An Internship Report
on

DEEP WEB, TOR PROJECT AND INVESTGATIONS

Submitted for partial fulfillment of the requirements for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

BY

Ms.Seelam Mrudula Naidu(2451-20-733-032))
Ms.P Uma Maheshwari(2451-20-733-303)
Mr.Mohammed Rafae Ahmed(2451-20-733-162)

Under the guidance of

Mrs. Bantu Saritha
(Associate Professor CSE dept)

Department of Computer Science and Engineering
Maturi Venkata Subba Rao Engineering College
(An Autonomous Institution)
(Affiliated to Osmania University & Recognized by AICTE)
Nadergul(V), Balapur(M), RR Dist. Hyderabad – 501 510

2022-23.

Maturi Venkata Subba Rao Engineering College
(An Autonomous Institution)

(Affiliated to Osmania University, Hyderabad)
Nadergul(V), Hyderabad-501510

Certificate

This is to certify that the project work entitled "**DEEP WEB, TOR PROJECT AND INVESTIGATIONS"** is a bonafide work carried out by **Ms. Seelam Mrudula Naidu (2451-20-733-032), Ms.P Uma Maheshwari(2451-20-733-303),Mr. Mohammed Rafae Ahmed (2451-20-733-162)** in partial fulfillment of the requirements for the award of degree of **BACHELOR OF ENGINEERING IN COMPUTER SCIENCE AND ENGINEERING** from Maturi Venkata Subba Rao Engineering College, affiliated to OSMANIA UNIVERSITY, Hyderabad, under our guidance and supervision.

The results embodied in this report have not been submitted to any other university or institute for the award of any degree or diploma.

Internal Guide
Mrs. Bantu Saritha
Associate Professor

Project Co-Ordinators

DECLARATION

This is to certify that the work reported in the present mini-project entitled "**Deep web, Tor Project and Investigations"** is a record of bonafide work done by us in the Department of Computer Science and Engineering, Maturi Venkata Subba Rao Engineering College, Osmania University. The reports are based on the mini-project work done entirely by us and not copied from any other source.

The results embodied in this mini-project report have not been submitted to any other University or Institute for the award of any degree or diploma to the best of our/ my knowledge and belief.

P Uma Maheshwari	Seelam Mrudula Naidu	Mohammed Rafae
(2451-20-733-303)	(2451-20-733-032)	(2451-20-733-162)

ACKNOWLEDGEMENTS

We are also thankful to our principal **Dr. G. Kanakadurga** and **Mr. J Prasanna Kumar**, Professor and Head, Department of Computer Science and Engineering, Maturi Venkata Subba Rao Engineering College, Hyderabad for providing excellent infrastructure for completing this mini-project successfully as a part of our B.E. Degree (CSE). We would like to thank our mini-project coordinator **Mrs. N Sabitha** for their constant monitoring, guidance, and support.

We convey our heartfelt thanks to the lab staff for allowing me to use the required equipment whenever needed.

Finally, we would like to take this opportunity to thank my family for their support through the work. We sincerely acknowledge and thank all those who gave directly or indirectly their support in the completion of this work.

ABSTRACT

The project explores the enigmatic realm of the deep web, focusing on the Tor Project and its browser as a gateway to obscured services and resources. Through practical activities, it offers a comprehensive understanding of this secretive landscape while addressing ethical considerations and legal boundaries inherent in deep web investigations. This project emphasizes the need for ethical conduct, it also examines privacy concerns and legal implications. Promoting responsible practices in the deep web environment. This project provides invaluable insights into the complexities of the deep web, empowering individuals to navigate uncharted territories while upholding the principles of ethical investigations.

TABLE OF CONTENTS

CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Problem Statement:

Addressing the hidden complexities of the deep web, this project tackles the challenges investigators face when venturing into its enigmatic realm for ethical investigations. With limited awareness, unfamiliarity with effective tools, and ambiguous legal boundaries, navigating this clandestine digital landscape becomes a daunting task. Moreover, the absence of structured guidelines and simulated scenarios compounds the problem, leaving investigators ill-equipped to develop comprehensive and ethical investigation plans. To fill this crucial gap, a project is needed that offers hands-on experience with the Tor Project and its browser, delves into the intricate ethical considerations and legal boundaries specific to deep web investigations, identifies powerful tools and techniques for seamless exploration, and simulates real-world scenarios to foster the development of robust and principled investigation plans. By addressing these challenges head-on, this project seeks to empower investigators with the necessary knowledge and skills to conduct responsible, effective, and legally compliant investigations within the deep web while ensuring privacy and upholding ethical standards.

