15th International Conference on Electronics Computer and Computation (ICECCO 2019)

A SYSTEMATIC LITERATURE REVIEW ON DIGITAL EVIDENCE ADMISSIBILITY: METHODOLOGIES, CHALLENGES AND RESEARCH DIRECTIONS

Elizabeth Ozioma Edward
Department of Cyber Security Science
Federal University of Technology
Minna, Nigeria
lizysteve@yahoo.com

Joseph A. Ojeniyi
Department of Cyber Security Science
Federal University of Technology
Minna, Nigeria
ojeniyija@futminna.edu.ng

***Abstract*—Admissibility of Evidence is the eligibility of particular pieces of evidence for inception as part of the evidence in a case. Admissibility means the character or quality to be accepted and allowed to be presented or introduced as evidence in court. To be admissible means capable of being legally admitted or allowable or permissible as evidence or worthy of gaining entry or being admitted. This study focus on carrying out a systematic literature review and meta-analysis on Digital Evidence Admissibility. The methodology employed in this study was the querying of four academic database resources systematically and fundamentally identifying kinds of literature related to digital evidence admissibility through identification, screening, eligibility and inclusion criteria. The advantage of this study is revealing the gap and trends in digital evidence admissibility as the article published between the period of 2015 through 2018 are relative with the following variation 64%, 21% 7%, for the following respectively, IEEE, Science Direct, ACM Digital library, as well as Research Gate. While at the period under review, 2019 is yet to record publication in the field of research in Digital Evidence Admissibility. The period under review witnessed a low academic publication in the field of Digital Evidence admissibility. This research will aid in projecting future research in the aforementioned research field.**

***Index Terms*—Digital Evidence, Digital Forensics, Evidence Admissibility, Systematic Review, Research Database.**

I. INTRODUCTION

Digital evidence is used commonly in computing and electronic environment where information is converted to binary form as in digital audio and digital photography. According to [1], digital evidence can be described as information of probative values stored or transmitted in a binary format that can or may be relied on in the court of law. The birth of digital communication and technology has helped to remove a lot of obstacles in the traditional method of evidence collection and the conventional media associated with it, although the emergence of the internet, social media, and the mobile technology has changed our way of living and businesses [2].

It is impossible to eliminate all crimes especially with the advent of technology in our world today because we are surrounded by digital devices that are used to carry out activities even to financial transactions. Any device that is part of one's life or organization can generate information that can be used as evidence, this evidence can be necessary for research on cybercriminals, hacking activities, phishing. Devices such as our smartphones, gaming console desktops, and laptop systems have become part of our modern society. With this device in place, the tendency to use the information derived from this device for criminal activities is high, hence, crimes such as fraud, drug trafficking, homicide, hacking forgery, and terrorism often involve computer systems. [3].

Digital evidence helps to investigate the crimes or identify direct evidence of computer-assisted crimes. Digital evidence dated back to the late 1990s and early 2000s when it was considered digital evidence. The legal profession, law enforcement agencies, policymakers, business community, education, and the government had a vested interest in digital evidence. The presentation of this evidence involves report preparation to present the findings to relevant stakeholders including the judge, jury, accused, lawyers and the persecutor as well. This report must be presented in a way that is suitable to the court of law [4].

Digital Evidence is any information of probative value that is either stored or transmitted in a binary form. Digital Evidence includes computer evidence, cell phones, digital fax, digital video, digital audio [5].

While Digital Evidence exploitation is more or less a new tool for law enforcement investigations, law enforcement depends mostly on digital evidence for major information about victims and suspects. As a result of the potential

978-1-7281-5160-1/19/$31.00 ©2019 IEEE

quantity of digital evidence present, cases, where such evidence is lacking, cannot easily be developed [6].

Admissibility of Evidence is the eligibility of particular pieces of evidence for inception as part of the evidence in a case. Admissibility means the character or quality to be accepted and allowed to be presented or introduced as evidence in court. To be admissible means capable of being legally admitted or allowable or permissible as evidence or worthy of gaining entry or being admitted [7].

