International Journal of Engineering & Technology, 7 (4.15) (2018) 12-15

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Proposed Proactive Digital Forensic Approach for Cloud Computing Environment

Ganthan Narayana Samy[1]*, Nurazean Maarop[1], Doris Hooi-Ten Wong[1], Fiza Abdul Rahim[2], Noor Hafizah Hassan[1], Sundresan Perumal[3], Pritheega Magalingam[1], Sameer Hasan Albakri[1]

[1]Advanced Informatics School, Universiti Teknologi Malaysia, Malaysia
[2]College of Computer Science and Information Technology, Universiti Tenaga Nasional, Malaysia
[3]Faculty of Science and Technology, Universiti Sains Islam Malaysia, Malaysia
**Corresponding author E-mail: ganthan.kl@utm.my*

Abstract

There are many challenges for the digital forensic process in the cloud computing due to the distinguished features of the cloud computing environment. Many of well-known digital forensic methods and tools are not suitable for cloud computing environment. The multi-tenancy, multi-stakeholder, Internet-based, dynamics expendability, and massive data, logs and datasets are examples of the cloud computing environment features that make conducting digital forensics in the cloud computing environment a very difficult task. Therefore, there is a need to develop an appropriate digital forensic approach for cloud computing environment. Thus, this paper proposed a proactive digital forensic approach for cloud computing environment.

Keywords: *Cloud Computing Environment; Digital Forensic; Digital Forensics Approach; Digital Forensics Processes.*

1. Introduction

The cloud computing model has emerged with some distinguished features such as low cost of computing services, high-performance, availability, ability of fast extensibility, and pay per usage [1]. There are many security attacks that can be used by hackers to attack cloud computing services such as cracking passwords, DoS and DDoS attacks, sending malicious software, and spam. Virtualization techniques also have many security concerns such as user-data segregation, data losing, data leaks and data remanence. Besides, compromising the hypervisor that manages all the virtual machines will make all the users' data in danger and compromise their privacy. In the cloud computing environment, digital forensic investigation is required in many cases such as cyber criminals attacking, suspicious activity, data breaches, policy violations, abusing assess rights, and data recovery.

One of the most common processes that follow the occurrence of any security incident is conducting a digital forensic investigation. Digital forensic process aims to find the evidences about the criminals by investigating the related data on the digital devices. There are some important processes that a forensics investigator must follow to conduct successful investigation. These processes may include; obtaining authorization to search and seize the related digital devices, documenting the chain of custody of seized devices, using sound methods and tools to create a forensic image of the data on the seized devices, examining and analysing the forensic images to obtain evidences, preparing forensic reports, and presenting evidence in the court [2].

However, there are many challenges for the digital forensic process in the cloud computing due to the distinguished features of the cloud computing environment. Many of well-known digital forensic methods and tools will not fit for cloud computing environment. The multi-tenancy, multi-stakeholder, Internet-based, dynamics expendability, and massive data, logs and datasets are examples of the cloud computing environment features that make conducting digital forensics in the cloud computing environment a very difficult task [3]. Therefore, there is a need to develop an appropriate digital forensic framework for cloud computing environment.

Thus, this paper presents a proposed cloud computing digital forensic framework. The next section of this paper highlights the related research work and Section 3 presents proposed framework. Section 4 focuses on experimental design. Section 5 discusses the proposed framework and finally, Section 6 concludes this paper.

2. Related Works

In [4-5] proposed framework that supports digital forensic in a cloud computing environment. Their proposed framework includes four steps, namely, evidence source identification and preservation, collection, examination and analysis, and reporting and presentation. They suggest that the first three steps can be performed in iteration, which give better chance to discover the required evidence [6]. Furthermore, other research proposed a Secure-Logging-as-a-Service (SecLaaS) architecture, which is a cloud base service aiming to gather all logs for the virtual machines. The proposed system designed to provide the required evidence to the digital forensic investigators as well as guarantees the logs integrity from any misuse by the cloud provider's internal staff or the digital forensic investigators [7].

