information

MDPI

Article

A Framework for More Effective Dark Web Marketplace Investigations

Darren R. Hayes [1,2], Francesco Cappa [3,*] and James Cardon [1]

1 Seidenberg School of Computer Science & Information Systems, Pace University, One Pace Plaza, New York, NY 10038, USA; dhayes@pace.edu (D.R.H.); jcardon@cisco.com (J.C.)
2 Dipartimento di Ingegneria Meccanica e Aerospaziale, Sapienza Università di Roma, Via Eudossiana 18, 00184 Roma, Italy
3 Department of Business and Management, LUISS Guido Carli University, Viale Pola 12, 00198 Roma, Italy
* Correspondence: fcappa@luiss.it

Received: 30 May 2018; Accepted: 23 July 2018; Published: 26 July 2018

Abstract: The success of the Silk Road has prompted the growth of many Dark Web marketplaces. This exponential growth has provided criminal enterprises with new outlets to sell illicit items. Thus, the Dark Web has generated great interest from academics and governments who have sought to unveil the identities of participants in these highly lucrative, yet illegal, marketplaces. Traditional Web scraping methodologies and investigative techniques have proven to be inept at unmasking these marketplace participants. This research provides an analytical framework for automating Dark Web scraping and analysis with free tools found on the World Wide Web. Using a case study marketplace, we successfully tested a Web crawler, developed using AppleScript, to retrieve the account information for thousands of vendors and their respective marketplace listings. This paper clearly details why AppleScript was the most viable and efficient method for scraping Dark Web marketplaces. The results from our case study validate the efficacy of our proposed analytical framework, which has relevance for academics studying this growing phenomenon and for investigators examining criminal activity on the Dark Web.

Keywords: Dark Web; AppleScript; Web scraping; Silk Road; Dark Web marketplace; Web crawler

1. Introduction

The more familiar World Wide Web (or "Clear Web") is relatively easy to traverse, using traditional Web browsers, like Microsoft's Internet Explorer or Edge, Google's Chrome or Apple's Safari. However, the World Wide Web only accounts for a portion of Internet traffic, while content on the Internet that is unindexed is referred to as the Deep Web [1–3]. The unindexed portion of the Internet that is intentionally hidden and inaccessible by standard Web browsers is referred to as the Dark Web [3–7]. The Dark Web is an encrypted network that utilizes the public Internet. Among the various overlay networks, such as Garlic Routing or Tunnel Routing, the most widely used one is Tor Routing, which was originally developed as part of a secure communication effort of the U.S. Naval Research Laboratory, to protect and anonymize traffic by passing it through multiple layers of encrypted relays [8]. The Dark Web is purposely hidden using a peer-to-peer (P2P) network and Dark Web sites are primarily accessed using the Tor Browser, which is a user-friendly browser that protects the anonymity of the user, and can be important for individuals seeking to overcome censorship, ensure their privacy, or for criminals who seek to obfuscate their identity [9–13]. According to the Tor Project's Website, "Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security" [14]. The success of the Dark Web can be attributed to

this protection of individual privacy, which is of importance to both criminals and privacy-conscious citizens [15].

The Dark Web has gained notoriety, in more recent times, because of the exponential growth of Dark Web marketplaces after the rise (2011) and fall (2013) of the Silk Road [16–18]. The Silk Road was a Dark Web marketplace that facilitated vendors (often criminals) to surreptitiously sell drugs, counterfeit documents and other illegal items, anonymously to consumers, using Bitcoin as the crypto-currency of choice for buying and selling these commodities [9,19–24]. Bitcoin provides vendors, and their clients, with an extra layer of security on the Dark Web by leaving virtually no paper trail [16,25]. This highly successful marketplace was devised and administered by Ross Ulbricht until he, and the Silk Road, were taken down by the Federal Bureau of Investigation (FBI) and Homeland Security Investigations (HSI) [8]. This infamous marketplace was arguably so successful because of its enormous selection of drugs, which included new psychoactive substances, in addition to the professionalism offered by its customer support and the fact that its customers felt safe shopping there [20]. Several other marketplaces have spawned since then and different studies have analyzed how the number of vendors and sales in Dark Web have evolved [8,19,26,27], while the majority of them have shown year-over-year increases. Consequently, scientific interest in the Dark Web has increased, with studies focused on traffic analysis [13,28,29], and, in particular, methods to analyze these marketplaces while unveiling the identities of these vendors [5,24,30–32]. For example, the FBI successfully profiled users on the Dark Web, although these results were achieved using methods that are not available in the public domain [33]. Thus, there is a growing need to develop methods to facilitate investigations, based on tools commonly available to both academics and practitioners. The focus of our study is to posit and test a set of techniques for scraping Dark Web marketplaces and to gather information for further analysis, in a more accessible way for public and private entities. While companies like DarkOwl or Intelliagg are selling similar services online [34,35], we illustrated how Dark Web investigations can be performed more effectively.

After developing an automated scraping methodology, we tested it on a specific Dark Web marketplace. An analysis of the scraped data provided the basis for a subsequent investigation of suspected criminals (illicit vendors). The results from this testing demonstrate the efficacy of the proposed analytical framework (Figure 1) for automating data collection and making that collection process more accessible to Dark Web marketplace investigators. This framework is different from other methods, which are limited in availability and may incur significant costs. The framework is comprised of a number of steps, which are reported in Figure 1 [36]. The outcomes of our study are relevant for both academics studying the recent growth of Dark Web marketplaces, and for public and private investigators seeking to examine the nefarious activities of criminals operating on the Dark Web. In terms of Dark Web marketplaces, we have considered the recent attention of the Bright Internet, which seeks to realize a safer Web for individuals [37], thereby benefiting society.

In particular, herein we have demonstrated the power of utilizing automated scripting techniques, compared to conventional methods, which are critical given the negative influence of the Dark Web activity on society.

The paper is organized as follows: in Section 2 we discuss the background and analytical framework proposed in Figure 1; in Section 3 we describe the methodology of our research; in Section 4 we report the results of our case study; in Section 5 we discuss the implications of our research, research limitations and future research opportunities.

2. Background and Literature Review

The Dark Web represents an additional tool of the trade for traditional criminals [38]. In November 2014, police from the European Union and the United States seized hundreds of Tor "*.onion*" domains utilized by numerous drug marketplaces—including Silk Road 2.0 [1,19,39]. Criminals on the Dark Web today not only sell drugs, weapons, counterfeit currency and documents, but also use this anonymized network for other nefarious dealings [19,22,40–43]. Thus, academics and investigative

agencies have been trying to reveal transactions on the Dark Web. The Silk Road has been an interesting case study [44], in addition to subsequent Dark Web marketplaces, like Silk Road 2.0 [20,39]. A number of studies have attempted to quantify the growth and membership of these popular and successful online communities [8,19,45,46], and also to analyze their business models [44,47]. One researcher, for example, examined the growth of 16 different marketplaces after the demise of Silk Road, and analyzed how vendor security practices have improved over time. [26]. In February 2015, the FBI seized a server on Tor, called Playpen, which was used to distribute child abuse images [1]. The FBI successfully deployed tracking software, referred to as a "NIT", to unwitting client computers, visiting the Playpen server, and then successfully identified the real IP addresses for 215,000 users [1]. There are also several examples of the Dark Web being used by terrorist organizations [3,48].

