Procedures for a Harmonised Digital Forensic Process in Live Forensics

George Sibiya[1], H. S. Venter[2] and Thomas Fogwill[1]
Meraka Institute
CSIR[1], P. O. Box 395, Pretoria, 0001
Tel: +27 12 841 3976
and Department of Computer Science
University of Pretoria[2]
email: {gsibiya, tfogwill}@csir.co.za[1]; hventer@cs.up.ac.za[2]

***Abstract* - Cloud computing is a novel computing paradigm that presents new research opportunities in the field of digital forensics. Cloud computing is based on the following principles: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. These principles require that cloud computing be distributed internationally. Even if the cloud is hosted locally, it is based on multi tenancy, which is a challenge when using an advanced "dead" forensic approach. For these reasons, digital forensic investigations in cloud computing need to be performed on live systems. There are challenges in cloud forensics itself, as there are no standardised digital forensic procedures and processes. This paper is part of an effort by the authors to standardise the digital forensic process, and we therefore focus specifically on live forensics. Since cloud computing services are provisioned over the Internet, live forensics and network forensics form an integral part of cloud forensics. In a bid to standardise a digital forensic process in cloud computing, there is a need to first focus on live forensics and network forensics. In this paper we present digital forensic procedures on live forensics that follow the draft international standard for Investigation Principles and Processes. A standardised live digital forensic process will form part of a standardised cloud forensic process.**

Keywords - Digital forensic process, cloud computing, computer crime, live forensics

I. INTRODUCTION

Despite the fact that digital forensics has been practised by law enforcement agencies since the advent of computer crime, it has not received adequate attention from the research community and until recently, there have been no efforts to standardise such investigations [1] [2]. This has contributed to a lack of standardised processes and procedures to be followed when conducting digital forensic investigations.

To further aggravate the already unfortunate situation, an all new computing paradigm – cloud computing – recently came into existence. Cloud computing builds on virtualisation technology to provide computational resources, platforms and software as services to cloud users without them having to own physical infrastructures. In cloud computing, users do not host their computational data in their vicinity. Instead, the data is stored remotely and they do not need to know where it is physically kept, as it may be distributed. Cloud computing therefore introduces more research an issue into digital forensics, which itself is still in its infancy. This paper addresses one of these research issues, namely the standardisation of a digital forensic process in the cloud, specifically with regard to the procedures for Random Access Memory (RAM) forensics that form an integral part of cloud forensics.

In this paper the authors consider three categories digital forensics, i.e., live forensics, network forensics and cloud forensics. In each of these categories there is a need for a harmonised digital forensic process. In this paper live forensics refers to RAM forensics. The current paper presents more detailed digital forensic procedures in live forensics based on the harmonised digital forensic process proposed by Venter and Valjarevic [3], in a digital forensic standard that is still under review**.** The detailed harmonised digital forensic procedures for network forensics and cloud forensics lies, however, beyond the scope of this paper. Since live forensics and network forensics form part of cloud forensics, the authors still need to publish papers on a harmonised digital forensic process for network forensics and cloud forensics.

The remainder of the paper is structured as follows. In section 2 the authors present a brief background on cloud computing, challenges in the digital forensic process and the harmonised digital forensic process.

II. BACKGROUND

In this section the authors present a brief background on cloud computing, challenges in the digital forensic investigation process and, lastly, the harmonised digital

forensic process proposed by Venter and Valjarevic [3]. The model presented in this paper builds upon the latter process.

A. *Cloud computing*

Cloud computing provides computing resources on a pay-per-use basis. It is based on five principles: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [4]. On-demand self-service means that a cloud user can create for example a virtual desktop and pay for the duration of its use, after which it can be "soft-destroyed" if it is no longer needed. Such services are referred to as measured services, as users are billed per usage. Cloud resources need to be accessible to customers irrespective of geographical location, hence the requirement for broad network access. Resource pooling refers to computational resources that are published in a cluster for consumption by customers on demand. If a resource is no longer in use, it is made available to other users. In a cloud environment, resources can be scaled up and down according to user needs. This is referred to as rapid elasticity.

In a cloud environment service, providers (CSPs) offer infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) and these services can be accessed by consumers over the Internet [5]. This eases the burden on vendors as they no longer need to own physical infrastructures (such as servers) for their computational needs.

