Towards a Standardised Digital Forensic Process: *E-mail Forensics*

Himal Lalla
Department of Information Systems
University of Fort Hare
East London, South Africa
Himal.lalla@gmail.com

Stephen V. Flowerday
Department of Information Systems
University of Fort Hare
East London, South Africa
sflowerday@ufh.ac.za

Abstract— **This paper discusses the challenges that face digital forensic investigators as well as process models currently employed. These models aid in the development of a methodology that is comprehensive and provides forensic investigators with a robust foundation in order to produce legally admissible evidence in a court of law.**

Keywords: Digital Forensic Methodology; E-mail Forensics; Legally Admissible Evidence

I. INTRODUCTION

We are living in the information age [6] in which important documents and information are stored on digital media and computer systems that have been incorporated into many institutions to improve efficiency and productivity [32]. Many companies and institutions use e-mail as a method to communicate and conduct business, and this has led to an increase in e-mail traffic volume [22]. This large amount of e-mail traffic has opened the door to abuse by criminals and terrorists because primarily they can remain anonymous [25].The anonymity factor of e-mail has made it difficult for digital forensic investigators to identify the authorship of an email, and to compound this problem further; there is no standardised procedure to follow [21]. Therefore, the problem arises as to authorship of the e-mail.

To address this issue digital forensic investigators have to follow a number of steps that are part of a process. The number of forensic models has added to the complexity of the field [13]. Therefore, this has led to a call for standardisation in the field of digital forensics. The lack of standardisation hinders the investigation process [24]. Notwithstanding this, there are a few procedures from different authors that are known to be the 'standard' procedures [21]. However, one notes that there are a number of discrepancies [21].

The lack of rules results in incomplete evidence collection and errors in interpretation [9]. To add further to this complexity, the legal foundation, which is evolving, will restrict digital forensics [35]. Therefore there is a need, firstly to standardise the process and secondly to comply with the law when collecting evidence in order for it to be legally admissible in a court of law.

The main objective of this paper is to produce a standardised methodology that will aid forensic investigators during an investigation and that results in legally admissible evidence. The following section will address the objective of the paper. Section II presents a theory that supports the paper and subsection B addresses the challenges that face digital forensic investigators. Subsection C presents some tools that digital forensic investigators use while subsection D outlines the digital forensic process models. Section III describes the approach that the paper takes while attempting to create a methodology. Section IV is the proposed methodology and section V is the conclusion of the paper.

II. CURRENT STATUS OF DIGITAL FORENSICS

The purpose of this section is to define why creating a new methodology will pose a challenge for digital forensic investigators by presenting a supporting theory.

A. Diffusion of Innovations Theory

This theory postulates that the innovation adoption process is one of information gathering and uncertainty reduction [1]. Diffusion research is distinctive due to the communication messages that individuals perceive as "new" [33]. Hence, the high uncertainty in information gathering.

Vernon's Product Life Cycle model was utilised to assert that the diffusion process has an S-shaped curve [40]. This curve gives rise to a bell shaped distribution of adopters that Rogers employs to differentiate between five categories of adopters ranging from "innovators" to "laggards" based on their time taken to adopt the innovation [1]. Thus with the call for standardisation, digital forensic investigators will fall into the different categories of adopters. Creating a new process by which forensic investigations should be conducted adds to a high degree of uncertainty inherent in all forensic investigations. The following sections will discuss the current status of the digital forensic field.

B. Challenges faced by digital investigators

This section will present some of the challenges that forensic investigators encounter. The scope of challenges is wide and varying in difficulty. These challenges can be categorised as follows: Enviromental; Technical Expertise; Regulatory and Procedural.

Enviromental challenges include the increasing number of users of computers amongst other variables. This pervasive nature of information and communication technology has led to an increase in electronic crime [5]. Criminals have therefore become more resourceful in their attempts to lure users into a false sense of security and steal personal information i.e. phishing and pharming, a new crime that has surfaced since the Internet came into being [5].

The technical expertise challenge is that of a skills shortage. E-mail investigations were mainly undertaken by law enforcement agencies; however, in the U.K. a wide variety of organisations have now begun to do so [38]. These organisations have appointed teams with a forensic expert in order to overcome the skills shortage; however the teams are not composed of digital forensic individuals specifically and this poses a problem [38]. The skills shortage is partly due to the fact that computer related crime is still limited to law enforcement agencies and the key to closing the gap lies in building a comprehensive approach to forensic education [41]. Therefore, the enviroment in which evidence recovery is performed is not ideal.

This issue is further compounded, as many organisations underestimate the admissibility and reliability requirements of digital evidence required by the legal system [23]. Thus, the policies and procedures in place are not adequate enough to provide legally admissible evidence in a court of law. This regulatory challenge forms the basis for all digital forensic investigations and hence is the most important challenge. Therefore, a methodology that provides a guide for the investigator must correlate with the law.

