Usability for Digital Forensics Professionals (Work in Progress)

Prakruthi Reddy and Cori Faklaris, *University of North Carolina at Charlotte*

Abstract

Research literature in digital forensics has explored numerous ways to address the challenges faced by the domain, from improving the technical capabilities of tools to developing fresh education methodologies. However, the usability of forensic tools has not received enough attention as a potential solution to alleviate some of these challenges. Additionally, existing publications on usability often group all forensic sectors together, overlooking variations in job roles, tasks, and workplace environments. In this paper, we summarize the existing challenges and approaches in research literature specifically related to digital forensics professionals in law enforcement. Next, we present a case for exploring usability in the context of digital forensics professionals. Finally, we outline our three-phased research plan, which involves a heuristic evaluation of popular forensic tools, an interview study with computer forensics professionals working in law enforcement, and the development of domain-specific heuristics to serve as effective metrics for evaluating digital forensics tools.

1. Introduction

Digital forensics is a field of forensic science focused on identifying, retrieving, storing, examining, and analyzing digital evidence [33]. It emerged as an ad hoc discipline in the late 1960s and 1980s within institutions such as the United States Department of Defense (DOD), the Federal Bureau of Investigation (FBI), and the Internal Revenue Service (IRS) [29]. Later, the boom in personal computers in the 1990s, along with the rise in crimes using these devices, drove the development and distribution of home-grown and commercial tools for extracting digital data from devices [29]. Furthermore, with the growth of the internet and the proliferation of online criminal activities in the 2000s, global interest in developing methods to tackle computer crime continued to grow. This led to the development of standardized methods by the National Institute of Standards and Technology (NIST) and the International Association for Computer Information Systems (IACIS) and the creation of technologically robust tools like EnCase and Forensic Toolkit (FTK) for collecting digital evidence [29] [7].

Although it was initially developed as a method to assist criminal investigations, today the field encompasses a wide range of sectors including law enforcement, government, corporations, legal, military, healthcare, and academia [7]. The professionals in these sectors occupy various titles such as computer forensics investigator, digital forensics examiner, cybersecurity analyst, incident response specialist, and IT auditor [35]. Their expertise is spread across computer crime investigation, intellectual property theft identification, fraud or unauthorized access evidence uncovering, digital evidence presentation in court proceedings, incident response during or after a cybersecurity incident, and malware analysis [7]. Our work focuses on digital forensics professionals within the law enforcement sector.

Digital forensics professionals in law enforcement work on collecting and analyzing digital evidence related to cases in a scientifically validated and forensically sound manner. They then present this evidence in court to assist in prosecuting criminals and ensuring justice [29]. According to the FBI's 2023 Internet Crime Report, 880,418 complaints of cybercrime were reported to the FBI by the public, a 10 percent increase from 2022 [36]. And within the law enforcement and criminal justice sector, the impact of digital forensics is ubiquitous, with over 90% of crimes having a digital element [37]. It is no surprise that the demand for these investigators is rapidly increasing, with the Bureau of Labor Statistics projecting a job outlook of 13% over the period between 2022 and 2032 [38].

While there is no single overarching entity that sets ethical guidelines for digital forensics professionals [39], various organizations have established codes of ethics based on principles of integrity, objectivity, professional care and competence, confidentiality, respect, and legal and ethical compliance [21]. Additionally, their role testifying in court, governed by U.S. Department of Justice (DOJ), holds them to high standards to aid in the deliverance of fair and legitimate justice [39]. However, despite the heavy reliance on digital forensics and the high standards placed upon professionals, they are constantly under scrutiny for not meeting expectations due to the immense challenges faced by this field [9] [31]. Therefore, it is essential to contribute to the development of the field to improve the reliability of their tools and

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024. August 11 -- 13, 2024, Philadelphia, PA, USA.

methods, which have become a cornerstone in determining justice in our world.

