DEVELOPING A FRAMEWORK FOR EVALUATING COMPUTER FORENSIC TOOLS

Colin Armstrong
Curtin University of Technology, School of Information Systems, WA

Paper presented at the Evaluation in Crime and Justice: Trends and Methods Conference convened by the Australian Institute of Criminology in conjunction with the Australian Bureau of Statistics and held in Canberra, 24-25 March 2003
Abstract

Forensic science is the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system. The discipline of computer forensics is growing because it is making an important transition from being a "black art", restricted to a few experts, into an essential element of the information security enterprise. A major factor influencing this transition is the latest generation of highly efficient computer forensic software tools. These new tools may lead corporate information security staff to rely on "point & click" wizardry that could jeopardise the prosecution of a case.

This paper discusses a research project that examines criteria that will help development of a framework to evaluate the appropriateness of computer forensic tools. The framework is intended for use by State and Federal Policing agencies. It is to be used to attest to the validity of the tools used in the gaining of forensic evidence. The project aims to develop a practically relevant and useful framework for Police that will uncover a set of reliable and acceptable criteria on which a framework can be built.

A law enforcement investigator may use tools, procedures and methods not readily available to the public and therefore not be readily understood and accepted. For an investigators finding to be accepted they must be recognised by other experts within the field and conform to national and international standards of practice. A computer forensic investigator risks loss of credibility if doubt can be introduced into the appropriateness of tools and / or actions deployed in the presented evidence. This research project will develop a framework to assist investigators remedy this situation.
Introduction

This research project was instigated by personnel at the Computer Crime Unit of the Western Australia Police Service Major Crime Squad and is being undertaken in conjunction with State and Federal computer forensic policing agencies within Australia. It addresses how issues faced by expert computer forensic witnesses and investigators presenting information regarding the examination and analysis of computer systems are addressed within the legal system.

Forensic is defined as belonging to, used in, or suitable to courts of judicature or to public discussion and debate (Bologna and Lindquist, 1995). Computer Forensics is the coherent application of methodical investigatory techniques to solve crime cases (Kruse and Heiser, 2001).

Police are responsible for upholding the law and investigating, apprehending and prosecuting breaches of the law. The successful prosecution of computer based crime is reliant upon the investigator being able to prove beyond a reasonable doubt who, what, how and when a criminal event occurred within the stringent principles of forensic examination of evidence. Computer crime is of such a nature that it is often difficult for the general public to perceive or to understand that a crime has actually occurred. Criminals are using computers to store records regarding drug deals, money laundering, embezzlement, mail fraud, telemarketing fraud, prostitution, gambling matters, extortion, and a myriad of other criminal activities (Icove et al, 1995). The victim may be a large corporation, may be far away, or may be considered an unfriendly nation, competitor or even an enemy.

An investigation may use tools, procedures and methods not readily be available to the public and therefore not be readily understood and accepted. For these investigative finding to be accepted they must be recognised by other experts within the field and conform to national and international standards of practice. The risks facing a computer forensic investigator include loss of credibility if another expert witness can demonstrate that proper or appropriate courses of action were mismanaged. It is the role of the independent expert to explain technical issues in layman's terms so that the judge, jury, accused, barrister and solicitor alike can understand the evidence put before them. (Armstrong, 2002)

This research project will examine a number of computer forensic tools and relate their attributes and performance to a framework that the researcher shall construct. This Computer Forensic Tool Evaluation Framework (CFTEF) would then enable the investigator to evaluate whether the tool chosen meets the requirements demanded to improve the success of a presentation of a case to the court.

Objectives

The primary aim of this research is to build and test a framework for the evaluation of software tools for use by State and Federal policing agencies in the forensic examination of computer systems. The framework would conform with and assist in the determination of a standard operating procedure to be adopted by computer forensic investigators. The research objectives will culminate with the discovery of a set of measurements that will permit the framework to determine the appropriateness of a computer forensic tool for a particular situation.

The objectives of this research are;

1. Identify and review the practices currently in use by policing agencies computer forensic investigators.

2. Determine the measurable criteria and desired outcomes required of software tools by policing agencies.
3. Evaluate a selection of software tools or products such as; Encase, Silent Witness, NTI, iLook, SMART,
4. Figure 2, shows the model for the construction of the framework to meet these objectives.

Significance

The credibility of an expert witness may be crucial to the outcome of a case. If the integrity and credibility of a Police Officer investigating and providing prosecution evidence in a crime is placed in doubt then the prosecution case may fail. Integrity and confidence in the process and the person may be the definitive factor in determining the success or failure of an investigation and prosecution.

There are a number of forensic computer software tools of varying sophistication. (see Casey 2000, Kruse and Heiser 2001, Klevinsky, et al 2002, Marcella and Greenfield 2002, Noblett, et al 2000, Vacca 2002) There is no concerted or single point of analysis to assist investigating personnel in their decision as to the appropriateness of a tool to a specific need. Kruse and Heiser (2001), point out that new tools provide approaches to automated examination and analysis. (Kruse and Heiser, 2001), (Barbin and Patzakis, 2002) This automation has the potential of leading to “point & click” wizards with little or no expertise or understanding in what is actually happening nor why. Training in “command line” level of the operations may be a necessity in proving one’s bona fides and expertise in the science of computer forensics.

This research will develop, implement and test the viability of an evaluation framework for computer forensic tools. This evaluation framework will guide a police investigator in the appropriateness of a chosen tool to a crime case situation. This guidance will strengthen and substantiate the discovered evidence. It will also save time in the police investigation process due to choosing the appropriate tool and thereby removing the need to repeat tests to acquire evidence. Choosing the most appropriate tool for a crime situation saves time not only in the actual gathering of evidence but also in the analysis of evidence held.

