Live Forensic Acquisition as Alternative to Traditional Forensic Processes

Marthie Lessing[1], Basie von Solms[2]

[1]Council for Scientific and Industrial Research
Meiring Naudé Road, Scientia
Pretoria, South Africa
marthie.lessing@gmail.com

[2]Academy for Information Technology
University of Johannesburg
Auckland Park Kingsway Campus
Johannesburg, South Africa
basievs@uj.ac.za

Abstract: The development of live forensic acquisition in general presents a remedy for some of the problems introduced by traditional forensic acquisition. However, this live forensic acquisition introduces a variety of additional problems, unique to this discipline. This paper presents current research with regards to the forensic soundness of evidence retrieved through live forensic acquisition. The research is based on work done for a PhD Computer Science at the University of Johannesburg.

1 Introduction

Both computer and non-computer professionals use computers every day. Accordingly, it is safe to say that computers play a significant role in both business and personal life, and that the resultant technological advances are remarkable.

One of the bigger Information Technology advances was the creation of the Internet to connect people globally. Unfortunately, the Internet not only aided worldwide communication and commerce, but also sparked the growth of electronic crime. Criminals now make use of computers on a daily basis to assist with and to commit crimes.

To act against these electronic offenders, it is necessary to develop new processes and techniques to retrieve evidence from computers. Specialists commonly refer to this discipline as Cyber Forensics [BJ05].

1.1 Defining Cyber Forensics

According to Jones [Jo07], Cyber Forensics is *"… the process of copying data from a computer in a forensic manner"*. Another definition is *"… 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"* [Us05].

There are a number of definitions available, varying with regards to the extent of the forensic process. However, it is generally accepted that forensic acquisition includes the transportation of the data from the crime scene to a safe location and safe storage, but excludes the interpretation of the acquired data.

The Federal Bureau of Investigation started to formally employ Cyber Forensics in 1984 as part of their criminal profiling initiative [Fe07]. In this regard, Cyber Forensics classifies as a retrospective profiling type, which is generally case specific and after the fact [NTV05]. Forensic investigators only enter the crime scene after the crime has been committed, and therefore need to follow a specific set of steps to avoid contamination or corruption of the evidence. Should the investigator contaminate the crime scene, it is likely that the evidence will not be usable in court.

Heated discussions exist in the world of Cyber Forensics. The two most prominent arguments are regarding pulling the plug (dead digital forensics), or exercising the analysis on a live, running system (live digital forensics). Whichever of the modes are applied, the basic Cyber Forensic methodology consists of three important principles:

- acquire the evidence without altering or damaging the original;
- authenticate that the recovered evidence is the same as the originally seized data; and
- analyse the data without modifying it [KH02].

The current forensic best practice is to unplug a machine to acquire an image of the hard drive. This technique can cause data corruption, system downtime and consequential revenue loss for businesses. Section 3 discusses this dead forensic acquisition in more detail. A newer technique, live forensic acquisition, emerged to counteract some of the problems caused by dead forensic acquisition. This technique refers to the acquisition of a forensically sound system image from a live machine, i.e. a machine that is still running. The system image can range from a mirror copy of a single USB drive, to a computer hard drive or a comprehensive image of the system network. Section 4 introduces live forensic acquisition in more detail.

1.2 Research Problem

The development of new criminal techniques leaves law enforcement techniques outdated. As a result, crime scene investigators cannot always apply dead digital forensics successfully to gather sufficient evidence to lead to a conviction. In response, cyber specialists developed live forensic acquisition techniques to specifically target these new criminal techniques. These new live forensic techniques, however, still need to be tested thoroughly before the law enforcement discipline will adopt them.

Unfortunately, despite the numerous benefits posed by live forensic acquisition, it brings about technical and legal difficulties as well: forensic investigators need to convince the court that their forensically acquired image is a true unaltered copy of the original. (This is necessary regardless whether the acquisition method is dead or live, but it is more complicated to prove with live forensic acquisition.) At present, there is no commonly accepted method of doing live acquisition and additional research is necessary. However, preliminary research presents a very viable attitude towards live forensic acquisition as alternative to traditional forensic acquisition.

2 Forensic Acquisition Process

Technically the forensic acquisition process should only incorporate the evidence collection stage. However, to ensure the forensic soundness of the acquired evidence, a comprehensive acquisition needs to start with the collection of evidence, and end with the successful transport and storage of the evidence. The next paragraphs will introduce the steps that form the forensic acquisition process. This applies to both dead digital forensics and live forensic acquisition.

2.1 Access the Acquired Device

Kruse and Heiser [KH02] list three methods to access the acquired device. Depending on the acquisition mode that the investigator chooses to follow, access to the acquired device might be different.

- The first method is to pull the power plug from the back of the computer (dead forensic acquisition - Section 3).
- The second method is to follow the normal administrative shut down procedure (dead forensic acquisition - Section 3).
- The third method is to keep the system running (live forensic acquisition - Section 4).

Regardless of which acquisition method is used, the very first step in any forensic investigation should be the isolation of both the system and the relevant data. The purpose of this isolation is two-fold: isolation can prevent the corruption of other systems, reducing the risk of a cascading failure throughout the organisation's IT infrastructure, and isolation freezes the state of the affected system, preserving an exact image to assist in the subsequent investigation [WP05].

