Fall 2017

Examining and Exposing the Darknet

Ton H. Don

EXAMING AND EXPOSING THE DARKNET

by

TON DON

(Under the Direction of Hayden Wimmer)

ABSTRACT

This thesis consists of two studies; the first study is “Diving into the Darknet” and the second is “Exposing the Darknet on Mobile Devices.” The Darknet is a network of hidden sites and services which are built based on anonymity. In “Diving into the Darknet,” we applied different data science methods to establish the relationships between the data in the data set. This data set has information related to seller, drug types, and transactions. Additionally, we used Tableau to visualize the data set. For the second study, we took a digital forensics perspective of the Darknet. Orfox and Orbot, a Browser Bundle which is used to access the Darknet through mobile devices, were installed on a Galaxy Note 5 with Android 6.0.1. After the investigation, some theories of past studies were disproved by our method combined with E3: DS, a mobile digital forensics software package by Paraben. We believe that the combination of information from a user’s point of view and a technical perspective of digital forensics would bring the Darknet to light. Through this thesis, we hope that knowledge about the Darknet will be revealed and better understood.

INDEX WORDS: Darknet, Mobile Digital Forensics, Tableau, Data Visualization.

EXAMING AND EXPOSING THE DARKNET

by

TON DON

B.S., Georgia Southern University, 2015

A Thesis Submitted to the Graduate Faculty of Georgia Southern University in Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

STATESBORO, GEORGIA

EXAMING AND EXPOSING THE DARKNET

by

TON DON

Major Professor: Hayden Wimmer

Committee: Lei Chen

Weitian Tong

Electronic Version Approved:

December 2017

DEDICATION

To my parents and my grandparents for all the help and support they have been giving me.

AKNOWLEDGEMENTS

Without the help of many people, a thesis would not be completed. The author would like to acknowledge all the time and efforts provided by the professors. The author would like to give special thanks to all the help and guidance of Drs. Hayden Wimmer, Lei Chen, and Weitian Tong.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF EQUATIONS

Page

LIST OF ABBREVIATIONS

TOR: THE ONION ROUTER

VPN: VIRTUAL PRIVATE NETWORK

IPS: INTERNET SERVICE PROVIDER

TAILS: THE AMNESIC INCOGNITO LIVE SYSTEM

RAM: RANDOM ACCESS MEMORY

1 INTRODUCTION

A place where both legal and illegal services are being traded online is known as a crypto market [6]. Silk Road, one of the most infamous crypto markets, was built based around anonymity using the Onion Router (TOR) network and Tor Browsing Bundle [4]. We conducted two studies which were related to the crypto market and its infrastructure. The first study focused on the data collected from Silk Road. The second study, on the other hand, targeted the technical aspect of the Darknet by performing digital forensics process on the Tor Browser Bundle using E3: DS.

For the first study, we chose Silk Road because it was the most studied crypto market from 2011 to 2013 [4, 6-9]. Because of the exposure of Silk Road, it was shut down by law enforcement. For this reason, more crypto markets rapidly surfaced. Fortunately, they were soon closed down due to scams or authority involvements [10]. The data from the market was collected using multiple methods and tools. As for the data set used for this study, Aldridge and Décary-Hétu stated that they created their own version of web crawler. The web crawler started on the home page of Silk Road, followed the listing URL, and download the listing page. The collected data consisted of various information like the type of drugs, number of transactions of sellers, or the active window of sellers. We believed that visualization is an effective method of communication. With the correct selection of visual aid, readers, planners, or decision makers can comprehend the information easier and faster than sorting through tables or pages of documents. Tableau is our statistical and visualization software packages of choice. With the capabilities of this software, the data is graphically displayed to show the effectiveness of visualization.

The Darknet is hidden from the internet. While in the Darknet, a user's identity is protected by

the infrastructure of Tor. This can either let users express themselves freely or give cybercriminals a place to provide illegal services, according to Mansfield-Devine [11]. Since anonymity and privacy are provided by the Darknet, it has become more common and created challenges for digital forensic investigators. Focusing on exposing the usage of the Darknet, we perform the second study. For this study, we used a mobile device, Samsung Galaxy Note 5, with Android version 6.0.1 installed as our evidence. Using Paraben's software, E3: DS, we successfully collected a user's Orfox browsing session's information. Past studies claimed that the Tor Browser Bundle protected a user's information [12, 13], but we proved otherwise. From this study, we proved that with the new digital forensics tool, we can reveal user's activities while surfing the Darknet. Next, the Tor Browsing Bundle does not fully protect user's identity while browsing. Finally, this study shows the weaknesses of the Tor Browsing Bundle which may be improved by the developers.

After the first study, the reader will be able to recognize how effective visualization could be if used correctly to present information. With the second study, the importance of digital forensics tool and method was proven. On top of that, future investigators and researchers can have a better insight on the Tor Browsing Bundle. Through this work, we hope readers will have a better understanding over the Darknet, from an informational to a technical perspective.

2 LITERATURE REVIEW

2.1 Crypto market

Crypto market is a web-based market where legal and illegal services are being traded from sellers to buyers. Aldridge and Décary-Hétu [6] took an interest in those market and wrote several articles based on the data collected from Silk Road. Predictions about how the crypto market will grow in the future can be made using various articles with the same interest. Many things must be taken into consideration. Should the online drug market be the priority or not? Law enforcement has shown that they have the upper hand, but with the ongoing activities of the market, they might not have much impact on the matter.

Silk Road Drugs was a website which had all the basic knowledge and step by step guide for anyone who wanted to enter the crypto market. According to Silk Road Drugs, the crypto market, also known as dark net market, was where legal and illegal goods and services were exchanged. Out of 20,000 listing on a crypto market, 12,000 of those listings would be associated with drugs. The rest of the listings were for e-books, software, accounts, guns, etc. Since the majority of online shopping conducted on these sites was highly illegal, there were requirements that needed to be met before anyone could access the market [14].

The first requirement was a Virtual Private Network (VPN). This application, aided through encryption, helped hide your actions on the Internet. The Internet Service Provider (IPS) monitored every activity from the user, that's why VPN was required. By using VPN, the possibility of users getting caught while they participated in illegal activities would drop. This also helped the vendors or the market stay open longer.

The next requirement was Tor (The Onion Router) Browser. This is a modified version of

Firefox. Tor Browser would provide users new IP addresses when they surfed the dark net. The connection would change every time it bounced off one to three random nodes before it reached the final destination. Furthermore, Tor Brower was the only web browser which could have accessed and opened ".onion" websites, also known as hidden websites.

Once all the requirements were met, users could start accessing crypto market sites. Another mandatory action before beginning online surfing was to make an account. All users needed to create an account was a username and password; no other form of identification was needed. After the account was created, the next step was to create a pin code. This pin code would act as a second factor of authentication that ensured the user was the owner of the account. After the pin code was successfully created, a kind of currency would be picked out by the user. The main reason behind choosing currency was to know how much a certain merchandise would cost in their country. The main form of money used throughout the dark net's transactions were Bitcoin [14].

What is Bitcoin exactly? Bitcoin, unlike any other currency, was impossible to be counterfeited or inflated, declared by the company [15]. In contrast to government issued money, Bitcoin was not inflatable because there was only a fixed amount of bitcoin in the market: 21 million. Another reason which made the dark net users use bitcoin was because it was not possible to block bitcoin payments or freeze a bitcoin wallet. Bitcoin also ensured that the buyer's identity was anonymous. The freedom of using bitcoin increased the user's responsibility for spending money.

After bitcoin was used to make a purchase on the market, the seller needed to ship the product to the buyer. However, neither the buyer nor seller's physical address was recorded during the account registration process. Once again, to protect users' identities, the physical address or related physical address, such as a PO Box, would be erased at the moment the product was marked as shipped. After the shipment arrived, the buyer had to finalize the order by telling Silk

Road to release the withheld payment and then rate the seller. This finalization step was mandatory; if a user did not proceed with the process, Silk Road would do so on its own [16].

Based on an article written about crypto market, while Silk Road was still in operation, the market generated around USD 16.7 million in 2012 and about USD 89.7 million in 2013 [6]. As the data stated, there was an increase of USD 73 million in just one year. Silk Road was not the only drug market in the world. It was impossible to imagine how big the global drug market could be, but Silk Road alone was a mere fragment of that world.

A list of drugs on Silk Road Crypto Market was downloaded in September of 2013. With the high price-quantity sales, drug was the main source of revenue for Silk Road. There was an increase of 600% from mid-2012 to September of 2013. This article would help researchers who did not have access to the data or technology to understand what was happening inside Silk Road, or online drug trade as a whole. With an attempt in collecting data, most of the drug listings were collected. The targets were the different drug categories, which consisted of 90% of the market. Out of all the listing, the data which they were trying to collect was the sellers' life span, price of the drug, rating of sellers, and transactions count. After all the calculation and analysis, they came up with a solution. The resellers were the ones who paid for large quantity of drugs or listing of at a higher price. Not only that, most of the revenue from crypto market was generated by the higher price listing [4].

Criminal activities were taking various forms; the dark net market was one of them. Authors took all aspects of the dark net market into consideration, from technologies to physical, and then chemical. Using the collected data from an independent researcher, reader would have a better overview of the dark net market. Not only that, this team of researchers would also take a step further asking for a permission from an Attorney General to buy the drugs for educational purposes. There was difference in the chemical description of the drug which was sold by the seller. However, the differences were based on different factors like how the buyer referred the

product. Also, online drug markets were a different way of distributing drug in a larger scale [17].

Research, performed in 2015, about dark net data was published with a method for the collected data set. In order to validate the method and the data collected, Gwern Branwen with a group of researchers replicated the whole process. They used the same mechanism and compared the results. Surprisingly, the data collected by Gwern and his group had a large margin of error compared to the original study. With a question in mind, Gwern concluded his study with a set of suggestions for future researcher on how to validate their results [18].

In this article, the researchers used a crawling mechanism. With this mechanism, the researchers were able to automate the data collecting process. Software called HTTrack was used to download all the information related to the visited site, including pictures and related link-structures. The targets of the crawling process were item, user, and category webpages. Instead of spending hours manually downloading all the needed information, the researcher would just let the machine run over a period then come back to check the results. A set of statistical analysis was performed on the crawled data to find patterns. First was what kind of drugs were sold on the market. Second was the countries evolved in the trading process, both sending and receiving countries. Next was the site revenue, how much they were generating. Last was how to treat what was happening within the trading process and how to stop this problem from happening [16].