The greatest challenge to analyzing the Dark Web, and investigating associated illegal activities, has been the lack of transparency and effective analytical tools because of encryption techniques and the anonymity of users [49]. These layers of encryption have provided anonymity to both vendors and their customers. Scholars and law enforcement must often rely on old-fashioned investigative techniques, which are available to the public. This approach involves taking data from the Dark Web and attempting to correlate that data, for example usernames, to make a positive identification on the World Wide Web. Alternatively, an investigator may run the data captured against an internal database of suspects or known criminals [46]. Dark Web marketplaces have thousands of product listings and user accounts, and therefore it is virtually impossible for manual investigative and analytical techniques to yield actionable data expeditiously. In fact, identifying marketplace owners, customers and products remains challenging [33]. Therefore, the aim of this research is to provide an analytical framework for automated scraping and analysis that can be more accessible to scholars and practitioners.

Identifying marketplace owners, and their customers, is still somewhat perplexing [33]. This research has provided empirical evidence of success, which has been derived from our proposed analytical framework (Figure 1). These results can be important for future studies that seek to further understand Dark Web marketplaces. The importance of doing so cannot be underestimated. Moreover, the relevance of this goal was also highlighted by the United Nation Office of Drugs and Crime, which emphasized the need to have more information about transactions and vendors on the Dark Web, in addition to those active on the World Wide Web [50]. Consequently, in our study we focused on developing and testing an analytical framework, displayed in Figure 1, using tools commonly available to scholars and practitioners.

Figure 1. Framework for automated and more accessible Dark Web market place investigations.

3. Methodology

As previously noted, our goal was to develop and validate the empirical efficacy of an analytical framework for scraping Dark Web marketplaces of interest, and correlating that data with Maltego and sites on the World Wide Web—a process that is outlined in Figure 1. Unlike many traditional Websites, we did not need to worry about violating any terms of service when scraping Dark Web marketplaces, since they are unauthorized. Furthermore, through our research, we determined that the Dark Web site that we scraped did not institute any type of throttling—a mechanism sometimes implemented on a Web server to prevent scraping or automated client requests. Thus, we did not need to integrate any type of time delay into our scripts.

Since neither traditional Web browsers, nor the Tor browser, can robustly search for Dark Web marketplaces, we initially used specific Websites on the World Wide Web to locate Dark Web marketplaces of interest. There are many helpful resources on the Web that can be used to find Dark

Websites of interest, but and the primary site of interest was the Reddit Website [51]. The ability of the user to search the Dark Web for narcotics or weapons has become easier [22,52] and there are many other helpful resources on the Clear Web that can be used to find Dark Websites of interest [53]. In terms of support for law enforcement, DARPA (Defense Advanced Research Projects Agency) has made the process of finding criminal actors, operating on the Dark Web, easier by developing a suite of tools, collectively known as Memex [3,54,55]. These tools were developed in collaboration with various universities and are primarily written in Python [32,56–58]. However, we have discovered that many of these individual search applications, within the Memex suite of tools, do not appear to be regularly maintained in terms of code updates, thereby rendering them inoperable. Additionally, not all of law enforcement agencies are authorized to use Memex, while other agencies may only have a specific investigative unit authorized to use the tool. Therefore, in this study we relied on different tools to develop an effective analytical framework for scraping Dark Web marketplaces, which is reported in Figure 1. The framework is important for both academics and investigators. In fact, using traditional methods of scraping, like Python scripts were not viable for our case study marketplace, as discussed later. In the following sections, we describe the steps involved in scraping marketplace data, correlating that data and then displaying our findings.

3.1. System Setup for the Dark Web

Our experimentation began with the installation of the Tor browser, from torproject.org, on a laptop. Prior to browsing Dark Web marketplaces we discovered the *.onion* URLs, for these marketplaces, from Websites on the World Wide Web, which in our case were Reddit (reddit.com) and DeepDotWeb (deepdotweb.com) [51]. The aforementioned Websites list the top Dark Web marketplaces.

Due to the sensitive nature of our research, we cannot disclose the specific marketplace that formed the basis of our study but we have detailed the ways in which data can be pulled from Dark Web marketplaces.

3.2. Creating a Web Crawler

The next step in gathering data from our Dark Web marketplace, was to create a Web crawler; a Web crawler is a programming script, which is used to open Web pages and then copy the text and tags from each page based on instructions within the script [59]. Many Web crawlers utilize the Python [32,56–58] scripting language, often leveraging the command line cURL tool to open the target Web pages. Attempting to use Python and cURL to scrape our target marketplace proved to be impractical. The Python *http.client* library module is what normally allows Python to be used for connecting to an http or https Website. This method works well on the regular World Wide Web but this library has no standard classes for handling Tor routing. The layered levels of encryption, and the selection/connection to intermediate Tor relays, are not available within Python. Lacking standard Tor libraries, within Python itself, the next option would be to use Python to leverage external http tools for the Tor access. For example, the "cURL" or "wget" tools are freely available command line utilities that can be used for http and https browsing. Using a tool like cURL, it is possible to build a Tor wrapper around that command line tool, which would allow cURL (or wget) to take advantage of the anonymization of Tor [60]. However, even following the above process, which would allow the use of cURL within a Tor wrapper, this process would still only provide (anonymized) access to the World Wide Web. The Dark Web *.onion* sites, which are not resolvable via the standard Domain Naming System, would still be out of reach.

Even if the *.onion* Domain Name System (DNS) lookup hurdle were overcome with something like a "requests" library, the marketplaces we investigated still presented the problem of CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) authentication, which is basically an obscured phrase that can be deciphered by humans but (in theory) not by automated bots. When using the Tor Browser natively, the browser provides the linkage between the CAPTCHA

challenges and responses, and then leverages that authentication for the duration of the browser's activity. By attempting to use the command line cURL utility, embedded in a Tor wrapper, the entire challenge/response process, and leveraging that authentication within an ongoing session, would need to be automated. The CAPTCHA system has been specifically designed to make this type of automation extremely difficult. Thus, the aforementioned hurdles made AppleScripts the best choice. With AppleScript, there is no need to develop a Tor-aware command line utility, or a *.onion*-aware DNS lookup system, or an automated CAPTCHA challenge/response system. Instead, AppleScript can be used to drive the native Tor client and only the process automation steps needed to be scripted.

