A BEST PRACTICE APPROACH TO LIVE FORENSIC ACQUISITION

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

[1] Council for Scientific and Industrial Research, Pretoria, South Africa

[2] Academy for Information Technology, University of Johannesburg

[1] marthiegrobler@gmail.com, mgrobler1@csir.co.za, 012 841 3262

[2] basievs@uj.ac.za, 011 559 2843

ABSTRACT

The development of the Live Forensic discipline instigates the development of a method that allows forensically sound acquisition to stand fast in a court of law. The study presents the development of a comprehensive model for forensically sound Live Forensic Acquisition, the *Liforac model*.

The *Liforac model* presents a number of concepts that are already available within the Cyber Forensics discipline, combined as a single document. It composes four distinct dimensions: *Laws and regulations*, *Timeline*, *Knowledge* and *Scope*. These dimensions combine to present a wide ranging model to guide First Responders and forensic investigators in acquiring forensically sound digital evidence. The dimensions were identified as part of an intense research study on the current application of Live Forensics and the associated problems and suggested controls.

The *Liforac model* is an inclusive model that presents all aspects related to Live Forensic Acquisition, suggesting ways in which a Live Forensic Acquisition should take place to ensure forensic soundness. At the time of writing, this *Liforac model* is the first document of this nature that could be found for analysis. It serves as a foundation for future models that can refine the current processes.

KEY WORDS

Forensically sound, Live Forensic Acquisition, Cyber Forensics, model

A BEST PRACTICE APPROACH TO LIVE FORENSIC ACQUISITION

1 INTRODUCTION

Up to date, forensic investigators approached live 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 and traditional crimes are committed using advanced technology (Maat 2004:i). These developments leave Law Enforcement outdated and therefore Forensic investigators need to turn to Live Forensics to ensure successful investigations.

There is a close relationship between Cyber Forensics and the justice system. US-CERT (2005:1) defines Cyber Forensics as *"… the discipline that combines elements of law and computer science to collect and analyse data from computer systems, networks, wireless communications and storage devices in a way that is admissible as evidence in a court of law"*. This results in evidence admissible in a court of law (Jones 2007:2). Now, forensic investigators can acquire even more forensically sound evidence when implementing Live Forensic Acquisition.

This paper discusses a theoretical approach that underwrites forensically sound Live Acquisition, presented as the *Liforac model*. The model allows forensic evidence to stand fast in a court of law and covers all aspects relevant to Live Forensics. Although the idea of this model is not to present a rigid restrictive set of steps to follow, the intention is to develop a full set of guidelines to assist forensic investigators throughout the Live Forensic Acquisition process.

The proposed theoretical model consists of four distinct dimensions. These dimensions were identified as part of a research study on the current application of Live Forensics and associated problems and controls. Section 2 addresses the Live Forensic discipline and some of the associated benefits. Section 3 walks through the development of the model, addressing each of the dimensions. Section 4 concludes the paper.

2 MOVING TOWARDS LIVE FORENSIC ACQUISITION

Live Forensics, referred to as Incident Response, is a methodology that advocates extracting live, real time system data before shutting down the system to preserve memory, process and network information that would

otherwise be lost in a traditional forensic acquisition. The essence of this acquisition type is to minimise impacts to the integrity of the system while capturing volatile forensic data (McDougal 2006:5,9). Live Acquisition refers to the acquisition of a machine that is still running and can retrieve both static and dynamic, volatile data (Forte 2008:13). Traditional Dead Forensics focuses only on collecting and analysing information from stagnant file systems.

The Live Forensic discipline has not been perfected yet. Currently all endorsed tools and techniques have minor impacts on the underlying system's operating state and can be considered in court as inadmissible (McDougal 2006:5). However, forensic investigators argue that a complete chain of custody document should be sufficient to explain and motivate any system changes and accordingly lead to court admissibility. Some changes can be explained in the context of the investigation, analogous to the explanation of a detective's fingerprints on a ransom note (Adelstein & Richard 2007:14).

