CLOUD FORENSICS: AN EXAMINATION OF THE CHALLENGES ASSOCIATED WITH TRADITIONAL COMPUTER FORENSIC TECHNIQUES IN CLOUD COMPUTING ENVIRONMENTS AND CONSIDERATIONS FOR FUTURE CLOUD FORENSIC PROCEDURES

by

Benjamin H. Jordan

A Capstone Project Submitted to the Faculty of

Utica College

July 2013

In Partial Fulfillment of the Requirements for the Degree of
Master of Science in Cybersecurity

Abstract

The introduction of cloud computing has caught on rapidly in the computer technology world. Cloud computing brings cost saving computing power advantages to individuals, businesses, and corporations. The need to own and maintain physical computer hardware is no longer needed with the ability to now virtualize everything from a hard drive to an entire server system. The virtualization of computer hardware takes place in what is known as the cloud. Cloud computing services are provided by third parties such as Amazon, Google and Microsoft. As cloud computing becomes more popular it is likely it will be used in, and for, computer related crimes. Cloud computing has brought new challenges and issues surrounding the forensic acquisition of evidence data in a cloud environment. The computer forensic community has faced challenges with any new introduction of computer technology such as mobile phones. Cloud computing is the next challenge that the computer forensic community must deal with. Cloud forensics is the next advancement in computer forensics that will be needed to investigate crimes committed in cloud environments. This research project examines the challenges that cloud computing has brought to the computer forensic world and ways it can be used in cybercrime. It also examines the new legal issues that have been brought upon the forensic community surrounding cloud-based investigations. Keywords: Cybersecurity, Professor Daniel Draz, cloud forensics, computer forensics, digital forensics, cloud computing, cybercrime.

Acknowledgements

I would like to thank my parents and friends who have pushed me to get through this program. I could have not done it without their support and constant motivation through this entire Cybersecurity program.

I wish to extend special thanks to Professor Daniel Draz of Utica College for taking countless hours of his own time to read and edit this research project to help me achieve itsfinal form.

I would also like to extend thanks out to all of my professors who have shared so much knowledge with me through the Cybersecurity Master's program at Utica College.

Table of Contents

Cloud Forensics: An Examination of the Challenges Associated with Traditional Computer Forensic Techniques in Cloud Computing Environments and Considerations for Future Cloud Forensic Procedures

Introduction

The use of cloud computing services has dramatically increased in recent years for commercial and private use. A recent survey by McKinsey & Company (McKinsey) found that nearly 80% of large companies in North America are using or looking to use cloud services (Griffith, 2013). 71% of Information Technology (IT) managers are expecting cloud computing budgets to grow larger of the next two years (Cruz, 2012). The cloud service market is on its way to generating over $100 billion a year (Griffith, 2013). Google claims that there are over 425 million Gmail users that include government agencies, businesses, and universities (Lardinois, 2012). Those who have a Google Gmail account have access to Google Drive, which is 5 gigabytes (GB) of free storage in the cloud.

Cloud computing has become so popular in the government sector that the United States (U.S.) government‘s spending on cloud-based services will reach $792 million by 2013 (Zawoad&Hasan, 2013). As the use of cloud-based services becomes more prevalent it is likely forensic examiners will soon face cloud-based investigations. Cloud computing companies do not have set processes or procedures for how to investigate or look into cloud issues (Cruz, 2012). The purpose of this research project is to explain the challenges associated with cloud-based investigations in order to understand and carry out cloud-based investigations.

Cloud Computing Basics

The National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of

configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell&Grance, 2011, p.2). Cloud Service Providers (CSPs) offer three major types of cloud computing service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Cloud computing servicemodels. SaaS provides the customer with access to the CSP provider's applications in a cloud infrastructure (Mell&Grance, 2011, p.2). The applications are available to the customer from various devices through an interface such as a web browser or program. Some common examples of SaaS cloud types are Google Drive, SkyDrive, or Dropbox. In this service model there is not a need for software distribution (Zawoad&Hasan, 2013). The customer does not have access to manage, or control, the cloud infrastructure including: network, servers, operating systems or storage (Mell&Grance, 2011, p.2).

PaaS has the capability to allow customers to deploy their own applications in a cloud infrastructure (Mell&Grance, 2011, p.2). The customers cannot manage or control the network, servers, operating systems, or storage (Mell&Grance, 2011, pp. 2-3). However, customers are able to control the deployed applications and configuration settings for the application-hosting environment (Zawoad&Hasan, 2013). In some cases, customers pay for the bandwidth and database usage (Zawoad&Hasan, 2013). Google App Engine, Windows Azure, and Oracle are common types of services for PaaS cloud systems.

IaaS allows the customer to rent processing power and storage to create their own cloud-based virtual machine (VM) environment (Zawoad&Hasan, 2013). VMs can allow customers to run multiple operating systems with various storage and memory settings that can greatly increase computing power from a virtual environment. IaaS allow customers to run their own

software and have the ability to control the software. Businesses may use this platform because it alleviates the need for owning a data center (Zawoad&Hasan, 2013). The advantage to this platform is that customers can scale the platform to their own requirements and computing power needs (Zawoad&Hasan, 2013). The customer does not have access to manage or control the underlying cloud infrastructure (Mell&Grance, 2011, p.3). Amazon EC2 is a popular IaaS platform that allows users to access virtual machines that can be fitted with any type of operating system. Using service such as Amazon EC2 gives customers the ability to run multiple virtual machines at one time for increased computing power.

Cloud computing has opened the doors for further criminal computing (Garfinkel, 2011). The cloud gives people, and criminals, an immense amount of computing power at their fingertips (Garfinkel, 2011). Criminals are now using cloud computing as a tool to carry out new and old crimes. Cloud computing can be used to store explicit material or the immense available computing power can be used to break encryption. Crimes that use cloud computing have emerged in this landscape which has brought new technical and legal challenges to digital forensics (Dykstra & Sherman, 2012).

The growth of cloud technology means that a large portion of investigations now involve data stored in, or actions performed in, a cloud computing environment (Zawoad&Hasan, 2013). Criminals are constantly finding new ways to exploit technology for criminal means and cloud computing has become their latest choice. Investigations involving digital forensics in a cloud environment have become known as *Cloud Forensics* (Zawoad&Hasan, 2013). Cloud computing is changing traditional forensics practices because of the nature of the evidence, lack of access, and the chain of custody (Dykstra & Sherman, 2012). The evidence handling procedures in computer forensics are evolving and are one of the most important aspects (Henry, 2009). Many

of the practices that are currently in place for traditional computer forensics struggle to be applied to cloud computing in the same manner.

Computer Forensics

Computer forensics is the practice of: preserving, collecting, confirming, identifying, analyzing, and presenting computer crime information (Zawoad&Hasan, 2013). Computer forensics has also been termed as "digital forensics" to classify the applied forensic process over digital devices (Saxena, Shrivastava, & Sharma, 2012). Digital evidence is fragile and volatile and requires specific methods to be followed in order to preserve the evidence (Birk& Wegener, 2011). According to NIST (Kent, Chevalier, Grance, & Dang, 2006) the four main phases of performing digital forensics include:

- Collection: acquiring, recording and identifying data from the possible sources while preserving the integrity of data.
- Examination: forensically processing the collected data using automated or manual methods, while preserving the integrity of data.
- Analysis: analyzing the results from the examination using legal methods and techniques to derive hypotheses that address the questions that were the motivation for performing the collection and examination.
- Reporting: reporting the results of the analysis that explain the actions used, tools and procedures selected, determining other areas that should be addressed, and provide recommendations.

The success of the investigation strongly depends on the first phase and if it is not possible to secure the evidence data then no analysis will be possible (Birk& Wegener, 2011). The introduction of cloud computing has caused the first phase to become much more difficult. If the

first phase cannot be successfully completed it may halt the investigation from moving forward. In addition to these four phases the chain of custody procedure is important. The chain of custody clarifies how and where the evidence is stored and who takes it into their possession (Birk& Wegener, 2011).

The phases in place for traditional digital forensic investigations can also be applied to cloud forensics investigations. Computer forensics is constantly balancing the need to obtain the most important data as efficiently as possible without altering any data in the process (Casey, 2010). However, cloud forensics constitutes for new and disruptive challenges for investigations (Birk& Wegener, 2011). There is a new need for investigators to understand how cloud computing systems operate in order to successfully carry out cloud forensic examinations.

Cloud Forensic Challenges

Challenges encountered during acquisition. The acquisition of the digital evidence is the most important of the any of the forensic phases (Zawoad&Hasan, 2013). If any errors occur in the collection phase they will carry on into the analysis and reporting phases, which will affect the entire investigation (Zawoad&Hasan, 2013). It could also affect the whether or not obtained evidence is admissible in court. The processes used during the collection phase must also pass the *Daubert*standard, which is discussed later in this research project. It is important that investigators follow strict acquisition guidelines to reduce the risk of the evidence being thrown out in court. The major drawback of cloud computing is being able to follow conventional data acquisition processes (Reilly, Wren, & Berry, 2011). The acquisition process becomes impractical because evidence is now stored in cloud datacenters (Reilly et al., 2011). The traditional acquisition process is impractical due to the changes of how the forensic evidence is now found and stored in the cloud.

The state of evidence. The digital evidence in the cloud can be found in three different states: at rest, in motion and in execution (Zawoad&Hasan, 2013). Data that is found in disk space is called data at rest (Zawoad&Hasan, 2013). Data is in motion when data is transferred from one entity to another, such as a file transfer over a network (Birk& Wegener, 2011). However acquiring the data in different states during the evidence data collection is more difficult in cloud environments than traditional computer forensics (Zawoad&Hasan, 2013). Data that can be loaded and executed as a process that is neither at rest nor in motion is said to be in execution (Birk& Wegener, 2011). For example, investigators may be able to acquire the executable data, an image snapshot. The snapshot of a cloud based VM can hold important information about the data that was being accessed on a VM when the snapshot was created. The snapshot of the VM is comparable to a hard drive image that could be loaded and run to obtain the data at rest and data in motion (Zawoad&Hasan, 2013). The forensic evidence is not only stored in different digital states, but can be spread out among different sections of the cloud.

Location of data. The storage of evidence data may no longer be found locally on a computer when a cloud service is used. Physical inaccessibility of digital evidence makes the collection harder than traditional forensics (Zawoad&Hasan, 2013). A forensically sound bit for bit method of data collection may not be applicable in a cloud computing environment (Slusky, Partow-Navid, &Doshi, 2012). A bit for bit collection may not be possible since the data is no longer stored on a local machine. The data in the cloud may be scattered which would not allow for a bit for bit collection of the evidence. A bit for bit collection can still be used, but it may only contain pieces of the entire forensic data. This is because the data may be stored in various locations of a cloud environment. Knowing where the data is, and actually acquiring the data,

can be much harder in a cloud environment (Reilly et al., 2011). Investigators may beunfamiliar with the cloud infrastructure to know where data could reside.

The IaaS, SaaS, and PaaS cloud models each have different locations and ways that data can be stored. In some cases it may be impossible for data collection from SaaS or PaaS cloud services (Zawoad&Hasan, 2013). The user may have stored the data on various cloud based virtual machines (VM's). If the VM's were not in use at the time of the collection the investigator may even overlook potential evidence.

Virtualized data could be spread out between many different physical devices (Grispos, Glisson, &Storer, 2011). Unlike data stored in local machines, data stored in cloud datacenters could be spread across thousands of VM's and servers (Reilly et al., 2011). The data may not reside permanently in one cloud virtual machine or physical location (Slusky et al., 2012). For example, Google uses the Google File System (GFS) to store data in the cloud (Grispos et al., 2011). It will appear to the customer that the data is stored in one location; however the GFS may store data in two or more physical locations (Grispos et al., 2011). Data for customers can be co-located and investigators must be able to prove that data did not co-mingle with other users' data making the acquisition more challenging (Zawoad&Hasan, 2013). This also plays an important part in the chain of custody and may cause investigators to not know whether or not data had been altered.

The lack of knowledge of knowing where exactly the data is stored means it could be difficult to piece together the sequence of events and establish a timeline (Reilly et al., 2011). The use of a timeline is often used by investigators to create timeframe of when and where a crime took place. Acquiring all of the storage devices from a cloud environment can be time consuming for the investigator and may disrupt the service offered by the provider (Grispos et

al., 2011). This is because cloud environments are so large and it allows for data to be spread out among various locations. It is important to collect all of the necessary evidence, but it may be a slow process to actually track down all of the forensic data in a cloud environment. For example a typical investigation may only include a computer and an external hard drive or device. The introduction of the cloud means that the data is can now be stored between dozens of virtual machines or on servers at multiple datacenters. Virtualization of data in the cloud makes it complex to identify and isolate all of the portions of the storage locations (Grispos et al., 2011). Once investigators are able to locate the data they face further challenges due to the cloud's capabilities.