1.2 Scope of Mini-Project:

The project aims to provide participants with a hands-on understanding of the deep web, the Tor Project, and the intricacies involved in ethical investigations. The following aspects are within the scope of the project:

Installation and Familiarization:

- Installing the Tor Browser and getting acquainted with its features and interface.
- Understanding the fundamentals of the Tor Project and its role in accessing the deep web.

Deep Web Exploration:

- Utilizing the Tor Browser to explore hidden services and resources within the deep web.
- Gaining familiarity with navigating the deep web environment and accessing relevant content.
- Adhering to ethical considerations and legal boundaries while exploring the deep web.

Ethical Considerations and Legal Boundaries:

- Examining the ethical implications of conducting investigations in the deep web.
- Identifying the legal boundaries and potential risks associated with deep web investigations.
- Discussing privacy concerns, maintaining anonymity, and avoiding engagement in illegal activities.

Tools and Techniques for Effective Deep Web Investigation:

- Identifying and analyzing tools and techniques for searching and navigating the deep web effectively.
- Exploring specialized search engines and directories tailored for deep web exploration.
- Evaluating the credibility and reliability of deep web sources.

Simulation of Investigation Scenario:

- Creating a simulated investigation scenario within the deep web environment.
- Developing a comprehensive plan for conducting ethical investigations in the deep web.
- Emphasizing the importance of maintaining ethical standards, privacy, and legality throughout the investigation**.**

CHAPTER 2

TOOLS AND TECHNOLOGIES

2.1 LITERATURE SURVEY:

- Chen, X., & Pan, Z. (2018). Deep Web Investigation and Research Based on Tor Network. In 2018 International Conference on Intelligent Computing, Automation and Systems (ICICAS) (pp. 233-236). IEEE.

  -This paper provides an overview of deep web investigation techniques using the Tor network, including accessing hidden services and exploring the darknet. It discusses the challenges, tools, and methodologies involved in conducting investigations within the Tor environment

- Jaishankar, K., & Smith, R. G. (Eds.). (2012). Ethical hacking and countermeasures: Secure network infrastructures. IGI Global.

  -This book delves into the ethical considerations and legal boundaries in conducting investigations, including those in the digital domain. It explores ethical hacking practices, legal frameworks, and the importance of maintaining privacy, confidentiality, and integrity during investigations.

- Denning, D. E., & Baugh, W. (2014). The dark web rises: Utilizing Tor for secure communications. IT Professional, 16(6), 20-27.

  -This article provides an overview of the Tor network, its applications, and the challenges associated with investigating illicit activities on the dark web. It discusses the ethical implications, legal boundaries, and countermeasures to mitigate risks.

2.2 SOFTWARE REQUIREMENTS:

- Tor Browser: The Tor Browser is the primary software required for this project.
- VPN (Optional): While not mandatory, using a virtual private network (VPN) alongside the Tor Browser can provide an additional layer of privacy and security during deep web exploration.

CHAPTER 3

LAB QUESTIONS

What is the deep web, and how does I differ from the surface web?

Surface Web:

This is the internet we all know and love. Some researchers call the Surface Web we use for everyday activities like social networking and reading news the Common Web. Here, conventional web spiders use sophisticated algorithms to collect data from hyperlinked pages and you browse it from search engines like Google or Yahoo. The Surface Web is, ironically, home to some of the Deep Web. Any web page that requires credentials to access is, technically, part of the Deep Web because a search engine cannot access that content

Deep Web:

The Deep Web is not just a playground for criminals, drug users, and terrorists. In a sense, an organization's intranet is a deep web as nobody outside the company has access to the information in it. There is something compelling about the Dark Web, in the same way unsavory true crime stories and tales of disaster are lapped up by readers of mainstream news publications.

