Usability of Digital Forensics: A New Approach Inspired by Usable Security

Tobias Hoppmann and Zinaida Benenson

Department of Computer Science, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Erlangen, Germany

Abstract. The field of usable security led to numerous improvements in IT security by anticipating and integrating users' requirements, motivations, and behaviors. Many successful enhancements arose from simple or unconventional adjustments to workflows, enabled by considering user context, capacities, and needs.

One important area of IT security remains largely untouched by these insights: digital forensics. Despite significant technological and methodological advances over the past decades, many challenges in this field persist or have intensified. In particular, within criminal proceedings, the perspectives of users and stakeholders, as well as the broader contextual factors, are often overlooked in favor of a narrow focus on evidence- or case-specific issues, leaving workflow and user needs unaddressed.

This paper provides a brief overview of the emerging research field of the *usability of digital forensics in criminal proceedings*, which integrates concepts of usability and usable security to address systemic challenges faced by digital forensics within its interdisciplinary and complex context. We outline key challenges, the current state of research, the potential for integration of the proposed model into digital forensics, and prospects for future developments.

Keywords: digital forensics · usable security · usability

1 Introduction

For more than 25 years, research in the field of usable security has focused on how to improve the usability of tools, interfaces, and processes. Its findings have increasingly been transferred to new contexts, for example by Acar et al. [1], who extend usable security to developer-centered security. In a similar vein, this paper informs an emerging and closely related field within IT security: the usability of digital forensics in the context of criminal proceedings.

Due to the social significance and impact of criminal proceedings, new solutions must be found to overcome the numerous challenges in digital forensics.

This work is licensed under a Creative Commons "Attribution 4.0 International" license. To view a copy of this license visit https://creativecommons.org/licenses/by/4.0/deed.en.
©2026 Copyright held by the owner/author(s).

Examining digital forensics together with criminal proceedings from a usability perspective represents a novel approach to addressing these challenges by adopting a systemic, rather than case- or evidence-focused, viewpoint. In this paper, we present some important challenges as well as the concept behind the usability of digital forensics in criminal proceedings and show the directions in which this field could develop in the future.

2 Challenges of Digital Forensics in Criminal Proceedings

Digital forensics and digital evidence play an increasingly important role in criminal proceedings [8]. At the same time, the field faces growing challenges which no longer seem to be manageable by technological approaches alone, including increasing data volumes, backlogs, the expanding diversity of hardware and software, the migration of data to cloud environments that span multiple legal jurisdictions and the demand for rapid provision of results [6, 8, 9, 17].

Criminal proceedings add further complexity through the involvement of diverse actors who collect digital evidence, conduct investigations, or rely on digital forensic results for decision making. Effective prosecution therefore depends on the interaction between digital forensic experts and these stakeholders [17], yet this relationship is not sufficiently examined. A likely reason is the strong orientation of digital forensics toward classical forensics and its historical framework as an analytical laboratory discipline, in which quality is primarily defined by methodological rigor and minimization of human influence [8, 19].

Tools and methods from digital forensics are used not only by forensic experts but also by investigators and other practitioners in criminal proceedings. Prosecutors, defense attorneys, and judges primarily engage with forensic results and increasingly digital evidence and related tools. Due to the high number of cases and the routine presence of digital evidence at crime scenes, evidence preservation is often carried out by minimally trained or untrained personnel rather than forensic experts [4, 12, 23].

As a result, criminal proceedings involve numerous interfaces with highly heterogeneous user groups with regard to digital skills, such as police officers, investigators, prosecutors, attorneys, judges, and digital forensic experts. Hibshi et al. [11] examined the usability of various digital forensic software tools in a study that combined interviews with digital forensic experts and a survey with participants of different backgrounds and technical knowledge. They found that the tools are not user-friendly or intuitive to use and do not support much collaborative work, which can easily lead to misinterpretations and negative impacts on cases. They also discovered that participants had different requirements in terms of simplicity and range of functions.

