JISTEM - Journal of Information Systems and Technology Management
Revista de Gestão da Tecnologia e Sistemas de Informação
Vol. 12, No. 2, May/Aug., 2015 pp. *233-244*
ISSN online: 1807-1775
DOI: 10.4301/S1807-17752015000200003

DIGITAL FORENSIC INVESTIGATION MODELS: AN EVOLUTION STUDY

Khuram Mushtaque
Kamran Ahsan
Federal Urdu University of Arts, Science and Technology, Karachi, Paquistão'
Ahmer Umer
Mohammad Ali Jinnah University, Karachi, Paquistão

ABSTRACT

With increased use of technology in organizations and rapid changes in technology cyber forensic process is also advancing into new ways. In this context, organizations also need to align their technological infrastructure to meet the challenges in conducting successful process of forensic investigations to attain maximum and desired benefits of it. The objective of this article is to perceive the status of different I.T comprising organizations in terms of cyber crime and forensic investigation process and we take Pakistan as a case here. For this purpose, a questionnaire was designed to survey different organizations to find out that how effectively they have secured their technology infrastructure and how supportive this setup could be for any forensic firm to perform the forensic investigation in case of occurrence of any cyber crime. In the critical analysis, the main finding reckoned as flaw found in these organizations was that they don't pay much importance to forensic investigation and because of this they don't incorporate forensic supportive tools such as employees' awareness training programs, clauses in hiring documents and acquiring the services of forensic firms as per requirement. This ignorance may lead organizations towards different types of losses in case of occurrence of cyber crime and if this situation is not addressed, forensic investigation process also could not be as accurate and successful as it has to be.

Keywords: Cyber Forensic; Organizations; Forensic Models; Cyber Crime; Forensic Firms

Manuscript first received/*Recebido em:* 13/11/2013 Manuscript accepted/*Aprovado em*: 10/04/2015

Address for correspondence / Endereço para correspondência

Khuram Mushtaque, Federal Urdu University of Arts, Science and Technology, University Rd, Karachi, Karachi, Paquistão E-mail Khuram.mushtaque@gmail.com

Kamran Ahsan, Federal Urdu University of Arts, Science and Technology, University Rd, Karachi, Karachi, Paquistão E-mail kamran.ahsan@fuuast.edu.pk,

Ahmer Umer, Mohammad Ali Jinnah University, Karachi, University Rd, Karachi, Paquistão E-mail ahmerumer@gmail.com

1. INTRODUCTION

In current era, majority of large enterprises rely heavily over the usage of technology in operations and other segments of the business. With the increased reliance and usage of technology, the risk of cyber crime becomes also more serious in case of occurrence. To counter this risk, digital forensic investigation firms provide assistance in conducting the forensic analysis after occurrence of any cyber crime. With the passage of time, the forensic investigation process has also modified and distributed into different phases to make this investigation more effective. Every phase has its own impact over the process of investigation.

(Sivaprasad & JangaJe, 2012): With the introduction of Information Technology in the business, every organization that comprises IT has started to take benefits of this technology. This is done by attaining the advantage over other competitors in the market, by providing new features to the customers after incorporating technology at the operational side specially, increasing the operational speed and reducing the probability for any error in operations. (Wen, 2012): IT also assists higher management in the process of decision making.

(Morozini, Claudio, Ivam. & Reinaldo. 2012): As we all know that room for improvement and step towards the perfection is always available in every field of the world, similarly there are very few loop holes in the information technology becoming key part of the business industry of today. Besides the entire physical infrastructure like machinery, human resource, buildings etc associate with the organization, information has also come up as the one of the most important asset of any organization comprising information technology in their business not to just support the IT operations but also provide the platform to connect with other business associated partners as well.

(Sladić, Milosavljević & Konjović, 2012): As the information technology relies heavily and works around the information, therefore it becomes tremendously important to protect the information by ensuring that no any unauthorized person can get the access and the integrity and confidentiality remains sustained. (Belabed, Aimeur, & Chikh, 2012): Ensure the timely availability of the information for associated operations and secure these operations from the different threats such e.g. Phishing are vital tasks for the technical persons for their organization.

