Modelling Live Forensic Acquisition

MM Grobler[1], SH von Solms[2]

[1] Council for Scientific and Industrial Research, South Africa
marthiegrobler@gmail.com, mgrobler1@csir.co.za
[2] Academy for Information Technology, University of Johannesburg, South Africa,
basievs@uj.ac.za

Abstract

This paper discusses the development of a South African model for **Li**ve **Fo**rensic **Ac**quisition - **Liforac**. The *Liforac model* is a comprehensive model that presents a range of aspects related to Live Forensic Acquisition. The model provides forensic investigators with guidelines on how to proceed during an investigation. It provides forensic investigators with a robust foundation to understand what needs to happen during an investigation, the order in which these actions need to take place and the reasoning behind these actions. It supports forensic soundness.

Keywords

Cyber Forensics, Live Acquisition, forensic soundness, forensic model

1. Introduction

Up to date, forensic investigators approached memory acquisitions with caution. The current norm is to perform traditional forensic acquisitions to ensure that evidence obtained remains forensically sound and useful in a court of law. However, new types of crime surfaced in the virtual world, while conventional crimes exploit advanced technology (Maat 2004:i). This adds to cyber crime's threat and complicates the investigation process due to crime's increased sophistication (Pan & Batten 2005:1).

These developments leave Law Enforcement outdated. In some incidents, legal aspects provide no safety against new criminal techniques (Jones 2007:1) and therefore forensic investigators need to turn to Live Forensics to ensure successful investigations. This technique allows investigators to recover additional data typically only retrievable from live systems.

1.1. Current Status of Cyber Forensics

The current forensic best practice, Dead Forensic Acquisition, involves unplugging a machine to acquire an image of the hard drive. This technique generally causes data corruption and system downtime. Live Forensic Acquisition emerged to counter the problems caused by Dead Acquisition. This technique refers to the acquisition of a forensically sound system image from a live, running machine.

Irrespective of the technique used, investigators present this evidence to court. If the data are admissible, forensic investigators refer to it as forensically sound (see Section 4).

However, very few South African courts currently accept Live Forensic Acquisition as forensically sound evidence. The main reasons for this inadmissibility of Live Forensics is firstly the lack of court precedence, and secondly criminals' liking to exploit new technology in an innovative manner.

1.2. Research Objectives

This paper describes a model that underwrites forensically sound Live Acquisition. Although the idea of a multi dimensional model guiding Live Forensics is not novel, the *Liforac model* is developed for the South African perspective. Forensics in South Africa is not a highly publicised topic and currently very little emphasis is placed on either Live Forensics or forensic soundness within the judicial system.

This *Liforac model* accordingly presents a number of general guidelines for the prospective forensic investigator. It aims to guide investigators on four levels: basic concepts of laws applicable to Cyber Forensics (country specific laws are not addressed and it remains the prerogative of the investigator to study these); the general timeline of actions that should be performed before, during and after the investigation to ensure a reasonable expectation of court admissibility; knowledge areas that can contribute either directly or indirectly to an investigator's better understanding of the forensic discipline; and a basic discussion and possible solutions to the most common problems associated with Live Forensics. The model is full of general guidelines and do not aim to provide distinct technical or legal detail.

The proposed model is developed after an intense literature study on popular forensic tools, current and applied Live Forensic methods and techniques, cyber crime and criminals and legislation related to cyber crime. The next section introduces the forensic discipline and concepts.

2. Forensic Introduction

Cyber Forensics is *"… the process of copying data from a computer in a forensic manner"* (Jones 2007:2). It is a discipline that combines elements of computer science and the law to collect and analyse data from computer systems and networks in such a way that the collected data is admissible as evidence in a court of law (US-CERT 2005:1).

The two forensic investigation techniques relevant to this paper are Dead Forensics and Live Forensics. Dead Acquisition is analysis done on a powered off computer (Jones 2007:2), often referred to as traditional forensics. It allows the examiner access to create a snapshot of the swap files and other system information as it was last running (Stimmel 2008:2).

Live Forensic Acquisition is similar to Dead Forensic Acquisition. It developed in response to the shortcomings of the traditional forensic acquisition techniques, addressing the retention of volatile data and encrypted files. Live Acquisition can retrieve both static and dynamic, volatile data (Forte 2008:13). This technique addresses many of the problems associated with Dead Forensic Acquisition, but brings about some additional problems. The most critical of these problems are data modification and court acceptance of evidence.

