PENINSULA PUBLISHING LLC

SHIFRA

Vol. **(2024)**, 2024, **pp**. 105–112
ISSN: 3078-3186

Research Article

Directed Mining of the Dark Web Using Hell9: Advanced Techniques for Exploring and Analyzing Anonymous Networks

Thaar Kh. Asman[1, *], Haider D. Abd [2]

[1] *College of Arts, University of Anbar, Anbar, Iraq*

[2] *College of Physical Education and Sport Science, University Of Anbar, Anbar, Iraq*

ARTICLE INFO

Article History

Received 2 Apr 2024

Revised: 20 May 2024
Accepted 20 Jun 2024
Published 12 Jul 2024

Keywords

Darknet,

Deep web,

Dark Web,

Deep net,

Tor.

ABSTRACT

In the World Wide Web the dark net is still theoretically part of the Internet. But its access software or configuration and permission is different from the other sites. The dark web is not indexed by the public web search engines, such as Google and Bing. If you type in any keyword there will be pages of millions returned as a result. For example, trying to quantify the vastness of the Internet. If one were to think about how many sites are representative for just one hundred keywords, and how many since “n” different number combinations are equally valid on search engine queries? When we browse the Internet using the web browsers to visit sites our eyes really just see what is called the Surface Web. Which is a part of the Internet you can visit from different hypertext information displayed as webpages simply. Still, without the help of search engines, you can use the various resources from Internet that the Surface Web cannot present to you. The deep web where Tor is used is a place hard for hackers, spies, and even government agencies to watch over users. However when they are monitoring the site they cannot tell how website operators are processing with their data files on them all of a sudden. This paper describes the Businessman, Scientist, Students & Any Person safely and Anonymously Getting onto the DarkNet 100% with HeLL9 Project.

1. INTRODUCTION

This Named "deep web" or "invisible web", it had its initial emergence in the mid-90s with the Internet coming into society at large. Pirates such as Dread Pirate Roberts and Ross William, journeyed first into this vast sea-blocked environment-that is, over the usual internet! -And markets emerged here. With no one really in control of them, these markets thrived! Such luxury goods of all types were always to be had for sale everywhere anyone wanted them: goods that any man sin his or her right mind would say could not possibly exist in this world of legal inspection and strict identity tagging. Why, graded essays (coinciding totally with the subject matter both at school or on exams) are available for the paying in five minutes' time from any internet-connected node within all parts outside China - or even more likely provided of course at some other point along its route out from wherever it originates before reaching another country. China's toxic reputation as a private-trade heaven by contrast needs no explanation at all this late date The internet is an increasingly safe environment for criminals. Dark Web is a part of the Internet (Deep Web) and cannot be accessed by regular browsers such as Google, Bing. This is due to the fact that no sites inside dark internet are indexed by those browsers; the total amount in fig1 of the dark internet is greater than that in surface Internet for which 4% belongs to it (Section 5).Just the 60 big sites in deep web contain forty times as much text as does the total amount of prose in surface networks [1].The World Wide Web has been established on two major foundations, the visible internet (surface internet) and the dark internet (invisible internet), with the visible part accounting for 90%-96% of all content It is easy for the user to get a overview of what is really going on by browsing in regular browsers with ISP’s, which transmit thousands upon hundreds of images a second.The deep internet is a kind of anonymous search. Employing a good VPN, people search the dark-web with safety ensured. Straddling two definitions, Dark Net (or Darknet) is a public umbrella term which includes both hidden segments of the Internet and superimposed architecture. It is impossible to access the Darknet with your ordinary search engine and network resulting from that software way of doing things shepherded down there (That is transferred by using place names). Since there is no Internet connected to the public, it can't be reached. A dedicated search engine utilizing special software is needed.

