Framework for a Digital Forensic Investigation

Michael Kohn[1], JHP Eloff[2] and MS Olivier[3]
[1]mkohn@cs.up.ac.za, [2]eloff@cs.up.ac.za, [3]molivier@cs.up.ac.za

Information and Computer Security Architectures Research Group (ICSA)
Department of Computer Science
University of Pretoria

Abstract - Computer Forensics is essential for the successful prosecution of computer criminals. For a forensic investigation to be performed successfully there are a number of important steps that have to be considered and taken. The aim of this paper is to define a clear, step-by-step framework for the collection of evidence suitable for presentation in a court of law. Existing forensic models will be surveyed and then adapted to create a specific application framework for single computer, entry point forensics.

1. Introduction

Over the past few years, computer forensics has risen to the fore as an increasingly important method of identifying and prosecuting computer criminals. Prior to the development of sound computer forensics procedures and techniques, many cases of computer crime were left unsolved. There are many reasons why an investigation might not lead to a successful prosecution, but the predominant one is a lack of preparation. The organization investigating the suspicious behaviour often lacks the tools and skills required to successfully gather evidence. Individuals attempting to investigate such suspicious activity may also lack the financial resources financial resources or tools to conduct such an investigation adequately and ensure that the evidence is undisputable in all circumstances. Moreover, there are instances when all of the above have been adequately put in place by an organization, but, due to a lack of training and correct procedure, the evidence collected can easily be disputed.

As a result, computer forensics seeks to introduce cohesion and consistency to the wide field of extracting and examining evidence obtained from a computer at a crime scene. In particular, the extraction of evidence from a computer is performed in such a way that the original incriminating evidence is not compromised. This is also useful when presenting a case without the support of legal expertise, as is often the situation since many organizations and individuals do not have in-house or personal legal representation.

This paper will propose a three phase framework that can be followed systematically to produce forensically sound evidence. The framework is an adaptation or combination of several existing forensic models.

The paper is structured as follows: the subsequent section will clarify important terminology used in the field of forensics; the third section will briefly discuss some

generally accepted frameworks; section four will introduce the proposed forensic framework, and closing remarks will be made in section five.

2. Background

According to the Oxford dictionary, the word forensic is defined as “relating to or denoting the application of scientific methods to the investigation of crime” and “of or relating to courts of law” [8]. At first, this appears to be quite a broad definition, but what is important in the first definition is that scientific methods are used in the investigation and the second definition emphasizes the fact that forensic activity usually relates to courts of law. Nonetheless, not all cases investigated end up in court. Examples are internal investigations and disciplinary hearings [7]. In conclusion, what would seem to be important is that, when a forensic investigation is launched, it is conducted in a scientific way and with a legal base as support.

Some authors make a clear distinction between computer and digital forensics [5]. Yet, for the purposes of this paper, no real distinction is made. Computer forensics can be defined as “analytical and investigative techniques used for the preservation, identification, extraction, documentation, analysis and interpretation of computer media (digital data) which is stored or encoded for evidentiary and/or root cause analysis” [7].

There are, however, methods which can help circumvent the, often tedious, task of ascertaining which factors are applicable to a particular forensic investigation. All organizations should have standards, policies and procedures in place that can assist in such an investigation. Standards that are important here are ISO17799 [10] and COBIT [11]. These standards do not cover a forensic investigation, but could be used to aid it.

As well as internal standards and policies, there are several legislative measures that support organizations attempting to prosecute computer crimes. In South Africa, there are a number of important Acts that can be referenced. These include the Electronic Communications and Transactions (ECT) [12] and the Promotion of Access to Information Act (PAIA) [13]. These, however, do not provide any clear guidelines as to how a forensic investigation should be conducted to ensure legal appropriateness.

Consequently, an important way for most organizations to protect themselves against computer crime is to institute internal policies and procedures which specify exactly what constitutes harmful action against or within an organization. These, however, are beyond the scope of this paper since there are a wide variety of possible solutions that can and have effectively been used.

Thus far it has been determined that implementing certain Standards, like ISO17799, can be a useful initial step by an organization towards effectively protecting its information and assets. Moreover, that specific policies and procedures should also be implemented within an organization to help protect the internal integrity of information and assets.

Once these basics are in place, the next step is to apply a sound forensic framework, which will consistently gather evidence suitable for presentation in a court of law, to ensure that criminal behaviour can be successfully prosecuted.

The Oxford dictionary defines a framework as “a supporting or underlying structure” [9]. A computer forensic framework can be defined as a structure to support a successful forensic investigation. This implies that the conclusion reached by one computer forensic expert should be the same as any other person who has conducted the same investigation [7].

A framework is also dependent on a number of structures. In the case of computer forensics, or forensics in general, legislation has to be considered to be of prominent importance. A forensic investigation has to be conducted in a scientific manner and must comply with all legal requirements, as set out in the second definition of forensics above. Evidence will have to be collected in this manner irrespective of the purpose i.e. internal investigation, disciplinary hearing or court case.

