Getting Lost in the Cloud (Computing)

By: Alex T. Bang
Robert Osgood
George Rodriguez

Scenario 1

You are a Detective with the Fairfax County Police Department (FCPD) working a child exploitation case. Your subject is using a remote storage site to protect and distribute his art work. You gained access to the site in a covert capacity and there over 80 gigabytes of images on the site. The Cloud Service Provider (CSP), Lugal, Inc., provides this service worldwide and has facilities in six countries: China, Kazakhstan, India, Romania, Italy, and Trenton, N.J. Lugal is a fee-for-service provider (unlike a Facebook or MySpace), however, the administrators at Lugal are having difficulty in determining exactly where your subject's images are being stored due to the dynamic data management schema used by Lugal. Your subject has used falsified personal identifying information (PII) to establish the site and pay the monthly bill ($15.00). Also, should the data reside in either China or Kazakhstan, evidence retrieval will be difficult since there are no Mutual Legal Assistance Treaties with either of these countries.

Scenario 2

You are an FBI Agent working a complicated and convoluted economic espionage case. Your subjects, a Group of 12 situated in seven countries (U. S., Mexico, Morocco, Brussels, Pakistan, Cuba, and the Ukraine), have illegally obtained over 50 terabytes (no let's make more challenging – 50 Petabytes) of data from dozens of victim companies. All of these companies are doing advanced applied research in the area of high speed mobile communications that will increase wide area bandwidth by a factor of 100 revolutionizing the data communications industry. This research is worth billions. The Group of 12 is operating under the guise of several straw companies, and they are moving the stolen data through Amazon Web Services (AWS).

Scenario 3

You are an internal investigator with the Suminomo Corporation, and you are based in San Francisco, California. The FBI has approached you concerning an international money laundering operation where your company is being used as a pass-through; however, last year, March 2011, your company outsourced all of its Information Technology (IT) to an

international CSP Nubes Cogitare (NC). NC is headquartered in Florence, Italy, but its remote storage facilities are in Bulgaria and Iran.

Scenario 4

You are a member of the San Diego Joint Terrorism Task Force (SD-JTTF) and have just received a call from the Principal of the Los Tiburones Middle School, El Cajon, California. The Principal states that she has received both a telephone call and an email that threatens to detonate a bomb on school grounds. The Caller ID on the phone number (619-555-9457) comes back to a prepaid phone and the email address is hosted by a company located in Venezuela.

All of the above scenarios are fictitious, but all could very easily be true. All involve Cloud Computing in some way, but each scenario may be dealt with differently depending upon a few factors to include the type of cloud service.

What is Cloud Computing?

The National Institute of Standards and Technology (NIST) probably has the most comprehensive definition of cloud computing, but before we take a look at NIST's definition, let's take a look at the Bob definition: Cloud Computing is Internet based remote computing services (RCS).

O.K., my definition isn't as grand, and I am definitely not getting paid by the word, but the problem with technology is someone is always trying to rebrand something in order to obtain some marketing objective. Cloud services have been available for many years. What has not been available until recently, is the general consumerism of the Cloud. If you own an iPhone, and iPad, or a Mac, there is a good chance that you are using the cloud (iTunes and/or iCloud (formerly MobileMe)[1]. So, any Terry, Diane, or Harriet can use and is using cloud services today and is doing so for little or no cost.

What are Cloud Services?

According to NIST[2], Cloud Computing is defined as: a model for enabling pervasive, convenient, on-demand network access to a shared pool of configurable computing resources

[1] iTunes and iCloud are products of Apple Computer. iTunes is their ground breaking music and video delivery service, and iCloud is Apple's remote storage solution.
[2] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

(e.g., networks, servers, storage, applications, and services) that can be quickly configured and deployed without any significant management effort or service provider interaction. There are five essential characteristics outlined by NIST that Cloud computing must have:

- On-demand self-service, where consumers can exercise autonomy in accessing the cloud and provisioning capabilities without relying on the CSP.
- Broad network access, where capabilities are delivered over commonly available platforms (i.e. the Web or mobile device).
- Resource pooling, where provider computing resources are pooled to serve multiple consumers using a multi-tenant arraignment.
- Rapid elasticity, where capabilities can be dynamically provisioned quickly both outward and inward.
- Measured service, where resource usage can be monitored, controlled, reported, automatically optimized, and subsequently billed.[3]

Although NIST only documents three service models, **Software as a Service (SaaS)**, **Platform as a Service (PaaS)**, and **Infrastructure as a Service (IaaS),** there are more service models that are less known such as **Forensics as a Service (FraaS)**, **Storage as a Service (StaaS) and Gaming as a Service (GaaS)**

- SaaS: In this type of service, the customer does not have control or access to the underlying cloud infrastructure to include servers, operating system, and storage or system capabilities. The customer usually has access to the applications purchased for use. The customer would most likely access the software via a browser or thin client. Web based email would fit this service model.

- PaaS: The customer has increased control over software, but no control of infrastructure or processors, memory, storage, or switches. The customer in this type of service can use or configure the applications on the cloud with CSPs tools. An example of PaaS is some online courses offer virtualized desktops where students can conduct programming in various development environments and operating systems featuring all necessary tools and applications. Typically the customer would access this environment through a remote desktop or some other access front end.

- IaaS: The customer has control of the processors, memory, storage, and switches per service level agreement (SLA) but does not have access to the underlying hardware or hypervisor. In many, but not all cases, the customer would have full

[3] Even free services cost something to someone.

access to a virtual machine (VM). The customer could install and store whatever he/she wanted on that system.

- FraaS: The customer, or the government, can obtain forensic resources from the CSP. More on FraaS later.

- StaaS: The customer leases storage space from the CSP. In the enterprise, StaaS vendors are targeting secondary storage applications by promoting StaaS as a convenient way to manage backups. The key advantage to StaaS is cost savings (personnel, hardware, and physical space). As an example, a company could choose to use StaaS instead of maintaining its own tape library or storage facility. The customer would enter into an SLA whereby the StaaS provider agrees to lease storage space on a fee per gigabyte and/or fee per transaction basis and the customer's data would be automatically transferred. The transfer can occur over the Internet or by private network. StaaS is generally seen as a good alternative for small or mid-sized businesses that lack the resources to implement and maintain their own storage infrastructure. StaaS also provides continuity of operations (COOP) alternatives by mitigating some of the risks in disaster recovery and providing long-term records retention.[4] StaaS has been consumerized through Apple's iCloud and Google Cloud Storage. With iCloud, owners of iPhones and iPads are automatically given free iCloud accounts for the purpose of backing up iTunes and other data.

- GaaS: The customer has direct on-demand access to games onto his/her computer through the use of a thin client. The actual game is stored on the operator's or game company's server and is streamed directly to computers accessing the server through the client. This is similar to video on demand only with interaction.[5] GaaS could be considered a subset of SaaS, but the gaming is so large that a separate distinction is warranted.

These service models are sold to customers by CSPs. CSPs can configure, provide, and allocate available processors, memory, storage, and switches to customers according to their SLAs. An SLA is the contract for service performance negotiated between you and a service provider. In the early days of cloud computing, all SLAs were negotiated between a client and the provider. Today with the advent of large utility-like cloud computing providers, most SLAs are standardized until a client becomes a large consumer of services.

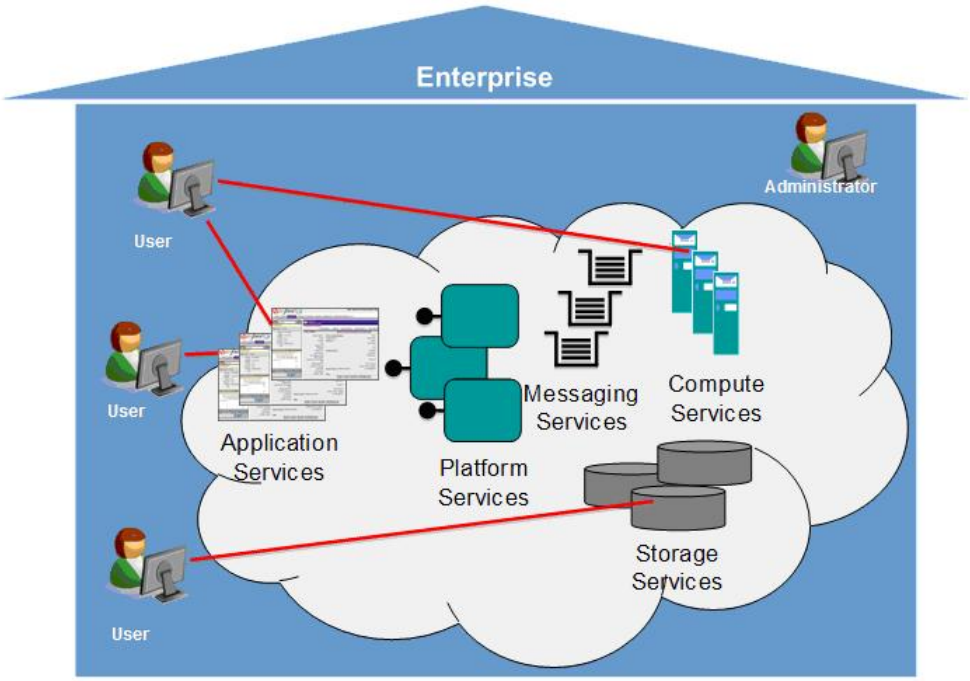
[4] http://searchstorage.techtarget.com/definition/Storage-as-a-Service-SaaS
[5] http://en.wikipedia.org/wiki/Cloud_gaming

How are Cloud Services Delivered?

Cloud services can be delivered in one of several ways.[6]

Private Cloud

The Private Cloud is intended for exclusive use by a single entity or an organization. The cloud infrastructure is internal to the organization, but could be managed by a third party. Generally speaking, such services would be provided over an intranet behind a firewall and/or with access via Virtual Private Network (VPN). Resources are dedicated and local to the organization. Generally, law enforcement would handle a private cloud the same for collection/seizure purposes as they would a traditional search of an office or residence with one proviso: law enforcement needs to be ready to potentially seize petabytes or even exabytes of data or a specific set of data depending on the evidentiary needs of the case and the storage capacity of the private cloud.