In order for evidence to be legally admissible, it needs to be compliant with the applicable legislation. South African law has its origins in Roman Dutch law, founded centuries ago, thereby making it difficult to cope with the advances in technology. Thus, this has constrained traditional methods of investigating and prosecuting crimes [26]. Therefore, there are loopholes in the law for criminals to exploit.

In August 2002, the Electronic Communications and Transactions Act 25 (hereafter referred to as the ECT Act) became law. This law was developed to govern e-commerce in South Africa, and it applies to any form of electronic communication i.e. e-mail, Internet, SMS, etc [29]. One of the primary issues that the Act seeks to address is the illegal activities of cyber criminals. The ECT Act includes the creation of new "Cyber Offences" and creates certain provisions for cyber inspectors [29]. The crux of the Act with regard to e-mails, is to permit electronic documents and e-mails as evidence; however, there is a requirement to show authenticity and integrity of the information [30]. The governance of electronic evidence collection, storage and presentation is lacking [39]. Hence this makes it difficult to produce legally admissible evidence as there is no standardised method of recovering digital evidence.

Another critical challenge that forensic investigators face is that of the forensic tools available at their disposal, which form part of the procedural challenge. These tools have a short life span and as a result they are not able to keep up with current investigations [3]. Tools such as Encase and Forensic Toolkit products have been around for over a decade but have limitations, such as processing speed and software errors [3]. Therefore it is even more difficult to satisfy the authenticity and integrity of information.

A further procedureal challenge is that of the scale of the forensic investigations. The trend has been increasing, from 80 GB in Fiscal Year (FY) 2003 to 250 GB in FY 2006 [14]. The latest statistic showed that 1.756 TB of data was processed for FY 2008 which was a 27% increase from the previous year [15]. The impact of this trend is that it adds to the already complex matter of acquisition and extraction of data sources adding to a list of technical problems [8]. In order for this challenge to be overcome, new tools need to be developed to cope with the demands of the latest investigations. The current tools have the ability to discover all important system files; however, they are in need of attention because they are not guarenteed to recover unreferenced files [2]. Thus, new tools are needed in the field in order to maintain the level of reliability and admissibility that is required in a court of law.

These challenges are not new, although the responsibility is now far greater than that initially placed on the digital forensic investigator. In order to address these challenges, the very nature of digital forensics needs to change. Digital forensic investigators can no longer rely on traditional techniques and methods, but must adapt to the environment in order to be successful in their investigations. This will require the use of innovative methods and cutting edge tools and techniques while remaining within the ambit of the law. Although the law forms the basis of every investigation, it is the responsibilty of the investigator to maintain a carefully documented chain of custody that will allow the use of evidence in a court of law. The procedural challenge is a crucial one, as the tools used are the key to gathering the evidence used in a court of law. The next section will discuss some of the tools and techniques available to the digital forensic investigator.

C. Data mining techniques

Forensic investigators have a myriad of techniques and tools at their disposal to perform the analysis of digital information stored on media. E-mail has become the new form of communication for millions of people and the anonymous nature of e-mail has made authorship identification a problem. It is suggested that while there is no proactive mechanism to protect e-mail, there are however techniques that can be used to determine authorship of e-mails, and one such technique is literary stylometry which is the determination of authorship from writing styles [12] [18]. Table 1 presents some tools and their strenghts and weaknesses.

Corney, Anderson, Mohay and De Val [12] have used stylometry in conjunction with a learning machine technique called Support Vector Machine to determine authorship. However, this approach will not yield admissible evidence in court [12]. Notwithstanding this, a framework was developed using stylometry, to address online messages specifically in order to identify the author of such messages [42]. The process can be divided into four steps: message collection; feature extraction; model generation and finally author identification.

TABLE 1. SUMMARY OF DIGITAL FORENSIC TOOLS

Tool	Strengths	Weaknesses
Support Vector Machine and Stylometry Used to determine authorship of e-mails [12]	• Based on Structural Minimisation principle • Provides a systematic way of determining the relative effectiveness of raw style markers	• Does not yield admissible evidence • More experimentation to determine sensitivity of authors to style markers
Writing-Style Features and Classification Techniques Used to address of online messages and said author [42]	• Experimental approach able to identify author • Structutral and content specific features allow identification of authors • Uses 3 classification techniques • Applied to multiple languages: English and chinese	• Identification of optimal set of features for online messages • More experimentation needed • Validation of proposed technique in the field
Integrated E-mail forensic analysis framework Java based application used to determine authorship of e-mails [20]	• Theoretical foundation based on statistical analysis, text mining and stylometry together with social networking techniques • E-mail geographic localisation – used to localise information relating to suspect e.g. e-mail server	• Level of cohesion of techniques needs to be increased in order to obtain more credible results • Further investigation is prompted for e-mail social networks
AutoMiner Noval data mining technique using frequent patterns and comparing it to write print of an individual [22]	• Unique identifier for authorship identification – namely write print which is dynamically extracted • Accuracy of 86 – 90% • Robust method for determining authorship	• As minimum supported threshold of intervals (features) increase, the accuracy decreases • Manual examination of write prints as many frequent patterns are not obvious
EnCase Enterprise Edition 4.19a designed to integrate with enterprise security architecture, providing enhanced access control and audit functions, and enabling digital investigators to process many systems on a network simultaneously. [10]	• Tool of choice for enterprise investigations • Extracts more data than PDIR • Does not alter data on remote system • Uses System calles SAFE to manage security • Data acquisition of 3.5 MB/s • Gives information about which files are opened • Can integrate with intrusion detction systems	• Data acquisition slow due to SAFE system initailly reading device • Require administrator privalages • Cannot view data on network shares limiting amount of data • Provide most information possible
ProDiscover IR 3.5 designed to examine one system at a time and is useful for focused investigations involving a small number of computers. [10]	• Alters last accessed date/time stamps when performing some processes • Has optional encryption and password protection • Only presents information that is verifiably complete	• Has optional encryption and password protection not enabled by default for servlet • Data acquisition of 5.5MB/s • Require administrator privlages • Cannot view data on network shares limiting amount of data