3. Frameworks

There is an old saying that prevention is better than cure. When applied to forensic frameworks this would seem to imply that preparation is the key to conducting a successful forensic investigation. Although preparation is important, it is impossible to be prepared for all types of behaviour. A sound base of previous knowledge and experience will always help, but a suggestion or documented case is not a complete resolution to solving a problem.

The number of forensic models that have been proposed reveals the complexity of the computer forensic process. Most focus on either the investigation itself or emphasize a particular stage of the investigation.

Kruse and Heiser refer to a computer forensic investigation methodology with three basic components. They are: acquiring the evidence; authenticating the evidence, and analyzing the data [1]. These components focus on maintaining the integrity of the evidence during the investigation.

The United States of America’s Department of Justice proposed a process model for forensics. This model is abstracted from technology. This model has four phases: collection; examination; analysis, and reporting. [5] There is a correlation between the ‘acquiring the evidence’ stage identified by Kruse and Heiser and the ‘collection’ stage proposed here. ‘Analyzing the data’ and ‘analysis’ are the same in both frameworks. Kruse has, however, neglected to include a vital component: reporting. This is included by the Department of Justice framework.

The Scientific Crime Scene Investigation Model proposed by Lee consists of four steps. They are: recognition; identification; individualisation, and reconstruction [1]. These steps only refer to a part of the forensic investigation process. These steps all clearly fall

within the ‘investigation’ stage of the process; there is neither a ‘preparation’ nor ‘presentation’ stage either side.

Casey proposes a framework similar to Lee. This framework focuses on processing and examining digital evidence. The steps included are: recognition; preservation; classification, and reconstruction [3]. In both Lee and Casey’s models, the first and last steps are identical. Casey also places the focus of the forensic process on the investigation itself.

The Digital Forensics Research Working Group (DFRW) developed a framework with the following steps: identification; preservation; collection; examination; analysis; presentation, and decision [4]. This framework puts in place an important foundation for future work and includes two crucial stages of the investigation. Components of an investigation stage as well as presentation stage are present.

Reith proposed a framework that includes a number of components that are not mentioned in the above frameworks. The full listed components are: identification; preparation; approach; strategy; preservation; collection; examination; analysis; presentation, and returning evidence [5]. This comprehensive process offers a number of advantages, as listed by the authors. For example, a number of the components can be included in other stages of an investigation, as will be shown later.

The model proposed by Ciardhuáin is probably the most complete to date. The steps or phases are also called ‘activities’. The model includes the following activities: awareness; authorization; planning; notification; search for and identify evidence; collection; transportation; storage; examination; hypothesis; presentation; proof/defense, and dissemination [6]. The steps are discussed in depth by the authors of the paper.

From the proposed frameworks mentioned above, the following can be seen quite clearly:

- Each of the proposed models builds on the experience of the previous;
- Some of the models have similar approaches;
- Some of the models focus on different areas of the investigation.

Perhaps the best way to balance the process is to ensure the focus remains on achieving the overriding goal: to produce concrete evidence suitable for presentation in a court of law.

4. Proposed Framework

The previous section outlined several important forensic frameworks. In this section a new framework will be proposed. The aim is to merge the existing frameworks already mentioned to compile a reasonably complete framework. The framework proposed in this paper has three stages. They are: preparation; investigation, and presentation. The previously proposed frameworks’ phases are grouped into these three stages. These stages also comply with the definition of forensics in general. If a forensic investigation

conducted these three stages as a minimum, there would be little doubt that a proper forensics process had been followed.

The aim of this paper is not to propose a complete framework exhibiting a number of finite steps. The grouping of defined steps into three, broad stages ensures a more adaptable framework. The preparation, investigation and presentation stages are illustrated in the following diagram.

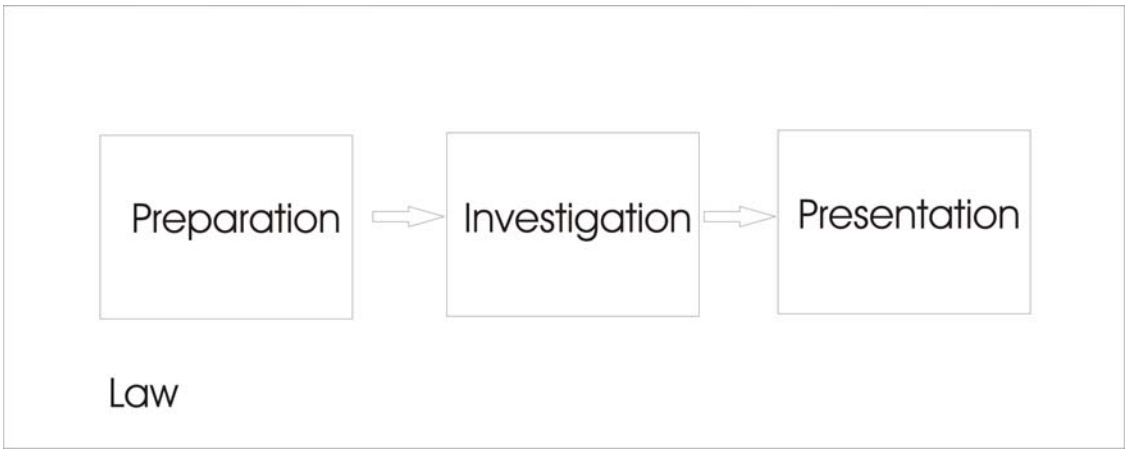

Figure 1: Investigation Stages

Figure 1 illustrates the order in which these stages should be conducted. It is also suggested that this framework should form part of a cycle within the investigation process.