In February of 2011, Silk Road started as an online anonymous trading market with infrastructure built in so the trader and buyer could conduct transactions [16]. Put into perspective, Silk Road was similar to Amazon or eBay. One of the major differences between Silk Road, compared to eBay or Amazon, was the focus on keeping their sellers and buyers' identities and transactions anonymous.

According to a study conducted in 2014 [4],all buyers and sellers from Silk Road were protected

by a system of escrow: sellers were paid anonymously with a hard to trace online currency called bitcoin; however, payments were not released until buyers were satisfied with the provided services. As part of the dark net while using these methods, Silk Road was operating from February of 2011 to October of 2013. Silk Road was seized and shut down by the United States Federal Bureau of Investigation after two and a half years of operation.

Shortly after Silk Road was shut down, Silk Road 2.0 and Sheep, clone sites comparable in size, were launched. However, Sheep did not last for too long. As reported, Sheep was shut down after a scam by it's administrators. Throughout 2014, various crypto markets like Agora, Pandora, and Silk Road 2.0 grew in size and tried to regain their users' trust back [6].

November of 2014, once again, the Federal Bureau of Investigation and several European agencies, also known as Operation Onymous, worked together to seize and shut down multiple crypto markets; Pandora, Blue Sky, Hydra, Cloud Nine, and Silk Road 2.0 [10]. After the operation was completed, the Global Drug Policy Observatory also reported that there was an undercover agent working as one of the administrators which contributed to the success of the operation [7]. In the end, the anonymous system, which was designed to protect the crypto market, was used to destroy it.

Even with the proliferation of crypto markets from around the world, not many of them survived. January of 2015, an article, written by an independent researcher named Gwern Branwen, reported that there were 43 new markets recently opened following the closure of Silk Road. Within the same year, 46 markets were closed down due to scams, hackers, or seizure by law enforcement [19]. Knowing that www.reddit.com was not a credible site, however, Gwern was a credible independent researcher. There were multiple studies which were conducted using his data set or methods [17, 19]. A website suggested by Gwern, called Darknet Stats, was created in secrecy with the purpose of tracking online and offline crypto markets [20]. As of the most recently updated list, there were 25 markets total and only 21 of them were still active.With the

explosion of internet usage, the Darknet drug markets emerged and flourished based on newfound channels to deliver illegal substances to consumers. Buxton and Bingham [8] attempted to discover how Darknet markets operated and how law enforcement interacted with them. With the tech-savvy generation, Darknet markets became an incentive for drug vendors to participate in reaching a new consumer base. Law enforcement strategies and policies were incapable of confronting the Darknet and hidden services [8].

Silk Road, one of the biggest online illegal trading services in the Darknet, was shut down in October 2013. Nicholas Christin and Kyle Soska conducted a study on the Darknet. Using web crawling mechanisms, the authors collected data from many websites. Next, they parsed all text from downloaded sites. All information was imported into a database. While the authors understood that there were limitations to their method, they anticipated that the information and their method could be improved in future works [9]

A list of drugs on the Silk Road crypto-market was downloaded in September of 2013 by Aldridge and Décary-Hétu [4]. With the high price-quantity sales, drug sales were the main source of revenue for Silk Road. There was an increase of 600% from mid-2012 to September of 2013. Authors found that 6 drug categories comprised of 90% of the market. Out of all the listings, they collected the sellers' lifespan, the price of the drug, rating of sellers, and transaction count. After calculation and analysis, they determined that the resellers were the ones who paid for the large quantity of drugs or listing of a higher price. Not only that, most of the revenue from the crypto-market was generated by the higher price listing [4]

Criminal activities are now able to be executed through innovative ways with the Darknet market one of the fastest growing criminal opportunities. Rhumorbarbe, et al. [17] takes all aspects of the Darknet market into consideration, from technologies to physical, and then chemical. Using the collected data from an independent researcher named Gwern, authors give readers a better overview of the Darknet market. Moreover, the team of researchers sought permission from an

Attorney General to buy the drugs for educational purposes. A difference was found in the chemical description of the drugs which were sold by the seller. Additionally, authors state that the online drug market is also a different way to distribute drugs on a larger scale [17].

The crypto-market is a web-based market where legal and illegal services are being traded from sellers to buyers. Aldridge and Décary-Hétu [6] took an interest in the market and wrote several articles based on the data collected from this market, specifically Silk Road. Using various articles with the same interests in the crypto-market, predictions about how the crypto-market will grow in the future were formed. Considerations emerged including the efficacy of law enforcement on crypto-markets. For example, should the online drug market be the priority or not? Even though, law enforcement showed that they have the upper hand but with the ongoing activities of the market, they might not have much impact [6].

Aldridge and Décary-Hétu [6] briefly walk readers through the history of the crypto-market, with a focus Silk Road. After that, the authors would go through an overview of how the market was operated. For this section, the author would show which basic tools buyers needed to start surfing the crypto-markets; all the way through how the transaction was finalized [6].

Christin [16] used a crawling mechanism to automate the data collection process. Software called HTTrack was used to download all information related to the visited site, including pictures and related link-structures. The targets of the crawling process were item, user, and category web pages. Instead of spending hours manually downloading all the needed information, the researcher would just let the machine run over a period time then come back to check the results. Statistical analysis was performed on the crawled data to extract patterns. First, the types of drugs sold on the market were analyzed. Second, researchers examined the countries evolved in the trading process, both sending and receiving countries. Next, they investigated revenue generated by the website. Finally, they made recommendations how to stop the illegal trading [16].

Research, performed in 2015, about Darknet data was published with a method for the collected data set. In order to validate the method and the data collected, a group of researchers replicated the process. They used the same mechanisms and compared the results. Surprisingly, the data collected by Gwern and his group had a large margin of error compared to the original study. With a question in mind, Gwern concluded his study with a set of suggestions for a future researcher on how to validate their results [18].

In November of 2014, once again, the Federal Bureau of Investigation and several European agencies, also known as Operation Onymous, worked together to seize and shut down multiple crypto-markets; Pandora, Blue Sky, Hydra, Cloud Nine, and Silk Road 2.0 [10]. After the operation was completed, the Global Drug Policy Observatory also reported that there was an undercover agent working as one of the administrators which contributed to the success of the operation [7]. In the end, the anonymous system, which was designed to protect the crypto-market, was used to destroy it.

2.2 Tableau

To extract information and find opportunities from all the generated data from the world, Tableau was created. Tableau was designed to transform and analyzing data faster and easier. A computer scientist, an Academy-Award winning professor, and a business leader came together to ensure Tableau can deliver that to all the users. There are 3 focusing points for Tableau:

1. VizQL was also known as a visual query language. Unlike regular query language where user had to have some knowledge about how to write query, VizQL allowed user to drag and drop items, then translate those actions into data queries, and visually send result out to the screen for user.
2. Live Query Engine was the first technology that let user natively query other databases, cubes, warehouse, cloud services, and Hadoop and did not require a user to have any knowledge about programing or advanced development. User only needed to point and click to access all of their data.
3. In-Memory Data Engine, which processes in memory as opposed to disk, allowed Tableau to use cache to improve the data processing speed.

Many Eyes and Tableau are emerging as the most popular online data analytic and sharing tools. The researchers wanted to understand the reason why these tools are so popular. Researchers traced and figured out how much Many Eyes and Tableau Public were being used for an extended period. Four dimensions were taken into consideration: (1) types of users which leveraged the system, (2) how users interacting with the published content, (3) how users analyzed a single data set, and (4) how they integrated data sources. Researchers also mentioned that there are room for improvement for web-based visualization analytics systems [21].

2.3 Digital Forensics Background for Tor

With technology growing at a rapid rate, digital forensic tools and methods are struggling to keep up with the pace. This leads to the issue and question about how investigators can obtain evidence from mobile devices. Not only that, different vendors have different log configurations and encryption for their devices. Three main issues were mentioned by the authors Watson and Dehghantanha [22]: (1) the onboard data storage is not accessible using traditional DF methods, (2) cumulative data sets might be in multiple locations, and (3) the existing tools might not be able to read retrieved data. Overall, Watson and Dehghantanha [22] described the challenges created by the massive network of mobile devices. Because of these existing challenges, it is harder for the investigators to perform their job and present their findings in order to locate or capture the culprit who commits the crime. The authors of [22] present an overview of how and where digital forensic invitation processes are lacking the strength to acquire evidence regarding mobile devices.

Dhar and Pingle [23] discussed the framework for digital forensic investigation (DFI). DFI has four steps, (1) investigation preparation, (2) evidence acquisition, (3) analysis of evidence, and (4) result dissemination. Dhar and Pingle [23] also mentioned a three-step diagram for DFI for Internet of Things (IoT). Since mobile devices are a part of IoT, this article gives some insight into the things needed to be examined.

There is not a clear line whether the Darknet is a good or bad place. It all depends on a person's purpose. There will be people who are looking for a place where they are not being monitored by their government or criminals who are trying to sell illegal goods and services. Using the infrastructure which was designed for anonymity, cyber-criminals can form groups based on their languages and then later link back to a bigger group of criminals. Mansfield-Devine [11] stated that the Darknet could be a better tool if it was used properly. There is not a good or bad tool, it is the purpose of which it is used for that makes it is good or bad [11].

The Onion Router (Tor) is a network of volunteer-operated servers which gives people the ability to improve their security and privacy over the Internet. There are a series of tunnels, to which Tor's users can connect while they are on the Internet. This allows them to access blocked sites or content. When using Tor, users can access different sites without being tracked. On top of that, Tor also has a hidden service, which allows websites to be published anonymously. The more users who are using Tor the more secure the network is [1].

Tor networks create a random pathway through several relays on the network. Furthermore, a twisty and hard-to-follow route is used so that users cannot be tailed. On top of that, user's footprints are also erased periodically. Each relay on the network only knows where to receive and send data to. Because of this, no relay knows the complete travel path of the information. All the traffic between the relays is encrypted except the last relay to the destination, refer to figure 2.2.1. However, each time the client hops from one relay to another, the client requests a new encryption key. This will further improve the security and protect the users. Another great feature of the Tor network is that it will request a new path through the relay every ten minutes or so. This way, users' paths cannot be followed. All the aforementioned features will secure and keep Tor's users' privacy protected [1].

