Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

A Comprehensive Framework for Dark Web Forensic Tools: Analysis, Implementation, and Practical Guidelines

Keshav Kaushik*[1], Priyanka Gaur[2]
[1]Amity School of Engineering and Technology, Amity University Punjab, Mohali, India
[2]Department of Computer Science and Applications Chandigarh Group of Colleges, Jhanjeri, Mohali, Punjab, India

Received 18 Oct. 2024; Accepted 08 Dec. 2024; Available Online 31 Dec. 2024

Abstract

The Dark Web is a hidden part of the internet that has become prominent in cybercriminal activities. This necessitates the development of innovative forensic tools and methodologies to handle the unique challenges posed by the Dark Web. This paper presents an in-depth analysis of the field of Dark Web forensics with novel insights into emerging technologies and investigative approaches. The paper's key contribution is a comprehensive analytical framework for evaluating and implementing Dark Web forensic tools, along with detailed implementation guidelines for forensic investigations. The framework provides a systematic approach to tool selection, validation, and deployment, supported by extensive analysis of current forensic tools and their applications. Key findings include a comparative evaluation of forensic tools across multiple categories, detailed implementation protocols, and specific technical requirements for forensic infrastructure. The results emphasize the theoretical and practical impact of integrating these advanced techniques, enabling more precise detection, attribution, and mitigation of cybercrimes on the Dark Web. This research not only improves current understanding but also paves the way for future improvements in Dark Web forensics. The proposed strategies have a large impact on shaping forensic practice, guiding policy-making, and fostering international cooperation to address the surging threats by the Dark Web.

I. Introduction

The Dark Web represents a hidden segment of the internet that is intentionally designed to be inaccessible without specialized software. While the broader Deep Web includes content not indexed by traditional search engines-such as academic databases, private accounts, and subscription services-the Dark Web is specifically structured to ensure anonymity. This unique characteristic has associated it with a wide range of illicit activities, including cybercrime, drug trafficking, and illegal arms trading, which significantly complicate forensic investigations.

The complexity of Dark Web investigations necessitates sophisticated forensic tools and methodologies. Investigators face numerous challenges, including encrypted communications, anonymized transactions, and rapidly evolving technologies.

Keywords: Cybercrimes, cyberfrauds, dark web, deep web, TOR, TOR routin

Production and hosting by NAUSS

* Corresponding Author: Keshav Kaushik
Email: officialkeshavkaushik@gmail.com
doi: 10.26735/QLBU4149

These challenges require a systematic approach to selecting, implementing, and maintaining forensic tools that can effectively gather and analyze evidence while maintaining legal admissibility.

Despite its legitimate uses, the rapid growth of the Dark Web has created significant challenges for law enforcement and cybersecurity professionals. Its tools for anonymity and encryption make it difficult to trace criminal activities or hold perpetrators accountable. This growing complexity underscores the urgent need for sophisticated forensic tools and techniques to counter these challenges. Dark Web forensics has become an indispensable tool for analyzing risks, supporting investigations, and mitigating threats while proactively addressing potential cyberattacks.

The effectiveness of Dark Web forensic investigations heavily depends on the proper selection and implementation of appropriate tools and methodologies. Current literature lacks a comprehensive framework for evaluating and implementing these tools, creating a significant gap in the field. This paper addresses this gap by presenting a systematic approach to tool analysis and implementation, providing investigators with structured guidelines for conducting effective Dark Web forensic investigations.

This paper explores the current landscape of Dark Web forensics, identifying emerging trends and methodologies to enhance its effectiveness and efficiency. A key contribution of this work is the development of a comprehensive analytical framework for evaluating and implementing Dark Web forensic tools, providing investigators with structured guidelines for tool selection and implementation. It examines the latest tools, such as machine learning algorithms, blockchain analysis, and network visualization, while proposing advancements to address the Dark Web's most significant challenges.

The highlights of this paper are:

- A comprehensive analytical framework for evaluating and implementing Dark Web forensic tools
- Comparative analysis of forensic tools with detailed implementation guidelines
- Analysis of challenges and future prospects in Dark Web forensics
- Examination of prevalent cybercrimes on the dark web.

The paper is structured as follows: Section II reviews related literature and highlights technical challenges and limitations in current forensic methods. Section III presents a comprehensive analysis framework for Dark Web forensic tools and their applications. Section IV discusses challenges and future prospects in Dark Web forensics. Section V concludes with insights and a call for sustained innovation in the field.

