Digital Forensics: the Need for Integration

P. Sant and M. Hewling

Institute for Research in Applicable Computing
University of Bedfordshire, Park Square, Luton, Bedfordshire
LU1 3JU, United Kingdom
e-mail: paul.sant@beds.ac.uk, moniphia.hewling@beds.ac.uk

Abstract

Digital forensics fast is becoming quite predominant within the legal court system which has had to deal with an increase of cases that involve the use of digital devices over the past decade. The procedures presently used in the digital forensic process were developed with a focus on the practitioner's expertise or interest. This resulted in very little regard for all fields that may be impacted by any one investigation. Such omissions have resulted in digital forensics seeming to be an ad hoc process resulting in a number of cases in which digital evidence has been deemed invalid, producing negative results. Alleviation of such issues is possible with the development of a standard framework flexible enough to accommodate the intricacies of all areas directly impacted by digital forensics. A complete framework incorporating views from computer scientists, lawyers, law enforcement officers and all other practitioners in related the field, needs to be developed. Such a framework should provide the basis from which a set of standards will be generated, defined and used to govern the acquisition of evidence from digital devices/sources, irrespective of their use in or to inform they will be used in a legal case. This paper proposes the development of such a framework integrating technical and legal dimensions.

Keywords

Digital Forensics, Computer Forensics, Digital Evidence, Digital Crime

1. Introduction

The apparent proliferation of digitally related crimes has been immense and is unavoidable in today's' technologically driven society. Increased connectivity has significantly increased the number of security related issues occurring and will continue to so do because of the dynamic nature of digital technology. In recent years there has been an increase in the use of digital devices as tools of convenience to access the World Wide Web to carry out activities such as banking, gaming, shopping and even studying. These activities have given rise to a number of security issues due to the fact that criminals have found a way to infiltrate their use. Additionally technology and digital devices facilitate these criminals by enabling more sophisticated methods of committing traditional crimes with a certain level of perceived invisibility. These developments have thus prompted the rise of fields such as Digital, computer, mobile, network and cyber forensics as well as cyber/internet, computer laws.

Digital forensics refers to the acquisition, preservation, analysis and presentation of digital evidence produced from the investigation of digital related crimes. Digital evidence recovered from the scenes of digital crimes are defined by Casey (2004) as "any data stored or transmitted using a computer that support or refute a theory of how an offence occurred or that address critical elements of evidence such as alibi". The basis of the investigation of any technological/digital related criminal act is reliant on digital evidence, which as alluded to before, is acquired through the digital forensics process. The definition or description of this process may vary depending on the expertise of the investigator or their background. This highlights one of the main issues in the field - the lack of a standard set of methodologies to carry out the digital forensics process.

The term 'forensics' refers to the application of science expertise in the form of knowledgebase and methodology within the court. This means that where evidence is gathered, the objective is for it to be used in legal proceedings. To ensure evidence is considered reliable when presented in courts, proper standards and procedures must be followed. This requirement is no different in the case of evidence acquired through all forensics fields and so it is for digital forensics The weaknesses identified above demonstrate the need for a comprehensive methodology that covers the multidimensional landscape of digital evidence. The remainder of this paper will address the limitations of existing approaches and propose a new framework that addresses the problems associated with existing models. The research commences by discussing the related work by researchers in the field and then goes on to explain the proposed approach. Section 2 will look at the aforementioned related work of other researchers, section 3 summarises the strengths and limitations of some of the existing models. The suggested framework will be highlighted in section 4 and the conclusion, in section five, present proposals for future work.

2. Related work

There are a myriad of existing digital forensic models some of which have been developed by organisations for their own use, or by law enforcement personnel for their own countries and even by other individuals based on their background, objective and even their employers' needs (Salemat et al 2008) and (Perumal 2009). These methodologies are in some part driven by the tools available to the investigator and focus on either the technical or legal aspects of the investigation. However, there are other models that focus solely on the acquisition of the evidence ignoring all other phases that may be required by a "forensic" investigation. These models all have positive and negative attributes most of which will be highlighted in this section.

