wi-Fi network or if many people in your country use Tor to circumvent censorship.

Configure a Tor bridge

Hide to my local network that I'm connecting to Tor

You might need to go unnoticed if using Tor could look suspicious to someone who monitors your Internet connection.

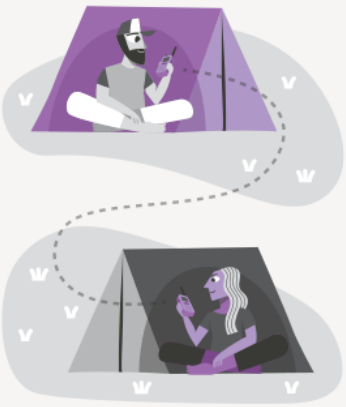
Learn more about how Tails connects to Tor

Connect to Tor

Tor Connection

Connected to Tor successfully

You can now browse the Internet anonymously and uncensored.



Start Tor Browser

View Tor Circuits

B. Packet Capture

Network packets were captured using network forensic tools and the netcat command from Kali Linux. The netcat command, a utility for network debugging and exploration, was used to capture network traffic transmitted between virtual machines. Dark web sites were accessed using the Tor browser, and packets were collected and stored in a format compatible with Wireshark for further analysis.

C. Traffic Analysis

The captured traffic was analysed using Wireshark and Network Miner to gain insights into the privacy and security provided by the Tor network running in the Tails operating system. This analysis included examining the nodes used for routing, the types of data being transmitted, and the timing of transmissions. Additionally, unencrypted traffic was scrutinized to better understand the network's structure and dynamics, including its routing patterns and the techniques employed to maintain users' security and privacy. The methodology used is represented in Fig. 4.