Hadjidj, et al. [18] have developed a framework based on a combination of established techniques: statistical analysis, text mining and stylometry together with social networking. The authorship attribution occurs in two steps; the first e-mail grouping is conducted using content and stylometry based clustering of the data. The second step is the classification phase which entails feature extraction from the body of the e-mail followed by model generation and application [18].

A C# application to determine authorship of an e-mail with the use of stylometric features was proposed [16]. The program has 3 phases: data collection, feature extraction and classification. Tests performed showed that the application correctly identified 80% of e-mails [16]. Therefore a number of techniques can be used effectively in combination with stylometry.

A novel method of data mining called AutoMiner has been proposed [22] and is an alogorithm which can determine authorship of an e-mail by extracting frequent patterns from the e-mail and comparing it to a write print of a suspected individual. Iqbal, Hadjidj, Fung, and Debbabi [22] point out that they do not claim that the write print can uniquely identify an individual; instead they believe it is accurate enough to to identify an individual from a list of suspects [19]. Hence the use of stylometry in conjunction with other techniques can be useful in the identification of an unknown e-mail author thus strengthening the investigator's case.

The problem that investigators are facing is that with all the information that a computer can store for one e-mail message, they are merely looking for some trace of evidence to indicate authorship [16]. Therefore without techniques such as Autominer, the investigators will have a difficult job to find that evidence.

Many investigators have compiled their own toolbox of executables in order to be prepared for all eventualities [10]; however, the digital forensic investigator needs to be wary of which tools can be applied. Investigators need to consider the tools they use as some tools can alter the state of the system from which evidence is being recovered; often they have to obtain evidence from remote live systems [37] and this increases the complexity of forensic retrieval of evidence.

It is for this reason that Casey and Stanley [10] compare two tools namely ProDiscover IR (PDIR) 3.5 and EnCase Enterprise Edition (EEE) 4.19a. These tools are used for incident response and to preserve evidence on live remote systems. Generally both tools do not alter data on the remote system; however PDIR changes last accessed date/time stamps [10]. There are a range of tools that have been developed for specific tasks [8]. The Forensic Toolkit (FTK) and Encase are two such examples and are commercial digital forensic suites used for the analysis of captured disk images [2]. There are also offline memory and log analysis tools that are used for memory acquisition, such as BodySnatcher [8]. It is therefore

imperative that the appropriate use of these tools is determined by the digital forensic investigator.

Digital forensic tools are not being developed fast enough to keep pace with the variety of forensic targets [10]. Ayers [3] shares this opinion; however they propose a set of requirements for the development for new tools while Arthur and Venter [2] suggests some improvements to tools such as FTK and EnCase and believe that the prosecutions of cyber crimes will increase if the suggestions are researched.

Researchers have performed experiments with the analysis of e-mail data and the most common technique used is that of stylometric analysis albeit in combination with a number of different applications. The tools that are available are varied and some are developed to perform a specific task; however the most popular and widely used tools are the commercial tools such as EnCase and Forensic Toolkit. Now that the tools have been dicussed, it is necessary to discuss the process in which the tools form part, namely the classification models.

D. Classification models

The explosion of growth that technology and in particular the computing world, has resulted in highly sophisticated equipment. This has in essence intensified the criminals' potential to perform criminal activity [32]. In light of this, law enforcement agencies have been busy trying to keep up with the criminal element that is persistent in abusing technology. In order for forensic investigators to perform their job, there are a number of steps that need to be well thought out and dealt with [13]. These steps are encompassed in digital forensic models. Table 2 lists a number of models and their respective processes. This section will describe and compare some of the models.

Forensic investigators follow a generalised methodology when conducting an investigation to ensure credibility and integrity of the digital devices [2]. The methodology followed is a stepwise process and is listed in Table 2. While this method is a sequential and a strict process, it ensures the integrity of evidence. All digital investigators use a variation of this method although the overall method is similar.

