A Model for Digital Evidence Admissibility Assessment

Albert Antwi-Boasiako, Hein Venter

Chapter 2

A MODEL FOR DIGITAL EVIDENCE ADMISSIBILITY ASSESSMENT

Albert Antwi-Boasiako and Hein Venter

Abstract Digital evidence is increasingly important in legal proceedings as a result of advances in the information and communications technology sector. Because of the transnational nature of computer crimes and computer-facilitated crimes, the digital forensic process and digital evidence handling must be standardized to ensure that the digital evidence produced is admissible in legal proceedings. The different positions of law on matters of evidence in different jurisdictions further complicates the transnational admissibility of digital evidence. A harmonized framework for assessing digital evidence admissibility is required to provide a scientific basis for digital evidence to be admissible and to ensure the cross-jurisdictional acceptance and usability of digital evidence. This chapter describes a harmonized framework that integrates the technical and legal requirements for digital evidence admissibility. The proposed framework, which provides a coherent techno-legal foundation for assessing digital evidence admissibility, is expected to contribute to ongoing developments in digital forensics standards.

Keywords: Digital evidence, admissibility assessment framework

1. Introduction

Despite the significance of digital evidence in legal proceedings, digital forensics as a forensic science is still undergoing transformation. The rapidly advancing information and communications technology sector and the evolution of cyber crimes and legal responses underpin these developments. Digital evidence admissibility is a key issue that arises from the application of digital forensics in jurisprudence. However, a reproducible and standardized framework that provides a foundation for the admissibility of digital evidence in legal proceedings has not been addressed holistically in the literature on digital forensics harmonization

and standardization. This research addresses the gap by proposing a harmonized model that integrates technical and legal requirements to determine the admissibility of digital evidence in legal proceedings.

2. Background

This section discusses digital forensics, digital evidence and previous research on digital forensics harmonization and standardization.

2.1 Digital Forensics and Digital Evidence

Digital forensics refers to the methodical recovery, storage, analysis and presentation of digital information [7]. Digital evidence is simply a product of a digital forensic process [11]. According to ISO/IEC 27037 [8], digital evidence is information or data stored or transmitted in binary form that may be relied upon as evidence. Digital evidence has become important because of the involvement of electronic devices and systems in criminal activities. A review of the literature and court documents suggests that digital evidence is generally admissible in many jurisdictions [14].

Digital forensics as a scientific discipline is rooted on classic forensic principles. It is underpinned by Locard's exchange principle, which states that contacts between two persons, items or objects will result in an exchange [4]. Thus, traces are left after interactions between persons, items or objects.

An example can establish the relationship between the exchange principle and digital forensics. In order for a laptop to be connected to a protected wireless network, the laptop must make its media access control (MAC) address available to the wireless network administrator (router) before receiving access. An exchange occurs between the two devices and traces are left after the connection is established (the router has logs of the wireless access and the laptop has artifacts pertaining to the access).

Computer users leave digital traces called digital footprints. Digital forensic examiners can identify computer crime suspects by collecting and analyzing these digital footprints.

The application of digital forensics in legal proceedings is significant. Digital forensics is applied in pure cyber crime cases and incidents as well as in cyber-facilitated incidents. This is because it is nearly impossible in today's information-technology-driven society to encounter a crime that does not have a digital dimension. Pure cyber crimes are those that can only be committed using computers, networks or other information technology devices or infrastructures; examples include hacking

and denial-of-service (DoS) attacks. Cyber-facilitated crimes, on the other hand, are conventional crimes that are perpetrated using computers, networks or other information technology devices or infrastructures; examples include murder, human trafficking, narcotics smuggling and sales, and economic crimes such as financial fraud.

