American Journal of Computer Science and Information Engineering
2018; 5(1): 9-14
http://www.aascit.org/journal/ajcsie
ISSN: 2381-1110 (Print); ISSN: 2381-1129 (Online)

AASCIT American Association for Science and Technology

Establishing a Process for Cyber Related Crimes Investigation Through Digital Forensics

Dipo Theophilus Akomolafe[1, *], Abiola Olawale Ilori[1], Yerokun Oluwatoyin Mary[2]

[1]Department of Mathematical Sciences, Ondo State University of Science and Technology, Okitipupa, Ondo State, Nigeria
[2]Department of Computer Science Education, Federal College of Education (Technical), Asaba, Delta State, Nigeria

Email address

dtakomolafe@yahoo.com (D. T. Akomolafe)

[*]Corresponding author

Citation

Akomolafe Dipo Theophilus, Ilori Abiola Olawale, Yerokun Oluwatoyin Mary. Establishing a Process for Cyber Related Crimes Investigation Through Digital Forensics. *American Journal of Computer Science and Information Engineering.* Vol. 5, No. 1, 2018, pp. 9-14.

Received: February 9, 2018; **Accepted**: March 10, 2018; **Published**: May 16, 2018

Abstract: As cyber related criminal attacks become more predominant in today's technologically driven society, the need for digital evidence to prosecute such activities has increased. The process used to acquire this digital evidence is digital forensics, a branch of Computer Science. Digital forensic is a new and developing field, still in its infancy, when compared to traditional forensic fields. Over the years, investigation in digital forensic field has been tool centered and being propelled by commercial developers. This, along with lack of established standards to guide digital forensics practitioners has raised divergent and confusing issues in the acceptability of digital evidence. Issues regarding the reliability, confidentiality, verifiability and consistency of digital evidences have been the major obstacles in the acceptance of digital evidence. Consequently, this paper aimed at addressing issues regarding digital forensics investigation process, methods, methodologies and standards for acquiring and preserving digital evidence using the grounded theory approach. Data were gathered using literature surveys, questionnaires and electronic interviews. The results obtained in the study pointed to the fact that there were no existing standards in place for digital forensics investigation process. A framework and methodology was established to address the identified issues thus laying the foundation for a single integrated approach to digital forensics.

Keywords: Digital Forensics, Digital Evidence, Cybercrimes, Grounded Theory

1. Introduction

Digital forensic is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime [2]. It is the branch which deals with the crimes which happen over the computers, where a single computer system constitutes an entire crime scene or in the least it may contain some evidence or information that can be useful in the investigation. However, in technical terms it can be defined as the process of identification, acquisition, preservation, analysis and documentation of any digital evidence [7]. As society becomes increasingly dependent on computer systems, from controlling critical infrastructure to providing public services over the web, the importance of protecting against and arresting threats from vandals, criminals, industrial espionage and cyber-terrorism grows dramatically. Computer forensic is a science of acquiring, preserving, retrieving, analyzing and presenting data that have been processed electronically and stored on computer media. Computer here means any electronic device like wrist watches, biro, camera, etc. The goal of digital forensic is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of establishing a fact; a crime has been committed or not. According to US department of Justice, FBI, Computer Forensic includes formalized and approved methodology to:

a. Collect
b. Analyze and
c. Present data in a court of law.

Cyber related crimes have become pervasive in today's technologically driven society. Cybercrime is any crime that is committed by means of special knowledge or exert of the computer technology. Cybercrime are harmful acts committed from or against a computer or network.

Cybercrimes differ from most crimes in these four ways:

They are easy to learn how to commit

a. They require few resources relative to the potential damage caused
b. They can be committed in a jurisdiction without being physically present in it
c. They are often not clearly illegal

With the continued increase in the use and availability of digital devices and with previously stored analogue data being made digital, there is the continued need for digital evidence to combat cyber criminals. The nature of digital evidence makes it different from other types of evidences [12].