The main benefit of this Live Acquisition model is consistent and verifiable forensic acquisitions. Another benefit is that it requires little or no downtime from the system in question and that it can retrieve data that is only available in RAM (Adelstein & Richard 2007:3).

3 DEVELOPING A FORENSICALLY SOUND MODEL

To develop a useful model, it is necessary to include a number of wide ranging components to cover all aspects relevant to Live Forensics. Forensic investigators are responsible for technical insight, knowledge of the law and complete objectivity during investigations. Only then can investigators present direct evidence of suspected misconduct or potential exoneration (Stimmel 2008:1). The best way to ensure verifiable and repeatable results is by creating the *Liforac model* that investigators can apply consistently.

Figure 1 presents the proposed *Liforac model*, comprising of four distinct dimensions: *Laws and regulations*, *Timeline*, *Knowledge* and *Scope*. These dimensions combine to present a model that guides First Responders and forensic investigators in acquiring forensically sound digital evidence. The dimensions were identified as the four most prominent aspects during the preliminary literature study. A number of drivers were identified in the preliminary study that strongly directed the decision to divide the model into these four specific dimensions. The extent of these drivers is beyond the scope of this paper.

The *Liforac model* can prove useful to explain the work of cyber crime investigators to non-specialists. This can be especially supportive when presenting digital evidence in a court of law (Ciardhuáin 2004).

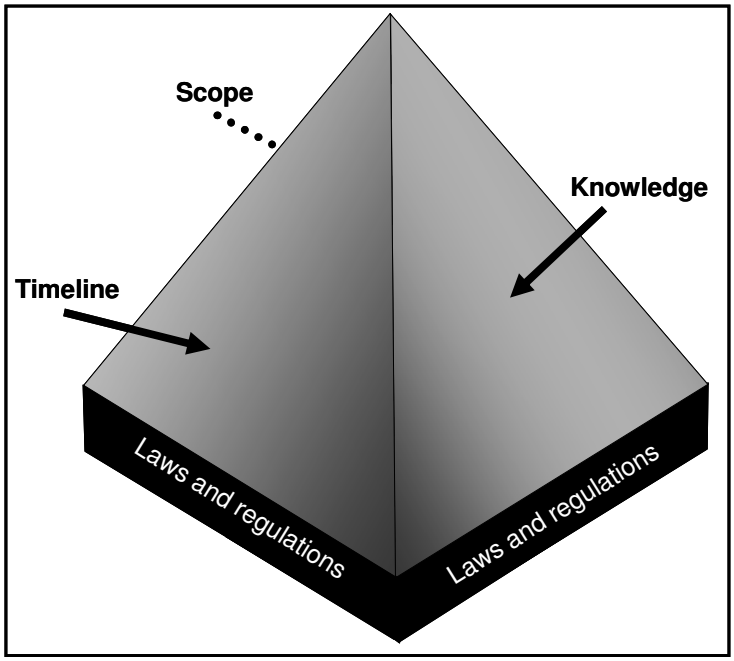

Figure 1: Liforac model

3.1 Laws and Regulations

The *Laws and regulations dimension* is the foundation of the *Liforac model*, forming the basis on which these dimensions rest. It considers in detail what the forensic investigator needs to know and do concerning laws and regulations to remain within the legal bound of the discipline. This dimension is not legally binding, but merely guides the organisation towards better technical understanding with regards to a legal subject.

With the emerging cyber crime rates and hike in cyber crime incidents, the *Laws and regulations* dimension is a very important part of the *Liforac model*. Not only is it necessary to pay attention to all aspects of cyber crime in order to do this, but these crimes need to relate to the legal discipline. This dimension divides into four sub dimensions:

- **Sub dimension 1: Common crime laws applicable to cyber crime.** Common crime laws, referred to as penal laws, are existing laws

created with only traditional crimes in mind. The stakeholders wrote the laws in such a manner that interpretation within given circumstances can include the legal punishment of acts related to computers, digital evidence and cyber issues (Nare 2008).

