ISSN No:-2456-2165

# Achieving Anonymity with the Help of TOR

## (TOR: A Review)

Harsh Kumar
Department of Computer Science and Engineering Manav Rachna International Institute of Research and Studies
Faridabad, Haryana

Akash
Department of Computer Science and Engineering Manav Rachna International Institute of Research and Studies
Faridabad, Haryana

Arun
Department of Computer Science and Engineering Manav Rachna International Institute of Research and Studies
Faridabad, Haryana

Dr. Prashant Dixit
Department of Computer Science and Engineering Manav Rachna International Institute of Research and Studies
Faridabad, Haryana

**Abstract:- Browsers play a critical role in today's world since they are the most often adopted programme for readily accessing web material. Here, data plays an important role because it is the thing with which anyone can learn about a specific individual's interests. In today's digital culture, users are becoming more aware of bad actors of secret data, but doing an unsafe task to store their data as well as making applications insecure. As a result, privacy protection is the solution, and many firms are providing this solution to consumers for a hefty price. However, many individuals are unaware of what an Onion Router browser or the TOR Network are. They are unaware that the Onion Router browser or the TOR Network can be an effective way to protect data by ensuring privacy goals. But, in addition to privacy, it also gives anonymity, which means that no one will ever know who is seeking and what he is searching for. Because of this fantastic feature, the majority of users use TOR browsers for personal and private communication, normal searches, and a variety of other hateful and spiteful activities. People frequently utilise these networks/browsers to remove annoying adverts. Tor is a well-known privacy-protection technology. TOR operates on a virtual encrypted tunnel that is used to transfer the user's data, enhancing the user's privacy policy and allowing the user to avoid being stalked by hackers. Many people, from ordinary people to terrorists and hackers, utilise these browsers or the TOR network. This article goes into detail about Tor, how it works, its goals, some of its related activities, and some of its challenges.**

***Keywords:-*** *Web Browser, Forensics, Private Browsing, TOR. Onion Routing, Anonymity, Tor Traffic.*

## I. INTRODUCTION

The TOR networks, which provide anonymity. Tor, the Onion Router, is open-source and hence free to use. TOR allows users to communicate anonymously. TOR is operated by volunteers, hence it is a volunteer-run system. This volunteer-run system conceals its users' activities. A free and global internet traffic is directed in this direction. TOR has its own network as well as its own browser. TOR is one of the most effective methods for ensuring privacy goals while also providing anonymity. And it is for this reason that it is so popular among its users. The Onion Router shields its users from malicious activities, allows for private communication, and can be used normally. It is the most well-known privacy-protection tool among users who are hooked to anonymity. It creates a virtual encrypted tunnel to convey data from the user. The TOR increases its users' privacy in this way. Tor, in essence, protects its users from those who keep an eye on the content that the user scrolls through, as well as those who monitor the user's every move and analyse the traffic in between. The Onion Router (TOR) is used by people of all professions, from the general public to governmental organizations, journalists, and even the intelligence department in military services. This network is utilised not just by these people, but also by terrorists, hackers, and attackers for harmful purposes. This volunteer overlay network has around 7,000 relays. These relays obtain access controls from those who monitor the network and analyse its traffic, and it also conceals its user's location. The Tor network is also known as the Dark Web. The dark web operates on a peer-to-peer network. It is sluggish because of the peer-to-peer connection. Not only does this TOR offer more hops. This is now a function of the users. Using this TOR browser is slower than using other browsers. As the number of people using the TOR network grows, Its user base has now surpassed one million. And there are over 7000 relays that route all of the traffic of its growing crowd. This places a strain on each server, resulting in latency.