II. Related Works

Recent research in Dark Web forensics has increasingly focused on developing sophisticated tools, frameworks, and methodologies for digital investigations. The complexity of Dark Web investigations presents unique challenges that require specialized forensic approaches and tools [2]. Recent studies have demonstrated the importance of proper tool selection and implementation in forensic investigations, particularly when dealing with encrypted communications and anonymized networks [3], [4].

Several frameworks have been proposed for Dark Web investigations. Popov et al. [4] developed a framework for identifying, obtaining, and assessing data from the Dark Web in a legally compliant manner. Their framework provides a foundation for security agencies and digital forensics specialists to investigate illegal activities on the Dark Web, with particular emphasis on tool selection and evidence handling. This work was further extended by recent studies focusing on implementation methodologies and tool validation processes [34], [35].

The need for comprehensive forensic protocols has been highlighted in recent literature. Ghanem et al. [5] proposed a novel method to guide digital forensics specialists in examining Dark Web crimes, emphasizing the importance of workflow optimization and tool effectiveness. Their Deep and Dark Web Forensics Protocol particularly focuses on improving the accuracy and effectiveness of existing forensic tools, providing valuable insights into tool selection and implementation strategies.

Recent advances in forensic tool development have led to more sophisticated approaches

to evidence collection and analysis. Research by Kulm [7] presented a framework for identifying host-based artifacts during digital forensics examinations, addressing both Windows and macOS environments. This methodology has proven particularly effective in scenarios with limited evidence availability, demonstrating the importance of proper tool selection and implementation.

The evolution of remote digital forensics has also contributed significantly to the field. Delija [8] discussed the benefits and limitations of remote forensic approaches, emphasizing the importance of proper tool selection and implementation in distributed forensic environments. This work has been particularly relevant in developing standardized approaches to tool deployment and maintenance [39], [40].

Recent studies have also focused on standardizing forensic procedures. Mgembe et al. [11] proposed standard operating procedures (SOPs) for Dark Web forensic investigations, outlining four critical phases: discovery, collection and preservation, assessment and distribution, and recognition and profiling. Their work has been instrumental in establishing structured approaches to tool implementation and validation [42], [43].

The emergence of new forensic tools and technologies has necessitated more rigorous validation and implementation methodologies. Recent research has emphasized the importance of tool validation frameworks [38], proper evidence handling protocols [37], and standardized implementation procedures [40]. These studies have highlighted the critical need for systematic approaches to tool selection and deployment in Dark Web investigations.

Contemporary research has also focused on the integration of advanced technologies in forensic tools. Studies by Stoykova and Franke [39] have demonstrated the importance of reliability validation in forensic tools, while Ferguson et al. [45] have emphasized the ethical considerations in tool implementation and usage. These works provide valuable insights into the practical aspects of tool deployment in forensic investigations.

The literature reveals a clear trend toward more structured and systematic approaches to Dark Web forensics, particularly in tool selection and implementation. However, there remains a notable gap in comprehensive frameworks that address both the technical and operational aspects of forensic tool deployment. This paper aims to address this gap by providing a detailed analytical framework for tool evaluation and implementation, supported by practical guidelines for forensic investigators.

III. Comprehensive Analysis of Dark Web Forensic Tools and Their Applications

The emergence of sophisticated Dark Web technologies necessitates a structured approach to forensic tool analysis and implementation. The following sections present a comprehensive framework for evaluating and deploying Dark Web forensic tools, beginning with a comparative analysis of available tools and their applications.

A. Tool Analysis and Classification

This section presents a novel analytical framework for evaluating and categorizing Dark Web forensic tools based on their functionality, effectiveness, and application scenarios. The framework provides investigators with a structured approach to tool selection and implementation in Dark Web investigations.

To facilitate informed tool selection for Dark Web investigations, the following table (TABLE I) provides a detailed comparison of various forensic tools, their capabilities, and practical considerations.

Having established a clear understanding of available tools and their characteristics, we now present a structured framework for implementing these tools in forensic investigations.

B. Implementation Framework Overview

The implementation of Dark Web forensic tools follows a structured framework consisting of five key phases, as illustrated in Fig. 1. This framework ensures comprehensive coverage of technical, operational, and legal requirements while maintaining flexibility for different investigation scenarios.