Investigators should collect information by interviewing system administrators and other users who might have had contact with the affected system [WP05]. In the event of a covert investigation, interviews might not always be possible. However, investigators should still try to gather as much information about the system before starting the acquisition process. Occasionally it might be possible to retrieve passwords beforehand, saving valuable time and effort on the investigator's side.

Once the system is completely isolated, the investigator should collect all possible non-technical information, such as the suspect's office attendance in the days preceding the incident. This information assists in establishing a potential time line of events leading to the suspected cyber crime [WP05].

To develop this timeline further, the investigator needs to check the BIOS (Basic Input Output System). The BIOS provides a variety of critical information, such as the time and date. It is also possible to identify the HPA (Hardware Protected Areas) and the DCO (Device Configuration Overlays) on the computer by investigating the BIOS. One method is to compare the hard drive settings stored in the CMOS with the values on the drive's labels. Alternatively, the investigator can do a similar comparison with a series of ATA commands (READ_NATIVE_MAX_ADDRESS and IDENTIFY_DEVICE). Some forensic applications, such as TSK and Maresware, also allow for the detection of a HPA presence. The HPA and the DCO are reserved areas for data storage outside the normal operating system file system. Since these areas are normally used for specialised application data and configuration data, forensic investigators do not necessarily search these areas for additional hidden data. Accordingly, knowledgeable cyber criminals can store incriminating data in both the HPA and the DCO [Be05]. Should the two sets of compared values differ, the investigator knows that there exist a HPA and can make a more specialised effort of locating these files.

Once the investigator identified the existence of the HPA and DCO, s/he can make a full bitstream copy of the system to copy these hidden areas [St08]. When this process is complete, the forensic investigator can initiate the forensic acquisition with a write blocker to prevent accidental writing to the protected hard drive.

2.2 Initiate the Acquisition with a Write Blocker

During forensic acquisition and analysis, it is possible to write to the evidence drive accidentally. Since this will lead to the immediate dismissal of the evidence from court, the investigator should take care not to compromise the evidence. The easiest way to ensure this is to use a write blocker.

A write blocker allows a system to read data from an external drive at full speed. At the same time, it blocks any write commands to the external drive to prevent the unauthorised modification or formatting of the drive under examination [Pa07]. Normally a computer writes data to, or reads data from a storage device via specific commands, transmitting these commands from the computer's interface connection to the storage device's interface connection. By using a write blocker, the investigator prevents the computer from writing to the evidence hard drive's interface [Ni03a].

There are two types of write blockers: software write blockers and hardware write blockers. A *software write blocker* replaces a hard drive access interface on a computer with external hard drives. It blocks any commands that could modify a hard drive [Ni03b]. A *hardware write blocker* is a hardware device that physically attaches to a computer system. Its main purpose is to intercept and block any modifying commands from reaching the storage device [Ni03a].

It is of high importance to preserve the evidence and create copies of the evidence for analysis purposes [WP05]. After the physical acquisition, coupled with the write blocker, it is necessary to document the incident and all the actions taken by the investigators. The chain of custody, discussed in the next section, reflects this.

2.3 Chain of Custody

In any investigation, the acquired data and devices should be accounted for during the entire extent of the forensic acquisition process. Technically, this chain of custody should commence the moment the forensic investigator enters the crime scene, and continue until the court case completes. Although this step does not only belong to the acquisition phase, it forms a fundamental aspect of the case's validity and the forensic soundness of the evidence.

According to Ghelani [Gh06], chain of custody defines as *"… the gathering and preservation of the identity and the integrity of the evidential proof that is required to prosecute the suspect in court"*. Scalet [Sc05] provides another definition: *"… A chain of custody is the process of validating how any kind of evidence has been gathered, tracked and protected on its way to a court of law"*. In essence, it is the maintenance of the integrity of the evidence from seizure until the time the investigator produces it in court [Tr94]. It serves to make it difficult for a defence attorney to argue that the forensic investigator tampered with the evidence whilst in his/her custody [KH02].

The ability to prosecute any case rests on the validity of the evidence used in court. A court considers evidence valid if forensic investigators can prove that the evidence is in the same condition as during the original seizure. To do this, people who handled the evidence should testify as to the condition the evidence was in before and after it entered their possession. The proper use of a chain of custody can replace this tedious process of testifying [Tr94]. Complete and accurate chain of custody logging procedures help to ensure that the court will authenticate electronic data. It is therefore crucial to ensure that the chain of custody adheres to the prescribed standards [Le08].

2.4 Transport and Storage of Evidence

To complete the Cyber Forensic acquisition process, the evidence needs to be transported from the crime scene to the forensic laboratory. At the laboratory, the evidence will be stored securely, unless it is being analysed by the forensic investigators.

Magnetic media are in general very sensitive, and not originally created with transport in mind. Accordingly, it is necessary to take certain precautions to ensure that the evidence arrives without any damage. For example, both during transportation and storage, the evidence should be stored in static-free packaging. Additionally, to ensure that nobody tampers with the evidence during transportation or storage, the last investigator to handle the evidence at the crime scene should seal the package and sign the seal. If anybody attempts to open the package, the seal will be broken and the signature spoiled. Every time somebody needs to access the evidence, the old package should be put into a new package, and the new package be sealed and signed [KH02].

