Journal of *Cybersecurity and Privacy*

MDPI

Article

D2WFP: A Novel Protocol for Forensically Identifying, Extracting, and Analysing Deep and Dark Web Browsing Activities

Mohamed Chahine Ghanem [1,2,*], Patrick Mulvihill [3], Karim Ouazzane [1], Ramzi Djemai [1] and Dipo Dunsin [1]

[1] Cyber Security Research Centre, London Metropolitan University, London N7 8DB, UK; pam0829@my.londonmet.ac.uk (P.M.); k.ouzzane@londonmet.ac.uk (K.O.); r.djemai@londonmet.ac.uk (R.D.); d.dunsin@londonmet.ac.uk (D.D.)
[2] Department of Computer Science, University of Liverpool, Liverpool L69 3BX, UK
[3] Cyber Threat Intelligence, Grant Thornton UK LLP, London EC2A 1AG, UK
* Correspondence: ghanemm@staff.londonmet.ac.uk

Abstract: The use of the unindexed web, commonly known as the deep web and dark web, to commit or facilitate criminal activity has drastically increased over the past decade. The dark web is a dangerous place where all kinds of criminal activities take place, Despite advances in web forensic techniques, tools, and methodologies, few studies have formally tackled dark and deep web forensics and the technical differences in terms of investigative techniques and artefact identification and extraction. This study proposes a novel and comprehensive protocol to guide and assist digital forensic professionals in investigating crimes committed on or via the deep and dark web. The protocol, named D2WFP, establishes a new sequential approach for performing investigative activities by observing the order of volatility and implementing a systemic approach covering all browsing-related hives and artefacts which ultimately resulted in improving the accuracy and effectiveness. Rigorous quantitative and qualitative research has been conducted by assessing the D2WFP following a scientifically sound and comprehensive process in different scenarios and the obtained results show an apparent increase in the number of artefacts recovered when adopting the D2WFP which outperforms any current industry or opensource browsing forensic tools. The second contribution of the D2WFP is the robust formulation of artefact correlation and cross-validation within the D2WFP which enables digital forensic professionals to better document and structure their analysis of host-based deep and dark web browsing artefacts.

Keywords: dark web; deep web; cybercrime; dark web forensics; digital crime investigation; cyber forensics; DFIR; dark web protocol; anonymous browsing; TOR; online black market

Citation: Ghanem, M.C.; Mulvihill, P.; Ouazzane, K.; Djemai, R.; Dunsin, D. D2WFP: A Novel Protocol for Forensically Identifying, Extracting, and Analysing Deep and Dark Web Browsing Activities. *J. Cybersecur. Priv.* **2023**, *3*, 808–829. https://doi.org/10.3390/jcp3040036

Academic Editors: Giorgio Giacinto, Carlos Rabadão and Mario Antunes

Received: 6 July 2023
Revised: 18 October 2023
Accepted: 25 October 2023
Published: 15 November 2023

1. Introduction

With the ongoing development of the Internet and the increased use of digital devices, crime has become a more digital phenomenon [1]. Users with more sinister and unlawful intentions are accessing areas of the Internet that are concealed from the public by being unindexed, as illustrated in Figure 1. In contrast, everyday Internet users access websites using a standard web browser, and the dark web uses numerous layers of encryption to encrypt all traffic, and services such as TOR, FREENET, WATERFOX, and TAILS are used to access it [2]. As a result of these layers of encryption, the dark web offers users a high level of anonymity [3,4]. This has resulted in several dark web marketplaces offering illegal goods like drugs, weapons, false passports, and more. In addition, users are further anonymised by cryptocurrency payment methods, such as Bitcoin, and encryption when browsing the dark web [5]. The term "dark web" is often used interchangeably with "deep web," "dark net," and "Invisible Internet Project [6]". However, the "Dark Web" refers to websites hosted within overlay networks typically inaccessible without dedicated

"Privacy and Anonymity" web browsers [7]. Its most important feature is that service users remain anonymous; neither a website provider nor a visitor can identify the service provider [8,9]. On the other hand, the deep web is any Internet information or data that cannot be found using a search engine. In addition, some estimates say the deep web is much larger than the visible or surface web [10–12]. The term "dark net" refers to the portion of the IP address space that is routable but not used [1]. The dark net is most associated with overlay networks that provide anonymous network connectivity and services [2]. In addition, the Invisible Internet Project (I2P) is an unknown peer-to-peer network layer that uses layered encryption and garlic routing, a variant of onion routing, to ensure the anonymity of communications [13]. The new generation of anonymity and privacy browsers, such as TOR and I2P, rely on a complex implementation of the onion routing topology initially introduced by the US Navy Research Lab in the mid-1990s to conceal the user's IP address [14]. As a result, attempts to trace or identify the user online by relying on traffic capture are nearly impossible. TOR and other networks are designed to protect against tracking, profiling, and eavesdropping attacks, providing privacy and anonymity by mainly using cryptography such as TOR multilayer encryption in conjunction with an "onion" routing network deployed by tens of thousands of volunteer networks to direct traffic over the Internet so a user's identity can be kept hidden from network interceptors [1].

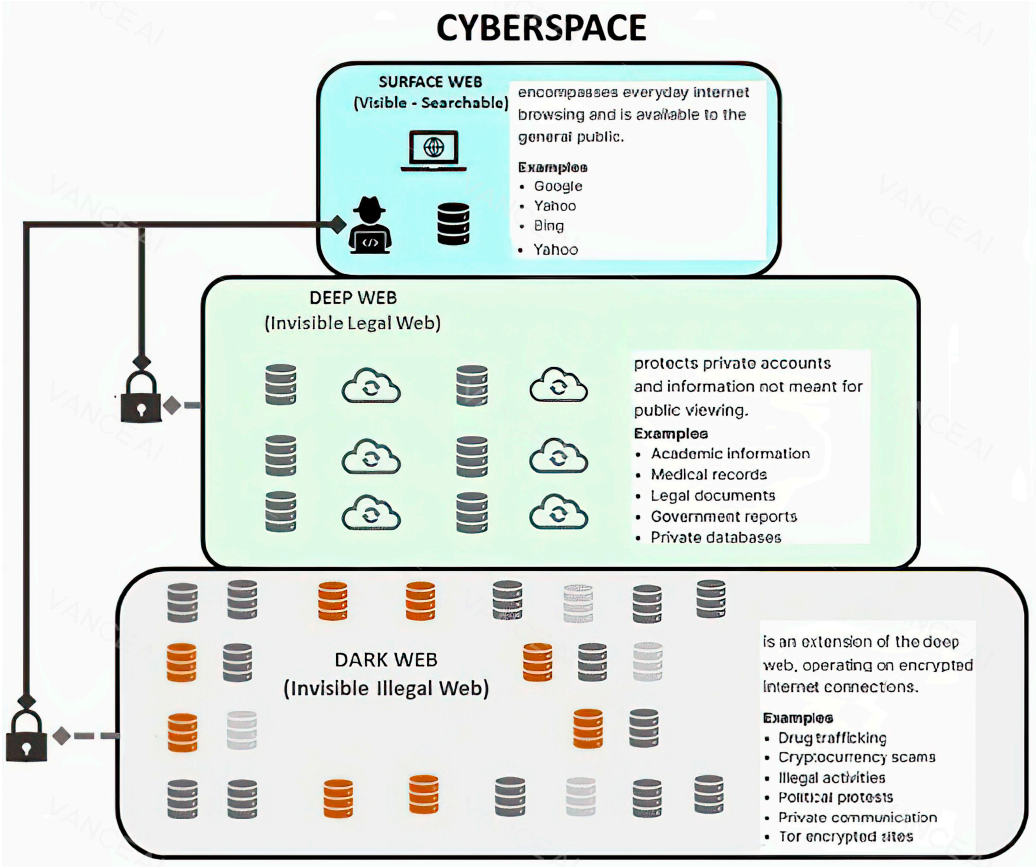

Figure 1. Anatomy of the surface, deep, and dark web in the context of visible and invisible content.

1.1. Research Context

The deep web and the dark web are often confused, but they are distinct concepts, each with its own characteristics and implications for cybercrime [2]. The deep web comprises any part of the Internet not indexed by search engines, and it can include legal and legitimate content. In contrast, the dark web is a small, hidden subset of the deep web accessible only through specialised software, and it is often associated with various illegal cyber activities [15]. Cybercriminals may use both the deep web and the dark web, but the

dark web is particularly notorious for hosting illegal marketplaces and forums dedicated to cybercrime [16]. This study will briefly introduce the use of privacy and anonymity preservation Internet browsers such as TOR, FREENET, TAILS, and WATERFOX which are used to access and navigate the deep and dark web for illegal activities. This work has a special focus on TOR browsers as one of the most-used tools amongst criminals and thus will be used to simulate activities for research purposes to mimic the real-world situation [17]. In addition, we will briefly describe the legitimate use of the same technology for security and privacy purposes which lead to the setting of a borderline between the two usages. Given the high volume and complexity of threats emanating from the deep and dark web (DDW), we decided to explore existing methodologies used by law enforcement agents in investigating DDW crime activities. In addition to the comprehensive study, we will create different forensic scenarios to test the proposed deep and dark web forensic protocol. The Internet is often described as consisting of three parts: the surface web, the deep web, and the dark web. While the terms "deep web" and "dark web" are regularly used interchangeably, it is helpful to highlight the complementary nature and not the interchangeability of these two terms.

