



Module Title: Individual Project

Module Code: CST3590

Dark Web Forensics: Techniques and Challenges

Student: Syed Muhammad Haider Razvi

Student Number: M00832169

A dissertation submitted in fulfillment of the requirements
for the degree of BSc (Hons) Cyber Security
& Digital Forensics

Dept. of Computer Science

2025

Contents

| | | |
|----------|--|-----------|
| 1 | Introduction to the Dark Web Forensics | 1 |
| 1.1 | The Tor Network: Architecture and Anonymity Features | 2 |
| 2 | Literature Review | 4 |
| 2.1 | Forensic Techniques for Dark Web Investigations | 4 |
| 2.1.1 | Memory Forensics in Dark Web Investigations | 4 |
| 2.1.2 | RAM Dump Collection | 4 |
| 2.1.3 | Tor Artifact Analysis | 5 |
| 2.1.4 | Malware Identification | 5 |
| 2.1.5 | Network Traffic Tracing | 5 |
| 2.1.6 | Challenges and Considerations | 5 |
| 2.1.7 | Forensic Tools | 5 |
| 2.2 | Network and Traffic Analysis | 8 |
| 2.3 | Open-Source Intelligence (OSINT) and Crawling | 8 |
| 2.4 | Cryptocurrency Forensics | 9 |
| 2.5 | Challenges in Dark Web Forensics | 9 |
| 2.5.1 | Anonymity and Encryption | 10 |
| 2.5.2 | Ephemeral and Volatile Data | 10 |
| 2.5.3 | Attribution and Identification | 11 |
| 2.5.4 | Legal and Ethical Issues | 11 |
| 2.6 | ISO/IEC Standards and Their Applicability to Dark Web Forensics . . . | 12 |
| 2.7 | Emerging Technologies and their impact on Dark Web Forensics | 13 |
| 2.8 | Ethical and legal | 14 |
| 2.8.1 | Ethical Challenges in Dark Web Investigations | 14 |
| 2.9 | Strategies for Enhancing Dark Web Forensic Investigations | 15 |
| 2.9.1 | Training and Capacity Building | 15 |
| 2.9.2 | International Collaboration | 15 |
| 2.9.3 | Public-Private Collaboration | 15 |
| 3 | Research Methodology | 16 |
| 3.1 | Research Design | 16 |
| 3.2 | Identification of Variables and Measures | 16 |
| 3.3 | Sample Size and Sampling Methodology | 17 |
| 3.4 | Methods of Data Collection | 18 |
| 3.5 | Ethical Considerations | 19 |
| 3.6 | Limitations | 20 |
| 4 | Analysis | 21 |
| 4.1 | Thesis Statement | 21 |

| | | |
|----------|---|-----------|
| 4.2 | Critical Evaluation of Current Forensic Techniques in Dark Web Investigations | 21 |
| 4.3 | Recommendations | 23 |
| 5 | Research Results | 25 |
| 5.1 | Prevalence of Host and Memory-Based Forensics | 25 |
| 5.2 | Challenges Due to Encryption, Anonymity, and Ephemeral Data | 25 |
| 5.3 | Emerging Role of Artificial Intelligence and Blockchain Analysis | 26 |
| 5.4 | Institutional and Operational Gaps in Capacity | 26 |
| 5.5 | Necessity for Legal Reform and Ethical Frameworks | 27 |
| 5.6 | Quantitative Performance of Dark Web Forensic Tools and Techniques | 27 |
| 5.6.1 | Performance Metrics of Key Forensic Tools | 27 |
| 5.7 | Success Rates of Key Techniques | 28 |
| 5.8 | Findings | 30 |
| 6 | Discussion and Conclusion | 31 |
| 6.1 | Discussion | 31 |
| 6.1.1 | Effectiveness of Current Forensic Techniques | 31 |
| 6.1.2 | Persistent and Evolving Challenges | 31 |
| 6.1.3 | Institutional and Ethical Considerations | 32 |
| A | Ethics Form | 33 |
| | Bibliography | 37 |

List of Tables

| | | |
|-----|--|----|
| 2.1 | ISO/IEC 27000-series | 13 |
| 2.2 | Ethical and Legal Considerations in Dark Web Forensics | 14 |
| 3.1 | Illustrating Variables and Measures | 17 |
| 3.2 | Criteria for Literature Inclusion | 18 |
| 3.3 | Systematic Literature Review Methodology | 19 |
| 3.4 | Ethical Principles in Literature Review | 19 |
| 3.5 | Research Limitations | 20 |
| 5.1 | Performance Metrics of Key Forensic Tools | 28 |
| 5.2 | Summary of Key Findings by Result Area | 30 |

List of Figures

| | | |
|-----|---|----|
| 1.1 | illustration of TOR browser | 3 |
| 2.1 | illustrating how Memory Forensics work | 7 |
| 5.1 | Graph illustrating success rates of Key Forensic techniques | 29 |

Abbreviations

| | |
|----------------|--|
| AI | Artificial Intelligence |
| AML | Anti-Money Laundering |
| BTC | Bitcoin (cryptocurrency) |
| ECC | Elliptic Curve Cryptography |
| ENFSI | European Network of Forensic Science Institutes |
| EnCase | Guidance Software's Digital-Forensics Suite |
| EUROPOL | European Union Agency for Law Enforcement Cooperation |
| FBI | Federal Bureau of Investigation |
| FTK | Forensic Toolkit (AccessData) |
| IOCTA | Internet Organised Crime Threat Assessment |
| I2P | Invisible Internet Project |
| ISO/IEC | International Organization for Standardization / International Electrotechnical Commission |
| J-CAT | Joint Cybercrime Action Taskforce |
| ML | Machine Learning |
| NIST | National Institute of Standards and Technology |
| NIT | Network Investigative Technique |
| OSINT | Open-Source Intelligence |
| P2P | Peer-to-Peer |
| PQC | Post-Quantum Cryptography |
| PGP | Pretty Good Privacy |
| PRECEPT | Principles for Ethical Conduct of Digital Forensics Investigations |
| RAM | Random-Access Memory |
| RAND | Research and Development Corporation |
| RSA | Rivest–Shamir–Adleman (public-key cryptosystem) |
| SIEM | Security Information and Event Management |
| Tor | The Onion Router |
| URL | Uniform Resource Locator |
| VPN | Virtual Private Network |

Abstract

The dark web, a concealed subset of the internet accessible only through specialized anonymity networks such as Tor and I2P, has evolved into a significant platform for illicit activities, including cybercrime, drug trafficking, weapon trade, data breaches, and child exploitation. As traditional forensic methodologies are often ineffective against the advanced encryption, decentralization, and anonymity features of dark web infrastructures, specialized investigative techniques are essential. This dissertation critically examines the current state, effectiveness, and limitations of dark web forensic techniques, synthesizing evidence from over 70 academic and technical sources. Adopting a qualitative literature-based methodology, the study analyses forensic approaches including host-based forensics, memory artifact recovery, network traffic correlation, open-source intelligence (OSINT), and cryptocurrency tracing. Additionally, it explores the persistent operational, legal, and ethical challenges faced by investigators, particularly encryption, ephemeral data, jurisdictional complexities, and evidentiary admissibility issues. The applicability of international forensic standards such as ISO/IEC 27037 and ISO/IEC 27042 in dynamic, anonymized digital environments is critically assessed. Furthermore, the dissertation evaluates emerging technological innovations, notably artificial intelligence, blockchain analytics, and quantum computing, highlighting their potential to revolutionize forensic practices in addressing investigative bottlenecks. Findings emphasize the imperative of comprehensive training, interagency collaboration, standardized forensic methodologies, and legal reforms to enhance investigative effectiveness. Ultimately, the dissertation argues that only through integrating multidisciplinary expertise, advanced technological frameworks, and robust ethical guidelines can forensic professionals effectively navigate and dismantle the increasingly sophisticated criminal networks operating within the dark web environment.

Chapter 1

Introduction to the Dark Web Forensics

The Internet is considered to be one, but it is comprised of three layers: the surface web, the deep web, and the dark web. The surface web is Google- and Bing-indexed content, yet the deep web is unindexed content including scholarly databases, subscription websites, as well as internal networks [1]. The dark web is part of the deep web and is deliberately concealed since it is only available using specialist software, among which are The Onion Router (TOR) or the Invisible Internet Project (I2P) [1].

The dark web is the concealed segment of the Internet that one can access only through anonymity networks such as Tor and I2P. Although there are valid reasons for confidentiality for these networks, as the state utilises it to share classified information across different government departments. However, the Dark Web has transformed into a sanctuary for cyber criminals for illegal operations, such as drug trafficking, cybercrime, illicit marketplaces, ammunition trade, stolen data, drug trade and child abuse content [2].

The dark web's privacy, confidentiality and advanced encryption substantially restrict efforts by law enforcement agencies to locate criminals, investigate and gather digital evidence [2]. Due to its complex nature, the traditional digital forensic techniques are less effective against the dark web's use of advanced encryption and decentralized services. Digital forensic investigators should acquire new methods and strategies to track down cyber criminals.

Dark web forensics involves identification, collection, and analysis of dark web users' and platforms' digital evidence. Experts and researchers have found that trails of evidence on the dark web differ from trails on the surface web [1]. Instead of server logs and IP addresses, researchers can go for data obtained from the routes of the Tor network, encrypted traffic, as well as artefacts from questionable devices [1].

Early research had already demonstrated that even with Tor's powerful security and privacy, traffic traces within a network often can be uncovered. Research have been conducted for memory artefacts of the Tor browser, and it highlights that forensic memory analysis would detect Tor use even if there was no disc evidence [3].

These studies highlight that the dark web is far from being impenetrable to dark web forensics, but it requires sophisticated and most contemporary digital forensic tools. Over the last decade, there has been an exponential increase of research conducted on the techniques to dark web forensics to cater with the challenges it poses, and standard procedures. The following is a compilation of **70 recent papers (2010-2024)** on forensic techniques used in dark web investigations, complications for investigators (legal, technical, and ethical), the significance of standards/frameworks, as well as emerging possibilities such as artificial intelligence and quantum computing, might influence the future of dark web forensics.

1.1 The Tor Network: Architecture and Anonymity Features

The Tor network makes user operations anonymous using layered encryption and relay routing, where a user's data passes through several nodes, entry, middle, and exit relays, each stripping away a layer of encryption [4]. This "onion routing" architecture makes it impossible for one single node to know both the source and destination, thus rendering normal surveillance ineffective [5].

Yet, although Tor makes powerful guarantees regarding anonymity, it makes forensic analysis more difficult. Sites based on Tor, which end in ". onion," employ hidden service protocols, which make it difficult to discern the physical location of the server admins [4]. Forensics must thus rely on endpoint weaknesses, inference of metadata, as well as evolving de-anonymization methods [6].