Cardwell et al. [6] divide digital forensics into three categories. The first step, litigation support, is the process of identification, collection, organisation and presentation of digital media while the second and third processes deal with the specific types of digital media [6]. Thus, it can be seen that in the first step of this model, the processes 'identification' and 'collection' are similar to Arthur and Venter's [2] 'discover' and 'recover' processes.

Cardwell et al. [6] deal with the methodologies in a practical way i.e. by detailing the steps in the different categories; other methodologies include similar principles. One such methodology is the U.S. Department of Justice Forensics process model. The model consists of four phases and is an abstract model not specific to any technology or methodology and therefore is a generalised process, focusing mainly on core aspects [32]. Hence this model will be more applicable in digital investigations as it can be adapted to the technology under examination.

TABLE 2. MODELS PROCESSES

Classification Model	Processes
Generalised Methodology Arthur & Venter, [2]	• Protect • Discover • Recover • Reveal • Access • Analyse • Print • Provide consultation
Cardwell, et al [6]	• Litigation support • Digital media analysis • Network investigations
U.S. Department of Justice Forensics Cardwell, et al [6]	• Collection • Examination • Analysis • Reporting
Kruse and Heiser's [13]	• Acquiring the evidence • Authenticating the evidence • Analyzing the data
Forza Framework [21]	• 6 questions: What, why, how, who, where, and when. • 8 roles: Case leader; System/business owner; Legal advisor; Security/system architect/auditor; Digital forensics specialist; Digital forensics investigator/system administrator/operator; Digital forensics analyst; Legal prosecutor
Liforac Model [17]	• Laws and regulations • Timeline • Knowledge • Scope
Lee, Palmbach &Miller [11]	• Recognition • Identification • Individualisation • Reconstruction
Casey 2004 [9]	• Recognition • Preservation, collection, documentation • Classification, comparison and individualisation • Reconstruction
The Digital forensic Research Workshop [11]	• Identification • Preservation • Collection • Examination • Analysis • Presentation • Decision
Reith, Carr, & Gunsch [32]	• Identification • Preparation • Approach Strategy • Preservation • Collection • Examination • Analysis • Presentation • Returning Evidence

Kruse and Heiser's methodology includes three components that ensure the integrity of the evidence while investigating [13]. There are a number of frameworks and methodologies that cover the digital forensic investigation differently and the above two are most commonly referred to

in literature, and this adds to the complexity of the digital forensic process [13]. However, Lee, Casey, Reith, Carr, and Gunsch are named as the most frequently quoted authors and their procedures are known to be the 'standard' procedures used during investigations [21]. Therefore, the need for a standardised process has become more evident.

A framework called FORZA (FORensics ZAchman) that links all the common procedures as well as binds eight roles and responsibilities of individuals involved in the investigation process has been presented [21]. It is argued that just as the IT Security field has a set of core values, namely Confidentiality, Integrity and Availability, so too should digital forensics and gives the fundamental principle as Reconnaissance, Reliability and Relevance [21]. The defined roles are combined with the Zachman framework that poses 6 questions: What, why, how, who, where, and when.

There are limitations in the process models [24] and four deficiencies were found at a digital forensic research workshop in 2001; procedural, technical, social and legal [24]. It is the scientific communities' responsibility to standardise procedures and to certify individuals with a formal educational process [28]. Many of the models that currently exist and that are widely used focus on traditional forensic acquisition of data and this is termed Dead Forensic. Grobler and Solms [17] present a South African model for live forensic aquisition called Liforac. The Liforac model is practical and consists of four dimensions based on existing theories [17]. The model is not a set of steps but rather a guideline for investigators; however, the problem of inadmissibility is encountered as many courts do not accept live forensic evidence due to a lack of precedent because of the innovative manner in which criminals exploit new technology [17].

Lee, Palmbach and Miller have proposed a model which consists of four stages which focus on the crime scene and not the entire investigation process and this model does not extend to the electronic crime scene [11]. Therefore this limitation will not allow for the preparation and presentation of evidence. Casey [9] presents a model with four steps that is similar to Lee Palmbach and Miller; but the model is successful when applied to standalone systems and networked environments [11]. During the Digital Forensic Research Workshop (DFRW) in 2001 a linear process model was developed which was driven by academia as opposed to the law enforcement. This is important as there is no standardisation which would need to come from within the scientific community. This model is not a comprehensive one but is the basis for future work [11]. This is an abstract model and is the key for a standardised process to be defined and have proposed a model based on the DFRW model with some additional steps defined [32].

Whilst these models are being proposed and used in the digital forensic field, there is no best practice or standardisation of the procedures followed. Thus, many of the models are guidelines that were developed ad hoc for performing investigations [24] and this therefore highlights the importance of the standardisation of procedures and techniques used. The models discussed all focus on the processing of the digital evidence. However. there is a need to create a standard methodology which will focus on the entire investigation process and the chain of custody. The following section will describe the approach taken in developing the proposed methodology.