Summary of the key contributions of this study are outlined below;

- We systematically assess related work on Digital Evidence Admissibility across four academic databases using a systematic literature review algorithm.
- We analyze existing digital evidence admissibility mechanisms using descriptive and quantitative approaches
- We propose future research directions in mitigating the existing challenges

The study aims to carry out a systematic literature review and meta-analysis on Digital Evidence Admissibility.

The remaining sections of the paper were arranged as follows Section II presents related literature. Section III reveals the methods employed in the research. Section IV presents the results and Section V shows the conclusion and recommendation.

II. RELATED LITERATURE

Their work in [8], synthesized and summarized the existing studies on Ensemble Effort Estimation techniques. The ensemble techniques were examined from six perspectives which are: the single models used to construct the ensembles, the estimation accuracy of ensemble techniques, the rules used to obtain the estimates, comparison of single models and EEE techniques in terms of accuracy, the methodologies used to construct ensembles, and the context favorable to the use of EEE. However, the authors in their research were able to cover studies published between January 2000 and January 2016. Besides, 24 empirical studies were identified. Also, they identified four methodologies that they used to construct ensembles of which three of them rely principally on statistical tests to select the best candidate models.

Choosing an appropriate threat analysis technique has become a big issue for practitioners due to a large number of existing techniques. [8], the authors compared 26 methodologies for the following: applicability, characteristics of the required input for analysis, characteristics of analysis procedure, characteristics of analysis outcomes and ease of adoption. Also, they gave an insight into the impediment for embracing the existing approaches. However, in their findings, they observed the following: the analysis procedure was not precisely defined, there is a lack of quality assurance of analysis outcomes and tools support and validations are limited.

When digital evidence is put forward in a court of law, it is often associated with a scientific evaluation of its importance or significance. When experts are faced with the validity of the Digital Evidence, the popular answer is yes to a reasonable degree of scientific certainty. [9] in their work solved the problem of weighted Digital Evidence using a novel methodology which are as follows: Digital Evidence Inventory (DEI) in other to provide digital forensic experts with the ability to capture evidence, Forensics Confidence Rating (FCR) structure which gives experts the ability to rate the level of confidence for each evidence, Global Digital Timeline (GDT) which can order evidence through time. Also, a sound digital evidence was achieved which was expressed in terms of confidence and ordered through a timeline. However, the authors recommended that more precise confidence of error rating probabilities and a semi-automated tool for the building of the Global Digital Timeline.

According to [10], any digital device produces information that may be of valuable evidence in the outcome of a cybercrime incident, security incident, or cyber-attack. Though the information often collected are not properly managed and preserved. It is often said that in the legal ground, once and information has been captured from the devices, it is of most important to keep and preserve it from the initial time. As a result, the authors solved the problem of improper preservation and management of digital evidence collection using a long term preservation technique. Furthermore, they re-examined the state-of-the-art about digital preservation in institutions, which was dedicated to a criminal investigation, analyzing the concept, related projects, tools and legal support in this area. However, the authors advised that a random sample with a larger scale of respondents should be put into serious consideration, a summary of the articles included for full-text review is reflected in Table I.

TABLE I. SUMMARY OF WORK INCLUDED FOR FULL-TEXT REVIEW

Author	Problem Being Solved	Method used	Result/Achievement	Limitations/Gaps
[9]	Weighted digital evidence.	1. Digital evidence inventory (DEI). 2. Forensics confidence rating (FCR). 3. Global digital timeline (GDT).	A sound digital evidence was achieved, expressed in terms of confidence and ordered through a timeline.	More precise confidence of error rating probabilities and a semi-automated tool for the building of the GDT
[10]	Improper preservation and management of	A long term preservation technique was used.	Re-examined state-of-the-art digital preservation in institutions, dedicated to a	Preserving digital evidence and ensuring integrity and increasing its admissibility.