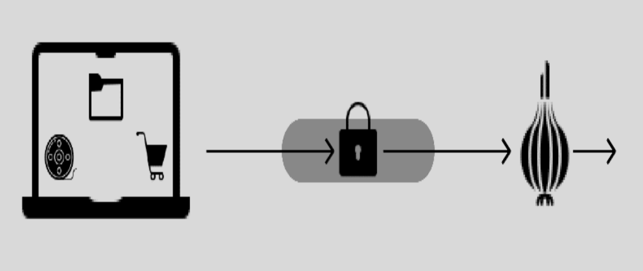

Fig 1 TOR Encrypts Data

## II. FRAMEWORK

The term "accessing network" refers to an architecture that restricts the network's vulnerability to traffic analysis. And this network employs Onion Routing, also known as the TOR network. This network fulfils the users' desire to remain anonymous. Tor is an open-source programme that is thus free to use. This is the finest choice for achieving anonymous communication. Anonymity and privacy protection are crucial components of this. And these crucial characteristics allow its users to express themselves freely. This network's mission is anonymity, which aims to secure its users' data (information). Because data can expose the true identify of a user. This information contains the user's true name, IP address, and location, among other things. A proxy server is a TOR. The TOR Network's goal is to safeguard its users' privacy and give the freedom and strength to conduct secret contacts without leaving traces on the internet or having Internet activities evaluated. The privacy issue is to guarantee that no one collects personal and private data from users, such as location, contact information, account information, and browser history, without their knowledge. Tor is now widely used for internet privacy, anonymity, and defence purposes.

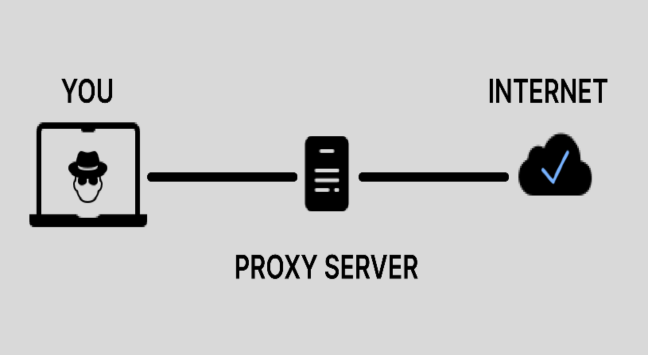

Fig 2 Tor Uses Proxy Server to Access Data.

- *Objective of TOR*

TOR primarily transports internet traffic and supports a network with over 7,000 relays, concealing the user's location and preventing unauthorised access or surveillance. It is impossible to learn about the user's activity when using TOR. It covers the user's web searches on the website, online postings, messages, and other modes of contact. As a free network, TOR has provided freedom to about 36 million individuals worldwide by providing free internet access. It also gives controlled privacy and anonymity. According to several statistics, the TOR network has over 2.5 million active users. The TOR network connects users to the internet via over 7000 nodes, which transport internet traffic. The bandwidth of the nodes is 25.5 Gbps.

- *Theory*

Route users is an imaginative technique to connect to the Tor overlay network. This is a newer version of Mozilla Firefox. The only difference is a few added features. Anonymity and privacy are among these benefits. When comparing Mozilla Firefox to the TOR browser, Slant recommends Tor for those who value their privacy. Slant is a product suggestion community. This community's goal is to give the public with the finest application product or game. When asked about the finest desktop web browser among TOR, Mozilla Firefox, and other browsers, this tilt community recommended its users by ranking the priority of the public. That is, as follows: The greatest desktop web browser is TOR, with Mozilla Firefox ranking ninth. The reason for using the TOR browser is that if one follows the instructions carefully, The Onion Router is the NEC+ Ultra in terms of safety and privacy. At least for the time being. It is more difficult to discover a user's activity on the TOR network. Visits to websites, communications, modes of contact, and posts on online platforms are examples of activities. The intention behind TOR is to provide security of the personal data and privacy. It provides the independence and the strength to accomplish confidential interactions without leaving traces on the internet and without having Internet activity calculated. Crucial features of TOR are: TOR launcher, TOR button, in addition that there is no script. Also, we can find HTTPS everywhere. By default, one browsing is built for the private mode. It includes the option to clear Browsing activity and some rarity related information like cookies and some surfing related data after the browser is exited.