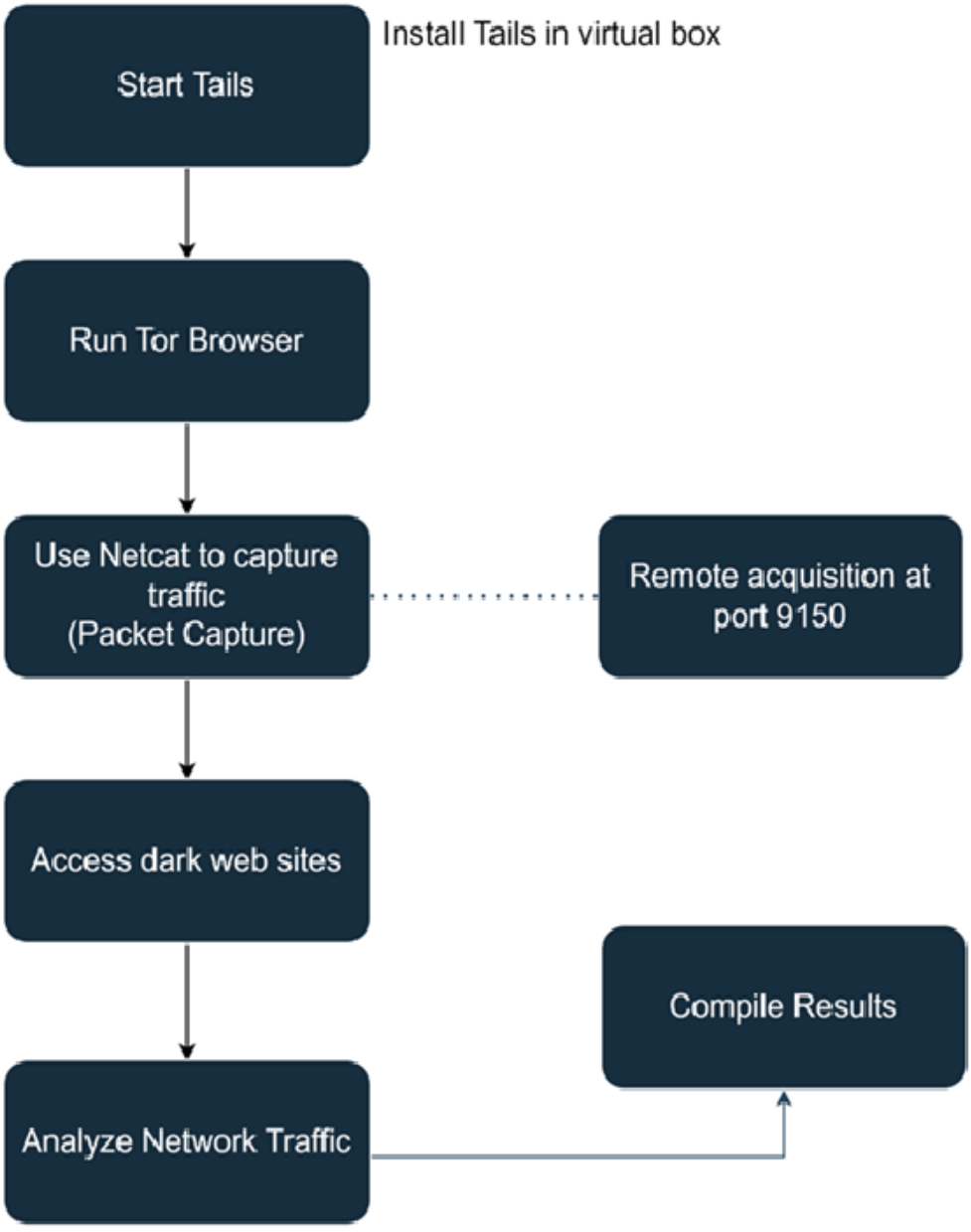


Figure 4Methodology Steps

RESULTS AND DISCUSSION

The forensic investigation of Tor traffic at the local host layer can provide valuable insights into a user's online activity. By intercepting and analysing unencrypted traffic at localhost (127.0.0.1), where the proxy listens on TCP port 9150, forensic investigators can trace all information sent from and to the system, enabling the capture and analysis of Tor traffic.

The results of the traffic analysis revealed that, even though the Tor network is designed to provide anonymity and encrypted traffic, unencrypted network traffic is transmitted between the local host's TCP sockets and is intended for the Tor network. This traffic can be intercepted and analysed by forensic investigators, providing information on the websites visited, data transmitted, and other details relevant to the investigation. The data was captured and analysed, with the following results:

A. IP Address

Through the analysis of host details, the forensic investigator can identify the IP address of the Tails operating system and the MAC address, both of which are essential in identifying the device that was accessing the dark web. The forensic investigator can also identify the Tor browser. Figure 5 shows the host details that the forensic investigator is able to retrieve, including the IP address and MAC address.