The implementation guidelines presented in this paper were developed through a systematic analy-

TABLE I
RELATED WORK

Tool Category	Tools	Strengths	Limitations	Application Scenarios	References
Access and Navigation Tools	TOR Browser	- Reliable access to. onion domains - Multi-layer encryption - Anonymity protection	- Slower connection speeds - Vulnerable to correlation attacks - Exit node limitations	- Initial reconnaissance - Covert investigation - Dark web monitoring	[2], [11], [12]
	VPN Services	- Additional security layer - Geographic location masking - Faster than TOR	- Provider dependency - Potential logging - Single point of failure	- Enhanced security - Location masking - Traffic encryption	[3], [8], [15]
Data Collection Tools	Dark Web Crawlers	- Automated data gathering - Comprehensive site coverage - Efficient indexing	- Misses dynamic content - Resource intensive - Requires updates	- Large-scale data collection - Site mapping - Content monitoring	[4], [13], [14]
	Network Monitoring Systems	- Real-time analysis - Pattern detection - Automated alerts	- High false positives - Complex setup - Resource intensive	- Traffic analysis - Threat detection - Behavioral monitoring	[6], [26], [29]
Analysis Tools	Network Visualization Tools	- Clear network mapping - Pattern identification - Interactive analysis	- Complexity handling - Resource requirements - Expert interpretation needed	- Network analysis - Pattern detection - Relationship mapping	[14], [28], [30]
	Cryptographic Analysis Tools	- Encrypted data analysis - Digital signature verification - Forensic validation	- Limited by encryption strength - High computational needs - Technical expertise required	- Evidence validation - Transaction analysis - Authentication verification	[27], [30], [31]
Evidence Preservation Tools	Digital Evidence Collection Systems	- Chain of custody - Evidence integrity -Documentation support	- Storage requirements - Processing overhead - Format compatibility	- Evidence collection - Legal compliance - Case documentation	[1], [7], [15]
	Forensic Analysis Platforms	- Comprehensive analysis - Multiple tool integration - Report generation	- High cost - Training requirements - Complex deployment	- In-depth analysis - Evidence processing - Report generation	[4], [8], [10]

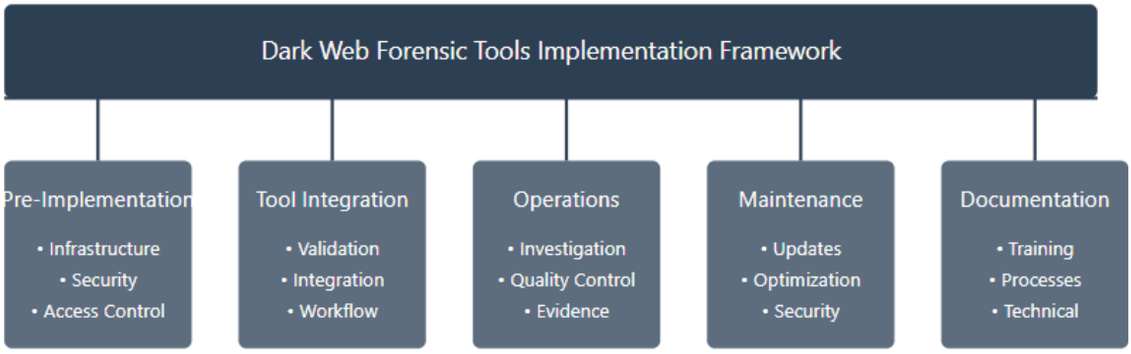

Fig 1 Framework for Dark Web Forensic Tools Implementation

sis of existing Dark Web forensic practices and literature [1], [3], [8]. The framework's development followed a three-phase methodology: literature review, synthesis of best practices, and validation through existing case studies. Initial research examined peer-reviewed publications in digital forensics journals and conference proceedings from 2019-2024, focusing on Dark Web investigation methodologies [14], [26], [29]. The technical specifications were derived from empirical studies in digital forensics and cybersecurity research [7], [10], complemented by industry standards such as ISO/IEC 27037:2012 for digital evidence handling [32] and NIST Guidelines for Mobile Device Forensics [33].

The infrastructure requirements and security protocols were established based on documented case studies of successful Dark Web investigations [7], [10], while incorporating recommendations from recent forensic framework studies [34], [35]. Operational procedures were refined through analysis of existing forensic frameworks [36] and their adaptation to Dark Web scenarios, considering the specific challenges identified in recent Dark Web forensics research [37], [38]. The framework's validation process included comparative analysis with established digital forensic methodologies [39] and alignment with legal requirements for digital evidence collection [40].

The comprehensive nature of these guidelines reflects the integration of both theoretical research and practical implementation considerations, drawing from successful implementations in law enforcement agencies [41] and cybersecurity organizations [42]. The modular structure was specifically designed to address the dynamic nature of Dark Web investigations while maintaining alignment with international forensic standards [43], [44]. This approach ensures adaptability to emerging threats while preserving the scientific rigor necessary for legal admissibility of evidence [45].