*Corresponding author email: Thaar.asman@uoanbar.edu.iq
DOI: https://doi.org/10.70470/SHIFRA/2024/012

Meanwhile, using this tool that changes your IP address multiple times in rapid succession means that lawbreakers will find it harder to track you down [2]

2. WHAT IS DARKNET OR DARK WEB?

To begin with, the Darknet, or Dark Web, is a part of the internet that many people don't even know about. The search engines that almost everyone uses, such as Google/Yahoo/Bing, have no idea what is there. And it's not indexed by any of those conventional search engines. You never have to worry yourself with discovering and delving deep into the deep web part. In essence This is where all the “dirty” goods actually reside: Child Porn, Darknet Markets you can buy drugs, weapons, guns etc.; Red rooms that broadcast live torture, rape scenes where people are disemboweled and vivisected right in front of your eyes on the web screen –murders for sightseers; human trafficking routes for any destination long or at home, child pornography videos where the young body parts become sexual objects again but this time for profit in an overseas country with different laws prohibiting such things locally. It's also the base operations mill in hacking operations conducted by groups such as Anonymous or LulzSec and just about any other black hat crime conceivable on this planet..The onion network is where the dark web is alone located, and through use of a Tor browser you can access it. Most people may be used to a Internet of perhaps 4-10%, but many times more of the total Internet is captured by this deeper, invisible side we are talking about. This shit is all on the onion network because the network is in no way under the control of any government, and that makes it the perfect home for the whole dark web consortium.While the dark web is located on the onion network thusly, due to u cant nametag ur websites ". com/.net/.org, only an.It's not like that at all". onion suffix is used for URLs. Therefore the deep web is really just the “big picture”, and underneath it there's a dark web that is more shady and sinister.

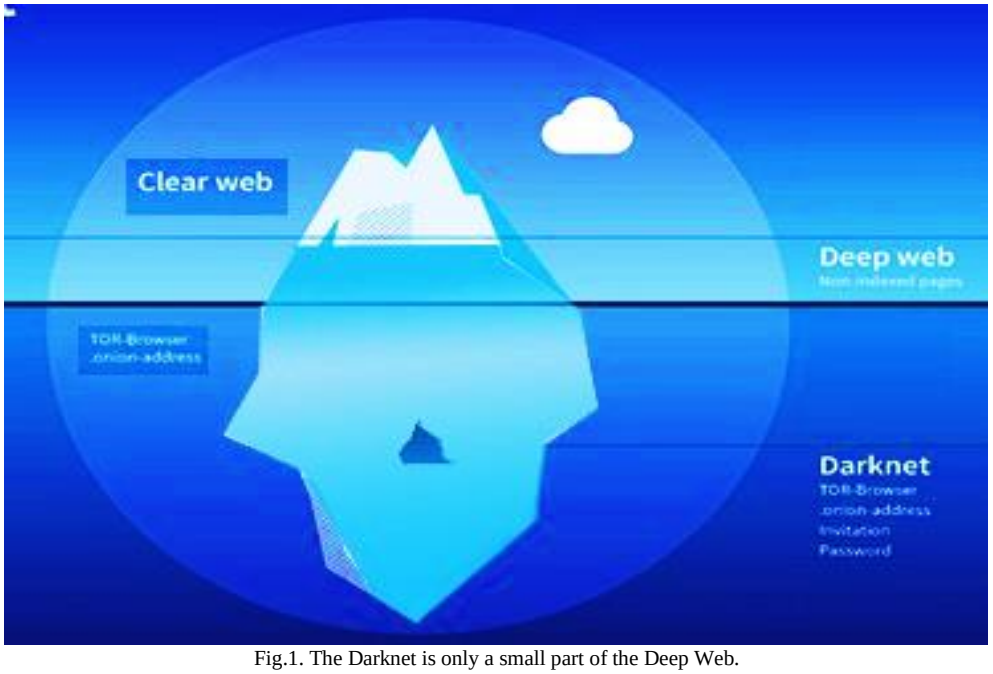

Fig.1. The Darknet is only a small part of the Deep Web.

