INFORMATION SYSTEM FORENSICS (IA 5210)

TERM PAPER TOPIC - CLOUD FORENSICS

CLASS PAPER SUBMITTED TO

PROFESSOR FREDERICK HOWELL

DEPARTMENT OF INFORMATION ASSURANCE

BY

PREET SHAH

BOSTON, MASSACHUSETTS

AUGUST 2015

TABLE OF CONTENTS

ABSTRACT

Cloud computing is a resourceful technology that supports large scale of applications. The cloud can be defined as a service provided using the internet for a variety of resources that can be accessed remotely through the web. Resources include Networks, Servers, Data Storage, Applications and Services. Cloud can be used with a variety of applications where the amount of data is too large to be stored, for example, healthcare, shopping sites, accounting applications, etc. Here, we have a huge amount of data to be stored locally on a server and this causes performance and network issues. Two factors make cloud computing popular in today's market: cost effectiveness and efficiency. Because of these factors nearly 40-50% of industries are shifting to cloud servers. This shows that cloud users are increasing daily and this trend will continue.

However, criminal activities in cloud servers are also increasing day-by-day. To support the forensic investigation, cloud service providers (CSPs) and customers have to develop adequate forensic capabilities. Better cloud forensics capabilities can facilitate the investigation. In this paper, we will start our discussion with basic cloud computing concepts. It is very important to understand the cloud computing concepts before we merge digital forensics and cloud computing. Later on we will move towards digital forensics in a cloud environment. We will also be discussing the three important dimensions of cloud forensics, the challenges faced in the investigation and the benefits of cloud computing in digital forensics. This paper is designed in such a way that it can help the readers to get an overview of cloud computing and cloud forensics.

1. INTRODUCTION

Definition

Cloud forensics is the application of digital forensic science in the cloud computing environment as a part of network forensics. In other terms, cloud forensics is the cross-discipline between cloud computing and digital forensics. As cloud computing is part of network, cloud forensics can also be considered as a subset of network forensics. Thus, cloud forensics follow the main principles found in the network forensic process with some techniques specially customized for the cloud computing environment.

Why do we need Cloud Forensics?

The demand of cloud computing is increasing exponentially. As per the Forbes report, IT companies spending on security technologies will increase 46% by next year, with cloud computing increasing 42% and business analytics investments is up by 38%. Thus, as the year passes the demand of cloud will be increasing. Although cloud computing has become increasingly popular, security remains a vital concern when accessing data online. The cloud service providers and the customers have yet to establish forensic capabilities that will support the investigation in case if any crime is committed. There are 3 main dimensions of Cloud Forensics which need to be understood and addressed by the Cloud Service Providers and the Customers are: Technical dimension, Organizational dimension and Legal dimension.

In the past years, hackers used the cloud service to hack into Sony's PlayStation (PS) network. There are numerous incidents related to cloud breaches that shows there is an urgent need to conduct cloud computing forensics. Hence, we need strong cloud forensic capabilities that facilitate forensic investigation.

2. CLOUD COMPUTING

Firstly, we will study basic cloud computing. It is very important to understand the cloud technology and it's mechanism before studying cloud forensic concept. Here, we will study different levels of cloud computing and its actual use in the market. Answering the following four questions will give us good insight of cloud computing.

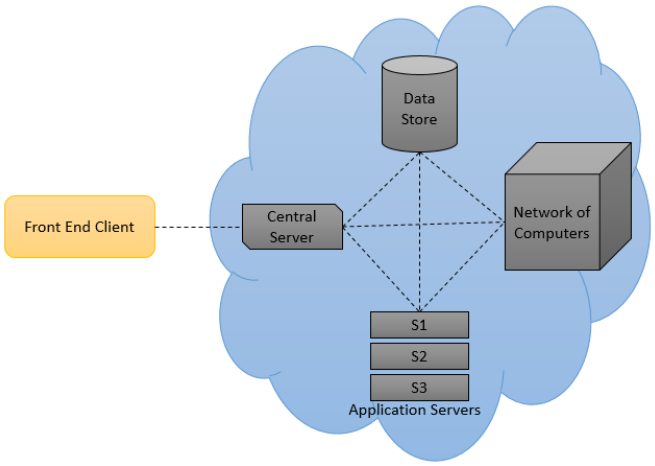
What is cloud computing?

