Journal of Forensic Sciences And Criminal Investigation
ISSN: 2476-1311

Juniper Publishers key to the Researchers

Research Article
Volume - 10 Issue 1 - July 2018
DOI: 10.19080/JFSCI.2018.10.555778

J Forensic Sci & Criminal Inves

Current State of Forensic Acquisition for IaaS Cloud Services

Douglas A Orr [1]* and Peter White[2]

[1]*Department of Criminal Justice of North Georgia, USA.*

[2]*Champlain College, USA*

Submission: July 10, 2018; **Published:** July 18, 2018

***Corresponding author:** Douglas A Orr, Department of Criminal Justice, University of North Georgia, US, Tel: 7068673084; Email: Douglas.Orr@ung.edu

Abstract

Although research has been conducted to investigate a forensically sound acquisition of evidence from cloud systems, it has not, up to this point, reached a defined standard that can be referenced and agreed upon by digital forensic practitioners today. This paper explores that gap in available forensic procedures by studying the forensic acquisition of evidence from an Infrastructure as a Service (IaaS) cloud environment. IaaS cloud service are rapidly replacing standard IT services traditionally hosted in datacenters that provide physical access to servers and data storage. This paper reviews the general concepts of IaaS hosting and then reviews the published research with options to address the lack of established digital forensic options for acquisition. The paper then proposes a simplified methodology capable of capturing forensic data from an IaaS cloud. Cloud based services are rapidly replacing the traditional Information Technology services built on physical servers. The change is impacting both the platforms that services are hosted on as well as the makeup of organizations that are providing these services.

Many small organizations can now quickly move from their initial concept of a service to sell into the rollout of a large and complex technology stack in a matter of days. This is impacting both the technology used where physical servers are no longer purchased for building a technical infrastructure as well as the makeup of the personnel supporting this infrastructure where a team of one or two people can now replace what traditionally required a larger IT team. These small organizations supporting Internet based services often are unprepared for performing large scale incident response or digital forensics across the infrastructure they have built and segmented. Traditional methods of digital forensics that required physical access to devices are no longer possible with the cloud-based technology model. However, with a number of changes in methodology, it is possible to leverage the benefits of cloud-based infrastructure to rapidly perform a broad based forensic acquisition. In order to accomplish this, some of the more traditional foundations of digital forensics require evolution to work within the bounds of this new technology.

Cloud Background and Needed Forensic Solution

Cloud business services often have three, and sometimes four, basic types from the perspective of the customer. Starting from the most basic is Infrastructure as a Service (IaaS) where basic services, such as virtual servers, are provided to the customer. Next is Platform as a Service (PaaS) where a customer-built application, such as a web app, will be hosted by the cloud platform provider. Last is Software as a Service (SaaS) where a business software, such as a sales platform, is provided to the customer as a hosted service. When a complete business process is delivered from a cloud service, it is called Business Process as a Service (BPaaS) [1]. BPaaS is an extension of SaaS that includes the servicing of a business process from a software platform along with personnel to support the service. An example of BPaaS may include the outsourcing of a Human Resources business process. A breakdown of the market scale of each of these types of services can be seen in Table 1.

Infrastructure as a Service (IaaS) Cloud Services

The focus of this paper will be on Infrastructure as a Service (IaaS) platforms for a number of reasons. As seen in Table1, IaaS consists of a large portion of the cloud services market, although not the largest, it is the fastest growing sector of the cloud services market. Accordingly, by way of Gartner news source, "The worldwide infrastructure as a service (IaaS) public cloud market grew 31 percent in 2016" [2]. IaaS is the portion of the cloud market that is largely replacing the traditional IT infrastructure. That traditional IT infrastructure would have been the focus of previous digital forensic investigations and civil litigation discovery and would have required a digital forensic expert to present evidence obtained during those examinations in court. Due to the variation and complexity of the many IaaS based services that can be built by a cloud customer, it is not likely that evidence derived from these infrastructures could be interpreted effectively in a court of law apart from the testimony of an expert witness. The expert opinion of a digital forensic analyst would be necessary to understand and communicate to the court evidence obtained from these environments. In this way, IaaS is different from SaaS, PaaS, and BPaaS which will have a common structure across all customers as well as standardized processes.

Table 1: Worldwide Public Cloud Service Revenue Forecast.

Cloud Service Type	Forecast 2017 (Billions USD)
Cloud System Infrastructure Services (IaaS)	30
Cloud Application Services (SaaS)	60.2
Cloud Business Process Services (BPaaS)	42.6
Cloud Application Infrastructure Services (PaaS)	11.9
Cloud Management and Security Services	8.7

For those services (SaaS, PaaS, and BPaaS), standard business records such as log files created as part of an accurate and reliable process may make it possible for an expert on the business process being investigated, such as a cloud service administrator, to present this evidence in court as an expert based on rule 702 of the Federal Rules of Evidence. This is less likely for IaaS which operates at a lower level and would require a digital forensic expert to forensically acquire, understand, and interpret the evidence for the court. In addition to focusing on IaaS cloud services over other types of cloud services, the authors focus on one particular brand of IaaS over all others, namely the IaaS cloud service from Amazon, Amazon Web Services (AWS). Due is due primarily to its market share far ahead of other cloud providers and its position in leading the market in defining new cloud services. Where specific technical solutions are described or defined, these will be based on AWS for the sake of clarity. Although common management practices for IaaS are used, these can be modified to cover other IaaS services such as Microsoft Azure and others in the future. The reason for focusing on Amazon AWS can be seen in Table 2. below which highlights the market dominance of AWS in this space. AWS has by far the most mature and complete platform for providing IaaS services.

