International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Review of Computer Engineering Studies
Vol. 9, No. 3, September, 2022, pp. 111-115
Journal homepage: http://iieta.org/journals/rces

Current Issues and Challenges with Scientific Validation of Digital Evidence

Syed Atir Raza[1*], Aqsa Anwar[2], Abdul Hannan Khan[3]

[1] School of Information Technology, Minhaj University Lahore, Lahore 54000, Pakistan
[2] School of Software Engineering, Minhaj University Lahore, Lahore 54000, Pakistan
[3] School of Information Technology, Minhaj University Lahore, Lahore 54000, Pakistan

Corresponding Author Email: atirraza.it@mul.edu.pk

https://doi.org/10.18280/rces.090304

Received: 21 August 2022
Accepted: 20 September 2022

Keywords:
digital forensics issues, cloud forensics, IoT forensics, erroneous, standardization issues, social media forensics

ABSTRACT

Computer forensics is an important part of any cybercrime investigation because it allows law enforcement to collect and examine data that can be used to prove a cybercrime. Despite the occasionally justified use of proof, it is frequently met with skepticism and ambiguity in the courts. There is currently a moratorium on the use of untested forensic method in courtroom court cases, it is still difficult to consistently prove the proof obtained through this method. Because of the nature of electronic records and the privacy restrictions that surround them, it is no longer possible to rely solely on the information gathered through this process. The purpose of this article is to discuss current challenges and issues in the field of computer forensics that are impeding scientific validation of digital forensics.

1. INTRODUCTION

With the advent of virtual generation and communications, some of the old barriers associated with traditional types of media have been removed. However, the development of the internet, social networking sites such as Facebook, etc. and as well as mobile generations have fundamentally altered our way of life and the way the world does business. Regardless, it has created space for criminal activities to flourish. Due to modern-day communications which are now primarily virtual, electronic mail, text messages, pictures, and video in the form of digital data transmissions have now become the preferred way of interacting and communicating with each other.

As the new generation is speedily traveling towards a digital world time deviant individuals continue to exploit these advances to victimize others, now the time is that where people are not harming each other using ammunition but with a computer i.e. the era of cyber war. Individuals or maybe a country is involved for their own sake and crimes have been done through technology just to steal out the data or any digital information or to get money. If we go a few years back where we can see that criminals are identified by pictures, identities, etc. But now it is difficult to identify the criminal directly as digital crime is increasing and no one can identify who is the actual criminal due to the cybercrime era.

In order to investigate such crimes digital forensics have been introduced based on a traditional forensics investigation and which is a demand of the present era. Although it is thoroughly reviewed in criminal instances, electronic evidence is frequently used with great reluctance and care Notably, the evidence must demonstrate its veracity and authenticity in order to be admitted into a court of law [1, 2]. Additionally, modern legal norms do not accept any approaches that do not adhere to strict requirements of independence, impartiality, and objectivity [3-6]. However, digital forensics implementation is not an easy task for the investigators as there are many issues and challenges faced by the investigators during the different phases of the investigation which will make any digital evidence doubtful to present in the front of judiciary [7-9].

In this article we have discussed some general issues and challenges for a digital evidence scientific validation such as non-availability of data sets, erroneous, etc. and as well as module wise issues and challenges that digital forensics investigators are facing.

2. BACKGROUND OF DIGITAL FORENSICS

The term "forensic science" refers to a broad range of disciplines, each of which offers tools and procedures, used for the identification, collecting, analysis, and justification of evidence in judicial proceedings. Notably, given that all forensic sciences apply reliable principles and procedures in the assessment of the evidence that is referred to as scientific evidence, digital forensics is one of the key fields of study. Additionally, the evidence must be empirical because this type of evidence can be used to support or refute a theory and determine whether a person is guilty or not [10-13]. Although forensics science has been around for 100 years including the first record fingerprints, digital forensics is a much younger field at it is related to the digital world, which gained popularity after the introduction of the personal computer in 1980s. Consider that the FBI established the first actual forensic science lab in 1932 to help you grasp the concept of digital forensics, which is still relatively new. Some of the first digital forensic tills were developed by FBI labs around 1984, with forensics investigations spearheaded by the FBI's specialized CART (computer analysis and response team) which was responsible for assisting in digital investigations. [14-16].

The FBI hosted one of the first formal conferences in 1993 i.e. The International Law enforcement conference on Computer Evidence whose main goal was to address the need of formal standards and procedures in digital forensics and evidence acquisition and validation [17, 18].