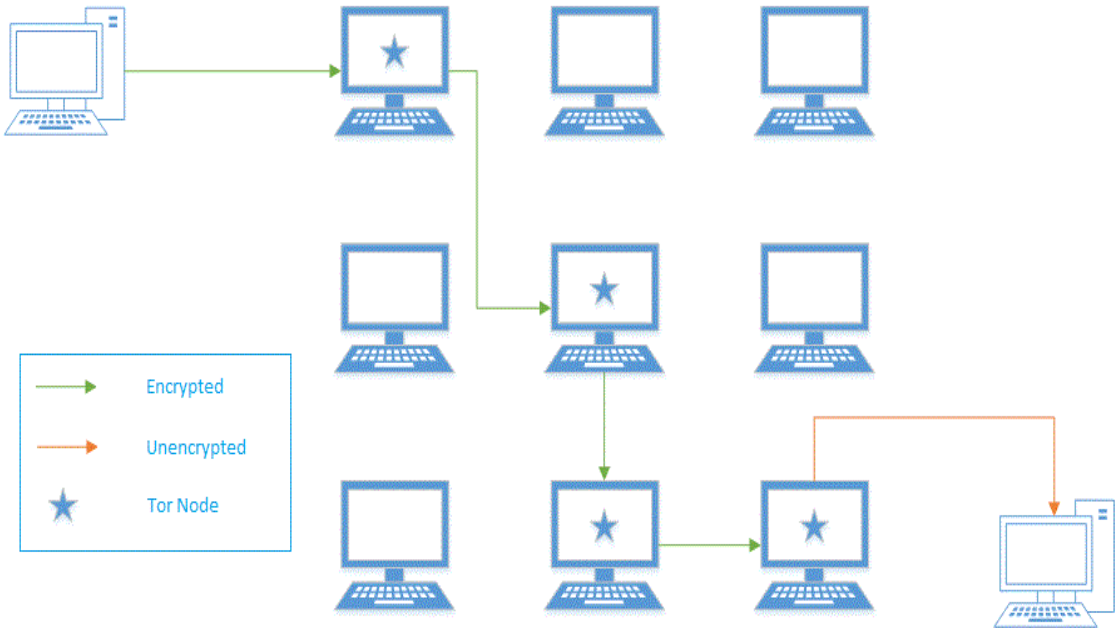

Figure 2.2.1 How Tor Works [1]

Tor is a tool which is used for both good and bad activities. Unfortunately, the Darknet, the network which was built based on anonymity, gave Tor a bad reputation. Jardine [24] tried to come up with a solution which would make Tor become more available to everyone. With most of the studies Jardine reviewed, the majority was about how Tor assisted the Darknet becoming a place for ill intentions; drugs trading, crime as a service, child pornography, etc. The author also mentioned the existence of VPNs and private search software which also made Tor a less attractive option. He also argued that government regulations were the reason which made people use Tor or the Darknet. The more political rights change, the higher the usage rate for Tor. Using Tor or the Darknet, users could freely express their opinions. In the end, there was not an ideal way to stop villainous activities. The author believed the best option was to police the network so that the Dark Web could bring more positive effects.

On the same topic of how Tor was being used, in 2016 Jardine [25] stated that political regressions of one's country were the reason why Tor's usage was rising. To express their liberal opinion without being monitored by their own government, the Tor network was the people's

tool of choice. In this study, Jardine showed how political regression affected the number of users on the Tor network. The relationship between political regression rate and Tor usage formed a U shape. If a country allowed its citizens to exercise their liberal and political rights, they were less likely to have people using the Tor network. According to Jardine [25], in 2013, there were 620 million internet users recorded. With a political regression scale of 14, this would cause an increase of 1,317,996 Tor bridges and 37,785,528 Tor relay users per year. The article gave us another perspective of the Tor network. It suggested that Tor could be useful for countries which were politically suppressed.

In 2013, Sandvik [26] reported about 100,000 downloads for the Tor Browser Bundle every month. Sandvik performed a forensic analysis of the Tor Browser Bundle on three operating systems: OS X 10.8, Windows 7, and Debian 6.0 Squeeze Linux. The processes of setting up all operating systems and Tor Bundle were the same. Many traces of the Tor Browser Bundle were found on each operating system. The researcher also suggested using The Amnesic Incognito Live System (TAILS) so that no traces would be left on the system. Tor should erase user's footprint from the system. Unfortunately, because of the default settings of the operating systems, the bundle could not remove the left-over tracks.

According to Dayalamurthy [13], the Darknet is the place where criminals and unethical users have access to illegal services and hidden links. They can be things such as child pornography, drug dealing, crime-as-a-service, and hidden hosting devices. For this study, Dayalamurthy [13] used the Tor Browser Bundle as the target for evidence acquisition. On top of that, the researcher used The Amnesic Incognito Live System (TAILS), a live bootable Linux operating system, to retrieve the artifacts from the windows OS. Using software to acquire memory artifacts was suggested in this study. There were many studies conducted using this method and it was much easier than retrieving them from the hardware. There were limitations in regard to collecting artifacts using a memory dump at the time this study was conducted. The researcher also

mentioned that this area of study was still new and more research needed to be conducted.

In order to find out more about the Tor network, Al Barghouthy and Marrington [27] performed a study over a rooted Samsung S2, Android v.4.1.1, using Orweb, a Tor browser built for Android devices. The main purpose of this study was to find digital evidence left over after using Orweb. The image of the device was created using rootkit method and recovery mode method. After the images were examined, there were traces of information of the places users visited such as URLs, email, IDs, encrypted messages, the RSA key, ports used, rejected ports, and date/time stamp. In conclusion, the researchers stated that it was not necessary to root the device. On top of that, acquiring the image using the Rootkit method was better since the device did not have to be rebooted, which was better for the artifacts on Random Access Memory (RAM).

Also taking an interest in Tor, Al-Khaleel, et al. [12] collected artifacts from the Tor Browser Bundle by extracting them from memory. To do so, they had to understand how Tor worked. After that, they designed an investigation model and experimental setup. There were six experiments. After the data from all the experiments were collected and carefully examined, they came to a conclusion. All the valuable information, which could be extracted from the Tor Browser Bundle, was only available when Tor and its' browser were open. The moment the browser or Tor was closed, all the artifacts were erased from memory.

Chrane and Kumar [15] conducted a study on Tor. The purpose of the article was to see if Tor could become the source for anonymity on the internet, as a mainstream browser. Unfortunately, it was not simple to make Tor work. For a novice Tor user, if the software was not properly configured, there would be no anonymity. It is not user-friendly. On top of that, with the rapid growth rate, there were no resources available, such as nodes, for Tor to be consistent. With a limited number of nodes, the Tor network would slow down or fail. There was a fix for this issue which was Universal Rate Limit. However, the Tor software was not compatible. Even though there were limitations for Tor, the authors still believed that Tor would be the future of the

Internet.

Supporting more than 26,000 devices, E3: DS by Paraben is software for mobile forensics. E3: DS allows users to access: image devices logically and physically, parse app data, carve data, bypass passwords, and unique content analysis. On top of that, E3: DS supports different operating systems: iOS (up to version 10.3.x), Androids (up to version 7.x), Blackberry (up to version10.x), Windows (up to version 10), etc. [28]

3 DIVING INTO THE DARKNET

3.1 INTRODUCTION

The crypto-market, also known as the Darknet market, was a term researcher used for illegal online drug trading markets. Having evolved from the traditional illegal drug trade, these markets focused on making transactions and identities anonymous. By doing so, sellers could constantly put their products onto display without concern for law enforcement. With evolving technology, buyers had increased the ability to participate. This illegal online activity slowly became a problem for which the authorities had no answer [4]. Following the exposure of Silk Road in 2013 [10], several researchers took an interest in this new kind of market [4, 7, 8, 16, 19, 20]. Various tools and techniques were used to extract the data in order to transform it into useful information. This process was complex and in-depth. In order to collect the raw data from the sites, HTTrack was employed by Munksgaard, et al. [18]. The sites took days to download and often times were canceled during the extraction process. Once the sites were downloaded, data science methods were used to clean and extract data. Some steps could be accomplished using tools, while others had to be done manually [16]. Because of the vast amount of time and effort that was put into collecting and analyzing the data, there were 2 sets of data discovered.

In this work, we adopted the data set from Dr. Aldridge's and Dr. David Décary-Hétu's previous research. Many attributes were not clearly described or documented; therefore, the majority of the obfuscated attributes were omitted, leaving only the meaningful ones. With the revised and reconstructed data set, Tableau, a visualization statistical package, is utilized to present and visualize the Darknet data. Next, we employ some common predictive methods from data science to determine the predictability of the data. The remainder of this paper is structured as follows: section 2 provides a literature review, section 3 details our methods and results, and

section 4 concludes this work.

3.2 METHOD

In 2013, Stephen Few, a researcher with more than 20 years of experience as an innovator, consultant, and educator in the field of business intelligence, wrote an article for human perception using data visualization. In this paper, Few mentioned one of the most influential psychological studies about visualization for human perception Gestalt principles: the law of proximity and the law of similarity [2]. As shown in figure 3.2.1, using the law of proximity, the human brain would see that there were three columns of circles forming a group instead of seeing six separate columns. Figure 3.2.2 was used to demonstrate the law of similarity. At first glance, the brain would tell us which objects would be in the same group because of the assigned colors.

