Digital Forensics Investigations in the Cloud

Neha Thethi, MSc
Information Security & Digital Forensics Research Group
School of Informatics & Engineering
Institute of Technology Blanchardstown
Dublin, Ireland
neha.thethi@gmail.com

Anthony Keane, MSc, PhD
Information Security & Digital Forensics Research Group
School of Informatics & Engineering
Institute of Technology Blanchardstown
Dublin, Ireland
anthony.keane@itb.ie

***Abstract*— The essentially infinite storage space offered by Cloud Computing is quickly becoming a problem for forensics investigators in regards to evidence acquisition, forensic imaging and extended time for data analysis. It is apparent that the amount of stored data will at some point become impossible to practically image for the forensic investigators to complete a full investigation. In this paper, we address these issues by determining the relationship between acquisition times on the different storage capacities, using remote acquisition to obtain data from virtual machines in the cloud. A hypothetical case study is used to investigate the importance of using a partial and full approach for acquisition of data from the cloud and to determine how each approach affects the duration and accuracy of the forensics investigation and outcome.**

Our results indicate that the relation between the time taken for image acquisition and different storage volumes is not linear, owing to several factors affecting remote acquisition, especially over the Internet. Performing the acquisition using cloud resources showed a considerable reduction in time when compared to the conventional imaging method. For a 30GB storage volume, the least time was recorded for the snapshot functionality of the cloud and dd command. The time using this method is reduced by almost 77 percent. FTK Remote Agent proved to be most efficient showing an almost 12 percent reduction in time over other methods of acquisition. Furthermore, the timelines produced with the help of the case study, showed that the hybrid approach should be preferred to complete approach for performing acquisition from the cloud, especially in time critical scenarios.

***Index Terms*—Cloud forensics, Cloud evidence acquisition**

I. Introduction

Crime on the internet takes numerous forms including hacking, fraud, scams, money laundering, industrial espionage, prostitution, abduction, drug smuggling, suicide assistance, defamatory allegations, cyber stalking, cyber terrorism, etc. Crimes committed using digital devices and the internet tends to leave digital trace evidence behind (*the Locard's Exchange Principle*), the identification of which can aid investigators in criminal investigations.

Where once it was the sophistication and maturity of the forensics tools that were the problem, today it is the growth in the amount of data to be analyzed that is fast becoming a problem. The average amount of data per case, as experienced by FBI's fifteen Regional Computer Forensic Laboratories, has grown 6.65 times (from 84 GB to 559 GB) in eight years (2003–2011) [1]. As a result of the huge low cost capacity of storage, acquisition and analysis of digital evidence is becoming extremely time-consuming. These issues are even more aggravated for remote acquisitions.

The term cloud forensics was first introduced in 2011 [2] to recognize the emerging need for digital investigation in the developing cloud computing environments, fueled by the forecasted potential return on investment (ROI). By 2014, the worldwide cloud services revenue is projected to reach over 148 billion USD according to Gartner, Inc. These figures are worrying for a forensic investigator in view of the fact that increased amount of user data in the cloud takes more time to image, examine and analyze as compared to the same amount processed in a traditional forensic investigation. Moreover, this dramatic increase in data volume is difficult to handle with low cost storage capacity outpacing network bandwidth and latency improvements [3].

II. Related Work

To date, the main research in Cloud Forensics has focused on the following areas: *Cloud Forensic Frameworks* by Ahmed & Raja [4], Sibiya [5], Garfinkel [10] and Martini & Choo [6]; *Evidence Acquisition* by Marturana [7] and Dykstra & Sherman [8]; *Issues and Challenges* by Ruan [2] and Birk & Wegener [9].

One of the most rational solutions to increase speed of investigation is to employ high performance computing for these investigations, [11]. Another means of providing high computational resources is by exploiting the resources of the cloud itself and providing forensics-as-a-service [7], [8] and [12]. Until these concepts are practically put into operation by the cloud providers, the existing traditional tools and techniques have to be employed for conducting cloud forensics.