Computer forensics and forensic computing referred to the use of computer related evidence during investigation and reporting of cyber related crimes. Today, however the terms digital forensics and digital investigations are frequently used to cover the process by which digital evidence is acquired, examined, analyzed and presented. The prevalent use of computers and its related digital technologies have become increasingly popular [11], these set of devices are increasingly being used to assist in committing electronic crimes and introducing new dimension to traditional crimes. It is of note that cybercrime never came days or years after the invention of cyberspace rather it came with it and the real challenge with cybercrime is that the accused or the criminal can stay hidden in the virtual domain [6]. Thus, digital forensics has been developed to investigate and prosecute offenders of digital crimes

Forensics has also become popular in the computer science field as digital devices are increasingly being used in the facilitating of crimes investigation and thus there is need for standardization in this area to ensure the viability of the evidence produced [3]. Digital devices are increasingly being used to commit crimes or as an accessory to a crime. Whereas the evidence from such scenes may be physical and easily accessible to crime scene officers' others may exist in the digital realm proving to be more of a challenge. The digital devices used for such crimes may contain traces of digital footprints which may be reproduced into digital evidence. The processes, skills and tools employed in digital forensics to gather, preserve and present digital evidence are still in their developmental stages and new ways of analyzing and interpreting its resultant digital evidence are constantly being developed and formalized. A standard process is yet to be adopted by all forensic investigator during cybercrime investigation, for example, in a survey conducted by the Forensic Focus in September 2015, around five hundred people were asked to voice their opinion on the biggest challenges faced today by the digital forensic investigators. This question stimulated overabundance of answers which comes down to lack of standard process in cybercrime investigation [9]. Though the cybercrime investigations vary, the process is likely to include recovery, interpretation and presentation [10]. This research takes a critical look at the field from an integrated perspective, identifying gaps in the various processes as it relates to standards and procedures in carrying out a digital forensics investigation.

The aim of this research was to create a digital forensics framework from which a detailed methodology will be derived to be used by digital forensic experts in the field when investigating cyber related crimes. It is aimed that the solution obtained will be supported by empirical evidence produced from data collection and analysis to ensure its relevance to practitioners in the field by combining methods, both qualitative (existing literature) and quantitative (interviews and questionnaires), to gather data from professionals in the field with the objectives to develop common code of practice for the digital forensics community, and also to devise a comprehensive methodology that will allow computer forensic practitioners to capture and preserve digital evidence acquired adequately, keeping in mind the volatility of the data.

2. Methodology

The research plan outlined the need for the research to review relevant academic papers published regarding digital forensics models/methodologies and frameworks. This review was expected to bring out certain patterns and information that would be further explored through a follow up survey. Three practitioners have performed three of the largest digital forensics/digital evidence related studies to date and they are [1, 2, 8]. This present study employs the grounded theory primarily because of lack of directly related empirical literature based on standards and guidelines in the digital forensics field. While there are a number of best practices and guidelines developed by different organizations and groups there is no evidence thus far of much empirical studies of standards and guidelines. Thus, this research has a qualitative focus with some quantitative data to ensure a rich set of data while embracing the concepts of the grounded theory. The stages of this study included phases of data gathering with intermediate outputs before the final output.

The study began with the collection of academic papers written highlighting computer/digital forensics models/frameworks/methodologies and standards. During the study, all valuable information noticed from different sources that contributed to the general concepts of the research was noted. A total of sixty (60) practitioners' responses were used in this phase of data gathering. These results were then analyzed using the Grounded theory techniques (Quantitative) as well as some qualitative techniques with a questionnaire being designed using both open ended and closed ended questions. This to ensure that there was a rich set of data as a combination of methods are deemed to produce much more than one method can in isolation as they complement each other [5].

3. Results

3.1. Background of Respondents

Sixty responses were received to the survey, however only fifty-two contained useful data. Eight of the respondents entered only their demographic data and left the other

questions blank. The survey sought to ascertain the diversity of the background of digital forensics practitioners. Results indicate that there were practitioners in the digital forensic field from various different backgrounds from Law enforcement, Technical personnel (computer science/Information technology), Management (Business oriented), and Legal (Lawyers, solicitors, barristers) etc.

Table 1. *Background of participants for the study.*

Background of respondents	No. Distributed	Percentage Distributed (%)	No. Responded	Percentage of Responses (%)
Law Enforcement	32	53	29	48
Technical	10	17	9	15
Management	8	13	6	10
Legal	10	17	8	13
Total	60	100	52	86

Table 1 above indicated that fifty-two participants responded out of the sixty questionnaires distributed. 56 percent of the participants that responded were of a law enforcement background, 17 percent were of a technical background, 12 percent were of a management background and 15 percent of the participants were of a legal background respectively.

