Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing:
Exploring and Evaluating Tools, Trust, and Techniques

Josiah Dykstra and Alan T. Sherman

Cyber Defense Lab, Department of CSEE
University of Maryland, Baltimore County (UMBC)
1000 Hilltop Circle, Baltimore, MD 21250
{ *dykstra, sherman* }*@umbc.edu*

Abstract

We expose and explore technical and trust issues that arise in acquiring forensic evidence from infrastructure-as-a-service cloud computing and analyze some strategies for addressing these challenges. First, we create a model to show the layers of trust required in the cloud. Second, we present the overarching context for a cloud forensic exam and analyze choices available to an examiner. Third, we provide for the first time an evaluation of popular forensic acquisition tools including Guidance EnCase and AccesData Forensic Toolkit, and show that they can successfully return volatile and non-volatile data from the cloud. We explain, however, that with those techniques judge and jury must accept a great deal of trust in the authenticity and integrity of the data from many layers of the cloud model. In addition, we explore four other solutions for acquisition—Trusted Platform Modules, the management plane, forensics as a service, and legal solutions, which assume less trust but require more cooperation from the cloud service provider. Our work lays a foundation for future development of new acquisition methods for the cloud that will be trustworthy and forensically sound. Our work also helps forensic examiners, law enforcement, and the court evaluate confidence in evidence from the cloud.

Keywords: Computer security, cloud computing, digital forensics, cloud forensics, EnCase, FTK, Amazon EC2.

1. Introduction

Discovery and acquisition of evidence in remote, elastic, provider-controlled cloud computing platforms differ from that in traditional digital forensics, and examiners lack appropriate tools for these tasks. While there are many important issues in this new field, we focus explicitly on data acquisition. Crimes that target or use cloud computing will undoubtedly emerge in this landscape, and investigators will rely on their existing expertise in tools like Guidance EnCase or AccessData Forensic Toolkit (FTK) unless alternative tools and techniques are provided.

Digital forensics for cloud computing brings new technical and legal challenges. Cloud computing makes forensics different, particularly given the remote nature of the evidence, lack of physical access, and trust required in the integrity and authenticity. While the goals of the forensic examiner are the same as before, the non-conventional difficult problems include forensically sound acquisition of remote data, large data volumes, distributed and elastic data, chain of custody, and data ownership.

Seizure and acquisition of digital artifacts are the initial steps in the forensic process (Casey, 2004). Two possible scenarios exist: remote investigators could collect forensic evidence themselves from the source, or providers could deliver it. Each scenario requires a different degree of trust in the data returned. Further, each scenario uses different technical implementations to recover the data. Given years of development, acceptance by the judicial system, and expertise in the field, market leaders in the commercial forensic tool space including EnCase and FTK are ideally prepositioned for the cloud forensic challenge (SC-Magazine, 2011). One question that remained until now, however, was an evaluation of the ability of such tools to acquire and analyze cloud-based evidence.

Cloud computing is a broad, generic term with many meanings and definitions. It has infiltrated the vernacular, bastardized in marketing and media. Cloud computing is an evolution and combination of decades of technology, resulting in a model of convenient, on-demand, elastic, location-independent computing resources. Though some definitions of cloud computing include popular web-based services such as email and social networking, we limit the scope of this paper to computing resources that are billed as utilities. More specifically, we use the *Infrastructure-as-a-Service* (IaaS) model (National Institute of Standards and Technology, 2011). In this model, the consumer has complete control over a guest operating system running in a *virtual machine* (VM). The provider retains control

and responsibility for the hypervisor (HV) down to the physical hardware in the datacenter. Since the Platform-as-a-Service and Software-as-a-Service models are built on IaaS, beginning with IaaS provides a fundamental basis from which to build future work.

In this paper, we assume that the target system of the forensic investigation still exists in the cloud. The elastic nature of cloud computing makes it possible for a criminal to commit a crime and then immediately destroy the evidence, but that situation is not considered here. While some cases will involve the cloud as the instrument of the crime, others will involve the cloud-hosted service as the target of the crime. The later is the scope of this paper.

In draft guidance (Federal CIO Council, 2011, p. 21) on the secure use of cloud computing, the Federal Chief Information Officers Council states that "incident response and computer forensics in a cloud environment require fundamentally different tools, techniques, and training." In this paper, we evaluate the validity of that statement with respect to data acquisition. Contributions of our work include:

- Results from three experiments that exercise existing tools for persistent and non-persistent data collection in a public cloud, Amazon's *Elastic Compute Cloud* (EC2).
- Analysis of alternatives for forensic acquisition at lower levels of the infrastructure stack, for cases when there is insufficient trust in data acquisition using the guest operating system.
- A demonstration of how virtual machine introspection can be used to inject a remote forensic agent for remote acquisition.
- Exploration of four strategies for forensic data acquisition with an untrusted hypervisor.

The rest of the paper is organized as follows. Section 2 reviews previous and related work. Section 3.1 presents a model of cloud trust. Section 3.2 presents the context for a cloud examination. Section 4 presents our experiments in using the native capabilities of EnCase, FTK, Fastdump, and Memoryze for data acquisition in EC2. Section 5 suggests alternative approaches. Section 6 discusses considerations and Section 7 concludes the work.

