BOOK CHAPTER | *"What Happens in Vegas Stays in Vegas"*

Evidence Confidentiality and Digital Forensic Experts

John Kwaku Oppong
Information Technology & Law Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: jokpon@yahoo.com
Phones: +233545909859, +233201711300

ABSTRACT

Digital forensics has increasingly galloped into the space of criminal justice and law enforcements as a unique tool for evidence and its dissemination. Technological advancement in database and information has also made digital forensics an important tool in law enforcement and judicial proceedings. On the other side of the coin, evidence confidentiality is an indefinite concept and one that is very dynamic and intricate. Therefore, the services of forensic experts in the digital forensic field are often required due to the significance of digital evidence to many investigations. This paper provides a brief information about evidence confidentiality and digital forensic experts.

Keywords: Digital Forensics, Evidence, Confidentiality, Forensic Experts, Justice, Law.

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: John Kwaku Oppong (2022): Evidence Confidentiality and Digital Forensic Experts
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 161-166
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P26

1. INTRODUCTION

Managing records over the years has evolved from paper form to paperless due to the emergence of digital devices. Records are primarily kept or stored for proper accountability and reference sake. Some of these records in the long-run serve as evidence in the matters of law and auditing purposes. Over the years, records management has evolved with several data protection enactments providing security to certain records and its use. In this modern era, evidence confidentiality issues can include potential breaches of data protection principles, such as in the UK Data Protection Act, breaches of client or contractual confidentiality, and contraventions of due legal process.

1.1 Background Of The Study

Digital forensics, the art of recovering and analysing the contents found on digital devices such as desktops, notebooks/netbooks, tablets, smartphones, etc., was little-known a few years ago (Pande, 2016).

While digital evidence exploitation is a relatively new tool for law enforcement investigations, law enforcement relies extensively on digital evidence for important information about both victims and suspects. Major shifts in the information technology landscape over the past two decades have made the collection and analysis of digital evidence an increasingly important tool for solving crimes and preparing court cases (Goodison, 2015).

2. LITERATURE REVIEW

This section of the paper deals with the concept of digital forensics, the law of evidence, forensic experts, the challenges and the way forward in the discipline.

2.1 Concept of Digital Forensics

Digital forensics is used to help investigate cybercrime or identify direct evidence of a computer-assisted crime. The concept of digital forensics dates back to late 1990s and early 2000s when it was considered as computer forensics (Sathiyanarayanan, 2016). The introduction of digital forensics was as a result of the increase in cybercrime and other criminal cases which required rigorous investigation processes and methods.

2.2 Law of Evidence & Confidentiality

According to New Zealand Law Commission (1999), the Law of Evidence is the set of rules by which judges determine what testimony and exhibits may be accepted and how they may be used. Evidence confidentiality and digital forensics is inseparable and the level of evidence confidentiality are usually regulated by law. These regulations have placed certain limitations on digital forensic experts on their roles and responsibilities. According to Koroway (1978), the law of evidence has long divorced itself from so simple an approach. Indeed, it is characterized by its pronounced exclusionary rules. Evidence may be excluded because it is too unreliable, as is true of much rumour, or it may be excluded as being too prejudicial, as in similar fact cases.

Confidentiality is regulated by privileges set out in enactments. In Ghana, the Evidence Act, 1975 N.R.C.D. 323, section 88 (1) & (2) states that:

(1) Except as otherwise provided in this Part or in any other enactment, a person does not have a privilege (a) to refuse when duly subpoenaed to be a witness; or (b) to refuse as a witness to disclose a matter; or (c) to refuse as a witness to produce an object or a writing.

(2) Except as otherwise provided in this Part or in any other enactment, a person may not prevent any other person from being a witness, from disclosing a matter, or from producing an object or a writing.

This section is part of many sections that set out limitations in disclosure of information. Other sections that set out disclosure or privilege rules are section 93, communications presumed confidential; section 98, disclosure of things owned by another; section 99 required reports; and section 100, Lawyer-client privilege. These are few of the many sections in the Evidence Act of Ghana that protect information through disclosure and privileges.

2.3 Forensic Experts

Digital forensic experts are generally responsible for data collection, analysis and its preservation for investigations and other legal proceedings. According to Francis (2021), digital forensics experts are experienced in preserving data in a manner that will stand up in legal proceedings, and analysing a range of digital evidence to provide verifiable and defensible answers to the key questions in an investigation.