Many of these conferences resulted in establishment of organizations concerned with digital forensics standards and best practices. The Federal Crime Laboratory Directors, for examples, established the SWGDE in 1998. The SWGDE was in charge of developing widely accepted best practices for computer evidence. The SWGDE also collaborated with other organizations such as the well-known American Society of Crime Laboratory Diectors (ASCLDs), founded in 1973 and has since played an important role in the ongoing development of best practices, procedures and training in forensic science. [19-21]. The Scientific Working Group on Digital Evidence (SWGDE) also looked into the topic of empirical validation in this area and presented a number of generic validation criteria [22, 23].

3. CURRENT CHALLENGES AFFECTING DIGITAL EVIDENCE ACCEPTANCE

In this research, a number of factors are taken into account that can be in opposition to the formal acceptance of digital forensics as a reliable and scientific subject. Notably, these problems are the most likely causes for the deficiency in formal forensic procedure testing and verification. The broad acceptance of digital evidence as being scientifically sound and legally sound will eventually be negatively impacted by the lack of empirical verification. Some of the challenges are as:

3.1 Non availability of standard datasets

With or without a standard the same data set can be used for a case's scientific investigation. The datasets selected depend greatly on the type of work being done. For instance, data set is required for a disease detection, facial dataset is required to find difference between Asian and non-Asian people. The comparison of two different approaches used for the same job, namely disease detection with the same input sources is also significant. The demand for effective testing has been increased as the field of computer forensics develops and works to establish a level of reliability in the methods employed by its practitioners. Testing requires test datasets, but creating them is a difficult task. Any testing performed using a test dataset that was not properly prepared and documented will be call into question, reducing the reliability of any subsequent testing. This has been found in other researches a comparable problem has been raised in the area of social media forensics and recommended depending on the publically available data component. However, there is a lot of publicly accessible social media data that is used in trails, the previously outlined strategy was not accepted for technique verification, standardization and toll comparison. Instead it might be preferable to create fewer reference datasets by replicating incidents of acknowledged electronic crime in various specified system-based scenarios [24, 25]. After having a detailed review of the literature the first issue and challenge in the field of digital forensics is found lack of standard datasets [26].

3.2 Erroneous

Time stamping is one of the most important module of digital forensics which is considered as a backbone of any forensics investigation that is being done digitally. Ten out of 100 randomly chosen computer forensics litigation cases studied recently alleged flaws in data collection and analysis, with only two of these cases having outcomes reserved. For irrelevant output and a wrong timestamp, the forensic software was held accountable. Evidence contamination during examination was also mentioned. The court found six of 13 additional appeals for sentence augmentation and sentence computation errors [8, 27].

In order to address problems in judicial process, the second criterion required linking an established error rate with the methods and equipment used for forensic data collection and analysis. The error rate, shown as false positives and false negatives is a measurement of how frequently errors occur in a given method. It is used to assess the strategy's accuracy and dependability. False positives are the number of incorrect indications that a specific condition attribute exists, whereas false negatives are the total number of incorrect indications that a condition or attribute does not exist. Notably, these error rates are utilized to quantify the associated accuracy and dependability of the approach as well as to define the confidence in a certain technique.

The random errors that result from unforeseen and unpredictable changes during the experiment are referred to by these error rates. The majority of mistakes made in digital forensic procedures are systematic rather than accidental; these mistakes are caused by the use of subpar or inappropriate techniques and instruments [8]. Therefore, estimating and assigning arbitrary error rates for any specific technique or software product does not vouch for its dependability and correctness. Furthermore, it is expected that crucial population components, such as blood for DNA analysis, remain constant for any accurate statistical computation [28, 29]. However, in areas with highly dynamic digital infrastructure, new media (such as Facebook, Instagram, snapchat twitter and cloud data) and hardware, such solid-state drives, are completely distinct from traditional media and devices. The tool or technique that worked well on one type of hard drive may not work at all well on another model [30-32]. Additionally, the investigative work done in digital forensics is incredibly dependent on the tools needed and required to interpret binary data. As a result, the speed and precision of scientific research in the field is a key factor in the success of analytical tools. There are two components to digital forensic software. First, the procedure or algorithm that determines how a task is to be carried out; this element is a part of systematic research and as well as some of the tools used for the digital evidence investigation are open source for which the error rate maybe higher which is the second major challenge in digital evidence validation and acceptance.

