A

Project Report

On

“DARK WEB”

SUBMITTED IN THE PARTIAL FULLFILLMENT OF THE

REQUIREMENT FOR THE AWARD OF DEGREE OF

BACHELOR OF TECHNOLOGY

In

Computer Science and Engineering

Submitted by

Gopal Pandey (12500115043)

Vibhav (12500115121)

Under the esteemed guidance of

Vipin Kumar Dubey

Assistant Professor

Dept. of CSE

Department of Computer Science and Engineering

Bengal College of Engineering & Technology

Durgapur, W.B

Department of Computer Science & Engineering

Bengal College of Engineering & Technology

Durgapur, W.B

CERTIFICATE OF APPROVAL

The project entitled **"Dark Web"** submitted by **Gopal Pandey (12500115043) and Vibhav (12500115121)** under guidance of **"Vipin Kumar Dubey" ,** is hereby approved as a creditable study of engineering subject to warrant it acceptance as a pre-request to obtain the degree for which it has been submitted. It is understood that by this approval the undersigned don't necessarily endorse or approve any statement made, opinion or conclusion drawn thereby but approve the project only for the purpose for which is submitted.

VIPIN KUMAR DUBEY	Mr. S.K ABDUL RAHIM
(Assistant Professor)	(Head Of Department)
Computer Science & Engineering	Computer Science & Engineering

Department of Computer Science & Engineering

Bengal College of Engineering & Technology

Durgapur, W.B

UNDERTAKING

We, **Gopal Pandey (12500115043) & Vibhav (12500115121)**, B.Tech, 8th Semester (Computer Science & Engineering), hereby declare that our project report, entitled "**Dark Web**" is our own contribution. The value or ideas of other people which are utilized in the report has been properly acknowledged and mentioned in the reference. I undertake total responsibility if any traces of plagiarism is found at any later stage.

_____

Gopal Pandey (12500115043)

_____

Vibhav (12500115121)

ACKNOWLEDGEMENT

"Gratitude is not a things of expression; it is more matter of felling"

There is always a sense of gratitude which one expresses towards other for their help and supervision in achieving the goal. This formal price of acknowledgement is an attempt to Express the feeling of gratitude towards people who helped us in successful completion of our training.

we would like to express our deep gratitude to Mr. Vipin Kumar Dubey, our project coordinator for his constant cooperation He was always there with his competent guidance and valuable suggestion throughout the pursuance of this project: We would also like to appreciate to all the respondents and group members whose responses and coordination were of utmost importance for the project.

Above all no words can express our feelings to your parents, friends and all those persons who supported us during our project. We are also thankful to all the respondents whose cooperation & support las helped us a lot in collecting necessary information.

Gopal Pandey (12500115043)

Vibhav (12500115121)

CONTENTS

LIST OF FIGURE

LIST OF TABLE

ABSTRACT

Many believe a Google search can identify most of the information available on the Internet on a given subject. But there is an entire online world – a massive one – beyond the reach of Google or any other search engine. Policymakers should take a cue from prosecutors – who just convicted one of its criminal masterminds – and start giving it some attention.

The scale of the Internet's underworld is immense. The number of non-indexed web sites, known as the Deep Web, is estimated to be 400 to 500 times larger than the surface web of indexed, searchable web sites. And the Deep Web is where the dark side of the Internet flourishes. While there are plenty of law-abiding citizens and well-intentioned individuals (such as journalists, political dissidents, and whistleblowers) who conduct their online activities below the surface, the part of the Deep Web known as the Darknet has become a haven for regulatory evasion, crime, and threats to national security.

This policy brief outlines what the Deep Web and Darknet are, how they are accessed, and why we should care about them. For policymakers, the continuing growth of the Deep Web in general and the accelerated expansion of the Darknet in particular pose new policy challenges. The response to these challenges may have profound implications for civil liberties, national security, and the global economy at large.

Keywords: computer crime, internet, deep web, darknet, law of war, law of armed conflict, regulation, geography, Tor, Silk Road, national security, cyber law, cyber crime, cyber security, cyber war.

CHAPTER – 1

1.1. INTRODUCTION

The Dark web is the World Wide Web content that exists on dark nets, overlay networks that use the Internet but require specific software, configurations, or authorization to access. [1][2] The dark web forms a small part of the deep web, the part of the Web not indexed by web search engines, although sometimes the term *deep web* is mistakenly used to refer specifically to the dark web.[3][4][5][6][7]

The Dark web is a place on the internet that is not accessible using the regular browsers or your regular connections. This is where all or most of the connections went.
Dark net websites are accessible only through networks such as Tor aka "The Onion Router" and I2P ("Invisible Internet Project"). Tor browser and Tor-accessible sites are widely used among the dark net users and can be identified by the domain ".onion". While Tor focuses on providing anonymous access to the Internet, I2P specializes on allowing anonymous hosting of websites.

The dark web is also used for illegal activity such as illegal trade of stolen assets such as bank information, personal information, as well as drugs and a media exchange for nefarious activities like terrorism.

The darknets which constitute the dark web include small, friend-to-friend peer-to-peer networks, as well as large, popular networks like Tor, Freenet, I2P, and Riffle operated by public organizations and individuals. Users of the dark web refer to the regular web as Clearnet due to its unencrypted nature.[1] The Tor dark web may be referred to as onionland,[2] a reference to the network's top-level domain suffix .onion and the traffic anonymization technique of onion routing.

1.2. BACKGROUND OF THE CONCEPT

Beyond the prying eyes of Google and Bing exists a vast cyberfrontier — by some estimates hundreds of times larger than the World Wide Web. This so-called "deepweb" is often more humdrum than sinister, littered with banal data and derelict URLs, but it is also home to an anything-goes commercial underworld, called the "darknet," that will make your stomach turn. It's a place where drugs and weapons are openly traded, where terrorists link up, and where assassins bid on contract killings. In recent years, the darknet has found itself in government cross-hairs, with the FBI and National Security Agency (NSA) cracking down on drug merchants and pornographers. Despite a series of high-profile busts, however, this lawless realm continues to hum along, deep beneath the everyday web.

October 29, 1969

Charley Kline, a student at the University of California, Los Angeles, types out the first message between computers connected by ARPANET, the Internet progenitor developed by the Pentagon's Defense Advanced Research Projects Agency. (Only the first two letters of the electronic dispatch, "LOGIN," make it all the way to computers at Stanford University.) Within just a few years, a number of isolated, secretive networks begin to appear alongside ARPANET. Some eventually become known as "darknets."

1980s

With the birth of the modern web, arguably marked by the 1982 standardization of the Internet protocol suite, the problem of storing sensitive or illegal data looms large. Early solutions involve physical "data havens" — the informational analogues of tax havens — in the Caribbean that promise to host everything from gambling operations to illegal pornography.

Late 1990s

As the Internet goes mainstream, falling storage costs coupled with advances in file compression set off an explosion of darknet activity, as users begin to share copyrighted materials. Soon, the Internet's peer-to-peer data transmission gives birth to decentralized data hubs, some of which, like so-called topsites — where most illegal music and movie files originate — are password-protected and known only to insiders. Others, like Napster, operate in the open and facilitate millions of file transfers per day.

2010

The cybersecurity and intelligence firm Procysive estimates that the darknet is home to "more than 50,000 extremist websites and more than 300 terrorist forums." The illicit sale of pirated digital content, it reports, "serves as a source of financing for [terrorist] operations."

June 1, 2011

A Gawker-affiliated blog publishes an exposé on Silk Road, a hidden marketplace that "makes buying and selling illegal drugs as easy as buying used electronics." It's like Amazon.com for crystal meth and LSD, except only available to Tor users with Bitcoin accounts. Traffic to Silk Road surges, and the value of a Bitcoin jumps from around $10 to more than $30 within days.

August 1, 2013

Irish authorities raid the Dublin apartment of Eric Eoin Marques, described by the FBI as "the largest facilitator of child porn on the planet." His arrest coincides with a mysterious shutdown of vast swaths of the darknet, allegedly as part of an FBI sting operation that exploited a breach in the web browser Firefox to identify Tor users. Users' identities are reportedly routed back to a server in Northern Virginia.

August 4, 2013

The U.S. government intercepts secret communications between al Qaeda chief Ayman al-Zawahiri and Nasir al-Wuhayshi, the head of the Yemeni-based al Qaeda in the Arabian Peninsula. The online confab leads to the shuttering of U.S. embassies in 21 countries across the Muslim world. According to researchers at the Institute for National Security Studies in Israel, the high-level al Qaeda talks "apparently took place in a part of the internet sometimes called deepnet, blacknet, or darknet."

CHAPTER – 2

2.1. WORLD WIDE WEB & DARK WEB

2.1.1. SURFACE WEB

The Surface Web (also called the **Visible Web**, **Indexed Web**, **Indexable Web** or **Lightnet**)[10] is the portion of the World Wide Web that is readily available to the general public and searchable with standard web search engines. It is the opposite of the deep web, the part of the web not indexed by a Search Engine.[11] The Surface Web only consists 10 percent of the information that is on the internet.[12] The Surface Web is made with a collection of static pages. These are Web pages that are in a server, available to be accessed by any search engine.[13]

According to one source, as of June 14, 2015, Google's index of the surface web contains about 14.5 billion pages.[14]

Surface Web

- Accessible
- Indexed for Search Engines
- Little illegal activity
- 4% of WWWcontent

2.1.2. DEEP WEB

The **deep web**,[15] **invisible web**,[16] or **hidden web**[17] are parts of the World Wide Web whose contents are not indexed by standard web search engines. The opposite term to the deep web is the surface web, which is accessible to anyone using the Internet.[18] Computer scientist Michael K. Bergman is credited with coining the term *deep web* in 2001 as a search indexing term.[19]

The content of the deep web is hidden behind HTTP forms[20][21] and includes many very common uses such as web mail, online banking, and services that users must pay for, and which are protected by paywalls, such as video on demand and some online magazines and newspapers.

The content of the deep web can be located and accessed by a direct URL or IP address, and may require a password or other security access past the public website page.

Deep Web

- Accessible by password, encryption, or through gateway software
- Not indexed for Search Engines
- Little illegal activity outside of Dark Web
- Huge in size and growing exponentially

2.1.3. DARK WEB

The darknets which constitute the dark web include small, friend-to-friend peer-to-peer networks, as well as large, popular networks like Tor, Freenet, I2P, and Riffle operated by public organizations and individuals. Users of the dark web refer to the regular web as Clearnet due to its unencrypted nature.[1] The Tor dark web may be referred to as onionland,[2] a reference to the network's top-level domain suffix .onion and the traffic anonymization technique of onion routing.

Dark Web

-Restricted to special browsers

-Not indexed for Search Engines

-Large scale illegal activity

-Unmeasurable due to nature

- 96% of WWWcontent

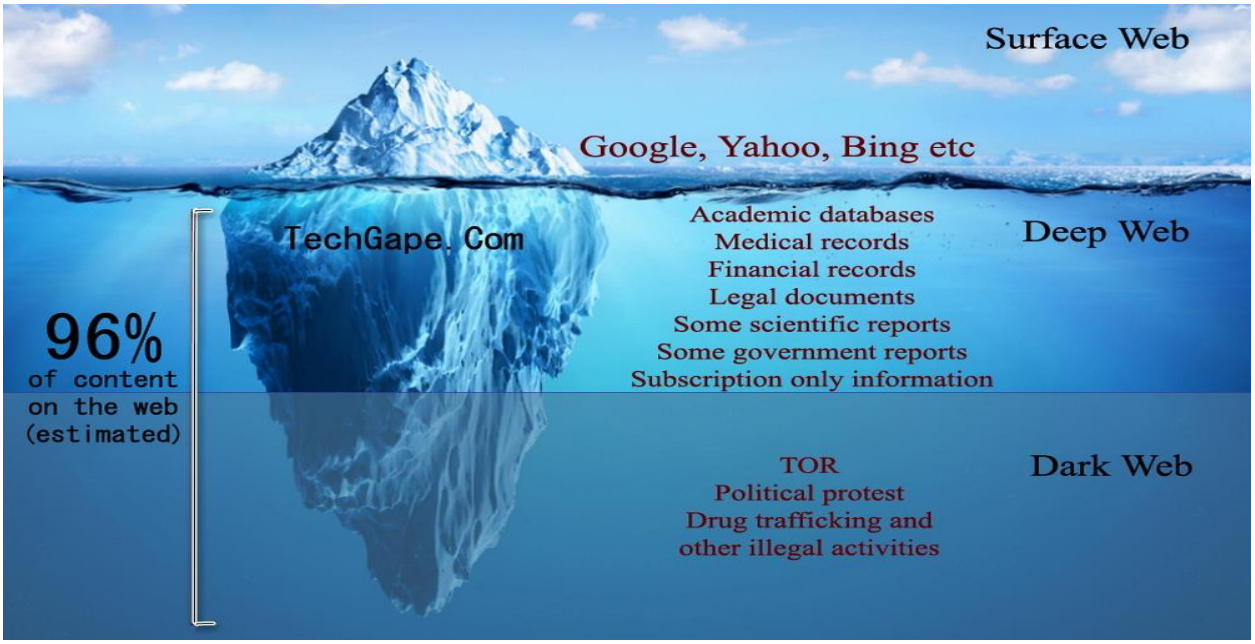

Fig 2.1: Type of web

2.2. HOW TO ACCESS DARK WEB

According to researchers, only 4% of the internet is visible to the general public. Meaning that the remaining 96% of the internet is made up of "The Deep Web". Dark web access is done using the TOR network with the TOR browser bundle. TOR is the most widely used dark web browser.

2.2.1. WHAT IS TOR?

Tor is free and open-source software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router".[22][23] Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays[24] to conceal a user's location and usage from anyone conducting network surveillanceor traffic analysis. Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms".[25] Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

Tor does not prevent an online service from determining when it is being accessed through Tor. Tor protects a user's privacy, but does not hide the fact that someone is using Tor. Some websites restrict allowances through Tor. For example, the Media Wiki Tor Block extension automatically restricts edits made through Tor, although Wikipedia allows some limited editing in exceptional circumstances.[26]

Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP address, multiple times and sends it through a virtual circuit comprising successive, random-selection Tor relays. Each relay decrypts a layer of encryption to reveal the next relay in the circuit to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or knowing the source IP address. Because the routing of the communication was partly concealed at every hop in the Tor circuit, this method eliminates any single point at which the communicating peers can be determined through network surveillance that relies upon knowing its source and destination.[27]

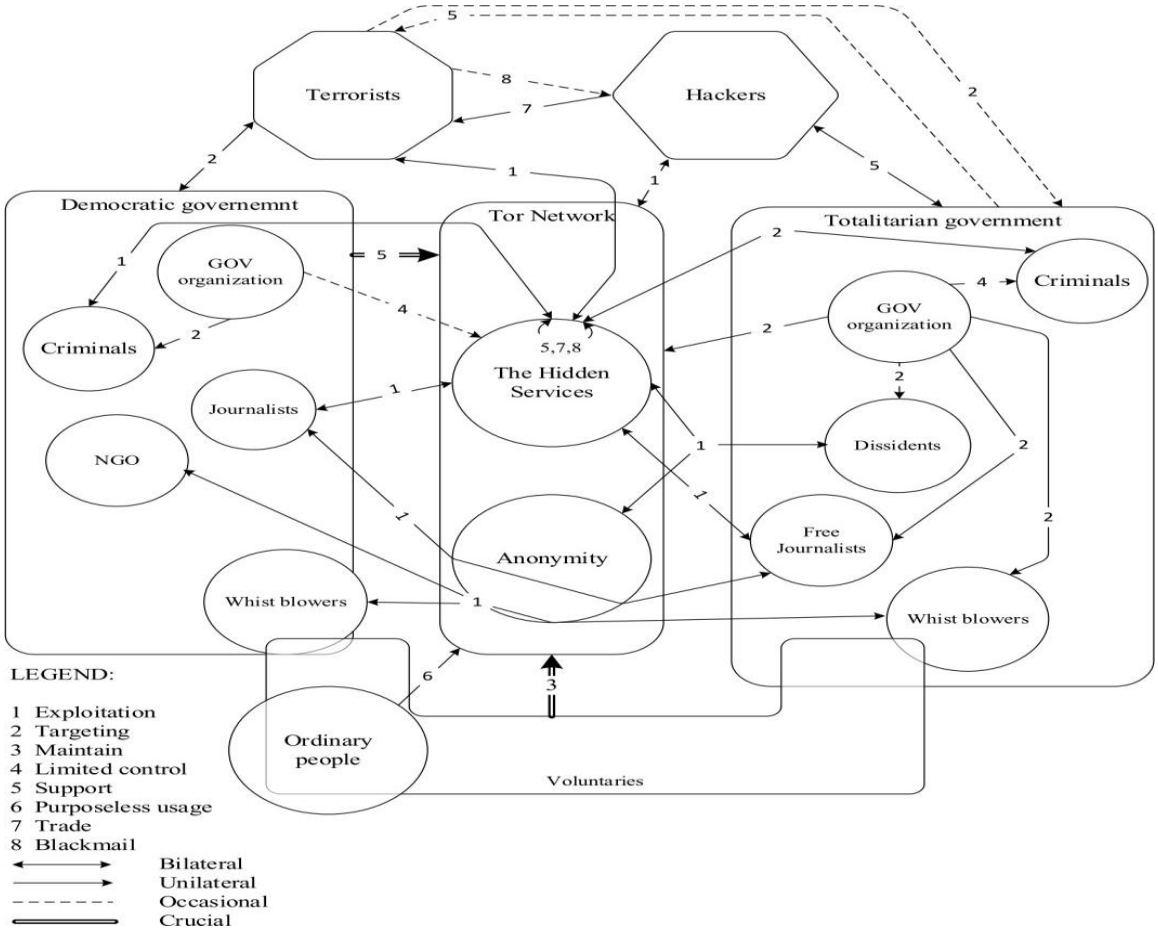

Fig.2.2 : Relationship, Actors, Functions and Tensions (RAFT) diagram of Tor

2.2.2. HOW TOR WORKS?

Tor works on the concept of 'onion routing' method in which the user data is first encrypted and then transferred through different relays present in the Tor network, thus creating a multi-layered encryption (layers like an onion), thereby keeping the identity of the user safe.