AppleScript, is a process automation utility, similar to PowerShell for Microsoft Windows. We relied on this tool because of its ability to (1) open and copy content from "*.onion*" Web pages, thereby eliminating the need to understand or process CAPTCHA authentications prompts when starting a new session, (2) its availability as a free scripting tool for Mac OS X, and (3) the availability of a Tor browser version for Mac OS X. Additionally, since AppleScript is generally used as an interpreted scripting language [61]. This allows an investigator to personally review any shared code (Figures 2–5), thereby giving them confidence in what the script is doing. This type of source-code review would be less reliable if a compiled language were used, since a binary executable could potentially have been altered and may differ from the source code it was purported to have been compiled from.

Our research was conducted primarily using AppleScript on an Apple MacBook Pro (mid-2015) running OS X El Capitan 10.11.6. The *Script Editor* utility is enabled within the *System Preferences* > *Security & Privacy* tab. After enabling the feature, the Script Editor itself can be found within the *Applications/Utilities* folder, or by searching for "Script Editor" with the Apple *Spotlight* utility. The only customization of the Script Editor tool, which we performed, was to enable logging even when the editor is not open and viewable.

The AppleScript written for this research was comprised of three parts. The first part contains generic housekeeping functions, written independently of the marketplace requirements. For example, this part contains functions that perform file read/write operations, calculate time stamps, manipulate text strings for parsing and searching, and perform generic browser functions. "Figure A1" in Appendix A displays a code sample for a function that prompts a user for input.

The second part of the AppleScript performs the Web scrapping of product listings from the target marketplace. This function parses the marketplace menus to determine all advertised product categories, and then steps through each page of each category in order to record the seller account and product information. A sample of this product scraping code is shown in "Figure A2" in Appendix A. The final part of the AppleScript includes the functions for parsing the user data for each of the product seller accounts. This scraped data provides user-specific information for each account, which is what provides the most interesting information from an investigative standpoint. A sample of the account-scraping code is shown in "Figure A3" in Appendix A. The data collected through the AppleScript, reported in "Figure A4" in Appendix A, has been analyzed to investigate the categories, number of listed items and sellers.

3.3. Determining the Structure of the Dark Web Marketplace

When designing and constructing a Web crawler, it is critical to map out the structure of the Website. This is because the AppleScripts are programmed to automatically enter different URLs and then search and copy data from each page, by using the HTML (HyperText Markup Language) tags and static text as a guide to the structure of the page. "Figure A4" in Appendix A shows examples of how these HTML tags can be used to parse the desired information from a marketplace Webpage.

These HTML tags would ultimately provide a structure for how the information would be stored in our database. To clarify, if we were using a Web crawler to scrape Amazon.com, then we would go to the home page and copy the information. We would then select a category like "Books" and then copy that information. Subsequently, we might go to the next sub-category—"Children's Books"—and then copy that information. Finally, we might go to the next level down (sub-category) and select

"Ages 3–5" and then copy that information to our database. There is a different URL structure for each category and sub-category—therefore we need to understand how the URL changes for each category and sub-category. This was important so that we could automate the Web crawler to enter each URL and find each category and sub-category. Nevertheless, it is critical to understand how the structure of URLs, the names and locations of HTML tags on Websites, both on the Dark Web and World Wide Web, continually change; these changes necessitate changes to the scripts in a Web crawler.

The Dark Web marketplace that we selected contained twelve top-level categories, e.g., "Drugs & Chemicals", and these categories were then further divided into more than 60 sub-categories, e.g., "Drugs & Chemicals > Ecstasy"; additionally, there were more than 100 third-level categories, e.g., "Drugs & Chemicals > Ecstasy > Pills". Like many similar Dark Web marketplaces, drugs were the most popular commodities [39]. Other highly populated listing areas of the marketplace we analyzed were "Credit/Gift Card Fraud" and "Identity Theft" data dumps.

The AppleScript we developed was able to record information about as many items for sale as possible. The URL for each category listing was comprised of three parts (1) marketplace address, (2) category number to be searched (i.e., any of the 117 third-level categories discussed earlier) and (3) the category page number to view, as displayed in Figure A5 in Appendix A.

Each marketplace category provided up to 50 pages of listings. Within each page, up to 15 items were listed for sale. The format of each of these listings was consistent, thereby allowing the AppleScript to record the relevant information—in particular, the *Account Name* of the seller, which would later prove to be key. An example of a listing, pulled from the marketplace, can be viewed in "Figure A6" in Appendix A. After pulling the data for more than 30,000 items for sale, a second AppleScript was written to download the account details for all the marketplace sellers. The Web URL for an Account listing was also comprised of three critical parts, as displayed in "Figure A7" in the Appendix A. Analogous to the previous example, the first part of the URL, displayed in "Figure A7", is the marketplace address. The second part of the URL is the account name, which was taken from the listings and which was obtained (scraped) by the first script. The third part of the URL, displayed in "Figure A3" in Appendix A, is the user tab view. The marketplace account pages were comprised of six different tabs, two of which were scraped by our script; the "About" tab listed user-provided information, which included email addresses, chat accounts and free form data; the "PGP" tab listed the user's PGP encryption key, which was a requirement for every seller. PGP (Pretty Good Privacy) is an encryption protocol used for secure communications, i.e., to prevent a third-party from eavesdropping on a user's email conversation. The rationale for capturing the PGP key was that it could potentially be later used to positively identify a vendor or customer if a suspect's computer was ultimately seized. Additionally, the PGP key, and *Account Name*, could potentially be used to link sellers on multiple marketplaces; many vendors who were operating in our case study marketplace maintained a presence on multiple Dark Web marketplaces. The *About* tab contained information that may be of interest to an investigator and included email/chat addresses, preferred currency and time zone.

3.4. Investigating Marketplace Vendors

The final step in our analysis involved an examination of sellers operating on our target marketplace. We identified vendors on the Dark Web marketplace using data collected from our Web crawler and subsequently used a number of free tools found on the World Wide Web to facilitate our investigation [62]. Given that there were over 3000 distinct vendors operating on this marketplace, we determined that we needed to substantially reduce our focus list of vendors, since the investigative process involves a manual examination, which was in contrast to our initial automated data collection with the (AppleScript) Web crawler. We decided to focus on drug dealers during our manual analysis. Our rationale for this selection was that some drug dealers were extremely active, they sell on multiple marketplaces and their usernames can be quite distinct, e.g., *st0n3d*.

The tool utilized for our analysis of individual vendors was called Maltego, from Paterva [63]. The company produces different versions of Maltego but we opted to use the free version. Maltego is a tool, which allows you to take distinct user characteristics and then perform a link analysis to display where that user can be found across the Web. For example, any combination of a username and/or telephone number, email address, IP address or other personally identifiable criteria can be added into the user interface; Maltego refers to these searches as "transformations".