	digital evidence collection.		criminal investigation, analyzing the concept, etc.	
[11]	Multimedia presentations can improve the understanding of technical terms and concepts presented in digital forensics.	A questionnaire-based survey using a convenient sample of judges, investigators, prosecutors, and staff in government and the legal system.	An indication that multimedia presentations can effectively improve training participant's skill of technical terms and concepts, in a digital forensic domain.	Considering a random sample with a larger scale of respondents.
[12]	Collecting volatile digital evidence.	The digital evidence management framework (DEMF) model was used in collecting volatile digital evidence.	DEMF model is good in improving the integrity and authenticity of the collected evidence in court.	Using the DEMF model to prove the integrity of the collected evidence in court.
[13]	Investigation of multiple devices in digital forensic.	A cloudlet-based digital forensic (DF) approach to complement existing cloud computing systems.	Cloudlet-based DF resource optimization, facilitate upward and downward scaling of resources to cope with a variety of data sizes, multiple devices, and concurrent multiple cases.	Further development and implementation of a cloudlet-based digital system.
[14]	Collisions in cryptographic hash function used in digital forensic tools.	They used a secure hash algorithm (SHA) to check the integrity of digital evidence.	The hashing algorithm was found to have a weakness called collision in which two different messages have the same hashing values.	The validity of digital evidence in the context of digital forensics to ensure the admissibility of evidence in court.
[15]	Using network event logs as admissible digital evidence	An event correlation model was used to collect available logs from connected network devices, then decision tree algorithm was applied to filter anomaly intrusion.	They introduced a new network forensics model that makes network event-logs admissible in the court of law.	Developing an automated tool for digital investigators for effective visualization of the victim's network structure.
[16]	Prototype for guidance and implementation of a standardized digital forensic investigation process.	An evaluation of the prototype was performed in two parts: 1. Using the software usability measurement inventory (UMI) to measure the reliability and quality of software. 2. A questionnaire was set up to evaluate whether the prototype meets its goals.	An indication that the prototype reaches most of its goals and is relatively easy to learn and uses the deployment of a procedure called last-on-scene (Los) algorithm for improving traceability and reduces overhead digital forensic complications.	Improving usability, allowing users to upload predefined XML files with keywords and also implementing proposed changes gathered from the evaluation testing.
[17]	IoT challenge in performing forensic investigation in digital evidence acquisition and analysis phases.	They deployed a procedure called last-on-scene (Los) algorithm which was used to improve traceability and reduces the overhead as well as digital forensic complications.	An improved theoretical framework for IoT forensic model that can cope with evidence acquisition was put forward.	Implement a proposed framework based on the Los algorithm and creating the needed testing in a real environment to prove its applicability.

III. METHODOLOGY

Few databases were explored to gather important literature related to Digital Evidence Admissibility. The articles were systematically examined using the identification of fundamental studies with other techniques. The research procedure followed in this work scaled through important papers from various academic databases as shown in Table II.

TABLE II. DATABASE, WEB ADDRESS, AND ARTICLE NUMBER

S/N	SOURCES	URL	NO OF ARTICLES
1.	ACM Digital Library	URL:http://dl.acm.org/	1
2.	Science Direct	URL:http://www.sciencedirect.com/	28
3.	IEEE Explore	URL:http://ieeexplore.ieee.org/	9
4.	Research Gate	URL:http://www.researchgate.net/	1
		Total	39

The research design in Fig. 1 represents the various mechanisms exploited in this research work using a systematic literature review algorithm in carrying out the research work.

A. Identification

The search term that was used in this work is digital evidence admissibility. Four Academic databases were used for the search which is: science direct, ACM digital library, IEEExplore, and research gate. Articles between the periods of four years were identified in the various databases which amount to a total number of 39 articles.