1.2. Research Motivation and Scope

Even though law enforcement and cybersecurity practitioners recognise that the deep and dark web does not have a "monopoly" on online threats or negative effects/effects, such as extremist views, criminal discussion, child pornography, terrorist propaganda, malicious hacking tutorials, stolen data marketing as hyped in the media, it remains the most technically challenging online tracking activities for law enforcement agencies across the world and highly popular amongst criminals [5]. Currently, most cyber investigators across the world are tackling deep and dark web forensic investigations as regular network forensics and are relying on the tool and framework automation in locating and analysing browsing data and related artefacts which fails in taking into consideration some important information considering the design and functioning of the used browsers. This study intends to formally address the deep and dark web forensic process and proposes a robust protocol for forensically identifying, extracting, and analysing deep and dark web criminal activities from users' machines and devices. It will investigate the digital forensic process when examining dark web content, methods of accessing it, types of illegal activities, and the use of anonymity and privacy for the benefit of cyber obfuscation on the dark web. Also, this study will critically examine the existing methodologies and methods currently adopted in dark web forensics. This study proposes a complete and comprehensive protocol, combining existing and new techniques and was designed, implemented, and tested around a few hypotheses and scoping choices, notably the use of TOR to simulate deep and dark web browsing activities and the testing limitation to the host (end-user) device investigation only. We will then test the proposed protocol in different scenarios, including various operating systems and Internet browsers. As a result, a novel and comprehensive protocol for assisting digital forensic professionals in conducting deep and dark web artefact forensic investigations from the host side was proposed. It is worth highlighting that even though the deep and dark web is accessible using a regular Internet browser such as Firefox, criminal activities are often carried out using a special browser such as TOR to guarantee privacy and anonymity which offers cybercriminals a sense of security and untraceability from law enforcement agencies; thus, the investigation of artefacts left on regular browsers is outside the scope of this work.

1.3. Paper Structure

This paper is currently divided into eleven sections, each of which contains information about issues pertinent to dark web forensics. Section 1 provides an overview of the study, its scope, and motivation. Section 2 presents in-depth background research on the subject, delves into the various deep and dark web forensic landscapes, and discusses findings that, to some extent, contribute to this paper. Section 3 covers the adopted research methodology

and justifies the choices made in this work. Section 4 summarises the novelty of this paper, notably the impact of the D2WFP on current practice. Section 5 tackles the order of volatility in digital forensics and incident response and its impact on web browsing investigation output. Section 6 introduces the proposed high-level protocol that mimics the four standard DFIR phases. Section 7 describes the detailed D2WF protocol and provides backing evidence for the order of tasks and subtasks. Section 8 explains the designed forensic scenario and the research input in the form of datasets. Section 9 describes the testing phase in terms of forensic processing, examination, and analysis. Section 10 presents the results with some criticalities. Finally, Section 11 concludes this study with a final reflection on how this study could be improved.

2. Literature Review and Research Gaps

The literature review dives into the background and technical details of the deep and dark web, describing its development as a tool for new types of criminals to grow their activities. The information was gathered from several reliable sources, including books, journal papers, reports, conference proceedings, and web pages.

2.1. Related Works

The Internet is a crucial tool for facilitating modern societal life. Through primary, traditional web browsers, and an Internet connection, users can access websites for social networking, online shopping, video streaming, public news, research, and more via the "surface web" [17]. The crucial distinction between the "surface web" and the "clear web" is that the latter phrase refers to the portion of the Internet that can be indexed by any traditional search engine [2,5]. The deep web stands in opposition to the surface web. The deep web is a collection of websites, communities, networks, and intranets that are purposefully not accessible via standard online browsing, in contrast to the surface web, which makes its material searchable via ordinary search engines [3]. However, because of its anonymity, the dark web offers services to those who could have illegal intentions over a global network that is essentially untraceable [18,19]. This raises an ethical problem due to the growth of the dark web, which has given rise to lucrative sectors like malware services, child pornography, and illicit Internet markets. In addition, the most prominent entrance to the dark web is TOR [8]. I2P is one solution used to access the dark web. Still, other anonymous software programmers like Freenet and OpenBazaar allow anonymous communications by storing and exchanging data via the machines linked to the network rather than utilising centralised servers [7]. Terrorist groups and extremist such as use the dark web to propagate propaganda, attract new members, and share data and films that support their illegal activities [15]. The dissemination of child pornography and unlawful online markets for illicit goods (drugs, weapons, passports) are the two crimes that are most frequently committed through the use of TOR [5]. However, other crimes include renting assassins and trafficking humans. One of the most well-known instances was the 2011 emergence of the drug bazaar on the dark web called "Silk Road." The FBI shut it down in October 2013 after it had operated for two and a half years and processed over $1,200,000,000 in transactions [8]. The fact that criminals frequently feel safer transacting on the dark web than on the street is one of the significant elements causing this crime, as has been pinpointed in two recent studies on policing the dark web [1,16]. Even if there is a higher likelihood that law enforcement will halt the business and take it offline, additional sites will replace it [10,17]. Police and law enforcement agency shutdowns are one of the reasons why many dark websites are only active for a limited time, usually between 200 and 300 days, according to analysis [20]. Other elements that have influenced the rising use of online criminal marketplaces include the growth and acceptance of cryptocurrencies, as illustrated in Table 1.

Table 1. A comparative analysis between the deep and dark web in the context of cybercrime.

	Deep Web	Dark Web
Accessibility and Content	• Part of the Internet that is not indexed by traditional search engines like Google, Bing, or Yahoo. • Content that is behind paywalls, requires authentication, or is hidden behind web forms. • Most of the deep web is legal and used for legitimate purposes, such as private databases, subscription-based websites, and confidential company intranets.	• A small, intentionally hidden portion of the deep web that can only be accessed using specialised browsers like TOR (the onion router). • TOR and similar browsers are intentionally designed to provide anonymity to users by routing their traffic through a network of servers. • ISP cannot trace back transactions and it is difficult for the client side to trace their identity or location.
Cybercrime Context	• The deep web is used by cybercriminals for communication and coordination purposes. • It is a hub for cybercrime. However, cybercriminals can use it to access certain resources or information that is not readily available on the surface web indexed by search engines.	• The dark web is known for being a hub for various illegal activities, including cybercrime. • It hosts marketplaces for illegal goods and services, such as drugs, firearms, stolen data (e.g., credit card information), hacking tools, and cyberattack services (e.g., DDoS-for-hire).
Regular or Crime Content	• Stolen data (breaches and exfiltrations). • Basic hacking forums (tutorials). • Password-protected facilities and online services. • Online banking, investment, and finance portals. • Subscription-based services.	• Cybercriminals often use the dark web to buy and sell hacking tools, trade stolen data, or plan cyberattacks. • Darknet marketplaces like SilkRoad and AlphaBay. • Anonymous communication channels for coordinating illegal activities are part of the dark web.

A 2016 study by RAND estimated that the three biggest online criminal markets at the time accounted for 65% of all crypto market listings. Cryptocurrencies like Bitcoin and Ethereum allow users to make payments anonymously as an additional layer of security [10]. In [19], a study was conducted to gain a deeper understanding of the dark web and its impact on people's lives. The researcher achieved the aim of his paper through the provision of various methods of access, the listing and description of available websites, and the provision of a list of precautions people should take before surfing the dark web. The article also discussed illegal activities and crimes committed on the dark web, its ethical and unethical sides, its pros and cons, and how legislative agencies and security agencies can administer the dark net to secure society. The study produced a robust research model on the dark web because it highlighted methods of accessing the darknet through various specific configurations, software, and authorisation. Also, the study considered the precautions a person should take while attempting to delve into the darknet world, especially for a first-time user, and the associated risks, such as malware and the loss of personal data and identity [20]. Finally, the researchers discussed the various applications of the dark web, emphasising its advantages and disadvantages but failing to address the security and enforcement part of the deep and dark web; thus, the findings were more about the precautions part which they should have considered regarding the illegitimate use of privacy-preserving browsers and the privacy and security offered to criminals because of their non-malicious activities, but [17] advanced this review with a systematic analysis of the role of AI in tackling the problem. Therefore, this study focused primarily on platform tools such as TOR, FREENET, TAILS, WATERFOX, and other methods put in place to enhance dark web security, such as the Invisible Internet Project (ISP), and enhanced Firefox with the usage of HTTPS Everywhere and VPN [21].

