Cyber Forensic Reporting: Benefits, Elements, Process, Expert Witnesses, and Ethical Considerations

Cheryl Ann Alexander[1] and Lidong Wang[2,*]

[1]*Institute for IT Innovation and Smart Health, Mississippi, USA*

[2]*Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA*

Abstract: Cyber forensic reporting creates a complete and evidence-based record. Appropriate cyber forensic reporting includes the investigation process with compliance and legal evidence, analysis, findings, and actionable recommendations for legal admissibility. In healthcare, cyber forensic reporting helps improve compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and facilitates the detection of vulnerabilities. This paper deals with cyber forensic reporting, which includes its benefits, elements, and process; expert witnesses; and ethical considerations. Cyber forensic reporting in healthcare is introduced. Expert witnesses in healthcare cyber forensic reporting are significant. There is a need for the right experts, including experts with specialized experience and knowledge in both healthcare and digital forensics.

Keywords: Cyber Forensic Reporting, Cybersecurity, Artificial Intelligence (AI), Expert Witnesses, Ethical Considerations, Healthcare.

INTRODUCTION

Digital forensics helps disclose the details of cybersecurity breaches and detect attackers. Cybersecurity breaches have been a major concern because they have a substantial impact on businesses, individuals, and legal systems. They can result in considerable legal ramifications, such as lawsuits, finesor penalties, and reputation damage. Digital evidence can be utilized in court to prove liability. An organization needs to comply with data security and privacy regulations when handling digital evidence. Forensic reporting is an important part of forensic investigations, and forensic reports are often utilized in legal proceedings.

A digital investigation is a multifaceted and complicated process. Two crucial issues require attention in a digital forensic report: 1) the investigation should be transparent, precise, and repeatable, and 2) it is a burden to demonstrate that evidence integrity is maintained during an investigation (Horsman, 2019; Varol and Sonmez, 2017). It is necessary to prepare suitable procedures and personnel for the broadly understood handling of incidents violating cybersecurity. This includes protecting digital evidence (according to the procedures, good practice, and suggestions covered in normative documents), executing cybersecurity policy, regulating the legislature to international standards, and training users and law enforcement officers (Kosiński *et al*., 2018).The main forensic processes of classification, authentication, and evaluation were applied to file recovery. It was demonstrated how the ENFSI (European Network of Forensic Science Institutes) Guideline for Evaluative Reporting can be used to express the results of file recovery classification, authentication, and evaluation (Casey *et al*., 2019).

The application of electronic health (e-health) is often lower than expected. Methods and development models utilized in the development process of a virtual reality (VR) application for forensic mental health care were studied. This research indicated that e-health development is much more than programming technology. It needs systematic research via methods that are appropriate for participants, an open and flexible mindset, structured project coordination by a multidisciplinary team, the inclusion of multiple perspectives in every decision, etc. (Kip, 2019).

In forensic psychiatry, a conversation with a patient about safety measures is suggested to avoid a violent incident. Research was conducted regarding patient safety incident reporting in forensic psychiatry. The incident report was anonymous, and the input was voluntary to guarantee that the reporting and processing were confidential. Data was captured from the PSiRS (patient safety incident reporting system) database of a forensic psychiatry hospital in Finland. The data from PSiRS provided information about the patient safety incident that was suitable for discovering risks in forensic psychiatry nursing (Kuosmanen *et al*., 2022).

*Address correspondence to this author at the Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA;
E-mail: lidong@iser.msstate.edu

E-ISSN: 1929-4409/25

The primary objective of the research in this paper is to deal with cyber forensic reporting. The remainder of this paper will be organized as follows: the second section introduces cyber forensic reporting: benefits, elements, and process; the third section presents cyber forensic reporting: expert witnesses; the fourth section introduces cyber forensic reporting: ethical considerations; the fifth section cyber forensic reporting in healthcare; and the sixth section is the conclusion.

CYBER FORENSIC REPORTING: BENEFITS, ELEMENTS, AND PROCESS

Cyber forensic reporting creates a complete, evidence-based record that involves the findings and analysis of a digital forensic investigation. Its crucial elements include the investigation scope, evidence collection and preservation, analysis method(s), findings, recommendations, etc. A quality cyber forensic report provides many benefits that mainly include presenting accurate and clear documentation of an incident, assisting in incident response and legal proceedings, and enhancing future cybersecurity. It helps recognize the root cause of a cyber incident and mitigation or remediation approaches. In addition, it demonstrates compliance with regulations and standards (Horsman, 2021).

