iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.54034

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Dark Web and Law Enforcement the Never-Ending Battle

Shobha Bagle
Student Development of Information Technology ZSCT's Thakur Shyamnarayan Degree College Kandivali (E), Mumbai, India

Abstract: ***What is the Web? Is it Google? Or, Facebook? Emails, messenger, Yahoo? Well, these and all other forms that we are aware of barely constitute 4% of the whole world wide web! So, are we just looking at the tip of the iceberg? What constitutes the remaining 96% of the web? Let's understand what 96% of our web consists of, there are 3 layers of the web 1) Surface Web 2) Deep, Web and 3) Dark Web .4% of the web that we use on a daily basis consists of the Surface Web which includes our Google, Facebook, WhatsApp, etc. The remaining 96% consist of Deep Web and Dark Web. Deep Web. As the name Dark Web the word Dark actually refers to secrets stored in dark, crime, illegal activities, and creepy things. Dark Web ca n be accessed through TOR (Onion Router). According to the statistics, the US citizen accounted for 34.81% of the Dark Web daily user count. It translates to 831,911 users. Russia took second place with 11.46%, and Germany ranked third with 7.16% of total active users. These are the statistics calculated for the year 2020.***

Keywords: TOR, Dark Web, Deep Web, Surface Web, Law Enforcement such as CIA and FBI, Onion domain, forums, IP, Bitcoin



Fig1. Layers of Web

I. INTRODUCTION TO DARK WEB

The dark web is hidden from the Surface Web. It cannot be reached with regular search engines or browsers , it requires the use of specialized software known as TOR also called the Onion Router.

The dark web provides anonymity by keeping transactions, communication and illegal activities hidden and private. This happens due to encryption and routing content through multiple web servers to keep its true identity hidden. Accessing the dark web requires Tor software that keeps things anonymous(hidden), and the term "dark web" is known to keep things hidden and secretive.

©IJRASET: All Rights are Reserved



Fig2. Image of Tor Browser

The dark web may be known to be the house for criminals, but that is not necessarily true. It can be abused or appreciated for an anonymous space on the internet. It is true that a large amount of illegal activity takes place on the dark web, but there are also a number of legitimate reasons to use it. In fact, the Dark Web was developed by the US Military. The idea is that the US military wanted to send information without being detected by the Chinese government, so they created Tor and Bitcoin. The websites on the Dark Web used. onion domain.

A. Thesis

While FBI has seized some of the website on Dark Web which displays ponographic content in 2015 also FBI has successfully arrested the people who buy and sell Drug in 2018 , Dark Web is a house for malicious users and criminals because Many illegal activities such as buying and selling drugs, human organs, fake credit cards , weapons etc takes place also sits like Red Room , Silk Routes can be there , According to FBI there are many pornographic vedios images on Dark Web also Drugs like heroine etc are selled, and Terrorism also takes place on Dark Web terrorist groups such as ISIS uses Dark Web for there planning and plotting .

II. USE OF DARK WEB

Smart people who buy recreational drugs online will not want to type it on a regular browser. He/she Would need to go online anonymously using a network that would never track His /Her IP address or physical location. Drug sellers, however, do not choose to set up an internet shop where Law enforcement can quickly catch them, for example, what is their domain or the IP address

The address of the site resides in the real world. There are also other reasons, besides from buying drugs, That people choose to stay anonymous or to set up sites that could not be tracked back to a particular Location or individual. People who wish to protect their data from government monitoring may need dark nets. Whistleblowers. They may want to share huge volumes of insider knowledge with Journalists, but they don't want the Government to track them. Dissidents in oppressive regimes require anonymity in order to keep the world aware of what is happening in their Region, City, Nation and World.

But on the other side of the coin, people who want to plot an assassination versus a high-profile target will Want a method that is guaranteed to be untraceable? Certain illegal activities, such as the selling of papers ,Such as passports and credit cards,pan cards and important government papers would also include a network that ensures anonymity. The same may

Be done about people who have leaked sensitive information from other individuals, such as emails and contact numbers.

A. Illegal Activities on Dark Web

Any type of crime which covers transactions, buying and selling of drugs, money, or even human beings and their organs, can be committed on the Dark Web. The darkest and the deepest corners of the internet are a platform for myriad offenses. Here are some examples of Dark Web crimes these all come under illegal activities

1) *Murder for Hire:* The site Besa Mafia is a marketplace for contract killings.
2) *Blackmail/Extortion:* This involves threats of releasing sensitive information or compromising photos of the victim unless and until the victim pays a stated amount in bitcoin.
3) *Illegal Drug Sales:* Alpha Bay was the largest Dark Web market for buying and selling of fentanyl and heroin. It was seized by the Department of Justice in 2017. Hundreds and thousands of people used it to buy drugs, fraudulent identification, malware, firearms, and toxic chemicals.
4) *Illegal Arms Sales:* Tens and thousands of dollar worth of guns are illegally sold each month on the Dark Web, according to sources.
5) *Sex Trafficking:* In the year 2015, the New York County's The D.A.'s Office used an experimental internet searching tool to catch and prosecute the leader and members of a sex trafficking ring.

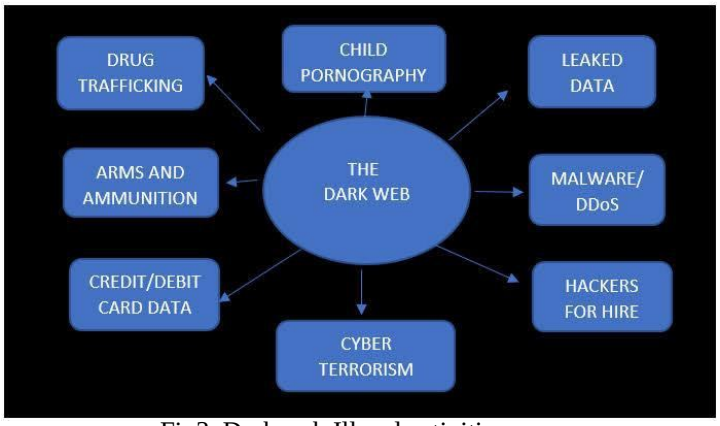


Fig3. Dark web Illegal activities

6) *Terrorism:* ISIS and other terrorist groups use the Dark Web for planning attack.
7) *Child Pornography:* 144,000 British users were using the Dark Web to access child pornography in 2018.