B. *Digital forensic challenges*

Originally, the digital forensic process consisted of four main steps, i.e. identification, acquisition, analysis and presentation of the evidence. With the advent of new computing paradigms such as cloud computing a need has arisen for digital forensics to have different specific areas of focus. These areas include Random Access Memory (RAM) forensics [6], network forensics [7] and cloud forensics [8]. In each of these areas, the four generic steps cannot be directly applied as there are sub-processes and actions that need to be taken that are unique to each specific area. Digital forensics itself has challenges, as there are no standardised digital forensic processes and procedures [1].

C. *Harmonised digital forensic process*

In addressing the lack of a standardised digital forensic process, the proposed standard [3] by Venter and Valjarevic presents a harmonised digital forensic process model as shown in Figure 1.

The harmonised digital forensic process consists of twelve phases, i.e. preparation, planning, incident detection, first response, incident scene documentation, potential evidence identification, evidence collection, evidence transportation, evidence storage, evidence analysis, presentation and conclusion.

The incident documentation phase depends on whether investigators have physical access to the incident scene or not. In a virtual environment, such as the cloud, a crime scene may not be physically accessible; hence it may not be documented.

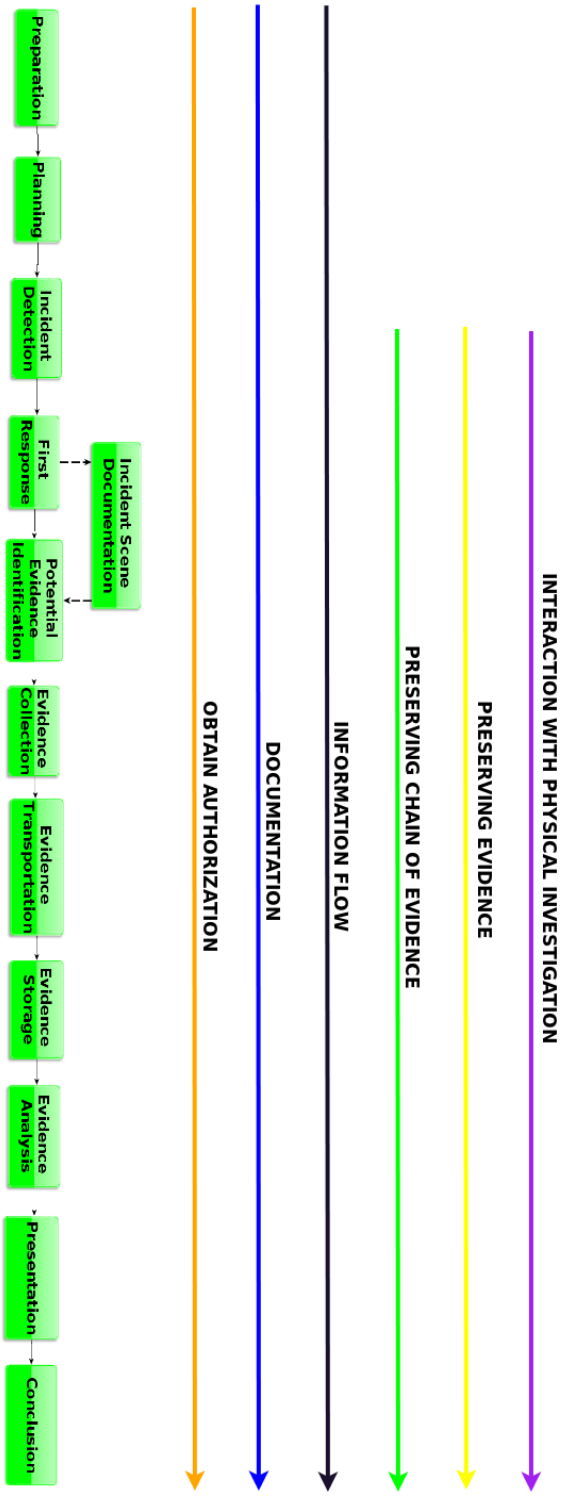

Figure 1: Harmonized Digital Forensic Process. Adapted from Venter and Valjarevic (2012).

Throughout the phases of the harmonised digital forensic process, there are accompanying parallel actions that can take place during each phase. These actions are: obtaining authorisation, documentation, defining an information flow, preserving the chain of evidence, preserving evidence, and interaction with the physical investigation.