(Den & Warnier, 2013): While organizations investing towards launching, updating and securing the security of their technology associated infrastructure and operations, still, threat of cyber crimes remains alive and open which could not just exploit the Data breaches badly but also could cause ruining to their entire business or also might affect some or large extent. (Pérez 2013): The biggest threat of such type is the threat from the insiders and they keep seeking for the right opportunity to commit their cyber crime in order to achieve their illegitimate objectives. Therefore identification of threat becomes another crucial segment needs to be monitored and controlled.

(Onome, Thereza & Formigoni, 2013): In order to deal with such criminals, along with annual external audit, many organizations have started acquiring the services of digital forensic firms. These digital forensic firms comprise with forensic experts and technical persons to provide their clients or organizations complete solution to their cyber crime affected scenarios. As these firms have no stack or association with any insider of organizations, therefore the investigations provided them remain trust worthy.

(Ma, Sun & Wang, 2011): Different models are followed by every forensic firm depending on the target organization and the type or intensity of the loss by committed cyber crime. These models are based on different phases containing different sets of steps in order to gather the valuable and effective evidences against the culprit of that crime which carry out limitation of time and legal constraints in linear course control and forensic administration to the entire forensic process. (http://en.wikipedia.org/wiki/Digital_forensics): Forensic firms also ensure that the evidences generated by them follow all the legal requirements of pertaining organization and also law of country so that these evidences could become admissible in the court of law as well if required to present over there.

In current research, first we have described the different models of digital forensic investigations year by year and have explained all the phases of these models according to their sequence. This has exhibited the evolution of the digital forensic investigation around the world and its importance in the different types of business industry. The core objective of all the described models remains same.

Apart from responsibilities and models used by digital forensic firms, we have also highlighted numerous addressable elements in different types of organizations of Pakistan in the context of enabling and helping out the firms to gather effective evidences as required. These elements if addressed properly could open more and more options for forensic firms to find better platform in the process of evidence collection available maximum in the crime scene.

2. FORENSIC MODELS

(Ojo & Adebayo, 2011): Since the introduction of the discipline of Digital Forensic in the field of Information Technology especially in the corporate business industry, the persons associated with technology started their efforts in order to overcome the audit and research challenges associated with digital forensic of the organizations as much as possible. (Nnoli, Lindskog, Zavarsky, Aghili & Ruhl, 2012): It was due to their understanding towards the significance of this field in the governance of IT but also organizations started investing over it after identifying the intensity of effect it could leave over the business and the economy of organizations. Most enterprises are seen wasting their precious time, efforts and resources to implement digital forensic investigation because of their lacking in awareness towards corporate forensic.

(Horsman, Laing & Vickers. 2012): The process of digital forensic investigations, as recommended by experts, must be conducted by its specialist persons who have totally unbiased approach to ensure trustworthiness over them and image against the organizations where the investigation will be performed. The remains a question mark over the internal person as forensic investigation performer and the evidences produced by internal process might not become as influential as this need to be in order to establish any culprit in the court of Law.

Figure 1 exhibits the different models launched in different years with the objective to provide guidelines to the Digital forensic investigative firms. Every model is divided in different steps and these steps kept expending as the time progresses and with the increase and identification of importance of the process of digital forensic investigation.

3. RESEARCH METHODOLOGY

Research methodology used in this research is questionnaire based survey because by survey provides unbiased and different types of feedbacks. After gathering it useful analysis can be produced addressing particular topic of interest which could become significant for the future decision making in that specific field. For this research, a question based on 72 questions related to digital forensic was designed and distributed in 80 different types of large enterprises comprising I.T. The feedbacks provided us significant information about the status of the technological and other issues related to forensic investigation procedure in these organizations. This attained information was later on analyzed in different angels to perform the critical analysis and highlight the addressable elements in large enterprises in this regard.