III. DESIGN SCIENCE

The study adopts the Design Science research methodology. This study includes empirical research as well as a literature review comprised of secondary data that includes theories, models and frameworks. All attempts will be made to keep the content as current as possible and this will form the theoretical base of the paper.

Design Science is technologically orientated and is essentially a problem solving process that leads to the development of an effective artefact, which is of four types: constructs; methods; models and implementations [27]. Hence this research output will be a methodology that is developed through intensive research. In order to assist understanding, execution and evaluation of Information Systems research a conceptual research framework was proposed [20] and is used to assess what is being produced from each paradigm against each other in the context of business needs. This model, called the Design Science Research Process is used for the production and presentation of Design Science research as seen in Figure 2 [31]. This research falls between the objectives and design phases of the conceptual process.

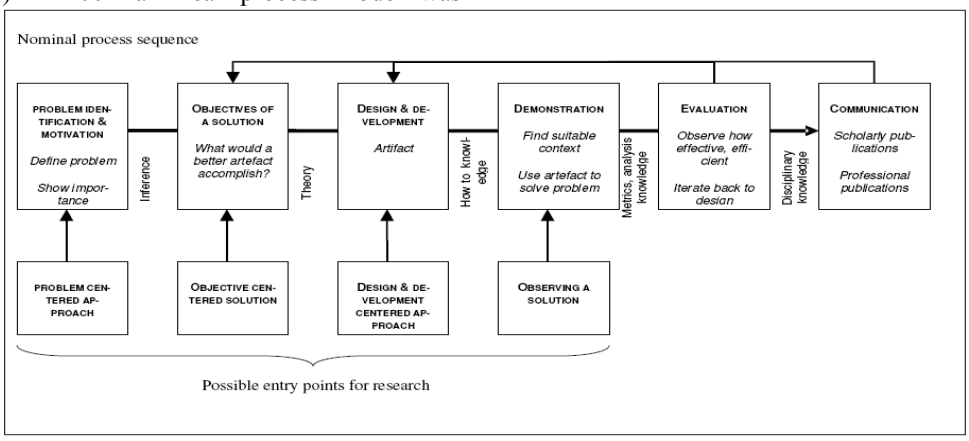
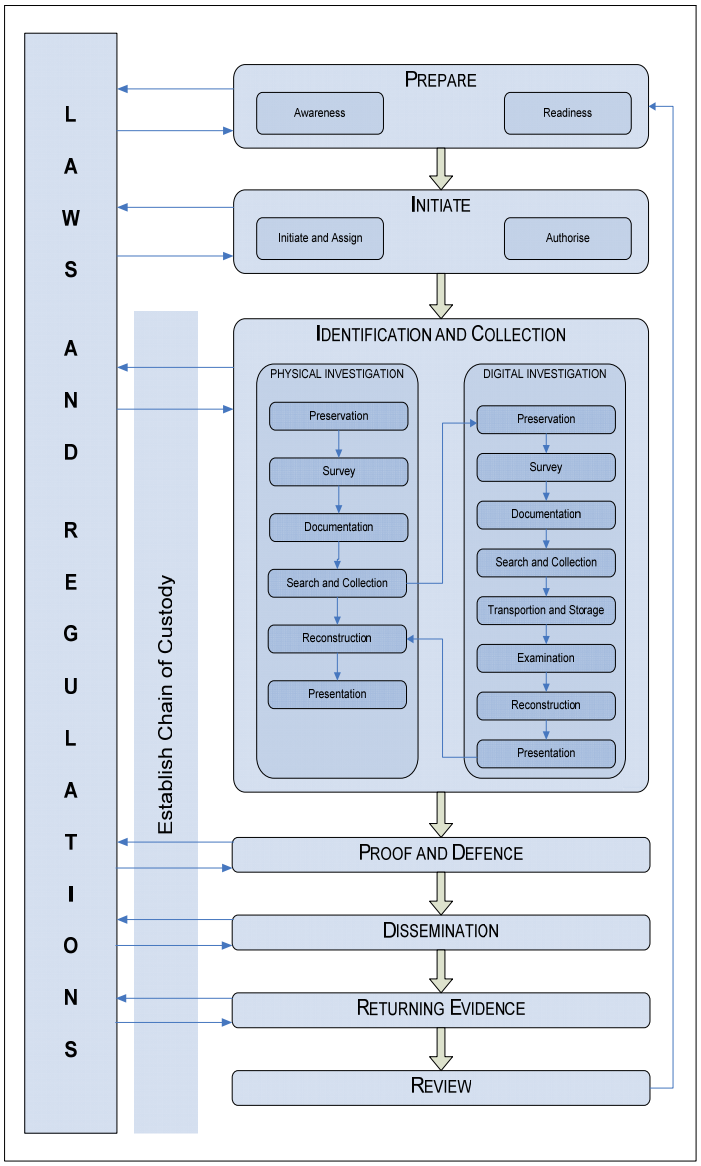


Figure 1. Design Science Research Process. Peffers, *et al.* [31]

IV. PROPOSED METHODOLOGY

In this section the proposed methodology is presented in Figure 2 followed by a discussion.