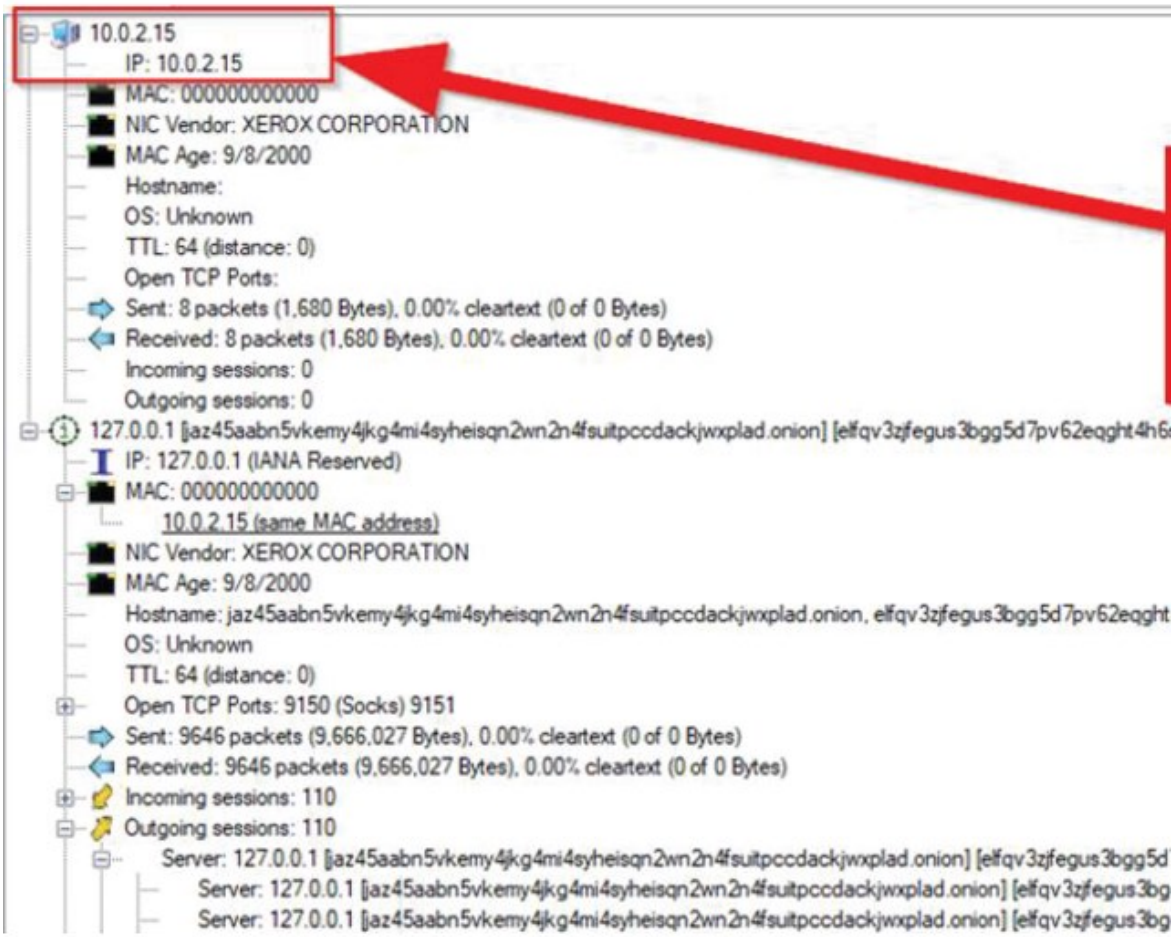


Figure 5Host Details

Through session analysis, the forensic investigator can see the visited URLs, as shown in Figure 6.

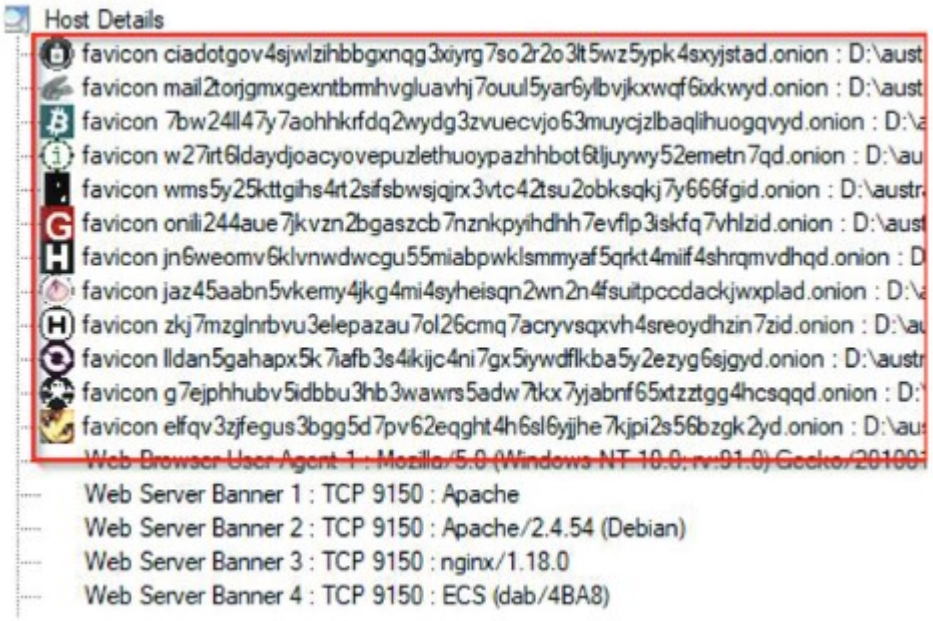


Figure 6Accessed URLs

B. Accessed Images and Files

Through the analysis of the images, the forensic investigator can find the accessed images of all the URLs the Tails operating system user visited (Fig. 7).