Evolution of Digital Forensic Investigation Models

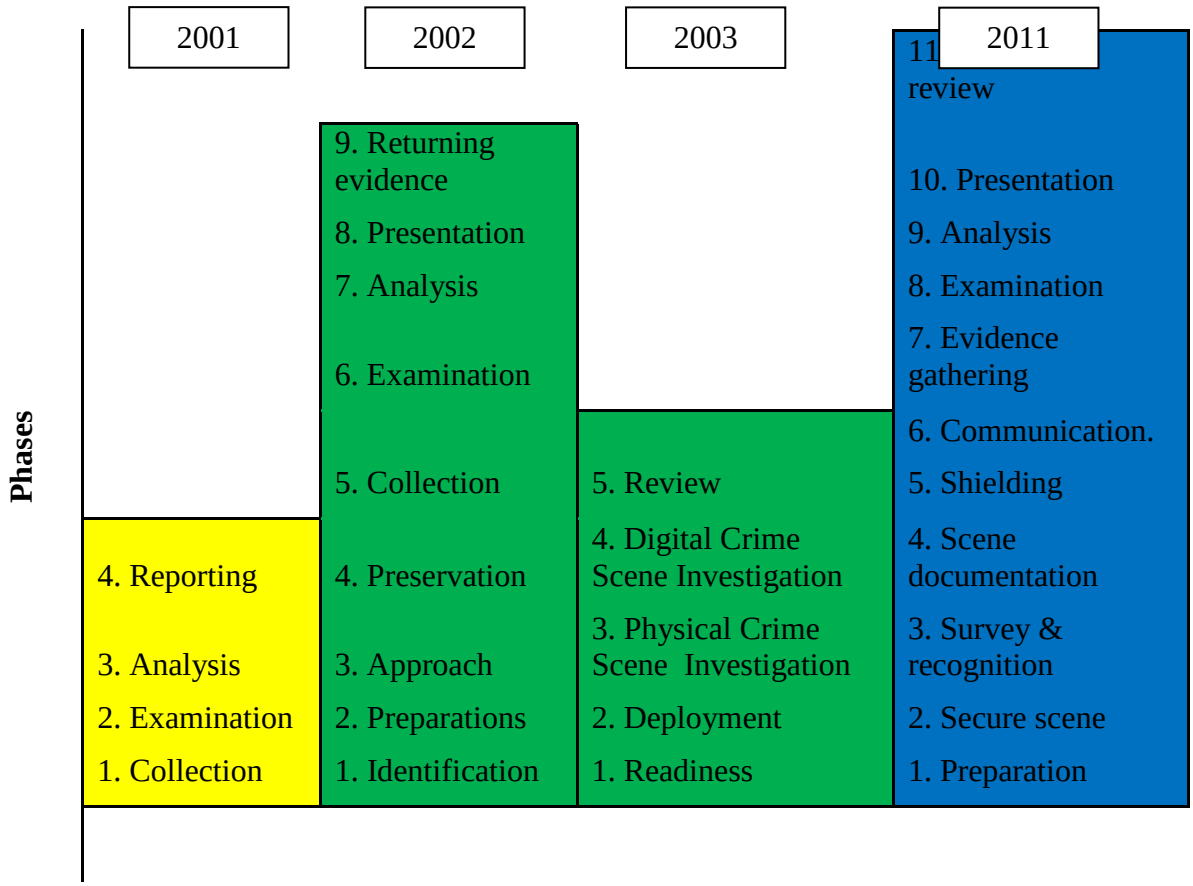

Figure 1: Forensic Models

(Valjarevic & S.Venter, 2012): The first digital forensic model was introduced in 2001. The instigator of this project was Ashcroft who was associated with the U.S National Institute of Justice. This model contained investigation process of crime scene associated with the electronic field and it become a guideline for the responders who were very novice to it. Later on, this model was also utilized by the law enforcement and other agencies to secure and identify the digital evidences.

The first (out of four) phase of this model is about the collection of the evidences after performing a thorough search process around the crime scene. Second phase contained the process of examination of which is to put together the evidences collected from previous phase as transparent and identify its source as well. Third phase is to perform the analysis of outcome of the phase of examination. After the analysis, last phase comprise reporting and drawing of outcomes of all previous phases and the information that was collected in entire process.

However, the only constraint of this model is that it remains unclear and is not explained properly.