In [8] proposed a network digital forensic framework based on the Digital Forensic Model (DFM) for IaaS cloud computing environment. Due to the dynamic structure of the IaaS, they proposed a real-time-based iterative forensic process. Their proposed framework contains eight phases; preparation of infrastructure, detection of incident, incident response, capturing of network traces, examination of incident packet, analysis of incident packet, extraction, and reporting. In evaluation phase the session traffic is captured and analysed to find details about the attacks, timeline of log, and performance. They used Snorby tool to distinguish the potential attack from the normal traffic. Log2timeline tool is used to extract the date and time from log files (such as system logs, application logs, and network device logs).

In [4] proposed a cloud based forensics framework for social networks. The proposed framework has five layers; infrastructure layer, virtualization layer, data pool layer, crawler layer and analysis layer. The infrastructure layer contains the cloud computing hardware infrastructure, including storage and network services. Virtualization layer is the cloud computing structure such as multi-tenant, parallel and distributed process, and multi-thread services. The data pool layer is used to manage isolating users' data and log files such as user log files, system log files, network log files, and attack log files. In crawler layer, the social network data will be collected, parsed and stored in the database. Finally, in analysis layer the log query will be served, as well as all the digital forensics activities.

In [9] proposed a forensic framework for cyber-physical cloud systems. The framework involves six components; risk management principles and practices, forensic readiness principles and practices, incident handling principles and practices, laws and regulations, CPCS hardware and software requirements, and industry-specific requirements. The proposed framework aims to integrate the forensics tools into the infrastructure of the cyber-physical cloud system, so it will be able to conduct proactive forensic data collection. This approach will be helpful for the cloud forensic system and will help to overcome the challenges that accompany the cloud environment characteristics. In addition, this approach will be useful for the cloud system that cannot be shut down to conduct digital investigations. However, implementing such approach need more research to be suitable for different cloud computing systems.

3. The Proposed Approach

In the proposed framework, there are two main phases, proactive phase and investigation phase. The proactive phase aims to prepare the virtual environment before any incident occurred. The early plan for digital investigation must be prepared and the necessary tool should be set up in the virtual machines. In the second phase is the investigation phase. This phase starts when the incident occurs and involve the following processes; readiness, identification, preservation and collection, analysis and examination, and finally reporting and presentation. Figure 1 depicts the phases of the proposed framework.

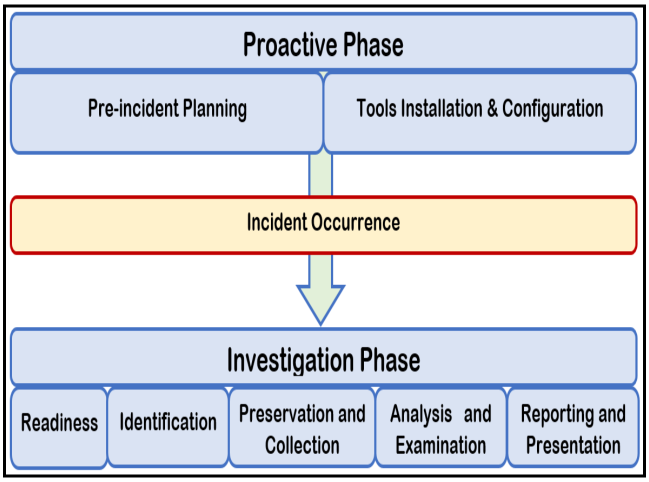


Fig. 1: The Proposed Approach.

3.1. Proactive Phase

This process, known as proactive process is performed before the incident occurrence. It should be performed during the cloud computing system installation. This process involves planning for the future digital forensic and install the proactive digital forensic tools.

3.1.1. Pre-Incident Planning

The infrastructure of the cloud computing is built on virtualization technology, which means that all data will vanish after virtual machine removing. Therefore, the successful digital forensic must capture data before it erased, this is only possible if there is pre-incident planning for the digital forensic processes. The pre-incident plan should cover both virtual machines and network. The logs of the network devices and the details of network traffic between the virtual machines must be captured and save to a log repository. In the Infrastructure as a Service (IaaS), the cloud customer will have the full control of the virtual machine, thus, the pre-incident plan should be included within the Service Level Agreements (SLA). The pre-incident plan should be included during virtual machine preparation and configuration. The log files should be sent to a log repository to ensure its safety and availability for the future digital investigation.