In [22], the authors examined and tracked the nature of activities on the dark web using digital forensic (DF) tools, particularly in light of the evolving technology that

renders traditional tools obsolete. They achieved their research aims by executing sampled, predetermined sites on a closed-paraben Electronic Evidence Examiner (E3) using a TOR browser on a Ulefone Note 7 mobile device. Also, they assessed and analysed the software's ability to track benign content. According to [18], in digital forensics, tools help to crawl and sift through large volumes of data that users generate. These tools, including The Sleuth Kit (TSK) and E3, are more accurate and save time since they crawl different types of data that are voluminous [23]. The study considered downloading benign content from sites that would encourage criminal activity and the ability of the tools to gauge illicit activity by using legal models as mirrors. However, the investigators ignored the use of various software, such as Encase and Forensic Toolkit, different browsers, various mobile devices, and devices running iOS or Windows OS, which could have yielded a different result. The study considered timestamps for the TOR browser and the usage of the application on the device while using E3 software. However, this study teaches us the need to use broad digital forensic methods for better results.

In [24], the researchers conducted a systematic literature review (SLR) on the dark web, its crimes, and better methods for control, as well as how investigators can leverage its main feature (anonymity) for crime control. The SLR approach helped them achieve their goal for this paper, using a definition of the research questions, a systematic review of the literature, a search for relevant data sources, the extraction of data, and analysis for meaningful reporting. The researchers stated that such a study helps provide knowledge about web crime spikes but also helps investigate the dark web's impact on users' lives [20]. Moreover, the study helps evaluate the challenges raised by the methods used to control crime and their weaknesses. The research model was good because different techniques could be garnered from it, including a statement of the hypothesis, determining the selection of materials, and analysing and synthesising data. The researchers classified data from 69 papers into two categories that answered their hypothetical questions: an outline of threats from illegal activities, methods of locating criminals on the dark web, and steps to control crime. Nevertheless, the evolving trends, such as the use of newer technology in the face of technological advancement, have been overlooked. In essence, this paper gives the reader an in-depth knowledge of crimes on the dark web.

In [25], the researchers used a honeypot, a protective tool, to investigate and gather data from malicious actions on the dark web. The goal of this study was to use and monitor two different honeypots; they researched and produced the honeypots on the dark web over seven months, then analysed the information gathered on cybercrimes and detected the prowess of the protection tool. The structure of this study allows a reader to see different applied methodologies, such as testing prevention tools, which in this case were two; background information about the dark web and the types of honeypots; an overview of related works; and an analysis of the data collected from the tools. The study considered using virtual machines (VMs) that contain the ChatRoom web server, web-based honey, and ELK log server, ensuring security and flexibility. The researchers also confirmed that the VMs were secure from private escalation with clean snapshots, provided that the VMs reverted to daily for security purposes.

In [26], the researchers ensured that log servers do not go off while they are set on a secured VM that guarantees safety [13]. However, to avoid fake logins and script attacks, the researchers used a captcha to ensure user authentication to the chatroom. However, future research must avoid improper comment data filtration because it leads to remote code implementation through unauthorised default settings. This study helps one to learn the use of different honeypots for the best results and understanding of dark web crimes and cyberattacks [17]. In [5], the researchers examined the importance of memory forensics, also known as a forensic study of the computer dump, a widely accepted part of the incident report process for investigations. They achieved the goals of this study through a discussion of recent trends and problems in online crime, an outline of the technical background and discussion of the expansion and growth of memory forensic techniques and tools, and a review of the current memory forensic scheme and its drawbacks. They opine that memory

forensic tools for analysing memory are essential because they help identify specific areas that have been compromised by malware or help uncover users' digital footprints. They also direct analysts to areas to focus on during malware investigations. According to [5], if an investigator does not know where to look, the investigator may waste valuable time as the crawler sifts through large datasets. The advancement of capacity in Artificial Intelligence (AI) enabled to address the problems of processing large data and their analysis and the development of frameworks without forensic memory capabilities, such as the OSX system in Apple products, which are attractive to criminals [27]. This paper sets an excellent example for anyone interested in helping forensic investigators with memories. They provided discussion, challenges, and a technical overview of the study and looked into emerging trends that are important for shaping future solutions in the digital space. As a result, this study demonstrates that a successful exploration of digital scenarios emphasises the importance of memory forensics, and an investigation into specific applications that aid in understanding their actions is unquestionably an advancement for that field.

2.2. The Landscape of Dark and Deep Web Forensics

Frameworks and techniques for dark web forensics are scarce compared to other types of computer forensics (based on what is in the public domain). However, some have made an effort to map this out. According to [2,14] research journals, browser forensic examinations focus on performing more conventional operations on the computer, such as database, RAM, network forensics, and registry. In contrast, dark web forensics should consolidate two fundamental areas: forensics connected to TOR activities and forensics linked to Bitcoin transactions [16].

The deep web and the dark web are often misunderstood and sometimes used interchangeably, but they are distinct in terms of their content and accessibility. When it comes to cybercrime, understanding the differences between these two is crucial: the focus of Bitcoin forensics, however, is on monitoring payments [18,23,24]. The techniques suggested are illustrated in Figure 2. The data mentioned above offer a starting point, but there is a general absence of knowledge and a reliance on using subpar opensource technologies.

Browsing Artefacts	**Evidence Location**		
	File System	**RAM**	**User and System Configuration**
URLs	No	Yes	Yes
Website Content	No	Yes	No
Search Queries	No	Yes	Yes
Bookmarks	Yes	Yes	Yes
Cookies	No	No	No
Email Addresses	No	Yes	No
Email Content	No	Yes	No
Usernames	No	Yes	No
Passwords	No	Yes	No
Download Files	Yes	Yes	No
Usage/Session	No	Yes	Yes
Timestamps	Yes	No	Yes

Figure 2. Summary of Internet activities and browsing artefact's location per category in Windows and Linux distributions [17].

This research direction will be significantly aided by studies and experiments carried out with better tools and in greater depth. This was accomplished through a research study from Marshall University that expanded on some of the earlier concepts, introduced the AccessData Forensic Toolkit as a tool for analysis, and went further in depth on the testing environments employed [6]. The use of RAM forensics by obtaining a live memory

dump of a suspect's computer (or, in this case, a virtual machine created by using an FTK imager) and then analysing this through FTK yields promising results, with index searches relating to TOR yielding results in both the memory dump and page file areas [6]. The study also considers the idea of observing registry and cache changes and contrasting a virtual machine before, during, and after using TOR, which did produce some information, allowing an investigator to suspect TOR is used (although nothing concrete), as well as using Wireshark to compare how the traffic compares between a standard browser and TOR, with there being a discernible difference (a comparison of the protocol hierarchy showed a clear distinction) [6]. These techniques aid in shaping what should be contained in the D2WFP and are helpful for later testing in this study. These forensic procedures are only sound if the device is captured while still switched on as TOR browser processes are allocated in the live memory, and only live RAM capture can preserve such crucial artefacts.

In [1], similar research was made to show forensic methods for TOR browsing on Windows 10 and Android 11 devices. The procedures are carried out following the earlier reports, with an emphasis on the registry, memory, and local file system in line with the idea of a scenario set up on a virtual machine. When thinking about the methods to be added to the framework, this offers a sound basis for what has to be tested. In contrast to the previous report, which was not simple, the entire report has numerous figures and tables that demonstrate the tests being conducted. The most helpful report was found as a result of this; it was a doctoral dissertation submitted to Dakota State University which focused on finding any dark web artefacts on a machine and creating a framework around this [14]. The depth of information in the report extends beyond the scope of this one. Still, it provides a solid foundation for what needs to be taken into account and lists every possible place where TOR-related activity might be hiding on a device. In [2], the authors focused on Internet browsing artefact extraction during live memory forensics and noted that EnCase and FTK are proven to be reliable in terms of covering, exploring, and analysing live memory artefacts compared to other publicly available tools but remain inefficient in the context of dark web browsing when TOR is used and impacting artefact collection and interpretation, notably by generating a large amount of unreadable data. The new generation of privacy-preserving browsers such as Brave and TOR are even more challenging when it comes to browsing data forensic examinations as the amount of encryption and encapsulation reduces the amount of readable data and this limits the investigation, as illustrated in the cryptographic upgrade of TOR which took effect in early 2017 [25].

2.3. Internet Browsing Forensic Evidence, Techniques, and Tools

As the background study has indicated, the issue of dark web forensics is primarily related to the process of investigating the digital equipment used to carry out criminal activities. The issue is gaining importance along with the growing Internet privacy and security landscape. The dilemma is the dual use of the technology and tools to access and maintain deep and dark web content, such as TOR and I2P. Furthermore, the current methods used fall short of effectively investigating DDW cases and thus combating such crime. The order of volatility plays a central part in this field. The RAM and caches on the running evidence machines should be systematically extracted using the Exterro FTK Imager or other equivalent tools. On the other hand, the volatility application is used to analyse the RAM further to identify the types of applications running on the process ID, downloaded documents, and visited websites. FTK Registry Viewer and Registry Editor are used on the host machine to analyse evidence of TOR installation, the last executed date, and other attributes that might be of significant value to investigators. Wireshark and Network Miner are tools for extracting data from networks. However, Wireshark lets users view packets of data as they travel through a computer network. As a result, the PCAP files enable investigators to gather and analyse web traffic information and network connections. The Internet Evidence Finder searches the SQLite Database for evidence related to users'

visits to web content and identifies TOR browsing histories. The FTK and UFED discovered the application-related data, including usage session, timestamp, and cookies. To sum up, we elaborated a summary of the evidence identification, techniques, and tools used in investigating the deep and dark web. Table 2 illustrates the adopted deep and dark web forensic evidence, techniques, and tools.