This distribution was deemed useful as it included personnel from the core areas representing the core facets of the digital forensics discipline. One of the pervasive issues with digital forensics is that often the investigation is conducted by persons not qualified in the field. This is widely accepted that due to the diverse nature of digital forensics, since there will be practitioners from varying backgrounds, however there is a basic level of qualification expected. Qualification in this sense refers to formal training in the area of acquiring digital evidence (digital forensics). The survey's indication of the majority of respondents being of a law enforcement background is not surprising as cyber related crime is a criminal act and thus currently a number of police forces worldwide are instituting a cybercrime department and developing cyber related laws. This indicates an increase in efforts by different groups (governments and private sector) to fight the increasing occurrences of cybercrime worldwide.

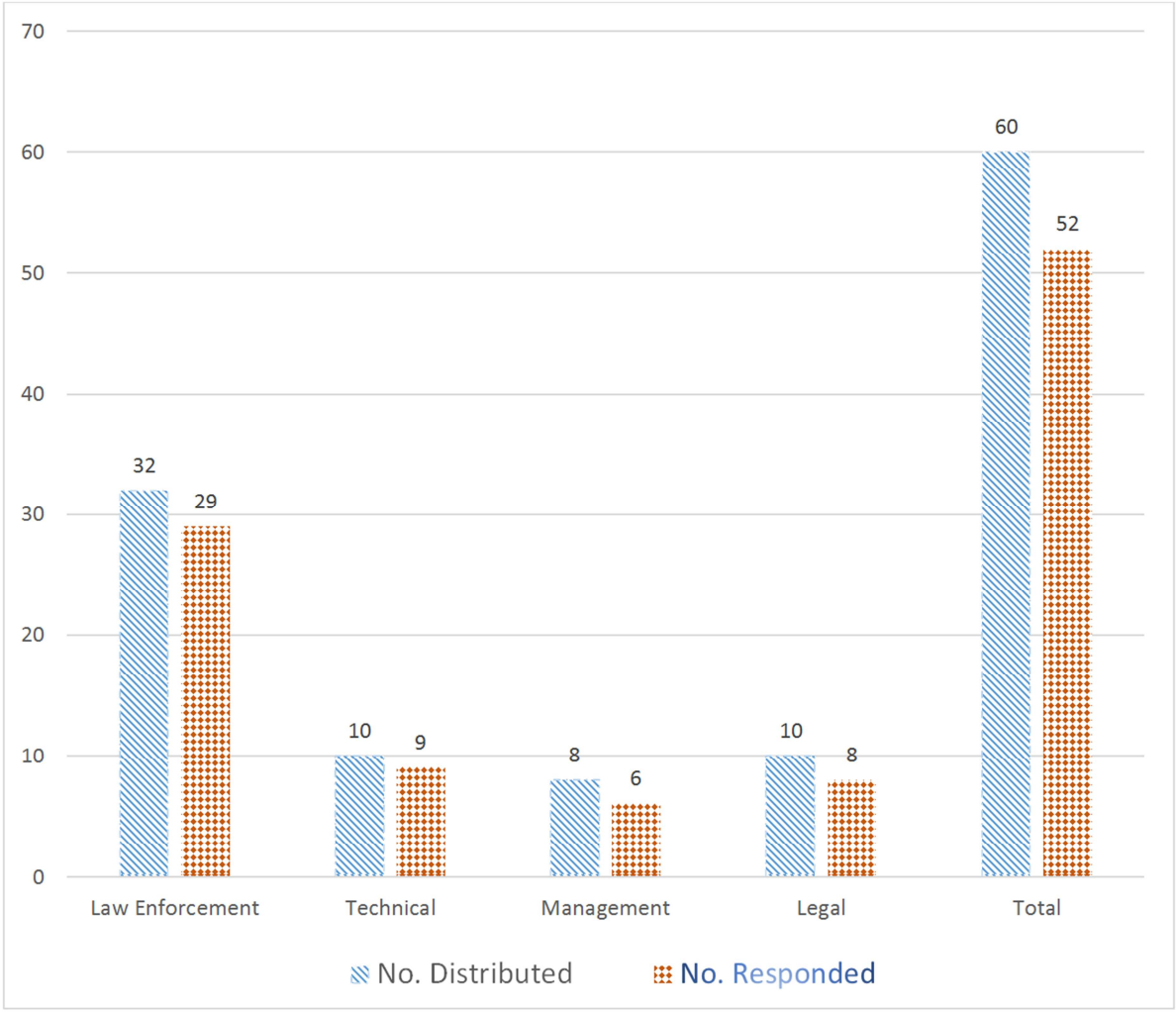

Figure 1. *Questionnaire feedback (No. distributed against No. responded).*

3.2. Years of Experience of Respondents

This study sought to ascertain the relative level of experience that practitioners in the field have, how long despite their background were they working as a digital forensics practitioner. Respondents were thus asked to indicate the number of years they had been practicing in the field. 