3. BACKSCATTER IN DARKNET

Bowling in the Darknet Darknet interface has an interesting form of technical communication. On a regular basis, this form of problem-solving communication means simply telling the consumers things to do that will adapt to lack of good communication and minor errors. In general, backscatter refers to accidental responses or traffic generated as a result of interacting with hidden services and / or the network actors in a dark net. But also generalize, it can mean traffic insolently intended by one side (usually incoming). pedalPress. org is also an origin of backscatter; this means the user traffic in compliance with it may come unexpectedly, or in what is generally an attack. Backscatter can also result without any special effort made in the Darknet. Typically, backscatter is experienced when using a system to probe or scan portions of the Darknet, such as opening an illicit site or hidden service, which in turn results in the network creating traffic in the opposite direction (the user or network scanning it). [3] The fact that it receives and reacts to network traffic is in what can be called backscatter 1.Scanning or probing: When automated systems attempt to scan for open or vulnerable services in the Darknet, any unaddressed or unhandled network packets may result in backscatter. The probe may not reach its target, but the server or network may respond, inadvertently sending traffic back to the source. 2.Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks: In the Darknet, where anonymity is a key characteristic, backscatter can sometimes be an artifact

of these attacks. For instance, when an attacker uses botnets or proxy servers to launch a DDoS attack, they may not see the full effect of the attack themselves, but the backscatter from misconfigured or unprotected nodes may return traffic that hints at attack propagation. 3.Data leakage: In some cases, Darknet networks or services that are poorly configured may inadvertently leak information back to probing users. This information could be sensitive and may inadvertently expose vulnerabilities or other network secrets.

4. HONEYPOTS AND DARKNETS

In dark networks, honeypots are a key monitoring tool for cybersecurity professionals and the police to observe, capture and understand cyber-criminal activities that target these secret networks. The ways, patterns and purposes behind cybercrimes can be found out by inducing malicious users into cooperating with embedded systems. However, careful planning, ethical considerations and legal implications must be considered in deploying them, particularly when setting them up on anonymous networks that are also secure like Tor. And them too served as a gateway for one to have a look at the parts of that iceberg which lurk under water, the TOR-Browser. Getting from Deep Web to Darknet is a different landscape. Conversely, you do not need any special equipment to access the familiar visible web - just an ordinary browser will suffice. Butbeneath the surface where normal network operates, where invisible and search engine-driven points in space link up is what we call 'deep web'. A software an. This is not so uncommon.The only means of access to the Deep Web is with a particular type of software and its companion browser settings[4][5].

5. THE NAVIGATION TO THE DEEP WEB

The DARK WEB cons of a number of the hidden.ALLs sites.This part of Intertraservers are hidden, but they still have an IP number of the same not encrypted, Tor browser must be used to Accessthese if we hope THEM via the dark net and do not want anyfeathers ruffled ToAccess sites on the deep web, you need special browsers like Tor browser, Freenet, and I2P. The deep web does not have an index or rating system to help people find the information you need. So you must know the site link before reaching it, there are many links which leads to different sites in a list of examples from 1 to TABLE1 as shown, flow. At the time when you ask for some specific site, the request goes from one node to another; but messages are enciphered ina manner such that neither of these nodes (or anyone else) location where the device is located knows only sending or receiving terminal. before entering the dark web you need to know this, how dangerous it is. for authorities or gangs might be out monitoring it and your computer alsoof course the hidden has tracking spyware, malware and viruses [4]

TABLE.I DARKNET SERVICE LINKS

Dark Web URL	Description
http://easycoinsayj7p5l.onion/	Bit coin wallet with a free bitcoin mixer
http://qc7ilonwpv77qibm.onion/	a western union exploits
http://nr6juudpp4as4gjg.onion/doublecoins.html	Double your bitcoins illegally host
http://5mvm7cg6bgklfjtp.onion/	discounted “Stolen” Electronics goods for sale (Apple Products and more)
http://ybp4oezfhk24hxmb.onion/	The hitman of service network

6. DARKNET SEARCH ENGINES

If we want to search for websites that you are interested in, ordinary search engines cannot help at all.Use Duck Duck Go for normal web searches and its.onion URL as the search or TORCH (Tor Search Engine) to search pages not seen by normal search engines. Do not give out personal information and remember that your anonymity is important.The Darknet is a place where you don't want to stir in the wrong pot of stew.The public may access Duck Duck Go's Darknet version using TOR at http://3g2upl4pq6kufc4m.onion.