Despite extensive research in the field of cloud forensics in recent times, no complete comparison statistics for popular digital forensic acquisition tools exists and, not much emphasis has been placed on evaluation of the time taken for acquisition of data. The reason for this is either, the investigators completely disregard the current tools and consider them incapable of dealing with the voluminous data, or, they simply do not use these tools at all. In a survey conducted by SANS [15], it was found that only 16% of respondents indicated they

978-1-4799-2572-8/14/$31.00 ©2014 IEEE

use tools designed specifically for such platforms. Additionally, about 36% use low-tech image captures and screen recordings for investigating virtualized and cloud-based systems, while 25% reported that they create their own tools as the need arises. However, such scripts are generally not acceptable in court proceedings.

In 2009, Gartner [13] published an overview of remote forensic tools and guidance for their use, targeted at enterprise environments. They cited EnCase [20] and FTK [21] as the most widely used products, with the greatest international support. A first time assessment of the evidence acquisition time was done by Dykstra and Sherman [8] using the remote agent deployment capabilities of these tools which resulted in successful acquisition of volatile and non-volatile data from the cloud. Their emphasis was on the success of acquisition of data rather than the comparison of approaches used for acquisition. They also recently developed a set of tools known as *Forensic OpenStack Tools (FROST)* [14] which is the implementation of a management plane forensic toolkit in a private instantiation of the OpenStack cloud platform. Such tools are not yet available for commercial CSPs like Amazon EC2.

Considering the reluctance or delay in adoption of forensic services by some CSPs and, lack of availability of enhanced alternative tools/techniques for cloud forensics, the remote capabilities of existing tools will continue to persist for evidence acquisition from the cloud for foreseeable future. And so, the time taken for imaging evidence from the Amazon EC2 cloud instances using FTK is thus evaluated in this paper.

III. Problem Statement

The primary objective of this research is to determine whether the time-taken to image the data for different storage capacities on the cloud will make it impossible for the forensic investigators to practically image all the evidence in a timely fashion to complete an investigation properly.

The secondary objective is to establish whether partial imaging of the data from the cloud as compared to a complete cloud image is sufficient to get an accurate result of the evidence. And final objective is to determine how a time critical case like child abduction is affected by the different approaches of acquisition in the cloud.

IV. Methodology

1) A hypothetical yet plausible case study is designed that emulates an actual kidnap and blackmail crime where the cloud is used as an instrument in the crime. We assess the effect of time taken for acquisition of data from different storage capacities, in time critical situations and acquisition of partial evidence. The scope of the case study designed is limited to the Guest OS layer in an IaaS infrastructure of the Amazon EC2 cloud instances.

2) In order to gather relevant data for analysis, the crime scenario in the case study is simulated by means of virtual machines (VMs) provided by Amazon EC2 in the form of instances.

3) The investigation framework proposed by Martini and Choo [6] exclusively for the purpose of cloud forensics is followed for investigating the crime described in the case study.

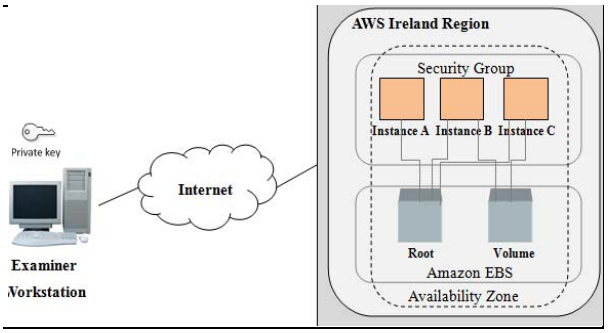

Fig 1: Experiment Implementation Environment

4) We obtain the image of storage volumes, memory dump as well as acquire volatile information. The data acquisition is performed using the following tools/techniques:-

- FTK Remote Agent (FTK 4.2.1)
- FTK Imager 3.0.0
- FTK Imager Lite 3.1.1
- Generation of Snapshot using Amazon's functionality and creation of image in a Linux instance using dd command

5) Time taken for remote acquisition of images using various approaches is recorded and results are subsequently analyzed.