Digital evidence is highly volatile. Unlike other traditional types of evidence, digital evidence can be altered rapidly through computing-related activities [18]. A few mouse clicks on a file could alter its metadata, which is a key determinant of evidence admissibility. When a user clicks on a file, he may not necessarily intend to alter the file metadata. However, doing so potentially alters metadata such as the last accessed time, which may render the file inadmissible as evidence. In order to ensure that evidence is admissible, the court must be satisfied that the evidence conforms to established legal rules – the evidence must be scientifically relevant, authentic, reliable and must have been obtained legally [13].

The fragility of digital evidence also presents challenges [1]. The rapidly-changing nature of technology, the fragility of the media on which electronic data is stored and the intangible nature of electronic data all render digital evidence potentially vulnerable to claims of errors, accidental alteration, prejudicial interference and fabrication. These technical issues combined with legal missteps or difficulties could affect the admissibility of digital evidence. Even when digital evidence is admitted, these factors could impact the weight of the evidence in question. Several efforts have focused on harmonizing digital forensic processes and activities in order to address the technical and legal issues regarding the admissibility of digital evidence.

2.2 Harmonization and Standardization

According to Leigland and Krings [12], digital forensic processes and techniques are generally fragmented. Approaches for gathering digital evidence were initially developed in an *ad hoc* manner by investigators, primarily within law enforcement. Personal experience in digital investigations and expertise gained over time have led to the development of *ad hoc* digital investigation models and guidelines [12].

Several researchers and practitioners have attempted to develop harmonized digital forensic frameworks. The first attempt at the Digital Forensics Research Workshop (DFRWS) in 2001 produced a digital forensic process model that consists of seven phases [16]: (i) identification; (ii) preservation; (iii) collection; (iv) examination; (v) analysis; (vi) presentation; and (vii) design. Reith et al. [17] have proposed an ab-

stract model of digital forensics. The Association of Chief Police Officers Good Practice Guide [2] and the U.S. Department of Justice Electronic Crime Scene Investigation Guide [21] are examples of efforts undertaken by law enforcement to harmonize digital forensics and provide common approaches for conducting digital forensic investigations. Valjarevic and Venter [23] have proposed a harmonized digital forensic model that attempts to resolve the fragmentation associated with digital forensic processes. The Scientific Working Group on Digital Evidence (SWGDE) [20] has published guidelines that cover specific incident investigations.

The standardization of digital forensics achieved major milestones when the International Organization for Standardization (ISO) published the ISO/IEC 27027 Standard – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence in 2012 [8] and the ISO/IEC 27043 Standard – Incident Investigation Principles and Processes in 2015 [10]. The two ISO/IEC standards provide guidelines for various incident investigations.

Despite the significant developments in digital forensics standardization, analysis suggests that current standards do not adequately address the issue of digital evidence admissibility. While it is essential to follow scientific investigative processes in conducting digital investigations, the admissibility of digital evidence is also impacted by other factors. Current standards are very applicable to digital forensic investigations, but they do not provide a basis for assessing the admissibility of digital evidence.

A review of the literature and court cases suggests that technical and legal requirements are considered when admitting digital evidence in legal proceedings [13]. However, the problem with digital evidence admissibility in the context of legal proceedings persists despite the formulation of standards for digital forensic processes. The question about which reproducible standardized criteria or benchmarks underpin digital evidence admissibility has not been answered by any of the existing digital forensic models. Therefore, it is imperative to develop a standardized model that harmonizes the technical and legal requirements in providing a foundation for digital evidence admissibility in legal proceedings.

3. Requirements for Assessing Admissibility

This section discusses the need for harmonizing the technical and legal requirements in order to determine the admissibility of digital evidence. It also specifies the technical and legal requirements that underpin the admissibility of digital evidence in legal proceedings.