The basic Cyber Forensic principles are simple. Yet, the variety of hardware, software, operating systems and platforms complicate the forensic process. It is rare that a forensic investigator knows exactly what to expect when walking into a field setting. In many cases, the client will provide some information regarding the number of systems in question, their specifications and current state. However, this provided information may be inaccurate. To counter this problem, the *Liforac model* is developed to guide the investigator in the acquisition process.

3. Developing the *Liforac model*

The premise of the model is not to present a rigid set of steps, but to develop a broad set of guidelines that can assist an investigator in the acquisition. To ensure a successful investigation, it is required to deliver verifiable, repeatable results. Therefore, forensic investigators are responsible for technical insight, legal knowledge and total objectivity during investigations. Only then can investigators present evidence of suspected misconduct or possible exoneration (Stimmel 2008:1).

The *Liforac model* is based on existing theories for physical and cyber crime investigations, and draws upon Biological Forensic principles. The model is practical and presents the same chronological steps that an actual investigation would take. It is presented as a general guideline to technology and is not tied down to specific or current products and procedures, ensuring an extended model lifetime (Carrier & Spafford 2003:1).

Figure 1 presents the generic *Liforac model.* This model comprises four distinct dimensions: Laws and regulations, Timeline, Knowledge and Scope. These four dimensions were identified as the four most prominent aspects during a preliminary literature study and the drivers strongly directed the decision to divide the model into these four specific dimensions (discussed in Section 3.5).

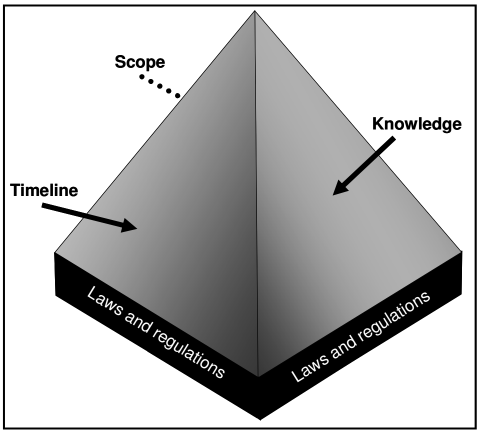

Figure 1: Generic *Liforac model*

3.1. Laws and Regulations

The Laws and regulations dimension is the foundation of the model. It affects all three the other dimensions and forms the basis on which these dimensions rest. Many forensic investigators agree that there is a gap between the technical aspects of Digital Forensics and the legal process. Generally, legal practitioners consider technical procedures difficult to understand and follow during an investigation or trial. They tend to get lost in the technical details without understanding the basic principles of forensic procedures (Ieong 2006:30).

To salvage this problem, forensic investigators require a solid legal and regulatory knowledge. This dimension divides into four components:

- **Component 1: Common crime laws applicable to cyber crime.** These laws refer to existing legislations created with traditional crimes in mind. The interpretation of these laws can allow extension to cyber crimes as well.
- **Component 2: Specific cyber laws.** These laws refer to laws created specifically with cyber crimes in mind.
- **Component 3: Court cases and precedents.** These laws are crucial in the acceptance of any new technology in court. Examples of these precedents are the Frye and Daubert tests.
- **Component 4: Definition of court admissibility.** This definition largely determines whether the court would allow Live Forensic Acquisition. This definition and implementation have a big impact on the Live Forensic discipline.

3.2. Timeline

The Timeline dimension focuses more on the process view of the model, indicating the sequence in which investigators need to execute processes. A timeline presents a visualisation of a sequence of events to show the relationship between the entities.

This dimension presents all actions taken by forensic investigators and visually presents it in the sequence it should execute to ensure sound forensic practices. This dimension divides into five components:

- **Component 1: Implied processes.** These processes refer to specific processes that contribute indirectly to the successful completion of this dimension. The absence of these processes may render the timeline unsuccessfully completed.
- **Component 2: Explicit processes.** These processes refer to specific processes that contribute directly to the successful completion of the dimension.
- **Component 3: Timeframe before the investigation.** Before the investigation, specific processes are necessary to ensure a solid planning and foundation stage.
- **Component 4: Timeframe during the investigation.** During the investigation, specific processes are necessary to ensure that investigators

collect all evidence in a forensically sound manner to ensure admissibility in court.

- **Component 5: Timeframe after the investigation.** After the investigation, specific processes are necessary to ensure that the chain of custody remains intact and the evidence are stored and returned safely after the investigation.

