Implementing the Harmonized Model for Digital Evidence Admissibility Assessment

Albert Antwi-Boasiako, Hein Venter

Chapter 2

IMPLEMENTING THE HARMONIZED MODEL FOR DIGITAL EVIDENCE ADMISSIBILITY ASSESSMENT

Albert Antwi-Boasiako and Hein Venter

Abstract Standardization of digital forensics has become an important focus area for researchers and criminal justice practitioners. Over the past decade, several efforts have been made to encapsulate digital forensic processes and activities in harmonized frameworks for incident investigations. A harmonized model for digital evidence admissibility assessment has been proposed for integrating the technical and legal determinants of digital evidence admissibility, thereby providing a techno-legal foundation for assessing digital evidence admissibility in judicial proceedings.

This chapter presents an algorithm underlying the harmonized model for digital evidence admissibility assessment, which enables the determination of the evidential weight of digital evidence using factor analysis. The algorithm is designed to be used by judges to determine evidence admissibility in criminal proceedings. However, it should also be useful to investigators, prosecutors and defense lawyers for evaluating potential digital evidence before it is presented in court.

Keywords: Digital evidence admissibility, factor analysis, evidential weight

1. Introduction

The application of digital forensics in criminal justice has become more relevant than ever because of the continuous evolution of cyber crime and its impact on individuals, organizations and governments. It is nearly impossible in today's information-technology-driven society to find a crime that does not have a digital dimension [7]. The relevance of digital forensics is also influenced by the fact that computer systems are being used to facilitate crimes such as fraud, terrorism and money laundering. National information infrastructures have become targets

for cyber attackers; this has rendered digital forensics an essential component of national strategies for combating cyber threats.

Meanwhile, advancements in computer engineering and information and communications technologies have led to novel sources of digital evidence. Unmanned aerial vehicles, driverless automobiles and Internet of Things devices have led to new developments in digital forensics because of the digital evidence that resides in these systems [1, 9].

However, the question of digital evidence admissibility remains a key issue when applying digital forensics in jurisprudence. The criminal justice sector is confronted with the challenge of proffering evidence that is admissible in court [12]. In addition to training in new legislation and technology, judges require a scientific approach for assessing digital evidence in court. These challenges have driven the research community to develop standardized processes and approaches to ensure that digital evidence is admissible in legal proceedings.

This chapter presents an algorithm underlying a harmonized model for digital evidence admissibility assessment, which assists in determining the evidential weight of digital evidence using factor analysis. The algorithm is designed to be used by judges in criminal proceedings, but it should also be useful to investigators, prosecutors and defense lawyers for evaluating potential digital evidence before it is presented in legal proceedings.

2. Background and Related Work

Several models and frameworks have been introduced to standardize digital forensic activities in order to address issues regarding the admissibility of digital evidence. These include a framework introduced by participants in the 2001 Digital Forensic Research Workshop [17], an abstract model of digital forensic procedure introduced by Reith et al. [18] and a harmonized process model introduced by Valjarevic and Venter [25]. A good practice guide produced by the (U.K.) Association of Chief Police Officers [3] and an electronic crime scene investigation guide published by the U.S. Department of Justice [23] are examples of efforts undertaken by law enforcement to harmonize digital forensics and provide a common approach for conducting digital investigations. The International Organization for Standardization has created the ISO/IEC 27037 Standard [13] and the ISO/IEC 27043 Standard [14] to support incident investigations.

Despite significant developments in rationalizing the domain of digital forensics, issues associated with the admissibility of digital evidence in legal proceedings have remained largely unresolved. To address this

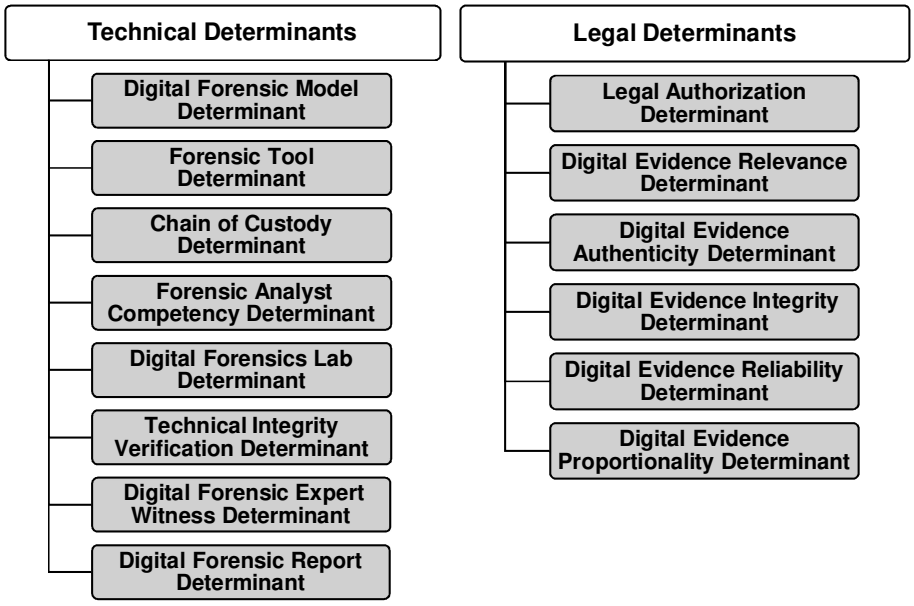


Figure 1. Requirements for assessing the admissibility of digital evidence.

gap, Antwi-Boasiako and Venter [2] introduced the Harmonized Model for Digital Evidence Admissibility Assessment (HM-DEAA). This model specifies technical and legal requirements – called "determinants" – that underpin the admissibility of digital evidence. Figure 1 presents the various technical and legal determinants specified in the harmonized model.