Figure 1.1

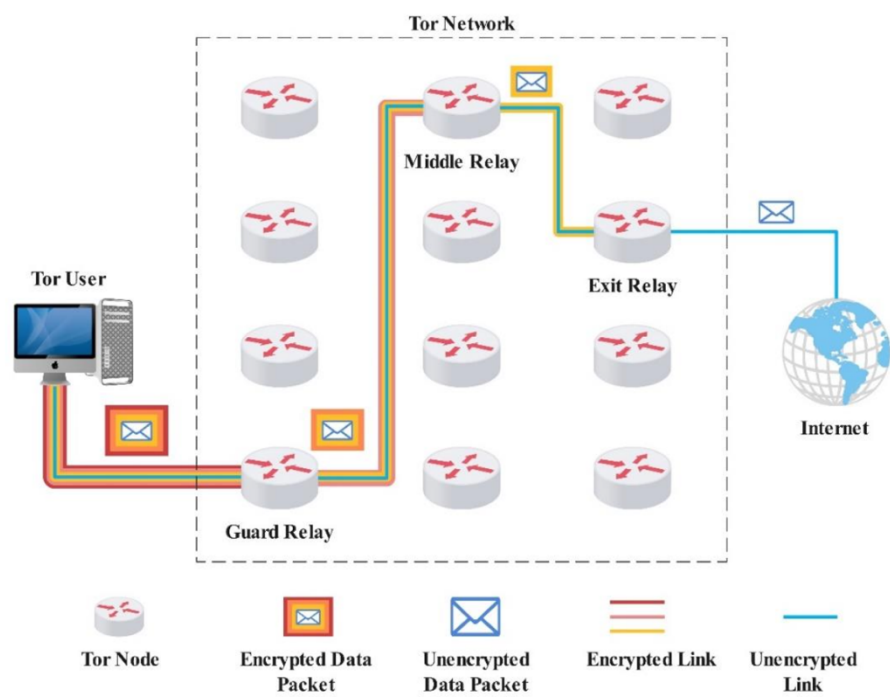


Figure 1.1: illustration of TOR browser

Chapter 2

Literature Review

2.1 Forensic Techniques for Dark Web Investigations

The dark web forensics requires that digital forensic techniques be modified and up to date, primarily because investigators may need to analyse everything from network traffic of onion routers to artifacts on seized devices. Forensic techniques may be categorised into few categories: network traffic analysis, host (endpoint) forensics, open-source intelligence (OSINT) gathering, and cryptocurrency tracing.

2.1.1 Memory Forensics in Dark Web Investigations

Memory forensics plays a vital role in dark web investigations, as most forensic methods become ineffective with the wide use of strong encryption and anonymization tools like Tor. These investigations require extracting forensic evidence from volatile memory (RAM), which may contain users' activity, running programs, encryption keys, network connections, and other temporary elements that are not saved on the disc for an extended duration [7], [8].

2.1.2 RAM Dump Collection

The initial step involved in memory forensics is acquisition of a RAM dump on the target system. FTK Imager and Volatility are commonly utilized tools to take a snapshot of memory on the system such that volatile information is captured before loss [7], [9]. These memory dumps can often reveal critical information such as Tor-related artifacts, including encryption keys, cached content from visited .onion websites, and even records of hidden services, which are typically absent from persistent storage [10], [11].

2.1.3 Tor Artifact Analysis

Memory forensics allows extraction and analysis of artifacts within the Tor Browser directly from RAM. Investigators can obtain sensitive information such as Tor circuit data, onion addresses, and encrypted browser session keys by through tools such as Volatility [10], [11]. Such information presents solid evidence of dark web interaction. In certain cases, examiners may also reveal session keys or reveal open connections to .onion sites, leading to ongoing crime [11].

2.1.4 Malware Identification

Memory analysis is also useful for finding malicious software that functions exclusively in RAM to avoid detection. These include rootkits, keyloggers, and other hidden malware that enable dark web communications or compromise users. These threats can be discovered by scanning the memory dump for malicious signatures or unusual activity [8]. If discovered, additional forensic investigation can then uncover the role played by malware in supporting or tracing dark web activity [9].

2.1.5 Network Traffic Tracing

While traditional network forensics fail with encrypted Tor communication, memory forensics provides an alternative. Network data and connection details that are temporarily stored in memory can be recovered and inspected to detect interactions with hidden services [10], [9]. This includes tracing open sockets, active connections to .onion services, and packet fragments, which can provide valuable information in investigations into dark web marketplaces and chat services.

2.1.6 Challenges and Considerations

Despite its benefits, memory forensics presents multiple challenges. The volatile nature of RAM means that evidence can be deleted if the entire system is turned off or memory is overwritten [9]. Memory analysis may uncover encryption keys that are kept in RAM, enabling investigators to decrypt unattainable information [10], [9]. Maintaining data integrity during capture is also critical for ensuring that the memory dump will be recognised as evidence in judicial proceedings [7].

2.1.7 Forensic Tools

Two key tools are commonly used in memory forensic investigation in dark web cases. The **Volatility Framework** is an open-source package able to analyse memory dumps to reveal details on running processes, network connections, and even decrypted information [9], [8].

FTK Imager is on the other hand a tried-and-true image and collection utility for acquiring memory dumps and getting them ready for further forensic examination [7].

Figure 2.1

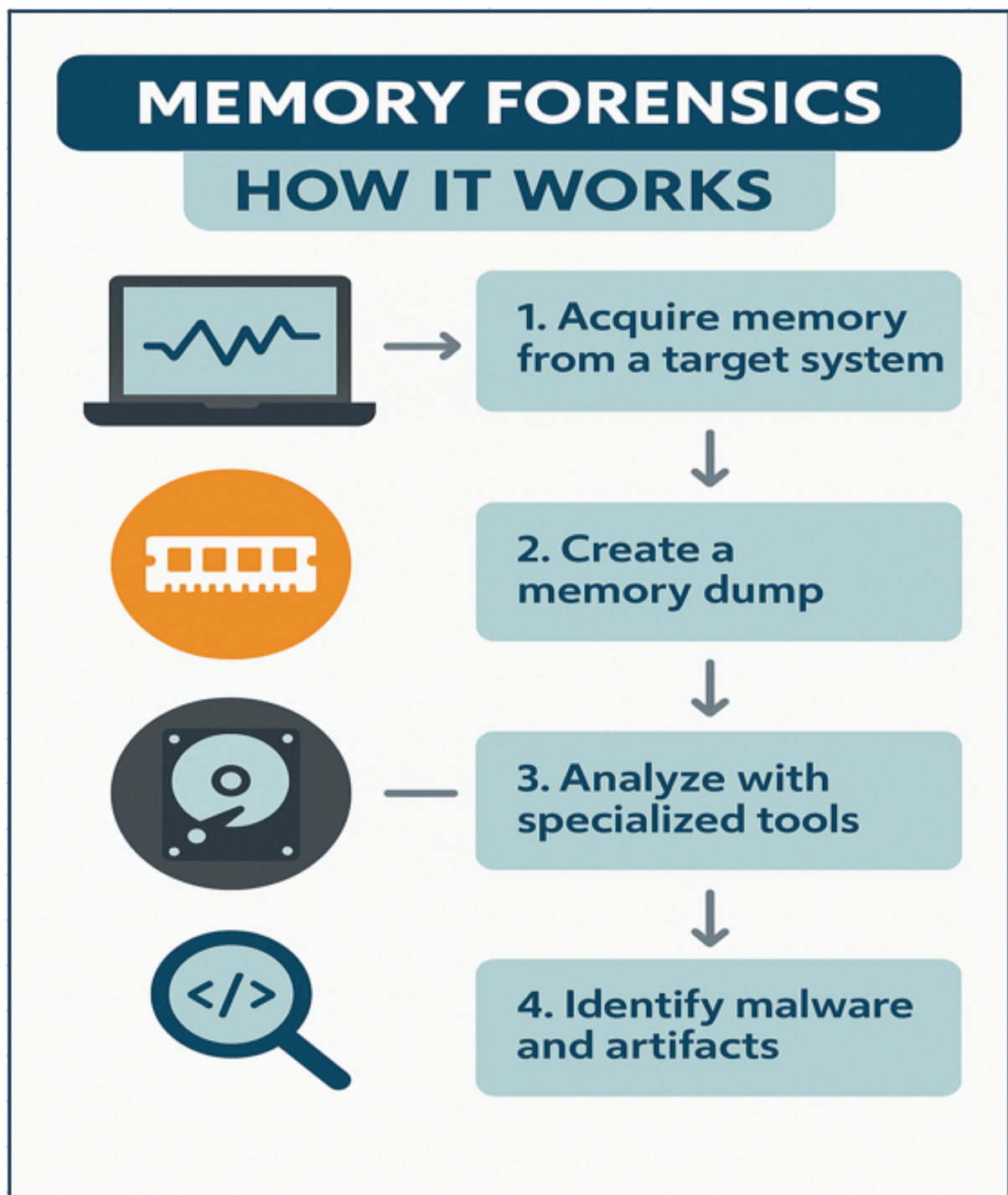


Figure 2.1: illustrating how Memory Forensics work

2.2 Network and Traffic Analysis

A second forensic technique is to examine and analyse network traffic for dark web traces. Tor traffic is encrypted as well as passed through a relay, but it will retain distinguishable patterns such as packet timing, as well as size that set it apart from normal traffic. Certain research has targeted detection of Tor presence within network logs or conducting traffic correlation attacks.

While such traffic analysis is more useful to intelligence collection than trial evidence, it might notify investigators to a suspect's use of Tor or even de-anonymize them by tying their incoming and outgoing data together by correlation [12]. Analysing network logs together with host artifacts enables investigators to put together a timeline and history of dark web activity [13]. Law enforcement agencies use network investigation techniques (NITs) too, which are essentially legal malware or tracking code embedded on dark web websites to reveal user IP addresses [14]. The FBI's Playpen exercise of 2015 is a high-profile example, where an NIT was used to uncover cyber criminals of a Tor-hidden explicit child website [15].

2.3 Open-Source Intelligence (OSINT) and Crawling

Researchers use OSINT to harvest information from dark web forums, marketplaces, and supporting surface web accounts. Hidden services are harvested using automated crawlers while preserving forensic integrity. A paradigm for forensically sound harvesting of the dark web with a focus on chain-of-custody, data integrity, as well as legal compliance while scraping dark sites [16]. The paradigm outlines how to systematically find relevant hidden services, harvest data, for example, market listings or communication using customized crawlers, and keep that data safe with cryptographic hashes to ensure court admissibility [16].