All the phases mentioned by previous frameworks can be incorporated into this framework. This framework also sets a legal base as foundation. The reason for this is so that a clear understanding of what the legal requirements are is established right at the start of the investigation and informs each subsequent step or phase. By focusing on this end goal and deciding what legal norms are to be used, the most applicable framework and integral steps will become clear.

The Preparation stage of the investigation should include the following:

- Standards used in the organization;
- Policies and procedures in place to assist in the investigation;
- Training;
- Legal advice;
- Notification to the correct authorities;
- Documentation of previous incidents;
- Planning, also known as an ‘approach strategy’.

The Investigation stage should include the following:

- Searching for and identifying evidence on a computer;
- Collection of the evidence from the computer (original is duplicated);
- Transportation of the evidence to a secure environment;

- Storage of evidence collected at the scene;
- Examination of the evidence using the proper tools (finding incriminating evidence);
- Analysis (looks at the product of the examination to determine the significance and value of the evidence found).

The final stage of any forensic investigation should include a Presentation stage. This stage is important because it satisfies the key requirement specified by the definition of the word ‘forensic’. This stage will include the following vital steps:

- Presenting the analysis, and
- Proving the analysis.

The steps in the final, Presentation stage of the investigation should prove the hypothesis reached during the investigation. The evidence presented should also hold up in court if the proposed framework and all previous steps were followed correctly.

The proposed framework draws on the experience of other authors [1] [2] [3] [4] [5] [6] and this research has highlighted two important points. Firstly, that knowledge of the relevant legal base prior to setting up the framework is vital since this will have a bearing on the whole investigative process. Secondly, that the process should include three stages — preparation, investigation and presentation — to meet the basic requirements of the definition of the word ‘forensic’.

5. Conclusion

The aim of this paper is to establish a clear guideline of what steps should be followed in a forensic process. These steps, in turn, should enable us to clearly define a framework that can be used in a forensic investigation. A study of previously proposed frameworks revealed that a number of steps or phases overlaped one another and that the difference was mainly one of terminology.

No new steps were added in the framework proposed in this paper. Instead, similar tasks were grouped into the stages required by a forensic investigation. The stages required are preparation, investigation and presentation. This framework can easily be expanded to include any number of additional phases required in the future.

It is, however, important to note that there are several levels of abstraction in the process. Nonetheless, two requirements were identified as needed at every level: the legal requirements of a specific system and documentation of all the steps taken.

6. Bibliography

[1] Baryamureeba, V. and Tushabe, F.: **The Enhanced Digital Investigation Process Model** Digital Forensics Research Workshop. 2004.

[2] Carrier, B. and Spafford, EH.: **Getting Physical with the Investigation Process** International Journal of Digital Evidence. Fall 2003, Volume 2, Issue 2, 2003.

[3] Casey, E.: **Digital Evidence and Computer Crime**, 2nd Edition, Elsevier Academic Press, 2004.

[4] National Institute of Justice. **Results from Tools and Technologie Working Group**, Goverors Summit on Cybercrime and Cyberterrorism, Princeton NJ, 2002.

[5] Reith, M., Carr, C. and Gunsch, G.:**An Examination of Digital Forensic Models,** International Journal of Digital Evidence. Fall 2002, Volume 1, Issue 3, 2002.

[6] Ciardhuáin, SO.: **An Extended Model of Cybercrime Investigations**, International Journal of Digital Evidence. Summer 2004, Volume 3, Issue1, 2004.

[7] Van Solms, SH. and Lourens, CP.: **A Control Framework for Digital Forensics**, IFIP 11.9, 2006.

[8] http://www.askoxford.com/concise_oed/forensic?view=uk : forensic accessed on 7 June 2006.

[9] http://www.askoxford.com/concise_oed/framework?view=uk : framework accessed on 7 June 2006.

[10] **Information Technology – Security techniques – Codes of Practice for information security management.** International Organisation for Standardization and the International Electrotechnical Commission. ISO/IEC 17799. 2005.

[11] Information Security, Audit and Control Association (ISACA). July 2000. COBIT 3rd Edition Control Objectives.
http://isaca.org.

[12] Electronic Communications and Transactions (ECT) Act 25 of 2002. South Africa.

[13] Promotion of Access to Information Act (PAIA), Act 2 of 2000. South Africa.