This existential foundation of digital evidence presents a techno-legal dilemma – a challenge or gap that exists in establishing a balanced interdependent relationship between the technical and legal requirements when establishing digital evidence admissibility and determining the weight of digital evidence in judicial proceedings. The harmonized model of Antwi-Boasiako and Venter [2] leverages an operational interdependency relationship between the technical and legal determinants to establish digital evidence admissibility.

Figure 2 presents the harmonized model. The three phases of the model are integrated, but they are distinct from each other due to their functional relevance in assessing digital evidence admissibility. The digital evidence assessment phase establishes the legal foundations of digital evidence. The digital evidence consideration phase focuses on the technical requirements that underpin digital evidence admissibility. The digital

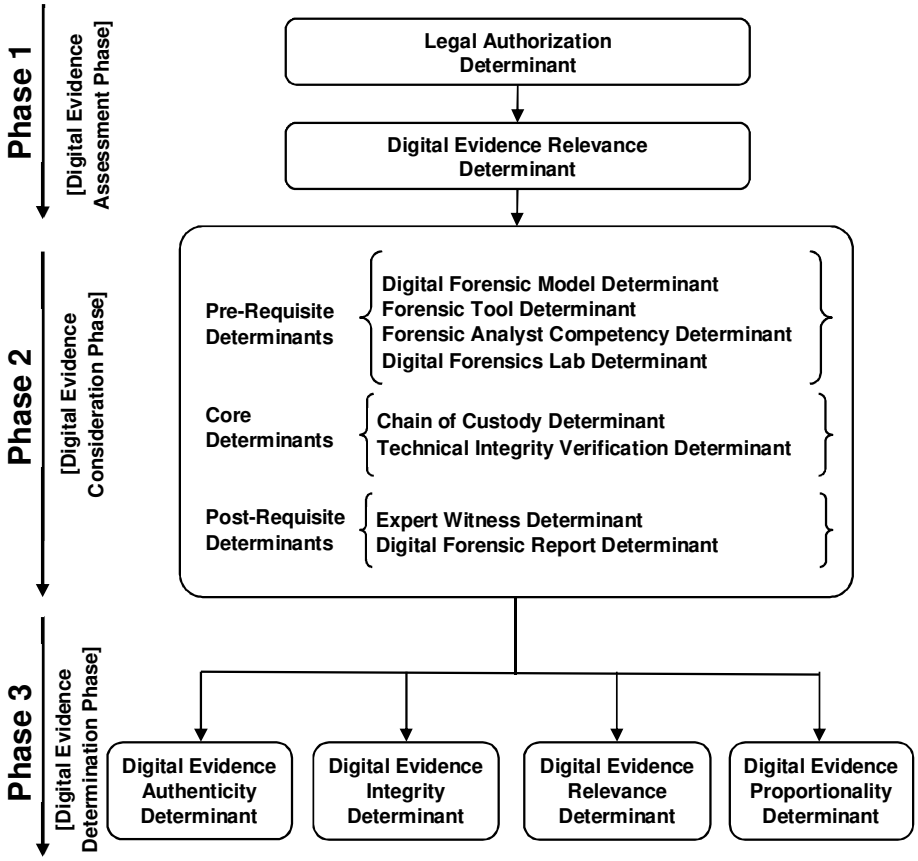


Figure 2. Harmonized Model for Digital Evidence Admissibility Assessment.

evidence determination phase underpins the judicial decisions regarding the admissibility and weight of digital evidence.

The research described in this chapter builds on the previous work by Antwi-Boasiako and Venter [2]. It presents an algorithm that underlies the implementation of the harmonized model for digital evidence admissibility assessment and enables the determination of evidential weight using factor analysis.

3. Validation Survey Methodology and Findings

A survey of judicial experts with knowledge and experience in digital evidence was conducted to validate the technical and legal determinants of digital evidence admissibility. The respondents were asked to assess

Table 1. Evidential weight impact description.

Score	Impact	Description
1	No Impact	Determinant has no effect on the digital evidence in question
2	Minimal	Determinant has very little effect on the digital evidence in question
3	Moderate	Determinant has some effect, but not significant enough, on the digital evidence in question
4	Significant	Determinant has considerable effect on the digital evidence in question
5	Very Significant	Determinant has exceptional effect on the digital evidence in question

the impact of each determinant on the weight of digital evidence. Table 1 shows the Likert scale [4] used by the survey respondents.