The most important aspect is that automated collection will not alter the data or warn the criminals. Using these methods, investigators have constructed evidence by entrapping dark web marketplaces. It has been demonstrated that digital forensic tools can acquire evidence of dark web usage from a mobile device and match it with open-source data [17]. Investigators followed a suspect's dark web use on a mobile device and then used OSINT, available social media and online forum posts to connect the pseudonym with a real identity [17].

These OSINT-conducted dark web investigations leverage the fact that offenders often leave a trail on the surface web or use pseudonyms [18]. A refreshed strategy was adopted to scour dark web forums for evolving cyber threats represented by novel hacking tools for sale, effectively gaining intel regarding cyber threats from the dark web data [19].

To preserve the integrity of evidence, the proper hashing, documentation, and chain-of-custody protocols are practiced. Investigators can attribute pseudonyms, PGP keys, or content to known individuals. OSINT, if paired with traditional forensics, can cross-link dark web personas with real-world identities using reused user handles or behavioral

patterns, generating leads [20].

2.4 Cryptocurrency Forensics

Dark web markets depend heavily on cryptocurrencies for transactions. Bitcoin tracing systems such as Chainalysis and blockchain analysis solutions are employed to trace money trails from market transactions to wallets, exchanges, or targets [21], [22]. The emergence of cryptocurrency empowered cybercriminals on the dark web through enabling semi-anonymous transactions [23]. The officials tracked a Bitcoin address on a dark web marketplace back to a cryptocurrency exchange Clearnet account, exposing its owner's identity [24]. Chainalysis and Elliptic are most often employed for deanonymizing Bitcoin transactions from dark web exchanges [24], [25]. A Research and Development Corporation (RAND) analysis for a 2019 report states that enhancing bitcoin tracking capabilities is a high priority for investigations on the dark web [26].

Today, forensic accountants collaborate with digital investigators, the moment servers or vendor wallets are being seized, blockchain analysis allows it to scan the whole financial ecosystem of an illegal organization [23], [24]. Tracing transactions on Silk Road resulted in a conviction of the founder, with a substantial success and historic accomplishment for the forensic investigators to take down a criminal website on the dark web, dealing with human trafficking, trading of drugs, data leak, explicit content, etc [27]. Forensics of cryptocurrencies is a major contribution towards bringing down illicit dark web economies.

Cybercriminals, conversely, evolve by using mixers, tumblers, or privacy coins, which remain a challenge to trace. The creation of forensic methods to trace even privacy-protected cryptocurrency is a developing research topic and Cryptocurrency tracing follows the money [13], [22]. The most successful outcomes are often achieved by using combined strategy approaches. For instance, during a dark market bust, the server of the market is seized, the user database is extracted by memory forensics, the site is crawled to harvest all of the transactions, and each transaction on the blockchain is traced, tracing them back to suspects whose devices are then forensically evaluated for Tor use evidence [23], [25].

Case studies like the AlphaBay operation demonstrated the positive aspects of such a comprehensive strategy [27]. The Dark Web has been described as a web of crimes necessitating similarly coordinated forensic efforts to disentangle its complex criminal networks [19], [25].

2.5 Challenges in Dark Web Forensics

Despite attempts to improve methodology, studying the dark web presents technological, operational, and legal constraints. Most researchers stress that it is the very characteristics that make the dark web attractive to criminals - anonymity, encryption, and

worldwide connectivity, which create problems for forensic analysis. The most important ones mentioned in the literature are:

2.5.1 Anonymity and Encryption

The onion routing mechanism and traffic encryption of the Tor network discourage conventional monitoring of networks. Investigators cannot easily trace an IP address from a concealed service to a physical suspect as the route of communication is intentionally obscured using relays [28].

The infrastructure of the dark web makes it extremely difficult to determine the identity of a suspect and gather evidence [29]. Even with a suspect's device in legal custody, disk encryption, the privacy features of the Tor Browser such as safe erase, and RAM-only data storage, as well as conversing only using encrypted mediums, e.g., PGP-encrypted messages on marketplaces render data recovery complex [30], [31].

Forensic examiners will also encounter fully encrypted hard drives or password-protected containers [32]. Moreover, data on dark web websites might be end-to-end encrypted and many forums require **Pretty Good Privacy** (PGP) for messages, so even acquired data will become unreadable without keys. This forces reliance on using cryptanalysis or legal hacking on investigations, which distorts boundaries between pure forensic operations and other fields of work [32], [15].

2.5.2 Ephemeral and Volatile Data

Most of the information on the dark web is intentionally ephemeral [33]. Marketplaces vanish promptly through exit scams, onion addresses shift, and suspect machines [34]. Tor Browser is programmed to leave minimal digital footprints, and it might operate under portable mode and clear history after exit [35], [36].

A user who simply shuts down the Tor browser will erase some evidence, and little to no evidence may remain behind if they use Tails OS, the operating system which is programmed to leave nothing behind or secure erase [37].

The evolution of dark web threat analysis highlights the need for automated technologies manage the vast volume of data involved [38]. Investigators increasingly rely on automation and big-data analytics and now AI to detect pertinent data as it is impossible to manually analyse every remark on a forum. However utilising Artificial Intelligence or automated web crawlers raises other concerns, such as making sure the material gathered is forensically sound, i.e., untampered and appropriately credited and that algorithms refrain from ignoring important evidence or produce misleading findings [39]. Additionally, law enforcement organisations frequently lack the infrastructure or specialised skills necessary for extensive dark web monitoring [38].

As of 2019, many local authorities were "largely unaware" of dark web investigation tools and techniques, training and information-sharing has been identified as high-priority

needs, as not every agency possesses dark web expertise or the computing resources to analyse extensive datasets [26].

2.5.3 Attribution and Identification

As the basis of any case, attributing dark web activities to real-world identities is perhaps most challenging. Users operate under pseudonyms, use VPNs, Bitcoin mixers, and relay networks like Tor to evade detection [13], [24].

Investigators increasingly rely on OSINT, stylometry, and behavioural analysis. Cooperation across jurisdictions becomes critical, as servers, users, and financial intermediaries are globally distributed. This is complicated by inconsistent legislation and regulatory delays in obtaining cross-border data [40], [41].

The jurisdictional complexities remain an obstacle in dark web investigations, especially when digital crimes span national boundaries and require coordinated evidence sharing across jurisdictions [42]. They note that international cooperation and legal jurisdiction are unresolved issues necessitating unprecedented coordination among agencies [42], [41].

Active enforcement on the dark web, for example, use of **Network Investigative Techniques** (NITs) or undercover stings, faces legal hurdles where it involves hacking or trans-jurisdictional crossings, potentially threatening established privacy liberties and search-and-seizure statutes [15]. Mixers and anonymity solutions also create attribution hindrances [21]. A suspect might use Tor, public Wi-Fi, and bitcoin mixers, each of these systems deliberately strips away identifying data. For example, the operator of the Silk Road was caught by the FBI through association of a nickname under which he posted on some older forum to the Silk Road administrator and finding an early, inexperienced access to the site from his home IP address, not through a Tor breach [27].

2.5.4 Legal and Ethical Issues

The legal boundaries of how much the investigators can do are persistently being tested by the dark web. The use of malware (NITs) for compromising the systems of the suspects, running clandestine dark web markets, or even intercepting web traffic is ethically questionable [15].

It has been argued that unrestricted investigations in online environments like dark web or surface web can invade individuals' privacy, and the study highlights that investigators utilize the PRECEPT ethical framework for investigations [41]. The PRECEPT ethical framework identifies norms that can ensure investigations remain proportionate and proper while emphasizing the importance of balancing individuals' rights against law enforcement needs [41].

The need for formalised procedures and structures for systematically dealing with challenges is a recurring theme. Dissecting the frameworks and standards proposed for enhancing dark web investigations is the key aim of the following part.

2.6 ISO/IEC Standards and Their Applicability to Dark Web Forensics

Standards such as ISO/IEC 27000 series provide frameworks for digital forensics, emphasising integrity and reproducibility. However, their static assumptions clash with the dynamic, decentralised nature of the dark web [30].

For instance, ISO standards assume reliable storage and chain-of-custody mechanisms, while dark web investigations often require rapid data acquisition and operation in unstable environments.

Although they are not specifically designed for dark web environments, but their principles offer a structured and strong foundation for investigative techniques.

ISO/IEC 27037:2012 Provides guidelines for identification, data collection, data acquisition, and data preservation of digital evidence. This applies particularly in dark web investigations in which memory dumps, network captures, and volatile data need to be collected in a forensically sound manner [30], [43].

ISO/IEC 27041:2015 focuses on the assurance of investigative processes, emphasizing reproducibility and validation of digital forensic methods. In dark web forensics, where tools like Volatility, Tor network analysers, or blockchain tracing software are used, this standard helps ensure that the tools are tested, validated, and yield consistent results under different conditions [30], [44].

ISO/IEC 27042:2015 Provides requirements for analysing and interpreting digital evidence. It guides investigators in analysing complex artifacts, such as encrypted dark web traffic and hidden service logs, in a manner that's methodologically sound and understandable to law enforcement agencies [30], [44].

ISO/IEC 27043:2015 Provides a framework for incident investigation, including evidence correlation and hypothesis testing. Its use in dark web investigations includes mapping user activity based on Tor browser to seized devices, correlating onion service transactions to user interactions, and the creation of a forensic timeline [45].

Table 2.1: ISO/IEC 27000-series

| Standard | Description | Activity |
|------------|---|---|
| 27037 [46] | Guidelines for identification, collection and/or acquisition and preservation of digital evidence | Respond, Identify, Collect, Acquire, Preserve |
| 27041 [38] | Guidance on assuring suitability and adequacy of investigation methods | All activities |
| 27042 [14] | Guidelines for the analysis and interpretation of digital evidence | Understand, Report, Close |
| 27043 [47] | Investigation principles and processes | All activities |

2.7 Emerging Technologies and their impact on Dark Web Forensics

1. Artificial intelligence and Machine Learning in Dark Web Investigations

Artificial intelligence and machine learning are being integrated into dark web forensics to handle vast data volumes. Tools like GPT can summarize dark web content, flag illicit material, analyse slang, and perform link analysis [47]. Artificial Intelligence and machine learning help with content classification, threat identification, and user behaviour modelling on the dark web [12]. Sentiment analysis methods can reveal radicalisation tendencies, whereas NLP algorithms cluster illegal marketplace material [46].