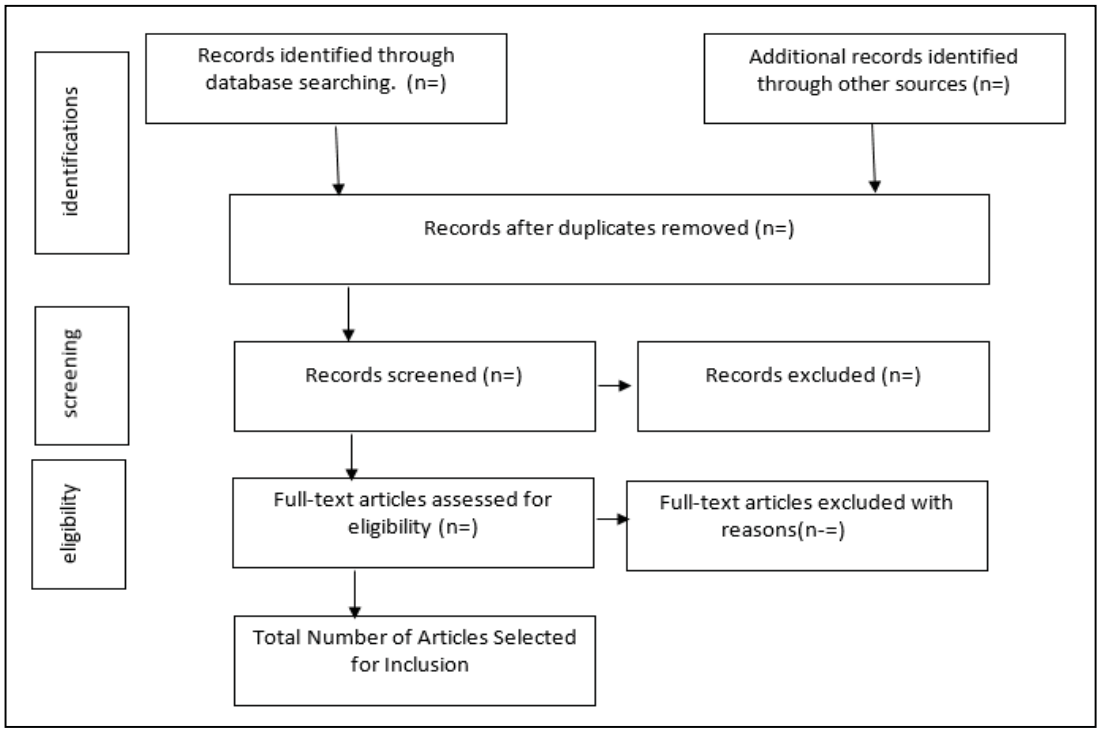

Figure 1 *Research Design*

B. Screening

Screening is the first step of a systematic review in which duplicates of articles that are common in search results are removed where possible before eligibility screening starts. After reading through the abstract and the title, the papers were screened and reduced to some 14 articles.

C. Eligibility

The eligibility step of a systematic review involves the application of eligibility criteria that determines which of the primary research studies Identified are relevant to the search term that was used to get primary sources. The eligibility of the papers was determined due to full-text assessment of the papers and were able to get a total of 9 articles.

IV. RESULT

a) Information Source and Coverage

Table III shows the breakdown of the search used for the systemic literature review. The search term used to navigate these databases is digital evidence, evidence admissibility, and digital evidence admissibility.

TABLE III. DATABASE AND COVERAGE

	SCIENCE DIRECT	ACM DIGITAL LIBRARY	IEEE XPLORE	RESEARCHGATE	Total
Identification (1993 to 2019)	142	1824	26	21	2013
Identification (2015 to 2019)	28	1	9	1	39
Screening(title or abstract)	3	1	9	1	14
Eligibility(full-text assessment)	1	1	6	1	9

b) Systematic Review of Articles

The Algorithm in Fig. 2 represents the strategy implemented in a systematic literature review on digital evidence admissibility. It shows the steps involved in the systematic review, the various databases sourced and the numbers of paper publications each specified year.