One encryption layer is decrypted at each successive Tor relay, and the remaining data is forwarded to any random relay until it reaches its destination server. For the destination server, the last Tor node/exit relay appears as the origin of the data. It is thus tough to trace the identity of the user or the server by any surveillance system acting in the mid-way.

Other than providing anonymity to standalone users, Tor can also provide anonymity to websites and servers in the form of Tor Hidden Services. Also, P2P applications like BitTorrent can be configured to use the Tor network and download torrent files.

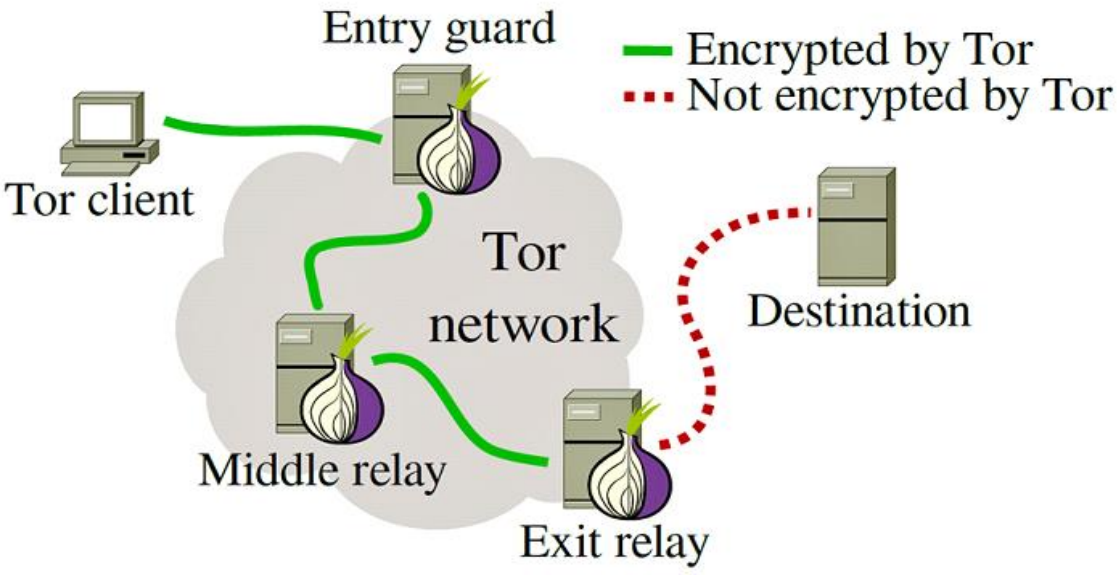

Fig 2.3: How Tor Work

2.2.3. TYPES OF RELAYS

By default, Tor bounces connections through 3 relays.

1. Client Guard
2. Relay Middle Relay
3. Exit Relay Desination

Entry/Guard Relay – This is the entry point to the Tor network. Relays are selected to serve as guard relays after being around for a while, as well as having shown to be stable and having high bandwidth.1

Middle Relay – Middle relays are exactly that – middle nodes used to transport traffic from the guard relay to the exit relay. This prevents the guard and exit relay from knowing each other.

Exit Relay – These relays are the exit point at the edge of the Tor network. These relays send traffic to the final destination intended by the client.

Generally, it is safe to run a guard or middle relay on any VPS or shared server (such as Digital Ocean or EC2), since all the server operators will see is harmless encrypted traffic (more on this later).

However, there are special responsibilities to consider when running an exit node. Since exit relays send traffic directly to the end destination, any illicit activity done through Tor appears to come from the exit relay. This leads to the rare possibility of raids, abuse notices, or more.

2.2.4. HOW TO ACCESS THE DARK WEB

Step 1: the ISP's (Internet Service Providers) and Law Enforcement are not trying to track those who use Tor to access the Dark Web, they are, and they are good at it so don't make it easy for them.

It should be brought to your attention that there was a recent Tor vulnerability which leaked your REAL IP address leading back to your real location. If you already have the Tor Browser then UPDATE it immediately. Vulnerabilities like these are happening more often to Tor.

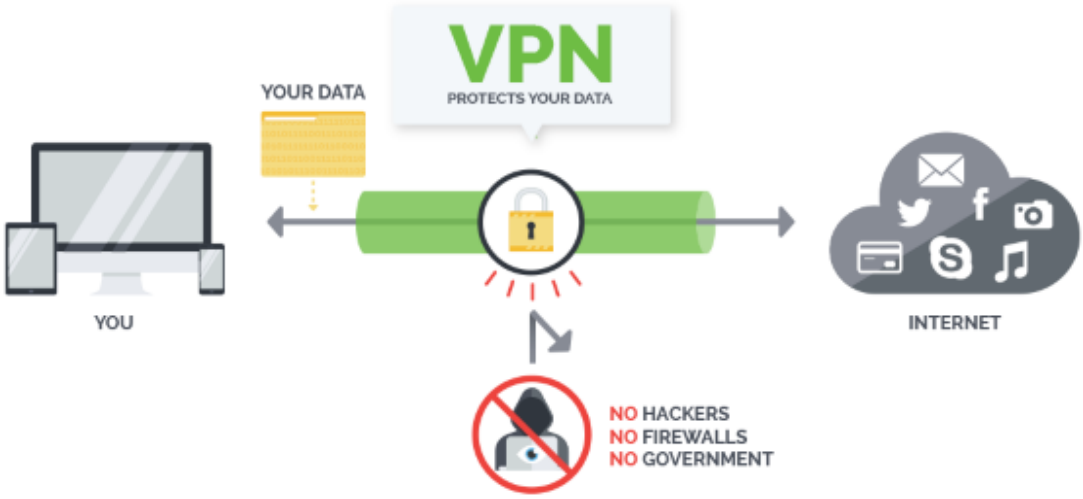

Fig.2.4: How Vpn Work

By using the simple VPN app, your darknet activities will be hidden from your ISP and government agencies as all of your internet usage will be encrypted. No one will even know you are using TOR, let alone browsing for darknet markets. The other benefit of using a VPN is to prevent hackers stealing your identity and or personal files and photos from your computer. You need to use a good VPN that keeps NO LOGS, fast performance, preferably accepts bitcoin as payment, has a kill switch for DNS leaks, and is compatible with TOR.

Step 2: To get dark net access you will need to download the dark web browser called TOR browser bundle. Only get it from the official TOR website, never download it from anywhere else!

Now close all of your browsing windows and all apps connecting to the world wide web like Google Drive, Skype, OneDrive, iCloud etc. Then open your VPN app and connect to another

location other than where you are at, make sure to use the Open VPN protocol as it is the most secure.

Open up your normal favorite browser and then download TOR

TOR Official Website: https://www.torproject.org/download/download.html

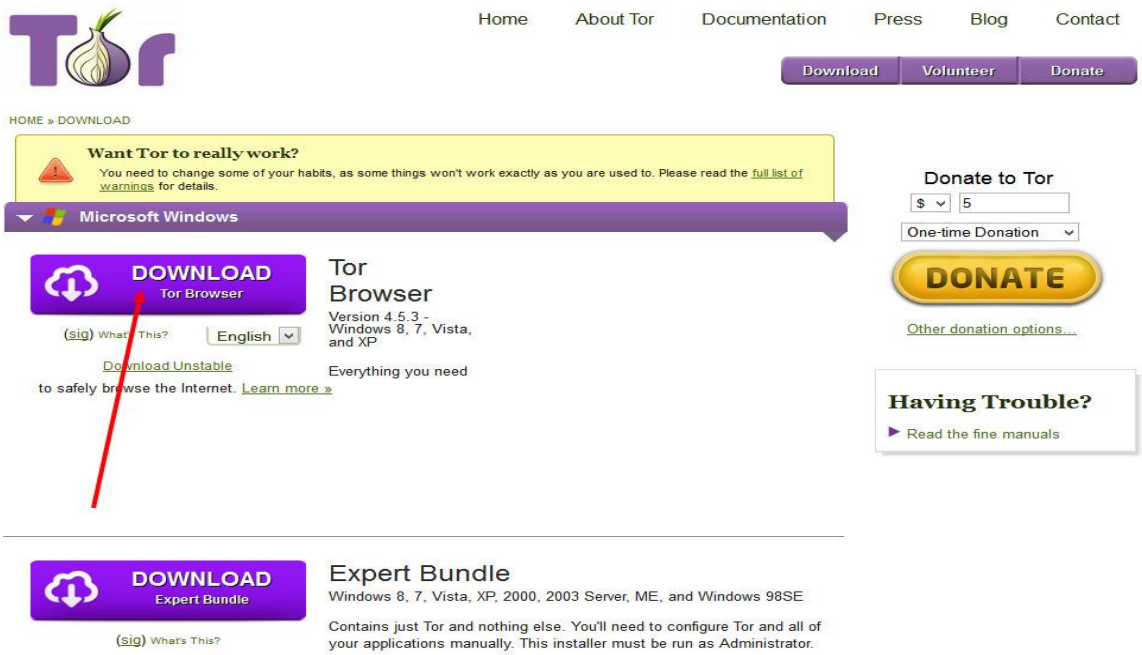

Fig.2.5: Tor Broswer

Step 3: Install the TOR browser bundle on your PC or Mac. When the download is complete, double-click the downloaded file, choose the destination folder (the folder where you want to extract tor browser), and choose extract.

Step 4: Start TOR Browser. Open the folder where you extracted TOR browser and double-click "Start Tor Browser". The TOR start page will open in a browser window (it's actually a portable version of Fire Fox stripped down). From here, we are able to gain access to .onion websites through dark web browser.

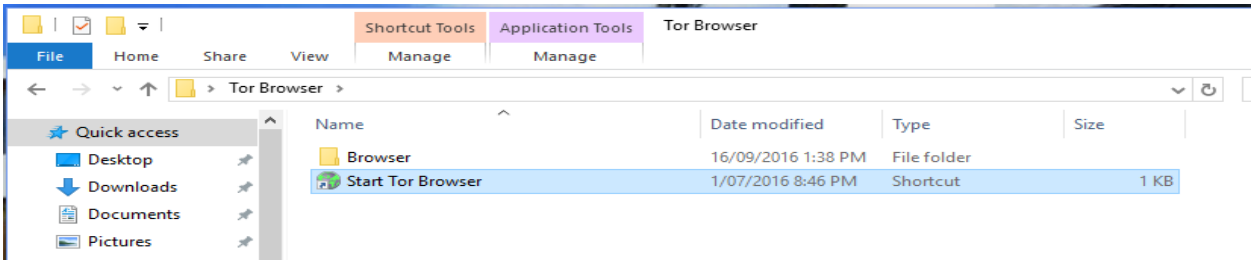

Fig.2.6: Start Tor Browser

CHAPTER – 3

3.1. DARKNET MARKET

A darknet market or cryptomarket is a commercial website on the web that operates via darknets such as Tor or I2P.[28][29] They function primarily as black markets, selling or brokering transactions involving drugs, cyber-arms,[30] weapons, counterfeit currency, stolen credit card details,[31] forged documents, unlicensed pharmaceuticals,[32] steroids,[33] and other illicit goods as well as the sale of legal products.[34] In December 2014, a study by Gareth Owen from the University of Portsmouth suggested the second most popular sites on Tor were darknet markets.[35]

Following on from the model developed by Silk Road, contemporary markets are Sybil prizes by their use of darknet sybil prize access (typically Tor), bitcoin payment with escrow services, and eBay-like vendor feedback systems[36].

3.1.1. Market types

Items on a typical centralized darknet market are listed from a range of vendors in an eBay-like marketplace format. [90] Virtually all such markets have advanced reputation, search and shipping features similar to Amazon.com. [91]

Some of the most popular vendors are now opening up dedicated own online shops separate from the large marketplaces. [92] Individual sites have even returned to operating on the with mixed success.[93]

Some internet forums such as the defunct Tor Carding Forum[94] and the Russian Anonymous Marketplace function as markets with trusted members providing escrow services and users engaging in off-forum messaging.[95] In May 2014 the “Deepify” service attempted to automate the process of setting up markets with a SAAS solution; [96] however, this closed a short time later.[97]

Following repeated problems associated with infrastructure, a number of marketplace software alternatives have arisen using blockchain or peer-to-peer technologies, including OpenBazaar, [54] Bitmarkets,[98], Nxt,[99] and Particl.[100]

3.1.2. Venders

To list on a market, a vendor may have undergone an application process via referral, proof of reputation from another market or given a cash deposit to the market.[37]

Many vendors list their wares on multiple markets, ensuring they retain their reputation even should a single market place close. Grams have launched “Info Desk” to allow central content and identity management for vendors as well as PGP key distribution.[38][39]

Meanwhile, individual law enforcement operations regularly investigate and arrest individual vendors[40] and those purchasing significant quantities for personal use.[41]

A February 2016 report suggested that a quarter of all DNM purchases were for resale.[36]

3.1.3. Products

Whilst a great many products are sold, drugs dominate the numbers of listings, with the drugs including cannabis, MDMA, modafinil,[42][43][45] LSD, cocaine, and designer drugs.

Personal information

Personally identifying information, financial information like credit card and bank account information, and medical data from medical data breaches is bought and sold, mostly in darknet markets but also in other black markets.[46][47] People increase the value of the stolen data by aggregating it with publicly available data, and sell it again for a profit, increasing the damage that can be done to the people whose data was stolen.[48]

Fraud and hacking services

Main article: Carding (fraud)

Cyber crime and hacking services for financial institutions and banks have also been offered over the dark web.[49] Markets such as AlphaBay Market would go on to host a significant share of the commercial fraud market,featuring carding, counterfeiting and many related services.[50] Loyalty card information is also sold as it is easy to launder.[51]

Prohibitions and restrictions

Many markets will refuse to list weapons[52] or poisons.[53] Markets such as the original Silk Road would refuse to list anything where the "purpose is to harm or defraud, such as stolen credit cards, assassinations, and weapons of mass destruction".[60]

Later markets such as Evolution would ban "child pornography, services related to murder/assassination/terrorism, prostitution, Ponzi schemes, and lotteries", but allow the wholesaling of credit card data.[50]

The firearms market appears to attract extra attention from law enforcement[54] as well as other weapons such as certain types of knives and blades.[55]

3.1.4. Silk Road.

The first pioneering marketplace to use both Tor and Bitcoin escrow was Silk Road, founded by Ross Ulbricht under pseudonym "Dread Pirate Roberts" in February 2011.[56][57] In June 2011, Gawker published an article about the site,[58][59] which led to "Internet buzz"[60] and an increase in website traffic.[61] This in turn led to political pressure from Senator Chuck Schumer on the US DEA and Department of Justice to shut it down,[62] which they finally did in October 2013 after a lengthy investigation.[63] Silk Road's use of all of Tor, Bitcoin escrow and feedback systems would set the standard for new darknet markets for the coming years.[64] The shutdown was described by news site DeepDotWeb as "the best advertising the dark net markets could have hoped for" following the proliferation of competing sites this caused,[65] and *The* Guardian predicted others would take over the market that Silk Road previously dominated.[66][67]

The months and years after Silk Road's closure would be marked by a greatly increased number of shorter-lived markets as well as semi-regular law enforcement take downs, hacks, scams and voluntary closures.