It will give you what you want. But remember to be careful with web addresses.Despite that fact, links are always misleading so think carefully before clicking your way on off into Darknetdom.The Tor Library, mentioned above, also has a directory -- or links to it, anyway -- that can look into.onion sites to return results which might be some good or other use for you.

So, if you are new to The Darknet, this is the first thing I would suggest: use The Tor Library for browsing since the links there have been checked to not have mismatches that could stir up trouble, and so will keep you far off both ill sites and dirty sites [6].

7. TOR ACEESS ADDRESSING

The principle of Tor or requirement is like this. Joe picks an onion at home for sending it out to his friend, it is not very big at all and he posts it to a friend living abroad who will remove the skin of their own onion, lemon not all at once but bit by little bit anyway These steps will be repeated with each friend, in this case there being only three friends. After peeling off

some skin the second friend knows what address does David (the first friend) live at but not much else-the same with skirts! No matter which of these are the first friend to the overall onion, all three people on this mail circuit must open their package to find out where to send (or where a package cannot be sent).
first friend only knows the address of the sender, second friend only knows address of first friend, the last friend only knows address of second friend the The end result is that everyone else who uses same sending algorithm would also gain anonymity.
On the other hand an onion skin is known as a layer or node, so that in Tor there are three layers: the originator at one end, then secondly that of an intervening station and finally itself A new generation onion is formed with the message encrypted according to RSA algorithm and encapsulated in two layers, each containing the address of a node web site so that it will pass through from originator to first address (interim) to read second address (final destination) and then be sent as mail Thus three-taking sites each form a circular path is shown below Figure,2,3,4 The TimeLine Project which coordinates all this communication between Tor users began at 5.[6]