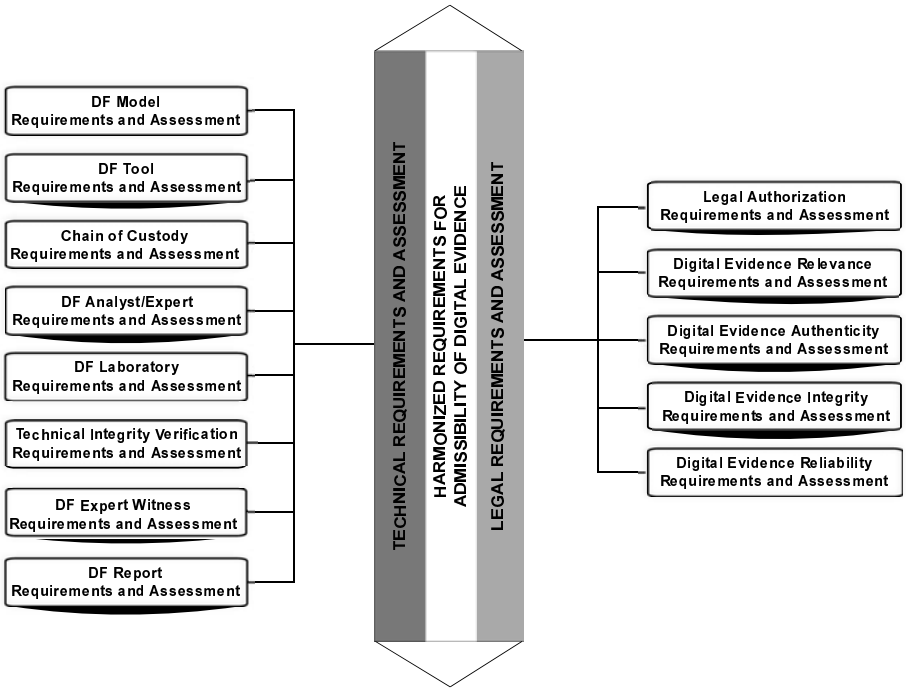

Figure 1. Technical and legal requirements for assessing admissibility.

3.1 Harmonization of Requirements

Analysis of the literature suggests that frameworks and standards pertaining to digital forensics do not address the question of digital evidence admissibility from a holistic perspective. In particular, the frameworks and standards specify technical processes and guidelines for incident investigators to follow when collecting digital evidence, but they fail to clarify the factors that underpin digital evidence admissibility.

Analysis of evidence admissibility in legal proceedings suggests the presence of technical and legal requirements that impact each other. In most jurisdictions, a legal authorization or search warrant (which is a legal requirement) is required before any digital device can be seized for a digital forensic examination (which is a technical requirement). Likewise, the manner in which digital evidence is retrieved during a digital forensic analysis (technical requirement) impacts the reliability of the evidence (legal requirement).

The harmonization of technical and legal requirements creates the foundation for determining the admissibility of digital evidence. Figure 1

presents the key technical and legal requirements that underpin digital evidence admissibility. These requirements are discussed in detail in the following sections.

3.2 Technical Requirements and Assessment

This section discusses the technical requirements assessed during legal proceedings in order to provide the foundation for digital evidence admissibility. The requirements are derived from standards, academic research, legal precedents and expert opinion, among other sources. The requirements have a bearing on digital evidence admissibility as well as on the determination of the weight of a particular piece of evidence.

- **Digital Forensic Models:** Various approaches are adopted by digital forensic investigators to obtain digital evidence. Each forensic approach or procedure is influenced by the nature of the incident, type of digital evidence, typology of the target digital device and electronic environment. For example, a procedure for extracting digital evidence from a mobile device is different from a procedure for extracting digital evidence from a hard drive. As a result, when a court assesses the admissibility of evidence, it must consider the specific forensic procedures that were used to retrieve and process the evidence in question. Digital forensic models embody a number of guidelines to ensure that appropriate digital forensic procedures are followed when conducting investigations. Key guidelines for digital forensic processes and procedures have been proposed by the Association of Chief Police Officers in the United Kingdom [2], Scientific Working Group on Digital Evidence in the United States [20] and International Organization for Standardization via the ISO/IEC 27043 Standard [10].