B. Legal and Useful Website on Dark Web

1) Hidden Wiki

The Hidden Wiki is the best place to begin your search on the dark web sites links. It's a community-edited wiki full of onion site indexes that is one of the oldest link directories on the dark web. Here, you'll find all the .onion links to sources and services on the dark web. Spend some time reading over articles, guides, or conspiracy theories, facts and figures. You'll encounter everything from drug marketplaces to hiring a hitman to buying and selling illegal weapons etc.

Warning! Be cautious while clicking on the links. Some of those links will lead to dead ends or worse, lead you into scams or other questionable activities.

There are several spin-off (fake)sites with similar names that you should take care to avoid danger, too.

2) DuckDuckGo

As previously mentioned, Google and Yahoo aren't well suited for searching and entering the territory of dark web. Instead, use DuckDuckGo, one of the better search engines you'll find on the dark web, to find what you're looking for. This secu re, anonymous search engine doesn't record logs of your search activity. But even though DuckDuckGo doesn't record (or share) your search history or obtain access to your email as Google does, DuckDuckGo consistently provides quick, reliable, and private results.

Info: DuckDuckGo also indexes (gives) surface web articles that can be accessed on Google or any normal browser, but you'll need to be on Tor or another darknet to access .onion search results on DuckDuckGo.

3) Sci-Hub

This website is of scientific knowledge and contains millions of documents based on scientific research. Here, you can find 99% of the academic articles and reports produced around the world as the site attempts to liberate information and share it openly with everyone. It is a legal and one of the best Scientific websites.

4) Wasabi Wallet

Cryptocurrency is, unsurprisingly, the currency of the dark web, and it has been the dark web currency for years. Thanks to cryptocurrency's lack of interference in governments or banks, it's a perfect match made in heaven. Wasabi Wallet is a privacy-focused bitcoin wallet, utilizing conjoins to allow users to obfuscate (track) where coins came from in a transaction. This site was created to provide security and privacy.

Info: Here, you can privately track, send, and receive bitcoin. It offers a virtual wallet, perfect for buying things on the darknet.

5) Secure Drop

Secure Drop offers safe and secure communication between journalists and news organizations and their sources (mainly whistleblowers taking appropriate precautions), perfect for leaking and sharing sensitive information which cannot but be shared through the surface web. When you access the site, you'll be given a randomly assigned (placed) code name to send information to a particular author or editor or journalist who then uploads the information using a system of designated flash drives and computers for further encryption and security. Info: Using that generated code name, you can also securely, and anonymously reply to messages from reporters on the Secure Drop platform. Several major news outlets and new organisations use SecureDrop.

Example: Reuters and The Financial Times

6) Hidden Answers

This is the dark web's version of Reddit or Quora. You can ask whatever you want without getting censored or traced by offici als. It may look abandoned (dead) at first, but as far as I have observed the members of the community will answer your questions. However, that part of the internet is unfiltered, so you might come across unpleasant conversations eg :- Cannabis recipe, how to poison a dog ? etc. If you are new to the dark web, here is a great place to learn more about it, but if you are uncomfortable with some disturbing questions then it's not a place for you to visit. Visiting the links from specific questions may be a bit safe as it's not Illegal.

C. Disturbing Things on Dark Web

1) Illegal Drugs: (Selling of drugs)
2) Weapon Trade:(Selling weapons)
3) Human Products: (Products made up of Human flesh, skin, and bones e.g: belts, jackets, shoes, etc.)
4) Animal Abuse:(Torturing animals)
5) Hitman for Hire: (Hiring someone to kill a person)
6) Human Trafficking: (Selling Human Organs)
7) Child Pornography: (Pornographic videos of children [minor])
8) Cannibal Cafe: (Discussion on eating human flesh and recipes on human flesh)
9) Red Rooms Live Streaming: (It is basically human torcher live streaming)
10) Lab Experiments: (There are experimental lab videos where various types of experiments like tolerance, starvation, transfusion, or shock therapy are done on humans or animals. Then, the failed experiment bodies are disposed of in the dumpster like how it's done in the meat shops.)
11) Human Auction: (Viewers bid on auctioned Human)

III. LAW ENFORCEMENT ON DARK WEB

A. The C.I.A

The US Navy's main reason for creating Tor was to help informants relay (sending and receiving) information safely over the internet. In the same spirit and intention, the Central Intelligence Agency (CIA) established a .onion site to help people access its resources worldwide anonymously and securely. Direct

B. Successful Operations by FBI

1) Operation Pacifier

The investigation saw the FBI hack the site Playpen (The largest onion website known for CHILD PORNOGRAPHY AND CHILD ABUSE), and host (display) its illegal content such as child pornographic vedios and images on its own servers for nearly two weeks in 2015.

The agency did so in order to collect the IP addresses of visitors that visit this website and inject malware into their systems to gather more information about those people. The FBI used network investigative technique (NIT) to obtain information about more than 1,000 US-based Playpen users and at least 1,300 unique IP addresses that were tracked in the US led to only 137 of Playpen's 215,000 users being charged.

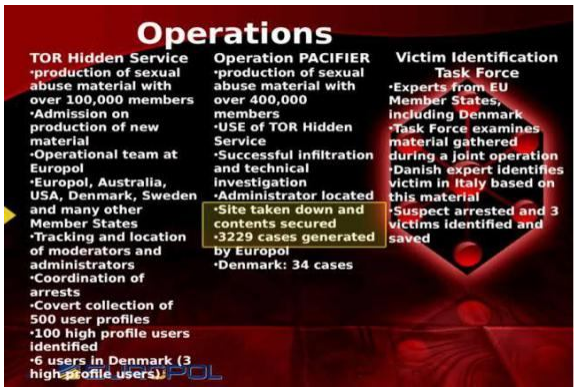


Fig4. Operation Pacifier

2) Operation Disarray

A joint law enforcement operation which was held on March 28, 2018, in Cleveland, Ohio, targeting drug traffickers and end users (basically people who buy drugs) who buy illegal narcotics like fentanyl on the dark web. An evidence bag showing fentanyl was seized during 'Operation Disarray ' by the FBI.