Some court cases are inevitably postponed several times, and can range a number of years. Accordingly, it is necessary to control *bit rot*. According to Church [Ch07], bit rot can be defined as *"… the degradation of magnetic media over time"*. It can be hugely problematic if your evidence has deteriorated beyond use when your court date comes up. It is therefore crucial to protect your evidence as best as possible, and use the original data as little as possible. This will not stop the deterioration, but at least slow it down [Au08].

3 Traditional Forensic Acquisition

The first of the two Cyber Forensic acquisition modes is dead acquisition analysis, often referred to as the traditional digital method. Dead acquisition involves examiners pulling the plug on a suspect system, avoiding any malicious process from running on the system and potentially deleting data from the system. It allows the examiner access to create a snapshot of the swap files and other system information as it was last running [St08].

A formal definition of dead acquisition analysis is *"… analysis done on a powered off computer"* [Jo07]. Usually there are four stages to traditional digital forensics:

- **Collection** entails the process on location: search and seizure and the acquisition of information in a forensically sound manner. The main actions are the forensic disk duplication and collection of random evidence, such as CDs, scraps of papers and personal interviews.
- **Examination** composes both a manual and an automatic investigation of the acquired data. This stage aims to identify and extract data relevant to the specific case, and includes file system parsing and extraction of mailboxes.
- **Analysis** is the process of using the identified data in a manner to prove that the actions performed on the computer was done by one or more individuals. This stage involves browsing, querying and correlating existing data [Al06].

- **Reporting** is the last stage in which the forensic examiner reports the information gathered in a written form [Jo07].

The forensic copying process is not straightforward, but with sufficient training and the correct forensic software packages, forensic investigators can copy the hard drive image, complete with unallocated sectors, slack space and file metadata. This is generally done by copying the seized hard drive bit by bit [Jo07].

Figure 1 illustrates the forensic process. The forensic investigator first approaches the computer and determines its power status. If the computer is powered on, s/he turns it off by either pulling out the power plug, or following the proper shut down procedure. Once the power is off, the forensic investigator physically removes the hard drive from the system, attaches it as an external drive to a forensic system and copies its content. The investigator takes the necessary precautions to ensure that no data modification takes place on the external drive. Depending on the specific situation, the investigator may either return the hard drive to the original system, or bag it as evidence.

For many years, traditional forensics has been the only means to perform forensic acquisitions. It is a simple procedure to follow, and straightforward steps have been tried and tested to perform these actions. However, this technique presents both advantages and disadvantages, discussed next.

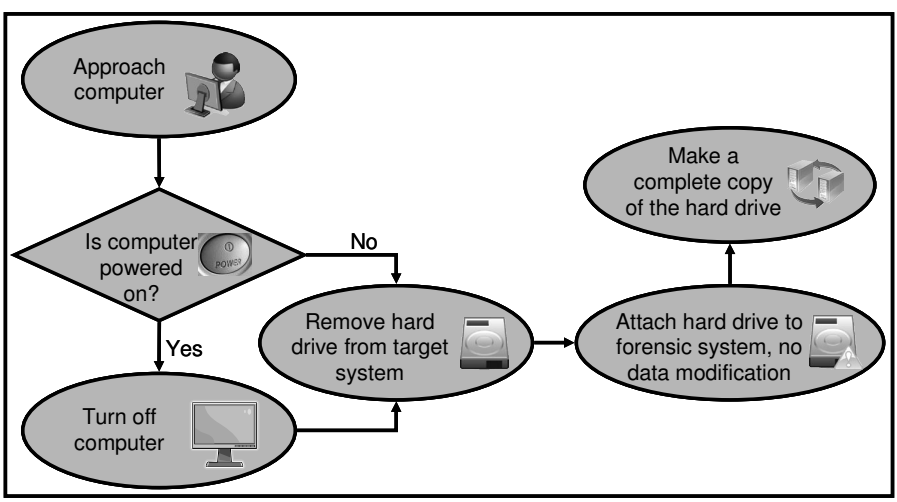

Figure 1: Traditional forensic analysis [Jo07]

3.1 Positive Aspects of Dead Acquisition Analysis

Under normal circumstances, the chance of forensic investigators accidentally overwriting or modifying evidentiary data is slim. Generally, sufficient precautions are in place to ensure that the computer allows *no modification during the copying process* to either the original or the copied image of the original hard disk [Jo07].

A distinguishing characteristic between dead and live forensics is that dead forensics cannot acquire live, volatile data. Once the computer is unplugged, the machine loses all the volatile memory in the RAM. However, a little known fact is that most modern *RAMs retain their contents for several seconds* after power is lost. The system does not immediately erase the volatile memory, but its content becomes less reliable when not refreshed regularly. A forensic investigator that is aware of this can therefore make use of this small window of opportunity to do a forensic acquisition [Ha08].

3.2 Limitations of Dead Acquisition Analysis

There are a number of limitations and problems associated with dead acquisition analysis. Some problems are more serious than other problems, but it is necessary to look at all instances.