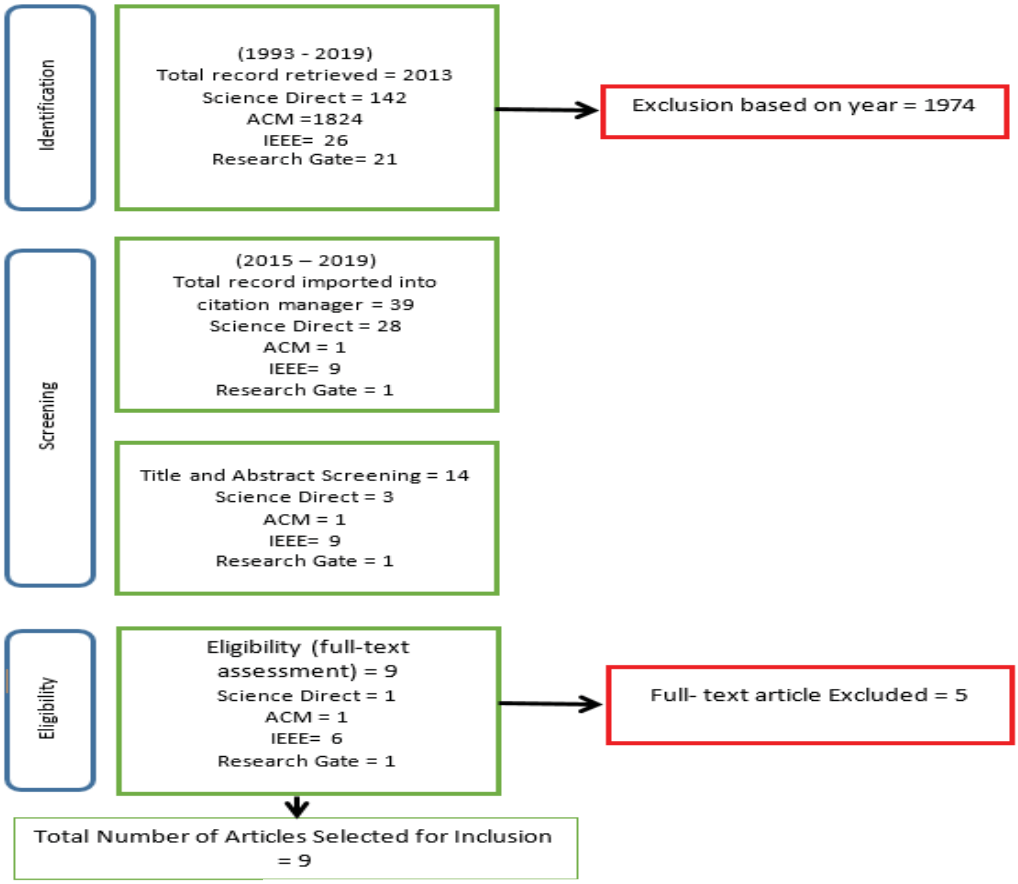

Figure 2. *A systematic literature review*

c) Distribution of academic papers by year of publication

The study analyses 9 research papers published between the years 2015 to 2019. The reason for the descriptive analysis is to provide interesting views regarding recent research trends in digital evidence admissibility, and also helps to visualize the diverse discipline research approaches developed so far in the systematic literature.

Furthermore, it supports the classification structure that is presented in Table IV. The descriptive analysis is based on two basic criteria which are: Distribution of academic papers spread across the year 2015 to 2019, and academic database sources, distribution of academic papers spread across the year 2015 to 2019.

The study as shown in Fig. 3 discovered that publications of papers in respect to Digital Evidence Admissibility in the year 2015 through 2017 are steady, having 4 publications each, however, publications from IEEE research database in 2015 and 2017 witnessed exponential growth to research gate and science direct within same period of year, an inverse was experienced in 2016 publication in which science direct had 3 publications and IEEE research database had 2 publications in respect to digital evidence admissibility, while 2019 experienced a null publication as of the time of compiling this review.