Further research by Roux et al. [19] and Wilson-Kovacs [23] documents instances of frictions between some of these groups and attributes them to factors embedded in broader organizational, procedural, and integrative contexts. Her work emphasizes the importance of a holistic perspective that considers all processes within criminal proceedings. Furthermore, Roux et al. [19] highlight the

scarcity of empirical research on forensic science in general and argue that its contribution, effectiveness, and efficiency are rarely examined within a comprehensive contextual framework.

Recent studies highlight the growing significance of human factors and collaboration between different user groups in digital forensics. Cognitive bias has been shown to influence forensic decision making across all phases of the process [18, 21], while structural shifts toward decentralized forensic units reflect increasing operational demands [6]. Technological developments such as *Digital Forensics as a Service (DFaaS)* further facilitate cooperation, joint investigations, and broader access to forensic results for stakeholders, including prosecutors and judges [3].

An increasingly important issue in digital forensics concerns stress responses, which can affect not only individual well being but also cognitive performance. Kelty et al. [15] report that digital forensic practitioners are frequently exposed to challenging material and high volumes of evidence, which can result in job strain, burnout, or secondary traumatic stress. Their findings indicate that supportive and resilient leadership, effective work environments, reduced exposure durations, and the provision of stress related leave represent promising organizational measures for these challenges.

Similarly to the findings of Adams and Sasse [2], many of these challenges have the potential to cause errors, misunderstandings, friction, and stress, highlighting the need for improved usability, better mutual understanding, and better coordination of organizational and work processes. In criminal proceedings, digital forensics interacts with various other disciplines, organizational structures, laws, and user groups, requiring additional knowledge, effort, and adaptation.

3 The Concept of Usability in Digital Forensics

To describe our understanding of the usability of digital forensics in criminal proceedings, we first outline the concepts introduced in Hoppmann et al. [13], our initial paper on this topic. We then extend this approach by examining how the proposed model can be embedded within the broader ecosystem of digital forensics and by providing a brief overview of the challenges arising from the complex interplay between digital forensics and criminal proceedings. As a point of departure, we begin by presenting the definition of the usability of digital forensics in criminal proceedings:

Definition 1 (Usability of Digital Forensics in Criminal Proceedings). *The extent to which digital forensic principles, methods, tools, and the presentation of their results can be used by the parties involved to contribute to the overarching goal of establishing the truth in criminal proceedings as comprehensively as possible, considering effectiveness, efficiency, and satisfaction.*

The presented definition is based on the fundamental definitions of digital forensics according to Palmer [16] and usability by ISO/IEC 9241-11 [14] and

combines these with the overarching goal of uncovering the truth as comprehensively as possible in the context of criminal proceedings. Although this objective derives from German law, it seems to adequately reflect the overarching purpose of criminal proceedings in other constitutional systems as well. Focusing on the purpose of criminal proceedings also corresponds to calls for greater consideration of the investigation process alongside court proceedings (both of which are part of criminal proceedings), as advocated by Roux et al. [19], for example. The use of the term "contribution" clarifies that this goal cannot be achieved solely or exclusively through digital forensics. At the same time, it appears to be a suitable guiding principle for digital forensics and digital investigations.

The definition's openness with regard to various parties involved in criminal proceedings makes it possible to apply the approach in different legal systems and to involve a wide range of actors in criminal proceedings. In addition, it is emphasized that the concept must be considered in light of the ISO 2018 usability criteria, taking into account effectiveness, efficiency, and satisfaction.

3.1 The Adaption of Usable Security Design Criteria

In addition to the applicability of the three usability criteria, effectiveness, efficiency and satisfaction, we showed in [13] that five design criteria for usable security derived from the work of Sasse et al. [20] can be transferred to digital forensics. These include tasks and goals, capabilities and limitations of users, capabilities and limitations of technologies, social as well as physical context. Although the capabilities and limitations of users and technologies can be transferred without difficulties, we need to extend the social context with a legal dimension and the physical context with a virtual context. In the specific context of criminal proceedings, legal requirements, such as laws, organizational dependencies, and procedural rules, play a substantially stronger role and should therefore be considered on equal footing with the social context. Additionally, extending the physical context to include a virtual context appears appropriate to better distinguish, for example, physical and virtual work environments such as crime scenes or cooperative DFaaS working environments.