Amount of data. Cloud services are attractive also because of the elastic ability to dynamically adjust the storage capabilities to real time requirements (Grispos et al., 2011). A typical IaaS cloud service could offer limitless data storage capabilities and when the user requires it (Grispos et al., 2011). If a customer was storing a few gigabytes of data in the cloud, but needed more storage space it would be very easy to obtain the additional space in the cloud. A single cloud environment could contain as much as 128 terabytes (TB) of storage using 46TBs of memory, spread among 1000 users and 512 servers (Reilly et al., 2011). It would be impractical for an acquisition of the entire 128TB of data and very time consuming.

An investigator may have to gather an extremely large amount of data that was placed in the cloud (Grispos et al., 2011). An investigator may also not have the capabilities to store such large amounts of data so that it can be analyzed for any potential evidence. If they cannot store all of the data, it leaves the risk of forensic data not being analyzed. The task of gathering such large amounts of data from a cloud environment compared to a typical computer poses an additional challenge for investigators.

Volatility of data. While acquiring the data, examiners must keep in mind that certain data that exists is more volatile than others. Taking a system offline to acquire data from a hard drive has a serious effect on the bottom line (Carvey, 2009). In this day and age, it may be impossible for an individual user, business or corporation to shut down their computer systems to be analyzed. Investigators may face some cases where the evidence should be collected before the system is shut down, acquiring a bit-stream image of the hard drive(s) (Carvey, 2009). This would require investigators to carry out a live forensic examination which needs to be handled differently than a "dead" forensic examination. A dead forensic situation would be when the computer has been turned off and data is collected and analyzed at a different location. There may be times when a cloud-based environment cannot be shut down and it must be handled as a live forensic examination. It could also involve multiple VM's that are running numerous applications from the cloud.

Portions of the information on a running computer are volatile, which means it will cease to exist once the power is removed (Carvey, 2009). The most volatile data typically resides in the physically memory, or random access memory (RAM) (Carvey, 2009). Data found in the memory can often give investigators a good idea of what was being done on the computer. For instance, the RAM can hold data about what processes were being run on the computer at the time of the collection. It could reveal that in the background there was a process running that was connected to a cloud service.

In the case of a cloud virtual machine, once the VM is turned off all of the volatile data will be lost before an image can be made (Zawoad&Hasan, 2013). If a virtual machine is restarted in an IaaS environment the volatile data will be lost. Unlike SaaS and PaaS cloud systems, IaaS cloud systems do not have persistent storage (Birk& Wegener, 2011). Registry

entries, or temporary Internet files, stored within a virtual cloud environment will be lost when the user exits the system (Zawoad&Hasan, 2013). The volatility of data in the cloud must be taken into consideration, if not it could mean the difference between obtaining or losing valuable information.

Encrypted data. Investigators often face computers and other devices that have been loaded with encryption software or encrypted data to hinder investigators from accessing data. During the collection of the forensic data investigators may encounter data that has been encrypted in the cloud. Even if the evidence were able to be collected it may not be able to be accessed due to the encryption in place. The CSP may encrypt the data in the cloud for the customers or customers may move their data into the cloud that has already been encrypted. It is not rare that data is encrypted before it is transmitted through the Internet.

Many CSPs are turning to encrypting their customers' data to ensure data integrity and confidentiality (Grispos et al., 2011). The keys that are used to encrypt the data are not stored in the cloud. If the investigator were able to obtain a court order to decrypt data could prove useless if the owner of the data cannot provide the key to decrypt it (Grispos et al., 2011). The investigator may have to obtain another court order that instructs the CSP to make the key available, which could take more time and face further obstacles.

Preservation of Data

Chain of custody. Once volatile data, or a bit stream image, is acquired it must be handled with care to ensure that the evidence is not lost or tampered with. Traditional forensic investigations maintain a strict chain of custody that shows how the evidence was collected, analyzed, and preserved in order to be presented as evidence in court (Grispos et al., 2011). A chain of custody provides a documented history of the entire lifetime of the evidence discovered

(Grispos et al., 2011). Documentation also includes how, when and by whom the evidence were gathered and managed by (Grispos et al., 2011). In a typical forensic procedure it begins with gaining control of the evidence such as a computer or hard drive. If the possession of the evidence it exchanged from one person to another it is documented. This ensures that the data was handled properly and securely. The evidence can then be moved to be isolated and analyzed separately (Grispos et al., 2011). However the remote nature of the cloud services means that the chain of custody may not be valid (Grispos et al., 2011).If the data is collected by the cloud provider it is likely the person is not a licensed forensic examiner (Zawoad&Hasan, 2013).

In a cloud environment multiple people may have access to the evidence and may rely on the cloud service to provide the evidence (Zawoad&Hasan, 2013). An employee may hand the data off to someone else and it may not be documented to ensure a proper chain of custody. A CSP employee could very well be unaware that a strict chain of custody needs to be followed. It also means that the chain of custody is not initially controlled by an investigator (Grispos et al., 2011). This would not guarantee theintegrity of the evidence in the event the case went to court (Zawoad&Hasan, 2013). The dependence of having used a third party to acquire the evidence poses an issue to the investigation process (Zawoad&Hasan, 2013).

Since evidence in the cloud may be located in many different locations under various controls, this makes the chain of custody difficult to preserve (Birk& Wegener, 2011). There may be various datacenters involved that need to collect data and present the evidence. The evidence could be handed off multiple times at each data center which makes the chain of custody much more complex. Cloud computing presents a new challenge to the chain of custody procedures and to what extent an investigator can control the data collection.

Control over data. In traditional computer forensic cases the investigators have full control over the devices such as the computer or the hard drive. In a cloud investigation the control over the data varies depending on the cloud service model (Zawoad&Hasan, 2013). Investigators may need to rely on the cloud service provider to collect the digital evidence (Zawoad&Hasan, 2013).

The time that it takes for the investigator to obtain control may cause for evidence to be destroyed (deliberately or accidentally) by the user or service provider (Poisel, Malzer, &Tjoa, 2013). In some cases, the files may need to be downloaded from the cloud. During the download process there is a risk of losing information about the file. The investigator may not be able to ensure that data is not lost during the download process. The investigators hands can be tied in controlling how the download process could affect the data. Metadata can be lost when data is downloaded from the cloud (Reilly et al., 2011). Metadata provides information about a file's creation, modified, and accessed times.

There is a general loss of control over the forensic examination because the data is stored elsewhere and is inaccessible (Reilly et al., 2011). This is unlike typical investigations where an investigator has in their possession a computer that holds the actual evidence. If the investigators do not have direct control of the cloud space, files could be deleted by the customer or service provider (Birk, 2011). File deletion is about control and has become more of an issue with the introduction of cloud computing (Birk, 2011). A user may be able to access the cloud through the Internet from another location or computer. Cloud computing gives the user the ability to access their data in the cloud just as long as they have an Internet connection. The user is not tied to using a specific computer to access their data stored in the cloud. Investigators may have one computer in their control, but the user could still access the data in the cloud from another

computer with an Internet connection. If the CSP does not block the user from accessing their cloud space it could allow the user to delete valuable data. A customer could also cancel the contract with the CSP causing the evidence to be destroyed (Birk, 2011).If investigators are unable to gain control over a cloud environment it can lead to loss of important artifacts (Reilly et al., 2011).

Validation of Data

Using hash values to validate evidence. When evidence is acquired by the examiner or investigator software hashing tools are commonly used to validate the integrity of the evidence (Grispos et al., 2011). A hash function is an algorithm that converts arbitrary length data strings into fixed "hash values" (Grispos et al., 2011). Hash values can be assigned to disk images, files or other data to ensure that the evidence has not been altered before and after the analysis (Grispos et al., 2011). MD5 and Sha-1 are common types of hash values implemented during forensic analysis.

The data that is stored in the cloud may be subject to hashing for integrity purposes. For example, the Amazon S3 cloud services uses MD5 hashing checksums for data stored using their services (Grispos et al., 2011). The use of hashing by the CSP is a helpful feature for investigators, but does create some challenges. Since the CSP uses their own hashing tools and they are controlled by the CSP, the investigator cannot test or evaluate the hashing features compared to their own forensic hashing tools (Grispos et al., 2011).

Typically an investigator uses a certain set of tools to validate the hash values of evidence and any difference in hash values can be investigated (Grispos et al., 2011). For instance, the investigator may download a copy of the evidence obtained from the cloud. The CSP may have already assigned the data with a MD5 hash value. If the investigator downloads a copy of the

evidence and the MD5 hash values are not the same it may indicate that the data was altered or lost.

When the CSP assigns the hash values to data the investigator may be limited as to what can be investigated when hash values do not match (Grispos et al., 2011). The investigator does not know if the hashing tools that the CSP uses are correct or if and what data was lost. A CSP may not even use hashing tools which would not allow the investigator to have an original hash value to match the collected data to. Not only does the validity of the evidence pose issues for the investigator, but may be the difference of whether or not the data is admissible in court.

As examiners and investigators continue to face challenges with the forensic procedures due to the introduction of cloud computing, it is likely they will face new legal issues. Cloud forensics presents new unique issues to the legal environment surrounding the cloud (Orton, Alva, & Endicott-Popovsky, 2013). The growth of the cloud has caused law enforcement and the judicial system to be unprepared for cloud based crimes (Dykstra, 2013). In order for forensic data to be collected from the cloud and the investigation to begin there may be a series of legal challenges the investigator may face.

Legal Limitations

Jurisdictional boundaries. Cloud computing companies use massive datacenters that can be spread out across the country and across international boundaries. A user's data may not reside in just one datacenter, but could have pieces of their data stored at different locations.There may be the assumption that laws protecting the data are based on where the data physically exists (Dykstra, 2013).However, there are no case laws or legal precedents that support this assumption (Dykstra, 2013). For instance, the cloud service datacenters could be located in: California, New York, Texas, or India. The laws and statutes in place to be able to

acquire the data from the datacenters could vary from state or country. In some states or countries it may be easier to gain access to the data while in others it may be very difficult. An investigator may

have a warrant that allows the investigator to search and seize evidence, but it may not carry the same power once it crosses into a different jurisdiction.

Requests to search and seize data in other jurisdictions could take time leaving time for the evidence to be lost or destroyed (Grispos et al., 2011). For example, states and countries could have varying legal processes in place that can complicate the collection of the evidence in the cloud. Data moving between different locations could also mean data is encrypted in one jurisdiction, but not another. A jurisdiction may legally require the data to be encrypted, which could make it much more difficult to collect the data. Investigators must know how the laws to acquire data vary from one jurisdiction to another. The user may not even be aware that their data stored in another jurisdiction is encrypted to meet legal requirements (Hay, Nance, Bishop, 2011).

If the investigator is unaware of differences in laws it may be difficult or impossible to obtain the evidence. The significant issue is whose substantive law applies when cases and evidence are located in different jurisdictions (Orton et al., 2013). The multi-jurisdictional situations will remain as one of the legal issues for cloud forensics and digital forensics in general.

Service level agreements (SLAs).SLA's are the contract between the customer and the CSP which are based on terms created by the CSP. The terms of an SLA can dictate how forensic investigations are handled (Orton et al., 2013). It may not be mentioned in an SLA the types of tools and techniques that could be used if a forensic investigation needed to be carried

out. From an investigative standpoint, the SLA will determine the availability of data from the customer that can be collected during an investigation (Orton et al., 2013).

An SLA could potentially restrict an investigator from collecting specific forensic data that could show how a crime was carried out or if the user was using the cloud for malicious purposes. If an SLA does not specify the type of process or forensic data that will be provided for the customer, then the CSP has no duty to provide such information (Orton et al., 2013). This does two things: it binds the access for forensic data that may not be otherwise available and lowers the quality of the best evidence available (Orton et al., 2013).

It is important that investigators have access to all of the relevant forensic data and by not having the best evidence it hinders the investigation process. The SLA may also have terms and conditions on how forensic data is stored once it is collected. This could allow investigators to have an easier or harder time to acquire the forensic data. If the data were stored in one location this could be a major benefit for investigators. Instead of searching for the data they would be able to find it at a central location. However the SLAs will vary by CSP and there are no laws currently in place that bind CSPs to store any forensic data in specific locations.

The *Daubert* standard. The procedures that are followed during a forensic examination of the cloud will be subject to the *Daubert* standard. The Daubertstandard determines whether a theory or technique has been tested, whether it has been peer reviewed, acknowledges the known error rate, and whether the theory or technique has been accepted within the relevant scientific community (Dysktra&Riehl, 2012). Since cloud forensics is a new area it may be difficult to establish all of these factors. The techniques on how data is collected during a cloud investigation have not come to a consensus among the forensic community. The empirical testing

of cloud forensic methods are challenging due to the evolving nature of cloud technology (Grispos et al., 2011). Existing forensic tools used in traditional forensic cases have set standards, but it is unclear how they can be applied to cloud forensics.