The first process in the methodology is the Preparation Process. This process contains two elements namely Awareness and Readiness. The organisation must to be aware [11] of the need for an investigation and ensure that the operations and infrastructure can sustain an investigation [4]. In order for an organisation to be aware of the need, there must be a trigger, and this will come from an event/s that has compromised data/information and has violated the law [36]. The aim of this process is to allow the organisation to prepare for a forensic investigation larger than that of an investigation dealing primarily with evidence recovery. The impact the investigation may have on the business processes must be established. This is a risk assessment task performed at business level [34]. Drawing from Rowlingson [34], the goals of a forensic readiness plan should be to:

- Recover legally admissible evidence without interrupting business processes
- Keep the cost of the investigation proportionate to the incident
- Ensure that the evidence makes a positive impact on the outcome of legal action

It is necessary to make these goals a priority. The organisation should be able to practically implement the plan and which should contain activities that are clearly defined [34]. This initial step should be explicit in a forensic methodology because it defines the relationship with the events clearly as it impacts other steps and therefore ensures that the correct approach to the investigation is taken [11]. From the forensic investigator's perspective, this first step corresponds with the preparation of tools needed to perform certain tasks during the investigation [7].

Once the incident has been identified, it is crucial for the organisation to initiate an investigation as soon as possible to minimise its impact. At this point the roles and responsibilities of the forensic team need to be established. Using the FORZA Framework, the eight roles can be specifically listed. These roles are easily identifiable; however accountability is given once the investigation begins. In order for the investigation to begin, the necessary authorisation must be obtained from key individuals within the organisation i.e. the system administrator may only require verbal authorisation from the management whereas law enforcement will need legal authorisation such as warrants [11]. The organisation may also be required to notify individuals and other parties involved in the investigation but this will depend on the scope of the investigation e.g. phone call to local authorities to report that a crime has occurred.

The next process is to Identify and Collect Evidence. There are two sub processes that occur concurrently: the physical crime scene and the digital crime scene investigations. The physical crime scene process deals with the physical aspect of the crime such as evidence that could have been left behind by the suspect relating to the incident identified i.e. flash drives. The goal is to provide a link between the suspect and the incident; the following steps have been identified by Carrier and Spafford [7] and are conducted by the law enforcement crime scene expert. This process contains six phases.

The Preservation phase is the securing of the incident site, which entails closing of exits and restricting access to the scene. The Survey phase occurs when the first responder identifies key pieces of physical evidence that contribute to the hypothesis of what crime has occurred. The Documentation Phase objective is to collect as much information thereby preserving aspects of the crime scene; tasks include photographs and documentation of the crime scene. The Search and Collection phase is an in-depth analysis of the physical crime scene. This includes targeting logs of access to the crime scene and evidence such as the computer. The Reconstruction phase is the process of analysing all the collected evidence and formulating a theory as to the events that transpired that lead to the incident in question. This is where the link between the suspect and the crime scene is made. The Presentation phase is

the final part of the physical investigation as it involves presentation of the evidence to corporate management or a court of law.

The digital crime scene begins during the Search and Collection phase of the physical crime scene and the results feed back into the physical crime scene investigation at the point of the reconstruction phase. The goal of the process is to identify electronic events on the system. This process follows the same six processes of the physical crime scene but it is tailored to the digital crime scene. The Preservation phase is the securing of the incident site, which includes closing off the computer from the network, and maintaining the integrity of log files in the system. During the Survey phase two types of digital evidence are identified: live data and static data. This is done due to the differences in evidence recovery and the impact of the law on the type of data. A live data survey is conducted together with the capturing of images of the digital system. The Documentation Phase is not a specific phase and is performed when the evidence is found but a chain of custody needs to be established early on in the investigation for the evidence is to be used in a court of law.

The Search and Collection phase includes copying of digital evidence and making use of technical and non-technical investigators on hand and the specific tasks that must be performed on the data using standardised and accepted procedures. The next step of Transport and Storage occurs when evidence is transported to a safe place where further analysis is performed. This step ensures the integrity of the evidence and reduces the risk of evidence tampering. The Examination phase is an in-depth analysis of the digital evidence and is the application of digital forensic tools and techniques that are used to gather evidence. The Reconstruction phase uses scientific methods of testing and rejecting theories based on the digital evidence; however, if information is missing the Search phase will commence again. The last step is the Presentation phase where the digital evidence is presented to the physical crime scene investigators.

The next process is Proof and Defence. Opposing theories will also be presented and therefore there is a need to provide substantiated proof of the events that occurred as well as defend the theory of the events that occurred. This is where the benefits of having a standardised digital forensic process enables, either the conviction of a suspect or the exoneration of an innocent individual. The following process of Dissemination involves the sharing of information in order to provide a basis for future investigations i.e. court precedents. Conversely, there are various policies and procedures that need to be followed as prescribed by the organisation and the law in order to share information relating to a crime. The process of Returning Evidence allows the investigation to come full circle in terms of addressing the physical and digital evidence removed for analysis. The evidence must be returned to the proper owners and the criminal evidence must be removed.