Cloud, in simple words means providing scalable resources remotely to a software using the internet. It is a sub-network of a network providing access to remotely access the resources. The information on cloud is stored in a physical server connected to internet where the subscribed devices can connect for the on demand services. There are various clouds available on the internet serving different purposes having their own finite boundaries. The internet serves as a common medium for accessing a cloud resource for a particular system. Hence, it can be said that the internet is a broad scale public resource cloud where there are various other private clouds hosted by different cloud owners serving a variety of purposes. The cloud resources are accessed using the internet using any protocols used for accessing resources remotely. The aim of the cloud is to perform more work at a lower cost. Another name of Cloud computing is on demand service, i.e. Pay per use services. All the maintenance of the service is being carried out by the Cloud Service provider and hence, the end user or the consumer is provided with the maintenance free services.

How cloud computing works?

Now, we will study the cloud architecture to understand the technical flow of data from cloud servers to the user's system and vice a versa. The Cloud computing architecture consists of

two layers: Front End and Back End, both of which are connected by internet. The Front End is with which the users interact with the web. This allows us to access the cloud computing system using internet or a software. The Back End consists of the hardware such as a grid of computers, servers and data stores which stores all files and information that comprises of computing services. Usually there will be a separate server for each service. There is a central server that administers the system which monitors traffic and client demands that ensures everything runs well. Additionally, the Central Server follows a set of rules known as protocols. It also uses the software service called middleware that allows the network computers to communicate with each other.



Cloud Architecture

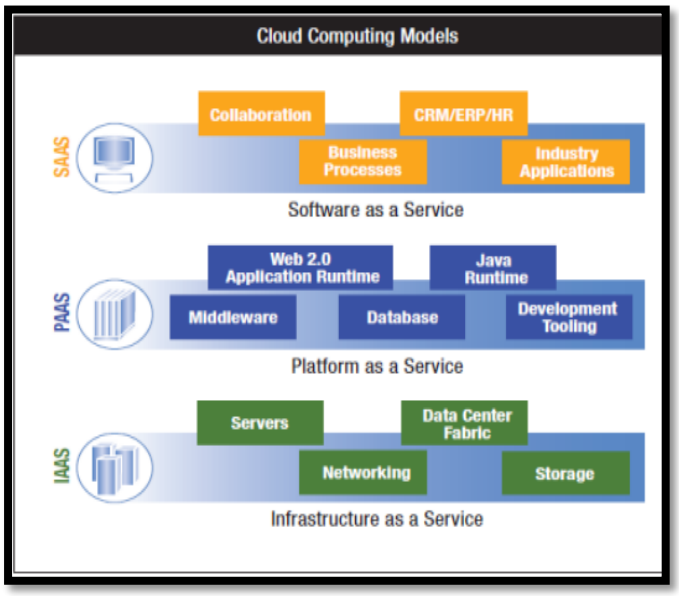
Why cloud computing is needed in today's life?

Traditionally, organizations have their own network storage servers where all the data and related services provided resides. This incurs hefty costs in terms of expense as well as performance and efficiency. Taking an example of Google, where there are millions of requests at a time coming to the server. If the server is hosted locally then there would be a large amount of load on the server serving all the clients efficiently. People now a days expects the response

from the server to be as quick as possible and the expectation is not even in seconds but in milliseconds or even less. In order to fulfil such requests using a physical data store is difficult where the entire load in on the server hosted. Using cloud we can eliminate the need of physical equipment and entire server can be hosted on the web where we can have more throughput for the services and with reasonable cost and increased efficiency and minimal maintenance. Every organization can have their own private/public cloud hosted on the internet. Flexibility, lower cost and fast performance are the factors contributing for the success of cloud computing.

What are the three layers of cloud computing?

Essentially, there are three layers under which the cloud services are divided which are briefly explained as below:



Cloud Computing Models

IaaS (Infrastructure as a Service): This is at the lowest level of the layer where the CSP provides the network equipment, servers, etc. via cloud and the consumer needs to build the operating systems, applications and required customizations on top of it. Mostly used by the Network

architects. For example, Amazon Elastic Compute Cloud (EC2), IBM Computing on Demand (CoD) and Microsoft Live Mesh.

PaaS (Platform as a Service): This provides the application development a room for hosting the application where all the required pre built run time environments are already stored such as the JVM. This is quite useful when there is a large application and the enterprise does not want to host on their private server. This service also helps developers to develop an application on top of the existing platforms available such as Yahoo Open Strategy.