Atlantis, the first site to accept Litecoin as well as Bitcoin, closed in September 2013, just prior to the Silk Road raid, leaving users just 1 week to withdraw any coins.[68][69] In October 2013, *Project Black Flag* closed and stole their users' bitcoins in the panic shortly after Silk Road's shut down.[70][71] Black Market Reloaded's popularity increased dramatically after the closure of Silk Road and Sheep Marketplace;[72] however, in late November 2013, the owner of Black Market Reloaded announced that the website would be taken offline due to the unmanageable influx of new customers this caused.[73] Sheep Marketplace, which launched in March 2013, was one of the lesser known sites to gain popularity with Silk Road's closure.[74] Not long after those events, in

December 2013, it ceased operation after two Florida men stole $6 million worth of users' Bitcoins.[75][76][77][78]

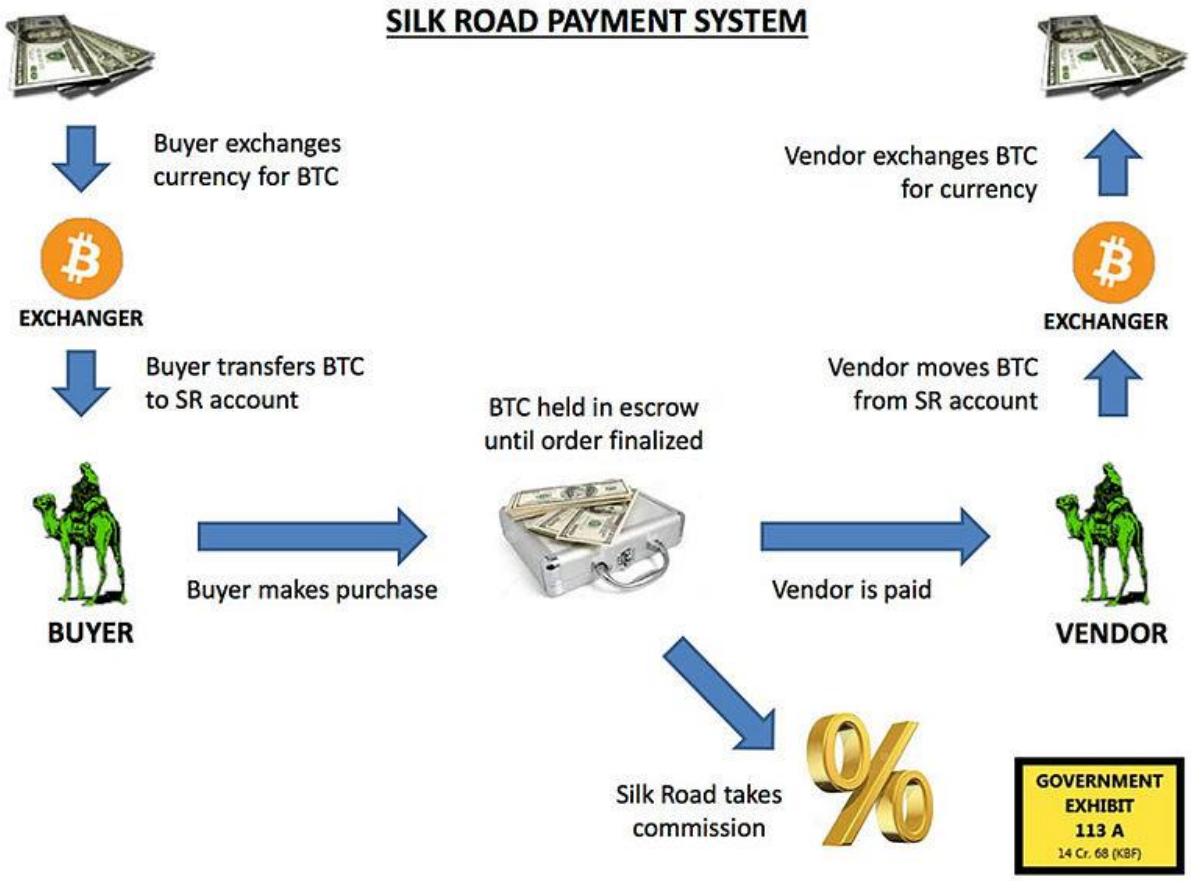

Fig.3.1: Silk Road Payment System

3.1.5. BITCOIN

Bitcoin (฿) is a cryptocurrency, a form of electronic cash. It is a decentralized digital currency without a central bank or single administrator that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.[76]

Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain. Bitcoin was invented by an unknown person or group of people using the pseudonym, Satoshi Nakamoto,[77] and released as open-source software in 2009.[78] Bitcoins are created as a reward for a process known as mining. They can be exchanged for other currencies, products, and services.[79] Research produced by University of Cambridge estimates that in 2017, there were 2.9 to 5.8 million unique users using a cryptocurrency wallet, most of them using bitcoin.[80]

Bitcoin has been criticized for its use in illegal transactions, its high electricity consumption, price volatility, thefts from exchanges, and the possibility that bitcoin is an economic bubble.[81] Bitcoin has also been used as an investment, although several regulatory agencies have issued investor alerts about bitcoin.[82]

SECURITY

The Bitcoin technology – the protocol and the cryptography – has a strong security track record, and the Bitcoin network is probably the biggest distributed computing project in the world. Bitcoin's most common vulnerability is in user error. Bitcoin wallet files that store the necessary private keys can be accidentally deleted, lost or stolen. This is pretty similar to physical cash stored in a digital form. Fortunately, users can employ sound security practices to protect their money or use service providers that offer good levels of security and insurance against theft or loss.

The rules of the protocol and the cryptography used for Bitcoin are still working years after its inception, which is a good indication that the concept is well designed. However, security flaws have been found and fixed over time in various software implementations. Like any other form of software, the security of Bitcoin software depends on the speed with which problems are found and fixed. The more such issues are discovered, the more Bitcoin is gaining maturity.

There are often misconceptions about thefts and security breaches that happened on diverse exchanges and businesses. Although these events are unfortunate, none of them involve Bitcoin itself being hacked, nor imply inherent flaws in Bitcoin; just like a bank robbery doesn't mean that the dollar is compromised. However, it is accurate to say that a complete set of good practices and intuitive security solutions is needed to give users better protection of their money, and to reduce the general risk of theft and loss. Over the course of the last few years, such security features have quickly developed, such as wallet encryption, offline wallets, hardware wallets, and multi-signature transactions.

Bitcoin is vulnerable to quantum computing, most systems relying on cryptography in general are, including traditional banking systems. However, quantum computers don't yet exist and probably won't for a while. In the event that quantum computing could be an imminent threat to Bitcoin, the protocol could be upgraded to use post-quantum algorithms. Given the importance that this update would have, it can be safely expected that it would be highly reviewed by developers and adopted by all Bitcoin users.

CHAPTER – 4

4.1. MAJOR ROLE OF DARKWEB

The promise of anonymity on the dark web opens itself up for use in multiple ways. Some legitimate reasons include civilians looking for protection from irresponsible corporations, censorship, ability to research into sensitive topics without concerns; militaries hosting hidden command and control services, journalists conducting their operations in countries without access to free media and speech; law enforcement performing sting operations, activists and whistle-blowers reporting abuses and speaking out against governments. All of these are applications which necessitate use of the dark web in some countries while not necessary in others [87] due to the variation in the legal landscape across nations.

While not all scenarios that benefit from anonymity are by default illegal, the dark web phenomenon indeed enables a fair share of illegal activities. One of these is providing adversaries – cyber threats – with an enabling infrastructure. This infrastructure includes command-and-control endpoints for botnets, markets allowing zero-day exploits to be traded, hackers for hire, private communication, coordination for attacks, variable-sized botnets for hire to launch DdoS attacks and pawning of breached data [88].

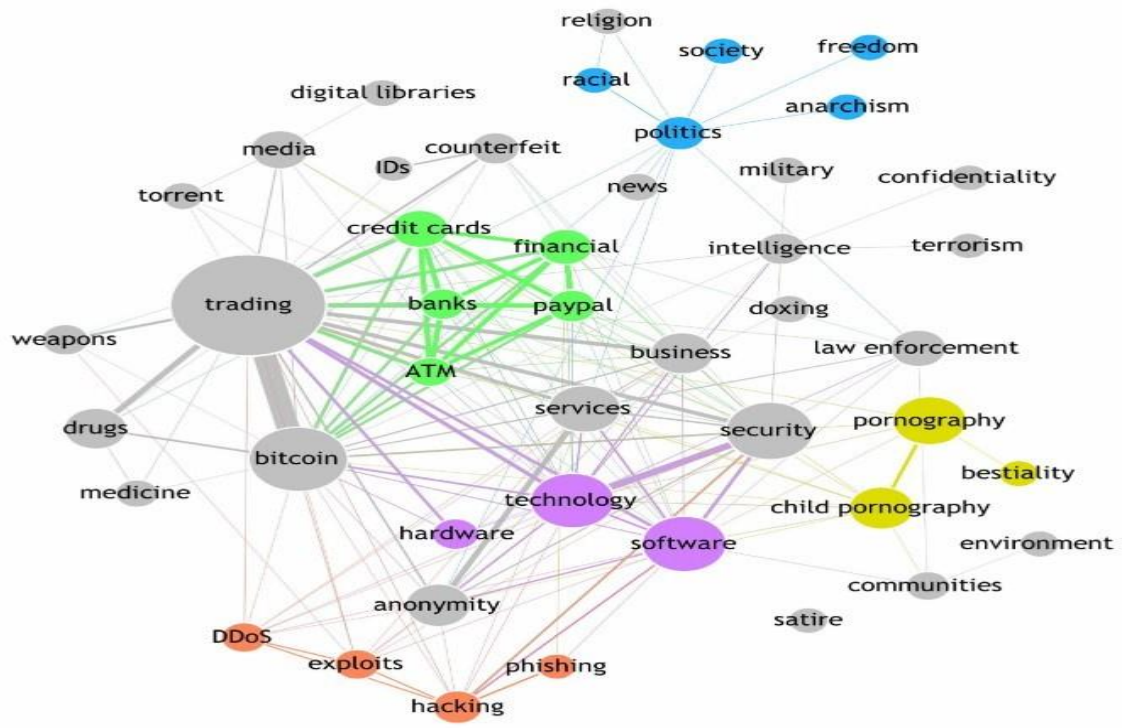

Fig.4.1 Dark Web Network

The graph in *Figure 4.1* above [89] is a representation of the various topics about which Tor hidden services – at least those with a website front – exist. [Size of a node is proportional to its topic presence, and weight of an edge expresses relatedness of the nodes.] Trading of illicit products, laundering currencies to facilitate those trades, security/hacking software, and illicit sexual content make up the top topics present [89].

Furthermore, individuals who wish to remain anonymous in the physical world can have a persona, or pseudonym, which represents them across multiple services online. They can have a stable and consistent presence online while at the same time be physically mobile and always on the move – something that may be a necessary extra step in avoiding legal prosecution in the physical world, especially in the highly collaborative nature of developed countries.

4.1.1. CYBERCRIME & TERRORISM

A general term for someone who gains unauthorised access to a system for malice or personal gain exists – a Black Hat [90]. However, given the breadth of actors and intentions involved, a classification system has been proposed to simplify discussion on cybercrime which can be of multiple types: offences against CIA of data/systems e.g. Advaned Persistent Threat (APT) – a highly evolved,

sophisticated and well-resourced threat actor – involved in espionage; computer-related e.g. identity theft; content-related e.g. child pornography, religious opinions in countries where it is illegal; copyright infringements; and a combination of the above e.g. cyberwarfare [91]. The offenders can also be categorised into individuals, e.g. insiders, hacktivists and script kiddies, or entities, e.g. nation state agencies.

Cybercrime has become increasingly accessible to anyone who wishes to engage in low-risk criminal activities while still having an impact on the target. Conducting Distributed Denial of Service (DdoS) attacks on websites is as convenient as hiring a botnet which offers DdoS-as-a-Service (DdoSaaS)[93], or launching Ransomware attacks on unsuspecting victims via phishing emails which contain malicious attachments or links [92]. These services let malicious actors – script kiddies in this case – pick the ‘low hanging fruit,’ i.e. targets without adequate security controls or training in place. Moreover, darknets also inadvertently serve as breeding grounds for future law enforcement personnel as these young ‘hackers’ amass knowledge about this underground infrastructure which later becomes valuable for the role of an information security professional; companies are starting to ‘hire hackers’ [93].

Sophisticated attacks involving a command-and-control (C2) channel being maintained between the attacker and the victim can be facilitated by Tor's hidden services. Tor's offer of anonymity and thus difficulty in being shut down is apt for purposes of a C2 server as seen in the fact that one of the most popular hidden services found on the Tor network was botnet C2 services [94].

Nation states have been expressing their concern at their need to prepare for warfare in the digital realm and realise that physical boundaries are meaningless in this domain[95]. This is of particular concern in cases where this warfare affects Critical Infrastructure (CI) and Industrial Control Systems (ICS) with the potential to have adverse real-world outcomes [96]. This ease-of- entry into being a cybercriminal is further helped along given the asymmetry of the warfare environment. Despite the cybercriminals not being as well funded or resourced as the organisations they target, they possess an advantage on the digital battlefield due having the liberty of choosing their tactic, timing and location whereas the defenders are required to be on alert at all times [97].

In warfare, deterrence and dissuasion have worked as useful military strategies in the past due to many reasons, one of them being the high barrier of entry into nuclear weapons. However, this does not apply in cyberspace as a weapon can be coded by people on, or bought easily from, the dark web [97]. By the same token, deterrence is no longer the domain of governments as sometimes

non-state actors can also become active participants in cyber warfare against common enemies [97]. Law enforcement agencies and hacktivist groups around the world have been active in the reduction of terrorist groups' activities on the surface web [98]. This has led to their migration to the dark web and made their conduct even more resilient to being disrupted [98]. Supporters can now freely express their opinions anonymously; the groups are less likely to be victims of hacktivists/vigilantes who try to shut down terrorism-related websites, and their operations can continue to be funded via virtual currencies, as discussed later in section Further to that, the dark web serves as a potential recruitment centre and training ground for newly formed groups or 'lone-wolf' terrorists. The latter has been attributed to a significant amount of terrorist activity around the globe and their identification on the dark web forums via natural language processing is an ongoing effort.

4.1.2. HOW HACKER USE DARKWEB

The role of hackers has changed over the years, in the past these professionals were viewed as dangerous criminals that needed to be kept at arm's length; meanwhile today they are highly sought from private companies, intelligence agencies and by criminal gangs.

"An increasingly large number of modern business operations rely on an understanding of the risks associated with software that can easily be made vulnerable to hacking." Reported in a post I published on the Fox News site on the role of hackers.

Hacking services are among the most attractive commodities in the underground market, it is possible to hire a hacker to request a "realistic" penetration test, or to pay to take over a Gmail or Facebook account for cyber espionage purpose.

4.1.2.a. DDOS ATTACK

In computing, a **denial-of-service attack** (**DoS attack**) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

In a **distributed denial-of-service attack** (**DdoS attack**), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DdoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, disrupting trade.

Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers suchas banks or credit card payment gateways. Revenge, blackmail and activism can motivate these attacks.

Method of attack

An application layer DdoS attack is done mainly for specific targeted purposes, including disrupting transactions and access to databases. It requires fewer resources than network layer attacks but often accompanies them. An attack may be disguised to look like legitimate traffic,

except it targets specific application packets or functions. The attack on the application layer can disrupt services such as the retrieval of information or search functions on a website.

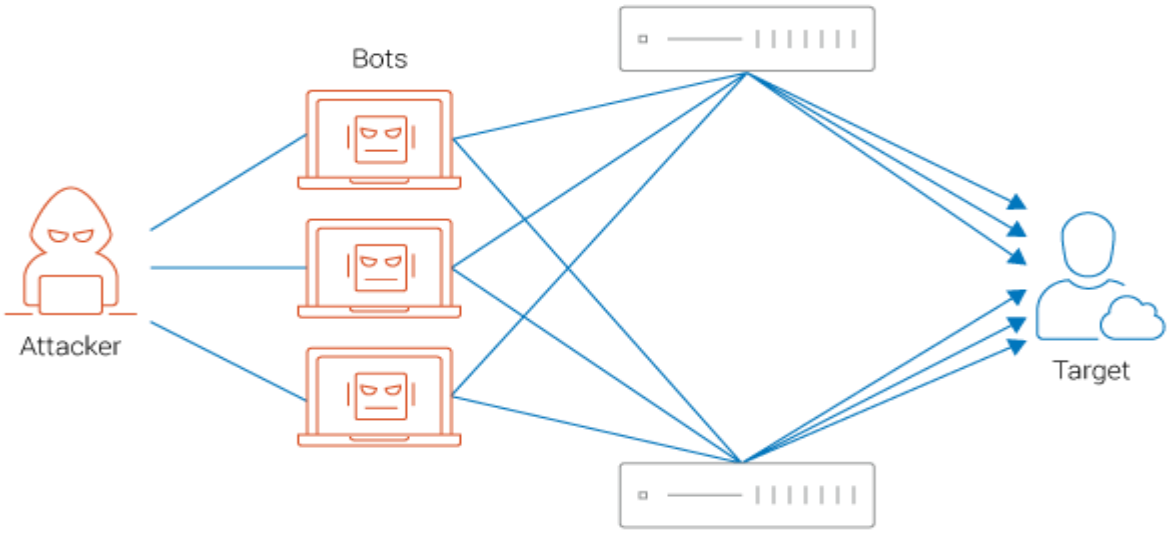

Fig.4.2: Ddos Attack

4.1.2.b. SYBIL ATTACK

A **Sybil Attack** is an attack occurring in peer-to-peer networks where the network operates multiple identities at the same time and undermines the authority/power in reputation systems. The objective of the attack is to gain the majority of influence in the network to carry out illegal actions in the system. A computer has the capability to create and operate multiple identities. To outsiders, these fake identities seem to be real. [99]

The name 29ybil comes from a book by the same name. Written by Flora Rheta Schreiber in 1973, the novel explores the treatment of Sybil Dorsett, a women diagnosed with dissociative identity disorder. The name was suggested by John R. Douceur, a Microsoft researcher, in 2002.

