MULTIDISCIPLINARY E-FORENSICS METHODOLOGY DEVELOPMENT TO ASSIST IN THE INVESTIGATION OF E-CRIME

AMY TENNYENHUIS and RODGER JAMIESON
SEAR – Security E-Business Assurance Research Group, School of Information Systems Technology and Management, University of New South Wales, Australia

Abstract: E-Crime in e-business is rising at an ever increasing rate with nations positioning themselves through alliances to fight this threat - evidenced by thirty countries recently signing a new cyber crime treaty. In order to combat this threat, law enforcement and other government and private organisations are turning to computer forensics, which is a new field that deals with investigating computer-related crimes. This paper describes the identification of research issues for methodology development via a Delphi study and the development of a standard methodology for computer forensics to assist in the investigation of e-Crime by use of semi-structured questionnaires and interviews.

1. INTRODUCTION

E-Crime in e-business is rising at an ever increasing rate (CSI, 2001) with nations positioning themselves through alliances to fight this threat evidenced by thirty countries signing a new cybercrime treaty (IDG News Service 23 Nov 2001). E-Crime has increased the exposure to e-business and has strengthed the resolve of organisations to increase security and control of their e-commerce applications (Cerpa & Jamieson, 2001). In order to combat this threat, law enforcement and other government and private organisations are turning to computer forensics, which is a new field that deals with investigating computer-related crimes. Computer forensics, also referred to as electronic discovery, electronic evidence discovery, computer forensic analysis, digital discovery, computer examination and computer analysis, is

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35692-1_36

K. V. Andersen et al. (eds.), *Seeking Success in E-Business*

the process of methodically examining computer systems, computer networks, computer media and peripherals for evidence (Rehman, 2000).

The Commissioners of Police of Australasia have recognised that unless law enforcement acts quickly, society could be seriously affected by unchecked electronic crime (Virtual Horizons - ACPR, 2000). It is therefore important to have a standard methodology developed to ensure proper procedures are followed so that these e-crimes can be detected, evidence adequately collected and presented in a court of law so that the perpetrators of e-crime can be brought to justice.

In Australia there is currently no standard methodology in place for computer forensic investigation and analysis. This is due to the many variables that affect the way a computer forensic investigation takes place, for example, the operating system, software applications, hardware platforms, legal system, and international boundaries (Rude, 2000). As such, many methodologies have been developed that take into consideration each of these factors, and the addition problem that digital evidence is hard to present as evidence in court or show the jury due its digital form. Despite their differences, it is important to understand the need for a standard computer forensic methodology and the factors influencing its development. A methodology is required as it establishes a protocol by which electronic evidence (physical and logical) is gathered and handled, to reduce the potential for this evidence to be corrupted or tainted.

This paper will discuss the research issues associated with and the structure and development of computer forensic methodologies. First the objectives of the research are set out followed by the theoretical foundation to the research. Secondly, the research methods are outlined together with the research results and progress to date.

2. RESEARCH OBJECTIVES

The aim of this research is to investigate and develop a framework for the development of a standard for computer forensic methodologies. The research aim may be broken down into related research objectives:

Identifying issues related to computer forensics methodologies from a multidisciplinary perspective;

- Investigating and developing a framework for a computer forensic methodology standard; and
- Investigating and documenting the skills and competencies required by a CFA to conduct a computer forensic examination (this last objective is outside the scope of this paper).

The result of this study should provide a list of competency variables from which a standard can be devised. Additionally, for methodologies, a list of the main steps in the process, the main functions, rules and guidelines and the main quality control specifications will be devised.

This research will have a number of outcomes:

- A validated normative computer forensic model developed from the literature;
- A high-level computer forensic methodology framework, consisting of major phases, steps, guiding principles and documentary requirements. Sound computer forensic methodologies can then be developed using this framework;
- A list of skills, knowledge, qualifications and experience that a computer forensic analyst must posses. This will form the basis for a competency standard;
- A taxonomy of emerging issues that have been rated and ranked by experts in the field; and
- Contacts and ongoing research between the University and the Australian Computer Crime Managers Group, in the form of a sub-group called the Computer Forensic Research Group. This joint research has been ratified by Australian Police Commissioners.