SaaS (Software as a Service): In this, both the above services, i.e. IaaS and PaaS are already built and ready to subscribe and used by the end users. So, as its functions suggested the main target audience are the end users. So, as we move from IaaS to SaaS the fees for the CSP increases, which is obvious as we are getting more as we move up from IaaS to SaaS. This acts as a model of software deployment where the customer gets the license to use the third party services. For example, Google Apps and Salesforce.com.

3. DIGITAL FORENSICS IN CLOUD ENVIRONMENT

In this chapter, we will study two important steps of digital forensics that are common in any digital crime investigation. Acquisition of data and Investigation processes are the two steps of digital forensics. We will explore acquisition and investigation process in the cloud environment. Before starting with the steps of digital forensics process, we will study tools that can be used in cloud forensic investigation.

Tools for cloud forensics

As cloud computing is a new technology in the market, we do not have broad range of tools for cloud forensic investigation. As studied earlier, cloud forensics is a part of network forensics, we can use network forensics tools in investigating cloud crime.

As per the research carried out by the UMBC cyber defense laboratory for examining the usability of the tools in cloud investigation, the below listed tools can be used.

TOOL	TRUST REQUIRED
FTK	OS, Host, Hardware, Network
EnCase	OS, Host, Hardware, Network
FTK Imager (disk/memory)	OS, Host, Hardware, Network
Fastdump	OS, Host, Hardware, Network
Volume block copy (dd)	OS, Host, Hardware, Network
Memoryze	OS, Host, Hardware, Network
Agent Injection	OS, Host, Hardware, Network
AWS Export	AWS Technician, Hardware and Software, AWS Hardware and AWS Network

Forensic Open-Stack Tools (FROST): FROST is for open source cloud computing platform that includes public and private cloud environments. Forensic Open-Stack tools provides forensic response capabilities for Cloud Service Providers (CSP). Significant feature of FROST is that it bypasses the hypervisor (hypervisor- virtual machine used for monitoring the cloud). Management Plane is a tool that can be used with the FROST for preserving the evidence. Collected data can safely be placed in management plane and we can reconfigure the cloud servers on the fly.

F- Response Now: F-Response Now uses a patent pending remote connectivity technology that enables an authenticated, read-only connection to be created between the investigator's system and the suspected system, irrespective of the network. This tool's performance varies on the internet connectivity.

Acquisition in Cloud

Acquiring the evidence from the suspected cloud server or system is extremely important. Acquisition of data from the cloud solely depends on the nature of the case. For example, if attacker accessed CSP's network by breaking the firewall, then we need to examine the firewall logs and IDS logs for investigation. Here, we will not try to collect data from the company's system. Hence, it totally depends on the nature of the case and so, there is not any set of rules for acquisition.

However, there are some basic steps that need to be followed for acquiring the data from the cloud, they are:

- If the investigation requires specific set of files than we can use standard acquisition methods.

- Cloud has large data and therefore, it is not feasible to make an image of the entire cloud server. Than have to limit the acquisition process by taking help of CSP.
- Setup another cloud system dedicated to the investigation. This system will be used only by approved authorized user.
- Use Snapshot for cloud system running on virtual machines. Snapshot provide valuable information of the entire incident.
- Prepare dummy cloud servers based on the information gathered from the Snapshot.
- Final step is to calculate the hash values of the dummy cloud servers and compare it with the actual cloud servers. Change in hash values, MAC dates and times, etc. will show the changes made in the files. This information can be very useful for the investigators to determine the altered files with the time of modification and the machine address.

Investigation in cloud

Investigation process includes investigating CSPs, investigating customers, investigating prefetch files and investigating stored cloud data on system.

Investigating CSP: Based on the SLA and the incident response team of CSP, investigation can be started. Investigators should ask few questions to CSPs as a part of investigation, they are:

- Can investigators take help of staff members and resources in investigation?
- Is knowledge base of existing cloud topology and devices are available?
- Are there any constraint (as per SLA) on collecting evidence from the cloud servers?
- Are there multiple CSPs involved in the suspected Cloud topology?
- Where is the exact location of cloud storage that contains suspected data?