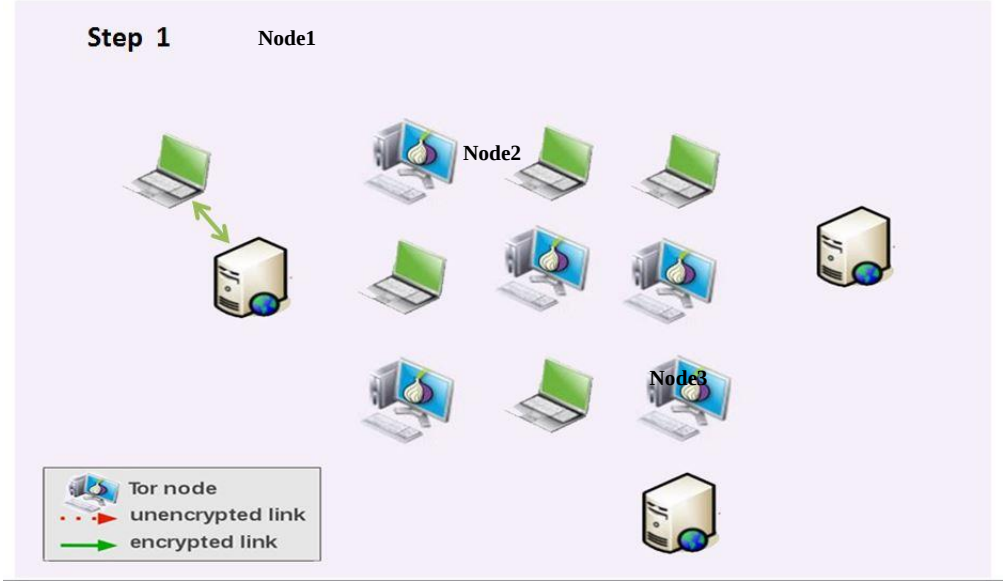

Fig.2. Tor communication steps1

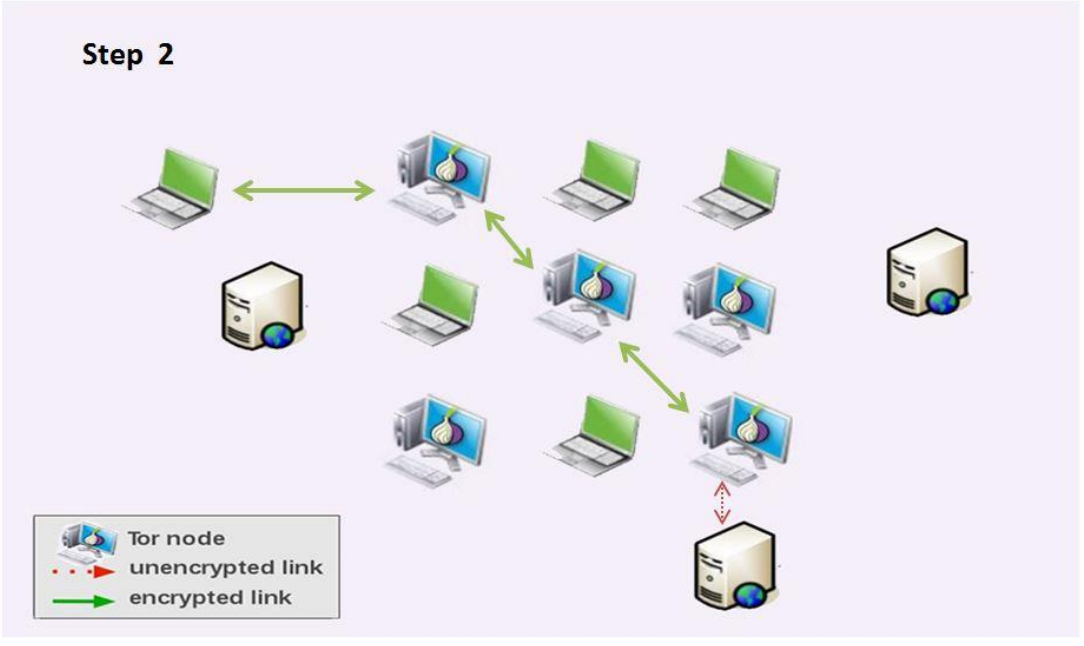

Fig.3. Tor communication steps2

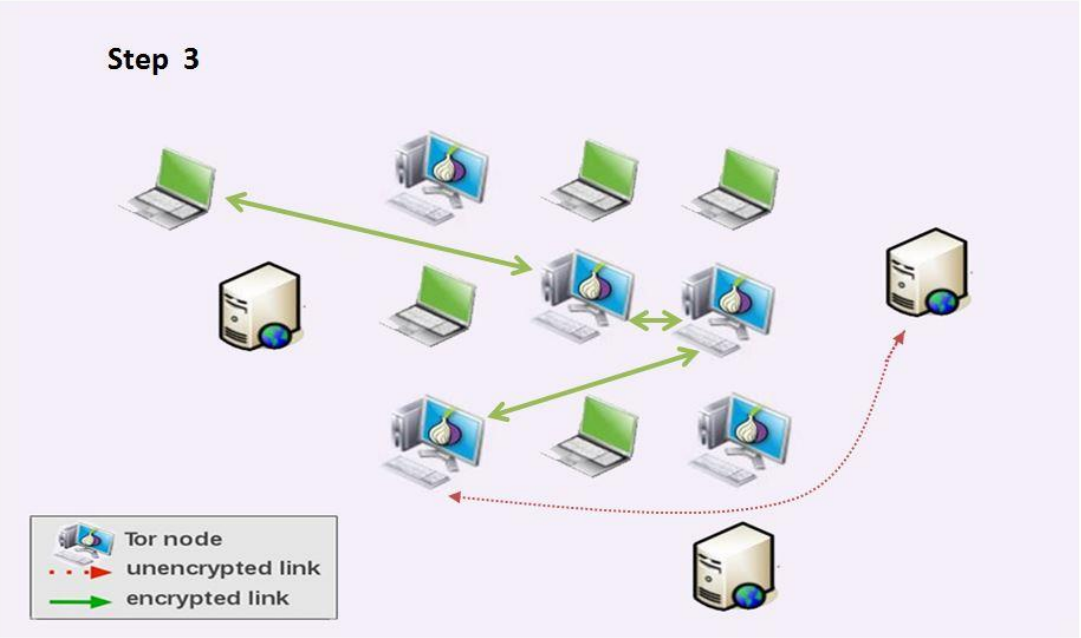

Fig.4. Tor communication steps3

By using the TLS protocol, TOR traffic is implemented. All information will be included in cells (onion). Control cell and relay cell are shown in Figure 2 and Figure 3 The former has a BlackID while the latter contains both CircularID and expiry date; Each one content CircularID to define its cell's circuitThe command to make this cell a control cell, CMD will bring a change. According to CMD's presence in either control or relay cell (CMD), mass command. Ay command leads a create command (there are many other commands). Made was destroyed/recycled connection (to disconnect a bridge node) further sustainability The capabilities command in relay node is also called relay has, data end outrouted circuit so on and commands therefore apply to life. Stream ID to identify end-to-end checksum for integrity checking in relay cell, and the length of the relay payload (Len) In relay node also the command is dividedrelay data, relay begin, relay end, relay teardown, relay connected, relay extend, relay extended, relay truncate, relay truncated, relay sendme, and relay drop
The Header

