THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 12 | Number 4 Article 5

12-2017

Digital Forensic Readiness in Organizations: Issues and Challenges

Nickson menza Karie 275404
Daystar University, menza06@hotmail.com

Simon Maina Karume Dr.
Laikipia University, skarume@gmail.com

Recommended Citation

Karie, Nickson menza 275404 and Karume, Simon Maina Dr. (2017) "Digital Forensic Readiness in Organizations: Issues and Challenges," *Journal of Digital Forensics, Security and Law*: Vol. 12 : No. 4 , Article 5.
DOI: https://doi.org/10.15394/jdfsl.2017.1436
Available at: https://commons.erau.edu/jdfsl/vol12/iss4/5

Digital Forensic Readiness in Organizations: Issues and Challenges

Cover Page Footnote

n/a

DIGITAL FORENSIC READINESS IN ORGANIZATIONS: ISSUES AND CHALLENGES

Nickson M. Karie[1, 2] and Simon M. Karume[3]
[1]Department of Computer Science, University of Swaziland, Swaziland
[2]Department of Computer Science, Kabarak University, Kenya
[3]Department of Computing and Informatics, Laikipia University, Kenya
Email: menza06@hotmail.com[1,2], skarume@gmail.com[3]

ABSTRACT

With the evolution in digital technologies, organizations have been forced to change the way they plan, develop, and enact their information technology strategies. This is because modern digital technologies do not only present new opportunities to business organizations, but also a different set of issues and challenges that need to be resolved. With the rising threats of cybercrimes, for example, which have been accelerated by the emergence of new digital technologies, many organizations, as well as law enforcement agencies globally, are now erecting proactive measures as a way to increase their ability to respond to security incidents as well as create a digital forensic-ready environment. It is for this reason that this paper presents the different issues and challenges surrounding the implementation of digital forensic readiness in organizations. The main areas of concentration will be: the different proactive measures that organizations can embrace as a way to increase the ability to respond to security incidents and create a digital forensic-ready environment. However, the paper will also look into the issues and challenges pertaining to data retention and disposition in organizations which may also have some effects on the implementation of digital forensic readiness. This is backed up by the fact that although the need for digital forensics and digital evidence in organizations has been explored, as has been the need for digital forensic readiness within organizations, decision-makers still need to understand what is needed within their organizations to ensure effective implementation of digital forensic readiness.

Keywords: Digital forensic readiness, organizations, issues and challenges, investigations, proactive measures, data retention and disposition

1. INTRODUCTION

Knowing that most organizations critically depend on data or information to help them in almost every activity they undertake on a daily basis, interfering with any of such organizational data or information can cause serious harm as well as threaten the organization's health. For this reason, preventing cybercrimes as well as securing organizational data or information has globally become inevitable. This is backed up by the fact that in the modern business environment, for example, cybercrime techniques targeting organizational data or information have become more sophisticated and better coordinated through all kinds of digital technologies.

In this regard, note that cybercrimes are criminal offenses committed via the Internet or otherwise aided by various forms of computer technology, such as the use of online social networks to threaten others or cause harm (Findlaw, 2016). More criminals today are exploiting the speed, convenience, and anonymity of the Internet technologies to commit a myriad of criminal activities that know no borders, either physical or virtual, causing serious harm and present real threats to victims throughout the world. Organizations, therefore, need to understand cybercrimes as well as the different proactive measures that can be undertaken in order to increase their ability to respond to security incidents and create a secure business environment.

The aim of this paper, therefore, is to present the different proactive measures that organizations need to undertake in order to increase their ability to respond to security incidents, as well as create a digital forensic-ready environment. This also implies that there is a definite need to consider current best practices to include, for example, certain aspects of digital forensic readiness to address the challenges brought about by cybercrimes in organizations. However, this paper will also highlight issues and challenges brought about by data retention and disposition policies in organizations which may also affect the process of implementing digital forensic readiness.