Investigating Customers: There are two ways cloud customers can use cloud application: using CSP specific application on their devices or by accessing through web browsers. If they are using CSP specific application than investigators have to investigate in the application folder because it would contain all the files transferred. If they are using web browsers then investigators have to check browser history and logs.

Investigating Prefetch Files: Microsoft has created prefetch file concept in order to reduce the computation time of the application. Prefetch files contain the DLL pathnames and metadata used by any application. This can reduce the launch time of the application and the system will work faster than usual. Prefetch files help investigator by providing application's MAC times and also provides the number of times an application has run on the device.

Investigating Stored Cloud data on system: There are many public cloud storage available in the market. Widely used public cloud storages are Dropbox, Google Drive and OneNote. Applications of these cloud storages have registry entries, so if an attacker uninstalls cloud application from his device, investigator can use the registry for the investigation. While investigating the cloud contents from the suspected machine, investigators should verify the contents of cloud application with the CSP's web connected login records. Users should also follow this method in order to check whether their cloud account has been hacked or not.

4. THREE DIMENSIONS OF CLOUD FORENSICS AND RELATED CHALLENGES

Cloud forensics is not just a technical issue but, a multi-dimensional issue. In this chapter we will study all the three dimension characteristics of cloud forensics- Technical dimension, Organizational dimension and legal dimension. We will also discuss the investigation challenges faced in each dimension.

Technical Dimension

As the name suggest, it consist of tools and procedures that are required to perform the forensic investigation in cloud computing environment. In this section, we will study data collection, live forensics, evidence segregation, proactive measures and virtualized environments.

Data Collection: This process include the following steps: identifying, labeling, recording and acquiring forensic data. The forensic data includes artifacts from the customer's end that reside on customer premises and the artifacts from service provider's end that are located in the cloud service provider infrastructure. Segregation of duties between service providers and customers in forensic responsibilities become different in different service models, and interaction between multi-tenants sharing same resources are different in different deployment models. The collection process should preserve the integrity of data with clearly defined segregation of duties between the customer and service provider. It should also follow the chain of custody throughout the investigation process.

Challenges: Now we will study the challenges in data collection process. In every combination of cloud service model, the cloud customer faces the challenge of decreased access to data. Access to data varies considerably based on the cloud model that is implemented. This means,

cloud customers generally have little or no control of the physical locations of their data. In fact, they may only be able to specify location at a high level of abstraction, typically as a container. Service providers intentionally hide data locations from customers to facilitate data movement and replication. For example, we require IP logs, virtual machine access logs and disk images in data collection process, all this information is crucial while conducting the investigation, but it is very difficult to gather these information from cloud servers.

Data storage Elasticity: It is considered to be one of the central attributes to cloud computing. Elasticity plays a major role in cost reduction. The cloud resources can be provisioned and released quickly on demand. Also, the resource acquiring and releasing can be automated to make sure that the application requiring the resource will have that resource at any given point of time.

Challenges: There are three main cloud forensic challenges in this technical dimension entity, they are:

1. Proliferation of Endpoints: the large number of resources connected to the cloud, the impact of a crime and the workload of an investigation can be massive.
2. Event-time synchronization: Time synchronization of events is complicated because the data of interest resides on multiple physical machines in multiple geographical regions, or the data may be in transit. Thus, making it difficult for the forensics expert to study the series of events taking place before the intrusion.
3. Retrieve deleted data: Deleted data is an important source of evidence in traditional digital forensics. In the cloud, the customer who created a data volume often maintains the right to alter it. When the customer deletes a data item, the removal of the mapping in the domain

begins immediately and is typically completed in seconds. Remote access to the deleted data is not possible without the mapping.

Virtualization: The capability of cloud to provide multi-tenant services at the infrastructure, platform, or software level is often justified by the ability to provide some form of virtualization to create economic scale. It is a key technology that is used to implement cloud services. If Virtual Machine (VM) technology is used in cloud infrastructure, then we must be concerned about compartmentalization and hardening of those Virtual Machines. Many cloud service providers' uses hypervisor to monitor and run the servers. Hypervisor is used to control and monitor the virtual cloud server without actually going to the physical location of the servers.

Challenges: It is always easy to attack main system rather than attacking multiple systems of interest. This logic is applied by the attackers and they usually try to attack the hypervisor. Hypervisor can be compared as the kernel of the old operating system. Due to lack of policies, procedures, tools and techniques it is very difficult for the forensic investigator to investigate the hacked hypervisor and gather the important information.

