ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 3, pp: (110-116), Month: July - September 2020, Available at: www.researchpublish.com

# An Overview of Darknet, Rise and Challenges and Its Assumptions

Zakariye Mohamud Omar[1], Jamaluddin Ibrahim[2]

Faculty of Information and Communication Technology, International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia

***Abstract:*** **The Internet today is beset with constant attacks targeting users and infrastructure. One popular method of detecting these attacks and the infected hosts behind them is to monitor unused network addresses because many Internet threats propagate randomly, Deep web content cannot be indexed by search engine such as Google, Yahoo and Bing and Darknet is lies within the deep web. Dark web has been intentionally hidden, and it is not accessible through standard browser. Deep web can be accessed by anyone who has The Onion Router (TOR) browser. TOR is a virtual and encrypted tunnel which allows people to hide their identity and network traffic and allow them to use internet anonymously. Dark web is virtually online market for anything, including but not limited to drugs, weapons, credit card data, forged documents, hire services for murder, narcotics and indecent pornography etc. Because of these reasons, it is difficult for law enforcement agencies or digital forensic professionals to pinpoint the origin of traffic, location or ownership of any computer or person on the Darknet. Silk Road was only accessible via the TOR network and hidden from mainstream web. There has been lot of buzz around Bitcoin, TOR network and Darknet, because most of the Darknet sites carried out transactions through anonymous digital currency, pear to peer, distributed and Bitcoin which is based on cryptography principal (D. Rathod, 2017). In this research paper, I proposed the rise and challenge of Darknet. I am also proposed and discussed Darknet Deployment and why use the Darknet.**

***Keywords:*** **Introduction to the Darknet, history of the Darknet, Why use the Darknet, The rise and challenge of Darknet, Assumptions of the Darknet, Darknet Deployment.**

## I. INTRODUCTION

Darknet or Dark web is an anonymizing network where connections are made only between trusted peers sometimes called "friends" (F2F) using non-standard protocols and ports. The term "Darknet" can be used to describe all non-commercial sites on the Internet, or to refer to all "underground" web communications and technologies, most commonly those associated with illegal activity or dissent. Darknet is the underground world for ecommerce in the Internet and also known as “Deep Web “It’s servers appear in anonymity because of a software called The Onion Router (TOR). The Darknet is part of the Deep Web, the biggest part of the Internet, which is not indexed by regular search engines. It's where public databases are found, along with subscription only and password protected services, and the content of social Networks and messaging sites. The Darknet can be accessed via the Tor browser, and Tor Hidden Services allow you to find anonymously run websites. No one uses his or her real name on the Darknet. Neither cybercrime nor the Darknet are straightforward they are a morass of contradictions and grey areas. Cybercriminal activity occurs on the surface net: harassment, copyright infringement, fraud, subversion, sabotage and terrorist propaganda. But although these actions are illegal, are some of them legitimate? Those who believe information should be free oppose copyright laws, while cyber subversion and sabotage can help topple authoritarian regimes; they were vital catalysts in the 2010-11 Arab uprisings.

Darknet was originally often associated with the Tor network, when the infamous drug bazaar Silk Road once made headlines. Anonymous communication between whistle-blowers, which is a person who exposes secretive information or activity that is deemed illegal, unethical, or not correct within a private or public organization. Journalists and news

organizations is also facilitated by the "Darknet" Tor network through use of applications such as Secure Drop. In 1969 a couple of university students sent the world's first computer to computer messages it was sent an opened to internet and early answers that to the internet. In the 1980s, access to the internet for normal citizens is still a dream. This was the decade when everything needed for a world wide web (www) would fall into place. In the early 80s, the TCP/IP standard is solidified. Internet pioneers also invented the domain name system (DNS) we use to resolve website names during this decade. The 1990s are without a doubt the time when the World Wide Web (www) went mainstream. Towards the end of the 1990s, there was a real increase in the technologies that allowed large amounts of data, such as multimedia, to be shared online. Without Dark Web alike peer-to-peer exchanges it's doubtful we had have the consumer-friendly online media world of today. In 2000s The Dark Web proper really got its start in March of 2000 with the release of Freenet. The service still exists today and provides a censorship-resistant way to use the web. A data haven called HavenCo was established in Sealand (a sea steading micro- nation) which promised to store sensitive information in a place where no government could stick its nose.