Table 2. A summary of deep and dark web forensic evidence, techniques, and tools.

Evidence	Techniques	Tools	Purpose
Host Machine	**Live RAM**	Exterro FTK Imager Volatility Framework Magnet AXIOM	Obtain the description of the types of URLs, wikis, and visited deep web websites, as well as other downloaded content.
Host Machine	**File System Forensics**	Exterro FTK (Registry Viewer) Windows Registry Editor	Regshot and analysis to obtain evidence of TOR installation's last executed date and other attributes
Network Traffic	**Network Forensics**	Wireshark Network Miner Kroll KAPE Cellebrite UFED	Gather and analyse evidence of web traffic, established VPN and proxy connections, and information on network connections available
Host Machine	**Browser Forensics**	Magnet Internet Evidence Finder (IEF) Dumpzilla	Locate, extract, and retrieve evidence related to users or visited dark web content and activities
Application Forensics	**Applications and Transactions**	Exterro FTK Cellebrite UFED Magnet AXIOM	Recover applications' related data, including usage session, timestamp, and cookies

3. Research Methodology

The first step in this methodology is to emulate the forensic scenarios carried out at the London Metropolitan University Cyber Security Research Centre. For consistency purposes, we opted to run the scenarios on various operating systems and web browsers. The chosen devices and machines for the scenarios are a Windows 10 machine, Kali 2021 version 3, Android 11, and iOS 14.2; this guarantees a comprehensive evaluation of the proposed protocol by assessing it with near-to-real-world data from top-used OS distributions. For forensic imaging, analysis, and examination, this study uses fully licensed Access Data FTK, Magnet AXIOM, and Cellebrite UFED tools. TOR is installed on all devices to access the dark web, store login information, and browse the web with Chrome and Microsoft Edge.

A forensic image is created due to the massive data generated during dark web browsing activities, which will then be analysed using FTK and Magnet. After the forensic images are created, an anti-forensic tool called BleachBit is installed on all devices and used to clear any browsing artefacts before creating new forensic images. Subsequently, we generate another browsing history on all devices before creating and storing away another set of forensic images. Fully licensed FTK and Magnet are used to analyse the forensic images for Windows 10 and Kali 2021.3. Simultaneously, forensic images for Android 11 and iOS 14.2 are analysed using the Cellebrite Physical Analyser software packages following the principles outlined in our proposed protocol. We then quantitatively analyse the data collected from the forensic scenario analysis and examinations. The outcomes are tabulated to compare the standard automated process to our proposed protocol. This study aims to compare the deep and dark web forensic protocol results to regular after anti-forensic BleachBit using FTK for Windows 10, AXIOM for Kali 2021.3, and UFED for Android 11 and

iOS 14.2. The results obtained from the analysis and examination show an apparent increase in the number of artefacts recovered when adopting our proposed protocol compared with regular automation and framework-based automated investigations. The desired outcome of this study is the development of a solid protocol for dark and deep web forensic investigations that is clear, efficient, and effective enough to be used as a reference by cyber forensic investigators. The protocol will aid forensic examiners and, more importantly, analysts in their work by relying on current industrial (licensable and non-licensable) tools and frameworks to which they have access.

4. Research Contributions and Novelty

The first contribution of this study is to examine and assess the efficacy of our proposed protocol for assisting and improving dark and deep web forensic investigations. The findings and results show that the proposed protocol extracts more artefacts than standard automation. The second contribution is to analyse and document how to investigate dark and deep web forensics using the strategy outlined in our proposed protocol, such as extracting artefacts from operating systems, network traffic, malicious browser plugin behaviour, and memory dump analysis. The third contribution of this study is to draw attention to the flaws of privacy tools, particularly TOR, such as its tendency to take longer to load when connecting to available node servers, slow performance because of routing data through different nodes, and the fact that data inserted on web pages are not encrypted. Lastly, the fourth contribution is significant because we value knowledge exchange and aligning teaching to industrial practice, which will be a direct output of this study. We aim to use both the proposed D2WFP protocol and evidence files created from simulated deep and dark forensic scenarios in the new cyber threat intelligence and dark web forensic curriculum to be delivered for undergraduate, postgraduate, and CPD students as well as for conducting future research works.

The initial protocol is elaborated based on theoretical knowledge and has been inspired by previous research and established forensic principles, as explained in Figure 3. We then proceeded with the elaboration of eight (08) forensic scenarios created on different OS, respectively, Windows, Linux, Android, and iOS, where we used TOR to access emulated deep and dark web addresses and content. At the end of the simulation, we dealt with forensic imaging by running an anti-forensic tool to delete artefacts and forensic re-imaging using FTK imager and UFED Extractor.

Process	Description
Identification	Distinguish between valuable and worthless evidence and primary and secondary memory evidence, such as additional MicroSD or cloud.
Preservation	Evidence is cloned while write-protected and stored with security. At the same time, the forensics processing will apply to the clones or images (e.g., a UFD image for mobile evidence and an AD1 image for computer-based HDD evidence).
Analysis	Examining and analysing data by applying forensic techniques and solutions to the forensic copy of the evidence in addition to data identification and indexation. This includes deleted data recovery, raw data carving, and partial data reconstruction.
Presentation	Reporting must effectively communicate all pertinent information in a way that non-experts may understand.

Figure 3. Standard digital forensics process.

We then moved to the forensic examination, recovery, and analysis using FTK, AXIOM, and UFED Physical Analyzer (PA) software packages following the application of the

principles outlined within the protocol. The identification phase differentiates between valuable data such as transaction records, timestamps, login credentials, browsing caches holding posts and/or comments as well as networking activities including pertinent IP addresses which are often related to higher layers in the order of volatility (OoV) and primary and secondary memory evidence, such as additional MicroSD or cloud storage. The evidence is cloned, preserved while write-protected, and securely stored when forensic processing is applied to the clones. We reviewed and analysed the data using forensic methods and solutions to the forensic copy of the evidence. However, the reporting must properly communicate all pertinent information in a way that non-experts may understand.

5. Order of Volatility in Cyber Forensics

We needed to grasp and understand the existing forensic processes and procedures in their parts covering web browsing artefacts in general before elaborating on the investigative protocol aimed at the realm of dark web forensics. The phases of the computer forensic procedure and the OoV are two essential elements that recur regularly. These are crucial factors to take into account when creating any framework for digital forensics since they dictate how investigators should handle a case from start to finish. The OoV defines which data should be collected first because the nature of the data make them quickly adaptable through simple machine activities.

Although there is no acknowledged volatility hierarchy, Figure 4 illustrates the order of volatility in browsing forensics and covers the specific example of Windows operating systems. This later indicates that examples of data other than RAM should be considered when gathering evidence. Investigators must take the computer forensic procedure into account. Although there are no set standards for this, the outcomes of all reported approaches are comparable.

OoV	Explanation
1	Cache and Registers
2	Routing tables
3	ARP cache
4	Process table
5	Kernel statistics and modules
6	Main memory (RAM)
7	Temporary file system
8	Secondary memory
9	Router configuration
10	Network topology

Figure 4. Order of volatility in digital forensics and incident response.

6. The Proposed High-Level Protocol

With these fundamental computer forensic principles identified, we can establish the protocol. A universal protocol is developed for the scope and objective of this study so that researchers can use it with various operating systems and software programmes. In-depth needs for scenarios like various operating systems (Windows, Mac, Linux, Live OS) or software packages for dark web access can be determined through further research on this topic (I2P, Freenet). The suggested protocol, known as the D2WFP, can be found in Figure 5. This protocol will serve as an essential manual for people who seek to examine possible evidence linked to crimes committed on the dark web, stressing the kinds of forensics that investigators should perform and the proper sequence in which to do so. The crucial procedures for locating the evidence and protecting it have been emphasised. If this is performed incorrectly, the forensic analysis may produce tainted evidence that is not admissible in court. Figure 5 illustrates the alignment of the proposed dark and deep web forensic protocol with the standard digital forensic phase divided into four

branches: evidence identification, acquisition and preservation, examination and analysis, and finding presentation.