Appropriate cyber forensic reporting includes the investigation process with compliance and legal evidence, analysis (especially root cause analysis), findings, and actionable recommendations, guaranteeing legal admissibility and good communication of technical facts to non-technical stakeholders such as legal teams or executives. Specialized knowledge and tools are needed for cyber forensic reporting to analyze digital evidence (Sunde, 2021).

There are challenges in cyber forensics (CF) due to complex situations (e.g., big data); therefore, advanced techniques such as artificial intelligence (AI) are required in the area of CF. AI should be understandable, interpretable, interactive, and authentic to apply AI to CF successfully. An explainable AI (XAI) system can play a significant role in CF, and such a system is called XAI-CF. The major requirements of a practical XAI-CF system were studied. The requirements were classified into four main categories and sixteen sub-categories, as illustrated in Figure **1**. An XAI-CF system helps make a decision, especially in a court of law; therefore, trust worthy is aprerequisite of the system. Experience and familiarity should be positive for the system to become trustworthy. Both transparency and human-meaningful explanation by the system increase trust. The integration of human-in-the-loop into the system helps improve the explanation by a machine. The system should be understandable to the CF stakeholders. The explanation is authentic if it correctly renders and expresses a mode's behaviors. For the system to be interactive, an easy-to-use human-computer interface is needed, and a user-centered design is also required. The visual design of the system helps improve usability. Exploratory means users and freely explore AI model behaviors. Reporting is the last step of the forensics process. XAI helps provide human-understandable explanations and complete cyber forensic reporting successfully (Alam and Altiparmak, 2024).

Cyber forensic accounting is the process of investigating and thwarting cybercrimes through forensic accounting. How cyber forensic accounting can enhance the quality of integrated reporting was studied. This study was based on four hypotheses: cyber anti-fraud policies, zero trust governance, digitally designed forensic procedures, and management control systems could influence the quality of integrated reporting in a positive and significant manner, respectively. Cyber anti-fraud policies employ forensic accounting principles to inspect and stop cybercrime. It is imperative to follow digitally designed forensic procedures for mitigating the incidence of cyber fraud. Management control systems (MCSs) use control processes and mechanisms for predetermined goals. MCSs and zero trust governance have the highest path coefficient, while digitally designed forensic procedures exhibit the lowest path coefficient.(Pham and Vu, 2024). The framework of the study and relevant Hypothesis 1 (H1), Hypothesis 2 (H2), Hypothesis 3 (H3), and Hypothesis 4 (H4) are shown in Figure **2**.

CYBER FORENSIC REPORTING: EXPERT WITNESSES

Expert witnesses are very important in explaining forensic methods and complex digital evidence. Expert testimony helps judges and juries understand technical evidence, which has a significant impact on legal outcomes. Seven factors within three types were presented that may unconsciously influence forensic experts' decision-making, as illustrated in Figure **3**. The first type is case-specific information, including case evidence, reference materials, and irrelevant case