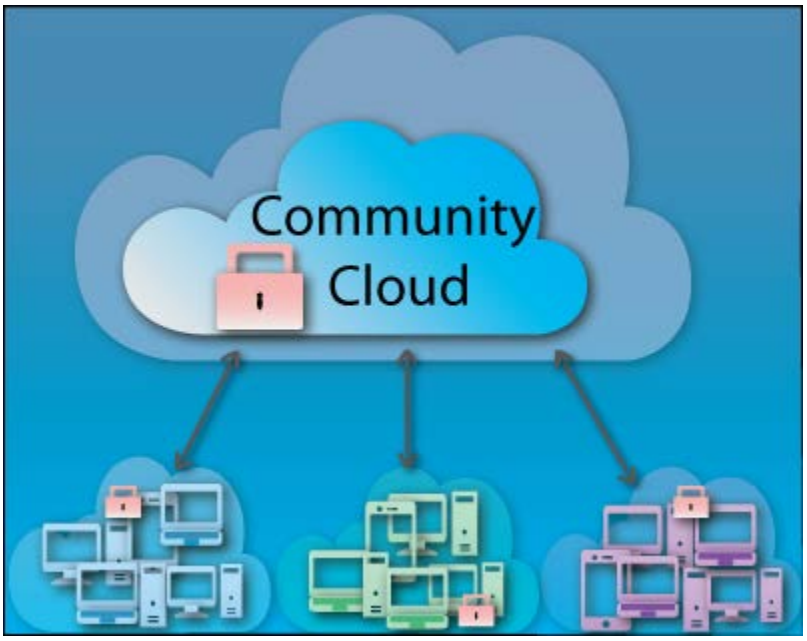


Private Cloud[7]

[6] http://csrc.nist.gov/publications/nistpub/800-145/SP800-145.pdf, National Institute of Standards and Technology, Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011.
[7] https://www.ibm.com/developerworks/mydeveloperworks/blogs/c2028fdc-41fe-4493-8257-33a59069fa04/entry/september_19_2010_1_45_pm7?lang=en

Community Cloud

A Community Cloud is shared by multiple organizations that have shared requirements. Amazon's AWS GovCloud(US) allows U.S. Government agencies and contractors to move more sensitive workloads into the Cloud that is physically and logically accessible by U.S. persons only. Law enforcement will need to work with the CSP where this delivery model is used. With a community cloud, data could be centrally located, but most likely data will be distributed over more than one physical location. Even if the community cloud is located in one physical location, coordination with the CSP is critical considering potential proprietary nature of the cloud configuration. To put it more succinctly, in what VM, on what server, in what rack, in what row, in what building is the evidence.



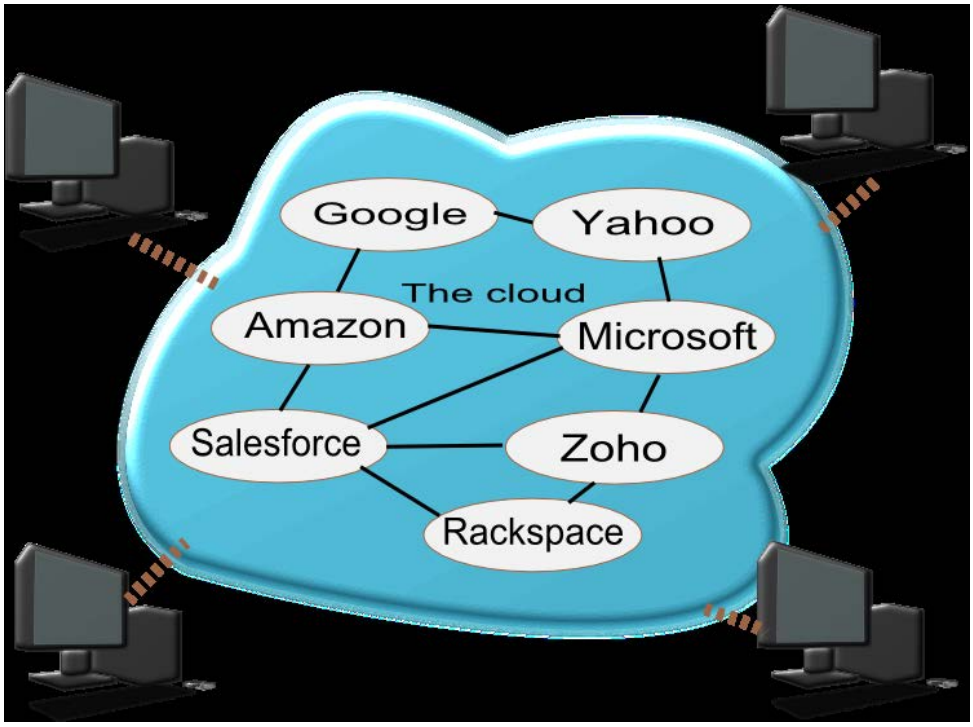
Department of Commerce Department of Education Department of Interior
Community Cloud[8]

Public Cloud

A Public Cloud is one that is available to the general public with the access to the Internet. A public cloud is what most consumers are exposed to. Apple's iCloud and Google's Cloud Platform are examples of public clouds. For law enforcement, the public cloud offers the most challenge. Not only is evidence geographically disperse, it may now be located in foreign country further complicating collection requirements. There is also a possibility that the CSP

[8] http://www.atomrain.com/it/technology/dissecting-cloud-iv-community-clouds

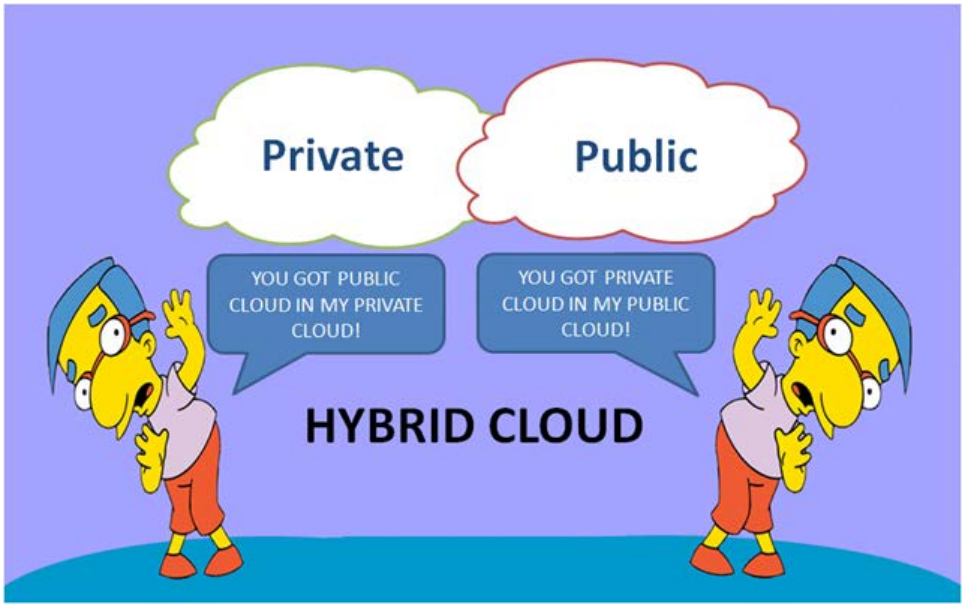
may not know the physical location of the evidence (I'm using the words evidence and data interchangeably here) or locating a particular piece of evidence may now be a major research project.



Public Cloud

Hybrid Cloud

A Hybrid Cloud is a composition of two or more distinct Cloud infrastructures. I don't have a good example here but you get the meaning. The main law enforcement challenge here is figuring out on what side (public or private) the evidence resides.



Hybrid Cloud[9]

Cloud in a Box

Cloud in a Box is really part of private cloud delivery, but I feel it deserves its own moment in the sun. Cloud in a Box (or Cloud in a Can[10]) is a turnkey solution offered by several vendors that make it easier for a customer to run self-service applications on hardware specifically optimized for those applications. You essentially buy pre-configured computer, plug it into your network, and voila you are running your cloud.[11] Law enforcement can generally deploy standard digital collection procedures when faced with cloud in a box with same proviso as the private cloud.

[9] http://blog.datacentermapping.com/2012/08/03/is-private-cloud-hosting-the-better-option/
[10] http://searchcloudcomputing.techtarget.com/definition/cloud-in-a-can-cloud-in-a-box
[11] Nothing is really that easy, but you get the idea.

Private / Public Cloud Comparison

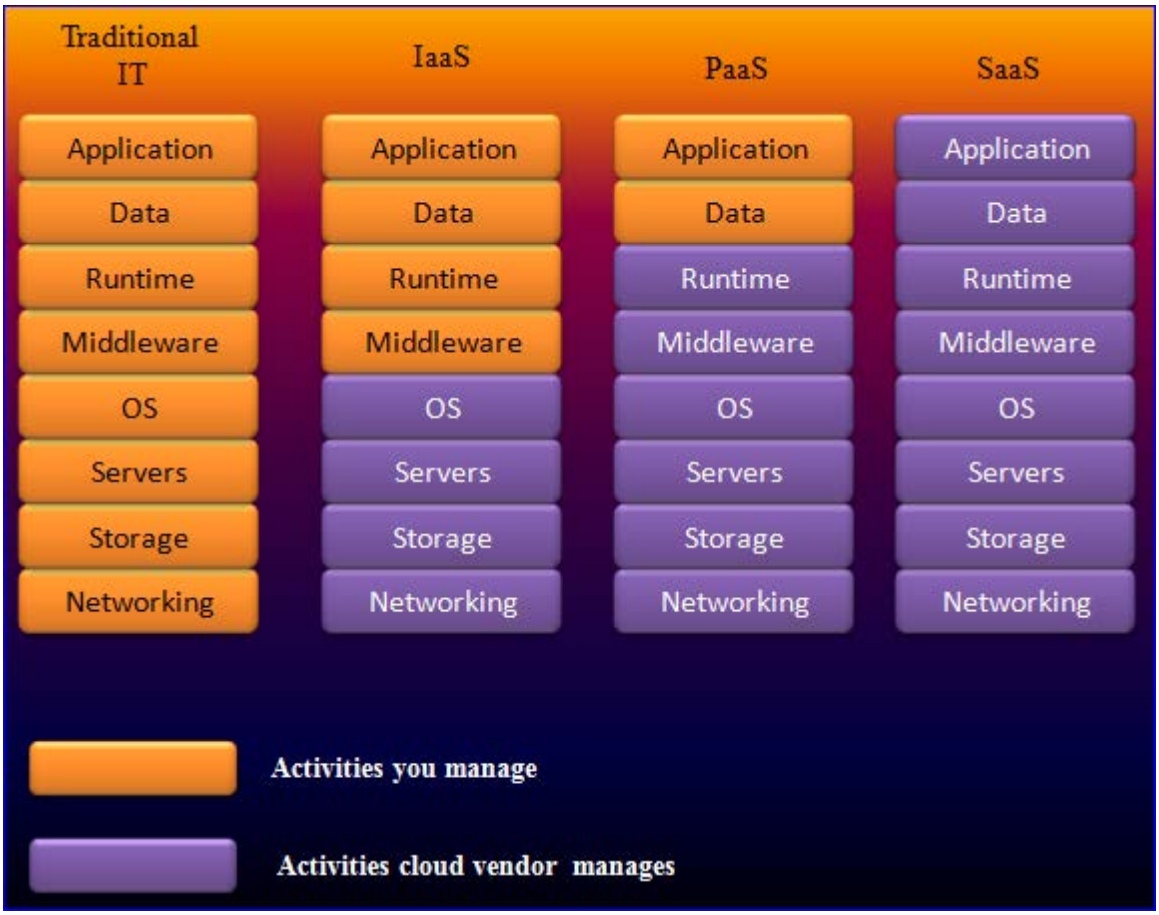
The table below contains the major differences between a public and private cloud.