- **Sub dimension 2: Specific cyber laws.** These laws, known as netlitigation, refer to laws created specifically with cyber crimes in mind. It addresses current issues related to cyber space, computers and electronic media or communication. Specific cyber laws are much more detailed and worth more in the event of a legal interpretation dispute. It helps organisations to prepare their systems for faster recovery in a cyber event and educate users on preserving electronic evidence.
- **Sub dimension 3: Court cases and precedents.** Court cases and precedents are crucial in the acceptance of any new technology in court. A court precedent can be defined as a *"… legal principle, created by a court decision, which provides an example or authority for judges deciding similar issues later"* (Lectric Law Library 2005). Precedents in court cases establish a principle or rule that another court needs to adopt when deciding cases with similar issues or facts. These laws are crucial in the acceptance of any new technology in court, for examples the Frye and Daubert tests.
- **Sub dimension 4: Definition of court admissibility.** The definition of court admissibility largely determines whether the court would allow Live Forensic Acquisition. This definition and its implementation has a big impact on the Live Forensic discipline and is in many cases the most important aspect to consider during the lifetime of a forensic investigation. To ensure that evidence can be admitted in court, the forensic investigator needs to ensure and maintain the accuracy, reliability and authenticity of the evidence at all times. The easiest way to accomplish this is by maintaining a proper chain of custody.

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. This dimension considers in detail what steps forensic investigators need to take to ensure a forensically sound investigation.

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 presents it visually in the sequence it

should execute to ensure sound forensic practices. In essence, this specific timeline representation consists of implied and explicit processes. This dimension divides into five components:

- **Component 1: Implied processes.** These processes refer to specific processes that may not necessarily contribute directly to the successful completion of the dimension, but the absence of these processes may render the timeline unsuccessful. Implied processes specific for the *Liforac model* include how to secure potential evidence, how to preserve data integrity, how to record actions during an examination, the audit trail, how to analyse the collected data and information, and the establishment of a responsibilities matrix (Haggerty & Taylor 2006:14).
- **Component 2: Explicit processes.** These processes refer to specific processes that contribute directly to the successful completion of the dimension. Explicit processes specific for the *Liforac model* include awareness, authorisation, planning, notification, search for and identification of evidence, examination of evidence, hypothesis and the dissemination of information. These processes are largely based on Ciardhuáin's (2004) model.
- **Component 3: Before the investigation.** This timeframe ensures full coverage of all possible activities involved before the actual acquisition starts. Not only is it necessary to prepare all the people on the case involved, but a solid foundation might help the case in court. This timeframe has three themes: *awareness*, *authorisation* and *planning*. The sub activities include determining the power status of the computer and system, selecting the investigation mode (overt or covert), isolating the system in question and secure it promptly, selecting the analysis mode (local or remote) and comprehensive pre-acquisition planning.
- **Component 4: During the investigation.** This timeframe ensures full coverage of all possible activities for the duration of the acquisition. It guarantees that investigators collect all the necessary evidence in a manner that will lead to its successful admission in a court of law. Opposing counsel often question the integrity of this acquisition process and occasionally prove an inadequate chain of custody that lead to the exclusion of crucial evidentiary artefacts from the proceeding. This is often based on methods and techniques used during the acquisition process. This timeframe has three main themes: *notification*, *search and identify,* and *examination.* The sub activities include the chain of

command, write blocking the target system, attaching the suspect hard drive to a forensic system, identifying logged on account and administrative rights, identifying the logged on system (real or virtual) and making a bit-by-bit copy of the suspect hard drive.