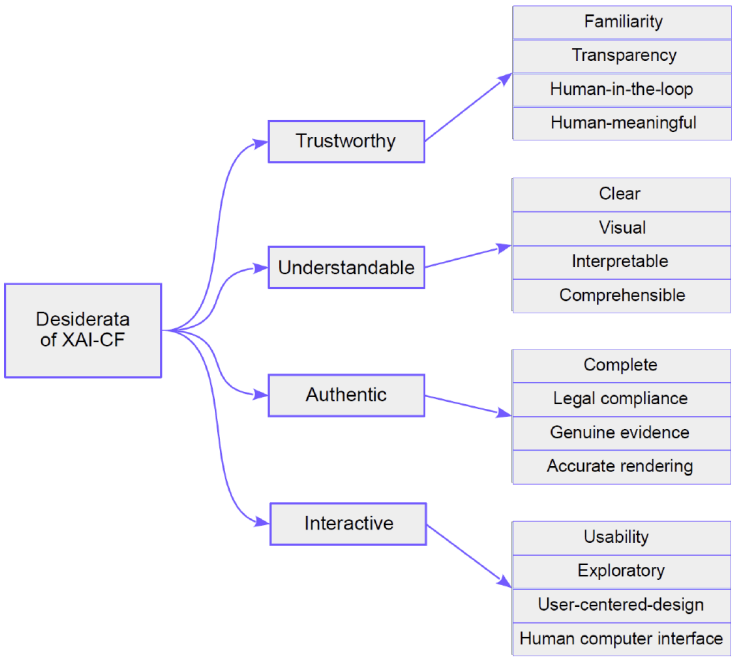

Figure 1: Desiderata of XAI-CF with four main categories and sixteen subcategories (Alam and Altiparmak, 2024).

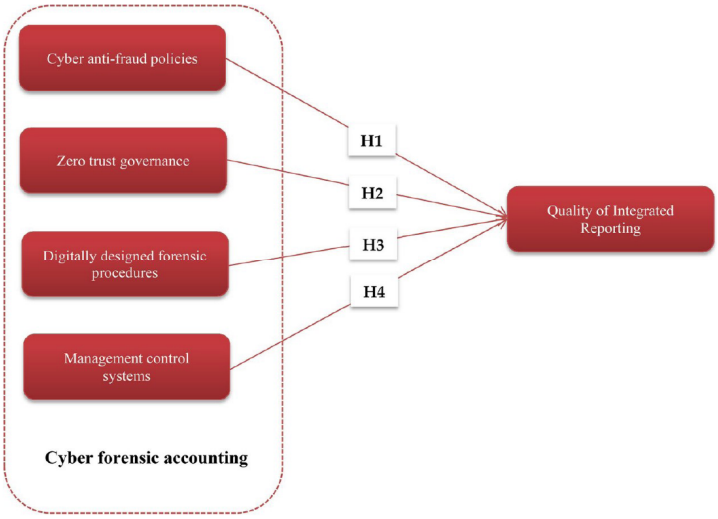

Figure 2: The impacts of cyber forensic accounting on the quality of integrated reporting (Pham and Vu, 2024).

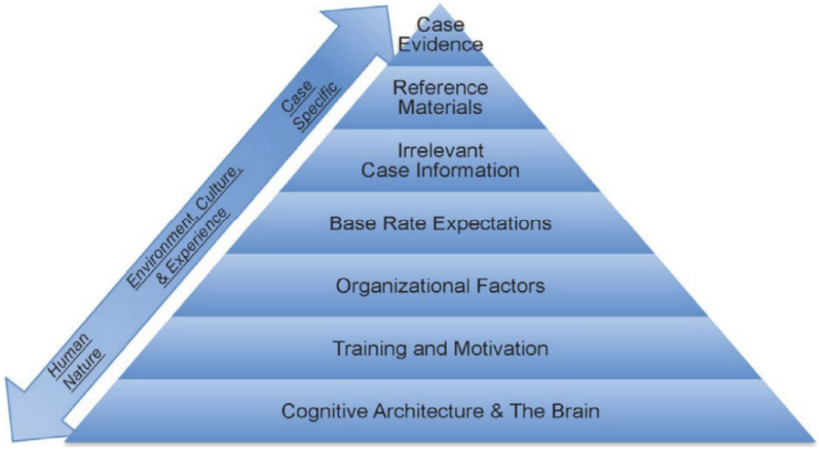

Figure 3: Seven factors within three types that may unconsciously influence forensic experts' decision-making (Dror, 2017).

information. The second type is environment, culture, and a forensic examiner's experience, including base rate expectations, organizational factors, and training and motivation. The third type is human nature, including basic forms of bias due to the cognitive architecture of the brain. The factors that are significant when considering what ought to be disclosed to a forensic examiner under the forensic disclosure model are: case evidence, reference materials, irrelevant case information, base rate expectations, and organizational factors (Dror, 2017).

A conceptual model of 'forensic disclosure' was introduced that deals with what information should be disclosed by and to forensic examiners. Forensic disclosure minimizes bias cascade or bias snowball effects by ensuring that an examiner does not convey unrelated information and only conveys his/her findings to the suitable stakeholders. Figure **4** shows the dynamic interactions and decision-making pathways of various domains in a forensic reconstruction process, which also conveys various pathways of interactions with forensic experts. The pathways of interactions with forensic examiners can be unidirectional or bidirectional (blue double arrows) in the figure. Cross-domain interactions are marked with dotted blue double arrows, while within-domain interactions are marked with black double arrows (Almazrouei *et al*., 2019).

