THE NEED FOR DIGITAL FORENSIC INVESTIGATIVE FRAMEWORK

I. Ademu[1], C. Imafidon[2]

[1]*Postgraduate Student, School of Architecture, Computing and Engineering, University of East London, London, United Kingdom,* ***iniademu2011@gmail.com***

[2]*Senior Academic, School of Architecture, Computing and Engineering, University of East London, London, United Kingdom,*
[2]*Former Head of Management Unit, Queen Mary, University of London, London, United Kingdom*
C.O.Imafidon@uel.ac.uk

Abstract

Since digital devices such as computers are vulnerable to attack by criminals, digital forensics is increasing in importance. Understanding digital forensic procedures will help to capture vital information which can be used to prosecute a suspect that compromises a digital devices or network. The majority of organizations rely deeply on digital devices and the Internet to operate and improve their business, and these businesses depend on the digital devices to process, store and recover data. A large amount of information is produced, accumulated, and distributed via electronic means. It is necessary for forensic experts to increase their abilities to gather evidence from digital devices. Also, deciding on the specific tools for computers or other digital devices that is needed to correctly analyze evidence is crucial. The advancement of the digital forensic investigation requires a new design, improved mechanism and processes. Forensic experts are faced with growth in data. Huge amount of data has expanded and grown in recent years and attempts to consume the storage space available. Digital forensic techniques are used primarily by private organisations and law enforcement agencies to capture, preserve and analyze evidence on digital devices. Digital evidence collected at a crime scene has to be analyzed and connections between the recovered information need to be made and proven. The search for digital evidence is thus a tedious task that consumes time. An extremely large amount of evidence needs to be processed in a very limited time frame which leads to delay in processing schedules. This paper underscores the need to understand the importance of a digital forensic investigative framework.

Index Terms: *autonomous coding, visual sudio, integrated development environment, relational reconstruction, data processing, investigative framework*

---------- *** ----------

1. INTRODUCTION

Digital forensic has been defined as the use of scientifically derived and proven methods toward the identification, preservation, collection, validation, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations (Reith et al, 2002). This definition covers the broad aspects of digital forensics from data acquisition to legal action. It describes digital forensics as a synonym for computer forensics, and defines it as the use of scientific methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation helping to anticipate unauthorized actions exposed to be disrupting intended operations. The aim of this research is to study the main activities or processes necessary for digital forensic investigation and to examine existing digital forensic models and the importance and need for an investigative framework.

2. DIGITAL EVIDENCE

Digital evidence is by nature fragile. It can be altered, damaged or destroyed by improper handling or improper examination. It is easily copied and modified, and not easily kept in its original state, precaution should be taken to document, collect, preserve and examine digital evidence

(Carrier, 2003). Buttressing this point is looking at one of the research carried out by (Sommer, 2004) he emphasized that data from computer can be accurately preserved and presented in court and like every other evidence digital evidence must be admissible, authentic, accurate, complete and convincing to juries, digital evidence is different from every other evidence in that it can change from moment to moment within a computer and along a transmission line, it can easily be altered without trace and can be changed during evidence collection. The main problem is how do expert measure the reliability of digital evidence?

Digital evidence is a data of investigative value that is stored on or transmitted by a digital device. Therefore digital evidence is "hidden" evidence in the same way that Deoxyribonucleic Acid (DNA) or fingerprint evidence is hidden. In its natural state, digital evidence cannot be known by the content in the physical object that holds such evidence. Investigative reports may be required to explain the examination process and any limitation (Pollitt, 2007).

3. DIGITAL FORENSIC INVESTIGATION PROCESS

The investigative process is structured to encourage a complete, accurate investigation, ensure proper evidence handling and reduce the chance of mistakes created by preconceived theories and other potential pitfalls. This process applies to criminal investigations as well as public and private inquiries dealing with policy violations or system intrusion. Investigators and Examiners work hand in hand in a systematic and determined manner in an effort to present accurate and reliable evidence in the court. While in the court evidence are handed over to the prosecutors who scrutinize the findings and decide whether to continue or discontinue the case.

A good investigative framework should aim at providing to the investigators and examiners structured and precise logical flow of event that collectively seeks to provide:

- Acceptance: steps or process and methods have earned professional consent
- Reliability: methods used can be trusted to support findings.
- Usability: the process can be repeated and applied by all regardless of time and place.
- Flexibility: the process or component is easily modified for use.
- Integrity: the state of evidence proven to be unaltered.
- Documentation: the process is recorded from start to finish for testimonial evidence.

