International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 4, July- August 2017 ISSN 2278-6856

Darknet Forensics

Dr. Digvijaysinh Rathod

Institute of Forensic Science, Gujarat Forensic Sciences University, Inida

Abstract

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 dark net. 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. In this research paper, I proposed darknet forensics techniques, which is a combination of TOR browser and Bitcoin wallet forensics. I am also proposed and discussed different technique to retrieve evidences from TOR browser and Bitcoin wallet, which helps digital forensics professional to perform darknet forensics.

Keywords: Deep web, Darknet, Bitcoin, TOR, Onion sites, RAM forensics, Bitcoin wallet

1. INTRODUCTION

Internet can be broadly divided in surface web or clear web and deep web, shown in figure-1. The surface web or clear web consist of web pages or web content which will be indexed by the popular search engine such as Google or Yahoo and accessible through standard browser without need of any special software and configurations [1]. Deep web content cannot be indexed by search engine such as Google, Yahoo and Bing and, Darknet is lies within the Deep web and Darknet is small section of it. Darknet has been intentionally hidden inside the deep web and cannot be accessed through standard web browsers because deep web content is not indexed by any of popular web browsers. Most of the Darknet content are found on TOR network which is anonymous network and this content can be accessed through TOR browser. TOR is a network of encrypted, virtual tunnels that allows people to use the internet anonymously, hiding their identity and network traffic. Using TOR's hidden service protocol; people can also host websites anonymously that are only accessible by those on the TOR network [2]. Deep web also termed limited-access network [3] which include private sites (requires credential to access it), un-linked sites, blocked sites (requires answer a CAPTCHA to access), dynamic web pages (requires complete URL to access it), Non-HTML or scripted content, and a network which in not open for every user.

Darknet sites are hosted with Domain Name System(DNS) root such as .BIT domains which are not controlled or managed by Internet Corporation for Assigned Names and Numbers ICANN and such sites hosted on limited-access network infrastructure requires special software - TOR to access it. Anyone can share,, communicate and disseminate ideas through the Internet but because of the darknet, despite many advantages of internet; terrorist groups, extremist groups, hate organizations and cybercrime criminals are using darknet to conduct criminal activities, promote their ideology or selling services or goods such as drug, weapon credit card data, forged documents, hire services for murder, narcotics and indecent pornography etc [5],. Anybody who wants to access any content from the dark net, need not to type keywords in a regular browser but will need to access it anonymously using TOR browser, which hide his/her identity such as IP address or physical location. Because of these reasons, it is difficult for law enforcement agencies or digital forensic professional to pinpoint the origin of traffic, location or ownership of any computer or person on the dark net. Implication of darknet comes in picture when Federal Bureau of Investigation (FBI) shutdown the website – silk road on October, 2013, which was an online black market and first modern darknet market for selling illegal drugs [6,7]. 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 dark web because most of the dark net sites carried out transactions through anonymous digital currency, pear to peer, distributed and Bitcoin which is based on cryptography principal. It is very difficult for digital forensic professionals to track such transaction because users and services are anonymous. The aim and objective of this paper is to discuss digital forensic techniques to deals with such darknet crimes.

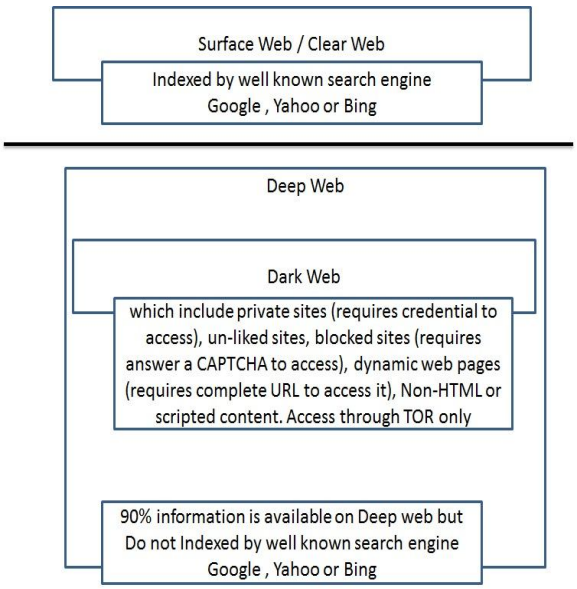

Figure 1 Overview of Surface web, Deep web and Darknet

2. DEEP WEB AND DARKNET TECHNOLOGIES:

Deep web and darknet is not a single location but distributed in entire internet and share one thing in common – that is, it is hidden from search engine crawlers and regular internet users. Our research shows that people can search darknet sites just typing .onion or .onion sites or finds detail for same on web site such as Tor Hidden Wiki, Onion.City and DNStats. Users need to use special software and configuration to access it. Few of deep web or darknet technologies are