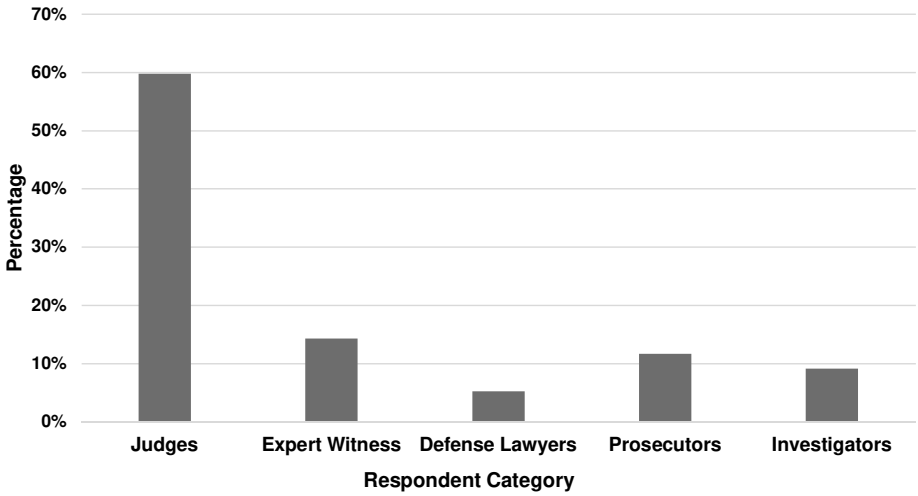


Figure 3. Survey respondent categories.

A total of 77 respondents participated in the survey. The respondents were drawn from common law and civil law jurisdictions across Africa, North and South America, Asia, Europe and the Middle East. Figure 3 shows the five categories of experts who participated in the survey.

An expert sampling method [10] used to obtain a scientifically-valid sample for the survey. Expert sampling provides an optimal means for constructing the views of respondents who are judged to be experts

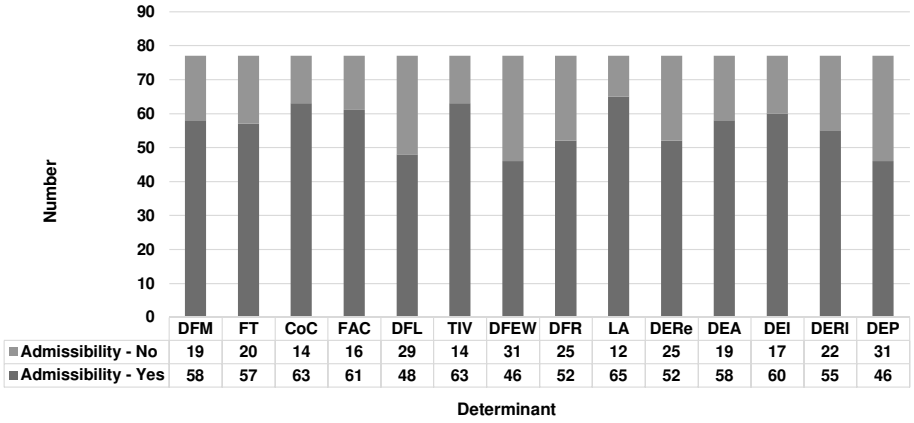
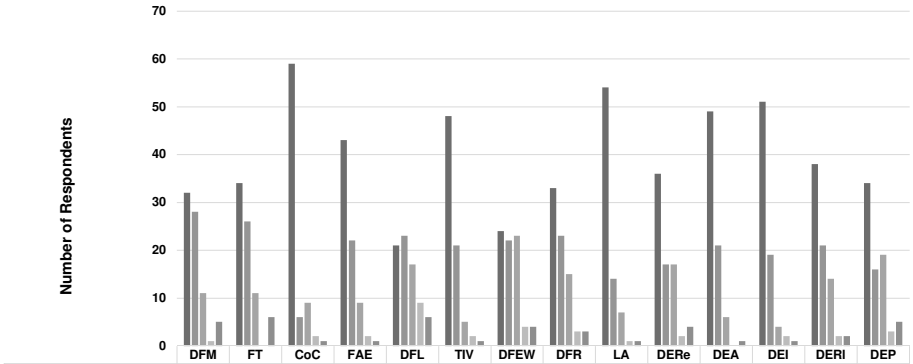


Figure 4. Responses related to the determinants of admissibility.

in the subject matter under investigation [10]. The survey was also consensus-oriented, which justified the application of expert sampling and the qualitative research approach [24]. The sample selection was justified using consensus theory [8, 26]. The quantitative method was instrumented through the use of statistical methods, including factor analysis, to identify and explore the distribution of survey data.

The research instrument was subjected to a number of validity and reliability tests, including questionnaire validity, face validity, content validity and construct validity, which are essential to achieving validity and reliability [22]. Questionnaire validity refers to the accuracy and consistency of a questionnaire in providing reliable research data. Face validity refers to the degree to which a measure appears to be related to a specific construct in the research; according to Burton and Mazerolle [6], face validity establishes the ease of use, clarity and readability of a research instrument. Content validity considers the extent to which a survey is relevant and representative of the target construct; it establishes the credibility, accuracy and relevance of the subject matter under investigation. Construct validity establishes a cause and effect relationship in a research instrument [22].