V. Case Study

Confidential information belonging to ABC Corporation is compromised and displayed on a public website which has an Amazon EC2 public DNS. An employee in the company finds out (on 10/07/2013 at 14:00 hours) and immediately notifies the head of IT. Within an hour the company calls in a forensic investigator and on request, they provide him with a list of employees who had access to the confidential information within the past month. He is also informed that one employee in particular, Tom Cullen, had not turned up for work since the past two days. In addition, the IT head was suspicious of this employee due to his abnormal behavior lately and because every attempt of contact with him was unsuccessful.

In this particular case, the use of the cloud instances in the crime is incidental and they are used as an instrument in the crime. This is quite convenient for criminals in most cases due to the cloud's flexibility of creating and destroying instances within minutes.

For the experiment, we use the Micro, M1 Small and M1 Medium Amazon EC2 instances with Windows Server 2008 R2 (64-bit) OS which will be referred to as Instance A, B and C respectively. The port RDP (tcp/3389) is open on all instances to carry out remote acquisition using the FTK Remote Agent. The evidence on Instance A and C was located on the persistent storage, whereas Instance B had the evidence in the temporary storage. Note that all data in the temporary storage of the instance is lost once the machine is powered off.

TABLE I. ACQUISITION TIME FOR DIFFERENT STORAGE VOLUMES OF VIRTUAL MACHINES USING DIFFERENT TOOLS

S.No	Tools	*Instance Storage Notation*	*Source Data Size (GiB)*	*Image File Size (GiB)*	*Image Acquisition Time (Hours)*	*Image Verification Time (Hours)*	*Total Acquisition Time (T) (Hours)*
1	FTK Remote Agent	S_p S_{tC} S_{tB}	30 149 399	1.46 1.73 2.19	8.48 43.51 108.28	0.75 3.21 9.77	9.23 46.93 118.0
2	FTK Remote Agent & FTK Imager (Mount VM)	S_p S_{tC} S_{tB}	30 149 399	1.46 1.73 2.19	12.54 63.09 149.59	0.18 0.99 2.29	12.72 64.08 151.8
3	FTK Imager Lite	S_p S_{tC} S_{tB}	30 149 399	1.46 1.73 2.19	5.66 23.82 75.82	4.91 22.84 60.84	10.57 46.66 136.6
4	FTK Imager Lite (Transferred to VM)	S_p S_{tC} S_{tB}	30 149 399	1.46 1.73 2.19	3.93 20.37 54.87	2.83 11.41 33.91	6.76 31.78 88.78
5	Snapshot (AWS) & dd command (Linux)	S_p	30	30	5.09	0.33	5.42

S_p : Persistent storage volume. $S_{pA} = S_{pB} = S_{pC} = S_p = 30$GiB.
S_{tC} : Temporary storage volume for instance C. $S_{tC} = 149$ GiB
S_{tB} : Temporary storage volume for instance B. $S_{tB} = 399$ GiB

We also make a few assumptions in the case study:

a) Availability of Credentials – A user registered with Amazon Web Services (AWS) needs to provide authentication for the AWS user account and, credentials for accessing each instance. The availability of user credentials along with administrative permissions for a cloud account/instance has low probability, nonetheless, the information is discovered during the course of the investigation as part of the case study, as remote acquisition of the VM image is impossible otherwise, using the techniques mentioned.

b) Child abduction – A survey conducted by SANS [15] reports the number of cases related to server infrastructure in the cloud, such as Amazon EC2, to be investigated is typically low. Amongst those cases, the possibility of an abduction case would likely be quite low. Despite the fact, the kidnapping incident is incorporated to call attention to the significance of the approach adopted for investigation in 'time critical' scenarios. If the investigator proceeds with the wrong approach in such cases, vital information could be lost and thus a life could be in danger.

In addition, we assume that the local machines from which the activity in the cloud was performed are not available to the examiner. Thus, techniques to explore artifacts in these machines presented by researchers such as Marturana [16] and Chung [17] are not applicable.

VI. INVESTIGATION PROCESS

We follow the investigation framework proposed by Martini and Choo [6] as mentioned earlier. Their framework consists of an iteration phase which enables commencement of identification and preservation of evidence even after it is discovered in the examination and analysis phase of the investigation. Even though this seems like an obvious procedure followed by examiners in a real world investigation, it is not explicitly addressed in any of the former widely used frameworks [18], [19].