3.1.2. Forensic Tool Installation and Configuration

During the virtual machine preparation and configuration, the forensic software and tool must be installed and configured. These tools will collect an important information about the users' activity, which make the digital forensic investigator job's faster, easier and more efficient. One of the good examples of the pre-incident tools that forensic investigators will benefit is the System Monitor (Sysmon) tool, which is a network monitoring tool designed to provide high performance and accurate network monitoring. Sysmon tool supported protocols including SMTP, IMAP, HTTP, TCP, UDP, NNTP, and PING tests. Forensic Open-Stack Tool (FROST) is another example of the forensic tools that can be used in the IaaS cloud computing model. OpenStack is an open-source computing platform intended for public and private cloud services. FROST is an integrated forensic tool in OpenStack platform. LogRhythm company has developed threat lifecycle management tools that monitor the network communications. These tools detect the network-based threats in real time and can alert the administrator and collect the forensics data that will help the forensic investigators.

3.2. Investigation Phase

After the incident occurred, the investigation phase will be started. The investigation steps will follow the same order as in traditional computing, yet, the procedures within each step will be according to the cloud computing requirement. There are five steps; readiness, identification, preservation and collection, analysis and examination, and finally reporting and presentation court [2].

3.2.1. Readiness

Readiness is the first step in the digital forensic investigation. In this step, two forensic activities should be achieved; selecting the forensic investigator team and define investigation scope and producers. The selected digital forensic investigators must be qualified to work with cloud computing techniques. Their knowledge and expertise should include forensic principles, guidelines, procedures, tools, and techniques, cloud computing infrastructure, virtualization, networking and internet technologies and protocols. Besides, the investigation scope and limitations, policies, and procedures of the forensic investigation must be defined. Cloud computing environment is a shared environment, thus more attention to privacy issues and laws that protect users' rights.

3.2.2. Identification

At this level, the investigation will be more specific, focused and limited to the incident. The incident related data must be identified by the investigation. At the end of this step, investigators must have identified what data related to the incident, where can be found, and the possibility of correlation (i.e. possibility of using more than one device in the committing crime). Moreover, the type of required documentation that should be used during data collection must be identified based on the incident and data that need to be collected.

3.2.3. Preservation and Collection

In the cloud computing environment, hyper-visor (i.e. virtual machine manager) use snapshot (i.e. taking a copy for the virtual machine) techniques to create images for the virtual machine to be used as restore point to restore the original status of the virtual machine. In many cases, users need to restore the original statues of the virtual machines such errors or malfunction because of installing new software or driver [10]. In the traditional computing environment, the seizing and preserving of the physical devices that used in the crime must be performed in this step. This is not applicable for cloud computing environment, where the main devices are virtual machines. However, the snapshot techniques can be used to create images for the virtual machine to keep its status after incident occurrence.

In [1] suggested where the digital investigators should look for evidence in the cloud computing environment for each of the cloud service models. In the Software as a Service (SaaS) model, the evidences are most likely stored on a desktop, laptop, tablet, or smartphone. Platform as a Service (PaaS) model the evidences are most likely found on a desktop or server, although it could also be stored on a company network or the remote service provider's infrastructure. In the Infrastructure as a Service (IaaS) model, the evidences are usually found on a desktop or server; infrastructure equipment can be owned by the company or the remote service provider. In this paper, we focus on the IaaS model, thus the snapshots taken from the virtual machines are the main resources of the evidence. Besides, in case the virtual machine is in the running mode, a copy of the memory can be taken from the virtual machine memory. Memory dumping is very important to collect data that may include critical information about the incident or the committed crime. The hypervisor logs and network monitoring reports are also important resources of the evidences.

3.2.4. Analysis and Examination

In this step, the collected data can be analysed and examined to extract the necessary evidences Data analysis should not be limited to the obvious data, but also deleted files. Criminals usually delete or overwrite the files that may include evidence of their crimes. This is one of the most challenges of the digital forensic investigators during the data analysis are the deleted or overwritten data. Any extracted files from the analysed virtual machines should be saved to the data repository and well documented for the next steps of the investigation. All the collected data must be analysed and examined including the snapshot for the virtual machines, memory dump files, hypervisor logs and network monitoring reports. Unlike the traditional cloud computing, where there are many forensic tools that can be used in data analysis, forensic tools in the cloud computing environment still need more development to be appropriate for cloud computing environment.