23 percent of the respondents indicated that they had been in the field for 1-5 years as against 33 percent who were under one year in the field. 13 percent indicated that they had been in the field for 6-10 years, 15 percent, 8 percent and another 8 percent of the respondents indicated that they had been in the field for 11-15 years, 16-20 years and 21 years and above respectively (as shown in Figure 2). This indicated that most of the respondents were experienced practitioners in the discipline of digital forensics with real life experiences.

Table 2. *Years of experience of respondents.*

Years in practice	Under 1 year	1–5 years	6–10 years	11–15 years	16–20 years	20 years+
Law Enforcement	11	5	4	7	2	0
Technical	3	5	0	1	0	0
Management	1	1	2	0	0	2
Legal	2	1	1	0	2	2
Total	17	12	7	8	4	4

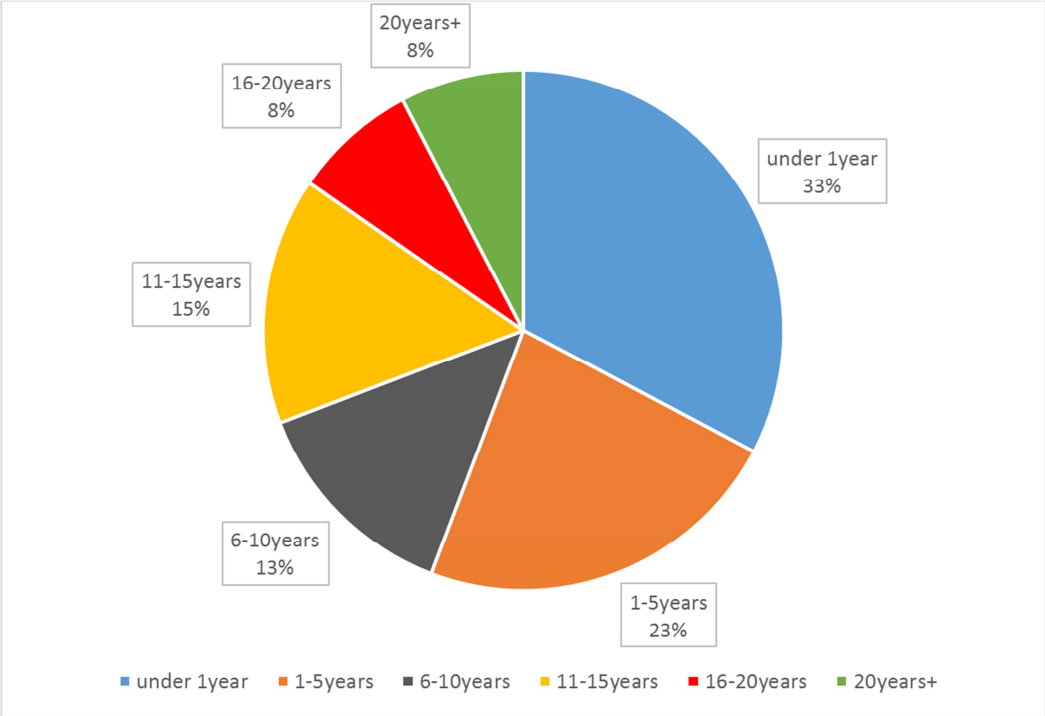

Figure 2. *Years of experience of respondents.*

3.3. Digital Forensic Policies/Tools

One of the main objectives of the survey was to ascertain the current state of digital forensic procedures with regards to procedures used to carry out a digital forensic investigation and the existence or need thereof for standards in the field. Respondents were required to respond to questions attempting to ascertain if there were any particular procedure and/or policies in use within their organizations and if so, were there any policies in place to guide these procedures. This question was followed by another seeking to find out how the procedures (if any) were developed.