It is argued that one of the key ways to acquire expertise in Digital Forensic Science is a practitioner's ability to reliably interpret any data they encounter and to demonstrate that they can do this effectively (Horsman, 2022). In Ghana, the EVIDENCE ACT, 1975 N.R.C.D. 323, section 67 (1) states that "A person is qualified to testify as an expert if, to the satisfaction of the Court, that person is an expert on the subject to which the testimony relates by reason of the special skill, experience or training of that person. Thus, the expert must also prove to the court how relevant his expertise will serve the court within the confines of the subject matter at stake.

2.4 Challenges

The exponential growth and advancements in the field of computing and network technologies have made existing digital forensics tools and techniques ineffective. The swift development in digital forensics resulted in a lack of standardization and training (Sathiyanarayanan, 2016). According to Al Fahdi, Clarke & Furnell (2013), the challenges of digital forensics can be categorized into three parts.

- Technical challenges – e.g. differing media formats, encryption, steganography, anti-forensics, live acquisition and analysis.
- Legal challenges – e.g. jurisdictional issues, privacy issues and a lack of standardized international legislation.
- Resource challenges – e.g. volume of data, time taken to acquire and analyse forensic media.

Limited capacities of law enforcement, prosecutors and the judiciary is the main impediment to an effective criminal justice response to cybercrime and other offences involving electronic evidence not only in Africa but in most countries around the world.

2.5 Implications For African Forensic Experts And Practitioners

With this field constantly growing in stature, there comes a wide array of implications for experts and practitioners on the African Continent. These implications take a bow into both positive and negative effects. In Ghana, the major forensic player is the Forensic Science Lab (FSL) of the Ghana Police Service and the Ghana Narcotics Control Board. On the positive side, rapid technological transformation helps forensic experts in the numerous ways listed below;

a) **Assisting in Law Enforcement**: The development of forensic science helps in law enforcement. Forensic experts are tasked to develop strategies that help resolve criminal or civil issues in court. According to Dutton et al (2015), innovations from forensic science research and development are bringing new techniques to crime solutions. With these, forensic experts from Africa can boast of their efforts in the assisting in law enforcement in the field.

b) **Increase in Capacity Building**: The more crime rates increase, it presents forensic experts with the need to tighten their grip with increased research labs, training programmes and new methods of handling criminal justice. According to A.O Amankwaah et al (2019) information from the Ghana Police Service website indicates that the chemistry and drugs analysis section of the Forensic Science Lab examines an average number of 800 cases of confiscated drug samples per year. These numbers are expected to double in the next few years, thus, increased workload calls for better and enhanced working conditions. In spite of the positive implications for experts and practitioners in the forensic field, many adversities are prevalent and needs to addressed. These are:

a) **Lack of Campaign and Awareness**: With over 50 states on the African Continent, only a selected few have managed to promulgate laws on forensic science and or digital forensics. According to the Council of Europe or of the Parties to the Budapest Convention on Cybercrime, as at 2016, the majority of African States (30) did not have specific legal provisions on cybercrime and electronic evidence in force. Only Ghana, Nigeria, Cameroon, Mauritania, Mauritius, Botwana, Ivory Coast, Senegal, Tanzania, Uganda and Zambia had substantive legal provisions on cybercrime and electronic evidence. Thus, the very few in the field are heavily tasked on getting the populace to understand the need for digital forensic science. The more the campaign is reached out to the many, the more people can exercise their right to engage a digital forensic scientist.

b) **Lack of Support to Privatise the Profession**: Unlike the developed world where there are many private forensic organizations, Africa on the other hand is far from privatising this profession. With law enforcement agencies being the primary customers, forensic science services are mostly provided by state-owned forensic science laboratories, with few exceptions such as in the UK where a commercialised private sector exists as stated by Amankwaah et al (2019) in Forensic Science in Ghana: Review. This field hugely depends on infrastructure such as sophisticated systems for fingerprint detection, DNA and blood sampling devices, video referencing devices and high quality storage devices. Many forensic experts are forced to struggle for limited employment space in the public sector. In other words, there is limited platform for forensic experts to perform in Africa except a few.