2.1. Pollit et al. methodology

One of the earlier models to be developed was the Computer Forensics Process by Pollitt (1995). This model is comprised of four stages and stresses the point that the digital forensics process should conform to the law while remaining committed to the scientific principles. This model was however designed with the object of acquiring evidence from crimes committed in cyberspace and thus would need to be amended by the practitioner for use in other settings requiring such an acquisition.

2.2. Kruse & Heiser's methodology

Kruse and Heiser (2001) was also one of the earlier models to be developed, though coming approximately six year after Pollitt's. This model has three basic steps depicting the entire digital forensics process. The focus of this particular model is on the core aspects of digital evidence acquisition, acquiring, authenticating and analyzing the evidence. There is no mention of preparation, seeking authorization to acquire the evidence or identifying the evidence. Whereas these may have been assumed, as it seems with other models, to be discussed this is not enough especially where the legal issues are concerned.

2.3. H.C. Lee's methodology

Also in 2001 H. C. Lee in his book 'Henry Lee's Crime Scene handbook' suggested a model that included an additional stage when compared to that of Kruse and Heiser. This model is more systematic and follows four very pertinent stages, which are recognition, identification, individualization and reconstruction. This model is similar to the previous methodology proposed by Kruse and Heiser in that it assumes/ignores particular phases of the forensics process and does not include stages suggesting preservation or that of seeking authorization to access the evidence. This model focuses mainly on the analysis of the evidence.

2.4. The DFRWS methodology

The Digital Forensic research workshop (DFRWS) has also developed a model for the Digital Forensic process. This model is more extensive than the previous models highlighted. It has seven stages and makes far fewer assumptions than the previous models covering integral stages not previously covered. However like a number of the other models, it ignores or assumes some of the legal aspects of the investigation and focuses more on the technical aspects. It includes the stage "decision" which is somewhat out of the remit of the forensics process, which is concerned mainly with investigation and presentation of the findings.

2.5. Reith et al.

In 2002, Reith, Carr and Gunsch proposed a model that had a number of phases in which at least two phases overlap. This model is based on the one developed by DFRWS previously (DRFWS, 2002). The phases proposed include identify, prepare, approach strategy, preserve, collect, examine, analyse, present and return evidence. This model, despite addressing some of the core areas of forensics, such as it does not include any suggestion of getting authorisation to preserve and /or collect the evidence, which is very important with regards to the legal aspects of any forensics process.

2.6. Eoghan Casey's Methodology

Eoghan Casey (2004) proposes one of the more popular models as depicted in his book 'Digital Evidence and Computer Crime'. In this model Casey focuses on the investigation itself and presents only four stages that are recognition, preservation, classification and reconstruction. This model focuses main on the investigation of the device itself and like many of the other models ignores other elements such as the legal ones.

2.7. Ciarhuain's methodology

The Ciarhuain Model is one of the more comprehensive models developed and has approximately twelve (12) stages and sub stages. This model, unlike the others, does specify phases pertinent to a digital forensics investigation but has been developed to address cyber related crimes (cyber forensics) and developed specifically for the Malaysian context. A number of the stages are also redundant and the need for preservation of the acquired evidence is not mentioned which is integral in ensuring the admissibility of the evidence should it be required for use in court.

2.8. Bogen and Dampier's methodology

The model by Bogen and Dampier was developed in 2005 and has three distinct phases and is referred to as a multi-view computer forensics model. The views are investigative process view, domain View and evidence view. Each view has related products Including models and dependencies. This approach is quite different from the others identified and does not directly build or expand on a preceding model. It was designed from a software engineering standpoint and is thus focussed on the technical aspects of the digital forensics process.

2.9. Yong's methodology

Another model to be mentioned is Yong's, in 2008, has network forensics at its core and is not openly general, though it could possibly be adapted. Yong's model focuses on the investigation of cyber crimes and includes phases such as preparation, classification of the cybercrime, deciding investigation priority among others. It takes the investigator through summoning the suspect (which is not a core responsibility of a forensic expert) to writing the report. A comprehensive set of steps presented for investigation cyber crime however very little explanation is provided.