- **Digital Forensic Tools:** Digital forensic practitioners have access to a number of open source and proprietary tools to assist in the collection, analysis and preservation of digital evidence. Although no explicit rules govern the use of digital forensic tools, there is generally a consensus in the scientific community that forensic tools should have been tested, validated and their error rates documented. The Daubert case in the United States [22] highlights the importance of digital forensic tool validation as a criterion for determining digital evidence admissibility. Organizations such as the National Institute of Standards and Technology (NIST), Scientific Working Group on Digital Evidence and International Organization for Standardization have developed frameworks and methods for testing digital forensic tools (see, e.g., ISO/IEC 27041 [9]).

- **Chain of Custody:** Chain of custody seeks to preserve the integrity of digital evidence. A document sponsored by the U.S. National Institute of Justice [15] defines chain of custody as a process used to maintain and document the sequential history of evidence. Chain of custody cuts across all the steps of an investigative process, but it is especially important during the digital evidence seizure stage. According to the Association of Chief Police Officers Good Practice Guide [2], an independent third party should be able to track the movement of evidence right from the crime scene all the way through the investigation chain to the courtroom. Giova [6] argues that digital evidence should be accepted as valid in court only if its chain of custody can be established.

- **Digital Forensic Analysts and Experts:** The qualifications of a digital forensic examiner are also an important requirement and assessment criterion related to digital evidence admissibility. Analysis suggests that digital forensics as a forensic science is a multidimensional discipline that encompasses computing (information technology), investigations and the law. A digital forensic examiner is expected to demonstrate his/her competence in digital forensics in order to handle digital evidence. Although no transnational competency standards have been created to validate the competence of digital forensic examiners, education and training, certifications and hands-on experience are generally considered to determine the suitability of an individual to handle digital evidence.

- **Digital Forensic Laboratories:** A well-organized digital forensic laboratory with standard operating procedures (SOPs) and quality assurance systems positively impacts investigative processes and, consequently, the quality of the produced evidence. The Association of Chief Police Officers Good Practice Guide [2] lists specific guidelines for setting up and operating digital forensics laboratories. For example, a failure to adopt relevant laboratory standard operating procedures could alter the original state of data stored on a mobile device. The use of a poor laboratory facility or inappropriate storage procedures could result in digital evidence being ruled inadmissible in legal proceedings [24].

- **Technical Integrity Verification:** Maintaining and verifying the integrity of digital evidence items are important technical considerations that could significantly impact their admissibility. Digital data is altered, modified or copied from one environment to

another either through human actions or uncontrolled computing activities [18]. Forensic examiners adopt various methods for maintaining and demonstrating the integrity of digital evidence. The use of a write blocker, for example, is a standard digital forensic requirement to maintain the integrity of evidence. Digital signatures, encryption and hash algorithms are also employed to maintain, validate and demonstrate the integrity of digital evidence.

- **Digital Forensic Expert Witnesses:** Individuals with relevant expertise, knowledge and skills are often called upon to serve as expert witnesses in legal proceedings [19]. According the U.S. Federal Rules of Evidence, an expert witness must be qualified on the basis of knowledge, expertise, experience, education and/or training. The scientific, technical and other specialized knowledge possessed by an expert witness enables the individual to testify to the facts in question [19].

- **Digital Forensic Reports:** The report produced by a digital forensic investigation is an important technical consideration that underpins digital evidence admissibility. Garrie and Morrissy [5] maintain that a digital forensic report must have conclusions that are reproducible by independent third parties. They also argue that conclusions that are not reproducible should be given little credence in legal proceedings. In Republic vs. Alexander Tweneboah (Ghana Suit No. TB 15/13/15 of 2016), the high court judge in the financial court division ruled against a report submitted by an expert witness from the e-Crime Bureau because the judge deemed that the report did not fully represent the digital evidence contained on an accompanying CD.