- In response to the efficiency of dead acquisition analysis, criminals have resorted to the widespread use of *cryptography*. Now, even though forensic examiners have a complete bit for bit hard drive image of the suspect system, it is encrypted and of no practical value. In this scenario, the drive can only be decrypted with a unique password. Since investigators cannot always rely on a suspect's cooperation in supplying this password, the method of acquisition should be adjusted – if the same encrypted disk was acquired with live forensic acquisition, investigators would be able to access the disk. This whole-disk encryption is not only limited to criminals, but is now also a default feature of some operating systems.
- Another limitation of traditional forensic acquisition has surfaced in the light of *network data*. The need for acquiring network related data (such as currently available ports) grew dramatically. This type of information is volatile, and is lost in the event that the computer powers down - the foundation of traditional digital forensic analysis [Jo07].
- To comply with traditional forensic requirements, *all data must be gathered and examined* for evidence. However, modern computers consist of gigabytes, and even terabytes, of data to be analysed [LK04]. These complex technologies, coupled with cyber crimes becoming more advanced, lead to more complex and time-consuming digital investigations. It is increasingly difficult to use modern tools to locate vital evidence within the massive volumes of data. Log files also tend to increase in size and dimension, complicating a Cyber Forensic investigation even further [Fe07].
- A *lack of standardised procedures* leads to uncertainties about the effectiveness of current investigation techniques. In turn, this has led to the suboptimal use of resources. In some instances, investigators gather worthless

data that take unnecessary time. In addition, this data have to be stored and takes up valuable space [LK04].

- Many unique *practical and legal constraints* make the application of Cyber Forensics both interesting and defiantly complex. An example of a practical constraint would be if the suspect system were a public machine in an internet café with the owner claiming a possible loss of income for the duration of the forensic investigation. An example of a legal constraint is the restriction of the methods in which forensic investigators can obtain data. This is especially relevant when practising live forensic acquisition.
- If forensic investigators do not follow these restrictions exactly, data acquired in certain ways may be *inadmissible in court* and not allowed as intelligence [Jo07]. This negates the criminal investigation completely. For this reason, it is important that forensic practitioners are equipped with tools and mechanisms that can result in the acquisition of forensically sound system images. Only when this is possible, can data be seen as evidence and be admissible in a court of law.
- Already mentioned in Section 3.1, dead forensics is *not the optimal method to acquire live, volatile data*. Although modern RAMs allows a couple of seconds grace period in which the volatile data is not erased, this time is often too little to do a proper acquisition.

Due to the many limitations of traditional forensics, live forensic acquisition seems a likely alternative. This allows forensic practitioners to access a variety of invaluable information that would have been lost in traditional forensic analysis [Jo07]. Unfortunately, the practice of live acquisition brings about its own limitations, especially with regard to legal implications. The next section addresses this acquisition mode.

4 Live Forensic Acquisition

The method of live forensic acquisition is similar to the method of dead forensic acquisition. It developed in response to the shortcomings of the traditional forensic acquisition techniques, considering the retention of volatile data, and a countermeasure for encrypted files on a live system.

The acquisition philosophy is the same in that both methods need to ensure that the acquired image remains unchanged. The sequence of steps also applies to both dead and live acquisition (collection, examination, analysis, reporting). Investigators, however, should tailor the inner workings of the stages to allow for a forensically sound live acquisition [Jo07].

Figure 2 presents the forensic investigator's actions during live acquisition. The investigator first approaches the computer and determines its power status. If the computer is powered off, s/he continues with the dead forensic acquisition procedure discussed in Section 3.

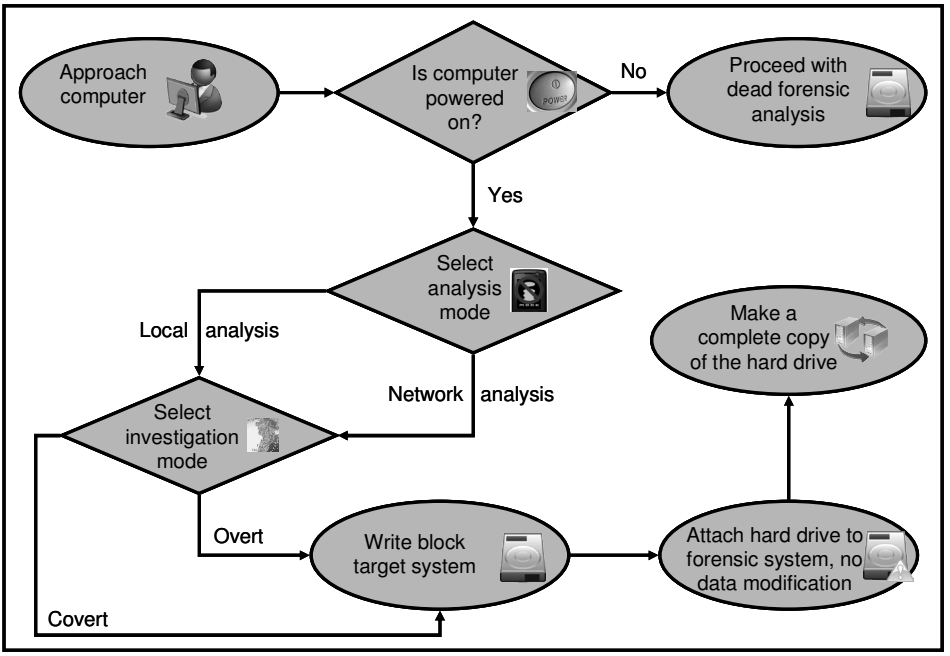

Figure 2: Live forensic analysis (Own compilation)