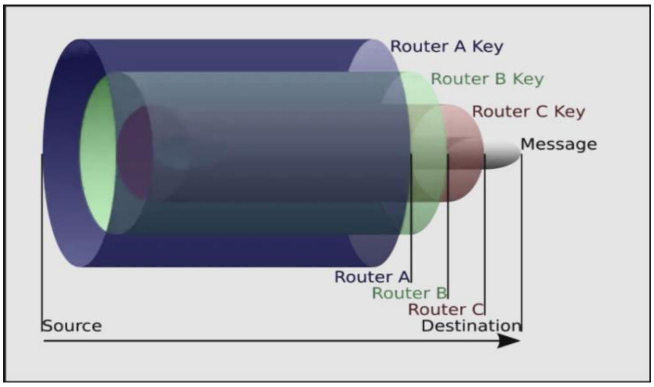

Fig 3 Layers in TOR

- *How will it Work ?*

The onion router's browsing is based on relays. This dark browsing utilises an overlay relay network that is distributed globally. This over-layer relay network assists internet users in retaining their anonymity and privacy. To communicate, this successively picks a network that creates a physical circuit. This adds at least three constantly relayed relays. Tor client downloads relay information into the source machine directory server. Using the Diffie-Hellman of Major Exchange Protocol, the encryption key is exchanged with the selected relay. Encryption is an application layer of the stack in communication protocols; this onion route is organised like several layers of onions. TOR encrypts information. It has a node destination at a later time. This implies that the IP addresses are alternately sent across a virtual circuit to the sequential and random-select tor relays. This occurs continually, and each relay delivers the remaining encrypted data to the others as a result. Those last relays then decrypt the sole true and final innermost layer of encryption, transmitting the actual data to the point while concealing the source of the most significant IP address. This occurs because the communication path was only partially covered at each hop of the tor circuit.

This strategy thus avoids any single point where communicating peers are resolved by network monitoring based on understanding their true source and destination. TOR conceals the user's identity and originating location and is also known as the DARK WEB since it is inaccessible to major search engines like Google. TOR is a discontinued model. And this is for building a web. Web is not accessed by Internet users and users using TOR. To connect to a server, it is used, so that the server will only talk to a client, which is routed through the TOR network, meaning that the search engine will not be able to find the content on them. With

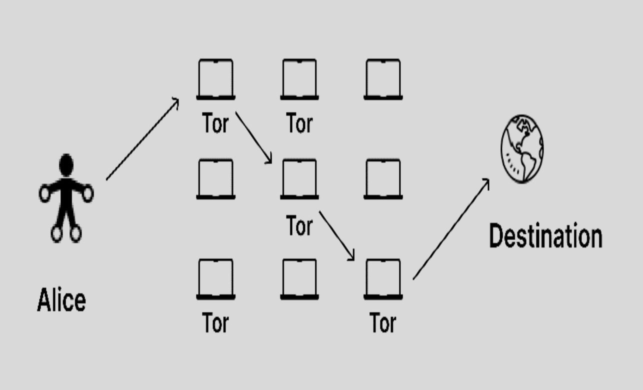

Fig 4 How TOR Works

The third encryption layer is decrypted by the exit node. Then This network, only routing is done using volunteers' computer the user can see that there is no encryption in network packets around the world to route traffic around the world, and many anymore, so that someone sniffs the data between the exit times there are fewer opportunities to locate the actual source. node or the exit node. There is also a Google server they The TOR browser sends a request called a pro-circuit request to control the two can read data as it is because the node without the Tor directory server. TOR is a server that has a list of available nodes in its network. This server will return an entry node to a middle node and an exit node back to your Tor browser. The TOR browser sends a request called a pro-circuit request to the Tor directory server.The server of this returns the entry, middle and an end node back to the browser of tor. Now, this layer is decrypted by the middle node. No one can read the data because it is encrypted with an exit that does not secure the server.