CYBER FORENSIC REPORTING: ETHICAL CONSIDERATIONS

Ethical considerations should be paid attention to in cyber forensic reporting. Primary ethical considerations lie in 1) avoiding biases or discrimination in the collection and analysis of digital evidence; 2) adhering to professional codes of ethics, professional standards, and legal compliance (such as regulations and laws); 3) ensuring transparency in methodologies, limitations, and potential errors; 4) collecting and retaining data only necessary for investigations to reduce possible privacy violations; 5) handling sensitive information with highest care and disclosing it only when legally necessary; and 6) maintaining unbiased evidence and accurate findings (avoiding any distortion or misrepresentation).

The core principles of digital forensic studies, namely, reconnaissance, reliability, and relevance, were addressed. The ETHICore framework was presented to bridge the gap between ethical compliance and technical proficiency in digital forensic readiness. The framework highlighted the benefits of making an organization forensically ready and resolving ethical issues related to digital forensic investigations. Figure **5** presents a roadmap of the feasible forensic investigation in detail, explaining various routes of each layer and sublayer from a technical perspective. This figure also illustrates how principles are applied to the framework with reference to each layer of each stage. The layers in the framework empower the capability of a forensic investigator to perform effective investigations and achieve credible evidence. The layers involve data examination, data acquisition, forensic preparation, identification, motivation, legal advice, and security(Adel *et al*., 2024).

CYBER FORENSIC REPORTING IN HEALTHCARE

In healthcare, cyber forensic reporting helps improve compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and facilitates detecting vulnerabilities that may result in breaches of sensitive patient data and severe ethical and legal outcomes. Adherence to legal and ethical standards is especially important for cyber forensic reporting in healthcare. Relevant laws, ethical guidelines, and regulations such as HIPAA should be observed or followed during cyber forensic reporting. The chain of custody for all evidence should be maintained to guarantee its integrity and admissibility in court. Robust security measures should be executed to protect data security and patient privacy (Kip, 2019).

The need for expert witnesses in cyber forensic reporting is essential in healthcare. Choosing the right experts is crucial. Experts with specialized experience and knowledge in both healthcare and digital forensics should be selected. Experts interpret complex healthcare data and explain complex findings to non-technical audiences. Expert witnesses facilitate investigating data breaches, guaranteeing compliance with regulations such as HIPAA, protecting sensitive data and patient privacy, and ensuring the admissibility of evidence in the legal system.

Approaches to forensic report writing in psychiatry, psychology, and associated mental health have moved to ethical considerations and other codes, evidentiary standards, and practice. One ethical principle applicable to forensic report writing is to be comprehensive, impartial, and scientific (Young, 2016). Table **1** (Young, 2016) shows principles and standards for evaluating forensic mental health and forensic report writing according to the overarching principle of integrity in ethics, science, and law.