	Public Cloud	Private Cloud
Owner	Third Party	Enterprise
Scalability	On-Demand and only limited by CSP	Limited by installed infrastructure, can be increased with adding equipment
Control and Management	SLA dependent	High level of control over resources, possible third party management
Cost	Lower cost	Higher Cost
Performance	Hard to achieve performance, dependent on SLA with CSP and other factors	Guarantee performance as supported/limited by your infrastructure
Security	CSP dependent	Depends on your internal security posture

Who has Control?

Whether the computers are virtualized or physical is an important factor to consider in an investigation of illegal activity, but just as important is who controls what, the CSP or the customer (criminal). SaaS provides the least control to the customer, and administrators that have access to traditional IT systems or onsite private clouds have the most control. The level of control is determined by analyzing the specific situation[12]. The following table illustrates the activities that the user/client manages. Users/clients that employ the private model with their own equipment (onsite) have the same level of control and manage the same resources of those that employ traditional IT infrastructure.

[12] http://cloudswave.com/blog/an-unusual-lesson-in-economics/



Who has control?

Why Are Cloud Services so Cost Effective Today?

Data centers have been around since Moses was a junior programmer at IBM, so why all of a sudden is Cloud Computing so cost effective. Your data still needs electricity, air conditioning, servers, storage, and bandwidth to run. The answer is virtualization.

So what is virtualization? Virtualization is those technologies that manage computer resources by providing a software or middle layer, known as an "abstraction layer," between the software and the physical hardware.[13] Virtualization turns physical resources into logical resources. Essentially virtualization turns a computer into a file or small group of files. These files can be easily moved or deleted. So a VM can exist on the computer in Akron Ohio today, and tomorrow that VM can be easily moved to Madrid Spain.

With virtualization, the operating cost of systems drops significantly since many VMs can concurrently reside on one physical server, save considerable space/real estate, power consumption, and scale readily. The VM density depends on the robustness of hardware (memory, storage capacity, number of core processors, etc.). Not only do you save money by reducing your hardware requirements, you also realize savings in power consumption and air conditioning as well. You also do not need as much physical space. Not all systems qualify for virtualization, but if you running a server at less than 50% processing capacity, virtualization is may be an option.

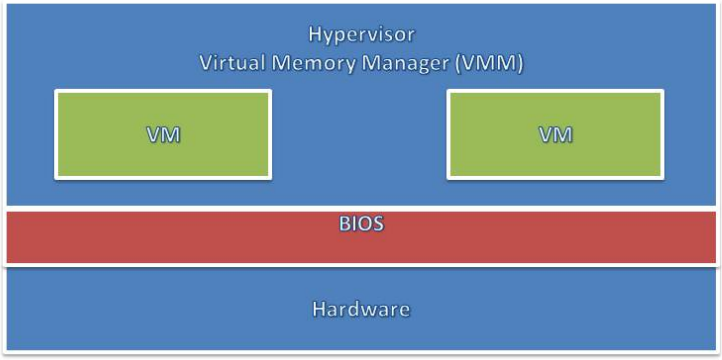
Generally, virtualization can be divided into two categories: server based and host based.[14] In server based virtualization, which is what you will most likely see in a CSP, the virtualization software is installed directly on the hardware (computer). A small operating system provides the platform for the VMs to operate. With server based virtualization, data can be saved and replicated among multiple locations. Server based virtualization is also known as hardware virtualization. Host based virtualization is where the virtualization software is installed over an existing operating system such as Windows or Linux. The middle layer provides the connectivity and resources for the VMs, but this middle layer is still dependent on the host operating system. Host based virtualization is also known as operating system virtualization.

[13] http://www.pcmag.com/encyclopedia_term/0,1237,t=virtualization&i=53961,00.asp
[14] Mastering Windows Network Forensics and Investigation – 2nd Edition; Anson, Bunting, Johnson, Pearson, Sybex 2012

To further muddy the waters, you may also come across Application Virtualization (AV). In AV, emulation software is loaded on to a host operating system, and an application is installed remotely and accessed locally.[15]

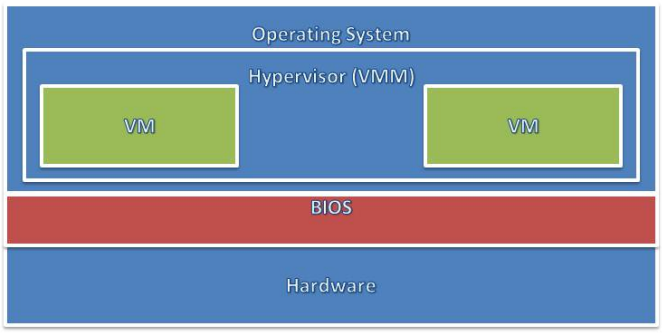
The software that manages VMs is known as a hypervisor. Hypervisors come in two flavors: Type 1 and Type 2. Type 1 hypervisors are associated with hardware/server based virtualization, and Type 2 hypervisors are associated with host based virtualization. An example of a Type 1 hypervisor is VMware ESXi and an example of a Type 2 hypervisor is VMware Workstation. The figures below show each type of hypervisor.

Type 1 Hypervisor



[15] Mastering Windows Network Forensics and Investigation – 2nd Edition; Anson, Bunting, Johnson, Pearson, Sybex 2012

Type 2 Hypervisor



The challenge for investigators is to identify virtualization and cloud services, or to put it another way, how do you locate, acquire, and analyze data in this environment.

There are several virtual machine companies out there today:

VMware	www.vmware.com
Xen	www.xen.org
VirtualBox	www.virtualbox.org
Parallels	www.parallels.com
KVM	www.linux-kvm.org

When dealing with cloud based virtual machines, some of the information the examiner needs before he/she can move forward are:

- How big is the network you are looking at?
- How is the network configured?
- What VMs have been compromised?
- What do these VMs do?
- Where are these VMs physically located?
- How were these VMs compromised?

Acquiring Data/Evidence in a Virtual Environment

There are a couple of scenarios in which you will need to collect evidence in a virtual environment. As an example, we will take a look at VMware, but the techniques are conceptually viable regardless of virtual environment that is being used. Generally, the scenarios are that the VM is running or the VM is not running (dead). In a running environment, evidence (RAM, volatile data, and drive image) can be done just like you were performing these techniques on an actual system. One point should be added here. Since virtual environments have the ability to take snapshots, these snapshots can be used to recreate the moment in time when the snapshot was taken. So, what is a snapshot? A snapshot is a virtual digital snapshot in time. The complete state of the VM at the time the snapshot is taken is preserved including what is in memory and the current state of the file system. The purpose of a snapshot is to allow the VM owner to roll back the VM to the exact point in time when the snapshot was taken.

In the Vmware world, snapshot memory information is stored in the *.vmem file. The VM file system is stored in the *vmdk file. Remember that a VM is nothing more than a small group of files that is brought to life by virtual machine manager. The following tables list VM files that you will come across during your collection of evidence[16]:

Extension	Description
.vmdk	Disk file
.vmsd	Snapshot metadata
.vmem	Snapshot memory contents
.vmsn	Snapshot
.nvram	VM BIOS
.vmxf	Team membership file
.vmx	VM configuration
.log	Ascii base log files

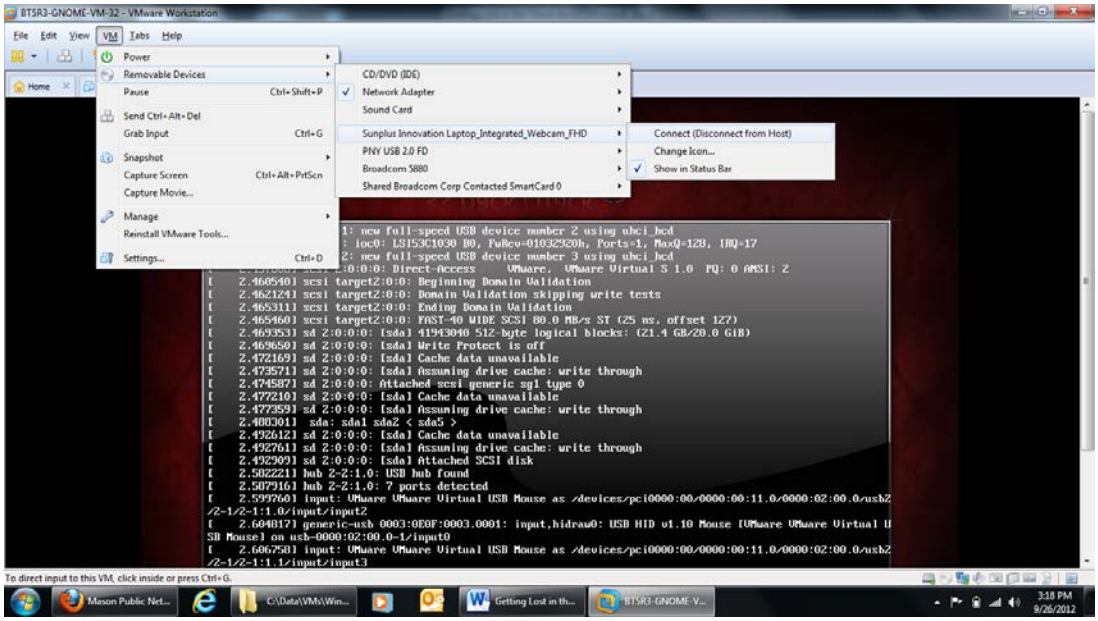
VMware Files

VMware Live System Memory and File System Capture

If your VM is currently up and running, then capturing a memory image, volatile data, and file system image is not much different than obtaining this information from a regular system. First, you would need to mount your tools and collection media to the virtual machine. Typically you would plug in your USB device(s) then associate the VM to your removable device(s). Without proper association you will not be able to run your tools and collect the required data. Associating a removable USB device with a particular VM is actually fairly

[16] VMware v8 was used.