The timeline can further be divided to indicate responsibilities of specific individuals (e.g. system owner, legal advisor, Digital Forensic specialists, forensic investigators), but this is beyond the scope of this paper (Ieong 2006:32).

3.3. Knowledge

The *Knowledge* dimension indicates the different stages of awareness and understanding investigators need to acquire to perform sound Live Forensics. With the ever-changing technologies, tools and techniques, forensic investigators need to stay abreast and updated with new developments.

To ensure that investigators are fully prepared for any type of forensic investigation, they need to ensure that their knowledge is always up to standard to allow for any eventualities. This dimension divides into seven components:

- **Component 1: Computer Science.** The formal definition of Cyber Forensics (Section 2) established a link between Cyber Forensics and Computer Science. Cyber Forensics will always have a computer component to it.
- **Component 2: World Trends and Events.** World trends and events have a persistent influence on Cyber Forensic knowledge. Forensic investigators need to renew their knowledge on new trends in cyber crime and the combating of these crimes constantly.
- **Component 3: Information Systems.** Information Systems are the organised collection, storage and presentation of information for decision-making. Since there is a direct relation between computers and information, this component is necessary in the knowledge dimension.
- **Component 4: Social Sciences.** Social sciences can play a role in Cyber Forensics due to its profiling nature. People tend to react in specific ways under certain circumstances, which may have an affect on the way the investigation is run.
- **Component 5: Forensic Sciences.** Forensic sciences are at the core of Cyber Forensic investigations. Cyber Forensics borrows many principles from Biological Forensics and there are many similarities between these two disciplines.
- **Component 6: Law.** Law has a very direct relationship with Cyber Forensics, as indicated by the Laws and Regulations dimension. A fully prepared forensic investigator should have a certain degree of legal knowledge.
- **Component 7: New Technology.** Similar to world trends, new technology, has a persistent influence on Cyber Forensic knowledge.

Forensic investigators need to update their knowledge on new technology constantly to ensure their own forensic readiness.

3.4. Scope

The Scope dimension addresses the practical problems related to Live Forensics. The concept of Live Forensic Acquisition is viable, but the identified practical problems drastically limit the scope of applicability of the dimension.

This study identified five components (practical problems) that define the scope of the Live Forensic discipline. At the moment, these components still pose serious problems to the successful admission of evidence to court, but the *Liforac model* provides guidelines on handling these problems. This dimension divides into five components:

- **Component 1: Access to the machine.** Not only must the investigator gain access to the building in question, but also to the office in which the computer is located, as well as to the physical machine by means of a username/password combination. Some investigations are covert, whilst others are overt. Both types bring about their own complications.
- **Component 2: Dependency on operating system.** The current forensic practices require the forensic investigation to interact with the suspect machine's operating system. Each operating system needs to be treated differently during a forensic investigation and can pose a practical problem.
- **Component 3: Data modification.** Any process, from user applications to the operating system itself, can modify computer data during acquisition. With current legislations, any data modification can render the evidence inadmissible in court.
- **Component 4: Demonstrate authenticity of the evidence.** All potential data of evidentiary value need to be properly authenticated before a court of law can accept it as legit evidence.
- **Component 5: Court acceptance.** Computer technology and digital evidence have not always been accepted by the judicial system. Without the court's extensive knowledge of all new technological developments, forensic investigators may have some trouble to introduce digital evidence.

Each of these dimensions gives origin to a number of components, based on the drivers identified in this paper.

3.5. Identifying Drivers

Cyber Forensics investigations are no longer viewed purely from a technical perspective. Business, system and legal aspects, as well as knowledge and practicality are all incorporated to encompass a single complex discipline (Ieong 2006:32). To ensure a balanced model that addresses all these aspects, the authors identified drivers to serve as building blocks for the *Liforac model*. In context of this paper, a *driver* can be seen as the motivating force behind a specific action. These actions serve as core concept behind specific parts of the *Liforac model.*

The in depth discussion and weighting of each of the 90 identified drivers are beyond the scope of this paper. However, the methodology followed is relatively straightforward. Firstly, an intense literature study was done on the Cyber Forensic discipline and drivers were identified as part of this research. These drivers can loosely identify as any definition, concept or detail that may be of importance to the development of a comprehensive Live Forensic Acquisition model. Each of the identified drivers are then individually considered and grouped according to theme. The resulting themes include a **knowledge** component, a link with **time or sequence,** a **legal or regulatory** component and **potential problems**.