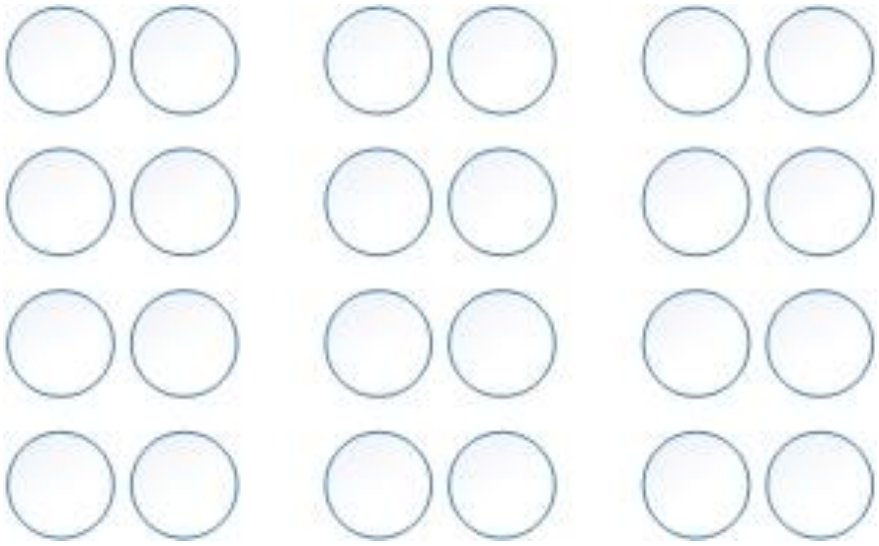

Figure 3.2.1: Law of Proximity [2]

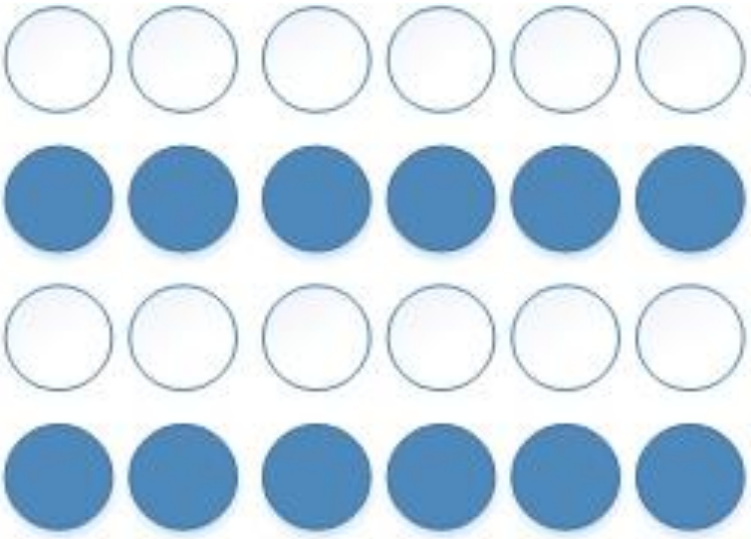

Figure 3.2.2: Law of Similarity [2]

Demonstrated in figure 3.2.3, visualization could be expressed as a message. As Andy Kirk described, a message was the channel of communication. The messenger embedded his/her ideas, discoveries, or results into a visual aid. This visual aid could be anything; a chart, an infographic, etc. Using the visual aid created by the messenger, the receiver should be able to process all the information through this message [3]. As the designer of this message, it depended on the field of study or the data which would be presented, the appropriate visual aid would be chosen.

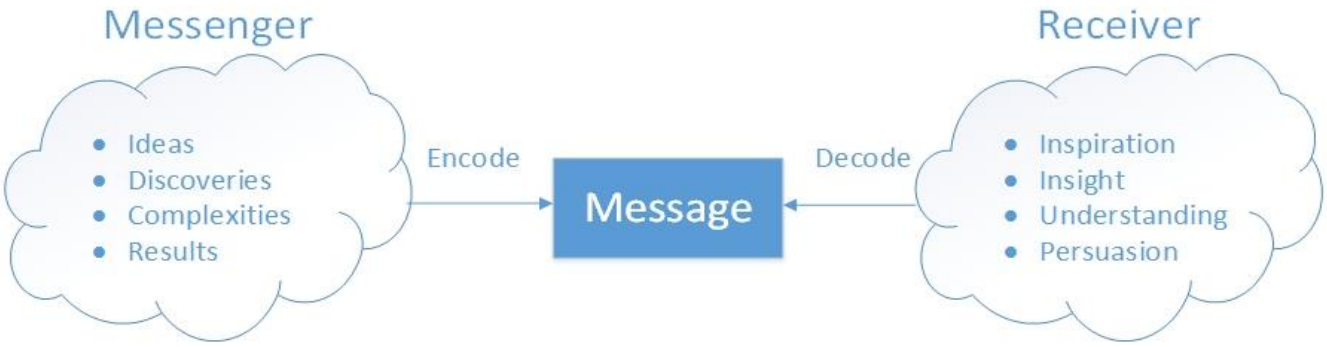

Figure 3.2.3: Relationship between messenger and receiver [3]

Maureen Stone, the founder of Stone Soup Consulting, published a book named “A Field Guide to Digital Color” in 2003. On top of that, as of the beginning of 2017, she has more than 30

published papers and 12 patents on digital color using interface technology and computer graphics. In [29], Maureen Stone explained how to choose the correct color to present your findings. A wrong decision with the color representation could affect the ability to deliver the message. A correct combination, however, will help the viewer understand the roles and the relationships of the elements [29].

Many Eyes and Tableau are emerging as the most popular online data analytic and sharing tools. The researchers wanted to understand the reason why these tools are so popular. Researchers traced and figured out how much Many Eyes and Tableau Public were being used for an extended period. Four dimensions were taken into consideration: (1) types of users which leveraged the system, (2) how users interacting with the published content, (3) how users analyzed a single data set, and (4) how they integrated data sources. Researchers also mentioned that there is room for improvement for web-based visualization analytics systems [21].

3.3 RESULTS

3.3.1 Visualizing the Darknet

Using the sample data set from [4], we imported the data into Tableau then generated figure 4. Figure 4 illustrates the top rank among all the sellers, from 1 to 10 with 1 as the highest and 10 as the lowest. Out of this group, we can also see the average rating on the top right of figure 3.3.1.1, from 5 to 3.4 with 5 is the highest rating a seller can get from a user and 3.4 is the lowest in this group. Not only that, we use red as the demonstration of rating, with the darker the color means the higher the rating, and the lighter means lower. Furthermore, we also take the life span of these sellers into consideration. Since we already used the color for average rating, we decide to use the size of the circle to express the total life span. The larger the circle, the longer or larger the total life span of the sellers, and vice versa.

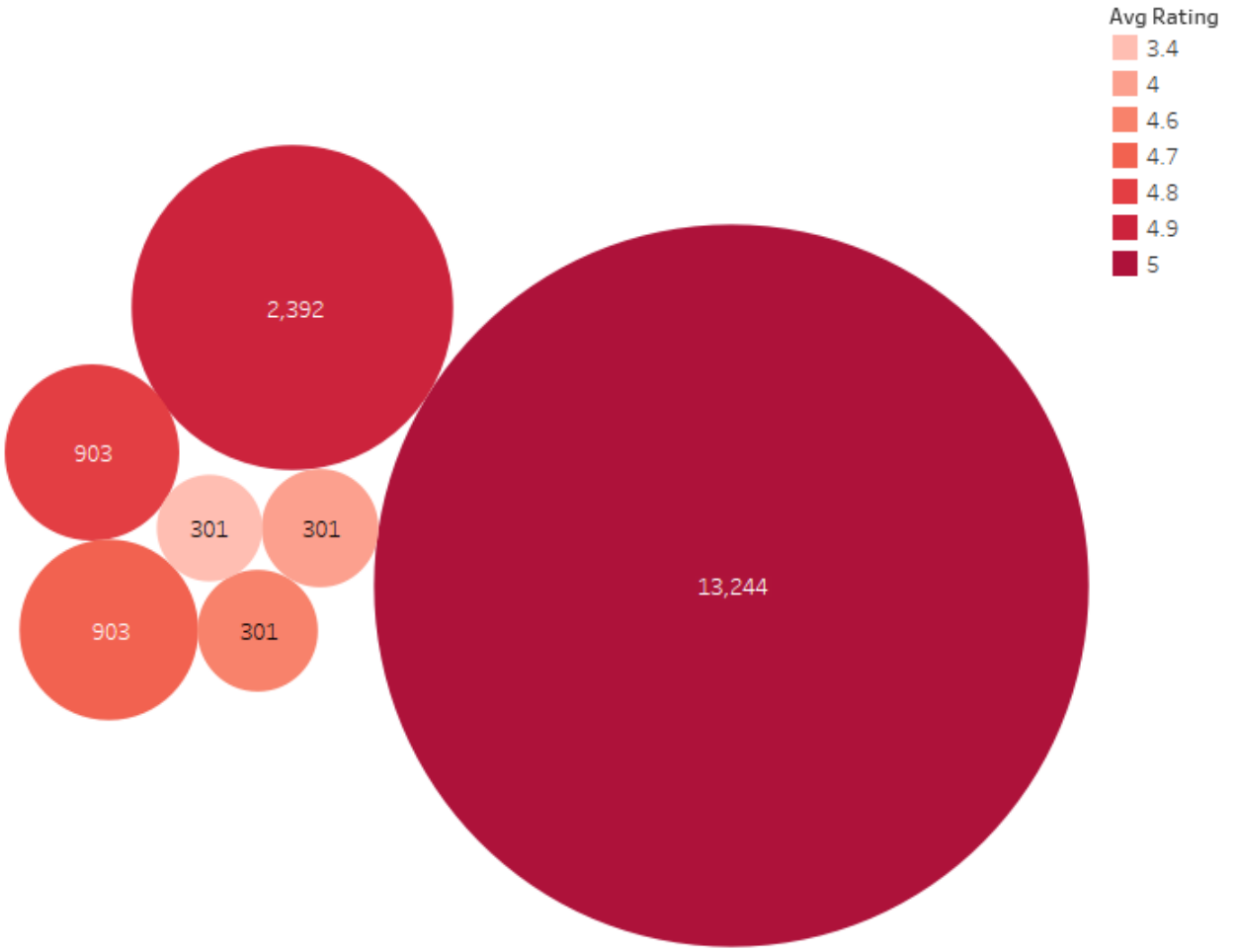

Figure 3.3.1.1: Top 10 sellers based on ranking [4]

Using the second data set from Dr. Aldridge and Dr. Décary-Hétu [4], we imported the data into Tableau. Using this data, we decided to create two maps. The first map, figure 5, is the countries from where all the trades are coming. The second map, figure 6, would have the countries to where the trades are delivered. In order to create figure 3.3.1.2 and 3.3.1.3, we display all the recorded categories. Not stopping at that, we also use the color scheme to show the origins and the destinations of the products. Each color is linked to a specific drug, by doing this, readers can clearly see the regions or countries which the drugs were coming from.