3.3 Issues with standardization

Computer forensics employs a wide range of electronic devices and data formats, all of which are property of various software developers and device manufacturers. It is difficult to develop standards for a diverse and large group of stakeholders. The parties' unwillingness to follow specific norms and rules complicates matters and frequently creates the possibility of conflicts interest between them. The academic and practitioner communities have long lamented the lack of Sops in computer forensics, emphasizing the importance of developing organized, dependable procedures for forensics investigations. Nonetheless, the domain has very few partially useful standards and practices [33, 34]. The fundamental causes of the lack of standardization are the explosive growth of underlying technologies in electronic calculation, storage, and communications. The most recent methods have also aided in the development of the new and expanding dimensions in the discipline, such as social media, cloud and IoT forensics. Many businesses are focusing on and capitalization on the recent interest in digital data and forensics these businesses rely on the variety of techniques and maximum privacy they offer clients and they are eager to provide users with as much variety and confidentiality as possible. In addition to this these elements continue to generate new complex legal and technical issues in this filed. Which results little progress in establishing adequate standards and best practices recommendations. The absence of best practices in specific fields, including the use of distinct methods in different regions can be seen as evidence of a lack of good practices or generally accepted norms in the scientific and legal communities. Furthermore, the Daubert standard's general acceptance criteria are severely hampered by this issue. Even the scientific community contributed to the development of best practices and guidelines times and again, scientists cannot enforce the adoption and application of best practices [5, 33].

3.4 Sub-fields of digital forensics are diverse and rapidly evolving

The majority of the validation issues that arise in digital forensics are the result of rapid advancements in electronic communications techniques and technology. This rapid development is making it difficult to establish analytical disciplines as legitimate science. Because of the speed and variety of newly developed techniques and gadgets in digital computing and communications it has been extremely difficult to develop good scientific ideas and rigorously test best practices for digital forensics. Social media, cloud networking and storage encryption methods and Internet of Things are few new technologies in the world of computer science and we all know that it takes a long time for any new field to mature into an exact science. In addition, each subject's beliefs and practices are contested and tested over time before being approved or disapproved based on established scientific criteria [35-37].

3.4.1 Issues in social media forensics

One of the subfield of digital forensics i.e. social media forensics has general difficulties with the main domain. Large datasets for conducting research are easily accessible through free social media platforms and other sources. Because of privacy laws or other constraints, most datasets cannot be shared or published by the owners of social media. Due to inherent bias in the majority of the collected datasets, publically available data sets are useful for general method testing but are insufficient for measuring and comparing the correctness and accuracy of various procedures. Another issue is determining how to incorporate and correlate data from social media in order to comprehend a crime [38].

The data is frequently used to establish a link between suspects, the crime and the victim, resulting in hundreds or even thousands of unrelated bit information being forensically obtained or analysis in single investigation. The procedure for correlating the data is typically fairly complex, causing information overload for the detectives or investigators. Furthermore, until the investigators can arrange the data into a single and unified representation the information may not make much sense or be useful in the investigation. Consistent data representation is therefore critical for quickly filtering out irrelevant material and obtaining insightful knowledge. However current methods and resources in the field do not support this feature [39].

3.4.2 Issues in cloud forensics

In cloud forensics only one of the many servers, thousands of virtual machines, and countless cloud users present at a cloud crime scene are pertinent to the inquiry. A actual gadget is almost tough to find or stop. Even if the investigators manage to access the actual device holding the data, it might not be the property of just one individual which is a big issue and challenge in digital evidence examination and acceptance [40].

3.4.3 Issues in multimedia forensics

There are numerous structures and processes in multimedia forensics for storing and capturing photos, music, and movies. As a result, forensics techniques used to evaluate and authenticate one format may or may not be applicable to other storage devices. As a result, assuming that they are appropriate in some wat without careful and controlled testing is incorrect. Another challenge is developing novel forensic tools and techniques for unusual or non-standard media types, formats and editing processes [41-43]. Because of the numerous types of multimedia data and the lack of unified and actual datasets the verification process in this case is difficult and time consuming. All of these issues are expected to make scientific validation much more difficult and problematic [24, 44].

3.4.4 Issues in IoT forensics

Forensics of IoT in comparison to what is currently saved in social media networks and the cloud, the IoT cloud store a broader range of data. In addition to their intended use, the number and type of connected devices may change, generating additional communication and mechanical data such as climatic temperature, speed capacity and so on. The resulting dataset would almost certainly be larger and more dynamic. Although IoT forensic disciplines are evolving there is currently little research looking into this specific filed particularly with open IoT-related vulnerabilities [45-49].