It seemed like a Dark Web dream, but by the early 2010s HavenCo was dead. The most important Dark Web development of all time happened in 2002, with the release of TOR or The Onion Router. It was created by non-other than the US government, as a way to help their own operatives remain invisible. Late in the 2000s came the advent of Cryptocurrency in the form of Bitcoin.

This is the era in which the Dark Web becomes a topic of public concern, rather than cyber security. Today The Dark Web is reportedly in decline. Despite this, there is an incredible variety of hidden services and significant information exchange happening out of sight of the mainstream web. Small groups of hackers collaborating on the Dark web can bring a multi-billion-dollar internet company to its knees. Finally, what will be the future of the darkness? The technologies and methods that support the Dark Web are incredibly sophisticated, while most governments would prefer that something like the Dark Web didn't exist, they themselves need technologies like encryption and onion routing for their own purposes.

## II. LITERATURE REVIEW

Since the study of the Dark Web is a new topic in academia, the available research on this topic is still limited. In this section, I examine the literature about Dark Web, the online black market user- base, Internet law enforcement, and virtual communities. The Dark Web is the global network through which users accessed Silk Road. Dark Web consists of Internet content that is not accessible through standard search engines. Information on the Dark Web is typically not available to the general population, and is intentionally hidden from the regular Internet, known as Clear net (see Figures 1 and 2 for details).

One of the primary modes of Dark Web access is The Onion Router (abbreviated as Tor) which "covers your online tracks by blending your internet traffic into data from many servers worldwide to make you functionally invisible" (Hodson, 2014, p.2).The Silk Road domain name, http://silkroad6ownowfk.onion,was only accessible through the Tor browser, and always consisted of a seemingly random set of characters followed by "onion". The Dark Web began with ARPANET, the Internet's progenitor that was developed by the Pentagon in 1969. As the inter-computer interaction began to grow, "a number of isolated, secretive networks started to appear alongside ARPANET" (McCormick, 2013, p. 22).

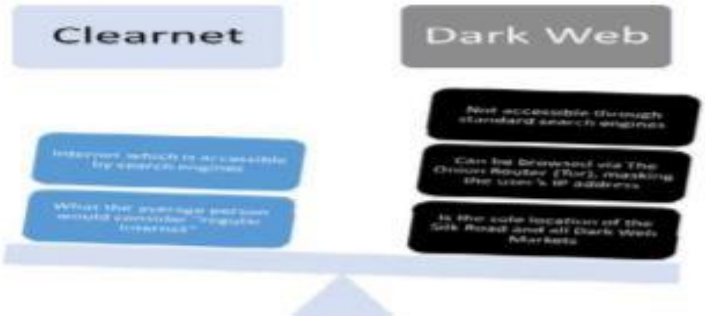
These networks eventually became the medium of choice for the U.S. Naval Research Laboratory, which introduced a browser called The Onion Router. Tor, as it is called now, "conceals the location and IP addresses of users who download the software" (McCormick, 2013, p. 22) in order to protect overseas American operatives and dissidents. However, the software became available for public consumption in 2004, and Tor domains dedicated to drug dealing, child pornography, and terrorism began cropping up. In fact, there is a concern of using Darknet because some people access the dark web for criminal purposes, others have legal reasons to do their online business anonymously.

So why we use the Darknet? In general, Darknet may be used for various reasons, such as: (a) to better protect the privacy rights of citizen's form targeted and mass surveillance. (b) Protecting dissidents from political reprisal. (c) Whistleblowing and news leaks. (d) Computer crime (Hacking, file corruption and etc.) (f) Sale of restricted goods on Darknet markets and File sharing (pornography, confidential file, illegal or counterfeit software etc.) Although the literature covers a wide variety of topics on Dark Web, the information is rather scattered and inconsistent.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 3, pp: (110-116), Month: July - September 2020, Available at: www.researchpublish.com

In addition to this, for each of the discussed themes, legal challenges and illegal use will be further examined. Another side theme to look out for is anonymity, which is an essential factor of Deep Web and its corrupt nature. Despite the literature presenting these themes in a variety of contexts, this paper will primarily focus on why the utilization of Deep Web and its components is destructive, harmful and highly prone to variety of illegal activities, due to weak regulations and lack of control and why it needs to be policed or stopped(González, P. 2013).

