J Inf Process Syst, Vol.14, No.2, pp.346~376, April 2018
https://doi.org/10.3745/JIPS.03.0095

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence

Humaira Arshad*, Aman Bin Jantan*, and Oludare Isaac Abiodun*

Abstract

Digital forensics is a vital part of almost every criminal investigation given the amount of information available and the opportunities offered by electronic data to investigate and evidence a crime. However, in criminal justice proceedings, these electronic pieces of evidence are often considered with the utmost suspicion and uncertainty, although, on occasions are justifiable. Presently, the use of scientifically unproven forensic techniques are highly criticized in legal proceedings. Nevertheless, the exceedingly distinct and dynamic characteristics of electronic data, in addition to the current legislation and privacy laws remain as challenging aspects for systematically attesting evidence in a court of law. This article presents a comprehensive study to examine the issues that are considered essential to discuss and resolve, for the proper acceptance of evidence based on scientific grounds. Moreover, the article explains the state of forensics in emerging sub-fields of digital technology such as, cloud computing, social media, and the Internet of Things (IoT), and reviewing the challenges which may complicate the process of systematic validation of electronic evidence. The study further explores various solutions previously proposed, by researchers and academics, regarding their appropriateness based on their experimental evaluation. Additionally, this article suggests open research areas, highlighting many of the issues and problems associated with the empirical evaluation of these solutions for immediate attention by researchers and practitioners. Notably, academics must react to these challenges with appropriate emphasis on methodical verification. Therefore, for this purpose, the issues in the experiential validation of practices currently available are reviewed in this study. The review also discusses the struggle involved in demonstrating the reliability and validity of these approaches with contemporary evaluation methods. Furthermore, the development of best practices, reliable tools and the formulation of formal testing methods for digital forensic techniques are highlighted which could be extremely useful and of immense value to improve the trustworthiness of electronic evidence in legal proceedings.

Keywords

Criminal Investigation, Data, Digital Forensics, Electronic Evidence, Reliability, Validation, Verification

1. Introduction

The advent of digital technologies and communications have removed many of the traditional barriers associated with conventional forms of media. However, the emergence of the Internet, Social Networking sites (i.e., Facebook) and along with mobile technology has radically changed our lifestyle

Manuscript received November 16; 2017; first revision December 22, 2017; accepted December 29, 2017.
Corresponding Author: Aman Bin Jantan (aman@usm.my)
* School of Computer Science, Universiti Sains Malaysia, Penang, Malaysia (humeraarshed@gmail.com, aman@usm.my, aioludare@gmail.com)

and the way we globally conduct business. Notwithstanding, it has also provided opportunities for criminal behavior to flourish. Modern communications which are now predominantly digital have meant that email, text messages, images, video in the form of electronic data transmissions have now become the preferred way of interacting and communicating with each other. Digital information and data have rapidly gained an inevitable and ever-present requirement in our everyday life by providing many opportunities not afforded previously. Unfortunately, this technology and digital evolution have also offered the same opportunities to those offenders who wish to abuse its intended application. Furthermore, people have discovered and invented sophisticated and innovative ways to commit traditional crimes using these technologies. Moreover, they have created new crimes like identity theft, cyberstalking, and ransomware. These offences are labelled as cybercrimes and are linked explicitly with digital technology resulting in many of today's current systems becoming vulnerable, and becoming viable tools supporting criminal activities given their availability.

However, with the advent of technology and digital communications, it has also helped to provide a set of new opportunities for criminal, and commercial investigators, who use this information to track the history of transactions, messages, and other forms of digital media by demographic location, or an individual's address, bank account, passport or other identifier, etc. Investigators (including law enforcement agencies) can increasingly follow a criminal's electronic footprint via audit trails and convict them based on digital evidence. Even though the electronic evidence is thoroughly examined in criminal proceedings; it is often accepted with extreme reluctance and caution. Notably, the evidence needs to show the authenticity and reliability for admissibility in a legal court of law. Although, for digital evidence, it requires disciplined and admissible scientific analysis, given that the data may easily be modified.

In legal proceedings, it is imperative to evaluate the quality and authenticity of any evidence critically to avoid unjustified decisions. The accuracy of forensic sciences has always been a cause for concern, and still; it is under debate. US National Academy of Sciences extremely criticized all the traditional analysis techniques such as matching of DNA, bite marks, fingerprints, firearm marks and footprint matching. They refuse to acknowledge them as exact, and precise science [1]. Moreover, it is emphasized to set up clear-cut scientific standards to verify the validity and reliability of forensic methods and allow the use of only scientifically proven methods in the courts [2]. A recent amendment to the US Federal Rule of Evidence 902(14) also advocates the use of best practices in digital forensics. Forensic methods, which lack suitable authentication and sound statistical foundation to justify different reasoning and outcomes are not acceptable. In addition, the methods that do not meet systematic standards of impartiality, objectivity, and independence, are also not approved in current legal practices [3,4].

It is a general observation that electronic evidence faces difficulty in meeting the standards of scientific criteria in courts [5]. Lack of trust in the digital forensic process and absence of an established set of rules for evaluation gives a smooth and accessible path for defense attorneys to challenge the evidence in courtrooms. They find several loopholes in the process of evidence collection and comparison to create reasonable doubt on the accuracy and credibility of the evidence. Critics also argued over the validity of digital forensic tools and methods [6]. Because of this, it is imperative to prove the domain as a rigorous, pragmatic and reproducible science, to offer its full support in the legal process.

Digital forensic techniques need to verify their accuracy and validation using systematically tested

methodologies. For this purpose, it is essential to establish the discipline on sound scientific principles to gain the desirable credibility and to avoid misconceptions and disagreements in the courts. However, confirming digital forensics as a precise and reproducible science is not a trivial task.

This article aims to explore the issues of scientific validation in the domain. These issues caused further complications in the systematic evaluation and validation of digital evidence. We followed a three-step approach for describing the issue. First, we examined the general criteria of empirical evaluation for forensic evidence and discussed the domain-specific problems. These issues appear to defy the assessment of digital evidence against the current scientific standards. In the second step, we explored some upcoming forms of electronic evidence. They further seem to complicate the issue of experimental evaluation. In the third step, we examined the potential solutions, already suggested, for these problems in literature and discussed their feasibility for empirical verification. Furthermore, we highlighted the future research goals, in the domain. We believe that a logical approach towards understanding the nature of electronic evidence and challenges within the field would allow us to explain the problem to the research community and suggest explicit goals for prospective research. It is not constructive to develop such methodologies and approaches in digital forensics; those are incapable of achieving legal and scientific validation.

Organization of this paper is as follows. Section 2 of this article outlines the general scientific criteria for evaluation of analytical evidence in legal proceedings. Furthermore, it outlines few significant organizational efforts to describe and standardize the requirements of the systematic and legal assessment, particularly for electronic evidence. Section 3 explains the current problems in the digital forensics; these issues contradicted the specified criteria for scientific evidence to support the fair and experimental evaluation. In addition, it explains the approaching technologies and laws related to the domain and their effects on the acceptance of electronic evidence and validation of forensic processes. Section 3 further lists the research goals for upcoming studies. Section 4 summarizes the discussion, and Section 5 presents the final debate.

2. Background

Forensic science can be defined as the use of scientific or technical approaches for the identification, collection, analysis, and explanation of evidence in legal proceedings and include an array of disciplines, each providing techniques and procedures. Notably, digital forensics is one of the primary domains given that all forensic sciences use valid principles and methods in the evaluation of evidence that is labelled as scientific evidence. Furthermore, the evidence must be empirical, as it provides support to either accept or counter a hypothesis and conclude on the guilty vs. non-guilty outcome. For actual evidence, it is essential that it can be explained and justified through systematic and experimental methods. The strength of any empirical approach relies upon the results of statistical analysis and appropriateness of the trial and controls in that domain. Accordingly, standards used to check the validity of scientific evidence may vary as per the field of forensic examination.

Over recent decades, forensic sciences have been criticized as ‘junk’ sciences in courtrooms. Junk science is the term commonly used to characterise and describe the problems among the law and scientific disciplines. Furthermore, the term is notably used within the context of expert testimony in lawsuits. Regardless of its extensive and frequent use, the term junk science has no precise definition or

meaning [7]. Similarly, it is also difficult to define a stable, reasonable or an exact science; these terms only present a contrast to junk science. However, "Good science" is characterised by the presence of testable hypotheses, reproducible results, verifiable process, peer-review or publication, general acceptance, standardization, experimentation, practicality, impartiality, realistic explanation, and use of precise methods. Good science becomes "Bad science," if it fails to formulate, deliver or conduct itself appropriately by mirroring at least one of the features mentioned above as valid science, either accidentally or unknowingly. Therefore, as an outcome, the incorrect, un-justifiable or incomplete result would occur, without the right explanation. Bad science is transformed into junk science when its faults are intentionally ignored or incorrectly justified if the scientific process purposely overlooks the features mentioned previously, or if the results are just based only on data analysis to deliberately support the wrong ideas [8].

For scientific evidence, it is essential for it to be based on an exact science to prove its credibility and reliability within the criminal-justice system. The same rules apply for the acceptance and validation of electronic evidence. The Daubert criteria are currently recognized as the benchmarks for scientific evidence which are almost like the features used to describe "Good Science." Additionally, it is common to follow the four Daubert criteria in legal proceedings, for evaluating the admissibility of scientific facts and testimony [9], including digital evidence [10,11]. However, these requirements are not exhaustive nor entirely conclusive, as the evidence and testimony may be accepted even when they do not meet any of the conditions. Also, they may potentially be rejected due to other factors, such as the relevance of the evidence or testimony. Nonetheless, these criteria are presently widely accepted for evaluating the reliability of forensic evidence [10,11]. The requirements are generalized as [12]:

(i) Either the scientific theory is already tested, or is it possible to prove empirically;
(ii) Availability of the known or probable rate of errors associated with the method;
(iii) Whether the procedure has been subject to peer review; and
(iv) Whether the relevant scientific community widely accepts the process.

Significant effort has been extended by various organizations to apply the criteria mentioned above within the digital forensic domain. Predominantly, the struggle continues to focus on formulating standard scientific objectives to evaluate the quality of electronic evidence and to streamline the collection and analysis processes. The European Network of Forensic Science Institutes (ENFSI), founded in 1995, with 67-member institutes from 36 European countries, is one such organization. ENFSI aim to improve the quality of forensic science, including the mutual exchange of information across Europe. Also, the forensic information technology (FIT) working group, from among 17 other working groups of ENFSI, deals with research, development, training, and educational matters. Furthermore, FIT also manages the technical issues associated with Internet investigations, the analysis of digital data, and the forensic examination of devices. FIT aims to provide a uniform standard and approach for member laboratories to achieve and support the ongoing need for the quality of evidence. Additionally, ENFSI has also developed and presented best practice manuals (BPM) in various disciplines, including digital forensics. The BPM for electronic forensic sciences emphasizes some key criteria and has extended the rules offered by the Daubert standard.

From among the best practices, several of the important best practices include the need for peer reviews to be undertaken of forensic processes and the development of examination protocols. The ENFSI has additionally proposed to establish contemporary techniques, calculate, and associate respective

error rates with these best practices, thereby estimating any uncertainty towards their intended outcomes. Furthermore, ENFSI has emphasized the verification of forensic processes and legal functions, also suggesting proficiency testing for laboratories and methods [13]. However, the BPM is not a set of standard operating procedures (SOP), nor is it the standard. Nevertheless, the BPM offers a general framework for procedures, quality goals, and training processes, and overall legal issues. NIST, SWGDE and FSR similarly, have directed their efforts towards developing standard methodologies and guidelines for digital forensic procedures. Even though these guidelines are infrequently adopted, a single unanimously defined criterion to evaluate electronic evidence has not been developed. Section 3.3 presents and discusses the best practices guidelines and efforts to standardize these areas within digital forensics.