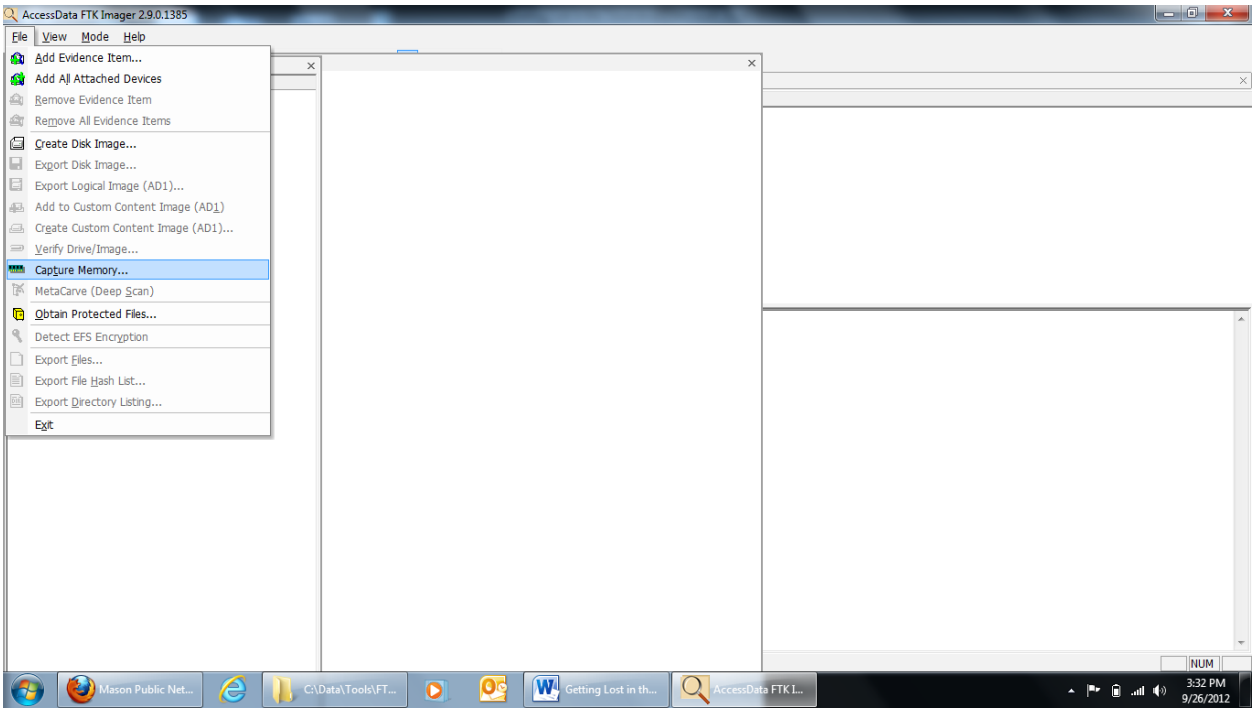
simple. Under VMware v8, click VM – Removable Devices – Highlight the Device – Click Connect. See the figure below.



Associating a Device with VMware v8

It should be noted that with Type 1 or hardware based VM environments like VMware ESXi you may not have the luxury of having an open USB ports to connect to. This is not a limitation of the VMM, but rather a hardware limitation. In this case, you made need to use an enterprise tool like those provided by AccessData or Guidance Software and collect your data via a network connection. This scenario is not much different than if your target computer was a hard system.

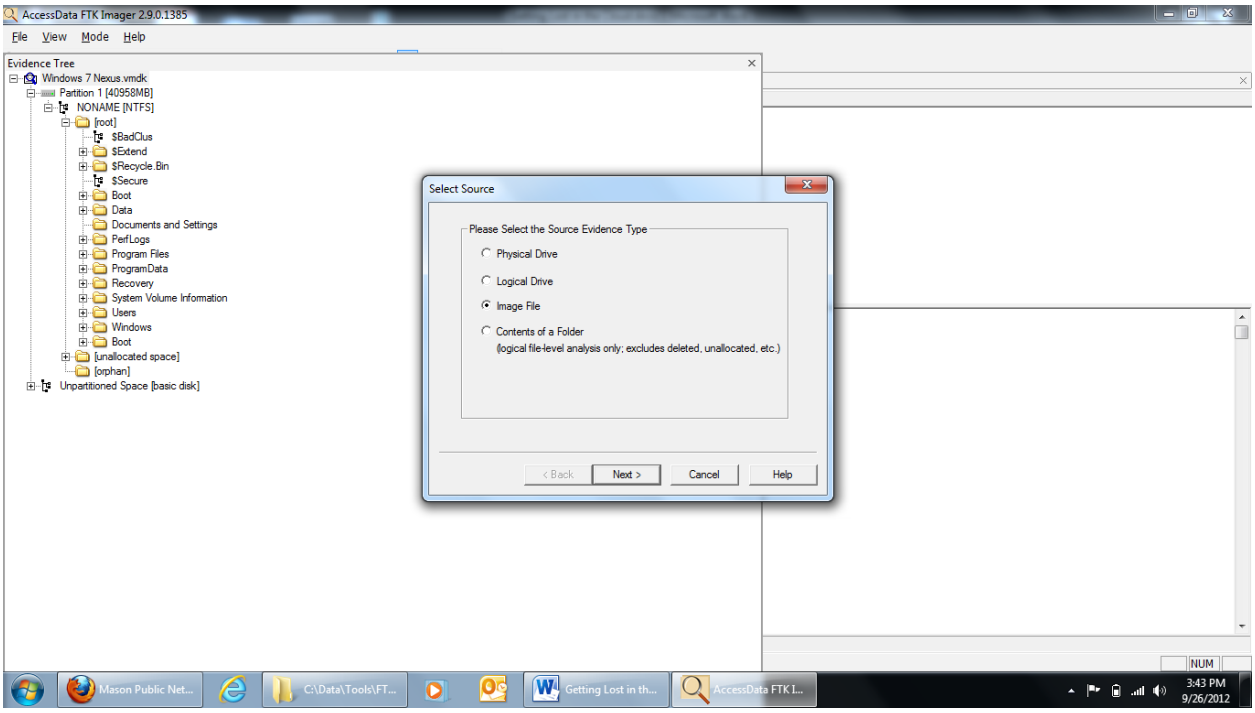
Getting back to our live collection, you would then run your tools. For example, you could run FTK Imager Lite (a favorite of mine) and capture memory as well as make a full disk image. FTK imager Lite does not require installation and will run easily from removable media. The figure below shows the options for FTK Imager Lite:



FTK Imager Lite

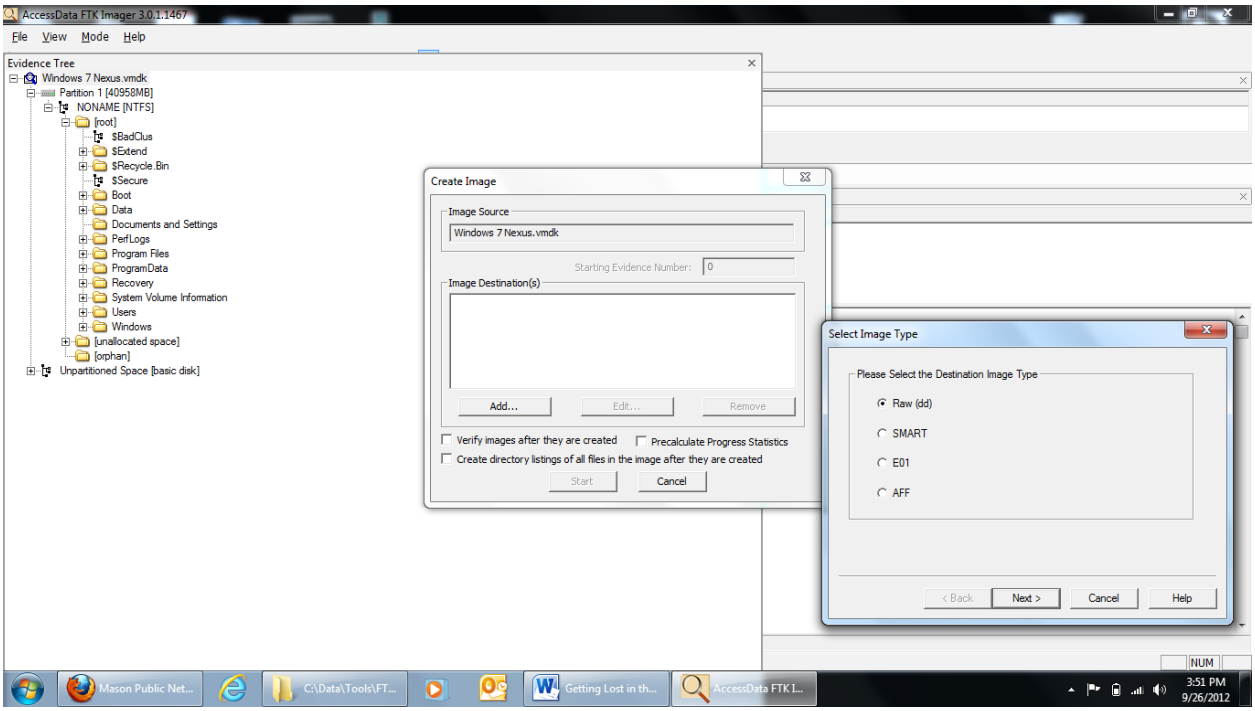
What if your VM is dead (not currently running)? In that case, the investigator would copy all of the files for that particular VM to removable for further analysis at the lab. One thing to remember is that is all cases, you need enough storage space to accommodate your collection. This may sound trivial, but if your target VM is 12 terabytes, then you will need more than 12 terabytes to affect your collection. Also, don't forget to take a digital fingerprint (MD5 or SHA) of the files that you are copying saving those hashes to its own file.

Back in the lab, you can turn those VM files into a workable image by using tools like FTK Imager. By simply adding an evidence item, you tell FTK to load an image file, point to the .vmdk file, and away you go.