Fig5. Shows fentanyl seized during Operation



Fig6. FBI agent conduct a search during operation

3) Operation Hyperion

The FBI joined with U.S. law enforcement agencies in Operation Hyperion, a successful international action aimed at disrupting and arresting the developer and the users of illicit Dark Net marketplaces.During this operation, FBI agents made contact with more than 150 individuals around the country who were suspected of purchasing illicit items from various Dark Net marketplaces. Some of these confessed to ordering a range of illegal drugs and controlled substances online, including heroin, cocaine, morphine, and ketamine.



Fig7. Screenshot of DarkNet

C. Some of the Methods Law Enforcement use to catch Dark Web Criminals

1) Physical observation (old techniques of officials to observe)
2) Intercepting parcels (Officials have contacts with the parcel companies)
3) Big Data and Machine Learning (Used to get IP address and Data)
4) Getting Data from other websites (Searching useful information from other website)
5) Tracing Cryptocurrency (Tracking transaction of Bitcoin)
6) Human Error (Silly mistakes)
7) Undercover Operations (e.g: Undercover Operation to trace Silk Road developer)

D. List of some of the popular and largest Dark Web siTES SEIZED by the Law Enforcement

1) AlphaBay
2) RaidForums
3) Silk Road.
4) IPStress
5) Silk Road 2.0
6) WeLeakInfo
7) NetWalker Ransomware.
8) DeepDotWeb
9) Hydra Market.
10) Playpen

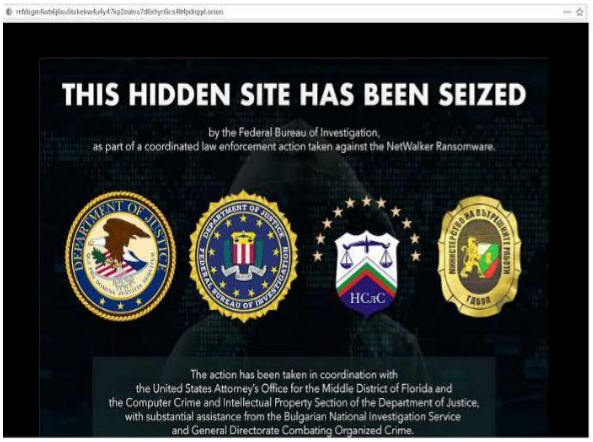


Fig8. Seized site of Netwalker Ransomware



Fig9. Seized site of WeLeakInfo



Fig10. Seized site of xDedic



Fig11. Seized site of DeepDotWeb

E. Personal Experience on Dark Web

1) I myself have tried accessing the Dark Web by using Tor and VPN.

2) I have visited the Hidden Answers website on Dark Web, Hidden Wiki, and Ahmia. fi and Torch.

3) I have seen flashing links for Drug sites, Hitman sites, Pornographic sites, and Fake Credit card sites but I never tried to visit them due to security purposes also these websites links were of no use to me

4) I had covered the camera so that it was safe for me and tried not to click on any unknown or suspicious site link, nor I tried to download any content, games, videos or pictures from Dark Web.

5) Eg: This is one such website I visited and some which I visited but was unable to take pictures so download the image from the internet

6) Here are some images of the website found on the Dark

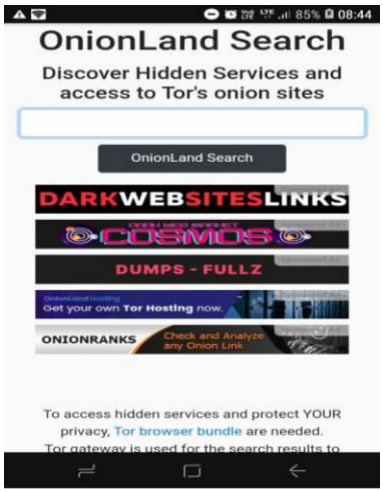


Fig12. Onion websites

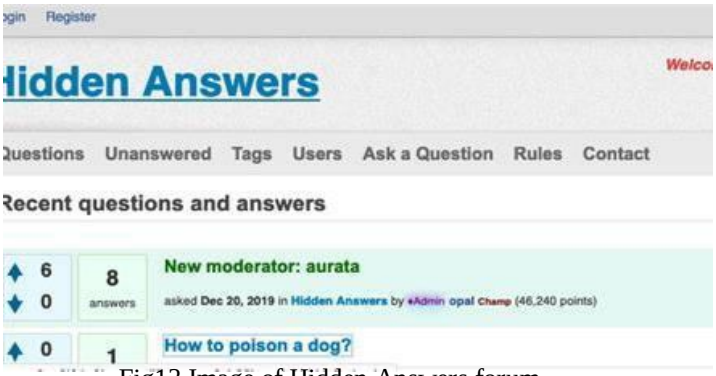


Fig13.Image of Hidden Answers forum

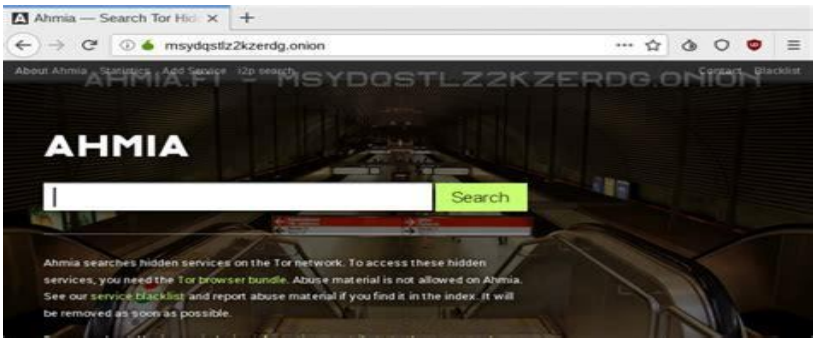


Fig14.Image of Ahmia search engien on dark web

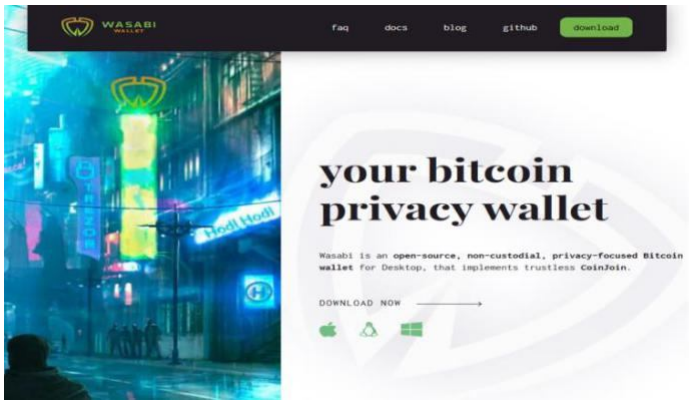


Fig15.Image of Wasabi Wallet

F. Ways to Access Dark Web

The dark web is a mysterious and infamous part of the internet that is much larger than the clear web and deep web. The most convenient and arguably safest way to access the dark web is by using Tor, also known as the onion router. While there are other browsers like Freenet, Whonix, Subgraph OS, and I2P, this article focuses on using Tor.