Once the criteria were entered, Maltego identified where on the Web those same user identifiers can be found. For example, a username may be associated with a Facebook account and a Twitter account; an email address could be associated with a LinkedIn account or a domain name registration. Additional analyses were then carried out on the Maltego results in order to eliminate false positives. For example, a specific username may be associated with one person for Facebook but that same username may be used by someone else on Twitter.

The following is the general workflow that we followed, when using Maltego, to identify vendors on the focus marketplace, which represents the last step of our analytical framework for Dark Web investigations:

1. Downloaded, installed and executed Maltego CE 4.0.11.9358 [63];
2. Selected 50 vendor account names, from the marketplace, which warranted further examination. Note that the free CE (Community Edition) version of Maltego only supports 50 entries at a time; the paid version allows more concurrent searches. Criteria used to select these vendor account names of interest, included:
    a. Interesting or unique names that a vendor may re-use on the World Wide Web;
    b. Accounts with a high trust and vendor level, is generally indicative of a more active vendor;
    c. Focused on categories of particular interest, i.e., drugs or credit card fraud;
3. Used the Maltego "Create a Graph" option to start a new investigation, and entered in the selected account names;
4. Once the account names were imported into Maltego, we executed different transforms against them:
    d. "To Email Addresses [using Search Engine]";
    e. "AliasToTwitterAccount";
    f. "To Website [using Search Engine]";
    g. "To Phone Numbers [using Search Engine]";
5. After the transforms finished running, we used the "Export Graph to Table" option to output the file into a flat text file for further investigation;
6. Manually parsed through the resulting table using Microsoft Excel or another application, and eliminated any obvious false positives—for example, "online@cvs.com" is almost certainly a generic email address legitimately used by the CVS Drug Store and would not warrant a further investigation;
7. Combined the results from Maltego with the address links already pulled directly from the marketplace and used the Tor browser to protect the investigator's privacy. Then we performed Web searches on the results that appeared to be most interesting. Note that this process can be very tedious, as it requires a manual examination and judgment calls to decide which routes are most likely to lead to a successful identification. For example:
    a. Drilled down into any Reddit or 4chan or Twitter or YouTube or similar public sites to try to find alternate accounts used by the user;
    b. Used the www.whois.com to find any domain name registration information for Clear Web Websites associated with these users; and
    c. Used Google Reverse Image Lookup to identify alternate versions/locations of any pictures identified as related to the users.

The aim of this research was to empirically demonstrate the efficacy of the aforementioned steps of the analytical framework reported in Figure 1, with the goal of making Dark Web marketplace investigations more accessible and automated. Our findings, derived from following the aforementioned steps are reported in the following section.

4. Results

The AppleScript Web crawler successfully pulled account information for more than 3000 vendors from the target marketplace. Figure 2 displays the structure of the data pulled, and Figure 3 displays a sample of actual data pulled by the Web crawler, which displays vendor information.

```
account,accountActivity,vendorLevel,trustLevel,memberSince,ICQ,eMail,Chat,Website,PGP,Data
```

Figure 2. Structure of Vendor Data from Marketplace.

MaryJane400,36345,8,8,March 19, 2015,698299060,No information,
MaryJane400@jwchat.org,http://ogjfsfodjgsjdfkkf.onion,{$KEY},{$DATA}

{$KEY}

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG C# v1.6.1.0

zTEXVFSWKO0BCADA9xL1i2FIlRSDeaLS5oh8uyBFh2zVlwLGiexQ1dgT1RYiFngO
yccdhpD3a9JqnHFW0FQOYBeYetMIajkCyzJnTLjPZPidipyISeWRd++UYI0I9bJb
k6MlKFyVs06ofM4kq43bf2g5PTSAZKo5kYuFZfn7TSR5vdTpB14oMpzy0QGb1kO/
+gCXXrA58g6EhnUiqGjIBP6hsdUh+3+g0Y4UWeJd/rqntzx8nMDWBWmLaJnshRvZ
nVRdqcqe3AtvncOV57yCdQic2C0vrj9jdPblQcPZ0wntA0+gNePRKMxV2gD439Gj
Xi5EvBY8S6HK8Dj1nIWYzfRXQY2Y+XrdP/P7ABEBAAG0FHJlZHNvbkBzYWZlLW1h
aWwubmV0iQEcBBABAgAGBQJUFijtAAoJEDgJmV8Xfj+XBRYIAJjdWz8+3GxK/GRx
zQKjWDQTxxT5WT/6UKOR5Re/Ei7T7vF2+/6C0bxQpOb7tY5qCFbJQ58fzRQlzZE+
yXZbdNe09WbDhcu+8ZtPVODwB3upbs6fG7UMm2roalo6I+i3LWaeIL+VOSd7RL0w
HCg9Fwc4mn+MTlE7qsr15yCg5z7mPzGXZze9qD+g8SsGYbMmOKaR5wE7bX7yUNRi
47yW7sVCwrgIpEbGtt34QXnm0lxLrbh855voqSayuQvc7ua9CF0dmGdC1F6YggNY
fplWzl6NfxLWahoaOv4YJm4udCiA3+gUlZDipTAKMIV20yL6zPBmJbZphwJzvvgQ
tODm9yA=
=PeRO
-----END PGP PUBLIC KEY BLOCK-----
```

{$DATA}

```
############################################################
CONTACT ME :
SHOP : http://sdfjj.su / http://rrthdfgfdtllnoqyuu.onion
JID : MaryJane400@jwchat.org
EML : MaryJane400@safe-mail.net - MaryJane400@dotanota.de
ICQ : 598277020
############################################################
```

Figure 3. Sample Vendor Data Retrieved from Marketplace.

Running the account script took approximately 15 s per account; as a result, running it against the 3000+ unique accounts took approximately 15 h to complete, which represents a reasonable amount of time to perform investigations. The script continuously kept track of all accounts that were previously found. This step allows subsequent AppleScript executions to complete in less time, since only new/unique accounts were collected upon each execution.

The script was written in such a way that it could be run against specific categories or against a fewer number of pages, to enable it to complete a more targeted crawl in a shorter space of time. Once the script stopped running, we had collected information on 33,667 unique listings, which were being offered for sale by 3388 unique seller accounts. Figure 4 below displays the structure of the data for each listing and Figure 5 displays sample data pulled from actual listing by the Web crawler.

```
itemNumber,sellingAccountName,itemDescription
```

Figure 4. Structure of Listing Data from Marketplace.