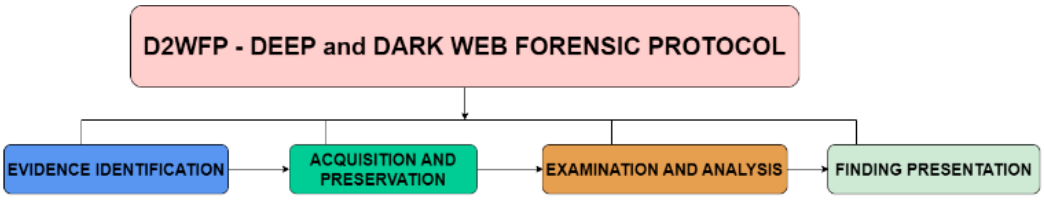

Figure 5. D2WFP—deep and dark web forensic protocol branches.

7. Detailed D2WF Protocol

7.1. Evidence Identification

Evidence identification is vital to a trial in the legal system. As a result, identifying what makes a piece of evidence vital to building a solid case is essential.

- ➢ Identify and collect suspect devices: identifying potential evidence that may have been used in a crime is crucial to ensuring it will be admissible in court. This can be achieved by examining the crime scene, speaking to witnesses, or reviewing surveillance footage.
- ➢ Identify extra storages (e.g., cloud and IoT): once potential evidence has been identified, collecting and documenting it accurately is crucial.
- ➢ Identify extra storages (e.g., cloud and IoT): during the evidence identification phase, it is critical to identify extra storage (e.g., cloud and IoT) that may contain vital data, and a process technique to extract these data should be developed.
- ➢ Determine the required hardware/software: determining what is necessary to complete the evidence identification will include hardware, software, and storage requirements. Each task is unique, and it is critical to tailor the needs of the task to the hardware, software, and storage requirements.

7.2. Acquisition and Preservation

Acquisition is the process of gathering and collecting evidence, whereas preservation is the act of keeping, protecting, or preventing evidence from deteriorating.

- ➢ Establish a chain of custody: a "chain of custody" is a paper trail or chronological documentation that shows the seizure, control, transfer, analysis, and disposition of physical or electronic evidence. When gathering evidence, it is critical to maintain a chain of custody to ensure its integrity and admissibility in court.
- ➢ Acquire volatile data following the order of volatility (OOV): Volatile data are information stored in a computer's temporary memory, and these are lost when the system is powered down. It is critical to acquire evidence in the order of volatility to ensure that as much data as possible are recovered from a system. This means that the most volatile data, i.e., data in a system's temporary memory, should be acquired first.
- ➢ Acquire physical or logical file system images: a physical file system image is a bit-for-bit copy of a storage device, such as a hard drive, that can be used to forensically examine the device's contents, whereas a logical file system image is a copy of data on a storage device that can be created without creating an exact bit-for-bit copy of the device. Logical file system images typically include only the files and folders required for a specific investigation.
- ➢ Import/backup cloud-based content: acquiring and backing up cloud-based content ensures that the evidence is not lost or tampered with if the cloud-based service is shut down or deleted.
- ➢ Extract networking and logging data: investigators will often need to collect networking and logging data from reconstructing events or tracking down suspects. This information can be obtained from network devices or servers.

- Secure evidence and store original devices in a safe: once the evidence has been collected, it must be secured and stored in a secure location. This will prevent the evidence from being lost or tampered with. Keeping the original devices in a safe location is also critical to ensure their integrity.

7.3. Examination and Analysis

Examination and analysis are the reconstruction and interpretation of evidence and follow the tasks below.

- Analyse RAM and examine URLs, web content, search queries, logging details, and downloaded files: examine the running processes, visited websites, downloaded files, system logs, open files, and network connections to reconstruct events.
- Analyse browsing data, file system/registry, examine URLs, bookmarks, usage sessions, timestamps, and caches: we can begin by looking at web browser data to obtain an idea of what the user is performing on the system. This provides an overview of the websites the user visits and the types of activities carried out. The -r option returns a grep list of all bookmarks saved by the user. We can use the grep -c option to print the number of times each URL has been visited. To see a list of all the cookies stored on the system, use the -f option with grep. We can use the grep -s option to see how many times each cookie has been accessed.
- Analyse logs and networking cookies, examine downloads and browsing: examine the log files with the command-line tool grep to search for specific keywords in the log files. We can use the grep -r option to see a list of all the IP addresses that the user has accessed. We can use the grep -c option to see how many times each IP address has been accessed.
- Analyse cloud backup and examine logging, browsing, and search queries: this search can reveal user activities during the examination and analysis phase. However, the information that is stored in the remote location through a network such as the Internet is further analysed, the logging details of the activities and who was involved are examined, and the search behaviour of the user is evaluated so that the investigator can organise and obtain more insight on the user's activities and the incidents that happened.
- Correlate findings and establish the final timeline: we reviewed the findings and looked for patterns or themes. If there are any gaps in the data, we conduct additional research to correlate the findings. Once we have a clear picture of what occurred, we create a detailed timeline of events that will serve as the foundation for the final report.

7.4. Findings Presentation and Reporting

The layout and reporting are the protocol's final phase, in which we summarise and draw a conclusion based on the evidence. Request further data (ISP, web servers): if applicable, we can request more information from the ISP or web servers.

- Process findings, correlate findings, and remove duplication: at this stage, we process all of the evidence files' findings and correlate them to remove any duplication.
- Summarise findings in accordance with the relevance and acceptance to reconstruct the crime environment and ensure that the evidence is admissible.
- Complete findings and present a technical report: when all the above digital forensic processes have been completed, the findings need to be presented and put in an orderly document that validates the evidence collected, tracked, and analysed. The findings should be protected and kept in a safe place for access when needed. Security of such information is vital to avoid tampering or loss of data.

The overall proposed deep and dark web forensic protocol (D2WFP) is represented in Figure 6.

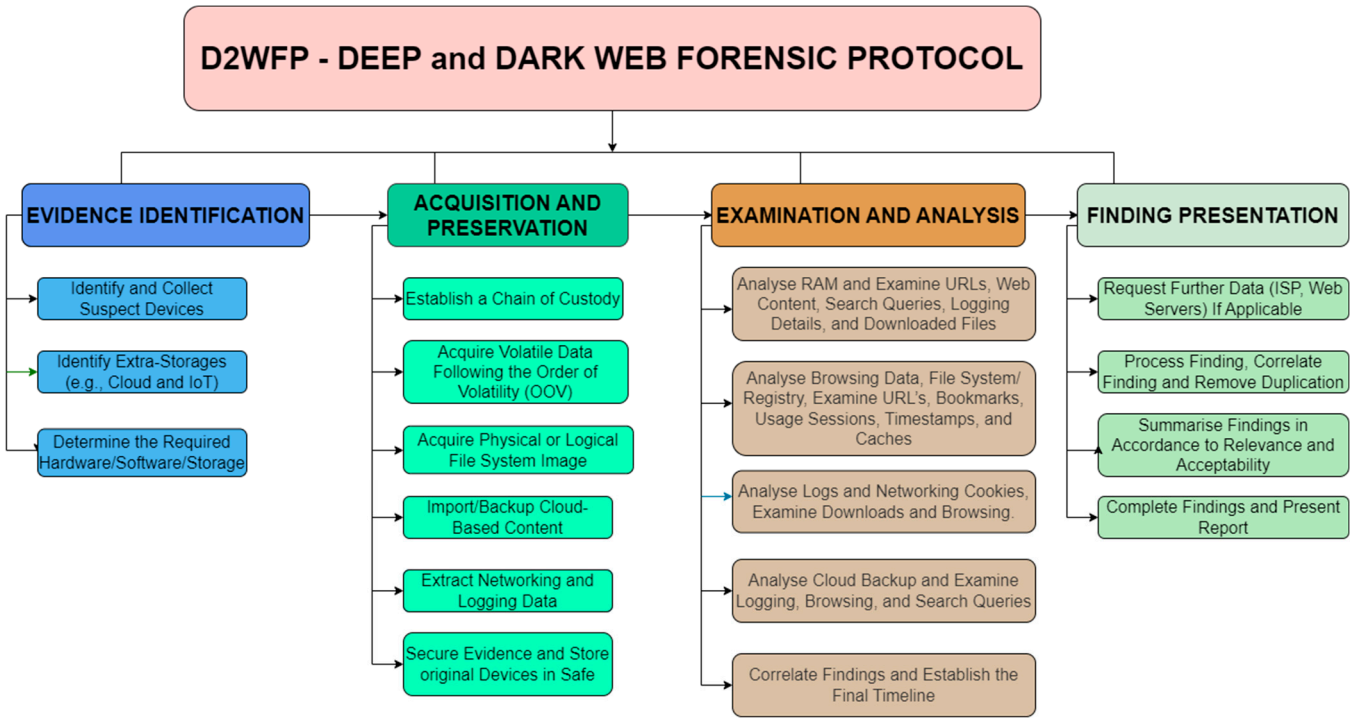

Figure 6. Detailed proposed protocol—deep and dark web forensic investigation protocol.