The easiest way to use Tor is to download the Tor browser, which functions like any other browser. The Tor browser reroutes your web requests through a series of proxy nodes located anywhere in the world, making it impossible to trace your connection back to you.

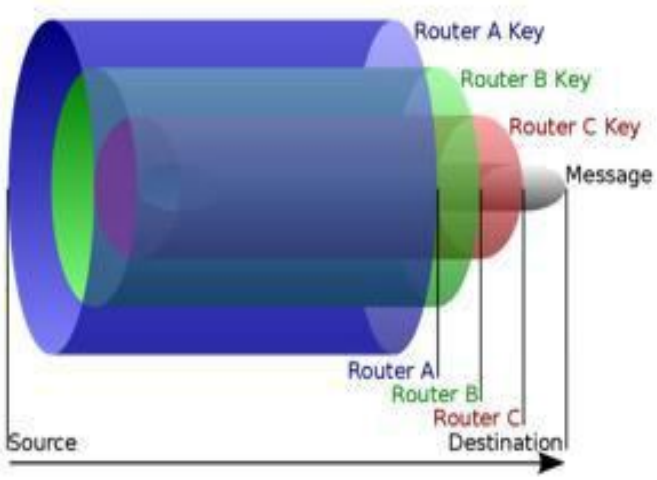


Fig16. Diagram of onion routing

1) Features of the Tor Browser

a) A combination of Firefox browser and the Tor project
b) Open-source software
c) Automatic data decryption at the client side
d) Uses an overlay network to direct internet traffic

2) Advantages of using the Tor Browser

a) Protects user privacy by hiding IP addresses
b) Secure and encrypted websites
c) Anti-spy protection that prevents others from tracking visited websites

3) Disadvantages of using the Tor Browser

a) Low latency is a major problem
b) Cannot download and upload large files
c) Exit node has data on visited websites, leading to security concerns.

G. How to browse Dark Web safely

It's essential to be aware of the dangers present on the dark web, as things can change quickly and hackers are becoming increasingly clever. The dark web is a complicated space, filled with scammers, malware, and phishing websites. To keep yourself safe, it's best to know what you want to achieve on the dark web before downloading any software or beginning to browse.

1) Protect Your Anonymity

Anonymity is key on the dark web to maintain your safety. The use of an operating system like Windows 10, which collects personal data, may put you at risk if a hacker gains access to your system. Instead, use a live mobile operating system like Tails, Whonix, ZeusGuard, or Qubes to provide better privacy protection. These systems leave no trace of your activity on your computer, are easy to use, and have the Tor browser pre-installed. However, keep in mind that many live operating systems do not support VPN, and it may make you more vulnerable to detection.

2) Use a VPN

Even if you use the Tor browser, your internet traffic can still be tracked. It's recommended to use a reliable VPN in addition to Tor to encrypt your web traffic and keep your IP address hidden from hackers or government surveillance. NordVPN is a good option for a VPN that works well with Tor.

3) Download Tor from the Official Website

If you're using a live mobile operating system like Tails or Whonix, the Tor browser is already pre-installed. Otherwise, download Tor from the official website to ensure you're using a legitimate version.

4) Ensuring Safety on the Dark Web

Before opening the Tor browser, it's crucial to take the following safety measures:

a) Close all non-essential applications such as Netflix and password managers.
b) Stop running any unnecessary services such as OneDrive.
c) Cover your webcam with a piece of paper, as it's easy for someone to access your webcam without you knowing.
d) Install a reliable and updated antivirus program on your device.
e) Install updated anti-malware software to protect against malware.
f) Turn off your device's location services.
g) On Windows 10, go to Settings > Privacy > Location > Disable Location and delete Location History.
h) On MacOS, go to System Preferences > Security & Privacy Panel > Privacy and disable "
i) By following these steps, you can better protect yourself while browsing the dark web.

5) Block Script Loading in Tor Browser

a) Scripts can track your online activities and become a part of your digital footprint. To prevent this, Tor browser has a built-in feature to disable script running. To activate it, go to the top right corner of the browser and click on the "S" symbol. Choose the "Enable restrictions globally" option.
b) This setting is crucial as many websites run scripts without warning. This can be particularly dangerous on the dark web as onion websites lack regulation and have a high risk of malware. By blocking scripts, you lower the chance of infecting your device. However, it is still important to exercise caution while surfing the dark web.
c) To check if script blocking is effective, look for the "S" symbol in the top right corner of the browser. If there's an exclamation point, scripts can still run, but if it's clear, your device is protected.
d) For disabling scripts in your everyday browser, you can use browser extensions such as Scriptsafe for Chrome or Brave and NoScript for Firefox. These extensions let you choose which websites can run JavaScript and which cannot. Keep in mind that disabling scripts may affect normal web functions.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

H. Conspiracy Theories related to Dark Web.

1) The Existence of Mariners Web

As the name goes Mariana Web, you must be wondering from where did the name come from? The name Marianas Web is believed to be the deepest part of the whole internet, and the name is actually inspired by Mariana Trench which is actually the deepest part of the world's ocean.

It is so "believed" because there is no such proof of its existence. Yes, there are many conspiracy theories that say that there is no such thing as Marianas web out there. Let's dig deep into it, and find out the actual truth.

It is actually believed that the Mariana web contains a lot of the secrets of powerful and giant agencies. It is said that you can find the most disturbing websites out there. There are some beliefs that the Marianas web hosts secret data of the secret agencies and also the government.