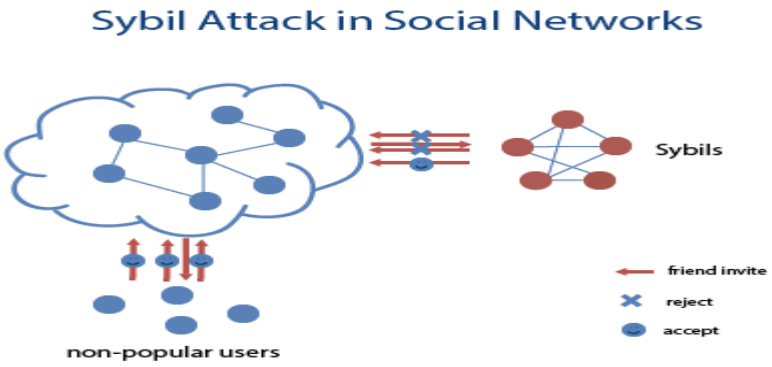

Fig.4.3: Sybil Attack

4.1.3. HOW NSA USE DARK WEB

According to a top-secret NSA presentation provided by the whistleblower Edward Snowden, one successful technique the NSA has developed involves exploiting the Tor browser bundle, a collection of programs designed to make it easy for people to install and use the software. The trick identified Tor users on the internet and then executes an attack against their Firefox web browser. The NSA refers to these capabilities as CNE, or computer network exploitation.The first step of this process is finding Tor users. To accomplish this, the NSA relies on its vast capability to monitor large parts of the internet. This is done via the agency's partnership with US telecoms firms under programs codenamed Stormbrew, Fairview, Oakstar and Blarney.

The NSA creates "fingerprints" that detect http requests from the Tor network to particular servers. These fingerprints are loaded into NSA database systems like Xkeyscore, a bespoke collection and analysis tool which NSA boasts allows its analysts to see "almost everything" a target does on the internet.

Using powerful data analysis tools with codenames such as Turbulence, Turmoil and Tumult, the NSA automatically sifts through the enormous amount of internet traffic that it sees, looking for Tor connections.

Last month, Brazilian TV news show Fantastico showed screenshots of an NSA tool that had the ability to identify Tor users by monitoring internet traffic.

The very feature that makes Tor a powerful anonymity service, and the fact that all Tor users look alike on the internet, makes it easy to differentiate Tor users from other web users. On the other hand, the anonymity provided by Tor makes it impossible for the NSA to know who the user is, or whether or not the user is in the US.

After identifying an individual Tor user on the internet, the NSA uses its network of secret internet servers to redirect those users to another set of secret internet servers, with the codename FoxAcid, to infect the user's computer. FoxAcid is an NSA system designed to act as a matchmaker between potential targets and attacks developed by the NSA, giving the agency opportunity to launch prepared attacks against their systems. Once the computer is successfully attacked, it secretly calls back to a FoxAcid server, which then performs additional attacks on the target computer to ensure

that it remains compromised long-term, and continues to provide eavesdropping information back to the NSA.

4.1.3.a. Exploiting the Tor browser bundle

Tor is a well-designed and robust anonymity tool, and successfully attacking it is difficult. The NSA attacks we found individually target Tor users by exploiting vulnerabilities in their Firefox browsers, and not the Tor application directly.

This, too, is difficult. Tor users often turn off vulnerable services like scripts and Flash when using Tor, making it difficult to target those services. Even so, the NSA uses a series of native Firefox vulnerabilities to attack users of the Tor browser bundle.

According to the training presentation provided by Snowden, EgotisticalGiraffe exploits a type confusion vulnerability in E4X, which is an XML extension for Javascript. This vulnerability exists in Firefox 11.0 – 16.0.2, as well as Firefox 10.0 ESR – the Firefox version used until recently in the Tor browser bundle. According to another document, the vulnerability exploited by EgotisticalGiraffe was inadvertently fixed when Mozilla removed the E4X library with the vulnerability, and when Tor added that Firefox version into the Tor browser bundle, but NSA were confident that they would be able to find a replacement Firefox exploit that worked against version 17.0 ESR.

4.1.3.b. The Quantum system

To trick targets into visiting a FoxAcid server, the NSA relies on its secret partnerships with US telecoms companies. As part of the Turmoil system, the NSA places secret servers, codenamed Quantum, at key places on the internet backbone. This placement ensures that they can react faster than other websites can. By exploiting that speed difference, these servers can impersonate a visited website to the target before the legitimate website can respond, thereby tricking the target's browser to visit a Foxacid server. In the academic literature, these are called "man-in-the-middle" attacks, and have been known to the commercial and academic security communities. More specifically, they are examples of "man-on-the-side" attacks. They are hard for any organization other than the NSA to reliably execute, because they require the attacker to have a privileged position on the internet backbone, and exploit a "race condition" between the NSA server and the

legitimate website. This top-secret NSA diagram, made public last month, shows a Quantum server impersonating Google in this type of attack.

The NSA uses these fast Quantum servers to execute a packet injection attack, which surreptitiously redirects the target to the FoxAcid server. An article in the German magazine Spiegel, based on additional top secret Snowden documents, mentions an NSA developed attack technology with the name of QuantumInsert that performs redirection attacks. Another top-secret Tor presentation provided by Snowden mentions QuantumCookie to force cookies onto target browsers, and another Quantum program to "degrade/deny/disrupt Tor access". This same technique is used by the Chinese government to block its citizens from reading censored internet content, and has been hypothesized as a probable NSA attack technique.

4.1.3.c. The FoxAcid system

According to various top-secret documents provided by Snowden, FoxAcid is the NSA codename for what the NSA calls an "exploit orchestrator," an internet-enabled system capable of attacking target computers in a variety of different ways. It is a Windows 2003 computer configured with custom software and a series of Perl scripts. These servers are run by the NSA's tailored access operations, or TAO, group. TAO is another subgroup of the systems intelligence directorate. The servers are on the public internet. They have normal-looking domain names, and can be visited by any browser from anywhere; ownership of those domains cannot be traced back to the NSA.

However, if a browser tries to visit a FoxAcid server with a special URL, called a FoxAcid tag, the server attempts to infect that browser, and then the computer, in an effort to take control of it. The NSA can trick browsers into using that URL using a variety of methods, including the race-condition attack mentioned above and frame injection attacks. FoxAcid tags are designed to look innocuous, so that anyone who sees them would not be suspicious. An example of one such tag [LINK REMOVED] is given in another top-secret training presentation provided by Snowden.There is no currently registered domain name by that name; it is just an example for internal NSA training purposes.The training material states that merely trying to visit the homepage of a real FoxAcid server will not result in any attack, and that a specialized URL is required. This URL would be created by TAO for a specific NSA operation, and unique to that operation and target. This allows the FoxAcid server to know exactly who the target is when his computer contacts it.

According to Snowden, FoxAcid is a general CNE system, used for many types of attacks other than the Tor attacks described here. It is designed to be modular, with flexibility that allows TAO to swap and replace exploits if they are discovered, and only run certain exploits against certain types of targets. The most valuable exploits are saved for the most important targets. Low-value exploits are run against technically sophisticated targets where the chance of detection is high. TAO maintains a library of exploits, each based on a different vulnerability in a system. Different exploits are authorized against different targets, depending on the value of the target, the target's technical sophistication, the value of the exploit, and other considerations. In the case of Tor users, FoxAcid might use EgotisticalGiraffe against their Firefox browsers.

According to a top-secret operational management procedures manual provided by Snowden, once a target is successfully exploited it is infected with one of several payloads. Two basic payloads mentioned in the manual, are designed to collect configuration and location information from the target computer so an analyst can determine how to further infect the computer. These decisions are made in part by the technical sophistication of the target and the security software installed on the target computer; called Personal Security Products or PSP, in the manual. FoxAcid payloads are updated regularly by TAO. For example, the manual refers to version 8.2.1.1 of one of them. FoxAcid servers also have sophisticated capabilities to avoid detection and to ensure successful infection of its targets. The operations manual states that a FoxAcid payload with the codename DireScallop can circumvent commercial products that prevent malicious software from making changes to a system that survive a reboot process. The NSA also uses phishing attacks to induce users to click on FoxAcid tags.TAO additionally uses FoxAcid to exploit callbacks – which is the general term for a computer infected by some automatic means – calling back to the NSA for more instructions and possibly to upload data from the target computer. According to a top-secret operational management procedures manual, FoxAcid servers configured to receive callbacks are codenamed FrugalShot. After a callback, the FoxAcid server may run more exploits to ensure that the target computer remains compromised long term, as well as install "implants" designed to exfiltrate data.

CHAPTER – 5

5.1. REVIEW OF LITERATURE

A major initial challenge of performing a literature review includes identifying and structuring the most relevant literature surrounding the topic. The primary approach taken for this included performing a keyword search with filters in major databases, going backwards and forward, i.e. reviewing citations for key articles, and reviewing material which cites those key articles, respectively [83]. A PAFMRQ-style analysis [84] was conducted on the topic to better articulate the task at hand (Appendix 6.1). Search engines which index academic content from databases and journals were used to search for literature. The two primary sources used for this were *EBSCOHost*[1] via the University of Melbourne's library services and *Google Scholar*[2].

The identification process, described below, was adapted from Mathiassen et al. (2007). The broad keywords used for the searches initially included "dark web" or "darknet" as these represented the main idea under investigation. Once Tor was determined to be the most popular version of the dark web, "tor" and "tor hidden services" were added to the keyword list. The search was also restricted to contain articles only published in the last five years, i.e. 2013-current. Due to the results being broad in nature, a random selection of papers was reviewed, and key themes of research around the dark web identified. From these, the themes of interest were then searched for specifically along with the main keyword ("dark web") by adding keywords like "markets", "cybercrime", future", "tor hidden services", "incident response", "information warfare" and "threat intelligence" one at a time. These additional keywords were used to allow a more detailed discussion on each aspect of the topic. This keyword search was completed on 13th April 2018 and a list of 151 journal articles, books and theses was compiled.

From the list, papers published in leading journals were identified via the use of *Computing Research & Education* Journal Portal [85] and *ACPHIS* Journal Ranking [86]. However, such papers were a small minority (<10%). Overall, there is limited availability of research which focuses on the dark web itself, and not just mentions it in passing. This may be due to multiple reasons, and the restrictive nature of the topic which makes it difficult to collect data on is speculated to be one of them. By nature, Tor Hidden Services are not indexed on a search engine which makes it necessary to

manually compile a list of '.onion' addresses before they can be crawled. Additionally, users of the dark web are by nature anonymous which makes it difficult to collect data about them e.g. geography. While the Tor Metrics project does present numerical data around Tor's usage, details of the traffic flows remain unknown. These two limitations: lack of collectible metadata and unindexed web content, in combination with behavior software required to access the network, make the dark web not a well-researched, or published, topic in academic literature.

The list was then used to populate a concept matrix based on a brief reading of each article. Papers were then manually filtered for stronger relevance by selecting only those which focused on the dark web and not merely considered it as a peripheral relevance. This resulted in 41 articles in the final list.

CHAPTER – 6

6.1. PRESENT INVESTIGATION

6.1.1. DISCUSSION OF LITERATURE

The internet has become the basis for a global online community of people from all over the world interacting with each other on a scale and a rate unprecedented in history. It has enabled the formation of a global digital society that transcends boundaries, be they nationalities, legal jurisdictions, race, religion, and others. This society, despite its amorphous nature, still constitutes of individuals bound by the laws of their country and similar restrictions. The governments have policies in place which allow for prosecution of said individuals if they were to participate in illegal behavior. For example, file sharing of illegal or copyrighted content online could be considered a breach of law and could result in legal prosecution of the people involved. This is possible because online identities, mainly IP addresses, are linked to the individuals or websites who possess them. In the case of a home desktop computer, the IP address assigned to it by the Internet Service Provider (ISP) is logged as such under the account holder's identity. This IP address is also logged by any service requested from that computer, e.g. by a news website. When this level of logging and accountability is extrapolated across the web, and internet, attribution for most activities conducted online – without precaution – is easy to perform especially for law enforcement as they can either monitor traffic on their own or request logs from those who possess them. Even companies which store our data privately must comply with the rule of law and hand over personal data if subpoenaed under a valid warrant.

6.1.2. Sites Where Never Visit

As per our investigation we are found several sites where we should never visit. Disgusting websites visit and please just don't go there in at.

6.1.2.a. reddit.com

websites never visit: I'm sad to say this exists is reddit.com / watch people die so this is totally sick and what is worrying is that there are over a hundred and twenty thousand subscribe to readers to this subredit.

Here is a place that uses come to find video footage of people as they die the number one rule of the subredit is I quote there must be a person not an animal actually dying in the link pretty self-explanatory moderators can and will remove posts at their own discretion.

If it apparent that no one die in your submission so, one example of a post here is a man who was crush in a scooter accident his beating heart can be seen boys are extremely disturbing is that you can also post request as to the type of death you would like to see next.

So ultimately I find all of this I'll bit much and I really don't think that any of you guys should visit any of these websites there yeah not nice do you guys have any suggestions of websites that we should stay away from let me know in the comments section down below.

Fig.6.1: reddit.com

6.1.2.b. The Death Clock

Fig.6.2: The Dead Clock

I don't care what kind of stuff some of you may believe in, but I refuse to believe that a computer generated random response death clock can accurately predict the date of my death. I don't even want to know the date of my death even if it is accurate. The website Death clock claims to be able to accurately predict the date that you're going to die. This can be psychologically very distracting and you should never engage in this type of crazy stuff.

6.1.2.c. Magic 8 Ball

Fig.6.3: Magic 8 Ball

A lot like the Death Clock, the magic 8-ball pretends to be able to guide your life. So it's basically you give 8 balls a good shake and ask a question like does he like me? And the ball gives you an

answer on the basis of that. Sources say that all of your dreams are literally crushed. You shake again and you get a completely different answer. So this is basically a lot like the prediction that can help you to take decisions at times. It can get very creepy, for example, I asked if he knows where I live and it can answer 'Yes'.

6.1.2.d. Take This Lollipop

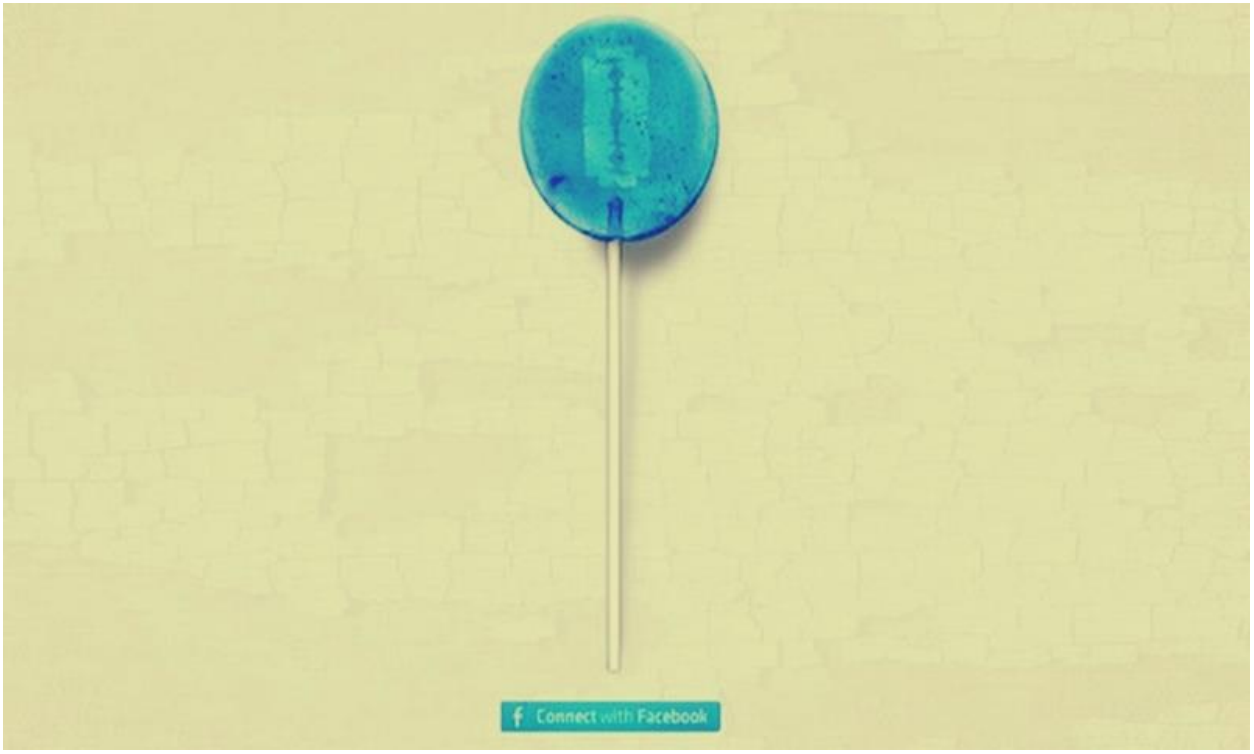

Fig.6.4: Take This Lolipop

The website 'Take This Lollipop' dares you to take a shiny blue lollipop. But by taking the lollipop, you share your Facebook details with the site. You're then greeted with a really creepy corridor followed by an even creepier guy browsing your Facebook photo and messages. He's very sweaty for some reason or another and his fingers are kind of gross. He seems to be getting a sick tortured pleasure from creeping you. He then gets up and gets in his car to find you and creep you in real life. The video then ends with a red lollipop with a razor in it. Now the whole thing is actually a propaganda film to warn people of the dangerous results of sharing too much detail on the Internet.