3. THEORETICAL FOUNDATION

3.1 Background

There has been a call for the development of best practices and standards in the computer forensic field. The Virtual Horizons paper (Virtual Horizons - ACPR, 2000) developed by the Australian Centre for Police Research has outlined world wide strategies for combating computer crime. One of the main associations dealing with international computer crime, the Association of Chief Police Officers Computer Crime Working Group have stated in a memorandum that 'forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed' (ACPO). Additionally, the International Hi-Tech Crime Forensics Conference and Workshops (IHCFC) held in London 1999, recommended that principles for evidence handling should be developed, an accreditation device should be provided, and the term 'forensically competent' should be defined (ACPO). Interpol has developed a Computer Crime manual which includes flowcharts to aid complicated investigations.

The G8 summit held in 1997 included as part of a Statement of Principles concerning computer crime that law enforcement personnel must be trained and equipped to address high-tech crimes and forensic standards for retrieving and authenticating electronic data to be used in criminal investigations and prosecutions must be developed and employed (Virtual Horizons - ACPR, 2000). The UK National Criminal Intelligence Service has recognised the importance of partnerships and international cooperation in terms of standardisation of investigative and forensic techniques (Virtual Horizons - ACPR, 2000).

In Australia, a study done by Wieszyk (1998a) found that only three out of eight police departments has guidelines for search and seizure. The Wieszyk report recommended that 'guidelines for the collection, analysis and presentation of computer evidence be developed to an Australian law enforcement standard and investigators be made aware of these guidelines'. The result of this has prompted may institutions in Australia to undertake studies to develop procedures and training for investigations. The Victoria Police Computer Crime Investigation Squad (CCIS) has included in its list of current e-crime objectives to 'develop computer crime investigation and computer evidence handling procedures and practices throughout the force, provide a force-wide field response capability for computer search and seizure operations; and to develop and manage internet investigations procedures and practices' (Virtual Horizons - ACPR, 2000).

The National Office for the Information Economy (NOIE) and the Action Group into the Law Enforcement Implications of Electronic Commerce (AGEC) have been researching into creating standards for computer forensics. Similarly the Australasian Computer Crime Program (ACCP) established the Computer Investigation techniques (CIT) program whose objectives were to 'establish links with national and international agencies/individuals in the area; identify, acquire and develop investigative tools; disseminate tools and information; and develop and provide a training regime for police investigators' (Virtual Horizons - ACPR, 2000).

As it can be seen there have been a number of national and international strategies for combating electronic crime.

3.2 Need for Methodologies

Many influences and success factors (Tennyenhuis and Jamieson, 2001) highlight the need for any methodology to be independent of the low-level details such as specific tools and methods to be used. As such, a computer forensic methodology can be broken down into logical layers. Computer forensics encompasses four functional areas: identification, preservation, analysis and presentation of digital evidence. At a high level these areas and corresponding principles form the basis for any computer forensics methodology. Due to the complexity of the computer forensic investigative process any methodology should include high-level steps, principles of examination, and standard operating procedures (SOP's). SOP's are guidelines how to go about analysing digital evidence at the process level. For example, part of the standard operating procedure could include details on how to backup a piece of media without specifying the software or the media.

By viewing the process as a three-levelled model the methodology is more flexible, as each layer is independent of the layer below. This means that the top two layers are independent of the many factors that make the computer forensics field dynamic such as changing technology and diverse software and evidence. The highest level should include the basic phases involved in the methodology as discussed above. The second level should comprise of a set of principles, which are structural guidelines that apply to forensic examinations (FBI, 2000a, FBI 2000b)

For example, the high level 'analysis' phase can be approached three different ways: Applications approach, modified operating system approach and black box approach (McKemmish, 1998).These methods are highly dependant on the tools and the operating environment. Details of these approaches should be documented at the lowest level of the methodology. Due to privacy reasons, law enforcement often do not want to divulge the tools and techniques they use at the lower layer. Using this model, it is possible for the law enforcement to follow the public methodology and then devise their own lower layer as long as it conforms to the principles set out in the second layer. This model allows us to understand the concept of the different layers of complexity and detail in a methodology. The flexibility is increased by the independence between the layers of the methodology as shown in this model. The first two levels will always be applicable as they are independent of tools and media.

After this initial understanding of what influences the structure and development of many of today's computer forensic methodologies, existing methodologies will be examined to determine their strengths and weaknesses.

3.3 Existing Methodologies

Throughout the world there is no standard methodology but rather a whole set of different methodologies devised by different specialists and organisations. The issue has been raised as to whether it is valid to produce a world standard for computer forensic methodologies (CRFG, 2001). In reality, a high level framework for developing computer forensic methodologies would be beneficial world wide. The majority of these methodologies differ only in terms and minor details. The major steps in each methodology are similar. Therefore, it would not be of much use to go through each methodology in turn and highlight the major phases, principles and techniques. Instead this paper will provide a view of existing methodologies by highlighting common steps and suggested rules and guidelines (in the next section) that are common to the documented methodologies of today.