Following are the steps for the investigation process in the experiment. Steps 1 and 2 are repeated after each of the Step 3 (a), (b) and (c) as more sources with potential evidence are recovered.

1. Evidence Source Identification and Preservation
2. Collection
3. Examination and Analysis
   a) Tom's Work Computer: Deleted file containing credentials for Instance A recovered.
   b) Instance A: Web pages containing confidential information found. Credentials for Instance B recovered from deleted file.
   c) Instance B: Password protected zipped file with pictures and document mentioning Tom's daughter had been kidnapped. Pictures of Tom involved in unlawful activity found. Credentials for Instance C recovered
   d) Instance C: Drug trafficking related documents and images found. Mr. X is the main culprit.
4. Reporting and Presentation

VII. RESULTS

A. Storage Volumes

The time taken for complete acquisition of persistent and temporary storage images from the remote machines is displayed in Table I. All the VMs possess a persistent storage of 30GiB and, Instance B and Instance C are attached with an additional temporary storage capacity of 399 GiB and 149 GiB respectively. The time was recorded for the three storage capacities.

The results indicated lowest time using the snapshot functionality of the cloud. However, this approach is applicable only for acquiring persistent storage. For temporary storage, the image acquired by FTK Imager Lite when transferred to the VM takes minimum time amongst all approaches. A scatter plot of these values along with the analysis is presented later.

We also calculated the complete storage, selective content, memory dump and volatile data acquisition times. Based on the results complied, we calculated the total time for acquisition phase of the investigation when using either complete or partial acquisition and analyzed these investigation approaches alongwith a hybrid approach.

B. Complete and Partial Imaging

The total time taken for complete and partial acquisition from a VM is given by the following equations:

$$CTotal_i = TC_i + TM_{min} + TV \quad (1)$$

$$PTotal_j = TEA + TS_j + TM_{min} + TV \quad (2)$$

where,
CTotal : acquisition time when storage volume is completely imaged
PTotal : acquisition time when storage volume is partially imaged
TC : total acquisition time from all storage volumes of VM
TM_{min} : minimum memory dump acquisition time
TV : volatile memory acquisition time
TEA : examination and analysis time
i : index allotted to tools used for complete acquisition $\{i : 1 \leq i \leq 5\}$
j : index allotted to tools used for partial acquisition $\{j : 1 \leq j \leq 4\}$

Tools/techniques used for **Complete acquisition** include FTK Remote Agent (i=1), FTK Remote Agent & FTK Imager (Mount VM) (i=2), FTK Imager Lite (i=3), FTK Imager Lite (Transferred to VM) (i=4) and Snapshot functionality (AWS) (i=5).

Tools/techniques used for **Partial acquisition** include FTK Remote Agent ('Preview Information Only' Functionality) (j=1), FTK Remote Agent & FTK Imager Custom Content Image (Mount VM) (j=2), FTK Imager Lite (j=3) and FTK Imager Lite (Transferred to VM) (j=4).

For calculating the total duration of the investigation, using these imaging approaches a timeline for each approach is constructed. The timelines illustrate the difference in duration of acquisition by each approach. When relying on AccessData tools for acquisition, conventionally, imaging of a system is performed using FTK Imager from an external drive (i = 3). In our experiment, this approach is used as a comparison parameter. With the help of the timelines, total time estimated for complete acquisition is 9, 11.5, 10, 8 and 8 hours for i = 1, 2, 3, 4 and 5 respectively. The time estimation of all partial as well as hybrid approaches is 5 days (as transfer of evidence from Cloud Service Provider (CSP) is also taken into account).

VIII. Discussion

A. Relationship between Acquisition Time and Storage Volume

On comparing the percentage change of acquisition time for all tools/methods, with the conventional method of acquisition (using FTK Imager from an external drive), we observe that mounting the VM and then imaging shows an increase of approximately 20 percent in time (Fig. 3).

All the other methods require lesser time. A 12 percent reduction is recorded with FTK Remote Agent. This value is 36 percent for FTK Imager Lite and, a significant 77 percent when using the snapshot generation functionality provided by AWS and dd command. As discussed earlier, this is attributable to the powerful computational resources of the cloud. On further analysis, we note that the slope of trendline is the steepest for imaging a mounted remote machine with FTK Imager, whereas it is the shallowest for imaging using FTK Imager Lite after transferring it to the VM. The steep slope suggests a rapid increase in time with increasing capacity.