Table 3. *How policies used by organization are developed.*

	YES	NO
i. Are there policies in place to guide the Digital Forensic process?	72%	28%
ii. Do you use a particular methodology when conducting digital forensic investigation?	25%	75%
iii. How were these policies developed?		Percentage
a. In house		48%
b. Bought from a commercial organization		0%
c. Adapted from another organization		20%
d. Others		32%

The result shows that there were no policies used by some practitioners at some point during digital forensics process. Seventy-two percent of the respondents said YES they had policies in place to guide the digital forensics processes while twenty-eight said NO. However, in the follow up question where practitioners were asked how these policies came about forty-eight (48) percent of the respondents said they developed them in-house, twenty (20) percent said they adopted them from other organizations while thirty-two percent (32) responded by selecting others. With forty-eight percent of practitioners stating that they developed their own policies in-house it safely be interpreted that most practitioners do their own thing. Practitioners choosing 'other' indicated that the policies they used were based on those from other organizations and groups.

4. Discussions

These results confirmed the following that while there are policies in place to guide practitioners in the digital forensics processes, these policies are mainly developed by the organizations themselves with a lesser percentage being adapted from other organizations. Organizations and individuals have their own guidelines that they create and adapt for use signifying that there is no one standard benchmark policy or guide that is used. Respondents were asked if they used any particular methodology when conducting investigations of a digital forensics nature, the respondents indicated that they do not use any one specific methodology to acquire digital evidence. Twenty-five (25) percent of the respondents answered yes while seventy-five (75) percent indicated that they did not, this is another attribute to the existing disjoint in the digital forensics field being the lack of uniformity in how specific tasks are carried out. Data here again indicates that practitioners in the field do their own thing, using their discretion based on a variety influencing factors.

This ad hoc use of varying procedures throughout the digital forensics process was further highlighted when respondents were asked to list the steps taken to carry out the digital forensics process from start to finish. The responses were varied, with practitioners indicating different tasks that signaling the beginning of the process and varying tasks that indicated the end. While some practitioners saw their cases ending at the outcome of a case others saw it ending when they presented their report. There are some practitioners that respond to a request for their services by researching the background of the case, others had a preliminary look at the devices involved, while some practitioners indicate that the first step before doing anything was to ensure that they got legal permission. There was also wide variation with intermediate procedures taken throughout the digital forensics process. The ad hoc ways in which digital forensics is carried out has been an ongoing challenge for the digital forensic community. These challenges present issues with the robustness of the resulting digital evidences. Such a variation in tool usage calls into question the issue of consistency and reliability. This is an issue that needs to be addressed in the field. Considering the gaps identified in the field of forensics practice during this research, a model was proposed to standardize digital forensics processes in investigating computer related crimes.

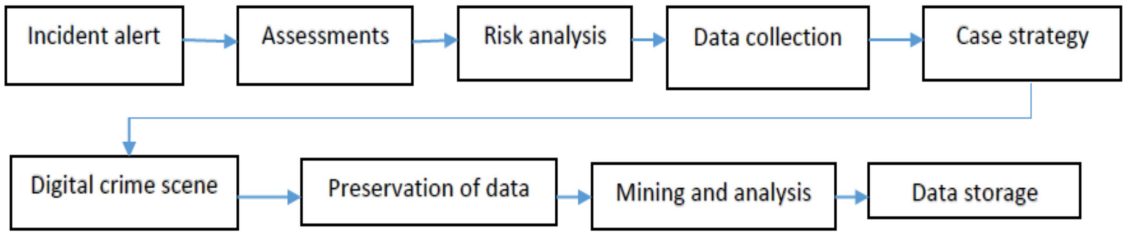

Figure 3. *Chart depicting general overview of the proposed standardized model for digital forensics investigation.*

From the analysis and evaluation of the results, some key elements in the process of investigation were extracted. These elements were common to all respondents and could therefore be harmonized to establish a pragmatic process for investigating cyber related crimes. The established processes are made up of the following components:

Organizations should perform forensics using a consistent process. In this process, Figure 3 can be collapsed into a four-phase forensic process, with collection, examination, analysis, and reporting phases. The exact details of each phase may vary based on the need for forensics.

There is a range of possible data sources an analyst can choose from during data gathering stage. Analysts should be able to survey a physical area and recognize all possible sources of data. Analysts should also think of possible data sources located elsewhere within an organization and outside the organization. Furthermore, analysts should be prepared to use alternate data sources if it is not feasible to collect data from a primary source.