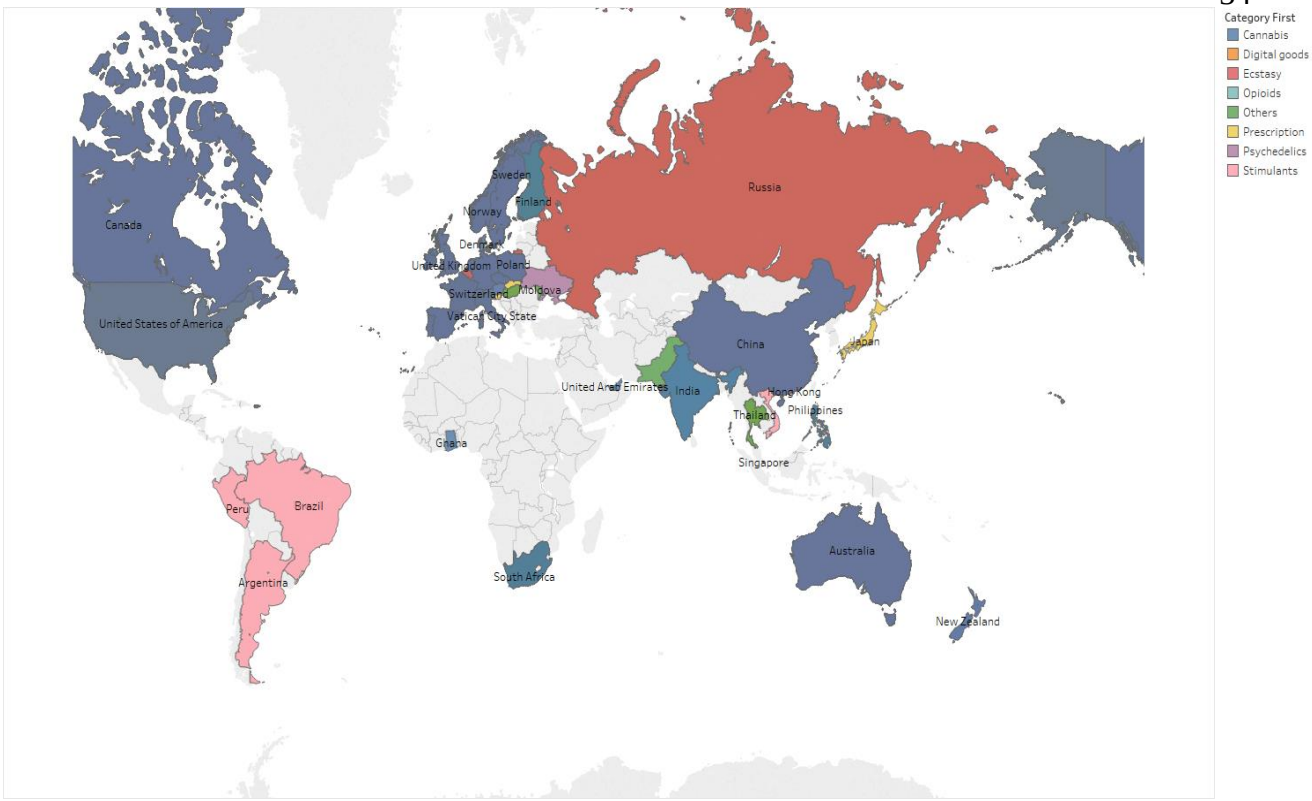

Figure 3.3.1.2: Sellers' countries of origin

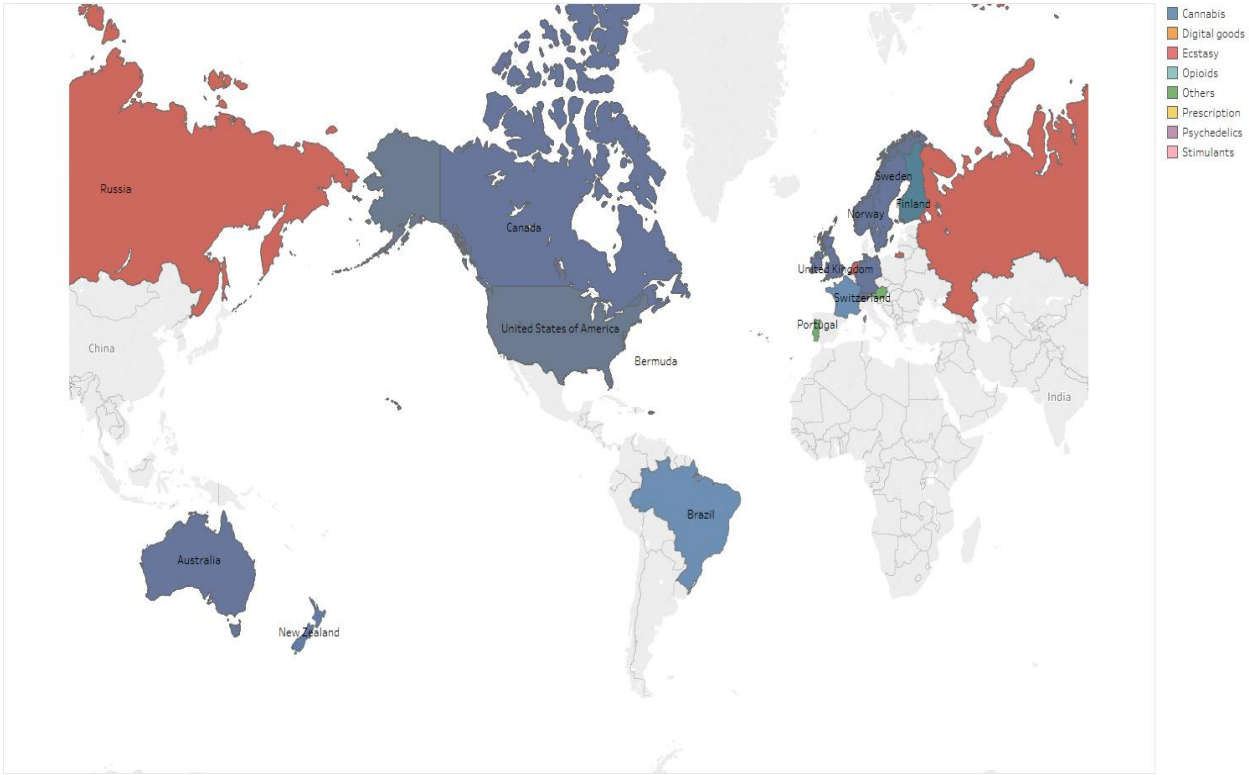

Figure 3.3.1.3: Transactions' destinations

3.3.2 Analyzing the Darknet with Data Science

According to EMC, linear regression is a statistical technique used to express a relationship between variables and a continuous outcome value. If linear regression is chosen as a method, it is safe to assume the relationship between the input and the output is linear. The reason for us to choose linear regression to express the relationship of the data set instead of any other method was because the data mainly consists of numeric value. Even when the prediction is restricted to a line, there are possibilities which the input can be transformed and modified so that the outcome will be linear [5].

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_{p-1} X_{p-1} + \varepsilon$$

Formula 3.3.2.1: Linear Regression [5]

With the data collected in Formula 3.3.2.1, we used a linear regression model for predicting the relationship between the attributes within the dataset. Y was the dependent variable, in our case it was the average rating for the seller. Not only that, X represented the independent variables which were life span, rank, transactions count, etc. For this study, we used to rank as our dependent variable. Since there were some missing data in the rank column, we decided to replace all the null value with the mean, 45.9. For the model summary, we found out that adjusted R-square value was 66%. This R-square result means that 66% of our data set fit into the linear regression model.

We also did an unstandardized and a standardized coefficient test. As the result shows, we can say that there is a relationship between the rank of the sellers who shipped their products worldwide and the number of transactions that they completed, with p-value is less than 0.001. Not only that, the ranking of the sellers also related to the number of products they sold because the significant value for bulk sellers is p = .049 which is less than p = .05. Residuals were tested to see the normality of the data set and are illustrated in Figure 3.3.2.1.

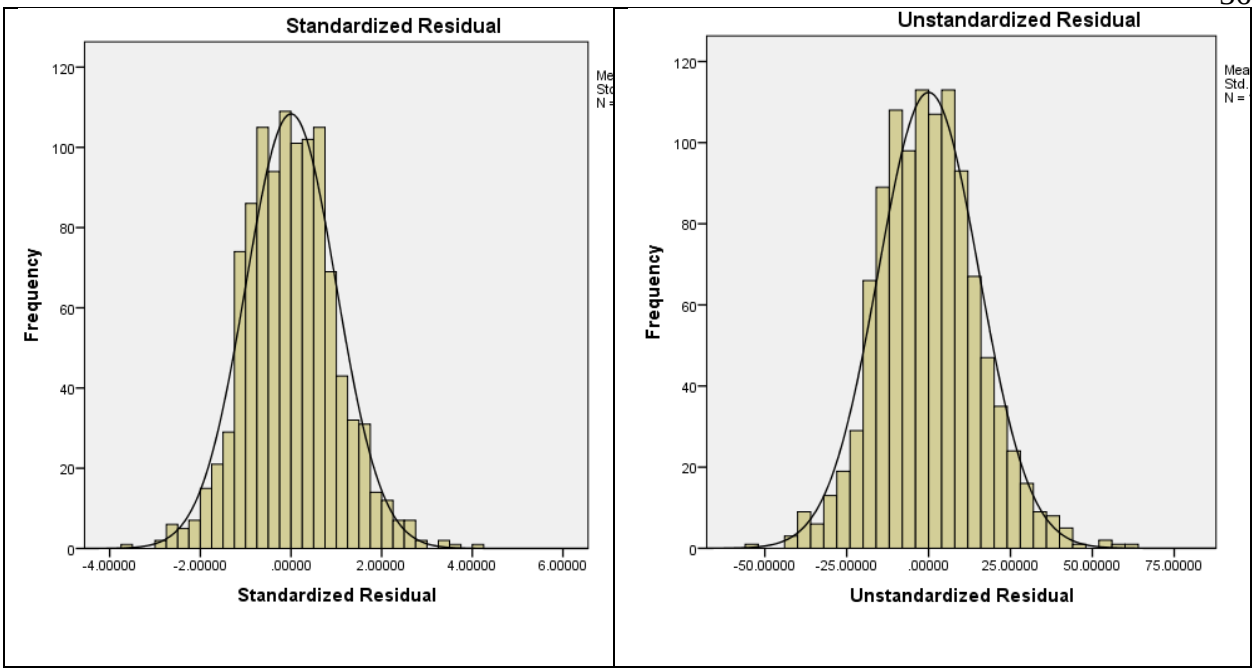

Figure 3.3.2.1: Residual tests

Using the same data set, we did a CART decision tree to find the pattern between the attributes. In order for this test to work with our dependent variable being rank, we had to transform the ranking of the data set. We assigned “highest” for sellers whose rank is between 76 and 100. We chose “high” for sellers whose rank is from 51 to 75. “Low” is for sellers whose rank is 50 to 26, and the “lowest” starts from 25 to 0. We chose the ranking (highest, high, low, lowest) as our dependent variable. After the CART decision tree test, we can break the data set down with 7 leaf nodes. The first split is where the transactions are less than 260.5 and equal to or greater than 260.5. Figure 3.3.2.3 details the decision tree produced by the CART algorithm.