3.2.5. Reporting and Presentation

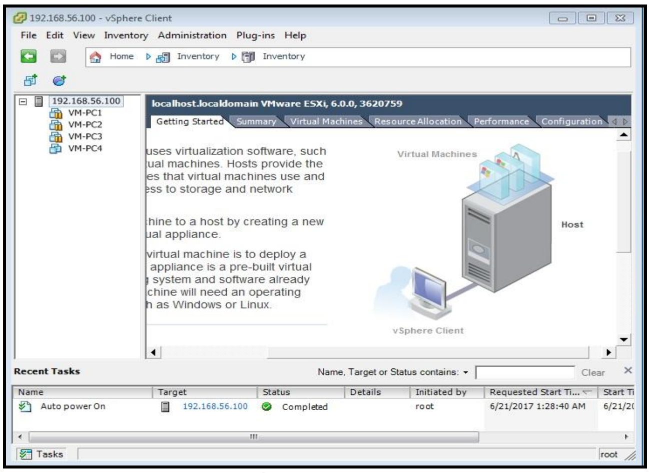
The results of the previous step that is form analysis and examination phase should be written in the final report of the investigated incident. The report must be written in clear and easy to understand by the audience whom do not have a technical understanding, yet not omitting any valuable information. Usually, the audience of the report will include judges, lawyers, and organization stockholders. The digital forensic investigators should be aware of consequences of potentially wrong or misinterpreted reports. The report should elaborate all the processes of the forensic investigation. This might include the potential evidence and how they were collected, the analysis techniques and how they were used. If there are any assumptions made, it must be clearly stated in the report with proper justification for the assumptions.

4. Experimental Design

To test the proposed framework, we designed a cloud computing environment. The aim of the experiment is highlighting the effectiveness of proactive approach in the digital forensics in the cloud computing environment. VMware vSphere ESXi Hypervisor v6 has been used to build the cloud environment. It is developed by VMware for deploying and serving virtual computers. Unlike other VMware products, vSphere ESXi Hypervisor has its own kernel and do not need an operating system (OS) to work. The physical hardware device that used to install the vSphere ESXi Hypervisor v6 has the following Specifications:

- System Manufacturer: Hewlett-Packard, HP Compaq Elite 8300 CMT
- System Type: x64-based PC
- Processor: Intel(R) Core(TM) i5-3570 CPU 3.40GHz, 4 Core(s), 4 Logical Processor(s)
- Physical Memory (RAM): 12.0 GB.
- Hard disk: 1 TB.

We created four virtual machines in the cloud infrastructure with 2GB RAM and 15GB hard disk for each. Windows 7 has been used as the operating system on the virtual machines. Figure 2 shows the vSphere ESXi Hypervisor v6 used in the experiment.



uses virtualization software, such
ual machines. Hosts provide the
es that virtual machines use and
ess to storage and network

hine to a host by creating a new
ual appliance.

virtual machine is to deploy a
appliance is a pre-built virtual
system and software already
chine will need an operating
h as Windows or Linux.

Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Ti
Auto power On	192.168.56.100	Completed		root	6/21/2017 1:28:40 AM	6/21/2(

Fig. 2: vSphere ESXi Hypervisor v6.

In this experiment, we used System Monitor (Sysmon) as a monitoring utility. Sysmon tool has been installed on the virtual machines during cloud computing environment preparation. Sysmon tool has been used to monitor the following activities:

4.1. Process Creation

Whenever a new process starts Sysmon create a Process Create event. In addition, it records the hash of the process image using either MD5, SHA1 or SHA256 hash algorithm. It records the process GUID for better correlation since Windows may reuse a process PID.

4.2. Process Termination

Sysmon also record an event whenever a process exits or terminated.

4.3. Driver Loaded

Sysmon creates a log record whenever Windows loads a kernel-mode driver. This will help to capture activity made by even sophisticated kernel-mode malware.

4.4. Image Loaded

Events capture details of the event log whenever a process maps an image into its address space, including its executable image and every DLL that it loads.

4.5. File Creation Time Changed

Sysmon records an event whenever a process explicitly changes the file creation timestamp of an existing file. The event data includes both the new and previous timestamps to help track the file's real creation time.

4.6. Network Connection Detected

Sysmon records an event for source process, IP addresses, port numbers, hostnames and port names for network connections. This can help to identify when malware is trying to spread within the network or when communicating with external endpoints.