2. Challenges in Digital Forensics

Given the relative newness of the digital forensics field, the nature of requirements inherent to the domain, and the rapid rate of technology development and adoption, it is no surprise that the field is fraught with a multitude of challenges [19]. Synthesized from eighteen works in the digital forensics research literature works categorizing the research taxonomy in digital forensics, the challenges are broadly discussed below:

2.1 Technology challenges

The use of encryption, large amounts of diverse data to collect, incompatible forensic tools, anti-forensic technology, emergence of cloud computing all construe the technically challenging aspects of conducting forensics investigation [19]. The ever-changing technology landscape demands a constant influx of creative solutions for extracting digital evidence which require superior expertise to develop. Additionally, digital forensics professionals are either given the option to specialize in a single technology (e.g., mobile phone forensics) or bear the burden of familiarizing themselves with a myriad of tools, formats, etc. to be able to accurately conduct their investigations [1].

2.2 Shortage of qualified investigators

Recruiting, retaining, and adequately training skilled professionals presents a substantial hurdle in the industry, primarily due to factors such as the time-intensive nature of investigations, insufficient funding for on-the-job training [31][9][1], short-supply of skilled individuals, and the allure of more lucrative opportunities in other sectors [10]. Furthermore, forensics professionals often face burn-out caused by being stretched thin due to disproportionate ratio of staffing to caseload and undertaking duties beyond their digital forensic responsibilities [5][9][10]

2.3 Legal challenges

2.3.1 Know-how: Digital forensics professionals must have extensive knowledge of legislative constraints and navigate them expertly during their investigations, as any misstep could result in their evidence being rejected in court [22].

2.3.2 Admissibility of digital evidence: Any deviation from forensically-sound methodologies such as underdeveloped evidence collection and processing, tool errors, unqualified expert witnesses who are unable to clearly explain the process and technology behind the investigation, etc., often lead to evidence being deemed inadmissible in court [8][22].

2.4 Discrepancy between researchers and practitioners

An analysis of viewpoints from both researchers and real-world forensics practitioners regarding the challenges within the field highlights a notable discrepancy: while researchers prioritize emerging issues like social networking and tool capability, practitioners are preoccupied with immediate concerns such as anti-forensics, encryption, and visualization. This disconnect often results in ineffective exploration and solution-generation within the digital forensics research taxonomy [1][32].

2.5 Trust in tools

***2.5.1 Stigma of automation*:** Automation offers the potential to significantly save investigative time and effort, reduce the need for deep expertise, and standardize investigations. However, skepticism persists regarding the reliability of investigations conducted with automated tools. Concerns include the potential for missing evidence, doubts about the technical competence of tool users, and the risk of inaccurate interpretations [1][18][23].

2.5.2 Tool validation: Despite the reliance on forensic tools, the current commercial toolkit development process makes it hard to determine the accuracy of the tools being utilized due to the lack of transparency with testing procedures and results [3][16][22]. Also, error in investigations due tool limitations is often indiscernible from issues caused by user-error [13].

***2.5.3 Tool development issues*:** In their 2020 study, Wu et al. analyzed 62 forensic tools and identified several issues including lack of coding standards, limited testing, interoperability issues, and scalability issues. They also noted that many of these tools had not received maintenance after their initial development [30].

***2.5.4 Poor documentation*:** Wu et al. (2020) found that many tools lacked proper documentation; additionally, they noted that the absence of standardized documentation practices led to significant variations in the quality and quantity of the available documentation [30].

2.6 Addressing privacy

Development of laws focused on protecting user privacy [1] brings to attention the large amounts of data collected from devices that could be out of scope for the investigation and associated warrants [12]. Further, there are growing concerns about the possibility of big data analytics on the unselectively gathered information revealing insights beyond the evidentiary needs of the investigation [31]. These cause challenges with the achievement of effective investigations while navigating fundamental human right of privacy [12].

It is interesting to note that some of these challenges are not unique to the field of digital forensics. For example, the shortage of qualified professionals is a challenge affecting the broader cybersecurity domain [34]. However, certain challenges are more pronounced in digital forensics, such as the legal and regulatory hurdles, due to the pressure faced by these professionals to adhere strictly to legal guidelines.

3. Approaches in Forensics Literature

Upon analysis of the literature in digital forensics, we found a need for the development of standardized methodologies, expert certifications, and advanced technologies to overcome challenges that digital forensics professionals encounter [37]. The approaches we found in the literature are summarized below, each tied to the challenges identified above.