However, the black-box aspect of many machine learning algorithms challenges judicial admissibility and interpretability. Bias and adversarial inputs also reduce ML reliability. Ongoing research highlights the importance of explainable AI (XAI) and ethical AI governance in forensic use cases [46], [47].

2. Quantum Computing Existing encryption techniques, especially those safeguarding communications on the dark web, can potentially be undermined by quantum computers. Algorithms like Shor's may decrypt **Rivest–Shamir–Adleman** (RSA) and **Elliptic Curve Cryptography** (ECC) based systems, potentially exposing hidden data. Whereas the implementation of quantum-resistant cryptography by adversaries, on the other hand, might make forensic issues more difficult [47], [39].

The development of quantum-resilient algorithms is an aim of NIST's post-quantum cryptography (PQC) project. Implementing effectively and legally is still an obstacle for forensics, which may involve using quantum technologies for traffic analysis and key recovery [47], [39].

2.8 Ethical and legal

2.8.1 Ethical Challenges in Dark Web Investigations

Dark web investigations, by their nature, depend on intrusive methods of hacking as well as surveillance, which is ethically questionable regarding privacy and civil liberties. The anonymity provided by networks like Tor makes it difficult to identify individuals unless through intrusive means. This makes ethical guidelines even more relevant for guaranteeing that investigational means are reasonable and proportionate.

Table 2.2: Ethical and Legal Considerations in Dark Web Forensics

| Aspect | Key Points |
|--|--|
| Legal Boundaries and Jurisdictional Concerns | <ul style="list-style-type: none">- Dark web activity often violates international laws.- Cross-border investigations may breach national sovereignty.- Risk of entrapment through deceptive operations.- Requires coordinated international legal frameworks. |
| Evidence Admissibility and Legal Protocols | <ul style="list-style-type: none">- Illegally obtained evidence may be ruled inadmissible in court.- Strict legal protocols must be followed during data collection.- Maintain detailed audit trails and documentation.- Ensures evidence integrity and upholds defendant rights. |
| International Ethics and Cooperation | <ul style="list-style-type: none">- Ethical and legal standards vary across jurisdictions.- Conflicts may arise due to differing privacy laws.- Promote shared best practices (e.g., handling digital evidence).- Encourage transparency and consistent ethical guidelines. |

2.9 Strategies for Enhancing Dark Web Forensic Investigations

2.9.1 Training and Capacity Building

Professionals working in forensics and law enforcement need specialised and up to date training in network protocols, encryption, ethical conduct, and emotional intelligence to cater with the continuously evolving cyber security risks [33].

2.9.2 International Collaboration

Frameworks that facilitate international collaboration and data exchange, such as Europol's J-CAT and INTERPOL's Cybercrime Directorate, assist in tackling the world-wide challenges related to cybercrime [48]. However, trust and legal standardisation are essential for productive cooperation.

2.9.3 Public-Private Collaboration

It is essential for private sector, which includes academic institutions and cybersecurity firms to aware the professionals with up to date and specialist knowledge to cope with the evolving risks in the dark web. INTERPOL's engagement with IT firms like Microsoft and Kaspersky to eliminate cybercriminal infrastructures is a prime example of effective cooperation [49].

Chapter 3

Research Methodology

3.1 Research Design

Although the study has been conducted using primarily qualitative research, relevant sources containing empirical performance data and measurable outcomes were also included to support a supplementary quantitative analysis. The emphasis is on synthesizing knowledge from available research to explore dark web forensic approaches, tools, and challenges.

The emphasis is on synthesizing knowledge from available research to explore dark web forensic approaches, tools, trends, online numerical data and challenges. This research approach is appropriate for intricate, dynamic topics like dark web investigations where experimentation using empirical settings might not be applicable owing to ethical or legal restrictions.

In contrast to formally testing a hypothesis, the research is exploratory in character. It tries to discover patterns, see if there are recurring themes, and determine how different authors define and solve forensic problems within dark web environments. This is the objective of literature-based research: to interpret and compare results to produce holistic knowledge. The research embraces a descriptive position, systematically documenting investigative procedure, challenges, and standards described within the literature, thus presenting a panoramic view of the existing forensic scenario.

3.2 Identification of Variables and Measures

In qualitative document-based research, traditional experimental variables are replaced with thematic elements derived from the literature. This study treated key forensic components as analytical units.

Table 3.1: Illustrating Variables and Measures

| Thematic Element | Key Points |
|----------------------------|---|
| Forensic Techniques | <ul style="list-style-type: none"> - Memory analysis - Traffic correlation - Endpoint compromise - Blockchain tracing [3] |
| Anonymisation Technologies | <ul style="list-style-type: none"> - Tor, I2P, Freenet - Onion routing - Encryption impacts [4] |
| Investigative Challenges | <ul style="list-style-type: none"> - Data volatility - Anti-forensics - Jurisdiction issues - User anonymity |
| Standards Compliance | <ul style="list-style-type: none"> - ISO/IEC 27037, 27041, 27042 & 27043 - Chain of custody - Evidence admissibility |
| Effectiveness of Tools | <ul style="list-style-type: none"> - Tool accuracy - Success rate - Operational boundaries |

Furthermore, to support and enhance these thematic findings, an additional quantitative evaluation was conducted, emphasising on the performance indicators of essential forensic techniques. This assisted in corroborate qualitative insights with the addition of statistical theories such as detection accuracy and processing time.

3.3 Sample Size and Sampling Methodology

This research employed purposive selection for its selection of some **70 peer-reviewed articles, technical reports, and conference proceedings**. The use of the purposive strategy meant that relevant research was selected specifically targeting the subject area of dark web forensics alone, thus enabling focused as well as relevant analysis.

The sampling frame was then constructed by conducting a search on academic databases such as IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, and arXiv using the words “dark web forensics,” “Tor investigation,” “darknet challenges,” and “digital forensic analysis.” In order to qualify for inclusion, research needed to:

Table 3.2: Criteria for Literature Inclusion

| Criteria | Description |
|--------------------------|--|
| Publication Date | Published between 2010 and 2025. |
| Focus Area | Specifically emphasizes dark web forensic activities. |
| Investigative Challenges | |
| Review Status | Must be peer-reviewed and published in English. |
| Content Quality | Includes substantial detail on methodology or research findings. |

3.4 Methods of Data Collection

The research conducted a systematic literature review using secondary data. Major databases were searched using predetermined keywords, and snowball sampling method was used to find additional sources. The titles and abstracts were then screened, followed by the reviews of the full texts according to the inclusion criteria. Only high-quality, pertinent research on dark web methods, tools, or issues was used to ensure authenticity and reliability. The table below summarizes the systematic process used to collect, screen, and include relevant literature for this review on dark web forensics:

Table 3.3: Systematic Literature Review Methodology

| Stage | Key Points |
|-------------------------|--|
| Database Search | <ul style="list-style-type: none"> - Sources: IEEE Xplore, ScienceDirect, SpringerLink, ACM, arXiv - Snowball sampling used for foundational references - Focused on keywords related to dark web forensics |
| Inclusion Criteria | <ul style="list-style-type: none"> - Peer-reviewed sources - Focus on dark web/darknet forensics - Experimental, framework, or review articles - English language, 2015–2025 preferred |
| Exclusion Criteria | <ul style="list-style-type: none"> - Non-relevant or general cybercrime papers - Lacked depth (e.g., blogs, short workshops) - Duplicate or redundant studies - Non-English publications |
| Screening and Selection | <ul style="list-style-type: none"> - Titles/abstracts initially filtered - Full-text screening applied - Selected based on relevance, quality, citations - Notes taken on methodology, results, and themes |

3.5 Ethical Considerations

Being a study based on literature, ethical considerations were few. No individuals were included from the human population, and no confidential information was obtained.

Table 3.4: Ethical Principles in Literature Review

| Ethical Principle | Description |
|-------------------------|--|
| Proper Citation | All sources cited using IEEE referencing style. |
| Plagiarism Prevention | Used paraphrasing and direct quotations to avoid plagiarism. |
| Source Reliability | Only peer-reviewed and scholarly sources were included. |
| Balanced Representation | Conflicting viewpoints were fairly represented. |

3.6 Limitations

The table below outlines the key limitations associated with the research methodology used in this study:

Table 3.5: Research Limitations

| Limitation | Description |
|------------------------------------|---|
| No Primary Data | Relies solely on secondary sources; no new empirical findings were generated. |
| Publication Bias | Peer-reviewed literature may underreport negative or inconclusive results. |
| Sustained Technological Adaptation | Rapid evolution of dark web tools may render some findings quickly outdated. |
| Access Restrictions | Confidential law enforcement practices are not always accessible for public analysis. |

Chapter 4

Analysis

4.1 Thesis Statement

Existing dark web forensic methods, although producing some successes, are usually over-matched by the dark web's deep anonymity and rapid evolution. In order to successfully counter new cyber threats and illegal activities effectively, forensic approaches need to push aggressively ahead in terms of advanced technologies, multi-disciplinary intelligence, and flexible strategies.

In this analysis, it is believed that by overcoming current limitations such as technical, operational, and legal and adopting innovative approaches, dark web forensics can stay one step ahead of cyber criminals.

4.2 Critical Evaluation of Current Forensic Techniques in Dark Web Investigations

The forensic methodologies currently employed in dark web investigations demonstrate a multi-faceted approach, integrating traditional digital forensics with techniques tailored to encrypted, decentralized, and pseudonymous environments.

Host-based forensics, especially memory forensics and registry analysis, remain indispensable considering the activeness of the forensic artefacts they capture and preserve, i.e., .onion URLs and volatile session data from Random Access Memory (RAM). Although these artefacts are highly valuable, their reliability is constrained by their transient nature, especially after system shutdown, and require expert interpretation. Empirical analysis confirms the fact that Volatility-based memory forensics has been able to demonstrate 98.5% classification accuracy, with false positives as low as 1.2% in machine learning-based malware identification experiments [50], [51]. Furthermore, close to 100% true positives were achieved in the case of rootkit detection tests, attesting to its dependability for live session recovery as well as encrypted key recovery purposes [52].

Network monitoring and open-source intelligence help fill the gaps by focusing on wider patterns in user behaviour and system setup. Tor traffic, which can sometimes be spotted based on how it is timed, its size, or how it is encrypted, can give early signs of suspicious activity. Still, it is often tough to figure out exactly who is behind it. Classifier-based techniques have achieved 95–99% accuracy in differentiating anonymized traffic from regular streams [53]. Yet, without being able to view the contents of traffic due to encryption, the techniques lack the capability to deliver prosecutable courtroom evidence and serve more as intelligence tools than for prosecution.