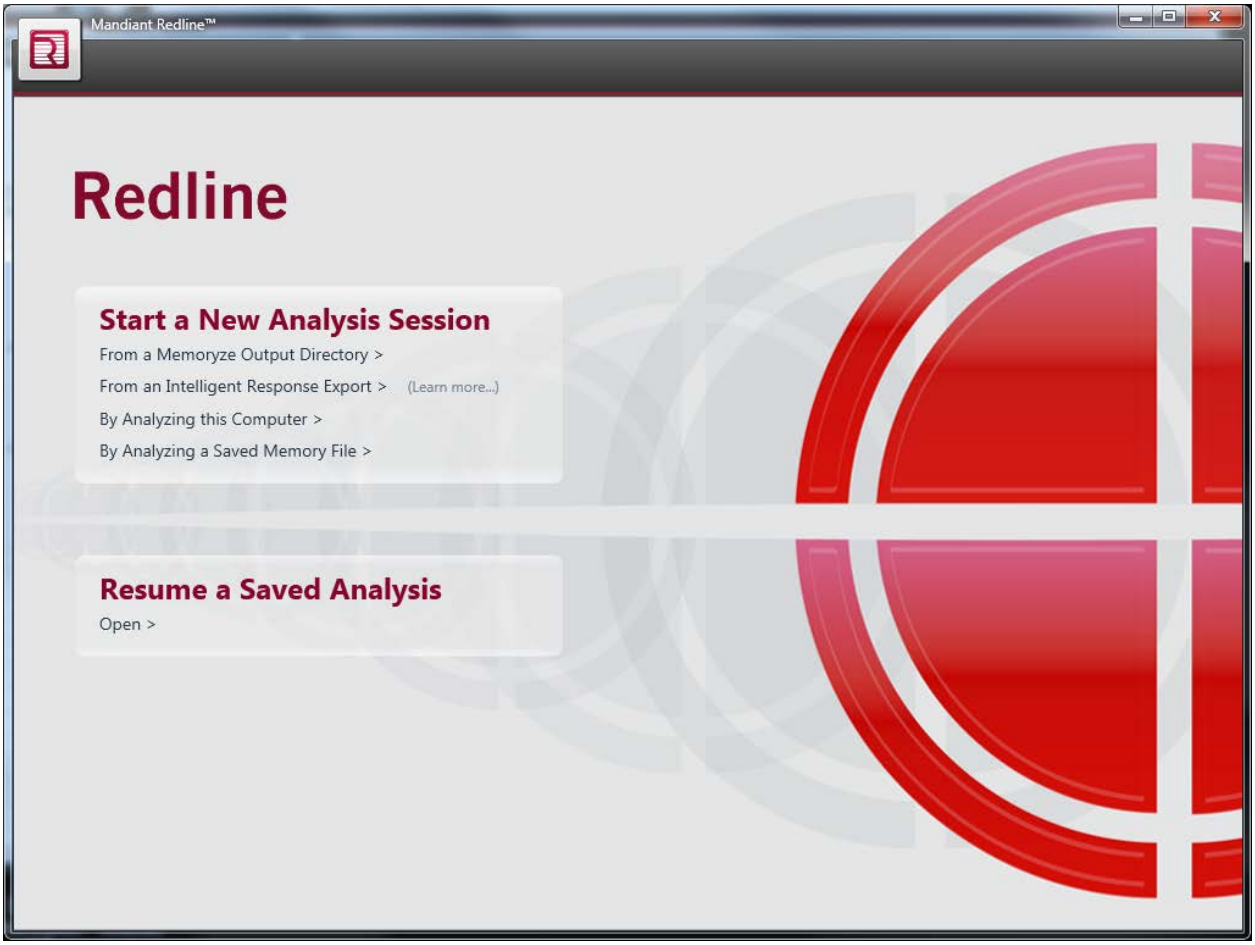
FTK Imager Load a .vmdk File

Once the vmdk file is loaded, you can simply export the image to a format commonly found with forensic tools (e. g. dd, EO1).



In the VMware environment, analyzing the *.vmsd file can provide some interesting insights to that VM's world. The vmsd file is text based and fairly easy to read. It is essentially a file that keeps track of the number of snapshots taken for that VM. This list will correspond to the snapshots *.vmsn files for that VM. This is an easy way to make sure that you have all of the snapshot files. Along with the vmsn file comes the *.vmem file. This file contains the memory for that particular snapshot. The vmem file can be analyzed with such tools as Volatility[17] or Redline[18].

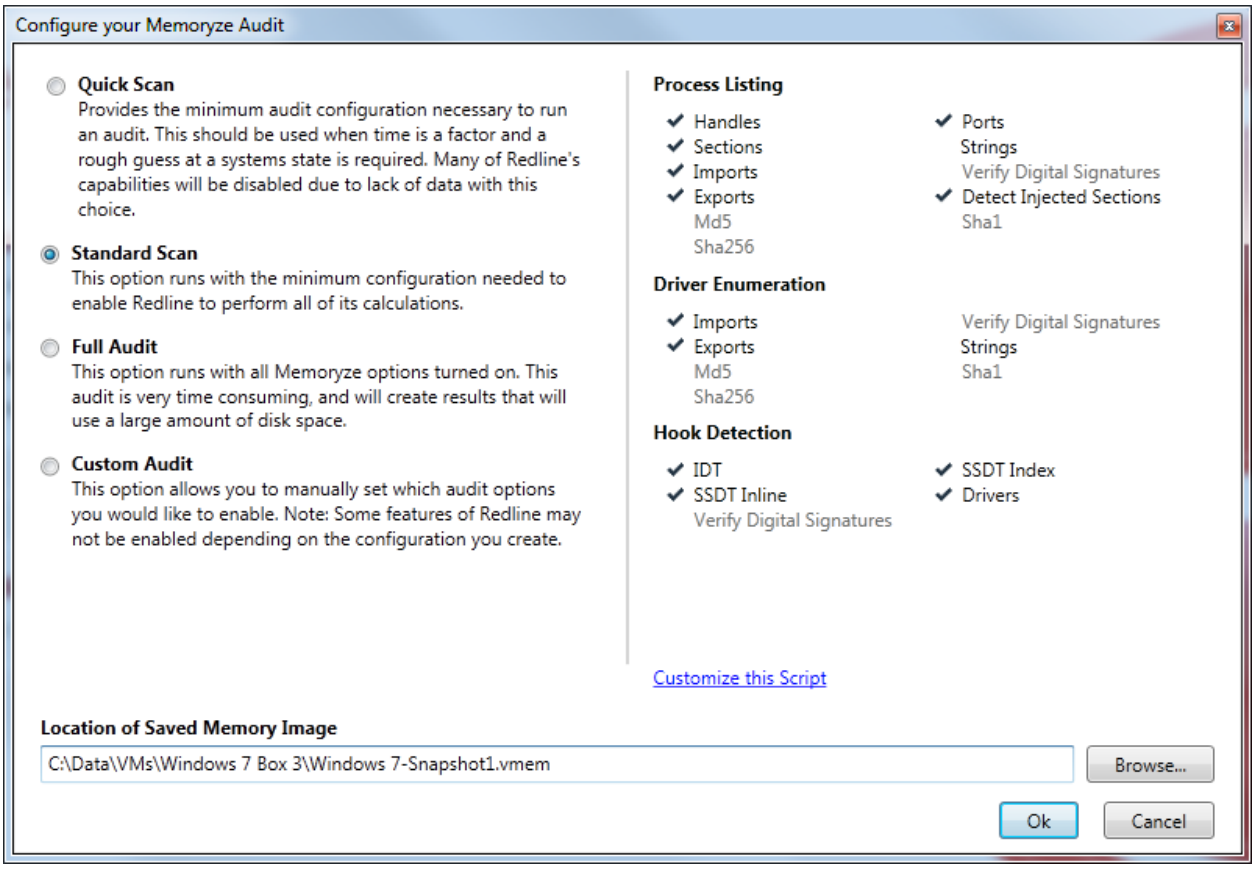
As an example, I will use Mandiant's Redline to examine the contents of a *.vmem file. First, start Redline.



Next, click on Start a New Analysis Session – By Analyzing a Saved Memory File.

You will be given your choice of scan options.

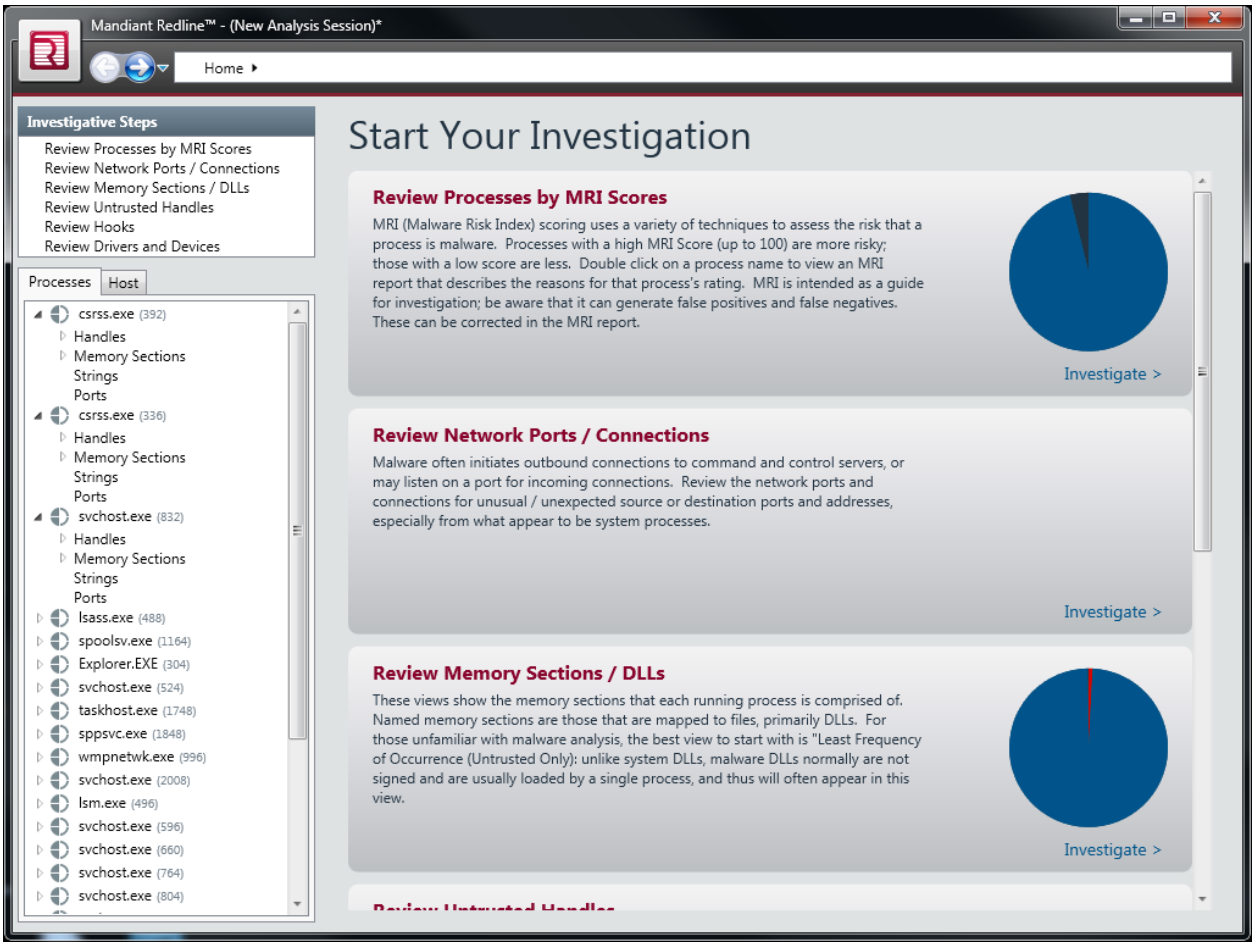
[17] www.volatilesystems.com/default/volatility
[18] www.mandiant.com



