BOOK CHAPTER | *"Shared Responsibilities"*

Liabilities of Shared System in Forensic Analysis

Eric Sowah Badger
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: niihack.gh@gmail.com
Phone: +233242004431

ABSTRACT

In today's connected world, there is a tendency for connectivity even in the sectors which conventionally have been not so connected in the past, such as power systems substations. Substations have seen considerable digitalization of the grid hence, providing much more available insights than before. This has all been possible due to connectivity, digitalization, and automation of the power grids. Interestingly, this also means that anybody can access such critical infrastructures from a remote location, and gone are the days of physical barriers. The power of connectivity and control makes it a much more challenging task to protect critical industrial control systems. This capability comes at a price, in this case, increasing the liabilities and risk of potential cyber threats to substations. (ASIF, FARHAN , & EKSTEDT)

Keywords: Digital Evidence Backlog, Digital Forensic Challenges

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

Citation: Eric Sowah Badger (2022): Liabilities of Shared System in Forensic Analysis
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 191-196
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P31

1. INTRODUCTION

One of the biggest threats facing businesses and corporations today is Cyber-attacks and threats. If these are large enough in scale and magnitude, it could even be considered an act of Cyber terrorism, in which a significant impact can be felt both regarding cost and human emotion. Whenever something like this occurs, two of the most common questions that get asked are:

- How did it happen?
- How can this be prevented from happening again in the future?

Obviously, there are no easy answers to this, and depending on the severity of the Cyber-attack, it could take weeks and even months to determine the answers to these two questions.

Regarding the latter, this can be answered via the means of conducting various, in-depth penetration testing exercises. In this regard, once the lines of defense have been beefed up, these tests can push these defense mechanisms to their absolute breaking point, to determine and uncover any hidden weaknesses or holes. Regarding the former, this is where the role of forensics comes into play. For instance, any remnants of the Cyber-attack and any evidence left behind at the scene need to be collected very carefully collected and examined. It is from this point onwards then the questions of "who, what, where, when, and why" can be answered by the forensics examiners and investigators. It is important to keep in mind that the field of forensics, especially as it relates to Information Technology is very broad, and involves many subspecialties. These include digital forensics, mobile forensics, database forensics, logical access forensics, etc. to just name a few

In this research, we provide some liabilities in the field of digital forensics. We focus primarily on the hindrance involved in conducting a computer forensics case.

1.1 Background to the Study

Smartphones and other forms of digital devices have become an important part of modern society. Although a vast majority of digital devices are harmlessly used for checking emails, browsing the internet, entertainment, and simplification other daily tasks, the global proliferation of digital devices has also facilitated criminal activity (ali, 2017) The same devices that provide societal benefits, are also being used for planning, initiating, sustaining and recording criminal activity (McMillan, 2013)Digital forensics (DF), although being a rather new phenomenon within the criminal investigation, is a crucial part of acquiring information about suspects and potential victims. Over 80 percent of court cases in recent years have involved some type of digital evidence, which has resulted in new challenges in how to process and assess forensic evidence.

Therefore, the need and demand for forensic tools that accurately extract and analyze digital evidence have accelerated. The widespread use of digital devices in society has resulted in a broad variety of digital forensic tools emerging on the market over the last two decades. (Benkhelifa, 2016)Different digital forensics tools are used within different stages of a digital forensics process. The digital forensics process can be categorized into an extraction stage and a data analysis stage, requiring separate tools and expertise (Ayers, Brothers & Jansen, 2014). A crucial problem that has emerged within digital forensics, is the fact that a majority of the emphasis has historically been put on the technical aspect associated with the collection and extraction of forensic evidence from physical devices. The technology used for extracting data has, thus, far surpassed the technology for adequately analyzing evidence. The technological deficiencies of analytic tools, along with lacking education among users are the two most crucial aspects affecting the efficiency of digital forensic processes. The lack of analytical capability commonly fails to identify crucial evidence.

2. RELATED LITERATURE:

Raghavan [2013] outlined some major challenge areas for digital forensics, gathered from a survey of research in the area: The table below presents the review of studies conducted.

Title of Paper	Author(s)	Purpose of study	Findings	Gaps
Emerging Cloud Computing or Cloud Forensic Challenges Emerging Cloud Computing or Cloud Forensic Challenges	Chen [2015] Almulla., [2013].	The usage of cloud services such as Amazon Cloud Drive, Office 365, Google Drive, and Dropbox is now commonplace amongst the majority of Internet users. From a digital forensics point of view, these services present several unique challenges, as has been reported in the 2014 National Institute of Standards and Technology's draft report	From a digital forensics point of view, these services present several unique challenges, as has been reported in the 2014 National Institute of Standards and Technology draft report Typically, data in the cloud is distributed over several distinct nodes, unlike more traditional forensic scenarios where data is stored on a single machine.	Cloud forensics also faces several challenges associated with traditional digital forensic investigations. Encryption and other anti-forensic techniques are commonly used in cloud-based crimes. an issue with cloud-based systems.
Internet of Things	Juniper [2015]	To outline some security concerns of IoT researchers, which feed directly into the desires of forensic investigators, incorporating issues such as availability, authenticity, and non-repudiation, which are important for legally-sound use of the data.	.IoT devices themselves typically have limited memory (and may have no persistent data storage). Thus any data that is stored for longer periods may be stored in some in-network hub, or sent to the cloud for more persistent storage.	The IoT has the potential to become a rich source of evidence from the physical world, and as such it poses its own unique set of challenges for digital forensic investigators Compared to traditional digital forensics, there is less certainty about where data originated from, and where it is stored.