EnCase is a popular forensic tool that has been tested and accepted in court for traditional forensics and has been used over a long term. Tools like Encase may be accepted by courts for traditional forensics, but there is little consensus by the forensic community about how this tool can be used in cloud forensics (Dysktra, 2013). The lack of consensus about the forensic tools and techniques used during cloud forensics poses a major issue of whether or not they can pass the Daubert standard. If cloud forensic techniques and tools cannot pass the Daubert standard then investigators will struggle to see their cases being admissible in court.

Minimal research has been directed towards dealing with cloud based forensic investigations. Very little research has been completed to developed theories and practices of cloud forensics (Zawoad&Hasan, 2013). This is because cloud computing is such a new type of technology and the forensic community has not had adequate time to address the issues. The ability to perform cloud based digital investigations is a highly relevant issue that is seldom discussed (Birk, 2011).

As Birk (2011) states: the field of digital forensics must be revised and adapted to meet new cloud environments. Forensic investigators have not implemented and put forward procedures for deal with cloud investigations (Reilly et al., 2011). Cloud forensics is not only an issue for forensic investigators, but cloud providers have not addressed how they will implement cloud forensic procedures (Reilly et al., 2011). Cloud computing presents a new branch to traditional forensics practices and through further research can better understand how to handle cloud forensic investigations.

This research project explores the challenges and issues that the computer forensic community now faces with the introduction of cloud computing. The forensic community has faced other challenges with the introduction of new computer technology. The challenges have been met and overcome to produce new forensic practices. Forensic examiners and investigators may have not had time to fully understand how cloud computing works and could be unaware of the challenges. The forensic examiners and investigators who are unfamiliar with cloud computing could benefit from information found in this research project.

Overview

The growth of cloud computing will continue to increase and is expected to grow for commercial and private use. As the cloud computing environments become more popular it is likely they will become involved in crimes and investigations. Criminals have already begun to use the cloud for malicious purposes. As cyber-crime continues to grow there will be a growing demand for cloud forensics. The current forensic processes and guidelines are being challenged by cloud computing. Investigators will find that traditional forensic methods may be limited to how effective they are when encountering a cloud based investigations. The forensic methods of collection, preservation, and analysis are now being changed to adhere to the evolving cloud computing technology. There are new legal issues that have now become present regarding the authenticity of data and ability to collect evidence in different jurisdictions. As more cloud computing becomes more popular new techniques, procedures and laws will need to be developed to handle cloud investigations. Future research should continue to understand the computer forensic and legal challenges that have been brought upon by cloud computing to provide continued guidance for approaching cloud forensics.

Literature Review

Cloud computing is quickly becoming a major utility just like water, gas, electricity, and telecommunications (Reilly et al., 2011). Organizations that are looking to reduce their IT costs are offloading infrastructure and software costs onto a third party (Jarabek, 2011). Cloud computing is an evolution and combination of computer technology that has resulted in on-demand, elastic and location independent computing services (Dykstra & Sherman, 2012). The term "cloud computing" has recently become much more of a commercial term. Cloud computing offers a cost effective solution for individuals and corporations to expand their computing needs. Cloud computing is not new technology, but a new way of providing computing resources and applications (Zimmerman &Glavach, 2011). A web search on the Internet for cloud computing services will result in many different options available. For instance, Google offers Google Apps which is a software-as-a-service (SaaS) and Google App Engine which is a PaaS. Amazon offers their EC2 service which is an IaaS platform. SaaS, PaaS, and IaaS cloud platforms are the three main types of cloud service deployments.

History of Cloud Computing

Cloud computing is simply the rental of computer space from another company's data center (Lillard, Garrison, Schiller, & Steele, 2010). The origins of cloud computing can be traced back to the mid-1990s with the commercialization of the Internet and the development of web applications like Salesforce.com (Lillard et al., 2010). Salesforce.com was the first practical cloud computing resource that delivered services through a website (Harauz, Kaufman, & Potter, 2009). Those using email at the time may not have realized it, but email companies were actually using cloud computing technology. The email services were using cloud computing concepts to store customers' data in the cloud. Faster Internet speeds and acceptance by companies to allow their data in the hands of cloud vendors drove the development of the cloud (Lillard et al., 2010).

However, the dot com crash slowed cloud computing development and only left the strongest cloud vendors to survive (Lillard et al., 2010). Soon companies such as: Google, Apple, Dropbox, Microsoft, and Amazon began to appear with web based cloud computing solutions. The low cost of on demand servers in combination with web based applications has driven cloud computing. Cloud users can now build their own massive virtual servers and all that is required is a valid credit card.

Cloud deployment models. The level of control and security needed by a customer may determine whether a public of private cloud is utilized. Larger companies and government agencies are likely to use the cloud by using a private cloud (Lillard et al., 2010). A private cloud has the features of a public cloud, but is hosted inside of a private firewall. It is usually an internal data center and located on premise (Zawoad&Hasan, 2013). Private clouds are able to maintain full control of who has access while still benefiting from the use of a cloud platform (Lillard et al., 2010). A public cloud would be the use of an external service such as Amazon, Dropbox or Google. The CSP owns the infrastructure and makes it available by selling their service to customers. The customer pays for the service and in return is given access to a cloud computing platform. There are also hybrid cloud services, which are a combination of both, that relies on a private cloud, but uses a public cloud service to accommodate usage (Gohring, 2011). It may require both on and off premise cloud infrastructure resources.

Cloud service characteristics. SaaS, PaaS, and IaaS have varying types of characteristics that define each type of cloud service. Customers are able to control different parts of the cloud structure based on if they choose a SaaS, PaaS or Iaas cloud service model. Unlike owning their own data center a company who chooses a cloud computing service will not have total control over the computing system (Lillard et al., 2010). Customers can choose the type of cloud service

they need based on the characteristics offered by the three cloud service types. The SaaS model provides customers the means to use the CSP's software application in the cloud. According to Kepes (2011), SaaS cloud service models are based on some of the following characteristics:

- Web access to commercial software
- Software is managed from a central location
- Users do not have to update software and patches
- Application Programming Interfaces (APIs) allow for integration between different types of software.

In PaaS, customers can deploy their own application and do not manage or control the underlying cloud infrastructure. PaaS brings the benefits offered by SaaS for applications and is a platform that allows for the creation of web applications quickly. Further, Kepes (2011) states some additional characteristics of PaaS cloud platforms include:

- Services to develop, test, deploy, host and maintain applications in a development environment
- Web based user interface used to create tools used to test, modify, and deploy applications
- Offers scalability of deployed software including load balancing
- Support for development team collaboration

The IaaS cloud service platform offers customers the ability to rent processing power and to use VMs through virtualization. Customers can build the infrastructure to their computing needs and can scale up their infrastructure at any time. Kepes (2011) outlines the common characteristics of the IaaS model, which are:

- Resources are distributed as a service

- Infrastructure allows for dynamic scaling
- Includes multiple users on a single piece of hardware
- Used by organizations without capital to invest in hardware or when rapid growth requires needed scaling of hardware

IaaS cloud services are reliant on virtualization technology, which is seen as providing security and isolation for the customer (Jarabek, 2013). Virtualization of IaaS cloud platforms does provide some potential security and security flaws, but also could benefit digital forensics procedures.

Virtualization. Virtualization is a broad term that refers to the abstraction of computing resources (Reilly et al., 2011). Virtualization takes a physical resource and brings it to a virtualized resource that can be shared. Within a cloud servers, storage, software, platform, infrastructure can all become virtualized (Reilly et al., 2011). Virtualization is the foundation of the IaaS cloud platforms (Jarabek, 2013). Server virtualization is the most popular and is provided by companies such as VMware or Citrix XenServer (Reilly et al., 2011). Using server virtualization a single physical machine can be divided into various VMs. The core of virtualization is the concept of a hypervisor or a virtual machine monitor (VMM) (Reilly et al., 2011). The hypervisor is a software layer that connects the operating system calls to the hardware. Hypervisors typically have a virtualized central processing unit (CPU) and memory facility (Reilly et al., 2011). The hypervisor is creates and runs the VMs connected to the physical host machine.

Virtualization does bring some security concerns due to the: scaling, diversity, transience, software lifecycle, data lifetime, mobility and identity (Jarabek, 2011). Scaling and diversity are a concern because of the ease in which VMs can be created. The ease of creating VMs can lead

to an explosive amount of different VMs within an organization (Jarabek, 2011). VMs can appear and disappear on an organization's network or become dormant for an extended period (Jerebak, 2011). This creates two problems: patch management and the length of time it may take to patch a dormant VM (Jarabek, 2011). Dormant VMs could be infected with worms or viruses and when a dormant VM re-emerges it could cause outbreaks of malware (Jarabek, 2010).

VM machines have the ability to roll back to an earlier state, but it risks un-patching a previous security flaw. The mobility of VMs can become an issue because if the physical machine controlling the VMs is compromised it leaves the risk for the VMs to become compromised too (Jarabek, 2011). If a customer had a physical machine that was controlling tens to hundreds of VMs this could be a major security concern. A physical machine compromised with malware could cause VMs to malfunction leading to a loss of business activity for the customer.

There may be security concerns with IaaS platforms and virtualization, but VMs can provide useful forensic advantages. For example, using VMware, allows for the user to create a "snapshot" of the VM. A snapshot is a "picture" of the VM machine that provides the image of the computer's hard drive, VMware configuration, and basic input/output system (BIOS) configuration (Jarabek, 2011). Virtualization has created security concerns, but cloud computing has created an entirely new type of tool to be used for criminal means.

Cloud computing security concerns. Cloud computing continues to grow in popularity, but security concerns surrounding the cloud are prevalent. The threat to the confidentiality, integrity, and authenticity of data remains as high concerns for cloud users. Data breaches are a threat to cloud computing and a single security flaw could allow attackers to access large

amounts of data (Samson, 2013). Privacy remains as a top security concern in cloud computing. Regulations regarding personal information vary across the world and data can be stored in different countries (Kulkarni, Gambhir, &Dongare, 2012). It can be difficult to verify the privacy regulations in other countries (Kulkarni et al., 2012). The next security concerns in cloud computing environments are data loss and leakage. A customer could encrypt their data in the cloud, but if they lose the encryption key they could lose their data (Samson, 2013). Data may not even be encrypted which could lead to data leakage. In cloud environments most data is not encrypted at the time of processing (Kulkarni et al., 2012).

Data in the cloud could also be lost if an attacker gained access into the cloud and deleted it or a careless CSP mishandled or lost the data (Samson, 2013). The risk of an attacker being able to obtain the users credentials remains as a security threat (Samson, 2013). If the attacker had a user's credentials they could manipulate data, falsify information or redirect where data is being sent (Samson, 2013).

Securing data storage remains another important security concern. It involves the way that data can be secured using encryption and managing encryption keys of data being transferred in the cloud (Kulkarni et al., 2012). The data at rest in a cloud can be secured by the CSP using cryptographic encryption methods (Kulkarni et al., 2012). Data in the cloud may only be as secure as the networks and servers that control the cloud environment. Virtual servers and applications need be secured much like their non-virtual counterparts (Kulkarni et al., 2012). Virtual firewalls can be used to isolate VMs from other hosts or other cloud resident systems (Kulkarni et al., 2012).

As the demand for cloud computing services increase, it is without a doubt that cloud computing security will become a larger issue. Cybercrime is continuing to become more

prevalent and often offers cyber criminals with high rewards with a low risk of being punishment (Gohring, 2011). The Internet has allowed people to become anonymous and carry out old crimes with new tools. Cyber criminals are now finding that cloud computing can be used for malicious purposes. They are also detecting security loopholes in cloud computing infrastructures just as they have exploited other computer technology loopholes. Those who are tasked with investigating cybercrimes face an uphill battle and the introduction of cloud computing is certainly not making it any easier. Investigators and examiners must take the time to understand how cloud computing services operate in order to carry out successful cloud-based digital forensic examinations.

Cybercrime

Cybercrime is continuing to evolve each day and cyber criminals continue to find new security holes to exploit. As technology becomes more computer-based it will offer even more potential targets for cyber criminals. The introduction of cloud computing has certainly given cyber criminals another target. There appears to be no sign that cybercrime is going to slow down in the near future, but in fact it continues to increase. Cybercrime is becoming a multi-billion dollar business. For example, in 2011 Russian cybercriminals earned over $4.5 billion (Essers, 2012). Cybercrime is becoming even more organized with cyber criminals sharing data with one another on the Internet. A report by the Internet AV companyMcAfee predicts that in 2013 cybercriminals and hacktivists will continue to evolve and strengthen the techniques and tools to assault bank, mobile devices, businesses, and homes (Chen et al., 2013).

Origins of cybercrime. The origins of cybercrime can be traced back to the introduction of the first mainframe computers. It has been recorded that the first instances of computers being used to commit crimes appeared in the 1960s (Brenner, 2010). Mainframe computers did not

develop until after World War Two (WWII) and were first used by government, more specifically the U.S. Census Bureau (Brenner, 2010). As mainframe computers became more popular early signs of computer crime began to appear. At this time the Internet did not exist and computers were not networked on a global scale. There were only select "insiders"-people who had access to the mainframe computers (Brenner, 2010). These insiders would spy on other employees, sabotage mainframes or data, but the most common motivator was financial gain (Brenner, 2010).