```
154864,MaryJane100,20mg adderall xr straight from the pharmacy
188400,MaryJane200,7x aderall 20 mg.
281776,MaryJane300,150mg Methylphenidate IR (Concerta/Ritalin) 15x 10mg Tablets
```

Figure 5. Example of Data from Retrieved Listings.

Figures 6 and 7 below provide some perspective about the marketplace listings, i.e., types and quantities of unique items being sold, and the number of unique sellers offering those items for sale, in each of the marketplace categories. In particular, Figure 6 shows the distribution of items for sale across the twelve root-level categories within the marketplace. The "Drugs & Chemicals" category has by far the most listings, with 18,358 (55% of the total), and illustrates how drugs represent the vast majority of transactions on Dark Web. Figure 7 displays the number of unique sellers who are offering those items for sale. Again, the "Drugs & Chemicals" category has the most unique sellers, with 2226 vendor accounts (66% of the total) mirroring the results of the most common item sold.

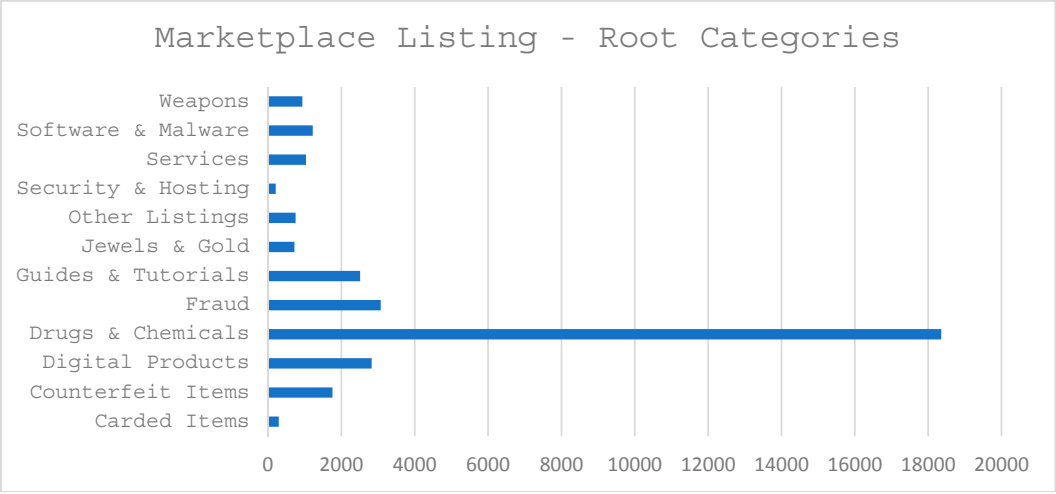

Figure 6. Marketplace Listing—Root Categories.

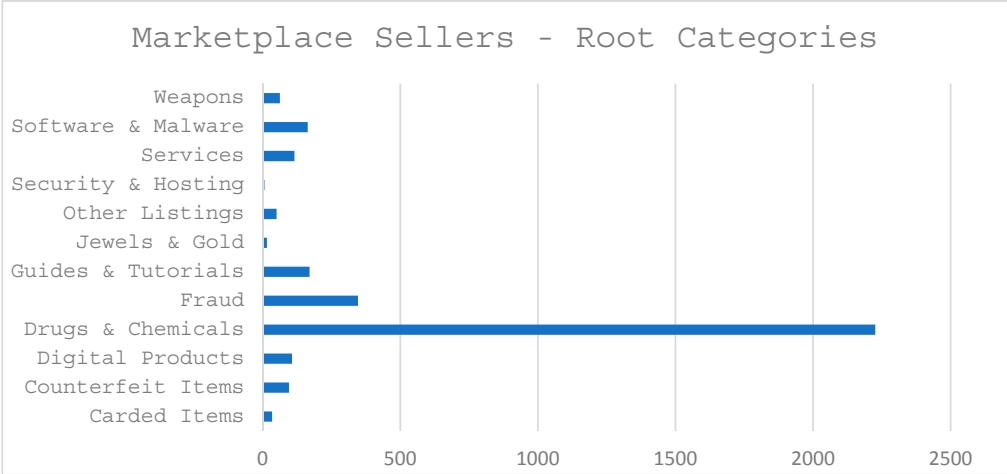

Figure 7. Marketplace Sellers—Root Categories.

Since the "Drugs & Chemicals" category makes up over half of the total marketplace offerings, and over two-thirds of the marketplace sellers, we drilled down further into the related sub-categories. The most active marketplace listing could be characterized as various forms of Ecstacy, with "Ecstacy/Other" being the most popular sub-category, with 1090 listed items for sale (although this category only makes up 6% of the overall Drugs category). There were various forms of Ecstacy available; the specific "Ecstacy/Other" subcategory contained 174 listings (8% of the total Drug sellers); Benzodiazepine Pills accounted for the largest single category, with 196 listings (9% of the total Drug sellers). Although the aforementioned data could be also be retrieved without a crawler, it is important to visualize the type of data that can be collected in an automated way using accessible tools for investigators within the context of the proposed analytical framework.

Ultimately, using Maltego, we positively identified four vendor accounts, amongst the most active accounts, as noted in Figure 8. However, none of these vendors appeared to reside in the United States. Figure 8 displays the vendors identified (the actual names of the vendors have been redacted for security reasons). Based on the data pulled from the marketplace, "Vendor Level", i.e., number of active product listings, was generally higher for the most active vendors. The value assigned to "Trust Level", is based on customer ratings and satisfaction with vendors. We do however know that these four vendors were very active on our subject Dark Web marketplace.

Vendor 1
Vendor Level (5) Trust Level (5)
Country: Germany

Vendor 2
Vendor Level (8) Trust Level (8)
Country: Russia

Vendor 3
Vendor Level (7) Trust Level (7)
Country: Panama

Vendor 4
Vendor Level (7) Trust Level (6)
Country: Bahamas

Figure 8. Marketplace Vendors Positively Identified (Names Redacted).

The results of our study empirically demonstrate the efficacy of our methodology to perform more automated searches and provide more access to information from Dark Web marketplaces through the use of AppleScript and free online tools, thereby supporting the applicability of the analytical framework proposed in Figure 1.

Like any Website scraping (Web crawling) on the Dark Web or Clear Web, the location of the data and HTML tags can change over time, and this necessitates changes to the Web crawler script. This issue will be examined in future research studies. An additional limitation of note is that when manually entering personal identifiable information, into Maltego, there were many false positives in the results. Thus, the importance of investigative expertise, to eliminate false positives, cannot be underestimated. Although this type of elimination is a manual process, the utilization of the analytical framework proposed in this study saves the investigator a substantial amount of time in identifying relevant information using several automated steps, thereby allowing an investigator more time to more effectively eliminate false positives and, ultimately, positively identify marketplace vendors.

Furthermore, there are many usernames that are virtually impossible to positively identify. For example, the account name *maghreb*, which means "Morocco" in Arabic, could not be tracked to a specific person through Maltego. Another pattern we noticed was that people would try to take the names of well-known companies, like "Go Daddy", as their usernames. Naturally, the overarching limitation of our study is the security and anonymity provided by PGP for communication between vendors and customers, the Tor browser for anonymous browsing and the use of a crypto-currency (Bitcoin) for transactions.

Finally, interacting with marketplace vendors and purchasing their products can provide an investigator with more personal information about sellers. We did not engage in dialogue with any vendor and did not purchase any products from the marketplace, which could be viewed as a limitation of the research and our findings.

5. Discussion and Conclusions

Recently, interest has increased in the Bright Internet, which is a safer Internet for users [37]. Consequently, there has also been increasing interest in illicit transactions on the Dark Web [24,31,64,65]. Currently, mainly proprietary or non-easily accessible and implementable techniques for Dark Web marketplace investigations are available [33,46]. Thus, there is an increasing need to make Dark Web investigations more accessible and more practical for scholars and practitioners [2,3,50]. With this study, we provided evidence for an effective analytical framework, reported in Figure 1, which has provided insight into vendors' origin statistics and can be very important for policymaker decisions and also for public and private investigations. Compared to currently available techniques, the analytical framework proposed in this study, can guide practitioners and academics towards a different and more effective way to perform Dark Web investigations. More specifically, we have made investigations more accessible to interested audiences, who may not have access to certain online services, and made searches more automated compared to traditional techniques. The goal of this research is to respond to the need to more effectively monitor Dark Web marketplaces [2,3,50]. Moreover, we also aim to stimulate research interest to further develop techniques that facilitate more efficient Dark Web investigations.

Historically, academic researchers, and government, have primarily relied on Python scripts, which are not always feasible and easy to implement to scrape Dark Web marketplaces [31,32,56–58]. In this study, we successfully created a more accessible Web crawler, using AppleScript, to scrape thousands of vendor account details, in addition to thousands of their product listings. The approach proposed in this paper advances the existing academic literature and practice in multiple ways: (i) it explains how Websites, like Reddit, can be used to identify Dark Web marketplaces, a process that can be further automated by future studies (ii) it provides an alternative to the highly-publicized Memex tool, while providing access to many law enforcement agencies, who generally do not have access to Memex; (iii) the Web crawler, developed with AppleScript, provides a more versatile method

of scraping, while providing the ability to verify the code in the scripts; (iv) it uses process automation to control the existing Tor Browser application avoided the complexity of managing the underlying onion network encryption layers, and also eliminated any need for the scraping utility to understand or process CAPTCHA authentication prompts. In fact, with AppleScript, there was no need to develop a Tor aware command line utility, or a *.onion*-aware DNS lookup system, or an automated CAPTCHA challenge/response system. Instead, AppleScript can be used to drive the native Tor client and it is only the process automation step that needed to be scripted; and finally (v) our analytical framework utilizes free tools, including AppleScript and Maltego, which are accessible to both scholars and practitioners.

The success of the Silk Road marketplace has inspired others to emulate the success of Ross Ulbricht. These marketplaces negatively impact the health and welfare of society and therefore we need to develop more means to disclose the names of drug dealers and other nefarious actors operating on the Dark Web [1]. As noted earlier in our research findings, drugs are by far the largest category for vendors. Although Tor largely provides anonymity for buyers and sellers on these Dark Web marketplaces, this research has demonstrated how data pulled from these marketplaces can be used to successfully identify criminal suspects who sell illegal narcotics, peddle stolen payment card information and trade other illicit items to interested consumers. Thus, the results of this research are tremendously important for both the academic community and for law enforcement agencies worldwide, who are searching for effective methods to track and disrupt Dark Web networks [1,5,8,9,31,32,40,66]. In fact, the existence of the Dark Web represents a threat for "Cyberpeace" [67–69], which can be defined as "a wholesome state of tranquility, the absence of disorder or disturbance and violence" [69], and the analytical framework proposed in this study for more accessible and automated investigations can positively impact both public and private organizations [70].

Author Contributions: All three authors equally contributed to the research and writing of this paper.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