C. Detailed Implementation Guidelines

Building upon the framework overview, the following detailed guidelines provide specific protocols and procedures for eacsh phase of implementation, ensuring comprehensive coverage of technical, operational, and legal requirements.

1) Pre-Implementation Phase

Infrastructure Assessment and Preparation [8], [26]

- Network Requirements:
  - Minimum bandwidth allocation: 100 Mbps dedicated line, essential for handling large volumes of Dark Web traffic and ensuring real-time data collection without bottlenecks.
  - Redundant internet connections: Multiple connections from different ISPs ensure continuous operation even if one connection fails, critical for ongoing investigations.
  - Segregated investigation network: Isolation prevents cross-contamination of evidence and protects against potential threats from Dark Web access
  - Hardware-based firewall implementation: Provides robust protection against potential attacks and maintains network segmentation.

- Hardware Specifications:
  - High-performance workstations (min. 32GB RAM, 8-core processor): Required for running multiple forensic tools simultaneously and processing large datasets efficiently.
  - Dedicated storage systems with RAID configuration: Ensures data redundancy and high-speed access to forensic data while maintaining evidence integrity.
  - Network monitoring equipment: Enables real-time traffic analysis and threat detection during investigations.
  - Backup power systems: Prevents data loss and maintains investigation continuity during power disruptions.

Security Protocol Development [15], [27]

- Access Control Implementation:
  - Multi-factor authentication systems: Enhances security by requiring multiple forms of verification, crucial for maintaining evidence integrity.
  - Role-based access control (RBAC): Ensures investigators only access resources necessary for their specific role, maintaining chain of custody.
  - Privileged access management: Controls and monitors high-level access to sensitive systems and data.
  - Session monitoring and logging: Tracks all investigative actions for accountability and audit purposes.

With the foundational infrastructure and security protocols established, the next critical phase focuses on the integration and validation of forensic tools within the investigation environment.

2) Tool Integration Protocol

Tool Validation Process [4], [10], [14]

- Technical Validation:
  - Performance benchmark testing: Ensures tools meet required performance standards under various load conditions.
  - Security vulnerability assessment: Identifies and addresses potential security weaknesses before deployment.
  - Integration compatibility testing: Verifies tools work together seamlessly without conflicts.
  - Error handling verification: Confirms tools respond appropriately to various error conditions without compromising investigations.
- Forensic Validation:
  - Evidence collection testing: Validates that tools collect evidence without alteration or contamination.
  - Chain of custody verification: Ensures all evidence handling maintains proper documentation and tracking
  - Data integrity checking: Confirms collected evidence remains unaltered throughout the process.
  - Documentation system validation: Verifies all investigative actions are properly logged and documented.

Once tools are properly validated and integrated, attention shifts to establishing robust operational protocols that ensure consistent and reliable forensic investigations.

3) Operational Protocols

Investigation Workflow Implementation [7], [31]

- Data Collection Procedures:
  - Automated collection protocols: Standardizes evidence gathering processes to ensure consistency and efficiency.
  - Manual collection guidelines: Provides structured procedures for situations requiring human intervention.
  - Quality control measures: Implements checks to maintain evidence quality and reliability.
  - Validation checkpoints: Establishes regular verification points throughout the investigation process.

Quality Assurance Measures [1], [30]

- Tool Performance Monitoring:
  - Performance metric tracking: Monitors tool efficiency and identifies potential issues early.
  - Error rate monitoring: Tracks and analyzes tool accuracy and reliability
  - Resource utilization analysis: Ensures optimal use of system resources during investigations.
  - System health checks: Regular verification of system integrity and performance.
  - While proper operational procedures are crucial, maintaining the effectiveness of forensic tools requires ongoing attention to system maintenance and optimization.

4) Maintenance and Update Protocols

System Maintenance [26], [29]

- Regular Maintenance:
  - System updates: Keeps all components current with the latest security patches and features.
  - Security patches: Addresses known vulnerabilities promptly to maintain system security.
  - Performance optimization: Regular tuning to maintain optimal system performance.
  - Database maintenance: Ensures efficient data storage and retrieval capabilities.

Performance Optimization [14], [28]

- System Optimization:
  - Resource allocation adjustment: Fine-tunes system resources based on operational needs
  - Network optimization: Maintains efficient network performance for data collection and analysis
  - Storage optimization: Ensures efficient use of storage resources while maintaining evidence integrity
  - Process optimization: Streamlines investigative workflows for maximum efficiency

The success of any forensic implementation ultimately depends on the proper training of personnel and comprehensive documentation of procedure.