If the computer is switched on, the investigator first needs to select whether the data will be copied locally, or through the network. Additionally, s/he needs to decide whether the investigation will take place overtly or covertly. The investigator then attaches a write block system (either hardware based or software based) to both the suspect machine and as an external drive to a forensic system to copy the suspect machine's content. Of course, a live forensic investigation is a lot easier if the logged on account has administrative rights. However, should the current account not have administrative rights, the user functionality the investigator can work with depends on the rights assigned to the current account and the software already installed on the suspect system. The vast number of possible scenarios is beyond the scope of this paper.

During a live forensic investigation, it is necessary to determine whether the logged on account lies in a real or virtual environment. In essence, the different environments require the same investigation method. However, if the logged on account links to a virtual machine, the investigator needs to do further analysis to acquire both the real machine's system image, as well as other possible virtual machines located on the real machine. It may be difficult to detect whether the forensic investigator accessed a real computing environment, or a virtual machine. A number of techniques exist that can indicate whether a system is real or virtual. By far the easiest technique is to look for:

- copyright notes or vendor strings in various files;
- VMware specific hardware drivers;
- VMware specific BIOS;

- VMware specific MAC addresses;
- installed VMware tools; and
- hardware virtualisation (e.g. virtual sets of some registers).

However, these traces can be rather unreliable since it is easy to modify. A more reliable trace method is to do hardware fingerprinting, or checking for hardware that is always present in a virtual machine. In the case of Microsoft virtual machines, a clear indicator is if the motherboard is made by "Microsoft Corporation". DEVCON, a command line version of Device Manager, is also useful in detecting what hardware is in a system, identifying any virtual machine hardware. For example, REM Virtual Server and Virtual PC both have their IDE disks named "Virtual HD" [Ar05].

A more reliable technique is to install virtual machine detectors (or fingerprinting tools), but this software may have a negative impact on the forensic soundness of the evidence. Examples of these tools are the Red Pill, Jerry, ScoopyNG and VMware Virtual Machine Detector.

4.1. Positive Aspects of Live Acquisition Analysis

In response to the limitations of dead acquisition analysis, live acquisition analysis has surfaced as a remedy. This analysis allows forensic examiners to *retrieve volatile information* specific to the suspect system's network settings. In many instances, this information is invaluable to the prosecution of a cyber criminal. It is thus possible to view the development of live acquisition analysis as an improvement of current methods of both dead and live acquisition [Ni06].

In contrast with the procedural deficiency of traditional forensic acquisition, live forensic acquisition limits the amount of data gathered. Often investigators investigate large parts of the system, but only gather the relevant pieces of information [LK04]. Live acquisition *addresses this procedural deficiency*, but it introduces a number of other problems.

4.2 Limitations of Live Acquisition Analysis

Although live acquisition addresses most of the problems associated with dead forensic acquisition, it brings about additional problems:

- *Every computer installation is different*. Although there are many common components and aspects, computer users can compile their system to their own desire. For this reason, it is the forensic examiner's job to ensure that s/he has sufficient knowledge of a wide variety of hardware, software and operating systems. It is indeed possible to come across any combination of these components, and the examiner should be prepared to handle all of these. Due to the range of possibilities provided by live forensic analysis, forensic examiners only learn the principles of live acquisition and the effect that specific actions may have on the validity of the evidence. It is further up to the

interpretation of the examiner to analyse the situation, and apply the forensic principles in such a way that his/her actions can be justified in a court of law.

- *Data modification* during the acquisition process and the dependence of the forensic acquisition on the suspect system's operating system is two of the more prominent concerns regarding live forensic acquisition. If the acquisition process alters the data, courts will dismiss the data as forensically unsound. Part of the live acquisition forensic examination process is to execute code running on the CPU of the suspect system. This can potentially change data in the CPU registers, RAM or the hard drive itself. Even if the forensic system specifies no explicit write commands, the suspect system's operating system may decide to swap the program to hard disk. This inherent operating system feature may complicate the incentive for allowing the concerned evidence in a court case and the evidence may be ruled inadmissible. In addition, inappropriate action taken by forensic examiners may ruin evidence. In the event that a forensic examiner handles a situation incorrectly, a preventable amount of data may be changed. For example, running an application on the suspect hard drive may overwrite some of the associated properties, such as recent actions. If the specifics of this application were critical to the case, it will cause many issues in court [Jo07].
- Linked to the problem of data modification are *slurred images*. Similar to when you take a photo of a moving object, slurred images is the result of acquiring a file system while some program modifies it. The smallest modification may cause a problem, since the file system first reads the meta-data section of the hard disk. If the files or folders on the file system change after the file system have read the meta-data, but before the files system acquires the data, the meta-data and sectors do not correlate anymore [Jo07]. Similarly, volatile memory does not represent a single point in time, but rather a time sliding view. When acquiring volatile data, investigators cannot always use write blockers, nor is there always a MD5 comparison to the original data [Vi06].
- Another recurring problem concerning live forensic analysis, especially network evidence from untrusted networks, is *authenticity and reliability*. Anti-forensic toolkits are also widely available, and may obstruct the collection of evidence from live network sources [Ni06]. By applying anti-forensic measures, clued-up criminals may reduce the effectiveness of a potential forensic investigation. It is, for example, possible to write a program that destroys evidence when the operating system detects a forensic acquisition program [Jo07]. These types of programs is developed by individuals or organisations that want to thwart legit forensic investigations, and aims to delete all incriminating evidence on the victim computer and computer system. Some of these programs include Evidence Eliminator, The Defiler's Toolkit, Diskzapper, CryptoMite, Tracks Eraser Pro and Invisible Secrets [Co07]. Another type of anti-forensic software, developed by the Metasploit Project, targets specific functionalities of legitimate forensic investigation tools. These anti-forensic wares interfere with the forensic software's results during an investigation [Hi07]. Anti-forensic tools work on a variety of platforms, and perform a number of different functions.