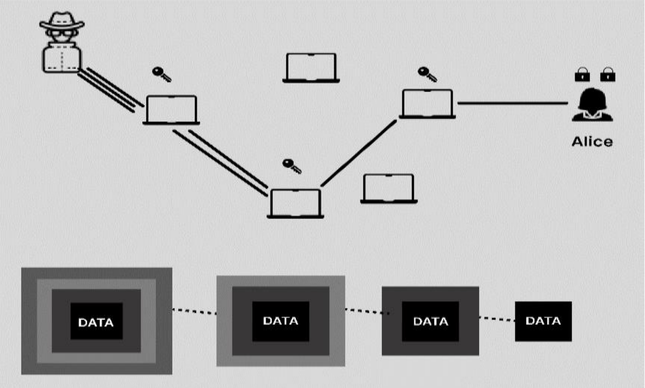

Fig 5 Only User have the Key to Access Data.

Now the middle node knows that the request should be sent to the exit node. Once the packet reaches the exit node it will be peeled from the third layer, this layer is encrypted with the exit node key and only the exit node can be cryptid.

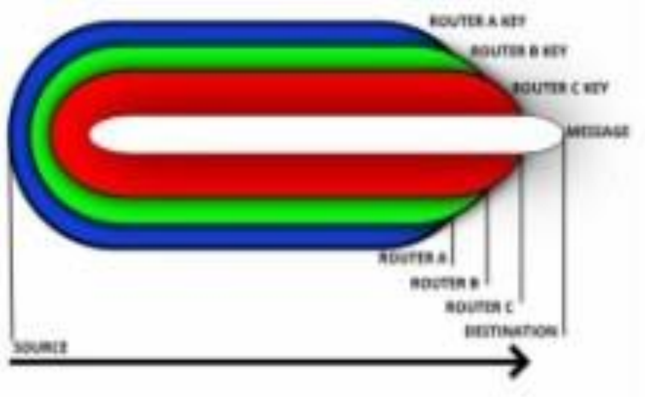

Fig 6 Layers in TOR while Routing.

The weakest point of security TOR NETWORK whatever exit node, can see your data. But they still can't track your Exit Address No request is to be sent to GOOGLE.COM server and the package will reach google.com server. If someone is trying to sniff the data here, they can only see that the request is going from the entry node IP to the middle node IP. Also, he cannot see what the contents of the packet are because it is encrypted with the middle node and only the middle node can decrypt it, so this guy cannot know which site you are visiting, He cannot see what you have discovered!

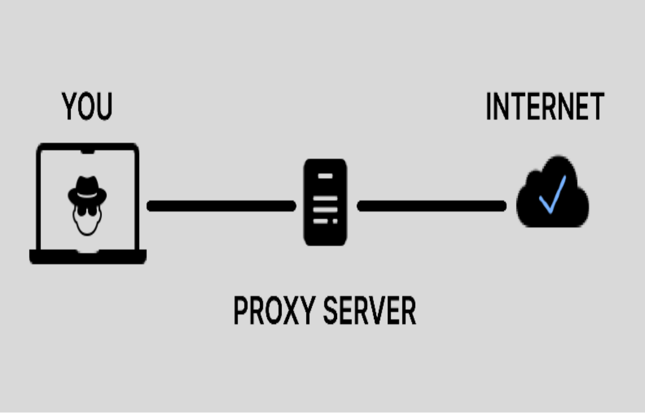

Fig 7 TOR Uses Proxy Server to Internet

➢ *Some Related Works*

Online anonymity in this surveillance age First and foremost, for the sake of free expression. The initial research was submitted and proposed with a Mix-Net inside while being in this realm of anonymity. This work was subsequently used to create further anonymous solutions. It employs a couple extra levels of encryption and mix arrays. But, the Remailer was the first actual application developed by other forgetfulness service providers. With a secret one Messages that utilises databases for mapping, the remailer has obtained Users' identities. For the anonymity of the service provider, privacy was preferable for user identification. Finally, due to legal concerns, the service was ended in 1996. The **Cypherpunk remailer** was then introduced to the general public. The Type I remailer is another name for this **Cypherpunk**. This is inspired by Cham's **Mix-Net Mix-Net**. This message was encrypted using public key cryptography. Mix Master was the superior version. Message segmentation and padding methods were utilised in cypherpunk. This was frequently an anonymity that was good at delivering pure anonymity but had a danger of tagging and blending attacks, which were eventually patched into the N-Mix minion remailer. The Onion Routing (TOR) protocol was developed considerably later, in 1995. At that time the US Naval Science Laboratory embarked on a project to style an anonymous network for military communications. Onion Routing was the name of the project. It was a network with minimal latency. For anonymity, encryption and an onion network layer were utilised. After a few years, the project's second generation was dubbed TOR (The Onion Routing). This was accomplished by using the TOR browser. It is a free software for using the TOR network. In addition, it operates entirely on privacy mode so that user privacy is often insured. As it provides a high level of anonymity very soon. This is the most preferred and most preferred method for the three users, who especially love the idea of anonymity by cyber criminals. As back tracking, information is the biggest challenge and that is why it is used for illegal cases.