Figure 7Files and Images

C. Communication

Clear-text communication was identified, as the emails sent in Tor Mail were found to be in clear text (Fig. 8). This allowed the forensic investigator to identify all the communications of the person who was accessing the dark web, which is important since cybercriminals often use the Tor network for communication.

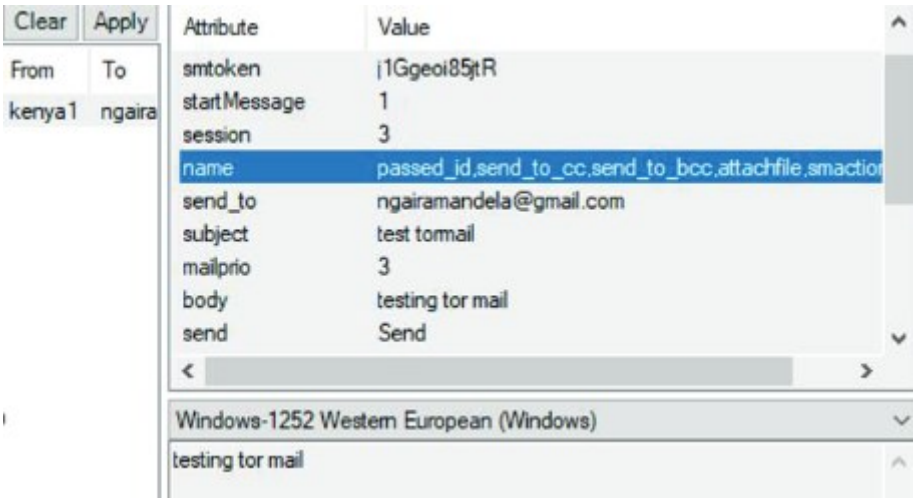


Figure 8Email Communication

D. Credentials

The credentials that were captured show that unencrypted traffic transfers credentials in clear text, as shown in Figure 9. The Tor Mail login credentials are visible in clear text, indicating that Tor Mail is not secure since passwords are saved in clear text. The forensic investigator can use these credentials to log in to Tor Mail for more evidence.

```
Host: mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion/squi
Content-Type: application/x-www-form-urlencoded
Content-Length: 94
Origin: http://mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion
Connection: keep-alive
Cookie: SQMSESSID=u8bkftro0rccaaf69k2o6l8dac; PHPSESSID=ku5u3lsrg7a29dkduhjtov32h8
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

login_username=kenya1&secretkey=kenya1&js_autodetect_results=1&just_logged_in=1&sms
Server: nginx/1.18.0
Date: Tue, 18 Oct 2022 15:10:35 GMT
Content-Type: text/html; charset=iso-8859-1
Transfer-Encoding: chunked
Connection: keep-alive
```

Figure 9 Plain Text Passwords

E. Summary of the Findings

Table I summarizes the key findings of the forensic analysis of the Tor network at the local host layer and highlights the limitations of the network for users, as well as the importance of these findings for forensic investigators.

Findings	Description	Importance to Forensic Investigator
Source and Destination	By examining unencrypted layer of Tor network, forensic investigators can discover the source and destination of a connection with a significant level of accuracy.	This information can be used to establish a trail of communication and track the activities of users on the network.
Visited URLs	Forensic investigators can track the URLs visited by a user while using the Tor network, providing valuable information about their online activities.	This information can be used to establish a timeline of user activities and determine their areas of interest.
Clear-Text Passwords	Clear-text passwords, which are vulnerable to interception, can also be obtained by forensic investigators at the local host layer.	This information can be used to gain access to sensitive information and accounts, facilitating further investigations.
Emails	Emails sent or received through the Tor network can be intercepted and analysed by forensic investigators at the local host layer.	This information can provide valuable insights into the communication patterns and relationships of users on the network.
Web Searches	Forensic investigators can also track and analyse web searches performed by a user while using the Tor network.	This information can be used to gain further insights into the interests and activities of users on the network.
Host computer's IP address	Forensic investigators can also acquire the Internet Protocol address of the host computer, which offers important details about the location and identity of a user.	This information can be used to track the physical location of users and further investigate their activities.