Furthermore, data mirroring over multiple machines in different jurisdictions and the lack of transparent, real-time information about data locations also contributes more hindrance in the investigation. There are chances that investigators might unknowingly violate laws and regulations because of lack of information about data storage jurisdictions. Additionally, it is very difficult for the cloud service providers to provide exact geographic location of the cloud server for the piece of data. All these factors clearly indicates that, it is a very challenging task for a forensic investigator to retrieve information from the cloud.

Organizational Dimension

Forensic investigation in cloud computing environment involves three entities, these being- consumer, cloud service provider, and sometimes the third party. Proper organizational structure is required in order to carry out cloud forensic activities flawlessly and effectively.

Organizational structure includes Service Level Agreements (SLAs) and policies. SLAs are the terms and conditions signed by two entities that are involved in one business (i.e. Client and CSP should have one SLA between them that contains all the information of the services provided by the service providers to the client). Policies are the organizational laws, these are for the internal staff members. Organizational structure will help us in understanding the set of rules that should be followed inside the organization in order to secure the information (in our case cloud data).

It is very important for any organization to secure their systems from internal attacks. For example, if an organization is using physical servers than they have to secure the server rooms properly with securities like, physical security, securing from natural calamities, securing from weather, etc. Similarly, if an organization is using cloud servers than they have to take security measurements to avoid internal attacks. This is because, most of the time internal attacks are occurring due to ignorance of the internal staffs. Also, internal staff, customers and external assistant should be trained enough to help the forensic investigators. If an organization has experienced forensic investigators and experienced technicians then it would make the investigation much easier. However, this is not the case in every organization.

Challenges: There are two major challenges faced in establishing forensic capabilities in the organization.

1. Internal Staffing: Many a times the organization uses their internal investigation team. Internal investigation team is either inexperienced or they do not have sufficient tools to investigate properly. Moreover, they use the network forensic tools which might not be sufficient for their investigation. Organizations should either hire the external forensic team or enhance their in-house forensics labs by getting proper tools. Also, the organization should hire experienced forensic experts for the cloud investigation, because in cloud investigation is one of the most challenging task.
2. External Dependency chains: We have studied about third parties involving in cloud services. Many a times there are more than 3 cloud service providers involved in providing the service (based on the location). This shows that one CSP is having dependencies over other CSPs. A cloud forensic investigation thus requires investigations of each individual link in the dependency chain. Correlation of the activities across CSPs is a major challenge. Lack of coordination between the CSPs involved can lead to problems. Due to the lack of procedures, policies and agreements related to cross-provider forensic investigations it is very difficult for the forensic team to investigate when multiple CSPs are involved.

Legal Dimension

The legal dimension of cloud forensics defines the policies and service level agreements to ensure that forensic activities do not breach laws and regulations in the jurisdictions where the data resides. It should include the policies and procedures that are common and applicable in all the tenants where the data are accessed and stored. This means, the confidentiality of other tenants that share the same infrastructure should be preserved.

SLAs define the terms of use between a CSP and its customers. The following terms regarding forensic investigations should be included in SLAs:

- The services, techniques supported and accesses provided by the CSP to customers during forensic investigations.
- Trusted boundaries, roles and responsibilities between the service providers and customers regarding forensic investigations.
- The process for conducting investigations in multi-jurisdictional environments without violating the applicable laws, regulations, and customer confidentiality and privacy policies.

All of the above points about rules, regulations and service level agreement details are ideal, actually it is not the real scenario in cloud computing and this therefore leads to different legal challenges in cloud forensic investigation.

Challenges: Legal challenges include identifying and addressing issues of jurisdictions for legal access of data; lack of effective channels for international communication and cooperation during an investigation, multi-tenant jurisdiction and missing terms in contracts and service level agreements.

Service Level Agreement (SLA): Transparency in the SLA creates the biggest challenge for the forensic investigators. Due to unawareness in the customers, non- transparency between CSPs and lack of international laws and regulations, SLAs are not prepared properly by the CSP and this creates the loop hole in the investigation process.

Multiple Jurisdiction and Tenancy: Laws and regulation differs from country to country or even part of country and multiple tenancy is the biggest characteristics of cloud computing. Customers can be connected to the cloud server from different locations. The absence of a worldwide regulatory body or even a federation of national bodies significantly affects the cloud forensic investigations.

