CERIAS Tech Report 2015-4
Cyber Forensics: The Need for An Official Governing Body
by Ibrahim Waziri Jr, Rachel Sitarz
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

DIGITAL FORENSICS: THE NEED FOR AN OFFICIAL GOVERNING BODY

Ibrahi Wazir Jr.
P Candidate Informatio Security
CERIAS
Purd University
Wes Lafayette I 47907
iwaziri@purdue.edu

Rache Sitarz
P Candidat in Cybe Forensics
Colleg Technology
Purd University
Wes Lafayette I 47907
rsitarz@purdue.edu

Abstract

In this paper we identified and addressed some of the key challenges in digital forensics. An intensive review was conducted of the major challenges that have already been identified. At the end, the findings proposed a solution and how having a standardized body that governs the digital forensics community could make a difference.

Limitation

This study is an intensive review of what other studies have identified as issues within the digital forensics community. It is not complete review of all the issues but just a selected few. The proposal of official governing body implementation and assigned responsibilities is based on the compilation of other studies recommendations. The roles breakdown at each level is based on the selected identified issues, as more issues are being identified so will the roles increase. The key challenges that will take to implement such a body such as funding, availability of professionals, work place, ranking of officials based on intellectuality etc. are not discussed in this study. Future study could focus other issues that have not been reviewed in this study.

Introduction

As a result of advancement in technology and the need for digital devices, different forms of technological crimes have evolved, which are all classified as digital crime. Along with this form of crime comes a countermeasure, which is digital forensics. Considering digital crime & forensics is still progressing. Presentation and acknowledgement of digital forensic evidence is still an issue within the judiciary system. Lack of awareness and availability of experts is still a problem. An error in evidence that results to freedom of the guilt and incarceration of the innocent still happens. To overcome the current issues, the study aims to analyze and look at how an official governing body within the digital forensics community can make a difference.

Previous Study

Meyers & Rogers (2004) presented an overview of some serious issues in the maturing discipline of computer forensics, and the paper also identified three areas within the legal system where computer forensics is most likely to be questioned. One problem addressed that needs an urgent attention is the lack of standards and certification. The paper analyzed federal and state court

cases and concluded with a call for standardization and certification within the computer forensics field. To better understand the issues within digital forensics, we first need to know how to define and control the anti-forensics problem. Harris (2006) attempts to arrive at a standardized method of defining anti-forensics, categorizing the anti-forensics techniques and outlining the general guidelines to protect forensic integrity.

As a result of lack of standards and an official governing body, many errors derived from faulty practices of unqualified professionals have resulted in grievous miscarriages of justice. This calls for assurance within the digital forensics community. The paper cyber forensics assurance Dardick (2010) discussed about how it is not uncommon in today's legal environment to have unsuccessful prosecutions based upon the faulty presentation of cyber forensics evidence and the resulting opinions and testimony given by "experts" witness. The paper referred to cases where the guilty is not proven guilty, or where innocent people are proven guilty when in fact they are not. Such cases are only solved when the opinions given and relied upon are repudiated. As such, the risk of repudiation needs to be minimized. The paper is about reducing the risk of repudiation. Many issues are a major concern in the digital forensics community, must of these issues require the law to be legislated. The paper "developmental trends in computer forensics and security in various aspects" by Aminnezhad (2012) analyzed each scenario to determine the trend of solutions in these aspects and evaluate the effectiveness in resolving the aforementioned issues.

Experts and professionals are facing difficulties in efficiently presenting findings. These are all as a result of lack of standardization for reporting digital evidence items in digital forensics. Bariki et al, (2011) proposed a standard for digital evidence to be used in reports that are generated using computer forensics software tools. The paper focused on developing a standard digital evidence items by surveying various digital forensics tools while keeping in mind the legal integrity of digital evidence items. It also used an online questionnaire to gain the opinion of knowledgeable and experienced stakeholders in the digital forensics domain. Fundamental principles such as reconnaissance, reliability and relevancy are important in carrying out digital forensics investigations. (Leong, R. 2006) highlighted the fundamental principle of digital forensics investigations, based on that highlight the study re-visit the investigation tasks and outlined eight different roles and responsibilities in digital forensics. For each role, it defined a set of six key questions, which are: What (the data attributes), Why (the motivation), How (the procedures), who (the people), Where (the location), and When (the time) question. With these questions, a digital investigation framework is composed.

Because most of the forensic investigative procedures used in the case of an intrusion into a networked computer system to detect the scope or nature of an attack are employed and constructed in an informal manner, which usually impede the effectiveness, or integrity of the investigation. Leigland & Krings (2004) proposed a formal model for analyzing and constructing forensic procedures, showing the advantages of formalizing forensic investigations. The paper presented a mathematical description of the model demonstrating the construction of the elements and its relationships. The model highlights definitions and updating of forensic procedures, identification of attack coverage, and portability across platforms.