There are six phases in the standard computer forensic methodology: preparation, identification, preservation, analysis, presentation and documentation, which are discussed below:

Preparation - The preparation stage involves preparing the personnel, materials and tools required for the investigation. During this stage the paperwork is prepared for the investigation and details are distributed to the personnel working on the case. The specialists are made aware (if they do not already know) of the various different forms of evidence that may be at the crime scene when they arrive. A preliminary plan is drawn which details what each specialist will be doing once they arrive at the scene, and the order in which each type of evidence is to be collected.

Identification - On arrival the team must approach and secure the crime scene. This involves protecting the crime scene from unauthorised personnel, determining whether to disconnect computers from remote access such as telephone lines, and determining whether to unplug machines from network access.

After the scene is secured, all computers, devices and all other aspects of the crime scene are documented. All evidence is identified, photographed, documented and tagged. This involves determining what evidence is present, where it is stored, in what format and determining what tools and procedures are required to facilitate the recovery of the evidence. (AIC, 1999). Documentation is especially important at this stage as it provides support for any accusations of negligence or charges that the investigator knowingly tried to hide evidence.

Preservation - Once the location and state of all evidence has been documented it should be backed up, protected and preserved so that no damage can be done.

All procedures performed on the evidence should be documented in the evidence log, which should detail the original state of the evidence, the procedure performed, the time it was performed and the investigator who performed the procedure. This evidence log is especially important as it will help to show that continuity of evidence was maintained. Continuity of evidence is a means of accounting for every move and change to the evidence including who touched it, when, why and for how long. Not maintaining continuity of evidence can quickly render evidence inadmissible in court as "Failure to substantiate the evidence's chain of custody may lead to serious questions regarding the authenticity and integrity of the evidence and the examinations rendered upon it" (Saferstein, 1998, 48).

Analysis - Once the evidence has been identified and secured, the search, recovery and analysis of the digital evidence is performed. This involves the extraction, processing and interpretation of the digital data. A plan should be devised describing the approach to be taken in analysing the evidence. This is particularly important as different types of digital evidence and media have different levels of volatility. Once all evidence has been found it should then be copied and analysed. This may involve searching for and retrieving deleted files, running word searches on file systems and documenting all evidence found and all procedures performed.

Presentation - Once the evidence has been processed and all the necessary preparation has been carried out the evidence should be prepared for court. This involves making sure all documentation such as evidence logs are readable and in an appropriate format for court. Investigators should prepare reports on what they did during the investigation and should be prepared to provide expert testimony. Evidence should be presented in a manner which is easy to read and which does not over complicate the evidence by disguising it in a mass of technical jargon. It is important to note that the complete and accurate evidence will be of little value in court if it is not presented in a way that can be understood by all members of the court, especially the jury.

Documentation - This phase of the methodology is perhaps not a phase as such but a continuing process. Throughout the investigation documentation should be constantly updated. The documentation may include various types of logs such as an evidence log, transport log, evidence lab analysis log and many other documents which together provide an accurate and detailed description of events that occurred from first arrival on the crime scene to the courts.

These six phases are common to the traditional computer forensic methodologies of today. They outline the major steps taken in an investigation. As mentioned earlier, there is little in the way of documented methodologies for computer forensics.

3.4 Comparison of Methodologies

There are several documented computer forensic methodologies, principles and guidelines that are available today. The IOCE and ACPO have developed draft standards guidelines and principles for computer forensics. The US Department of justice has released guidelines for the search and seizure of computers. However, this document is very detailed and specific to the US law. Timothy E. Wright, Peter Stephenson, Mathew Braid, and Thomas Rude have all documented their own computer forensic methodology. Additionally, the model developed by Rodney McKemmish will serve as a good guide on the development of a framework (refer Figure 1). These principles, guidelines and methodologies will be synthesised to create a normative methodology model, which will be discussed following a brief description of the critical success factors, influencing factors, existing principles, guidelines and methodologies.