2. Previous and Related Work

The US federal government evaluates some of the most widely used forensic tools to ensure reliability. The National Institute of Standards and Technology's (NIST) Computer Forensic Tool Testing (CFTT) project is charged with testing digital forensic tools, measuring their effectiveness, and certifying them (National Institute of Standards and Technology, 2003). They evaluated EnCase 6.5 in September 2009, and FTK Imager 2.5.3.14 in June 2008 (National Institute of Standards and Technology, 2009, 2008). They have never tested nor certified the enterprise versions of these products that include remote forensic capabilities. NIST also publishes a Digital Data Acquisition Tool Specification, which "defines requirements for digital media acquisition tools in computer forensic investigations" (National Institute of Standards and Technology, 2004). The most recent version of the specification was written in 2004, before cloud computing as we know it existed.

Several researchers have pointed out that evidence acquisition is a forefront issue with cloud forensics (Dykstra and Sherman, 2011a; Ruan et al., 2011; Taylor et al., 2011). Dykstra and Sherman's analysis of two hypothetical case studies illustrated the non-trivial issues with collecting evidence from a cloud crime (Dykstra and Sherman, 2011a,b). Ruan *et al.* (Ruan et al., 2011) suggested that evidence collection should obey "clearly-defined segregation of duties between client and provider," though it was unclear who should collect volatile and non-volatile cloud data and how. Taylor *et al.* (Taylor et al., 2011) also lamented about the lack of appropriate tools for data from the cloud, noting that "Many of these tools are standardised for today's computing environment, such as EnCase or the Forensics Tool Kit [sic]."

Virtual machine introspection (VMI) is a technique whereby an observer can interact with a virtual machine client from the outside through the hypervisor. In 2003, Garfinkel and Rosenblum (Garfinkel and Rosenblum, 2003) first demonstrated a technique for intrusion detection inside a virtual guest using VMI. In 2009 using VMware's VMSafe, Symantec demonstrated injecting anti-virus code into a virtual machine from the VMware hypervisor (Conover and Chiueh, 2008). From that year, researchers have proposed various applications of VMI to forensic memory analysis (Nance et al., 2009; Dolan-Gabitt et al., 2011). Santana (Santana, 2009) reports that Terremark uses introspection for monitoring, management and security for their vSphere cloud computing offering. So far no attempt has been made to inject a forensic tool, such as an EnCase servlet, into a virtual machine from the hypervisor.

In 2009, Gartner (Heiser, 2009) published an overview of remote forensic tools and guidance for their use, targeted at enterprise environments. They cited EnCase and FTK as the most widely used products, with the greatest international support. These tools, however, have their faults: in 2007, a vulnerability was found in the authentication between the remote EnCase agent and the server (Giobbi and McCormick, 2007). From a legal perspective, Guidance Software's own "EnCase Legal Journal" for 2011, a comprehensive examination of legal issues and decisions about electronic discovery, has no mention of judicial decisions or statutory law related to the complex legal questions surrounding remote data acquisition (Guidance Software, 2011). We are analyzing the intersection of forensics for cloud computing and legal statues for search and

seizure.

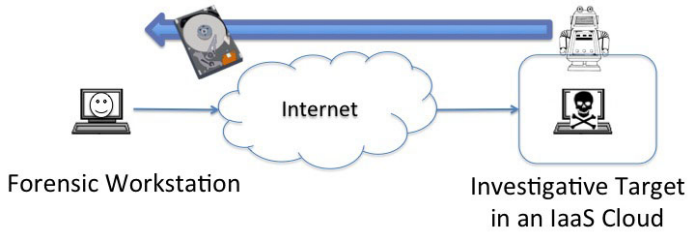

Figure 1: General technique for remotely acquiring forensic evidence over the Internet using a remote agent controlled by a trusted workstation.

EnCase Enterprise and FTK include a client-server feature for remote forensics. In each case, a small executable is installed on the client machine (EnCase calls the executable a "servlet;" FTK calls it an "agent"). Figure 1 illustrates how the server, built into or on top of the vendors' forensic analysis software, communicates with the client over a secure connection, and can command the client to return forensic data including a hard drive image. The forensic examiner may conduct some forensics remotely on the client, or return to the server for local analysis. Remote forensics is employed in large enerprises where machines may be geographically disperse, but the incident response team centeralized.

3. The Cloud Forensic Examination

In this section we explore the forensic examination of a cloud-based crime. As a foundation, we first present a model to reason about the trustworthiness of evidence from the cloud, since the level of trust influences the choices for how an exam should be conducted. Second, we pose choices that determine how to approach a forensic investigation.

3.1. Layers of Trust

Before evaluating tools for acquisition, it is important to understand trust in the cloud environment. When brought to court, the judge or jury must ultimately decide if they believe and trust the evidence presented to them. This choice embodies a specific confidence about whether the result is accurate and reliable. In traditional forensics, where the target machine is physically present, some of the same trust issues exist, as we shall explain.

Consider an example where a single desktop computer has been used to plan a murder. If law enforcement removes the hard drive for imaging, they must trust their hard drive hardware to read the disk correctly. If they run forensic tools on the live computer, they may have to trust the integrity of the host operating system in addition to the hardware. If the suspect computer was hosted in the cloud, new layers of trust are inherently introduced. We do not consider the trust in the forensic acquisition tools themselves nor in the human agents executing those tools, since these components, while important, are outside the cloud environment.