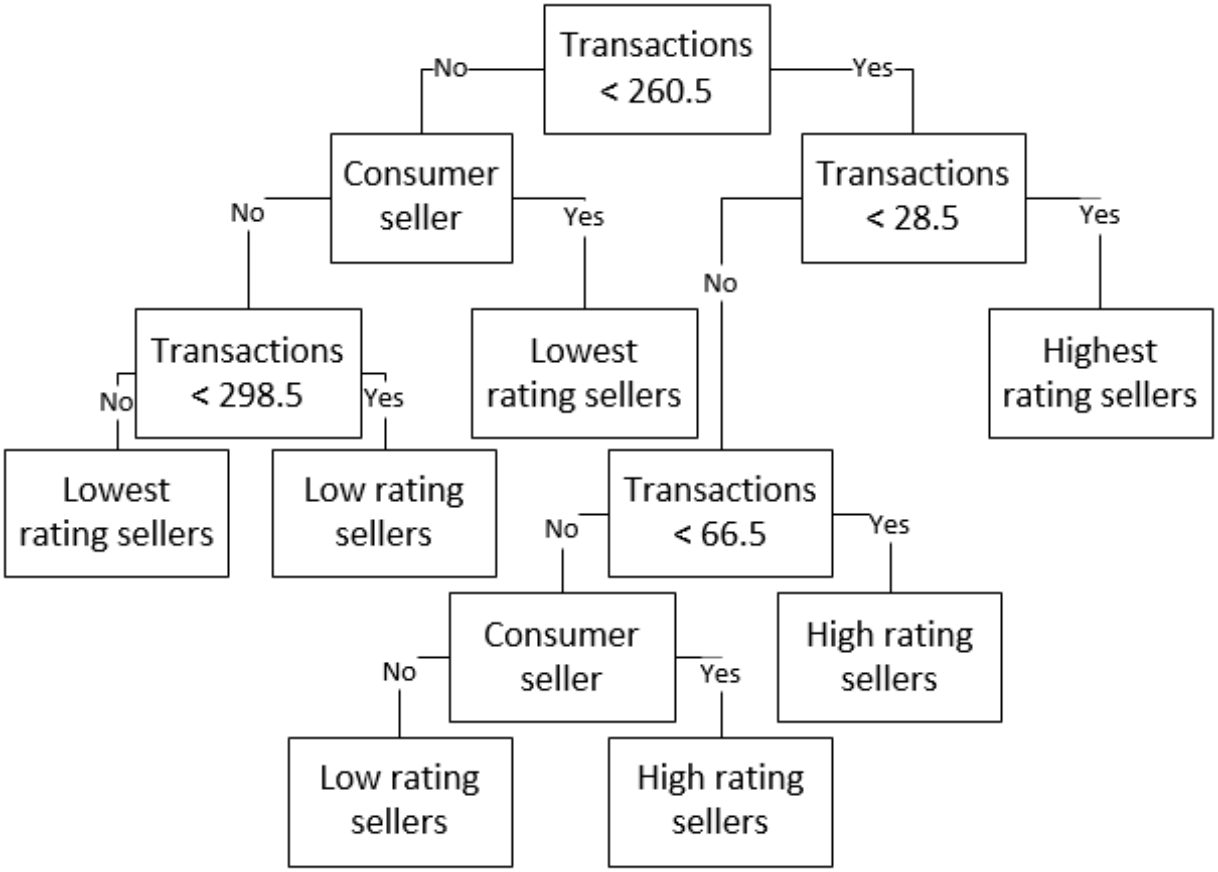

Figure 3.3.2.3: CART Decision Tree

For the group of sellers who has less than 260.5 transactions, the tree breaks down to sellers who have less than 28.5 transactions and sellers who have equal to or more than 28.5. The group of sellers who has less than 28.5 transactions has the highest rating. As for sellers who made more than or equal to 28.5 transactions, the decision tree splits between sellers who completed equal or greater than 66.5 transactions, and sellers who had less than 66.5 transactions will be categorized as high. As for sellers who had 66.5 transactions or more, they are broken down into high if they are consumer sellers and low if they are not consumer sellers.

As for the group of sellers who recorded with more than or equal to 260.5 transactions, they split between sellers who used their own product and sellers who do not. The ones who do are categorized as lowest rank. This time, the sellers who have less than 298.5 transactions are in low ranking, and the ones who completed equal to or more than 298.5 transactions are in the lowest ranking. There are 1083 instances in this model. While using the CART decision tree, we

can see that there is a 62.8 percent, which are 680 cases, that we can correctly classify the ranking of the sellers. However, we will incorrectly specify the other 37.2 percent, 403 cases. As for logistic regression test with 10-fold stratified cross-validation in place, the result is similar to the CART decision tree method. However, the correctly classified instances number is a bit lower compare the decision tree, 666 cases as 61.5 percent. The incorrect number of classified instances is 417, which is 38.5 percent.

3.4 CONCLUSION

Unlike other studies where their focuses are in criminal justice or terrorism [30-33], the purpose of our research is to review visualization and demonstrate the application of Tableau to the visualization of Darknet data as well as apply basic data science to Darknet data. We did not seek to validate the information or the data validity from the original study; however, we aim to demonstrate a new method to improve understanding of Darknet data. Many studies were conducted about crypto-markets. Unfortunately, these studies did not employ software such as Tableau to display the results nor did they apply data science and predictive analytics. Throughout this research, we learn (1) how crypto-markets are operating, (2) how the data related to the markets is collected, (3) how visualization can be used, (4) how we can use Tableau to process and display the result and (5) an application of data science for predictions in Darknet markets. We hope that this study will help future researchers further advance their results and help readers better understand their findings. As for future research, we suggest to try learning R and implementing with Tableau. Since Tableau integrates with R, this will provide even more customization, visualization, and analyzation on the data. If implemented correctly, we believe that this could turn Tableau into a very powerful data analysis and visualization tool for future studies.

4 EXPOSING THE DARKNET ON MOBILE DEVICES

4.1 INTRODUCTION

With technologies and mobile devices growing rapidly every day, it was more difficult for digital forensic tools and methods to keep pace [34]. We introduce a digital forensics tool, E3: DS created by Paraben. Our main interest is to examine artifacts from Orfox, a Tor-based web browser, on a Galaxy Note 5 Android smartphone. Based on what we found during our research, the most recent study about digital forensics on a mobile device, a Samsung S2 smartphone running Android 4.1.1, was performed in 2014 [27]. By examining the collected artifacts, we can reconstruct the user's Orfox browsing session.

Digital forensics (DF) is an interdisciplinary research area and practice between forensic science and computer science. DF uses methods which are scientifically derived and proven to acquire evidence through a well-defined process. Using this evidence, investigators can reconstruct the crime scene in order to find the culprit or help with future unauthorized activities or operations [35, 36]. Using E3: DS, we can access the needed information on the Galaxy Note 5 device. Then, after spending time carefully examine all the information, we can present our findings and show the security and privacy weaknesses which currently exist on the mobile Tor Browser Bundle. With the findings, law enforcement can improve their current digital forensics process on mobile devices. As for Tor users and developers, this will alert them as he users will be more careful while using the software and the developers will try to figure out how to overcome the vulnerabilities.

4.2 METHOD

In this study, we used a Samsung Galaxy Note 5 as our device. The model of the device was SM-N920G with 32 GB of storage. The operating system, which was installed on the device, was Android Marshmallow version 6.0.1. Version 6.0.1 was the newest version what was available on an Android device at the time the study was conducted, with an exception for Google's devices which had Android version 7 installed.

Orbot is open-source software which includes Tor, Polipo, and LibEvent. With Orbot, users can have a local HTTP proxy (port 8118) and a SOCKS proxy (9050) which allow them to access the Tor network. On a rooted Android device, Orbot can also redirect the traffic through the Tor network. The version which we use for this study is 15.2.0-RC-8-multi. We installed Orbot through the Android Play Store.

Orfox is also an open-source software and part of the Tor Project. It is built using the same source code as the Tor browser. Furthermore, Orfox is modified with more features which enhance privacy and make the software compatible with the Android operating system. The version of Orfox which we installed on our device is Fennec-45.5.1esr/TorBrowser-6.5-1/Orfox-1.2.1, which was uploaded on December 1st, 2016.

We went to [37] to download all the necessary software and performed the rooting process. The software, which we used, were ODIN v3.12.2, Magisk v12.0, Samsung antiroot removal v2.4, phh's SuperUser v1.0.3.3, and TWRP for Galaxy Note 5 International SM-N290G. The steps for the rooting process could be found on the site.

For our Samsung Galaxy Note 5, we navigated to the device's settings. Once we were in, we chose Developer options. While in Developer options, these options were turned on: developer, stay awake, OEM unlock, USB debugging, and verify apps via USB.

To generate data, we browsed through a list of sites: Facebook, Twitter, eBay, and Amazon. There were more steps in the web browsing process; however, we will discuss the

details in the result section. All of the aforementioned tasks were performed using Orfox when Orbot was active. To ensure that the device connected to the Tor network and the software functions properly, we visited check.torproject.org for a connection test.