In comparison, tasks and goals are identified as the decisive factor that distinguishes usable security from the usability of digital forensics in criminal proceedings. Whereas IT security measures typically represent secondary tasks and goals, digital forensic activities in criminal proceedings directly contribute to the primary tasks and goals of criminal proceedings included by the definition. Due to the contribution to uncovering the truth assumed in the definition, digital forensics and its tasks and goals become a primary contribution, regardless of the decision of the parties in the court proceedings to introduce its results. Therefore, we classify tasks and goals, together with the usability criteria of effectiveness, efficiency, and satisfaction, as core criteria that must always be considered when assessing the usability of digital forensics in the context of criminal proceedings.

3.2 Subdivision of Usable Digital Forensics

The field of usable digital forensics becomes significantly broader when situated within the even more comprehensive context of criminal proceedings. Beyond the already extensive scope of digital forensics itself, we proposed a division into three sub-aspects: human, technical, and organizational [13], visualized in Figure 1.

As illustrated there, the extended design criteria presented in Section 3.1 can be systematically mapped onto these three sub-aspects. The capacities and limitations of users and technologies are assigned to the human and technical aspects, respectively. In contrast, the two more environmental and contextual criteria are associated with the organizational aspect, where they are aligned more closely to human- or technology-centered considerations.

However, this subdivision must not be interpreted as absolute, as the majority of problems in digital forensics incorporate aspects of all three domains. Instead, classification should be conceptualized as a relative positioning within a continuous problem space spanned by the three domains, as shown in Figure 1, in which individual problems exhibit varying degrees of alignment with each domain.

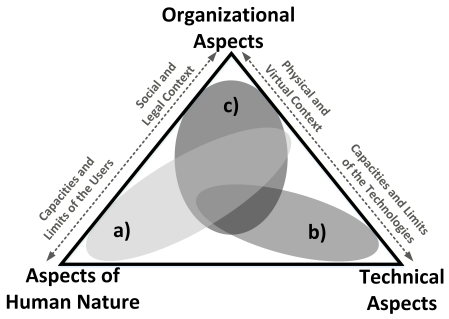

Fig. 1: Exemplary presentation of the coverage of various digital forensics issues (a to c) within a spectrum of organizational, human, and technical aspects.

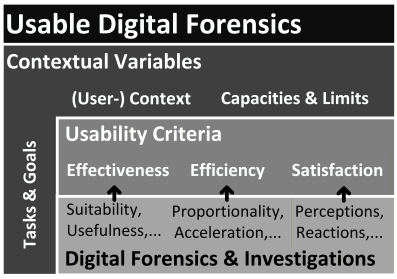

Fig. 2: Presentation of usability in digital forensics as additional layers and the transition from digital forensics requirements to the three usability criteria.

3.3 Usable Digital Forensics as an Additional Layer

Although the proposed definition is grounded in a strong theoretical foundation, we believe that the model remains susceptible to potential misconceptions. These include the conflation of *usability* and *usefulness*, as well as possible concerns that applying usability principles might negatively affect the quality of digital

forensics, which holds a central position within forensic practice [19]. In the following, we will show that these misunderstandings can be dispelled by presenting usability as an additional layer above digital forensics and investigations, as illustrated in Fig. 2.

To clarify the distinction between usability and usefulness, we argue that usability refers to the interaction between users and a system, while usefulness refers to the actual needs of users to achieve their individual and case-specific goals [22]. This understanding aligns with terminology commonly used in the fields of usability [14] and digital forensics, as reflected, for example, in the work of Gruber et al. [10] on the usefulness of phenomenon-specific knowledge of cybercrime in digital investigations. The concept of usability of digital forensics in criminal proceedings focuses more strongly on technological and organizational interfaces as well as on the capacities and limitations of users and technologies, with the criminal proceeding serving as the unifying context. This perspective is therefore systemic rather than case- or evidence-specific.