Figure 4 highlights the responses related to the determinants of admissibility. As an example, consider the chain of custody (CoC) determinant. Fourteen survey participants (18% of the respondents) indicated that chain of custody does not affect the admissibility of digital evidence in a court of law whereas 62 participants (82% of the respondents) indicated that it affects evidence admissibility. Several factors may have contributed to these responses. Chain of custody is widely recognized by



	DFM	FT	CoC	FAE	DFL	TIV	DFEW	DFR	LA	DERe	DEA	DEI	DERI	DEP
Very Significant Impact - 5	32	34	59	43	21	48	24	33	54	36	49	51	38	34
Significant Impact - 4	28	26	6	22	23	21	22	23	14	17	21	19	21	16
Moderate Impact - 3	11	11	9	9	17	5	23	15	7	17	6	4	14	19
Minimal Impact - 2	1	0	2	2	9	2	4	3	1	2	0	2	2	3
No Impact - 1	5	6	1	1	6	1	4	3	1	4	1	1	2	5

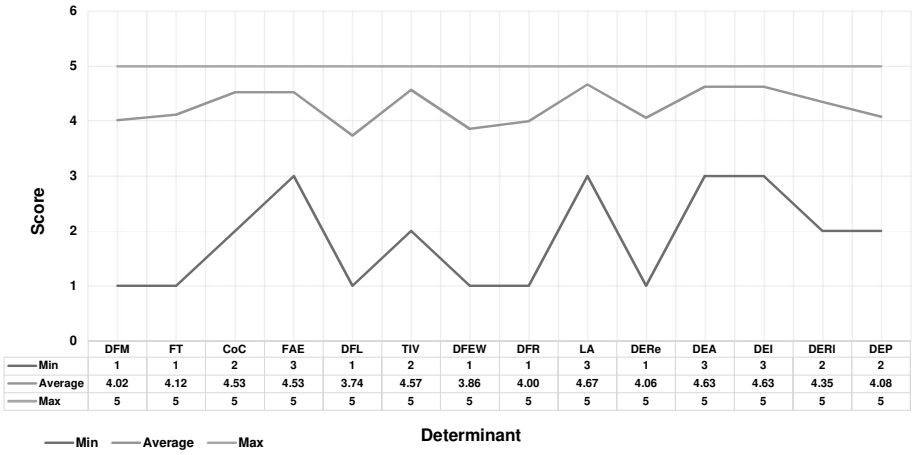
Determinant

Figure 5. Likert scores assigned to the determinants of admissibility.

experts as one of the most important requirements for digital evidence admissibility; this is confirmed by the high positive response rate of 82% for the determinant. However, the understanding of respondents and prevailing legal practices in their jurisdictions may have contributed to the higher than expected 18% negative response rate for chain of custody.

The survey participants were also asked to rate the impact of each determinant on the evidential weight using the Likert scale of 1 to 5 shown in Table 1. Figure 5 shows the scores for the determinants. Once again, consider the chain of custody determinant (CoC) as an example. Fifty-nine survey participants (77% of the total) rated the impact of chain of custody on digital evidence admissibility as very significant (Likert score of 5); six respondents (8%) rated the impact as significant (score of 4); nine 9 respondents (12%) rated the impact as moderate (score of 3); two respondents (3%) rated the impact as minimal (score of 2); and one respondent (less than 1%) rated no impact (score of 1).

Figure 6 graphs the minimum, average and maximum scores for the determinants. For example, the average rating of the impact of the chain of custody determinant on digital evidence admissibility is 4.53. It is important to note that an analysis of the data revealed that no conspicuous variations existed in the responses provided by judges versus other criminal justice actors relative to the importance of the determinants. This implies that all the criminal justice actors considered in the research have common understanding and expectations of the application of dig-



	DFM	FT	CoC	FAE	DFL	TIV	DFEW	DFR	LA	DERe	DEA	DEI	DERI	DEP
Min	1	1	2	3	1	2	1	1	3	1	3	3	2	2
Average	4.02	4.12	4.53	4.53	3.74	4.57	3.86	4.00	4.67	4.06	4.63	4.63	4.35	4.08
Max	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Figure 6. Distributions of scores for the determinants of admissibility.

ital evidence in criminal proceedings. However, the levels of technical and judicial knowledge and experience appear to be important factors that contributed to the variations seen in the scores.

4. Proposed Algorithm

The next step after validating the determinants and assessing their impacts on digital evidence admissibility is to apply the algorithm presented in Figures 7 and 8. The algorithm flowcharts cover the three phases of the harmonized model: (i) digital evidence assessment; (ii) digital evidence consideration; and (iii) digital evidence determination. The algorithm formalizes the sequential activities from the introduction of digital evidence in court through the various stages of witness presentation and cross-examination to the final determination of the case by the court.

During the first phase, digital evidence assessment, the legal foundations of digital evidence are established. The relevance of the evidence to the case is determined by the court after legal authorization is established. This phase covers pre-trial activities in most jurisdictions. The trial could be terminated at this stage if a proper legal foundation is not established.

If the proper legal foundation is established, the case moves to full trial corresponding to the second phase – digital evidence consideration. The prerequisite requirements, core requirements and evaluation requirements, which are all technical determinants listed in Figure 2, are assessed during this phase.