By the mid1960's embezzlement and fraud were the most common types of computer crimes taking place (Brenner, 2013). Once the Internet and personal computer (PC) were introduced in the late 1980s cybercrime began to transform even further (Brenner, 2013). Soon hacking and malware were beginning to appear in the computer community. By the end of the 1990's, U.S. Attorney General Janet Reno (Reno) called for a multilateral "crackdown on cybercrime" (Brenner, 2010). Cybercriminals continued progress from the late 1990's which has brought cybercrime to its current state.

Current cybercrime and cyber-attacks. The introduction of mainframe computers and early hacking practices at Massachusetts Institute of Technology (MIT) laid the foundation for the current state of cybercrime. Global losses from phishing attacks alone in 2012 were estimated at $1.5 billion with a 59% increase from 2011 (RSA, 2013). A report produced by Symantec suggested that the estimated cost of cybercrime in 2012 was up to $110 billion (Filshtinskiy, 2013).

Cybercrime and cyber-attacks have reached all parts of the world that have an Internet connection. Malware, botnets, child pornography, phishing schemes, denial of service (DOS), distributed denial of service (DDoS) attacks, and other various cyber-attacks now litter the

Internet. A botnet is a network of maliciously compromised computers that can be controlled by a single or multiple command-control location (Lillard et al., 2010). The U.S. infrastructure ranging from government agencies, power grids or the financial system have all become victims and targets of cyber-attacks.

Cybercriminals are not the only ones using computers to their advantage, but now state-sponsored cyber-attacks are numerous. A visible sign of state-sponsored cyber-attacks came to view when the Stuxnet malware was discovered in 2010 on a computer in an Iranian nuclear enrichment facility (Finkle, 2013). The creation of the Stuxnet is believed to be developed the U.S. and Israel (Finkle, 2013). Stuxnet had the capability of causing the centrifuges at the nuclear plant to spin out of control causing them to become unusable.

In Romania, a remote town called RamnicuCalcea, has become a cybercrime hotspot. The town has been filled with cybercriminals ranging from hackers to low level scammers (Bhattacharjee, 2011). It has been named "Hackerville" by law enforcement officials around the globe (Bhattacharjee, 2011). The cybercrimes committed by criminals in this area have brought tens of millions of dollars into the area (Bhattacharjee, 2011). The main business of this town is cybercrime and business is booming (Bhattacharjee, 2011).

Cybercriminals are quick to adapt to new computer technology and to use it for malicious activities. Those who work to fight against cybercrime and cyber-attacks face a slow and grueling uphill battle. As soon as one security loophole or vulnerability is fixed another is found by cybercriminals. The advancements in computer technology and new cybercrime techniques have brought crime to the cloud. Criminals have already found ways that the cloud can be used for malicious purposes and are finding security vulnerabilities.

Cloud Computing as a Tool in Cybercrime

Using cloud computing to break encryption and passwords. As new computer technology is produced criminals are constantly looking to find ways to exploit it for security vulnerabilities or to use it as a tool. Cloud computer has become a resource for cybercriminals because it is cheap and can offer unlimited amounts of computing power. Unlike malware or other malicious tools, cloud computing offers a well-managed, reliable and scalable infrastructure (Garfinkel. 2011).

The additional computing power that is offered by cloud services has allowed criminals to crack encryption algorithms much faster. Thomas Roth (Roth), a German IT security researcher was able to crack a six character implementation of the SHA-1 crypto algorithm (Higgins, 2011). In order to break the encryption he used Amazon's EC2 cloud service that runs by graphics processing units (GPU) (Higgins, 2011). The GPU units consisted of eight Amazon Nvidia GPU instances that were able to crack 400,000 passwords per second (Higgins, 2010). That means that between the eight GPUs, a single GPU could crack up to 50,000 passwords per second. GPUs offer more computing power than the common central processing unit (CPU) found in PC's. In contrast, an Intel Quad-Core CPU has the capability of cracking about 7,000 passwords per second (Higgins, 2011).

Many of the current security protocols were designed when password crackers might only have access to a few computers (Garfinkel, 2011). Encrypted passwords that may have used to take 30 years to crack can now be done in a much faster (Garfinkel, 2011). The cost of a GPU instance is estimated to be around $2.10 an hour (Higgins, 2011). Roth estimated that the Amazon machines he used to crack the encryption keys cost him around $1.68 (Garfinkel, 2011). The low cost of having massive amounts of computing power available through cloud services is

very attractive to cybercriminals. Since the costs of renting cloud computing are relatively cheap a hacker could rent hundreds of GPUs or CPUs from Amazon at once.

When hackers broke into Sony's Playstation game network in April 2010, it was reported that they used Amazon's EC2 service to break some of the encryption (Garfinkel, 2011). The breach of the Sony Playstation network gave attackers' access to thousands of Playstation's customers' credit card information.

Cloud password cracking service. There are cloud based services that have been created for cheap password cracking. CloudCracker is a web based cloud service that allows people to pay $17 to have access to the password cracking service (Greenberg, 2012). CloudCracker has the ability to break standard WPA-PSK wireless network password using dictionaries of possible passwords (Greenberg, 2012). For users trying to break obscure passwords, they are able to purchase an upgraded service for $136.CloudCracker uses a collection of 400 CPUs and 70 GPUs that distributes the password cracking tasks (Greenberg, 2012). CloudCracker is a service that is meant to be used by penetration testers and not for malicious purposes.However, it cannot be guaranteed that it will not be used for malicious purposes. A hacker could easily pay for the CloudCracker service using a stolen credit card and would appear to be a legitimate user.

Exploitation of cloud-based web browser. Computer scientists at North Carolina State University and the University of Oregon were able to produce a new browser-based exploit that allows for large scale computations using cloud services for free (Goodin, 2012). The hack of the browser could potentially be used to wage powerful online attacks cheaply and anonymously (Goodin, 2012). The proof-of-concept attack was based on Puffin, a cloud based web browser. Puffin and other cloud based browsers are typically used only to accelerate the loading of web pages using JavaScript that are used on mobile devices (Goodin, 2012). It is more efficient than

using the limited and low computing power of mobile devices (Goodin, 2012). In this type of attack a customized browser could be used to mimic a cloud based browser such as Puffin (Goodin, 2012). This means that attackers trick the cloud based servers by appearing as Puffin, but instead use the cloud servers for other means.

The exploit allows for computationally intensive tasks to be pushed onto the cloud based browser (Goodin, 2012). The hack works by breaking up jobs into large numbers of smaller jobs and pointing them to multiple instances of the custom mimicked browser (Goodin, 2012). Attackers could use this technique to carry out DoS attacks or for password cracking. This type of technique could be used to generate more than 24,000 cryptographic hashes per second (Goodin, 2012). This type of attack has the potential to abuse cloud infrastructures such as Amazon's Silk browser, Cloud Browser from AlwaysOn Technologies, and Opera Mini (Goodin, 2012).

Cloud based cyber-attacks. Using cloud computing to crack passwords has not been the only use of the cloud for malicious purposes. Cybercriminals are using cloud services to create and launch cyber-attacks by using cloud computing resources. Attackers have found that they can compromise VMs to use them as VM botnets (Pacella, 2011). The attackers can rent large numbers of VMs across multiple cloud instances to create massive botnets (Pacella, 2011). For example, an attacker could purchase cloud space from Amazon's EC2 cloud using stolen credit cards. Once they have set purchased multiple VMs using the stolen credit cards they can begin building their botnet. Once the botnet is compiled the attacker can then send out coordinated DDoS or DoS attacks using a single command (Pacella, 2011). In a DDoS or DoS attack the target could be flooded with thousands of empty data packets sent by the VMs. At a DefConconference in 2010, computer consultants were able to replicate this actual type of attack.

They created an Amazon cloud account and used three VMs to target a website's server. The attack was able to be carried out with without any type of e-mail from Amazon alerting them of the activity (Pacella, 2011). Once the VMs were shut down there was not a trace of the nefarious activity (Pacella, 2011). An actual cloud based DDoS or DoS attack could have the potential to take down major websites of a business or corporation causing millions of dollars in financial losses. As cloud based cybercrimes such as these become more prevalent the need for cloud forensics will become even greater.

Cloud Forensics

Cloud forensics is the bridging of cloud computing and computer forensics. Cloud computing requires a different mindset to investigative and forensic procedures (Lillard, Garrison, Schiller, & Steele, 2010). Cloud forensics applies the principles and techniques of computer computing to the cloud computing environment (Zawoad&Hasan, 2013). It is a subset of network forensics since cloud computing is based on broad network access and network forensics handles investigations networks (Ruan, Carthy, Kechadi, &Crosbie, 2011). Cloud forensics should follow the main phases of network forensics that are tailored to cloud computing investigations (Ruan et al., 2011). According to Lillard et al., (2010), when conducting cloud forensic investigations forensic examiners and investigators should consider the following caveats:

- It is not guaranteed that the examiners forensic computer is not compromised after accessing the cloud to download its contents. Current practices do not have forensic workstations connected to the Internet for this reason.
- The browser used to access the cloud cannot be trusted since the reply to the Web request may pass through several machines before it gets back to the forensic workstation.

- There is no guarantee that the data is displayable, so some data may need to be downloaded without being able to record it from the computer display.
- The cloud service may give a different view of the data than how it is viewed on the suspect browser. For example, Amazon allows different welcome pages to different customers depending on the location.

Cloud forensic tools. There are a number of widely used forensic tools available to investigators and examiners that include:AccessData FTK, EnCase Enterprise, Fastdump from HBGary, Memoryze from Mandiant, and FTK Imager from AccessData. These tools have been trusted by courts and have been used throughout traditional digital forensic investigations. Seizure and acquisition are the initial steps in any forensic examination (Dykstra & Sherman, 2012).

In cloud computing investigations two scenarios exist: investigators can remotely collect the evidence themselves or the CSP can provide it (Dykstra & Sherman, 2012). A question that remains is whether currently available forensic tools could be used to analyze cloud based evidence. Sherman and Dykstra (2012) found that these types of forensic tools can be used in cloud environments. Using an Amazon EC2 public cloud as a live test bed, they tested how the FTK, EnCase, FTK Imager, Fastdump, and Memoryze could collect data from the guest operating system, virtualization layer, and host operating system. The tools were all capable of obtaining forensic evidence data from the Amazon EC2 cloud. However, Dykstra and Sherman did not recommend using FTK and Encase for remote forensics of the cloud because too much trust is required between the CSP and examiner. The need for forensic tools that can be used among various cloud platforms is needed.

Using the cloud as a forensic tool. Cloud computing has the potential to assist examiners and investigators in cloud based digital investigations. Digital forensics could take advantage of using the available services and resources provided by cloud systems (Reilly et al., 2011). The major benefits include large amounts of storage, high availability and massive computing power (Poisel, Malzer, &Tjoa, 2013). Another main benefit of using cloud computing to aid digital forensic investigations is having centralized data. If the data is all in the same place it assists in forensic readiness and leads to quicker and coordinated response to incidents (Reilly et al., 2011). IaaS providers could develop dedicated forensic servers within the cloud and can be ready for use when needed (Reilly et al., 2011).

Examiners and investigators could also use cloud services to potentially store hard drive images in the cloud. It would utilize the resources of IaaS platforms to store the data (Reilly et al., 2011). The availability of large computing power could help examiners compute intense jobs. For instance, examiners may need to crack password or encryption keys or examine multiple images at one time (Reilly et al., 2011). Carrying out multiple types of these activities may be limited on an examiners workstation, but could be increased by using the large available computing power in the cloud. In addition, examiners could use the benefits of built-in hash authentication of cloud disk images. For example, Amazon generates MD5 hash values when data is stored, which means examiners would no longer have generate time consuming MD5 hashes of evidence (Reilly et al., 2011).

Forensic support by a CSP. The use of a CSP to support the acquisition of forensic data is a viable option. The CSP is pre-positioned to preserve and collect data since they have direct control over the cloud infrastructure (Dykstra & Sherman, 2012). The CSP could collect data

from a virtual machine, but also from logging mechanisms, packet captures and billing records (Dykstra & Sherman, 2012).

The use of forensic tools for remote acquisition would not be needed if the CSP and its infrastructure were trusted and the CSP was willing to provide evidence directly to the investigator (Dykstra & Sherman, 2012). For example, an investigator could serve the CSP with a search warrant for a customer's stored cloud data. The CSP could have a certified forensic examiner on site that collects the data from the cloud infrastructure. This could be done at an offline workstation connected to the back end of the cloud (Dykstra & Sherman, 2012). The CSP could quickly gather log information, access logs, VM information, netflow records, and firewall logs (Dykstra & Sherman, 2012). The data would be validated using MD5 hashes that were given when the data was originally stored in the cloud. It could then be copied to a media device and given to the investigator.