Following the model of 2001, in 2002 Carr, Reith and Gunsch made an effort to further clarify the digital forensic investigation model by adding some more phases into this process. They incorporated the traditional approach of accumulating the evidences to simplify in this model.

First phase of this model is to identify the occurred incident and its type and provide all the assistance to achieve the goal of this phase. Second phase is to get prepared regarding the methods and the procedures which will be used in remaining phases of this forensic model. It also guides about the preparation of different search warrants if required in order to gather the evidences. Third phase is to devise appropriate approaches and processes which will be adopted in the fifth phase of evidence gathering.

Fourth phase of preservation is to preserve all the components and devices potentially containing the relevant evidences. After securing the evidence containing devices and components, fifth phase of collection is used to unify the procedures in order to record the physical scene. Sixth phase is to examine, which treats with the finding of the relevant suspect of the crime that was committed. Seventh phase is to analyze the importance of items on which the inspection has been performed.

Presentation of the all phases that are involved in this model is the phase which comes at later stage after the analysis phase while last and ninth phase contains the process of returning the devices and sources of digital evidences to the real owner after accomplishment of the task of forensic investigation.

The only flaw or room for improvement in this phase indentified is that the third phase is quite similar to the second phase to some degree.

Third model of digital forensic investigation was introduced by Spafford and Carrier in 2003. This model was named as Integrated Digital Investigation Process and became another guideline for the forensic examiners in order to perform digital forensic investigation and gather the evidences. This model was again resized into five phases.

The objective of first and initial phase named as readiness phase was to ensure that the actions and provided infrastructure are good enough to favor and assist the investigation process appropriately. Therefore this phase is used only to get ready for the remaining phases of investigation process. Second phase is of deployment, it supplies a system to the forensic examiners through which they could become capable to detect and incident and then certify it.

Third phase is about the gathering and examining the physical evidences from the crime scene and go through the keen observation of the acts that where associated during the incident was occurring. Fourth phase is sequel to third phase, but it deals with the examining and gathering of digital evidences which were obtained by the

physical crime scene investigation phase. The remaining process used in phase is similar to the third phase of this model. Fifth and final phase is to review the entire analysis that was performed during previous phases of digital forensic investigation process and then underline those areas where the room for improvement exists.

The reason behind this model not being used mostly and not known as the best model for digital forensic investigation is that deployment phase of this model deals with the certification of the occurred incident, on the other hand practically it is impossible to endorse the digital crime earlier than appropriate investigation.

(Khan, Kock & Memon, 2010): In 2004 a Ciardhuain proposed a model for digital forensic investigation which didn't have detailed phases and proper guidelines therefore it could not get familiar and in utilization as the previous models. (Ademu, Imafidon & Preston, 2011):Similarly in 2005 Ruibin Yun and in 2009 Perusal proposed their models for investigation and evidences collection but had same lacking of unclear and detailed explanation of their process and also they didn't categorized their models into separate phases. Therefore these models also couldn't get the identification and credit as they needed to be.

(Ankit Megha, Saurabh & Gupta. 2011): In 2011 Preston, Ademu and Imafidon proposed their model for investigation process which became the most recent guideline with utmost detailed description of phases and the distribution of the entire process into separate phases. This model was titled as systematic digital forensic investigation model (SRDHM) and it contained 11 phases to perform investigation process.

First phase of this model was preparatory phase as it has to be in the initial stage of an investigation process. In this phase, the forensic examiner obtains the understanding that what type of the crime has been committed and what are the activities which were associated during occurrence of the crime. Then examiner plans about the material that was collected in order to pack the sources of evidences. Besides, examiner must also keep in mind about the different legal constraints and the target organizational limitations as well.

In this phase, if required, examiner also attain the relevant and necessary search warrants, different authorizations from the higher management with their full support and dispatching of the legal notices to all the relevant segments or parties associated with the committed crime. Another vital function performed in this phase is to design a proper policy that will be adopted during the inquiry.

Second important phase is to protect the crime scene in order to sustain the integrity of all the evidences and devices at the crime scene. These devices may come up as the main sources of evidences at any stage of investigation. For this, examiner makes sure that no any unauthorized person gets the access of these devices after the investigation process started. Quality of evidence is also decided in this phase. But the main theme of this phase is ensuring the integrity of the crime scene and its infrastructure.