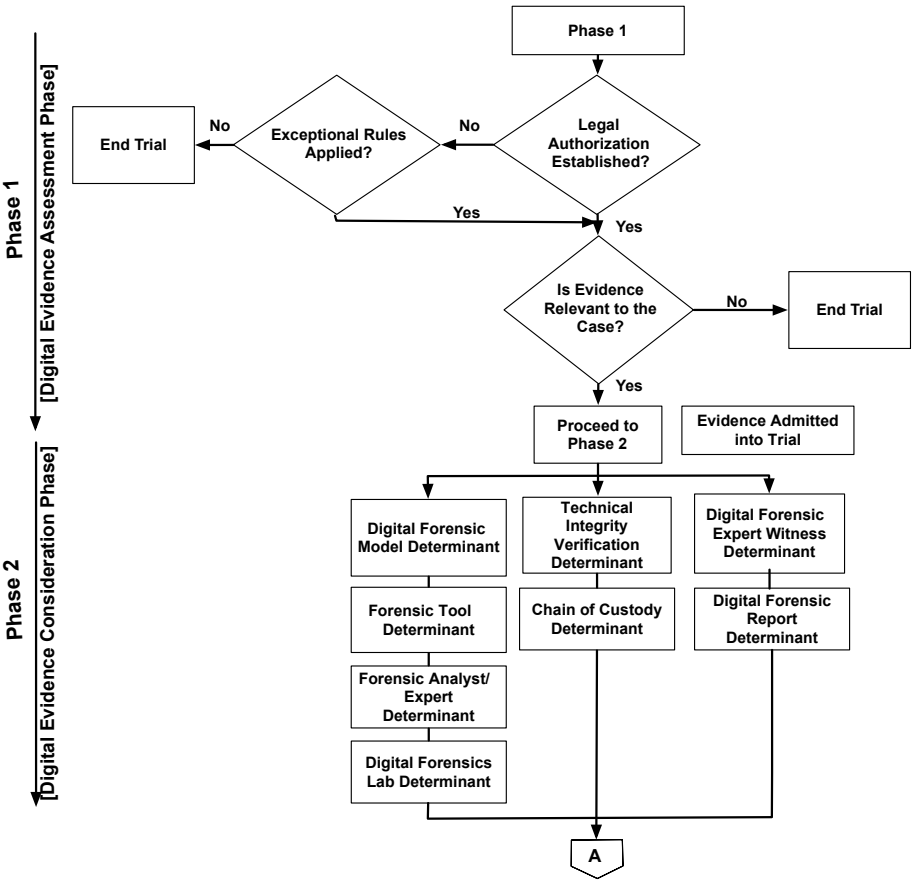


Figure 7. Flowchart of the digital evidence assessment and consideration phases.

The third phase, digital evidence determination, forms the basis of judicial decisions. In most jurisdictions, the decision could be acquittal or conviction and sentencing. The sentence would be the maximum, average or minimum based on the evidential weight established through the operationalization of the harmonized model.

5. Evidential Weight Determination

This section presents the foundation for determining the evidential weight of digital evidence using the determinants discussed in this chapter.

Evidential weight is the weight that a judge would attach to a particular piece of evidence that is tendered in a court of law. According to Mason [15], assessing evidential weight involves scrutinizing a piece