4. EXISTING DIGITAL FORENSIC MODEL

The first DFRWS was held in Utica, New York (2001). The goal of the workshop was to provide a forum for a newly formed community of academics and practitioners to share their knowledge on digital forensic science. The audience were military, civilian, and law enforcement professionals who use forensic techniques to uncover evidence from digital sources. The group created a consensus document that drew out the state of digital forensics at that time. The group agreed and among their conclusions was that digital forensic was a process with some agreed steps. They outline processes such as identification, preservation, collection, examination, analysis, presentation and decision (Palmer, 2001). Some of their identified matrixes were identified by the group as fundamental processes, although many will debate the forensic nature of each step of the process. This can be called a comprehensive or an enhanced model of the Department of Justice (DOJ) model because it was able to cover stages that were not covered in any previous model, such as presentation stage. The main advantage of DFRWS is that it is the first large-scale organisation that is lead by academia rather than law enforcement, this is a good direction because it helps define and focus the direction of the scientific community towards the challenge of digital forensic, but the DFRWS model is just a basis for future work.

Reith et al (2002) examined a number of published models/framework for digital forensics. The basis of this model is using the ideas from traditional (physical) forensic evidence collection strategy as practiced by law enforcement (e.g. FBI). The authors argued that the proposed model can be term as an enhancement of the DFRWS model since it is inspired from it. Using this model, future technologies and the technical details required to forensically analyse them can be instantiated to provide a standard methodology for providing electronic evidence (Reith et al, 2002). This will improve the science of forensic because it involves a basis for analysing new digital technology while at the same time provide a common framework for law enforcement and the judicial system to feasibly work within a court of law.

Carrier and Spafford (2003) proposed a model, which the authors provide a review of previous work and then map the digital investigative process to the physical investigation process. The model known as the Integrated Digital Investigation Process was organised into five groups

consisting of 17 phases. End to End Digital Investigation adopted by (Stephson, 2003) consist of 9 activities. It combined an extended digital forensic investigation process. The model takes into account the source of the incident, destination of the incident and the intermediate devices along the path through the network

Baryamueeba and Tushaba (2004) suggested a modification to Carrier and Spafford's (2003) Integrated Digital Investigation Model. The model is known as Enhanced Digital Investigation Process, the authors described two additional phases which are traceback and dynamite which seek to separate the investigation into primary crime scene (computer) and secondary crime scene (the physical crime scene). The goal is to reconstruct two crime scenes to avoid inconsistencies.

Ciardhuain (2004) argues that the existing models are general models of cybercrime investigation that concentrate only on processing of evidence in cybercrime investigation. The author proposed an extended model for cybercrime. It provides a good basis for understanding the process of cybercrime investigation, tackling certain activities such as presenting the information flow in an investigation and captures its full scope and not just processing the evidence. Even though the model was generic, it concentrated on the management aspect. The author argues that the available models are generic model of cybercrime investigation focusing on investigative process such as gathering, analysing and presenting the evidence. The model is designed to assist public and corporate forensic investigations. The model assists in the development of model investigative tools. The investigative tools for conducting investigation are not provided.

Freiling and Schwittany (2007) proposed a model for the purpose of introducing a new process framework to investigate computer security incidents and its aim is to combine the two concepts of incident response and computer forensic to improve the overall process of investigation. The framework focuses generally on the analysis of digital evidence. Perumal (2009) proposed a model that clearly defines that the investigation process will lead into a better prosecution as the very most important stages such as live data acquisition and static data acquisition has been included in the model to focus on fragile evidence. Polli et al (2010) proposed a generic model for network forensic analysis based on various existing digital forensic model, it covers tools, process model and framework implementation. This was specifically for the network based investigation.

The Systematic Digital Forensic Investigation Model proposed by (Agawal et al, 2011). This model has been developed with the aim of helping forensic practitioners and organizations for setting up appropriate policies and procedures in a systematic manner. The proposed model in this paper explores the different processes involved in the investigation of cyber crime and cyber fraud in the form of an eleven stage model. The model focuses on investigation cases of computer frauds and cyber crimes. The application of the model is limited to computer frauds and cyber crimes.