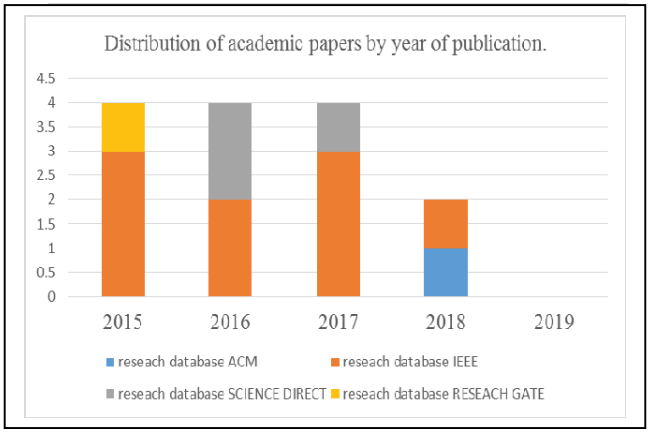

Figure 3. *Distribution of academic papers by year of publication*

Table IV. List of database sources with several articles.

Database Journals	Number of articles
ACM Digital library	1
Science direct	3
IEEE Explore	9
Research Gate	1

In this research, it was observed that the IEEE research database has the highest paper publication of 9 articles as indicated in Table IV, with 64% of the entire articles reviewed in this research in digital evidence admissibility in the year 2015 to 2019 as shown in Fig. 4, while ACM digital library and research gate have the least publications in digital evidence admissibility in the same year under review, with an article each which is 7% of the total journals reviewed in this research work.

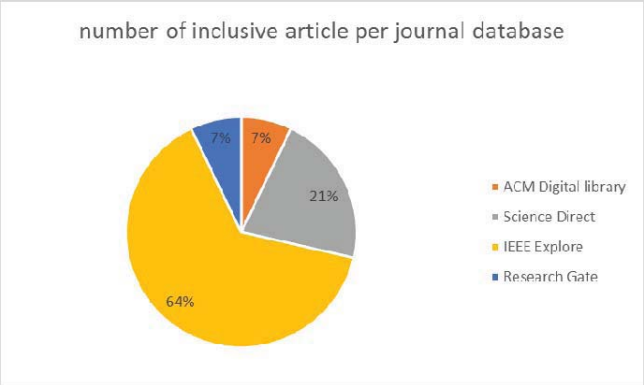

Figure 4. ***Number of inclusive articles per journal database***

d) Methodologies of Digital Evidence Admissibility

Few among other methodologies of Digital Evidence Admissibility reviewed in this work are 1.[9], used Digital Evidence Inventory (DEI), Forensic Conference Rating(FCR), and Global Digital Timeline (GDT) to solve the problem of Weighted Digital Evidence, achieve a sound digital evidence which was expressed in terms of Confidence and ordered through a timeline. 2.[10], used a long term preservation technique to address the problem of improper preservation and management of digital evidence collection. The result indicates that multimedia presentations can be used to effectively improve training participants' understanding in some technical terms and concepts particularly in the digital forensic domain. 3. [12], used the Digital Evidence Management Framework model to solve the problem of Volatile Digital Evidence collection, and the result shows that the DEMF model is good in improving the integrity and authenticity of the evidence collected in court. 4.[14] used a secured hash Algorithm to check the integrity of digital evidence in solving the problem of collisions in the cryptographic hash function used in digital forensic tools. Results showed that the hashing algorithm has a weakness called collisions in which two different messages have the same hashing values.

e) Challenges of Digital Evidence Admissibility

Digital Evidence Admissibility, has lots of challenges based on the literature reviewed. Which are: security, prominent and well-publicized area, cloud computing which limits its use as a sole platform for investigating Digital forensic data, likewise data ownership around what happens to data and how it is fragmented, challenge in maintaining evidence trial, inefficiency of network event logs as digital evidence because, in a typical network, the large number of event logs generated are increasingly becoming an obstacle for forensic investigators to analyze, detect and verify malicious activities. In using Digital Evidence Management Framework (DEMF) in the process of collecting volatile Digital Evidence, the Acquisition of volatile data for further forensic analysis also stands as a challenge to both practitioners and researchers.