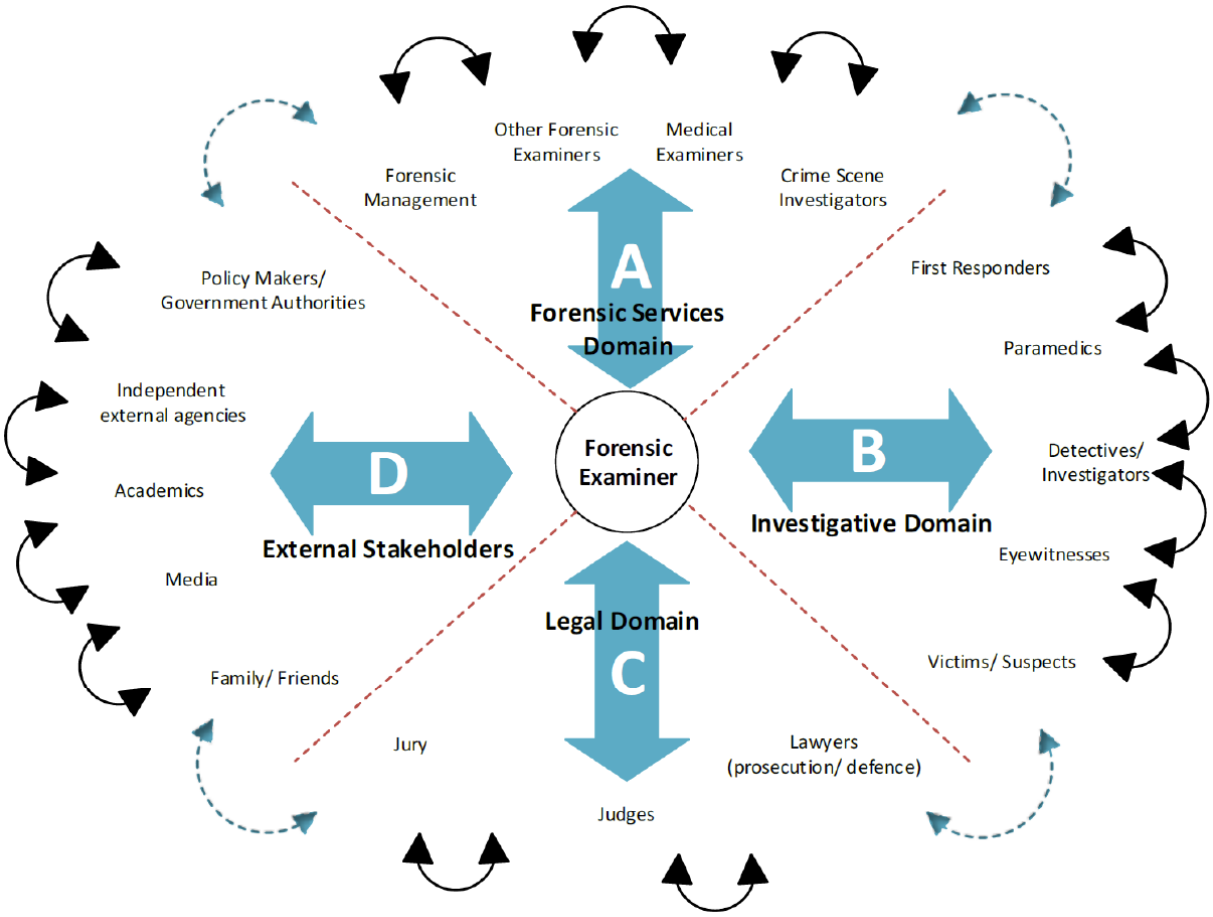

Figure 4: Dynamic interactions and decision-making pathways of various domains with forensic examiners (Almazrouei *et al*., 2019).