Recently, a key amendment to the US Federal Rule of Evidence 902, as Rule 902 (14) was proposed; to streamline the admissibility of electronic evidence, and from January 1, 2017, the bill comes into effect within the United States. Previously, Rule 902 provided a list of the self-authenticating documents, which included: government documents, notarized documents, newspapers and publications, and business records. Moreover, these records do not need further evidence of authenticity for their admittance in a legal, judicial court. Presently, sub-part (14) includes reference to electronic data in the list of documents, if the document or documents are collected and certified through a digital identification process conducted by a certified and qualified person. Accordingly, the person must apply best practices for collecting, preserving, and verifying the evidence. At present, certified digital evidence only reflects a stable assumption surrounding authenticity, and remarkably, the associated Government Advisory Committee (GAC) has emphasized the application of generated “hash values” and to verify these after collecting evidence to confirm the self-authenticating criteria. In addition, subpart (13) of the Evidence Rule 902, states that an electronic record is similarly self-authenticating if generated by a process that produces accurate and precise results. The only way to manage the accompanying identification and verification process is to use specially designed tools for the collection and preservation (including archiving) of evidence obtained from digital documents and other forms of electronic media.

Indeed, the rule would also offer adequate credibility of the electronic evidence. However, at the same time, it would reject the use of non-verifiable and non-defensible forensic techniques required and agreed to by the courts. Therefore, it is likely as a result, that the legal community would adopt the practice globally. Although, when the legal fraternity finally decides to adopt these practices, they would hopefully realize the need to integrate “best practices” and “certified processes" into their present and future work practices, and at the same time, acknowledging the limitations associated with digital forensics. Nonetheless, if many of the constraints and issues could be resolved, this may also help to provide the necessary support and confirmation as to the value of digital forensics.

Recently, a variety of professional forums have raised many scientific validation and verification issues with present digital forensic disciplines. In September 2015, the president of the United States requested his Council of Advisors on Science and Technology (PCAST) to examine prior reports produced by the National Council on Strength and Fitness (NCSF) and Organization of Scientific Area Committees (OSAC) on forensic sciences. The PCAST council aimed to provide new contributions for strengthening forensic-science disciplines and ensuring the systematic reliability of forensic evidence in the USA. As part of this work, forensic science practices (including those considered as being state-of-the-art practices) and relevant literature, of the scientific and legal assessments made in the 2009

National Research Council (NRC) report were examined. PCAST concluded that the most useful contribution in this domain would be to add further clarity to the systematic interpretation of "reliable principles and methods" and to unambiguously describe "scientific validity" in the context of individual forensic disciplines. Furthermore, the Scientific Working Group on Digital Evidence (SWGDE) examined the issue of empirical validation in this domain, presenting several, but general validation criteria.

In this article, the issues which affect the development and adoption of best and certified practices in digital forensics are considered. Also, problems necessary for the research community to address will be discussed, along with further explanation focusing on developing practical methods for the scientific assessment of forensic techniques in legal proceedings. It is considered that these issues be resolved to meet the essential criteria for accuracy and reliability.

3. The Issues Associated with the Acceptance of Digital Evidence as Scientific Evidence

In this study, several aspects are considered which could conflict with the formal recognition of digital forensics as a sound and scientific discipline. Notably, these issues constitute the most probable reasons attributed to the lack of appropriate formal testing and verification of forensic methods. Eventually, the shortage of empirical verification will adversely affect the overall acceptance of digital evidence as being legally sound and reliable scientific evidence.

3.1 Standard Data Sets

Scientific research can be performed with or without a standard and with the same data sets. The choice of data sets highly depends upon the nature of the work. Some studies, such as intrusion detection, require access to Malware samples. Likewise, in a facial recognition system, the demand for images of human faces are needed, but for encryption schemes, certain data sets may not be required. Moreover, the same input sources are essential for comparing two different techniques used for the similar purpose, i.e., intrusion detection. Similar data sets are also necessary to test the proposed improvements in an existing approach. Therefore, researchers are required to use identical data sets to evaluate and test new techniques or to re-implement other methods to assess and check their own (proprietary) data sets. The latter process requires full access to the specifications or requirements for the new technique or proposed new changes plus the implementation plan or strategy of the person's work. Thus, evaluating the results on identical data sets is the preferred choice, saving considerable time and effort.

Throughout the literature, it evident that researchers in the field of digital forensics are still facing the problem of not having standard data sets for comparative experimentation purposes [14-20]. Also, the availability, quantity, completeness, integrity and quality of existing data sets are significant issues as they appear to be insufficient in both size and scope [21].

Accordingly, these facts seriously interfere with the acceptance of digital forensic research as a robust and reliable discipline. Furthermore, any dependable science should be able to produce consistent

outcomes, each time, under specified conditions because reproducibility is a crucial aspect of systematic methods. However, in the absence of standard data sets, it is almost impossible to compare the results from the different research methods and to evaluate these on their practical use. In fact, it is not logical to argue this point, without performing thorough testing and comparisons being made, and to gauge whether a specific technique can solve a problem or issue, and can offer better results than the other techniques on the data set. Additionally, it would be equally suitable to apply this approach for similar problems on distinct data sets in the domain. At the same time, systematic testing is not achievable without the same data sets and may not be manageable to share data from actual criminal cases with the scientific community due to privacy and data sovereignty constraints. Consequently, researchers are therefore bound to evaluate their study or proposed techniques based on personal, unreal or immaterial data only.

In the absence of standard data sets, academics to test their work, have been using various methods to obtain suitable data. Accordingly, they usually rely on smaller sets of publicly available data, and more often than not, create their own data sets whereby, the process of data collection, pre-processing and organization, usually creates an unintentional bias in the data sets. For instance, to identify cases of Cyberbullying researchers mainly collect data from publicly available and accessible sources such as from online Twitter posts. Typically, the usual percentage of online posts associated with bullying are minor compared to the size of the total data. So, to increase the size of abusive content in their training data, researchers will often filter the sample data using specific and offensive keywords. Therefore, as a result, the data may acquire more occurrences associated with bullying within it. The increase in target content helps in training, applying the models in a specific scenario or situation and the identification process. However, the data set obtained using this method would potentially be biased. Likewise, several researchers collected data from within a different period and from various locations using a distinct set of keywords. Indeed, the results obtained from the technique to identify instances of cyberbullying justifies the approach to trace abusive behavior in online social media communications. Notably, comparing any false or true positive hit rates from these results with actual and known population data is unreasonable in this scenario. Moreover, in this instance, if the approaches use two wholly distinct and biased data sets for testing, the resultant identification and error rates may not even provide a precise and useful measurement to compare two different techniques to identify instances of abuse or cyberbullying.

Most of the work in digital forensics has focused on the areas of extraction, analysis, and the presentation of data as evidence; with limited effort on establishing standard corpus [14]. Between 1998 and 2006, Garfinkel et al. [14] acquired more than 1,250 hard drives and in 2009, presented some forensic datasets with accompanying metadata. Even so, the researchers did not entirely adopt that corpus in subsequent studies due to the limited set of files and disk images. In 2006, DFRWS initiated the Common Digital Evidence Storage Format (CDESF) Working Group, to establish a standard format for storing and transferring evidence and related metadata. Unfortunately, the working group did not achieve their overall purpose and objectives and were dismissed in 2007 due to the lack of available resources. Importantly, the Computer Forensic Reference Data Sets (CFRDS) project sponsored by NIST is currently offering several sample cases, to researchers, although, these cases may only provide limited help to researchers in their experimentation work [22], as these data sets are few and limited in scope and diversity.

In another study, the importance of real data sets and various issues of creating and using synthetic data was conducted [23]. The study highlighted the limitations of purpose-built data corpus. According to the study, manufactured data sets are too specific for general solutions, and besides, it is difficult to prove that the results are also suitable for real data. Importantly, the relevance of data corpus and its transferability are also significant issues. The study also describes an approach to constructing synthetic data corpus and the means to avoid the generic pitfalls. A separate study also acknowledges the limitations of data corpus, further explaining them in the context of social media data [21].

The authors in another study highlight a similar problem within the area of social media forensics; they recommended relying on the publicly available data portion for social media forensics [15]. While a large volume of social media data is openly accessible and used for experimentation; the approach as explained earlier was not accepted for verification and standardization of techniques and comparison of tools. Instead, it may be more appropriate to create fewer reference data sets by simulating instances of known electronic crime using various specified system based configurations. However, during the creation of these sets, academics and researchers must observe all necessary parameters and manage the issues, associated with the creation of syntactic data corpus for digital forensics, as discussed in [21,23]. Furthermore, the synthesized data sets should be viewed as a contribution in the domain. There are presently limited examples of these data sets, (i.e. corpus of Twitter) created for sentiment analysis [24]. Subsequently, in the absence of standard data corpus, it is impossible for any technique or tool to evaluate against the initial two Daubert criteria related to comprehensive testing and known error rates.

3.2 Establishing Error Rate

In a recent study of 100 random digital forensics lawsuits, 10 of these cases claimed errors in data collection and analysis with only two of these cases reversed [25]. Incorrect output and a wrong timestamp were blamed on the forensic software being at fault. Furthermore, the contamination of evidence during examination was cited. Another 13 cases appealed for miscalculation in sentences and sentence enhancement, and from among these claims, six were proven to be valid in court. In this regard, the State of Florida v. Casey Anthony (2011), the murder trial of a 2-year-old girl, is an example where false forensic evidence was offered. The forensic software used to search for the term "Chloroform" reported that the word was cited 84 times by the primary suspect while it was only once [26], mentioned, with the erroneous data, proving to be a severe setback for the prosecution.

To address the issues in legal proceedings, the second Daubert criteria requires associating an established error rate with the techniques and tools used for forensic collection and evaluation. The error rate is the measure of the frequency of errors in a given method; it is used to establish the accuracy, and reliability of that approach, and is presented as false positives and false negatives. False positives represent the number of instances which incorrectly indicate a particular condition or if an attribute is present, while, false negatives represent the total occurrences which incorrectly show that a specific state or trait is absent. Notably, these error rates are used to describe the confidence in a given technique and are used to quantify the associated accuracy and reliability of the technique. However, these error rates are used to refer to random errors; these errors arise from unknown and unpredictable changes during the experiment.

In digital forensic techniques, most of the errors are systematic instead of random; these errors arise

due to the use of imperfect or inappropriate methods and tools. Therefore, calculating and associating arbitrary error rates for any given method or tool does not confirm the reliability and accuracy of that technique or software tool. Furthermore, for any reliable statistical calculation, it is assumed that essential components of the population remain static such as blood for DNA analysis. However, where the digital infrastructure is highly dynamic, a new kind of media (i.e., Facebook, cloud data) and hardware such as a solid-state drive, is entirely different from older media and devices. The tool or method tested on one type of hard drive with high accuracy may prove altogether inaccurate for another model [27].