- In some instances of live forensic acquisition, *limited amounts of information is gathered*. This may not always constitute a complete representation of the original affected system, and can be interpreted as possible data corruption [LK04]. The investigation into this aspect will contribute to a comprehensive model for live acquisition.

Considering the extensive lists of limitations for both traditional digital forensic and live forensics, it is necessary to compare these disciplines with regards to the forensic soundness principle. The next section looks at this.

5 Forensic Soundness

A vast number of technical issues can physically constrict Cyber Forensics, being a rather technical application of computer related knowledge. In addition to these limitations, numerous laws strictly bind forensic practitioners to the letter, the implementation of these sometimes rather disdain [Jo07].

Evidence can either make or break an investigation. Therefore, it is crucial to ensure that all evidence is admissible in court. Should the court reject any item of evidence, it can either hurt the case, or at the very least, portray the investigators as incompetent.

According to Bejtlich [Be06], 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, precisely as such data appears on the source drive relative to the other data on the drive. Finally, a forensically-sound duplicate will not contain any data… other than which was copied from the source drive."* Since this traditional definition of forensic soundness does not allow any leeway for live response and acquisitions, Mike Murr redefined forensic soundness by adding *"… The manner used to obtain the evidence must be documented, and should be justified to the extent applicable"* [Mu06].

The most important question in determining the admissibility of evidence concerns the authenticity of the data. If the data is changed in any way, counsel will have a very hard time convincing the court to include it as evidence [Br05]. Accordingly, this data needs to be considered as forensically sound before it can classify as evidence.

The growing number of attorneys and courts that rely on the results of digital examinations ignited a global debate on the exact constitution of sound forensics. All parties involved agree that forensic acquisitions should not alter the original evidence source in any way. However, forensic experts show that the act of preserving certain digital sources in many cases require the alteration of the original evidence item. For example, the common method of performing live forensic acquisition requires that the investigator load the acquisition tool into memory. This overwrites some of the system's volatile data. This is a distinct alteration of the original data evidence source [Ca07].

Another example concerns the use of remote forensic tools. These tools necessitate the investigator to establish a network connection, accordingly altering the original evidence source. Even the use of hardware write blockers when acquiring data from an IDE hard drive may temporarily reconfigure evidentiary data to access the HPA [Ca07].

5.1 Volatile nature of Cyber Forensics

Cyber Forensics as a discipline tends to be highly volatile. This is in part because the discipline relies on technology, which in itself can be very unstable, but also because the discipline largely constitutes incident response in reaction to unpredictable criminal behaviour.

This volatile nature can best be described by the Heisenberg uncertainty principle in quantum physics. The Heisenberg principle states that locating a particle in a small region of space makes the momentum of the particle uncertain. Additionally, measuring the momentum of a particle precisely makes the position uncertain [Wi08a]. This is very similar to the concept of live forensic acquisition. The mere action of collecting evidence figuratively makes the environment unstable. This translates as rendering evidence forensically unsound.

According to Heisenberg, it is possible to measure the position of an atom with a photon. The uncertainty principle states that, when the photon is introduced, it will change the momentum of the atom by an uncertain amount that is inversely proportional to the accuracy of the position measurement. The amount of uncertainty can never be reduced below the limit set by the principle, regardless of the experimental setup [Wi08a].

Similar to the uncertainty principle, is the *observer effect.* This principle refers to changes that the physical act of observing will make on the observed phenomenon. The same example applies to this principle. In order to see an electron, a photon must first interact with it. This interaction will indefinably change the path of the electron [Wi08b].

Although the modification of evidentiary data remains a huge problem, it is not a new concept. Methods in traditional biological forensic disciplines, such as DNA analysis, also alter the original evidence. However, courts still accept this evidence. When a traditional forensic examiner collects samples of biological material, he/she needs to scrape or smear the original evidence. In many instances, DNA tests are highly destructive. Although investigators can extract information from the original evidence, investigators cannot present the original blood sample or skin sample to the court as evidence. Despite the changes that occur during preservation and processing, courts consider these methods as forensically sound. In fact, investigators regularly admit DNA evidence as evidence [Ca07].