8. Forensic Scenarios Design and Dataset Generation

In this study, we aimed to cover as many digital pieces of evidence as possible. We used the resources available to us to create realistic digital forensic scenarios by using four different types of devices, each running a different operating system and all using the TOR browser or an equivalent browser for Apple iOS. The first machine was running Windows 10, the second was running Kali Linux 2021, the third was a mobile device running Android 11, and the last was an iPhone running iOS 14.2. Table 3 (below) summarises all activities carried out identically on all four devices including the type of activities performed, tools and services used, the scope and aim behind performing the activity, and the frequency of the activities which stands for the number of separate activities performed. The following three (03) steps were adopted to generate the dataset following the predefined scenarios:

- Download, install, and adjust TOR browser: we visited the official Tor Project website (https://www.torproject.org/) and downloaded the Tor browser or pre-established app for four different operating systems (Windows, Android, iOS, and Linux). We then proceeded to the installation when required. The last part was to align the TOR browser privacy and anonymity parameters to ensure consistency throughout the four different OSs.
- Arming TOR browser: we launched TOR to confirm the successful installation which automatically connects to the OR network and routes your Internet traffic through it. Then, we aligned the TOR browser privacy and anonymity parameters to ensure the consistency of our simulations.
- Browse deep and dark web content: once the Tor browser was open, we performed a series (similar to each of the four devices) of dark and deep web content browsing including visiting websites, using online services, and connecting to hidden wikis and services anonymously. All these activities were carried out in respect of legal and ethical boundaries and experiments were stopped before any engaging in illegal activities on the deep and dark web.

Table 3. Summary of all activities carried out including the type of activities performed, tools and services used, the scope and aim behind performing the activity, and the frequency of the activities which stands for the number of separate activities performed.

Activity Type	Tool or Service	Target and Scope	Frequency
D2W Search	Torch	Last working link: torchizzuasvoc3p6xed6u4owzoeyajrijthabikjnv5vnkcdppt6aid.onion Performing dark web search and bookmarking using Torch engine that indexes around 1.1 million pages in D2W.	12
	DuckDuck Go	Last working link: duckduckgogg42xjoc72 × 3sjasowoarfbgcmvfimaftt6twagswzczad.onion Performed deep web search and bookmarking for hidden services also accessible on the regular web but offered without any logs.	9
D2W Markets	Venus	Last working link: venusuwqyvt73sd6mqmpvyef3u5gjw3bfgn2aypd2ljtopylgintszqd.onion Browsing and enquiring following the anonymous mode of the marketplace.	2
	Rxholesale	Last working link: rxwsalevpsunomwywonwis4r5pnx7eohk4iqktmnnyq72lufhffahyid.onion Browsing the illegal drugs catalogue (no active purchase or ordering) from the UK and EU top dark web drug store.	2
D2W Email	Cock.li	Last working link: xdkriz6cn2avvcr2vks5lvvtmfojz2ohjzj4fhyuka55mvljeso2ztqd.onion Creating an account, authenticating, and communicating using Cock.li onion mirror webmail provider with the minimum privacy preservation mode.	5
	Riseup	Last working link: 5gdvpfoh6kb2iqbizb37lzk2ddzrwa47m6rpdueg2m656fovmbhoptqd.onion Creating an account, authenticating, and communicating using Riseup provides using generic mode.	3
D2W IDs Forgery	Elf Qrin's Lab	Last working link: elfqv3zjfegus3bgg5d7pv62eqght4h6sl6yjjhe7kjpi2s56bzgk2yd.onion Browsing and simulating (not ordering) the request of fake US identity including fake IDs, SSN, driver's licence, and credit card numbers generator. Testing the "Get a dark web new identity" feature.	2
D2W Financial Services	CashCow	Last working link: cashcowgpgemkxm5bnwlumwicmjlolx4nnhvuvgg6d4nes3z7k7awtqd.onion Browsing features offered in CashCow including dark web PayPal transfer service.	1
	CashCards	Last working link: cashcardix5cpw4foar3gfenz5k3ccvqflrnj2mdm4o7xygfmmfchcyd.onion Browsing features offered by CashCards including credit cards, CC Fulls, dumps, and CVV.	1
	Light Money	Last working Link: lmoneylrnftm7qyr76nglfwecix7vn72b7uv6srbyvy2pr25pet42bad.onion Creating an account, authenticating, and browsing available dark web gift cards and exploring offered wire transfers.	3

For consistency purposes, LEAs were asked to execute the same scenario in terms of browsing, creating accounts, logging, saving credentials, and bookmarking websites. All the following predefined LEA scenarios included a local replication of shutting down hidden wikis, as illustrated in Table 3. All these activities were carried out on a simulation equivalent setup for teaching and research purposes, and LEAs adhered to strict research guidelines to avoid any misconduct. After completing the forensics case, we moved on to forensic evidence identification and acquisition, mainly by performing live memory

capture (RAM) with the FTK Imager and UFED, and capturing networking data from the access points. In addition, we used the FTK Imager to acquire forensic bit-stream HDD images for the two hard drives used in the Windows 10 and Kali Linux 2021 machines.

We did, however, perform a logical plus file system extraction for Android 10 and iOS 14.2 devices because physical extraction was impossible as neither device was jailbroken or rooted. Following the completion of the first round of data acquisition, the next step was to apply anti-forensic measures mimicking the cybercriminal operative mode in order to delete Internet browsing and activity tracks. This was performed through the use of BleachBit to remove any existing browsing artefacts. Imaging of the device was performed using the UFED Touch 2 tablet provided by Cellebrite and was demonstrated for mobile devices and OpenText TX1 for computer hard drives, as illustrated in Figure 7.

Figure 7. Microsoft Windows 10, Linux Kali 2021.3, Apple iOS 14.2, and Google Android 11.1 forensic imaging.

We performed anti-forensic tasks by installing BleachBit, a browsing anti-forensic software, on all four devices before acquiring the image files again. We performed several rounds of the deletion of Internet browsing activities to determine whether our proposed protocol is applicable in anti-forensic cases. We then jailbroke the iOS device and rooted the Android device before performing a second round of data acquisition on the mobile devices. As a result, we created a new set of images for the hard drive running Windows 10 and Kali Linux 2021, as well as completed the physical extraction (available after jailbreaking and rooting) for iOS and Android smartphones. Figure 8 illustrates the use of BleachBit to delete caches, temporary files, and browsing-related artefacts.

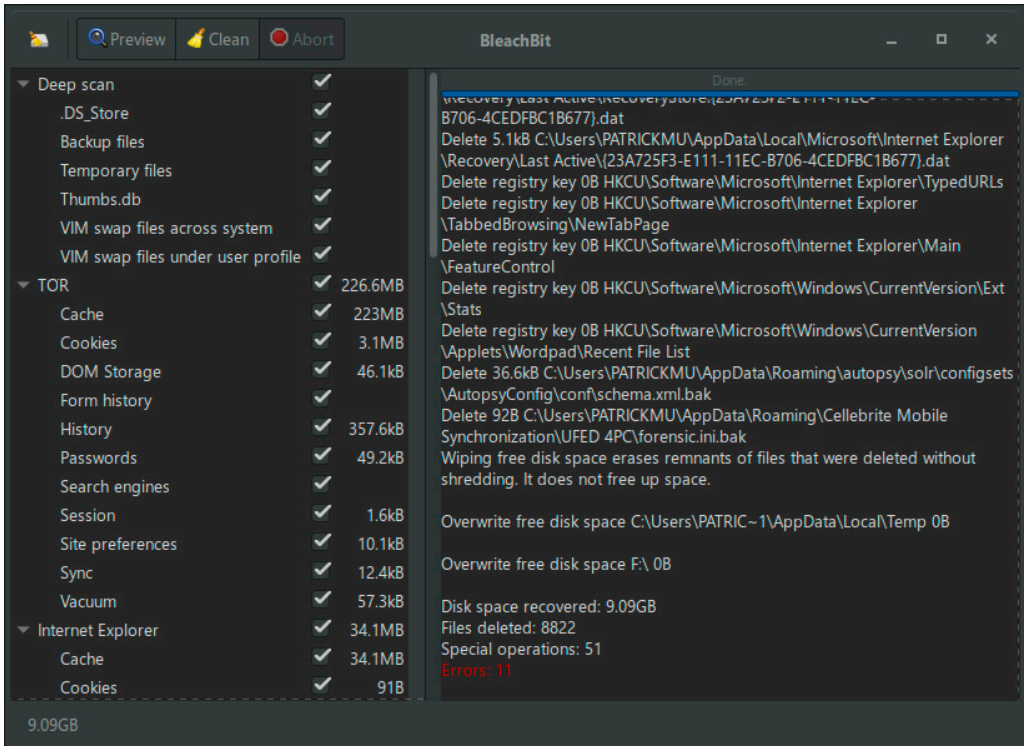

Figure 8. Applying anti-forensics by deleting all browsing artefacts using the BleachBit tool.