```
--*******************************
-- Prompt with a dialog
--*******************************
on MakeSelection(myPrompt, myButtons, myTimeout) -- return string
tell me to activate -- Ensure that the new dialog has focus

set selected to ¬
   display dialog myPrompt buttons myButtons ¬
       giving up after myTimeout

if DEBUG ≠ 0 then ¬
   log "You pressed '" & button returned of selected & "'"

return button returned of selected
end MakeSelection
```

Figure A1. Sample Code Snippet for Dialog Prompt.

```
-- Parse the html text to find each of the displayed listings
repeat while (html ≠ null)
-- Find the next listing
set html to SnipString("right", html, ¬
"<a class=\"notext\" href=\"listing.php?id=")

if html ≠ null then
-- Snip this listing number out of the html text
set end of listingNumList to SnipString("left", html, "\">")

-- Snip this listing title out of the html text
set html to SnipString("right", html, "href=\"listing.php?id=")
set html to SnipString("right", html, "\">")
set end of listingTitleList to SnipString("left", html, "</a>")

-- Snip this listing account out of the html text
set html to SnipString("right", html, "href=\"user.php?id=")
set end of listingUserList to SnipString("left", html, "\"")

if DEBUG > 0 then log end of listingNumList & ¬
" (" & end of listingUserList & ") = " & end of listingTitleList
end if -- html ≠ null
end repeat -- while (html ≠ null)
```

Figure A2. Sample Code Snippet for Product Scraping.

```
if DEBUG > 0 then ¬
log "Crawling new user (" & userCount & " / " & (count of userList) & "): " & user

-- Get the user information for this user
set targetUrl to "view-source:" & marketPlace & "/user.php?id=" & user & "&tab=1"
set userInfo to GetUserInfo(targetUrl)

-- Open an output file to save the user information
set outFileName to myDir & "user-" & user & "-" & GetTimeStamp() & ".txt" as string
set outFile to open for access outFileName with write permission

-- Write the user information into the output file
repeat with info from 1 to length of userInfo
write item info in userInfo & NEWLINE to outFile
end repeat
```

Figure A3. Sample Code Snippet for Account Scraping.

```
"<a class="category" href="search.php?frc={CAT#}">{CATEGORYNAME}</a>

<a class="notext" href="listing.php?id={LISTING#}">

<img src="{IMAGEURL}”

({COST} BTC)

href="listing.php?id={LISTING#}">{TITLE}</a>

>Item # {LISTING#} - {CATEGORYNAME}<

href="user.php?id={USERID}"
```

Figure A4. Sample HTML Tags from a Selected Marketplace Listing.

```
http://4589fh9newd0d.onion/search.php?cat74=on&pg=2
```

Figure A5. URL Construction for Each Category.

```
Category,Sub Category,Category #,Item #,Account Name,Account Activity

Fraud,Accounts & Bank Drops / Other,191,139406,MaryJane900,20621
```

Figure A6. Output Format of Each Listing on Our Focus Marketplace.