The approaches to alleviating *technological challenges* are focused on building new tools and updating existing ones [28]. A tremendous amount of work also exists on assisting the *professional shortage problem* through developing curricula for education [40] and standardizing forensic techniques [14]. In addressing the *legal challenges*, literature prioritizes educating forensic investigators on current laws and developing expertise in the domain [8]. Toward addressing the *issues of trust* in tools, paradigms have been proposed to validate and verify forensic software [3]. Finally, to *protect privacy*, the focus has been on overcoming encryption through backdoors [2] and the development of privacy-aware tools that can be configured to only display case-relevant data [25].

Several digital forensics process models describe the various steps and phases of a digital forensic investigation, such as Integrated Digital Forensic Process Model (IDFPM) [20]. While existing literature explores the applicability of these processes to digital forensic investigations, further research is needed to understand how digital forensic tools integrate into these models and how the interaction between different tools in each phase is facilitated. Additionally, an open question remains regarding how data is transferred between tools. Given the challenges in tool interoperability, it is crucial to explore how these issues are addressed in real-life scenarios.

We find that the totality of research literature we have analyzed so far has not sufficiently considered investigating the usability of digital forensics devices to address certain challenges in the domain. Outside the usable security research space, the benefit of improving usability of the digital forensics tools to assist with forensically-sound investigations has been largely ignored. And within the usable security research space, these benefits have not been explored thoroughly. When they are addressed, there are many unanswered questions, and the work is not followed up.

Hibshi et al. (2011) utilize a survey-based approach to identify usability problems with forensics tools [11]. However, by relying on surveys to gather opinion on forensic tool usability, the work fails to provide the necessary foundation to build usability design guidelines. In [26], Northrop and Lipford (2014) perform a qualitative interview of network forensics experts to identify issues with open-source network forensics tools and suggest guideline for future design and development. Although, the paper does categorize factors that guide decision-making related to forensic tools, they focus specifically on one open-source technology, Wireshark, which does not adequately represent all open-source and commercially available digital forensics software. Additionally, the authors only consider evaluating open-source toolkits which are known to lack sufficient resources dedicated to usability [24].

Expert tools utilized in law enforcement forensics have undergone a massive transformation in the last 20 years. Since the development of the first commercial forensics tool FTK Imager in the early 2000s, the number of commercial forensic tools available has grown to over 60 today [41]. The functionality offered with these tools has also steadily increased. However, one question remains unanswered: has the usability of digital forensics' tools kept pace?

Moreover, usability literature groups all forensic professionals together. This consolidation arises from the shared use of similar tools among professionals in various sectors, yet it overlooks the diverse job roles, tasks, and workplace environments within digital forensics.

4. Motivation

Understanding user perceptions and experiences allows for the development of usability design metrics, which can serve as guidelines for creating learnable, efficient, memorable, error-free, and pleasing tools [6]. Botta et al. (2007) conducted an ethnographic study to better understand the human, organizational, and technical aspects of IT security management [4]. By utilizing semi-structured interviews and qualitative analysis techniques, they uncovered several previously unknown characteristics and needs that define the day-to-day role of security practitioners [4]. This work was later utilized by Jaferian et al. (2011) to create a new set of domain-specific heuristics for IT security tools, addressing various aspects of their usage [17].

However, gauging the usability of law enforcement forensics tools using current literature is challenging, as digital forensics professionals and their tools have been understudied in existing research. Furthermore, we believe there is a lack of literature aimed at obtaining a holistic view of digital forensics professionals in law enforcement, while similar studies exist for IT security professionals [4] and incident response specialists [30].

Additionally, we propose that several challenges within the domain can be alleviated by improving the usability of digital forensics software. Therefore, it is critical to collaborate with digital forensics professionals in the law enforcement sector to gain an insiders' view of their workplace and tools.