As for the remaining part, the paper is structured in the following format: Section 1 has set the scene of the paper through an introduction; Section 2 will introduce the literature review as background while Section 3 will provide related work. Thereafter, Section 4 will discuss the issues and challenges of digital forensic readiness in organizations followed by data retention and disposition in organizations in Section 5. The paper then concludes with Section 6 and makes mention of the future work.

2. LITERATURE REVIEW

This section provides literature background on the following areas: digital forensics, digital forensic readiness, and finally, data retention and disposition. Digital forensics has been discussed to show the scientific process of the digital investigation while digital forensic readiness is discussed as a way organizations can record activities and data in such a manner that the records are sufficient in their extent for subsequent forensic purposes. Finally, data retention and disposition are discussed to show for how long certain data or information captured as Potential Digital Evidence (PDE) should be retained in an organisation and how it should be disposed when no longer needed or when no lawsuit is filed or is reasonably anticipated.

2.1 Digital Forensics

According to Resendez et al., (2012) Digital Forensics (DF) combines elements of law and computer science to collect and analyse data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law. Being related to law and technology means that DF investigators are expected to do more than just following the known traditional digital forensic investigation techniques (Khatir, M., Hejazi, S.M., Sneiders, E., 2008). This is because the different types of cybercrimes, distribution of networks, and complexity of information and communication technology add to the complexity of the digital investigation process (Khatir, M., Hejazi, S.M., Sneiders, E., 2008). The legal processes are also different for different jurisdictions. For this reason, organizations need to adopt rigorous and flexible processes to counter the different challenges facing DF.

Karie and Kebande (2016) add that DF involves proper forensic examination of digital evidence by forensic analysts through the Law

Enforcement Agencies (LEAs); however, the forensic examination of digital evidence is also true for the defense attorneys as well as for any other legal issues pertaining to a business organization. The main objective of digital forensics is thus to unearth digital evidence that will assist the defense attorneys, LEAs and prosecutorial offices through the presentation of digital evidence in a court of law or any civil proceedings.

As the technological trends in DF keep changing, new challenges are also constantly mushrooming in the domain which needs to be resolved. This scenario, therefore, calls for new approaches to be developed in the digital forensic domain with the ability to effectively assist organizations and investigators in dealing with new challenges that may crop up as a result of technological change or domain evolution. Such approaches should further assist in establishing an effective Digital Forensic Readiness (DFR) process in the organizations. The next subsection introduces the concept of digital forensic readiness in organizations.

2.2 Digital Forensic Readiness (DFR) in Organizations

Forensic readiness as defined by Mohay (2005) as the extent to which computer systems or computer networks record activities and data in such a manner that the records are sufficient in their extent for subsequent forensic purposes, and the records are acceptable in terms of their perceived authenticity as evidence in subsequent forensic investigations.

While digital forensics readiness is still rare in many organizations according to André (2014), the dependence on information technology and its pervasiveness in business have created the need for building DFR capabilities in organizations (Sommer, 2012).

Antonio and Labuschagne (2013) also add that research has shown that a carefully considered and planned legally contextualized digital forensic readiness strategy can provide organizations with an increased ability to respond to security incidents, while maintaining the integrity of the evidence gathered and keeping investigative costs low. However, according to Sommer (2012), organizational needs for digital forensic capabilities also differ; thus, each organization should consider a practical readiness level that caters for their needs.

Being digitally forensic-ready as stated by André (2014) can help organizations with quicker recovery, improved business continuity, and compliance, as well as an improved success rate in legal actions by having available the collected digital evidence. Besides, it also provides a tool to fight insider threats, deters employees from non-compliance with organization rules and evidence in the case of employee disciplinary hearings. Therefore, DFR should be an essential part of any security processes within organizations. However, once digital data is captured, the concept of data retention and disposition comes in to play and is explained next.

2.3 Data Retention and Disposition in Organizations

For as long as organizations would want to implement DFR effectively, one challenge that will always be there is that the data or information captured using the DFR process is usually subject to data retention and disposition policies. Most organizations have data retention and disposition policies that provide for a systematic review, retention and disposition of data or information captured, created, or maintained within the organization. Such policies contain a schedule for how long certain data or information should be retained and how it should be disposed of, unless such data or information is under a legal or other similar

investigation or is otherwise subject to a litigation hold.