9. Forensic Processing, Examination, and Analysis

The created images needed to be processed and analysed using relevant forensic software according to the evidence file types. FTK and Magnet were used for the Windows 10 images to ensure that all potential artefacts were picked up to compare the two industrial tools. To analyse the evidence files and provide comparison results, we used a Cellebrite Physical Analyser and Magnet. When processing the Windows images in FTK, we chose the most appropriate forensic profile to ensure we could find all relevant artefacts after the completion of the FTK processing. The steps for processing the evidence within AXIOM were very similar to FTK. For mobile devices, we imported the .ufdx file generated by the Cellebrite tablet to process the mobile images into the Cellebrite Physical Analyzer. In addition, we attempted processing the caches and RAM dump obtained from the remaining devices using the AXIOM Magnet embedded volatility module. Figure 9 illustrates the performed forensic processing, construction, reconstruction, and indexation processes.

In terms of forensic processing, we analysed and examined the indexed data from both the automated tools and D2WFP. We initially examined the browsing history, which contains data about the navigation history of the user, which is used to track down if the user visited some malicious sites hosted on the dark web; we examined the data related to web searching alongside the navigation history to obtain complete insight on the browsing activities. Secondly, we examined the security and logins data, including security logging, saved passwords, extensions, and addons. Thirdly, we examined the cache and temporary data by looking into self-explanatory. A cache is generated when navigating websites and all sorts of temporary files created by the browser, notably cache data, images, and JavaScript, which are great data sources during a forensic investigation. Fourthly, we examined all forms and database files used or generated by the browser; this step aims to acquire more information about the website or places the user visited, including form data which are anything typed inside forms and stored by the browser. Finally, we examined the data related to data transfer and specifically downloads.

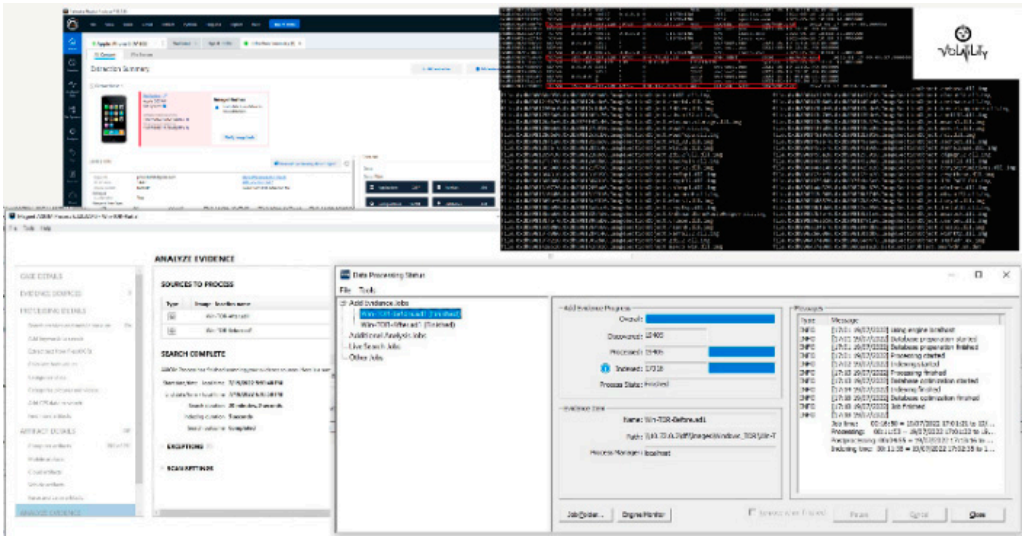

Figure 9. Forensic processing including data recovery, reconstruction, and indexation using FTK, AXIOM, UFED, and volatility.

We then analysed and compared artefacts such as browsing history, security and logins, cache and temporary files, SQLite DB forms, and downloads that we could determine from all the created forensic images. Following image analysis, the primary quantitative data analysis technique was hypothesis analysis, which compares the study hypothesis with the findings using sample data from the developed images. However, the quantitative analysis generated tables highlighting the artefacts discovered for each image, such as cookies, login information, and browsing history. We subsequently investigated the testing results by confirming the extent and amount of information retrieved about TOR activities. The results are presented visually in Tables 2 and 3. We highlight the number of recoverable artefacts for various types of devices and the impact of the tools used in removing the web-based artefacts.

Table 4 illustrates the number of artefacts by category obtained using DFIR tools and the D2WFP before any anti-forensic activities have taken place. On the other hand, Table 5 illustrates the number of artefacts by category obtained using DFIR tools and the D2WFP after applying anti-forensic measures by deleting the Internet and browsing artefacts using BleachBit.

Table 4. D2WFP—deep and dark web forensic protocol result compared with regular automation using FTK for Windows 10, AXIOM for Kali 2021.3, and UFED for Android 11 and iOS 14.2.

Artefacts	Protocol	Windows 10	Linux Kali 2021	Android 11	Apple iOS 14.2
Browsing	Regular	1094	1086	1238	991
	D2WFP	**1325**	**1631**	**1562**	**1133**
Security & Logins	Regular	30	30	30	30
	D2WFP	**53**	**77**	**66**	**34**
Cache & Temp	Regular	6732	5328	3627	4381
	D2WFP	**10,938**	**9677**	**7201**	**6320**
SQLite DB Form	Regular	227	328	196	188
	D2WFP	**636**	**801**	**786**	**295**
Downloads	Regular	106	106	112	112
	D2WFP	**317**	**429**	**299**	**243**

Results are generated automatically without accounting for empty or invalidated entries.

Table 5. D2WFP—deep and dark web forensic protocol result compared with regular automation after anti-forensic BleachBit using FTK for Windows 10, AXIOM for Kali 2021.3 and UFED for Android 11 and iOS 14.2.

Artefacts	Protocol	Windows 10	Linux Kali 2021	Android 11	Apple iOS 14.2
Browsing	Regular	107	239	226	287
	D2WFP	**679**	**799**	**804**	**453**
Security & Logins	Regular	07	09	06	02
	D2WFP	**17**	**19**	**20**	**09**
Cache & Temp	Regular	1126	907	1372	774
	D2WFP	**4681**	**5414**	**5755**	**2413**
SQLite DB Form	Regular	15	44	67	06
	D2WFP	**354**	**403**	**409**	**154**
Downloads	Regular	25	29	22	09
	D2WFP	**109**	**174**	**188**	**68**

Results are generated automatically without accounting for empty or invalidated entries.

10. Results and Discussion

In this section, we discuss the effectiveness of the proposed protocol, D2WFP, by examining and performing a quantitative evaluation which consists of comparing the results found in the forensic testing of the D2WFP against the results generated from the automated DFIR tools and framework, namely FTK, AXIOM, and UFED. The carried testing is limited to the use of an anonymity and privacy-preserving browser in criminal activities and only covers artefacts recovered from criminal machines or devices. During the elaboration of the protocol, several tests were carried out, and the results obtained enabled us to make some tweaks or changes to improve the D2WFP. The first set of tests covered a comparative analysis of the number of investigative leads (deep and dark web artefacts) related to web browsing using TOR. We clearly distinguished the higher number of artefacts indexed when adopting the D2WFP than those indexed using the relevant tool/framework. The difference observed is significantly higher in Linux, Windows, and Android and notably in the number of browsing history, cache, and temporary files. The D2WFP outperforms the automated tools in all other categories, such as security, logins, SQLite DB forms, and downloads. In the iOS context, despite having the number of indexed browsing artefacts in favour of the D2WFP, the gap is less significant due to the security and memory handling restrictions implemented in the iOS and macOS. The analysis of the ongoing results illustrates the D2WFP's effectiveness in locating, extracting, and exploiting deep and dark web activities through indexing by, on average, 35–45% more than the number of artefacts discovered by industrial tools when working in regular automation mode.

The second set of tests covered the analysis of the four forensic images obtained after running an anti-forensic software BleachBit version 4.4.1 to erase browsing data artefacts. Here, again, the obtained results illustrate the effectiveness of the D2WFP compared with regular automated DFIR tools and frameworks in terms of the number of deep and dark web artefacts related to web browsing using TOR indexed. The proportion in terms of the difference between regular automation in FTK, AXIOM, and UFED compared with the D2WFP is distinguished, notably the higher number of artefacts indexed in browsing, security, and cache when the figures show that by adopting the D2WFP, the number of indexed artefacts (mostly recovered and carved) is four times higher compared with the number of artefacts indexed using the relevant tool/framework. The observed difference is significantly higher in Linux, Windows, and Android, particularly in the number of browsing history, cache, and temporary files. The D2WFP outperforms the automated tools in all other categories, such as security, logins, SQLite DB forms, and downloads. In the

context of iOS, the number of indexed artefacts is in favour of the D2WFP, but the gap is less significant due to security.

To sum up, the proposed D2WFP is introduced here to formally structure the activities of browsing artefact investigations and guide DFIR practitioners in tackling deep and dark web browsing artefact investigations. The protocol applies to most of the anonymity and privacy-preservation browsing tools and not only TOR which was adopted for our case study. Forensically investigating DDW browsing activities when adopting the D2WFP outperforms any regular forensic automated tool as the obtained results were validated in comparison with FTK, AXIOM, and UFED which are the industry leaders. The adoption of the D2WFP resulted in finding, extracting, and reconstructing more artefacts than with those automated tools (regular automation) and the obtained results were validated in the context of the four most-used Oss, namely Windows, Linux, Android, and iOS.