2.10. The Salemat and Perumal methodologies

Two of the more recent models Salemat et al (2008) and Perumal (2009) are the more comprehensive of the existing models. In an article entitled "The Mapping process of Digital forensics Investigations" (Salemat (2008), Salemat et al noted, "No formal theory exists for the digital examinations process". This is a point supported by Perumal (2009), Ricci (2006), among others. Salemat et al then proceed to produce what they term the "mapping process of the digital forensics investigations framework". The output of this process is a combination of the previous frameworks eliminating redundancies and detailed explanations of particular steps that were deemed vague. This has resulted in a five-phase step of activities with the headings, preparation, collection and preservation, examination and analysis, presentation and reporting. This structure of activities is written specifically for the Malaysian Criminal Justice system. It is very comprehensive and addresses key areas such authorization (but not continuous legal adherence or ethics), live and static data acquisition for use as evidence (not filtering of pertinent/relevant evidence) and storage of data. Overall Salemat's model is a very comprehensive methodology; however the focus seems to be on data acquisition as there is no mention of presentation which is critical part of any forensics process as one of the objectives of forensics is to present the findings of the investigation.

3. Strengths and weaknesses of Digital Forensics Models

Model/Designer	Year	Strengths (Includes)	Weaknesses (Excludes)
M. Pollitt	1995	Identification	Authorisation Live acquisition
W Kruse II., G Hieser	2001	Authentication	Authorisation Live acquisition
H. Lee	2001	Identification Reconstruction	Preservation Authorisation Presentation Moving of evidence to controlled area.
M. Reith, C. Carr, G. Gunsh	2002	Identification	Authorisation Live acquisition Moving of evidence to controlled area.
E. Casey	2004	Identification Reconstruction	Focus is on the investigation Authorisation Moving of evidence to controlled area.
S. O. Cuardhuian	2004	Awareness	Preservation Cybercrime Focus Overlapping of steps Live acquisition
C. Bogen & D. Dampier	2005	Includes various digital devices	Technical Oriented
FORZA – R. Ieong	2006	Legal inclusion	Focuses on legal aspects
Y.D. Shin	2008	Criminal profiling Classification of crime	Legal aspects
S. Perumal	2009	Archiving	Classification of crime

Table 1: Strengths and weaknesses of digital forensic models

3.1. Concerns

Some of the major concerns arising from examination of the models identified include:

a) Lack of legal authorisation to acquire and examine the evidence.
b) The need for preservation of all evidence immediately
c) The identification of the fact that a controlled environment is needed to carry out the investigation.
d) A step-by-step directive that can be followed by practitioners (usually provided with the tools but not good enough as the instructions are dependent on the developer of the tool).
e) Not having any particular tools identified to be used at the different stages. The methodology was written in isolation, separate from the tools. (NB Carrier has addressed this concern somewhat with sleuth kit)
f) Reconstruction of the crime scene to enable accurate criminal profiling is not addressed by most of these methodologies
g) Computer Scientists for some reason are intent on ignoring the legal aspects of "forensics".
h) Both live and static data needs to be captured in digital forensics.
i) Creation of logs to ensure proper presentation of the findings.
j) Lacks the identification of human resources training requirements

4. The Proposed Framework

4.1. Introduction

It is clear that for digital forensics to be recognised as a true division of the forensic science arena the evidence gathered through the process must be able to satisfy the Daubert testing criteria (among others). This becomes difficult with different personnel and organisations developing their own methodologies. Thus there needs to be standardised framework complete with a set of standards and a dedicated but flexible methodology which digital forensics practitioners, internationally, will use as a bench mark when carrying out their duties. This framework must not only satisfy technical and legal criteria but also adhere to ethical expectations, education and be flexible enough to meet the needs of a dynamic field. The proposed framework is flexible enough to be adapted for the various divisions in digital forensics for example, Mobile forensics, network forensics, cloud forensics and computer forensics

The proposed framework has three major phases that will be further broken down in to more specific categories. This proposed framework is designed to be prescriptive and rigorous while ensuring speed and accuracy. It is prescriptive because it includes recommendations of tools at particular stages in the process and is guided by standards. It is rigorous because it is expected that no phase will be excluded throughout the investigation. This measure ensures the model is accurate and reliable from a legal and scientific perspective and adaptable for any region.