If the two concepts are conflated, for example, when usability is equated with usefulness for a particular party, concerns may arise that usability could undermine the requirements of digital forensics. Digital forensics is governed by numerous requirements, such as objectivity, reproducibility, traceability, and preservation of integrity and authenticity [5]. In contrast, usefulness may vary substantially between parties, for instance, with regard to the value of digital evidence for the prosecution or defense in court. Both, general quality criteria and party specific usefulness, can be understood as measures of goal attainment and thus of effectiveness. To distinguish between them more clearly, we refer to the former as suitable quality criteria and to the latter as useful quality criteria. In this sense, it seems important to clarify that when we use the term "suitability," we are arguing about whether the object of consideration is a good fit for the nonpartisan goals of criminal proceedings.

Comparable conceptual relationships can also be identified for the two remaining usability criteria: efficiency and satisfaction. Efficiency allows the integration of considerations related to effort and resource use with legal requirements such as proportionality and principles of acceleration and satisfaction adds a dimension that captures user expectations and diverse user responses, including physical, cognitive, and emotional reactions.

We therefore argue that the requirements of digital forensics can be mapped onto the three usability criteria, which reorganize these requirements and make them accessible for usability analysis without altering their core substance. From our perspective, usability criteria and contextual factors, such as tasks and goals, as well as the contexts, capacities, and limitations presented in Section 3.1, represent additional layers above digital forensics and investigations. By basing itself upon digital forensics and investigations, the core principles of these fields remain unaffected by the concept of usability. However, the challenge of this approach lies in correctly transferring criteria and problems to the domain of usability.

3.4 The Challenge of Complexity

Another key distinction between usable security and the usability of digital forensics lies in the degree of interdisciplinary complexity. Although both domains are inherently interdisciplinary, applying usability to digital forensics further amplifies this complexity.

In classical digital forensics, forensic science and computer science are considered foundational scientific disciplines, complemented by digital investigations as both a practical origin and a field of research [7]. The inclusion of usability and usable security research, as well as the context of criminal proceedings, introduces new influences from previously external disciplines ranging from law and cybercriminology to neuroscience. Integrating these diverse concepts into a single field of research is undoubtedly a challenge. At the same time, the almost universal applicability of usability research offers the opportunity to serve as an interface between these fields.

Although we primarily focused our definition of usable digital forensics in criminal proceedings (Definition 1) on the theoretical and scientific areas of forensics and computer science, this approach requires further development in the direction of digital investigations in order to promote greater integration into criminal proceedings. Investigation is a key part of criminal proceedings, especially when it comes to incorporating more user groups, such as police investigators or prosecutors, into digital forensic processes. Figure 3 shows the different scientific influences and, by adjusting the perspective of the graphic, illustrates the need to continue to evolve the approach to incorporating digital investigations.

4 Conclusion

Digital forensics faces increasing technical, organizational, and human challenges in criminal proceedings. This paper provides a brief overview of some of these challenges and outlines the core idea underlying the usability of digital forensics in criminal proceedings. Although the proposed concept is still at an early stage, it offers a structured overview of the field that goes beyond tool usability and explicitly accounts for organizational and human factors.

The perspective enabled by this concept moves beyond evidence-focused and case-specific views and appears increasingly necessary, as fundamental challenges such as backlogs continue to intensify despite advances in digital forensics, while new challenges are likely to emerge, for example through the growing potential for interdisciplinary collaboration enabled by DFaaS.

In addition to highlighting the definition proposed by Hoppmann et al. [13], which is based on established principles of digital forensics, usability, and criminal proceedings, we describe the adaptation of the usability principles and the design criteria derived from the work of Sasse et al. [20] and how it differs from these. Furthermore, we demonstrate how this concept can be embedded within digital forensics in criminal proceedings and discuss the dimensions of complexity that characterize this research area in this context.