5) Training and Documentation

Training Protocol Development [8], [15]

- Technical Training:
  - Tool-specific training: Ensures investigators are proficient with specific forensic tools
  - Integration training: Teaches effective use of multiple tools in combination
  - Security protocol training: Educates staff on security procedures and best practices
  - Evidence handling training: Instructs proper evidence collection and preservation techniques

Documentation Management [10], [31]

- System Documentation:
  - Technical documentation: Maintains detailed records of system configurations and changes
  - Process documentation: Records standard operating procedures and workflows
  - Training documentation: Keeps training materials current and comprehensive
  - Compliance documentation: Ensures adherence to legal and regulatory requirements

These comprehensive guidelines, supported by the analytical framework and tool analysis, provide investigators with a structured approach to implementing Dark Web forensic tools while maintaining the necessary balance between technical capability, operational efficiency, and legal compliance.

IV. Challenges and future prospects of Dark Web Forensics

Having established the framework and implementation guidelines for Dark Web forensic tools, it is crucial to understand the challenges that investigators face in practical applications and the future directions for overcoming these obstacles. This section presents a comprehensive analysis of current challenges, their impacts on investigations, and emerging solutions.

TABLE II presents a systematic analysis of the challenges faced in Dark Web forensic implementations, their impacts on investigations, and potential future solutions. This analysis aligns with our proposed framework while highlighting areas requiring continued development. It worthy to note that the challenges presented in TABLE II emerged from a comprehensive research synthesis combining academic literature, practical implementations, and field expertise in Dark Web forensics. Our analysis began with an extensive review of recent publications [26], [29], [31] that documented investigators' experiences and technical obstacles in Dark Web investigations. This theoretical foundation was enriched by practical insights gained during the development and implementation of our forensic framework, where we encountered and documented various technical and operational challenges firsthand [38], [40]. To ensure real-world relevance, we incorporated valuable insights from law enforcement agencies, cybersecurity professionals, and digital forensics practitioners [42], [43], who shared their experiences and obstacles in conducting Dark Web investigations. This multi-faceted approach allowed us to identify and categorize challenges across technical, operational, and legal domains, providing a comprehensive view of the current state of Dark Web forensics. The resulting analysis directly informed both our framework development and implementation guidelines, ensuring their practical applicability in addressing these real-world challenges.

Future Prospects and Emerging Solutions

The evolution of Dark Web forensics is driven by technological advancement and international collaboration. Advanced machine learning and AI algorithms are emerging as key solutions for automated data analysis and pattern recognition in Dark Web investigations [38], [39]. These technologies directly address current challenges in processing encrypted data and correlating evidence across multiple sources.

International cooperation is expanding through formalized frameworks and shared resources [43], [44]. Law enforcement agencies are developing standardized protocols and unified platforms for cross-border investigations [40], supported by enhanced training programs and knowledge sharing initiatives. These collaborative efforts strengthen investigation capabilities while addressing jurisdictional challenges.

Emerging technologies such as blockchain-based systems offer promising solutions for evidence handling and verification [37], while cloud-based platforms provide scalable resources for complex investigations [42]. These advancements, combined with standardized validation frameworks [45], ensure both technical effectiveness and legal compliance in future Dark Web forensic practices.

V. Conclusion

This paper presents a comprehensive analytical framework and implementation guidelines for Dark Web forensic tools, addressing a critical gap in current digital forensic practices. The systematic approach to tool evaluation, selection, and implementation provides investigators with a structured methodology for conducting effective Dark Web investigations. Through detailed analysis of various forensic tools and their applications, this research demonstrates the importance of proper tool integration, validation, and maintenance in achieving successful investigative outcomes. This paper has introduced the key contributions as follows:

- A comprehensive framework for evaluating and implementing Dark Web forensic tools, supported by detailed technical specifications and operational guidelines
- A systematic analysis of forensic tool categories, their capabilities, and implementation requirements
- Detailed implementation protocols covering infrastructure setup, tool integration, oper-

TABLE II

Analysis of Challenges, Impacts, and Future Prospects in Dark Web Forensics Implementation