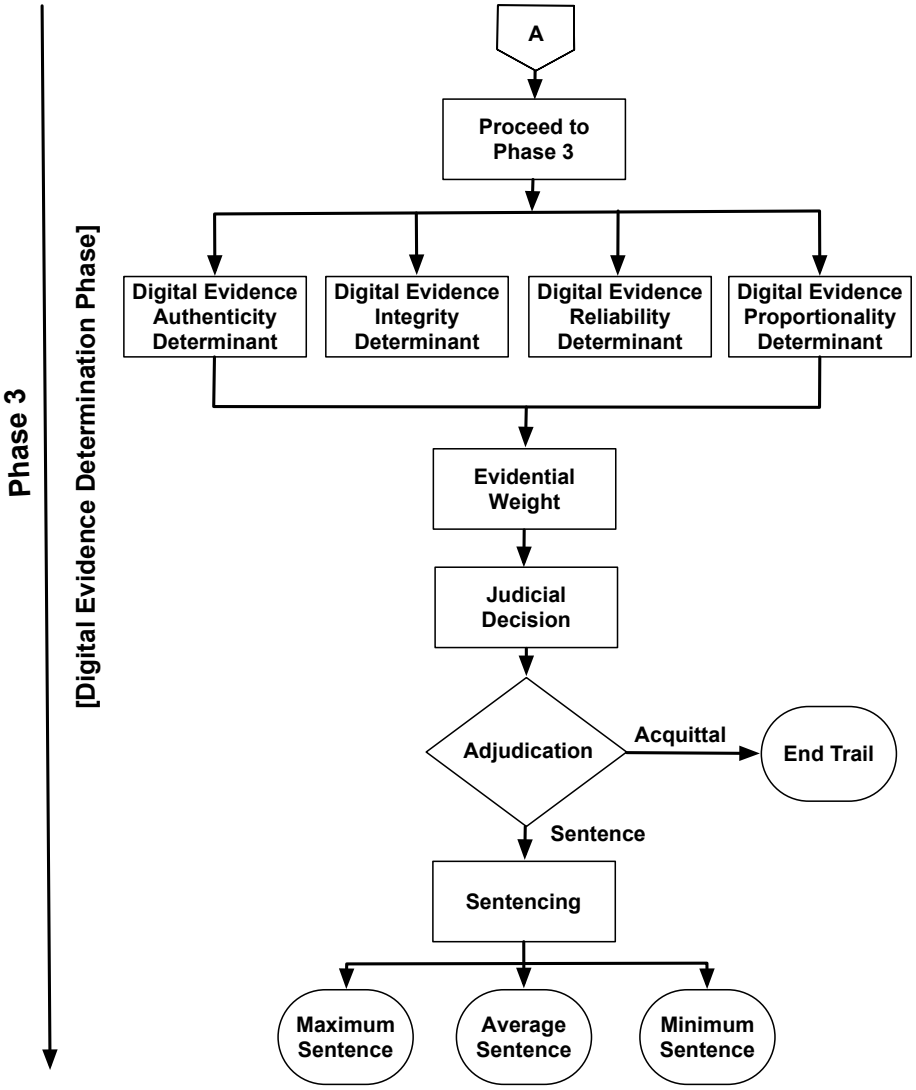


Figure 8. Flowchart of the digital evidence determination phase.

of evidence and deciding whether or not it is acceptable and relevant to arriving at a decision during a trial.

The research described in this chapter employed factor analysis [5] to statistically analyze the survey data in order to determine evidential weight. Factor analysis was selected because it is well suited to exploratory data analyses. In particular, it was used to obtain the weights of the variables required to make judicial decisions. The survey con-

ducted in this research provided the data used to operationalize factor analysis [16].

In order for a dataset to be suitable for factor analysis, a correlation must exist between the determinants and it must pass the Kaiser-Meyer-Olkin (KMO) sampling adequacy test. The correlations between the determinants were computed using the sample Pearson correlation coefficient [21] as follows:

$$r = \frac{N\sum xy - (\sum x)(\sum y)}{\sqrt{[N\sum x^2 - (\sum x)^2][N\sum y^2 - (\sum y)^2]}} \tag{1}$$

where r is the correlation coefficient between determinants x and y (x and y are the individual survey responses); N is the number of survey respondents; $\sum xy$ is the sum of the products of paired x and y scores; $\sum x$ is the sum of x scores; $\sum y$ the sum of y scores; $\sum x^2$ the sum of squared x scores; and $\sum y^2$ is the sum of squared y scores.

Note that the correlation is calculated for each pair of determinants. Also, the numerator in the equation is the covariance between the two determinants and the denominator is the product of the standard deviations of the two determinants.

The Stata statistical software package [19] was used to compute the correlations. For example, a correlation of 0.324962 was established between the forensic tool (FT) and digital forensic model (DFM) determinants, and a correlation of 0.500934 was established between the legal authorization (LA) and technical integrity verification (TIV) determinants.

The KMO sampling adequacy test was performed to ensure that the dataset was suitable for factor analysis. The KMO sampling adequacy varies from zero to one; a value close to one denotes well suited to factor analysis whereas a value close to zero denotes inappropriate for factor analysis. A KMO sampling adequacy value of 0.77 was obtained, suggesting that the dataset is adequate for factor analysis [20].

Factor analysis assumes that a linear relationship involving the latent factors exists in the survey data. In general, a factor $factor_{nj}$ in the data is expressed as:

$$factor_{nj} = b_1X_{1j} + b_2X_{2j} + ... + b_nX_{nj} + e_j \tag{2}$$

where the b_i terms denote factor loadings (e.g., factor scores such as that relating determinant FT to determinant DFM as computed by Stata); X_{ij} terms correspond to the determinants; j is an observation (i.e., factor); n is the number of variables (i.e., number of determinants); and e_j is an error term.

The coefficient formula for the determinants is given by:

$$\begin{aligned}\text{Factor Analysis of Determinants} &= b_1 DFM + b_2 FT + b_3 CoC + \\ &\quad b_4 FAC + b_5 DFL + b_6 TIV + \\ &\quad b_7 DFEW + b_8 DFR + b_9 LA + \\ &\quad b_{10} DERe + b_{11} DEA + \\ &\quad b_{12} DEI + b_{13} DERI + \\ &\quad b_{14} DEP + e_j \end{aligned} \tag{3}$$

The b_i values in Equation (3) are used to compute the evidential weight EW as follows:

$$\begin{aligned} EW &= w_1 DFM + w_2 FT + w_3 CoC + \\ &\quad w_4 FAC + w_5 DFL + w_6 TIV + \\ &\quad w_7 DFEW + w_8 DFR + \\ &\quad w_9 LA + w_{10} DERe + \\ &\quad w_{11} DEA + w_{12} DEI + \\ &\quad w_{13} DERI + w_{14} DEP + \\ &\quad e_j \end{aligned} \tag{4}$$

where the w_i terms correspond to the determinant weights Wd_i computed as:

$$Wd_i = \frac{b_i n^2}{\text{Total Variance}} \tag{5}$$

Note that i denotes a determinant; n is the number of determinants; b_i is a factor score generated by factor analysis; and the total variance is the sum of the squares of the b_i factor scores.