f) Future Research Directions in Digital Evidence Admissibility

Directions for future research in this research work capture the limitations, gaps and future work found in Digital Evidence Admissibility. Progress has been made in systematic literature review but more needs to be done in Digital Evidence Admissibility to cover the following areas:

Research Direction 1: Automation framework and tool development for digital investigation enhancement visualization. A network forensic model has been introduced in this area which makes network event-logs admissible in the court of law by collecting available logs from connected network devices, and the decision tree algorithm was applied to filter anomaly intrusion. Therefore, future research should be devoted to the development of an automated tool that could help digital investigators to better understand and visualize the structures of victims.

Research Direction 2: Development and implementation of cloudlet-based Digital Forensic framework. The existing work focused on the investigation of multiple devices in digital forensics using a cloudlet-based forensic approach in complimenting the existing cloud computing systems. It will be important that future research should focus on the development and implementation of the cloudlet-based digital forensic framework.

Research Direction 3: Implementation details and analysis of Last on Scene based framework involving legal procedures in agreement with international laws, data privacy laws differences and their relationships to IoT. Studies have shown that there are various problems faced by the Internet of Things(IoT) in performing a forensic investigation in digital evidence acquisition and analysis phases. As a result, a procedure called Last on Scene Algorithm(LOS) has been deployed in this work which was used to improve traceability and also reduces the overhead, as well as digital forensic complications and an improved theoretical framework for IoT forensic model that can cope with evidence acquisition, was proposed. Future research should, therefore, focus on the implementation of the proposed framework based on the Los Algorithm and also creating the needed testing in a real environment to prove its applicability.

Research Direction 4: Refinement-based video content and Native-language based Narration for enhancing understanding of Digital Evidence. Studies in the existing work examine the extent to which multimedia presentations can help in the improvements and understanding of technical terms and concepts presented in digital forensics by conducting a questionnaire-based survey using a convenient sample of judges, investigators, prosecutors and staff in government and the legal system. However, results from the study indicate that multimedia presentations can be used to

effectively improve training participant's understanding of technical terms and concepts, particularly in the digital forensic domain. Future work should consider a random sample with a larger scale of respondents. This simply means that an online survey could be utilized to reach more participants from different areas, which would improve the statistical soundness of the data. Future studies should also include refinements for the video content and the use of the participant's native language for audio narration.

Research Direction 5: A single information Unit based and environment preserving framework on Digital Evidence Admissibility. The existence of digital evidence preservation has no much progress as it relates to improper preservation and management of digital evidence collection considering the specific needs of each application environment. There is the need to improve on the existing work by Designing a Framework useful in preserving digital evidence and ensuring the integrity and increasing its admissibility. Therefore, evidence related content and environment should be treated as a single information unit.

Research Direction 6: Fine-tuning Algorithms for the blockchain protocol and a semi-automated tool for the building of the GDT in Weighting Forensic Evidence. Findings in the existing work have shown that digital evidence was weighted using three parameters which are: Digital Evidence Inventor (DEI) which provides digital forensics experts with the ability to form a digital evidence blockchain to capture evidence, Forensic Evidence Rating(FER) which gives experts the ability to rate the level of confidence for each evidence in a forensic confidence rating structure, and Global Digital Timeline(GDT) which was used to order evidence through time. Their results provide courts of law with sound digital devices, having a confidence level expressed in metrics and ordered through a timeline. Future research is needed in the area of fine-tuning Algorithms for the blockchain protocol and a semi-automated tool for the building of the GDT in weighting forensic evidence.

Research Direction7: Soft computing-based Framework with dynamic optimization enhancement. Soft computing refers to a partnership of methods to produce appropriate and low-cost production for hard problems. In this study, there are various challenges faced with as it relates to Digital Evidence Admissibility and they can be enhanced dynamically in the future by using soft computing methods to address them.