Circular ID	CMD	Data (payload)

Fig. 5. Control node Structure

The Header

Circular ID	relay	Stream ID	Len	CMD	Data (payload)

Fig. 6. Relay Cell Structure

The Tor network is built of multiple hidden volunteer servers. These servers are the nodes in the network, First Tor check some nodes (layers) information from the directory servers you cite and then pick a few arbitrary relays to start the connection, like Figure 4 shows sequentially the steps of making a connection are as follows:
The first relay (node1) sends an instruction of "create" to the control cell of its TOR client.
After receiving that control cell, node1 returns one with a "created" instruction in it and its public key (K1) for secure communication between themselves too.
The TOR client will send relay cell bearing a "relay extend" direction and address of next relay (node2) to node1.
Node1 returns a control cell bearing a "create" command to the second relay (node2).
In return for this, Node2 will send a "created" directive back to the first relay (node1), together with its public key (K2).
This means that the connection has been made in both directions for TOR client and second relay.

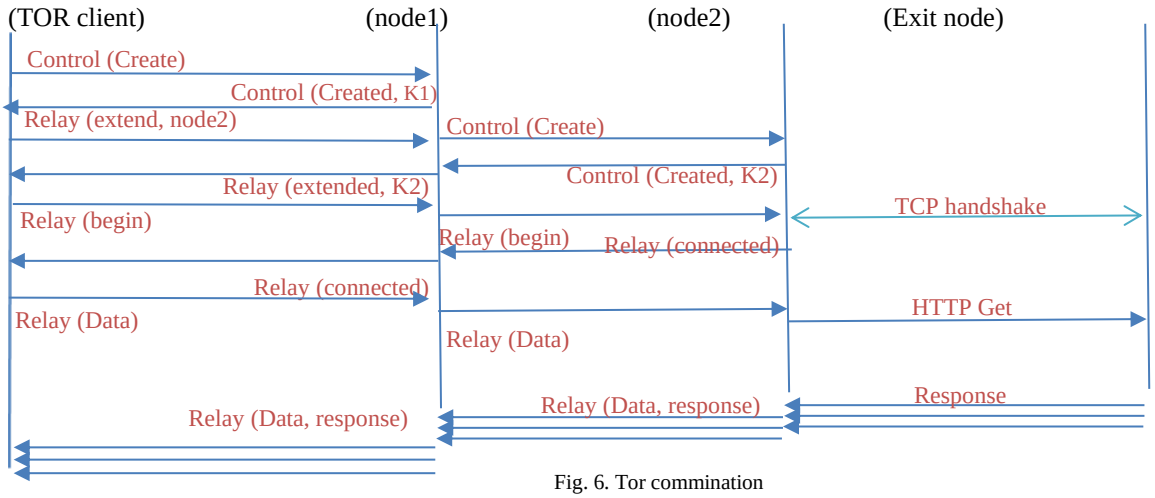

Fig. 6. Tor commination

Node1 accepts the control cell from node 2, and then sends relay cell with K2 back to Tor client.