Table 2: IaaS Public Cloud Services Market Share.

IaaS Cloud Service Company	Market Share Percent 2016
Amazon AWS	44.2
Microsoft Azure	7.1
Alibaba	3
Google	2.3
Rackspace	2.2
Others	41.2

Review of Previous Research

The need for new digital forensic investigation capabilities to support cloud infrastructures is driven by the steady growth and usage of cloud IaaS replacing traditional corporate IT infrastructures. This migration to cloud services is a long-standing trend and is highlighted in McKinsey Research reports from 2010 describing how the Cloud is used to tackle complex challenges and control costs [3]. Today, this change is happening for organizations of all sizes whether they are smaller and leverage cloud services to grow quickly or if they are indeed larger and move toward cloud infrastructure for financial reasons. Although cloud services provide the ability to rapidly implement new systems, they remove the capability to directly access the physical hardware which was previously deemed a basic requirement for performing a digital forensic investigation. In dealing with this new reality, many researchers have been exploring the impact of this change.

Literature Review

Alenezi et al. [4]. call out the need for digital forensic readiness in organizations due to the increased number of security breaches of cloud environments, describing cloud environments as an attractive battleground for cybercrime and the need for digital forensic toolkits to access forensic-relevant data. Towards the objective of providing a measurement capability for cloud forensics readiness, they have proposed three categories of factors including Organizational, Technical, and Legal factors that will provide a measurement of the readiness of organizations to execute on a cloud forensic capability. As researchers investigate the new facets of cloud forensics, the categorization system provided by [4]. show how these fit in as building blocks of the whole comprehensive capability of cloud based digital forensics. At this stage, the limited guidance provided by NIST has not brought the understanding of how to execute cloud based digital forensics significantly forward [5]. The NIST draft report addressed cloud forensics by identifying a long list of existing challenges to digital forensics in the Cloud but has not to this point published a comprehensive and specific standard on how to approach digital forensics in the Cloud. This leaves digital forensic practitioners with limited guidance on how to proceed with their current cases that require a cloud-based digital forensic investigation.

Cloud Forensic Methodologies

With the lack of physical access to cloud systems, many researchers have performed extensive research aiming to resolve this issue with a new or modified methodology that solves this problem in a novel way. These attempts at proposing a new methodology generally fall into one of two groups. The first group focuses on the Cloud Service Provider as the means to resolving the physical access problem. As the Cloud Service Provider does have physical access to the cloud environment, they propose new requirements and expectations on the cloud service provider to fill the physical access gap with new tools. Examples of these methodologies include [6]. who propose a system for tracking the provenance of individual files. Their system is less applicable to IaaS and more aligned with other cloud services such as cloud file storage. It does, however, propose novel ways of meeting forensic requirements. Their model would implement a service that tracks file provenance though file hashing but is heavily dependent on the Cloud Service Provider for implementation and is also at odds with the cost management focus of cloud systems. [7]. also attempt to solve

How to cite this article: Douglas A Orr, Peter White. Current State of Forensic Acquisition for IaaS Cloud Services. J Forensic Sci & Criminal Inves 2018; 10(1): 555778. DOI: 10.19080/JFSCI.2018.10.555778.

the physical access problem by placing new requirements on the Cloud Service Provider.

They propose a set of changes to the operation of cloud services including two-factor authentication that fosters an environment prepared in advance for a digital forensic investigation. Other researchers have looked at the cloud environment in its current state and rather than proposing changes to how the environment operates, they have investigated options to work within the current restrictions of the cloud environment and still provide an effective digital forensic capability. The authors believe the guidance provided by these researchers is significantly more valuable to the digital forensic investigators of today who need current solutions for existing cases. Such persons, for example, are [8]. who add valuable insight into the process of performing forensics on cloud systems by adding a stage where an understanding of Background Technology is required. In their methodology, it is important for the digital forensic investigator to master a full understanding of the cloud environment and its background [8].

They identify that most cloud environments are purpose-built to operate with specific functionalities. Through their methodology, the digital forensic investigator must possess an understanding of the Client Side, Server Side, and Developer Side. These steps are clearly necessary as cloud environments are often built to run a defined function and are not generic systems such as laptops for which specific forensic artifacts are commonly understood. Due to cloud system's purpose built design, they do not lend themselves easily to a simple forensic process using a repeatable methodology. In cloud forensic investigations, it is much more common to have a customized environment where the digital forensic investigator will need to engage a subject matter expert on that particular environment. Other researchers have looked specifically at the digital forensic models that are in place.