The Relational Reconstruction model was proposed by (Ademu et al, 2011). The model identifies the need for reconstrcution and interaction. The investigator should have consistent interaction with all resources for carrying out the investigation. Knowing the need of the victim and determined to meet the need is important. Better case goal can be defined. Optimal interaction with tools used by an investigator is very important. Tools need to be used by people who knows how to use them properly following a methodology that meets the legal requirement associated with the particular jurisdiction. Investigators need to have the patience, to stay on the target and have to learn any new techniques while performing an investigation. Very little testing has been formalized in this field for the specific need of digital forensic, investigators wishing to be prudent should undertake their own testing methods and this should be a normal part of the process used in preparing for legal matters and this should also meet the leal requirement of the jurisdiction. The model also help capture the expertise of investigation as a basis to the development of advanced tools incorporating techniques such as identifying the Visual Basic Integrated Development Environment with a set of rich features which are likely to be required for developing tools that can assist digital investigators during digital forensic investigation.

5. WHY THE NEED FOR INVESTIGATIVE FRAMEWORK

Digital evidence is admissible in court as long as the process used to produce the evidence is known to produce reliable results. According to Kruse II (2002), the basic forensic methodology known as the three A's is evidence must be acquired without altering or damaging the original, investigator must authenticate that recovered evidence is the same as the originally seized data and data must be analyzed without modifying it. Digital evidence must not be modified or damaged during any part of the investigation process. Hash sums should be calculated on collected digital evidence data, and also the source of the evidence and compared to ensure the authenticity and integrity of the data.

An investigative framework should provide a process for conducting a digital forensic investigation. There are multiple of factors complicating the investigative process. The more clearly the investigative process is defined, the more likely an

investigation will be successful if such process is used for investigation. An investigative framework, properly thought out and constructed would give a step by step process for conducting an investigation into a suspected digital device. A clear and structured process will allow investigators and examiners determine early in the investigation that an attack has occurred and it can also lead them to a final conclusion Casey (2002). It is important to know that this does not imply that all such conclusions are successful. A worrying large percentage of investigation ends with the conclusion that the victim was attacked, but the source of the attack cannot be determined.

Casey (2004) discussed that the U.S. Supreme Court provides certain criteria in the Daubert vs. Merrel case that may be used as guidelines by courts to determine whether or not evidence is admissible in court. Conventional applications in the jurisdiction therefore have to adhere to the requirements stipulated by the Daubert standard to allow the evidence they collect to be admissible in court. Few investigators have the time and skill to evaluate and analyze their chosen tools to determine whether or not it obeys the rules of the criteria stated by the Daubert standard. Even though the tools obeys the rule to the criteria and perform well in a trusted environment, they may give inconsistent results in an untrustworthy environment Casey (2004). This is because some software applications rarely contain all the operating logic needed to perform basic functionality that can be supplied by external drivers or the operating system, the application rely rather on libraries and drivers may be compromised to produce results that are inconsistent with the digital evidence.

Most commercial forensic toolkit seems are very expensive to buy. This creates a problem because not every investigation team has the finance to invest in the very expensive toolkit and may have to use the available open source tools, but this has less functionality and needs investigators with more technical skills. It could be better to use existing functionality supplied by commercial forensic tools, since their functionality has been tested and proven, but it is virtually impossible due to the fact that the source code of these tools is not available to the general public. A solution is needed to allow investigator to perform rapid digital forensic investigation on a consistent and structured framework in an attempt to speed up digital forensic investigation.

Therefore, an important part of the investigative process is the exploratory testing that has been discovered in the course of this research. If an exploratory testing process is applied early in the investigation, actual reasoned examination begins, concrete facts begin to take shape that support or falsify hypotheses built by the investigative team, if properly applied this can help in achieving a higher degree of avoidance of improper handling or damaging digital evidence.

6. CONCLUSION

Digital evidence must be precise, authenticated and accurate in order to be accepted in the court. Digital evidence is fragile in nature and they must be handled properly and carefully. Detailed digital forensic investigative processes provide important assistance to forensic investigators in establishing digital evidence admissible in the court of law.

The digital forensic community needs a structure framework for rapid development of standard operational procedures that can be peer – reviewed and tested effectively and validated quickly. Digital forensic practitioners can benefit from the iterative structure provided in this research to build a forensically sound case and also for the development of consistent and simplified processes of digital forensic investigation that can be a guideline for standard operational procedure and a framework for developing future technology in the digital forensic investigation.