The process is repeated, one hop at a time, until the last relay in the circuit (the exit node) which will make a three-way handshake to the Tor client 's intermediate address;) After this handshake is performed, the exit node sends a relay cell with connected command to show for certain that the connection has been established. [5]

It is worth noting that the connection Tor builds to its destination is long and convoluted. In each step of this process, several programmatic operations are performed, so the time it takes to reach the service increases[6]. Among these operations are:

1. encryption and decryption operations, each node in the path between sender client encodes packet with its own unique key and then passes this from nack to next node.
2. Transmission line integrity operations, for time-to-time providers will conduct maintenance tasks. We can see from the repeately changing addresses of services that maintenance operations are essential when faced with surveillance or lyargonzon primo an nekkid anwa ininsitions white pde to ipsswyutter little flitters.
3. The number of Tor onion addresses increases continously .

8. EXPECTED STEPS FOR SAFE ACCESS TO THE DARKNET

As such, the Darknet is potentially very dangerous and people need to be careful. Here are some precautions you can take during your visits in the dark places. Please remember that while you are searching the Darknet, police are doing their browsing also and trying to find out who is hosting websites and where are people going on them. You know, when Internet serves cyber surfer, every website will trace your IP address, which often tells others who you are and where your home happens to be! The dark internet does not mean that wholesale risks should be run. The right procedure for most people to get onto the dark net is as follows [7]: -

1- Boot any system (Linux, Windows, Unix, Mac) on USB.
2- Change your location every 15 min.
3- RUN VPN software and also connect your computer to any Onion over VPN server. After you have connected, move on. VPN will cloak your IP address with an IP address in another country [8].
4- Run your Tor Browser. Tor Browser uses Tor routing to hide away all the packets sent over the network when you open it as long as it read the success message. Once you are in, just type in any onion URL. URLs can be found in any category from the site homepage [9].
5- Turn off the scripts running in the TOR settings (click on the button just before the address bar). This is because most of the sites on Darknet are criminal in nature. If you happen to land on one, they could be tracking you. In addition, scripts that are written in JavaScript can be harmful if they end up storing something onto your computer[10]
6- Don't download anything (like DOC and PDF files) to your computer. No BitTorrents, and no downloads; they may interfere with your real IP address by storing things within your regional machine. These data contain resources located elsewhere on the Internet and will be downloaded outside of Tor by the application that opens them. This is tantamount to revealing your Tor IP address, which could spell trouble [11] [12]
7- Done Now

9. INVESTIGATIONS AND ANLAYSIS

This complex and invisible space called the dark web can be probed through certain advanced tools, techniques. Or you could say, through a whole variety of research methods Just as the deep ocean lies invisible below the surface of water, the dark web is an uncharted expanse of the Internet That Cannot be explored unless `Tor" and `I2P" connect togetherfor Users. The dark web's diverse existences make it a good subject for investigating and analyzing. Hell9 ("Drilling") is invisible because of its advanced techniques and tools that produce data from within this complex space. One of these tools is Hell9, which may allow users to bypass the limitations they face when accessing dark networks. In this context of investigation and analysis, advanced techniques are used to explore data within the dark web, no matter whether it is by analyzing illegal activities such as cyber attacks or illegal trading, monitoring security patterns within these networks the main point is to unearth hidden data and study how Data extraction act. "Navigational-Drilling" refers to targeted research that employs precise methods or analysis to enter the complex and invisible darknets, which are probably encrypted or protected. The Hell9 tool may be designed for this type of investigation and provide a sophisticated means to access information within darknets in a safe and efficient manner. The following terms:Cybersecurity: To detect illegal actions happening on the dark web. data retrieval and practices within networks not easily Redesigned from 00 to 10 using onlineAvailable.Cached data analysis: A study of hidden data on the darknet for insights into privacy, surveillance, etc. Data extraction Living in modern times, Ill9 is an advanced technology for understanding darknets and studying hidden activities happening in complex environments. Moreover, it employs the latest methods to ensure that data can be accessed and analyzed confidently and efficiently.