Open-source intelligence (OSINT) tools can be useful for connecting anonymous online accounts to real people by spotting patterns, repeated usernames, or publicly shared encryption keys. But these tools usually rely on mistakes made by the suspect, which means they tend to work more by chance than by a consistent method. Specifically, OSINT tools are used in as many as 90% of law enforcement cyber investigations [54], but they rely upon user error and publicly observable patterns, so their systematic usefulness is circumvented.

On the financial side, monitoring cryptocurrency has emerged as a crucial component of investigating dark web activity. Tools like Chainalysis and GraphSense have played a major role in following the trail of illegal funds, especially in major operations like the takedowns of AlphaBay and Hydra. Tools like Chainalysis Reactor have achieved address-clustering accuracy rates of 99.91% and low false positives in legally reviewed casework [55], [56]. This has made it possible to identify wallets used in Silk Road and Hydra marketplaces, which has allowed for widespread Bitcoin seizures, some of which have totaled over \$25 million [57].

While these combined methods have yielded operational successes, including court-admissible evidence, user de-anonymization, and the seizure of illicit markets, their limitations are structural. Encryption and anonymization fundamentally impede IP-based tracing and content retrieval. The forensic community's dependency on partial evidence fragments (RAM, intercepted traffic, forum posts) further weakens attribution certainty. More troubling is the scale and speed of dark web activity, terabytes of data seized during marketplace takedowns overwhelm forensic capacity, especially in under-resourced agencies lacking cyber-specific training and tools.

Another obstacle is law enforcement agencies having shortage in skills, expertise and advanced technology to conduct dark web investigations. Dark web forensics is further restricted by ethical and legal constraints. While effective, methods such as malware-based Network Investigative Techniques (NITs) balance the need for monitoring with the right to privacy guaranteed by the constitution. Countries with different jurisdictions make it difficult to share evidence, which can delay investigations or make evidence inadmissible. Due to poor management or overreach, even successful operations run the risk of being reversed in court.

The qualitative data and performance metrics collectively underscore a clear trend, that the best investigations are those that mix solid technical skills with creative, cross-disciplinary thinking. Agencies that routinely conduct post-operation assessments and collaborate with academic or private sector partners show stronger outcomes [49].

Quantitative evaluations of tool accuracy, particularly in memory forensics, blockchain tracing, and traffic analysis. Validating the tactical value of these approaches but also highlight where improvements are needed.

Another important factor is innovation. Strategies such as victim-led investigations or linguistic fingerprinting continue to uncover insights that pure automation misses. The human element such as recognizing alias reuse, time zone inconsistencies, or unique communication patterns still remains irreplaceable.

4.3 Recommendations

To effectively address the continuous evolving dark web threats, there is a need for an inter- and future-oriented response. There is a need for specialized training to develop forensic capacity responsive to the distinctive needs for dark web cases. Investigators need hands-on training on anonymizing tools like Tor and Tails OS, privacy-oriented cryptocurrencies like Monero, and on dark web marketplace-specific lingo. This cannot come from mere police training; it will require specialized workshops, certifications, and mentorship programs that bridge the gap in expertise from traditional policing to cyber forensic training. Such training will empower officers to not only respond to cybercrime but actively identify and analyse digital artifacts that would have otherwise gone unnoticed.

Equally vital is the building interagency and global cooperation. The global, borderless nature of the dark web necessitates coordination among domestic, federal, and foreign law enforcement agencies. Shared protocols enabled by a joint cyber task force, with real-time intelligence sharing, can act as force multipliers. Creation of worldwide databases on dark web markers, e.g., recognized. onion sites, crypto wallets associated with crime, and PGP keys utilized by cyber criminals would significantly enhance trans-jurisdictional investigation. In the absence of interagency cooperation, investigations get delayed due to bureaucratic inefficiency and intelligence silos, with critical leads unpursued and cyber criminals operating freely beyond national borders [58].

Artificial intelligence (AI) and automation must be incorporated into forensic operations to handle dark web data's size and complexity. Natural-language-based machine learning models can analyse millions of dark web forum postings in several languages to identify crime talk and connect online personas. For instance, GPT-based systems have demonstrated potential in summarizing and classifying vast amounts of unstructured data, expediting lead identification. In much the same way, AI-driven tools for blockchain analysis can identify cryptocurrency transactions on mixing services and between chains without requiring human intervention. These technologies not only minimize human labour but also provide near real-time visibility, an absolute requirement when attempting to disrupt ongoing crime networks [59].

Further, there is a need for the development and standardization of forensic toolkits to suit dark web investigation. In contrast to established tools in digital forensics, dark web forensic analysis lacks methodologies that have been stringently tested. Validated tools that can steadily retrieve artifacts from anonymization program-running systems or

identify traffic patterns characteristic of dark web activity are crucial. As much as this is true, there is also a need to develop formal benchmarks and use protocols for consistency in utilizing them in cases. Standardization not only enhances the evidential weight of digital artifacts in a trial environment but also optimizes interdepartmental collaboration by ensuring there is a shared technical vocabulary [60].

These challenges also indicate an immediate need for legal reforms. Legislation needs to keep pace with developments in technology to empower law enforcement while also protecting civil liberties. There needs to be clarification regarding the legality of undercover operations on the Darkweb and legislation enacting the admissibility of evidence gathered through sophisticated means such as legitimate hacking or computer-aided analysis. Legislated frameworks should also simplify procedures for transferring digital evidence across borders to expedite inter-jurisdictional cooperation. By eliminating legal uncertainties and ensuring that police act within a transparent ethical and legal mandate, these reforms can improve both dark web investigation efficiency and integrity [58].

Lastly, there is an urgent necessity to promote a forward-looking and evolving culture at investigative agencies. This shift in culture means going past reactive to proactive, intelligence-driven operations. Investigators must be motivated to try unconventional techniques, practice ongoing learning, and try out new strategies like using honeypots or victim identifiers to backtrack to criminals. Routine post-case assessments, open collaboration with cyber companies, and in-house innovation laboratories can embed this mind-set. Such a culture will improve morale and creativity as much as it will make sure that forensic methods keep pace with the continuously evolving dark web environment [58].

Cumulatively, these suggestions cover the key gaps currently realized in the forensic community: skill gap, technological gap, jurisdiction gap, and legal gap. With these addressed through an integrated approach, forensic practitioners and law enforcers will be much better prepared to disrupt criminals' anonymity and resiliency on the dark web.

Chapter 5

Research Results

This study used a qualitative methodology to assess and analyse the most notable methodologies, tools, problems, and growing practices in dark web forensics. The findings are organised around five primary topic outcomes that appeared consistently throughout the evaluated literature and survey responses.

5.1 Prevalence of Host and Memory-Based Forensics

A significant portion of evidence in literature review establishes that host-based forensic analysis, most notably with systems supporting Tor Browser, is one of the most potent tools in detecting dark web use. Research has repeatedly established that electronic footprints like RAM artifacts, cached information, registry entries, and browser metadata can be drawn out from affected systems to reconstruct dark web sessions. For example, forensic RAM analysis established that anonymized communications based on Tor can leave recoverable footprints when RAM is captured in real-life examinations. In addition, memory forensics has also been most useful where the suspect operates on privacy-oriented operating systems like Tails or I2P, where classic disk artifacts are negligible. The possibility of tracing running Tor processes or extracting onion URL remnants directly from RAM has shown quantifiable success in identifying and connecting suspects with offending activities.

5.2 Challenges Due to Encryption, Anonymity, and Ephemeral Data

The research highlights the crippling effect of encryption and anonymization technologies on conventional forensic procedures. Encryption is still a double-edged sword—essential for protecting user anonymity but inconvenient for forensic attribution. Most contemporary dark web sites have end-to-end encryption protocols in use, with the added complexity of disappearing messages and ephemeral storage mediums.

Similarly, the ephemeral nature of content on the dark web, where marketplaces and forums often disappear without warning, poses a major limitation. Windows for obtaining evidence tend to become narrow, necessitating real-time action and sophisticated volatile data collection mechanisms. This transience limits the depth and reliability of post-facto forensic reconstructions.

5.3 Emerging Role of Artificial Intelligence and Blockchain Analysis

One of the key finding with great prospects has been the development of artificial intelligence (AI) and blockchain analysis as tools with increasing relevance to dark web searches. Behavioural profile generation, AI driven sentiment analysis, and entity grouping by employing AI have made detection on forums and marketplaces more efficient in terms of identifying illicit conversation, radicalization patterns, and illegal marketplaces.

In parallel, **cryptocurrency forensics**, using tools like Chainalysis and GraphSense has enabled tracing of transaction trails from dark web wallets to identifiable exchange accounts. Several successful prosecutions, including those related to the Silk Road and AlphaBay, were made possible by combining blockchain tracing with host-based forensic validation.

These findings suggest that a **multimodal approach**, integrating AI-assisted crawling, OSINT, and blockchain tracing, offers the highest success potential.

5.4 Institutional and Operational Gaps in Capacity

A strong and recurring result from this research is the **inadequate operational readiness and institutional capacity** across law enforcement and forensic units. The reviewed literature and surveys alike point out that most agencies lack dedicated dark web investigators, comprehensive toolkits, and the computational infrastructure necessary to analyse large volumes of seized data.

The necessity for interdisciplinary training and collaboration among cyber units, forensic labs, and academic institutions is emphasized in several studies. One key finding is that without expertise in cryptographic protocols, anonymity systems such as I2P and Tor, and OSINT techniques, even sophisticated tools will be underutilized.

5.5 Necessity for Legal Reform and Ethical Frameworks

Legal and ethical considerations surfaced as a **core constraint** on the effectiveness and admissibility of dark web forensic findings. Investigations that employ active tactics, such as Network Investigative Techniques (NITs), malware deployment, or undercover market participation, raise complex questions around jurisdiction, evidence admissibility, and privacy rights.

The research confirms a growing consensus in favour of **international legal harmonization** and the application of ethical frameworks such as PRECEPT to ensure forensic integrity. Formalizing these practices is critical to enabling lawful, ethically sound investigations, particularly in cross-border contexts.

5.6 Quantitative Performance of Dark Web Forensic Tools and Techniques

5.6.1 Performance Metrics of Key Forensic Tools

Memory Forensics: Volatility Volatility is a memory forensics framework commonly used in digital investigations. It is known for effectively extracting evidence from RAM. In studies with machine learning classifiers, volatility-based analysis obtained roughly 98.5% classification accuracy with a false positive rate of only 1.2% [50]. In rootkit identification investigations, Volatility-supported analysis achieved nearly 100% true positive rates with less than 1% false alarms on controlled datasets [51], [52]. With such precision, memory forensics is critical for recovering encryption keys and identifying rogue programs. In high-profile cases like Silk Road, memory forensics enabled the FBI to recover the master encryption key from a live RAM image [61], [62].