6.1.2.e. Rotten.com

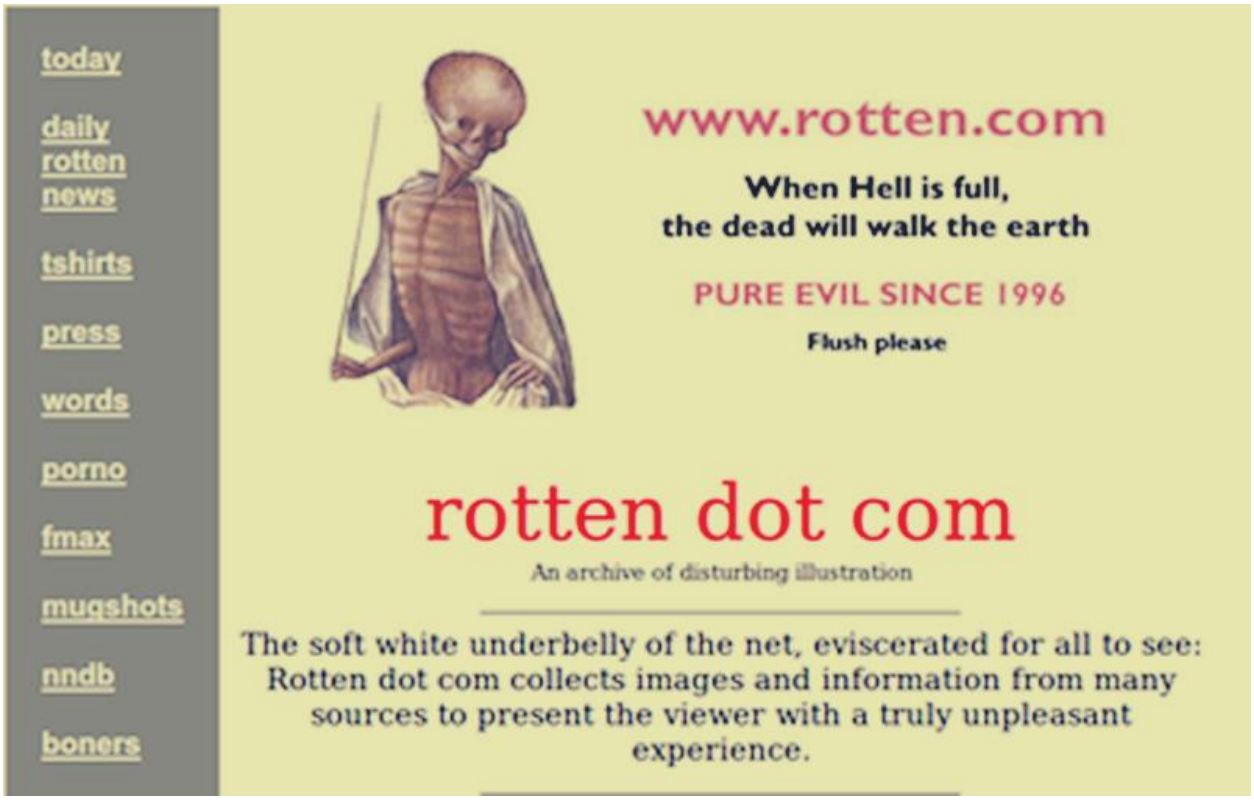

Fig.6.5 Rotten.com

Rotten.com is one of those websites that contains very disturbing content on their website. This site is not safe for work and contains all the things that are not to be seen. It includes extreme knife fights and other disturbing things. Our advice would be that you should better keep yourself away from these kinds of websites. Rotten . Com appears to those with a morbid sense of curiosity the site reads the soft white underbelly of the net eviscerated for all to see rotten. Com collect images and information from many sources to present.

The viewer with a truly unpleasant experience for example you can browse pictures of dismemberment severed hands knife fights disembowelment it all gets pretty gross and category is not safe for work / life in general why would you look at that stuff doesn't get worse unfortunately yes.

6.1.2.f. Rate My Poo

Fig.6.6: Rate My Poo

Unfortunately, this is one that I really wish I had never seen. I'm not sure I'm ever gonna forget it or not. Rate my poo is a website where you literally do just that. You have to rate other people's poos and get them to rate yours. Basically, you take a picture of it, upload it and people can give it a score of out of 10. There are a few people who would actually really enjoy this site. This is really a disgusting thing to visit on the internet.

6.1.2.g. 4 Chan

Fig.6.7: 4 Chan

4 Chan is generally a much darker and more anonymous version of Reddit. It does get pretty dark and I would absolutely recommend that you should be well clear of it. On 4 Chan, anything goes which is kind of the problem and you literally don't know what you're going to find? Someone may be leading a group of idiots into microwaving their new iPhones whilst another will be posting a picture of a freshly murdered body. So, you don't actually need to go on there to see and do bad things. Not all 4 Chan users are the devil but unfortunately, the anonymity of the site has allowed for nude celebrity picture leaks, child porn, animal abuse, threats of violence and cyber bullying. I would suggest you stay away from this website.

6.1.2.h. Silk Road

Fig 7.8: Silk Road

So to be honest, you'll probably never find yourself here. Silk Road is a dark web website that allows you to buy and sell drugs as well as if the allegations are true, you can hire a hitman to kill people on your behalf. The initial Silk Road which labeled itself as an anonymous marketplace was created by William Albrecht and was run on to offer hidden services. So, users could browse anonymously. The FBI later seized the site and Silk Road 2.0 was created and then shut down again. So, there is still a Silk Road but you should better stay away from it.

6.1.2.i. Ever.com

Fig.6.9: Ever.com

we have the world's worst website ever.com. I mean does what it says on the tin warning websites you should never visit.

If you like nice smooth user-friendly slickly designed websites. Or if you're epileptic the world's worst website ever.

We figured out the internet I would say check this out. But really just save yourself during its kind of horrible. There whimsically scrolling text color words.

6.1.2.j. Bluewaffle.net

we have blue waffle.net want to see a picture of an infected gangrenous looking moist lady part no.

I thought not probably then don't visit blue waffle.net so what is the vilest of all of the websites that you should never visit guess it's kind of hard to pick but this next one really made me the saddest.

6.2. Other Browser We Can Access Dark Web

6.2.1. I2P – Invisible Internet Project

Fig.6.10: I2P

Unlike TOR browser, I2P or Invisible Internet Project is a bundled package that offers a wide range of different services. The I2P program lets you access the web through a layered data stream to protect your identity.

The connection through I2P is fully encrypted with both public and private keys. The browser uses TCP / UDP and IP data transfer protocols to protect your online activity and uses them to encrypt all the data and internet traffic.

I2P builds a separate network to allow the users to access the internet. It helps I2P control the internet traffic and data and the second layer of the Internet remains hidden and private. The anonymous overlay network protects all the activity from being tracked by dragnet surveillance or ISP monitoring.

The USP of I2P is the decentralized file storage system and distributed network database. It uses the “Darknet” technology. Remember, I2P is a growing network and it grows stronger day by day as the network expands. So, it is your best bet if you don’t want to opt for TOR right now.

6.2.2. Whonix

Fig.6.11: Whonik

Whonix is a dark web browser built on TOR's free software. Anonymity and privacy are the key factors to access deep web content and Whonix provides that via open and distributed relay network powered by TOR.

TOR ensures that the connections are fool-proof and eliminates any DNS leaks whatsoever. The connections through TOR make Whonix so powerful that even malware with root privileges can't track down the user's real IP address.

The best part about Whonix is that it's not only a deep web browser but also a fully functional operating system where you can setup and manage your own server without getting traced. Many popular applications are already pre-configured and installed for immediate use.

Whonix is the only operating system designed to run on a VM paired with TOR. One of the best highlights of Whonix is the "Data Stream Isolation" feature. Although it is paired with TOR, the chances of identity correlation are near to impossible as Whonix doesn't utilize the same exit-relays and circuits by TOR.

6.2.4. Subgraph OS

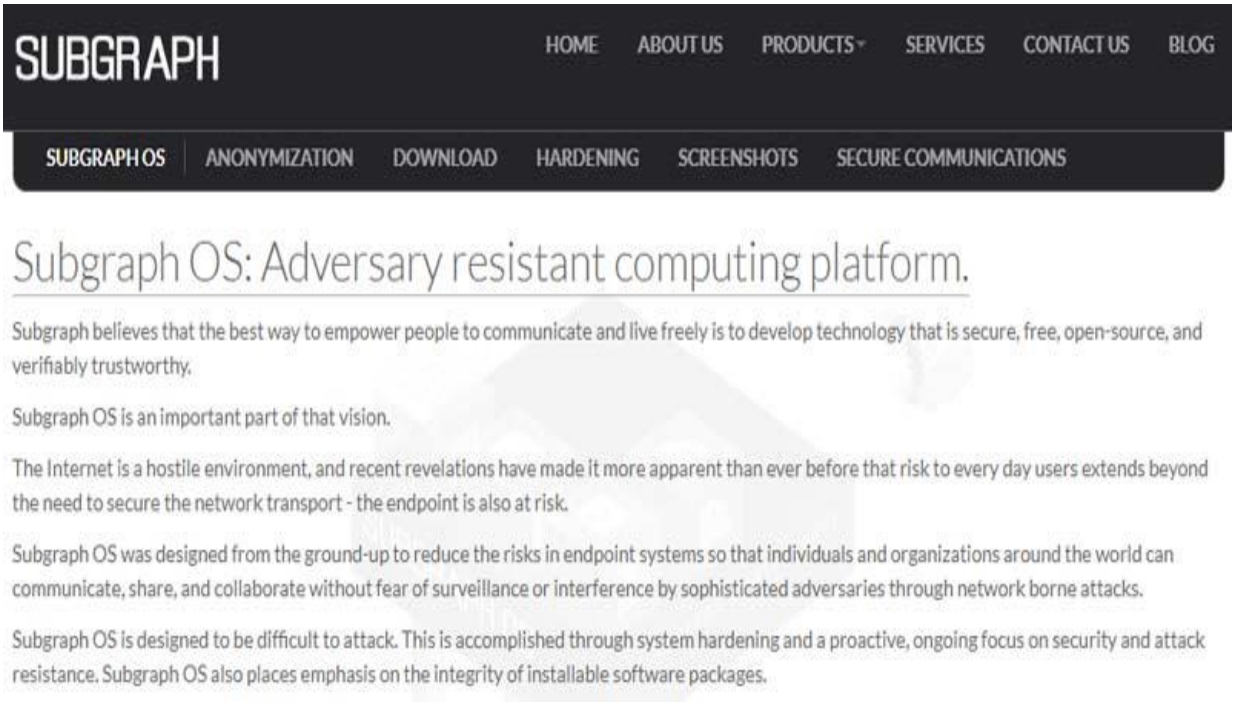

Fig.6.12: Subgraph OS

Here's another open-source deep web browser based on TOR project. Subgraph OS is not really a standalone browser but a complete operating system just like Whonix. The main idea behind Subgraph OS is to provide a free, private, and secure environment for users to access the entire World Wide Web.

Subgraph OS is built on different layers to help users with a streamlined access to the internet without hindering their privacy or compromising the security. The open-source platform uses Kernal Hardening, Filesystem encryption, and Metaproxy to build a hardening layer to their network.

If that's not enough, the program is further protected by container isolation. It sandboxes each instance that contains any malware before entering the network. Subgraph OS also features a custom-coded IM and Email client to eliminate other vulnerabilities as well. Some other added security layers include Package Security, Binary Integrity, etc.

With so many secured layers to protect your online activity, Subgraph OS is definitely one of the best dark web browsers on the internet.

6.2.5. TAILS – The Amnesic Incognito Live System

Fig.6.13: TAILS – The Amnesic Incognito Live System

Like every other dark web browsers mentioned above, TAILS also secures its connections using TOR network. TAILS, an acronym for The Amnesic Incognito Live System, is a live operating system designed to ensure privacy and anonymity to its users.

You can access this network or OS using a USB stick or a DVD. The program uses the highly advanced cryptographic tools to add an encrypted layer to all the connections. These tools add a protective shield to all the files, emails, and instant messages sent or received by you.

When you boot TAILS OS on your computer, your original OS is temporarily disabled to ensure security. Your computer gets back to normal when you shut down TAILS.

The main highlight of TAILS is the fact that it doesn't require any hard-disk storage or utilize your hard-disk space in any scenario. It only requires RAM power to run the program smoothly and even the virtual memory is neatly cleaned up with every boot or shutdown to ensure that nothing is left behind.

Every connection runs via TOR's distributed layer network and the connection is terminated whenever the connection tries to skip the TOR network. The program was initially created as a counter measure to prevent network surveillance and traffic analysis in order to stop Government to keep a watch on the activities of people and track their personal identities.

Privacy and security on TAILS is brilliant as the program is equipped with some state-of-the-art cryptographic tools which not only protect your privacy but also the USB drive as well.

CHAPTER – 7

7.1. RESULT AND DISCUSSION ACCORDING TO IMPLEMENTATION

Hosting sites on the dark web is free and can be accessed through Tor browser. Since it is hosted on our own computers it cannot be closed. This tutorial will help you to understand how to host ".onion" websites on the dark web. For that first, you need to know about Xampp server and tor browser, without its knowledge you cannot host your website.

3. First download tor browser. Open the folder containing tor and create a new folder with any name, we will name this folder as "tor domain".

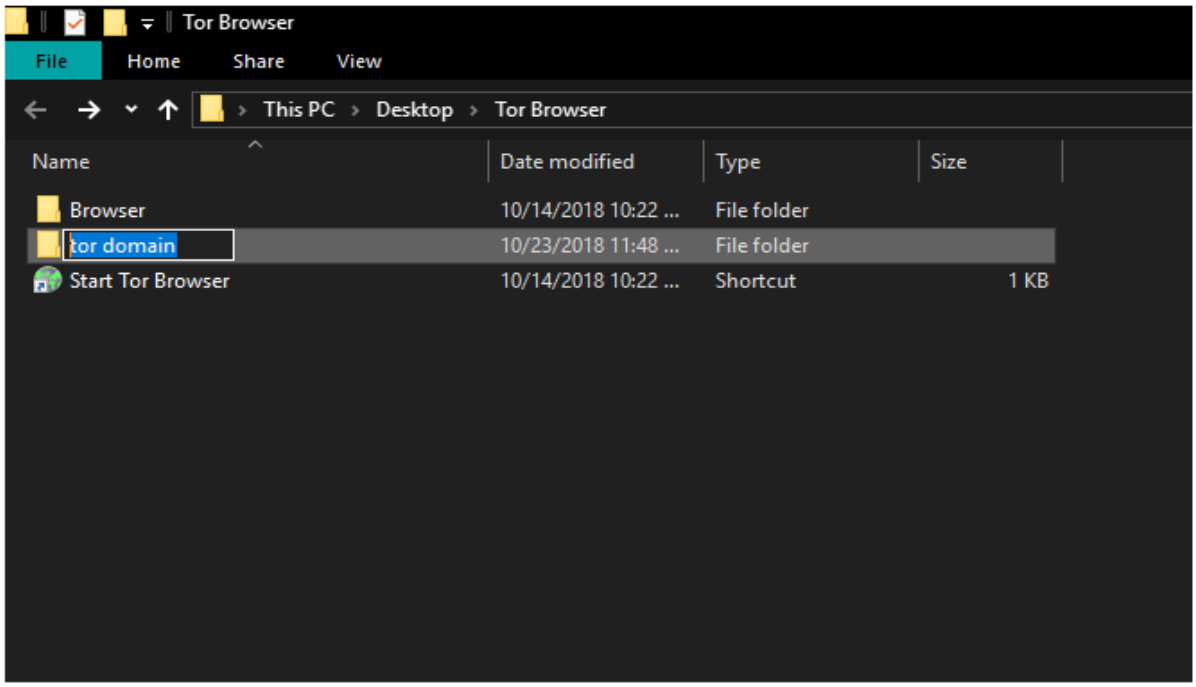

Fig.7.1: Tor Containing Floder

2. Go to the following location as described C:\Users\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor. You should be able to see a file name "torrc".