*Figure 2*




## III. LITERATURE FINDINGS

### *A. Tor*

"[T]he [O]nion [R]outer (TOR) is an anonymity network designed to facilitate anonymous Internet communication" (Abbot, 2010). It is an "implementation of an onion routing architecture designed by The Onion Routing project" (González, 2013). Onion architecture is multiple levels of encryption that are reminiscent of layers of an actual onion. Tor is a fairly new project, it started off as an "invention of Naval Research Laboratory", but soon saw its public release, in 2004, and became an open source project (González, 2013). For clarification reasons, anyone can freely change, use or share open source - labeled software. Tor has two main functions: creation of proxy servers, which provide anonymity for their users ("collectively form the Tor Network"); and "[software, known as Tor Browser that provides access to the network]" (Abbot, 2010). For crucial understanding of Tor Project, it is very important to notice that Tor Network and Tor Browser are "two distinct entities" (Abbot, 2010). While the progress of browser is supervised, no one has any authority or jurisdiction over the network. The Network can be pictured as virtual underground tunnels that resist transparency and censorship, and keep unprecedented, evil data in the shadows. Tor Network is the most illicit and dangerous part of Deep Web and The reason is anonymity.Tor doesn't 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, Wikipedia blocks attempts by Tor users to edit articles unless special permission is sought.

Tor enables its users to surf the Internet, chat and send instant messages anonymously, and is used by a wide variety of people for both licit and illicit purposes ,for or example, criminal enterprises, hacktivism groups, and law enforcement agencies at cross purposes. Tor aims to conceal its users' identities and their online activity from surveillance and traffic analysis by separating identification and routing. It is an implementation of onion routing, which encrypts and then randomly bounces communications through a network of relays run by volunteers around the globe. These onion routers employ encryption in a multi-layered manner (hence the onion metaphor) to ensure perfect forward secrecy between relays, thereby providing users with anonymity in a network location. That anonymity extends to the hosting of censorship-resistant content by Tor's anonymous onion service feature.[1] Furthermore, by keeping some of the entry relays (bridge relays) secret, users can evade Internet censorship that relies upon blocking public Tor relays.

According to Weaknesses Tor cannot and does not attempt to protect against monitoring of traffic at the boundaries of the Tor network (i.e., the traffic entering and exiting the network). While Tor does provide protection against traffic analysis, it cannot prevent traffic confirmation (also called end-to-end correlation).

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 3, pp: (110-116), Month: July - September 2020, Available at: www.researchpublish.com

*Figure 1*


## IV. THE RISE AND CHALLENGE OF DARKNET

This policy brief examines the expansion of drug markets on the Dark Net or 'hidden web' and the challenges they pose for both law enforcement agencies and the international legal framework within which those agencies ultimately operate.

The Dark Net drug markets are one manifestation of an increasingly complex, transnationalised and lucrative trade that the extant United Nations drug control system, The 1961 Single Convention on Narcotic Drugs, the bedrock of the international drug control architecture, does much to lock the international community into arcane and bureaucratic counter-narcotic responses oriented toward criminalization and law enforcement. However, evidence has demonstrated that this approach has failed to achieve a significant or sustainable reduction in drug supply or demand. The challenges of globalisation, transnational organised crime, HIV, and the electronic communications revolution, drug treaty system and associated 'traditional' counter narcotics strategies are increasingly inadequate tools which to address emerging challenges such as the Dark Net drug markets.

In the 2014 World Drug Report, the rise of hidden, Dark Net drug markets was belatedly acknowledged. The Report set out that the variety of drugs available on the Dark Net appeared to be 'diverse and growing' and this posed 'unique challenges for law enforcement. As outlined by Interpol in the September 2014 Internet Organised Crime Assessment (iOCTA), the relationship between customer and vendor in the hidden markets is purely transactional. 'Criminals in cyberspace do not need to be close to the crime scene, they might never even travel to the target country', their activities can be conducted transnationally and 'with minimum effort and risk by hiding their identity', the Assessment notes. By contrast, in the off-line world 'criminals normally need to be physically present at the crime scene and can typically only commit one offence at a time.