B. Effect of Acquisition Approach (complete, partial or hybrid) on the Forensic Investigation

With the partial approach we see an improvement over the complete acquisition in that the total time taken to acquire evidence is considerably reduced. However, since partial evidence is acquired on a logical level (i.e. it does not contain permanently deleted files or information from unallocated space) it may not be acceptable in the court of law. In such situations, a hybrid approach is possibly better for which acquisition time is calculated using the complete and partial acquisition time values in this experiment. Fig. 2. Shows the main activities involved in each of the three approaches.

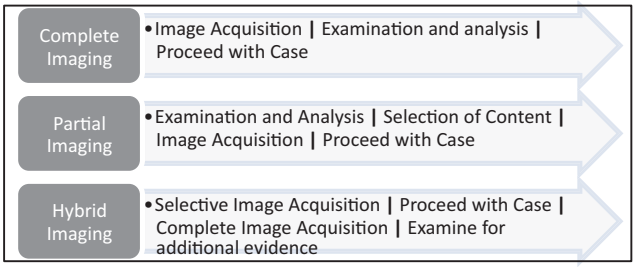

Fig 2. Overview of the order of Main Activities involved in each Image Acquisition Approach

The time calculations for hybrid approach show a reduction of 5 days when compared to the conventional acquisition approach. Since it takes the same amount of time as the selective imaging in this particular case, the former is preferable as it acquires complete evidence. This leaves little room for uncertainty when the examiner presents the case.

Hence, we can safely say that by exploiting the powerful computational resources of the cloud for acquiring a complete image, and using the remote capability of FTK for partial, memory and volatile data acquisition, the time for a remote acquisition can be reduced by a significant amount. However, due to the increased level of trust required for image creation in the cloud, this option must be carefully considered by examiners.

C. Impact of the Cloud on Digital Forensics Investigations

The cloud is an excellent instrument for criminals since VMs can be created and terminated at will, in a matter of a few minutes, leading to obliteration of evidence if not discovered in

time. Furthermore, data is usually not recoverable if permanently deleted from the VM. The reason for this is multi-tenancy. Since resources in the cloud are shared and the forensic activities are required to be carried out in compliance with the laws and regulations maintaining confidentiality of other tenants [2], complete imaging of the hard disk on which the VM resides is usually not permitted by CSPs.

In the following section, we take a look at the impact of the cloud on a forensic investigation when presented with incomplete evidence and in a time-critical scenario.

situations where data is deleted permanently or, the VM is not discovered in time.

2) Time Critical Scenarios

In time-critical cases like terrorist threats or child abductions, the delay in evidence analysis, even if it is a few hours, may prove to be disastrous as lives could be in danger. If in such cases, evidence resides in the cloud, the increase in time for acquisition is significant as compared to a device such as hard disk, thus delaying the analysis all the more.