11. Conclusions and Future Works

Cybercriminal activity on or through the dark web is on the rise. Although designed as legitimate tools for online security, anonymity, and privacy purposes, deep and dark web browsers allow public access to parts of the web that are not ordinarily searchable, indexed, or accessible through standard browsers. This study proposed a novel and comprehensive investigative protocol to guide and assist digital forensic professionals in investigating crimes committed on or via the deep and dark web. In this study, we critically analysed the limitations in current automation, identified the research gap, and developed the D2WFP following scientific and experimental approaches. The proposed D2WFP protocol incorporates new and improved existing methods, mainly by establishing a sequence for performing tasks and subtasks to improve the current tools' output accuracy and effectiveness, observing the order of volatility, and implementing a systemic approach covering all browsing-related hives and artefacts. A quantitative examination of the protocol's capabilities was carried out following the testing using several cases, both on computer and mobile devices running four different OS. The investigations and examinations were conducted using the professional version of Access Data FTK, Magnet AXIOM, and Cellebrite UFED. The results show an apparent increase in the number of artefacts recovered when adopting the D2WFP compared with regular tools and framework-based automated investigations. In future work, we will consider the impact of the different levels of security in all anonymity and privacy-preserving browsers (TOR, FREENET, WATERFOX, TAILS) and will analyse the security settings' impact on the DFIR activities, mainly by considering the different modes such as "standard", "safer", and "paranoid".

Author Contributions: Conceptualisation, M.C.G., P.M. and D.D.; methodology, M.C.G., P.M. and K.O.; software, M.C.G., P.M., R.D. and D.D.; validation, M.C.G., P.M., R.D. and D.D.; formal analysis, M.C.G. and K.O.; investigation, M.C.G., P.M. and D.D.; resources, M.C.G.; writing—original draft preparation, M.C.G., P.M. and D.D.; writing—review and editing, K.O. and R.D.; supervision, M.C.G. and K.O.; project administration, K.O. and M.C.G. funding acquisition, M.C.G. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the UK HEIF fund from the Cyber Security Research Center under Grant RES02M3732.

Institutional Review Board Statement: This research was granted exemption by institutional ethics committee at SCDM during the meeting of 6 April 2022 as it doen't fall under any of the cases requiring ethical approval. Furthermore, it is worth to highlight that datasets were created from the forensic imaging of privately owned computer and mobile devices. The deep and dark web activity were emulated and only covered previously reported criminal websites by fully certified forensic examiners in respect of the Computer Misuse Act 1990 and Regulation of Investigatory Powers (RIPA) Act 2000, along with the ethical principles set by the Biometrics and Forensics Ethics Group, notably governing principle number 5.

Data Availability Statement: Datasets generated during this research work are available to researchers upon request.

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

References

1. Arshad, M.R.; Hussain, M.; Tahir, H.; Qadir, S. Forensic Analysis of Tor Browser on Windows 10 and Android 10 Operating Systems. *IEEE Access* **2021**, *9*, 141273–141294. [CrossRef]
2. Brinson, R.; Wimmer, H.; Cheng, L. Dark Web Forensics: An investigation of tracking dark web activity with digital forensics. In Proceedings of the Interdisciplinary Research in Technology and Management (IRTM), Kolkata, India, 24–26 February 2022. [CrossRef]
3. Balduzzi, M.; Ciancaglini, V. Cybercrime in the Deep Web. In Proceedings of the 2015 Black Hat EU Conference, Amsterdam, The Netherlands, 10–13 November 2015.
4. Baronia, D. Dark Web and Tor Forensic. 2021. Available online: https://informaticss.com/dark-web-and-tor-forensic/ (accessed on 12 October 2022).
5. Gehl, R.W. *Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P*; MIT Press: Cambridge, MA, USA, 2018.
6. Cherty, A.; Sharma, U. Memory forensic analysis for investigation of online crime- A review. In Proceedings of the IEEE 6th International Conference on Computing for Sustainable Global Development, New Delhi, India, 13–15 March 2019.
7. European Monitoring Centre for Drugs and Drug Addiction and Europol. *Drugs and the Darknet: Perspectives for Enforcement, Research and Policy*; Publications Office of the European Union: Luxembourg, 2017.
8. Forensic-Pathways. Dark Web Investigations/Monitoring. 2020. Available online: https://www.forensic-pathways.com/dark-web-investigationsmonitoring/ (accessed on 12 October 2022).
9. Godawatte, K.; Raza, M.; Murtaza, M.; Saeed, A. Dark Web Along with the Dark Web Marketing and Surveillance. In Proceedings of the 2019 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), Gold Coast, QLD, Australia, 5–7 December 2019; IEEE: Piscataway, NJ, USA, 2019.
10. Goodison, S.E.; Woods, D.; Barnum, J.D.; Kemerer, A.R.; Jackson, B.A. *Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web*; Research Report; RAND Corporation: Santa Monica, CA, USA, 2019.
11. Handalage, U.; Prasanga, T. Dark Web, Its Impact on the Internet and the Society: A Review. *J. Comput. Commun.* **2020**, *7*, 30–43. [CrossRef]
12. Protrka, N. Cybercrime. In *Modern Police Leadership*; Palgrave Macmillan: London, UK, 2021; pp. 143–155.
13. Rafiuddin, M.F.B.; Minhas, H.; Dhubb, P.S. A dark web story in-depth research and study conducted on the dark web-based on forensic computing and security in Malaysia. In Proceedings of the 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 21–22 September 2017; pp. 3049–3055. [CrossRef]
14. Leng, T.; Yu, A. A framework of darknet forensics. In Proceedings of the International Conference on Advanced Information Science and Systems, Depok, Indonesia, 23–25 October 2021. [CrossRef]
15. Maisammaguda, D. Digital Notes on Computer Forensics, India: Malla Reddy College of Engineering and Technology. Maryville University, 2017. Top 4 Data Analysis Techniques That Create Business Value. 2019. Available online: https://online.maryville.edu/blog/data-analysis-techniques/#qualitative (accessed on 4 December 2022).
16. Matic, S.; Kotzias, P.; Caballero, J. Caronte: Detecting location leaks for deanonymizing tor hidden services. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 12–16 October 2015; pp. 1455–1466.
17. Ghanem, M.C. Cryptographically Upgrading TOR Network to Enforce Anonymity by Enhancing Security and Improving Performances. *Preprints.org* **2023**, *1*, 2023070982. [CrossRef]
18. Nazah, S.; Huda, S.; Abawajy, J.; Hassan, M.M. *The Evolution of Dark Web Threat and Detection: A Systematic Approach*; IEEE: Piscataway, NJ, USA, 2020; pp. 171796–171819. [CrossRef]
19. Rogers, B. *Tor: Beginners to Expert Guide to Accessing the DarkNet, TOR Browsing, and Remaining Anonymous Online*, 1st ed.; CreateSpace Independent Publishing Platform: Scotts Valley, CA, USA, 2017.
20. Zeid, R.B.; Moubarak, J.; Bassil, C. Investigating the darknet. In Proceedings of the International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020. [CrossRef]
21. Ozkaya, E.; Islam, R. *Inside the Dark Web*; CRC Press: Boca Raton, FL, USA, 2019. [CrossRef]
22. Popov, O.; Bergman, J.; Valassi, C. A framework for forensically sound harvesting the dark web. In Proceedings of the Central European Cybersecurity Conference, Ljubljana, Slovenia, 15–16 November 2018; pp. 1–7.
23. Holland, B.J. Transnational cybercrime: The dark web. In *Encyclopedia of Criminal Activities and the Deep Web*; IGI Global: Hershey, PA, USA, 2020; pp. 108–128.
24. Jardine, E. *The Dark Web Dilemma: Tor, Anonymity and Online Policing*; Global Commission on Internet Governance Paper Series; Centre for International Governance Innovation: Waterloo, ON, Canada, 2015; Volume 21, pp. 1–11. [CrossRef]
25. Tazi, F.; Shrestha, S.; Cruz, J.D.L.; Das, S. SoK: An Evaluation of the Secure End User Experience on the Dark Net through Systematic Literature Review. *J. Cybersecur. Privacy* **2022**, *2*, 329–357. [CrossRef]

26. Samtani, S.; Zhu, H.; Chen, H. Proactively identifying emerging hacker threats from the dark web: A diachronic graph embedding framework. *ACM Trans. Priv. Secur. (TOPS)* **2020**, *23*, 1–33. [CrossRef]
27. Dunsin, D.; Ghanem, M.; Ouazzane, K. 'The Use of Artificial Intelligence in Digital Forensics and Incident Response in a Constrained Environment', World Academy of Science, Engineering and Technology, Open Science Index 188. *Int. J. Inf. Commun. Eng.* **2022**, *16*, 280–285.