Generally, the retention and disposition policies detail the procedures for the retention and disposal of data or information to ensure consistency, accuracy and that every action is fully recorded and document. Unless otherwise specified, the retention and disposal policy in many organizations combines both hard and soft copy data, or even other information captured. Any data or information disposed of either earlier or kept for longer than listed in the policy document will need to be recorded for audit purposes. This further makes the retention and disposition of data or information captured through the DFR process a challenge to organizations. Section 5 details some of the issues and challenges associated with data retention and disposition in organizations. The next section presents related work for this study.

3. STATE OF THE ART: RELATED WORKS

There exist several related works from different researchers which have made valuable contributions towards the study presented in this paper. In this section, a summary of some of the most prominent efforts in previous research work is provided.

To begin with, Barske, Stander and Jordaan (2010) presented a DFR framework for South African Small and Medium Enterprises (SME's). However, their paper did not address the main issues and challenges of DFR facing organizations but rather concentrated on DFR concepts and how they apply to SME's. In addition, the paper did not talk about data retention and disposition in organizations. On the contrary, this paper examines some of the issues and challenges surrounding DFR as well as data retention and disposition in organizations.

In another effort by Antonio and Labuschagne (2012), the authors argue that the growing threats of fraud and security incidents present many challenges to law enforcement and organizations globally. This has given rise to the need for organizations to build effective incident management strategies, to enhance their reactive capability to security incidents. They then propose in their paper, proactive activities that an organization can undertake in order to increase its ability to respond to security incidents and create a digitally forensic-ready environment. Antonio and Labuschagne (2012) study also did not address any issues and challenges with regards to implementing DFR as well as data retention and disposition policies in organizations.

More research by Antonis, Marthie, and Chang-Tsun (2011) proposed steps that can be used to guide the formulation of a forensic readiness policy in organizations. Ngobeni, Venter, and Burke (2010) in their paper also proposed a wireless forensic readiness model designed to help monitor, log and preserve wireless network traffic for digital forensic investigations. Their research is complemented by Aadil, Sameh and Tahar (2015) who presented the building blocks for a model for automated network readiness and awareness.

Several other related works exist on issues and challenges surrounding digital forensic readiness, however, neither those nor the cited references in this paper have presented DFR issues and challenges facing organizations in the way that is discussed in this paper. However, the authors acknowledge the fact that the previous research works have offered valuable insights toward the study in this paper. The next section presents a detailed discussion of the digital forensic readiness issues and challenges.

4. DIGITAL FORENSIC READINESS ISSUES AND CHALLENGES

As noted by Issam (2016), there is a growing need for establishing DFR in organisations today. However, Cobb (2013) states that DFR sounds like a daunting challenge to most the organizations. This is because according to Reilly et al. (2011), many areas, for example, the emergence of cloud computing has not been thoroughly considered in terms of its forensic readiness, hence posing a challenge to many organizations.

In this section of the paper, therefore, a discussion of some of the issues and challenges surrounding DFR in organizations is presented. However, the authors acknowledge that the issues and challenges explained in this section were only selected as examples to facilitate this study and do not by any means constitute an exhaustive list. Therefore, more specific issues and challenges can and should be added as the need arises in future. The subsections to follow presents the common issues and challenges which are discussed in tandem with the proactive measures that can help increase the ability of an organization to respond to security incidents and create a digital forensic-ready environment.

4.1 Lack of a DFR Plan in Organizations

A DFR plan according to Benny (2014) is a policy document that sets out exactly what to do when digital evidence is required, either as part of the legal action, regulatory response, internal investigations or disciplinary procedures. The objective of a DFR plan is to maximize the amount of evidence data that is readily available and to minimise the time and costs needed to secure the required evidence. Organizations can use the DFR plan as a point of reference to identify the types of evidence data needed during incident investigations.