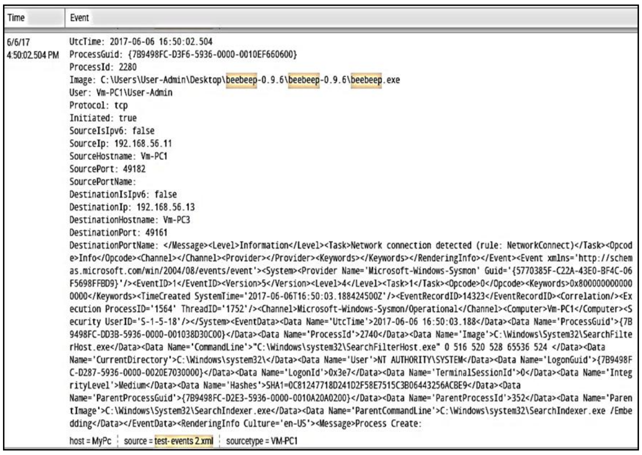
4.7. Create Remote Thread Detected

Sysmon also creates a log event whenever it captures information when one process starts a new thread in another process. The new thread runs in the virtual address space of the target process and has full access to memory and other resources belonging to that process.

4.8. Raw Access Read Detected

Sysmon tool also records the raw disk and volume accesses when the disk or volume is opened directly rather than through higher-level APIs. Malicious toolkits commonly perform such operations to bypass higher-level security protections and auditing.

An open source LAN messenger application named BeeBEEP has been used to make network connections between the virtual machines and share some files. BeeBEEP is supporting chat and files sharing with all the users within local network such of an office or home. It can work without a server. In this experiment, BeeBEEP has been used on the virtual machines to create chat sessions and share files between the users. Figure 3 shows a report generated by Sysmon tool, the report details include the BeeBEEP application, the source and destination IPs, and other details.



```
Time            Event
6/6/17          UtcTime: 2017-06-06 16:50:02.504
4:50:02.504 PM  ProcessGuid: {7B9498FC-D3F6-5936-0000-0010EF660600}
                ProcessId: 2280
                Image: C:\Users\User-Admin\Desktop\beebeep-0.9.6\beebeep-0.9.6\beebeep.exe
                User: Vm-PC1\User-Admin
                Protocol: tcp
                Initiated: true
                SourceIsIpv6: false
                SourceIp: 192.168.56.11
                SourceHostname: Vm-PC1
                SourcePort: 49182
                SourcePortName:
                DestinationIsIpv6: false
                DestinationIp: 192.168.56.13
                DestinationHostname: Vm-PC3
                DestinationPort: 49161
                DestinationPortName: </Message><Level>Information</Level><Task>Network connection detected (rule: NetworkConnect)</Task><Opcod
                e>Info</Opcode><Channel></Channel><Provider></Provider><Keywords></Keywords></RenderingInfo></Event><Event xmlns='http://schem
                as.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06
                F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x800000000000
                0000</Keywords><TimeCreated SystemTime='2017-06-06T16:50:03.188424500Z'/><EventRecordID>14323</EventRecordID><Correlation/><Ex
                ecution ProcessID='1564' ThreadID='1752'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Vm-PC1</Computer><S
                ecurity UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>2017-06-06 16:50:03.188</Data><Data Name='ProcessGuid'>{7B
                9498FC-DD3B-5936-0000-001038D30C00}</Data><Data Name='ProcessId'>2740</Data><Data Name='Image'>C:\Windows\System32\SearchFilte
                rHost.exe</Data><Data Name='CommandLine'>"C:\Windows\system32\SearchFilterHost.exe" 0 516 520 528 65536 524 </Data><Data
                Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{7B9498F
                C-D287-5936-0000-0020E7030000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='Integ
                rityLevel'>Medium</Data><Data Name='Hashes'>SHA1=0C81247718D241D2F58E7515C3B06443256ACBE9</Data><Data
                Name='ParentProcessGuid'>{7B9498FC-D2E3-5936-0000-0010A20A0200}</Data><Data Name='ParentProcessId'>352</Data><Data Name='Paren
                tImage'>C:\Windows\System32\SearchIndexer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\SearchIndexer.exe /Embe
                dding</Data></EventData><RenderingInfo Culture='en-US'><Message>Process Create:
                host = MyPc | source = test- events 2.xml | sourcetype = VM-PC1
```

Fig. 3: Example of the event report for Sysmon Tool.