Deep Web vs Surface Web:

The main difference is that the Surface Web can be indexed, but the Deep Web cannot. You can still access it though. You yourself spend a lot of time in the Deep Web, but you probably do not know it. Deep web site examples are:

- Websites you can only get in with a username and password, like email and cloud service accounts, banking sites, and even subscription-based online media restricted by paywalls
- Companies' internal networks and various databases
- Education and certain government-related pages
- Dynamic content, coming from a database where the page you see was displayed as a result of a query you put into that page's search box

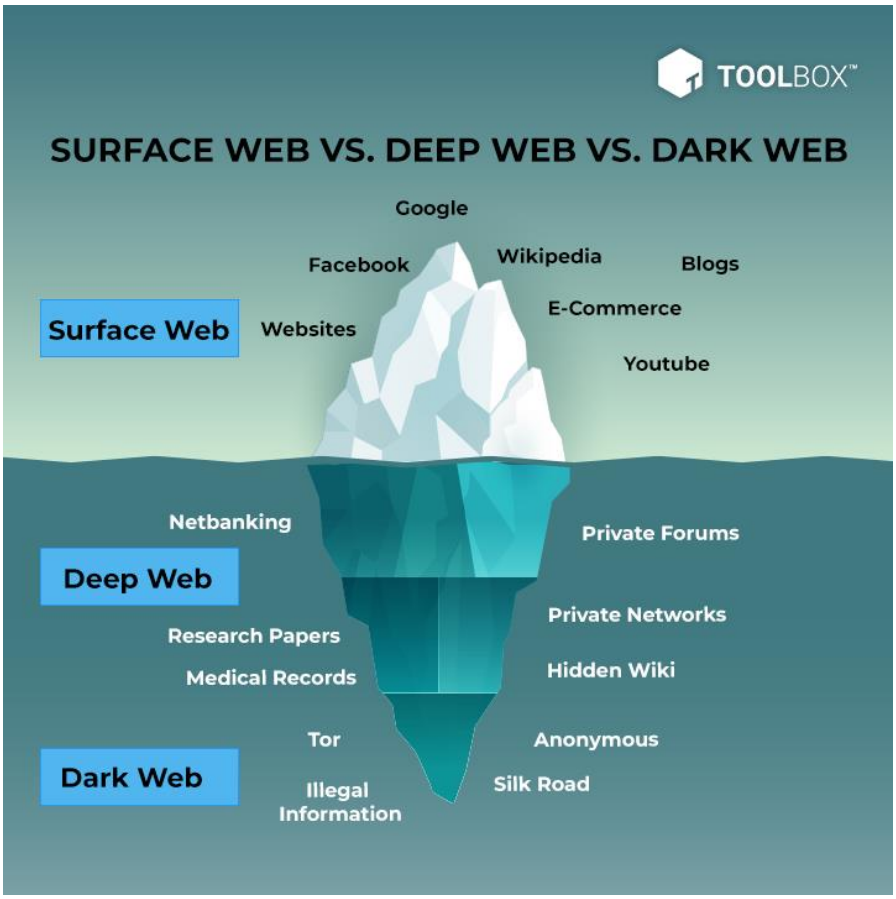


Fig3.1 Surface Web vs Deep Web vs Dark Web

Explain the Tor Project and its role in providing online anonymity

The Tor Project, a remarkable endeavor driven by a global community, spearheads the mission to safeguard online privacy and empower individuals with a shield of anonymity. At its core lies Tor, aptly named after the layers of protection it provides, akin to the intricate layers of an onion. Tor serves as a fortress, obscuring users' identities and obfuscating their online activities through a labyrinthine network of volunteer-operated relays.

The profound significance of the Tor Project lies in its ability to grant users the power to traverse the digital landscape incognito. As individuals navigate the internet using the Tor Browser, their data undergoes a rigorous encryption process, traversing multiple relays in a

carefully orchestrated dance. At each step, the user's identity is shielded, leaving no traceable trail for prying eyes to follow. It is a symphony of security, orchestrated by countless dedicated volunteers who believe in the inherent right to privacy.

But the Tor Project goes beyond mere anonymity. It serves as a bastion for those seeking refuge from oppressive regimes, enabling journalists to expose corruption, activists to organize for change, and citizens to freely access information that may be otherwise suppressed. It stands as a testament to the power of technology in protecting civil liberties and fostering a space where one's digital presence is free from unwarranted scrutiny.

However, it is crucial to recognize that while the Tor Project offers a robust layer of protection, it does not guarantee foolproof security. Users must remain vigilant, exercise caution, and understand the limitations and potential risks associated with the websites they visit and the content they engage with. Personal responsibility and an understanding of the evolving digital landscape are vital.