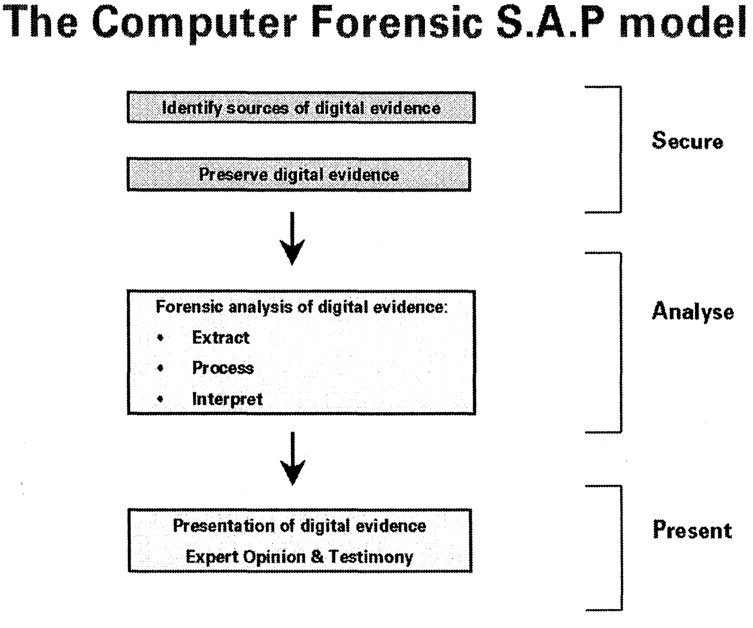
The Computer Forensic S.A.P model
Identify sources of digital evidence
Preserve digital evidence
Secure
Forensic analysis of digital evidence:
Extract
Process
Interpret
Analyse
Presentation of digital evidence
Expert Opinion & Testimony
Present

Figure 1. CFSAP Model (McKemmish, 2001)

From the literature review of existing methodologies it is possible to develop a methodology matrix, which illustrates the corresponding phases of the existing methodologies with the phases of a normative methodology. This normative methodology was developed by a synthesis of the existing methodologies. This methodology is a hypothetical model of the possible phases in a methodology. This matrix set out in Table 1 gives support to the normative methodology showing the comparison of each phase with the existing methodologies.

Phase of the normative model	Description	Stephenson 2000	Wright 2000	McKemmish , 2001	Braid, 2001	Rude, 2000
Preparation	The preparation stage involves preparing the personnel, materials and tools required for the investigation	Launch	Formulate plan	Secure		Preparation
Identification	The identification phase involves securing the scene and identifying the evidence	Launch	Approach and secure Crime Scene, Document crime scene layout	Secure: Identification	Identification	Snapshot
Preservation	The preservation phase involves backing up, protecting and preserving the evidence to prevent tampering and damage	Launch		Secure: Preservation	Preservation	Transport, Preparation for Examination
Analysis	This involves the extraction, processing and interpretation of the digital data.	Incident Analysis	Search for evidence, Retrieve Evidence, Process evidence	Analyse: Extraction, processing and interpretation	Analysis	Examination
Presentation	This stage involves preparing the case and evidence for court	Evidence analysis and Report preparation	Process Evidence	Presentation	Presentation	

Table 1. Comparison of Computer Forensic Methodology Phases

4. RESEARCH METHODOLOGY

The research methodology consists of the following phases: literature review; conduct of a research forum on e-crime and computer forensics;

Delphi study arising from the forum to determine the major issues surrounding computer forensics methodologies; semi-structured questionnaires and interviews with personnel from key law enforcement and private investigation agencies at both federal and state levels; construction of a normative computer forensics methodology; comparison of the normative methodology with those used by expert practitioners; refinement of a standard computer forensic methodology; review of the methodology by expert practitioners.

4.1 Data Collection and Methods

The collection of data in this research will be based around the formation of a normative methodology model. This normative model will help to collect the various actions, principles and steps that a computer forensic investigator performs into a framework. This is consistent with the retroductive strategy where, according to Blaike (2000, 71), ‘the literature review may provide some assistance in the construction of hypothetical explanatory model”, when conducting retroductive research.

The methods used to collect data must be able to capture the accounts of the computer forensic specialists in a precise and conducive way. According to Blaike (2000, 234) “the qualitative interview, particularly the in-depth variety, can get close to the social actors’ meanings and interpretations”. Similarly, written questionnaires and research forums are data collection methods that can be used when undertaking exploratory research.

This research is primarily exploratory in nature and therefore this study positions itself as the basis for further research in the area. The results of this study will need to be validated and further explored in future research as the framework is the first step in an iterative process. The issues rose in the research forum and the implications and limitations of this research will form the basis for future research in the area.