Table 1 models trust in IaaS cloud computing in six layers. The other cloud models, Platform-as-a-Service and Software-as-a-Service, would have additional layers on top to account for the platform or service provided. In IaaS, the consumer retains administrative control over Layers 5 (Guest OS) and 6 (Guest application), despite no physical access. Furthermore, the forensic acquisition activity would be different at each layer. Each layer requires a different amount of confidence that the layer is secure and trustworthy; the farther down the stack, the less cumulative trust is required. In public clouds, all layers require some trust in the provider, especially trust against malicious insiders. Ultimately, it is the judge or jury that must have confidence in the data to render a legal decision.

Imagine a situation where a forensic investigator has remote access to the guest virtual machine operating system. The investigator could collect evidence contained inside the VM, install a forensic tool and obtain live evidence remotely, or suspend/terminate the VM and analyze it offline. Unfortunately, acquisition at this layer requires trust that the guest operating system, hypervisor, host operating system, underlying hardware, and network produce complete and accurate evidence data, and are free from intentional and accidental tampering, compromise, or error. Note that with Type 1 hypervisors, such as Xen, the hypervisor is the lowest software layer, thus eliminiating one layer of trust.

As a risk mitigation strategy, the forensic examiner should examine evidence at multiple layers. This technique allows an investigator to check for inconsistency and to correlate evidence. Arranging individual contexts together into groups is a basic concept from archaeology, known as straigraphic interpretation. Garfinkel (Garfinkel, 2006) proposed a related technique for examining multiple drives to correlate evidence across seemingly unrelated evidence, such as for identifying members of social networks. We suggest extending this idea to identify suspicious activity at one layer of the cloud, and in corroborating forensic hypotheses.

Investigators may be tempted to conduct their investigation remotely on a running machine particularly given the size of the remote data, the time and cost to retrieve a full drive image, and the propensity to conduct live forensics. These are valid goals, and ones we will return to in Section 4.

Currently, law enforcement asks the provider for data. A search warrant or subpoena is issued to the provider, and the provider executes the search, collects the data, and returns it to law enforcement. Though this process frees law enforcement from needing remote acquisition technology and from the burden of understanding details of the cloud environment, it does not free them from significant trust

Layer	Cloud Layer	Acquisition Method	Trust Required
6	Guest application/data	Depends on data	Guest operating system (OS), hypervisor, host OS, hardware, network
5	Guest OS	Remote forensic software	Guest OS, hypervisor, host OS, hardware, network
4	Virtualization	Introspection	Hypervisor, host OS, hardware, network
3	Host OS	Access virtual disk	host OS , hardware, network
2	Physical hardware	Access physical disk	Hardware, network
1	Network	Packet capture	Network

Table 1: Six layers of the IaaS cloud enviroment and potential forensic acquisition techniques for each, including the cumulative trust required by each layer.

in the result nor from needing to process the data. Instead, the examiner and jury must now trust the integrity of the technician at the provider to execute the search in a trustworthy manner, the technician's hardware and software used to collect the data, and the cloud infrastructure (at least network and hardware) to retrieve, reassemble, and report the data.

3.2. Choices in Cloud Forensics

We now consider how to conduct a forensic exam of IaaS cloud computing by considering the following issues. The layers explored in Section 3.1 are also choices of where to conduct a forensic investigation. In particular, the investigator can choose at what layer of the cloud the forensic process will be executed. Considerations for this decision revolve first around the technical capability to conduct forensics at that level, and second the trust in the data returned. The layer also influences what type of forensic data are available for collection, such as packet captures at Layer 1 (Network), physical files at Layer 2 (Physical Hardware), or virtual files at Layer 3 (Host OS). For each data type the data must adhere to strict chain of custody and must include a mechanism for integrity checking.

One must choose who will conduct the exam and where will it be conducted. Possible choices for who will execute the exam include law enforcement, an employee of the cloud provider, or an independent examiner. Choices for where the exam will take place include at the provider's corporate headquarters, at one of the provider's remote datacenters, at a remote law enforcement facility, or at an independent third party facility. These choices are as much about practicality and logistics as the law and the examiner's qualifications. Requiring a non-employee of the provider to conduct an exam on provider premises would impose an unacceptable logistical burden to the provider. As we will discuss in Section 6, verifying the integrity and completeness of the data is still a challenge.

Cost is another choice affecting how an exam is conducted. When forensic data are requested, the cost in dollars and labor to preserve and produce records might be passed on to the requestor, or sold as a service by the cloud vendor.

Technical choices of how to conduct a forensic exam of cloud computing are numerous but closely mimic the choices in a traditional exam. First, the specific crime dictates whether the forensic process will be conducted on a live or dead machine. Second, regardless of whether the forensic data come from a workstation or the cloud, the forensic goal of determining what happened is the same, except that the volume and format of data may differ. The examiner's choice of analysis tools may be influenced by the format of data collected (*e.g.*, traditional files vs. cloud "blobs"), volume of data, and data type (*e.g.*, netflow logs, billing records, drive images).

Cloud computing introduces one powerful new option: virtual machine snapshots. With many cloud implementations that utilize virtualization it is possible to take a snapshot of a running machine and later restore and run the snapshot offline as if it were live. This offers the ability to create a historical record, as well as do "live" forensics after the fact.