4. Research Question

By performing our study on digital forensics professionals in law enforcement, we aim to understand the following:

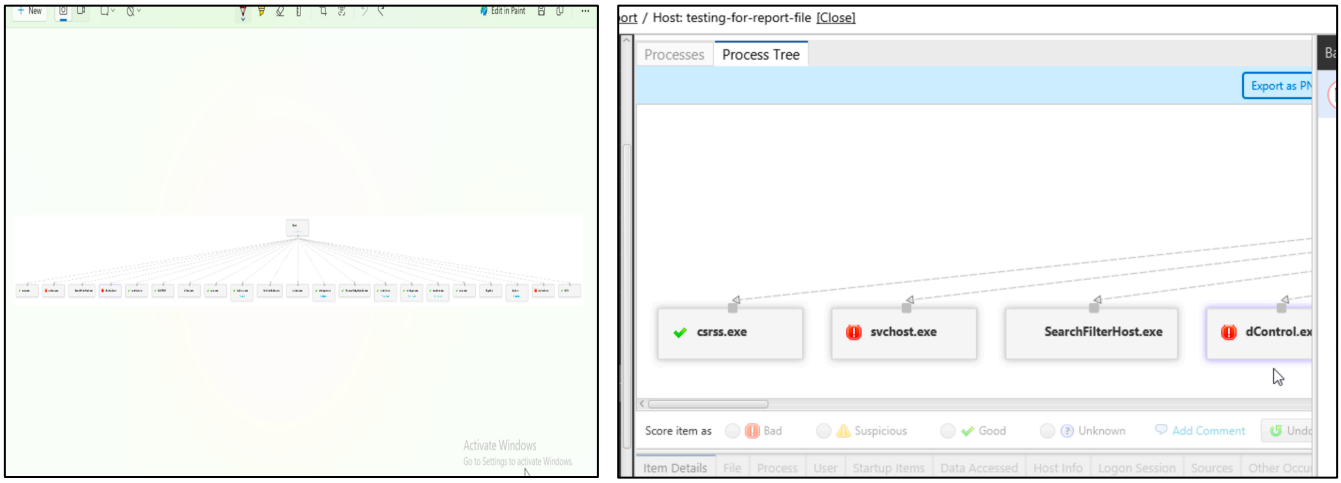

Figure 1a: Exported process tree image file from Cyber Triage. Figure 1b: The process tree as viewed within the Cyber Triage application.
The exported image file format does not allow for a zoom-in to view each branch of the process tree. When viewed within Cyber Triage, there is no option to view the entire tree in a single window.

- ***RQ 1 -*** *How does the intersection of the workplace and tools of digital forensics play out?*
- ***RQ 2 -*** *What are digital forensics professionals satisfied with? What do they feel is lacking?*
- ***RQ 3 -*** *What gaps and challenges exist that can be addressed by usable tools**?***

To achieve this, we developed a three-phase research project to explore usability challenges and solutions for digital forensics professionals. Section 4 will detail the phases of our research.

5. Initial Heuristic Evaluation

The first step in our research work involved performing a heuristic evaluation of a state-of-the-art, popular digital forensics tool utilizing the Nielsen Norman Group's 10 Usability Heuristics for User Interface Design [6]. We performed this evaluation to (1) assess the usability of digital forensics tools in 2024 and (2) determine if Nielsen's heuristics adequately capture all user interface issues with the forensic tool.

We evaluated Cyber Triage—an automated digital forensics and incident response tool for malware analysis, ransomware and account hijacking investigations [42]. We selected Cyber Triage as our commercial forensic toolkit for conducting the heuristic evaluation as Sleuth Kit Labs, our industry collaborators, generously provided us with a complimentary copy of the software. Furthermore, Sleuth Kit Labs also supplied the necessary mock evidence data. The identified usability issues were rated on a scale from 1 (cosmetic issue) to 4 (usability catastrophe). While we did not identify any issues with a severity rating of 4, we found six usability issues rated as 3 (major usability issue), four rated as 2 (minor usability issue), and seven rated as 1.

Furthermore, we found that Nielsen's heuristics were not sufficient for identifying all usability issues. We encountered several issues that could not be categorized into any of the ten heuristics. One of the issues identified showed that Cyber Triage did not allow for the proper viewing of visualizations within the application, and any exported image file did not render a serviceable visualization either [Figure 1].