In summary, the Tor Project acts as a guardian of online privacy, embracing the principles of freedom, anonymity, and security. It empowers individuals worldwide to explore the vast expanses of the internet without sacrificing their right to privacy. Through its innovative technology and passionate community, it represents a beacon of hope in an increasingly interconnected and surveilled world.

Fig3.2 Tor Project

What are the potential benefits and risks associated with the tor network

Benefits of the Tor Network:

Anonymity: The primary benefit of the Tor network is its ability to provide users with a higher level of anonymity compared to traditional web browsing. By routing internet traffic through multiple relays, Tor conceals the user's IP address and makes it challenging to trace their online activities, promoting privacy and protecting against surveillance.

Censorship Circumvention: Tor can help users bypass internet censorship imposed by governments or institutions. It allows individuals in repressive regimes to access blocked websites and communicate freely, empowering them to exercise their right to information and freedom of expression**.**

Whistleblower Protection: Tor provides a secure platform for whistleblowers to anonymously share sensitive information with journalists, activists, or organizations without fear of reprisal. It enables them to expose corruption, human rights violations, or other misconduct while minimizing the risk of identification**.**

Access to Hidden Services: The Tor network hosts hidden services, also known as the dark web, which can offer valuable resources, including online communities, information repositories, and platforms for free expression. These services can facilitate research, collaboration, and the exchange of ideas in a relatively private and secure environment.

Risks and Challenges of the Tor Network:

Illicit Activities: The anonymity provided by Tor can attract individuals engaged in illegal activities, such as selling illicit goods or services, sharing explicit content, or coordinating criminal activities. This poses a challenge in distinguishing between legitimate uses and illicit behavior on the network.

Malicious Exit Relays: While Tor relays are operated by volunteers, there is a possibility of some relays being compromised or operated by malicious entities. Such relays could potentially intercept or manipulate users' traffic, compromising their privacy and security.

Vulnerabilities and Exploits: Like any software or network, the Tor network is not immune to vulnerabilities or exploits. While the project strives to maintain a robust and secure system, there is always a risk of undiscovered flaws or attacks that could compromise user anonymity or expose sensitive information**.**

Performance and Latency: Due to the multi-hop nature of Tor's routing, internet traffic may experience increased latency or slower speeds compared to direct connections. This trade-off is necessary to ensure anonymity, but it can affect the browsing experience, particularly for bandwidth-intensive activities.

Perception and Targeting: The use of Tor might raise suspicion or draw attention from authorities or other entities monitoring internet traffic. Some individuals, such as journalists, activists, or researchers, may face increased scrutiny or be subjected to targeted surveillance due to their use of Tor, potentially compromising their privacy and safety.

How can investigations be conducted in deep web while adhering to ethical guidelines

Key considerations to ensure ethical conduct:

Clear Purpose and Justification: Define the purpose of the investigation and ensure it aligns with legal and ethical standards. Clearly articulate the objective, scope, and boundaries of the investigation to guide your actions.

Legal Compliance: Familiarize yourself with the legal frameworks governing your jurisdiction and ensure that your investigative activities are in full compliance with applicable laws. Be aware of any restrictions or potential legal risks associated with accessing certain content or engaging in specific activities within the deep web.

Informed Consent and Privacy: Respect privacy rights and obtain informed consent when collecting or using personal data. Remember that deep web users have a reasonable expectation of privacy, and obtaining information without proper consent or legal authorization may violate ethical standards.

Avoid Unlawful Activities: Conduct investigations within the boundaries of the law. Avoid engaging in or promoting illegal activities during the investigation process, as this compromises ethical integrity and potentially exposes investigators to legal repercussions.

Minimize Harm and Intrusion: Ensure that your investigation activities minimize harm to individuals and organizations. Avoid unnecessarily intruding upon private spaces or disrupting legitimate operations. Consider the potential consequences of your actions and prioritize minimizing any negative impact**.**

Respect Anonymity: Recognize and respect the anonymity of users within the deep web. Avoid attempting to de-anonymize individuals unless there are exceptional circumstances and clear legal justifications. Balancing the need for investigation with the preservation of privacy is crucial.