This includes [9]. who referenced the models of [10]. and NIST [11]. identifying where these digital forensic models need to evolve in order to meet the needs of cloud based digital forensics. They propose a four-stage model including Evidence Source Identification and Preservation; Collection; Examination and Analysis; and Reporting & Presentation. The model focuses heavily on Law Enforcement Agency (LEA) access to evidence with a significant reliance on the Cloud Service Provider's retention of evidence through a preservation notice. This significantly limits the applicability and value of this model when attempting to apply it to other types of cases and cause the digital forensic investigator to be dependent on the cloud service provider.

Cloud Forensic Tools, Techniques, and Procedures

The digital forensic investigator will need to be armed with new tools, techniques, and procedures in order to perform an effective investigation of various cloud environments. A number of researchers have made progress identifying and defining the new set of challenges [12]. identify cloud infrastructure as a platform commonly used by cyber criminals to support the exploitation of their victims but also find that it would be difficult, if not impossible, to perform an investigation and discovery in the cloud environment without relying on Cloud Service Providers (CSPs). Therefore, dependence on the cloud service providers (CSPs) is ranked by them as the greatest challenge when investigators need to acquire evidence from cloud systems in a timely yet forensically sound manner. They also identify the lack of persistent storage in cloud services as a critical impediment to investigations which applies to both memory and virtual disks which can be lost irretrievably when a cloud system is powered down.

The solution they propose involves the use of agents to regularly collect forensic data including system and memory images that provide a comprehensive storage of digital forensic data [13]. propose a similar model of a prepared collection, acquisition, and preservation infrastructure but implemented as a service from the cloud service provider. Accordingly [14]. propose an agent-based solution that is intended to remove dependency on the Cloud Service Provider [15]. suggest that cloud forensics is best implemented as a set of services built into a forensic enabled cloud and succinctly focused on the capture and retention of log data as the critical factor toward achieving this. A number of researchers have proposed Virtual Machine Introspection as a forensic tool. These include [16] as well as [17] and [18]. Virtual Machine Introspection (VMI) is a technique for externally monitoring the runtime state of a system-level virtual machine [19].

While this would be a valuable tool for monitoring systems for purposes such as the detection of viruses, Federici (2013) identifies VMI as a risk to digital forensics of cloud systems in that the separate channel it would provide to access the memory of a cloud system would indeed significantly reduce the control the system administrator has over the cloud system and invalidate the digital evidence that can come from it. The authors agree with [20]. on this point and would instead highlight the point that, since the cloud service provider does not have access to read and modify the internal state of a cloud instance, the customer who controls that particular cloud instance can be certain of their ability to acquire the exact state of that system when necessary for digital forensic purposes [21]. highlight the criticality of capturing log data for cloud infrastructure and the value it can provide when investigating cyber threats.

They define a system based on Commercial off the Shelf (CotS) logging tools and show the value of data analysis when performing a cloud investigation [22]. explore the state of research into log-based forensics with particular applications to cloud forensics in more detail and stress the need for implementation of this service early as the cloud environment is being built. They also highlight the challenges that would be

How to cite this article: Douglas A Orr, Peter White. Current State of Forensic Acquisition for IaaS Cloud Services. J Forensic Sci & Criminal Inves 2018; 10(1): 555778. DOI: 10.19080/JFSCI.2018.10.555778.

posed if this data were unavailable [23]. expand on cloud based forensic logging by proposing a modular and comprehensive logging capability built into the management layer of the cloud. This would require it to be built and integrated by the Cloud Service Provider [24]. highlight the importance of isolating a cloud instance that is under investigation and describe a system for locating and isolating a cloud instance through cloud services.

Advances from Cloud Incident Response Research

Cloud Incident Response is an active area of research with a significantly larger number of researchers actively investigating ways to advance capabilities. As this research is highly applicable to the area of cloud forensics, it is valuable to highlight forensic capabilities built into cloud platforms by the Cloud Service Providers, as well as new tools and methods to apply to digital forensics [25]. outlines the basic structure for cloud forensics using tools built into cloud platforms to capture a volume snapshot from a compromised system, capturing valuable metadata from the cloud platform, and performing analysis on the cloud server using a cloud based forensic workstation [26]. expanded on this covering a more comprehensive and capable cloud forensic process by adding a process for isolating the cloud server and applying tagging to track evidence [27]. made available a set of tools presented at the annual Black Hat security conference allowing an investigator to automate many of the processes and procedures outlined by the earlier researchers as well as providing an advanced toolset for acquiring system memory from cloud servers [28].

Proposed IaaS Forensic Process Model

The authors address the complexities involved with performing digital forensics in a cloud environment with a focus on organizations that make use of large Infrastructure as a Service (IaaS) implementations of cloud-based services. The methodology assumes and requires the digital forensic investigator to have full access rights to the Cloud Services (CS) where the digital evidence resides and perform digital forensic collection by accessing those services [29-32]. Because of this requirement, the methodology is meant to primarily address situations involving incident response or civil litigation where full access rights to the Cloud Services are assumed and no direct physical access to the infrastructure is required. The many questions regarding the authority to seize and search cloud-based evidence are not within the scope of this paper and we will not address complex legal questions, such as cross-border issues, that can complicate digital forensics on cloud-based systems. In criminal investigations, it may be possible, however, to use a different methodology by addressing the Cloud Service Provider (CSP) through writ or summons and, in that way, collect digital forensic evidence of the CSP customer.