2.6 Opportunities And Way Forward

The digital forensic science discipline has many multidimensional opportunities that needs attention. This discipline is encouraged in every facet of life. Some of the field that require evidence confidentiality the most are the medical industry, courts, defence and security agencies, telecommunication and the e-commerce industry.

3. RESEARCH GAPS/FINDINGS

Many organizations, especially in Ghana and other parts of Africa, are not well informed about the significance of a forensic expert and the use of digital evidence. There is little exploitation about legal reforms that will protect the discipline whilst keeping the interest of forensic experts in Ghana and other parts of Africa. Like any other discipline, this field need to set standards and code of ethics in order to thrive to the apex of its abilities. More inquiry is needed in the area of witness protection as well.

4. CONCLUSION

The digital space and its technological advancement is very significant in the long-run for many organizations. The use of social media devices in this era has called for the need to prioritise digital evidence confidentiality and forensic science. With the view of strengthening the legal reforms around this discipline, crime rate and corruption will reduce drastically.

5. RECOMMENDATION FOR POLICY AND PRACTICES

This section of the paper outlines recommendations for policy and practices. These recommendations are expected to shape the discipline and create a congenial field for the experts and the end-users of this industry. Below are some recommendations to achieve this target;

- Comprehensive Legal Framework on Cyber Security: The digital evidence and forensic science field is a very dynamic area with constant technological change. Laws on digital forensics needs to meet a number of requirements. Some of them are the constant technological advancement; the laws must keep pace with the rapid evolution of sophisticated devices otherwise risks becoming outmoded already by the time it gets rolled out. Secondly these laws must protect the integrity of human rights and be compatible with laws of other countries to promote peace and harmony.

- Infrastructural Development: One of the many ways to improve the industry is to build enough facilities to train more experts for the field. Storage and handling infrastructure need to be available to store and manage evidence appropriately. A policy for secure storage and handling of potential evidence comprises security measures to ensure the authenticity of the data and also procedures to demonstrate that the evidence integrity is preserved whenever it is used, moved or combined with new evidence.

- Continual Practical Training: Training of existing experts and new experts is very key in maintaining established standards in the industry, this will enable all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.

- The Need for Research to Establish Limits and Measures of Performance.

6. DIRECTION FOR FUTURE WORKS

Further inquiries can be done into the areas mentioned below;

- The role of Digital Experts in Subscriber Identification Module Fraud in Ghana.
- Digital Evidence - Bank and Regulatory Systems for Evidence Management.
- Importance of Computer Forensics in the digital currency market.

REFERENCES

1. Amankwa, A.O., A., Amoako, E.N., Bonsu, D. O. M., & Banyeh, M. (2019). Forensic Science in Ghana: A Review. Forensic Science International: Synergy, 1, 151-160
2. Al Fahdi, M., Clarke, N. L., & Furnell, S. M. (2013, August). Challenges to digital forensics: A Survey of Researchers & Practitioners attitudes and opinions. In 2013 Information Security for South Africa (pp. 1-8). IEEE.
3. Council of Europe/Project Cybercrime (2016). The state of cybercrime legislation in Africa – an overview
4. Dutton, G., Mcleod-Henning, D., Nguyen, M., Scott, F., Castellanos, V., Dupont, A., & Ernst, C. (2015). The Impact of Forensic Science Research and Development. National Institute of Justice.
5. EVIDENCE ACT, 1975 N.R.C.D. 323
6. Francis, A. (2021, June 2). SRM. Retrieved from SRM: https://insights.s-rminform.com/digital-forensics-general-counsel.
7. Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the US criminal justice
   system: Identifying technology and other needs to more effectively acquire and utilize digital evidence.
8. Horsman, G., & Shavers, B. (2022). Who is the digital forensic expert and what is their expertise?. Wiley Interdisciplinary Reviews: Forensic Science, e1453.
9. Koroway, E. (1978). Confidentiality in the Law of Evidence. Osgoode Hall LJ, 16, 361.
10. New Zealand Law Commission. (1999). Evidence Report 55–Volume 1: Reform of the Law. Wellington: New Zealand Law Commission.
11. Pande, J., & Prasad, A. (2016). Digital forensics. Uttrakhand Open University.
12. Sathiyanarayanan, M. (2016). Introduction to Digital Forensics. University of London, UK.