Three of these actions – obtaining authorisation, documentation, information flow – are carried out during the course of the entire harmonised digital forensic process, while preservation of chain of evidence, preservation of evidence and interaction with the physical investigation only start after the incident has been detected. The parallel actions performed are discussed in detail in [3].

In the next section we present procedures that are followed in live forensics based on the phases of a digital forensic process.

III. DIGITAL FORENSIC PROCEDURES IN LIVE FORENSICS

With cloud computing, multiple users share hardware resources. This restricts forensic investigators to performing live forensics, as they cannot shut down an entire cloud infrastructure to acquire evidence.

Such action would not only disrupt other users hosted in the same cloud, but also destroy volatile information. In this section we present a model that provides detailed procedures for the live digital forensic process based on the harmonised digital forensic process presented in the previous section. Procedures are clearly specified actions that need to be taken or implemented to complete a task [9]. We therefore define a procedure as a set of actions that can easily be followed by an investigator, without seeking additional help, to accomplish a forensic investigation phase. The procedures discussed are depicted in **Figure 2**.

Live digital forensics involves conducting a digital forensic investigation on a system without shutting the system down. During the live digital forensic process, most of the evidence is acquired from the RAM.

In the subsequent subsections, we discuss the digital forensic procedures based on ten of the phases of the harmonised digital forensic investigation process. The ten phases we focus on are planning, preparation, incident detection, first response, incident scene documentation, potential evidence identification, evidence collection, evidence transportation, evidence storage and evidence analysis.

The other phases – presentation and conclusion – are generic and require no unique actions to be performed in a live forensic scenario. They are therefore carried out as described in [3].

A. Planning

The planning phase in live forensics provides a well-defined path for the flow of evidence from one phase to the next.

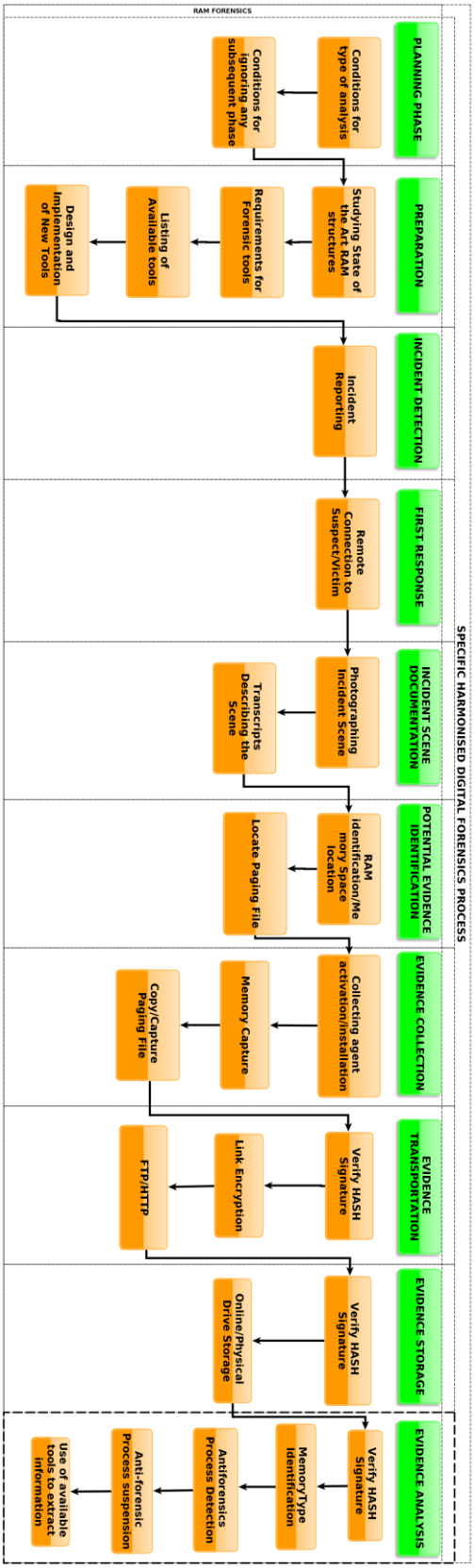

Figure 2: Harmonised Digital Forensic Procedures in Live Forensics.

Live forensics can be performed in two ways, i.e. live system analysis and capturing of the RAM from a live system so that it can be analysed in a more controlled and secure environment [10].

As such, if an approach is adopted where analysis is done on a live system, some phases such as evidence storage may not be necessary.