a. VPN with TOR: In order to hide the fact that they are using TOR, some people use VPN in addition to TOR which is extra level of privacy.
b. Invisible Internet Project (I2P): It is an anonymous overlay network (network within network) to protect communication from dragnet surveillance and monitoring by third parties such as ISPs. People will use I2P to maintain the privacy of their communication or activity. People can use I2P for an
c. email, web browsing, blogging and forum, web site hosting, file sharing and real-time chating [11, 8].
d. Free Anonymous Internet (FAI): The Free Anonymous Internet project (FAI) is a decentralized 'deep web' service that is using blockchain technology to create a private, secure, peer-to-peer alternative to the regular World Wide Web. FAI comes with its own digital currency based on the Bitcoin code, but also enables its users to publish their own media content and to browse content posted by others in complete privacy – without anybody being able to spy on what you are doing. There is even a built-in decentralized marketplace to buy and sell products with other users [11, 9].
e. Free Net: Freenet is free software which lets you anonymously share files, browse and publish "freesites" (web sites accessible only through Freenet) and chat on forums, without fear of censorship. Freenet is decentralized to make it less vulnerable to attack, and if used in "darknet" mode, where users only connect to their friends, is very difficult to detect. Communications by Freenet nodes are encrypted and are routed through other nodes to make it extremely difficult to determine who is requesting the information and what its content is [11, 10].
f. ZeroNet – Based on torrent technology in combination with Bitcoin encryption, this is a new system which is not well developed but which I think holds promise for the future [11, 12].

3. FRAMEWORK FOR DARK NET FORENSICS:

The proposed forensic techniques for darknet forensics is categorized in two categories; TOR forensics and Bicoin forensics, as anyone can use darknet using TOR browser and most of the dark net sites do transaction using Bitcon – digital currency. Proposed techniques for darknet forensics are depicted in Table 1 with techniques, tools and purpose.

a. TOR browser forensics: Evidences related to TOR browser can be extracted in four different way

i. RAM Forensics: RAM forensics is considered as volatile memory forensics. Belkasoft RAM capturer will be used to capture dump of RAM and Hex dump will be used to view hexadecimal view of RAM dump. Purpose behind RAM forensics is to extract evidences related to file types and web sites visited.
ii. Registry changes: Registry forensics will be carried out by the Regshot and extracted evidences provide information related to TOR installation and date of last accessed.
iii. Network forensics: Network forensics will be carried out by wireshark and network miner and extracted evidences provide information related to web traffic.
iv. Database: Places Database of TOR browser is located at \Tor Browser\Browser\TorBrowser\Data\Browser \profile.default and database viewer can be used to view the content of the database.

b. Bitcoin Transaction Forensics: Bitcoin transaction forensics can be carried out by extracting forensic artifacts from installed Bitcoin wallet application on user's system. Internet Evidence Finder has the capability to recover Bitcoin artifacts.

4.Conclusion

Table 1: Darnet Forensics Techniques

Category	Techniques	Tools	Purpose
TOR Browser Forensics	RAM forensics	Belkasoft RAM Capturer, Hex dump	Detail about file types, web sited visited and other downloaded content
	Registry changes	Regshot	Detail about TOR installation and last executed date and other attributes
	Network forensics	Wireshark and Network Miner	Traffic analysis
	Database	Database viewer	To find evidences related to users or visited web content
Bitcoin transaction Forensics	Bitcoin wallet	Internet Evidence Finder (IEF)	To recover Bitcoin address, Query Bitcoin block chain

On one hand darknet has been intentionally hidden inside the deep web and cannot be indexed by search engine and accessed through TOR browser only and on the other hand most of the darknet sites carried out the transaction through the anonymous digital currency such as Bitcoin. It is difficult for digital forensic professionals to track such dark web activity because users and services are anonymous. Terrorists, cybercrime criminals, extremist groups and hate organization have already been started using dark web to committee cybercrime and this will increase day by day. I am sure that the forensic techniques proposed in this research paper, which is combination of TOR browser and Bitcoin wallet forensics will helps digital forensic professionals to deals with cybercrime cases related to dark web.

References

[1]. https://www.magnetforensics.com/computer-forensics/bitcoin-forensics-a-journey-into-the-dark-web/

[2]. Balduzzi M., Ciancaglini V. (Trend Micro), “Cybercrime in the Deep Web”, Black Hat EU, Amsterdam 2015.

[3]. https://www.magnetforensics.com/computer-forensics/bitcoin-forensics-a-journey-into-the-dark-web/

[4]. Tianjun Fu, Ahmed Abbasi and Hsinchun Chen , “A Focused Crawler for Dark Web Forums”, JOURNAL OF THE AMERICAN SOCIETY FOR INFORMATION SCIENCE AND TECHNOLOGY, 61(6):1213–1231, 2010

[5]. https://www.magnetforensics.com/computer-forensics/bitcoin-forensics-a-journey-into-the-dark-web/

[6]. https://en.wikipedia.org/wiki/Silk_Road_(marketplace)

[7]. https://geti2p.net/en/

http://cryptorials.io/free-anonymous-internet-project-browse-publish-shop-in-private/

[8]. https://freenetproject.org/pages/about.html

[9]. http://cryptorials.io/how-to-access-the-deep-web-or-darknet-a-beginners-guide/

[10]. https://github.com/HelloZeroNet/ZeroNet

Major Jeremy Cole, USAF, “Dark Web 101”, AIR & SPACE POWER JOURNAL