This would bypass the investigator from having to remote into the cloud infrastructure and search for the data. It would use the expertise of the CSP knowing how the data is found in their cloud infrastructure. The CSP may not have to reveal proprietary information that may have been given up during a remote acquisition. However, the investigator or examiner goes about acquiring data from the cloud, either remotely or using a CSP, they must be familiar with laws and statutes in place to obtain evidence.

Legal considerations related to cloud forensics. Cloud forensics will require that there is a strong understanding of following legal procedures presented during investigations. Cloud forensics will follow similar legal procedures, like traditional forensics, but current legal procedures may have to be altered to encompass cloud forensics. Investigators and examiners

who encounter cloud-based investigations should be well versed in how privacy laws, search and seizure laws and obtaining warrants are related to cloud based crimes.

In the U.S. the legal issues of obtaining data from the cloud can be focused around the Federal Rules of Civil Procedure (FRCP), Federal Rules of Criminal Procedure(FRCRP), and the Fourth Amendment to the U.S. Constitution (Fourth Amendment). Cloud forensics following and understanding the proper legal processes will be important to validate evidence to be presented in court.

Fourth Amendment applied to the cloud. The Fourth Amendment applies to the areas of expectation of privacy, requirements for a warrant, and execution of a warrant.In order for investigators and examiners to gather evidence from the cloud it must abide by what is valid under the Fourth Amendment. The Fourth Amendment reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (Cornell,n.d).

When dealing with the Fourth Amendment a consideration that should be considered is whether there is a reasonable expectation of privacy. Cloud computing allows users to not have to store any data on their PCs or mobile devices. The data is stored in the hands of a third party, for example Google or Amazon. The other privacy aspect of cloud computing is that the customer may be viewed as given explicit, or implicit, consent for others to access their data (Orton et al., 2013). These two factors may determine or limit whether the customer has any reasonable expectation of privacy in cloud data.

Reasonable expectation of privacy. Cloud computing has brought a new aspect to this area of the law and when a customer is entitled to privacy. Courts determine whether there is reasonable expectation of privacy by looking at the person's subjective expectation of privacy and how society accepts that as objectively reasonable (Orton et al., 2013). The highest privacy interest is attached to items being located in a private dwelling. The expectation of privacy becomes a cloudy area when the computer is not in the private dwelling, but is shared with other members of the public (Orton et al., 2013). Cloud computing becomes involved in these situations because the data can be accessed or stored from outside the home or workplace. This creates challenges for the courts to differentiate the boundaries when one has a reasonable expectation of privacy (Orton et al., 2013).

In the case of *Katz v. U.S.*, 389 U.S. 347 (1967), the U.S. Supreme Court (Supreme Court) held that "what a person knowingly exposes to the public, even in his home or office, is not subject of Fourth Amendment protection" (Orton et al., 2013). The Supreme Court has also held that a person does not have legitimate expectation of privacy when participating with a third party (Orton et al., 2013). This general principle that someone has no reasonable expectation of privacy with a third party can be justified in two ways. The first, is referred to as "disclosed to the public" which pertains to the nature of sharing information with the public (Orton et al., 2013). For instance, if someone shares their information by sharing it on a street corner or publishing for the public, there is little disagreement the individual has no privacy.

If data is distributed in this manner, through cloud storage or other means, it is not protected by the Fourth Amendment (Orton et al., 2013). For example, data may be stored through blogs stored on third party servers and if these blogs are made publicly available then there is no reasonable expectation of privacy (Orton et al., 2013). The other justification is

referred to as "third-party doctrine," which is based on the risk an individual assumes when sharing information with a third party (Orton et al., 2013). The third party can disclose the information to others that include law enforcement (Orton et al., 2013). This justification is important to the context of cloud computing.

Reasonable expectation of privacy in the cloud. It becomes questionable whether or not customers have a reasonable expectation of privacy when they store data in the cloud. Once data is stored in the cloud does it mean it was for the public to view and does it constitute as voluntarily turning data over to a third party? This is an issue that still remains in regards to cloud computing environments.

If cloud computing were compared to the reasonable expectation of privacy when dealing with IP addresses, it would appear that cloud computing users would not have a reasonable expectation of privacy. In the case of *U.S v. Christie,* 624 F.3d 558 (2010), the U.S. Third Circuit Court of Appeals held that individuals do not have a reasonable expectation of privacy in their IP addresses (Thompson, 2013). This case involved the Federal Bureau of Investigation (FBI) acquiring Internet protocol (IP) addresses of computer users who were accessing child pornography websites. The FBI had requested the names of users who were linked to the IP addresses for the Internet service (Thompson. 2013). The court found that there was not a reasonable expectation of privacy in IP addresses because information is shared with third parties-the Internet Service Provider (ISP) and that IP addresses are voluntarily turned over to third party servers (Thompson, 2013). In the case of *Forrester v. U.S.*, 512 F.3d 500 (2007), the court held that:

> email and Internet users do not have an expectation of privacy in the to/from addresses of their messages or the IP addresses of the website they visit because they should know that

this information is provided to and used by the service provider for the specific purpose of directing and routing of information (Thompson, 2013).

These two cases may be applied to cloud computing, but it has yet to be seen whether or not future courts will apply the distinctions of the expectation of privacy between cloud computing and traditional forms of electronic communications (Thompson, 2013).

Another element that may apply to whether or not cloud computing customers have a reasonable expectation of privacy is whether there were reasonable steps taken to conceal the contents. This element encompasses whether or not an individual took steps to minimize the data that can be viewed by others. In a non-cloud environment this applies to someone locking their luggage or briefcase or password protecting or encrypting file, or a computer (Orton et al., 2013). These steps demonstrate a subjective expectation of privacy that decrease the disclosure to others (Orton et al., 2013).

The use of password protected access or encrypted data in the cloud would indicate a subjective privacy expectation (Orton et al., 2013). Other issues that may affect the expectation of privacy of data in the cloud may surround: the absence of evidence of abandonment, whether the data was created by the user or third party, the nature of the contents, and the contractual relationship between the individual and third party. These issues present further unique issues pertaining to the reasonable expectation of privacy using cloud computing.

Obtaining a search warrant for cloud data. In the event that the courts do determine that cloud users have a reasonable expectation of privacy, investigators will need to execute a warrant for the cloud data. Before a warrant can be issued there are a number of requirements needed. The first requirement is that the warrant must be approved by a court of law (Dykstra, 2013). The next is that the Fourth Amendment requires probable cause, in a sworn statement that

the law enforcement official requesting the warrant believes that the search will find criminal activity (Dykstra, 2013). In this case, a law enforcement official would have to establish that a crime was committed using the cloud or in the cloud. There are likely to be no issues associated with cloud computing with regard to establishing a crime was committed (Orton et al., 2013).

The last requirement requires that the warrant specifies the place, person, or thing to be searched. In cloud computing this can become difficult since the data in the cloud can be scattered. CSPs are often hesitant to discuss their infrastructure that would be needed to specify a search strategy (Dykstra, 2013).

It is recommended that judges should decline to impose limitations of issuing cloud-based warrants (Dykstra, 2013). The precise location of the cloud information stored may not be known and can create a major block for investigators (Orton et al., 2013). To avoid the judge not granting a warrant due to the vagueness of the location of the data, investigators should include a description of the data (Dykstra, 2013). The computer files should be included rather than the physical hardware and in the case of cloud computing the hardware is owned by the CSP (Dykstra, 2013). In the case of cloud computing, the CSP may not be able to provide the physical hardware without affecting other customers.

The "property to be seized" in the warrant should fall into FRCRP Rule 41(b): property that constitutes evidence of the commission of a criminal offense (Dykstra, 2013). This would give a very broad authorization covering anything that the investigator believes would reveal information. The warrant could also be labeled to encompass 'contraband,' the fruits of crime or things otherwise criminally possessed, which in cloud environments contraband can be found in numerous forms (Dykstra, 2013). Contraband in the cloud could include: stolen credit cards, passwords or software, malware, or child pornography. If a hacker broke into a VM the machine

could be viewed as the fruits of the crime that was acquired as a result of a crime of unauthorized access (Dykstra, 2013).

Another category that a warrant could fall in is listed in the FRCRP Rule 41 (b): "property designed or intended for use, or which is or had been used as a means of committing a criminal offense" (Dykstra, 2013). Cloud computing has shown that VMs can be used in computer crimes such as botnets, DDoS attacks or distributing child pornography.

Once there is sufficient evidence for a warrant to be granted the warrant is served upon the CSP, who in turn executesit. The warrant is carried out by the CSP because law enforcement officers may not have the resources or expertise to carry out the warrant. This would be consistent with traditional search warrants. For instance, when officers go to a building looking for evidence they do not ask the occupants (Dykstra &Riehl, 2012). The officers know what they are searching for and would not rely on an occupant who lacks incentive to be thorough (Dykstra &Riehl, 2012). The key focus should be that the seizure of evidence should be concentrated on the data rather than the hardware and that the data can be spread across multiple locations (Dykstra, 2013).

Review

Cloud computing is changing the landscape of digital forensics and how forensic procedures and techniques are carried out. Although cloud forensics is based on traditional forensics practices, it brings new technological aspects to the table. The biggest shift from traditional forensics to cloud forensics may be that data is no longer stored locally, but through virtualization. Current available forensics tools can be used in cloud forensics investigations, but there is a need for cloud specific forensic tools.Cloud computing has the potential to aid the digital forensic field and perhaps bring in new techniques that will allow digital forensics to

become more efficient. Cloud computing offers large IT benefits to individuals and customers, but to cybercriminals as well. There is no end in sight for cybercrime to decrease and it will become more likely that cybercriminals will also embrace cloud computing power to carry out crimes. The malicious activities that cybercriminals and researchers have found can be carried out using cloud computing are only the tip of the iceberg.

Cloud security should remain as a discussed topic among CSP and customers. A breakdown of cloud security could allow for a new breeding ground of cybercrime. As examiners and investigators face cloud-based investigators it is important to understand the legal procedures to acquire and preserve cloud data. The introduction into the legal considerations surrounding the Fourth Amendment and obtaining warrants is merely a small part to the legalities of seizing evidence in cloud environments. The Electronic Communications Privacy Act (ECPA) of 1984 (18 U.S.C. §§ 2510–2522) and the Stored Electronic Communications Act (SCA) of 1986 (18 U.S.C. Chapter 121 §§ 2701–2712)were not covered in this research project, but should also be considered during cloud based investigations.

Discussion of the Findings

The introduction and use of cloud computing has vast computing advantages for individuals, businesses, and corporations. Cloud computing's potential to offer unlimited access to scalability and elasticity of virtual computing platforms has driven its popularity. As cloud computing becomes more popular it, without a doubt, will be involved in digital forensic investigations. The intersection of cloud computing and digital forensics has brought new challenges to carrying out traditional digital forensic practices. The challenges range from the initial collection of evidence to the legal issues of having access to the data. Traditional digital forensics techniques and procedures are being altered to fit cloud based investigations. The

digital forensic investigation of cloud computing platforms has resulted in cloud forensics. Studies by Dykstra (2013), Jerebak (2011), and Orton et al. (2013) suggest that cloud forensics techniques and procedures are still being developed and are in their infancy.

Major Findings

Virtualization does not come without issues. The virtualization is the heart of what allows cloud computing systems to exist and operate. Cloud forensics may need to focus on virtualization since it is such an important part of cloud computing.However, the handling of cloud incidents seems more challenging as the desires of the customers investigating a potential breach can clash with the privacy interests of the CSP (Jerebak, 2013). Investigators and examiners will need to familiarize and understand virtualization in order to understand how cloud computing operates.

If the virtualization of computing resources were not possible then cloud computing would not be nearly as efficient as it is. Jerebak (2013) states the security issues that surrounds virtualization is not an entirely new problem. The same security concerns have long existed for physical computing machines. Physical computer systems need to be constantly updated with new security patches and if they are not then they are at risk of unpatched holes being exploited. If physical computers are not used for periods of time it is likely they will not be updated with the newest software updates. For example, computer technology companies such Microsoft, Adobe, and Java are often releasing new security and software updates that users may choose to update or not.

As efficient as it is, virtualization does not come without problems. The efficiency of virtualization can also be its own worst enemy.The largest security risk to cloud computing may be the assumed layer of protection (Jerebak, 2013). Since virtualization allows users to create a

massive amount of VMs, some may become dormant. Dormant VMs may not receive the most up to date software and security patches. If the dormant VMs are then restarted at a later point the user may be unaware that the VMs have vulnerabilities because they were not updated. A single VM that has not been updated with the most current security patches could leave an entire cloud instance at risk. An attraction to cloud computing is that customers often do not need to update software and security patches. The CSP may offer the maintenance of the actual platform to run VMs, but may not keep track that each customer is updating their VMs. In return, the customer may not update their VMs because they believe that this responsibility falls on the CSP. Jerebak (2013) states that this problem could be eliminated if the CSP keeps track of the software on a client's VM and compares it to a list of known vulnerabilities.