When those legal issues have been addressed through the courts in some way (granting legal access to the evidence) then the methodology outlined here may also be applicable toward digital forensic evidence collection from a cloud environment [33]. The methodology offered here addresses the acquisition of evidence in a cloud system based on the access rights of the Cloud Customer. The Cloud Customer will build and manage their cloud infrastructure through access to the Cloud Services with no direct physical control of the system where the evidence resides. As the methodology is only dependent on these Cloud Services, it will be labeled by the authors as the Cloud Services Based Methodology (CSBM) for digital forensic evidence acquisition and collection. The alternative would be to address the Cloud Service Provider (CSP) through writ or summons and collect digital forensic evidence of the Cloud Customer through the CSP. The authors suggest that the Cloud Services Based Methodology reasoning is to be preferred over the Cloud Service Provider Based Methodology as there is no dependency on the Cloud Service Provider to acquire and make available the evidence from the cloud servers [34].

Making Cloud-Based Acquisition Feasible for IaaS

The forensic methodology presented here is based on the usage of the AWS Command Line Interface (AWS CLI). The AWS CLI provides command-based access to all of the functions of the AWS Application Programming Interface. This is extremely beneficial to the forensic process. First, it provides a well-documented interface to the AWS infrastructure. Second, it is easily documented by the digital forensic investigator. The examples that follow will make use of this command interface. Third, the AWS infrastructure also provides extensive logging to any changes made to the infrastructure as well as activity-based logging for running services.

```
$ aws ec2 create-tags --resources i-INSTANCE-ID --tags "Key=CaseNumber, Value=123abc"
```

Figure 1.

In many cases, however, this logging needs to be enabled or the appropriate level of logging detail configured in advance for this evidence to be available to a digital forensic investigator [35-39]. As these settings are likely to be different in all cloud customer environments, it is beneficial for a set of logging best practices to be promulgated specifically supporting digital forensic investigations of cloud environments. Tagging is used throughout the management of cloud services to apply useful tracking information to data or configuration items. Tags should be used extensively by digital forensic investigators of cloud systems to track and identify the virtual pieces of evidence in a cloud environment. Tags can be applied using any Key Value pair such as is the case in the following example of tagging a case number to an AWS instance (Figure 1). Cloud tools can then be

How to cite this article: Douglas A Orr, Peter White. Current State of Forensic Acquisition for IaaS Cloud Services. J Forensic Sci & Criminal Inves 2018; 10(1): 555778. DOI: 10.19080/JFSCI.2018.10.555778.

used to take action on certain pieces of cloud-based evidence based on the tags applied to them.

System Metadata

A benefit of performing forensic investigations on cloud systems is that substantial amounts of logging and metadata are available to support the investigator. A critical command that will be useful in all investigations is the describe-instances command [40]. This will be used to capture base information on all instances in an AWS account used throughout the acquisition and investigation. This includes 1) the OS type and version necessary for the acquisition of memory from the running cloud instance; 2) the instance ID necessary to identify the instance for network isolation and capturing the attached volumes; and, 3) many other data points such as the system IP. This data is one of the first items that will need to be captured when performing a cloud forensic investigation. In yet another example we would describe all instances in the 'us-east-1' availability zone along with a sample of the potential output (Figure 2). The second command that will likely be used to capture information from a target system is the get-console-output command to capture the most recent data from the server console (Figure 3). The data returned from the get-console-output command is comparable to taking a picture of the console monitor of a running physical server [41]. An example of the data acquired is shown below in Figure 4. which includes the latest console messages from the system.

```
$ aws ec2 --region us-east-1 describe-instances

Output:
{
 "Instances": [
  {
   "StackId": "71c7ca72-55ae-4b6a-8ee1-a8dcded3fa0f",
   "PrivateDns": "ip-10-31-39-66.us-west-2.compute.internal",
   "LayerIds": [
    "26cf1d32-6876-42fa-bbf1-9cadc0bff938"
   ],
   "EbsOptimized": false,
   "ReportedOs": {
    "Version": "14.04",
    "Name": "ubuntu",
    "Family": "debian"
   },
   "Status": "online",
   "InstanceId": "4d6d1710-ded9-42a1-b08e-b043ad7af1e2",
   "SshKeyName": "US-West-2",
   "InfrastructureClass": "ec2",
   "RootDeviceVolumeId": "vol-d08ec6c1",
   "SubnetId": "subnet-b8de0ddd",
   "InstanceType": "t1.micro",
   "CreatedAt": "2017-02-24T20:52:49+00:00",
   "AmiId": "ami-35501205",
   "Hostname": "ip-192-0-2-0",
   "Ec2InstanceId": "i-5cd23551",
   "PublicDns": "ec2-192-0-2-0.us-west-2.compute.amazonaws.com",
```

Figure 2.