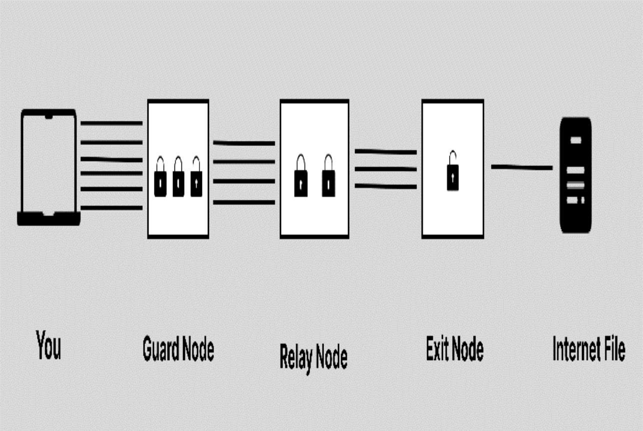

Fig 8 TOR Relay

## III. LITERATURE REVIEW

With the goal of Forensic study of Tor Browser, **Jadon Iqbal** suggested: Although this browser has many flaws, TOR is fairly useful despite having certain faults since it enables both privacy and anonymity at the same time. It provides crucial features such as a TOR button, no script, and HTTPS, which increases everyone's anonymity and privacy.

- **Jadon Iqbal** analyses the system registry, RAM, and hard drive for all artefacts that store the system browser when it opens and exits the user system when it closes. He summarised the artefacts related to Tor installation, use, and browsing behaviours. Tow Browser mostly leaves several artefacts in system memory on the user's machine. It may contain artefacts retrieved from the host system. Jadon also explored numerous situations in order to encounter a forensic investigator during the inquiry. It is critical to recover information from memory and hard disc. These critical essential bits of knowledge will benefit the tor user. And, with the incoming budget, researchers and investigators will soon receive a lot of assistance. This publication will assist researchers and investigators on a tight budget.
- **Muir M, Limit P**: He proposed that an investigator may be a Tor. The literature study revealed limited research in the subject of tor forensics, implying that the demand for further forensics had grown critical. A approach that permitted live forensic analysis followed by static analysis of virtualized testing machines was presented here. This makes the forensic procedure more intensive in order to gather the most knowledge about the accessible browsers in the shortest amount of time. This study article explains experimental technique while also providing general conclusions for trials that may be used in real-world investigations.
- **Eduardo Hidalgo:** Enrique Alegre is the target. This study looked into the automatic classification of photos and pictures submitted to the Tor Dark Net.
- **Rebecca Nelson, Atul Shukla:** They investigated digital artefacts and their locations, which may be accessed via Google Chrome, Mozilla Firefox, and TOR, respectively, all of which have private modes. That investigation was pushed into the current digital realm, where we may uncover artefacts, and many allegations regarding the privacy of individual surfing modes were also proven.

## IV. PROBLEM WITH TOR

You may be more anonymous on the Internet with the free TOR browser than you would with a browser like Mozilla Firefox or Google Chrome. However, TOR (which stands for Onion Onion) is slower than other browsers and allows for certain potentially dangerous conduct.

The dark web or TOR is sluggish because we normally need to use special browsers like TOR browsers, which do not connect directly with your computer to the dark web sites, or because your requests run via those three nodes, which use peer-to-peer connections rather than core network connections. When you request a website and it shows on your screen, the delay between those stages increases.