Menon & Siew (2012) identified the key challenges in tackling modern economic cybercrimes, and evaluated the existing legal and enforcement mechanisms in place; the paper also proposed a way forward to address these challenges. The paper first started by analysis of the main difficulties posed by the borderless, complex and rapidly evolving nature of modern economic and cybercrimes. Which allowed the key shortcomings of the present legal and enforcement infrastructure to be identified, by examining different models ranging from vertical supranational

structures such as the International Criminal Court and the proposed European Public Prosecutor, to soft-law regimes such as the intergovernmental network, the financial action task force, as well as intermediate approaches like Eurojust, a hybrid model incorporating elements from these various regimes is proposed. Rogers & Seigfried (2004) did a pilot study and attempted to add to the growing body of knowledge regarding issues in computer forensics. The study consisted of an internet-based survey that asked respondents to identify the top five issues in computer forensics. The result indicated that education/training and certification were the most reported issue (18%) and lack of funding was the least reported (4%). The findings emphasize the fragmented nature of the computer forensic discipline. And currently there is a lack of national framework for curricula and training development, and no gold standard for professional certifications.

Today, cloud computing is undoubtedly one of the most discussed topics in information technology. Brik & Wegener (2011) focus on the technical aspects of digital forensics in distributed cloud environments. The study contributed by assessing whether it is possible for the customer of cloud computing services to perform a traditional digital investigation from a technical point of view. Lastly the paper discussed possible solutions and new methodologies helping customers to perform such investigations.

Giannelli (2008) discusses about the need to regulate crime labs, due to wrongful convictions. The paper documents the failures of crime labs and some forensics techniques; such as microscopic hair comparison and bullet lead analysis. Some cases involved incompetence and sloppy procedures, while others entailed deceit, but the extent of the abuses, covering decades in several instances demonstrates that the problems are systematic.

All these previous studies have one thing in common; they all aim at identifying the issues and problem faced within the digital forensics investigation and evidence presentation. They all tried to propose a solution to how each issue can be handled. However to better address all the issues; there is a need for an official governing body within the digital forensics community. This official governing body can be responsible for setting standards and regulations, and also provide stability in other to avoid most of the aforementioned problems.

Current Issues as Identified

Some of the issues identified within the Digital Forensics community include:

- Privacy Issues
- Lack of certifications and standardizations
- Lack of awareness between the general public and law enforcements
- Lack of standardized labs & tools
- Lack of standard in reporting digital evidence
- Error rates in evidence presentation
- Legal issues

Introducing Digital Forensic Authorities

We propose the official digital forensic authorities that need to be implemented to ensure stability within the digital forensic community. These authorities need to be implemented at the 3 different levels of government, which are: The Federal, state & local levels. The chart below shows the authorities and the role each has to play to ensure that the issues are minimized.

- **The Federal level:**
  - Create the standards & regulation that should be practiced within the digital forensic community
  - Implement a generic ethics for professionals and experts
  - Work with federal courts
  - Professional and experts validation through certifications
  - Digital forensic tools verification and qualification
  - Student Opportunities (Internships)
  - Trainings
  - Lab standard verifications
  - Private labs/investigators registrations
  - Crime Scene Investigation

- **The State level:**
  - Labs supervision
  - Local law enforcement trainings
  - Expert verifications
  - Implementation of state laws
  - Private investigators licensing
  - Expert witness verifications
  - Student opportunities
  - Crime Scene Investigation

- **The local level**
  - Community awareness
  - Evidence collection/compilations
  - Crime scene investigation
  - Student Opportunities