3.3 Legal Requirements and Assessment

Most jurisdictions have legal requirements that provide the grounds for admissibility of digital evidence in legal proceedings. This section discusses the legal issues pertaining to the admissibility of digital evidence as listed in Figure 1.

- **Legal Authorization:** Assessing digital evidence often requires legal authorization. Human rights, data protection and privacy impacts on accused parties and victims must be respected. Although there may be exceptions, the law generally provides safeguards for protecting the rights of individuals. Obtaining a legal authorization grants judicial legitimacy to the evidence in question; indeed, this may be the most important step in obtaining and handling

digital evidence. Search warrants are normally required to seize electronic devices and digital evidence. Failure to obtain a legal authorization may undermine the best evidence rule and jeopardize the case [13]. Admitting evidence that is not supported by legal authorizations could result in prosecutors and law enforcement (i.e., the state) trampling on civil liberties [9].

- **Digital Evidence Relevance:** Relevance is an important determinant of digital evidence admissibility. According to Mason [14], in order for evidence to be admissible, it must be "sufficiently relevant" to the facts at issue. Evidence cannot be admissible if it is not deemed to be relevant [12]. For a piece of evidence to be deemed relevant in legal proceedings, it must tend to prove or disprove a fact in the proceedings [3]. Evidence that has probative value must prove the fact in question to be more (or less) probable than it would be without the evidence.

- **Digital Evidence Authenticity:** Authenticity is another important criterion that impacts the reliability of evidence. According to Mason [14], for digital evidence to be admitted in a court of law, there must be adduced evidence that the evidence in question is indeed what it is purported to be. For example, for a digital record to be admissible, the court would have to be convinced that the record was indeed generated by the individual who is purported to have authored the record. The American Express Travel Related Services Company Inc. vs. Vee Vinhnee case [14] highlights the importance of the authenticity requirement. In this case, the judge felt that American Express failed to authenticate certain digital records and proceeded to rule against American Express on the basis of its failure to authenticate the records. American Express subsequently appealed, but the appeals court affirmed the lower court decision.

- **Digital Evidence Integrity:** Integrity refers to the "wholeness and soundness" of digital evidence [14]. Integrity also implies that the evidence is complete and unaltered. An assessment of evidence integrity is a primary requirement for digital evidence admissibility and serves as the basis for determining the weight of evidence. Mason [14] contends that digital evidence integrity is not an absolute condition but a state of relationships. In assessing the integrity of digital evidence, courts, therefore, consider several factors and relationships – primarily the technical requirements discussed in the previous section. Courts require the integrity of evidence to be

established and guaranteed during investigations and the evidence to be preserved from modifications during its entire lifecycle [13]. In the Republic of South Africa, the originality of digital evidence depends on its integrity as outlined in Section 14(2) of the Electronic Communications and Transactions Act of 2002.

- **Digital Evidence Reliability:** In order for evidence to be admissible in court, the proferrer of the evidence must establish that no aspect of the evidence is suspect. Leroux [13] states that, for evidence to be deemed reliable, "there must be nothing that casts doubt about how the evidence was collected and subsequently handled." The Daubert case [22] provides the basis for assessing the reliability of scientific evidence in the United States. In particular, this celebrated case specifies five criteria for evaluating the reliability (and by extension, the admissibility) of digital evidence: (i) whether the technique has been tested; (ii) whether the technique has undergone peer review; (iii) whether there is a known error rate associated with the technique; (iv) whether standards controlling its operations exist and were maintained; and (v) whether the technique is generally accepted by the scientific community.

The integration of the technical and legal requirements discussed above provides the foundation of a harmonized framework for assessing digital evidence admissibility. It must be emphasized that cross examination in legal proceedings is an important element that impacts the assessment of the technical and legal requirements. The next section explores the relationships between the requirements and the considerations involved in determining digital evidence admissibility.