However, we were unable to define this issue as a separate, new heuristic due to a lack of literature supporting the necessity of such a heuristic. Specifically, we were uncertain whether digital forensics professionals relied on tools for their visualizations or if such visualizations were valued in investigations. This uncertainty prompted us to develop the interview study for Phase 1 of our research plan, aiming for a deeper understanding of the interaction between digital forensics professionals and their tools.

Our objective with the heuristic evaluation was not merely to uncover issues with digital forensic software, but rather to verify that we had identified issues that did not adhere to Nielsen's established heuristics. While we could have continued performing heuristic evaluations on other forensic toolkits to further pinpoint issues that do not align with Nielsen's heuristic list, we found that focusing on one toolkit, supplemented by literature reviews and informal discussions with industry and government partners, allowed us to adequately recognize the necessity for domain-specific heuristics. However, this approach also has limitations, as we lack

sufficient data to determine how frequently such issues recur across various toolkits.

5. Proposed Plan of Research

For our work, we rely on three data sources: literature reviews, interviews with digital forensics professionals focused on understanding the intersection of their tools and workplace requirements, and insights from heuristic evaluation of forensics toolkits. This agenda is divided into three phases as follows:

5.1 Phase 1: Interview study with digital forensics professionals

During Summer 2024, we will undertake a semi-structured interview study aimed at exploring the workplace environment, tools used, and their integration into digital forensics workflows. The necessary Institutional Review Board (IRB) materials have been submitted and approved in accordance with the university's guidelines.

We aim to recruit participants who either currently work and/or have previously worked in law enforcement in a digital forensics-related role, have experience with digital forensics software toolkits, are 18 years and older, and located in the United States. Additionally, we will strive to achieve a reasonably diverse participant sample that accurately represents the gender and education demographics within the domain of digital forensics. Each participant will receive a $50 Amazon e-gift card upon completing the interview.

During the interview, participants will be asked about their journey and background in digital forensics, including their specialized education, training, and current role. Questions will also delve into their workflow, tool usage, challenges they face, experiences with privacy concerns, team dynamics, and perspectives on the tools they use, as well as what they find most rewarding about their work.

Upon completion of the interviews, qualitative analysis techniques will be used to analyze the transcripts and answer the study questions.

Conducting this interview study will provide us with the opportunity to identify how the challenges identified by the computer forensics research community manifest in the cases encountered by digital forensic professionals. Based on our analysis of current literature, heuristic evaluation using Nielson's heuristics, and informal conversations with forensic investigators in law enforcement, we list below a few of the several potential working hypotheses that hold ground.

5.2.1 H1: Digital forensics tools must generate usable reports

For criminal investigation and trial proceedings, the importance of forensics reports in collaboration, communication, and legal proceedings cannot be overstated. For example, a poor report could undermine the quality of an investigation and lead to the evidence collected deemed inadmissible in court [15]. Therefore, it is important that tools automate the process of produce these reports for utmost accuracy. They must also allow for the reports to be configurable based on the needs of the investigator such as legal requirements.

5.2.2 H2: Digital forensics tools should offer thoughtful freedom

Northrop and Lipford (2014) report that one reason forensic professionals choose open-source tools is the flexibility and user control they offer. This freedom includes filters for data, integration options with other tools, and support for different protocols. However, it's worth noting that excessive control and freedom could overwhelm users. Moreover, this feeling of overload could make the tool more challenging for novice users, leading to errors [26]. Therefore, it is necessary for developers to be cognizant of the needs of digital forensics professionals to allow for freedom of use without stifling performance.

5.2.3 H3: Digital forensics tool should offer utmost system visibility

Offering investigators complete visibility into the system and the modifications occurring to the evidence within it would address the challenges of lack of legal and investigator trust in tools [13]. It would also assist in the creation of audit trails and reduce misconfiguration of tools due to the increased transparency offered [26]. Additionally, it would help address issues hindering the admissibility of forensic evidence in court due to data collection and interpretation issues [8].