First, we started E3: DS via our USB dongle. Once the application started, there were two options which were suggested by the software. One of the options was “Acquire Device”, this was what we would choose if we already had a case. The other option was “Add Evidence”, we chose this option. If “Add Evidence” option was chosen, a new case would be created automatically. Then, we navigated to “Mobile Data” and chose “Mobile Data Acquisition”. “Acquisition Wizard” appeared and asked for device type: “Portable Device”, “Android”, and “Samsung GSM”. Since we were using a Samsung Galaxy Note 5 with an Android operating system, we chose the Android option. Then, the type of acquisition was asked. We chose “Full Logical Acquisition”. As for the next screen, all the options were left as default and we chose “Start Acquisition” and waited until the process was finished.

Below, figure 4.2.1, was the screen shot of all the folders which were collected by E3: DS after the acquisition process. Under the device, we can see there is a file system folder, contacts, authentication data, call history, installed applications, SMS, MMS, media store, calendar, default browsing history, and settings. As for this study, we paid more attention to the file system folder.

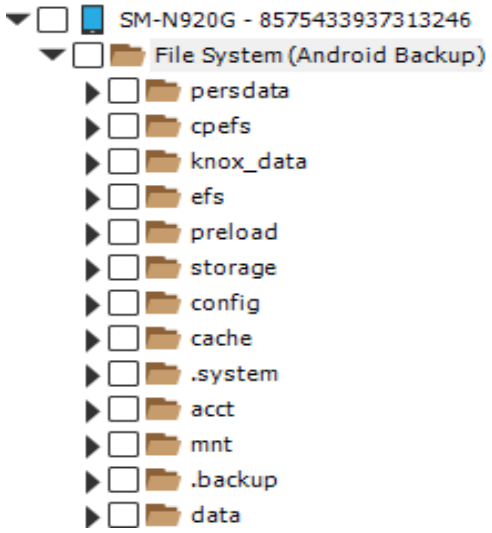

Figure 4.2.1: File system of the mobile device.

4.3 RESULT

After the acquisition process was finished, we explored our interested folders and files. After a few hours of examining all the collected files and directories, we found our target. Located inside "SM-N920G/FileSystem/data/User/0/info.guardianprohect.orfox/files/mozilla/51xiouku.default/", there was a file named "browser.db-wal". Using E3: DS, we could display the content of this file in text format. There were traces of what the user did during the Orfox browsing session.

Below were the four sites which we found tracks and believe to be a good example to show our findings with the Tor Browser Bundle. We split them into two categories: shopping and social media. For shopping, we chose Amazon and eBay. For social media, we used Facebook and Twitter. After showing the evidence, a comparison between two sites of the same category was presented.

4.3.1 Shopping

The first site we discussed in this section was Amazon. Figure 4.3.1.1a presented a link found in our text file. By analyzing the leftover evidence from the Orfox browser, we could see that the user was trying to sign in to the site. On top of that, there was information about the character encoding which is UTF-8. Figure 5.1a also showed us that Amazon was pulling the user's order

history and account status policy. Not only that, the user selected a few products which were available in the store. The selected products were Samsung Galaxy S8, S8 Plus, and a case for Samsung Galaxy S8 Plus, refer to figures 4.3.1.1b, 4.3.1.1c, and 4.3.1.1d.

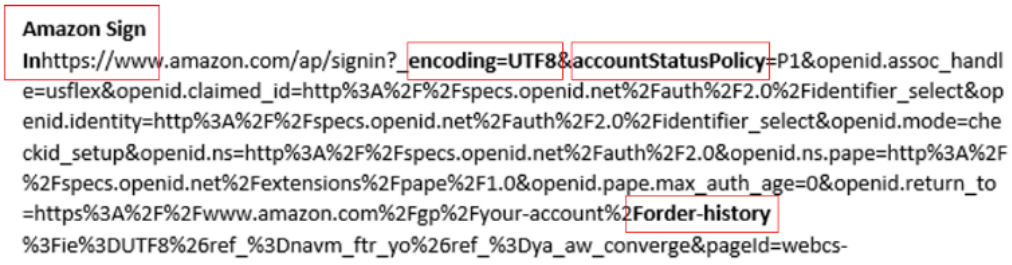

Figure 4.3.1.1a: Information on Amazon log in page.

Figure 4.3.1.1b: User's search history on Amazon.

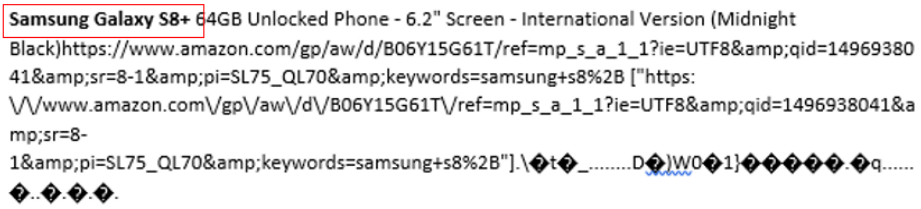

Figure 4.3.1.1c: More user's search history on Amazon.

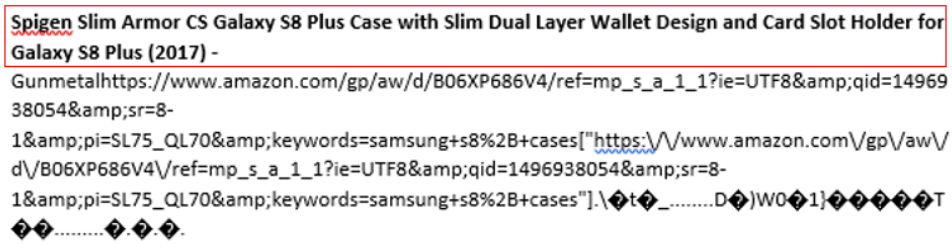

Figure 4.3.1.1d: Item user was interested in on Amazon.

The next shopping site which we used was eBay. As shown in figure 4.3.1.2a, there were traces left over from the user while at the sign-in page. Not only that, there was information about the

kind of protocol which was used to secure users' information. Furthermore, the user was visiting the Cell Phones and Smartphones section of eBay. The two devices which the user took an interest in were Samsung Galaxy S8 and S8 Plus, figure 4.3.1.2b. The final piece of evidence was Spigen, a producer of Samsung Galaxy S8/S8 Plus [Air Skin] Ultra Slim Lightweight Case Cover, figure 4.3.1.2c.

Figure 4.3.1.2a: eBay login page's information.

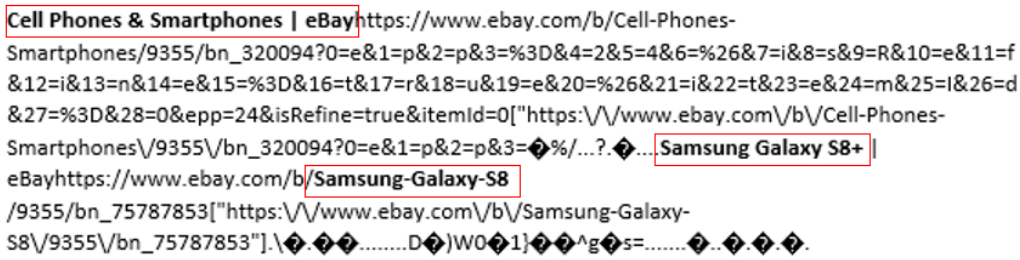

Figure 4.3.1.2.b: User's search history on eBay.

Figure 4.3.1.2.c: The last item searched on eBay by the user.

We intentionally chose the same products while surfing two shopping sites so that there would be a better comparison between them. After presenting all the collected evidence from the Galaxy Note 5, we saw that the information regarding the browsing sessions was identical. The product listing names were shown, refer to figure 4.3.1.1b, 4.3.1.1c, 4.3.1.1d and 4.3.1.2b, 4.3.1.2c. The only difference was the information about how the sites were set up, the format or the protocol that one site preferred over another, refer to figure 4.3.1.1a and 4.3.1.2a.

4.3.2 Social Media

The first site which we used for the social media example was Facebook. As shown in figure 4.3.2.1a, the user accessed Facebook and performed a search query with the key word “georgia southern”. Next, the user visited the active friend list on this Facebook account. Another search was performed, and the search query for this time was “danny don”, refer to figure 4.3.2.1b. The last piece of evidence which we found on the text file was presented on figure 4.3.2.1c. It was another search query with the keyword “ton don”.

Figure 4.3.2.1a: Facebook’s search query by the user.

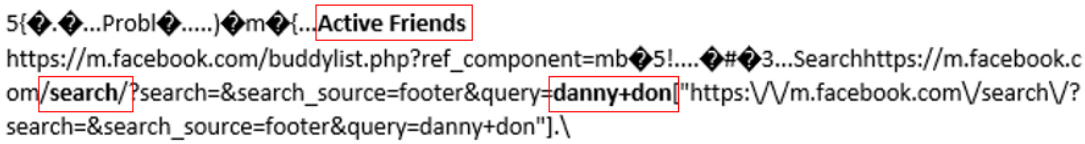

Figure 4.3.2.1b: Information about user’s search query.

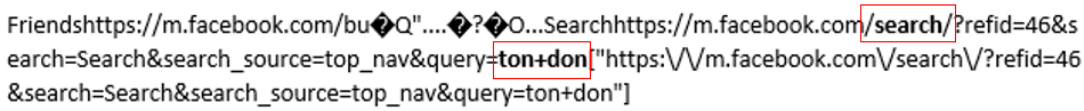

Figure 4.3.2.1c: Last searched query by the user.

Another example for social media site was Twitter. By looking at figure 4.3.2.2a, we saw the user’s Twitter ID, handle, and information about the website, the mobile Twitter site in this case. After signing into Twitter, the user’s search queries were found, figure 4.3.2.2b, 4.3.2.2c, and 4.3.2.2d. The last thing we want to present for the Twitter web browsing session was in figure 4.3.2.2e. GASouthernNews was the last thing the user visited while browsing Twitter.

Figure 4.3.2.2a: User's ID and handle shown on Twitter.