4. Model for Assessing Evidence Admissibility

This section discusses the proposed harmonized model for digital evidence admissibility assessment and its application in legal proceedings. A harmonized conceptual model was developed in order to integrate the requirements discussed above. The conceptual model shown in Figure 2 provides a framework for establishing the dependencies and relationships between the various requirements and assessment considerations.

The conceptual model encapsulates three levels of harmonization, called phases, which are integrated in the proposed harmonized model for digital evidence admissibility assessment. The three phases are integrated but differ from each other in terms of their functional relevance to digital evidence admissibility assessment. Figure 3 presents the proposed harmonized model for digital evidence admissibility assessment.

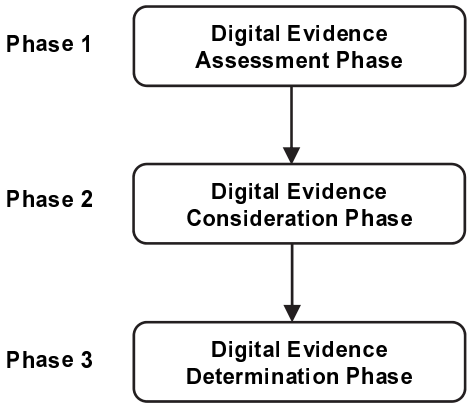

Figure 2. Digital evidence admissibility assessment model schema.

4.1 Phase 1: Evidence Assessment Phase

The digital evidence assessment phase establishes the legal foundation of the digital evidence in question. For example, when digital evidence residing on a hard drive belonging to a suspect is presented in court, the first consideration of the court is to determine the legal basis for the seizure of the hard drive. Essentially, the legal authority of the prosecution to seize the device has to be firmly established. In most jurisdictions, a court order may satisfy this requirement. Organizational policies and protocols may also provide the basis for the legal authority. Therefore, Phase 1 addresses the preliminary questions related to the legal admissibility of digital evidence. Generally, digital evidence is deemed inadmissible if it fails to meet the requirements imposed in this important phase. Indeed, Phase 1 also provides the grounds for further consideration of the digital evidence in question.

4.2 Phase 2: Evidence Consideration Phase

This phase focuses on the technical standards and requirements that underpin digital evidence admissibility. Technical considerations associated with the handling and processing of digital evidence are considered after the legal basis of the evidence has been established. This phase is subdivided into three categories:

- **Pre-Requisite Requirements:** These requirements must be considered before any core technical activities are conducted. The requirements include digital forensic model, tool, analyst/expert and laboratory requirements and assessments.