A second consequence of Silk Road's interdiction was a rise in registration on other Dark Net sites such as Black Market Reloaded and Sheep Marketplace, which provided a mechanism for verifying trusted Silk Road vendors in order to encourage their customers to follow. Just as the interdiction and break up of Colombia's Medellin 'cartel' and assassination of its leader Pablo Escobar had no impact on levels of cocaine supplied from Colombia, so closing Silk Road and arresting Dread Pirate Roberts had no long term or catastrophic impact on the Silk Road project or hidden markets more broadly; quite the reverse. It stimulated new competition, innovation in business models and the launch of Silk Road 2.0 as communicated by Libertas one of the moderators on Silk Road in November 2013.

As outlined by Martin (2014), illicit drugs have been bought and sold on the internet since it was first established. According to Markoff (2005), cited in Martin, the first online ecommerce transaction was a 1971 marijuana exchange between students at Stanford University using the Arpanet accounts at the institution's Artificial Intelligence Laboratory and their counterparts at Massachusetts Institute of Technology. This underlines the 'dual use' challenge that the advent of the internet posed for the IDCR, with unstoppable and positive advances in global communications creating an enabling environment for illicit drug supply and use. Supply or demand Conceived before the challenges of globalisation, transnational organised crime, HIV, and the electronic communications revolution, the drug treaty system and associated

'traditional' counter narcotics strategies are increasingly inadequate tools with which to address emerging challenges such as the Dark Net drug markets.

Although the internet has been available to the public since the 1990s, the Dark Net has only emerged in recent years. The growing sophistication of terrorists' use of the Dark Net presents a tough challenge for governments, counter-terrorism agencies, and security services. When IBM's security division published its security threats report for 2015, it highlighted the threat of cyberattacks coming from the Dark Net, using Tor networks. There is clearly an urgent need to develop new methods and measures for tracking and analyzing terrorist use of the Dark Net. Thus, for example, the Defense Advanced Research Projects Agency (DARPA) believes the answer can be found in MEMEX, a software that allows for better cataloguing of Deep Web sites. MEMEX was originally developed for monitoring human trafficking on the Deep Web, but the same principles can be applied to almost any illicit Deep Web activity.

When Silk Road was closed, commentators predicted a crash in Bitcoin's value. However, just as the Dark Nets bounced back and strengthened as a result of law enforcement efforts, Bitcoin rebounded rising to $305 within weeks.

Recent years have seen a dramatic growth in the sale of a variety of illicit substances on Dark Net drug markets, with on line sales projected to increase exponentially due to expanding internet availability, evolving technologies and the profusion of social media. This new form of retail market poses a major challenge to not only law enforcement agencies but also the UN international drug control system and related legal structures within which these agencies operate. For vendors and purchasers who use the sophisticated, user friendly and increasingly secure Dark Net sites, hidden markets present a safer environment for drug transactions and they reduce the multiple risks (coercion, violence, arrest, exposure to other drugs) associated with 'street' sales. Experience to date shows that enforcement efforts through surveillance, hacking and other forms of interdiction may be successful in closing down a particular site, but at the cost of proliferating hidden drug markets and incentivizing technological innovation. Given an acknowledged lack of technical capacity, legal constraints and poor international enforcement coordination, Dark Net interdiction efforts should prioritizes high-end crimes such as child sexual exploitation, cyber terrorism and weapons trafficking, and work with self-regulating, 'ethical' drug sites to enhance understanding of high-level criminality on the Dark Net. The key advantage of Silk Road 1.0 over competitors was the site's use of Bitcoin 'digital coins which are not issued by any government, bank, or organization, and rely on cryptographic protocols and a distributed network of users to mint, store, and transfer.'27 Crypto currencies enable direct and anonymous transactions without oversight. These technologies enable online vendors and Source: Runa Sandvik 10 buyers to communicate and exchange funds anonymously and with little risk of detection. The United States government has determined its role in regulating the Dark Web, and used tactics that take down criminal Dark Web activity while protecting the anonymity of innocent users to the maximum extent possible. The most effective and reasonable tactics are those that can target specific anonymous users and hold them accountable for their actions rather than deanonymising vast swathes of user data. The FBI used a hacking tool to identify the IP addresses of users accessing a hidden Tor child abuse site called Playpen (Cox 2016). Within a month of being launched in 2014, Playpen had 60,000 member accounts. By 2015, there were 215,000 accounts, 117,000 posts, and 11,000 unique visitors per week (Cox 2016). This tactic managed to capture only those who were accessing the child abuse site while leaving other users of Tor untouched.