Table 2 presents the computed factor loadings $b_i n^2$ and determinant weights Wd_i based on the survey results.

6. Results and Discussion

The equations presented in the previous section were applied to a hypothetical case involving digital evidence. Table 3 presents the results obtained by applying factor analysis to evidence in the hypothetical case. In the table, a determinant weight Wd_i denotes the weight of determinant i as established by factor analysis. A determinant score Sd_i in the table, which corresponds to the score assigned to determinant i by the court for the case in question, is given by:

Table 2. Evidential weight determination.

Determinant	**Factor Loading ($\mathbf{b_i}$)**	**Factor Score ($\mathbf{b_i n^2}$)**	**Determinant Weight ($\mathbf{Wd_i}$)**
DFM	0.247633	0.061322	0.034
FT	0.412889	0.170477	0.095
CoC	0.344163	0.118448	0.066
FAC	0.372313	0.138617	0.025
DFL	0.212455	0.045137	0.077
TIV	0.371712	0.138170	0.077
DEFW	0.237606	0.056457	0.031
DFR	0.326640	0.106694	0.059
LA	0.240957	0.058060	0.032
DERe	0.193218	0.037333	0.021
DEA	0.495371	0.245393	0.136
DEI	0.611801	0.374300	0.208
DERl	0.332325	0.110440	0.061
DEP	0.375614	0.141086	0.078
Total Variance		1.801933	

Table 3. Evidential weight determination and analysis.

Determinant	**Determinant Weight ($\mathbf{Wd_i}$)**	**Determinant Score ($\mathbf{Sd_i}$)**	**Weighted Value ($\mathbf{Wv_i}$)**
DFM	0.034	3.8	0.129
FT	0.095	4.5	0.428
CoC	0.066	3.0	0.198
FAC	0.025	2.5	0.063
DFL	0.077	3.4	0.262
TIV	0.077	2.3	0.177
DFEW	0.031	5.0	0.155
DFR	0.059	4.7	0.277
LA	0.032	3.7	0.118
DERe	0.021	4.2	0.088
DEA	0.136	4.0	0.544
DEI	0.208	2.4	0.499
DERI	0.061	3.6	0.220
DEP	0.078	3.5	0.273
Total Evidential Weight	3.431		

$$Sd_i = \frac{\text{Sum of Assessment Scores}}{\text{Total Mark}} \times 5 \quad (6)$$

where each determinant has a maximum mark allocation of five.

Each of determinants is assessed in court using different parameters, which are essentially the key questions addressed during evidence presentation and cross-examination. For example, relative to the digital forensic tool (FT) determinant, the following key questions are considered to determine the score:

- Which forensic tool(s) was/were used in the forensic examination?
- Was the use of each tool licensed?
- Was open-source or proprietary software used?
- What are the implications of using each tool?
- Was each tool tested or validated?
- What is the error rate of each tool?
- What is the level of acceptance of each tool by the researcher and practitioner communities?
- Are there any scientific publications about each tool?

The answers to these questions are determined based on scientific and industry requirements in order to accept a forensic tool in digital investigations. While the questions are not exhaustive, they provide key assessment parameters that would be used in court to provide a score for the given determinant. A score of 4.5 for the digital forensic tool determinant was obtained by applying Equation 6. This value was computed for the determinant based on the assessment questions.

Using Equation 4 and the data in Table 3, the evidential weight is computed as:

$$\begin{aligned} EW = {} & 0.034DFM + 0.095FT + \\ & 0.066CoC + 0.025FAE + \\ & 0.077DFL + 0.077TIV + \\ & 0.031DFEW + 0.059DFR + \\ & 0.032LA + 0.021DERe + \\ & 0.136DEA + 0.208DEI + \\ & 0.061DERI + 0.078DEP \end{aligned} \quad (7)$$

The weighted value Wv_i, which corresponds to the evidential weight of determinant i, is computed as:

$$Wv_i = Wd_i \times Sd_i \tag{8}$$

where Wd_i is the weight of determinant i and Sd_i is the determinant score.

Thus, the total weighted value of all the determinants is given by:

$$\sum_{i=1}^{n} Wd_i Sd_i = Wd_1 Sd_1 + Wd_2 Sd_2 + Wd_3 Sd_3 + ... + Wd_n Sd_n \tag{9}$$

where n is the number of determinants.

Upon inserting the values from Table 3, the value of the evidential weight is computed as:

$$\begin{aligned} EW &= (0.034 \times 3.8) + (0.095 \times 4.5) + (0.066 \times 3) + \ldots (0.078 \times 3.5) \\ &= 3.431 \end{aligned} \tag{10}$$

Expressing the evidential weight as a percentage $EW\%$ yields:

$$\begin{aligned} EW\% &= \frac{EW}{5} \times 100 \\ &= \frac{3.431}{5} \times 100 \\ &= 68.62 \end{aligned} \tag{11}$$

The evidential weight of 3.431, which corresponds to 68.62%, is tendered in court and provides the basis for a judicial decision. The percentage value of the evidential weight could guide the court on the sentencing level, which can be the maximum, average or minimum sentence. However, it should be noted that judicial decisions are also impacted by other mitigating factors. This is because judges have certain discretionary powers under the law that they may exercise when they deem necessary. The mitigating factors include the age of the accused, guilty plea, number of years already spent in custody, demonstration of remorse and other extenuating factors.