Moreover, investigative work in digital forensics is exceedingly reliant on tools which are necessitated and required to make sense of binary data. Accordingly, the success of analytical tools decidedly depends upon the velocity and accuracy of scientific research within the domain. Digital forensic software consists of two parts. First, the method or algorithm which dictates the execution of the task; this component is part of the systematic research. Secondly, the implementation of the algorithms or research methods through code writing or programming, performed by software developers. Software code (used to develop the program) is known to possibly have inherent bugs (i.e. incorrect logic or instructions) for several reasons. Furthermore, the impact of these bugs may vary and can produce inaccurate results. Forensic software tools will undoubtedly compete with the challenges brought about by exceedingly dynamic and sophisticated technology. Also, formal and detailed software testing is often overlooked or rushed, given the competition of other similar products entering the market or through competing and emerging technologies (i.e. mobile devices). The excessive costs involved in testing software, the time required, skilled resources, and the absence of verifiable and recursive protocols are formidable factors in preventing adequate and comprehensive testing of software tools. Therefore, it is not a reasonable practice to calculate error rates individually for either software tools or underlying techniques and associate them with the overall process. Further, it is imperative to test and evaluate the fundamental methods; first independently and then in combination with code fragments.

Few studies have suggested using formal methods which are helpful in reducing some of these costs in contrast to using ad-hoc and time-consuming verification processes, which may help to improve the quality of software. Also, formal verification could assist in the design and development of more intelligent and capable methods for managing digital investigations [28,29]. Few models have suggested an individual specification and supporting documentation to accompany each identified software function that may serve as required criteria to validate the tool [30]. This representation allows the development of formal methodologies, which can confirm, verify and evaluate a distinctive task or function when needed, irrespective of the original and overall intent of the tool. During the testing process, a set of performance metrics may help to identify and decide on the necessary scientific measurements relating to the precision and accuracy of this approach as this may help to offer extensibility and neutrality in the process, and manage the dynamically reactive nature of the testing practices. In this regard, NIST initiated a Computer Forensics Tool Testing (CFTT) project to develop testing methodologies for computer forensic software [31]. Furthermore, to propose guidelines for general tool specifications, requirements, and formulate procedures, criteria, and materials for comprehensive testing. Although its contribution stayed limited to a few instances, such as disk imaging, write blocking and file recovery. In 2014, they also published guidelines for mobile device forensics.

A report by the SWGDE explained in detail the nature of errors and error mitigation strategies [27]. This report made a significant contribution by identifying digital forensic techniques and tools as distinct parts in the process. Furthermore, the report focused separately on identifying potential sources of errors for the overall process, theorizing that error mitigation strategies are not just limited to only finding error rates. However, it is helpful and essential to calculate them where they are applicable. An error mitigation process in digital forensics should be clearly articulated and specific, relating to the task at hand. The report also recommends to distinguish between limitations and error rate, for instance, hash algorithms are designed with minimal false positives such as for MD5; it is one chance in 2128. Furthermore, each imaging software application should be capable of managing readable data around bad sectors differently, resulting in distinctive output and multiple hash values. The resultant difference in output data is not an error but is just a fundamental limitation in hardware failure.

Moreover, in this report, the working group concluded that the identification of potential errors along with specific error mitigation strategies and additional testing was helpful to prove the reliability of the tools. Ultimately, these techniques increased the confidence in the overall process. Notably, this work places a strong emphasis on systematic and exhaustive testing of tools. Indeed, this study helped to understand fundamental validation problems associated with underlying techniques, and explaining the need for separate error handling strategies for each. Also, the report identified the potential sources of errors, although not implying any specific solution for the comparison and evaluation of tools and techniques. Forensic techniques and tools for social media or the cloud platform are still considered to be in their infancy. Finding potential sources of errors and formal testing models remains as an open issue in this domain.

3.3 Standardization Issues

Digital forensics deals with a vast assortment of electronic devices and information formats which are further proprieties of a diverse group of software developers and device manufacturers. Indeed, creating standards, for such a large and varied group of stakeholders, is a challenging task. Also, complicating matters further, the participants are reluctant to agree to certain standards and rules and often resulting in potential conflicts of interest with one another [32]. The academic community and practitioners have always complained about the shortage of SOPs in digital forensics and have strongly voiced the requirement of having systematic and sound methods for forensic investigations [33-35]. Still, very few partially productive standards and procedures are available within the domain.

In the United States, the National Institute of Standards, and Technology (NIST) was established to develop an infrastructure for forensic sciences and to address related standardization and quality issues. NIST consulted with the OSAC for various forensic disciplines; one of the five Scientific Area Committees (SACs) dealt with digital and multimedia domain. In June 2010, NIST and OMTP (later renamed as WAC) unfortunately, only managed to introduce a few requirements for advanced SIM cards and mobile device security and failed to provide any unified environment for developers [36,37].

The SWGDE, initially known as the Technical Working Group (TWG), was also established in the United States with the primary aim to develop collaboration and cooperation among several organizations to ensure consistent procedures and practices were adopted in the domain. The group provided some basic guidelines and definitions for digital forensics with several of the guiding

principles published and later adopted by the G8 [38]. During their tenure, SWGDE issued more than 50 best practice guidelines. Notably, few standards have implemented these procedures such as ASTM E2763 (ASTM 2012). ASTM describes the standard methods for seizing, handling, imaging, analyzing, documenting and reporting of potential evidence. Although, ASTM does not incorporate all aspects of an electronic investigation; such that the standard does not include at this stage, any information for using forensic tools or managing multiple operating systems.

The Forensic Science Regulator (FSR), another government body in the UK, ensures that both appropriate and quality standards are practised across the judicial system. The FSR further identified the requirements that were needed for new and improved standards and provided a compliance guideline, setting out the rules for forensic science providers. In 2008, the first forensic regulator was appointed, and since then, the office of the FSR continues to ensure that law enforcement organizations follow appropriate quality control principles for forensic science laboratories and legal practitioners. The present FSR has set the goal of achieving accreditation for digital forensics in 2017, which seems a challenging task given the lack of any formal validation processes within the field. Additionally, the Digital Forensics Specialist Group (DFSG) is currently advising and assisting the FSR on achieving their goals [39], focussing on the necessity of 'Method validation' to meet quality standards in digital forensics. In 2016, a guidance draft was published emphasizing on the validation of forensic methods instead of software tools, like black box testing that does not require the source code for validation purposes [40]. While this approach does not require proprietary source code, the validation process still requires an assessment to be conducted on known data samples, which are relatively limited in digital forensics.

Subsequently, the diversity of the domain, the uniqueness of each investigation, rapidly evolving technologies and different legislations are constraining the standardization in this field [34,35]. As a result, any single set of guidelines or standards will be unable to address all digital forensic process dimensions and different aspects, and therefore, a diverse set of rules and guidelines relating to their own legislation tend to be adopted. Moreover, given that multimedia, the cloud, and social media evidence is a relatively new and evolving field, there are no established guidelines and standards to administer, report and evaluate them. Indeed, digital communications are not limited by physical boundaries, and therefore, electronic crime could occur anywhere, and at any time, whether it is the cloud or on social media and other community networking sites. Therefore, cross-jurisdiction digital forensics capabilities are still limited.

The rapid expansion in underlying technologies associated with electronic computation, storage and communications, are the main reasons for the lack of standardization. Furthermore, latest techniques have led to the development of new and broadening dimensions in the field, such as social media, cloud, and IoT forensics. Recent attention towards digital data and forensics is quickly turning into an area of focus and opportunity for many companies; the business of these corporations thrives on the diversity of techniques and the maximum privacy they offer to clients and are eager to provide as much variation and confidentiality to users as possible. Also, these factors are continuing to add further technically unique and legally intricate challenges in this domain. Therefore, most of the effort and focus to establish appropriate standards and best practices guidelines remain limited.

Therefore, the lack of unified practices and standard operating procedures affects the role of digital evidence in legal proceedings. For instance, the State of North Carolina v. Bradley Cooper is an example

where the only decisive evidence was a Google map image, sourced by the suspect, pointing to the exact location where the law enforcement officers found the victim's dead body [41]. However, this evidence became controversial due to the improper handling of the evidence by the law enforcement officers. Both the prosecution and defense remained unsuccessful in their efforts to prove or disprove its validity. Similarly, the trial of United States v. Anthony Suarez and Vincent Tabbachino (2010), is a further example of procedural misconduct. In this trial, the criminals receive a conviction on corruption and bribery charges, and the evidence was the incriminating SMS messages. However, the accused was later evicted in a retrial because the Federal Bureau of Investigation (FBI) failed to preserve and produce the SMS messages [42].

The unavailability of best practices in specific areas, including the implementation of different procedures in various regions reflect the lack of generally agreed-upon standards or sound practices in science and law enforcement communities. Furthermore, this issue seriously interferes with the general acceptance criteria stated in the Daubert standard. Even the scientific community involved in the development of the guidelines and best practices, however, enforcing the adaptation and implementation of best practices is beyond the reach of scientists.

3.4 Anti-Forensic Techniques & Tools

In general, any attempt or methodology used to modify, upset, refute or restrict a valid scientific forensic investigation is considered as being anti-forensics (AF). AF still does not have any agreed-upon definition [43], despite several efforts to provide a standard description as presented in [44-46]. Concealment and evasive behaviors are universal in all criminal disciplines. Sometimes criminals will intentionally perform these behaviors to mislead an analysis or examination, and often merely exist due to common factors. The inability to identify these evasive behaviors during an inquiry will severely compromise the integrity of the extracted evidence. Moreover, AF procedures directly affect the reliability of digital evidence if the trustworthiness of the evidence is successfully challenged in court and creates significant doubt; the evidence would be deemed useless.

Connecticut v. Amero is an example of a wrongful conviction due to the unawareness of adware existing on the device. The forensic tool used to extract and examine the data failed to differentiate between human activity by the user and the effect of malware residing on the device [26]. In this trial, initially, a school teacher was sentenced for felony charges for possession and exhibition of pornographic material on her work computer. Afterwards, they presented evidence that confirmed that the incriminating content was produced by the malicious code and not by the user. Therefore, the court reversed the conviction as the evidence proved to be wrong.

Another argument suggests that legal software packages are considered reliable, by the courts without significant proof of their dependability. In fact, that is a direct violation of Daubert's essential criteria for the acceptance of scientific evidence [6]. In 2007, the US Black Hat conference further emphasized this point and demonstrated several attacking mechanisms on forensic methods through AF tools [47]. The participants concluded that the legal tools and techniques used for the analysis and identification of evidence were at the time, not developed to resist AF attacks, and the testing methods often ignored AF activities during their evaluation and validation. Furthermore, in 2012, a survey found that only 2% of research papers in the domain were related to anti-forensic research, therefore indicating that forensic analysis and research efforts were not sufficient to manage such extensive and intricate problems [48].

Various anti-forensic techniques are identified and classified in multiple studies [43,44,49]. The most widely accepted taxonomy categorized the AF activities into data hiding, artefact wiping, trail obfuscation and direct attacks against both the forensic process and tools [50]. In 2016, other studies extended the existing taxonomy by the identification of techniques and tools for AF [51], where they provided the identification and classification of various anti-forensic tools. The presented taxonomy includes a diverse set of common code fragments; they are not designed for this purpose, neither are they known as AF tools but are readily usable for anti-forensic purposes. In 2017, Hausknecht and Gruicic [52] further refined the AF taxonomy where they separated the AF techniques into low and high-tech categories. They included physical data destruction, hard drive scrubbing, steganography, and cryptography to low-tech anti-forensic methods and cited data saturation, file signature masking, hiding data in the slack and unallocated space using nonstandard RAID configurations and NSRL scrubbing among high-tech techniques [53]. Notably, these taxonomies and identification of AF tools serve as a cautioning to the vigilant forensic community. The identification of probable indications of anti-forensic activity is another open problem, and investigators need to be aware of indications of these events like the presence of encrypted virtual machines and AF tools.