V. CONCLUSION AND RECOMMENDATION

The findings of this research work showed a relative variation in publication experienced between 2015 through 2018 across the explored academic resource databases as it relates to digital evidence admissibility and the quantification of publication between the aforementioned periods was low, with 2019 having no publication as at the time of conducting this research on Digital Evidence Admissibility. As a result of the discovery in this research, the author, therefore, recommend that a systematic review be conducted whenever possible for several reasons which are: systematic review in their very nature tend to be of high quality, more comprehensive and less bias than other types of literature review which makes them more likely to be published and to have an impact, The high quality and transparency of systematic reviews mean that they are relatively safe bet with academic markers and journal peer reviewers**.** It is far less stressful to conduct and far more manageable than other types of literature review because it involves breaking a potentially massive task down into sections and subsections and enables progress to be mentioned concretely, while in future work, more academic research databases need to be explored in other to widen the horizon knowledge on the research area under review.

REFERENCES

[1] V. Dubey, "Admissibility of Electronic Evidence : An Indian Perspective," vol. 4, no. 2, 2017.

[2] H. Arshad, A. Bin Jantan, and O. I. Abiodun, "Digital Forensics : Review of Issues in Scientific," vol. 14, no. 2, pp. 346–376, 2018.

[3] F. De Ingeniería and G. D. R. Rafael, "Model for digital evidence preservation in criminal research institutions – PREDECI Fernando Tiverio Molina Granja *," vol. 9, no. 2, pp. 150–166, 2017.

[4] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "International Journal of Advanced Research in Digital Forensics," vol. 7, no. 4, pp. 274–276, 2017.

[5] C. M. Whitcomb, "An Historical Perspective of Digital Evidence : A Forensic Scientist ' s View," vol. 1, no. 1, 2002.

[6] S. E. Goodison, R. C. Davis, and B. A. Jackson, "Digital Evidence"

[7] S. Idhiarhi, "Admissibility and evaluation of electronically generated evidence: practice and procedure," no. April, pp. 0–31, 2018.

[8] A. Idri, M. Hosni, and A. Abran, "PT US CR," *J. Syst. Softw.*, 2016.

[9] D. Billard, "Weighted Forensics Evidence Using Blockchain," in *International Conference on Computing and Data Engineering - ICCDE 2018*, 2018, pp. 57–61.

[10] F. M. Granja and G. D. R. Rafael, "Preservation of Digital Evidence : Application in Criminal Investigation," in *Science and Information Conference*, 2015, pp. 1284–1292.

[11] N. Dwi, W. Cahyani, B. Martini, and K. R. Choo, "Using Multimedia Presentations to Enhance the Judiciary ' s Technical Understanding of Digital Forensic Concepts : An Indonesian Case Study," 2016.

[12] M. Bača, J. Ćosić, and P. Grd, "Using DEMF in Process of Collecting Volatile Digital Evidence," in *39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2016, pp. 1442–1446.

[13] S. N. Mthunzi, E. Benkhelifa, Y. Jararweh, and M. Al-ayyoub, "Cloudlet Solution for Digital Forensic Investigation of Multiple Cases of Multiple Devices," pp. 235–240, 2017.

[14] Z. Erlisa, Z. E. Rasjid, B. Soewito, G. Witjaksono, and E. Abdurachman, "ScienceDirect 2nd International Conference A review of collisions in cryptographic hash function used in digital A review of collisions in cryptographic hash function used in digital forensic tools forensic tools," in *2nd International Conference on Computer Science and Computational Intelligences*, 2017, vol. 116, pp. 381–392.

[15] A. Al-mahrouqi, "Efficiency of Network Event logs as Admissible Digital Evidence," 2015.

[16] M. Ingels, "Evaluation and Analysis of a Software Prototype for Guidance and Implementation of a Standardized Digital Forensic Investigation Process," 2015.

[17] A. T. Framework, "An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I :," 2017.