After performing first two phases successfully, an initial survey is conducted by examiner to the crime scene with the objective of identifying the sources of evidences and brings up an strategy to start looking for evidences. During the evaluation of electronic devices examiner may require aid from other experts as well in order to deal the crime scene. Interviewing the relevant persons after their identifications is another function of this phase performed preliminarily.

Significant and effective information gathering can be done by inquiring the different users, administrators or even from the owners of the devices which could produce key evidences for examination. After collecting and developing the evidences from this phase, examiner should also plan that how to analyze these evidences in the later stages of this process in different phases.

Documentation of the entire scene is also another key phase of this model for investigation process. It includes the documenting of all the gathered data that is visible such as different snaps etc. This may help to review the entire process at any stage. All the logs and records about people's entrance and exit from the crime scene also must be documented with the date and its time.

In fifth phase of current model, examiner list downs the all possible communication ways of the associated devices and blocking these communication systems so that nobody could alter, modify, delete or overwrite the information after the process of examination starts. This might be done by isolating these devices completely with all other connected devices. Blocking Bluetooth and wireless services are two most common ways of communication that must be considered by the examiner in this phase.

Sixth phase, which might be the most important phase of all, is to gather the evidences. This is the primary objective of entire investigation model and all phases of it. This phase requires keen consideration and attention to design a most effective system through which the desired and evidences can be gathered which later on could be presented in the court of law and get the status of admissible over there as well to establish the culprit.

To collect volatile evidences from the devices especially from mobile devices need quick decision making as the data in ROM can be modified. Quick response is also needed if the battery of evidence source is low. In this case, image can be created of entire data existed on that device and then it can be dispatched to any other device to analyze easily and freely. For this sake, tools used in this process for image creation also must be best and swiftest. Another way is to replace the low battery with the newer one and then perform the examination and gathering of evidences without restraint.

Second type evidences gathered is non volatile evidences. Such evidences more than often exist in the external media such as flash drives etc. Here again, examiner needs effective and appropriate tools for gathering the evidences from such storage medias. Different methods can be used to assure the integrity of the gathered evidences such as the method of write protect and hashing.

Evidences, which were collected in the previous phase, need to be packed, transported and stored as properly in the electronic devices so that nobody could harm or modify them. This is done in this phase of the model. All necessary and universal techniques must be adopted in order to secure such electronic devices such as supply of the required temperature, saving it from the dust etc after the packaging process done.

After the successful packaging and transportation of gathered evidences, in this phase, these evidences are examined by the expert forensic examiners. After this phase, the team of experts analyzes these evidences and defines the relationship between different segments of data, disclose the data that was hidden and provide the results of all phases of entire forensic model in the end.

After the successful gathering of evidences and analyzes by the forensic experts, these evidences need to be presented in front of any authority such as the higher management of the targeted organization or in front of court of law. Therefore, these

evidences must be presented in a form that clearly exhibits that the person highlighted as culprit is in real a culprit and all the presented evidences are supporting this claim as well.

Reviewing the result is the final phase of this model. All the steps performed in the previous all phases are keenly reviewed and analyzed. Many lessons and room for improvement can come up after performing the review of all steps one by one. These lessons may help examiners to incorporate them in the next coming investigations in the future.

4. FINDINGS

- In our findings of current research, we have highlighted the different important security elements that need to be addressed by enterprises of Pakistan as effectively and appropriately that it assists the digital forensic examination process towards collecting the evidences and establishing the actual culprit behind the committed cyber crime.
- Every element highlighted here is equally importance as it possesses capability to provide evidence or hint or even provides the path the reach out the offender of cyber crime and then prove in the court of Law as legitimized matter.