In this section, we move from one covert router to another, which leads to encryption. Because of the jumping/hopping, both encryption and decryption require a lengthy time to process. Following each encryption, each hop establishes a network or link with the other hop. You may require a minimum of 3 to 10 hops; these hops may be greater, depending on the browser settings. If it takes more than 10 hops, your pace will be exceedingly slow as the time to reply increases.

Some websites are not loading because they have vanished. The '.onion' domain is a volatile market. Some sites may run out of financing, while others may host unlawful information that is removed by law authorities.

## V. TOR CAN BE RISKY

The Onion Routing browser allows its users to access the "Surface Web" and the "Deep Web". The "Surface Web" is known by most people on the Internet whereas the "Deep Web" is the leftover part of the Internet. Here, the information is unorganised that means data is not organised into websites. Hence it cannot be found easily. Deep Web provides valid methods to protect private data. But a part of the Deep Web, called the Dark Web, hides illegal activities, such as drugs, guns, child pornography, and stolen credit numbers. Even computer-security experts are wary of the Deep Web; The average computer user should avoid this.

A dark browser is a web browser intended to prevent a user's online activity from being tracked by anyone and even network surveillance, making it difficult for ISPs to trace it. Not that no one can trace it, no! It is traceable but is very difficult to detect even for hackers.

- *Why is an Alternative Required?*

While the Tor browser allows browsing the Internet with privacy, there are a few downsides as well: There are complaints of the users of being less user friendly. And also, it was difficult to navigate. Also, they find it slower than CLEARNET. And it was not a big help when browsing the dark web.

## VI. THERE ARE SOME ALTERNATIVES FOR THIS TOR NETWORKS

With these losses, some alternatives like VPN service +TOR browser, Freenet, Invisible Internet Project (I2P), Whonix OS, Tails, TechnologyReviews24 Verdict.

In **VPN service + TOR browser,** the best option of TOR browser would be TOR browser, which will have some enhancements! Yes. Tor can be made almost invincible when used with a paid Virtual Private Network (VPN) service. As VPN can hide the user IP address. VPN hides its actual location, making it unrecoverable. Freenet is one of the top options for the Tor browser. Freenet is a peer-to-peer system i.e., a distributed network system which is somewhat like the websites of torrent. This enables the user to maintain online privacy and avoid surveillance. Users who are wishing to use the Internet using Freenet can directly download and install the software on their system and can begin the journey of using it through a routine browser. To download the software, go to the Freenet download page. **Invisible Internet Project (I2P)** is also a popular one for private browsing. It works on the same principle of Freenet and Torrent. But still it gained anonymity through some private connections which were done between two parties. Its effectiveness is one of the unique points in selling I2P. It is transferring large amounts of data over the Internet with complete anonymity. Visiting the I2P download page one can start the journey to Internet anonymity. Another effective solution is **Whonix OS.** It is also an open source and hence free operating system. It runs somewhat like a virtual machine on the already existing Operating System. WOS uses the TOR network as its underlying root and forces all connections to pass through the anonymous TOR network. Whonix, thus, creates a completely anonymous environment over existing ones preventing the virus on the PC from sending data. Not only this, but the negative point in this is also the sheer size of the full package. For Windows, the size of the Whonix OS is 1.6 GB. To download the software for your own computer, go to the Whonix download page. Another Alternative is **TAILS.** Tails is like Whonix OS. It is a live OS. The full form of TAILS is The Amnesic Incognito Live System. For anonymous browsing, TAILS basically uses TOR. The system, which can be accessed using a bootable pendrive, forces its traffic to cross through it in the anonymous TOR network by creating complete anonymity for the user. The negative aspect for using Tales involves the huge download size of 1.1 GB as well.

- *The Idea is to:*

As there are only 7000 nodes which makes the network slow and steady. If we want our network to be fast, safe and much more popular among the general public, we need to increase the number of nodes. If the number of nodes gets increased then the privacy of any individual will not be in any kind of threat. Now the question is how to increase the number of nodes? Our idea or our assumption to increase the number of nodes by linking each device with each other i.e by making each device in the network as node. Because of this the more the devices, the better will be the network. The users will use their network to provide nodes to the other users. The second question is, why will people make their devices as nodes? The solution for this question will be, if we provide a kind of reward to the users who are making their devices as nodes then it may be possible.