5.2.4 H4: Digital forensics tools should address the right to privacy

Given the current evidence seizure procedures, expecting law enforcement to collect only case-relevant data is impractical [25]. Therefore, the endeavor to safeguard the privacy of innocent individuals' data must be addressed during the evidence analysis process in forensics tools. This may entail integrating privacy measures into the tool design, such as implementing access control, concealing irrelevant portions of evidence, and establishing comprehensive logging of all access to the collected evidence.

5.2.5 H5: Digital forensics tools should offer visualization

The benefits of using visualizations to analyze large quantities of data are well-established. In digital forensics, where vast amounts of data are collected as evidence, there is a growing need for novel visualization techniques to aid investigators in their analysis [27]. This can be accomplished by designing visualizations specifically for identifying and distilling irrelevant data.

5.2.6 H6: Digital forensics tools must be documented thoroughly

Forensic evidence faces rejection in court if the testifying investigator cannot adequately furnish technical details regarding the evidence, methodologies, and tools employed in the investigation [32]. Additionally, the absence of published testing results for these applications poses a challenge to establishing the scientific validity of the investigative process

[3]. Furthermore, as automation becomes more prevalent in forensics, it becomes crucial for investigators to comprehend the operations of the systems handling the evidence [18]. Consequently, investigators must possess a fundamental understanding of the tools they utilize, which necessitates comprehensive and thorough documentation.

Future work will include substantiating these hypotheses with established literature in HCI. These hypotheses do not encompass every potential theme identified in our literature reviews and informal discussions. Instead, they represent the recurring themes that were most prominent during our initial planning for the interview study.

5.2 Phase 2: Develop usability metrics

Nielson's heuristics don't cover all the needs of digital forensics professionals. Thus, the development of separate domain-specific heuristics is necessitated. Our literature analysis and informal conversations have indicated that certain challenges like documentation, report generation, lack of training, and increasing trust in tools can be addressed with usable software. In this phase, we will develop the heuristics to provide more tailored guidance for improving the usability of digital forensics tools.

5.3 Phase 3: Perform Heuristic Evaluation

After understanding the requirements of digital forensics professionals and developing specialized, domain-specific heuristics for evaluating the usability of digital forensics tools, we will undertake a study to test the heuristics by recruiting digital forensics professionals in law enforcement to evaluate multiple forensic tools. This process will aim to refine a comprehensive list of tested heuristics.

6. Future Work

To summarize the above, we see a need for future work in understanding the experiences of digital forensics professionals to empathize with them. Our next steps will be to begin recruitment and conduct interviews for Phase 2 of our research. Additionally, we will continue to perform literature reviews in the digital forensics and HCI domain to ground our research in established literature. We plan on publishing the qualitative analysis of the interview. Next, we will move on to developing domain-specific heuristics for evaluating forensics tools.

7. Conclusion

By examining prior work on the challenges in digital forensics and engaging in informal conversations with digital forensics professionals, we gained insights that underscored the importance of improving usability to overcome these challenges. This paper reviewed existing literature on digital forensics in law enforcement and analyzed common challenges such as technology, professional shortages, legal hurdles, collaboration between researchers and practitioners, and privacy issues. We then presented our plan for future work, which involves collaborating with digital forensics professionals to identify how software tool usability affects investigative performance. Additionally, we proposed six hypotheses based on our analysis and conversations, which we believe will emerge within our interviews. We aim for our work to contribute to the development of usability standards for digital forensics software used in law enforcement.

Acknowledgement

We would like to thank our industry and government sponsors for their financial support and advice to date.