Evidence Collection and Handling: Maintain proper protocols for evidence collection, handling, and preservation. Follow accepted standards to ensure the integrity, authenticity, and admissibility of evidence. Document the chain of custody to ensure it withstands legal scrutiny.

Professionalism and Transparency: Conduct yourself professionally and maintain transparency throughout the investigation process. Clearly communicate your intentions, methodologies, and limitations to stakeholders involved. This fosters trust, accountability, and legitimacy in your investigative work.

Regular Ethical Reviews: Continuously evaluate the ethical implications of your investigative activities. Regularly reassess your methods and actions to ensure ongoing compliance with ethical guidelines and adjust your approach if necessary

What tools and techniques can be used to navigate and search he deep web effectively

To navigate and search the deep web effectively, various tools and techniques can aid in discovering relevant information and hidden services. Here are some commonly used tools and techniques:

Tor Browser: The Tor Browser is the essential tool for accessing the deep web. It provides a user-friendly interface and ensures secure and anonymous browsing by connecting to the Tor network. By using the Tor Browser, you can access hidden services and explore the deep web safely.

Deep Web Search Engines: While traditional search engines like Google cannot index deep web content, several specialized deep web search engines can help navigate the hidden layers. Examples include DuckDuckGo's Tor-based search engine, Torch, and Grams, a search engine for darknet marketplaces.

Directories and Indexes: Deep web directories and indexes serve as curated lists of hidden services and resources. These platforms provide organized categories and links to various deep web websites and services. The Hidden Wiki and Onion Link List are popular examples of such directories.

Blockchain Explorers: In the deep web, blockchain explorers allow you to browse and search blockchain data for cryptocurrencies like Bitcoin. They provide transaction histories, addresses, and other relevant information for exploring the financial aspects of the deep web.

Decentralized Marketplaces: Deep web marketplaces operate within the Tor network and facilitate the buying and selling of goods and services. Platforms like AlphaBay and Dream Market (prior to their takedowns) were widely known. It's important to note that engaging in illegal activities on these marketplaces is strictly against ethical and legal guidelines.

Reverse Image Search: Reverse image search tools, such as Tineye and Google Reverse Image Search, can be helpful in locating the original source or related instances of an image found on the deep web. This can aid in identifying and verifying content.

Forum and Community Platforms: Deep web forums and communities provide valuable information and discussions on various topics. Platforms like Dread, Intel Exchange, and Hidden Answers can serve as sources of knowledge and insights from users within the deep web community**.**

Verification Tools: When encountering information or claims on the deep web, employing verification tools can help evaluate the credibility and reliability of the content. Fact-checking websites like Snopes and Politifact, along with reputable news sources, can be used to cross-reference and validate information.

CHAPTER 4

ACTIVIY

In the pursuit of investigating the deep web using TOR, extensive exploration was carried out using tor.taxi as a trusted resource.

Tor.taxi:

It is widely recognized for its reliable collection of onion links, which are essential for accessing hidden websites on the deep web. The darknet, which is a part of the deep web, consists of hidden websites that are not accessible through traditional search engines. Tor.taxi acts as a trusted resource for individuals looking to access darknet markets while minimizing the risks associated with phishing scams or fake websites It verifies and lists the URLs of various darknet markets, offering information on their current status, mirror links, and any important announcements.