These themes are further researched and elaborated on to eventually merge into a single model with four distinct dimensions: the *Liforac model.* The grouping according to themes is based on the opinion of the authors:

- the *Laws and regulations dimension* consists of 41 drivers (an example driver of this dimension is the retrospective profiling nature of Cyber Forensics);
- the *Timeline dimension* consists of 10 drivers (an example driver of this dimension is the role of the First Responder in the Cyber Forensic investigation process);
- the *Knowledge dimension* consists of 29 drivers (an example driver of this dimension is the Cyber Forensic methodology); and
- the *Scope dimension* consists of 10 drivers (an example driver of this dimension is that the accuracy of results and the integrity of digital evidence need to be maintained at all times).

4. Forensic Soundness

Evidence can either make or break an investigation. It is crucial to ensure that all evidence is admissible in court and considered as forensically sound. Should the court reject any item of evidence, it can hurt the case. At the very least, this rejection can portray the investigators as incompetent.

According to Bejtlich (2006), a forensically sound copy of a hard drive is *"… created by a method that does not, in any way, alter any data on the drive being duplicated."* A forensically sound duplicate must contain a copy of every bit, byte and sector of the source drive, including unallocated empty space and slack space. A forensically sound duplicate will not contain any data other than that which was copied from the source drive. He further states that a forensically sound copy of a drive is *"…may inherently … alter the source evidence, but does not explicitly alter the source evidence".*

Since neither of these definitions of forensic soundness allows any leeway for Live Acquisitions, Murr redefined forensic soundness by adding *"… the manner used to obtain the evidence must be documented, and should be justified to the extent applicable"* (Murr N.D.). The complete *Liforac model* includes an entire section of the chain of custody, the responsibility matrix and the audit trial that jointly guarantees forensic soundness in all reasonable cases.

5. Conclusion

This paper focused on the further development of the Live Forensic discipline. The motivation of this study is based on the hypothesis that allows forensically sound acquisition to stand fast in a court of law. It showed that Live Forensic Acquisition is as comprehensive as Dead Forensic Acquisition, by considering the general Cyber Forensic discipline, forensic tools, practical problems experienced during acquisition, legal aspects and cyber crimes. Considering the study as a whole, it successfully completed all the objectives set out to present a forensically sound Live Acquisition model.

6. References

Bejtlich, R. 2006. *Forensically Sound Evidence*. Tao Security. Available from: http://taosecurity.blogspot.com/2006/08/forensically-sound-evidence.html (Accessed 20 March 2008).

Carrier, B. & Spafford, E. 2003. Getting physical with the digital investigation process. *Digital Evidence.* Volume 2, Issue 2. Pp 1 – 20.

Forte, DV. 2008. Volatile data vs. data at rest: the requirements of digital forensics. *Network Security.* Volume 2008, Issue 6. Pp 13 - 15.

Ieong, RSC. 2006. FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation.* Volume 3, Supplement 1. Pp 29 – 36.

Jones, R. 2007. *Safer Live Forensic Acquisition.* University of Kent at Canterbury. Available from: http://www.cs.kent.ac.uk/pubs/ug/2007/co620-projects/forensic/report.pdf (Accessed 11 January 2008).

Maat, SM. 2004. *Cyber Crime: A Comparative Law Analysis*. University of South Africa. Available from: http://etd.unisa.ac.za/ETD-db/theses/available/etd-08172005-103637/unrestricted/00front.pdf (Accessed 14 January 2008).

Murr, M. *Windows Incident Response - What is 'forensically sound"?* Available from: http://windowsir.blogspot.com/2006/08/what-is-forensically-sound.html (Accessed 4 August 2008).

Pan, L. & Batten, LM. 2005. *Reproducibility of Digital Evidence in Forensic Investigations.* 2005 Digital Forensic Research Workshop (DFRWS), New Orleans. Available from: http://www.dfrws.org/2005/proceedings/pan_ reproducibility.pdf (Accessed 16 April 2009).

Stimmel, CL. 2008. *Best Practices for Computer Forensics in the Field.* Available from: http://ezinearticles.com/?Best-Practices-for-Computer-Forensics-in-the-Field&id=124243 (Accessed 10 January 2008).

US-CERT. 2007. *Quarterly trends and analysis report.* Available from: http://www.us-cert.gov/press_room/trendsandanalysisQ107.pdf (Accessed 17 January 2008).