This can also affect cloud forensics in the case that investigators were to stumble upon active or dormant VMs. If an investigator was unaware that a VM(s) they were investigating was not updated with new security patches it could put the user at risk (Jerebak, 2011). A dormant VM may be infected with malicious content that made its way onto the system and once restarted continues to spread malware (Jarabek, 2011). The investigators may also be searching for data that could potentially be found on a dormant VM.

The main benefit of virtualization from a forensic aspect is the ability for VMs to create snapshots (Reilly et al., 2011). Since VMs exist in the cloud and a copy of a disk image cannot be made, the data the snapshot retains can be just as useful. A snapshot is the equivalent to a virtual hard drive and provides a view of what was running at the time the snapshot was taken (Reilly et al., 2011). Snapshots can be made as the VM continues to run and provides different points the VM can be restored to. As the VM continues to run it will create more snapshots (Reilly et al., 2011). The snapshots would appear to be a significant source for evidence data.

However, the use of VM artifacts in court is still questionable and may not be able to be used (Reilly et al., 2011).

When a VM is booted there are notable changes made to the VM image and once rebooted it makes changes to the original (Reilly et al., 2012). In case a VM were booted during an examination it has potential to change the original data. If changes are made to the original data it means that it has undergone change and would be challenged in court (Reilly et al., 2012). This is why traditional computer forensics techniques prefer a bit-wise copy of the original evidence (Reilly et al., 2012). A bit-wise copy is the preferred way for evidence to be presented in court (Reilly et al., 2012). Virtualization could also prove useful to investigate a system that uses virtualization, but traditional techniques can be used on a physical system (Reilly et al., 2012). This may support the reasoning of why cloud forensics should be focused on virtualization (Reilly et al., 2012).

Cloud security is a concern. Cloud computing has had to jump right into considering security measures since it is such an essential part to IT structures (Reilly et al., 2011). CSPs and their customers do not want their data being exposed to unauthorized users (Reilly et al., 2011). Even with security measures being a focus by CSPs and customers there are still growing concerns with cloud security.A single security flaw could allow an attacker access to large amounts of data (Samson, 2013). The presence of cloud security threats and risks means that there will be a need to investigate security breaches. Researchers at the DefCon conference were able show how the cloud can be used maliciously, but it was done in contained environment (Pacella, 2011). The cloud was able to be used maliciously without a single alert by the CSP (Pacella, 2012). If CSPs aren't watching all activity that occurs in the cloud how can

theyguarantee that all the data is secure? This also suggests that cybercriminals could use the cloud for malicious purposes without being caught.

Another security issue that exists is the amount of privacy in the cloud. Data can be stored throughout datacenters that scattered throughout the U.S. or other countries. Each jurisdiction may have different regulations that protect the privacy of data (Kulkarni et al., 2012). For cloud customers it can be difficult to determine what privacy regulations apply to certain areas (Kulkarni et al., 2012). For example, privacy regulations in another country or jurisdiction could allow for easier access to a user's data than other areas. In relation to cloud forensics, this can affect how data is gathered during an investigation. Potential regulations in another country may not need to meet legal requirements that are needed in the U.S. Data loss and leakage are other clear concerns for cloud computing. Users may choose to keep most of their data in the cloud. However the data could be mishandled or lost by the CSP (Samson, 2013). Data can also be lost by an attacker who chooses to delete it from the cloud (Samson, 2013). As Samson states, data loss can also cause problems for customers who are legally required to store data to remain in compliance with certain laws, such as the Health Insurance Portability and Accountability Act (HIPAA) (Samson, 2013). Cloud computing and other new technologies are transforming the face of information security (RSA, 2013).

Cloud forensics comes into the picture with cloud security in the event that a breach, deletion or loss of data in the cloud does occur.If the security is exploited, the customers, businesses, and corporations will need and want a way to investigate a breach. Cloud forensics will be integral to investigating the security breach and find what and if any data was manipulated or stolen. As CSPs continue to address security needs, cloud forensics may take a backseat. Security is needed at all times, whereas cloud forensics may just be needed at certain

times (Reilly et al., 2011). In order for computer forensics and cloud forensics to be successful measures must be put in place before an incident occurs (Reilly et al., 2011).

CSPs cannot wait for an incident to happen and expect to react successfully with cloud forensic techniques that are created at the time of the incident. CSPs, or customers, will need to have adequate cloud forensic procedures in place to investigate the situation. The cloud forensic procedures should be clear so that there are not issues that hinder a cloud examination from occurring in an acceptable amount of time.

No end in sight for cybercrime. Cybercrime has become a multi-billion dollar business for cybercriminals. As cybercriminals in Russia have found they can make billions of dollars by sitting in front a computer (Essers, 2012). Traditional crimes can now be committed by a keyboard and a few simple clicks of a mouse. The case in RamincuValcea, Romania shows how a small poor town can turn to a life of luxury by committing cybercrime (Bhattacharjee, 2011). The streets of RamincuValcea are filled with luxury cars and men who appear to all have high paying jobs, but their high paying jobs are stealing money on the Internet (Bhattacharjee, 2011). Cybercrime is easy to commit and cybercrime is a beautiful business model (Gohring, 2011). Cybercrime is becoming more professional in many ways and is unlikely to see a slowdown (Gohring, 2011). Cybercriminals can go online to forums or assemble teams for writing malware. It makes it very easy and attractive for people to commit cybercrimes which has low overhead and low risk (Gohring, 2011). If there is low risk and the chances to make a lot of money then cybercriminals will continue to carry out cybercrime. As stated in a report by McAfee (2013), cybercriminals and hacktivists are going to continue to evolve and strengthen.

Cloud computing gives cybercriminals more power. For legitimate and illegitimate uses the main draw to use cloud computing is unlimited computing for a low, low price

(Garfinkel, 2011). There appears to be no reason for cybercriminals to not use cloud computing in cybercrime. Cloud computing options are widely available to criminals and easy to obtain. It is almost certain that as companies move to the cloud, attackers will focus more of their effort towards it (Jerebak, 2013). The nature of cloud computing allows cybercriminals to fly under the fraud detection radar and slip back into the shadows. Compare cloud computing to Grand Central Station in New York (USA)where it is easy to mix in with a crowd or take a ride to another jurisdiction beyond the law's reach (Garfinkel, 2011).

The use of cloud computing for password cracking is an emerging use by cybercriminals (Garfinkel, 2011). Criminals are able to exploit the power to cloud computing for malicious acts. In this case, cloud computing gives criminals more power to break into encrypted files by using dozens of computers at one time (Garfinkel, 2011). Garfinkel (2011) further states many of today's security protocols were created when password crackers only had access to a small number of computers. When the security protocols were created it was not known at the time that cloud computing would soon cause the security protocols to become obsolete. Cloud computing for password cracking has already been used in the attack against Sony's Playstation game network (Garfinkel, 2011). The introduction of GPU-based cloud services have been an even further game changer in cloud based password cracking. The expanded use of cloud based GPUs for cloud capability was shown by security specialist Roth (Garfinkel, 2011).

Cloud computing is, and will be, another powerful tool to for cybercriminals to utilize for cyber-attacks. As it was shown at the DefCon conference a simulated cyber-attack can be successfully carried out using cloud resources (Pacella, 2011). The simulated attack was carried out and the activity was not flagged by the CSP (Pacella, 2011). This indicates that CSPs cannot, or do not, track all the traffic on a given cloud platform. It also suggests that CSPs cannot tell

which customers are going to use the cloud for legitimate or illegitimate reasons. This type of nefarious activity is likely prohibited by CSP, but policing the cloud is expensive and not rewarding (Garfinkel, 2011). The availability of computing power that the cloud provides will greatly affect future cybercrimes. Once cybercriminals realize that they can harness cloud computing for malicious acts cloud forensics will have an even more important role in investigating cloud based crimes.

A clear need for cloud forensics. As digital forensics has shown there is a constant need to adapt to new types of computer technology. For instance, in recent years digital forensics has had to adapt to mobile computing technology involving cell phones and tablets. Investigators and examiners needed a way to gather and analyze data from mobile devices. Digital forensics had to apply traditional computer forensics practices to handle mobile forensics. In this case digital forensics will need to adapt in the same way to incorporate cloud computing. The increased adoption of cloud computing by individuals, businesses, corporations, and cybercriminals presents a clear need for cloud forensics. Whether it is investigating the loss of data or the nature of a cloud based attack, cloud forensics will be needed. Traditional computer forensic procedures cannot be applied in the same manner to cloud environments. This is because the data is no longer found on a physical machine or hard drive. Cloud forensics must apply the same principles and techniques from traditional forensics to cloud forensics (Zawoad&Hasan, 2013).

Current forensic tools and forensic support. The current forensic tools that have been widely used in traditional computer forensics investigations can be used in cloud examinations. Sherman and Dykstra (2012) found that tools such as: FTK, EnCase, Fastdump, Memoryze, and FTK Imager were successful in a cloud environment. This means that investigators and examiners do have options to carry out a cloud forensic examination. FTK and Encase are court

accepted tools that have been effectively used in trials and withstood arguments of their validity (Sherman & Dykstra, 2012). However, even with the available forensic tools that does not mean that the investigator, or examiner, have a clear understanding on how to handle a cloud environment. The examiner still needs to know how to use the tools in a cloud environment and if the cloud environment will allow the use of such tools. Sherman and Dykstra (2012) also concluded that these tools may not be practical because of the remote nature and trust between the examiner and CSP. If these tools can be used, but are not recommended then new forensic tools are needed. The development of specific cloud forensic tools should be a focus by the forensic community. Forensic tools specifically for cloud environments will be needed as the growth of cloud computing and cloud based crime continues to grow.

Legal understandings must be clear. Cloud forensic investigations cannot occur without first understanding the legal aspects and without a clear understanding they have the potential to leave investigations dead in the water. Cloud forensics must follow the proper legal processes and requirements that will be beneficial for presenting evidence in court (Orton et al., 2013). Cloud forensic investigations must follow laws in place to ensure that the evidence has been validated to be used in court (Orton et al., 2013).

Traditional computer forensic examinations are based on the authenticity and reliability of how the data was collected. In cloud forensic examinations the acquisition can vary, but the end result must still show that the data is authentic and reliable. There is limited information and uncertainty regarding how the law reads in reference to cloud computing (Orton et al., 2013). Current laws in place are ill-equipped to handle legal issues of cloud computing and lack solutions (Orton et al., 2013).

The development of cloud forensic procedures and tools may not address the legal issues. Cloud forensics need to first address the complex legal requirements to acquire the data before tools are developed (Orton et al., 2013). The legal requirements may determine how a cloud forensic tool can collect data to allow it to be authentic enough to be admitted in court (Orton et al., 2013). From another legal standpoint, cloud customers must understand how their data can be acquired and used in the event a cloud forensic examination is needed.

Cloud computing creates unique issues regarding search and seizure limitations of the Fourth Amendment and more specifically whether there is a reasonable expectation of privacy in the cloud (Orton et al., 2013). A reasonable expectation of privacy in the cloud may depend on a number of variables that include: how the data was concealed, the nature of the data, who created the data, abandonment of data, or the contractual relationship (Orton et al., 2013). The existence of unique legal issues means that investigators may still not have a clear understanding of search and seizure procedures in cloud environments. Investigators will need to enter cloud forensic investigations with the assumption that privacy rights exists and that a warrant or its equivalent will be required (Orton et al., 2013).

Research by Dykstra (2013) indicated that current law enforcement manuals have not been made public by any CSP that describes the data available during search warrants. This suggests that even with a search warrant investigators may have limited access to the data. The requirements that are needed to obtain a warrant should not be a problem as long as it has been established a crime was committed (Orton et al., 2013).The requirements for obtaining a search warrant leave room for broad generalizations to be made. For instance, a search warrant for the cloud should not specify a specific address (Dykstra, 2013). If a specific address were used a warrant may not be able to access data stored in other locations (Dykstra, 2013). Investigators

will need to know what data is involved and the type of files, but do not have to give a specific location (Dykstra, 2013).The investigator would not need to specify the exact VM that the data was stored on.It is key point that the seizure of evidence is concentrated on the data rather than the location (Dykstra, 2013).

The "property to be seized" should also focus on the files and not the actual physical hardware (Dykstra, 2013). In a cloud computing environment the customer does not own the physical hardware (Dykstra, 2013). One exception would be if the investigation was based on a CSP and in that case the CSP owns the physical hardware (Dykstra, 2013). Investigators should also include specific words that give a broad generalization of the data. An investigator who uses the word "contraband" in their warrant may have more access to the data than a warrant that does not include "contraband" (Dykstra, 2013). This is because contraband can apply to various things types of data and using such terminology is legally acceptable (Dykstra, 2013).