5. Discussion

In our experiment, the collected data that generated by Sysmon tools have been analysed by using Splunk software. Splunk software is developed by the Splunk Enterprise, it monitors and analyses machine data from any source and it is compatible with Sysmon tool. Splunk helps to analyse everything from transactions to security events and network activity.

Unlike cloud computing environment, implementing and using the proactive forensic approach in the traditional computing environment is not always applicable. It may be applicable in case of the devices that owned by organizations, but not the individuals. The usage of proactive approach is very effective in a cloud computing environment, where the installing and configuring forensic tools during the systems preparation is applicable. The enhanced approach overcome the weaknesses and limitations exist in the current forensics approaches. This approach will help the digital forensic investigators to extract the required evidences. The forensic investigations will be conducted in less time and obtained more accurate and reliable results.

Humans play the main role in the forensic analysis and investigation, while conducting forensics investigation. The professionals who are going to conduct the forensics investigation must be well trained, know a background of the business of the organization and type of the services that the cloud service in which the investigation will be conducted. The forensic investigators must know exactly what kind of the data they will retrieve, and they must able to distinguish between the good and bad evidences. However, in the proactive approach, the main source of the data will be the pre-installed forensic tools. The reports generated by these tools can be customized to provide the required evidences in very clear form. Most of the current proactive forensic tools are not comprehensive and usually limited with few and specific functions. Therefore, using a combination of forensic tools can be very effective. The cloud service provider must consider embedding forensic tools in their cloud computing environments and conduct more efforts to enhance the existing forensic tools and its generated reports.

The proactive forensic approach will be very effective in a cloud computing environment due to many factors. First, it can be implemented easily by the service provider. Second, it will provide a valuable resource of information that can be used to create sound and solid evidences. Third, it will reduce the time of digital forensic investigation, which save time and money and as well as the investigators' efforts.

6. Conclusion

Cloud computing environment has some distinguished characteristics that make the usage of the current forensic approaches are not applicable. In this paper, a proactive digital forensic approach has been proposed to be used in the cloud computing environment. An experiment has performed to show the effectiveness of the proposed approach. This experiment showed that the proactive forensic approach is very effective and overcome the weaknesses of the current forensic approaches in the cloud computing environment. In this study, the proactive approach has been used in an infrastructure as a service (IaaS) model, however, it can be applied in other cloud computing model by embedding suitable forensic tools in the structure of the cloud computing before service delivery process.

Acknowledgement

The authors would like to thank Malaysian Government and Universiti Teknologi Malaysia (UTM) for supporting this work through the Fundamental Research Grant Scheme (FRGS) under Grant vote number RK130000.7838.4F714.

References

[1] Alsubaih, A., Hafez, A., & Alghathbar, K. (2013). Authorization as a service in cloud environments. Proceedings of the IEEE Third International Conference on Cloud and Green Computing, pp. 487-493.

[2] British Standards Institution, ISO/IEC 27043:2016 Information technology. Security techniques. Incident investigation principles and processes, 2016.

[3] Han, F. (2016). Cloud based forensics framework for social networks and a case study on reasoning links between nodes. International Journal of Future Generation Communication and Networking, 9(1), 23-34.

[4] McKemmish, R. (1999). What is forensic computing? Australian Institute of Criminology.

[5] Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. NIST Special Publication, 10, 800-86.

[6] Martini, B., & Choo, K. K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 9(2), 71-80.

[7] Zawoad, S., Dutta, A. K., & Hasan, R. (2013). SecLaaS: secure logging-as-a-service for cloud forensics. Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, pp. 219-230.

[8] Ahmad, S., Saad, N. L., Zulkifli, Z., & Nasaruddin, S. H. (2015). Proposed network forensic framework for analyzing IaaS cloud computing environment. Proceedings of the IEEE International Symposium on Mathematical Sciences and Computing Research, pp. 144-149.

[9] Ab Rahman, N. H., Glisson, W. B., Yang, Y., & Choo, K. K. R. (2016). Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Computing, 3(1), 50-59.

[10] Hirwani, M. (2012). Forensic acquisition and analysis of vmware virtual hard disks. Proceedings of the International Conference on Security and Management-World Congress in Computer Science, Computer Engineering and Applied Computing, pp. 1-7.