In a separate study, a counter forensic framework, proposed analysis and authentication requirements were proposed [54], with the researchers further recommending that all tools in the anti-forensic environment be tested [52,55]. Accordingly, this examination in the AF environment would offer a substantial improvement to establish reliability parameters for the legal acceptance of forensic tools. Furthermore, it is not practical nor feasible to describe the relevance of AF techniques such as the anti-forensic methods that relate to networks, as these may not apply to mobile devices and vice versa. Therefore, to determine and explain the potential effectiveness of these approaches, it is necessary to consider the underlying platform and configuration of devices and networks. However, there is an unlimited number of settings, machines, and software to study, and virtually a limitless number of combinations which will further increase the difficulty of the already complicated task of identification and classification of AF techniques and tools.

3.5 Diversity and Quick Evolution in Digital Forensic Sub-Fields

Various challenges met by digital or cyber forensics in general have been outlined and classified in several previous works [15,29,56-62]. In a study presented in [63], the authors reviewed the research literature from 2000 to 2012 and separated the issues into five key categories of complexity, diversity, quantity, unified time-lining, consistency, and correlation, and also, prioritize the analysis problem of large data, among other issues. In 2015, a further researcher provided a more recent classification of the problems by providing an excellent taxonomy of existing issues concerning technical, legal, enforcement, personnel-related, and operational challenges [64].

The extraordinary evolution in the field of electronic communications techniques and technologies are the underlying reasons for most of the validation issues arising in digital forensics. This rapid progression is significantly resisting the emergence of analytical disciplines as valid science. Notably, in 2014, a literature survey reported a significant increase in mobile devices and cloud forensic research [65], and interestingly, this study did not identify any research related to social media forensics in the period 2008 to 2013. This is mainly because the survey did not list those topics for which the authors could not find more than five publications.

The rapid speed and variety of emerging techniques and devices in digital computing and communications have made it extremely difficult to develop sound scientific principles and to test best practices thoroughly for digital forensics. Indeed, social media, cloud computing and storage, encryption techniques and the IoT are a few of the emerging technologies in the domain. Also, every new discipline takes a considerable amount of time to evolve as an exact science Furthermore, the theories and practices in each subject are debated and tested for many years before finally being accepted or rejected on sound scientific grounds and principles. However, the timeline of digital communications history is too concise and incredibly intricate to aid the development of the related forensic science as an exact discipline. Section 5 of this article, further discusses the effect of the progression of electronic technologies towards scientific development and validation in the field.

In the next section, upcoming frontiers in digital forensics and their specific issues are discussed, which are contradicting even the established and accepted practices of the domain. These fields need a new set of technical solutions and legal adaptations to be determined. Therefore, the objective of this section is not to provide a review on the respective sub-fields such as social media or cloud forensics, but instead, to provide an insight on the manner of how the emergence of these fields is affecting the already established practices in the domain. Moreover, they are further enhancing the difficulties to prove digital forensics as a valid science. To explain this point, the latest sub-fields in the domain currently in practice, along with their unique challenges, are briefly discussed. Additionally, observations are also presented on the current standards and practices that are inadequate to manage these issues, and several immediate and open research areas are also listed, requiring urgent attention and addressing with a precise focus on legal and scientific validation.

3.5.1 Social media forensics

Social media evidence is a new forefront of criminal proceedings, both for traditional and for cybercrimes. However, it also raises unique legal and technical challenges for digital forensics. Trials involving social media evidence are increasing each day. According to various surveys, in 2012, there were 689 published cases where social media data was presented as evidence, and further highlighting that from 2015 this practice has been quickly increasing [66]. Furthermore, in 2016, 14,000 decisions were reported for the 12-month period in the United States, and among these, 9,500 cases were vastly reliant on social media data as evidence. Notably, these numbers represent a 50% increase from the prior year [67,68].

Investigators are attracted to social media due to the ubiquitous, personal and footprint like nature of the data. A treasure trove of proofs created by the suspect, or the victim, would be favourable if not gratefully received by detectives. Therefore, if they manage to investigate the proofs (i.e., data) correctly for its value and potential, it might offer exceptional support in the criminal investigation process. The metadata accompanying the content and other information on social media sites likewise holds enormous potential to assist in investigations. Moreover, social media data is readily available and accessible to use as evidence for litigation purposes and investigations. The published contents on social media along with an associated timestamp are often used to locate the whereabouts of an individual; could help to corroborate an alibi, or might be suggestive of some prior or recent criminal activity.

However, to gain the added benefit of data hosted on social media Internet sites, investigators must deal with intimidating technological and legal issues. Technical issues are frequently due to the

complexity and diversity of information residing on networks, and the legal aspects involve the admissibility of evidence and data collection issues. Social media evidence is not self-authenticating in itself, so, it requires some circumstantial and corroborating information for authentication. Occasionally, the defendant's constitutional privacy rights restrict the collection of evidence from his or her public media platforms. Apart from the legal issues, the diversities in social media platforms in addition to their rapid and unstructured evolution, are challenging factors in collecting data. Furthermore, it is necessary to review the preservation and retrieval of evidence and the chain of custody procedures in social media forensics to present more competent evidence in lawsuits.

It is evident that the traditional methods of extraction and preservation of forensic data are unsuitable for social media forensics. The trial of State of Louisiana v Smith is an aggravated assault case. The suspect posted a picture of himself carrying a firearm and threatening messages to the victim on Facebook [69]. Later, the prosecution presented the printouts of the photos and Facebook posts as evidence, which was rejected by the court due to insufficient authentication.

In studies related to social media forensics, most of the work is always focused on the extraction of data artefacts from devices and the online networks [70-72]. Currently, some methods and practices are used for artefact extraction, where they can successfully retrieve data [73,74]. However, preserving the data with its varied components and presenting it as acceptable evidence remains an issue.

The overall issues from the primary domain also exist in the sub-fields of digital forensics such as standard data sets. The large sets of data are easily accessible from open social media platforms and other sources to conduct studies. Researchers cannot share or publish most of the data sets due to privacy or other constraints. The openly available data sets are helpful in the general testing of methods but are unsuitable for measuring and comparing the correctness and accuracy of different techniques due to the inherent bias in most of the collected data sets, as discussed previously in Section 3.1. Automated methods for analysing public media data for legal purposes are limited. Importantly, these tools are essential for managing the massive amounts of data accessible from social media sites and are needed to extract useful information and knowledge concerning crimes, or about suspects from large pools of data; data can include a lot of irrelevant information as well.

Moreover, integrating and correlating the data from social media to gain an understanding of a crime is a further issue. In a single investigation, often hundreds if not thousands of disparate pieces of information are forensically acquired for analysis as the data is commonly used to establish a relationship among the suspects, the crime, and the victim. The process of correlating the data is usually quite complicated and tends to create an information overload issue for the detectives or investigators. Furthermore, the information may not make much sense or provide aid in the investigation until the investigators can manage the data into a single and cohesive representation. Therefore, consistent data representation is essential to filter the unnecessary data quickly and to gain useful knowledge and insight. However, current techniques and tools available within the domain at present do not offer this functionality.

3.5.2 Cloud forensics

Recently, Cloud forensics has become a significant element in electronic investigations; to locate digital data involved in a crime, and saved in the cloud (virtual storage). The acquisition and analysis of forensic data hosted in the cloud environment are problematic. Many of the issues that arise are due to

highly distributed and complex cloud architecture. Other reasons include the multi-tenant usage model, virtualization and the volatile nature of the data itself. Also, privacy issues are a tremendous concern [75,76]. Therefore, these problems emphasize the need for attention and creation of legal and technical frameworks. The already established practices in digital forensics are at this stage, not applicable to the cloud environment such as searching, and the collection of data, due to the lack of individual ownership of devices and data stored in the cloud.

Various challenges of the domain are outlined in the related literature [77-81]. The NIST provided a comprehensive list of 65 challenges associated with the cloud computing forensic science. The issues include technical, legal, and operational categories. However, NIST did not offer any solutions to these problems. The most protruding problems are related to the distributed nature of resources (Applications, Storage, etc.) in the cloud and the enormous user base. The legal constraints surrounding privacy, security and ownership are further complicating matters. The highly dispersed and multi-tenanted structure of the cloud is seriously challenging the basic concepts of the crime scene's boundaries and ownership in digital forensics and is a further issue in managing a 'chain of custody' in a cloud environment.

Crime scenes in the cloud involve several thousand virtual machines, many servers and an enormous number of cloud users; with only one of these users relevant to the investigation. Tracing or stopping a real device is almost impossible. Even if the investigators somehow gain access to the physical device containing the data, it may not belong to a single user. Therefore, stopping and making an electronic image of that machine may affect the privacy or rights of other users. Additionally, the process will disrupt the service for everyone using that service. Few studies have suggested Digital Forensics-as-a-service (DFaaS), to manage the issues of data acquisition on the cloud [82,83]. Forensics-as-a-service seems a natural and the most probable solution to the current challenges in the cloud environment. If DFaaS is adopted and implemented, it may address various technically intricate aspects of the domain in the future. In the cloud environment, the user has no physical interaction in the cloud with others. Users identify themselves only through their unique identifier (ID) and password. There are many ways to intercept the identification or take it from the user by force or through deception (i.e., scam) and often is misused inappropriately by another person to gain access to the cloud from anywhere due to the open nature of the cloud. Therefore, it would be challenging to authenticate the ownership of data attributed to a specific user in distributed and virtual environments.

The capability of investigators to collect and analyze evidence from a cloud environment ultimately depends upon the tools and techniques used. Even so, there is a huge gap when it comes to automated software tools that are available to investigators for dealing with cloud forensics. Furthermore, in this study, the observation regarding the correlation between tool development and evidence across multiple cloud providers is highlighted as a further open problem and issue within this domain. The infrastructure and services offered in the cloud present enormous diversity and heterogeneity given that there is an inadequate level of standardization concerning the infrastructure, making it challenging to develop specialized tools for forensic acquisition and analysis.

The DFaaS method, if implemented, may only help to solve the issues in the acquisition of data from the cloud. Other problems may still exist, such as analyzing and correlating data acquired from distributed sources and preserving the integrity of ever-changing data. Authenticating the authorship of data would always be challenging as it is necessary to review the authenticity and admissibility criteria to manage forensic data obtained from a cloud service.

3.5.3 Encryption techniques

Encryption is an important data hiding and AF technique with legal backing and is an essential method to ensure the privacy of users and the integrity of communications residing in the computer, device or digitally residing on the Internet. Most operating systems, are presently providing integrated support for encryption; all users have access to improved security and data protection capabilities. The existence of easy to use encryption programs has made it convenient for individuals and organizations to protect the security of their data, such as using programs such as BitLocker and FileVault for Windows and MAC respectively. Furthermore, it is now quite challenging for digital forensic examiners and investigators to retrieve evidence from encrypted data files. Numerous studies have identified encryption as the most challenging factor in electronic examinations and investigations, such as [59,84,85]. Additionally, in a survey that was conducted to identify the most demanding factors associated with technology, most participants that are forensic analysts identified encryption as being the most challenging factor in current practices [59].