If the crime was committed on a cloud based website and the investigator came across criminal material they would not need a warrant. For example, child pornography or stolen data may be posted on a website that is viewed by the investigator. This is known as "plain view" and does not require a warrant to obtain the evidence (Dykstra, 2013). By understanding the legal requirements investigators and examiners can create a cloud forensic design to improve the efficiency of valid evidence collection (Orton et al., 2013).

Once the requirements have been gathered for the search warrant the CSP executes the warrant for law enforcement (Dykstra, 2013). However, it does appear to create problems with conflict of interest (Dykstra, 2013). It especially poses an issue if the CSP is the center of the investigation. In that case, investigators would not want the CSP to be handling potential collection of evidence. The process of how the search would be carried out by the CSP needs to

be well understood (Dykstra, 2013). Until that process is determined the technicians should be questioned about how the records are created and how the data was retrieved (Dykstra, 2013).

In a court case each technician does not need to be called upon, but a witness who can explain and be cross examined concerning the evidence (Dykstra, 2013). Additional issues that remain are: who at the CSP executed the search, what were their credentials, can they attest to the reliability and authenticity of the data, the security of the workstation used to collect the data, and who had access to the data (Dykstra, 2013). These questions show that the most challenging aspects of cloud forensics are the expert witness testimony and the forensic methodology used (Dykstra, 2013). Cloud crimes are not widespread and it is difficult to predict how the legal system will handle such cases (Dykstra, 2013).

Comparison to Other Studies

This research project discussed the common challenges posed by cloud computing found in current literature in the area of cloud forensics. The basic structure and operating procedures of IaaS, SaaS, and PaaS cloud computing platforms was included. It is typical for other studies to include the basic understandings of how different cloud computing platforms operate. The major issue that is found in most studies is the challenges associated with cloud forensic investigations. Challenges of cloud forensics are a common topic among other studies because cloud computing is new compared to traditional computer forensic practices. There are issues that stem from the acquisition of the evidence data to the legal requirement that need to be met during cloud investigations. In this research project, cybercrime was discussed as well as the ways cloud computing can be used in cybercrime. Other cloud forensics studies may not specifically discuss cybercrime and the way it can affect cloud computing. However it is important to understand that cybercrime is a growing concern and that cloud computing is likely to be involved in future

cybercrime. A topic that was not discussed in relation to cloud security was the use of side channel attacks. Side channel attacks have been mentioned in other studies discussing cloud forensics. Many studies touch on the legal issues surrounding cloud forensics and this research also highlights certain legal variables. This research project was not meant to disprove other studies, but was to display and highlight the key issues that surround cloud forensics and the cloud security.

Limitations of the Project

This research project had certain limitations which could limit the ability to understand the issues pertaining to cloud forensics. A major limitation is that cloud forensics is a fairly new topic and is limited by the amount of available research. One other limitation of this study was that it did not provide actual scenarios from the beginning to the end of a cloud based investigation. However, Dykstra and Sherman (2011) provided two hypothetical case studies to understand the issues in cloud forensics. This research project was also limited to the extent it covered the legal requirements for seizing evidence from cloud environments. Legal concepts of cloud forensics in relation the Fourth Amendment and obtaining search warrants were covered. However, the research paper did not discuss legal concepts involving: subpoenas, government involvement, statutory limitations of the ECPA and SCA, production of evidence in court, and general rules applicable to electronic evidence.

Another limitation was that there is lack of legal cases that involve cloud based crimes. Since there are no legal precedents set for cloud forensics it leaves uncertainty as to how it will affect cloud forensics. This project is unable to give answers on how the legal system will actually handle cloud forensic examinations and how evidence data will be accepted. In this research project current forensic tools were not tested on an actual cloud platform. A firsthand

account of how actual forensic tools work in a live cloud environment was not given. The use of common computer forensic toolkits such as FTK and Encase were mentioned in this research project but relied on the results from other studies.

Recommendations and Conclusions

Future Research

Network forensics. This research project did not cover the investigative use of network forensics for cloud computing environments. Some authors have suggested that network forensics plays a role in investigating a cloud computing environment (Reilly et al., 2011; Lillard et al., 2010; Ruan et al., 2011). This is because cloud computing operates through various types of computer networks. It can include the networks which bridge the user to the cloud or from one cloud instance to another. Network forensics would be best applied in a cloud environment where the user owns the network and computer hardware used to access the cloud (Lillard et al., 2010). Ruan et al. (2011) defined cloud forensics as a subset of network forensics. Cloud computing operates on broad networks, therefore cloud forensics follows the phases of network forensic techniques (Ruan et al., 2011).

Using network forensics for cloud computing must address the issue that once the data hits the internal and external processes it will be hard to track and trace (Lillard et al., 2010). Once the data has gone into the cloud, network forensics becomes part of the computer and systems forensics. Using network forensics can also be used to isolate internal systems from an incident and determine what level of compromise was internal and external (Lillard et al., 2010).

Network forensics can also influence the end result of an investigation of an event as long as the data was collected at the entry and exit points of the network (Lillard et al., 2010). The use of built-in firewall logs and system logs will generally point to an entry time, place, and IP

address (Lillard et al., 2010). This information can be used to help determine how an event was spread in a network and ways to prevent it in the future.

The majority of network forensics is monitoring the network traffic in order to isolate the number of servers needed to be taken down for investigation (Lillard et al., 2010). However, this is problematic in a cloud environment because the traffic on the backplane of the network is not going to be available(Lillard et al., 2010). The traffic that will only be available is the network traffic that will be visible by any network forensics tool that is operated at the server level (Lillard et al., 2010). In a cloud environment there may be a large number of VMs being used. This poses a challenge to network forensics because it is impossible to isolate a series of compromised computers and to sniff the local network (Lillard et al., 2010).

The tools needed to investigate cloud environments using network forensic techniques can include:Wireshark for Windows and Linux, WinPcap for Windows, Snort for Windows and Linux (Lillard et al., 2010). The use of current network forensic tools in a cloud environment needs to go to a back-to-basics per system monitoring process (Lillard et al., 2010). The reason for going back to the basics is because these programs work and have been proven to be effective. Further research of network forensic tools could be conducted on how Wireshark, WinPcap, and Snort can be used to gather evidence data from cloud environments.

A cloud test-bed could be set up to analyze how current network tools can be used in the cloud. The cloud test-bed could analyze the different types of network traffic found in cloud environments. The network traffic could include the traffic found in the hypervisor or between different cloud platforms. The reliability and results from the network forensic tools should be analyzed to determine if certain tools work better than others. The network forensic tools could be used with other forensic tools such as FTK or EnCase. The research could be used to show

how network forensics can be used in combination with other traditional forensic toolkits. The network forensic tools may provide data that were not found by FTK or EnCase. It may also result in the need for new network traffic tools to be developed to handle cloud environments. The current literature is limited on how network forensic tools can applied to cloud forensic investigations.

Using cloud computing for evidence data management. It has been discussed that evidence data can be collected and stored from a single cloud management plane (Grispos et al., 2011; Reilly et al., 2011; Dykstra & Sherman, 2012.). This is another area requiring further research of how the cloud can be used to aid investigations. Cloud computing could be used by investigators to store and acquire evidence data.

As Reilly et al. (2011) explain having all the data in a centralized location is a major benefit of cloud computing. This would allow investigators to have a quicker response to incidents and aid forensic readiness (Reilly et al., 2011). Using a single cloud management plane could also allow investigators to download log files, disk images, and packet captures to a single management plane on demand (Dykstra & Sherman, 2012).

CSPs could build dedicated forensic platforms in the cloud ready for use at any time by an investigator. For example, evidence data could be transferred in forensically sound manner from the location of the investigation to cloud storage (Grispos et al., 2011). This would eliminate the need for an investigator having to download data to a forensic workstation. Over time, an investigator may acquire large amounts of data from acquired disk images.

Cloud computing platforms offer peta-bytes of storage and large amounts of computing power resources. Investigators could take advantage of this and potentially store forensic data in the cloud (Reilly et al., 2011). Another additional benefit of using the cloud platforms for cloud

forensics is the built-in availability of hash authentication of disk images (Reilly et al., 2011). The Amazon S3 cloud service generates an MD5 hash value for data stored in the cloud (Reilly et al., 2011). This would eliminate the need for investigators to have to generate MD5 hash values for evidence (Reilly et al., 2011). However, it does raise concerns regarding the chain of the custody and the risk of a data breach by the CSP (Grispos et al., 2011).

A cloud test bed environment could be developed and used to see the benefit of how the cloud can be used in cloud forensics. This could be done in a real-time scenario that reflects a possible forensic examination in a cloud environment. A single data management plane would need to be created using the resources from a CSP. Research could be conducted on how evidence data can be moved safely and securely from the source of the investigation to a single cloud management plane. Ensuring that evidence is unaltered when transferred to and from the cloud should be closely examined. Once the data has been moved the use of built-in MD5 hash verification should be utilized. A copy of the data evidence should be made to adhere to traditional computer forensic best practice techniques. Once a copy is made in the cloud it should be verified by its MD5 hash value to show that no changes were made during the copying process in the cloud. The author's recommendation is to use a CSP that offers MD5 hash authentication during the testing. The authentication of evidence data is a necessary procedure that has been established by traditional computer forensics.

Further research could also be conducted on how evidence could be downloaded from a single cloud management plane. The evidence data may be stored in the cloud, but the actual analysis may need to be carried out on a dedicated forensic workstation. Again, the MD5 hash value of the data transferred from the cloud to a workstation should be of major importance. Other areas that should be examined are ensuring that if the cloud is used for storage, the local

laws of data protection are observed (Grispos et al., 2011). Grispos et al. (2011) also recommend that in the event that sensitive evidence is stored in the cloud the access to the data is limited by certain users. Limiting the number of users to the data would also help ensure that a strict chain of custody is maintained. Traditional forensic practices call for a strict chain of custody to be maintained and accurate logs of who handled the evidence.

Data acquisition from SaaS and PaaS cloud infrastructures. Cloud forensics is faced with new challenges specifically concerning data acquisition. This is another area that is recommended for further examination, specifically the SaaS and PaaS cloud infrastructures. Even though these platforms are all found in the cloud they do not operate in the same manner. The greatest difference appears to be the amount of control over the cloud infrastructure in IaaS, SaaS, and PaaS infrastructures.

Dykstra and Sherman (2012) provided research on how to acquire data from an IaaS platform. They provided analysis of different strategies for the challenges met during forensic acquisition from an IaaS infrastructure. However, there is a limited amount of literature about acquiring forensic evidence data from SaaS and PaaS cloud platforms. Current forensic tools and methods may be insufficient with the different types of cloud infrastructures. If the current forensic tools and methods are proven to not work then alternative options will need to be developed (Grispos et al., 2011). In an IaaS environment data acquisition is possible through the collection of snapshots from the VMs. However, this may not hold true for SaaS and PaaS platforms where the data is not controlled directly by the user. As previously discussed, the user has different limitations in SaaS and PaaS environments. This could pose challenges for an investigator since they could be acting as the user to acquire forensic data.

Through a test-bed environment using PaaS and SaaS cloud infrastructures the challenges of acquiring forensic data could be analyzed. Once cloud test-beds have been set up using PaaS and SaaS platforms the use of forensic tools and methods could be tested on each infrastructure. Using the cloud test-beds data could be placed in each of the cloud infrastructures to simulate data found during an investigation. The same forensic tools and methods should be used on both of the infrastructures to compare and contrast how effective, or ineffective, each tool and methods are.

Current forensic tools such as FTK and EnCase could be employed into the cloud infrastructures. FTK and EnCase were both used in the research study conducted by Sherman and Dykstra (2012). Dykstra and Sherman (2012) found that FTK and EnCase were the easiest to use. The research test-bed could also address how the cloud can be stabilized, to the extent possible, allowing the investigator to acquire sufficient evidence (Grispos et al., 2011). If there is a way to stabilize a cloud platform it should be discussed how it could be done and how to tell if it is in fact stable. The point of stabilizing a cloud platform would be to allow the investigator to have full control. Since the different cloud infrastructures have different ranges of user control, research should be conducted to determine how much control an investigator has over the data. Unlike an investigator having full control of an actual computer, an investigator may not be able to have full control in the cloud. The amount of control an investigator has over the evidence poses a challenge. For instance, if there is limited control of data then can it be further altered and if it is altered is there a way to determine it was? It is recommended that these questions be further examined using PaaS and SaaS cloud test-beds. Once these challenges have been addressed new forensic tools and methods can be developed to further handle cloud forensic investigations in PaaS and SaaS infrastructures.