If the idea works well then, the number of nodes will be increased, speed of the network will be increased and hence there will be a great increase in the number of the users and as a result privacy will be provided to all the users who are in need of it.

## VII. CONCLUSION

Tor isn't flawless, and the user is still the weakest link. With enough time and money, the government can figure out who the user is, so instead of expecting a blanket of anonymity, it's preferable to design a specialised use case. Tor is used by journalists, the military, the police, and political activists all across the world. Anonymity and security are not the same thing. The Tor browser has all of the same security vulnerabilities that browsers have. There is no indication that the Tor network was ever compromised, but users are still vulnerable to browser assaults. To target criminals, the FBI famously employed spyware built by a former Tor engineer. Many groups oppose the government's power to hack. Although Tor can assist you in being anonymous, keep in mind that your personal conduct is also a vulnerability. If you use any service that may be traced back to you, your position will be weakened. Being anonymous on the internet is difficult and needs a lot of discipline. Tor can help you save time along the road.

## REFERENCES

[1]. Goldschlag, David M., Michael G. Reed, and Paul F. Syverson. "Hiding routing information." International workshop on information hiding. Springer, Berlin, Heidelberg, 1996.

[2]. Burzstein, Gaurav Aggarwal Elie, Collin Jackson, and DanBoneh. "An analysis of private browsing modes in modern

[3]. Said, H., Mutawa, N.A., Awadhi, I.A., & Guimaraes, M. (2011). Forensic analysis of private browsing artifacts. 2011 International Conference on Innovations in Information Technology, 197-202.

[4]. Chivers, H. (2014). Private browsing: A window of forensic opportunity. Digital Investigation, 11(1), 20-29.

[5]. Ghafarian, A., & Hosseini, S.A. (2015). Analysis of Privacy of Private Browsing Mode through Memory Forensics. International Journal of Computer Applications, 132, 27-34.

[6]. Filleau, J., & Zizyte, M. What Private Browsing Leaves Behind.

[7]. Gao, X., Yang, Y., Fu, H., Lindqvist, J., & Wang, Y. (2014, November). Private browsing: An inquiry on usability and privacy protection. In Proceedings of the 13th Workshop on Privacy in the Electronic Society (pp. 97-106).

[8]. Huang HY., Bashir M. (2020) "Seeking Privacy Makes Me Feel Bad?": An Exploratory Study Examining Emotional Impact on Use of Privacy-Enhancing Features. In: Arai K., Kapoor S., Bhatia R. (eds) Advances in Information and Communication. FICC 2020. Advances in Intelligent Systems and Computing, vol 1129.Springer,Cham. https://doi.org/10.1007/978-3-030-39445-5_44

[9]. Danezis, G., & Clulow, J. (2005, June). Compulsion resistant anonymous communications. In International Workshop on Information Hiding (pp. 11-25). Springer, Berlin, Heidelberg.

[10]. Hellegren, Zelda. (2016). Deciphering Crypto-Discourse: Articulations of Internet Freedom in Relation to the State. SSRN Electronic Journal. 10.2139/ssrn.2909373. 4

[11]. Ohana, D. J., & Shashidhar, N. (2013). Do private and portable web browsers leave incriminating evidence?: a forensic analysis of residual artifacts from private and portable web browsing sessions. EURASIP Journal on Information Security, 2013(1), 6.

[12]. Edman, M., & Yener, B. (2009). On anonymity in an electronic society: A survey of anonymous communication systems. ACM Computing Surveys (CSUR), 42(1), 1-35.

[13]. Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2), 84-90.

[14]. Kelly, D. J. (2009). A taxonomy for and analysis of anonymous communications networks.

[15]. Srusti D. Mehta , Deepak Upadhyay, 2020, A Review on Classification of Tor-Nontor Traffic and Forensic Analysis of Tor Browser, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 09, Issue 04 (April 2020),

[16]. Jadoon, Abid & Iqbal, Waseem & Amjad, Muhammad & Afzal, Hammad & Bangash, Yawar. (2019). Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web. Forensic Science International. 299.