Another study investigated and identified the impacts of encryption on digital forensics [84], where the majority of reasons for encryption was found to be the obligation to ensure the confidentiality of personal information and intellectual property was protected. Criminals are also acutely aware of the advantages of cryptographic methods using it as an accessible escape route to evade forensic investigations. Furthermore, encryption software can quickly and easily encode data and is equally possible to encrypt entire devices. In certain situations, devices can be configured to wipe or remove all data from the device if access to the device or program is un-authorized. In almost 60% of investigative cases, the examiners and prosecutors are only able to access small data portions or not at all [84].

Notwithstanding, encryption poses a significant challenge for acquiring evidence, as forensic investigators regularly deal with strongly encrypted data. Usually, the direct attack to break, crack or penetrate strong encryption is useless, but several other options avail themselves for forensic examiners. For example, the laws in the UK state that suspects submit their encryption keys to law enforcement agencies and officers as part of an investigation. In October 2007, the UK activated Part III of the Regulation of Investigatory Powers Act, where the authorities can forcibly request and demand suspects to provide their encryption keys. The alternative is to face up to five years in prison. While in the US, a federal court stated that it was not legitimate to compel citizens to turn over or submit their encryption keys due to the Fifth Amendment, which protects their privacy [86]. Even so, in more severe cases, where the charges are much harsher, suspects prefer prison time instead of providing the encryption keys to the authorities; as these keys offer access to data which may implicate them and others further with more severe crimes.

Two leading multinational organizations, namely Apple and Google, produced 96.3% of global cellular devices, incorporating default encryption on all the smartphone devices [87-90]. Both companies implemented encryption in response to the constant insistence of users and the international community to ensure digital security and privacy of data is protected [91]. Furthermore, both companies announced giving up the cryptographic keys used to decrypt secured devices; only users have encryption keys. Furthermore, without the encryption keys, companies are unable to unlock digital devices and access the data stored inside the device, even under a court order [92].

Also, in certain best-practice guidelines, it was recommended to turn off the evidentiary device at the

time of seizing the device to prevent any alteration of the data. With current ubiquitous device encryption and full disk encryption schemes, shutting down the machine or device may stop future access to all the pertinent digital evidence. Therefore, examiners may need to consider choosing live forensic acquisition in shutting down a system [85]. Under current practices, acquiring the data without shutting down the device may provide an opportunity for the defense counsel to take advantage of this fact. In this instance, the defense attorneys may accuse the investigators of altering the evidence, either deliberately or unknowingly, and thus damaging the integrity of the evidence and its admissibility in court.

Therefore, previously established best practices, guidelines and procedures will need to be amended. Changes should be introduced to allow forensic examiners to access live systems, although, at the same time, any changes must ensure the integrity of data is not compromised. Likewise, an innovative method is also necessary to ensure the integrity of data from live forensic investigations. Notably, this issue is also highlighted in the State of Arizona v. Jodi Ann Arias (2015) trial regarding a murder investigation. During the search and arrest, an investigator from the Mesa Police Force had started the computer, where, the system automatically updated the programs and data held within the computer. Subsequently, the digital evidence collected from that system was rejected by the court due to mishandling of evidence and possibly altering the state of the hard disk. The court also stated that the practice was detrimental to best practice and procedure followed by the Mesa Police Force. The procedures required the machine to be shut down or switched off as part of their procedures to retrieve and embargo the device.

Encryption, therefore, implies an apparent trade-off between enhanced consumer privacy and successful investigation. FBI vs. Apple is a further classic example of a compromise where the investigators were faced with the challenge imposed by the encryption and auto-wiping features of an iPhone 5C (Apple) device. In this instance, the investigators were not able to access the data, despite legal and government support, notwithstanding the sensitivity and sheer size of the case in question. Later, the investigators were only able to retrieve data with the help of a zero-day exploit routine [59].

Despite these issues, it is difficult to argue against the achievements brought about through encryption and the impact it has had towards information and data security. Tremendous effort has been made to find common ground among encryption and privacy laws. However, the proposed solutions to this issue, remained impractical due to the ineffectiveness of domestic laws on foreign companies [93-95]. Indeed, the quantum computing in the future may offer hope to investigators to explore the potential of brute force attacks on encryption algorithms [96-99]. Almost all modern encryption techniques rely on numerical complexity for their security, so with the emergence of quantum computing, many of the mathematical problems may become manageable to allow brute force attacks. Nevertheless, encryption schemes are also evolving along with emerging technologies and advancements, such as Honey Encryption techniques, which relies on deceiving the intruder instead and instilling computational complexity [84]. Thus, it would be an ongoing battle between encryption and forensics.

Furthermore, under this scenario, defining and implementing strict standards such as “preserve everything, but change nothing” would be inconsistent with current technologies and unreasonable in a legal context. While it may be reasonable to follow this standard in some situations, it is unpractical with the volatile and now common trend of dynamic data. Therefore, by highlighting this rigid practice as “best practice” only invites unnecessary and unavoidable criticism towards digital evidence. In fact, the legal infrastructure should insist upon the preservation of volatile computer data, as observed in

some cases where the investigators collect and save data collected from live systems [86]. Also, forensic analysis of a live system is a further emerging trend, although, it does not offer a complete solution for issues of encryption but instead, may provide support in few instances.

3.5.4 Multimedia forensics

Digital evidence in the form of multimedia, such as images and videos, is fast becoming a recognised group of forensic artefacts and are most frequently found on social media networking sites and platforms. Vast volumes of images, audios, and videos are created, transmitted, stored, and manipulated daily which are hosted on public Internet platforms, which again, are potential sources of evidence for prosecutors and lawyers. However, with the diffusion of digital images, and with commonly and freely available tools that can edit digital photos, the preciseness and authenticity of a photograph, for example, could become doubtful. Therefore, it is crucial to authenticate photos and other images appropriately before presenting as potential evidence [85]. Media forensics emerged during the last decade as a research field, offering several methods and tools mainly focussing on still images. Although, they differ regarding their maturity and respective limitations [86], and most of the approaches have not considered nor adequately addressed anti-forensic techniques applied to multimedia [87,88]. Currently, the most pressing challenge is to identify and in some cases, differentiate between legitimate or illegitimate processing. Editing, an image, is not considered to be tampering, and modifications to an image like altering the compression ratio or reducing the amount of noise are not illegal. So, a threshold is required to distinguish and quantify legitimacy and deceptive processing [89]. Indeed, this problem is not easily addressed, because the same modifying or editing operations can be valid in one situation but misleading in another case.

There are many structures and mechanisms for storing and capturing images, audio and videos. Therefore, forensic methods used to examine and authenticate one format, may or may not provide accurate results on other storage devices. Accordingly, it is illogical to assume their appropriateness, in one way or another without performing thorough and controlled testing. Also, it is another issue to test new forensic tools and methods for unusual or non-standard media types, formats, and editing operations. Therefore, the verification process in this instance is difficult to achieve in the absence of unified and real data sets and is quite time-consuming due to the various forms of multimedia data [86]. All these issues are expected to complicate and challenge scientific validation even further.

3.5.5 IoT forensic

The number of devices manufactured globally continues to increase. The increase is brought about through the ever-growing evolution of mobile technology and online digital communications. The next breakthrough of digital and mobile computing and communications will be the “Internet of Things” (IoT). Furthermore, due to the rapid expansion of IoT, new and innovative applications and services are being developed which will enhance and progressively change our lifestyle and the way we globally conduct business. The IoT will bring about sweeping changes, and bring with it, new challenges and opportunities, including challenges for the digital forensics domain. Criminals, including organised crime syndicates, may take advantage of these modern technologies and applications with malicious

intent in mind, more than ever before. For instance, exploiting the vulnerability of health or safety equipment or causing critical infrastructure (i.e. power, water, road infrastructure, etc.) to fail, thereby threatening the lives of people and nations.

Therefore, it is vital to develop and adopt digital forensic procedures to include IoT applications and around the infrastructure to deal with these emerging challenges. The enormous number of devices that are interconnected via the Internet or via mobile digital networks store and continuously transmit data. Within the complex, and highly distributed IoT environment, without the proper controls and security measures in place, this could lead towards new crime syndicates and radical organisations to evolve, thereby taking hold of sensitive information and data. The IoT will potentially generate a diverse and an enormous amount of potential evidence. Therefore, it is essential to amend the legal frameworks, to safeguard and protect against criminally motivated crime and injustice. Indeed, it is an entirely new paradigm that challenges traditional jurisdiction, integrity, and chains of custody.

The TRENDnet incident, in addition to the Volkswagen scandal that occurred in 2015 is an excellent example of IoT investigations where the inquiries failed to impose penalties in both cases. In 2013, the Federal Trade Commission in the US filed a complaint against TRENDnet. The company provided remote monitoring of residential homes to clients through Internet-connected live cameras. According to the accusation that was made, the defendants failed to deliver the required security network setup as requested. As a result, hackers penetrated the network and gained access to the CCTV footage, posting it on the Internet. The plaintiff accused the defendants of compromising the security and privacy of their clients. Even so, no financial penalties were imposed on TRENDnet for their failure to provide the required installation setup. Similarly, in the Volkswagen case, the US Environmental Protection Agency (PTA) accused the company of deliberately cheating on the emission test through software embedded in the cars, therefore violating the Clean-Air Act (CAA). The software was designed to detect the emission test and turn off the pollution-control device. As a result, the car passed the emission tests, producing 40 times more nitrogen oxide than what the allowable limit allowed. The problem affected more than 11 million vehicles globally. However, the company never incurred any penalties as their software had legal protection against any open review made by a third party or parties. These unproductive investigations are again, further indicators to support the introduction of IoT Forensics.

Technically, the IoT may store more diverse data than what is presently stored in social media networks and the cloud. The number and type of connected devices could also vary along with their intended use, thereby creating additional volumes of communication and mechanical data such as climate temperature, speed, capacity, etc. The resultant data would be massive and possibly more dynamic. While the disciplines surrounding IoT forensic are evolving, there are currently limited studies investigating this particular area, especially regarding open issues associated with the IoT.

4. Summary

The most prominent challenges in the digital forensic domain are highlighted in Section 3, in addition, it the identified the reasons that causing these issues. The discussion explained the reasons restricting the scientific validation in the digital forensic domain; it also discussed the current issues which are most relevant to digital forensic research and listed the open research areas within the field.

Table 1. Issues with formal and scientific validation in DF

Issues with formal and scientific evaluation of DF	Reasons	Aims for future research
1. Lack of data corpus	Privacy laws	- To create new datasets by simulating some known digital crimes in various detailed system configuration. - To develop discrete function based test cases for tool validation [30].
2. Lack of formal testing	- Quick evolution - Excessive cost - Time intensive - Lack of verifiable and recursive testing protocols in the domain.	- To focus on developing new and formal testing methods [28,29]. - To establish matrices to measure the precision and accuracy of forensic methods and tools.
3. Lack of established error rate	- Lack of proper understanding of the issue. - Diversities in the domain. i.e., an infinite number of combinations of hardware, software, and data formats. - Dynamic nature of the digital medium.	- To identify potential errors in tools and underlying methods. - To develop additional testing methods - To develop customize error mitigation strategies for a specific process.
4. General acceptance issues	- A diverse group of software developers and device manufacturers. - Conflicting interests - Reluctance to join standards [32]	- A consensus on legal and technical frameworks, although it would be beyond the scope of the research community.
5. Anti-forensic methods	- Sometimes it is not deliberate; data merely is overwritten by another process. - A side effect of other regular tools. - Attempt to ensure the privacy of individual through encryption tools. - Attempt to de-anonymize on the internet. - Anti-forensic tools are readily available.	- Essential testing in anti-forensic environment [52,55]. - To define appropriate AF configurations for distinct forensic methods. - Include identification of blind spots in forensic tools as part of tool validation. - To identify most common AF tools. - To spot the probable indications of anti-forensic activity in specific domains. - The potential effect of anti-forensic tools on forensic methods.
6. Rapid evolution and diversity	- Advancements in digital communication and computing techniques and technologies - New devices - Open standards - Privacy issues - Lack of proper legal infrastructure	- Pro-active approaches - To propose adjustments in legal frameworks.