Developing a DFR plan as a proactive measure can, therefore, help organizations prevent going down expensive ways during incident investigations. This further helps increase the ability to respond to security incidents and create a digital forensic-ready environment in the organization. The lack of a plan in any organization can severely limit investigations into any security incident. For this reason, organizations should have a DFR plan as a way to ensure that evidence generators are in place to capture unwanted activities and that the evidence captured is also correctly preserved to assist in any investigation, and finally that it can robustly support future legal remedies.

4.2 Lack of Forensic Readiness Policy

A Forensics Readiness Policy (FRP) is a document that details the immediate procedures to be employed for any forensic investigation of digital evidence. The objectives of an FRP is to provide a systematic, standardised and legal basis for the admissibility of digital evidence that may be required from a formal dispute or legal process. The policy may include evidence in the form of log files, emails, backup data, mobile computing, network, removable media and others that may be collected in advance of an event or dispute occurring (Unknown, 2016). According to Griffin (2014) an FRP should be formulated to confirm an organization's commitment:

1. To gather admissible evidence legally and without interfering with business processes
2. To gather evidence targeting the potential crimes and disputes that may adversely impact the organization
3. To allow an investigation to proceed at a cost in proportion to the incident

4. To minimise interruption to the business from any investigation
5. To ensure that evidence makes a positive impact on the outcome of any legal action, in order to continue core business functions of all business stakeholders in the event of a major incident.

Having an FRP is thus another proactive measure that can help organizations respond to security incidents and create a digital forensic-ready environment before the onset of any investigation process.

4.3 The Legal System and Law Enforcement Challenge

Legal systems and law enforcement challenges as noted by Karie and Venter (2015) deals with jurisdiction; prosecuting digital crimes; admissibility of digital forensic tools and techniques; insufficient support for legal criminal or civil prosecution; ethical issues; and privacy of individuals in organizations. However, according to John (2016), one single most important tool when dealing with internal employees is the 'Acceptable Use' policy document, which should be part of an employee's employment contract. The 'Acceptable Use' policy document should indicate what an employee is allowed to use their work IT infrastructure for; what data may be accessed and other rules that apply during working hours. This document should also put into consideration users' rights to privacy. While organization policies are important, measures should be put in place to protect users' privacy.

Furthermore, the collection of evidence and presentation of the same evidence data may be held to different standards in court. The process of evidence data collection and imaging, for example, can be quite different and the consequences of the case may have very different impacts. For this reason, when implementing DFR in any organization, the consideration of the legal systems and law enforcement as well as user privacy is essential as any violations might make it difficult to produce legally admissible digital evidence. One good example is the requirement to maintain records for at least 180 days upon notification of an investigation (EEOC, 2017). In other jurisdiction, however, agencies are required to complete investigations within or even earlier than 180 days after the filing of the last complaint or 360 days after the filing of the original complaint (EEOC, 2017). The infrastructure to investigate digital crimes should also be based on the prevailing cyber laws; hence any violations can make it difficult for practitioners to prepare court admissible reports.

4.4 Lack of Knowledgeable and Skilled Personnel

According to Desai et al. (2009), digital forensics has become an important field due to the increase in digital crimes. This makes DFR also an important component of any organization today. However, there is a shortage of knowledgeable and skilled digital forensic personnel in this field. Qualified digital forensic experts are a challenge to find, even in the private sector, hence posing a challenge to DFR implementation in organizations. Staff training and compliance with a forensic readiness plan, however, can be a good proactive measure for organizations as it will ensure that all staff members in the organization are aware of the correct procedures to follow during a digital investigation process.

4.5 DFR Cost Implications

Implementing DFR in an organization may require technological as well as financial support. According to CESG (2015), for organizations that only need to deal with digital forensics provision as a contingency there should be no need for direct investment of in-house

technology capability, however, it can be prudent to develop some internal capability when it is found that there are frequent incidents of which the detection or investigation are assisted by digital forensic technology. The in-house capability may not just be used to support an evidence gathering function, but also a good proactive measure as a way to undertake an intelligence function or root cause analysis. There will be direct costs with the need to acquire and maintain any in-house capability. Requirements may range from a single laptop to a laboratory facility. Costs will also be incurred in the essential training of staff and maintenance of their competence (CESG, 2015).