[17]. Olivier, M. S. (2003). A layered architecture for privacy-enhancing technologies. South African Computer browsers." Proceedings of the 19th USENIX Security Journal, 2003(31), 53-61.

[18]. Symposium. 2010.

[19]. Muir, M., Leimich, P., & Buchanan, W. J. (2019). A forensic audit of the Tor Browser Bundle. Digital Investigation, 29, 118-128.https://www.researchgate.net/publication/342338294_A_Review_ of_ Web_ Browser_Forensic_Analysis_Tools_and_ Techniques

[20]. Oh, J., Lee, S., & Lee, S. (2011). Advanced evidence collection and analysis of web browser activity. Digital Investigation, 8(SUPPL.), S62-S70. https://doi.org/10.1016/j.diin.2011.05.008

[21]. Eduardo Fidalgo, Enrique Alegre, Laura FernÃ¡ndez-Robles, VÃctor GonzÃ¡lez-Castro, Classifying suspicious content in tor darknet through Semantic Attention Keypoint Filtering, Digital Investigation, Elsevier, May 2019.

[22]. S. Helmers, A brief history of anon. penet.fi – the legendary anonymous remailer, Comput Mediated Commun. Mag. 4 (1997) 9.

[23]. D.J. Ohana, N. Shashidhar, do private and portable web browsers leave incriminating evidence? a forensic analysis of residual artifacts from private and portable web browsing sessions, EURASIP J. Inform. Security 2013 (2013) 6.

[24]. Tor Project, Tor Metrics, (2017)

[25]. On the Memory Artifacts of the Tor Browser Bundle Conference Paper · April 2014 CITATIONS 3 READS 1,264

[26]. Internet and data of the users accessing it.

[27]. Security and privacy threats: https://www.zdnet.com /article/online-security-101-how-to-protect-your privacy-from-hackers-spies-and-the-government/

[28]. TOR anonymity network, https://en.wikipedia.org /wiki/Tor_(anonymity_network)

[29]. https://blog.insiderattack.net/deep-dive-into-tor-the-onion-router 6de 4c25beba7

[30]. https://vpnoverview.com/privacy/anonymous-browsing/is-tor-safe

[31]. https://ieeexplore.ieee.org/abstract/document/9089497/authors#au tho rs

[32]. Tor Project, Tor Browser, (2017) Available at: https://www.torproject.org/projects/torbrowser. html. en.

[33]. Top Ten Alternatives to Tor Browser: https://menafn.com/1099536827/Top-Ten Alternatives -to-Tor-Bro wser

[34]. Why is the dark web so slow and why do some sites not even load? https://www.quora.com/Why-is-the-dark-web-so-slow-and-why-d o-some-sites-not-even-load

[35]. TOR browser is secretive, slow and can be risky: https://www.startribune.com/tor-browser-is-secretive -slow-and-can-be risky/565990601 /?refresh =true

[36]. Abusing TOR Anonymity Network for High-Bandwidth anonymous internet usage: https://blog.securityinnovation.com/ abusing-the-tor-anonymity-ne twork-for-high-bandwidth-anonymous-internet-usage

[37]. Why Tor is slow and what we're going to do about it: https://blog.torproject.org/why-tor-slow-and-what-were-going-do about-it

[38]. How can I make TOR run faster: https://support.torproject.org/tbb/tbb-22/

[39]. How to Make Tor Run Faster: How to Make Tor Run Faster

[40]. Why is the Tor browser slow? How can it be improved: https://www.quora.com/Why-is-the-Tor-browser-slow-How-c an-it-be-improved

[41]. The Trouble with Tor: https://blog.cloudflare.com /the-trouble-with-tor/

[42]. The trouble with TOR: https://www.esecurityplanet.com/applications/the-trouble-wit h-tor/

[43]. Web Browser Forensics in Google Chrome, Mozilla Firefox, and the Tor Browser Bundle :https://link.springer.com/chapter/10.1007/978-3-030 -23547- 5_12