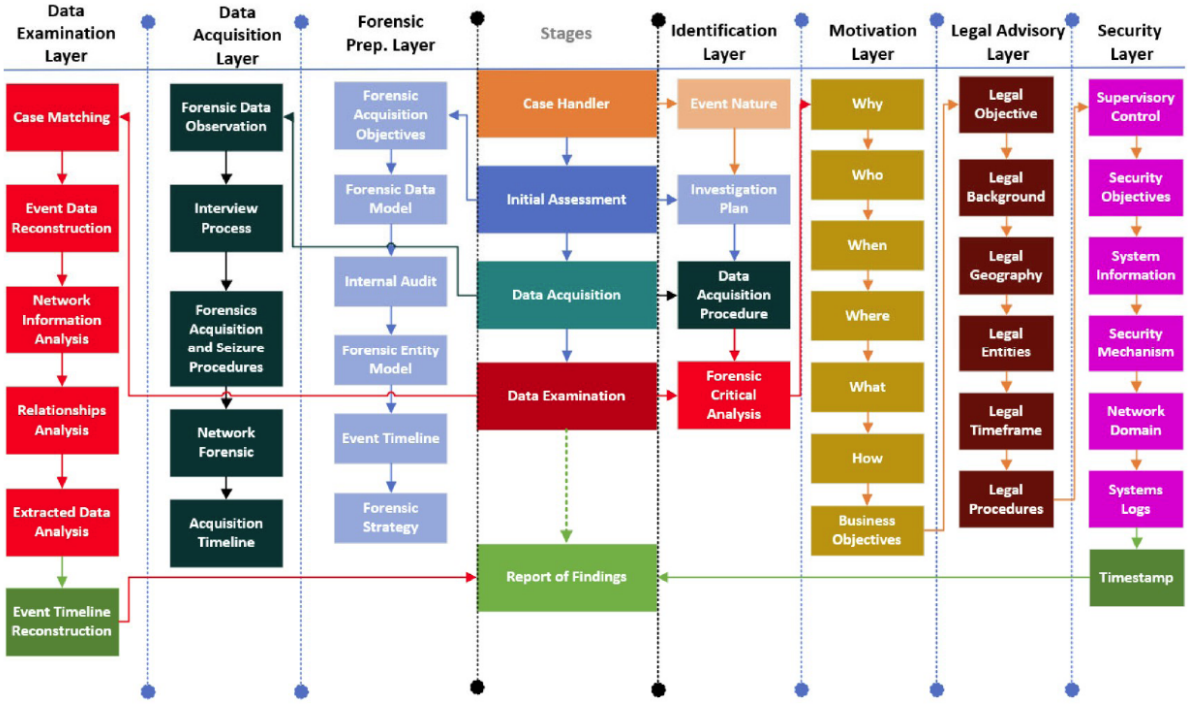

Figure 5: ETHICore: Ethical compliance and oversight framework (Adel *et al*., 2024).

Table 1: Principles and Standards for Evaluating Forensic Mental Health and Forensic Report Writing

Principles	Subcomponents	Details
Competence & communication	Competence	Proper education, training, and experience. Sufficient knowledge in evaluating forensic mental health. Not practicing outside competence areas.
	Communication	Being accurate, effective, & economical. Controlling the message. Using headings in reports, definitions as required, plain language, & minimal technical jargon/language
Dignity & divide	Dignity	Respect for the evaluate & standards of assessing forensic mental health. Conducting oneself with objectivity & honesty. Not attributing malingering or using any related term just based on test results but after considering the whole file. Considering that bias works both ways, with the evaluatee possibly engaging in negative response bias, malingering, gross exaggeration, etc.
	Divide	Avoiding the pull of biases in the adversarial divide Being unbiased & impartial & checking for the same throughout. Watching for confirmation bias & others that may apply
Procedure & protection	Procedure	Applying the right forensic mental health procedure. Selecting good tools for the legal question at hand. Evaluating in the proper context. Aiming to meet admissibility standards to court according to applicable laws.
	Protection	Obtaining proper authorization from all parties involved. Proceeding based on having obtained voluntary informed consent, unless contraindicated by the court order or otherwise not required.
Data gathering& determination	Data gathering	Be careful, thorough, & comprehensive. Employing the most suitable model to guide data collection, communication, & interpretation. Utilizing multiple sources of information for each area evaluated, with all methods & tools being valid as well as reliable. Diagnoses being supplementary information unless otherwise required. Clinical features being associated with the purposes at hand, & evaluated through all the sources of information. Dealing with functional issues associated with the legal question(s) at hand, or other behaviors associated with the question(s).
	Determination	Utilizing scientific reasoning and procedures throughout. Facts/data/information being related clearly to the sources utilized in the evaluation in the report. Separating facts/data/information from hypotheses/inferences, interpretations/opinions, and conclusions & their justifications. Utilizing case-specific (idiographic) evidence in evaluating/describing current clinical condition/functional abilities in connection to the history of any symptoms & the demonstrated capacities to address causal connection & legal issues. Utilizing nomothetic evidence the same way, i.e., describing the results of the psychological test the structured instrument, & any other specialized tools that apply to the questions at hand. Addressing final legal questions as allowed, required, & suitable (e.g., on disability, forensic capacities, etc.).

CONCLUSION

Appropriate cyber forensic reporting includes the investigation process with compliance and legal evidence, analysis (especially root cause analysis), findings, and actionable recommendations, guaranteeing legal admissibility and good communication of technical facts to non-technical stakeholders such as legal teams or executives. Expert testimony helps judges and juries understand technical evidence. Ethical considerations should be paid attention to in cyber forensic reporting.

In healthcare, cyber forensic reporting helps improve compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and facilitates detecting vulnerabilities. The need for expert witnesses in cyber forensic reporting is essential in healthcare. Choosing the right experts is crucial. Experts with specialized experience and knowledge in both healthcare and digital forensics should be selected.