For this reason, organizations often worry of the cost implication when considering DFR (Grobler and Louwrens, 2007). This makes it hard sometimes to convince the organization management of the benefits of DFR.

4.6 Lack of Organization Guidance in Implementing DFR Standards

As discussed by Valjarevic and Venter (2013) DFR enables an organization to prepare itself in order to perform an investigation in a more efficient and effective manner. However, the problem that still remains is that there is no standardised DFR process model with appropriate implementation procedures and guidelines to help organizations achieve admissibility of digital forensic evidence in any court of law or civil proceedings. This also implies that there is a lack of an effective and standardised implementation of DFR measures within organizations.

As a way to help organizations in implementing DFR, standardised procedures and guidelines need to be created as proactive measures so as to help organizations create a more efficient and effective digital forensic investigation process. The next section handles data retention and disposition issues and challenges in organizations.

5. DATA RETENTION AND DISPOSITION ISSUES AND CHALLENGES

The primary objective of any data retention and disposition policy is to ensure that all necessary data or information captured including records and documents are adequately protected, retained, and disposed when required to ensure proper accountability. However, such a policy is subject to meeting the laws of a particular jurisdiction as well as safeguards the history and reputation of an organization. The policy is also meant to protect the organization during litigation or audit, minimize the cost of data or information retention, and optimize the use of space.

This section explains some of the data retention and disposition issues and challenges and how they can affect the implementation of an effective digital forensic process in organisations.

5.1 Compliance with Regulatory or Legal Requirements

For any organization, compliance with regulatory or legal requirements is an organization's adherence to laws, regulations, guidelines, and specifications relevant to its business. Any violations of regulatory compliance regulations often result in legal punishment, including fines. For this reason, any data captured as a result of DFR must also be in line with the legal requirements of a particular jurisdiction. Generally, compliance means conforming to a rule, such as a specification, policy, standard or law (Lin and Tom, 2017).

Because of the increasing number of regulations and need for operational

transparency, organizations these days are increasingly adopting the use of consolidated and harmonized sets of compliance controls (Silveira et al., 2012). This approach is used to ensure that all necessary governance requirements including that of data retention and disposition can be met without the unnecessary duplication of effort and activity from resources. If compliance with regulatory or legal requirements is not followed in any organization, it can in the end affect the digital forensic readiness process.

5.2 Litigation Hold Requirements

In the legal world, a litigation hold is a written directive advising custodians of certain documents and electronically-stored information to preserve potentially relevant digital evidence in anticipation of future litigation (Stephanie, 2010). This is sometimes a challenge when you don't get the right custodians, more especially, when such custodians aren't complying. As a result, it also becomes a challenge in implementing an effective DFR process.

5.3 Releasing or Disposing of Court-ordered Data

It is possible that at times an organization can receive an injunction. In such a case, a court issues an order prohibiting a person from taking a particular action or requiring them to take a particular action. When this happens, it becomes hard for an organization to release or dispose data related to digital forensic readiness hence posing a challenge to effective utilization of DFR data captured.

5.4 Retention and Disposal Schedule Challenge

In many organizations, a retention and disposal schedule defines how long different types of data or information need to be kept, and when they should be disposed of. There is a possibility that data may be disposed of early deliberately or sometimes accidental. When this happens then DFR suffers the lack of any digital evidence to support an investigation. However, this is also influenced by existing laws and regulations in a particular jurisdiction.

5.5 Data Storage and Disposition Cost

Storing data for a long time can cost an organization millions of dollars. It is possible that a big percentage of the data captured using some of the DFR technologies in organizations isn't necessarily required for legal or regulatory purposes. This, therefore, creates unnecessary storage cost. The question of what to store or what to dispose of is always a big challenge to many organizations and the effect can be felt when implementing DFR.