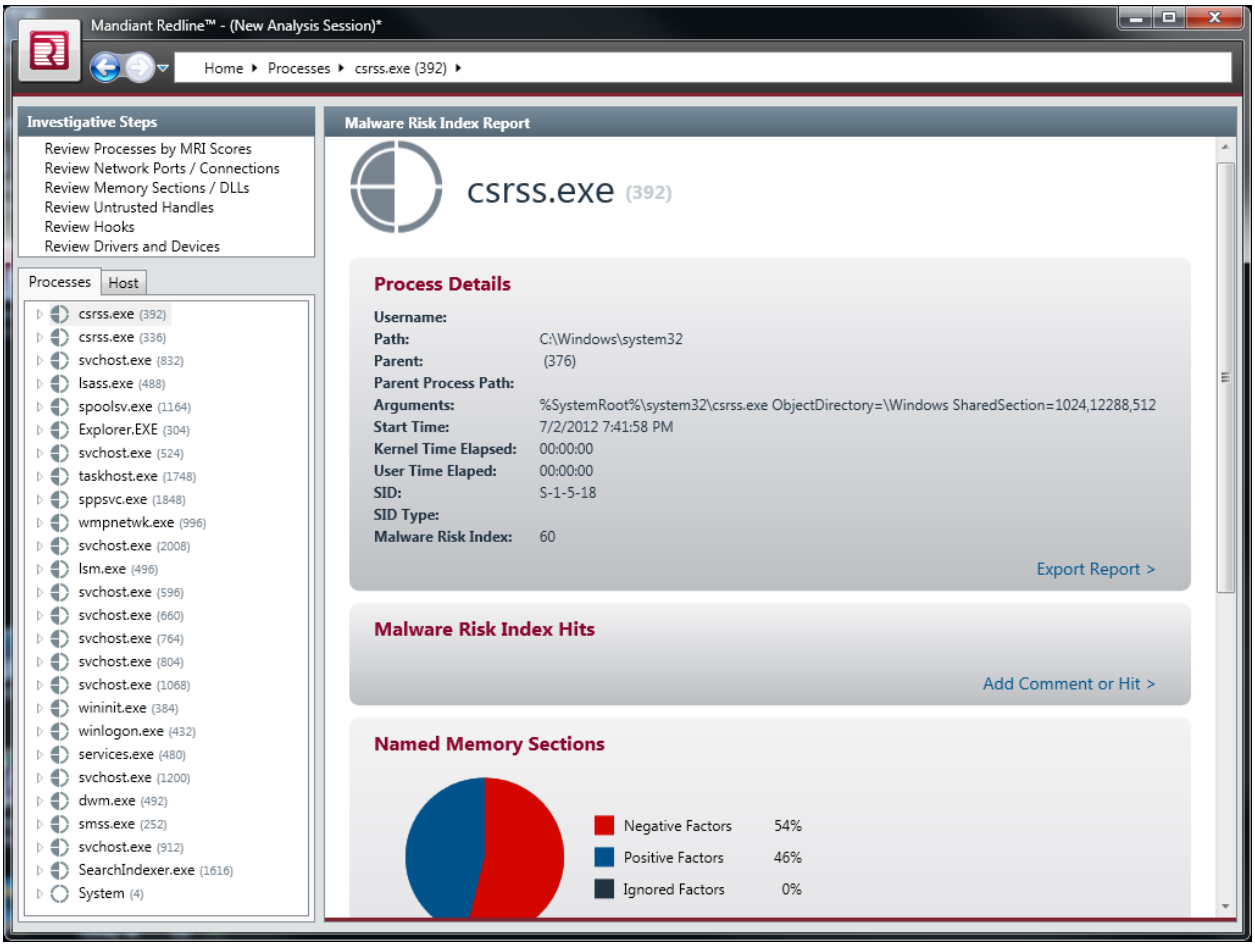
Click on the Browse Button and locate the *.vmem file you want Redline to analyze.

Click OK.

It will take a few minutes, but then you will something that looks like what you see below:


Mandiant Redline™ - (New Analysis Session)*
Home
Investigative Steps
Review Processes by MRI Scores
Review Network Ports / Connections
Review Memory Sections / DLLs
Review Untrusted Handles
Review Hooks
Review Drivers and Devices
Processes
Host
csrss.exe (392)
Handles
Memory Sections
Strings
Ports
csrss.exe (336)
Handles
Memory Sections
Strings
Ports
svchost.exe (832)
Handles
Memory Sections
Strings
Ports
lsass.exe (488)
spoolsv.exe (1164)
Explorer.EXE (304)
svchost.exe (524)
taskhost.exe (1748)
sppsvc.exe (1848)
wmpnetwk.exe (996)
svchost.exe (2008)
lsm.exe (496)
svchost.exe (596)
svchost.exe (660)
svchost.exe (764)
svchost.exe (804)
Start Your Investigation
Review Processes by MRI Scores
MRI (Malware Risk Index) scoring uses a variety of techniques to assess the risk that a process is malware. Processes with a high MRI Score (up to 100) are more risky; those with a low score are less. Double click on a process name to view an MRI report that describes the reasons for that process's rating. MRI is intended as a guide for investigation; be aware that it can generate false positives and false negatives. These can be corrected in the MRI report.
Investigate >
Review Network Ports / Connections
Malware often initiates outbound connections to command and control servers, or may listen on a port for incoming connections. Review the network ports and connections for unusual / unexpected source or destination ports and addresses, especially from what appear to be system processes.
Investigate >
Review Memory Sections / DLLs
These views show the memory sections that each running process is comprised of. Named memory sections are those that are mapped to files, primarily DLLs. For those unfamiliar with malware analysis, the best view to start with is "Least Frequency of Occurrence (Untrusted Only): unlike system DLLs, malware DLLs normally are not signed and are usually loaded by a single process, and thus will often appear in this view.
Investigate >

Redline then provides an excellent platform for which to examine a*.vmem file. Redline will even rate each process/service by its own Malware Risk Index (MRI). Redline does admit that it can report false positives as well as false negatives.



Current Federal Laws/Rules/Decisions That Pertain to Collecting Evidence in a Cloud Computing Environment

So what legal vehicles and processes are available today to assist law enforcement in their quest for evidence in the cloud?

Fourth Amendment of the U.S. Constitution

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized[19]." The fourth amendment of our Constitution is one of the cornerstones of liberty that we hold so dear. It is clear though that the framers of the Constitution could have never imagined the digital world that we live in today. Even so, the fourth amendment still holds up fairly well (with a few slight modifications).

U.S. v Ziegler[20]

A person has a reasonable expectation of privacy in his office and on his workplace computer; however, the employer can consent to searches and seizures of equipment that the company owns. This rule also applies to businesses that employ services in the cloud[21].

Federal Rules of Evidence (FRE) 702[22]

A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

- The expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue
- The testimony is based on sufficient facts or data
- The testimony is the product of reliable principles and methods
- The expert has reliably applied the principles and methods to the facts of the case.

[19] http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html
[20] http://caselaw.findlaw.com/us-9th-circuit/1421016.html
[21] http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf
[22] http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/2010%20Rules/Evidence.pdf

There will definitely arise situations where expert (opinion) testimony will be required in cloud computing matters. FRE 702 provides the framework for how someone qualifies as an expert witness. Expert witness status is only required when the witness needs to present an opinion or conclusion to the court as evidence. Most testimony only requires that witnesses present facts not opinions or conclusions.

Federal Rules of Criminal Procedure Rule 41, the Search Warrant[23]

A magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located within his or her jurisdiction or outside the jurisdiction of any state or district, but within any of the following: a United States territory, possession, or commonwealth. The government must show that it has Probable cause that the evidence obtained in the cloud is related to a crime, contraband, fruits of a crime, or other items illegally possessed or property designed for use, intended for use, or used in committing a crime.

A warrant may authorize the seizure of electronically stored media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant (normally within 14 days) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review. Warrants for electronically stored information can be issued by any court of competent jurisdiction (in the U.S.) whether or not that data is stored within that particular district.[24]

The use of the search warrant will be heavily utilized by law enforcement in cloud related matters. There are some deficiencies in the current state of the how search are executed that we will address later.

The Electronic Communications Privacy Act (EPCA) (18 USC 2701-2712)[25]

Whoever intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in 18 USC 2701(b). ECPA also created the 2703D court order and the 2703F preservation letter.

[23] http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/2010%20Rules/Criminal%20Procedure.pdf
[24] As amended by the Patriot Act
[25] http://uscode.house.gov/download/pls/18C121.txt

18 USC 2703-D Court Order

A court order for disclosure under subsection 18 USC 2703(b) or 18 USC 2703(c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not be issued if prohibited by the law of that State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(Note: The main difference between a Rule 41 and an 18 USC 2703(d) court order is the level proof required. For a Rule 41 search warrant probable cause is required and for an 18 USC 2703(d) court order it is only necessary to prove that there are reasonable grounds to believe that the contents are relevant.)

18 USC 2703-F Preservation Letter

This type of order is issued by a government entity under 18 USC 2703(f), and it orders the provider of wire or electronic communication services or a remote computing service to take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process. The service provider will be required to retain the requested information for a period of 90 days. This time period can be extended for an additional 90-day period upon a renewed request by the governmental entity. This request for information that the provider has as of the date of the request, and is not intended to capture information received after the request is made.

Foreign Intelligence Surveillance Act (FISA), (50 USC 1801-1806)[26]

For the purposes of obtaining foreign intelligence, the government can obtain a court order for electronic surveillance or physical search from the FISA court, the government needs to provide the necessary probable cause that the target of the surveillance is a “foreign power” or an “agent of a foreign power”, and that the places at which electronic surveillance is requested is used or will be used by that foreign power or its agent. It is also possible for the

[26] http://uscode.house.gov/download/pls/50C36.txt

government to obtain the same information by Presidential authority and without a court order, if the target of investigation has no substantially likelihood of being a United States person or party. Additionally, the court must find that the proposed surveillance meet certain minimization requirements.

Title III (18USC2510-2522)[27]

Real-time content monitoring is an interception of electronic communication and a Title III court order is required is criminal matters. In national security matters, FISA controls how real-time content monitoring is conducted. Under Title III, the government must provide facts supporting the probable cause standard of proof that a person(s): is committing a predicate offense[28]; that person is utilizing the facility to be intercepted for criminal purposes; and government has tried traditional investigative methods and failed or, if the government were to employ such traditional investigative methods, why they would fail. The government's facts supporting probable cause need to be current (no more than 30 days old).

Even with these extensive legal tools, as will be later shown, some modification is required to meet the new challenge of cloud computing.

The Standard Digital Media Investigation

The typical computer forensic investigation begins by first identifying the potential source of evidence and where it is located. The evidence is commonly found in the suspect's computer, USB thumb drive, mobile device, a tablet, or other types of consumer electronics or storage devices. The devices are often found at one's home, work, at a crime scene, or on the person and can be directly tied to the suspect.

The identified evidence is then acquired using known, forensically sound tools and procedures. The examiner is able to acquire forensic evidence because the device in question has been located and the examiner has physical access to the suspect device—a key distinguisher. The examiner will image storage devices, computer hard drives, and may elect to capture physical memory if the device is running and is accessible. Hardware write blockers are used to prevent contaminating the evidence when imaging the devices and MD5/Hash values (or SHA1/2) are generated before and after the acquisition to verify the integrity of evidence. The original media is then preserved.

[27] http://uscode.house.gov/download/pls/18C119.txt
[28] Predicate offenses are serious crimes and include violent felonies, drug dealing, money laundering, fraud, etc.

The newly acquired evidence is analyzed and filtered for relevant findings. Various tools can be used to conduct analysis of the acquired evidence (often with Guidance Software's EnCase and/or AccessData's FTK), but as previously mentioned, examiners have wide choices of commercially available and open source tools to assist them with the investigation and analysis. These tools can be used to analyze imaged hard drives, external storage devices, or physical memory dumps acquired from live computers. The relevant findings are then presented to the court (or other parties of interest) and a clear chain of custody and a well-documented process governs the computer forensics investigation.