While there are limits to applying the harmonized model in judicial proceedings, it is important to emphasize that mitigating factors are considered after the model has provided a judge with scientific guidance to make a judicial decision. Therefore, any mitigating factors and the discretionary powers given to a judge as an arbiter of justice do not affect the scientificness of the harmonized model as a judicial tool.

7. Conclusions

The algorithm presented in this chapter operationalizes the harmonic model for digital evidence admissibility assessment and customizes the model to enable the determination of evidential weight. The algorithm and evidential weight determination are designed to be used by judges in criminal proceedings. They should also be useful to investigators, prosecutors and defense lawyers for evaluating potential digital evidence before it is presented in legal proceedings.

It is important to note that advances in digital forensics are expected to impact the results of future surveys of the type conducted in this research. Different results in future surveys would result in different weights to the determinants as well as different sets of determinants. Such changes are to be expected in the rapidly-evolving field of digital forensics. Nevertheless, the harmonized model, survey research methodology and evidential weight determination framework are sound and robust, implying that surveys would have to be conducted periodically to generate new data, determinants and determinant weights that will keep up with trends in digital forensics and how digital evidence is used in legal proceedings.

Future research will focus on developing an expert system that operationalizes the harmonic model for digital evidence admissibility assessment. The expert system, which will draw on concepts from computational forensics [11], could be applied in real cases, including jury trials, to establish the utility of the harmonized model across the various types of criminal proceedings.

References

[1] S. Alabdulsalam, K. Schaefer, T. Kechadi and N. Le-Khac, Internet of Things forensics: Challenges and a case study, in *Advances in Digital Forensics XIV*, G. Peterson and S. Shenoi (Eds.), Springer, Cham, Switzerland, pp. 35–48, 2018.

[2] A. Antwi-Boasiako and H. Venter, A model for digital evidence assessment, in *Advances in Digital Forensics XIII*, G. Peterson and S. Shenoi (Eds.), Springer, Cham, Switzerland, pp. 23–38, 2017.

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

[4] D. Bertram, Likert Scales ...are the Meaning of Life, CPSC 681 – Topic Report (`poincare.matf.bg.ac.rs/~kristina/topic-dane-likert.pdf`), 2008.

[5] A. Bryman and D. Cramer, Constructing variables, in *Handbook of Data Analysis*, M. Hardy and A. Bryman (Eds.), SAGE Publications, London, United Kingdom, pp. 18–34, 2004.

[6] L. Burton and S. Mazerolle, Survey instrument validity, Part I: Principles of survey instrument development and validation in athletic training education research, *Athletic Training Education Journal*, vol. 6(1), pp. 27–35, 2011.

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

[8] D. Child, *The Essentials of Factor Analysis*, Bloomsbury Academic, London, United Kingdom, 2006.

[9] T. Cowper and B. Levin, Autonomous vehicles: How will they challenge law enforcement? *Law Enforcement Bulletin*, FBI Training Division, Federal Bureau of Investigation, Quantico, Virginia (`leb.fbi.gov/articles/featured-articles/autonomous-vehicles-how-will-they-challenge-law-enforcement`), February 13, 2018.

[10] I. Etikan and K. Bala, Sampling and sampling methods, *Biometrics and Biostatistics International Journal*, vol. 5(6), article no. 00148, 2017.

[11] K. Franke and S. Srihari, Computational forensics: An overview, *Proceedings of the Second International Workshop on Computational Forensics*, pp. 1–10, 2008.

[12] S. Goodison, R. Davis and B. Jackson, Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, Technical Report RR 890-NIJ, RAND Corporation, Santa Monica, California, 2015

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

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

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

[16] Organisation for Economic Co-operation and Development, *Handbook on Constructing Composite Indicators: Methodology and User Guide*, OECD Publishing, Paris, France, 2008.

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

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

[19] StataCorp, Stata Release 15, College Station, Texas (`www.stata.com/products`), 2019.

[20] Statistics How To, Kaiser-Meyer-Olkin (KMO) Test for Sampling Adequacy (`statisticshowto.com/kaiser-meyer-olkin`), 2016.

[21] Study.com, Pearson Correlation Coefficient: Formula, Example and Significance, Mountain View, California (`study.com/academy/lesson/pearson-correlation-coefficient-formula-example-significance.html`), 2019.

[22] H. Taherdoost, Validity and reliability of the research instrument: How to test the validation of a questionnaire/survey in a research, *International Journal of Academic Research in Management*, vol. 5(3), pp. 28–36, 2016.

[23] Technical Working Group for Electronic Crime Scene Investigation, Electronic Crime Scene Investigation: A Guide for First Responders, NIJ Guide, NCJ 187736, U.S. Department of Justice, Washington, DC, 2001.

[24] R. Trotter, Qualitative research sample design and sample size: Resolving and unresolved issues and inferential imperatives, *Preventive Medicine Journal*, vol. 55(5), pp. 398–400, 2012.

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

[26] S. Weller and A. Romney, *Systematic Data Collection*, SAGE Publications, Newbury Park, California, 1988.