4. CONCLUSIONS

This has been concluded that digital forensic science is a legitimate field that has to develop over time, just like any other science. Without knowing the core limitations of scientific validity and the opposing facets of the field, it is inappropriate to refer to digital forensics as invalid science. The quickening pace of advancement in digital computing and communication technology reduces the amount of time that digital forensics has to develop. It is clear from the explanation that it would be unfair to hold the researchers accountable for their failure to make an effort to create scientific methodologies. As was previously indicated, underlying methods and technologies are developing really quickly. The different types of digital devices will continue to exist. They will employ various platforms and storage formats depending on their shape, structure, componentry, and communication mechanisms. Indeed, fresh and innovative technology replaces outdated technology every few months. Due to the quick growth and ongoing evolution of digital communications and technology, benchmarking in digital forensics is very challenging to implement. They are also extending the field of digital forensics at the same rate they are growing. To be fully probed, however, both the quality and scientific foundation of digital forensic methods are required for legal acceptability. Therefore, if the researcher follows appropriate procedure, even in the lack of globally recognized standards and specified procedures, they can still demonstrate the validity and reliability of their suggested or advanced methodologies. They should first define the validity and reliability standards for this purpose because doing so may allow them to explain the rules for discrete activities rather than creating the complete forensic process at once. The diversity and rate of evolution of the industry make it difficult, if not impossible, to create universal standards for digital forensics. Confirming the forensic procedures using conventional scientific testing methods, such as testing on a standard data corpus, is also difficult at the same time. Therefore, researchers can help improve the procedures that are presented and guarantee that the methods are reliable in order to meet the legal standards in the courts. Before using, the adopted approaches must be thoroughly tested and validated for accuracy. Prior to use, these methods must be known for their potential error rates and limitations in order to facilitate further testing under various conditions. Furthermore, obtaining the sound presumption of authenticity requires thorough testing and organized verification. Therefore, the only way to guarantee the development and continued sustainability of digital forensics is to employ extremely precise methods based on reliable scientific principles and foundations.

REFERENCES

[1] Harris, H.A., Lee, H.C. (2019). Examination of physical pattern evidence. Introduction to Forensic Science and Criminalistics, CRC Press, pp. 101-116. https://doi.org/10.4324/9781315119175-5

[2] Carew, R.M., Errickson, D. (2020). An overview of 3D printing in forensic science: The tangible third-dimension. J. Forensic Sci., 65(5): 1752-1760. https://doi.org/10.1111/1556-4029.14442

[3] Williams, P.A., Simpson, N.P., Totin, E., North, M.A., Trisos, C.H. (2021). Feasibility assessment of climate change adaptation options across Africa: An evidence-based review. Environ. Res. Lett., 16(7): 73004.

[4] Pelker, C.A., Brown, C.B., Tucker, R.M. (2021). Using Blockchain Analysis from Investigation to Trial. Dep't Just. J. Fed. L. Pr., 69: 59.

[5] Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. Comput. Law Secur. Rev., 42: 105575. https://doi.org/10.1016/j.clsr.2021.105575

[6] Neal, T.M.S., Slobogin, C., Saks, M.J., Faigman, D.L., Geisinger, K.F. (2019). Psychological assessments in legal contexts: Are courts keeping 'junk science' out of the courtroom? Psychol. Sci. Public Interes., 20(3): 135-164. https://doi.org/10.1177/1529100619888860

[7] Munkhondya, H., Ikuesan, A., Venter, H. (2019). Digital forensic readiness approach for potential evidence preservation in software-defined networks. ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS, vol. 268.

[8] Horsman, G. (2019). Tool testing and reliability issues in the field of digital forensics. Digit. Investig., 28: 163-175. https://doi.org/10.1016/j.diin.2019.01.009

[9] Neale, C., Kennedy, I., Price, B., Yu, Y., Nuseibeh, B. (2022). The case for Zero Trust Digital Forensics. Forensic Sci. Int. Digit. Investig., 40: 301352. https://doi.org/10.1016/j.fsidi.2022.301352

[10] Lucas, D.M. (2019). Junk Science' and Reasonable Doubt. Forensic Sci. Rev., 31(1): 20.

[11] Weinberg, M. (2021). Juries, judges, and junk science-expert evidence on trial. TheJudicial Review: Selected Conference Papers: Journal of the Judicial Commission of New South Wales, 14(4): 315-342.