Legal issues surrounding cloud forensics. Another area that is recommended for continued studies are the legal challenges faced by cloud forensics. As Dykstra (2013) explained, cloud based crimes are not widespread and it is difficult to predict how the legal system will react. Orton et al. (2013) provided the first comprehensive work on the legal processes for cloud forensics. Orton et al. (2013) also established a foundation for further research of the legal aspects. As mentioned, there are constitutional and statutory limitations as well certain requirements to obtain a warrant to carry out a cloud forensic investigation (Dykstra, 2013; Orton et al., 2013). Orton et al. (2013) also stated that requirements could be established to enable cloud computing environments to become a forensically ready. As Dykstra (2013) stated, future public court cases involving cloud forensic investigations could test the viability of search and seizure in cloud environments.

Additional research is also needed to establish how future cases will affect how cloud crimes are handled. The research should cover the cloud forensic legal aspects of data acquisition, chain of custody, and presentation of the evidence. It could also cover how cloud computing can be used in a legally acceptable manner to aid cloud forensic investigations. For instance, using cloud computing cloud for storage of evidence data or to break encryption or passwords by investigators. This type of research would assist in developing laws and statutes on how cloud forensic evidence is handled. The end goal of the research should be to inform the cloud forensic community on how to legally approach cloud forensic investigations.

Conclusions

Cloud computing is not going to disappear from the computer technology field anytime soon. More and more individuals, corporations, and businesses are turning to cloud computing for its economical computing resources. Dykstra (2013) stated “cloud computing is gaining

momentum and where the people, the data, and the money go, so does crime." The combination of the continued growth of cybercrime and cloud computing could mean a larger demand for cloud forensics (Grispos et al., 2011). Cloud forensics techniques and guidelines are continuing to evolve and are not at their final stage of completion. Until CSPs and forensic investigators can establish clear cloud forensic guidelines, cloud forensics will continue to see changes. The computer forensic field continues to adjust to new types of computer technology and will need to do so with cloud computing.

The introduction of cloud computing does not come without challenges to the computer forensic community. This research project has considered the new challenges that are faced by investigators conducting cloud forensics. Cloud investigations could be hampered by the initial data acquisition process. The reason for this is because data is no longer stored on a local machine, but is virtualized in a cloud environment. Cloud computing no longer gives a forensic investigator the luxury of physically having a computer, or hard drive, in front of them.

Challenges also arise from the preservation of data that includes the chain of custody and control of the data. These challenges can also lead to legal issues of whether or not evidence data can be found admissible in a court of law. Investigators face additional legal limitations associated with cloud computing based on areas such as jurisdictional boundaries and SLAs. The analysis of challenges created by cloud computing for the computer forensic community shows that there must be an emphasis to resolve the issues. Until these challenges are met the computer forensic community does not have a clear path on how to handle cloud forensic investigations.

This research project provided insight about how cloud computing has brought new challenges to traditional computer forensics. It is important to have an understanding of how cloud environments operate before approaching a cloud forensic investigation. This project also

addressed the ways that the cloud can be used in cybercrime. The ways that cloud computing is beneficial for businesses and corporations have the same benefits. It is likely that cloud based cybercrime will soon appear and use the cloud for malicious purposes. The likelihood of using the cloud in cybercrime displays a clear need for cloud forensic techniques.

A brief legal understanding of how the current laws and statutes may apply to cloud forensic situations. The lack of clear laws regarding cloud forensic investigations creates a struggle for how cloud data can be acquired and analyzed. There is a need for the legal and forensic community to develop law that is equipped to handle cloud forensic investigations. There is still much room for further research of cloud forensics and new techniques and methods to address cloud forensics are in its infancy. This project has left room open for further research into the technical and legal challenges that are faced by cloud forensics. It is likely it will take collaboration between academia, CSPs, and expert computer forensic professionals to develop and bring new standards of cloud forensics to the computer forensic community.

References

Bhattacharjee, Y. (2011). How a Remote Town in Romania Has Become Cybercrime Central. Wired. Retrieved June 2, 2013 from: www.wired.com/magazine/2011/01/ff_hackerville_romania.

Birk, D. (2011). Technical Challenges of Forensic Investigations in Cloud Computing Environments. Retrieved May 6, 2013 from http://www.zurich.ibm.com/~cca/csc 2011/submissions/birk.pdf

Birk, D., & Wegner, C. (2011). Technical Issues of Forensic Investigations In Cloud Computing. Retrieved May 6, 2013 from http://code-foundation.de/stuff/2011-birk-cloudforensics.pdf

Brenner, S. (2010).*Cybercrime Criminal Threats from Cyberspace.* Santa Barbara, CA: Praeger.

Carvey, H. (2009). *Windows Forensic Analysis*. Burlington, MA: Syngress Publishing Inc.

Chen, X., Dirro, T., Greve, P., Gupta, P., Li, H., McEwan, W., Paget, F., Schmugar, C., Shah, J., Sherstobitoff, R., Sommer, D., Sun, B., Szor, P., &Wosotowsky, A. (2013).2013 Threat Predictions. McAfee An Intel Company. Retrieved June 1, 2013 from http://www.mcafee .com/us/resources/reports/rp-threat-predictions-2013.pdf

Cornell. (n.d.). Fourth Amendment: An Overview. Cornell University Law School. Retrieved June 3, 2013 from http://www.law.cornell.edu/wex/fourth_amendment

Cruz, X. (2012, November 5). The Basics of Cloud Forensics. Cloud Times. Retrieved May 1, 2013 from http://cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics/

Dykstra, J. (2013). Chapter 7: Seizing Electronic Evidence from Cloud Computing Environments. 156-185, doi: 4018/978-1-4666-2662-1.

Dykstra, J., &Riehl, D. (2013).Forensic Collection of Electronic Evidence from Infrastructure – As-A-Service Cloud Computing.*Richmond Journal of Law & Technology,* 19(1), 1-47. Retrieved May 11, 2013 from http://jolt.richmond.edu/v19i1/article1.pdf

Dykstra, J., & Sherman, A. (2012).Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and Evaluating Tools, Trust, and Techniques.*Digital Investigation*, 9, S90-S98, doi: 10.1016/j.diin.2012.05.001

Essers, L. (2012). Russian Cybercriminals earned $4.5 billion in 2011. Computerworld. Retrieved May 24, 2013 from http://www.computerworld.com/s/article/ 9226498/Russian _cybercriminals_earned_4.5_billion_in_2011.

Filshtinskiy, S. (2013). Cybercrime, Cyberweapons, Cyberwars: Is There Too Much Of It in the Air? *Communications of the ACM*, 56(6), 28-30. doi:10.1145/2461256.2461266

Finkle, J. (2013). Researchers say Stuxnet was deployed against Iran in 2007. Reuters. Retrieved June 11, 2013 fromhttp://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUS BRE91P0PP20130226

Garfinkel, S. (2011, October 17). The Criminal Cloud.MIT Technology Review. Retrieved May 2, 2013 from http://www.technologyreview.com/news/425770/the-criminal-cloud/

Gohring, N. (2011). Private Cloud vs. Public Cloud vs. Hybrid Cloud.PCWorld. Retrieved June 2, 2013, from http://www.pcworld.com/article/243133/private_cloud_vs_public_ cloud_vs_hybrid_cloud.html

Gohring, N. (2011). Cybercrime getting easier to commit, feds say. COMPUTERWORLD. Retrieved June 5, 2013 fromhttp://www.computerworld.com/s/article/9220645/ Cybercrime_getting_easier_to_commit_feds_say

Goodin, D. (2012). Hack cloud let browsers use cloud to carry out big attacks on the cheap. Arstechnica. Retrieved May 25, 2013 from http://arstechnica.com/security/2012/11/hack could-let-browsers-use-cloud-to-carry-out-big-attacks-on-the-cheap/

Greenberg, A. (2012). Moxie Marlinspike's CloudCracker Aims for Speedier, Cheaper Password Cracking. Forbes: Security. Retrieved May 29, 2013 from http://www.forbes.com/sites/ andygreenberg/2012/02/14/moxie-marlinspikes-cloudcracker-aims-for-speedier-chea per-password-cracking/

Griffith, E. (2013, March 13). What is Cloud Computing? PCMAG. Retrieved May 6, 2013 from http://www.pcmag.com/article2/0,2817,2372163,00.asp

Grispos, G., Glisson, W.B., &Storer, T. (2011). Calm before the Storm: The Emerging Challenges of Cloud Computing In Digital Forensics. Retrieved May 5, 2013 from http:// www.dcs.gla.ac.uk/~tws/papers/grispos11calm-rev2425.pdf

Hay, B., Nance, K, & Bishop, M. (2011). Storm Clouds Rising: Security Challenges for IaaS Cloud Computing. Paper presented at proceedings of the 44th Hawaii International Conference on System Sciences. Retrieved May 10, 2013 from http://nob. cs.ucdavis.edu/ bishop/papers/2011-hicss-1/iaas.pdf

Henry, Paul. (2009, September 12). Best Practices in Digital Evidence Collection. Retrieved May 4, 2013from http://computer-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/

Higgins, K. (2011) Cloud-Based Crypto-Cracking Tool To be Unleashed at Black Hat Dc. DarkReading. Retrieved May 31, 2013 from http://www.darkreading.com/authentication/ cloud-based-crypto-cracking-tool-to-be-u/229000423

Jarabek, C. (2011). A Review of Cloud Computing Security: Virtualization, Side-Channel Attacks and Management. University of Calgary: Department of Compute Science.

Kaufman, L, & Potter, B. (2009). Data Security in the World of Cloud Computing. *Security & Privacy, IEEE*, 7(4), 61-64.

Kent, K., Grance, T., Chevalier, S., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology. Retrieved May 8, 2013 from http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86 .pdf

Kepes, B. Understanding the Cloud Computing Stack SaaS, Paas, IaaS. Diversity Limited. Retrieved June 1, 2013 from http://broadcast.rackspace.com/hosting_knowledge/white papers/Understanding -the-Cloud-Computing-Stack.pdf

Kulkarni, G., Gambhir, J., &Dongare, A. (2012). Security in Cloud Computing. *International Journal of Computer Engineering & Technology (IJCET),* 3(1), 258-265.

Lardinois, F. (2012, June 8). Gmail Now has 425 Million User, Google Apps Used by 5 Million Businesses and 66 of the Top 100 Universities. Techcrunch. Retrieved May 2, 2013 from http://techcrunch.com/2012/06/28/gmail-now-has-425-million-users-google-apps-used-by-5-million-businesses-and-66-of-the-top-100-universities/

Lillard, T., Garrison, C., Schiller, C., & Steele, J. (2010) *Digital Forensics for Network, Internet, and Cloud Computing.* Burlington, MA: Syngress.

Ludwig, S. (2011, November 29). Cisco: Global cloud traffic will increase 12-fold by 2015. Venturebeat. Retrieved May 2, 2013 from http://venturebeat.com/2011/11/29/cisco-global-cloud-traffic/

Orton, I., Alva, A., & Endicott-Popovsky, B. (2013).Legal Process and Requirements for Cloud Forensic Investigations.*IGI Global*, doi: 10.4018/978-1-4666-2662-1.ch008

Pacella, R. (2011). Hacking The Cloud. *Popular Science, 278(4), 68-71*.

Poisel, R., Malzer, E., &Tjoa, S. (2013). Evidence and Cloud Computing: The Virtual Machine Introspection Approach. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 4*(1), 135-152.

Reilly, D., Wren, C., & Berry, T. (2011).Cloud Computing: Pros and Cons for Computer Forensic Investigations.*International Journal Multimedia and Image Processing (IJMIP),*1, 26-34.

RSA. (2013). The Year in Phishing. RSA-EMC2.Retrieved May 30, 2013 from http://www.emc. com /collateral/fraud-report/online-rsa-fraud-report-012013.pdf

Ruan, K., Carthy, J., Kechadi, T., &Crosbie, M. (2011). Cloud Forensics. *Advances in Digital Forensics*, 7, 35-46.

Samson, T. (2013). 9 top threats to cloud computing security. InfoWorld. Retrieved June 4, 2013 from http://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428

Saxena, A., Shrivastqva, G., & Sharma, K. (2012).Forensic Investigation in Cloud Computing Environment.*The International Journal of Forensic Computer Science*. 2, 64-74. doi:10.5769/J201202005. Retrieved May 5, 2013 from http://www.ijofcs.org/V07N2-PP05-FORENSIC-INVESTIGATION.pdf

Slusky, L., Partow-Navid, P., Doshi, M. (2012).Cloud computing and computer forensics for business applications.*Journal of Technology Research*, 3, 1-10. Retrieved May 7, 2013 from http://www.aabri.com/manuscripts/11935.pdf

Thompson II, R. (2013). Cloud Computing: Constitutional and Statutory Privacy Protections.Congressional Research Service. Retrieved June 3, 2013 from http://www.fas.org sgp/crs/misc/R43015.pdf

Zawoad, S., &Hasan, R. (2013, February 26). Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. Retrieved May 3, 2013 fromhttp://cryptome.org/2013/02/cloud-forensics.pdf

Zimmerman, S., &Glavach, D. (2011). Cyber Forensics In the Cloud. *IAnewsletter, 14(1), 4-7*