Similarly, digital forensic investigators need to acquire data from a suspect system and analyse, examine and alter its presentation to produce meaningful information to the courts. This meaningful information is rarely in the same format as the format in which the investigator acquired the original data (similar to a traditional forensic investigator acquiring a piece of fingernail, and running DNA analysis to present to court).

When considering the use of traditional digital forensic measures, courts should allow the minor alteration of original evidence, similar to the allowed minor alterations of original evidence in traditional biological forensics. However, investigators should still adhere to the basic Cyber Forensic principles and not alter evidence in such a way that the meaning thereof changes. The legal system therefore needs to be updated to accept digital forensic analysis in a court of law, as long as the data still adhere to the definition of forensic soundness presented in Section 5. Investigators should still focus on maintaining the reliability and authenticity of the evidence [Ca07].

It is not practical to set an absolute standard that dictates the preservation of everything and the modification of nothing. This excludes the viability and usability of both Cyber Forensic processes and traditional forensic methods. This would send the entire legal system in disarray [Ca07].

5.2 Ensuring forensically sound acquisition

The key to forensic soundness is documentation, or a proper chain of custody. The acquisition process should change the original evidence as little as possible. Investigators should document any changes whatsoever and assess it in the context of the final analytical results [Ca07].

In most cases, courts will accept the forensic soundness of a piece of evidence if the supporting documentation is sufficient. This documentation should report on the evidence's origin and the way investigators handled it since acquisition. The acquisition process needs to preserve a complete and accurate representation of the original data. Investigators should do this in such a way that courts can validate its authenticity and integrity [Ca07]. However, this open standard allows for exploits by cyber specialists that knows how to manipulate both the digital evidence and the chain of custody.

There is no specific test to determine whether digital evidence possesses the required scientific validity. However, Cyber Forensic evidence proposed for admission in court should at the very least satisfy two conditions. Firstly, the evidence should be relevant. Secondly, evidence must be *"… derived by the scientific method"* and *"… supported by appropriate validation"*. Cyber Forensics is very technical in nature and therefore grounded in science, including computer science, mathematics and physics [RS05].

In order to ensure that digital evidence is in fact forensically sound, counsel need to investigate the evidence and the investigator's reliability thoroughly. When witnesses are involved, counsel needs to investigate the testing and verification of their theories and practical techniques of Cyber Forensics. Additionally, counsel may investigate differences of opinion among Cyber Forensic experts regarding the validity and acceptance of specific tools and techniques [RS05].

6 Conclusion

Although intense research still needs to be done before live forensic acquisition can formally be introduced into law enforcement, the preliminary study shows that live forensic acquisition measures up to traditional digital forensics. When the volatile nature of forensics as a whole (including live forensics, traditional digital forensics and traditional biological forensics) is considered, it should be clear that forensic soundness is possible. However, similar to biological forensic practices, some minor (controlled) modifications should be allowed, without rendering the digital forensic evidence inadmissible from court.

Bibliography

[Al06] Alink, W., Bhoedjang, RAF., Boncz, PA. & De Vries, AP. 2006. XIRAF – XML-based indexing and querying for digital forensics. *Digital Investigation.* Volume 3, Supplement 1. Pp 50 - 58.

[Ar05] Armstrong, B. 2005. *Detecting Microsoft virtual machines.* Available from: http://blogs.msdn.com/virtual_pc_guy/archive/2005/10/27/484479.aspx (Accessed 4 August 2008).

[Au08] Australian Government. 2008. *How Do I Protect and Handle Magnetic Media?* Available from: http://www.naa.gov.au/records-management/secure-and-store/physical-preservation/faq/ magnetic-tape.aspx (Accessed 25 February 2008).

[Be05] Bedford, M. 2005. Methods of discovery and exploitation of Host Protected Areas on IDE storage devices that conform to ATAPI-4. *Digital Investigation.* Volume 2, Issue 4. Pp 268 - 275.

[Be06] Bejtlich, R. 2006. Forensically Sound Evidence. *TaoSecurity.* Available from: http://taosecurity.blogspot.com/2006/08/forensically-sound-evidence.html (Accessed 20 March 2008).

[BJ05] Brungs, A. & Jamieson, R. 2005. Identification of Legal Issues for Computer Forensics. *Information Systems Management,* Volume 22, Number 2. Pp 57 - 66.

[Br05] Brown, CLT. 2005. *Computer Evidence: Collection and Preservation*. Charles River Media. Available from: http://www.charlesriver.com/resrcs/chapters/1584504056_1stChap.pdf (Accessed 18 April 2008).

[Ca07] Casey, E. 2007. What does "forensically sound" really mean? *Digital Investigation.* Volume 4, Issue 2. Pp. 49- 50.

[Ch07] Church, CA. 2007. *Long Term Hard Drive Storage and Data Integrity*. Available from: http://photo.net/bboard/q-and-a-fetch-msg?msg_id=00NXpz (Accessed 25 February 2008).

[Co07] Computer Network Defence. 2007. *Anti-Forensic Tools*. Available from: http://www.networkintrusion.co.uk/foranti.htm (Accessed 20 June 2008).

[Fe07] Fei, BKL. 2007. *Data Visualisation in Digital Forensics*. University of Pretoria. Available from: http://upetd.up.ac.za/thesis/submitted/etd-03072007-153241/unrestricted/dissertation.pdf (Accessed 17 January 2008).