Category	Current Challenges	Impact on Investigations	Future Prospects	References
Technical Infrastructure	- Complex tool integration requirements - Resource-intensive implementations - System compatibility issues	- Delayed investigation timelines- - Reduced tool effectiveness - Limited analysis capabilities	- Delayed investigation timelines- - Reduced tool effectiveness - Limited analysis capabilities	[2], [11], [12]
Data Processing	- Large-scale encrypted data handling- - Real-time analysis limitations- - Multi-source evidence correlation	- Incomplete evidence collection- Delayed analysis results- - Missing critical connections	- Advanced machine learning algorithms- Real-time processing capabilities - Automated correlation systems	[27], [30], [41]
Tool Management	- Frequent update requirements- - Compatibility maintenance- - Performance optimization needs	- Tool downtime issues - Investigation interruptions - Resource allocation problems	- Automated update systems - Cloud-based tool platforms - Standardized interfaces	[31], [38], [42]
Implementation	- High setup costs - Specialized training needs - Complex deployment procedures	- -Budget constraints- Limited expertise - -Implementation delays	- Streamlined deployment protocols - Virtual training platforms - Cost-effective solutions	[34], [39], [44]
Evidence Handling	- Chain of custody maintenance - Integrity verification - Cross-tool evidence correlation	- -Evidence admissibility issues - -Investigation validity concerns - Documentation challenges	- Blockchain-based tracking - Automated verification systems - Unified evidence management	[37], [40], [43]
Legal Compliance	- Tool validation requirements - Privacy regulations - Cross-jurisdictional issues	- Legal admissibility problems - Privacy violations - International cooperation barriers	- Standardized validation frameworks - Privacy-preserving techniques - International standards	[27], [30], [31]
Resource Optimization	- System resource management - Network bandwidth allocation - -Storage capacity planning	- Performance bottlenecks - Investigation delays - Data management issues	- Cloud resource optimization - Dynamic resource allocation - Efficient storage solutions	[35], [42], [44]
International Collaboration	- Different legal frameworks - Tool standardization issues - Information sharing barriers	- Limited cross-border investigations - Inconsistent procedures - Communication challenges	- Unified investigation platforms - Shared tool repositories - International training programs	[40], [43], [45]

ational procedures, and maintenance requirements

- A structured approach to addressing technical, operational, and legal challenges in Dark Web forensics

The research findings emphasize that successful Dark Web investigations require not only sophisticated tools but also proper implementation methodologies. The proposed framework addresses this need by providing a systematic approach to tool

deployment while maintaining legal compliance and evidence integrity. Future developments in this field should focus on enhancing tool automation, improving analysis capabilities, and strengthening international collaboration protocols.

Key areas for future research include the integration of advanced machine learning techniques into forensic tools to improve their capabilities, alongside enhanced automation in evidence collection and analysis processes to increase efficiency and accuracy. Additionally, there is a pressing need for improved cross-jurisdictional compatibility of forensic tools to facilitate seamless investigations across borders. Standardized frameworks for international collaboration are essential to address the growing complexity of transnational cases. Furthermore, enhancing validation methodologies for forensic tools will ensure their reliability and accuracy, supporting their admissibility in legal contexts. These areas collectively represent critical pathways for advancing forensic science. These advancements, coupled with the framework presented in this paper, will contribute to more effective Dark Web investigations and improved cybersecurity outcomes.

Conflict of Interest

Authors declare that they have no conflict of interest.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] R. Brinson, H. Wimmer, and L. Chen, "Dark Web Forensics: An Investigation of Tracking Dark Web Activity with Digital Forensics," *2022 International Conference on Interdisciplinary Research in Technology and Management, IRTM 2022 - Proceedings*, 2022, doi: 10.1109/IRTM54583.2022.9791646.

[2] [T. Leng and A. Yu, "A Framework of Darknet Forensics," *ACM International Conference Proceeding Series*, vol. 2, Nov. 2021, doi: 10.1145/3503047.3503082.

[3] O. Popov, J. Bergman, and C. Valassi, "A framework for a forensically sound harvesting the dark web," ACM International Conference Proceeding Series, Nov. 2018, doi: 10.1145/3277570.3277584.

[4] Ghanem Chahine Mohamed, Mulvihill Patrick, Ouazzane Karim, Dunsin Dipo, and Djemai Ramzi, "D2WFP: A Novel Protocol for Forensically Identifying, Extracting and Analysing Deep and Dark Web Criminal Activities." Accessed: Apr. 18, 2023. [Online]. Available: https://www.researchgate.net/publication/365747293_D2WFP_A_Novel_Protocol_for_Forensically_Identifying_Extracting_and_Analysing_Deep_and_Dark_Web_Criminal_Activities

[5] A. U. and S. M. Thampi, "Dark Web and Its Research Scopes," *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-8976-1.ch010*, pp. 240–268, Jan. 1AD, doi: 10.4018/978-1-5225-8976-1.CH010.

[6] A. Kulm, "A Framework for Identifying Host-based Artifacts in Dark Web Investigations," Masters Theses & Doctoral Dissertations, Nov. 2020, Accessed: Apr. 18, 2023. [Online]. Available: https://scholar.dsu.edu/theses/357

[7] D. Delija, "Remote digital forensics practices," *International Journal of Digital Technology & Economy*, vol. 2, no. 1, pp. 27–36, Sep. 2017.