This study will use the existing literature in two main ways. First, the literature will be used to develop a normative methodology model, which will be used to formulate and direct the collection of the data. Secondly, prior research in the area of competency standards will help focus the collection of data for competencies. Through the use of a semi-structured written questionnaire, interview, and a research forum, a framework for a computer forensic methodology will be developed. This framework will need to be refined and explored further.

The exploration, description, development and explanation of practices and behaviours relating to computer forensic analysis relies on the generation of theory from in-depth accounts of social actors in the field. Therefore the research methodology adopted by this study will be that of

Grounded Theory. Grounded Theory is a qualitative research methodology that seeks to develop theory that is grounded in data systematically gathered and organised (Myers, 2001). Denzin and Lincoln (1994, 273) define Grounded Theory as a "general methodology for developing theory that is grounded in data systematically gathered and analysed". Prior research in computer forensic search and seizure in Australia has also chosen Grounded Theory as its theoretical framework (Wieszyk, 1998b). This methodology was chosen as it allows theory to emerge rather than verifying or negating hypotheses, whilst also allowing conceptualisation and operationalisation to occur at the same time as data collection and analysis (Wieszyk, 1998b).

4.2 Interviews and Research Forum

There were two rounds of interviews. The purpose of the first round was to undertake exploratory research to determine the main issues and views on methodology and competency standard development and determine whether the subject had a methodology or competency standard in place. The second or main round of interviews will be used to explore specifically the computer forensic techniques and skills used by the various investigators in terms of their own phases and in terms of the normative model developed from the literature. Details on actual steps undertaken in the forensic analysis are explored during the interviews. In line with the methodology of Grounded Theory, transcripts of the interviews were written up and a qualitative data analysis tool called NVIVO was used to code and categorise the answers to the interviews. This tool was then be used to collate, compare and contrast different answers to the questions. NVIVO was used to categorise the answers into groups for each of the phases of the normative model, allowing for easy analysis of the answers to the interview questions.

The purpose of the research forum was to bring together various experts in the computer forensic field in Australia to brainstorm the current and emerging issues in the area of computer forensic methodology and competency standard development. During the brainstorming session, the issues raised were documented. At the end of the discussion, the experts were asked to give a level of importance and a rank to each issue using a Delphi technique (Sarantakos, 1998). Following on from the forum will be three more rounds of Delphi ranking and importance scaling where respondents will rank and give each issue a level of importance whilst also having the chance to raise additional issues.

4.3 Research Subjects

Contacts with subjects for the interviews were made during attendance at an industry e-Crime conference. The study population for this research consists of three main groups:

- Law enforcement agencies and Government Regulators
- Private sector organisations
- Independent associations

The first group consists of representatives from the Australian Federal Police (AFP) and various other law enforcement agencies (including the Royal Canadian Mounted Police - RCMP) and government regulators such as the Australian Securities and Investment Commission (ASIC).

A research group called the Computer Forensic Research Group (CFRG) consisting of representatives from ASIC, AFP, W.A Police, and NSW Police, and UNSW was formed for the purpose of developing a framework for the development of a methodology standard, and exploring competency standards. The law enforcement members of the group were also members of the Australian Computer Crime Managers Group (ACCMG), whose charter covers e-crime and computer forensic. The proposal for this study was presented at the ACCMG leading to the formation of the CFRG, and the launch of this research after approval from the ACCMG.

The second group consists of representatives from the large consulting companies and other private sector companies dealing with computer forensics. The third group consists of representatives from working groups and organisations that are addressing issues relating to computer forensics.

5. PROGRESS TO DATE

5.1 Research Forum Results

From the research forum, a number of issues were determined for the area of computer forensic methodology and competency standards development. These are listed below:

1. Need a definition for computer forensics. There are a number of different areas in computer forensics:
   - Digital Evidence Recovery
   - Cyber/Intrusion Forensics
   - Forensic Data Analysis
   - Research and Development – Keeping tools and processes up to a

standard, and development
across other specialised areas such as electrical engineering (communications)

2. Develop computer forensics as a multi-disciplinary occupation
3. Exploration and development of relationship between forensics, and security in terms of skills
4. Identify skills for computer forensic investigators through putting in place the correct methodologies which will drive the development of competencies.
5. Connections and communication between communities: forensic, legal, security, risk management, law enforcement etc
6. Knowledge and information sharing between public and private sector with regards to competencies and standards
7. Discussion of privacy grades and context
8. Investigate ethical issues and acceptable levels
9. Define what elements or parts of the computer forensic field require or would benefit from the development of standards
10. Technical nature of standards
11. Explore the difference between civil and criminal investigations with respect to standards
12. Why do you need methodologies and standards?
13. Compile a stock take of interests and stakeholders
14. Set up of a Working group/professional body
15. Development of a testing mechanism for the methodology
16. Who to appoint as an accreditation body.
17. Setting up accreditation for various roles involved in investigating computer crimes