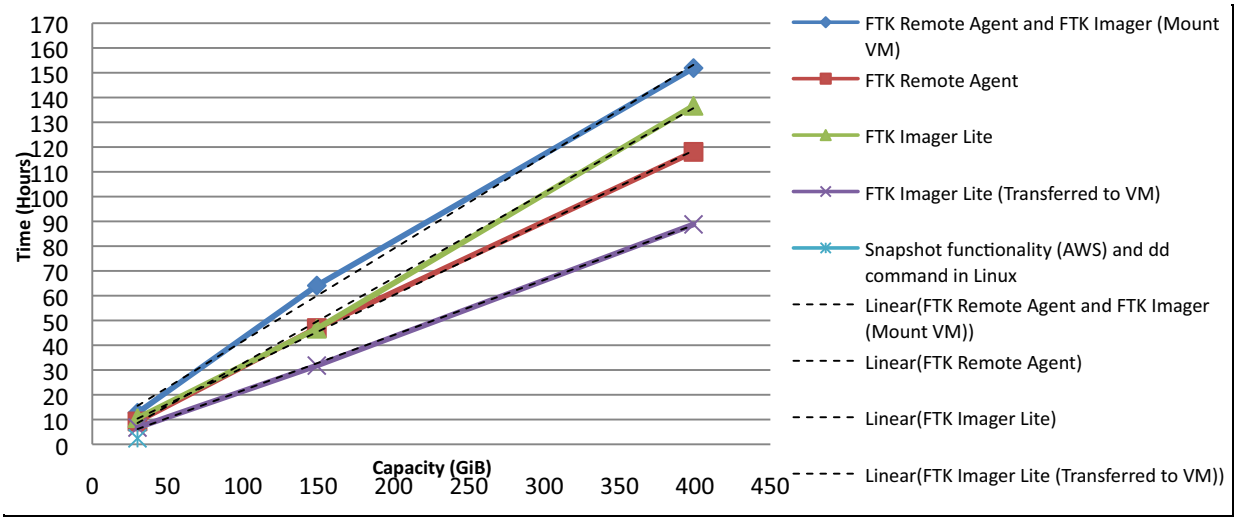

Fig. 3. Scatter Plot Representing the Relationship between Time Taken for Image Acquisition and Different Storage Capacities of Virtual Machines in the Amazon EC2 Cloud (Plotted using values in Table I)

1) Incomplete Evidence

We consider the events in our hypothetical crime scenario to elucidate. Based on the information recovered by completely imaging, Instance A allows the examiner access to Instance B only because the file containing the credentials was not permanently deleted. If it was, discovery of Instance B would be unlikely depending solely on digital evidence at hand. Let's say the examiner requests evidence from the CSP. Even in that case, given that Tom accesses Instance A using a device other than his work computer, and Mr. X accesses it using Instance C, there would be no indication of existence of Instance B. This could lead to the identification of perpetrator, however Tom would seem innocent and the abduction incident would go undiscovered, unless the device from which Tom accesses the instance was available to the examiner.

Let us also suppose that the examiner does find information in the logs provided by the CSP leading to discovery of Instance B. Since the transportation of evidence would take a few days, there is a fair chance that this evidence would have been wiped out by the time the examiner analyses the logs. Since email was one of the first tools to embrace the internet and make the transition to "cloud-based", the issues discussed apply to communication via email service too.

In a traditional scenario, the outcome would most likely differ. Thus, owing to issues of multi-tenancy and flexibility of deleting instances, which are unique to the cloud, the outcome of a cloud forensics investigation may be erroneous in

In such situations, if the examiner uses a more appropriate approach than others, it could save considerable amount of time for acquisition, thereby providing sufficient time for evidence analysis. As discussed earlier, in some cases, the use of existing tools to perform cloud forensics is necessary, such as for VMs in the IaaS platform of AWS, since it does not provide any exclusive forensic services. Relying on collecting of evidence from the CSP alone could take days which would not be suitable for time critical cases.

Based on our experiment, the examiner will discover the abduction information in time if selective acquisition is performed using FTK Remote Agent, FTK Remote Agent mounting capability & FTK Imager or, FTK Imager Lite (transferred to VM). , if the examiner uses the conventional method of imaging i.e. FTK Imager Lite from an external drive (i = 3), the perpetrator will have effortlessly obliterated all evidence by terminating Instance B before the examiner starts acquisition.

IX. Conclusion and Future Work

The Using the commercial tool, AccessData's Forensics ToolKit, we carried out partial and complete remote acquisition of evidence data from the Micro, Small and Medium storage volumes in the Ireland region of Amazon EC2 cloud. The statistical analysis results presented are intended to help investigators select appropriate methods for evidence

acquisition. Five methods of data acquisition were investigated using a statistical analysis of time. All the approaches except one showed reduction in time for acquisition on comparison with the conventional approach of imaging remote data (using FTK Imager Lite from an external drive). The last two methods used computational resources of the cloud, and thus required minimum time. For a 30GiB storage volume, the least time recorded was for the snapshot functionality where the duration for acquisition was observed to reduce by almost 77 percent. However, this method was not applicable to acquire data from ephemeral storage, since the snapshot functionality of AWS can only be used for persistent storage volumes. Among the other methods, FTK Remote Agent proved to be most efficient showing a nearly 12 percent reduction in time, as compared to the conventional approach.