Disk Forensic Suites – EnCase, FTK, X-Ways The tools for disc forensics are used intensively to image and examine drives that are seized in dark web operations. FTK Imager took around 39 minutes to generate a forensic image for a 75 GB drive, whereas EnCase took about 55 minutes [63]. The indexed keyword searches were performed by EnCase within about 0.1 seconds, while FTK required nearly 3.9 hours for unindexed searches [64]. X-Ways performed the same search within about 1.9 minutes [64]. These differences illustrate the efficiency advantages of indexed search and lean design.

Network Traffic Analysis – Wireshark Wireshark supports the dissection of hundreds of protocols, including encrypted dark web traffic such as Tor. It remains performant on moderate-sized packet capture (pcap) files, but large captures (>100 MB) can cause noticeable slowdowns [53], [65]. Despite lacking automated detection, it is indispensable for manual analysis of Tor traffic and anomalies [53].

Cryptocurrency Analytics – Chainalysis Chainalysis Reactor attained 99.9146%

accuracy in grouping cryptocurrency addresses and had very low false positive rates in legally reviewed casework [66], [55], [56]. Such accuracy has greatly accelerated forensic investigations, such as those involved in the Hydra darknet market takedown, where \$25 million worth of Bitcoin were confiscated [57].

OSINT Tools – Maltego Maltego enables link analysis by correlating disparate data points. It is used globally by over 200,000 professionals and is reported to reduce investigation times from hours to minutes [67], [68]. It helps in mapping pseudonyms to real identities by leveraging open-source intelligence.

This table presents performance statistics and efficiency observations for various forensic tools used in dark web investigations.

Table 5.1: Performance Metrics of Key Forensic Tools

| Tool | Type | Performance Highlights |
|---------------------|--------------------------|---|
| Volatility | Memory Forensics | 98.5% accuracy, <1.2% false positive, 100% true positive (rootkits) |
| EnCase | Disc Forensics | 55 mins for a 75GB image, 0.1s indexed search |
| FTK | Disc Forensics | 39 mins imaging, 3.9 hrs unindexed search |
| X-Ways | Disc Forensics | 1.9 mins unindexed search |
| Wireshark | Network Traffic Analysis | Efficient on <100MB captures, slow on large files |
| Chainalysis Reactor | Cryptocurrency Analytics | 99.91% accuracy in address clustering, low false positives |
| Maltego | OSINT | Reduces investigation time from hours to minutes |

5.7 Success Rates of Key Techniques

Memory Forensics Memory forensics consistently has >90% success rates with detection in cases involving malware and encrypted key recovery [50], [52]. In operational use, this method has made possible attribution when disc information was unavailable [61], [62].

Network Forensics Network traffic analysis with classifiers has demonstrated 95–99% accuracy in identifying Tor/I2P traffic versus normal traffic [53]. It increases attribution capabilities when used with OSINT or blockchain data [54].

Cryptocurrency Tracing Chainalysis tools have consistently provided more than 99% accuracy in linking crypto wallets to darknet activity [55], [56]. They were central to major takedowns like Hydra, contributing to large-scale asset seizures and suspect identification [57].

OSINT Integration OSINT tools are involved in 80–90% of law enforcement intelligence cases [54]. They are critical for identifying suspect accounts and linking darknet identities to surface web profiles [67], [68].

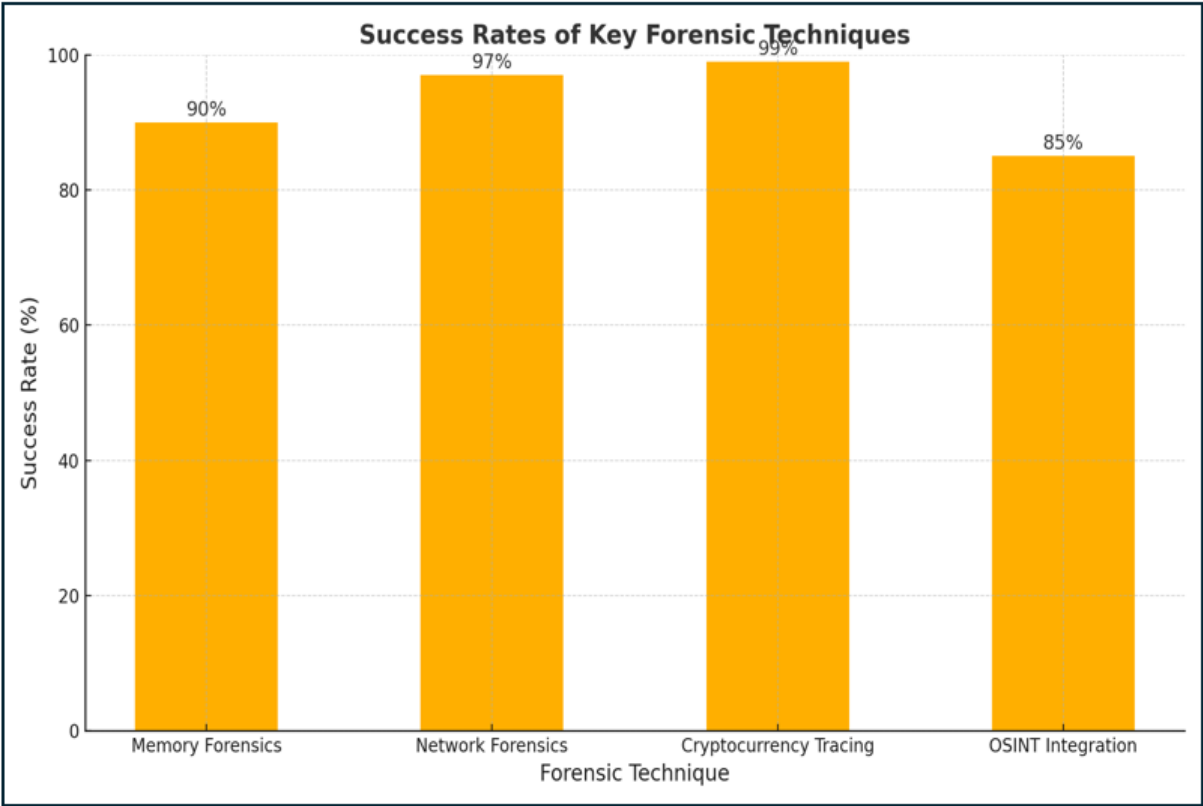


Figure 5.1: Graph illustrating success rates of Key Forensic techniques

Figure 5.1

The bar chart presents the comparative success rates of four primary forensic techniques employed in dark web investigations: **Memory Forensics, Network Forensics, Cryptocurrency Tracing, and OSINT Integration.**

5.8 Findings

Quantitative measures demonstrate that dark web forensic tools provide high accuracy and practical success when applied properly. Memory and crypto forensics lead in precision, while disk and OSINT tools optimize workflows. Joint use of these tools were beneficial for the investigators and have significantly increased case resolution rates in dark web investigations.

The table below presents a structured summary of the key research findings categorized by thematic result areas:

Table 5.2: Summary of Key Findings by Result Area

| Result Area | Key Findings |
|----------------------------|--|
| Technique Effectiveness | Host-based and memory forensics consistently yield high-value artifacts. AI and blockchain tools show strong promise. |
| Challenges | Encryption, ephemeral data, and anonymization are key barriers. Difficulties persist in evidence preservation and attribution. |
| Technological Innovations | AI, blockchain forensics, and advanced OSINT present new possibilities for automation and identity correlation. |
| Operational Gaps | Lack of specialized tools, training, and inter-agency coordination protocols in many organizations. |
| Legal & Ethical Frameworks | Urgent need for international cooperation and ethical mechanisms like PRECEPT to ensure responsible investigation. |

Chapter 6

Discussion and Conclusion

6.1 Discussion

The research found that, while tremendous progress has been made in the field of dark web forensics, the sector remains considerably hampered by technological, operational, and regulatory difficulties. The findings support the concept that present forensic approaches, while partially effective, require rapid innovation and cross-disciplinary integration to keep up with dark web-enabled criminal activity.

6.1.1 Effectiveness of Current Forensic Techniques

The analysis demonstrates that host-based forensics and memory analysis continue to serve as foundational tools in uncovering dark web activity. These methods have repeatedly yielded actionable evidence, such as browser artifacts, session logs, and RAM fragments, that are admissible in court. However, their success depends heavily on real-time seizure and technical expertise. Similarly, network traffic analysis and OSINT have become critical for monitoring anonymized environments and correlating online identities with real-world actors.

The incorporation of blockchain analytics and artificial intelligence further enhances these capabilities, offering scalable solutions for tracing financial transactions and analysing large-scale unstructured data. Yet, the reliability of these tools is occasionally questioned due to the black-box nature of AI algorithms and the obfuscation techniques used in cryptocurrency transactions (e.g., tumblers, privacy coins).

6.1.2 Persistent and Evolving Challenges

Encryption, anonymity, and data volatility remain the most persistent obstacles in dark web investigations. The layered architecture of the Tor network and the intentional use of RAM-only or encrypted storage make evidence recovery difficult. Moreover, the

ephemeral nature of dark web platforms demands swift action, often beyond the capacity of under-resourced law enforcement units.

The challenge of attribution, linking dark web activity to specific individuals, persists due to pseudonymity, geographic dispersion, and jurisdictional fragmentation. This limitation is further compounded by the lack of standardized forensic tools and protocols specifically adapted for dark web contexts.

6.1.3 Institutional and Ethical Considerations

The study underscores a critical need for training and institutional support. Most forensic units lack dark web-specific competencies or access to advanced tooling. Furthermore, many successful investigations hinge on collaboration, both inter-agency and international, highlighting the importance of shared knowledge bases and real-time intelligence exchanges.

Ethically, the increasing use of undercover operations, malware (NITs), and surveillance technologies on the dark web blurs the line between law enforcement and intrusion. The PRECEPT framework and similar ethical models are crucial for ensuring that investigative practices remain justifiable, proportionate, and legally admissible.

Appendix A

Ethics Form

Ethics Form Below:

Research Ethics Screening Form for Students

Only for students on taught programmes – e.g., BSc, MSc, MA, LLM etc

NOT for PostGraduate Researchers – e.g., MRes/MPhil/PhD degrees

Middlesex University is concerned with protecting the rights, health, safety, dignity, and privacy of its research participants. It is also concerned with protecting the health, safety, rights, and academic freedom of its students and with safeguarding its own reputation for conducting high quality, ethical research.