Organizations should be proactive in identifying and collecting useful and relevant data. Security standards such as Configuring auditing on OSs, implementing centralized logging, performing regular system backups, and using security monitoring controls can create diverse sources of data for forensic tasks and responsibilities, therefore must be put in place and enforced.

Data collection must be performed using a standard process. The recommended steps in this process are:

a. sources of data identification,
b. developing a plan to acquire the data,

c. data acquisition and
d. data integrity verification.

The data acquisition plan should prioritize the data sources, establishing the order in which the data should be acquired based on the likely value of the data, the volatility of the data, and the amount of effort required. However, before the commencement of data collection, a decision should be reached by the analysts or management regarding the need to collect and preserve evidence in a manner that guarantee its safety, preserve its integrity and supports its use in future legal or internal disciplinary proceedings. In such situations, a clearly defined chain of custody should be followed to avoid allegations of mishandling or tampering of evidence. If it is unclear whether or not evidence needs to be preserved, by default it generally should be preserved.

Adopting a methodical approach to studying the data The foundation of forensics is using a methodical approach in analyzing the available data to either draw appropriate conclusions based on the available data or determine that no conclusion can be drawn with the available evidence. If evidence might be needed for legal or internal disciplinary actions, it is necessary to carefully document the findings and all steps taken.

Analysts should review their processes and practices at every stage. Regular reviews of current and recent forensic actions can help identify policy shortcomings, procedural errors, and other issues that might need to be remedied, as well as ensuring that the organization comply with current trends in technology and changes in law.

5. Conclusion

The need for standardization in the field has been duly noted and this need cannot be over emphasized. This work presents a framework of standards incorporating principles from a/an educational, ethical, legal and technical perspective. This study was mainly qualitative (Grounded theory) but employed some quantitative methods (questionnaires). It was conducted in stages which are an initial survey of the existing literature in the field identifying any gaps and omissions. This was then followed with a gathering of data from practitioners in the field with regards to the initial design created and then finally designed a proposed model to standardize digital forensic investigation processes.

Recommendations

The problem of standardization in the area of digital forensics has been an issue from the initial stages and still faces major challenges. It is integral that agencies and practitioners adhere to a defined set of standards and operating procedures to ensure this evidence and methodology is accepted globally.

Errors in analysis and interpretation of digital evidence are more likely where there is no standard procedure for collecting, preserving and analyzing digital evidence [4]. Hence, there is need for standardization of the procedures used in investigation cyber related crime through digital forensics processes.

References

[1] Carlton, G. H. (2007). “A grounded theory approach to identifying and measuring forensic data acquisition tasks”. Journal of Digital Forensics, Security and Law, 2 (1), 35-55.

[2] Carrier, B. D. and Spafford, E. (2004). “An event based Digital Forensics Investigation Framework.” Center for Education and Research in Information Assurance and Security.

[3] Casey, E. (2011). “Digital Evidence and Computer Crime, Forensic science, Computers and the Internet”. Academic Press, London, UK.

[4] Chaikin D. (2007). “Network Investigations of Cyber Attacks: The limits of digital evidence, Springer Science and Business Media”.

[5] Hall, B. and Howard, K. (2008). “A Synergistic Approach: Conducting Mixed Methods Research With Typological and Systemic Design Considerations”. Journal of Mixed Methods Research, 2 (3) 248-269.

[6] Harbawi Malek, and Asaf Varol. "The role of digital forensics in combating cybercrimes". Digital Forensic and Security (ISDFS), 2016 4th International Symposium on. IEEE, 2016.

[7] Kent, Karen, et al. (2006). "Guide to integrating forensic techniques into incident response." NIST Special Publication 10: 800-86.

[8] Kessler, G. C. (2010). “Judges’ awareness, understanding, and application of digital evidence” (Doctoral dissertation, Nova Southeastern University).

[9] Lillis David, et al. (2016). "Current Challenges and Future Research Areas for Digital Forensic Investigation". arXiv preprint arXiv:1604.03850.

[10] Metropolitan Police Service (2015). Information for Prospective Bidders, Digital Cyber and Communications Forensics Unit.

[11] Nance, K., Hay, B. and Bishop, M. (2009). “Digital forensics: Defining a research agenda”. Proceedings of the Forty-Second Annual Hawai'i International Conference on System Sciences. Los Alamitos, CA: IEEE Press.

[12] Schatz, B. (2010). “Towards reliable volatile memory acquisition by software”. Digital investigation, 4, 126-134.