Each of the forum attendees filled out a Delphi rating system, rating each issue with a level of importance and also ranking all issues with an importance ranking. From the initial forum round of the Delphi study, the following top five issues relating to computer forensics methodology emerged:

- Need for a definition of computer forensics
- Define what elements or parts of the computer forensic field require or would benefit from the development of standards
- Who to appoint as an accreditation body and the setting up accreditation for various roles involved in investigating computer crimes
- Knowledge and information sharing between public and private sector with regards to competencies and standards

- Identify skills for computer forensic investigators through putting in place the correct methodologies which will drive the development of competencies.

Having derived these seventeen issues from the research forum, they have been sent to representatives from the Australian computer crime managers group who are currently completing the first round of the Delphi study. Following completion of this first round, the averaged results will be the fed back to participants together with their own ratings and rankings, and the participants will be requested to complete the second round of the Delphi study.

5.2 Methodology Development

The five phases of the normative methodology set out in Table 1 form the basis for a normative methodology model. This four-layer model, as shown in Figure 2, is used to illustrate the main components of any computer forensic methodology. The first layer defines the five high-level phases that are to be performed in any computer forensic investigation. Each phase in this layer is dependent on the previous and all phases must visited in turn. This layer is applicable to all cases and should be developed to be independent of factors that may change such as jurisdictions, tools and techniques.

The next three layers support the top layer but have been broken down logically into three layers. The documentation layer supports the top layer by providing a source of reference and repository for all the information gathered throughout the five steps. In essence, the first and second layer can be thought of as one layer where documentation is an ongoing and a cumulative process. The third layer, contains principles which support the above two layers by dictating the how to perform each of the phases. The fourth layer, standard operating procedures details the lo level process description of tools and techniques that are used throughout the process. The layer is technology specific and thus differs between cases, technologies and countries and changes with the dynamic nature of the IT industry. This layer includes definitions of tools, their applicability and expected results. In addition to this, this layer includes several standard operating procedures which detail techniques that are used at the lowest level e.g. how to perform a bit-level backup of a hard disk.

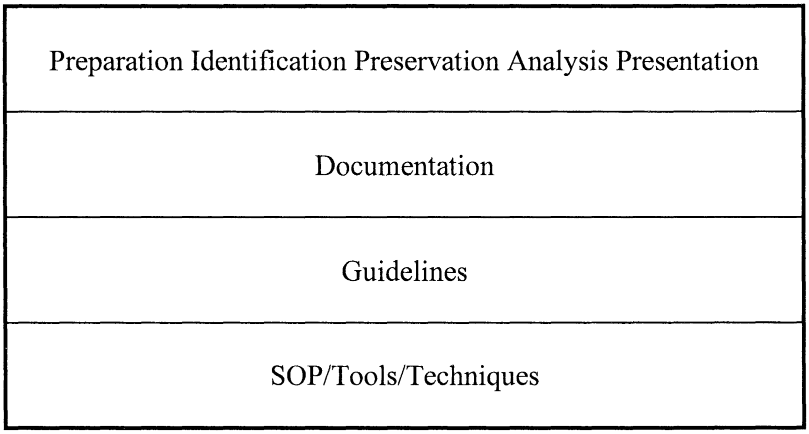
Preparation Identification Preservation Analysis Presentation
Documentation
Guidelines
SOP/Tools/Techniques

Figure 2. The Normative Methodology Mode

The modular structure of the model allows each layer to be interchangeable and independent of the other layers. This promotes flexibility of each component and allows for reuse and customisation of each component for different cases or for use in different jurisdictions or countries. For example, two cases will differ primarily by the different tools and techniques that will be used, and somewhat on the rules and guidelines that are relevant. However, the overlying process that is taken to investigate the crime, as described in the top layer of the model, will be identical for both cases. Similarly, as technology changes, the tools and techniques will change in accordance with the changing technologies. The top layer will remain unchanged despite the subsequent changes to the bottom layer. Differences across jurisdictions and countries should be evident primarily in the middle layer, as different laws will effect the rules and guidelines for handling evidence.In theory, using this model will produce an internationally applicable methodology, which is flexible to the differing rules, standards and regulations and to the changing technology. This model has many strengths:

- It is applicable to many cases.
- The top layer is supported by rules and guidelines
- The structure can cope with changing technology and dynamic environments
- Change will generally only effect the bottom layer (as technology is the most dynamic)
- As the computer forensic field is mainly in the law enforcement industry, dealing with crime, the model is easily adapted to accommodate the sensitive nature of some of the tools and techniques that law enforcement agencies may use. The first three layers can be made public as they

contain little material that is sensitive in nature, and the bottom layer can be proprietary. Thus, the bottom layer is interchangeable. Additionally, because the second layer dictates rules for evidence handling, evidence can be easily exchanged without releasing the method for retrieving the evidence.

- The bottom layer is made up of toolkits and Standard operating procedures (SOP's)

Currently a standard computer forensics methodology has been developed from the literature and derived out of results from the semi-structured questionnaires and interviews. This standard methodology consists of seven phases and forty two steps within those seven phases. A summary of these phases is set out in Table 2.

Phase of the Derived Model	Description
Preparation	The preparation stage involves preparing the personnel, materials and tools and equipment required for the computer forensic examination.
Identification	The identification phase involves securing the scene and identifying the evidence from the data set.
Baseline	The baseline phase involves testing of original evidence to provide a baseline or control result for future verifications to ensure consistency and accuracy.
Preservation	The preservation phase involves backing up, protecting and preserving the evidence to prevent tampering and damage
Verification	The verifications phase involves testing of outputs/results to ensure consistency and accuracy. Failure at this stage may dictate a return to the identification and preservation phases.
Analysis	This involves the extraction, processing and interpretation of the digital data.
Presentation	This stage involves preparing the case and evidence for court

Table 2. Derived Standard Computer Forensic Methodology Phases

To complement the standard computer forensics methodology, a list of twenty seven principles were derived from the semi structured questionnaires and interviews, together with a skills matrix and documentation required for each phase within the standard computer forensics methodology. Three examples of principles would be: storage equipment should be sterilised if possible; comply with search warrant/Anton pillar principles/ or gain users consent at all times: maintaining continuity of evidence -- account for any change to the data set/evidence. The following three examples illustrate the skills required to carry out computer forensics examination: knowledge of possible sources of evidence; computer software knowledge and experience of specific operating system and network operating systems related knowledge; knowledge of and experience with computer forensics tools - their operation and limitations. Examples of required documentation would include: search warrants; mud maps - an initial sketch of surroundings equipment and items; and forensics software log files.

Currently the standard computer forensics methodology, principles, the skills matrix and documentation derived from the research are being reviewed by representatives from the Australian Computer Crime Managers Group. Following this review, the results will be released into the public domain and be published.

6. CONCLUSIONS

This paper reviewed existing methodologies and the discussed the development of a standard computer forensic methodology. The issues raised open possible areas of future research in the computer forensics field for developing best practice or a standard methodology for international computer forensic investigators and investigating agencies. The shortfalls of traditional models, which also needs further investigation, suggest that there may be a better approach that could be taken to combat e-crime. There are also questions regarding the viability of accrediting computer forensic methodologies, techniques and investigators. This area is particularly important, as the results of such research will have influence on the way CFA's conduct investigations, as well as the training required for investigators. The availability of a standard computer forensic methodology and an accreditation device should improve the quality of computer forensic investigations in addition to advancing the computer forensic field to a recognised profession.

The idea of a proactive computer forensic methodology combined with the rules, guidelines and existing experience in the computer forensic field, may lead to an open standard international methodology, which is applicable to most cases and to computer evidence. This new methodology may be able to combat the shortfalls of traditional methodologies.

For certain, any future or standard methodology developed must include evidence handling procedures and principles, and must be independent of the tools and digital media. This will ensure that the methodology will be widely applicable to cases well into the future, despite the ever-changing technology.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the contributions made by the members of the Australian Computer Crime Managers Group, ASIC, AUSTRAC, PWC, Deloitte Touche Tohmatsu, KPMG, for their time and patience in completion of the questionnaires and interviews, and their reviews of the resulting frameworks. Also to the members of the e-Crime and e-Forensics Research Forum held in September 2001 by the Security, E-business, and Assurance Research Group (SEAR- sear.web.unsw.edu.au) for their contributions of research issues leading to the development and conduct of this research. The authors also wish to acknowledge the contribution by Ken Stevens for his help in reviewing the research.