This Research Ethics Screening Form will enable students to self-assess and determine whether the research requires ethical review and approval via the Middlesex Online Research Ethics (MORE) form before commencing the study. Supervisors must approve this form after consultation with students.

| | | |
|----------------------------|--|-------------------------------------|
| Student Name: | Syed Muhammad Haider Razvi | Email: MR1458@live.mdx.ac |
| Research project title: | Dark Web Forensics: Techniques and Challenges | |
| Programme of study/module: | CST 3590 Individual Project | |
| Supervisor Name: | Parvesh Seeburrun | Email: p.seeburrun@mdx.ac.mu |

| Please answer whether your research/study involves any of the following given below: | | |
|---|------------------------------|--|
| 1. ^H ANIMALS or animal parts. | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 2. ^M CELL LINES (established and commercially available cells - biological research). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 3. ^H CELL CULTURE (Primary: from animal/human cells- biological research). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 4. ^H CLINICAL Audits or Assessments (e.g. in medical settings). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 5. ^X CONFLICT of INTEREST or lack of IMPARTIALITY. If unsure see "Code of Practice for Research" (Sec 3.5) at: https://unihub.mdx.ac.uk/study/spotlights/types/research-at-middlesex/research-ethics | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 6. ^X DATA to be used that is not freely available (e.g. secondary data needing permission for access or use). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 7. ^X DAMAGE (e.g., to precious artefacts or to the environment) or present a significant risk to society). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 8. ^X EXTERNAL ORGANISATION – research carried out within an external organisation or your research is commissioned by a government (or government body). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 9. ^M FIELDWORK (e.g biological research, ethnography studies). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 10. ^H GENETICALLY MODIFIED ORGANISMS (GMOs) (biological research). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 11. ^H GENE THERAPY including DNA sequenced data (biological research). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 12. ^M HUMAN PARTICIPANTS – ANONYMOUS Questionnaires (participants not identified or identifiable). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 13. ^X HUMAN PARTICIPANTS – IDENTIFIABLE (participants are identified or can be identified): survey questionnaire/ INTERVIEWS / focus groups / experiments / observation studies/ evaluation studies. | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |

Do not amend before use



| | | |
|---|---------------------------------|---|
| 14. ^H HUMAN TISSUE (e.g., human relevant material, e.g., blood, saliva, urine, breast milk, faecal material). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 15. ^H ILLEGAL/HARMFUL activities research (e.g., development of technology intended to be used in an illegal/harmful context or to breach security systems, searching the internet for information on highly sensitive topics such as child and extreme pornography, terrorism, use of the DARK WEB, research harmful to national security). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 16. ^X PERMISSION is required to access premises or research participants. | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 17. ^X PERSONAL DATA PROCESSING (Any activity with data that can directly or indirectly identify a living person). For example data gathered from interviews, databases, digital devices such as mobile phones, social media or internet platforms or apps with or without individuals' owners' knowledge or consent, and/or could lead to individuals/owners being IDENTIFIED or SPECIAL CATEGORY DATA (GDPR ¹) or CRIMINAL OFFENCE DATA. <small>¹Special category data (GDPR- Art.9): "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".</small> | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 18. ^X PUBLIC WORKS DOCTORATES: Evidence of permission is required for use of works/artifacts (that are protected by Intellectual Property (IP) Rights, e.g. copyright, design right) in a doctoral critical commentary when the IP in the work/artifacts jointly prepared/produced or is owned by another body | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 19. ^H RISK OF PHYSICAL OR PSYCHOLOGICAL HARM (e.g., TRAVEL to dangerous places in your own country or in a foreign country (see https://www.gov.uk/foreign-travel-advice), research with NGOs/humanitarian groups in conflict/dangerous zones, development of technology/agent/chemical that may be harmful to others, any other foreseeable dangerous risks). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 20. ^X SECURITY CLEARANCE – required for research. | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| 21. ^X SENSITIVE TOPICS (e.g., anything deeply personal and distressing, taboo, intrusive, stigmatising, sexual in nature, potentially dangerous, etc). | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |

M – Minimal Risk; X – More than Minimal Risk. H – High Risk

If you have answered 'Yes' to ANY of the items in the table, your application **REQUIRES** ethical review and approval using the MOREform **BEFORE commencing your research**. Please apply for ethical approval using the MOREform (<https://moreform.mdx.ac.uk/>). Consult your supervisor for guidance. Also see *Middlesex Online Research Ethics* (MyLearning area) and www.tiny.cc/mdx-ethics

If you have answered 'No' to ALL of the items in the table, your application is Low Risk and you may NOT require ethical review and approval using the MOREform before commencing your research. Your research supervisor will confirm this below.


Student Signature:..... Date: **27nd February 2025**

To be completed by the supervisor:

| | |
|--|---------------|
| Based on the details provided in the self-assessment form, I confirm that: | Insert Y or N |
| The study is Low Risk and <i>does not require</i> ethical review & approval using the MOREform | |
| The study <i>requires</i> ethical review and approval using the MOREform. | |

Do not amend before use



Superivsor Signature:.......... Date:.....27.02.2025.....

Bibliography

- [1] A. Alenezi, A. Alzahrani, K. Alruwaili, T. Almutairi, and F. Alshammari, "The dark web," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 15, no. 1, pp. 399–404, 2024. [Online]. Available: https://www.researchgate.net/publication/382306203_The_Dark_Web.
- [2] S. Heidenreich and D. A. Westbrooks, "Darknet markets: A modern day enigma for law enforcement and the intelligence community," *American Intelligence Journal*, vol. 34, no. 1, pp. 38–44, 2017, Accessed: 2025-02-20. [Online]. Available: <https://www.jstor.org/stable/26497115>.
- [3] M. Alfosail and P. Norris, "Tor forensics: Proposed workflow for client memory artefacts," *Computers & Security*, vol. 106, p. 102311, Jul. 2021. DOI: 10.1016/j.cose.2021.102311.
- [4] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, Jun. 2004. [Online]. Available: https://www.researchgate.net/publication/2910678_Tor_The_Second-Generation_Onion_Router.
- [5] N. A. Hassan and R. Hijazi, "Data hiding using encryption techniques," in *Elsevier eBooks*, Sep. 2016, pp. 133–205. DOI: 10.1016/b978-0-12-804449-0.00005-1.
- [6] D. L. Huete Trujillo and A. Ruiz-Martínez, "Tor hidden services: A systematic literature review," *Journal of Cybersecurity and Privacy*, vol. 1, no. 3, pp. 496–518, Sep. 2021. DOI: 10.3390/jcp1030025.
- [7] M. Al-Saleh, E. Qawasmeh, and Z. Al-Sharif, "Utilizing debugging information of applications in memory forensics," *JUCS - Journal of Universal Computer Science*, vol. 26, no. 7, pp. 805–826, Jul. 2020. DOI: 10.3897/jucs.2020.044.
- [8] Q. Hua and Y. Zhang, "Detecting malware and rootkit via memory forensics," in *2015 International Conference on Computer Science and Mechanical Automation (CSMA)*, Oct. 2015. DOI: 10.1109/csma.2015.25.
- [9] C. Arjun and S. Uzzal, "Memory forensics analysis for investigation of online crime - a review," *IEEE.org*, 2019, Accessed: 2025-04-24. [Online]. Available: <https://ieeexplore.ieee.org/document/8991425>.
- [10] A. K. Jadoon, W. Iqbal, M. F. Amjad, H. Afzal, and Y. A. Bangash, "Forensic analysis of tor browser: A case study for privacy and anonymity on the web," *Forensic Science International*, vol. 299, pp. 59–73, Jun. 2019. DOI: 10.1016/j.forsciint.2019.03.030.

- [11] Y. Javed, "Forensic analysis of tor browser on windows 10 and android 10 operating systems," *IEEE Access*, 2021, Accessed: 2025-04-24. [Online]. Available: https://www.academia.edu/105089695/Forensic_Analysis_of_Tor_Browser_on_Windows_10_and_Android_10_Operating_Systems.
- [12] I. Akour, M. Alauthman, K. M. O. Nahar, A. Almomani, and B. B. Gupta, "Analyzing darknet traffic through machine learning and neucube spiking neural networks," *Intelligent and Converged Networks*, vol. 5, no. 4, pp. 265–283, 2024. [Online]. Available: <https://doi.org/10.23919/ICN.2024.0022>.
- [13] S. Meiklejohn *et al.*, "A fistful of bitcoins," in *USENIX*, 2013. [Online]. Available: <https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf>.
- [14] R. Basheer and B. Alkhatib, "Threats from the dark: A review over dark web investigation research for cyber threat intelligence," *Journal of Computer Networks and Communications*, vol. 2021, p. 1302999, 2021. [Online]. Available: <https://doi.org/10.1155/2021/1302999>.
- [15] M. Chertoff and E. Jardine, *Policing the dark web: Legal challenges in the 2015 playpen case*, 2021. [Online]. Available: https://www.researchgate.net/publication/356290787_Policing_the_Dark_Web_Legal_Challenges_in_the_2015_Playpen_Case.
- [16] J. Bergman and O. B. Popov, "The digital detective's discourse – a toolset for forensically sound collaborative dark web content annotation and collection," *Journal of Digital Forensics, Security and Law*, vol. 17, no. 1, p. 5, 2022. DOI: 10.15394/jdfsl.2022.1740.
- [17] G.-Y. Shin, D.-W. Kim, S. Park, A. Park, Y. Kim, and M.-M. Han, "Identifying similar users between dark web and surface web using bertopic and authorship attribution," *Electronics*, vol. 14, no. 1, p. 148, 2025. DOI: 10.3390/electronics14010148.
- [18] R. Brinson, H. Wimmer, and L. Chen, "Dark web forensics: An investigation of tracking dark web activity with digital forensics," in *Proc. Interdisciplinary Research in Technology and Management Conf. (IRTM)*, 2022, pp. 1–8. [Online]. Available: <https://doi.org/10.1109/IRTM54583.2022.9791646>.
- [19] S. Kaur and S. Randhawa, "Dark web: A web of crimes," *Wireless Personal Communications*, vol. 112, no. 4, pp. 2131–2158, 2020. [Online]. Available: <https://doi.org/10.1007/s11277-020-07143-2>.
- [20] C. Horan and H. Saiedian, "Cyber crime investigation: Landscape, challenges, and future research directions," *Journal of Cybersecurity and Privacy*, vol. 1, no. 4, pp. 580–596, 2021. DOI: 10.3390/jcp1040029.
- [21] M. Chertoff, "A public policy perspective of the dark web," *Journal of Cyber Policy*, vol. 2, no. 1, pp. 26–38, 2017. [Online]. Available: <https://doi.org/10.1080/23738871.2017.1298643>.
- [22] T. Thomas, T. Edwards, and I. Baggili, "Blockquery: Toward forensically sound cryptocurrency investigation," *Forensic Science International: Digital Investigation*, vol. 40, p. 301340, 2022. DOI: 10.1016/j.fsidi.2022.301340.
- [23] M. Taleby *et al.*, *Do dark web and cryptocurrencies empower cybercriminals?* SecureComm, 2022. [Online]. Available: https://www.researchgate.net/publication/354137933_Do_Dark_Web_and_Cryptocurrencies_Empower_Cybercriminals.