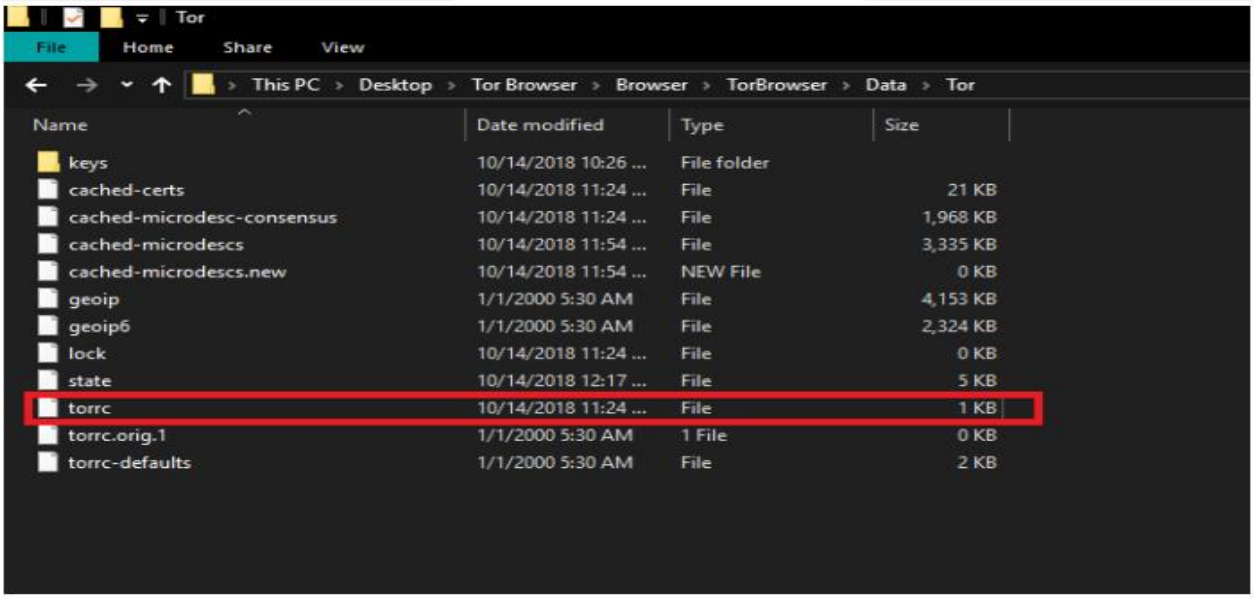

Fig.7.2: Torrc

3. Open that file with notepad or any other text editor and enter the following lines and save it:# Hidden Service

HiddenServiceDir C:<path location of your new folder>(in our case-tor domain folder)

HiddenServicePort 80 127.0.0.1:80

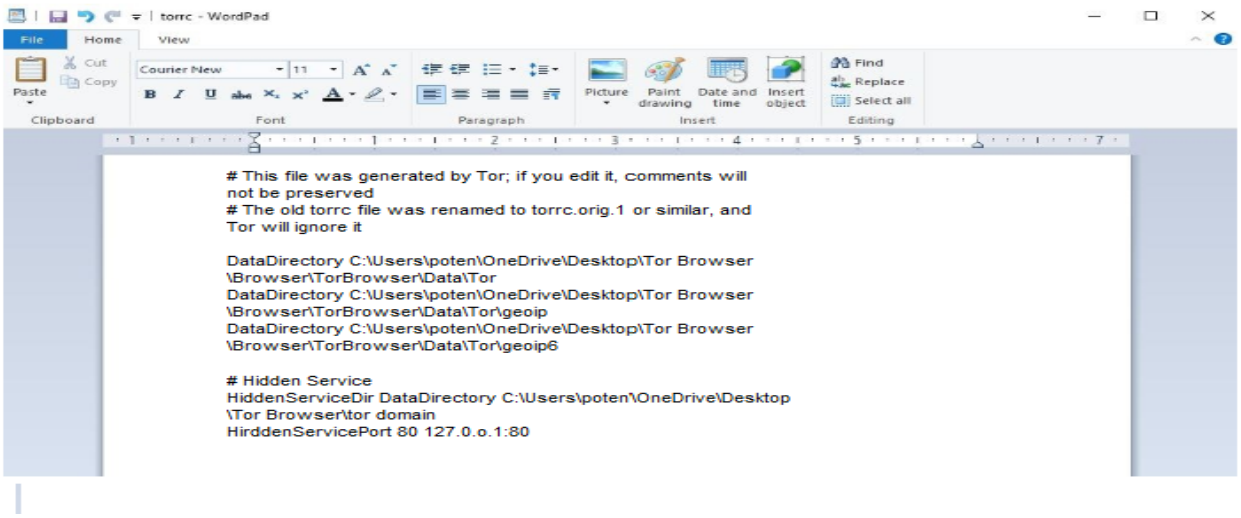

Fig.7.3: Hidden Port

Now close the tor browser and folder.

4. Download XAMPP Server , Run XAMPP server and open the folder where you have installed. Now you should see a folder named “htdocs”.

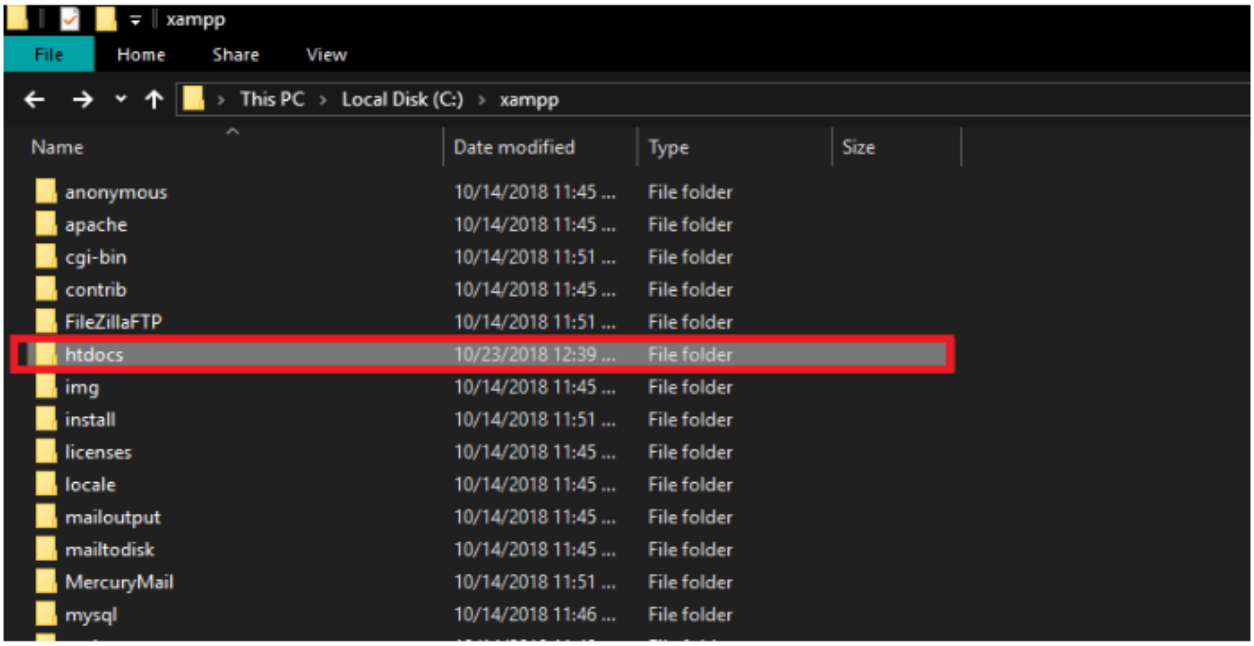

Fig.7.4: Htdocs Folder

Delete everything from that folder and make your HTML webpage there. Save that file with a .html extension and open XAMPP application. All your files related to your webpage should be located in this folder.

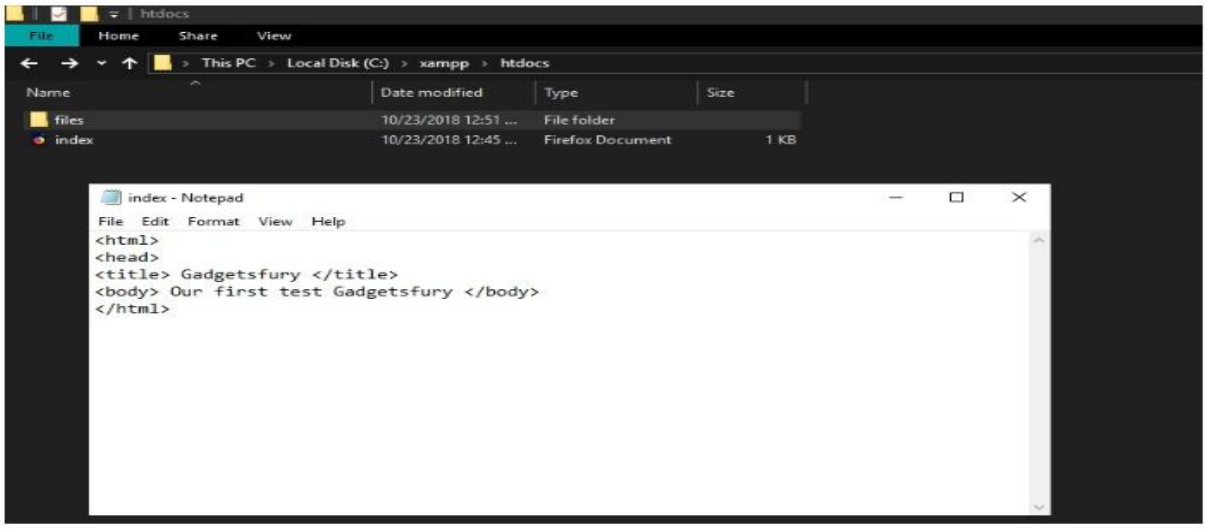

Fig.7.5: Html codes

5. Open the XAMPP application and click start on Apache and MySQL. You have just created a local server!

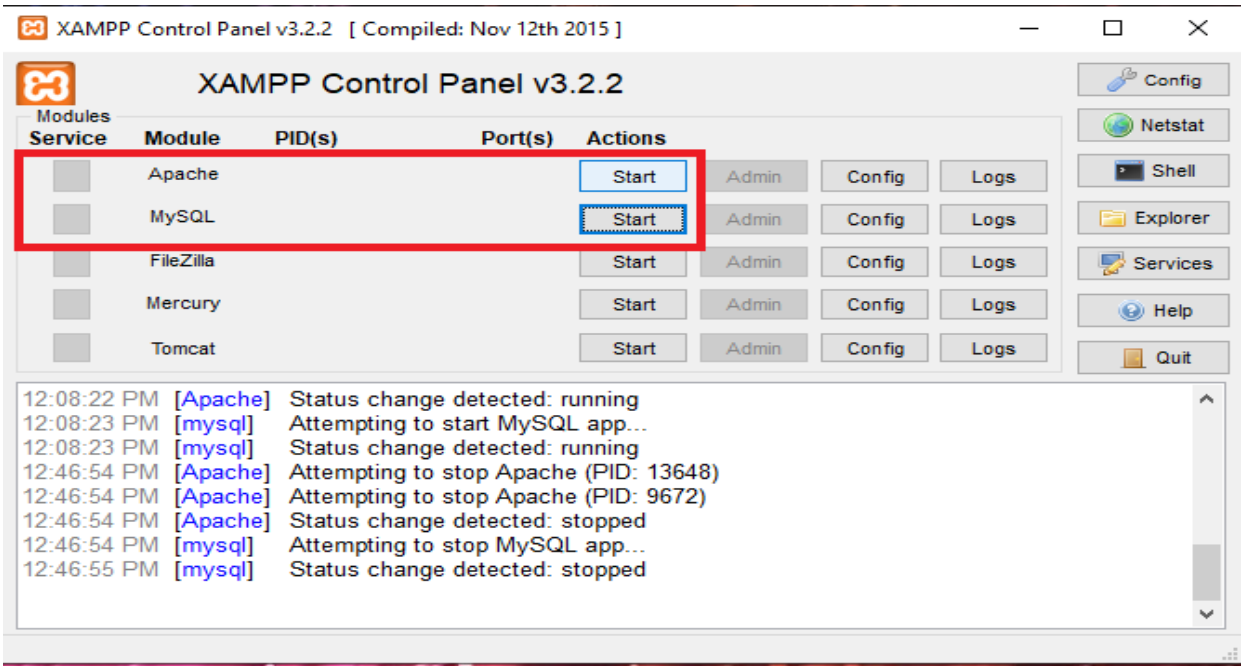

Fig.7.6: Xampp Server

6. Now go to your normal browser and search for your local host. You can also search for 127.0.0.1, this is the IP for localhost.

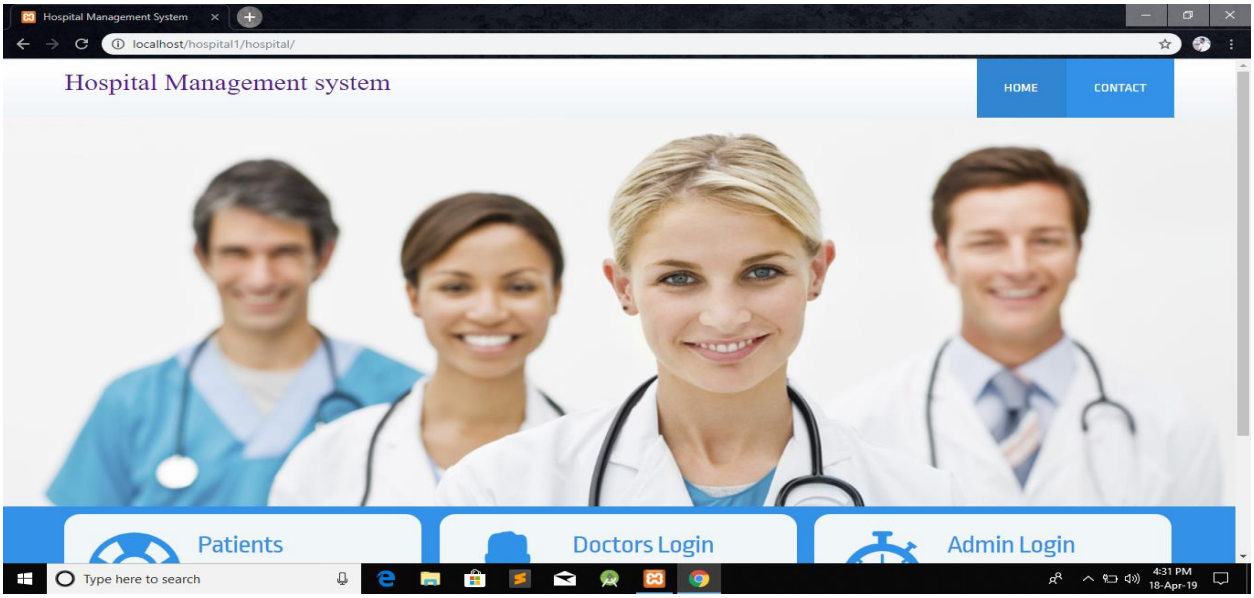

Fig.7.7: 127.0.0.1 IP

For accessing files, type localhost/<name of the folder> or 127.0.0.1/<name of the folder>. In our case the name of the folder was files.

Fig.7.8: Index File

6. Now, let us see how to host it on the dark web and add .onion domain to your site. Open your Tor browser folder again and click “Start tor browser”. Wait for few seconds and your tor browser should open if the steps are followed correctly. After opening close the browser.

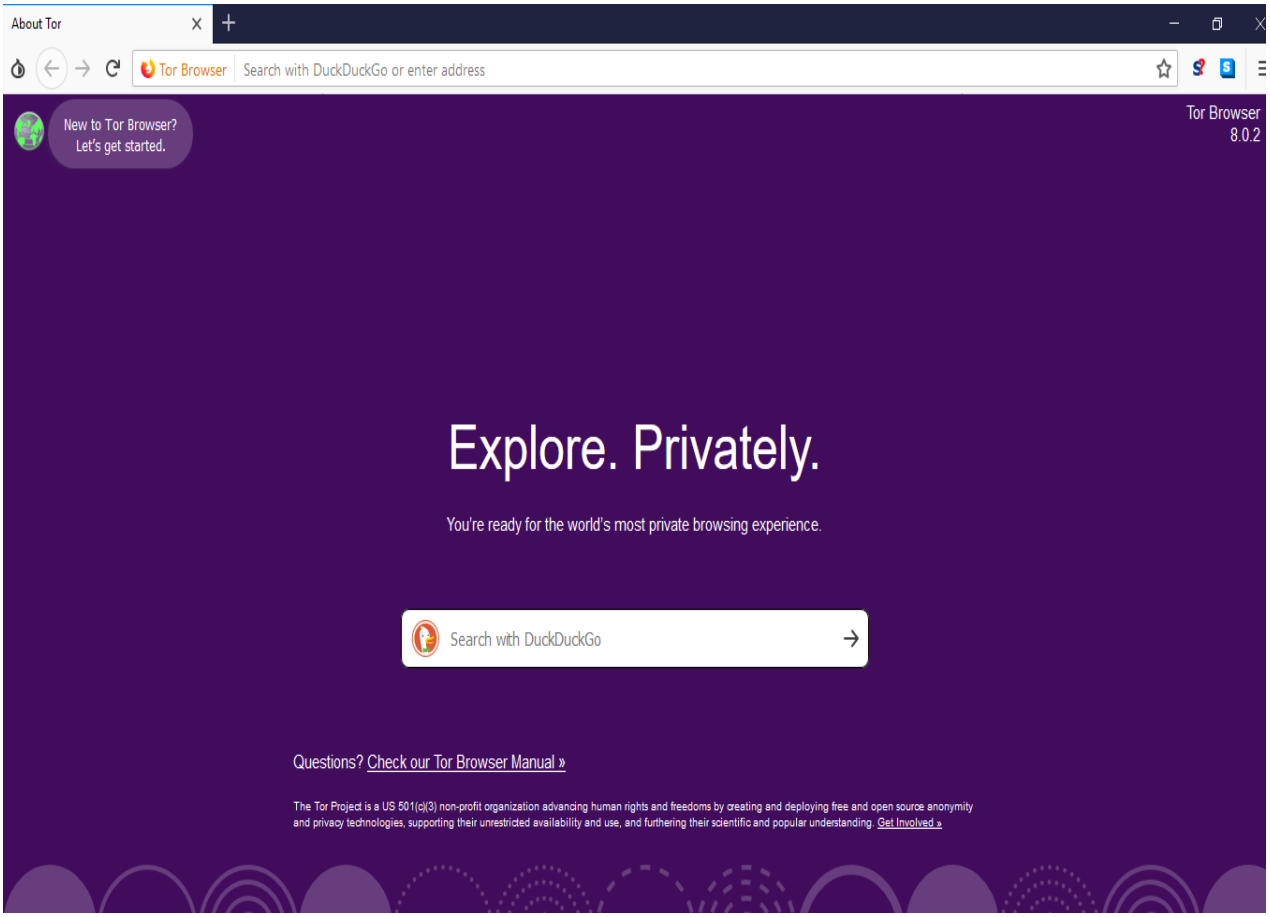

Fig.7.9: Tor Broswer

7. Go to your tor domain folder and there you will see a new file with a name “hostname”. Open this file with notepad and you will get your website URL.