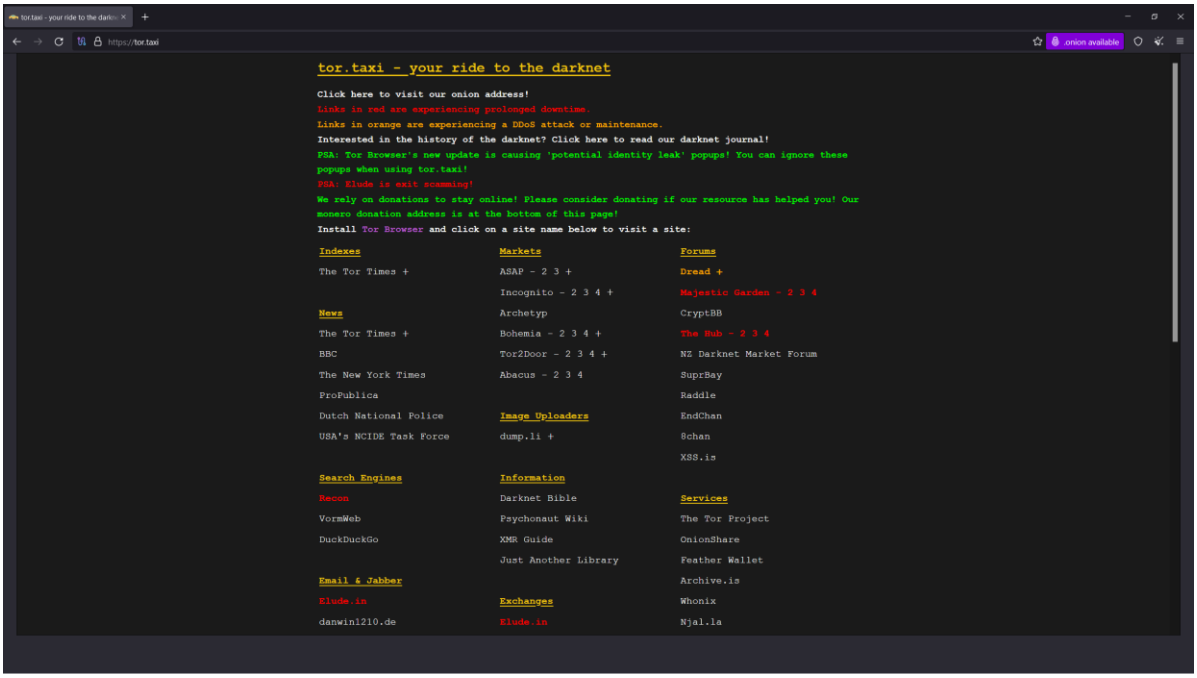


Fig4.1 Tor.taxi

NOTE:

It is important to highlight that throughout the project, strict adherence to ethical guidelines and legal boundaries was maintained. The exploration of the Bohemia Marketk, or any other deep web marketplace, was conducted solely for research purposes and did not involve engaging in any illegal activities.

The NewYork Times :

The New York Times onion link offered a glimpse into the presence of reputable and well-established news organizations within the deep web. It exemplified the recognition that even mainstream media outlets are taking note of the importance of providing access to their content for users who prioritize anonymity and privacy.

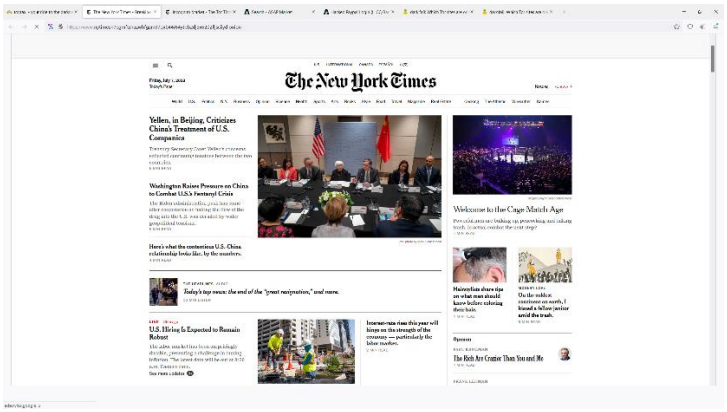


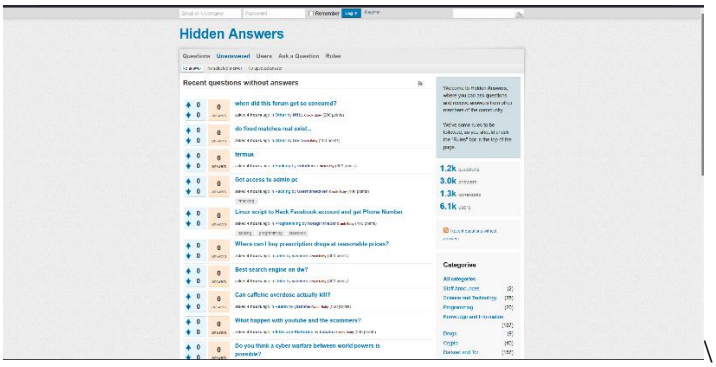
Fig4.2 The NewYork Times

By accessing The New York Times onion link, users were able to browse a selection of news articles, features, and multimedia content published by the renowned publication. This demonstrates that even within the deep web, there are opportunities for individuals to access credible news sources and stay informed about global events.