Since we don't have any proof, there are different theories that talk differently about the Mariana web. I have addressed few of them below:

a) It said that Marianas Web is run by an AI (Artificial Intelligence) that has gained Sentience in this world.
b) It is a rumour (Hear it address to Marianas Web) that was designed to distract people from the Dark Web's market takedowns.
c) Now here goes a saying that the Network on which Mariana Web works comprised Closed Shell Systems.
d) It is supposed that Mariana Web holds a lot of History's Darkest Secrets and Mysteries which are hidden from the citizens.eg: One such mystery is the Cicada 3301 puzzle which was created to find a highly intelligent person.

Now, you must be wondering how you can gain access to Marianas web? Here we go with the answer:

It is believed that Marianas web can be accessed only through highly intelligent supercomputers known as Quantum Computers only. But as we know that Quantum Computers have come into existence.In 2015, we know that Google and NASA had jointly confirmed the existence of functional Quantum Computers. But we know that Quantum Computers need a very extreme environment as its CPU can work well only in a vacuum whose pressure has to be 10 billion times lower than that of our earth's atmosphere. Also, point to be noted that the temperature of that vacuum should be 0.015 degrees. So there is a debate about the Existence of Quantum Computers.According to my understanding there is a possibility of the Existence of Marianas web again we don't have any evidence about it so it goes as a conspiracy theory until the date when we get a proof of its existence.

2) The Existence of Red Rooms

Before finding out the truth that Red rooms exist or it's just a conspiracy theory let us know What is Red Room? Why is it a horrible place to be?

Red rooms are actually said to be some of the most horrific places on the deep web that one can find. In a red room, you can reportedly view activities such as viewing livestream of someone which is being tormented and murdered yes you heard it right, and some have even reportedly claimed that viewers can actually participate in these livestreams by exchanging cryptocurrencies for some specific acts of violence which they want to perform.

According to the IT experts that frequent the deep web, if the red rooms do exist then they would be so heavily guarded safely that only a select few of the people would be able to access them. Numerous red rooms which are fake have been reported, as the law enforcement have been sting operations across the dark web, making it even more difficult to find a 'Real' Red Room. Now, to my understanding and knowledge.

Streaming Live Videos On The Deep Web Is Reportedly as to be a Very Difficult task

a) Firstly, the Dark Web is a small Subset of the deep web
b) It is known that the dark web is largely accessed through the Tor network, famously known as "The Onion Routing" project.
c) The chief argument is that it is claimed that Tor is unable to stream live videos.
d) We know that Tor is not only a way to get access to the deep web but the other networks make accessing red rooms even more difficult.
e) Due to which some people say that if red rooms exist then they would be somewhere safely guarded in a heavily restricted area of the first layer of the internet that is the Surface Web

Reportedly Some have Claim Red Rooms do Exist On The Surface Web But Are Only Accessible Via The Dark Web.

©IJRASET: All Rights are Reserved

Sites similar to Red Rooms that have been found on the Dark Web.

- 'Animal Crush' Sites Similar To Red Rooms have been reported by the FBI as the 'Cruel Onion' that have striking similarities to the well-known R3ed Room. This site has repeatedly been viewed to be doing cruelty to small animals, and viewers can actually allegedly make requests for specific acts of violence via cryptocurrency.
- 'The Human Experiment' Is Allegedly A Red Room Site.
- This website is said to be a legitimate red room, yes you heard it correct where criminals allegedly perform horrible and terrifying medical experiments on animals and as well as on humans in an exchange for cryptocurrency.
    - Many sceptics believe it's just a way to scare people so that they stay away from the deep web.

Note: This is a note that I have found while doing research on this topic. This is for those people who say red rooms are not possible due to the lack of live transmissions of video capabilities in Tor network.There is proof that live transmissions are actually possible over Tor network. Yes,you heard it correctly, Red Rooms are very real,as usually there is not a specific link and you need to be known for the people to gain an access to the “door”. Enter the Red Room at your own risk. But you know what you aren't gonna hear people talking publicly about the Red Rooms, so the majority of the people still believe that the red rooms don’t exist, and are really too “crazy” to exist… without even ever knowing what goes on in the dark web. Movies like Hostel 3 have shown examples of these Red Rooms, haven't they?.But hey wait, these moves can be fake but still deep down we all feel or think that deep into the Dark Web's unreachable corner there might be a Red Red Room that actually exists.

I. Case study of the famous Silk Road Website of the Dark Web.

1) Background

An online drug marketplace known as 'Silk Road' has been operating on the 'Dark Web' since February 2011.The founder of Silk Road was 'Ross Ulbricht 'Silk Road was designed to revolutionise shown as contemporary consumption of drugs. It was a concern for the Law Enforcement to stop the 'Silk Road Website'.

Before his arrest, Ulbricht’s website had more than $1.2 billion in sales for selling illegal drugs and other products, in an exchange of cryptocurrency before his arrest. People died due to buying drugs from that site, reportedly there were around 6 people,including a young man in Australia who jumped out of a window.

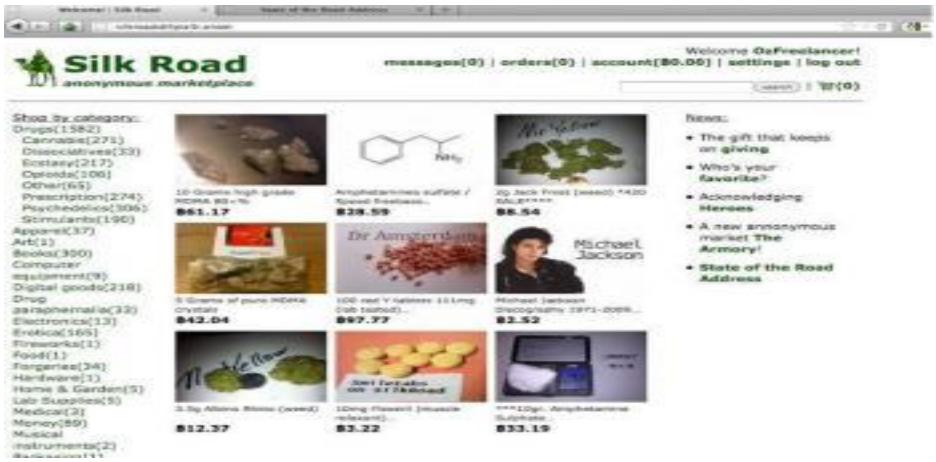


Fig 17. Silk Road website

2) The arrest of Ross Ulbricht

On Oct. 1, 2013, police arrested Ross Ulbricht at the San Francisco public library in a science fiction section.The young man was literally working on the site when they arrested him, said the agents who arrested Ross. The site was then seized by the FBI authorities; they also replaced the site with an image notifying the public of its seizure. By tracing some of Ross's early requests to other people to help him build the site, the FBI tracked Ulbricht. The first connection was made by an IRS investigator. The investigator actually found the connection by linking/ tracing the username 'altoid', which Ulbricht used it in his early days of Silk Road to announce the website on the Dark Web, and a forum post was spotted where Ulbricht, using his nickname 'altoid', asked for the programming to help him and gave an email address that contained his real name.