Table 1 here, provides the list of findings explained in the previous discussion. Table 2 listed the latest appearances of digital forensics and their effect on the evaluation of the digital forensics process. Furthermore, it also identified the open research problems in relevant sub-domains.

Table 2. New frontiers in digital forensics and their effect on digital forensics process

New frontiers in digital forensics	Effect on digital forensic process	Future research goals
1. Social media forensics	- Ceasing a profile may not be possible. - Dynamic data, previous methods of integrity management would no longer be sufficient. - Traditional methods of extraction and preservation of the forensic data are not suitable for social media forensics.	- New tools for collecting, searching, indexing, preserving, and authenticating social media evidence. - Evidence correlation across multiple Social media would be another issue. - Right visualizations - Novel formats to present and preserve data.
2. Cloud forensics	- Further, complicate the acquisition and analysis of forensic data in cloud environment due to --Highly distributed architecture --Multi-tenant usage model --Virtualization --Volatile nature of the data - Privacy issues [75,76]. - The issue with the chain of custody. - Difficulty in proving the ownership of data. - Client-side encryptions - Diversity makes it hard to develop consistent standard practices.	- To propose new methods for collecting and preserving and indexing forensic data from cloud environment [75,76]. - Evidence correlation in the distributed environment would also be an issue. - Need for significant adaptations in legal and technical frameworks, already established, digital forensics.
3. IoT forensics	- Limitless crime scene borders. - Highly distributed environment. - An enormous number of devices.	- To suggest new and very distinct methods of evidence gathering from a diverse set of devices. - Major legal adaptations.
4. Encryption	- A tradeoff exists between enhanced consumer privacy and successful investigation.	- To find common ground between encryption and privacy laws. - Develop new methods for live forensics.
5. Multimedia forensics	- Unusual media types, formats, and editing operations - The lack of standard and real data sets for research [86].	- Anti-forensics methods in multimedia. - Define threshold for legitimate or illegitimate processing.

5. Conclusion

We believe that digital forensic science is not a junk or invalid discipline, however, it needs time to mature and establish like all other sciences. Referring digital forensics as invalid science is unjustified without understanding the fundamental constraints of scientific validity and opposing aspects of the domain. The time for digital forensics to flourish is shortened by rapidly developing digital computing and communication technology. As evident from the discussion in the previous section that, it would be unfair to blame the researchers for lack of effort in developing scientific methods. Equally, the

regulating authorities are struggling hard for implementing quality controls in the domain. Notably, legal issues (i.e. privacy laws) are a significant limiting factor besides rapid progression in the field, however, these issues are not part of this discussion. An excellent discussion on legal issues for prosecuting cybercrimes is presented in [100], by Cameron Brown.

Therefore, it is also unfair to compare the validity and consistency of digital forensic methods to the benchmarks of other well-founded disciplines (i.e. Physics, Chemistry, or Biology) given they took centuries to develop. For instance, the laws of physics are debated since the time of Aristotle in 500BCE, and modern physics first emerged in the 16th and 17th century [101]. Likewise, chemistry started developing in the 9th century, and advanced scientific methods in chemistry appeared in 1662. Firstly, gunpowder was used in the early 1800s; it is an explosive consist of several chemicals used in bullets to kill living things. Preliminary gunshot residue analysis, a forensic study that used the knowledge from chemistry, was conducted in 1971 [102]. That timeline indicates these disciplines are supported by thousands of studies, debates, and experimentation. These subjects availed a larger time span in refining scientific practices to achieve the current status.

In comparison, all forensic sciences, in general, are more recent; and digital forensics is the latest. Such as the fingerprints were initially studied in 1686 and used for identification in 1882, and preliminary criminal fingerprint identification occurred in 1892 [103]. Likewise, in 1928 scientists identified DNA as a source of inheritance, they made an original DNA model in 1953 and started DNA profiling in 1984. Eventually, the initial conviction based on DNA evidence was built in 1988 in the Enderby murder case in Leicestershire, England [104]. Even then, it involves over 30 years since the preliminary DNA model to the first conviction supported by DNA analysis. Meanwhile, the studies refined the knowledge and improve the practices for DNA matching. Besides, a DNA study has an advantage of having a static target. Every species has the same structure and components of DNA though have different properties. Unfortunately, the fundamental technologies are too diverse and dynamic in digital forensics.

Underlying techniques and technologies are evolving at a tremendous pace as mentioned earlier. Digital device types will continue to vary from one device to another. Their shape, structure, componentry, and methods of communication will use different platforms and storage formats. Indeed, every few months, new and novel gadgets will replace old gadgets.

Media advertising continues to capture the attention and imagination of users to upgrade. Similarly, changes in underlying technologies may appear during the formulation of forensic techniques given the pace at which technology is evolving. People immediately shift to novel communication methods such as social media or upgrade their mobile devices as mentioned. The digital forensic process is not proactive by nature, like other similar sciences, it requires continual revision to keep abreast and ahead of modern technology, rather than after the technology is already in place and being used.

In the review of digital forensic history, the timeline is concise and is more complicated than other subject areas. One of the first and publicly known electronic investigations was Cliff Stoll's detection of the hacker, by Markus Hess in 1986. The term computer forensics initially appeared in 1992 in an article written by Collier and Spaul [105] where they explained the new discipline. By the mid-90s, computer and Internet usage had become quite common.

The first cellular device appeared in the market in 1994; a Simon Personal Communicator produced

by Bellsmith [106]. Then by the year 2000, desktop computers, the Internet, and cellular phones were ubiquitous in society. Notably, in the year 2000, the first conviction based on digital evidence occurred where Michelle Theer was found guilty in a murder inquiry of her late husband. Emails were extracted from her computer revealing her involvement in a conspiracy for the killing [107]. During this time, initial investigations only involved the examination of electronic devices for traditional crimes.

Digital forensic science is now established to some degree, progressing rapidly since 2005. At that time, academic, and law enforcement communities acknowledged digital forensics as a distinct discipline [108]. Meanwhile, the first identifiable social media site appeared in 1997, named, Six Degrees, followed by MySpace and LinkedIn networking sites, which became prominent in the year 2000, Facebook emerged in 2005, followed by YouTube in 2006 and others after that. Moreover, these innovations were reasonably different from personal computers. Amazon Web Services introduced their cloud storage service, AWS S3 in 2006 and the first iPhones quickly started to replace cellular devices in 2007 having greater capability and processing power than previous conventional mobile phones. All these events occurred in a short span of three decades, which does not allow enough time for the proper birth and growth of a scientific discipline. Furthermore, this brief period included hundreds of new electronic techniques and technologies, indicating a rapid progression in this domain.

However, in this study, it is not presenting this argument as an excuse to ignore the use and development of scientific practices in digital forensics. Nevertheless, the aim instead, is to explain that it is a typical phenomenon and to prompt and encourage further research to be carried out in this domain. Researchers need to focus on developing empirical methods, which comply with legal infrastructure as it changes. Moreover, researchers need to discover novel approaches for experimental verification in this discipline and consider the underlying aspects and dynamics of the field given technological changes and its impact on electronic evidence.

Validity and reliability are two crucial features required to establish the correctness and confidence of scientific methods. Furthermore, a way or technique is valid if it does what it is supposed to do correctly. Reliability refers to preciseness and consistency, both independent of each other, and essential for the right systematic method or technique. In scientific research, these characteristics are studied, tested, and repeatedly revised to gain suitable acceptance. Therefore, it is important if not vital for academics and practitioners to ensure correctness and reliability of their methods. Moreover, because it is only possible to achieve trustworthiness and acceptance for approaches through extensive testing in various environments.

Benchmarking in digital forensics is extremely difficult to implement due to the rapid development and constant evolution of digital communications and technologies. Given the pace at which they are expanding, they are likewise, expanding the scope of digital forensics. Still, it is necessary to ensure both the quality and scientific background of digital forensic processes, for legal acceptance, to be thoroughly investigated. So, even in the absence of universally accepted standards and defined practices, the researcher can still prove the validity and reliability of their suggested or advanced approaches if they follow due process. For this purpose, they should determine the validity and reliability criteria first as they might explain the rules for discrete tasks instead of establishing the entire forensic process all at once. Accordingly, this bottom-up approach to describe and test the reliability and validity of individual

methods would assist in building confidence in the overall process in this domain.

Furthermore, it is imperative to develop innovative approaches to authenticate the reliability and accuracy of digital evidence and to meet scientific and judicial standards. Besides, it is appropriate to measure statistical error rates where feasible and to calculate the percentage of certainty by specific methods. Additionally, customized error mitigation strategies for discrete tasks will further improve the assessment process. Also, digital forensic researchers should focus on developing proper testing strategies and models to gain scientific validation and legal acceptance and approval. Notably, SWGDE also advised the same [38] and suggested to establish the optimum criteria in relevant sub-domains such as the cloud or for social media forensics. The explicit specification of required behaviour and validation criteria for individual methods would also be useful for this purpose as proposed by Cole et al. [25] who suggested that all tools and methodologies used in criminal and legal proceedings must fulfill these criteria. Indeed, these specifications will also assist in defining the parameters for future evaluations.

Open source testing for the forensic method is not workable without common data sets. However, if automated tools are implementable to support best practices and latest techniques and methods, the user community, such as investigators and legal practitioners, will be able to thoroughly check these datasets for potential errors. Furthermore, the process of testing would provide a readily available approach to test both the tools and the underlying approaches. Users and researchers will be able to make meaningful comparisons between software packages and to discover their shortcomings and suggest additional or revised functionality and requirements to support automated tools.

An appropriate and robust (if not indisputable) testing process should be developed and introduced to detect potential software weaknesses and vulnerabilities, documenting them in advance as anti-forensic environments that typically exploit these susceptibilities. Additionally, it would be helpful to achieve the basic standards for scientific evaluation and to contribute towards attaining the desired credibility for electronic evidence given the current and future challenges. In short, the digital forensic community must focus on developing solutions that are proven and evaluated by methodical means. New approaches should support and be able to confirm these methods, as traditional methods of experimental verification are not entirely suitable or appropriate at this time for digital forensics due to the issues, mentioned in this study. Otherwise, electronic evidence will continue to fail to prove the usefulness and value of digital forensics in a legal court of law.

Indeed, it is challenging if not difficult to develop universal standards for digital forensics, due to the diversity and rate of expansion in the medium. Also, at the same time, it is equally challenging to confirm the forensic practices through traditional means of scientific testing such as testing on standard data corpus. Researchers can, therefore, contribute to enhance the accuracy of suggested methods and ensure the reliability of proposed approaches to meet the legal criteria in the courts. The adopted techniques must be thoroughly tested and verified for their accuracy before applying. These approaches must be known for their potential error rates and limitations before using and support further testing under different circumstances. Furthermore, extensive testing and systematic verification are essential towards earning the sound presumption of authenticity. Therefore, highly accurate approaches based on solid scientific practices and foundations are the only option to ensure the advancement and future viability of digital forensics.