Large Enterprise Issues: Addressable Elements

- Only 55% of recipients are fully aware about the Domain of Cyber Forensics. It means that 45% organizations have employed the I.T persons who are considered to be most responsible and considered as reliable I.T person don't even know anything about the Domain of Cyber Forensics, it is really alarming situation and addressable too.
- 58% organizations don't have a formal, institutional plan that outlines Digital Forensics for the institution as a whole. It means that if any situation arises to conduct a Digital Forensic Investigations then the employees may deny any responsibility since this section is not addressed by the institutional plan at all.
- 50% of the organizations may collapse by single incident in the absence of Cyber Forensic Policy and procedure. It shows the significance of this domain needs to be addressed at enterprise level and also reveals the flaws in the I.T security level in these organizations.
- 79% of organizations don't even acquire the service of cyber forensic firms.
- 46% of organizations' I.T operations section is being spoiled mostly affected by cyber crime.
- 51% or organizations don't conduct any awareness training programs for employees to educate them about cyber crime and forensics. It is quite shocking situation because if we don't educate our employees to face any such situation or avoid or prevent it, then how may we expect that our security measure are up to the mark.
- 47% enterprises don't contain any clause addressing the cyber crime in their hiring terms and conditions document. It needs to be addressed to ensure the function of accountability against the employees.
- 73% organizations don't employ any tool to record the key strokes of client. It eliminates another effective element of collecting evidences therefore must be addressed.

- 28% organizations don't use cameras as per requirement of recording the physical activities. Physical evidences are often undeniable in the court of law therefore need to work on it as well to rectify it.
- 25% companies store the recorded videos forever, while only 15% perform it for 1 year. The requirement of these durations may vary organization to organization by considering its nature of business, but still this sector should be improved.
- If the primary media of recorded videos is lost then backup of these videos becomes essential. 25% organizations don't opt to take backups of videos is not reckoned as fool proof scenario.
- If we allow employees to use their blue-tooth service freely, especially in the financial institution like Banks which contain extremely confidential information of customers then it will be mentioned as a vulnerable part of I.T security as well. 57% of organizations don't restrict their employees or other to use blue-tooth inside the organization, which is highlight able matter.
- 33% of organizations allow their employees to download freeware on their computers. This percentage is worry because freeware downloading may cause some security or monitoring tools troubles to record or collect the appropriate evidences.
- 28% of enterprises don't adopt any mechanism and monitor the downloading or installing new applications in the client systems. This ought to be addressed to prevent clients doing it by them and this may also create hurdles in the forensic process.
- 51% organizations have permitted employees to store the critical data directly to their storage devices. This issue is seriously addressable as well because often it doesn't leave any evidences of data being stolen or used illegitimately.
- The percentage of organizations that let their employees to execute (.exe) files directly from the web or emails. 28% is the percentage which needs to be reduced as much as possible as well.
- 26% companies have not employed policies that prohibit users from disclosing their passwords to anybody else. This situation may create ambiguity in the process of accountability in terms of forensic; therefore it also needs to be addressed.
- 19% of organizations have not yet implemented polices that require users to lock their workstations when they leave their desks.
- 32% organizations have not implemented policies that prohibit users from allowing anyone else to use the computer after they've logged in.
- 53% is huge number of those organizations that don't employ any snapshot tool to collect the evidences and monitor the client screens. It is an effective tool to collect the evidences therefore this matter need to be addressed on priority basis.
- Finally, another addressable issue needs to be highlighted here is that 42% of organizations have allowed employees to erase the web browser's history and temp files. It may also cause serious damage and obstacle in the process of evidence collection, therefore mentioned here.

5. CONCLUSION

In this paper, different types of enterprises of Pakistan are being evaluated to perceive the status of security measures adopted in order to enable successful digital forensics' investigation process. For this, first we have identified the elements of IT security of these organizations associated with digital forensic. These elements must be set in appropriate and conventional manner as so that if there is occurrence of any cyber crime then there must be enough tails left behind which could produce and provide ample evidences against the criminal to be produced in the court of law. If these elements are ignored and are not tackled as these needs to be, then it brings the situation full of flaws and which could leave huge impact over the business and associated segments of any IT comprising enterprise.