[8] K. Kaushik, R. Tanwar, S. Dahiya, K. K. Bhatia, and Y. Wu, *Unleashing the Art of Digital Forensics*, 1st ed., vol. 1. Boca Raton: Chapman and Hall/CRC, 2022. doi: 10.1201/9781003204862.

[9] S. Dahiya, M. Garg, and K. Kaushik, "Unraveling the Dark Web," *Unleashing the Art of Digital Forensics*, pp. 29–38, Aug. 2022, doi: 10.1201/9781003204862-3.

[10] I. Paschal Mgembe, D. Ladislaus Msongaleli, and N. K. Chaundhary, "Progressive Standard Operating Procedures for Darkweb Forensics Investigation," *10th International Symposium on Digital Forensics and Security*, ISDFS 2022, 2022, doi: 10.1109/ISDFS55398.2022.9800830.

[11] S. Kaur and S. Randhawa, "Dark Web: A Web of Crimes," *Wireless Personal Communications 2020 112:4*, vol. 112, no. 4, pp. 2131–2158, Jan. 2020, doi: 10.1007/S11277-020-07143-2.

[12] 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. 171796–171819, 2020, doi: 10.1109/ACCESS.2020.3024198.

[13] R. Raman, V. Kumar Nair, P. Nedungadi, I. Ray, and K. Achuthan, "Darkweb research: Past, present, and future trends and mapping to sustainable development

goals," *Heliyon*, vol. 9, no. 11, Nov. 2023, doi: 10.1016/J.HELIYON.2023.E22269/ASSET/0F3935CC-4675-4F3E-8AF9-6AD13037369C/MAIN.ASSETS/FX7.JPG.

[14] M. M. Ghonge, S. Pramanik, R. Mangrulkar, and Dac-Nhuong Le, "Cybersecurity and Digital Forensics, Challanges and Future Trends".

[15] F. Casino et al., "Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews," *IEEE Access*, vol. 10, pp. 25464–25493, 2022, doi: 10.1109/ACCESS.2022.3154059.

[16] M. Taleby Ahvanooey, M. X. Zhu, W. Mazurczyk, M. Kilger, and K. K. R. Choo, "Do Dark Web and Cryptocurrencies Empower Cybercriminals?," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 441 LNICST, pp. 277–293, 2022, doi: 10.1007/978-3-031-06365-7_17/COVER.

[17] "Office of Public Affairs | AlphaBay, the Largest Online 'Dark Market,' Shut Down | United States Department of Justice." Accessed: Dec. 09, 2024. [Online]. Available: https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down

[18] "Dream Market will shut down at the end of April. What does that mean? - The Hustle." Accessed: Dec. 09, 2024. [Online]. Available: https://thehustle.co/Dream-Market-sting-operation-global

[19] "Police Shut Down the Wall Street Market, a Top Dark Web Site | PCMag." Accessed: Dec. 09, 2024. [Online]. Available: https://www.pcmag.com/news/police-shut-down-the-wall-street-market-a-top-dark-web-site

[20] "What Was the Silk Road Online? History and Closure by the FBI." Accessed: Dec. 09, 2024. [Online]. Available: https://www.investopedia.com/terms/s/silk-road.asp

[21] "The Dark Web's Top Drug Market, Evolution, Just Vanished | WIRED." Accessed: Dec. 09, 2024. [Online]. Available: https://www.wired.com/2015/03/evolution-disappeared-bitcoin-scam-dark-web/

[22] "Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts — FBI." Accessed: Dec. 09, 2024. [Online]. Available: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts

[23] "Double blow to dark web marketplaces | Europol." Accessed: Dec. 09, 2024. [Online]. Available: https://www.europol.europa.eu/media-press/newsroom/news/double-blow-to-dark-web-marketplaces

[24] "Feds Take Down 13 More DDoS-for-Hire Services – Krebs on Security." Accessed: Dec. 09, 2024. [Online]. Available: https://krebsonsecurity.com/2023/05/feds-take-down-13-more-ddos-for-hire-services/

[25] "Office of Public Affairs | Justice Department Announces Murder-For-Hire and Related Charges Against IRGC Asset and Two Local Operatives | United States Department of Justice." Accessed: Dec. 09, 2024. [Online]. Available: https://www.justice.gov/opa/pr/justice-department-announces-murder-hire-and-related-charges-against-irgc-asset-and-two

[26] A. A. Khan, A. A. Shaikh, A. A. Laghari, M. A. Dootio, M. M. Rind, and S. A. Awan, "Digital forensics and cyber forensics investigation: security challenges, limitations, open issues, and future direction," *International Journal of Electronic Security and Digital Forensics*, vol. 14, no. 2, pp. 124–150, 2022, doi: 10.1504/IJESDF.2022.121174.