The final process is the review phase and is performed after the investigation to determine how effective certain processes and techniques were and whether the digital and physical investigators worked well together. This phase is used to identify areas of improvement and to refine the processes. The objective is to focus on poor practices and errors encountered during the evidence recovery process.

A. Advantages and Disadvantages

1) Advantages

The main advantage is the definition of the processes within the digital forensic investigation in totality, thereby allowing for better prosecution in a court of law. Inclusion of the integrated digital forensics process model has allowed for a greater definition of the forensic investigation. The proposed methodology has included the collection of 'live data' during the digital forensic investigation and therefore has allowed for a greater spectrum of evidence recovery.

2) Disadvantages

As with many of the digital forensic models, the proposed model is an abstract one that is standardised to cater for the broader spectrum of investigations. This does not detract from the value that will be gained using the methodology as covering the steps and processes during an investigation will improve the reliability and admissibility of evidence. The inclusion of live data in the evidence recovery process creates the problem of inadmissibility of evidence as the courts have yet to establish precedent.

V. METHODOLOGY APPLICATION TO E-MAIL FORENSICS

Using a hypothetical scenario of a company whose directors have been sent a threatening and anonymous e-mail one can gauge the novelty that the methodology contributes. If an employee is suspected of sending the e-mail, due to the content of the e-mail i.e. only knowledge certain people would have, the first step is to follow the readiness plan since the company will be aware of the need to investigate. The initiation process will involve the hiring of a forensic investigator if the company does not have the resources in house to deal with such a scenario. The authorisation will come in the form of written or verbal communication to the investigator. During the examination phase, the investigator will need to follow further steps that are specific to e-mails i.e. determine the author of the e-mail, extract evidence supporting the conclusion on authorship. The investigator will identify evidence, such as the actual e-mail message that was sent, word documents, text files etc. Using techniques data mining and date time stamps, the investigator can determine from the list of suspects the computer that was used and this can be seized for further analysis. To further add to the investigators case, the application of techniques such as write-prints and stylometry can be applied to the e-mail and thereby aid in the determination of the author of the e-mail.

VI. CONCLUSION

The aim of this methodology is to provide a standardised process for investigators to follow. As with other models the need to standardise the process is more prevalent as digital investigators use their own version of the models that have been presented. The proposed methodology endeavours to encompass the entire forensic investigation process in order to allow for a stepwise methodology to be developed. The methodology also seeks to improve the admissibility of evidence in a court of law and this has been included in the model with compliance with the law during different processes.

The proposed methodology is comprehensive and outlines the processes that must be followed during an investigation. This adoption of new methodologies can be explained using the Diffusion of Innovation theory. Although the processes are not new, many smaller processes are defined and the adoption of these processes by investigators will vary. Therefore it is necessary to understand the entire investigation process as a whole, which will allow standardisation of the processes. The application of such a methodology needs to be tested with a specific scenario e.g. an e-mail investigation. This is the basis for further work.

REFERENCES

[1] Agarwal, R., Ahuja, M., Carter, P. E., & Gans, M. (1998). Early and Late Adopters of IT Innovations: Extensions to Innovation Diffusion Theory. Proceedings of the DIGIT Conference (pp. 1-18). Florida : Florida State University.

[2] Arthur, K. K., & Venter, H. S. (2004). An Investigation into Computer Forensic Tools. ISSA. Pretoria: Information and Computer Security Architectures (ICSA) Research Group.

[3] Ayers, D. (2009). A second generation computer forensic analysis system. Digital Investigation , 6 (3), 34-42.

[4] Baryamureeba, V., & Tushabe, F. (2004). The Enhanced Digital Investigation Process Model. Institute of Computer Science, Makerere University ??? , 1-9.

[5] Brody, R. G., Mulig, E., & Kimball, V. (2007). Phishing, Pharming and Identity Theft. Academy of Accounting and Financial Studies Journal , 11 (3), 43-56.

[6] Cardwell, K., Clinton, T., Cohen, T., Collins, E., Cornell, J. J., Cross, M., et al. (2007). Best Damn Cybercrime and Digital Forensics book period. United States of America: Syngress Publishing, Inc.

[7] Carrier, B., & Spafford, E. H. (2003). Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence , 2 (2).

[8] Case, A., Cristina, A., Marziale, L., Richard, G. G., & Roussev, V. (2008). FACE: Automated digital evidence discovery and correlation. Digital Investigation , 65-75.

[9] Casey, E. (2004). The need for knowledge sharing and standardization. Digital Investigation , 1-2.

[10] Casey, E., & Stanley, A. (2004). Tool review e remote forensic preservation and examination tools. Digital Investigation , 284-297.

[11] Ciardhuain, S. O. (2004). An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence , 1-22.

[12] Corney, M., Anderson, A., Mohay, G., & De Val, O. (2002). Identifying the Authors of Suspect Email. Computers Security Journal .