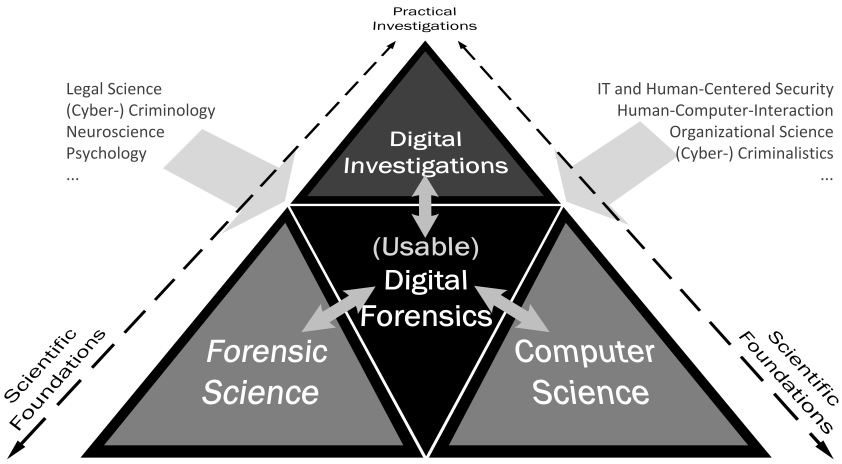

Fig. 3: Presentation of the core scientific foundations of digital forensics: forensic science, computer science, and digital investigations. The perspective distortion suggests that usable digital forensics must continue to develop in the direction of digital investigations. In addition, the influences of previously external scientific areas, which must also be considered in the usable digital forensics approach, are indicated.

The model and the definition of usability of digital forensics in criminal proceedings provide a robust foundation as well as clear points of departure for targeted further development. In particular, a more fine-grained differentiation of the three aspects of human, technological, and organizational nature enables the systematic structuring of the relevant domains that contribute to usability in this context. Based on this, appropriate methods for evaluating usability can be selected and applied. In addition, the integration of digital investigations into the model and the empirical demonstration of its applicability represent key avenues for extension. In summary, these approaches offer promising and substantial perspectives for future research in this field.

The presented concept has the potential to address a range of systemic challenges in digital forensics by focusing analysis on effectiveness, efficiency, and satisfaction. This includes, for example, organizational issues in workflow, technical aspects such as tool usability, and human factors, including the need to mitigate stress responses.

We hope that our research will also inspire scholars from various disciplines to explore usability in the broader context of criminal proceedings as a means of addressing challenges in digital forensics, just as we were inspired by research in the field of usable security to develop the concepts presented here.

References

[1] Acar, Y., Fahl, S., Mazurek, M.L.: You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users. 2016 IEEE Cybersecurity Development (SecDev pp. 3–8 (2016), https://doi.org/10.1109/SecDev.2016.013

[2] Adams, A., Sasse, M.A.: Users are not the enemy. Communications of the ACM **42**(12), 40–46 (1999), ISSN 0001-0782, https://doi.org/10.1145/322796.322806

[3] van Baar, R.B., van Beek, H., van Eijk, E.J.: Digital Forensics as a Service: A game changer. Digital Investigation **11**, S54–S62 (2014), ISSN 17422876, https://doi.org/10.1016/j.diin.2014.03.007

[4] Bossler, A.M., Holt, T.J.: Patrol officers' perceived role in responding to cybercrime. Policing: An International Journal of Police Strategies & Management **35**(1), 165–181 (2012), ISSN 1363-951X, https://doi.org/10.1108/13639511211215504

[5] Casey, E.: Digital evidence and computer crime: Forensic science, computers and the Internet. Elsevier Acad. Press, Amsterdam, 3rd ed. edn. (2011), ISBN 978-0-12-374268-1

[6] Casey, E., Ribaux, O., Roux, C.: The Kodak Syndrome: Risks and Opportunities Created by Decentralization of Forensic Capabilities. Journal of forensic sciences **64**(1), 127–136 (2019), https://doi.org/10.1111/1556-4029.13849

[7] Dewald, A., Freiling, F.C.: From Computer Forensics to Forensic Computing: Investigators Investigate, Scientists Associate. 2191-

5008 (2014), ISSN 2191-5008, URL https://open.fau.de/items/59207fb2-3139-4cd5-8bc7-3b187a85667b/full

[8] Garfinkel, S.L.: Digital forensics research: The next 10 years. Digital Investigation **7**, S64–S73 (2010), ISSN 17422876, https://doi.org/10.1016/j.diin.2010.05.009