## V. ASSUMPTIONS OF THE DARKNET

The idea of the Darknet is based upon three assumptions: 1. any widely distributed object will be available to a fraction of users in a form that permits copying. 2. Users will copy objects if it is possible and interesting to do so.3. Users are connected by high bandwidth channels Biddle P, England P, Peinado M, Willman B. (2003).

The Darknet is the distribution network that emerges from the injection of objects according to assumption 1 and the distribution of those objects according to assumptions 2 and 3. One implication of the first assumption is that any content protection system will leak popular or valuable content into the Darknet, some fraction of users possibly experts will overcome any copy prevention mechanism because the object will enter the Darknet before copy protection is applied. The term "widely distributed" is intended to capture the notion of mass market distribution of objects to thousands or millions of practically anonymous users. This is in contrast to the protection of military, industrial, or personal secrets, which are typically not widely distributed and are not the focus of this journal.

The edge labels can be used to model relevant information about the physical network and may include information such as bandwidth, delay, availability, etc. Most of the people believe the Darknet is so dangerous while others believe "dark web" is not quite as dangerous as it's made out to be, although it depends what you're doing with it. The dark web consists of web content built on top of "darknets," such as Tor, I2P, Freenet, GNUnet, and ZeroNet. The fundamental purpose of all of these is to keep people anonymously, especially if they live in countries where the internet is heavily censored.

Tor creators remain strong advocates of Tor's benefits. Roger Dingledine, an original developer, said, 'There are important uses for hidden services, such as when human rights activists use them to access Facebook or to blog anonymously,' and that 'These uses for hidden services are new and have great potential' (Ward 2014). Tor is a tool which can be used anonymously for both legal and criminal purposes. While it is essential to acknowledge the important role that anonymity plays in protecting human rights activists from oppressive regimes, it is also important to consider the challenges that anonymity poses to the law enforcement community. Indeed, most Tor users are just seeking privacy and may be using Tor for legitimate reasons. Only 1.5% of Tor users are actually accessing the Dark Web, although they generate a lot of traffic (Ward 2014).

The trouble is that Tor and the Dark Web are virtually inseparable. It is impossible to make a tool that keeps users anonymous while also tracking their activity to make sure that they are not accessing illegal websites. Tor's creators would like to think that the browser mainly carries the traffic of journalists valiantly writing stories from countries without laws protecting free speech, but that is not the case. The majority of traffic to hidden Dark Web sites using Tor is for viewing and distributing images of child abuse and purchasing illegal drugs. Child abuse accounts for the largest portion of Dark Web traffic. Dr Gareth Owen and Nick Savage, researchers at the University of Portsmouth, conducted a six-month study that explored Tor's usage and hidden services. They concluded that more than 80% of Tor traffic requests to hidden sites that were observed in the study were directed towards known child abuse sites (Owen and Savage 2015). They did acknowledge that this data may not be a perfectly accurate representation, since government agencies often use computers that will automatically access websites containing images of child abuse as a part of their investigation. It is virtually impossible to determine what portion of the 80% is police activity and what portion is traffic created by a human at a computer. Even if half of the child abuse traffic observed were police activity, much user traffic remains on the Dark Web targeting child abuse sites.

## VI. DARKNET DEPLOYMENT

This section represents an overview of Darknet deployment. The first step in Darknet technique is to deploy a sensor monitoring system. Therefore, understanding the network architecture is a most. Thus, a careful configuration must be done on the dynamic host server or the upstream router to forward unreachable packets to the Darknet sensors.

Two major elements must be done for this deployment setup, namely, the storage and network requirements and the deployment techniques. First, it is critical to identify the exact storage and network requirements for a Darknet system. In order to collect Darknet data, PCAP and Nerflow formats are the most suitable for this network traffic. The amount of Darknet packets received are based on the placement of the sensors, the size of the monitored IPs and the configuration setup. In terms of placement, previous studies has shown that the traffic collected by two different but equally sized Darknet is not the same. In terms of size of the Darknet and network requirements, a study has shown that a small /24 sensor has approximately a rate of 9 packets per second, while a /16 sensor receives 75 packets per second, and a large /8 monitor receives over 5000 packets per second (Bailey et al., 2006).Second, in terms of deployment techniques, there are mainly three major Darknet deployment approaches: i) the first is to simply send Address Resolution Protocol (ARP) replies for each dark address to the router. This technique, although it is simple, it works well when the Darknet addresses are well known and are limited in size. When the unused addresses reach thousands or million, the monitoring activity becomes less efficient; ii).