From the time that an act of a crime is committed until that crime is prosecuted in the courts there are many possible areas of research. The focus of this research project addresses issues associated with the examination of digital data within the boundary of research shown in Figure 1.

Apart from assisting Government crime investigation agencies this framework will assist corporate information security personnel. There are two aspects of consideration in this non-police and non-government agency area. Firstly, in the corporate sector information security personnel watch over a wide range of security risk. They may need to investigate in-house activities that later become a matter for prosecution through the court system. It is imperative that the tools used are understood and that the amount of intrusion is understood so as not to taint prospective or potential evidence. There is a significant risk that well-intentioned but misdirected security staff may destroy or contaminate material or evidence of potential significance. Secondly, while both the public and private sector are at one end of the spectrum. At the other end is organised crime. Prosecuting crime is not a cost effective activity. Security personnel and services tend to be under staffed, under funded, and work within tight sets of rules of play and legal constraints. On the other hand, organised crime is not limited by these constrains being able to allocate proceeds of crime as an investment to further their activities.

The significance of this research is also demonstrated by the absence of academically conducted research, refereed conference proceedings and published books on this subject. The danger of criminal activity not being successfully prosecuted due to the failing of a computer forensic process is very real. This is further exasperated by the provision of advice that works against the objectives of computer forensic investigators. Advice given by Bologna and Lindquist (1995) discusses how
to use a computer, modem, communication software, procomm, tymnet and databases such as TRW and D&B. They then state that, "You are now ready to dig into files. The procedure is to (1) turn on the PC; (2) insert the communications software diskette in the A: drive; (3) when the program is loaded, dial up the database provider; (4) when connection is made, sign on with your user ID and then your code name; (5) when the menu is displayed, select an area of interest and follow instructions.” (Bologna and Lindquist, 1995). Further, in discussions on forensic accounting of large computerised account systems Bologna fails to acknowledge computer forensic science in any way (Bologna and Lindquist, 1995). Anyone following this advice will seriously compromise any prospective computer forensic investigation because the very search for evidence will intrude and alter critical files. A primary principle of computer forensic investigation is to conduct any analysis of digital evidence on a replication of the original data after it has been gathered in such a manner that the original data is not contaminated or altered.

Finally, the significance of this research is in the timing. Recent terrorist activities have provided impetus to security related research. The sense of urgency and high profile given these events has motivated an openness and willingness within the policing and security organisations to share information in the battle to combat crime. Since the events of 11th September 2001 and the Bali bombing 12th October 2002, there has been a proliferation of materials generated aimed as a response to public demand to the people of the USA. It would appear that this is an emerging field of work.

Research Program

I believe that the thinking world, academia, has a responsibility to work with the action world, the public and private sectors to develop solutions and improved methods of conducting the work of business. Both sectors work to achieve maximum benefit for time and money invested. It is the thinking world where time and money can best be invested into resources for research. Academics in the Thinking World work together with international and national colleagues conducting research and sharing their findings. Those employed in the Action World tend to be fully occupied attending to their immediate duties and not have the opportunity to think through the impacts and implications of solutions to problems. Working together as shown in Figure 6., both Worlds may benefit.

<table>
<thead>
<tr>
<th><img src="image1.png" alt="Investigation Path" /></th>
<th><img src="image2.png" alt="Model for the Construction of the (CFTEF)" /></th>
</tr>
</thead>
<tbody>
<tr>
<td>Research Boundary on the Crime to Court Investigation Path</td>
<td>Model for the Construction of the (CFTEF) Computer Forensic Tool Evaluation Framework</td>
</tr>
</tbody>
</table>

1. **Investigation Path**
2. **Model for the Construction of the (CFTEF)**
The program for this research follows normal academic principles whereby a chosen topic is investigated, researched and results are reported. As shown in Figure 6, it addresses an Action World need by applying Thinking World skills for the mutual benefit of both. Figure 5, shows the Crime to Court Path and indicates areas of focus from two participants of the Action world. The boundary of this research is shown in Figure 1, which also establishes its location along the Crime to Court Path.

The model for constructing the Framework and determining its mechanical application is derived from applying the three-level hierarchical model, Figure 4, proposed by Noblett and others (2000). It consisting of the following:

1. An overarching concept of the principles of examination
2. Policies and practices, and
3. Procedures and techniques. (Noblett et al., 2000)

Action World needs are not restricted to just the level where the problem generating the need originates. To be relevant to that organisation and other similar organisations contributions to the solution should be drawn from the levels shown in Figure 4. The solution must be able to be related to the organisations reason for existing. The contributions to the CFTEF are derived from all levels for this reason. Figure 2, explains the several parts that contribute to the formulation of the rating of a tool in given circumstances, and Figure 3, shows the steps taken in selecting an appropriate tool when implementing the CFTEF.
When all of these parts are bought together into a coherent whole we will have the makings of another weapon in the continuing battle against elements of crime.

Conclusions

There is a demonstrable need from the Action World for research into how to improve Worlds Best Practice that would lead to greater confidence in investigators gaining successful prosecution of computer related crime. This paper discusses aspects of creating a tool to assist investigators of computer related crime to better select an appropriate tool.

This research project addresses one small aspect by focussing on producing a Framework to support the appropriateness of a selected forensic computing tool. For this research to be relevant to practitioners and to meet Action World needs it is important that the Thinking World and Action World work together. To this end, I invite all practitioners and those associated with or interested in this area of research to participate in furthering our knowledge by joining in correspondence with those of us researching this subject.
Appendix 1. – Bibliography / References