In the planning phase, a decision may be made to skip any phase under certain conditions. There are also certain conditions on which to base the decision of whether to analyse a live system or captured RAM.

Actions to be performed in this phase therefore comprise the following:

- Setting conditions for performing a live system analysis and not an analysis of captured RAM.
- Setting conditions for not performing any of the sub-sequent phases.

If none of these conditions are met, the investigation will go through all the other phases as they follow in the next subsections.

B. Preparation

At this stage, conditions will already have been laid out on whether to analyse a live system or preserved images of the captured RAM.

This phase involves studying existing operating systems running on state-of-the-art devices. More attention will be paid to the RAM structures of those operating systems. Such information will be used in acquiring appropriate tools or in designing and developing new tools to be used in the investigation process.

The output from this phase is a list of tools that will be used in a given scenario after an incident has been detected. The procedure in this phase consists of the following actions:

- Studying the state of the operating systems' RAM structures
- Making a list of requirements that need to be met by forensic tools that can be used in RAM forensic investigation.
- Listing the available tools that may be used in RAM forensics.
- Designing and developing new tools if none exists that meets the specified requirements.

C. Incident detection

An incident that requires live forensics can be detected by network monitors such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), or by users who may become aware of suspicious activities in their system.

This phase consists of one action:

- Incident reporting

Incident reporting can therefore be performed by two groups of people involved in the system: firstly the network administrators who are informed by IDS and IPS of malicious activities in the network, and secondly the system users themselves who may observe a malicious activity in their system.

D. First response

First response refers to the precautionary measures taken and first actions carried out once an incident has been detected. Depending on whether the forensic investigator has access to the physical machine, a physical acquisition device will be connected at this stage or a remote secure connection will be established. If an investigator or first responders have access to the crime scene system, this may involve shutting down the system. Such an action can however not be performed in virtual environments such as the cloud. The procedure in this phase involves a single action:

- RAM analysing or capturing device connection/Remote connection to remote system

E. Incident scene documentation

Documentation of the incident scene depends largely on the accessibility of the incident scene. If the scene is accessible to investigators, this phase would be carried out as originally proposed by Venter and Valjarevic in [3]. If the incident scene is physically accessible to investigators, the procedure in this phase involves the following actions:

- Taking photographs of the scene
- Writing transcripts that describe the scene

F. Potential evidence identification

In this phase, a RAM to be captured is identified. In the case of virtualised environments, this will involve identifying memory space of an isolated instance. The procedure followed in the potential evidence identification phase includes two actions:

- Locating memory space
- Locating page file

G. Evidence collection

In the evidence collection phase, the first action to be performed is the activation of an evidence collection agent. If such an agent has not been installed yet, it will immediately be done and precautions will be taken to ensure that evidence is not tainted.

The second action taken in this phase is the actual capturing of physical memory. This can be done through a command from the remote workstation of an investigator or from an attached PCI device if an investigator has physical access to the crime scene system.

The captured RAM file is subsequently fed into the next phase, which is evidence transportation.

Actions performed are therefore:

- Collecting agent activation/installation
- Memory capture/Issuing of RAM capture command
- Copying/Capturing of page file

H. *Evidence transportation*

If the RAM was captured into a physical device, the transportation measures are those carried out in traditional forensic procedures. If the RAM was captured remotely, the transportation link (FTP/TCP) needs to be secured, in other words encrypted. The actions are:

- Hash signature verification
- Link encryption
- FTP/HTTPS transportation

I. *Evidence storage*

The procedure in this phase includes the following actions:

- Verification of the hash signatures of the captured RAM.
- Storage of the evidence. Evidence can be stored in secured online storage or physical devices.

J. *Evidence analysis*

Based on the analysis of a RAM, information that can be obtained includes user names and passwords, network addresses, running processes and terminated processes, open TCP/UDP ports, raw sockets, active connections, running threads, object signatures that can be used to identify those objects, etc. [11] [6] [12]. The analysis outcomes are summarised more effectively in the form of questions in [13]:

- What processes were running on the suspect system at the time the memory image was taken?
- What (hidden or closed) processes existed?
- Are there any (hidden or closed) network connections?
- Are there any (hidden or closed) sockets?
- What is the purpose and intent of a suspected file?
- Are there any suspicious DLL modules (Windows)?
- Are there any suspicious URLs or IP addresses associated with a process?
- Are there any suspicious open files associated with a process?
- Are there any closed or hidden files associated with any process?
- Are there any suspicious strings associated with a particular process?
- Are there any suspicious files present and can they be extracted?
- Can a malicious process be extracted from the memory and be analysed?
- Can the attackers be identified using discovered IP addresses?
- Is there a user account created by the attacker on the system?
- Did the malware modify or add any registry entry (Windows)?
- Does the malware use any type of hooks to hide itself?
- Did the malware inject itself into any running processes?
- What is the relationship between different processes?
- What is the intent and purpose of a discovered malware?