4.2. Layout of the Framework

Educational training and qualification along with legal and ethical principles encompass the framework. These are addressed by the associated standards. From this framework the proposed methodology will be derived. The initial phase of the proposed methodology, the initiation phase comprises of those tasks involved in ensuring that all necessary actions are carried out and appropriate documentation produced before commencement of the actual investigation. Information ascertained at this phase includes, type of service required by the requester, type of intrusion, personnel involved in the intrusion and data type involved. From this stage is apparent what type of authorisation is needed to commence the investigation. The deliverable form this phase of the process is a formal document containing the results of the aforementioned information as well as documentation of any legal documents requested and/or received.

The investigation phase is very complex and critical to the overall process. During this phase the practitioner must be constantly aware of the fact that they are collecting evidence that may be used in a legal setting and thus "rules of evidence" will determine the admissibility of the evidence acquired. This stage needs to be carefully planned and coordinated to ensure that there is no spoliation of the evidence. Specific guidelines will be included to ensure this is alleviated. The investigation phase involves activities ranging from the locating of the devices involved in the incident through to the analysis of data pertinent to the investigation. On locating these devices the immediate environment should be physically preserved and protected. The scene should be diagrammatically captured with the use of drawings and/or photographs showing location of the devices. The investigation should then identify suspect devices and peripherals and proceed to preserve any live data. Another critical stage in this phase is the removal of devices to a controlled environment for analysis. Careful care and planning must be in place to ensure that the various laws are strictly adhered to. Once in the controlled area preservation and analysis of the data will proceed. Throughout this stage a standard code of ethics should be adhered to and there should be constant communication with all stakeholders.

The forensics process suggests application law and thus the practitioner must not only be aware but appropriately trained to produce a written and formal report. The final phase of this framework will focus on the production of report on the overall process specifying outputs from the previous phases. This phase will encompass much more than writing a formal report on the findings and should be relevant to apprehending a suspect. This phase will include the inventory of all items seized and/or analysed during the previous phases. All equipment and forensic tools used throughout the investigation will also be formally recorded. The methodology employed throughout the investigation as derived from the framework will have met the Daubert Standard. Other integral parts of the reporting phase include the virtual reconstruction of the crime scene and the creation of an attacker profile. These done in conjunction with the legal requirements will enable the production of a more detailed and relevant report that will positively support an expert witness in court.