REFERENCES

ACPR (2000), The Virtual Horizon: Meeting the Law Enforcement Challenges - Developing an Australasian law enforcement strategy for dealing with electronic crime, Report Series No: 134.1, Police Commissioners' Conference Electronic Crime Working Party, Australasian Centre for Policing Research, Adelaide.

ACPO, (2000), Memorandum by the Association of Chief Police Officers Computer Crime Working Group URL=www.parliament.the-stationery-office.co.uk/pa/ld199900/ldselect/ldeucom/95/0031502.htm

AIC (1999), What is Forensic Computing, Australian Institute of Criminology – Trends and Issues No. 118, June, URL=www.aic.gov.au/publications/tandi/tandi118.html

Blaike, N. (2000), Designing Social Research, Polity.

CFRG (2001), Meeting minutes for the CFRG meeting, Australian Computer Crime Managers Group – Computer Forensics Research Group, 15 October 2001

CSI/FBI (2001), 2001 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends, 7 (1), Spring, 1-18.

Cerpa, N. & R. Jamieson (2001), A Security Trust and Assurance Research Framework for Electronic Commerce, Proceedings of the IFIP TC8 Working Conference on Electronic Commerce, Salzburg, Austria, 22-23 June.

Denzin, N.K. & Y. S. Lincoln, (1994), Handbook of Qualitative Research, Sage Publications.

FBI (2000a), Three-Level Hierarchical Model for Developing Guidelines for Computer Forensic Evidence, Forensic Science Communications, October 2000, 2 (4), URL = http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/cmptrfl.htm

FBI (2000b), Recovering and Examining Computer Forensic Evidence, Forensic Science Communications, October, 2 (4), URL = www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer..htm

IDG News Service (2001), Update: Thirty countries sign cybercrime treaty, IDG News Service, 23 Nov 2001.

Lek, M., Anandarajah, B., Cerpa, N. & R. Jamieson (2001), Data Mining Prototype for Detecting e-Commerce Fraud, Proceedings of the ECIS'2001, Bled Slovenia, 27-29 June.

McKemmish, R. (1998), Report from the 1998 Donald Mackay Churchill Fellowship to Study Overseas Development in Forensic Computing, The Winston Churchill Memorial Trust of Australia, Brisbane.

McKeown, M. & R. Jamieson, (2001). Computer Forensics – Intrusion Detection, SEAR Working Paper, UNSW, Sydney, November, No 2001_3.

Myers M. D. (2001), Qualitative Research in Information Systems, URL = www2.auckland.ac.nz/msis/isworld, October.

Rehman Technology Services. (2000), Computer Forensics, Electronic Discovery, Electronic Evidence Discovery, Digital Discovery, Computer Analysis, Computer Examination, Computer Expert, URL = electronic-discovery.com (2000, October 26)

Rao, V., Cerpa, N. & R. Jamieson, (2001), A Comparison of Online Electronic Commerce Assurance Service Providers in Australia, Proceedings of the Fourteen Bled Electronic Commerce Conference, Slovenia, 24-26 June, 2001.

Rude, T. (2000), Evidence Seizure Methodology for Computer Forensics, September 2000, URL = www.crazytrain.com/seizure.html

Saferstein, R. (1998), Criminalistics: An Introduction to Forensic Science, 6th ed., Prentice Hall, Upper Saddle River, New Jersey.

Sarantakos, S, (1998). Social Research, MacMillan.

SC Magazine (2000), Computer Forensics April 2001, SC Magazine URL = www.scmagazine.com/scmagazine/2000_04/cover/cover.html

Stephenson, P. (1999), Investigating Computer-Related Crime, CRC Press.

Tennyenhuis A & Jamieson R (2001), Computer Forensics Methodologies, SEAR Working Paper, UNSW, Sydney, September, No 2001_2.

Wieszyk, M. (1998a), Computer Evidence Search & Seizure: Results of National Surveys & Interviews – A report for the national police research unit, ACPR, Adelaide.

Wieszyk, M. (1998b), Computer Evidence search & Seizure, Research Masters thesis.

Wong, K., Ng, B., Cerpa, N., & R. Jamieson (2000), An Online Audit Review System for Electronic Commerce, Proceedings of the Thirteen Bled Electronic Commerce Conference, Slovenia, 19-21.

Wright, T. (2000), The Field Guide for Investigating Computer Crime: Overview of a Methodology for the Application of Computer Forensics Part 2, URL = www.securityfocus.com/focus/ih/articles/crimeguide2.html.