Forensics and the Cloud

Cloud computing forensics can be an ambiguous and difficult task that must be overcome by forensic examiners and investigators. This is of course dependent on the type of cloud service in question and who has control. It is ambiguous because cloud forensic practice is still emerging and guidelines and legal framework are largely undocumented. In a follow-up publication to the NIST SP 800-145 that defined cloud computing environment, NIST reported that cloud computing is a developing area and its ultimate strengths and weaknesses are not yet fully researched, documented, and tested (SP 800-146, May 2012)[29]. It is difficult because utilization of existing tools is not always possible and using or repurposing existing tools is not always effective in this new environment.

Many researchers and practitioners have observed this dilemma and stated that different service providers use varying proprietary technology and their implementation must be learned but are difficult or simply not accessible for examination. The Defense Technical Information Center noted that there has been very little research done on the current state of the tools, processes, and methodologies to obtain legally defensible digital evidence in the cloud (IA Newsletter, Winter 2011)[30]. Garfinkel, a researcher from the Naval Postgraduate School, observed in his article "Digital Forensics Research: The Next 10 Years" that one of the issues that may present potential crisis in the digital forensics is the growing use of the "cloud" for remote processing and storage, and how it threatens forensic visibility.[31]

[29] http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf, National Institute of Standards and Technology, Cloud Computing Synopsis and Recommendations, May 2012, retrieved on July 3, 2012.

[30] S. Zimmerman and D. Glavach. "Cyber Forensics in the Cloud". IA Newsletter, Defense Technical Information Center, Winter 2011.

[31] Simson Garfinkel, Digital Forensics Research: The Next 10 Years, ScienceDirect, 2010.

A major advantage of Cloud computing is independence from hardware and operating system profiles. It allows users to access their computing environment and resources from virtually anywhere in the world with the Internet. When data is pushed to the public cloud by a consumer using the IaaS model, it can be stored in one of many data centers and replicated multiple times across data centers and distributed within the cloud for load balancing, access optimization, and/or replicated for redundancy and availability, as is the case for Amazon Web Services (AWS) Simple Storage Service (S3) and Google Cloud Storage[3233]. The natural question that arises when an investigator attempts to seize or acquire image of the storage device is "where is the data?"

In traditional forensics, physical access by the user and ownership boundaries are well defined and relatively easy to establish[3435]. But the task of locating the data source in the cloud is not so trivial, as the CSP themselves may not know exactly where the data resides at a specific point in time. This is further complicated by the fact that the service providers and their resources are often geographically dispersed spanning the country and even crossing international borders.

Additionally, investigators are largely dependent on the CSP to make due diligence in locating the data source, forensically acquiring, preserving, and providing the information in a manner that would be acceptable in court. While the law enforcement organizations may have the added benefit of legally compelling the CSP to comply with a court order, the public, corporations, and private citizens do not enjoy the same privilege. But even law enforcement may not always have the legal authority to mandate CSP cooperation if jurisdiction cannot be obtained or the process may be very time consuming; multiple data source locations mean multiple jurisdictions. The very nature of cloud storage (IaaS model) denies investigators the physical access to data sources. Forensic investigations into the private (and hybrid) clouds, however, offers similar access to the resources as in traditional computer forensics since the architecture is owned by the single organization or entity that are physically accessible by the investigators.

---

[32] http://code.google.com/apis/storage, Google Cloud Storage – a Simple Way to Store, Protect, and Share Data, retrieved on 2 July 2012.

[33] https://aws.amazon.com/s3, Amazon Simple Storage Service (Amazon S3), retrieved on July 7, 2012.

[34] S. Zimmerman and D. Glavach. "Cyber Forensics in the Cloud". IA Newsletter, Defense Technical Information Center, Winter 2011.

[35] D. Reilly; C. Wren; and T. Berry. "Cloud Computing: Pros and Cons for Computer Forensic Investigations". International Journal Multimedia and Image Processing (IJMIP), Volume 1, Issue 1, March 2011.

Another facet of cloud computing that increases difficulty is that there will always be multiple parties that must be involved in the collection process. Forensic investigations in cloud computing environments always involve at least two other parties: the CSP and the customer. When the CSP outsources services to other parties, the scope of the investigation widens even more. The investigator must research how many third party members were involved and each of their hosting servers, storage devices, and other relevant resources. This leads to difficult legal challenges with few precedents that are necessary to derive guidance and authority.

This is not the only third party issue that needs to be addressed. The issue of isolating and identifying data for positive ownership and attribution that comes from a multi-tenant environment inherent to cloud computing must be considered. In a multi-tenant environment, multiple consumers are sharing infrastructure and computing resources. In a SaaS model, various customers will be sourcing the same application data from the same hardware which means that data belonging to multiple tenants is likely stored in the same database and may even share the same tables. In IaaS, virtual machines providing the infrastructure may be sharing the same physical host as other virtual machines instances that belong to other customers. How can different instances maintain system and data integrity? How are they insulated from each other to prevent accidental or deliberate contamination?

As one would expect, cloud computing raises some unique law enforcement concerns regarding the location evidence, storage, and subsequent analysis. For example, if a business becomes the target of an investigation, it could move its working environment to a cloud environment or move within the cloud itself. This would enable the enterprise to continue its criminal operation essentially playing hide and seek with law enforcement. Since the data can be stored anywhere in the world, its dispersal could be to a location or country where data laws are not readily enforced or non-existent. Establishing a chain of custody for this information would become difficult or impossible if its integrity and authenticity cannot be fully determined. We are back to where was it stored, who had access to the data, etc. There are also potential forensic issues when someone exits a cloud application. Items subject to forensic analysis, such as registry entries, temporary files, and other artifacts (which are stored in the virtual environment) could be lost making malicious activity difficult to substantiate.[36]

[36] http://www.forensicmag.com/print/289; Barbara, John J.; Cloud Computing: Another Digital Forensic Challenge

The Future of Forensics and the Cloud

Recommendations:

Establish an Internet Based FraaS as a law Enforcement Resource

Setting up FraaS as a law enforcement resource to include StaaS so that Law Enforcement Agencies (LEAs) can access (with the appropriate court order) data in a cloud environment and be able to image that data in a forensically sound manner no matter how large the data set. This capability would also require the necessary bandwidth (OC 192 or better) to facilitate the imaging of large data sets over the Internet.

How would such a FraaS work?

First Congress would need to appropriate the funds to establish a Law Enforcement Agency (LEA) FraaS, and this resource (let's call it the LE-FraaS) would service any federal, state, or local LEA.

The LEA requiring the resources of the LE-FraaS would notify the LE-FraaS and provide a signed copy of the warrant. The LE-FraaS would then allocate storage space (just like a StaaS) for the forensic collection. The LEA would then work with the CSP serving the appropriate warrant, and the data (evidence) in question can be transferred directly to the LE-FraaS. The data will be digitally fingerprinted and logged and this will be a critical part of the chain of custody required by U.S. courts in order to verify, validate, and attribute the data (evidence).

Logging would include at a minimum:

1. MD-5 Hash
2. SHA – 1/256/512 Hash
3. IP address of the data source
4. Host name of the data source
5. Mac address of the data source
6. Beginning date/time stamp (when download began)
7. Ending date/time stamp (when download was completed)

This methodology solves a couple of problems that LEAs have in dealing with cloud data, first, it eliminates or at least significantly reduces the need for LEA's to bring large data storage

devices on site. Just as in the FBI/ICE Megaupload case[37], when you are dealing with terabytes, petabytes, or even (God forbid) exabytes of data, the ability to bring such storage on site anywhere is logistically challenging at best. At worst, it's a nightmare. It's also expensive. By having an Internet based LE-FraaS, any CSP that is connected to the Internet could be accessed (with the appropriate court order) and the data downloaded to the LE-FraaS. CSPs will, by business necessity, have access to large amount of Internet bandwidth anyway in order to operate, so high transfer rates (OC level) will already be built into the CSP infrastructure.

The LE-FraaS also provides a process/methodology that can be vetted in a court of law to assure the public that cloud based evidence is being appropriately and correctly seized and protected.

LE-FraaS security will have to be state of the art since such a site will be the target of any and every digital hoople with an axe to grind. The best authentication, accreditation, and accounting will need to be employed in order to protect this digital evidence.

The Communications Assistance for Law Enforcement Act (CALEA) and/or the Electronic Communications Privacy Act (ECPA) will most likely need to be amended requiring CSPs to comply with and be compatible with LE-FraaS evidence collection technical requirements.

Modify the Laws Regarding Cyber Search Warrants

Modifying search laws such that a warrant will be valid if the data can be seen from a location. Prior to the passing of the Patriot Act, if an LEA wanted to serve a warrant on the service provider; an affidavit, application, and order would have to approved in the jurisdiction where the service provider resided. So, for example, if you wanted to serve Microsoft a search warrant to seize emails from a Hotmail account, you would need to go to Redmond, Washington and present your order to a local (federal or state) judge. It is easy to see that such a system is not scalable, overly burdensome to the local judiciary, and not in the best interest of the public.

The Patriot Act, in addition addressing critical counterterrorism needs, also, addressed pressing cyber matters as well. The Patriot Act allows, in matters where electronic evidence was involved, that a court of competent jurisdiction (where case venue resides), authorize the order. Also, that court order can be transmitted electronically (i.e. via facsimile) to the service

[37] http://www.fbi.gov/news/pressrel/press-releases/justice-department-charges-leaders-of-megaupload-with-widespread-online-copyright-infringement

provider for the requested data. This not only made sense, but created a much more efficient way for LEAs to seize electronically stored evidence.

In the U.S., search warrants must be location specific. Even the Patriot Act did not change this. So, let's say you have a search warrant to search location X for evidence of a crime and let's say that you are also looking for electronically stored evidence as well. During the course of searching location X, you discover that electronic evidence pertinent to you investigation is located in location Y. You know this because the system administrator on location X has advised that electronic data is stored in location Y, but that location Y is directly electronically accessible via location X. Presently, you would need to get an amended warrant to include site Y.

With the advent of cloud based services, the law once again is lagging behind. As with the Patriot Act, the generally accepted process needs to be modified so that, when dealing with electronically stored evidence, if you are executing a search warrant on location X, and location X has access to electronically stored data which falls under the items to be seized, but that data is located in location Y, that electronically stored data should be subject to seizure without warrant modification. One could call this a virtual location where the location in question is not bounded by a specific physical address, but by its logical access and connectivity.

Let's take a look at an example to see how this would fit. An LEA gets a search warrant to search iPhone. The LEA has the device's passphrase. Examination of the iPhone reveals that data was uploaded to iCloud. The iPhone has access to the iCloud data. Using the concept of virtual location, iCloud storage is simply an extension of the iPhone's storage capacity, and, subsequently, is subject to seizure under the existing court order. Please note, in this example, the LEA has a search warrant for a specific location (the iPhone), and through that location, the cloud base data was accessible. Such a paradigm shift is not without some pitfalls. For example, let's say that with our previous iPhone example, the subject was using some data storage application (app) that was storing data in Europe. Are there any European privacy law issues?