This paper identifies and discusses key issues in cyber forensic reporting, especially the great impacts of AI on cyber forensic reporting. AI is revolutionizing cyber forensic reporting in healthcare by reducing bias, improving accuracy and reliability, and enhancing automation, streamlining, and efficiency. Future research in cyber forensic reporting can be the applications of AI/machine learning (ML)/deep learning (DL) in performing big data analytics and addressing the challenges of cloud forensics, IoT (Internet of Things) forensics, and network forensics.

ACKNOWLEDGEMENTS

The authors would like to express their thanks to Technology and Healthcare Solutions, USA, for its help and support.

DECLARATION OF THE USE OF AI TOOLS

The authors declare that they did not use AI tools in writing this paper.

CONFLICT OF INTEREST

The authors would like to announce that there is no conflict of interest.

ETHICS

In this article, ethical principles related to scientific research articles are observed. The corresponding author confirms that both authors have read, revised, and approved the paper.

REFERENCES

Adel, A., Ahsan, A., & Davison, C. (2024). ETHICore: Ethical Compliance and Oversight Framework for Digital Forensic Readiness. Information, 15(6), 363. https://doi.org/10.3390/info15060363

Alam, S., & Altiparmak, Z. (2024). XAI-CF--Examining the Role of Explainable Artificial Intelligence in Cyber Forensics. arXiv preprint arXiv:2402.02452. https://doi.org/10.2139/ssrn.4833246

Almazrouei, M. A., Dror, I. E., & Morgan, R. M. (2019). The forensic disclosure model: what should be disclosed to, and by, forensic experts?. International Journal of Law, Crime and Justice, 59, 100330. https://doi.org/10.1016/j.ijlcj.2019.05.003

Casey, E., Nelson, A., and Hyde, J. (2019). Standardization of file recovery classification and authentication. Digital Investigation, 31, 1-26. https://doi.org/10.1016/j.diin.2019.06.004

Dror, I. E. (2017). Human expert performance in forensic decision making: seven different sources of bias. Australian Journal of Forensic Sciences, 49(5), 541-547. https://doi.org/10.1080/00450618.2017.1281348

Horsman, G. (2019). Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework. Digital Investigation, 28, 146–151. https://doi.org/10.1016/j.diin.2019.01.007

Horsman, G. (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

Kip, H., Kelders, S. M., Bouman, Y. H., & van Gemert-Pijnen, L. J. (2019). The importance of systematically reporting and reflecting on eHealth development: participatory development process of a virtual reality application for forensic mental health care. Journal of medical Internet research, 21(8), e12972. https://doi.org/10.2196/12972

Kosiński, J., Kośla, R., & Gontarz, T. (2018). Cybersecurity and the handling of cyber incidents. Internal Security, 10(2), 107–128. https://doi.org/10.5604/01.3001.0013.4219

Kuosmanen, A., Tiihonen, J., Repo-Tiihonen, E., & Turunen, H. (2022). Voluntary patient safety incidents reporting in forensic psychiatry—What do the reports tell us?. Journal of psychiatric and mental health nursing, 29(1), 36-47. https://doi.org/10.1111/jpm.12737

Pham, Q. H., & Vu, K. P. (2024). Insight into how cyber forensic accounting enhances the integrated reporting quality in small and medium enterprises. Cogent Business & Managemesnt, 11(1), 2364053. https://doi.org/10.1080/23311975.2024.2364053

Sunde, N. (2021). What does a digital forensics opinion look like? A comparative study of digital forensics and forensic science reporting practices. Science & justice, 61(5), 586-596. https://doi.org/10.1016/j.scijus.2021.06.010

Varol, A., and Sonmez, Y. U. (2017). Review of evidence analysis and reporting phases in digital forensics process. 2017 International Conference on Computer Science and Engineering (UBMK), 923–928. https://doi.org/10.1109/UBMK.2017.8093563

Young, G. (2016). Psychiatric/psychological forensic report writing. International journal of law and psychiatry, 49, 214-220. https://doi.org/10.1016/j.ijlp.2016.10.008

Received on 02-05-2025 Accepted on 06-06-2025 Published on 10-07-2025

https://doi.org/10.6000/1929-4409.2025.14.12