Acknowledgement

This research is partially supported by the Fundamental Research Grant Scheme (FRGS) (No. 203/PKOMP/6711426), SFRG Lab, School of Computer Sciences, Universiti Sains Malaysia.

References

[1] National Research Council, *Strengthening Forensic Science in the United States: A Path Forward*. Washington, DC: National Academies Press, 2009.

[2] President's Council of Advisors on Science and Technology, *Report to the President Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods*. Washington, DC: Executive Office of the President, 2016.

[3] D. M. Risinger, M. J. Saks, W. C. Thompson, and R. Rosenthal, "The Daubert/Kumho implications of observer effects in forensic science: hidden problems of expectation and suggestion," *California Law Review*, vol. 90, no. 1, 2002.

[4] P. Roberts, "Paradigms of forensic science and legal process: a critical diagnosis," *Philosophical Transactions of the Royal Society B*, vol. 370, no. 1674, article no. 20140256, 2015.

[5] M. Meyers and M. Rogers, "Digital forensics: meeting the challenges of scientific evidence," in *IFIP International Conference on Digital Forensics*. Boston, MA: Springer, 2005, pp. 43-50.

[6] E. Van Buskirk and V. T. Liu, "Digital evidence: challenging the presumption of reliability," *Journal of Digital Forensic Practice*, vol. 1, no. 1, pp. 19-26, 2006.

[7] G. Edmond and D. Mercer, "Trashing junk science," *Stanford Technology Law Review*, no. 3, 1998.

[8] R. G. Behrents, "Lucy fell from a tree and plunged 40 feet to her death," *American Journal of Orthodontics and Dentofacial Orthopedics*, vol. 150, no. 5, pp. 719-722, 2016.

[9] H. F. Fradella, A. Fogarty, and L. O'Neill, "The impact of Daubert on the admissibility of behavioral science testimony," *Pepperdine Law Review*, vol. 30, no. 3, pp. 403-444, 2002.

[10] D. J. Ryan and G. Shpantzer, "Legal aspects of digital forensics," 2002 [Online]. Available: http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf.

[11] D. B. Garrie, "Digital forensic evidence in the courtroom: understanding content and quality," *Northwestern Journal of Technology and Intellectual Property*, vil. 12, no. 2, article no. 5, 2014.

[12] S. Mahle, "An introduction to Daubert v. Merrell Dow," 2008 [Online]. Available: http://www.daubertexpert.com/basics_daubert-v-merrell-dow.html.

[13] European Network of Forensic Science Institutes, "Best Practice Manual for the forensic examination of handwriting," *Report No. ENFSI-BPM-FHX-01*, 2015.

[14] S. Garfinkel, P. Farrell, V. Roussev, and G. Dinolt, "Bringing science to digital forensics with standardized forensic corpora," *Digital Investigation*, vol. 6, pp. S2-S11, 2009.

[15] I. Baggili and F. Breitinger, "Data sources for advancing cyber forensics: what the social world has to offer," in *Proceedings of the 2015 AAAI Spring Symposium Series*, Palo Alto, CA, 2015.

[16] R. Bekkerman, "Automatic categorization of email into folders: benchmark experiments on Enron and SRI corpora," University of Massachusetts Amherst, MA, 2004.

[17] MAWI Working Group Traffic Archive [Online]. Available: http://mawi.wide.ad.jp/mawi/.

[18] H. Visti, "ForGe: computer forensic test image generator," 2013 [Online]. Available: https://articles.forensicfocus.com/2013/10/18/forge-computer-forensic-test-image-generator/

[19] M. Powell, "The canterbury corpus," 2001 [Online]. Available: http://corpus.canterbury.ac.nz/.

[20] "UMass Trace Repository," 2009 [Online]. Available: http://traces.cs.umass.edu/index.php/Main/HomePage.
[21] C. Grajeda, F. Breitinger, and I. Baggili, "Availability of datasets for digital forensics: and what is missing," *Digital Investigation*, vol. 22, pp. S94-S105, 2017.
[22] "Hacking Case," 2007 [Online]. Available: https://www.cfreds.nist.gov/Hacking_Case.html.
[23] Y. Yannikos, L. Graner, M. Steinebach, and C. Winter, "Data corpora for digital forensics education and research," in *IFIP International Conference on Digital Forensics*. Heidelberg: Springer, 2014, pp. 309-325.
[24] K. Roberts, M. A. Roach, J. Johnson, J. Guthrie, and S. M. Harabagiu, "EmpaTweet: annotating and detecting emotions on Twitter," in *Proceedings of the 8th International Conference on Language Resources and Evaluation*, Istanbul, Turkey, 2012, pp. 3806-3813.
[25] K. A. Cole, S. Gupta, D. Gurugubelli, and M. K. Rogers, "A review of recent case law related to digital forensics: the current issues," in *Proceedings of the Conference on Digital Forensics, Security and Law*, Daytona Beach, FL, 2015, pp. 95-103.
[26] A. Eckelberry, G. Dardick, J. A. Folkerts, A. Shipp, E. Sites, J. Stewart, and R. Stuart, "Technical review of the trial testimony State of Connecticut vs. Julie Amero," 2007 [Online]. Available: http://sunbeltblog.eckelberry.com/wp-content/ihs/alex/julieamerosummary.pdf.
[27] Scientific Working Group on Digital Evidence, "SWGDE establishing confidence in digital forensic results by error mitigation analysis," Scientific Working Group on Digital Evidence, 2017.
[28] S. L. Garfinkel, "Digital forensics research: the next 10 years," *Digital Investigation*, vol. 7, pp. S64-S73, 2010.
[29] J. I. James and P. Gladyshev, "Challenges with automation in digital forensic investigations," 2013 [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1303/1303.4498.pdf.
[30] J. Slay, Y. C. Lin, B. Turnbull, J. Beckett, and P. Lin, "Towards a formalization of digital forensics," in *IFIP International Conference on Digital Forensics*. Heidelberg: Springer, 2009, pp. 37-47.
[31] National Institute of Standards and Technology, "Computer Forensic Tool Testing Program (CFTT)," 2017 [Online]. Available: https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt.
[32] D. Bennett, "The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations," *Information Security Journal: A Global Perspective*, vol. 21, no. 3, pp. 159-168, 2012.
[33] L. Pan and L. Batten, "Reproducibility of digital evidence in forensic investigations," in *Proceedings of the 5th Annual Digital Forensic Research Workshop*, New Orleans, LA, 2005, pp. 1-8.
[34] G. Palmer, "A road map for digital forensic research," in *Proceedings of the 1st Digital Forensic Research Workshop,* Utica, NY, 2001, pp. 27-30).
[35] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *International Journal of Digital Evidence*, vol. 1, no. 3, 1-12, 2002.
[36] W. A. Jansen and A. Delaitre, *Mobile Forensic Reference Materials: A Methodology and Reification*. Gaithersburg, MD: US Department of Commerce, National Institute of Standards and Technology, 2009.
[37] Wholesale Applications Community, "What is WAC," 2015 [Online]. Available: http://www.wholesale appcommunity.com/what-is-wac/.
[38] Scientific Working Group on Digital Evidence [Online]. Available: https://www.swgde.org/.
[39] G. Tully, *Forensic Science Regulator's Annual Report 2014-2015*. Birmingham, UK: The Forensic Science Regulator, 2015.
[40] Forensic Science Regulator, *Draft Guidance : Digital Forensics Method Validation*. London: Crown Prosecution Service, 2014.
[41] State of North Carolina v. Bradley Graham Cooper (No. COA12-926) [Online]. Available: http://wwwcache.wral.com/asset/specialreports/nancycooper/2013/02/28/12166096/4128-sccoa.pdf.

[42] United States v. Suarez, 2010 WL 4226524 (D.N.J. Oct. 21, 2010) [Online]. Available: https://www.ediscoverylaw.com/2010/11/court-imposes-adverse-inference-for-failure-to-preserve-text-messages-related-to-criminal-investigation/.

[43] R. Harris, "Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem," *Digital Investigation*, vol. 3, pp. 44-49, 2006.

[44] C. S. J. Peron and M. Legary, "Digital anti-forensics: emerging trends in data transformation techniques," in *Proceedings of E-crime and Computer Evidence Conference*, Technip, Monaco, 2005.

[45] S. L. Garfinkel, "Carving contiguous and fragmented files with fast object validation," *Digital Investigation*, vol. 4, pp. 2-12, 2007.

[46] M. C. Stamm, W. S. Lin, and K. R. Liu, "Temporal forensics and anti-forensics for motion compensated video," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1315-1329, 2012.

[47] T. Newsham, C. Palmer, and A. Stamos, "Breaking forensics software: weaknesses in critical evidence collection," 2007 [Online]. Available: https://pdfs.semanticscholar.org/cc18/d7cc9017d35277d966fe62481a251280748d.pdf.

[48] I. Baggili, A. BaAbdallah, D. Al-Safi, and A. Marrington, "Research trends in digital forensic science: an empirical analysis of published research," in *International Conference on Digital Forensics and Cyber Crime*. Heidelberg: Springer, 2013, pp. 144-157.

[49] M. Wundram, F. C. Freiling, and C. Moch, "Anti-forensics: the next step in digital forensics tool testing," in *Proceedings of the 7th International Conference on IT Security Incident Management and IT Forensics*, Nuremberg, Germany, 2013, pp. 83-97.

[50] M. Anobah, S. Saleem, and O. Popov, "Testing framework for mobile device forensics tools," *The Journal of Digital Forensics, Security and Law*, vol. 9, no. 2, pp. 221-234, 2014.

[51] G. C. Kessler, "Anti-forensics and the digital investigator," 2007 [Online]. Available: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1000&context=adf.

[52] K. Hausknecht and S. Gruicic, "Anti-computer forensics," in *Proceedings of the 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO),* Opatija, Croatia, 2017, pp. 1233-1240.

[53] M. Rogers, "Anti-forensics: the coming wave in digital forensics," in *Proceedings of the Center for Education and Research in Information Assurance and Security*, West Lafayette, IN, 2006.

[54] K. Conlan, I. Baggili, and F. Breitinger, "Anti-forensics: furthering digital forensic science through a new extended, granular taxonomy, *Digital Investigation*, vol. 18, pp. S66-S75, 2016.

[55] R. Bohme and M. Kirchner, "Counter-forensics: attacking image forensics," in *Digital Image Forensics*. New York, NY: Springer, 2013, pp. 327-366.

[56] M. K. Rogers and K. Seigfried, "The future of computer forensics: a needs analysis survey," *Computers & Security*, vol. 23, no. 1, pp. 12-16, 2014.

[57] S. Biggs and S. Vidalis, "Cloud computing: the impact on digital forensic investigations," in *Proceedings of the International Conference for Internet Technology and Secured Transactions*, London, UK, 2009, pp. 1-6.

[58] G. Al Sadi, "Cloud computing architecture and forensic investigation challenges," *International Journal of Computer Applications*, vol. 124, no. 7, pp. 20-25, 2015.

[59] D. Lillis, B. Becker, T. O'Sullivan, and M. Scanlon, "Current challenges and future research areas for digital forensic investigation," in *Proceedings of the 11th ADFSL Conference on Digital Forensics, Security and Law*, Daytona Beach, FL, 2016.