©IJRASET: All Rights are Reserved

Agents eventually made the entire case from that little detail. At the library in San Francisco, two of the FBI agents staged a lover's fight to distract Ulbricht until a third agent grabbed his laptop, inserted a flash drive into his computer and copied all the computer's files. Based on all the charges on Ross in February 2015 jury sentenced him for a lifetime in prisonment with an additional 40 years with 0% possibility for parole.Till date he is still serving his sentence at a Federal prison which is located in Arizona. The charges included

- Money laundering
- Conspiracy to commit computer hacking
- Conspiracy to traffic narcotics.

J. Recent case of Illegal selling of C0VID-19 Vaccine.

Analysis of 194 dark web marketplaces until July 2021 showed that they started offering COVID-19 related products such as masks and tests early on during the pandemic when these goods were in shortage in the traditional economy. This study expands on previous investigations by including the vaccine availability period and examining the pandemic's wider impact on DWMs. The focus was on vaccines, with 250 listings found for approved vaccines and fabricated proof of vaccination and COVID-19 passports. The study also revealed a decrease in DWM offerings for COVID-19 related products as the demand was met by the regular economy. Most vendors were specialized in one type of listing and willing to ship worldwide. COVID-19 mentions in 10,330 listings were used to represent the pandemic's impact on traditional DWMs products, with recreational drugs being the most affected.



Fig 18. Image of Illegal selling of Pfizer vaccine

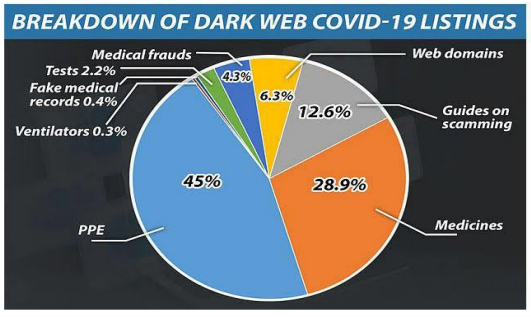


Fig 19. Breakdown of dark web COVID-19 listing

K. People's Experiences on Dark Web

1) One Hitman, Please

This is from a Reddit user whose username is as: IAmASharkFin: "A website which was advertising a hitman, his services costing were increasingly more bitcoins based on the type of your target. I don't remember the specific amounts, but the order went something like this as given, from least to greatest: Civilians, Police, Politicians, Children. Shudder."

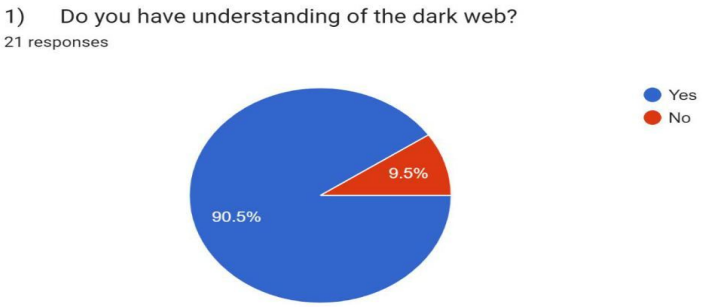
2) Recipes for Human Meat

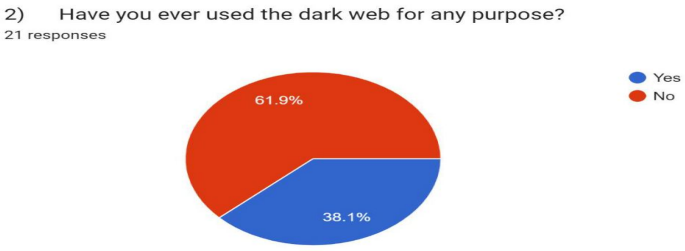
Reddit user bacon leiter reports as following,

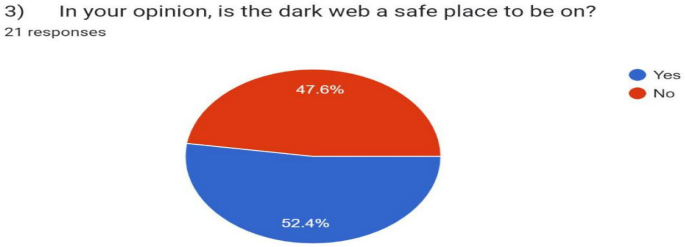
"In CompSci, we often get bored and dig around. One day we ran into the deep web out of curiosity. The most disturbing site we found was a very comprehensive guide for cooking a women.This page actually contained information on what body types to use for specific cuts, also how to prepare these cuts, and how to cook a girl so she lives as long as possible. It horrifies me that people are way worse than the freaks on Criminal Minds That exist." Note: I have just mentioned 2 people's experiences. You can find many on the internet.

Questions

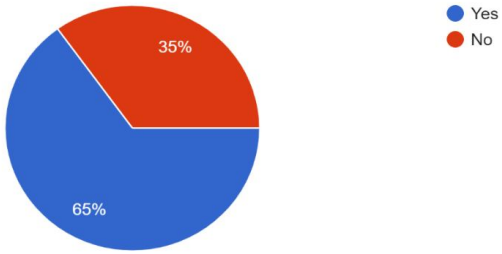
1) Do you have understanding of the dark web?
2) Have you ever used the dark web for any purpose?
3) In your opinion, is the dark web a safe place to be on?
4) Do you believe law enforcement agencies are in tracking and apprehending individuals who use the dark web for illegal activities?
5) Do you think that law enforcement agencies have the necessary resources and technology to effectively monitor the dark web?
6) Do you believe that the dark web should be shut down or regulated?
7) In your opinion, should the privacy of individuals using the dark web be protected, even if they are using it for illegal activities?
8) Have you ever heard of any instances where law enforcement agencies have successfully cracked down on illegal activities on the dark web?
9) Do you think that the use of encryption and privacy tools on the dark web makes it more difficult for law enforcement to track individuals engaging in illegal activities?
10) Do you think any measures must be taken to reduce illegal activities on the dark web while balancing privacy concerns?