[9] Garfinkel, S.L.: Digital Forensics Past and Future (2022), URL https://simson.net/ref/2022/2022-06-10.pdf

[10] Gruber, J., Voigt, L.L., Benenson, Z., Freiling, F.C.: Foundations of cybercriminalistics: From general process models to case-specific concretizations in cybercrime investigations. Forensic Science International: Digital Investigation **43**, 301438 (2022), ISSN 26662817, https://doi.org/10.1016/j.fsidi.2022.301438

[11] Hibshi, H., Vidas, T., Cranor, L.: Usability of Forensics Tools: A User Study. In: Morgenstern, H. (ed.) 2011 Sixth International Conference on IT Security Incident Management and IT Forensics (IMF 2011), pp. 81–91, IEEE, Piscataway, NJ (2011), ISBN 978-1-4577-0146-7, https://doi.org/10.1109/IMF.2011.19

[12] Holt, T.J., Clevenger, S., Navarro, J.: Exploring digital evidence recognition among officers and troopers in a sample of a state police force. Policing: An International Journal of Police Strategies & Management **43**(1), 91–103 (2019), ISSN 1363-951X, https://doi.org/10.1108/PIJPSM-07-2019-0119

[13] Hoppmann, T., Lassak, L., Sasse, M.A., Freiling, F., Benenson, Z.: Defining the Usability of Digital Forensics in Criminal Proceedings: Reconciling the Technical and the Legal Sides. In: Proceedings of the Digital Forensics Doctoral Symposium (DFDS '26), ACM, Linköping, Sweden (2026), ISBN 979-8-4007-2120-5, https://doi.org/10.1145/3785318.3785324

[14] ISO/IEC 9241-11: International Organization for Standardization - Ergonomics of Human-System-Interaction: Part 11: Usability: Definitions and Concepts (2018)

[15] Kelty, S.F., McQueen, E., Pymont, C., Green, N.: Avoiding Burnout at the Digital Forensics Coalface: Targeted strategies for forensic agencies in the management of job-related stress. Forensic Science International: Digital Investigation **38**, 301127 (2021), ISSN 26662817, https://doi.org/10.1016/j.fsidi.2021.301127

[16] Palmer, G.: A Road Map for Digital Forensic Research: (Technical Report DTR-T001–01). Utica, New York (2001), URL https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf

[17] Pollitt, M.M.: Triage: A practical solution or admission of failure. Digital Investigation **10**(2), 87–88 (2013), ISSN 17422876, https://doi.org/10.1016/j.diin.2013.01.002

[18] Renaud, K., Bongiovanni, I., Wilford, S., Irons, A.: PRECEPT-4-Justice: A bias-neutralising framework for digital forensics investigations. Science & justice : journal of the Forensic Science Society **61**(5), 477–492 (2021), https://doi.org/10.1016/j.scijus.2021.06.003

[19] Roux, C., Crispino, F., Ribaux, O.: From Forensics to Forensic Science. Current Issues in Criminal Justice **24**(1), 7–24 (2012), ISSN 1034-5329, https://doi.org/10.1080/10345329.2012.12035941

[20] Sasse, M.A., Brostoff, S., Weirich, D.: Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security. BT Technology Journal **19**(3), 122–131 (2001), ISSN 1573-1995, https://doi.org/10.1023/A:1011902718709

[21] Sunde, N., Dror, I.E.: Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. Digital Investigation **29**, 101–108 (2019), ISSN 17422876, https://doi.org/10.1016/j.diin.2019.03.011

[22] Tsakonas, G., Papatheodorou, C.: Exploring usefulness and usability in the evaluation of open access digital libraries. Information Processing & Management **44**(3), 1234–1250 (2008), ISSN 0306-4573, https://doi.org/10.1016/j.ipm.2007.07.008

[23] Wilson-Kovacs, D.: Effective resource management in digital forensics: An exploratory analysis of triage practices in four English constabularies. Policing: An International Journal of Police Strategies & Management **43**(1), 77–90 (2020), ISSN 1363-951X, https://doi.org/10.1108/PIJPSM-07-2019-0126