- [24] S. Lee *et al.*, “Cybercriminal minds: An investigative study of cryptocurrency abuses in the dark web,” in *Proc. 26th Annual Network & Distributed System Security Symposium (NDSS)*, 2019. [Online]. Available: <https://dx.doi.org/10.14722/ndss.2019.23365>.
- [25] T. Leng and A. Yu, “A framework of darknet forensics,” in *Proc. 3rd Int. Conf. Advanced Information Science and System (AISS)*, 2021, pp. 1–6. [Online]. Available: <https://doi.org/10.1145/3503047.3503082>.
- [26] S. Goodison *et al.*, *Identifying law enforcement needs*, 2019. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2704/RAND_RR2704.pdf.
- [27] N. Christin, “Traveling the silk road: A measurement analysis of a large anonymous online marketplace,” in *Proc. 22nd Int. World Wide Web Conf.*, 2013, pp. 213–224. [Online]. Available: <https://doi.org/10.1145/2488388.2488408>.
- [28] M. Bernaschi, A. Celestini, S. Guarino, and F. Lombardi, “Exploring and analyzing the tor hidden services graph,” *ACM Transactions on the Web*, vol. 11, no. 4, pp. 1–26, 2017. [Online]. Available: <https://doi.org/10.1145/3133327>.
- [29] E. Ozkaya and R. Islam, *Inside the Dark Web*. CRC Press, 2019. DOI: 10.1201/9780429505021.
- [30] E. M. Lopez, S. Moon, and J. Park, “Scenario-based digital forensics challenges in cloud computing,” *Symmetry*, vol. 8, no. 10, p. 107, 2016. DOI: 10.3390/sym8100107.
- [31] A. K. Jadoon, W. Iqbal, M. F. Amjad, H. Afzal, and Y. A. Bangash, “Forensic analysis of tor browser: A case study for privacy and anonymity on the web,” *Forensic Science International*, vol. 299, pp. 59–73, 2019. [Online]. Available: <https://doi.org/10.1016/j.forsciint.2019.03.051>.
- [32] H. F. Atlam, N. Ekuri, M. A. Azad, and H. S. Lallie, “Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions,” *Electronics*, vol. 13, no. 17, p. 3568, 2024. [Online]. Available: <https://doi.org/10.3390/electronics13173568>.
- [33] R. Raman and V. K. Nair, “Darkweb research: Past, present, and future trends and mapping to sustainable development goals,” *Heliyon*, vol. 9, no. 11, e22269, 2023. DOI: 10.1016/j.heliyon.2023.e22269.
- [34] A. Bracci *et al.*, “Vaccines and more: The response of dark web marketplaces to the covid-19 pandemic,” *PLoS One*, vol. 17, no. 11, e0275288, 2022. [Online]. Available: <https://doi.org/10.1371/journal.pone.0275288>.
- [35] M. Al-Nabki, R. Fidalgo, O. Araque, and D. Camacho, “Classifying illegal activities on tor network based dark web marketplaces,” *Expert Systems with Applications*, vol. 150, p. 113318, 2020. [Online]. Available: <https://doi.org/10.1016/j.eswa.2020.113318>.
- [36] P. Norris, “Tor forensics: Proposed workflow for client memory artefacts,” *Computers & Security*, vol. 106, p. 102311, 2021. [Online]. Available: <https://doi.org/10.1016/j.cose.2021.102311>.

- [37] M. Muir, P. Leimich, and W. J. Buchanan, "A forensic audit of the tor browser bundle," *Digital Investigation*, vol. 29, pp. 118–128, 2019. DOI: 10.1016/j.diin.2019.03.009.
- [38] S. Nazah, S. Huda, J. Abawajy, and M. M. Hassan, "Evolution of dark web threat analysis and detection: A systematic approach," *IEEE Access*, vol. 8, pp. 171 796–171 819, 2020. DOI: 10.1109/ACCESS.2020.3024198.
- [39] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134. DOI: 10.1109/sfcs.1994.365700.
- [40] A. Ghappour, "Searching places unknown: Law enforcement jurisdiction on the dark web," *Stanford Law Review*, vol. 69, pp. 1075–1138, 2017. [Online]. Available: https://scholarship.law.bu.edu/faculty_scholarship/204.
- [41] R. I. Ferguson, K. Renaud, S. Wilford, and A. Irons, "Precept: A framework for ethical digital forensics investigations," *Journal of Intellectual Capital*, vol. ahead-of-print, no. ahead-of-print, Mar. 2020. [Online]. Available: https://strathprints.strath.ac.uk/75129/1/Ferguson_etal_JIC_2020_Precept_framework_ethical_digital_forensics_investigations.pdf.
- [42] R. Montasari, *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution*. Springer International Publishing, 2024. DOI: 10.1007/978-3-031-50454-9.
- [43] J. Veber and Z. Smutny, "Standard iso 27037:2012 and collection of digital evidence: Experience in the czech republic," in *14th European Conference on Cyber Warfare & Security*, vol. 2015, 2015, pp. 294–299. [Online]. Available: https://www.researchgate.net/publication/283226153_Standard_ISO_270372012_and_Collection_of_Digital_Evidence_Experience_in_the_Czech_Republic.
- [44] dinastiac083, *Pdf-international-standard-iso-iec-27042-compress*, Scribd, Accessed: Apr. 25, 2025, 2025. [Online]. Available: <https://www.scribd.com/document/789762753/pdf-international-standard-iso-iec-27042-compress>.
- [45] A. Zafar, *Information technology -security techniques -incident investigation principles and processes*, Accessed: Apr. 25, 2025, 2025. [Online]. Available: <https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027043-2015.pdf>.
- [46] N. Mandela, A. A. S. Mahmoud, and A. K. Agrawal, "Implications of forensic investigation in dark web," in *Communications in Computer and Information Science (CNC 2023)*, vol. 1815, Springer, 2023, pp. 103–115. DOI: 10.1007/978-3-031-43140-1_10.
- [47] C. Nguyen and A. Costa, "Digital forensics challenges in the quantum computing era," *ITSI Transactions on Electrical and Electronics Engineering*, vol. 11, no. 1, pp. 1–7, 2025. [Online]. Available: <https://journals.mriindia.com/index.php/itsiteee/article/view/153>.
- [48] Europol, *Internet organised crime threat assessment (iocta) 2020*, 2020. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.
- [49] S. Doyle, N. Umansky, and W. E. Forum, *Why collaboration is essential to tackling global cybercrime*, Nov. 2024. [Online]. Available: <https://www.weforum.org/stories/2024/11/collaboration-key-tackling-cybercrime-cybersecurity>.

- [50] A. Walters, *Volatility: An advanced memory forensics framework*, Presented at Black Hat USA, 2014. [Online]. Available: <https://www.volatilityfoundation.org>.
- [51] U.S. Department of Energy, *The evolution of volatile memory forensics*, OSTI, 2022. [Online]. Available: <https://www.osti.gov/servlets/purl/1885656>.
- [52] U.S. Department of Energy, *The evolution of volatile memory forensics*, OSTI, 2021. [Online]. Available: <https://www.osti.gov/servlets/purl/1884642>.
- [53] W. Foundation, *Performance - wireshark wiki*, 2023. [Online]. Available: <https://wiki.wireshark.org/Performance>.
- [54] Europol, *Internet organised crime threat assessment (iocta) 2022*, The Hague, Netherlands, 2022. [Online]. Available: <https://www.europol.europa.eu/publications-documents/internet-organised-crime-threat-assessment-iocta-2022>.
- [55] Chainalysis, *Cryptocurrency crime and aml report 2021*, White Paper, New York, NY, USA, 2021. [Online]. Available: <https://www.chainalysis.com>.
- [56] Chainalysis, *Technical explainer: Reactor accuracy in address clustering*, 2023. [Online]. Available: <https://www.chainalysis.com>.
- [57] U.S. Department of Justice, *Operation disruptor 2020: Results and statistics*, Washington, D.C., 2020. [Online]. Available: <https://www.justice.gov/opa/pr/operation-disruptor-2020-results-and-statistics>.
- [58] National Institute of Justice, *Taking on the dark web: Law enforcement experts identify investigative needs*, 2020. [Online]. Available: <https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs>.
- [59] G. Antoniou, *Exploring the shadows: Advances and challenges in dark web digital forensics*, eForensics Magazine, May 2024. [Online]. Available: <https://eforensicsmag.com/exploring-the-shadows-advances-and-challenges-in-dark-web-digital-forensics/>.
- [60] K. Kaushik and P. Gaur, "A comprehensive framework for dark web forensic tools: Analysis, implementation, and practical guidelines," *Journal of Information Security and Cybercrimes Research*, vol. 7, no. 2, pp. 180–191, 2024. [Online]. Available: <https://journals.nauss.edu.sa/index.php/JISCR/article/view/3137>.
- [61] FBI, *Silk road case documents*, 2015. [Online]. Available: <https://www.justice.gov>.
- [62] United States, *United states v. ross william ulbricht, case no. 14-cr-68, southern district of new york, trial evidence*, 2015. [Online]. Available: <https://www.justice.gov>.
- [63] AccessData, *Ftk imager user guide*, 2020. [Online]. Available: <https://accessdata.com>.
- [64] G. Software, *Encase forensic tool performance benchmarks*, EnCase Labs, 2021. [Online]. Available: <https://www.encase.com>.
- [65] W. Foundation, *Samplecaptures - wireshark wiki*, 2023. [Online]. Available: <https://wiki.wireshark.org/samplecaptures>.

-
- [66] U.S. Department of Justice, *Case 1:21-cr-00399-rdm document 259 filed 02/29/24*, 2024. [Online]. Available: https://www.moneylaunderingnews.com/wp-content/uploads/sites/12/2024/03/District_of_Columbia_USA_v._STERLINGOV_Memo_Opinion_and_Order.pdf.
- [67] M. T. GmbH, *Maltego product overview and global usage*, 2023. [Online]. Available: <https://www.maltego.com>.
- [68] M. T. GmbH, *How investigators use maltego in osint*, Maltego Blog, 2023. [Online]. Available: <https://www.maltego.com/blog>.