5.6 Disasters and Emergencies Challenge

Dealing with disasters and emergencies in an organization simply means planning a coordinated or co-operative process of preparing for urgent needs with available resources. Disasters and emergencies can lead to destruction of property and information in an organization. The biggest challenge is in preparing responders to respond as fast as possible when disasters and emergencies strike. Many organizations lose data and information because of the lack of the much-needed preparedness to face disasters and emergencies.

5.7 Dealing with Organizational Disciplinary Issues

Employee discipline is always relevant to any organization. This is because discipline promotes a minimum acceptable behavior by employees. Indiscipline and misconduct of employees can affect many activities in an organization, including all stakeholders. With the advancement in technology, undisciplined employees may remotely disable any DFR

technologies in the organization. This, in turn, affects the effective implementation of DFR in organizations. The next section concludes this paper and highlights the future work.

6. CONCLUSION

In this paper, the authors have presented and explained the different issues and challenges surrounding digital forensic readiness, as well as data retention and disposition in organizations. This was done in tandem with the proactive measures that organizations can undertake in order to increase their ability to respond to security incidents and create a digital forensic-ready environment. The presentation in this paper can be of great value to digital forensic practitioners, law enforcement agencies, as well as organizations globally. The organizations and practitioners, for example, can use the information in this paper in the development of dynamic proactive measures to deal with cybercrimes as well as DFR. However, there is still much research to be done, besides the identified issues and challenges surrounding DFR in this paper, so as to provide directions on how to address the data retention and disposition issues and challenges related DFR in organizations. Future research will involve coming up with a model that can help in practical implementation and evaluation of some of the solutions suggested in this study.

REFERENCES

Aadil, A., Sameh, A. and Tahar, K., (2015). Cyberspace Forensics Readiness and Security Awareness Model. International Journal of Advanced Computer Science and Applications, (IJACSA)Vol. 6, No. 6. pp.123-127

André, H., (2014). Are you ready? Forensically speaking - On digital forensic readiness. Available at: http://leidensafetyandsecurityblog.nl/articles/are-you-ready-forensically-speaking-on-digital-forensic-readiness [Accessed May 07, 2016].

Antonio P., and Labuschagne, L., (2012). A conceptual model for digital forensic readiness. Proceedings of the ISSA Conference; 2012Aug. 15-17, Johannesburg, SA. IEEE Publishers, 2012; pp.1–8

Antonio P., and Labuschagne, L., (2013). Readiness Planning. Proceedings of the 9th Annual IFIP WG 11.9 International Conference on Digital Forensics. pp.53-66

Antonis, M., Marthie, G., and Chang-Tsun, L., (2011). Digital Forensic Readiness: An Insight into Governmental and Academic Initiatives. IEEE Publishers, 2012; pp.1-8

Barske, D., Stander, A., & Jordaan, J. (2010). A Digital Forensic Readiness Framework for South African SME's. Proceedings of the ISSA Conference; 2010 Aug. 2–4; Sandton, Johannesburg, SA. Piscataway, NJ: IEEE Computer Society Publishers, 2010;1–6

Benny, L., (2014). Forensic Readiness Plans. Available at: http://www2.deloitte.com/au/en/pages/risk/articles/forensic-readiness-plans.html [Accessed May 07, 2016].

CESG, (2015). Good Practice Guide Forensic Readiness. Issue No: 1.2. Available at: https://www.cesg.gov.uk/content/files/guidance_files/Forensic%20Readiness%20(Good%20Practice%20Guide%2018)_1.2.pdf [Accessed May 07, 2016].

Cobb, M., (2013), "Digital forensic investigation procedure: Form a computer forensics policy", Available at http://www.computerweekly.com/tip/Digital-forensic-investigation-procedure-Form-a-computer-forensics-policy [Accessed February 18, 2013].

Desai, A.M, Fitzgerald, D., Hoanca, B., (2009). Offering a digital forensics course in Anchorage, Alaska. Inform Syst Edu J 2009;7(35); http://isedj.org/7/35/.