Our research could be considered as useful teaching for the enterprises where high valued segments rely heavily over the security and performance of IT and if somebody succeeds to penetrate and harm these segments then it could leave significant loss over the business and reputations of the enterprise. Then it also becomes complex for the digital forensic firm to gather optimum and desired evidences to establish the actual culprit of that specific cyber crime. On the other hands, questions is not to just collect evidences, but another major issue is to satisfy and meet the law and regulations of country so that presented evidences could become admissible in the court of law. These would not just bring up the actual culprit on the screen but also will open the doors for the compensation of the victimized enterprise.

References

Ankit Agarwal, Megha Gupta, Saurabh Gupta & S.C. Gupta. (2011). Systematic Digital Forensic Investigation Model, *International Journal of Computer Science and Security (IJCSS).* Volume (5). Issue (1).

Belabed, A. Aimeur, E. & Chikh, A. (2012). A personalized whitelist approach for phishing webpage detection, *Seventh International Conference on Availability, Reliability and Security, IEEE*

Den Hengst, Marielle. & Warnier, Martijn. (2013). Cyber crime in privately held information systems, *European Intelligence and Security Informatics Conference, IEEE*

Horsman, Graeme. Laing, Christopher. & Vickers, Paul. (2012). A case based reasoning framework for improving the trustworthiness of digital Forensic Investigations, *11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE*

http://en.wikipedia.org/wiki/Digital_forensics

Imoniana Onome, Antunes Joshua Thereza Pompa, Maria. & Formigoni, Henrique (2013). The forensic accounting and corporate fraud, *JISTEM - Journal of Information Systems and Technology Management.* Vol. 10, No. 1, pp.119-144

Khan, Ayaz. Kock Wiil, Uffe. & Memon, Nasrullah. (2010). Digital Forensics and Crime Investigation: Legal Issues in Prosecution at National Level, *Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, IEEE*

Ma, Guofu. Sun, Chaochao. & Wang, Zixian. (2011). Study on Digital Forensics Model Based on Data Fusion, *International Conference on Mechatronic Science, Electric Engineering and Computer, IEEE*

Morozini De Lira, Arnaldo. Claudio, Parisi. Ivam Ricardo, Peleias. & Reinaldo Severino Peters, Marcos. (2012). Uses of ERP systems and their influence on controllership functions in Brazilian companies, *JISTEM - Journal of Information Systems and Technology Management.* Vol. 9, No. 2, pp.323-352

Nnoli, Henry. Lindskog, Dale. Zavarsky, Pavol. Aghili, Shaun. & Ruhl, Ron. (2012). The Governance of Corporate Forensics using COBIT, NIST and Increased Automated Forensic Approaches, *ASE/IEEE International Conference on Social Computing and ASE/IEEE International Conference on Privacy, Security, Risk and Trust, IEEE*

O. Ademu, Inikpi. O. Imafidon, Chris. & S. Preston, David. (2011). A New Approach of Digital Forensic Model for Digital Forensic Investigation, *IJACSA, International Journal of Advanced Computer Science and Applications,* Vol. 2, No. 12

Ojo Nehinbi, Joshua. & Adebayo, Funmi. (2011). Audit and Research Challenges in Digital Forensics, *International Conference on Cybernetic Intelligent Systems, IEEE*

Pérez Lorences, Patricia (2013). The evaluation and improvement of IT governance, *JISTEM - Journal of Information Systems and Technology Management.* Vol. 10, No. 2, pp.219-234

Sivaprasad, Abirami. & JangaJe, Smita,(2012). A Complete Study on Tools & Techniques for Digital Forensic Analysis, *International Conference on Computing, Electronics and Electrical Technologies ICCEET, IEEE*

Sladić, G. Milosavljević, B. & Konjović. Z.(2012). Modeling Context for Access Control Systems, *10th Jubilee International Symposium on Intelligent Systems and Informatics, IEEE*

Valjarevic, Aleksandar. & S.Venter, Hein. (2012). Harmonised Digital Forensic Investigation Process Model, *IEEE*

Wen Hsing, Chen. (2012). Management practices and influences on it architecture decisions: a case study in a telecom company, *JISTEM - Journal of Information Systems and Technology Management.* Vol. 9, No. 3, pp.563-584

Imoniana Onome, Antunes Joshua Thereza Pompa, Maria. & Formigoni, Henrique