System volatile data collection

Capturing volatile system data over SSH will not vary in any way from the collection of a physical server. Data collection scripts and procedures used in other incident response scenarios can be used here. Key data to collect include open network connections, list of open files, and data on running processes.

How to cite this article: Douglas A Orr, Peter White. Current State of Forensic Acquisition for IaaS Cloud Services. J Forensic Sci & Criminal Inves 2018; 10(1): 555778. DOI: 10.19080/JFSCI.2018.10.555778.

Although much of this data can be acquired from memory analysis, there are cases where imaging memory from a system may cause it to crash [42-45]. Isolating the network of the system may also cause network connections to drop and there may also be instances where a packet capture is warranted on a compromised system prior to isolating it from the network. In these cases, it is valuable to access the system using a root level key and collect this data prior to network isolation and memory acquisition. When to do this is situationally specific. However, it is best done with a tested collection script and using validated system binaries when possible [46].

```
$ aws ec2 get-console-output --instance-id i-1234567890abcdef0
```

Figure 3.

```
i-1234567890abcdef0 [    0.000000] Command line: root=LABEL=/ console=tty1 console=ttyS0 selinux=0
nvme_core.io_timeout=4294967295
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
...
Cloud-init v. 0.7.6 finished at Wed, 09 May 2018 19:01:13 +0000. Datasource DataSourceEc2.  Up 21.50
seconds
Amazon Linux AMI release 2018.03
Kernel 4.14.26-46.32.amzn1.x86_64 on an x86_64
 2018-05-09T19:07:01.000Z
```

Figure 4.

System isolation

```
$ aws ec2 create-security-group --group-name isolation-sg --description "Forensic Isolation Security
Group" --vpc-id vpc-1a2b3c4d

Output:

{
  "GroupId": "sg-12345678"
}
```

Figure 5.

```
$ aws ec2 describe-security-groups --group-names isolation-sg

Output:

{
  "SecurityGroups": [
    {
      "IpPermissionsEgress": [],
      "Description": "Forensic Isolation Security Group "
      "IpPermissions": [],
      "GroupName": "isolation-sg",
      "OwnerId": "123456789012",
      "GroupId": "sg-12345678"
    }
  ]
}
```

Figure 6.

How to cite this article: Douglas A Orr, Peter White. Current State of Forensic Acquisition for IaaS Cloud Services. J Forensic Sci & Criminal Inves 2018; 10(1): 555778. DOI: 10.19080/JFSCI.2018.10.555778.

Once the investigation's target systems have been identified, the next immediate step is to isolate the instances from all unnecessary network communication. Cloud services provide an effective means to accomplish this through the use of Security Groups. In this step, the cloud instance will be isolated from all network traffic with the exception of SSH (tcp port 22) which will be allowed to log into the instance from a forensic acquisition system and extract a copy of the system memory [47]. No other network traffic would be allowed. The following command line will create a network isolation security group named 'isolation-sg' with a description of 'Forensic Isolation Security Group' and an example VPC ID of 'vpc-1a2b3c4d' although the real VPC ID will vary in each case (Figure 5). This creates the shell of the security group which will be later configured and applied to the instance. The command returns a GroupId which is assigned to the security group that was previously created. The GroupId created in the above example is used to configure and apply the security group to the instances which are our target for forensic acquisition (Figure 6). If the Group ID was not captured when it was returned by the create-security-group command, then it can be retrieved using the describe-security-groups command as shown below which affirms the configuration of the security group [48].

With the security group created, a network policy must now be added to allow SSH ingress from the forensic acquisition system. This is applied by referencing the Group Id of the security group. The example below assumes that the IP address of our forensic acquisition system is '10.1.2.3' (Figure 7). The isolation security group that has been created must now be applied to the instance that is being acquired. The following command would apply this security group to a specific instance based on the Instance ID (Figure 8). This command will supersede any previous security group configuration and, in effect, remove any previous network traffic that was allowed and only allow the network traffic that is allowed in the defined security group. At this point, the target instance is effectively network-isolated. It is now possible to SSH to the instance from a forensic acquisition system over the network for the purpose of acquiring volatile data and memory from the target system [49].

```
$ aws ec2 authorize-security-group-ingress --group-id sg-12345678 --protocol tcp --port 22 --cidr
10.1.2.3/32
```

Figure 7.

```
$ aws ec2 modify-instance-attribute --instance-id i-"4d6d1710-ded9-42a1-b08e-b043ad7af1e2" --groups
sg-12345678
```

Figure 8.