While the remote acquisition methods employed in this research are only applicable to the Guest OS layer of virtual machines residing in the IaaS platform of the Amazon EC2 cloud and evaluation was primarily based on the AccessData FTK tools, it is indicative of what one can expect in Cloud evidence acquisition. The case study demonstrated how the easy creation and destruction of instances could have serious consequences for gathering evidence and thus affecting the outcome of an investigation.

It is probable that Cloud forensics is faced with the situation of never having the opportunity to image the complete evidence and that Cloud forensic investigations will always be based on incomplete evidence.

X. BIBLIOGRAPHY

[1] R. C. F. L. RCFL, "The RCFL Program's annual report for Fiscal Year 2011," 2011.

[2] K. Ruan, J. Carthy, T. Kechadi and M. Crosbie, "Cloud Forensics: An Overview," *Advances in Digital Forensics,* vol. VII, pp. 15-26, 2011.

[3] G. Richard and V. Roussev, "Digital Forensics Tools: The Next Generation," in *Digital Crime and Forensic Science in Cyberspace*, P. Kanellis, Ed., Idea Group Inc, 2006, pp. 76-91.

[4] S. Ahmed and M. Raja, "Tackling cloud security issues and forensics model," *High-Capacity Optical Networks and Enabling Technologies (HONET),* pp. 190 - 195, 2010.

[5] G. Sibiya, H. S. Venter and T. Fogwill, "Digital Forensic Framework for a Cloud," South Africa, 2012.

[6] B. Martini and K. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digital Investigations,* vol. 9, no. 2, p. 71–80, 2012.

[7] F. Marturana, G. Me and S. Tacconi, "Cloud computing implications to Digital Forensics: a new methodology proposal," in *Seventh International Workshop on Systematic Approaches to Digital Forensic Engineering*, 2012.

[8] J. Dykstra and A. T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques," *Digital Investigation,* vol. 9, no. Supplement, p. S90–S98, 2012.

[9] D. Birk and C. Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments," Oakland, CA, 2011.

[10] S. Garfinkel, A. Nelsona, D. White and V. Roussev, "Using purpose-built functions and block hashes to enable small block and sub-file forensics," *Digital Investigation,* vol. 7, no. Supplement, p. S13–S23, 2010.

[11] V. Roussev, C. Quates and R. Martell, "Real-time digital forensics and triage," *Digital Investigation,* no. (In press), 2013.

[12] C. Federici, "AlmaNebula: A Computer Forensics Framework for the Cloud," in *Procedia Computer Science, The 4th International Conference on Ambient Systems, Networks and Technologies (ANT 2013), the 3rd International Conference on Sustainable Energy Information Technology (SEIT-2013)*, 2013.

[13] J. Heiser, "Remote forensics software," Gartner RAS Core Research Note G00171898, 2009.

[14] J. Dykstra and A. Sherman, "Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform," *Digital Investigation,* vol. 10, no. Supplement, p. S87–S95, 2013.

[15] SANS, "The SANS Survey of Digital Forensics and Incident Response, A SANS Whitepaper," SANS Institute, Austin, 2013.

[16] F. Marturana, M. Gianluigi and S. Tacconi, "A Case Study on Digital Forensics in the Cloud," in *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012 International Conference*, Sanya, 2012a.

[17] H. Chung, J. Park, S. Lee and C. Kang, "Digital forensic investigation of cloud storage services," *Digital Investigation,* vol. 9, no. 2, p. 81–95, November 2012.

[18] R. McKemmish, "What is Forensic Computing? Trends and Issues in Crime and Criminal Justice," *Australian Institute of Criminology,* vol. 118, pp. 1-6, 1999.

[19] K. Kent, S. Chevalier, T. Grance and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," NIST Special Publication 800-86, 2006.

[20] Guidance EnCase, “EnCase Forensic,” 2013. [Online]. Available: https://www.encase.com/products/Pages/encase-forensic/overview.aspx. [Accessed September 2013].

[21] AccessData, “Forensic Toolkit,” 2013. [Online]. Available: http://www.accessdata.com/products/digital-forensics/ftk. [Accessed September 2013].