4. Cloud Forensics Using Today's Tools

In this section, we measure and evaluate the ability of EnCase Enterprise and AccessData FTK to remotely acquire forensic evidence from cloud computing and measure their effectiveness. Both products are widely deployed today, benefit from tool expertise in the field, are trusted by the courts, and have a remote acquisition feature that has been targeted at geographically dispersed corporate LANs. Our goal is to evaluate the ability and scientic accuracy of these features to acquire forensic data from cloud computing environments over the Internet. We also test live forensic acquisition tools using Fastdump from HBGary, Memoryze from Mandiant, and FTK Imager from AccessData. These experiments evaluate the success at gathering evidence, the time to do so, and the trust required.

4.1. Motivation

Experimentation and testing of today's most popular forensic tools have not previously been applied to cloud computing. We propose three experiments using the IaaS cloud model, since that gives the examiner the most access and control of all cloud models. In particular, we use a public cloud, EC2 from Amazon Web Services (AWS), as a live test bed. *Experiment 1* collects forensic data from Layer 5, the guest operating system. *Experiment 2*

collects data from Layer 4, the virtualization layer. *Experiment 3* collects data from Layer 3, the host operating system. Because *Experiment 2* and *Experiment 3* use the Amazon cloud, we assume that the provider is producing the correct, untampered data.

The goal of these experiments is to evaluate the ability of five tools to acquire forensic data from cloud computing environments over the Internet. Consider how an investigator might approach his or her first case involving cloud computing. The investigator would likely pick the most popular volatile and non-volatile forensic software acquisition tools and seek to use them in the cloud environment. The first tools we chose were Guidance EnCase and AccessData FTK, since both are widely deployed today, benefit from tool expertise in the field, and are trusted by the courts. They have been used in thousands of trials, and withstood arguments about their effectiveness (Guidance Software, 2011). Each product has a remote acquisition feature that has been targeted at geographically dispersed corporate LANs. We also chose three memory acquisition tools—Fastdump, Memoryze, and FTK Imager—to determine their success in the cloud.

4.2. Extracting Data From Amazon EC2

Extracting data from Amazon's EC2 implementation requires extra work. Here we explain what we learned and ultimately used to acquire forensic data. One choice for acquiring remote, persistent storage is to download a copy of the volume, or a snapshot thereof. Amazon stores virtual hard drives, called Elastic Block Storage (EBS) volumes, in its Simple Storage Service (S3), but they are not exposed to the end user for downloading.

Two options exist to obtain the data for an entire volume. The first is to create a snapshot from a drive being investigated, create a volume from that snapshot, attach the new volume read-only to a trusted Linux instance in EC2, and then create an ISO disk image of the volume that could be downloaded. The second is to detach the target volume from the host under investigation, attach it to a trusted Linux instance in EC2, and use a low-level copying utility (*e.g.*, the Unix data duplication tool *dd*) to create a block copy which can be stored in S3 and downloaded.

Amazon provides a service to export data from S3 onto a physical device and ship it to the requestor, but the customer must provide the storage device and is billed $80 per storage device handled plus $2.49 per data-loading-hour (Amazon Web Services, 2011).

In neither of these cases is it is possible to verify the integrity of the forensic disk image. Amazon does not provide checksums of volumes as they exist in their cloud, so one cannot positively assert that the image retrieved is identical to the original. Further, no hardware write blocker can be used to protect the integrity of the exhibit. However, it is possible to guarantee that the data have not been modified in transit (*e.g.*, hashing the image before export and again after it has arrived from shipping).

4.3. Methods

For each experiment, we used a non-cloud based standalone control machine to evaluate the success of the test. The control was a Dell workstation with 32-bit Windows 2008 R2, a single 30GB disk drive and 2GB RAM. We connected the machine to the Internet and installed the Apache web server. We created several web pages with identifying names and content. Some files were deleted. We artificially compromised the machine using a web-based vulnerability, and assumed that a criminal and forensic investigation had commenced. We imaged the drive with EnCase and FTK.

Experiment 1 tested the advertised ability of popular tools to collect forensic data remotely in the cloud at the guest OS (Layer 5). Success or failure would be measured by (a) if the tool was able to collect evidence remotely, and (b) how accurately the data compared to those from a standalone control machine. We prepared a single, Internet-connected (proxied), forensic examiner workstation with 64-bit Windows 7 Enterprise. EnCase Enterprise 6.11, including the SAFE (Secure Authentication For EnCase), was installed according to the manufacturer's instructions. FTK 3.2 was also installed. In Amazon EC2, we provisioned a new virtual machine to simulate the target of an investigation. This machine was an Amazon-provided Windows 2008 R2 32-bit image with a single 30GB disk drive and 1.7GB RAM. We configured the Amazon firewall to allow only Remote Desktop Protocol (RDP) (tcp/3389).

We connected to the target machine using RDP and proceeded to exercise normal behavior of a user configuring a webserver. We downloaded and installed Apache and created several web pages with identifying names and content. Some files were deleted. We again artificially compromised the machine using a web-based vulnerability and assumed that a criminal and forensic investigation had commenced.

EnCase Servlets and FTK Agents are the remote client programs that communicate with their host server controllers. Each can be deployed in a variety of ways. In a corporate environment, agents are typically deployed to Windows machines over the network using Windows file shares. The products also allow manual file delivery (*e.g.*, USB). In our experiment, we transferred the agent to the target virtual machine over RDP and executed it. We modified our firewall to allow communication with the agent: the EnCase servlet used tcp/4445 and the FTK agent used our user-defined port of tcp/3399.