CONCLUSION

In this paper, we have performed a forensic analysis of the local host layer by intercepting traffic using the netcat tool. We describe the composition and operational principles of Tor usage on the dark web and conduct a network forensic analysis. The research has demonstrated that, despite Tor offering its users a certain degree of confidentiality, the Tor network is nonetheless susceptible to forensic investigation.

By monitoring the local host layer, including the Tails operating system, forensic investigators can gain valuable information about the activities of users on the network. Our findings indicate that the dark web, which is accessible through the Tor network, is a hub for criminal activities, making it a priority for forensic investigators. Despite the limitations presented by the network's encrypted layer, it is still possible to study the unencrypted layer to accurately determine a connection's source and destination.

Future research in this area could include investigating machine learning techniques and the feasibility of analysing the encrypted layer of the network. It is important for users to be aware of the limitations of the Tor network and to use it responsibly in order to preserve their privacy and security.

REFERENCE

[1] L. W. Cong, C. R. Harvey, D. Rabetti, and Z.-Y. Wu, “An anatomy of crypto-enabled cybercrimes,” Jan. 2023, [Online]. Available: https://www.nber.org/papers/w30834. doi: 10.3386/W30834.

[2] A. Baraz and R. Montasari, “Law enforcement and the policing of cyberspace,” *Advanced Sciences and Technologies for Security Applications*, pp. 59–83, 2023, doi: 10.1007/978-3-031-09691-4_4/COVER.

[3] N. Al Barghouthy, A. Marrington, and I. Baggili, “The forensic investigation of android private browsing sessions using orweb,” in *Proc. 2013 5th Int. Conf. Comput. Sci. Inf. Technol.*, 2013, pp. 33–37, doi: 10.1109/CSIT.2013.6588754.

[4] N. Al Barghouthy and A. Marrington, “A comparison of forensic acquisition techniques for android devices: A case study investigation of orweb browsing sessions,” in *Proc. 2014 6th Int. Conf. New Technol., Mobility Secur.*, 2014, doi: 10.1109/NTMS.2014.6813993.

[5] R. Brinson, H. Wimmer, and L. Chen, “Dark web forensics: An investigation of tracking dark web activity with digital forensics,” in *Proc. 2022 Int. Conf. Interdisciplinary Res. Technol. Manage.*, IRTM 2022, 2022, doi: 10.1109/IRTM54583.2022.9791646.

[6] A. Ahmed, A. R. Javed, Z. Jalil, G. Srivastava, and T. R. Gadekallu, “Privacy of web browsers: A challenge in digital forensics,” *Lecture Notes in Electrical Engineering*, vol. 833, pp. 493–504, 2022, doi: 10.1007/978-981-16-8430-2_45/COVER.

[7] M. Asim, M. F. Amjad, W. Iqbal, H. Afzal, H. Abbas, and Y. Zhang, “AndroKit: A toolkit for forensics analysis of web browsers on android platform,” *Future Gener. Comput. Syst.*, vol. 94, pp. 781–794, May 2019, doi: 10.1016/J.FUTURE.2018.08.020.

[8] M. A. I. Mohd Aminuddin, Z. F. Zaaba, A. Samsudin, F. Zaki, and N. B. Anuar, “The rise of website fingerprinting on Tor: Analysis on techniques and assumptions,” *J. Netw. Comput. Appl.*, vol. 212, p. 103582, Mar. 2023, doi: 10.1016/J.JNCA.2023.103582.

[9] 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 Sci. Int.*, vol. 299, pp. 59–73, Jun. 2019, doi: 10.1016/j.forsciint.2019.03.030.

[10] S.-Y. Teng and C.-Y. Wen, “A forensic examination of anonymous browsing activities,” *Forensic Sci. J.*, vol. 17, no. 1, pp. 1–8, Dec. 2018, doi: 10.6593/FSJ.2018.1701.01.

[11] A. Warren, “Tor browser artifacts in Windows 10 2,” 2017.