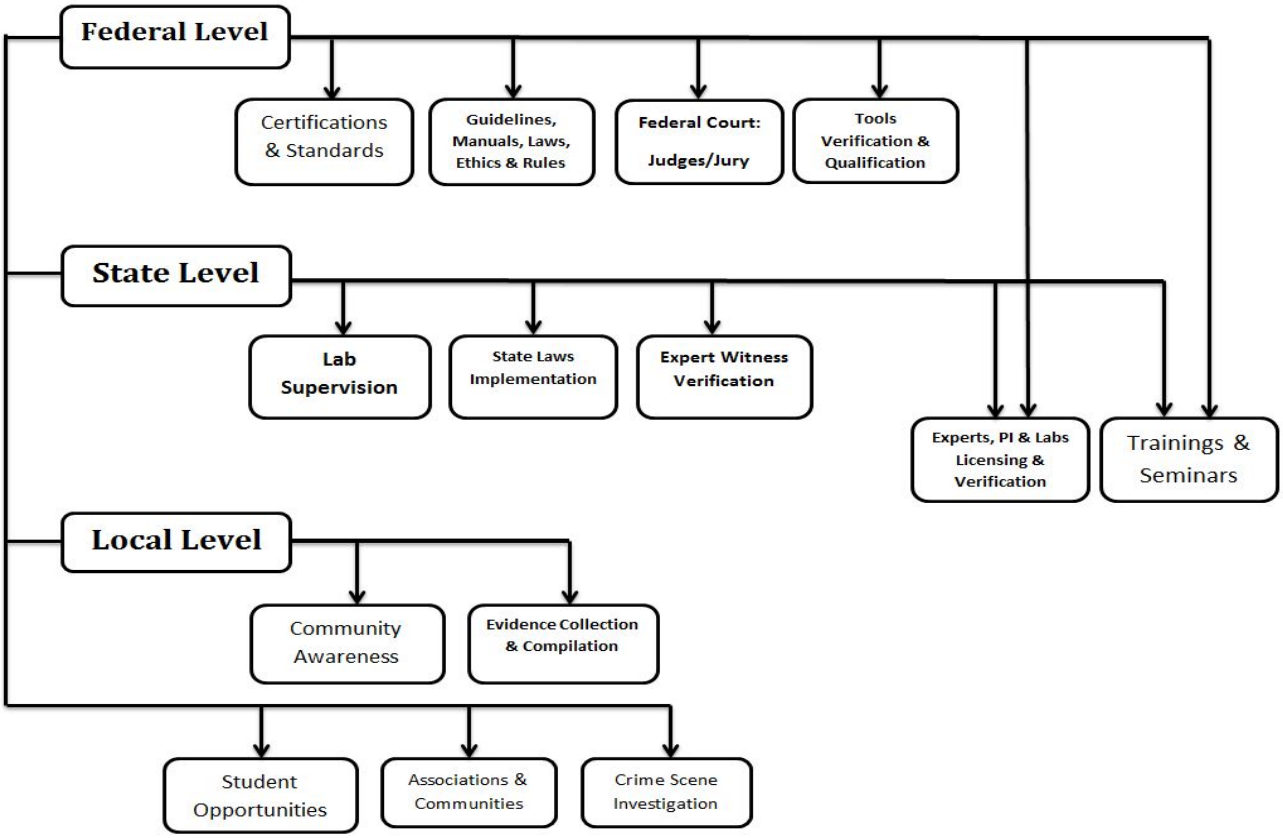

Chart: Official Governing Body Responsibilities

Conclusion & Future Study

Digital crime keeps growing in correlation with digital devices use. However there is still numerous numbers of issues within the digital forensics community. These issues hinder transparency and justice with regards to evidence collection, judicial decision-making etc. The lack of a defining body that set regulations leads to difficulties within the digital forensics community. This paper proposes an official governing body that could help solve some of the identified issues. The paper also outlines the responsibilities of these bodies at different levels.

Future study could focus on how these bodies could be implemented and how the officials needed for these bodies could be validated and assigned to roles.

References:

Meyers, M., & Rogers, M. (2004). Computer Forensics: The Need for Standardization and Certification. *International Journal of Digital Evidence, 3*(2).

Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation, 3s*, 44-49.

Dardick, G. (2010). Cyber Forensics Assrance. *Proceedings of the 8th Australian Digital Forensics Conference,* 57-64.

Aminnezhad, A., Dehghantanha, A., & Abdullah, M. (2012). A survey on Privacy Issues in Digital Forensics. *International Journal of Cyber-Security and Digital Forensics (IJCSDF), 1*(4), 311-323.

Bariki, H., Hashmi, M., & Baggili, I. (2011). Defining a Standard for Reporting Digital Evidence Items in Computer Forensics Tools. *International Conference on Digital Forensics & Cyber Crime, 53*, 78-95.

Leong, R. (2006). FORZA - Digital Forensics Investigation Framework that incorporate Legal Issues. *Digital Investigation, 3s*, 29-36.

Leigland, R., & Krings, A. (2004). A Formalization of Digital Forensics. *International Journal of Digital Evidence, 3*(2), 1-32.

Menon, S. Siew, T.G. (2012),"Key challenges in tackling economic and cyber-crimes", *Journal of Money Laundering Control*, Vol. 15 Iss 3 pp. 243 – 256

Rogers, M., & Seigfried, K. (2004). The future of computer forensics: A needs analysis survey. *Computers & Security, 23*, 12-16.

Brik, D., & Wegener, C. (2011). Technical Issues of Forensic Investigations in Cloud Computing Environments. *Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on,* 1-10.

Giannelli, P. (2008). WRONGFUL CONVICTIONS AND FORENSIC SCIENCE: THE NEED TO REGULATE CRIME LABS. *Case Research Paper Series in Legal Studies*.

Kloosterman, A., Sjerps, M., & Quak, A. (2014). Error rates in forensic DNA analysis: Definition, numbers, impact and communication. *Forensics Science International: Genetics, 12*, 77-85.