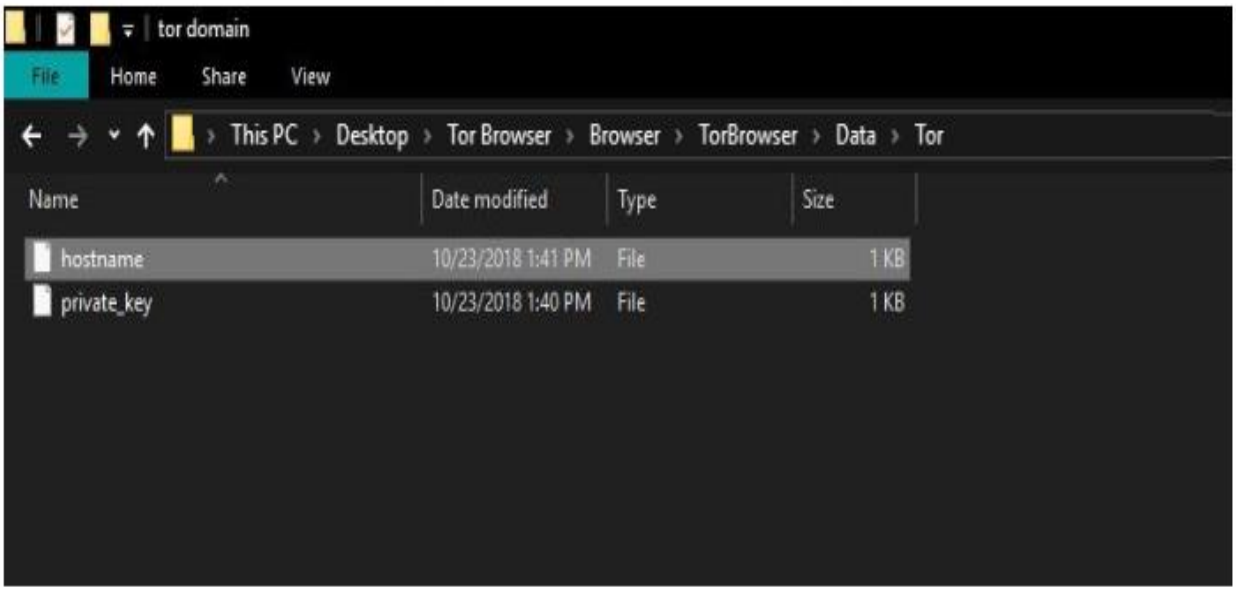

Fig.7.10: Tor Domain

8. Copy this link and open this link on the tor browser. Just make sure your XAMPP server application is running.

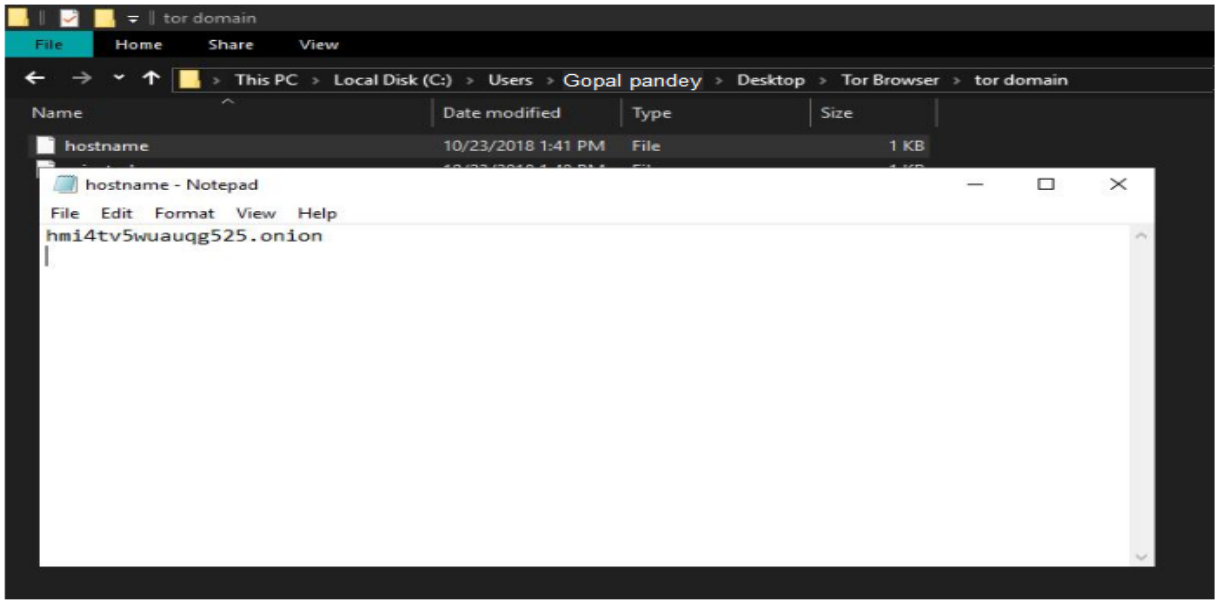

Fig.7.11: Onion Domain

9. Open your link in tor. You have just created a website with .onion extension. And this can be accessed only through tor browser. Your regular browser cannot open this link. Basically, you just hosted your website on the dark web. This site now can be opened from anywhere around the world provided he/she knows this URL.

Fig.7.12: Program On Dark Web

To share files with your friends just add the files in your htdocs folder and add "/files" at the end of your URL. Whatever files you put in that folder will be now downladable. This site can only be accessed as long as your computer stays connected to the internet. To stop this site you have to stop your Xampp server application.

CHAPTER - 8

8.1. MODEL FOR FUTURE RESEACH

Having looked at the literature on the topic of dark web/darknets/tor hidden services, the following research gaps have been identified and proposed.

8.1.1. Enabling Cybercrime: Criminals Dependence on Dark Web

Cybercriminals have benefitted from hidden services by way of being able to buy exploits – including zero-day – from marketplaces, engage with other criminals on forums, host command-and-control (C2) servers for botnets & exfiltration malware, and hire professional criminals or their skills 'as-a-service' [100].The anonymity attribute the dark web confers to its users makes these activities possible and enables cybercriminals to conduct their affairs.

There are various types of cybercrimes and actors present, from the amateur 'script-kiddies' using readily-available tools and exploits to target highly vulnerable systems aka the "low-hanging fruit", to the highly focused and skilled Advanced Persistent Threats (APT) known to be behind significant cases of espionage against large organisations and nation states. The APT phenomenon is known to use zero-day exploits as one of the ways of gaining privileged access to target systems [101]. The creative tactics of APTs poses a significant challenge to even the most mature incident response teams [96]. However, there was no significant literature found explicitly exploring a link between the dark web and APT phenomena, and if investigated it can potentially be exploited in curbing or better defending against cyber-attacks from APTs in the future.

Research questions:

8.1.1.a. Given one of the enabling features of the APT phenomenon is their use of zero-day exploits, and that dark web marketplaces allow trading of said exploits, how significant a role does the dark web phenomenon play in condoning the APT phenomenon?

8.1.1.b. To what extent is the dark web crucial to the success of APT attacks?

8.1.2. Distributed Hidden Services (non-Client-Server model)

Hidden services on the dark web, e.g. '.onion' sites part of, and accessible through, the Tor network make use of the anonymity feature of Tor to keep their location and address private but yet are reachable by interested parties. This strength of theirs makes it challenging for law enforcement to shut them down as their hosting provider and geographical location is hidden. However, as seen in recent cases of darknet marketplaces like Silk Road, Hansa and AlphaBay being shut down they are not impervious to regulation [102]. As a result, marketplace operators, and interested traders, are exploring ways of removing the bottleneck associated with having a centralised marketplace web platform. In these situations when anonymity is not enough, a more distributed implementation is potentially the answer and can be seen in its early stages in the form of multiple new decentralised markets either built on Tor [103] or the blockchain technology [104]. There is scope to utilise the significantly distributed nature of the internet to continue expanding upon the phenomenon. Dark web markets which work on a more distributed model as opposed to a client-server one would become even more resistant to being shut down – OpenBazaar being a recent example.

Research can also be conducted into the scalability of the dark web over time: whether the current internet infrastructure continues to support this phenomenon or become a limiting factor in its usage. Moreover, given that some methods for deanonymization of clients or services rely on controlling sufficient nodes on the Tor network [104], further investigation can be conducted into what level of growth, or user adoption, of Tor is required before these methods become economically infeasible to exploit. This research could help law enforcement reprioritise its approaches for monitoring the dark web.

Research questions:

8.1.2.a. What trends can be observed about existing web infrastructure – especially hidden services moving in the direction of being more decentralised?

8.1.2.b What technological, and other, factors currently affect this transition and how will this affect the scalability and observability of the dark web?

8.1.3. Role & Capability of Law Enforcement

As the medium of communication between people becomes more and more decentralised and thus harder to regulate, it is possible that unethical (and illegal) content will proliferate in a direction that will keep it away from the watchful eye of the law.

Part of current law enforcement operations' focus is on deanonymization of hidden services, of marketplace operators, of site administrators and anyone else involved in the facilitation of a relatively centralised (but anonymous) infrastructure used to conduct illegal activity on the dark web. As technology advances, these elements may become increasingly difficult to track, identify and shut down especially as they cease to exist in their current form [103].

Research questions:

8.1.3.a. What strategies can the law enforcement use to exercise control over the dark web? Are there merits to focus on targeting users, servers or the protocol, e.g. Tor itself?

8.1.3.b How can we, as a society, reduce unethical behaviour, e.g. child sexual abuse, in the presence of a market demand that seems to be forever present combined with markets that are difficult to shut down?

Furthermore, the question of what can be done is separate from what should be done about the technology from a regulatory perspective. The two ideas seem mutually exclusive in their pure forms as promoting the full extent of civil liberties by way of allowing unrestricted and unmonitored access to internet technologies mean illicit activities will likely flourish [106]. However, civil liberties may suffer when policies restricting the use of the surface, or dark, web are brought into existence.

Research question:

8.1.3.c Where on the spectrum of allowing civil liberties vs clamping down on unethical behaviour should the law position itself at?

It is argued that our efforts need to be refocused on initiatives elsewhere in the process, e.g. prosecuting the traders as opposed to facilitators of the marketplace – as this becomes more and more difficult to do with technological advancements. [107] suggests increasing the number of sting operations and focusing on bringing down the source of drugs rather than the marketplace itself as the phenomenon grows over time.

CONCLUSION

The internet can be classified into three different areas – surface, deep and dark – based on their identifiability and accessibility aspect. One of those areas, the dark web (aka darknets), is defined as being that part of the internet which affords anonymity to its users and hosted web services (hidden services). From a technical viewpoint, the dark web is a distributed system and an overlay network which can be accessed via the use of special software. A literature review was conducted into the roles the dark web plays in modern digital society, its enablement of cybercrime and its relationship with law enforcement. Conducting a literature review on this topic was challenging as information available and research conducted on the topic is relatively limited due to its 'secretive' and generic/non- identifying nature. Many hidden services rely on word-of-mouth popularity and certain communities are invite-only with restricted access not just due to payment but reputation in certain communities.

The first research question required investigation of the roles the dark web currently serves. It was revealed that it plays a plethora of roles, more than may seem on the surface. While online marketplaces for illicit drugs are still a major one, they remain one of many; marketplaces for trade of software exploits, forums for discussion amongst special interest groups, cybercriminal infrastructure, extremist recruitment, financial transactions and money laundering are some of the other significant uses. It is also seen to be growing its user base as evidenced by increasing bandwidth and nodes on the network, much of which is to support anonymous browsing of the surface web.

The second research question involved looking at the significance of the dark web to cybercriminal activities and operations. This was found to one of the roles the dark web plays, especially in the case of providing zero-day vulnerabilities thus enabling the APT phenomenon. There is evidence to show that it serves as a training ground for cybercriminals, e.g. APT actors, via discussion boards, hosts infrastructure used to conduct, support and commodify cybercriminal operations in the form of exploit trade, exploit-as-a-service business model, hosting command-and-control servers as Tor Hidden Services, and providing anonymity to

escape legal prosecution for online activity. However, the criticality of this role remains questionable as it may be considered to only lower the barrier to entry into the world of cybercrime. More established and well-resourced actors are purported to use their own private infrastructure, e.g. botnet proxies to anonymise their actions, discovering their own zero-day vulnerabilities and using other means to finance their operations.

Finally, the third research question was about law enforcement curbing illegal activity on the dark web. It was found that law enforcement continues its attempts to close markets responsible for the sale of illicit items, especially recreational drugs. However, the infrastructure reacts to these incidents and attempts to mitigate the vulnerabilities exploited – technical and otherwise – by the authorities. In

response, the Tor protocol is continually updated to fix protocol vulnerabilities, the market operators improve their operational security, the financial backbone – cryptocurrencies – introduces newer and more anonymous variants alongside an increase in money laundering ('tumbling') services, hidden services become more distributed and without a central server that can be seized, and escrow functions are evolving to be based not just on trust but also on cryptographic improvements.

Looking at the evolution of dark web and the increasing user base of Tor, this phenomenon of people congregating together away from interference – legal and otherwise – and judgement to share content, opinions and to trade is likely going to continue developing. People are innovating to come up with even more resilient systems to ensure a 'safe space' for their actions, especially if it is deemed illegal – socially acceptable or not. In the debate on privacy versus security that developed countries are having with their citizens, the technology factor is weighing in stronger than before as it becomes not just a matter of legality but of technical capability to monitor and conduct surveillance on people. It is possible that in the future this debate would be over as technology advances to the point where privacy is not at the mercy of governments but in the hands of users and private corporations. The discussion on this topic then no longer remains in the domain of technology but is one that needs an interdisciplinary contemplation by experts in areas of psychology, sociology, law, and others.

APPENDIX - 6.1

Component	**Definition**	**Specific**
Real-world Problem (**P**)	The problem setting represents people's concerns in a real-world problematic situation	The Dark Web is a component of the Web that is notorious for illicit and anonymous activity, particularly drug trade. The nature of the dark web is surrounded by secrecy. Is the dark web a one-off occurrence in response to something in the real world or is it a manifestation of a broader phenomenon? If it is the latter, it is important to identify characteristics and predict its future if law enforcement wants to keep up.
Area of Concern (**A**)	The area of concern represents some body of knowledge in the literature that relates to P.	- Anonymous overlay networks ('Dark Web') and its documented uses - Information security and its affiliation with the Dark Web
Framework (**F**)	The conceptual framing helps structure collection and analyses of data from P to answer RQ; FA draws on concepts from A, whereas FI draws on concepts independent of A.	- dark web as a phenomenon, not just a haven for drug-buyers - dark web as an unregulated free market, an online version of the black market - dark web as a private space for individuals to engage with others

Methodology (**M**)	The method details the approach to empirical inquiry, specifically to data collection and analysis.	Literature review on 'Dark Web', 'Darknets' and 'Tor hidden services' via Google Scholar and EBSCOHost. A
		concept-centred approach to analysing the literature.
Research Question (RQ)	The research question relates to P, opens for research into A, and helps ensure the research design is coherent and consistent.	- What is the dark web used for? - What activities does the dark web harbour other than trade of illicit drugs? - How is the dark web dealing with the law enforcement being an adversary? - Can the Dark Web be considered a phenomenon and if so what projections can be made about its future?
Contributions (C)	Contributions influence P and A, and possibly also F and M.	Ca: identify gaps in research and propose a research agenda to improve knowledge about the nature, future and control of the dark web.