[12] R. Nelson, A. Shukla, and C. Smith, “Web browser forensics in Google Chrome, Mozilla Firefox, and the Tor browser bundle,” *Studies in Big Data*, vol. 61, pp. 219–241, 2020, doi: 10.1007/978-3-030-23547-5_12/COVER.

[13] M. Muir, P. Leimich, and W. J. Buchanan, “A forensic audit of the Tor browser bundle,” *Digit. Investig.*, vol. 29, pp. 118–128, Jun. 2019, doi: 10.1016/j.diin.2019.03.009.

[14] M. Alfosail and P. Norris, “Tor forensics: Proposed workflow for client memory artefacts,” *Comput. Secur.*, vol. 106, p. 102311, Jul. 2021, doi: 10.1016/J.COSE.2021.102311.

[15] A. Kulm, “A framework for identifying host-based artifacts in dark web investigations,” [Online]. Available: https://scholar.dsu.edu/theses/357.

[16] M. R. Arshad, M. Hussain, H. Tahir, S. Qadir, F. I. Ahmed Memon, and Y. Javed, “Forensic analysis of Tor browser on Windows 10 and Android 10 operating systems,” *IEEE Access*, vol. 9, pp. 141273–141294, 2021, doi: 10.1109/ACCESS.2021.3119724.

[17] H. Al Jawaheri, M. Al Sabah, Y. Boshmaf, and A. Erbad, “Deanonymizing Tor hidden service users through Bitcoin transactions analysis,” *Comput. Secur.*, vol. 89, p. 101684, Feb. 2020, doi: 10.1016/J.COSE.2019.101684.

[18] R. A. Sandvik, “Forensic analysis of the Tor browser bundle on OS X, Linux, and Windows,” 2013, [Online]. Available: https://www.novainfosec.com/2213//4/17/noriben-your-personal-portable-malware-sandbox/.

[19] M. J. Chiu Huang, Y. L. Wan, C. P. Chiang, and S. J. Wang, “Tor browser forensics in exploring invisible evidence,” in *Proc. 2018 IEEE Int. Conf. Syst., Man, Cybern.*, SMC 2018, Jan. 2019, pp. 3909–3914, doi: 10.1109/SMC.2018.00663.

[20] R. Montasari and A. Boon, “An analysis of the dark web challenges to digital policing,” *Advanced Sciences and Technologies for Security Applications*, pp. 371–383, 2023, doi: 10.1007/978-3-031-20160-8_19/COVER.

[21] S. Kaur and S. Randhawa, “Dark web: A web of crimes,” *Wirel. Pers. Commun.*, vol. 112, no. 4, pp. 2131–2158, Jun. 2020, doi: 10.1007/s11277-020-07143-2.

[22] F. Mohsen, A. Shtayyeh, M. Struijk, R. Naser, and L. Mohammad, “An approach to guide users towards less revealing internet browsers,” in *Emerging Trends in Cybersecurity Applications*, Springer Int. Publ., 2023, pp. 69–94, doi: 10.1007/978-3-031-09640-2_4.

[23] H. Thorat, S. Thakur, and A. Yadav, “Categorization of illegal activities on dark web using classification,” *Int. Res. J. Eng. Technol.*, 2020, [Online]. Available: http://parazite.nn.fi/roguesci/.

[24] C. Steel, “Stolen identity valuation and market evolution on the dark web,” *Int. J. Cyber Criminol.*, 2019, doi: 10.5281/zenodo.3539500.

[25] I. Pete, J. Hughes, Y. T. Chua, and M. Bada, “A social network analysis and comparison of six dark web forums,” [Online]. Available: https://www.torproject.org/.

[26] V. M. Vilić, “Dark web, cyber terrorism and cyber warfare: Dark side of the cyberspace,” 2017, [Online]. Available: http://hackdefencesecurity.blogspot.rs/2012/02/1.html.

[27] K. Jacka, “Beyond the surface web: How criminals are utilising the internet to commit crimes,” *Advanced Sciences and Technologies for Security Applications*, pp. 109–118, 2023, doi: 10.1007/978-3-031-09691-4_6/COVER.

[28] M. Lakomy, “Dark web jihad: exploring the militant Islamist information ecosystem on The Onion Router,” 2023, doi