10. CONCLUSION

The surface internet is heavily monitored and controlled by different kinds of entities that might even want to limit one's online privacy in general. On the other hand, DarkNet is both anonymous and hidden: which does not work with important search engines on purpose foundless information is spread from here including illegal activities. Thus, even while he knows about the transactions, law enforcement itself may be unable to identify or arrest the participants. In this way, both the current crop of Internet surveillance and computer hacking technologies are jeopardizing national security and the structural integrity of the web by making it possible for government agencies to intercept and analyse e-mail between organizations, businesses, individuals throughout the world with disturbing ease. DarkNet is clearly useful to individuals, corporations and governments for legitimate private communication and security reasons. But by its very nature it provides an environment which attracts crime offenders or even terrorists to operate in. More importantly there is no acceptable way at present to allow the DarkNet become a force for good while preventing its misuse by criminals. Tor uses a multi-hop route to in-crease its anonymity, In this way one more hop is equal to higher anonymity. But on the other hand it also means performance and also lead times, there is a balance between the level of Anonymity and time.

Funding:

This research was not funded by any institution, foundation, or commercial entity. All expenses related to the study were managed by the authors.

Conflicts of Interest:

The authors declare that there are no conflicts of interest to disclose.

Acknowledgment:

The authors wish to acknowledge their institutions for their instrumental support and encouragement throughout the duration of this project.

References

[1] H. Saleh, “Beneath the Surface: Exploring the Dark Web and its Societal Impacts,” 2023.

[2] C. Guan, D. Ding, J. Guo, and Y. Teng, “An Ecosystem Approach to Web3.0: A Systematic Review and Research Agenda,” *Journal of Electronic Business & Digital Economics*, vol. 2, no. 1, Jul. 2023.

[3] Z. M. Omar and J. Ibrahim, “An overview of Darknet, rise and challenges and its assumptions,” *International Journal of Computer Science and Information Technology*, vol. 8, no. 3, pp. 110–116, 2020.

[4] F. Mohammed and M. Hamza, “A Dark Web Story: In-Depth Research and Study Conducted on the Dark Web based on Forensic Computing and Security in Malaysia,” in *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering*, 2017.

[5] B. Shavers and J. Bair, *Hiding Behind the Keyboard: Uncovering Covert Communication Methods with Forensic Analysis*, 1st ed., Elsevier, 2016.

[6] F. Astika and I. I. Uzzin, “Detecting and Blocking Onion Router Traffic Using Deep Packet Inspection,” in *International Electronics Symposium (IES)*, IEEE, 2016.

[7] J. Park and H. Mun, “Improving Tor Hidden Service Crawler Performance,” in *IEEE Conference on Dependable and Secure Computing (DSC)*, 2018.

[8] G. H. Owenson and N. J. Savage, “The tor dark net,” 2015.

[9] G. Weimann, "Going dark: Terrorism on the dark web," *Studies in Conflict & Terrorism*, vol. 39, no. 3, pp. 195–206, 2016.

[10] M. Hatta, "Deep web, dark web, dark net: A taxonomy of 'hidden' Internet," *Annals of Business Administrative Science*, vol. 19, no. 6, pp. 277–292, 2020.

[11] S. Chatterjee and A. Nath, "Auto-explore the web–web crawler," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 5, no. 4, 2017.

[12] E. Dilipraj, "Terror in the Deep and Dark Web," *Air Power Journal*, vol. 9, no. 3, pp. 121–140, 2014.