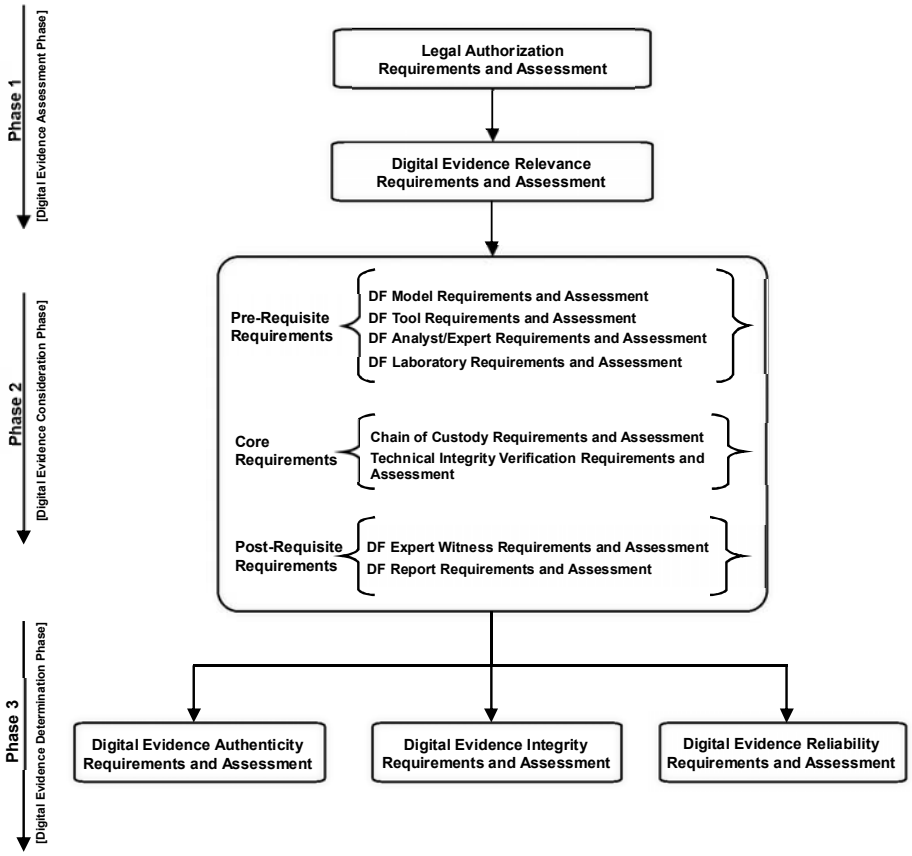

Figure 3. Harmonized model for digital evidence admissibility assessment.

- **Core Requirements:** These principal technical requirements significantly impact the determination of the admissibility of digital evidence. The requirements comprise chain of custody and technical integrity verification requirements and assessments.

- **Post-Requisite Requirements:** These requirements further elaborate or explain the requirements in the two previous categories. The requirements comprise digital forensic expert witness and report requirements and assessments.

Phase 2 focuses on the technical requirements and considerations of digital evidence. The phase is very important because judicial conclusions (Phase 3) are based primarily on the assessment outcomes of the technical requirements.

4.3 Phase 3: Evidence Determination Phase

This phase underpins court decisions in determining the admissibility and weight of digital evidence. The determinations of the Phase 3 requirements are based on the assessment outcomes of the Phase 2 requirements (technical requirements). The determination of the weight of a piece of digital evidence is based on the results of the various technical considerations; each technical criterion has a specific impact (impact factor) on the evidence. For example, although the lack of a digital forensic laboratory may impact a case involving digital evidence, the failure to document and track the chain of custody of a piece of digital evidence could have a wider impact on the evidence than the lack of a laboratory facility.

5. Application in Legal Proceedings

The harmonized model provides a holistic techno-legal foundation for assessing digital evidence admissibility in legal proceedings. The model integrates the key technical requirements associated with digital forensics and the legal principles that underpin evidence admissibility across different jurisdictions. As a result, the harmonized model helps address the issue of digital evidence admissibility from a trans-jurisdictional perspective with particular emphasis on the cross-border handling of digital evidence. By incorporating best practices for digital evidence assessment and exchange across different jurisdictions, the harmonized model also contributes to digital forensics standardization efforts.

In summary, the proposed harmonized model for digital evidence admissibility assessment is designed to provide a techno-legal foundation for: (i) determining if digital evidence is admissible; and (ii) determining the weight of digital evidence that has already been admitted subject to further research.

6. Conclusions

Developments in computer science and information technology are expected to significantly impact the technical and legal requirements that provide the foundation for the admissibility of digital evidence. The proposed harmonized model for digital evidence admissibility assessment has been created to ensure that future technological developments in the fields are integrated into the digital forensic process. As such, the proposed model contributes to ongoing efforts in digital forensics standardization being undertaken by academia, industry and law enforcement.

The problem of admissibility of digital evidence is the central theme of this research. The novelty lies in the introduction of a reproducible, trans-jurisdictional and standardized model that underpins the admissibility of digital evidence in legal proceedings. Key technical and legal requirements are identified and integrated within the framework for assessing digital evidence admissibility.

Different technical requirements have different impacts on the determination of evidentiary weight. Future research will investigate the impact level of each requirement in the harmonized model on the determination of the weight of a piece of evidence. In addition, future research will evaluate practical applications of the harmonized model in legal proceedings, with the goal of creating an expert system that would provide advice, guidance and assessments of the admissibility and weight of digital evidence.