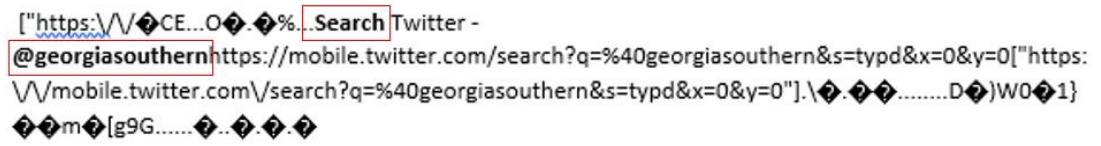

Figure 4.3.2.2b: User's searched query on Twitter.

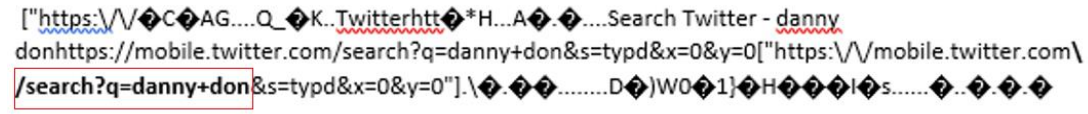

Figure 4.3.2.2c: Another search query performed by the user.

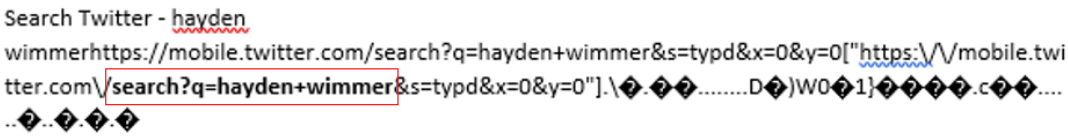

Figure 4.3.2.2d: More search query from the user.

Figure 4.3.2.2e: Last place the user visited.

Comparing the evidence found on the device between Facebook and Twitter, there were a lot of similarities. All the information about user's search queries were left behind after the web surfing session, figure 4.3.2.1b, 4.3.2.1c compare to figure 4.3.2.2b, 4.3.2.2c, 4.3.2.2d. The major difference between Twitter and Facebook was the user's ID and handle for Twitter were recorded, figure 5.4a.

4.4 CONCLUSION

In the past, multiple studies were conducted upon the Tor Browser Bundle. Since there were limited digital forensics tools and methods for the bundle [13], most of the studies analyzed the memory dump from the mobile device [12, 13, 27]. Because there has been a huge improvement in forensics tools and methods, we can better analyze the mobile device, Galaxy Note 5, from a new perspective. The Tor Browser Bundle is meant to leave no traces after the browsing session to protect user's privacy, but we prove otherwise. We found not only the places where the user visited, but we also discovered performed activities by the user. The information from this study can be useful to digital forensics investigators, the Tor Browser Bundle users, and developers. From an investigator's perspective, using this study, they can accurately examine mobile devices which have Tor software installed. For users, they can see that the Tor Browser Bundle doesn't fully cover their tracks. As for the developers, this study will give them more insight into their software weaknesses. For future studies, the same process will be used on different mobile devices and operating systems. More scenarios will be created and further tested to discover more about the software.

5 CONCLUSIONS

This thesis consists of two studies based on the same topic, the Darknet. For the first study, we focused on the information side of the Silk Road. Silk Road was one of the most studied online illegal trading websites from 2011 to 2013 [1-5]. On Silk Road, sellers and buyers conducted countless transactions anonymously. Using a collected data set from a previous study, the relationship between different variables of the data set were established. With the visualization capabilities of Tableau, the findings were presented normally and graphically to show the effectiveness of data visualization.

In the second study, we performed a digital forensic examination on a mobile device. Privacy and anonymity tools are increasingly commonplace which provides challenges for digital forensics investigators. Similarly, digital forensic tools continue to evolve which presents concerns to users. The Darknet is an illegal online service trading market which is hidden from the normal internet users. To address the concerns from both perspectives, this work sought to expose Darknet usage. We employed the commonly adopted Tor Browser Bundle on the Android platform. Using a mobile digital forensic software by Paraben, E3: DS, we extracted the mobile device's data, a Samsung Galaxy Note 5 using Android 6.0.1. We successfully extracted the data on the mobile devices and proved that users' information and traces were not fully protected by the Tor Browser Bundle, thereby refuting previous studies.

6 REFERENCES (use endnote or MS Word citation manager)

[1] TorProject.org, "Tor: Overview," 2017.

[2] S. Few, "Data visualization for human perception," *The Encyclopedia of Human-Computer Interaction, 2nd Ed.*, 2013.

[3] A. Kirk, *Data Visualization: a successful design process*: Packt Publishing Ltd, 2012.

[4] J. Aldridge and D. Décary-Hétu, "Not an'Ebay for Drugs': The Cryptomarket'Silk Road'as a Paradigm Shifting Criminal Innovation," *Available at SSRN 2436643*, 2014.

[5] EMC Education Services, *Data Science and Big Data Analytics: Discovering, Analyzing, Visualizing and Presenting Data*: John Wiley & Sons, 2015.

[6] J. Aldridge and D. Décary-Hétu, "Cryptomarkets and the future of illicit drug markets," *European Monitoring Centre of Drugs and Drug Addiction (EMCDDA)*, 2016.

[7] P. S. Alois Afilipoaie, "Operation Onymous: International law enforcement agencies target the Dark Net in November 2014," *Global Drug Policy Observatory*, 2015.

[8] J. Buxton and T. Bingham, "The rise and challenge of dark net drug markets," *Policy Brief*, vol. 7, 2015.

[9] K. Soska and N. Christin, "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem," in *24th USENIX Security Symposium (USENIX Security 15)*, 2015, pp. 33-48.

[10] Department of Justice. (2014). *Dozens of Online 'Dark Markets' Seized Pursuant to Forfeiture Complaint Filed in Manhattan Federal Court in Conjunction with the Arrest of the Operator of Silk Road 2.0*. Available: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/dozens-of-online-dark-markets-seized-pursuant-to-forfeiture-complaint-filed-in-manhattan-federal-court-in-conjunction-with-the-arrest-of-the-operator-of-silk-road-2.0

[11] S. Mansfield-Devine, "Darknets," *Computer Fraud & Security*, vol. 2009, pp. 4-6, 2009.

[12] A. Al-Khaleel, D. Bani-Salameh, and M. I. Al-Saleh, "On the Memory Artifacts of the Tor Browser Bundle," in *The International Conference on Computing Technology and Information Management (ICCTIM)*, 2014, p. 41.

[13] D. Dayalamurthy, "Forensic Memory Dump Analysis And Recovery Of The Artefacts Of Using Tor Bundle Browser–The Need," 2013.

[14] Anonymous. (2016). *Crypto Market Guide*. Available: http://silkroaddrugs.org/crypto-market-guide/

[15] C. Chrane and S. A. Kumar, "An Examination of Tor Technology Based Anonymous Internet," in *Proceedings of the 15th Informing Science Institute (InSite) International Conference, Tampa, FL*, 2015.

[16] N. Christin, "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace," in *Proceedings of the 22nd international conference on World Wide Web*, 2013, pp. 213-224.

[17] D. Rhumorbarbe, L. Staehli, J. Broséus, Q. Rossy, and P. Esseiva, "Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data," *Forensic science international*, vol. 267, pp. 173-182, 2016.

[18] R. Munksgaard, J. Demant, and G. Branwen, "A replication and methodological critique of the study “Evaluating drug trafficking on the Tor Network”," *International Journal of Drug Policy*, 2016.

[19] G. Branwen. (2015). *2014 in DNMs: by the numbers*. Available: https://www.reddit.com/r/DarkNetMarkets/comments/2r58vs/2014_in_dnms_by_the_numbers/

[20] Anonymous. (2014). *DarkNet Stats*. Available: https://dnstats.net/

[21] K. Morton, M. Balazinska, D. Grossman, R. Kosara, and J. Mackinlay, "Public Data and

Visualizations: How are Many Eyes and Tableau Public Used for Collaborative Analytics?," *ACM SIGMOD Record,* vol. 43, pp. 17-22, 2014.

[22] S. Watson and A. Dehghantanha, "Digital forensics: the missing piece of the Internet of Things promise," *Computer Fraud & Security,* vol. 2016, pp. 5-8, 2016.

[23] K. Dhar and Y. Pingle, "Digital Forensic Investigations (DFI) using Internet of Things (IoT)," in *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on*, 2016, pp. 1443-1447.

[24] E. Jardine, "The Dark Web dilemma: Tor, anonymity and online policing," 2015.

[25] E. Jardine, "Tor, what is it good for? Political repression and the use of online anonymity-granting technologies," *new media & society,* p. 1461444816639976, 2016.

[26] R. A. Sandvik, "Forensic Analysis of the Tor Browser Bundle on OS X, Linux, and Windows," 2013.

[27] N. Al Barghouthy and A. Marrington, "A comparison of forensic acquisition techniques for android devices: a case study investigation of orweb browsing sessions," in *New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on*, 2014, pp. 1-4.

[28] P. Corporation, "E3:DS," 6/5/2017 2017.

[29] M. Stone, "Choosing colors for data visualization," *Business Intelligence Network,* vol. 2, 2006.

[30] D. C. Alexander, "Student Projects Involving the Analysis of Web Sites of Extremist and Extremist-Affiliated Groups in the United States," *Journal of Applied Security Research,* vol. 6, pp. 184-195, 2011.

[31] W. Eberle, J. Graves, and L. Holder, "Insider threat detection using a graph-based approach," *Journal of Applied Security Research,* vol. 6, pp. 32-81, 2010.

[32] C. Roberts, "The US Federal Protective Service: A troubled agency—The need for improved contract guard training and oversight," *Journal of Applied Security Research,*

vol. 7, pp. 478-488, 2012.

[33] T. W. Van Dongen, "Break it down: An alternative approach to measuring effectiveness in counterterrorism," *Journal of Applied Security Research,* vol. 6, pp. 357-371, 2011.

[34] D. Lillis, B. Becker, T. O'Sullivan, and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," *arXiv preprint arXiv:1604.03850,* 2016.

[35] B. Carrier, "Defining digital forensic examination and analysis tools using abstraction layers," *International Journal of digital evidence,* vol. 1, pp. 1-12, 2003.

[36] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *International Journal of Digital Evidence,* vol. 1, pp. 1-12, 2002.

[37] M. Lee, "How to Root Galaxy Note 5 on Android 6.0/6.0.1 Marshmallow!," 2016.