[Gh06] Ghelani, S. 2006. *Chain of Custody - A Suspect's Chargesheet*. Available from: http://images.google.co.za/imgres?imgurl=http://www.niiconsulting.com/checkmate/wp-admin/images/0206/cocfrm.jpg&imgrefurl=http://www.niiconsulting.com/checkmate/2006/02/chain-of-custody-a-suspects-chargesheet/&h=407&w=500&sz=25&hl=en&start=16&um=1&tbnid=vm5fqnvwwpkYM:&tbnh=106&tbnw=130&prev=/images%3Fq%3D%2522chain%2Bof%2Bcustody%2522%26um%3D1%26hl%3Den%26sa%3DN (Accessed 25 February 2008).

[Ha08] Halderman, JA., Schoen, SD., Heninger, Na., Clarkson, W., Paul, W., Calandrino, JA., Feldman, AJ., Appelbaum, J. & Felten, EW. 2008. Lest We Remember: Cold Boot Attacks on Encryption Keys. Proc. 2009 USENIX Security Symposium. Pp 1 - 16.

[Hi07] Hilley, S. 2007. Anti-forensics with a small army of exploits. *Digital Investigation.* Volume 4, Issue 1. Pp 13 - 15.

[Jo07] 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).

[KH02] Kruse II, WG. & Heiser, JG. 2002. *Computer Forensics: Incident Response Essentials*. Addison-Wesley: Boston.

[Le08] LexisNexis. 2008. *Preserving Chain of Custody in E-Discovery.* Available from: http://www.lexisnexis.com/applieddiscovery/clientResources/techTips9.asp (Accessed 25 February 2008).

[LK04] Leigland, R. & Krings, AW. 2004. A Formalisation of Digital Forensics. *International Journal of Digital Evidence*. Volume 3, Issue 2. Pp 1 – 32.

[Mu06] 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).

[Ni03a] NIST. 2003a. *Hardware Write Blocker Device (HWB) Specification*. National Institute of Standards and Technology. Available from: http://www.cftt.nist.gov/HWB-posted.pdf (Accessed 26 February 2008).

[Ni03b] NIST. 2003b. *Software Write Block Tool Specification & Test Plan*. National Institute of Standards and Technology. Available from: http://www.cftt.nist.gov/documents/SWB-STP-V3_1a.pdf (Accessed 26 February 2008).

[Ni06] Nikkel, BJ. 2006. Improving evidence acquisition from live network sources. *Digital Investigation*. Volume 3, Issue 2. Pp 89 – 96.

[NTV05] Nykodym, N., Taylor, R. & Vilela, J. 2005. Criminal Profiling and Insider Cyber Crime. *Digital Investigation.* Volume 2, Issue 4. Pp 261 - 267.

[Pa07] PARALAN. 2007. *Computer Forensic Protection - SCSI Write Blocker - Models SR14A and SR15A SCSI Forensics*. Available from: http://www.paralan.com/sr14.html (Accessed 26 February 2008).

[RS05] Ryan, DJ. & Shpantzer, G. 2005. *Legal Aspects of Digital Forensics*. Available from: http://www.danjryan.com/Legal%20Issues.doc (Accessed 26 March 2008).

[Sc05] Scalet, SD. 2005. *How To Keep A Digital Chain Of Custody*. Available from: http://www.csoonline.com/read/120105/ht_custody.html (Accessed 25 February 2008).

[St08] 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).

[Tr94] Trench, RL. 1994. Chain of Custody: Keeping Track of Property and Evidence. *International Association for Property and Evidence, Inc*. Evidence Log - 1994 Vol 94, No 4. Available from: http://images.google.co.za/imgres?imgurl=http://www.iape.org/EvidenceLog/1994-04/sample-chain-of-custody-tag.gif&imgrefurl=http://www.iape.org/EvidenceLog/1994-04/chain-of-custody-keeping-track.html&h=265&w=508&sz=16&hl=en&start=4&um=1&tbnid=thR-tyQLVby4FM:&tbnh=68&tbnw=131&prev=/images%3Fq%3D%2522chain%2Bof%2Bcustody%2522%26um%3D1%26hl%3Den%26sa%3DN (Accessed 25 February 2008).

[Us05] US-CERT. 2005. *Computer Forensics.* Available from: http://www.us-cert.gov/reading_room/forensics.pdf (Accessed 20 March 2008).

[Vi06] Vidas, T. 2006. *Forensic Analysis of Volatile Data Stores*. CERT Conference. Available from: http://www.certconf.org/presentations/2006/files/RB3.pdf (Accessed 27 March 2008).

[Wi08a] Wikipedia, the free encyclopaedia. 2008a. *Uncertainty Principle*. Available from: http://en. wikipedia.org/wiki/Uncertainty_principle (Accessed 25 March 2008).

[Wi08b] Wikipedia, the free encyclopaedia. 2008b. *Observer Effect*. Available from: http://en. wikipedia.org/wiki/Observer_effect (Accessed 4 April 2008).

[WP05] Weise, J. & Powell, B. 2005. *Using Computer Forensics When Investigating System Attacks.* Available from: http://www.sun.com/blueprints (Accessed 27 February 2008).