ACKNOWLEDGEMENT

The authors would like to thank the following for their support during this research:
Dr David Preston and University of East London's of School of Architecture, Computing and Engineering Anne-Marie Imafidon, University of Oxford, (Keble College). Oxford OX1

REFERENCES

[1]. Ademu, I. Imafidon, C. Preston, D., (2012) Intelligent Software Agent applied to Digital Forensic and its Usefulness Vol. 2 (1) Available (online): http://interscience.in/IJCSI_Vol2Iss1/IJCSI_Paper_21.pdf Accessed on 10th April 2012

[2]. Ademu, I. Imafidon, C. I. Preston, D. (2011) A New Approach of Digital Forensic Model for Digital Forensic Investigation Vol. 2, (12) Available (online): http://thesai.org/Downloads/Volume2No12/Paper%2026-A%20New%20Approach%20of%20Digital%20Forensic%20Model%20for%20Digital%20Forensic%20Investigation.pdf Accessed 28th April 2012

[3]. Agawal, A. Gupta, M. Gupta, S. Gupta, C. (2011) Systematic digital forensic investigation model Vol. 5 (1) Available (online): http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume5/Issue1/IJCSS-438.pdf Accessed on 30th April 202

[4]. Baryamureeba, V. Tushabe, F. (2004) The Enhanced digital investigation process (2004) Available (online): http://www.dfrws.org/2004/bios/day1/tushabeEIDIP.pdf Accessed on 15th May 2012

[5]. Ciardhuain, S. (2004) An extended model of cybercrime investigation Available (online): www.ijde.org/citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.80...Accessed on 11th April 2012

[6]. Carrier, B. Spafford, H. (2003), Categories of digital investigation analysis techniques based on the computer history model. Available (Online): http://dfrws.org/2006/proceedings/16-carrier.pdf Accessed on the 12th April 2012

[7]. Carrier, B. (2003) Defining digital forensic examination and analysis tools using abstraction layers Vol. 1 (4) Available (online): http://www.cerias.purdue.edu/homes/carrier/forensics Accessed on 20th September 2011

[8]. Casey, E (2004) Digital evidence and computer crime forensic science, computers and the internet 2nd Edition Pg 101 Academic Press – London

[9]. Casey, E. (2002) Handbook of computer crime and investigation Pg 116 Academic Press - London

[10]. Freiling, F. Schwittany, B. (2007) A common process model for Incident Response and computer forensic Available (online): http://whitepapers.hackerjournals.com/wp-content/uploads/2010/06/A-Common-Process-Model-for-Incident-Response-and-Computer-Forensics.pdf Accessed on 17th April 2012

[11]. Kruse II, W. Heiser, J (2002) Computer Forensics Incident Response Essentials Pg 170 Addison - Indianapolis

[12]. Palmer, G. (2001) a road map to digital forensic research Available (online): http://www.dfrws.org/2001/dfrws-rm-final.pdf Accessed on 25th April 2012

[13]. Panda labs Annual Report (2009) Available (online):http://www.pandasecurity.com/img/enc/Annual_Report_Pandalabs2009.pdf Accessed on 5th May 2012

[14]. Perumal, S. (2009) Digital forensic model based on Malaysian investigation process Vol. 9 (8) Available (online): http://paper.ijcsns.org/07_book/200908/20080805.pdf Accessed on 7th May 2012

[15].Polli, E, Joshi, R. Niyosi, R. (2010) Network Forensic Frameworks: Survey and research challenges Available (Online): http://www.sciencedirect.com/science?_ob=MiamiImageURL&_cid=273059&_user=132444&_pii=S1742287610000113&_check=y&_origin=&_coverDate=31-Oct-2010&view=c&wchp=dGLzVlt-zSkzS&md5=f0345fa37fdcbc76113b1d98c9a83367/1-s2.0-S1742287610000113-main.pdf Accessed on 28th April2012

[16]. Pollitt, M. (2007) An Ad Hoc Review of Digital Forensic Models, Vol. 10(12) Available (Online): http://www.ieeexplore.ieee.org/ie15/4155337/4155338/04155349.pdf? Accessed on the 17th April 2012

[17]. Reith, M. Carr. C. Gunsch, G. (2002). An examination of digital forensic model. Department of Electrical and Computer Engineering Air force institute of technology. Wright-Patterson. Available (Online): http://www.utica.edu/academic/institudes/ecii/ijde/articles.cfm?action Accessed on the 7th May 2012