5. BENEFITS OF CLOUD COMPUTING IN FORENSIC INVESTIGATION

In the previous chapter we have studied the challenges in each dimension of cloud forensics, now we will study the benefits of cloud computing in digital forensics investigation.

Cost Effectiveness

Cloud computing is generally used by small and medium scale industries because it reduces the cost of securing and maintaining the physical servers. Generally, small and medium scale industries cannot afford internal or external forensics team, for them, a low cost cloud forensics services is a boon. Actually, security and forensics services are less expensive when implemented on large scale and so, it is one of the biggest factors that lures IT industries.

Data Abundance

Unlike physical servers sitting in the company premises that stores the original copy of data, cloud servers replicate the data in multiple servers of different zones. There are two advantages of replicating the data objects in different cloud servers: It reduces the risk of data loss due to device failure or device unavailability and it also reduces the risk of losing the vital evidence from the servers.

Overall Robustness

A few technologies are available in the market that help in improving the overall robustness of cloud forensics. For instance, Amazon S3 automatically generates an MD5 hash when an object is stored. IaaS offers on-demand cloning of virtual machines. As a consequence, in the case of a suspected security breach, a customer can make an image of a live virtual

machine for offline forensic analysis, which results in less downtime. Furthermore, using multiple image clones can speed up analysis and in turn speed up investigation tasks. This enhances the analysis of security incidents and increases the probability of tracking attackers and patching security loop holes. Amazon S3, for example, allows user logs access to the bucket and objects within it. The access log contains details about each access request including request type, requester's IP address, requested resource, etc. This is useful information in digital forensic investigation.

Scalability and Flexibility

Scalability and flexibility in terms of resource use is another benefit of cloud computing, which also applies to forensic services. For instance, cloud computing provides unlimited pay-per-use storage by allowing comprehensive logging without affecting performance. Furthermore, it increases the efficiency of indexing, searching and querying log records. Cloud instances can also be scaled as required based on the logging load.

Policies and Standards

Forensic policies and standards play an important role in technological advancements. However, cloud computing is still in the early stage and a unique opportunity exists to lay a foundation for cloud forensic policies and standards to enhance and stay with the technology.

Forensics as a Service

Security as a service is emerging in cloud computing, anti-virus software for cloud and cloud platforms for forensic computing are really helpful. Security vendors are changing their delivery methods to include cloud services by promoting security in cloud service. Thus, cloud computing can become a powerful weapon in the forensic investigation.

6. CONCLUSION AND AREAS OF IMPROVEMENT

Firstly, we have analyzed and found that cloud forensics is a cross-discipline between network forensics and cloud computing. We have studied various aspects of digital forensics in cloud environment in terms of challenges and benefits of cloud computing in forensics investigation. We have also noticed the significant features of cloud computing like multiple locations, low cost services, multi-tenancy, etc. However, these factors make the challenges for the digital forensic investigation.

We have also studied that demand of cloud service is increasing day-by-day. Similarly, the chances of crime can also increase and so, we need better forensic capabilities in terms of procedures, tools and policies. Cloud forensics is an emerging field in cloud computing. Cloud forensics cannot be ignored and so, FaaS (Forensics as a Service) should also be considered with IaaS, PaaS and SaaS. Cloud forensics gives a new direction and scope to digital forensic investigation. Cloud forensic is not confined to cloud crime, it can be useful in other digital forensic investigations as well.

Areas of Improvement: From our entire paper, we found that there are two areas that are lacking in cloud forensics, these are:

1. Acquisition tools: New technology tools need to be designed in order to acquire the desired data easily from the cloud storage.
2. Transparency in Service Level Agreement between CSP to customer and between CSP to CSP (multi-tenancy). This is required to make the investigation easier and it will also help in maintaining a chain of custody.

REFERENCES

Benson, Patrick. "The Cloud Defined, Part 1 of 8: On-Demand Self Service. "*The Cloud Defined, Part 1 of 8: On-Demand Self Service*. 22 Apr. 2013. Web. 30 June 2015. <http://www.pbenson.net/2013/04/the-cloud-defined-part-1-of-8-on-demand-self-service/>.

Birk, Dominik, and Christoph Wegener. "Technical Issues of Forensic Investigations in Cloud Computing Environments." *2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering* (2011). Web. 19 July 2015. <http://www.zurich.ibm.com/~cca/csc2011/submissions/birk.pdf>.