```
http:// 4589fh9newd0d.onion/user.php?id=MaryJane400&tab=1
```

Figure A7. URL Construction for Each Account Listing.

References

1. Hurlburt, G. Shining Light on the Dark Web. *Computer* **2017**, *50*, 100–105. [CrossRef]
2. Chertoff, M.; Simon, T. *The Impact of the Dark Web on Internet Governance and Cyber Security*; Centre for International Governance Innovation and Chatham House: Waterloo, ON, Canada, 2015.
3. Weimann, G. Going dark: Terrorism on the dark web. *Stud. Conf. Terr.* **2016**, *39*, 195–206. [CrossRef]
4. Mansfield-Devine, S. Darknets. *Comput. Fraud Secur.* **2009**, *2009*, 4–6. [CrossRef]
5. Song, J.; Lee, Y.; Choi, J.W.; Gil, J.M.; Han, J.; Choi, S.S. Practical in-depth analysis of ids alerts for tracing and identifying potential attackers on darknet. *Sustainability* **2017**, *9*, 262. [CrossRef]
6. Robertson, J.; Diab, A.; Marin, E.; Nunes, E.; Paliath, V.; Shakarian, J.; Shakarian, P. Darknet Mining and Game Theory for Enhanced Cyber Threat Intelligence. *Cyber Déf. Rev.* **2016**, *1*, 95–122.
7. Robertson, J.; Diab, A.; Marin, E.; Nunes, E.; Paliath, V.; Shakarian, J.; Shakarian, P. *Darkweb Cyber Threat Intelligence Mining*; Cambridge University Press: Cambridge, UK, 2017.

8. Bradbury, D. Unveiling the dark web. *Netw. Secur.* **2014**, *2014*, 14–17. [CrossRef]
9. Broséus, J.; Rhumorbarbe, D.; Mireault, C.; Ouellette, V.; Crispino, F.; Décary-Hétu, D. Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective. *Forensic Sci. Int.* **2016**, *264*, 7–14. [CrossRef] [PubMed]
10. Jardine, E. Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies. *New Media Soc.* **2017**. [CrossRef]
11. George, A. Shopping on the dark net. *New Sci.* **2015**, *228*, 41. [CrossRef]
12. Aceto, G.; Pescapé, A. Internet Censorship detection: A survey. *Comput. Netw.* **2015**, *83*, 381–421. [CrossRef]
13. Pescape, A.; Montieri, A.; Aceto, G.; Ciuonzo, D. Anonymity Services Tor, I2P, JonDonym: Classifying in the Dark (Web). In Proceedings of the 2017 29th International Teletraffic Congress (ITC 29), Genoa, Italy, 4–8 September 2017.
14. Tor Project. Available online: https://www.torproject.org/ (accessed on 9 September 2017).
15. Scholz, R.W. Sustainable digital environments: What major challenges is humankind facing? *Sustainability* **2016**, *8*, 726. [CrossRef]
16. Rhumorbarbe, D.; Staehli, L.; Broséus, J.; Rossy, Q.; Esseiva, P. 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 Sci. Int.* **2016**, *267*, 173–182. [CrossRef] [PubMed]
17. European Monitoring Center for Drugs and Drug Addiction. *European Drug Report—Trends and Developments*; European Monitoring Center for Drugs and Drug Addiction: Lisbon, Portugal, 2017.
18. Lacson, W.; Jaishankar, K.; Jones, B. The 21st Century DarkNet Market: Lessons from the Fall of Silk Road. *Int. J. Cyber Criminol.* **2016**, *10*, 40–61.
19. Broséus, J.; Morelato, M.; Tahtouh, M.; Roux, C. Forensic drug intelligence and the rise of cryptomarkets. Part I: Studying the Australian virtual market. *Forensic Sci. Int.* **2017**, *279*, 288–301. [CrossRef] [PubMed]
20. Van Hout, M.C.; Bingham, T. "Silk Road", the virtual drug marketplace: A single case study of user experiences. *Int. J. Drug Policy* **2013**, *24*, 385–391. [CrossRef] [PubMed]
21. Ahmed, M.; Litchfield, A.T. Taxonomy for Identification of Security Issues in Cloud Computing Environments. *J. Comput. Inf. Syst.* **2016**, 1–10. [CrossRef]
22. Revell, T. US guns sold in Europe via dark web. *New Sci.* **2017**, *235*, 12. [CrossRef]
23. Pergolizzi, J.V.; LeQuang, J.A.; Taylor, R.; Raffa, R.B. The "Darknet": The new street for street drugs. *J. Clin. Pharm. Ther.* **2017**, *42*, 790–792. [CrossRef] [PubMed]
24. Kirkpatrick, K. Financing the dark web. *Commun. ACM* **2017**, *60*, 21–22. [CrossRef]
25. Masoni, M.; Guelfi, M.R.; Gensini, G.F. Darknet and bitcoin, the obscure and anonymous side of the internet in healthcare. *Technol. Health Care* **2016**, *24*, 969–972. [CrossRef] [PubMed]
26. Soska, K.; Christin, N. Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. In Proceedings of the 24th USENIX Security Symposium, Washington, DC, USA, 12–14 August 2015; pp. 33–48.
27. Tor Metrics. Available online: https://metrics.torproject.org/hidserv-dir-onions-seen.html (accessed on 2 March 2018).
28. Dainotti, A.; Pescape, A.; Claffy, K. Issues and future directions in traffic classification. *IEEE Netw.* **2012**, *26*, 35–40. [CrossRef]
29. Dainotti, A.; Pescapé, A.; Sansone, C. Early classification of network traffic through multi-classification. In *Traffic Monitoring and Analysis TMA 2011. Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6613, pp. 122–135.
30. Park, J.H.; Chao, H.C. Advanced IT-based Future sustainable computing. *Sustainability* **2017**, *9*, 757. [CrossRef]
31. Chen, H.; Chung, W.; Qin, J.; Reid, E.; Sageman, M.; Weimann, G. Uncovering the dark Web: A case study of Jihad on the Web. *J. Am. Soc. Inf. Sci. Technol.* **2008**, *59*, 1347–1359. [CrossRef]
32. Zulkarnine, A.T.; Frank, R.; Monk, B.; Mitchell, J.; Davies, G. Surfacing collaborated networks in dark web to find illicit and criminal content. In Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 27–30 September 2016; pp. 109–114.
33. Spitters, M.; Klaver, F.; Koot, G.; van Staalduinen, M. Authorship Analysis on Dark Marketplace Forums. In Proceedings of the 2015 European Intelligence and Security Informatics Conference, Manchester, UK, 7–9 September 2015; pp. 1–8.

34. DarkOwl. Available online: https://www.darkowl.com/ (accessed on 28 June 2018).
35. Intelliagg. Available online: https://www.intelliagg.com/ (accessed on 28 June 2018).