- **Component 5: After the investigation.** This timeframe ensures full coverage of all possible activities involved after the actual acquisition ends. This ensures that the chain of custody remains intact and the evidence are stored and returned safely after the investigation. This timeframe has three main themes: *hypothesis*, *information dissemination* and *controls.* The sub activities include updating the chain of command, securely sealing all packages, transporting and storing evidence, examining and analysing evidence with forensically sound software and providing a written report.

3.3 Knowledge

The *Knowledge* dimension indicates the different stages of awareness and understanding investigators need to perform sound Live Forensics. This dimension looks in detail at the people involved in successful Live Forensics: who they are and what training and skills they should possess.

With the ever-changing technologies, tools and techniques, forensic investigators need to stay updated with all new developments. To ensure that investigators are fully prepared for any type of forensic investigation, they need to ensure that their knowledge is up to standard to allow for any eventualities. This dimension divides into seven components:

- **Component 1: Computer Science.** Computer science is a wide discipline, containing a wide range of topics. For the purpose of being a forensic investigator, it is recommended that the individual have a proper computer science foundation and background. Although a computer science degree is not enforceable, it may help the investigator in understanding basic concepts. The knowledge built from these specialised topics may be helpful in certain forensic investigations. In some cases, computer science knowledge may be applied directly, whilst in others it ensures that investigators are more familiar with the specific scenario found at the crime scene.
- **Component 2: World Trends and Events.** World trends and events have a continual influence on Cyber Forensic knowledge. Forensic investigators need to update their knowledge on new trends in cyber crime and the combating of these crimes constantly. World

trends and events can have a dramatic impact on technology and related trends. In this case, it may be very helpful for forensic investigators to work in conjunction with the local CERT/CSIRT. These organisations work closely with CERTs/CSIRTs in other countries and can draw statistics regarding technological attack trends. For example, once a specific worm hits a specific country, it might take an average of 48 hours before the same worm generally hits South Africa. Cyber investigators can benefit from these statistics.

- **Component 3: Information Systems.** Information Systems are the organised collection, storage and presentation of information and related knowledge for decision-making. It can be defined as a collection of practices, algorithms and methodologies that transforms data into information and knowledge that is useful for individuals or groups of people (UMBC 2008). A proper information system foundation can aid a forensic investigator in the understanding of certain forensic principles and the interaction between the cyber criminal and his/her computer. Since there is a direct relationship 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 human and profiling nature. People tend to react in specific ways under certain circumstances, which may have an affect on the way the investigation is run. Forensic investigators now not only understand the hardware and software aspects of the suspect machine, but also may try to think like the person operating the suspect machine. He/she may psychologically step into the suspect's footsteps and think where the suspect may have hidden evidentiary files and folders. This discipline is not a prerequisite for forensics, but may make the investigator's task easier when the behavioural aspect is also considered.
- **Component 5: Forensic Sciences.** Forensic sciences are the core of Cyber Forensic investigations. When considering Biological Forensics, a basic understanding of this discipline contributes to a better understanding of Cyber Forensics. Many of the investigatory principles remain the same, although the physical application of the techniques and the tools differ drastically. A general understanding of this discipline may be beneficial.
- **Component 6: Law.** Cyber Forensics cannot stand separate from the law. Any forensic investigator need to have updated

knowledge on current and pending legislation that may have an impact on the way forensic investigations are done. This aspect is so important that forensic investigators should not be allowed to enter the crime scene without sufficient knowledge for fear that they might contaminate the crime scene. A fully prepared forensic investigator should have a certain degree of legal knowledge.

- **Component 7: New Technology.** New technology, similar to world trends, has a persistent influence on Cyber Forensic knowledge. Every time new technology is publicly available, or an upgrade of software or a hardware component is on the shelves, investigators need to be trained on this. The chances are good that investigators may encounter these new technologies in an investigation. If they do not know how to handle these upgrades properly, investigators may encounter problems that may have a negative effect on the investigation. Forensic investigators need to update their knowledge on technology constantly to ensure their own forensic readiness.