Title of Paper	Author(s)	Purpose of study	Findings	Gaps
Lack of expertise	Vincze, [2016].	To make appropriate decisions regarding what the forensic examiners and investigators need to be able to do their jobs.	The rapid changes in forensic tools, techniques, and standards also require ongoing education and training, which can be difficult to manage in this already hectic field of work. Therefore, the lack of adequately trained personnel has led to fierce competition between governmental agencies and private companies over the most competent applicants	supervisors and higher management at law enforcement agencies generally lack the experts
The automation dilemma	Vincze, [2016]	For evidence to be considered reliable and valid in the court of law, the forensic investigator is required to understand and be able to clarify the process of how the evidence was forensically collected, which makes it almost as important as identifying the evidence in the first place	The concern is that automation will result in investigators beginning to lose understanding of the underlying concepts of the investigations by blindly relying on the results that the tools produce.	The digital forensics market has been skeptical of adopting tools for automating the investigation process.

3. IMPLICATIONS FOR RESEARCH, PRACTICE, POLICIES, AND ONLINE SAFETY IN AFRICA

This strategy puts forward practices for transformational change to Digital Forensics science across several areas in Africa:

Improved operations: Standardizing, industrializing, and providing services centrally - 'doing it once for the benefit of many' are the foundations to transform Digital Forensics science service. Standardizing processes will allow forces to collaborate on casework, technology, R&D, and quality assuring processes This will underpin everything we do in the future, including automation. To develop the operating model, TF and FCN, in tandem with forces and partners, will build on the three-tier approach Digital Forensics Portfolio Board (DFPB) outlines which many forces have already adopted. This tiered model will be delivered nationally and provide national, regional, and local elements.

Improved commercial practices: Bringing how policing engages with the commercial sector onto a sure and strategic footing is key to transforming DF science service. Coordinating this engagement nationally and agreeing on joint requirements, will enable policing to leverage its collective buying power and act as an 'intelligent customer'. This will allow us greater influence to ensure the market develops the capabilities we will need and ensure the supplier market is sustainable and resilient.

Developing the workforce: To transform Digital Forensics Science, we must invest in our people. We need to recruit and retain a skilled workforce who are motivated, fully trained, well managed, and equipped with access to the right tools and processes to deliver a world-class Digital Forensics service to the criminal justice system. Building trust: Legislation and ethics. The right legislation and ethical frameworks are critical to building and maintaining public trust and confidence in Digital Forensics science in policing. We will support the Government to ensure that legislation is fit for purpose in a digital age and addresses future technological advances.

4. CONCLUSION

In this theory, several current challenges in the field of digital forensics are discussed. Each of these challenges in isolation can hamper the discovery of pertinent information for digital investigators and detectives involved in a multitude of different cases requiring digital forensic analysis. Combined, the negative effect of these challenges can be greatly amplified. These issues alongside limited expertise and huge workloads have resulted in the digital evidence backlog increasing to the order of years for many law enforcement agencies worldwide. The predicted ballooning of case volume shortly will serve to further compound the backlog problem – particularly as the volume of evidence from non-traditional sources, such as cloud-based and Internet-of-Things sources, is also likely to increase.

Also investing resources into purchasing modern and effective tools to address the workload is an effective solution. However, this is impeded in practice by lacking knowledge and expertise among the investigators that law enforcement uses to assess the evidence. Buying a powerful tool is only viable if the person using the tool is skilled enough to utilize its full potential. Since the users lack the competence to effectively use the tools, law enforcement has a hard time motivating these purchases.

REFERENCES

1. Rogers, M. (2016). Psychological profiling as an investigative tool for digital forensics, in Digital Forensics: Threatscape and Best Practices. Amsterdam, The Netherlands: Elsevier, 2016
2. Lori Cameron is a Senior Writer for the IEEE Computer Society and currently writes regular features for *Computer* magazine, *Computing Edge*, and the Computing Now and Magazine Roundup websites
3. Nicole Beebe. Digital Forensic Research: The Good, the Bad and the Unaddressed. In Advances in Digital Forensics V, pages 17–36. Springer, 2009.
4. David Lillis, Bret A Becker, Tadhg O'Sullivan, Mark Scanion [MAY,2016]