System Memory Acquisition

Recent advancements have made the acquisition of system memory from cloud instances significantly more accessible. This allows memory acquisition to be added to any cloud digital forensic process in a reliable and very straightforward way. Although there are commercial tools available for the acquisition of Windows memory from a running system, until recently, it has been difficult to acquire memory across the range of different Linux distributions running in AWS [50]. Linux memory acquisition was a critical stumbling block in cloud forensics as the great majority of cloud instances are running Linux. According to a recent comparison, Linux systems comprise 92% of AWS instances while Windows makes up the remaining 8%. The solution for cloud Linux memory acquisition stems from two open source projects. The LiME project, short for Linux Memory Extractor, is a toolset for building a Loadable Kernel Module that can reliably create a forensically sound memory dump with hashing.

```
$ margaritashotgun --server 10.31.39.66 --username root --key root_access.pem --module lime-3.13.0-
74-generic.ko --bucket memory_capture_bucket
```

Figure 9.

As the loadable kernel module is a system specific driver loaded onto a running system, it is necessary to have a complied kernel module for each kernel and system architecture. The need for a broad library of separate kernel modules has been addressed by Threat Response through the library of LiME kernel modules made available with their open source project Margarita Shotgun. Margarita Shotgun is a tool specifically built to enable memory acquisition from cloud instances and places said recovered memory image into an S3 bucket for storage and later analysis. An example of the Margarita Shotgun command line is shown below Figure 9. This shows the process for acquiring memory from a single instance, although the same process can be used to acquire memory from many cloud instances at once [51]. The necessary components are 1) the IP address of the instance to connect to; 2) a root level access key; 3) the lime kernel memory module to use from the library; and, 4) the S3 bucket where the memory image is stored.

How to cite this article: Douglas A Orr, Peter White. Current State of Forensic Acquisition for IaaS Cloud Services. J Forensic Sci & Criminal Inves 2018; 10(1): 555778. DOI: 10.19080/JFSCI.2018.10.555778.

System Storage Acquisition

```
$ aws ec2 describe-volumes

Output:

{
  "Volumes": [
    {
      "AvailabilityZone": "us-west-2a",
      "Attachments": [
        {
          "AttachTime": "2017-09-17T00:55:03.000Z",
          "InstanceId": "i-a071c394",
          "VolumeId": "vol-e11a5288",
          "State": "attached",
          "DeleteOnTermination": true,
          "Device": "/dev/sda1"
        }
      ],
      "VolumeType": "standard",
      "VolumeId": "vol-1234567890abcdef0",
      "State": "in-use",
      "SnapshotId": "snap-f23ec1c8",
      "CreateTime": "2017-09-17T00:55:03.000Z",
      "Size": 30
    },
  ]
}
```

Figure 10.

```
$ aws ec2 create-snapshot --volume-id vol-1234567890abcdef0 --description "Analyst Name CaseNo-123abc EvidenceNo-123abc"

Output:
```

Figure 11.

```
$ aws ec2 create-volume --snapshot-id snap-0123456789abcdefg
```

Figure 12.

Cloud management tools make the acquisition of storage volumes quick and easy as cloud services are focused on specific tools to manage this resource. The first step is to identify the volumes in use particularly those attached to the instances that are being investigated. To collect metadata on volumes, the describe-volumes command is used to capture all necessary information along with valuable metadata including creation and attach times (Figure 10). When the target volume is identified,

How to cite this article: Douglas A Orr, Peter White. Current State of Forensic Acquisition for IaaS Cloud Services. J Forensic Sci & Criminal Inves 2018; 10(1): 555778. DOI: 10.19080/JFSCI.2018.10.555778.

capturing the state of the volume is a straightforward task using the create-snapshot command (Figure 11). The volume ID is used to specify the volume to snapshot and appending the informational description text, such as analyst, case number, and evidence number, can be added using the description field [52]. Reconstituting the volume from the snapshot is also a simple task using the create-volume command by specifying the snapshot ID (Figure 12). This will create a new volume with a new volume ID which can then be attached to your cloud based forensic workstation.

Capturing Process and Function

For the forensic analyst to effectively analyze the cloud environment, it is necessary to capture additional background information on the design and function of the systems involved. This investigation should include System Developer Interviews to capture the detailed function of the systems and processes being investigated. Along with the interviews, it is necessary to gather available system design documentation to support the analysis and presentation phases of the investigation. In addition, automated build processes are often used when creating cloud instances and deploying new code to these systems [53]. These automated build processes will potentially provide a detailed timeline of the planned changes to the system and software on the instance being investigated and provide a valuable source for supporting information.

Forensic Analysis

We do not focus on the forensic analysis process here. Once the acquisition of cloud evidence has been completed, the forensic analysis process can progress in much the same way as it would for physical systems. However, some benefits of cloud forensic analysis should be highlighted here. The first point is the ease with which snapshots of volumes can be recreated and attached to a forensic workstation running in the Cloud. This allows volumes to be immediately analyzed if the investigation is still at a triage stage or to create and image files on the volume to be removed from the cloud environment. The investigation of cloud-based systems also allows the digital forensic investigator to create an exact clone of the entire system environment being investigated [54]. This goes beyond creating a virtual machine from a single system as the complete environment can be recreated from the cloud configuration and data storage allowing the systems being investigated, along with their supporting servers, to be launched into a segregated environment [55]. Particularly in cases of system compromise where malware may remain on the compromised systems, this may be a valuable tool for investigators [56].