3.4 Scope

The *Scope* dimension addresses practical problems related to Live Forensics. The concept of Live Forensic Acquisition is viable, but the identified problems drastically limit the scope of applicability of the dimension. This dimension looks in detail at the problems associated with Life Forensic Acquisition and identified five components, or 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* will provide guidelines on handling these problems. This dimension has five components:

- **Component 1: Access to the machine.** Gaining access to the machine is the first practical problem that an investigator may encounter. Not only must the investigator gain access to the building and specific office in which the computer is located, but also to the physical machine by using a username/password combination. Some of the controls for this practical problem include a legit search warrant, cooperation from the suspect and system administrator and reasonable.
- **Component 2: Dependency on operating system.** The current forensic practices require interaction with the suspect machine's operating system. Each operating system needs to be treated differently during a forensic investigation and accordingly can pose a major practical problem. This practical problem has one

possible control to counter this dependency: a thorough foundation of related knowledge.

- **Component 3: Data modification.** Any process can modify computer data during acquisition, from user applications to the operating system itself. With current legislations, any data modification can render the evidence inadmissible in court. Some of the controls for this practical problem include thorough forensic training and up-to-date research.
- **Component 4: Demonstrate the authenticity of evidence.** All potential evidence needs to be properly authenticated before a court of law can accept it as legit evidence. This practical problem has a number of controls: expert witness testimony, comparison by expert witnesses with precedents, circumstantial evidence, public records, evidence produced as result of an accurate process or system, evidential weight, digital signatures, hashing techniques, timestamps and checksums.
- **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. One control has been identified for this practical problem: awareness and education.

4 CONCLUSION

Irrespective of the method of retrieval, investigators present the evidence to court. If the data are admissible in court, cyber investigators refer to it as forensically sound. Very few courts currently accept Live Forensic Acquisition as forensically sound due to the lack of court precedence and criminals' liking to exploit new technology in an innovative manner.

The development of the Live Forensic discipline and acquisition technique instigated the development of a method that allows forensically sound acquisition to stand fast in a court of law. The hypothesis of this paper is that forensic investigators using the *Liforac model* are likely to be more successful in a court of law. The application of this model is not a foolproof method to ensure that a case will be won in court, but rather a method to ensure that opposing counsel cannot argue forensically unsound methods and techniques.

The *Liforac model* is a comprehensive model that presents all aspects related to Live Forensic Acquisition, suggesting ways in which a

Live Forensic Acquisition should take place to ensure forensic soundness. At the time of writing, this *Liforac model* is the first document of this nature that could be found for analysis. It serves as a foundation for future models that can refine the current processes.

5 REFERENCES

Adelstein, F. & Richard, GG. 2007. *Live Forensics Tutorial. Part 2: Live Forensics.* Available from: boanchanggo.tistory.com/attachment/hk360000000001.ppt (Accessed 3 April 2009).

Ciardhuáin, SO. 2004. An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence*. Volume 3, Issue 1. Pp 1 - 22.

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

Haggerty, J. & Taylor, M. 2006. Managing corporate computer forensics. *Computer Fraud & Security.* Volume 2006, Issue 6. Pp 14 - 16.

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).

Lectric Law Library. 2005. *The 'Lectric Law Library's Lexicon on Precedent.* Available from: http://www.lectlaw.com/def2/p069.htm (Accessed 30 October 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).

McDougal, M. 2006. *Live Forensics on a Windows System: Using Windows Forensic Toolchest (WFT).* Available from: http://www.foolmoon.net/downloads/Live_Forensics_Using_WFT.pdf (Accessed 3 April 2009).

Nare, S. 2008. Personal interview. 10 September 2008.

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).

UMBC. 2008. What is an Information System (IS). *University of Maryland, Baltimore County.* Available from: http://www.is.umbc.edu/aboutIS.asp (Accessed 10 November 2008).

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