References

1. M. Al Fahdi, N.L. Clarke, and S.M. Furnell. 2013. Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. In *2013 Information Security for South Africa*, 1–8. https://doi.org/10.1109/ISSA.2013.6641058
2. Adedayo M. Balogun and Shao Ying Zhu. 2013. Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology. https://doi.org/10.48550/arXiv.1312.3183
3. Jason Beckett and Jill Slay. 2007. Digital Forensics: Validation and Verification in a Dynamic Work Environment. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 266a–266a. https://doi.org/10.1109/HICSS.2007.175
4. David Botta, Rodrigo Werlinger, André Gagné, Konstantin Beznosov, Lee Iverson, Sidney Fels, and Brian Fisher. 2007. Towards understanding IT security professionals and their tools. In *Proceedings of the 3rd symposium on Usable privacy and security* (SOUPS '07), 100–111. https://doi.org/10.1145/1280680.1280693
5. Alexa Dodge, Dale Spencer, Rose Ricciardelli, and Dale Ballucci. 2019. "This isn't your father's police force": Digital evidence in sexual assault investigations. *Australian & New Zealand Journal of Criminology* 52, 4: 499–515. https://doi.org/10.1177/0004865819851544
6. World Leaders in Research-Based User Experience. 10 Usability Heuristics for User Interface Design. *Nielsen Norman Group*. Retrieved May 21, 2024 from https://www.nngroup.com/articles/ten-usability-heuristics/
7. Oxygen Forensics. 2023. What is Digital Forensics? *Oxygen Forensics*. Retrieved May 22, 2024 from https://oxygenforensics.com/en/resources/what-is-digital-forensics/
8. Daniel B. Garrie. 2014. Digital Forensic Evidence in the Courtroom: Understanding Content and Quality.

Northwestern Journal of Technology and Intellectual Property 12: 121.
9. Greg Gogolin. 2010. The Digital Crime Tsunami. *Digital Investigation* 7, 1: 3–8. https://doi.org/10.1016/j.diin.2010.07.001
10. Diarmaid Harkin, Chad Whelan, and Lennon Chang. 2018. The challenges facing specialist police cybercrime units: an empirical analysis. *Police Practice and Research* 19, 6: 519–536. https://doi.org/10.1080/15614263.2018.1507889
11. Hanan Hibshi, Timothy Vidas, and Lorrie Cranor. 2011. Usability of Forensics Tools: A User Study. In *2011 Sixth International Conference on IT Security Incident Management and IT Forensics*, 81–91. https://doi.org/10.1109/IMF.2011.19
12. Ilyoung Hong, Hyeon Yu, Sangjin Lee, and Kyungho Lee. 2013. A new triage model conforming to the needs of selective search and seizure of electronic evidence. *Digital Investigation* 10, 2: 175–192. https://doi.org/10.1016/j.diin.2013.01.003
13. Graeme Horsman. 2018. "I couldn't find it your honour, it mustn't be there!" – Tool errors, tool limitations and user error in digital forensics. *Science & Justice* 58, 6: 433–440. https://doi.org/10.1016/j.scijus.2018.04.001
14. Graeme Horsman. 2021. Standardizing digital forensic examination procedures: A look at Windows 10 in cases involving images depicting child sexual abuse. *WIREs Forensic Science* 3, 6: e1417. https://doi.org/10.1002/wfs2.1417
15. Graeme Horsman. 2021. The different types of reports produced in digital forensic investigations. *Science & Justice* 61, 5: 627–634. https://doi.org/10.1016/j.scijus.2021.06.009
16. Graeme Horsman. 2024. Sources of error in digital forensics. *Forensic Science International: Digital Investigation* 48: 301693. https://doi.org/10.1016/j.fsidi.2024.301693
17. Pooya Jaferian, Kirstie Hawkey, Andreas Sotirakopoulos, Maria Velez-Rojas, and Konstantin Beznosov. 2011. Heuristics for evaluating IT security management tools. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (SOUPS '11), 1–20. https://doi.org/10.1145/2078827.2078837
18. Joshua I. James and Pavel Gladyshev. 2013. Challenges with Automation in Digital Forensic Investigations. https://doi.org/10.48550/arXiv.1303.4498
19. Nickson M. Karie and Hein S. Venter. 2015. Taxonomy of Challenges for Digital Forensics. *Journal of Forensic Sciences* 60, 4: 885–893. https://doi.org/10.1111/1556-4029.12809