Limitations

Indeed, our methodology lacks the ability to capture detailed historical forensic data as described in the previous research of some researchers. However, the target of the methodology here is on developing a practical and pragmatic solution for forensic acquisition of cloud systems to be executed in any environment. The one particular weakness of this methodology is that the value of the forensic data available is highly dependent on the acquisition and retention of logs from the cloud environment. As this must be configured in advance of an investigation, it is largely out of the direct control of the forensic investigator.

Conclusion

Presented here is a methodology for digital forensic acquisition of an AWS cloud environment based on the best tools and services available today. It provides direction and guidance to digital forensic investigators who have cases involving AWS cloud environments. Based on the tools and processes available, we suggest it is possible to execute a forensic acquisition in an AWS cloud environment comparable to a physical acquisition of servers from a datacenter.

References

1. Gandhi B (2011) Business Process as a Service (BPaaS) delivered from the cloud. IBM Cloud Computing News.
2. Meulen R, Pettey C (2017) Gartner Says Worldwide IaaS Public Cloud Services Market Grew 31 Percent in 2016. Gartner Press Release.
3. Bughin J, Chui M, Manyika J (2010) Clouds, big data, and smart assets: Ten tech-enabled business trends to watch. McKinsey quarterly 56(1): 75-86.
4. Alenezi A, Hussein RK, Walters RJ, Wills GB (2017) A Framework for Cloud Forensic Readiness in Organizations. In Mobile Cloud Computing, Services, and Engineering (Mobile Cloud), 2017 5th IEEE International Conference on 199-204.
5. Mell P, Grance T (2014) Nist cloud computing forensic science challenges. Draft Nistir, 8006.
6. Aung NA, Min MM (2014) Cloud Forensic Investigation using Digital Provenance Scheme. ICAET, Singapore p. 29-30.
7. Damshenas M, Dehghantanha A, Mahmoud R, Bin Shamsuddin S (2013) Cloud computing and conflicts with digital forensic investigation. International Journal of Digital Content Technology and its Applications 7(9): 543.
8. Datta S, Majumder K, De D (2016) Review on Cloud Forensics: An Open Discussion on Challenges and Capabilities. International Journal of Computer Applications 145(1).
9. Martini B, Choo KKR (2012) An integrated conceptual digital forensic framework for cloud computing. Digital Investigation 9(2): 71-80.
10. McKemmish R (1999) What is forensic computing ? Trends & Issues in Crime and Criminal Justice 118: 1-6.
11. Kent K, Chevalier S, Grance T, Dang H (2006) Guide to integrating forensic techniques into incident response. SP800–86. Department of Commerce, Gaithersburg, USA.
12. Alqahtany S, Clarke N, Furnell S, Reich C (2016) A Forensic Acquisition and Analysis System for IaaS. Cluster Computing 19(1): 439-453.
13. Eleyan A, Eleyan D (2015) Forensic Process as a Service (FPaaS) for Cloud Computing. In Intelligence and Security Informatics Conference (EISIC) European pp. 157-160.
14. Kebande VR, Venter HS (2018) On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges. Australian Journal of Forensic Sciences 50(2): 209-238.

How to cite this article: Douglas A Orr, Peter White. Current State of Forensic Acquisition for IaaS Cloud Services. J Forensic Sci & Criminal Inves 2018; 10(1): 555778. DOI: 10.19080/JFSCI.2018.10.555778.

15. Liu C, Singhal A, Wijesekera D (2017) Identifying evidence for implementing a cloud forensic analysis framework. In Orlando, Florida: Accepted by IFIP International Conference Digital Forensics.

16. Baboo CDSS, Megalai SM (2015) Cyber Forensic Investigation and Exploration on Cloud Computing Environment. Global Journal of Computer Science and Technology 15(1).

17. Poisel R, Malzer E, Tjoa S (2013) Evidence and Cloud Computing: The Virtual Machine Introspection Approach. JoWUA 4(1): 135-152.

18. Farina J, Scanlon M, Le Khac NA, Kechadi MT (2015) Overview of the forensic investigation of cloud services. In Availability, Reliability and Security (ARES), 2015 10th International Conference on 556-565 IEEE.

19. Payne BD (2011) Virtual Machine Introspection. In Encyclopedia of Cryptography and Security 1360-1362.

20. Federici C (2013) Alma Nebula: a computer forensics framework for the Cloud. Procedia Computer Science 19: 139-146.

21. Irfan M, Abbas H, Sun Y, Sajid A, Pasha M (2016) A framework for cloud forensics evidence collection and analysis using security information and event management. Security and Communication Networks 9(16): 3790-3807.

22. Khan S, Gani A, Wahab AWA, Bagiwa MA, Shiraz M, et al. (2016) Cloud log forensics: Foundations, state of the art, and future directions. ACM Computing Surveys (CSUR) 49(1): 7.

23. Khan S, Gani A, Wahab AWA, Bagiwa MA, Shiraz M, et al. (2016) Cloud log forensics: Foundations, state of the art, and future directions. ACM Computing Surveys (CSUR) 49(1): 7.