4.3. Overview of the proposed framework

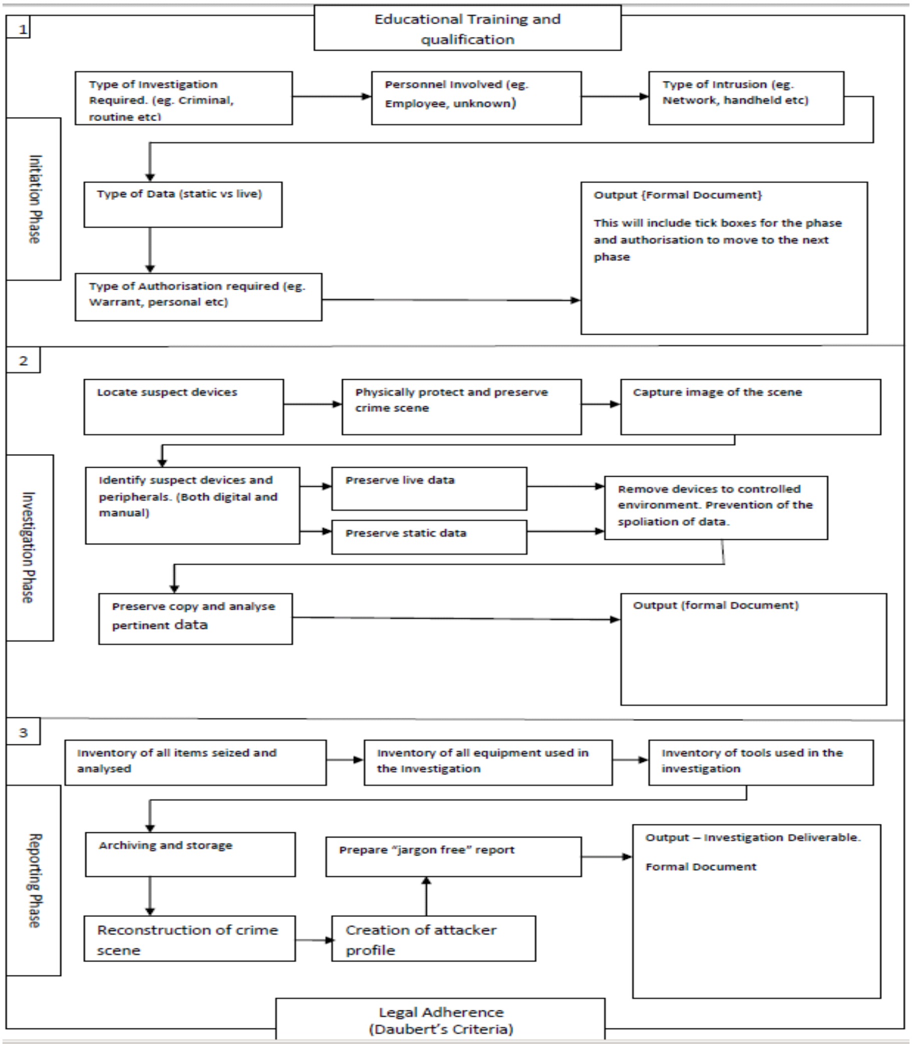
Educational Training and qualification
1
Initiation Phase
Type of Investigation Required. (eg. Criminal, routine etc)
Personnel Involved (eg. Employee, unknown)
Type of Intrusion (eg. Network, handheld etc)
Type of Data (static vs live)
Output (Formal Document)
This will include tick boxes for the phase and authorisation to move to the next phase
Type of Authorisation required (eg. Warrant, personal etc)
2
Investigation Phase
Locate suspect devices
Physically protect and preserve crime scene
Capture image of the scene
Identify suspect devices and peripherals. (Both digital and manual)
Preserve live data
Preserve static data
Remove devices to controlled environment. Prevention of the spoliation of data.
Preserve copy and analyse pertinent data
Output (formal Document)
3
Reporting Phase
Inventory of all items seized and analysed
Inventory of all equipment used in the Investigation
Inventory of tools used in the investigation
Archiving and storage
Prepare "jargon free" report
Output – Investigation Deliverable.
Formal Document
Reconstruction of crime scene
Creation of attacker profile
Legal Adherence (Daubert's Criteria)

Figure 1: Proposed framework

4.4. Daubert's test

The mere number of models/methodologies identified in this paper suggest that there is very little or no formalization in the Digital Forensics Field. This present a huge problem for the development of Digital Forensics as a forensic science and digital evidence presented in courts are quite likely to fail the Daubert's test. Daubert's test is used to check whether or not forensic evidence presented in courts is sound. The Daubert's test is a legal standard used in courts to authenticate the statements of testifying experts. It refers directly to the methods used to acquire evidence in the various forensics fields. It seeks to ascertain whether the evidence/testimony being given is relevant, seeking to answer questions such as- was the data gathered using scientific methods and procedures, is the evidence based on mere assumptions or from a comprehensive knowledge base. It also seeks to ascertain whether the evidence being given is reliable, finding out if the practitioners is authorised, qualified and /or experienced in the particular field. The major questions comprising the Daubert's test include:

I. Has was the theory used been tested?
II. Has the theory been peer reviewed (less chance of error)?
III. What is the reliability/error rate of this particular theory?
IV. What is the extent of general acceptance by the scientific community?
V. Are there standards and controls in place governing its operation?

5. Conclusion

A standardized methodology (way of working) will be of benefit to all involved in the world of digital forensics. The definition of a framework that includes all aspects and core fields that are involved in the digital forensics process will help to alleviate some of the issues that exist within the discipline at present. It has been identified that although several subject areas are impacting on the field there is no collaborative and integrated approach. Digital forensics is a wide area and thus all professionals that are impacted must be able to communicate eliminating "area specific" jargon and assumptions that one field is more important than the other. Computer Scientists must accept that to be digital forensics practitioners they must become knowledgeable of the different laws that are related to the field. Legal experts must accept that digital forensics is more than just using a particular tool and become knowledgeable of the digital forensics field. Law enforcement officers must be cognisant of both of the above. Organisations must be made to realise though they may "forensics ready" (if there is such a term) and have various security personnel in place within the organisation it is not enough to use the Information technology department/technician to investigate a digital crime. The work proposed addresses these issues and lays the foundations of a framework that will accurately and rigorously address the multidimensional nature of digital forensics.