We also tested FTK Imager Lite version 2.9.0. The product was copied over the Remote Desktop connection from the examiner's workstation and run interactively. FTK Imager Lite does not require installation, and runs self-sufficiently once uncompressed. For this experiment we attached a second 100 GB storage volume onto which we saved an image of the primary volume captured by FTK Imager.

Finally, we ran Fastdump, Memoryze and FTK Imager to acquire images of system memory, resulting in three 1.7GB images.

Experiment 2 tested popular forensic tools at the virtualization layer by injecting an agent into the virtual machine (Layer 4). Success or failure was again measured by (a) the ability of the tool to collect evidence, and (b) how accurate the data were compared to those from a standalone control machine. We prepared an installation of the Eucalyptus cloud platform (Eucalyptus, 2011) from the Ubuntu distribution on a Dell workstation. Eucalyptus supports the Xen hypervisor for managing virtual machines, and LibVMI (LibVMI, 2011) is a library for monitoring guest operating systems in Xen. We used the LibVMI library to write into memory of the guest virtual machine. With this capability, we demonstrated injecting an EnCase Servlet and FTK Agent directly into a running guest. As with *Experiment 1*, we communicated with the agent over the network.

Experiment 3 tested forensic acquisition at the host operating system level by exercising Amazon's Export feature (Layer 3). This experiment most closely resembles the process probably used to satisfy subpoenas and search warrants, since the data are exported from Amazon's internal network at a data center. Additionally, AWS maintains a chain of custody for the storage device while it is in its custody. We measured success or failure by (a) the ability of the technique to collect evidence, and (b) the accuracy of the data as compared to those from the standalone control machine. AWS Export involves a service request to Amazon and shipping them a storage device. Unfortunately, it is currently possible only to export data from an S3 bucket and not from an EBS volume. To meet that requirement, we attached the EBS volume from the compromised machine to a Linux VM, and used *dd* to store an image of the volume in an S3 bucket. We requested from AWS an export of this bucket, and shipped a Seagate FreeAgent eSATA external hard drive. The storage device was returned with a copy of the data.

4.4. Results

The manual installation of the EnCase Servlet and FTK Agent in *Experiment 1* was successful and we were able to acquire a hard drive and memory image remotely. Analyzing these images in EnCase Forensic and FTK Investigator respectively correctly revealed a timeline of activity, including the installation of Apache and the webpages we created and deleted. The analysis revealed no unusual artifacts of the virtual environment, nor any apparent anomalies to raise doubt about the integrity of the data. The speed of the acquisition process was limited by our learning how to use the remote agents and the network bandwidth to transfer the data. The later took approximately 12 hours each for EnCase and FTK to transfer the 30GB disk image and 2GB memory image using our university's OC-12 connection.

Experiment 2 successfully resulted in a complete image of the drive and a correct timeline. VM introspection is a powerful tool for forensics and allows live investigation of a host without revealing the presence of the investigator. However, introspection is a special feature which must be implemented by the cloud service provider. This was the only experiment where we were able to verify cryptographically the integrity of the image, since we had access to the physical disk and could compare hash values of the EnCase image and the original disk.

The AWS Export process in *Experiment 3* also successfully returned a complete image of the drive. We were able to load this drive into EnCase and FTK with no difficulties, and verified the contents of the drive. An added benefit of this method is that AWS generates a log report with metadata for each file exported. This report contained the following for each file: date and time of the transfer, location on the storage device, MD5 checksum, and number of bytes. These data are saved in an S3 bucket that we specified in the export request. Using expediated shipping, it took five days to receive our data, at a cost of $125. We imagine that this process would closely mimic the steps taken by AWS when complying with a search warrant or subpoena.

EnCase and FTK were easiest to use. Despite setup and learning time required to use the remote capabilities, the features of the tools were familiar and easy to execute. The 12-hour time required to retrieve our disk image was significantly shorter than the 120 hours required for the AWS Export process for this data volume. Downloading data achieved an average of 2.5 GB per hour. AWS Export spent 4 hours loading our data, while the remaining 116 hours were spent in transit. At these rates, the most time effective choice is the export process when more than 240 GB of data will be retrieved.

Table 2 summarizes the results of data acquisition in EC2. Each tool and technique successfully resulted in evidence production, but each requires substantial trust in the cloud infrastructure at all levels.

5. Alternatives for Forensic Acqisition

In this section we briefly propose four alternate solutions to acquiring cloud-based data: Trusted Platform Modules (TPMs), the cloud management plane, forensics-as-a-service, and contract support. The adoption of one or more of these alternatives would make remote acquisition more trustworthy than acquisition using EnCase or FTK since trust is rooted at lower cloud layers.