The procedure in this phase starts off with the following actions:

- Verification of the hash signature
- Identification of the memory type

Verification is done by calculating the hash signature of the RAM copy and the HASH signature obtained from the incident scene documentation. The identification of the memory type is important as it involves determining the system source (hence, the tools that can be used to analyse) the RAM. The process structure of a RAM varies with every system type, e.g. in Windows the RAM process structure varies with every version of and service pack for Windows.

If the RAM is analysed on a live system or the captured RAM is booted in a virtual machine, the next action to be performed is:

- Identification of anti-forensic processes

Anti-forensic processes are the processes that result from activities performed by an attacker while hiding file systems and malicious activities that are running on a system.

Once anti-forensic processes have been identified, the next action is:

- Suspension or deactivation of those processes

The deactivation of anti-forensic processes will reveal hidden processes and the revealed processes may even lead the investigator to new locations where evidence needs to be gathered.

One last action remains to be taken in this phase:

- Use of available tools to answer the questions listed above.

Answering these questions will help the investigator to substantiate or dispute their hypotheses.

IV. CONCLUSION

In contributing towards the standardisation of the digital forensic process, this paper has presented detailed forensic procedures on live forensics that follow the proposed investigation principle and process standard. The goal of the authors is to establish a standard investigation process in a cloud environment. Both live forensics (as addressed in this paper) and network forensics form part of a standardised cloud forensic process. The authors have submitted a paper on network forensics based on the ISO/IEC 1st WD 27043 draft standard. After that, their focus will shift to cloud forensics.

REFERENCES

[1] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Elsevier, Digital Investigation*, no. 7, pp. S64 - S73, 2010.

[2] M. Bandor, "Process and Procedure Defination: A Primer," 2007. [Online]. Available: http://www.sei.cmu.edu/library/assets/process-pro.pdf. [Accessed 26 March 2012].

[3] H. Venter and A. Valjarevic, " Investigation Principles and Processes. Unpublished International Standard". South Africa Patent ISO/IEC 27043, 2012.

[4] "Cloud Forensics - Lab systems solutions," 2012. [Online]. Available: http://www.labsystems.co.in/images/Cloud_Forensics_-_A_Lab_systems_approach.pdf. [Accessed 26 March 2012].

[5] M. Taylor, J. Haggerty and D. Lamb, "Forensic Investigation of Cloud system," Network Security, 2011.

[6] M. Burdach, "Physical Memory Forensics," 2012. [Online]. Available: http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Burdach.pdf. [Accessed 26 March 2012].

[7] A. Caballero and S. Fidge, "Network Forensics," CrossTec Corporation, Florida, 2012.

[8] S. Zimmerman and D. Glavach, "Cyber Forensics in the Cloud," *The Newsletter for Information Assurance Technology Professionals*, pp. 4 - 7, 2011.

[9] "Process versus procedures," 2012. [Online]. Available: http://www.transition-support.com/Process_versus_procedure.htm. [Accessed 26 March 2012].

[10] A. Walters and N. L. Petroni, Jr., "Volatools: Intergrating Volatile Memory Forensics into Digital Investigation Process," Komoku, Ink, College Park, Maryland, 2007.

[11] G. L. Garcia, "Forensic physical memory analysis: an overview of tools and techniques," TTK T-110.5290 Seminar on Network Security, 2007.

[12] T. Vidas, "Post-moterm Ram Forensics," CanSecWest , 2007.

[13] I. Eroraha, "Memory Forensics: COllecting and Analysing Malware Artifacts from RAM," netSecurity, Dulles, 2011.

Author Biography: George Sibiya holds a Masters degree in computer science from the University of Zululand. He is currently enrolled for a PhD in computer science degree with the University of Pretoria and is doing his research with the Meraka Institute, CSIR. His research interests are in computer security and cloud computing.