Digital forensics is a dynamic field that is currently faced with a number of issues. This study aims to highlight some of these issues and develop amicable solutions. The field of digital forensics encompasses various fields and criteria that must be satisfied before any evidence acquired can be accepted in a court. Facets include investigative, technical, ethical and legal. The digital forensic investigator must to ensure that at all times all aspects of the job are considered because ignoring any one area can impact significantly the outcome of an investigation. For example the main objective of a digital forensic investigation is to collect, analyze and preserve digital evidence that may be used in a legal case thus ignorance of any of the laws regarding the information technology/computer field can significantly impact on the case.

Whereas there has been some increase in research with regards to the digital forensics field there is still much more to be done. In his article Digital forensics research: The next 10 years Simon Garfinkel states simply, 'There is no standard set of tools or procedure" just 2 things that still need researching (Garfinkel, 2010). Two main areas are identified that need further research: i) the legal issues as they relate to digital forensic and ii) the evidence acquired and the issue of a methodology governed by a set of standards that may be used internationally by digital forensic investigators. Having a methodology governed by a set of standards will also help in satisfactory responses to the questions posed by the Daubert's test. The proposed framework addresses these key issues as well as the incorporation of the reconstruction of the crime scene and creation of an attacker profile. While this presents more assurance in digital evidence acquired through the digital forensics process being acceptable in courts internationally it also promotes the apprehension of the unknown attacker/s in digital related crimes.

6. References

Brill, A. Pollitt, M. (2006) T*he evolution of Computer Forensics Best practices, An Update on Programs and Publications.* Journal of Digital Forensic Practice 2006; 1:3-11. Available from http://www.informatik.uni-trier.de/~ley/db/journals/jdfp/jdfp1.html#BrillPW06

Carrier B. D., (2003) Open Source Computer Forensic Manual. Available from: http://www.digital-evidence.org/

Casey, E. (2004). *Digital Evidence and Computer Crime, Forensic science, Computers and the Internet*. Academic Press, London, UK

Cuardhuain S. O., (2004) An Extended Model of Cyber Crime Investigation. Journal of Digital Evidence. Vol. 3. Issue 1

Garfinkel S., (2010) *Digital forensics research: The next 10 years. Digital Investigations 7.* 2010 S64-S73. Available from www.sciencedirect.com Accessed on August 20, 2010

Ricci I. S. C. (2006) *Digital Forensics Framework that incorporate legal issues*. Available from www.sciencedirect.com Accessed on October 20, 2010

Kruse W. Heiser J. G. (2001). Computer Forensics: Incident Response Essentials (1st ed.), Addison Wesley Professional. USA

Lee H, C., Palmbeach T. M., Miller M. T. (2001*) Henry Lee's crime scene handbook.*

Elsevier Academic Press Available from: http://academic.evergreen.edu/curricular/social_dilemmas/fall/Readings/Week_06/Crime%20Scene%20Handbook.pdf

Meyers M., Rogers M. (2004) 'Computer Forensics: The need for standardization and Certification'*, International Journal of Digital Evidence*, Vol. 3, issue 2. Available from www.ijde.org

Pollitt M., (1995) *Principles, Practices, and Procedures: An approach to standards in computer forensics.* Available from; www.digitalevidencepro.com/resources/principles.pdf

Perumal S., (2009) Digital Forensics Model Based on Malaysian Investigation Process, IJCSNS Vol. 9 No. 8 Available from www.sciencedirect.com

Ricci I. S. C. (2006) *Digital Forensics Framework that incorporate legal issues*. Available from www.sciencedirect.com Accessed on October 20, 2010

Salemat S. R. Yusof R. Sahib S. (2008) *Mapping Process of Digital Forensic Investigation Framework.* International Journal of Computer Science and Network Security Vol. 8 NO 10 Available from www.sciencedirect.com