References

[1] J. Ami-Narh and P. Williams, Digital forensics and the legal system: A dilemma of our time, *Proceedings of the Sixth Australian Digital Forensics Conference*, 2008.

[2] Association of Chief Police Officers, Good Practice Guide for Computer-Based Evidence, London, United Kingdom, 2008.

[3] S. Brobbey, *Essentials of the Ghana Law of Evidence*, Datro Publications, Accra, Ghana, 2014.

[4] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press, Waltham, Massachusetts, 2011.

[5] D. Garrie and J. Morrissy, Digital forensic evidence in the courtroom: Understanding content and quality, *Northwestern Journal of Technology and Intellectual Property*, vol. 12(2), article no. 5, 2014.

[6] G. Giova, Improving chain of custody in forensic investigations of electronic digital systems, *International Journal of Computer Science and Network Security*, vol. 11(1), 2011.

[7] M. Grobler, Digital forensic standards: International progress, *Proceedings of the South African Information Security Multi-Conference*, pp. 261–271, 2010.

[8] International Organization of Standardization, Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, ISO/IEC 27037:2012 Standard, Geneva, Switzerland, 2012.

[9] International Organization of Standardization, Information Technology – Security Techniques – Guidance on Assuring Suitability and Adequacy of Incident Investigative Methods, ISO/IEC 27041:2015 Standard, Geneva, Switzerland, 2015.

[10] International Organization of Standardization, Information Technology – Security Techniques – Incident Investigation Principles and Processes, ISO/IEC 27043:2015 Standard, Geneva, Switzerland, 2015.

[11] G. Kessler, Judges' awareness, understanding and application of digital evidence, *Journal of Digital Forensics, Security and Law*, vol. 6(1), pp. 55–72, 2011.

[12] R. Leigland and A. Krings, A formalization of digital forensics, *International Journal of Digital Evidence*, vol. 3(2), 2004.

[13] O. Leroux, Legal admissibility of electronic evidence, *International Review of Law, Computers and Technology*, vol. 18(2), pp. 193–222, 2004.

[14] S. Mason, *Electronic Evidence*, Butterworths Law, London, United Kingdom, 2012.

[15] National Forensic Science Technology Center, Crime Scene Investigation: A Guide for Law Enforcement, Largo, Florida, 2013.

[16] G. Palmer, A Road Map for Digital Forensic Research, DFRWS Technical Report, DTR-T001-01 Final, Air Force Research Laboratory, Rome, New York, 2001.

[17] M. Reith, C. Carr and G. Gunsch, An examination of digital forensic models, *International Journal of Digital Evidence*, vol. 1(3), 2002.

[18] E. Roffeh, *Practical Digital Evidence: Law and Technology, Part I*, CreateSpace Independent Publishing Platform, Seattle, Washington, 2015.

[19] S. Schroeder, How to be a digital forensic expert witness, *Proceedings of the First International Conference on Systematic Approaches to Digital Forensic Engineering*, pp. 69–85, 2005.

[20] Scientific Working Group on Digital Evidence, SWGDE Best Practices for Computer Forensics, Version 3.1 (`www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensics`), 2014.

[21] Technical Working Group for Electronic Crime Scene Investigation, Electronic Crime Scene Investigation: A Guide for First Responders, National Institute of Justice, Washington, DC, 2001.

[22] U.S. Supreme Court, Daubert v. Merrell Dow Pharmaceuticals Inc., *United States Reports*, vol. 509, pp. 579–601, 1983.

[23] A. Valjarevic and H. Venter, Harmonized digital forensic process model, *Proceedings of the Information Security for South Africa Conference*, 2012.

[24] C. Vecchio-Flaim, Developing a Computer Forensics Team, InfoSec Reading Room, SANS Institute, Bethesda, Maryland, 2001.