[60] K. Curran, A. Robinson, S. Peacocke, and S. Cassidy, "Mobile phone forensic analysis," *International Journal of Digital Crime and Forensics*, vol. 2, no. 3, pp. 15-27, 2012.

[61] S. Schjolberg and S. Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime*. Oslo, Norway: Cybercrimedata, 2011.

[62] K. Nance, B. Hay, and M. Bishop, "Digital forensics: defining a research agenda," in *Proceedings of the 42nd Hawaii International Conference on System Sciences*, Big Island, HI, 2009, pp. 1-6.

[63] S. Raghavan, "Digital forensic research: current state of the art," *CSI Transactions on ICT*, vol. 1, no. 1, pp. 91-114, 2013.

[64] N. M. Karie and H. S. Venter, "Taxonomy of challenges for digital forensics," *Journal of Forensic Sciences*, vol. 60, no. 4, pp. 885-893, 2015.

[65] M. Damshenas, A. Dehghantanha, and R. Mahmoud, "A survey on digital forensics trends," *International Journal of Cyber-Security and Digital Forensics*, vol. 3, no. 4, pp. 209-235, 2014.

[66] "X1 Social Discovery," [Online]. Available: http://www.x1.com/products/x1_social_discovery/case_law_2012.html.

[67] "2015 mid-year e-Discovery update," [Online]. Available: http://www.gibsondunn.com/publications/Pages/2015-Mid-Year-E-Discovery-Update.aspx.

[68] J. Patzakis, "Hundreds of thousands of legal cases estimated to address social media in 2016," 2016 [Online]. Available: https://blog.x1discovery.com/2016/08/31/hundreds-of-thousands-of-legal-cases-estimated-to-address-social-media-in-2016/.

[69] State of Louisiana v. Demontre Smith (No. 2015–K–1359) [Online]. Available: https://law.justia.com/cases/louisiana/fourth-circuit-court-of-appeal/2016/2015-k-1359.html.

[70] M. Bader and I. Baggili, "iPhone 3GS forensics: logical analysis using apple iTunes backup utility," *Small Scale Digital Device Forensics Journal*, vol. 4, no. 1, pp. 1-15, 2010.

[71] J. Lessard and G. Kessler, "Android forensics: simplifying cell phone examinations," *Small Scale Digital Device Forensics Journal*, vol. 4, no. 1, pp. 1-12, 2010.

[72] D. Walnycky, I. Baggili, A. Marrington, J. Moore, and F. Breitinger, "Network and device forensic analysis of android social-messaging applications," *Digital Investigation*, vol. 14, pp. S77-S84, 2015.

[73] M. Huber, M. Mulazzani, M. Leithner, S. Schrittwieser, G. Wondracek, and E. Weippl, "Social snapshots: digital forensics for online social networks," in *Proceedings of the 27th Annual Computer Security Applications Conference*, Orlando, FL, 2011, pp. 113-122.

[74] M. Mulazzani, M. Huber, and E. Weippl, "Social network forensics: tapping the data pool of social networks," in *Proceedings of the 8th Annual IFIP Working Group,* Pretoria, South Africa, 2012, pp. 1-20.

[75] H. Chung, J. Park, S. Lee, and C. Kang, "Digital forensic investigation of cloud storage services," *Digital Investigation*, vol. 9, no. 2, pp. 81-95, 2012.

[76] V. Roussev and S. McCulley, "Forensic analysis of cloud-native artifacts," *Digital Investigation*, vol. 16, pp. S104-S113, 2016.

[77] N. H. Ab Rahman, N. D. W. Cahyani, and K. K. R. Choo, "Cloud incident handling and forensic-by-design: cloud storage as a case study," *Concurrency and Computation: Practice and Experience*, vol. 29, no. 14, article no. e3868, 2017.

[78] D. Quick and K. K. R. Choo, "Forensic collection of cloud storage data: does the act of collection result in changes to the data or its metadata? *Digital Investigation*, vol. 10, no. 3, pp. 266-277, 2013.

[79] B. Martini and K. K. R. Choo, "Cloud forensic technical challenges and solutions: a snapshot," *IEEE Cloud Computing*, vol. 1, no. 4, pp. 20-25, 2014.

[80] S. Simou, C. Kalloniatis, S. Gritzalis, and H. Mouratidis, "A survey on cloud forensics challenges and solutions," *Security and Communication Networks*, vol. 9, no. 18, pp. 6285-6314, 2016.

[81] X. Jin and G. Yang, "Model-checking of merging events for digital forensics," *International Journal of Digital Content Technology and its Applications*, vol. 6, no. 22, pp. 785-793, 2012.

[82] Y. Wen, X. Man, K. Le, and W. Shi, "Forensics-as-a-service (faas): computer forensic workflow management and processing using cloud," in *Proceedings of the 4th International Conferences on Clouding Computing, GRIDs, and Virtualization*, Valencia, Spain, 2013, pp. 208-214.

[83] S. Zawoad and R. Hasan, "Cloud forensics: a meta-study of challenges, approaches, and open problems," 2013 [Online]. Available: https://arxiv.org/abs/1302.6312.

[84] A. M. Balogun and S. Y. Zhu, "Privacy impacts of data encryption on the efficiency of digital forensics technology," *International Journal of Advanced Computer Science and Applications*, vol. 4, no. 5, pp. 36-40, 2013.

[85] S. Lowman, "The effect of file and disk encryption on computer forensics," 2010 [Online]. Available: https://www.lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

[86] United States District Court for the District of Vermont, "In re grand jury subpoena to Sebastien Boucher," No. 2:06-mj-91, 2009 WL 424718, 2009.

[87] D. Olenick, "Apple iOS and Google Android smartphone market share flattening: IDC," 2015 [Online]. Available: http://www.forbes.com/sites/dougolenick/2015/05/27/apple-ios-and-google-android-smartphone-market-share-flattening-idc/#345f7bcd2d4e.

[88] "IDC: Smartphone OS Market Share," 2017 [Online]. Available: https://www.idc.com/promo/smartphone-market-share/os.

[89] C. I. Wong, K. Y. Wong, K. W. Ng, W. Fan, and K. H. Yeung, "Design of a crawler for online social networks analysis," *WSEAS Transactions on Communications*, vol. 13, pp. 263-274, 2014.

[90] The Washington Post, "Compromise needed on smartphone encryption," 2014 [Online]. Available: https://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html?utm_term=.20649329becb.

[91] Human Rights Council, "Human Rights Council holds panel discussion on the right to privacy in the digital age," 2014 [Online]. Available: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15017&.

[92] D. E. Sanger and M. Apuzzo, "James Comey, F.B.I. Director, hints at action as cellphone data is locked," 2014 [Online]. Available: http://www.nytimes.com/2014/10/17/us/politics/fbi-director-in-policy-speech-calls-dark-devices-hindrance-to-crime-solving.html.

[93] J. L. Hall, "The NSA's split-key encryption proposal is not serious," 2015 [Online]. Available: https://cdt.org/blog/the-nsas-split-key-encryption-proposal-is-not-serious/.

[94] K, Schaul, "Encryption techniques and access they give," 2015 [Online]. Available: https://www.Washingtonpost.com/apps/g/page/world/encryption-techniques-and-access-they-give/1665/.

[95] P. Swire and K. Ahmad, "Encryption and Globalization," Columbia Science and Technology Law Review, vol. 13, pp. 416–481, 2012.

[96] C. Thompson, "The revolutionary quantum computer that may not be quantum at all," 2014 [Online]. Available: https://www.wired.com/2014/05/quantum-computing/.

[97] D. Poeter, "IBM says it's 'on the cusp' of building a quantum computer," 2012 [Online]. Available: https://www.pcmag.com/article2/0,2817,2400930,00.asp.

[98] T. Simonite, "Digital summit: Microsoft's quantum search for the 'next transistor,'" 2014 [Online]. Available: https://www.technologyreview.com/s/528256/digital-summit-microsofts-quantum-search-for-the-next-transistor/.

[99] V. Wadhwa, "Quantum computing is about to overturn cybersecurity's balance of power," 2015 [Online]. Available: https://www.washingtonpost.com/news/innovations/wp/2015/05/11/quantum-computing-is-about-to-overturn-cybersecuritys-balance-of-power/?utm_term=.4bbf79aa1abf.

[100] C. S. Brown, "Investigating and prosecuting cyber crime: forensic dependencies and barriers to justice," *International Journal of Cyber Criminology*, vol. 9, no. 1, pp. 55-119, 2015.

[101] A. J. Slavin, "A brief history and philosophy of physics," 1994 [Online]. Available: https://www.trentu.ca/physics/history_895.html.

[102] Columbia University, "History of chemistry," [Online]. Available: http://www.columbia.edu/itc/chemistry/chem-c2507/navbar/chemhist.html.
[103] History of Forensic Psychology, "Fingerprint analysis," [Online]. Available: http://forensicpsych.umwblogs.org/research/criminal-justice/fingerprint-analysis/.
[104] D. A. Mandal, "History of DNA research," 2012 [Online]. Available: https://www.news-medical.net/life-sciences/History-of-DNA-Research.aspx.
[105] P. A. Collier and B. J. Spaul, "A forensic methodology for countering computer crime," *Artificial Intelligence Review*, vol. 6, no. 2, pp. 203-215, 1992.
[106] B. Reed, "A brief history of smartphones." 2010 [Online]. Available: https://www.pcworld.com/article/199243/a_brief_history_of_smartphones.html.
[107] K. Bryan, "Psychologist Michelle Theer, her Internet affair with John Diamond, and the murder of air force captain Marty Theer," 2017 [Online]. Available: https://soapboxie.com/military/Michelle-Theer-John-Diamond.
[108] M. Pollitt, "A history of digital forensics," in *IFIP International Conference on Digital Forensics*. Heidelberg: Springer, 2010, pp. 3-15.

Humaira Arshad https://orcid.org/0000-0003-3615-6202

She is Assistant Professor in the Department of Computer Sciences & IT at the Islamia University of Bahawalpur, Pakistan. She joined the faculty of Computer Sciences & IT in 2004. Previously, she holds a Master's degree in information technology from National University of Science and Technology (NUST), Pakistan. Presently, she is studying for Ph.D. at School of Computer Science in Universiti Sains Malaysia. Her areas of Interest are digital & social media forensics, information security, online social networks, cybersecurity, intrusion detection, reverse engineering and semantic web.

Aman Bin Jantan https://orcid.org/0000-0001-9899-2287

He is an Associate Professor at the Faculty of School of Computer Sciences in Universiti Sains Malaysia. He got his Ph.D. and Master's degrees from Universiti Sains Malaysia. He has published over fifty articles in reputable journals and some of them has won local, national and international recognition. His research interest amongst others are artificial intelligence, cybersecurity, ICT application to national security, cryptography, forensic, computer & network security, e-commerce/web intelligence, compilers design & development techniques.

Oludare Isaac Abiodun https://orcid.org/0000-0003-0138-6446

He is a Senior Lecturer in Bingham University Kadope, Nigeria. Currently he is doing his PhD at School of Computer Science in Universiti Sains Malaysia. He also holds a Ph.D. in Nuclear and Radiation Physics from Nigerian Defense Academy, Kaduna. His research interests are computer science, ICT application to national security, security management, artificial intelligence & robotics, cybersecurity & digital forensic, terrorism & society, cryptography, nuclear security.