Cloud computing is not only changing the way we live, it is also changing the way law enforcement will have to deal with evidence collection.

Glossary

Cloud - Internet based remote computing services.

Cloud Service Provider (CSP) – Anyone who provides cloud services

Communications Assistance for Law Enforcement Act (CALEA) (47 USC 1001-1010) – The purpose is to provide law enforcement agencies the ability to conduct electronic surveillance by requiring TSPs and ISPs (2005 FCC Ruling) to modify their equipment to allow for the interception of telephone, broadband Internet and VOIP traffic in real-time. Thus, CALEA only applies to: telephone, broadband Internet, and VOIP. It appears that it currently does not apply to traffic in the cloud.

Electronic Communication - Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include: any wire or oral communication; any communication made through a tone-only paging device; any communication from a tracking device (as defined in section 18 USC § 3117); or electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

Electronic Communications Privacy Act (ECPA) – Passed in 1986, ECPA under Title II (Stored Communication Act (SCA)), protects communications stored in computers making it illegal to access a stored communication thereby obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage.

Electronic Storage - Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

Forensics as a Service (FraaS) – Computer forensic resources provided on cloud artifacts

Gaming as a Service (GaaS) - Customer has direct on-demand access to games onto his/her computer through the use of a thin client

Infrastructure as a Service (IaaS) – Customer has control of the processors, memory, storage and switches per SLA but does not have access to the underlying hardware or hypervisor.

Intercept - The aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.
Letters Rogatory - Is a formal request from a court to a foreign court for some type of judicial assistance. The most common remedies sought by letters rogatory are service of process and taking of evidence. This formal request is normally used when the country where the records are sought is not a member of the Mutual Legal Assistance Treaty (MLAT).

Mutual Legal Assistance Treaties (MLAT) - During 1977, the United States signed the Mutual Legal Assistance Treaty (MLAT) with a number of countries in Switzerland. These countries formed an agreement for the purposes of gathering and exchanging information in an effort to enforce public or criminal laws. Member countries can request assistance from other member countries using this process in order to obtain information or assistance. Assistance could be denied by either country for political or security reasons, or if the criminal offence in question is not equally punishable in both countries.

Oral Communication - Any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication.

Pen Register - A device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

Platform as a Service (PaaS) - Customer has increased control over software, but no control of infrastructure or processors, memory, storage or switches.

Remote Computing Service (RCS) - The provision to the public of computer storage or processing services by means of an electronic communications system.

Service Level Agreement (SLA) – Terms of service agreement between a provider of some service (i.e. an Internet Service Provider) and a customer.

Software as a Service (SaaS) - Customer does not have control or access to the underlying cloud infrastructure to include servers, operation system, and storage or system capabilities. The customer mostly has access to the applications purchased for use.

Storage as a Service (StaaS) - customer leases storage space from a Cloud Service Provider

Trap and Trace - A device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

Virtualization - is those technologies that manage computer resources by providing a software or middle layer, known as an "abstraction layer," between the software and the physical hardware.

Virtual Machine (VM) - Is a software implementation of a machine (i.e. a computer) that executes programs like a physical machine. A VM is a completely isolated guest operating system installation within a normal host operating system or hypervisor.

Virtual Private Network (VPN) – Usually refers to a network where at least parts of it traverse the Internet, however, the data is encrypted making the connection(s) virtually private.

Wire Communication - Any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

Appendix
Obtaining Evidence from the Cloud

The table below outlines procedures that can be used in order to obtain information from CSPs. In order to determine which process to use, the examiner should cross reference the information desired with the legal requirements provided.

Information Desired	Code Section	Legal Document Required	Notice	Type of Proof	Remarks
Contents of Wire or Electronic Communications in Electronic Storage less than 180 days	18 USC 2703 (a)	Rule 41 SW	No Notice	The government must show that it has Probable cause that the evidence obtained in the cloud is related to a crime, contraband, fruits of a crime, or other items illegally possessed or property designed for use, intended for use, or used in committing a crime.	
Contents of Wire or Electronic Communications in Electronic Storage more than 180 days	18USC 2703 (b)	Same documents as those required for the Contents of wire or electronic communications in RCS	Varies	Varies	There are several ways of obtaining information from an ECS, however due to some recent court decisions in the sixth circuit, jurisdictions covered by the sixth circuit are limited in the processes that can be used. The sixth circuit Court of Appeals in *US v. Warshak* found that individuals have a reasonable expectation of privacy in their e-mails and that the Fourth Amendment protects e-mails held by ISPs. Therefore, that circuit requires rule 41 search warrant for e-mails held in storage for more than 180 days.

Contents of Wire or Electronic Communications in a Remote Computing Service	18USC 2703 (b)	Rule 41 SW	No Notice	The government must show that it has Probable cause that the evidence obtained in the cloud is related to a crime, contraband, fruits of a crime, or other items illegally possessed or property designed for use, intended for use, or used in committing a crime.	
Contents of Wire or Electronic Communications in a Remote Computing Service	18USC 2703 (b)	2703d court order	Prior Notice	Reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation	May obtain delayed notification pursuant to 18 USC 2705
Contents of Wire or Electronic Communications in a Remote Computing Service	18USC 2703 (b)	Administrative subpoena	Prior Notice	Information sought is related to an investigation	
Records Concerning ECS or RCS	18USC 2703 (c)	Rule 41 SW	No Notice	The government must show that it has Probable cause that the evidence obtained in the cloud is related to a crime, contraband, fruits of a crime, or other items illegally possessed or property designed for use, intended for use, or used in committing a crime.	Name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service.

Records Concerning ECS or RCS	18USC 2703 (c)	2703d court order	No Notice	Reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation	Name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service.
Records Concerning ECS or RCS	18USC 2703 (c)	Subpoena	No Notice	Information sought is related to an investigation	Name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service.

Records Concerning ECS or RCS	18USC 2703 (c)	Consent	Notice	No proof	Name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service.
Records Concerning ECS or RCS	18USC 2703 (c)	Formal Request	No Notice		Used in telemarketing cases, then only for Name, address, place of business of subscriber
Backup of RCS contents	18 USC 2704	18 USC 2703(d) court order	Prior Notice	Reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation	Notice will be made by government agency making the request unless the notice is delayed pursuant to 18 USC 2705
Backup of RCS contents	18 USC 2704	Subpoena	Prior Notice	Information sought is related to an investigation	Notice will be made by government agency making the request unless the notice is delayed pursuant to 18 USC 2705
Real-time intercept of Communications	18 USC 2518	Court Order	No Notice	PC a predicate offense is being committed and PC that the device to be intercepted is being used to further the predicate offense. Evidence must be current (30 days). All other techniques must have been tried or if tried	Every 10 days, letter is required to be submitted to the judge. However, the order is good for only 30 days max.

				will fail.	
Real-time intercept of Communications or search for contents (data)	50 USC 1802, 50 USC 1821	Presidential Authority or FISA judge court order	No Notice	No substantial likelihood United States person or party or Foreign power or agent	Purpose of obtaining information is for foreign intelligence purposes
Telephone toll and Transactional Records	18 USC 2709	Official Letter	Prior Notice, unless FBI Director or designee certification	FBI director or designee letter	Also known as the National Security Letter; requests name, address, length of service. Case must be related to international terrorism or clandestine intelligence activities
Pen Register or Trap & Trace	18 USC 3123	Court Order	No Notice	Reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation	Real time transactional information in both data and voice communications. Device or process, which records or decodes dialing, routing, addressing, or signaling information. Also, this order can be used to obtain e-mail headers, date, time, and IP addresses. Order is good for up to 60 days.

Bibliography

Anson, Steve; Bunting, Steve; Johnson, Ryan; Pearson, Scott (2012); Mastering Windows Network Forensics and Investigation – 2nd Edition; Sybex

Badger, G. e. (2011, May). National Institute of Standards and Technology. Retrieved June 4, 2012, from NIST: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146/pdf

Barbara, J. (2009, October 1). Cloud Computing: Another Digital Forensic Challenge. Retrieved June 1, 2012, from Forensic Magazine: http://www.forensicmag.com/print/289

Biggs, S. a. (2010, January 29). Cloud Computing: THe impact on digital forensic investigations. Retrieved June 1, 2012, from Institute of Electrical and Electronics Engineers Xplore Digital Library: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5402561

Chow, R. e. (2011). Controlling Data in the Cloud: Outsourcing Compuiation without Outsourcing Control. Retrieved June 1, 2012, from Karlstad University: http://www.it.kau.se/cs/education/courses/dvad07/p5_2011/ccsw.pdf

Dykstra, J. &. (2011, December 31). Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies. Retrieved June 15, 2012, from UMBC , CSEE Online publication Manager: http://publications.csee.umbc.edu/publications/561

Dykstra, J. a. (2012, April 18). Acquiring Forensic Evience from Infrastructure-as-a-Service Cloud Computing. Retrieved June 15, 2012, from University of Mayland, Batimore County, Josiah

Dykstra page: http://www.csee.umbc.edu/~dykstra/DFRWS_Dykstra.pdf

Garfinkel, S. (2010). Digital Research: The next 10 years. Retrieved June 1, 2012, from Defense Technical Information Center: http://www.dtic.mil/dtic/tr/fulltext/u2/a549288.pdf

Grance, J. &. (2011, December). Guidelines on Security and Privacy in Public Cloud Computing. Retrieved June 4, 2012, from National Institute of Standards and Technology : http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

Grance, M. &. (2011, September). The NIST Definition of Cloud Computing . Retrieved June 4, 2012, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Lawton, G. (2011, January 6). Cloud Computing crime poses uniue forensic challenges. Retrieved June 1, 2012, from Search Cloud Computing: http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-crime-poses-unique-forensics-challenges?vgnextfmt=print

Ludwig, S. e. (2011). Cloud Computing and Computer Forensics for Business Applications. Retrieved June 4, 2012, from Academic and Business Research Institute : www.aabri.com/manuscripts/11935.pdf

Rengan, M., & Ye, D. (2011, August 31). IBM System x Private Cloud Offering: Solution and Component Guide. Retrieved July 1, 2012, from IBM: http://www.redbooks.ibm.com/redpieces/abstracts/redp4731.html?Open&pdfbookmark

Ruan, K. e. (2011). Cloud Forensics an Overview. Retrieved June 1, 2012, from Cloud Forensics Research: http://cloudforensicsresearch.org/publication/Cloud_Forensics_An_Overview_7th_IFIP.pdf

Ruan, K. e. (2011). Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability. Retrieved June 4, 2012, from Cloud Forensics Research: http://www.cloudforensicsresearch.org/publication/Survey_on_Cloud_Forensics_and_Critical_Criteria_for_Cloud_Forensic_Capability_6th_ADFSL.pdf

Sosinsky, B. (2011). Cloud Computing Bible. Indianapolis: Wiley Publishing, Inc