36. Fiss, P.C.; Hirsch, P.M. The discourse of globalization: Framing and sensemaking of an emerging concept. *Am. Sociol. Rev.* **2005**, *70*, 29–52. [CrossRef]
37. Lee, J.K. Research Framework for AIS Grand Vision of the Bright ICT Initiative. *MIS Q.* **2015**, *39*, 3–13.
38. Moloney, P. *Dark Net Drug Marketplaces Begin to Emulate Organised Street Crime*; National Drug and Alcohol Research Centre: Sydney, Australia, 2016.
39. Dolliver, D.S. Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. *Int. J. Drug Policy* **2015**, *26*, 1113–1123. [CrossRef] [PubMed]
40. Kim, W.; Jeong, O.R.; Kim, C.; So, J. The dark side of the Internet: Attacks, costs and responses. *Inf. Syst.* **2011**, *36*, 675–705. [CrossRef]
41. Koch, R. The Darkweb—A Growing Risk for Military Operations? *Information* **2018**, in press.
42. Harrison, J.R.; Roberts, D.L.; Hernandez-Castro, J. Assessing the extent and nature of wildlife trade on the dark web. *Conserv. Boil.* **2016**, *30*, 900–904. [CrossRef] [PubMed]
43. Dalins, J.; Wilson, C.; Carman, M. Criminal motivation on the dark web: A categorisation model for law enforcement. *Digit. Investig.* **2018**, *24*, 62–71. [CrossRef]
44. Van Hout, M.C.; Bingham, T. Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *Int. J. Drug Policy* **2014**, *25*, 183–189. [CrossRef] [PubMed]
45. Christin, N. Nicolas Traveling the silk road. In Proceedings of the 22nd International Conference on World Wide Web—WWW '13, Rio de Janeiro, Brazil, 13–17 May 2013; ACM Press: New York, NY, USA, 2013; pp. 213–224.
46. Edwards, M.J.; Rashid, A.; Rayson, P. A Service-Indepenent Model for Linking Online User Profile Information. In Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference, The Hague, The Netherlands, 24–26 September 2014; pp. 280–283.
47. Phelps, A.; Watt, A. I shop online—Recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digit. Investig.* **2014**, *11*, 261–272. [CrossRef]
48. Qin, J.; Zhou, Y.; Chen, H. A multi-region empirical study on the internet presence of global extremist organizations. *Inf. Syst. Front.* **2011**, *13*, 75–88. [CrossRef]
49. Lacey, D.; Salmon, P.M. It's Dark in There: Using Systems Analysis to Investigate Trust and Engagement in Dark Web Forums. In Proceedings of the International Conference on Engineering Psychology and Cognitive Ergonomics, Los Angeles, CA, USA, 2–7 August 2015; Springer: Cham, Switzerland, 2015; pp. 117–128.
50. UNODC. *World Drug Report*; UNODC: Vienna, Austria, 2016.
51. Reddit. Available online: https://www.reddit.com/r/darknetmarkets (accessed on 9 September 2017).
52. Zetter, K. New "Google" for the Dark Web Makes Buying Dope and Guns Easy. Available online: https://www.wired.com/2014/04/grams-search-engine-dark-web/ (accessed on 26 October 2017).
53. Zillman, M.P. *Deep Web Research and Discovery Resources 2017*; Deep Web: Naples, FL, USA, 2017.
54. Defense Advanced Research Project Agency Memex. Available online: https://www.darpa.mil/program/memex (accessed on 5 October 2017).
55. Zetter, K. Darpa Is Developing a Search Engine for the Dark Web | WIRED. Available online: https://www.wired.com/2015/02/darpa-memex-dark-web/ (accessed on 26 October 2017).
56. Mahto, D.K.; Singh, L. A Dive into Web Scraper World. In Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 16–18 March 2016.
57. Baravalle, A.; Lopez, M.S.; Lee, S.W. Mining the Dark Web: Drugs and Fake Ids. In Proceedings of the IEEE International Conference on Data Mining Workshops, ICDMW, New Orleans, LA, USA, 11–20 November 2017; pp. 350–356.
58. Wanjala, G.W.; Kahonge, A.M. Social Media Forensics for Hate Speech Opinion Mining. *Int. J. Comput. Appl.* **2016**, *155*, 975–8887.
59. Plachouras, V.; Carpentier, F.; Faheem, M.; Masanès, J.; Risse, T.; Senellart, P.; Siehndel, P.; Stavrakas, Y. ARCOMEM Crawling Architecture. *Future Internet* **2014**, *6*, 518–541. [CrossRef]
60. Unix & Linux Stack Exchange Anonymous Url Navigation in Command Line? Available online: https://unix.stackexchange.com/questions/87156/anonymous-url-navigation-in-command-line (accessed on 30 May 2018).

61. Landhauber, M.; Weigelt, S.; Tichy, W.F. NLCI: A natural language command interpreter. *Autom. Softw. Eng.* **2016**, *24*, 839–861. [CrossRef]
62. Hayes, D.; Cappa, F. Open Source Intelligence for Risk Assessment. *Bus. Horiz.* **2018**, in press. [CrossRef]
63. Paterva Home Maltego. Available online: https://www.paterva.com/web7/ (accessed on 11 September 2017).
64. Tarafdar, M.; Gupta, A.; Turel, O. Special issue on 'Dark side of information technology use': An introduction and a framework for research. *Inf. Syst. J.* **2015**, *25*, 161–170. [CrossRef]
65. George, J.F.; Derrick, D.; Marett, K.; Harrison, A.; Thatcher, J.B. The dark internet: Without darkness there is no light. In Proceedings of the AMCIS 2016: Surfing the IT Innovation Wave—22nd Americas Conference on Information Systems, San Diego, CA, USA, 11–14 August 2016.
66. Roberts, N.C. Tracking and disrupting dark networks: Challenges of data collection and analysis. *Inf. Syst. Front.* **2011**, *13*, 5–19. [CrossRef]
67. Hartong, M.; Goel, R.; Wijesekera, D. Security and the US rail infrastructure. *Int. J. Crit. Infrastruct. Prot.* **2008**, *1*, 15–28. [CrossRef]
68. Rice, M.; Miller, R.; Shenoi, S. May the US government monitor private critical infrastructure assets to combat foreign cyberspace threats? *Int. J. Crit. Infrastruct. Prot.* **2011**, *4*, 3–13. [CrossRef]
69. Shackelford, S.J. Business and cyber peace: We need you! *Bus. Horiz.* **2016**, *59*, 539–548. [CrossRef]
70. Parent, M.; Cusack, B. Cybersecurity in 2016: People, technology, and processes. *Bus. Horiz.* **2016**, *59*, 567–569. [CrossRef]