5.1. Rooting Trust with TPMs

The deployment of TPMs would root trust in cloud computing hardware. Several researchers have previously suggested this (Krautheim, 2010; Krautheim et al., 2010;

Experiment	Tool	Evidence Collected	Time (hrs)	Trust Required
1	EnCase	Success	12	OS, HV, Host, Hardware, Network
1	FTK	Success	12	OS, HV, Host, Hardware, Network
1	FTK Imager (disk)	Success	12	OS, HV, Host, Hardware, Network
1	Fastdump	Success	2	OS, HV, Host, Hardware, Network
1	Memoryze	Success	2	OS, HV, Host, Hardware, Network
1	FTK Imager (memory)	Success	2	OS, HV, Host, Hardware, Network
1	Volume Block Copy	Success	14	OS (imaging machine), HV, Host, Hardware, Network
2	Agent Injection	Success	1	HV, Host, Hardware, Network
3	AWS Export	Success	120	AWS Technician, Technician's Host, Hardware and Software, AWS Hardware, AWS Software

Table 2: Results of three experiments acquiring cloud-based forensic evidence using popular tools, including the time to retrieve the data and trust required in the guest operating system (OS), hypervisor (HV), host operating system, host hardware, network, and Amazon Web Services (AWS) components.

Santos et al., 2009; Sato et al., 2010). A TPM can provide one or more capabilities: machine authentication, hardware encryption, signing, secure key storage, and attestation. Previous solutions for TPMs in cloud computing focus on provisioning trusted guest VMs rather than on attestation of the host platform. If TPMs were installed in each cloud server, the hardware and associated software could validate what software is installed on each machine and verify the health and status of each machine. Despite this benefit and low cost, TPMs have limitations of their own and are not perfectly secure. It is still possible, for example, to modify a running process without detection by the TPM.

While appropriate for future consideration, we believe the primary hinderance to this approach today is that cloud vendors have large amounts of heterogeneous, commercial hardware which is replaced as needed rather than all at once, much of which does not have a TPM. While future hardware may include a TPM, the provider cannot guarantee that each server in its cloud has one today. Nevertheless, customer demand today or in the future may drive providers to introduce trusted hardware for some or all customers.

5.2. Collection from the Management Plane

Cloud computing has a powerful attribute that could be used to support trustworthy forensics: consumers manage and control virtual assets via a management plane, an out-of-band channel that interfaces with the cloud infrastructure. In Amazon Web Services, this system is called the AWS Management Console. This web-facing system interfaces with the provider's underlying filesystem and hypervisor, and is used to provision, start and stop virtual machines, and manipulate the firewall.

The management plane is particularly attractive because it is user driven. The provider, end users, and law enforcement could download log files, disk images, and packet captures from the management plane on demand. Further, with forensic acquisition occuring under the hypervisor, retrieving VM images and other data would require trust only in Layers 3 and below.

While attractive, this solution does require trust in the management plane, a potential vulnerability which does not exist with non-virtualized, physical computers. As a web-facing interface, the management plane opens a new attack surface which must be protected by the provider. Access to the management plane should be logged and strictly enforced with identity and access management. Communication between the user and the management plane endpoint should be done securely (*e.g.*, using SSL).

5.3. Forensic Support as a Service

Provider support for forensic acquisition is a natural choice. The provider is already pre-positioned to preserve and collect the data since they control the infrastructure, not only from a virtual machine, but also from infrastructure logging mechanisms, packet captures and billing records. Technology for remote acquisition would be moot if the provider and its infrastructure were trusted and the provider was willing and able to provide evidence to the investigator directly. At their choosing, providers could offer these services to their clients with little effort and cost. Voluntarily doing so would demonstrate their care for security, and put reluctant security-minded clients at ease knowing that investigation was possible. At least one provider, Terremark, offers forensic-as-a-service (Terremark, 2009). Potential drawbacks to a forensic support service include response time (potentially mitigated by the Service Level Agreement) and the provider's lack of knowledge about how customers are using the cloud to meet their goals.

Consider the following protocol for trust-preserving, provider-assisted evidence production. Law enforcement serves a cloud provider with a search warrant for data related to a particular IP address, including the client records for the user of that IP and the virtual machine serving content. A technician at the provider, certified as a forensic examiner by an independent third party, sits down at an offline forensic workstation connected to the backend cloud infrastructure. The provider executes the warrant and gathers the data requested, validating the data with cryptographic checksums. Among the data requested

are virtual machines, access logs from the Management Console, data provenance logs, netflow records for the requested IP, and firewall logs. The data are copied to media for law enforcement. This protocol works at Layer 3, which requires trust in the host operating system, hardware, network, and the technician in this case. Though the protocol still requires trust in the hardware (which could be mitigated by using a TPM), there are basic assurances that the operating system, network, and technician are trustworthy.

5.4. Legal Solutions

Laws could require investigative support from a cloud provider. Contrary to forensics-as-a-service, this support would be legally mandated and might take the form of entitlements to law enforcement for monitoring and surveillance of suspected criminal activity.

No provider has publically advertised the options for forensic collection available to law enforcement. It is unknown whether the Communications Assistance for Law Enforcement Act (CALEA) (United States Code, 1994), a federal law that codifies how telecommunication carriers must support law enforcement in wiretaps, or others like it might apply to cloud computing. CALEA demands certain technical interfaces on the part of the provider to facilitate this collection. Such capabilities are necessary if the courts decide that CALEA, or similar legislation, applies to cloud providers. Even if wiretaps are a sufficient legal instrument for collecting data, the technical implementation must make such collection easy.