20. M. D. Kohn, M. M. Eloff, and J. H. P. Eloff. 2013. Integrated digital forensic process model. *Comput. Secur.* 38: 103–115. https://doi.org/10.1016/j.cose.2013.05.001
21. Lucifer. 2023. Role of Ethics in Digital Forensics : A Digital Code of Conduct. *Forensics Insider*. Retrieved May 22, 2024 from https://www.forensicsinsider.com/digital-forensics/ethics-in-digital-forensics/
22. Rebecca Mercuri. 2010. Criminal Defense Challenges in Computer Forensics. In *Digital Forensics and Cyber Crime*, 132–138. https://doi.org/10.1007/978-3-642-11534-9_13
23. Christa M. Miller. 2022. A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy* 6: 100296. https://doi.org/10.1016/j.fsisyn.2022.100296
24. David M. Nichols and Michael B. Twidale. 2006. Usability processes in open source projects. *Software Process Improvement and Practice* 11, 2: 149–162. https://doi.org/10.1002/spip.256
25. Ana Nieto, Ruben Rios, Javier Lopez, Wei Ren, Lizhe Wang, Kim-Kwang Raymond Choo, and Fatos Xhafa. 2019. Privacy-aware digital forensics. In *Security and Privacy for Big Data, Cloud Computing and Applications*. IET Digital Library, 157–195. https://doi.org/10.1049/PBPC028E_ch8
26. Erik E. Northrop and Heather R. Lipford. 2014. Exploring the Usability of Open Source Network Forensic Tools. In *Proceedings of the 2014 ACM Workshop on Security Information Workers* (SIW '14), 1–8. https://doi.org/10.1145/2663887.2663903
27. Grant Osborne and Benjamin Turnbull. 2009. Enhancing Computer Forensics Investigation through Visualisation and Data Exploitation. In *2009 International Conference on Availability, Reliability and Security*, 1012–1017. https://doi.org/10.1109/ARES.2009.120
28. Ameer Pichan, Mihai Lazarescu, and Sie Teng Soh. 2015. Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation* 13: 38–57. https://doi.org/10.1016/j.diin.2015.03.002
29. Mark Pollitt. 2010. A History of Digital Forensics. In *Advances in Digital Forensics VI*, 3–15. https://doi.org/10.1007/978-3-642-15506-2_1
30. Janine L Spears. Job Stress in the Cybersecurity Incidence Response Work Role.
31. Eva A. Vincze. 2016. Challenges in digital forensics. *Police Practice and Research* 17, 2: 183–194. https://doi.org/10.1080/15614263.2015.1128163
32. Tina Wu, Frank Breitinger, and Stephen O'Shaughnessy. 2020. Digital forensic tools: Recent advances and enhancing the status quo. *Forensic Science International: Digital Investigation* 34: 300999. https://doi.org/10.1016/j.fsidi.2020.300999
33. 2016. Digital evidence. *NIST*. Retrieved May 21, 2024 from https://www.nist.gov/digital-evidence
34. 2024. The cybersecurity industry has an urgent talent shortage. Here's how to plug the gap. *World Economic Forum*. Retrieved July 7, 2024 from https://www.weforum.org/agenda/2024/04/cybersecurity-industry-talent-shortage-new-report/
35. Cyber Defense Forensics Analyst | CISA. Retrieved May 22, 2024 from https://www.cisa.gov/careers/work-rolescyber-defense-forensics-analyst

36. FBI Releases Internet Crime Report. *Federal Bureau of Investigation*. Retrieved May 22, 2024 from https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-releases-internet-crime-report
37. National Policing Digital Strategy – Police Digital Service. Retrieved May 22, 2024 from https://pds.police.uk/national-policing-digital-strategy-2020/
38. Forensic Science Technicians. *Bureau of Labor Statistics*. Retrieved May 21, 2024 from https://www.bls.gov/ooh/life-physical-and-social-science/forensic-science-technicians.htm
39. Computer Forensics: Legal and Ethical Principles | Infosec. Retrieved May 22, 2024 from https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-legal-ethical-principles/
40. Fostering an "investigating mindset": Why is it important in digital forensic science education? - Horsman - 2024 - WIREs Forensic Science - Wiley Online Library. Retrieved May 21, 2024 from https://wires.onlinelibrary.wiley.com/doi/full/10.1002/wfs2.1511
41. Forensics Wiki - Tools. Retrieved July 7, 2024 from https://forensics.wiki/
42. Fast & Affordable Digital Forensics Tool for Incident Response. *Cyber Triage*. Retrieved May 21, 2024 from https://www.cybertriage.com/