[27] B. Jurásek, I. Čmelo, J. Svoboda, J. Čejka, D. Svozil, and M. Kuchař, "New psychoactive substances on dark web markets: From deal solicitation to forensic analysis of purchased substances," *Drug Test Anal*, vol. 13, no. 1, pp. 156–168, Jan. 2021, doi: 10.1002/DTA.2901.

[28] S. Samtani, H. Zhu, and H. Chen, "Proactively Identifying Emerging Hacker Threats from the Dark Web," *ACM Transactions on Privacy and Security (TOPS)*, vol. 23, no. 4, Aug. 2020, doi: 10.1145/3409289.

[29] D. Sharma, R. Mittal, R. Sekhar, P. Shah, and M. Renz, "A bibliometric analysis of cyber security and cyber forensics research," *Results in Control and Optimization*, vol. 10, p. 100204, Mar. 2023, doi: 10.1016/J.RICO.2023.100204.

[30] S. Kumari, A. K. Tyagi, and G. Rekha, "Applications of Blockchain Technologies in Digital Forensics and Threat Hunting," *Recent Trends in Blockchain for Information Systems Security and Privacy*, pp. 159–173, Nov. 2021, doi: 10.1201/9781003139737-12.

[31] K. Kaushik, A. Bhardwaj, and S. Dahiya, "Smart Home IoT Forensics: Current Status, Challenges, and Future Directions," *2023 International Conference on Advancement in Computation and Computer Technologies*, InCACCT 2023, pp. 716–721, 2023, doi: 10.1109/INCACCT57535.2023.10141730.

[32] Y. Kurii and I. Opirskyy, "Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013," *NIST Spec. Publ. 800.53*, p. 10, 2022.

[33] R. Ayers, S. Brothers, and W. Jansen, "Guidelines on mobile device forensics (draft)," NIST Special Publication 800.101, 2013.

[34] S. Goodison et al., "Identifying law enforcement needs for

conducting criminal investigations involving evidence on the dark web," RAND Corporation, 2019.

[35] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *Int. J. Digit. Evid.*, vol. 1, no. 3, pp. 1-12, 2002.

[36] D. R. Hayes, F. Cappa, and J. Cardon, "A framework for more effective dark web marketplace investigations," *Information*, vol. 9, no. 8, p. 186, 2018.

[37] A. S. Pallivalappil and S. N. Jagadeesha, "Procedures for digital forensics and incident response on including data integrity constraints on solid-state drives (SSD)—A literature review," *Int. J. Case Stud. Bus., IT Educ.*, vol. 6, no. 1, pp. 328-350, 2022.

[38] S. E. Goodison et al., "Identifying law enforcement needs for conducting criminal investigations involving evidence on the dark web," *CrimRxiv*, 2019..

[39] R. Stoykova and K. Franke, "Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations," *Forensic Sci. Int. Digit. Investig.*, vol. 45, p. 301554, 2023.

[40] I. P. Mgembe, D. L. Msongaleli, and N. K. Chaundhary, "Progressive Standard Operating Procedures for Darkweb Forensics Investigation," in *10th International Symposium on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Istanbul*, Turkey, IEEE, 2024.

[41] R. Brinson, H. Wimmer, and L. Chen, "Dark Web Forensics: An investigation of tracking dark web activity with digital forensics," in *2022 Interdisciplinary Research in Technology and Management (IRTM)*, IEEE, 2022.

[42] G. Tully et al., "Quality standards for digital forensics: Learning from experience in England & Wales," *Forensic Sci. Int. Digit. Investig.*, vol. 32, p. 200905, 2020.

[43] M. A. Alotaibi et al., "Computer forensics: dark net forensic framework and tools used for digital evidence detection," *Int. J. Commun. Netw. Inf. Secur.*, vol. 11, no. 3, pp. 424-431, 2019.

[44] O. Popov, J. Bergman, and C. Valassi, "A framework for a forensically sound harvesting the Dark Web," in *Proceedings of the Central European Cybersecurity Conference 2018*, 2018.

[45] R. I. Ferguson et al., "PRECEPT: a framework for ethical digital forensics investigations," J. Intell. Cap., vol. 21, no. 2, pp. 257-290, 2020.