Table 1: PAFMRQ analysis of current work

REFERENCES

1. Greenberg, Andy (19 November 2014). "Hacker Lexicon: What Is the dark web?".
2. Egan, Matt (12 January 2015). "What is the dark web? How to access the dark website – How to turn out the lights and access the dark web (and why you might want to)". Archived from the original on 19 June 2015. Retrieved 18 June 2015.
3. Solomon, Jane (6 May 2015). "The Deep Web vs. The dark web". Archived from the original on 9 May 2015. Retrieved 26 May 2015.
4. Greenberg, Andy (19 November 2014). "Hacker Lexicon: What Is the dark web?". Wired. Archived from the original on 7 June 2015. Retrieved 6 June 2015."Clearing Up Confusion – Deep Web vs. dark web". BrightPlanet. 2014-03-27. Archived from the original on 2015-05-16.
5. NPR Staff (25 May 2014). "Going Dark: The Internet Behind The Internet". Archived from the original on 27 May 2015. Retrieved 29 May 2015.
6. The dark web Revealed. Popular Science. pp. 20–21
7. Greenberg, Andy (19 November 2014). "Hacker Lexicon: What Is the dark web?". Wired. Archived from the original on 7 June 2015. Retrieved 6 June 2015.
8. "Clearnet vs hidden services – why you should be careful". DeepDotWeb. Archivedfrom the original on 28 June 2015. Retrieved 4 June 2015.
9. Chacos, Brad (12 August 2013). "Meet Darknet, the hidden, anonymous underbelly of the searchable Web". Archived from the original on 12 August 2015. Retrieved 16 August2015.
10. "Redefining light and dark". Gondwanaland.com. November 28, 2005.
11. Barratt, Monica (January 15, 2015). "A Discussion About Dark Net Terminology". Drugs, Internet, Society. Retrieved June 14, 2015.
12. "What is the difference between the Surface Web, The Deep Web and the Dark Web?". Pink Hat Technology Management. Retrieved 2018-09-29.
13. "The Surface Web". Dark Side of the Web. 2012-05-11. Retrieved 2018-09-29.
14. de Kunder, Maurice (June 14, 2015). "The Size of the World Wide Web". WorldWideWebSize.com. Retrieved June 14, 2015.

15. Hamilton, Nigel. "The Mechanics of a Deep Net Metasearch Engine". CiteSeerX 10.1.1.90.5847.
16. Devine, Jane; Egger-Sider, Francine (July 2004). "Beyond google: the invisible web in the academic library". The Journal of Academic Librarianship. **30** (4): 265–269. doi:10.1016/j.acalib.2004.04.010. Retrieved 2014-02-06.
17. Raghavan, Sriram; Garcia-Molina, Hector (September 11–14, 2001). "Crawling the Hidden Web". 27th International Conference on Very Large Data Bases.
18. "Surface Web". Computer Hope. Retrieved June 20, 2018.
19. **a** **b** Wright, Alex (2009-02-22). "Exploring a 'Deep Web' That Google Can't Grasp". The New York Times. Retrieved 2009-02-23.
20. Madhavan, J., Ko, D., Kot, Ł., Ganapathy, V., Rasmussen, A., & Halevy, A. (2008). Google's deep web crawl. Proceedings of the VLDB Endowment, 1(2), 1241–52.
21. Shedden, Sam (June 8, 2014). "How Do You Want Me to Do It? Does It Have to Look like an Accident? – an Assassin Selling a Hit on the Net; Revealed Inside the Deep Web". Sunday Mail. Retrieved May 5, 2017 – via Questia. (Subscription required (help)).
22. Li, Bingdong; Erdin, Esra; Güneş, Mehmet Hadi; Bebis, George; Shipley, Todd (14 June 2011). "An Analysis of Anonymity Usage". In Domingo-Pascual, Jordi; Shavitt, Yuval; Uhlig, Steve. Traffic Monitoring and Analysis: Third International Workshop, TMA 2011, Vienna, Austria, April 27, 2011, Proceedings. Berlin: Springer-Verlag. pp. 113–116. ISBN 978-3-642-20304-6. Retrieved 6 August 2012.
23. "Tor Project: FAQ". www.torproject.org. Retrieved 18 January 2016.
24. "Tor Network Status". Retrieved 14 January 2016.
25. Glater, Jonathan D. (25 January 2006). "Privacy for People Who Don't Show Their Navels". The New York Times. Retrieved 13 May 2011.
26. PATRICK KINGSLEY (June 10, 2017). "Turks Click Away, but Wikipedia Is Gone". The New York Times. Retrieved June 11, 2017.
27. Rocky Termanini (5 March 2018). The Nano Age of Digital Immunity Infrastructure Fundamentals and Applications: The Intelligent Cyber Shield for Smart Cities. CRC Press (Taylor & Francis Group). pp. 210–211. ISBN 978-1-351-68287-9.

28. Bennett, Cory (2015-04-04). "Private 'darknet' markets under siege". Retrieved 15 May 2015.
29. DeepDotWeb (2013-10-28). "Updated: List of Dark Net Markets (Tor & I2P)". Retrieved 17 May 2015.
30. Winder, Davey (21 Apr 2015). "Is this new zero-day dark market the real deal?". Retrieved 17 May 2015.
31. van Hardeveld, Gert Jan; Webber, Craig; O'Hara, Kieron (2017). "Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets". American Behavioral Scientist. **61** (11): 1244–1266. doi:10.1177/0002764217734271.
32. Whitaker, Ross (14 July 2015). "Why I Had to Buy My Wife's Inhaler on the Dark Web". Retrieved 14 July 2015.
33. Plenke, Max (18 May 2015). "Inside the Underground Market Where Bodybuilders Find Dangerous, Illegal Steroids". Retrieved 5 September 2015.
34. Bartlett, Jamie (5 October 2014). "Dark net markets: the eBay of drug dealing". Retrieved 17 May 2015.
35. Mark, Ward (30 December 2014). "Tor's most visited hidden sites host child abuse images". Retrieved 28 May 2015.
36. Gayle, Damien (11 February 2016). "Online market 'is turning drug dealers from goons to geeks'". Retrieved 13 February 2016.
37. DeepDotWeb (2013-10-28). "Updated: List of Dark Net Markets (Tor & I2P)". DeepDotWeb.
38. DeepDotWeb (17 May 2014). "A Sneak Peek To Grams Search Engine "Stage 2: Infodesk"". Retrieved 8 August 2015.
39. Aldridge, Judith (2017). "Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement". International Journal of Drug Policy. **41**: 7. doi:10.1016/j.drugpo.2016.10.010
40. J Martin, Alexander (24 July 2015). "Global drug-dealing cyber crime web was centred on ... Aberdovey". Retrieved 8 August 2015.
41. "Cheltenham drug user who bought cannabis on 'dark web' with Bitcoin was caught by Home Office". Gloucestershire Echo. 21 May 2016. Retrieved 28 May 2016.

42. Normann, Claus; Berger, Mathias (November 2008). "Neuroenhancement: status quo and perspectives" (PDF). European Archives of Psychiatry and Clinical Neuroscience. **258**: 110–114. doi:10.1007/s00406-008-5022-2. PMID 18985306.
43. Woolf, Nicky (31 May 2015). "Silk Road sentencing: why governments can't win the war on darknet drugs". The Guardian. Retrieved 30 December 2016.
44. Valette, Jean-Jacques. "Du commerce illicite à la liberté d'expression totale, on a plongé dans le darknet". We Demain. Retrieved 30 December 2016.
45. Holt, Thomas J.; Smirnova, Olga; Chua, Yi-Ting (2016). Data thieves in action : examining the international market for stolen personal information. Palgrave Macmillan. ISBN 978-1-137-58904-0.
46. "The Value of Stolen Data on the Dark Web". Dark Web News. 1 July 2017.
47. Rossi, Ben (8 July 2015). "The ripple effect of identity theft: What happens to my data once it's stolen?". Information Age.
48. "The Dark Net: Policing the Internet's Underworld". World Policy Journal. **32**.
49. G, Joshua (20 April 2015). "Interview With AlphaBay Market Admin". Retrieved 21 August 2015.
50. Hall, Kat (16 December 2015). "At least 10 major loyalty card schemes compromised in industry-wide scam". Retrieved 16 December 2015.
51. Cox, Joseph (9 July 2015). "The Dark Web's Biggest Market Is Going to Stop Selling Guns". Retrieved 26 July 2015.
52. Cox, Joseph (July 21, 2015). "The Crackdown on the Dark Web Poison Trade". Retrieved 26 July 2015.
53. Leyden, John (11 September 2015). "'Walter Mitty' IT manager admits to buying gun on dark web". Retrieved 11 September 2015.
54. Cox, Joseph (22 September 2015). "A Survey of the Dark Web Knife Trade". Retrieved 23 September 2015.
55. Justin Norrie; Asher Moses (12 June 2011). "Drugs bought with virtual cash". The Sydney Morning Herald. Fairfax Media. Retrieved 5 November 2011.
56. Public statement from a Silk Road spokesperson 1 March 2011.

57. Adrian Chen (1 June 2011). "The Underground Website Where You Can Buy Any Drug Imaginable". Gawker. Archived from the original on 13 June 2011. Retrieved 15 June2011.
58. Solon, Olivia (1 February 2013). "Police crack down on Silk Road following first drug dealer conviction Technology". WIRED. Retrieved 19 April 2013.
59. Jump up to:[a] [b] Gayathri, Amrutha (11 June 2011). "From marijuana to LSD, now illegal drugs delivered on your doorstep". International Business Times. Retrieved 13 April 2013.
60. "Schumer Pushes to Shut Down Online Drug Marketplace". NBC New York. Associated Press. 5 June 2011. Retrieved 15 June 2011.
61. "Sealed Complaint 13 MAG 2328: United States of America v. Ross William Ulbricht"(PDF). 27 September 2014. Retrieved 27 January 2014.
62. Deep Web. 2015.
63. Crawford, Angus (31 July 2014). "Dark net drugs adverts 'double in less than a year'". Retrieved 24 May 2015.
64. Alex Hern (18 October 2013). "Silk Road replacement Black Market Reloaded briefly closed". The Guardian. Retrieved 18 October 2013.
65. Samuel Gibbs (3 October 2013). "Silk Road underground market closed – but others will replace it". The Guardian. Retrieved 18 October 2013.
66. Chen, Adrian (20 September 2013). "Popular Underground Drug Market Shuts Down for 'Security Reasons'". Archived from the original on 7 July 2015. Retrieved 5 July 2015.
67. Greenberg, Andy (30 October 2013). "'Silk Road 2.0' Launches, Promising A Resurrected Black Market For The Dark Web". Forbes. Retrieved 6 November 2013.
68. DeepDotWeb (30 October 2013). "Project Black Flag Waves the White Flag". Retrieved 5 July 2015.
69. Bilton, Nick (2013-11-17). "Disruptions: A Digital Underworld cloaked in anonymity". New York Times.
70. Greenburg, Andy (1 December 2013). "Silk Road Competitor Shuts Down And Another Plans To Go Offline After Claimed $6 Million Theft". Forbes. Retrieved 4 January 2014.
71. Patrick Howell O'Neill (27 March 2015). "Suspected Dark Net master thief busted trying to buy luxury Czech home". Daily Dot.

72. Shin, Laura (30 May 2016). "Mystery Solved: $6.6 Million Bitcoin Theft That Brought Down Dark Web Site Tied To 2 Florida Men". Retrieved 1 June 2016.

73. Adrianne Jeffries (2013-04-29). "Drugs, porn, and counterfeits: the market for illegal goods is booming online". The Verge. Retrieved 2013-12-02.

74. "Dark marketplace closes after theft of £3m in bitcoins". BBC News. 2013-12-02. Retrieved 2013-12-02.

75. Mandalia, Ravi (2013-12-01). "Silk Road-like Sheep Marketplace scams users; over 39k Bitcoins worth $40 million stolen". Techie News. Retrieved 2013-12-02.

76. "Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Banking, Housing, and Urban Affairs Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Policy" (PDF). fincen.gov. Financial Crimes Enforcement Network. 19 November 2013. Archived (PDF) from the original on 9 October 2016. Retrieved 1 June 2014.

77. S., L. (2 November 2015). "Who is Satoshi Nakamoto?". The Economist. The Economist Newspaper Limited. Archived from the original on 21 August 2016. Retrieved 23 September 2016.

78. Davis, Joshua (10 October 2011). "The Crypto-Currency: Bitcoin and its mysterious inventor". The New Yorker. Archived from the original on 1 November 2014. Retrieved 31 October 2014.

79. "What is Bitcoin?". CNN Money. Archived from the original on 31 October 2015. Retrieved 16 November 2015.

80. Hileman, Garrick; Rauchs, Michel. "Global Cryptocurrency Benchmarking Study"(PDF). Cambridge University. Archived (PDF) from the original on 10 April 2017. Retrieved 14 April 2017.

81. Wolff-Mann, Ethan (27 April 2018). "'Only good for drug dealers': More Nobel prize winners snub bitcoin". Yahoo Finance. Archived from the original on 12 June 2018. Retrieved 7 June 2018.

82. "Bitcoin". U.S. Commodity Futures Trading Commission. Archived from the original on 1 July 2018. Retrieved 17 July 2018.

83. Webster, J., Watson, R.T., 2002. Analyzing the past to prepare for the future: Writing a literature review. MIS Q. xiii--xxiii.

84. Mathiassen, L., 2017. Designing Engaged Scholarship: From Real-World Problems to Research Publications. Engag. Manag. Rev. 1, 2.

85. CORE, 2018. Journal Portal [WWW Document]. Comput. Res. Educ. URL http://portal.core.edu.au/jnl-ranks/ (accessed 4.13.18).

86. ACPHIS, 2018. IS Journal Ranking [WWW Document]. Aust. Counc. Profr. Heads Inf. Syst. URL http://www.acphis.org.au/v2wp/rank-order/ (accessed 4.13.18).

87. Chertoff, M., Simon, T., 2015. The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance.

88. Winkler, I., Gomes, A.T., 2016. Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies. Syngress.

89. Spitters, M., Verbruggen, S., van Staalduinen, M., 2014. Towards a comprehensive insight into the thematic organization of the tor hidden services, in: Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint. pp. 220–223.

90. Springer, P.J., 2017. Encyclopedia of Cyber Warfare. ABC-CLIO.

91. Tsakalidis, G., Vergidis, K., 2017. A Systematic Approach Toward Description and Classification of Cybercrime Incidents. IEEE Trans. Syst. Man, Cybern. Syst.

92. Skopik, F., 2017. Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level. CRC Press.

93. Crawley, A., 2016. Hiring hackers. Netw. Secur. 2016, 13–15.

94. Biryukov, A., Pustogarov, I., Thill, F., Weinmann, R.-P., 2014. Content and popularity analysis of Tor hidden services, in: Distributed Computing Systems Workshops (ICDCSW), 2014 IEEE 34th International Conference On. pp. 188–193.

95. Biryukov, A., Pustogarov, I., Thill, F., Weinmann, R.-P., 2014. Content and popularity

analysis of Tor hidden services, in: Distributed Computing Systems Workshops (ICDCSW), 2014 IEEE 34th International Conference On. pp. 188–193.

96. Ahmad, A., Hadgkiss, J., Ruighaver, A.B., 2012. Incident Response Teams - Challenges in Supporting the Organisational Security Function. Comput. Secur. https://doi.org/10.1016/j.cose.2012.04.001

97. Nye Jr, J.S., 2017. Deterrence and dissuasion in cyberspace. Int. Secur. 41, 44–71.

98. Weimann, G., 2016a. Going Dark: Terrorism on the Dark Web. Stud. Confl. Terror. 39, 195–206.

99. Hooda, Parikshit. "Sybil Attack". GeeksforGeeks. Retrieved April 12, 2019.

100. Chertoff, M., Simon, T., 2015. The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance.

101. Ask, M., Bondarenko, P., Rekdal, J.E., Nordbø, A., Bloemerus, P., Piatkivskyi, D., 2013. Advanced persistent threat (APT) beyond the hype. Proj. Rep. IMT4582 Netw. Secur. Gjøvik univ. Coll. Springer.

102. Bhaskar, V., Linacre, R., Machin, S., 2017. Dark web: The economics of online drugs markets. LSE Bus.

103. Deep Dot Web, 2017. Decentralized Darknet Markets Have Arrived: OpenBazaar 2.0 beta launches with support for TOR [WWW Document]. Deep Dot Web. URL https://www.deepdotweb.com/2017/09/23/decentralized-darknet-markets-arrived-openbazaar-2-0-beta-launches-support-tor/ (accessed 4.19.18).

104. Silkos, 2017. Silkos (SLK) Technical White Paper.

105. Biryukov, A., Pustogarov, I., Weinmann, R.-P., 2013. Trawling for tor hidden services: Detection, measurement, deanonymization, in: Security and Privacy (SP), 2013 IEEE Symposium On. pp. 80–94.

106. Chertoff, M., 2017. A public policy perspective of the Dark Web. J. Cyber Policy 2, 26–38.

107. DiPiero, C., 2017. Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web.