The second approach is considered more scalable and link a static range of IP address block to the monitor. This is a Simple approach, but it needs the dark address block to be specifically separated for analysis; iii) the third approach is done by forwarding all non-configured packets to the sensor. It is like forwarding all unused packets of an organization network to the sensor. The above-mentioned methodologies deal with unused and reachable dark addresses. However, to capture unused and non-reachable packets, RFC 1918 (Groot, Rekhter, Karrenberg, Lear, 1996) specifies some IP ranges that fit in this category. We refer the reader to (Bailey et al., 2006) for more information regarding these techniques and

how to implement them. The deployment of a Darknet monitoring system requires an understanding of the topology of the local network. Since a Darknet monitor observes traffic to unused addresses, the upstream router or dynamic host configuration server must be instructed to forward undeliverable packets to the monitor. In this section we highlight some of the important challenges associated with configuring the network and then discuss how to provision adequate storage and network resources for a Darknet system.

## VII. CONCLUSION

In short, The Internet today is beset with constant attacks targeting users and infrastructure. One popular method of detecting these attacks and the infected hosts behind them is to monitor unused network addresses because many Internet threats propagate randomly. The term "Darknet" can be used to describe all non-commercial sites on the Internet, or to refer to all "underground" web communications and technologies, most commonly those associated with illegal activity or dissent. How to access the dark web safely. The Dark Web is, by its nature, anonymous and incapable of discriminating between criminals and ordinary users and the Enforcement agencies must address this issue by employing tactics that maintain the privacy of the average user while unmasking the criminal. According to Weaknesses Tor cannot and does not attempt to protect against monitoring of traffic at the boundaries of the Tor network. Tor enables its users to surf the Internet, chat and send instant messages anonymously, and is used by a wide variety of people for both licit and illicit purposes ,for or example, criminal enterprises, hacktivism groups, and law enforcement agencies at cross purposes.

## REFERENCES

[1] Biddle P, England P, Peinado M., Willman B. (2003) The Darknet and the Future of Content Protection. In: Feigenbaum J. (eds) Digital Rights Management. DRM 2002. Lecture Notes in Computer Science, vol 2696. Springer, Berlin, Heidelberg

[2] Buxton, Julia, and Tim Bingham. "The rise and challenge of dark net drug markets." Policy brief 7 (2015): 1-24.

[3] González, P. (2013). Fingerprinting Tor. Information Management & Computer Security, 73-90. Guitton, C. (2013).

[4] https://anshchoudhary.wordpress.com/2017/03/14/therise-and-challenge-of-dark-net-drug-markets/.

[5] https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1298643

[6] https://www.comparitech.com/blog/vpn-privacy/how to access the deep web-and darknet, Paul Bischoff, 2018.

[7] https://www.technadu.com/dark-web- history/52017/.

[8] https://en.wikipedia.org/wiki/Whistleblower.

[9] Jean-L. Richet. (2015).Cybersecurity Policies and Strategies for Cyberwarfare Prevention book. Information Science Reference, An Imprint of IGI Global, 66.

[10] K. Jaishankar. (2016). International Journal of Cyber Criminology (IJCC), ISSN: 0973-5089 January – June 2016. Vol. 10 (1): 40–61. DOI: 10.5281/zenodo.58521.

[11] M. Bailey. (2016). Practical Darknet Measurement. 40th Annual Conference on Information Sciences and Systems, 1497, 1498, 1499. DOI: 10.1109/CISS.2006.286376.

[12] Rathod , " Darknet Forensics " , International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 6, Issue 4, July - August 2017 , pp. 077079 , ISSN 2278-6856.

[13] Senker. (2016), Cybercrime & the Dark Net: Revealing the hidden underworld of the internet, London: Arcturus Publishing, ISBN 9781784285555.