[13] Eloff, J., Kohn, M., & Olivier, M. (2006). Framework for a Digital Forensic Investigation. ISSA. University of Pretoria: Information and Computer Security Architectures (ICSA) Research Group.

[14] FBI. (2006, September 30). Retrieved April 15, 2010, from Regional Computer Forensics Laboratory: www.rcfl.gov/Downloads/Documents/RCFL_Nat_Annual06.pdf

[15] FBI. (2008, September 30). Retrieved April 15, 2010, from Regional Computer Forensics Laboratory: www.rcfl.gov/Downloads/Documents/RCFL_Nat_Annual08.pdf

[16] Goodman, R., Hahn, M., Marella, M., Ojar, C., & Wescott, S. (2007, May 4). The Use of Stylometry for Email Author Identification: A Feasibility Study. Proceedings of Student/Faculty Research Day, CSIS, Pace University . White Plains, New York, USA: Pace University.

[17] Grobler, M. M., & Solms, S. H. (2009). Modelling Live Forensic Acquisition. 4th International Workshop on Digital Forensics & Incident Analysis (pp. 8- 15). Athens, Greece: CSIR.

[18] Hadjidj, R., Debbabi, M., Lounis, H., Iqbal, F., Szporer, A., & Benredjem, D. (2009). Towards an Integrated E-mail Forensic Analysis Framework. Digital Investigation , 5 (3-4), 124–137.

[19] Hershkop, S. (2006). Behavior-based Email Analysis with Application to Spam Detection. Columbia : Columbia University.

[20] Hevner, A. R., & March, S. T. (2003). The Information System Research Cycle. MIS Quarterly , 28 (1), 111-113.

[21] Ieong, R. S. (2006). FORZA - Digital forensics investigation framework that incoporate legal issues. Digital Investigation , 3 (1), 29-36.

[22] Iqbal, F., Hadjidj, R., Fung, B. C., & Debbabi, M. (2008). A Novel Approach of Mining Write-Prints for Authorship Attribution in E-mail Forensics. Digital Investigation , 5 (1), 42-51.

[23] Kent, J., & Ghavalas, B. (2005). The unique challenges of collecting corporate evidence. Digital Investigation , 2 (4), 239-243.

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

[25] Lim, M. J.-H. (2008). Computational Intelligence in E-mail Traffic Analysis. Tasmania: University of Tasmania.

[26] Maat, S. M. (2009, August 25). Cyber crime: A comparative law analysis. Retrieved September 23, 2009, from Unisa: http://uir.unisa.ac.za/handle/10500/2056

[27] March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. Decision Supprt Systems , 15 (4), 251-266.

[28] Meyers, M., & Rogers, M. (2004). Computer Forensics: The need for Standardisation and certification. International Journal of Digital Evidence , 1-11.

[29] Michalsons, L. (2005a, June 07). Guide to ECT Act. Retrieved September 16, 2009, from Michalsons Attorneys: www.infoseclaw.co.za/infoseclaw.htm

[30] Michalsons, L. (2005b, June 07). Guide to E-mail Management. Retrieved September 16, 2009, from Michalsons Attorneys: http://www.roylaw.co.za/Uploads/Files/Michalsons%20Infosheet%20-%20Guide%20to%20Email%20Management.pdf

[31] Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., et al. (2006). The Design Science Research Process: A Model for Producing and Presenting Information Systems Research. DESRIST , (pp. 84-106). CA.

[32] Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence , 1 (3), 1-12.

[33] Rogers, E. M., Singhal, A., & Quinlan, M. M. (2007, June 19). Diffusion of Innovations. New York, New York, USA: Free Press.

[34] Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. Internation Journal of Digital Evidence , 2 (3), 1-28.

[35] Ryan, D. J., & Shpantzer, G. (2005, April). Legal Aspects of Digital Forensics. Washington, Washington, D. C, United Stated of America.

[36] Stephenson, P. (2002). The Forensic Investigation Steps. Computer and Fraud Security , 17-19.

[37] Szezynska, M., Huebner, E., Bem, D., & Ruan, C. (2009). Methodology and Tools of IS Audit and Computer Forensics – The Common Denominator. Springer-Verlag Berlin Heidelberg , 110-121.

[38] Taylor, M., Haggerty, J., & Gresty, D. (2009). The legal aspects of corporate e-mail investigations. Computer Law & Security Review , 25 (4), 372–376.

[39] Watney, M. (2009). Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position. Journal of Information, Law & Technology , 1-10.

[40] Wonglimpiyarat, J., & Yuberk, N. (2005). In support of innovation management and Roger's Innovation Diffusion theory. Government Information Quarterly , 22 (3), 411–422.

[41] Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003). Computer Forensics Education. IEEE Computer Society , 15-23.

[42] Zheng, R., Li, J., Chen, H., & Huang, Z. (2006). A Framework for Authorship Identification of Online Messages: Writing-Style Features and Classification Techniques. Journal of the American Society for Information Science and Technology , 57 (3), 378–393