[12] Sinha, M. (2021). Junk Science at Sentencing. Geo. Wash. L. Rev., 89: 52.

[13] Sinha, M. (2021). Radically Reimagining Forensic Evidence. Alabama Law Rev. Forthcoming, U Maryl. Leg. Stud. Res. Pap., no. 2021–10, 2021.

[14] Marshall, A.M. (2022). The unwanted effects of imprecise language in forensic science standards. Forensic Sci. Int. Digit. Investig., 40: 301349. https://doi.org/10.1016/j.fsidi.2022.301349

[15] Roy, S., Wu, Y., LaVenia, K.N. (2019). Experience of incorporating NIST standards in a digital forensics curricula. 2019 7th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-6. https://doi.org/10.1109/ISDFS.2019.8757533

[16] Stoykova, A. (2022). Standards for Digital Evidence: An inquiry into the opportunities for fair trial safeguards through digital forensics standards in criminal investigations.

[17] Solanke, A.A., Biasiotti, M.A. (2022). Digital forensics AI: Evaluating, standardizing and optimizing digital evidence mining techniques. KI-Künstliche Intelligenz, pp. 1-19. https://doi.org/10.1007/s13218-022-00763-9

[18] Humphries, G., Nordvik, R., Manifavas, H., Cobley, P., Sorell, M. (2021). Law Enforcement educational challenges for mobile forensics. Forensic Sci. Int. Digit. Investig., 38: 301129. https://doi.org/10.1016/j.fsidi.2021.301129

[19] Wilson-Wilde, L. (2018). The international development of forensic science standards—A review. Forensic Sci. Int., 288: 1-9. https://doi.org/10.1016/j.forsciint.2018.04.009

[20] Airlie, M., Robertson, J., Krosch, M.N., Brooks, E. (2021). Contemporary issues in forensic science—Worldwide survey results. Forensic Sci. Int., 320: 110704. https://doi.org/10.1016/j.forsciint.2021.110704

[21] Roux, C., Willis, S., Weyermann, C. (2021). Shifting forensic science focus from means to purpose: A path forward for the discipline? Sci. Justice, 61(6): 678-686. https://doi.org/10.1016/j.scijus.2021.08.005

[22] Bhat, W.A., AlZahrani, A., Wani, M.A. (2021). Can computer forensic tools be trusted in digital investigations? Sci. Justice, 61(2): 198-203. https://doi.org/10.1016/j.scijus.2020.10.002

[23] Kumar, G., Saha, R., Lal, C., Conti, M. (2021). Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. Futur. Gener. Comput. Syst., 120: 13-25.

https://doi.org/10.1016/j.future.2021.02.016

[24] Pasquini, C., Amerini, I., Boato, G. (2021). Media forensics on social media platforms: A survey. EURASIP J. Inf. Secur., 2021(1): 1-19. https://doi.org/10.1186/s13635-021-00117-2

[25] Basumatary, B., Kalita, H.K. (2022). Social media forensics-A holistic review. 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 590-597. https://doi.org/10.23919/INDIACom54597.2022.97631 2

[26] Horsman, G., Lyle, J.R. (2021). Dataset construction challenges for digital forensics. Forensic Sci. Int. Digit. Investig., 38: 301264. https://doi.org/10.1016/j.fsidi.2021.301264

[27] Horsman, G., Sunde, N. (2020). Part 1: The need for peer review in digital forensics. Forensic Sci. Int. Digit. Investig., 35: 301062. https://doi.org/10.1016/j.fsidi.2020.301062

[28] Horsman, G. (2018). I couldn't find it your honour, it mustn't be there!'–Tool errors, tool limitations and user error in digital forensics. Sci. Justice, 58(6): 433-440. https://doi.org/10.1016/j.scijus.2018.04.001

[29] Sommer, P. (2018). Accrediting digital forensics: What are the choices? Digital Investigation, 25: 116-120. https://doi.org/10.1016/j.diin.2018.04.004

[30] Chiang, C.P., Wang, S.J., Chen, Y.S. (2022). Manipulating cyber army in pilot case forensics on social media. J. Supercomput., 78(6): 7749-7767. https://doi.org/10.1007/s11227-021-04172-x

[31] Alonso-Fernandez, F., Belvisi, N.M.S., Hernandez-Diaz, K., Muhammad, N., Bigun, J. (2021). Writer identification using microblogging texts for social media forensics. IEEE Trans. Biometrics, Behav. Identity Sci., 3(3): 405-426. https://doi.org/10.1109/TBIOM.2021.3078073

[32] Amerini, I., Baldini, G., Leotta, F. (2021). Image and video forensics. Journal of Imaging, 7(11): 242. https://doi.org/10.3390/jimaging7110242

[33] Casino, F., Dasaklis, T., Spathoulas, G., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., Patsakis, C. (2021). A cross-domain qualitative meta-analysis of digital forensics: Research trends, challenges, and emerging topics. arXiv Prepr. arXiv2108.04634.