We have begun to analyze the unique legal problems raised by the application of current law to cloud computing, particularly for search and seizure of data from cloud providers. These issues are intertwined with the technical ability to acquire data, and range from whose law governs cloud data to who can legally execute the warrant. This work will empower legal practitioners to understand how cloud crimes relate to traditional computer crimes, and give them the tools to prosecute such cases. An exemplar search warrant for cloud evidence would give law enforcement a starting point to request the relevant data from a provider.

6. Discussion

The nature of online remote forensics introduces security considerations. For example, a forensic examiner's workstation must have access to the Internet to acquire the evidence. While precautions such as firewalls and proxies may help shield the workstation from attack and compromise, the possibility of infection becomes more likely than if the workstation were standalone or on an isolated network. This risk must be accepted, or remediated with appropriate technology (*e.g.*, monitoring, patching).

One attractive feature of using existing tools which are executed by the examiner, as in *Experiment 1*, is that no changes to the cloud infrastructure are necessary, and no assistance from the provider is required. Introspection, as in *Experiment 2*, requires considerable change to the environment made by a provider, even though that feature could be exercised without the provider's intervention. Data export, as in *Experiment 3*, requires no change to the infrastructure, but must be executed by the provider.

Our experiments assume that the cloud consumer is the victim of the crime and the plantiff in the investigation. However, an equally likely scenario is one in which a criminal creates a system in the cloud, uses it to commit a crime, and removes the cloud system entirely. This situation demands proactive logging of data by the provider which may be of forensic relevance in the future. Shields, *et al.* (Shields et al., 2011) created a proof-of-concept continuous forensic evidence collection system that could be used to record the creation and deletion of cloud provisions. Finally, if the cloud provider is the criminal, the forensics service is also suspect and another alternative must be considered to investigate the crime.

A forensic shortcoming, and potential legal problem, is the lack of validation for the disk images. Forensic examiners are accustomed to using cryptographic hashes to validate that the copy of a hard drive that they have taken is identical to the original. With no hash available for the original data source, examiners and jurors are unlikely to accept the evidence. In our experiments, we were unable to verify cryptographically that our cloud images were identical to the standalone control because of differences such as different hardware (thus drivers) and network configurations. These differences did not affect the ability to reconstruct the crime.

The EnCase Servlet and FTK Agent used for our experiments had some limitations. These programs typically have System privileges, giving them unfettered access to memory and disks. However, as with all software, they are vulnerable to malicious code that may have already compromised the target machine. The agent could be installed at any time in the lifecycle of the virtual machine; installing at the time the VM is provisioned prevents the disruptive installation after an incident has taken place. Cloud providers such as Amazon employ user-configurable firewalls that must also be opened to allow the agents to communicate with the command and control node. Though not inherently a vulnerability, open ports do increase the attack surface. Fortunately, EnCase and FTK employ network encryption between the client and server to provide confidentiality and authentication.

Consumers must consider the cost associated with a remote forensic investigation. Imaging and retrieving a virtual hard drive and its associated memory will incur potentially significant bandwidth costs. Our experiment used an instance with a 30 GB virtual disk and 1.7 GB memory. Amazon currently bills outbound data transfer at $0.150 per GB, for the first 10 TB / month. Therefore, the retrieval of the disk and memory images totaled only $3.60. One TB of data would cost $150.

7. Conclusion

We have demonstrated that today's most widely used forensic tools are technically capable of remote acquisition of data in Amazon EC2. We have also shown that given the many layers of trust required, technology alone is insufficient to produce trustworthy data and solve the cloud forensic acquisition problem. The four alternatives we presented offer options that bridge technology and provider support.

Our recommendation for forensic acquisition of IaaS cloud computing is the management plane. This option offers the most attractive balance of speed and control with trust. We encourage cloud providers to make forensic data available to users in this way, and we have begun an implementation to do so. While EnCase and FTK successfully returned evidence, we do not recommend using them for remote forensics in the cloud because too much trust is required.

Several areas remain for future work. First, our experiments were specific to IaaS using EC2. These results do not carry to other cloud models and environments, such as Microsoft Azure or Google AppEngine, where forensic software cannot be installed and run as they can in EC2. Future work will be required to find suitable parallels on those platforms. Second, cloud users would benefit from consumer-driven forensic capabilities exposed to them by the provider. We intend to work with providers to allow clients to retrieve forensic logs and metadata (*e.g.*, cryptographic checksums of disk volumes) directly from the online management console. Third, solutions are needed to preserve evidence and prevent the loss of forensic evidence when cloud resources are released. Finally, we plan to further explore legal questions of acquisition, particularly those arising from Fourth Amendment concerns about search and seizure, jurisdiction, and ownership in future work.

Cloud computing is gaining momentum and where the people, the data, and the money go, so does crime. Our work lays a foundation and path to enable forensic examiners to take the initial steps in the forensic investigation of cloud-based crimes.

8. Acknowledgments

We would like to thank the anonymous reviewers for their helpful suggestions. We thank Simson Garfinkel for comments on early drafts. We wish to extend special thanks to Timothy Leschke and the Defense Cyber Crime Institute (DCCI) at the Department of Defense Cyber Crime Center (DC3) for the use of equipment and feedback on early drafts.

Sherman was supported in part by the Department of Defense under IASP grant H98230-11-1-0473. Dykstra was supported in part by an AWS in Education grant award.

References

Amazon Web Services . AWS Import/Export. Available at `http://aws.amazon.com/importexport/`; 2011. Last accessed December 28, 2011.

Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 2nd ed. Amsterdam: Elsevier Academic Press, 2004.

Conover M, Chiueh T. Code Injection From the Hypervisor: Removing the need for in-guest agents. In: Proceedings of Blackhat USA. 2008. Last accessed November 1, 2011.

Dolan-Gabitt B, Payne B, Lee W. Leveraging Forensic Tools for Virtual Machine Introspection. Technical Report, Georgia Institute of Technology, GT-CS-11-05; 2011.

Dykstra J, Sherman AT. Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies. In: Proceedings of the 2011 ADFSL Conference on Digital Forensics Security and Law. ASDFL; 2011a. p. 191–206.

Dykstra J, Sherman AT. Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies. Journal of Network Forensics 2011b;3(1):19–31.

Eucalyptus . Eucalyptus: The Open Source Cloud Platform. Available at `http://open.eucalyptus.com/`; 2011. Last accessed November 1, 2011.

Federal CIO Council . Guidelines for the Secure Use of Cloud Computing by Federal Departments and Agencies (Draft Version 0.41). 2011.

Garfinkel S. Forensic Feature Extraction and Cross-Drive Analysis. Digital Investigation 2006;3:71–81.

Garfinkel T, Rosenblum M. A virtual machine introspection based architecture for intrusion detection. In: Proceedings of the 10th Annual Symposium on Network and Distributed System Security (NDSS 2003). 2003. p. 191–206.

Giobbi R, McCormick J. Vulnerability Note VU912593: Guidance EnCase Enterprise uses weak authentication to identify target machines. Available at `http://www.kb.cert.org/vuls/id/912593`; 2007. Last accessed September 21, 2011.

Guidance Software . EnCase Legal Journal. Available at `http://www.guidancesoftware.com/DocumentRegistration.aspx?did=1000017380`; 2011. Last accessed September 21, 2011.

Heiser J. Remote forensics software. Gartner RAS Core Research Note G00171898; 2009.

Krautheim FJ. Building Trust into Utility Cloud Computing. Ph.D. thesis; Department of Electrical Engineering and Computer Science, University of Maryland, Baltimore County; Baltimore, Maryland; 2010.

Krautheim FJ, Phatak DS, Sherman AT. Trusted Virtual Environment Module: Managing Trust in Cloud Computing. In: 3rd International Conference on Trust and Trustworthy Computing. 2010. p. 211–27.

LibVMI . Virtual Machine Introspection (VMI) Tools. Available at `http://vmitools.sandia.gov/`; 2011. Last accessed November 1, 2011.

Nance K, Hay B, Bishop M. Investigating the Implications of Virtual Machine Introspection for Digital Forensics. In: Proceedings of the International Conference on Availability, Reliability and Security (ARES '09). 2009. p. 1024–9.

National Institute of Standards and Technology . Computer forensic tool testing (CFTT) project overview. Available at `http://www.cftt.nist.gov/project_overview.htm`; 2003. Last accessed September 21, 2011.

National Institute of Standards and Technology . Digital Data Acquisition Tool Specification. Available at `http://www.cftt.nist.gov/Pub-Draft-1-DDA-Require.pdf`; 2004. Last accessed September 21, 2011.

National Institute of Standards and Technology . Test Results for Digital Data Acquisition Tool: FTK Imager 2.5.3.14. Available at `http://www.ncjrs.gov/pdffiles1/nij/222982.pdf`; 2008. Last accessed September 21, 2011.

National Institute of Standards and Technology . Test Results for Digital Data Acquisition Tool: EnCase 6.5. Available at `http://`

www.ncjrs.gov/pdffiles1/nij/228226.pdf; 2009. Last accessed September 21, 2011.

National Institute of Standards and Technology . The NIST Definition of Cloud Computing. Available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf; 2011. Last accessed January 8, 2012.

Ruan K, Carthy J, Kechadi T, Crosbie M. Cloud forensics: An overview. In: Advances in Digital Forensics VII. 2011. .

Santana M. Cloud Security: Beyond the Buzz. Available at http://www.linuxworldexpo.com/storage/10/documents/CI7\%20Mario\%20Santana.pdf; 2009. Last accessed September 21, 2011.

Santos N, Gummadi K, Rodrigues R. Towards trusted cloud computing. In: Proceedings of USENIX HotCloud. 2009. p. 3–.

Sato H, Kanai A, Tanimoto S. A Cloud Trust Model in a Security Aware Cloud. In: Proceedings of the 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet. SAINT '10; 2010. p. 121–4.

SCMagazine . Best computer forensic tool. SCMagazine 2011;Last accessed November 1, 2011.

Shields C, Frieder O, Maloo M. A system for the proactive, continuous, and efcient collection of digital forensic evidence. In: The Proceedings of the Eleventh Annual DFRWS Conference. volume 8; 2011. p. S3–13.

Taylor M, Haggerty J, Gresty D, Lamb D. Forensic investigation of cloud computing systems. Network Security 2011;2011(3):4–10.

Terremark . Secure Information Services. Available at http://www.terremark.com/uploadedFiles/Services/Security_Services/TMRK_SIS_Gatefold2_4pagelayout_Screen.pdf; 2009. Last accessed November 1, 2011.

United States Code . Communications Assistance for Law Enforcement Act (CALEA). 47 USC 1001-1010; 1994.