24. Delport W, Olivier M (2012) Isolating instances in cloud forensics. In IFIP International Conference on Digital Forensics pp. 187-200.

25. Mogull R (2014) Cloud Forensics 101. Securosis Blog.

26. De La Fuente T (2016) Forensics in AWS: an introduction. Blyx Blog.

27. Krug A, McCormack A, Ferrier J, Parr J (2016) Hardening AWS Environments and Automating Incident Response for AWS Compromises. Blackhat USA 2016 Las Vegas, NV, USA.

28. Price D (2018) The True Market Shares of Windows vs. Linux Compared.

29. Moore S, Meulen R (2018) Gartner Forecasts Worldwide Public Cloud Revenue to Grow 21.4 Percent in 2018. Gartner Press Release.

30. Peterson G, Shenoi S (Eds.) (2012) Isolating Instances In Cloud Forensics. Advances in Digital Forensics VIII: 8th IFIP WG 11.9 International Conference on Digital Forensics, Pretoria, South Africa 383: 187-200.

31. Pichan A, Lazarescu M, Soh ST (2015) Cloud forensics: Technical challenges, solutions and comparative analysis. Digital Investigation 13: 38-57.

32. Plunkett J, Le Khac NA, Kechadi T (2015) Digital Forensic Investigations in the Cloud: A Proposed Approach for Irish Law Enforcement: 26-28.

33. Poisel R, Tjoa S (2012) Discussion on the challenges and opportunities of cloud forensics. In International Conference on Availability, Reliability, and Security 593-608.

34. Purnaye P, Jyotinagar V Cloud forensics: Volatile data preservation. International Journal of Computer Science Engineering 1(1): 41-43.

35. Rani DR, Sultana SN, Sravani PL (2016) Challenges of digital forensics in cloud computing environment. Indian Journal of Science and Technology 9(17).

36. Shirude D, Soman S, Paranjape V, Pradhan G (2017) Cloud Forensics: Drawbacks in Current Methodologies and Proposed Solution. International Journal of Engineering Research and Applications 7(2): 79-81.

37. Simou S, Kalloniatis C, Kavakli E, Gritzalis S (2014) Cloud forensics solutions: A review. In International Conference on Advanced Information Systems Engineering 299-309.

38. Zawoad S, Hasan R, Skjellum A (2015) OCF: an open cloud forensics model for reliable digital forensics. In Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on pp. 437-444.

39. Zawoad S, Hasan R, Skjellum A (2016) Towards Achieving Reliable Digital Forensics In IAAS And STAAS Clouds Using The Open Cloud Forensics Model 4(3).

40. Access Keys. In AWS, an access key consists of a Key ID and a Secret Access Key. It is used for authentication by the cloud customer to access the cloud environment.

41. Availability Zone. A location where Amazon AWS services are hosted. A region, such as 'us-east' would correspond to a specific datacenter, and availability zones, such as 'us-east-1' or 'us-east-2' would correspond to independent sections of that datacenter.

42. CloudTrail. A service that enables governance, compliance, operational auditing, and risk auditing of your AWS account through logging of event history.

43. Direct Connect. A dedicated network connection from a cloud customer to AWS.

44. Elastic Block Store (EBS). Provides persistent block storage volumes for use with Amazon EC2 instances.

45. Elastic Compute Cloud (EC2). Provides a web service to build and manage compute services in AWS.

46. Guard Duty. A managed threat detection service that continuously monitors for malicious or unauthorized behavior.

47. Identity and Access Management (IAM). A service allowing cloud customers to create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources.

48. Instance(s). A virtual server in Amazon's Elastic Compute Cloud (EC2).

49. Kernel Module. Code that can be loaded into the kernel on demand, extending the function of the kernel without the need to reboot the system.

50. Object Storage. A storage architecture that manages data as objects, as opposed to file systems that manage data as files, or block storage which manages data as blocks on a storage drive.

51. S3 Storage. Simple Storage Service from AWS, providing an object storage service allowing storage, retrieval, redundancy, and monitoring of access.

52. Security Group. Act as a virtual firewall allowing the configuration of inbound or outbound network traffic rules.

53. Tag. Tagging. A key value pair that can have customer defined values which is used for tracking configuration objects in AWS cloud.

54. Virtual Private Cloud (VPC). A logically isolated section of the AWS cloud that is configured by the cloud customer.

55. VPC Flow Logs. Captures IP traffic information to and from virtual network interfaces in the AWS cloud.

56. Volume Snapshot. Captures a point in time snapshot of an EBS volume and can be triggered by a cloud customer on demand.

How to cite this article: Douglas A Orr, Peter White. Current State of Forensic Acquisition for IaaS Cloud Services. J Forensic Sci & Criminal Inves 2018; 10(1): 555778. DOI: 10.19080/JFSCI.2018.10.555778.

DOI: 10.19080/JFSCI.2018.10.555778

How to cite this article: Douglas A Orr, Peter White. Current State of Forensic Acquisition for IaaS Cloud Services. J Forensic Sci & Criminal Inves 2018; 10(1): 555778. DOI: 10.19080/JFSCI.2018.10.555778.