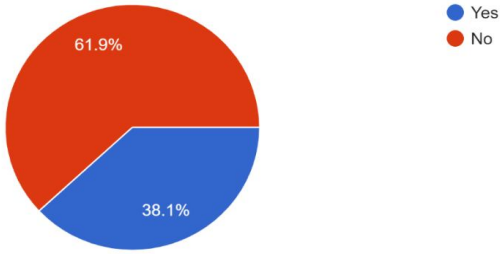




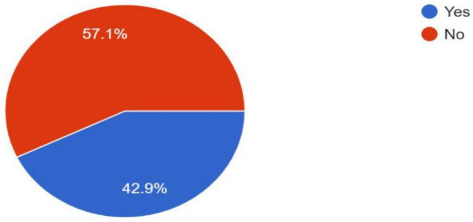
4) Do you believe law enforcement agencies are in tracking and apprehending individuals who use the dark web for illegal activities?
20 responses



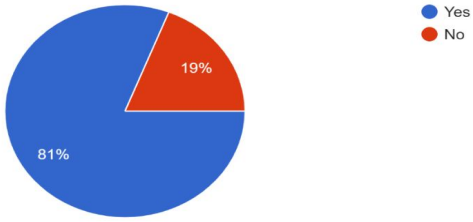
5) Do you think that law enforcement agencies have the necessary resources and technology to effectively monitor the dark web?
21 responses



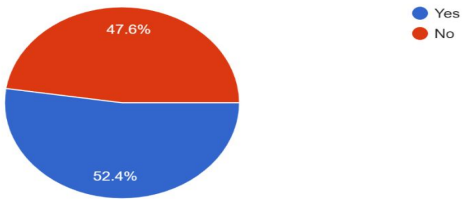
6) Do you believe that the dark web should be shut down or regulated?
21 responses



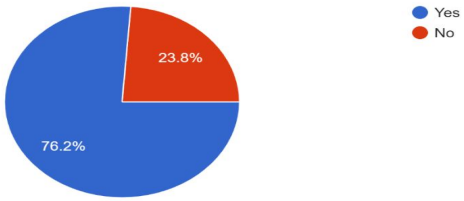
7) In your opinion, should the privacy of individuals using the dark web be protected, even if they are using it for illegal activities?
21 responses



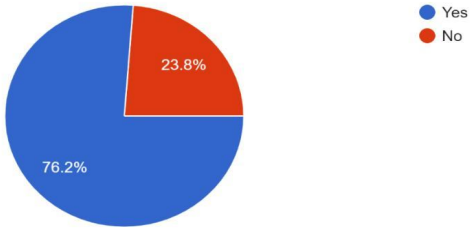
8) Have you ever heard of any instances where law enforcement agencies have successfully cracked down on illegal activities on the dark web?
21 responses



9) Do you think that the use of encryption and privacy tools on the dark web makes it more difficult for law enforcement to track individuals engaging in illegal activities?
21 responses



10) Do you think any measures must be taken to reduce illegal activities on the dark web while balancing privacy concerns?
21 responses



IV. CONCLUSION

The Dark Web networks such as TOR have provided many possibilities for malicious users to exchange legal and illegal “goods” anonymously. The Dark Web is a growing asset, especially in terms of illegal services and activities. The evolving technology with encryption (security) and anonymity (like the Dark Web and its special software) has put law enforcement and policymakers under challenge to effectively struggle with harmful users who are operating in cyberspace. According to my research on Dark Web, I came across many Dark Web sites and I tried to access some of the Legal and Useful websites which I have described in my Personal Experience block.Here is the list of frequently asked questions about Dark Web and Law Enforcement which I have discovered while doing my research.

1) Is the Dark Web legal to use?

Answer: Dark web is legal to use and any one can use Dark web but it shouldn't be used for any sort of illegal activities, if you do so you'll end up in the law enforcement's radar and soon behind the bars.

2) Who gives funds for the Dark Web?

Answer: As far as i have got the information the Us Government and Google also some other different agencies give funding to the Dark Web.

3) How does the Dark Web earn money?
Answer: Top secret government information. Intelligence Data, Formulas and Trade Secrets,Credit Card Information,Security Plans and/or Blueprints . Personal and Business Financial Records,Medical Records,Hire-a-Hacker,Selling your old identity and buying a new one and Increasing the number of your social media followers etc…..

4) Why doesn't the Government ban the Dark Web?
Answer: Since the Government and their secret information and their work is mostly done on Dark Web (as dark web is more highly untraceable and safe as well as anonymous) hence all the top agencies work is done on Dark Web.Due to which the government cannot ban it.

5) Who uses the Dark Web?
Answer: Community, Criminals, Law Enforcement and Security agencies, Journalist and Private citizens.

6) What are the good things that you get on the Dark Web?
Answer: Banned books, Secret articles and journals that the government doesn't want normal people to know about and you get Anonymity.

7) What is Tor Browser?
Answer: Tor, in short is a Browser for The Onion Router,is a free and an open-source software for enabling 'anonymous' communication.
8) How does Tor Browser keep us anonymous on the internet?
Answer: Tor Browser uses the Onion routing technology. Onion routing is a peer-2-peer (P2P) network that actually enables the user to browse the internet anonymously. Onion routing uses different/ multiple layers of encryption of your IP address. Your IP address is masked with different layers of encryption which makes it difficult to track a person's IP address eventually making them anonymous.