Hidden Answers:

Hidden Answers is a popular question-and-answer platform offering a unique space for users to seek and share information anonymously.Hidden Answers provided an intriguing glimpse into the vibrant community of deep web users engaging in knowledge exchange and discussions. Users can pose questions on a wide range of topics, from technical queries to

philosophical inquiries, and receive responses from fellow users within the Hidden Answers community.



4.3 HIDDEN ANSWERS

It offers an alternative avenue for individuals to seek information, guidance, and insights without revealing their identities. It embraces the core principles of anonymity and privacy that underpin the deep web environment, allowing users to express themselves freely and access knowledge without fear of judgment or repercussion.

Bohemia:

Bohemia Market was known for its presence as a marketplace that offered a diverse range of products, including legal and illicit items. While some products may be legal, it's important to note that engaging in any illegal activities within such marketplaces is strictly against ethical guidelines and illegal in many jurisdictions. It operates within the realm of anonymity, facilitating the buying and selling of various goods and services.

Deep web marketplaces like Bohemia Market often utilize encryption and cryptocurrency transactions to provide users with enhanced privacy and security. It is crucial to exercise caution and discernment when accessing and interacting with these platforms, as they carry inherent risks, including exposure to fraudulent sellers, potential legal consequences, and compromising personal safety.

It was visited to provide a comprehensive understanding of the dynamics and complexities within the deep web environment. Exploring deep web marketplaces sheds light on the underground economies that exist within the digital realm and their implications for law enforcement and society.

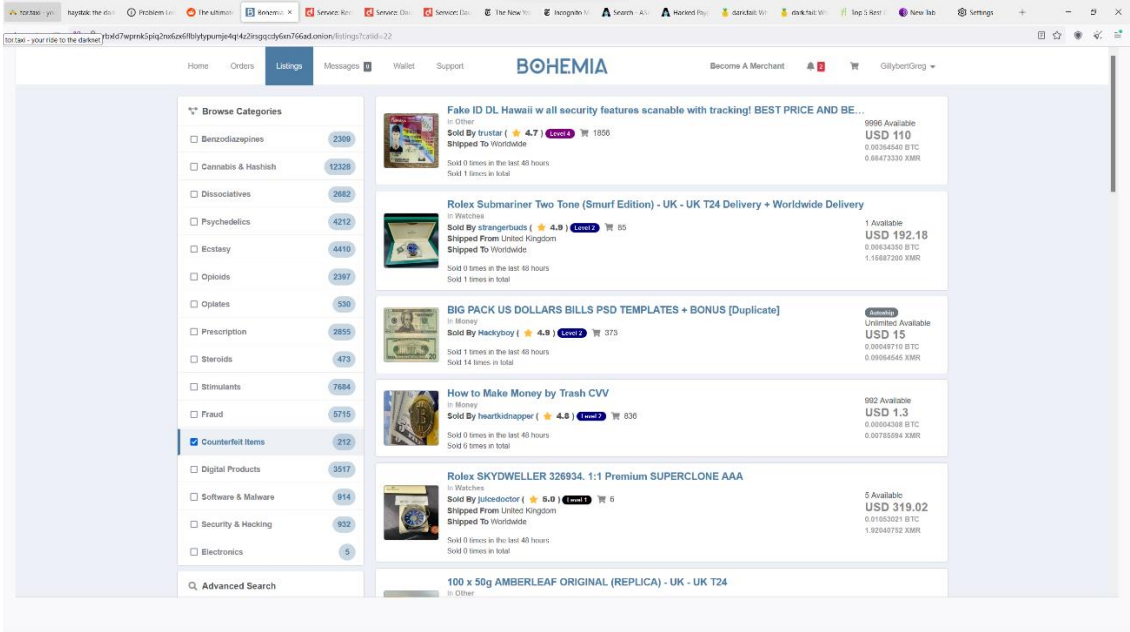


Fig.4.4 Bohemia

CHAPTER 5
CONCLUSION

CONCLUSION

In conclusion, the websites that were viewed throughout the project were crucial in helping to expand our awareness of the deep web environment. Each website offered distinct views into the complex web's fabric, from dependable news sources to community-driven platforms and deep web marketplaces. The project fostered a responsible and informed approach to investigating and comprehending the complexities of this intriguing environment while adhering to ethical considerations at all times.