EEOC (2017), Development of Impartial and Appropriate Factual Records. Available at: https://www.eeoc.gov/federal/directives/md-110_chapter_6.cfm [Accessed August 16, 2017].

Findlaw (2016). Cyber Crimes. Available at: http://criminal.findlaw.com/criminal-charges/cyber-crimes.html [Accessed June 6, 2016].

Griffin, F., (2014). Forensic Readiness Planning- Available at http://www.griffinforensics.com/forensicreadinessplanning.html#sthash.q3ylEAZf.dpuf [Accessed May 07, 2016].

Grobler, T., and Louwrens, B., (2007). Digital Forensic Readiness as a Component of Information Security Best Practice. In IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy, and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J.,von Solms, R., (Boston: Springer), pp. 13-24.

Issam, Z., (2016). Building Digital Forensics Readiness in the Corporate World. Available at:

http://www.internalauditor.me/article/building-digital-forensics-readiness-in-the-corporate-world/ [Accessed May 6, 2016].

John, D., (2016). Forensic Readiness Planning. Available at: http://first-response.co.uk/blog/forensic-readiness-planning/ [Accessed May 07, 2016].

Karie, N.M & Kebande, V.R., (2016). Building Ontologies for Digital Forensic Terminologies. International Journal of Cyber-Security and Digital Forensics (IJCSDF) 5(2): pp75-82

Karie, N.M. and Venter H.S., (2015). Taxonomy of Challenges for Digital Forensics. Journal of Forensic Sciences. Vol. 60, No. 4. pp.885–893

Khatir, M., Hejazi, S.M., Sneiders, E., (2008). "Two-Dimensional Evidence Reliability Amplification Process Model for Digital Forensics". Digital Forensics and Incident Analysis, 2008. WDFIA '08. Third International Annual Workshop on Digital Forensics and Incident Analysis. pp.21-29.

Lin, Tom C. W.(2017), Compliance, Technology, and Modern Finance (2016). 11 Brook. J. Corp. Fin. & Com. L. 159 (2016); Temple University Legal Studies Research Paper No. 2017-06. Available at SSRN: https://ssrn.com/abstract=2904664

Mohay, G., (2005), "Technical Challenges and Directions for Digital Forensics", Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 155-161

Ngobeni, S., Venter, H., and Burke, I., (2010). A Forensic Readiness Model for Wireless Networks. Advances in Digital Forensics VI. Pp: 107-117

Reilly, D., Wren, C., Berry, T., (2011). Cloud computing: pros and cons for computer forensic investigations. Int J Multimedia Image Process 2011;1(1):26–34.

Resendez, I., Martinez, P., and Abraham, J., (2012), An introduction to digital forensics. [Online] Available at: http://acetweb.org/journal/ACETJournal_Vol6/An%20Introduction%20to%20Digital%20Forensics.pdf [Accessed May 02, 2016].

Silveira, P., Rodriguez, C., Birukou, A., Casati, F., Daniel, F., D'Andrea, V., Worledge & C., Zouhair, T. (2012), Aiding Compliance Governance in Service-Based Business Processes, IGI Global, pp. 524–548

Sommer, P. (2012). Digital Evidence, Digital Investigation, and E-Disclosure: A Guide to Forensic Readiness, The Information Assurance Advisory Council (IAAC).

Stephanie F.S., (2010) Litigation Holds: Ten Tips in Ten Minutes. aVAILABLE AT: http://www.ned.uscourts.gov/InternetDocs/cle/2010-07/LitigationHoldTopTen.pdf [Accessed August 07, 2017].

Unknown (2016). ICT Forensic Readiness Policy Available at: www.meht.nhs.uk/EasysiteWeb/getresource.axd?AssetID=1892 [Accessed May 6, 2016].

Valjarevic, A. and Venter, H. S., (2013). Implementation guidelines for a harmonised digital forensic investigation readiness process model. Proceedings of Information Security South Africa 2013 Conference, Johannesburg. Pp.1-9.