9) Which law enforcement recites on the dark web?
Answer: CIA, FBI and ICE etc recites on the dark web.
In this research paper, I have provided the
a) Information about the Dark web ● What is the Dark Web?
- Who developed the Dark Web?
- Which domain do Dark Web sites use?

b) Use of Dark Web
c) Illegal Activities on it
d) Legal and Useful website
- Website Links that are useful
- Warning and Info about those websites

e) Disturbing things found on Dark Web
f) Law enforcement
- C.I.A 's website link on Dark Web
- F.B.I 's successful Operations
- A short Audio message from F.B.I on Dark Web

g) Personal Experience on Dark Web
h) Conclusion
i) Reference Links
- Reference links are provided which I have used while gathering information

j) Biography

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

V. ACKNOWLEDGEMENT

This Research Paper wouldn't have been possible without the exceptional support and guidance of my supervisor Sir Sudhakar Vishwakarma. His knowledge and guidance helped me in achieving success in my Research Paper. I acknowledge him for his contribution in guides and showing the right path for my research work.

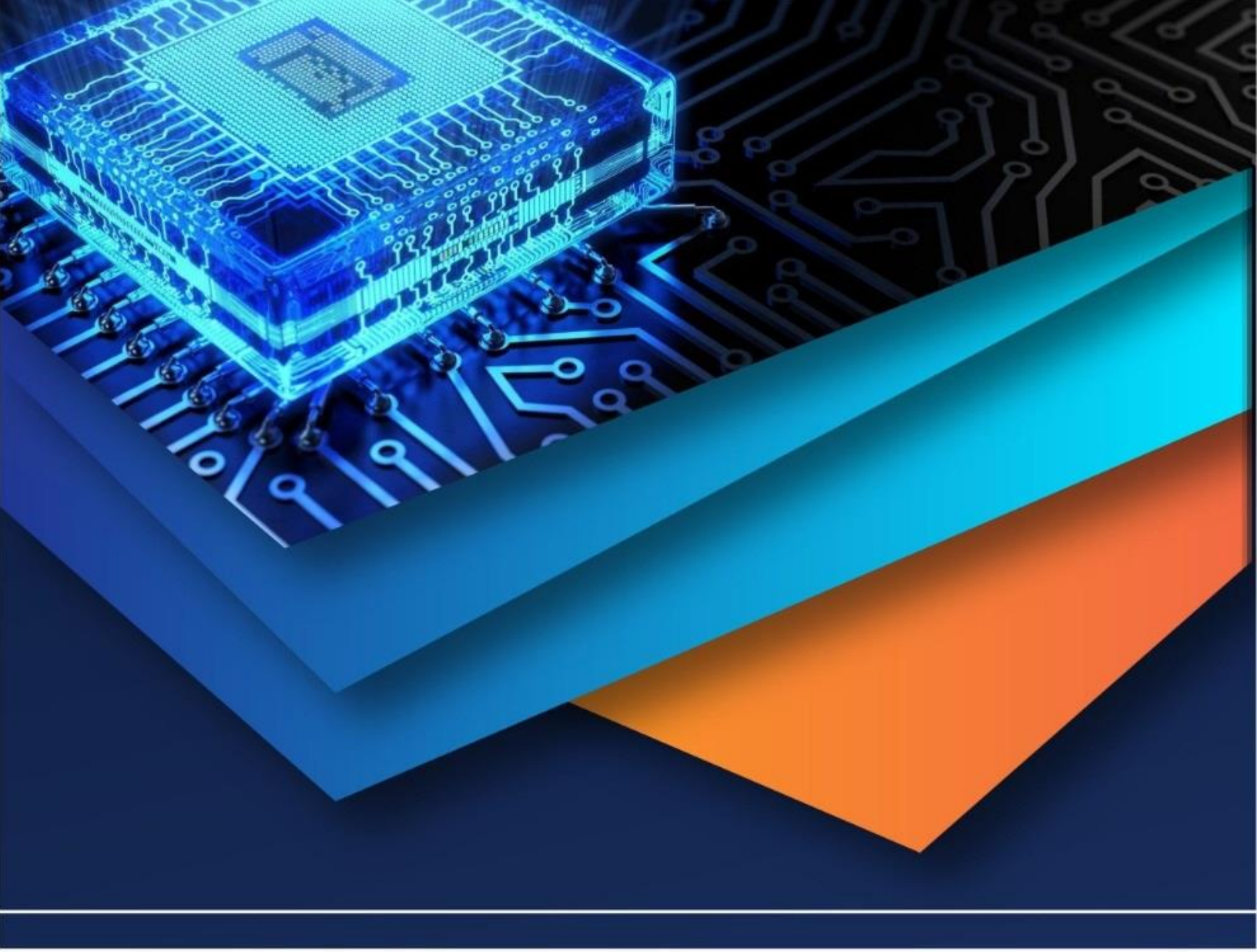
REFERENCES

[1] Jamie, B. (2014). The Dark Net.
[2] Lightfoot, S., & Pospisil, F. (2017). Surveillance and privacy on the deep Web. ResearchGate, Berlin, Germany, Tech. Rep.
[3] Senker, C. (2016). Cybercrime & the Dark Net: Revealing the hidden underworld of the internet. Arcturus Publishing.
[4] Henderson, L. (2022). Tor and the dark art of anonymity (Vol. 1). Lance Henderson.
[5] Diodati, J., & Winterdyk, J. (2021). Dark Web: The Digital World of Fraud and Rouge Activities. In Handbook of Research on Theory and Practice of Financial Crimes (pp. 477-505). IGI Global.
[6] Gehl, R. W. (2018). Weaving the dark web: legitimacy on freenet, Tor, and I2P. MIT Press.
[7] Ozkaya, E., & Islam, R. (2019). Inside the dark web. Crc Press.
[8] Inside the Dark Web – Erdal Ozkaya, 2019
[9] Beckstrom, M., & Lund, B. (2019). Casting light on the Dark Web: A guide for safe exploration. Rowman & Littlefield.
[10] Martin, J., Munksgaard, R., Coomber, R., Demant, J., & Barratt, M. J. (2020). Selling drugs on darkweb cryptomarkets: differentiated pathways, risks and rewards. The British Journal of Criminology, 60(3), 559-578.
[11] Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. Calif. L. Rev., 107, 1753.
[12] Davenport, D. (2002). Anonymity on the Internet: why the price may be too high. Communications of the ACM, 45(4), 33-35.

BIOGRAPHY

Shobha Bagle, a first year student pursuing Bsc.IT from Thakur Shyamnarayan Degree College. I personally have a deep interest in topics related to Dark Web, Deep Web, Ethical Hacking, Machine Learning and AI.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)