Chen, Guangxuan, Yanhui Du, Panke Qin, and Jin Du. "Suggestions to Digital Forensics in Cloud Computing ERA." *2012 3rd IEEE International Conference on Network Infrastructure and Digital Content* (2012).

Coloumbus, Louis. "Roundup Of Cloud Computing Forecasts And Market Estimates, 2015." *Forbes*. Forbes Magazine, 24 Jan. 2015. Web. 10 July 2015. <http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/>.

Cruz, Xath. "The Basics of Cloud Forensics." *CloudTimes*. 5 Nov. 2012. Web. 26 June 2015. <http://cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics/>.

Daryabar, Farid, Ali Dehghantanha, and Nur Udzir. "A Survey About Impacts of Cloud Computing on Digital Forensics." (2013): 77-94.

Dykstra, Josiah, and Alan T. Sherman. "Design and Implementation of FROST: Digital Forensic Tools for the OpenStack Cloud Computing Platform." *Digital Investigation* (2013). Web. 10 July 2015. <http://www.dfrws.org/2013/proceedings/DFRWS2013-9.pdf>.

Dykstra, Josiah, and Lon Gowen. "NIST Cloud Computing Forensic Science Challenges." (2014). Web. 1 Aug. 2015. <http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf>.

Grispos, George, Tim Storer, and William Bradley Glisson. "Calm Before the Storm." *International Journal of Digital Crime and Forensics* (2014): 28-48.

Herbst, Nikolas, Samuel Kounev, and Ralf Reussner.
"Elasticity in Cloud Computing: What It Is, and What It Is Not." *Elasticity in Cloud Computing: What It Is, and What It Is Not*. 28 June 2013. Web. 26 July 2015. <https://www.usenix.org/conference/icac13/technical-sessions/presentation/herbst>.

Keshavarzi, Amin, Abolfazl T. Haghighat, and Mahdi Bohlouli.
"Research Challenges and Prospective Business Impacts of Cloud Computing: A Survey." *2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)* (2013). Web. 27 July 2015.

Nelson, Bill, Amelia Philips, and Chris Steuart.
Guide to Computer Forensics and Investigation. 5th ed. Vol. 1. 481-510.

Peterson, Gilbert.
Advances in Digital Forensics VIII 8th IFIP WG 11.9 International Conference on Digital Forensics, Pretoria, South Africa, January 3-5, 2012, Revised Selected Papers. 8th ed. Vol. 1. Heidelberg: Springer, 2012. Print.

Ruan, Keyun, Joe Carthy, Tahar Kechadi, and Mark Crosbie.
"Cloud Forensics: An Overview." (2011). Web. 12 July 2015. <http://www.researchgate.net/publication/229021339_Cloud_forensics_An_overview>.

Ruan, Keyun, and Joe Carthy. "Cloud Forensic Maturity Model." (2012).

Srinivas, J., K. Venkata Subba Reddy, and A. Moiz Qyser.
"Cloud Computing Basics." *International Journal of Advanced Research in Computer and Communication Engineering* 1.5 (2012). Web. 2 July 2015. <http://www.ijarcce.com/upload/july/12_CLOUD COMPUTING BASICS.pdf>.

Stavinoha, Ken.
"What Is Cloud Computing and Why Do We Need It?" (2010). Web. 11 July 2015. <http://isacahouston.org/documents/WhatisCloudComputingandWhyDoWeNeedIt.pdf>.

Stuart, Keith, and Charles Arthur.
"PlayStation Network Hack: Why It Took Sony Seven Days to Tell the World." 27 Apr. 2011. Web. 11 July 2015. <http://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony>.

Vael, Marc.
"Cloud Computing Overview." *Cloud Computing Overview*. Web. 13 July 2015. <http://www.isaca.org/Groups/Professional-English/cloud-computing/Pages/Overview.aspx>.

Zargari, Shahrzad, and David Benford.
"Cloud Forensics: Concepts, Issues, and Challenges." *2012 Third International Conference on Emerging Intelligent Data and Web Technologies* (2012).

Zawoad, Shams, and Ragib Hasan.
"Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems." (2013). Web. 1 July 2015. <http://arxiv.org/pdf/1302.6312.pdf>.