[34] Cusack, B. (2021). Extracting benefits from standardization of digital forensic practices. Polic. A J. Policy Pract., 15(1): 59-67. https://doi.org/10.1093/police/paz064

[35] Pratama, I.P.A.E. (2021). Computer forensic using photorec for secure data recovery between storage media: A proof of concept. Int. J. Sci. Technol. Manag., 2(4): 1189-1196. https://doi.org/10.46729/ijstm.v2i4.256

[36] Montasari, R., Hill, R. (2019). Next-generation digital forensics: Challenges and future paradigms. 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), pp. 205-212. https://doi.org/10.1109/ICGS3.2019.8688020

[37] Doshi, M.A., Sharma, P. (2020). Digital forensics analysis for network related data. Int. Res. J. Eng. Technol, 7(4): 1390-1398.

[38] Bérubé, M., Tang, T.U., Fortin, F., Ozalp, S., Williams, M.L., Burnap, P. (2020). Social media forensics applied to assessment of post–critical incident social reaction: The case of the 2017 Manchester Arena terrorist attack. Forensic Sci. Int., 313: 110364. https://doi.org/10.1016/j.forsciint.2020.110364

[39] Powell, A., Haynes, C. (2020). Social media data in digital forensics investigations. Digital Forensic Education, Springer, 2020, pp. 281-303. https://doi.org/10.1007/978-3-030-23547-5_14

[40] Ghosh, A., De, D., Majumder, K. (2021). A systematic review of log-based cloud forensics. Inven. Comput. Inf. Technol., pp. 333-347. https://doi.org/10.1007/978-981-33-4305-4_26

[41] Singh, S., Jung, K.H. (2022). Special issue on emerging technologies for information hiding and forensics in multimedia systems. Multimed. Tools Appl., 81: 19463-19470. https://doi.org/10.1007/s11042-022-13190-7

[42] Khan, A.A., Shaikh, A., Cheikhrouhou, O., Laghari, A.A., Rashid, M., Shafiq, M., Hamam, H. (2022). IMG-forensics: Multimedia-enabled information hiding investigation using convolutional neural network. IET Image Process., 16(11): 2854-2862. https://doi.org/10.1049/ipr2.12272

[43] Kumari, M. (2021). An overview on advanced multimedia forensic techniques and future direction. Cyber Crime Forensic Comput. Mod. Princ. Pract. Algorithms, 11: 49. https://doi.org/10.1515/9783110677478-003

[44] Verdoliva, L. (2020). Media forensics and deepfakes: An overview. IEEE J. Sel. Top. Signal Process., 14(5): 910-932. https://doi.org/10.1109/JSTSP.2020.3002101

[45] Janarthanan, T., Bagheri, M., Zargari, S. (2021). IoT forensics: An overview of the current issues and challenges. Digit. Forensic Investig. Internet Things Devices, pp. 223-254. https://doi.org/10.1007/978-3-030-60425-7_10

[46] Surange, G., Khatri, P. (2021). IoT forensics: A review on current trends, approaches and foreseen challenges. 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 909-913. https://doi.org/10.1109/INDIACom51348.2021.00163

[47] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E.K. (2020). A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. IEEE Commun. Surv. Tutorials, 22(2): 1191-1221. https://doi.org/10.1109/COMST.2019.2962586

[48] Alenezi, A., Atlam, H., Alsagri, R., Alassafi, M., Wills, G. (2019). IoT forensics: A state-of-the-art review, callenges and future directions. In Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk - COMPLEXIS, pp. 106-115. https://doi.org/10.5220/0007905401060115

[49] Alsulami, H. (2022). Implementation analysis of reliable unmanned aerial vehicles models for security against cyber-crimes: Attacks, tracebacks, forensics and solutions. Comput. Electr. Eng., 100: 107870. https://doi.org/10.1016/j.compeleceng.2022.107870

NOMENCLATURE

ASCLDs	American Society of Crime Laboratory Directors
SWGDE	Scientific working group on digital evidence)