

# Facilitating Fluffy Forensics 3.0

---

- 📍 Andrew Hay, CTO, LEO Cyber Security
- 📞 [+1.415.940.9660](tel:+14159409660)
- ✉️ [andrew.hay@leocybersecurity.com](mailto:andrew.hay@leocybersecurity.com)
- 🌐 [www.leocybersecurity.com](http://www.leocybersecurity.com)
- 🐦 [@andrewsmhay](https://twitter.com/andrewsmhay)



# About Andrew Hay

---

- Andrew Hay
- Co-Founder and CTO @ LEO Cyber Security
- Former:
  - CISO @ DataGravity
  - Director of Research @ OpenDNS
  - Chief Evangelist & Director of Research @ CloudPassage
  - Senior Security Analyst @ 451 Research
  - Sr. Security Analyst in higher education and a bank in Bermuda
  - Product, Program, and Engineering Manager @ Q1 Labs
- Wrote some books, blog, spend more time on planes than I care to mention...



# Overview

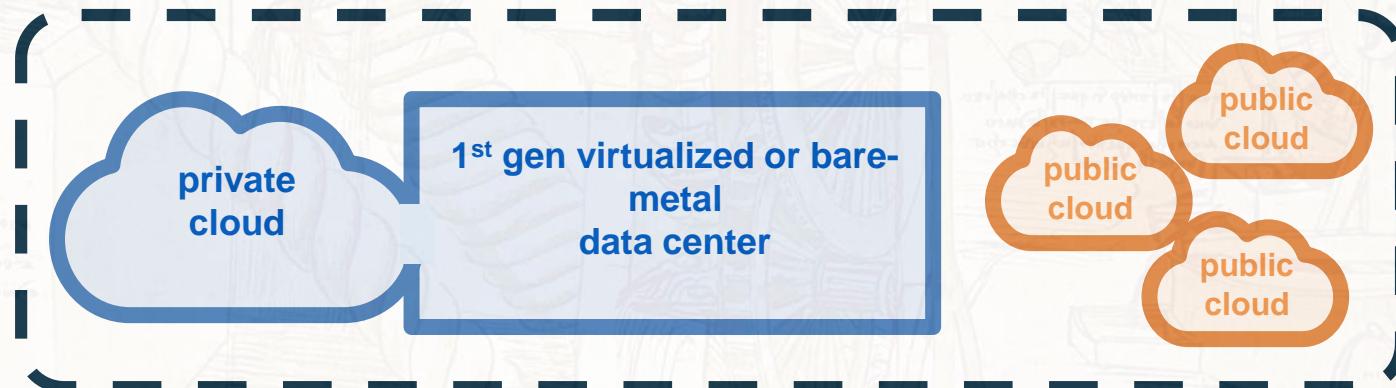
---

- Cloud architectural challenges for responders
- How existing forensics/IR tools can help
  - and what they can do better
- Advantages of conducting forensics/IR in cloud environments



# Cloud Architectural Challenges For Responders

# Cloud Architectures



**Cloud means many things to many people**

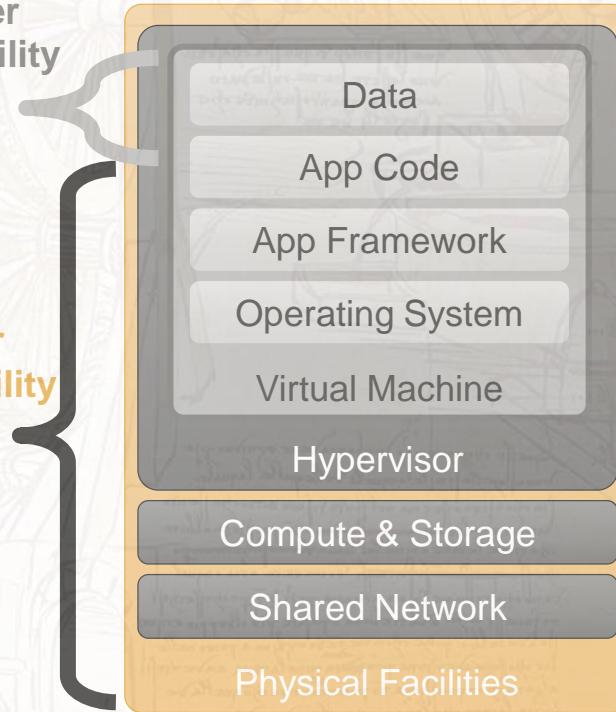
- Private, public, or hybrid?
- SaaS, PaaS, or IaaS?
- On-prem, off-site, hosted?
- Single tenant, multi-tenant?

# Cloud Security Responsibility

SaaS



PaaS



# Cloud Security Responsibility

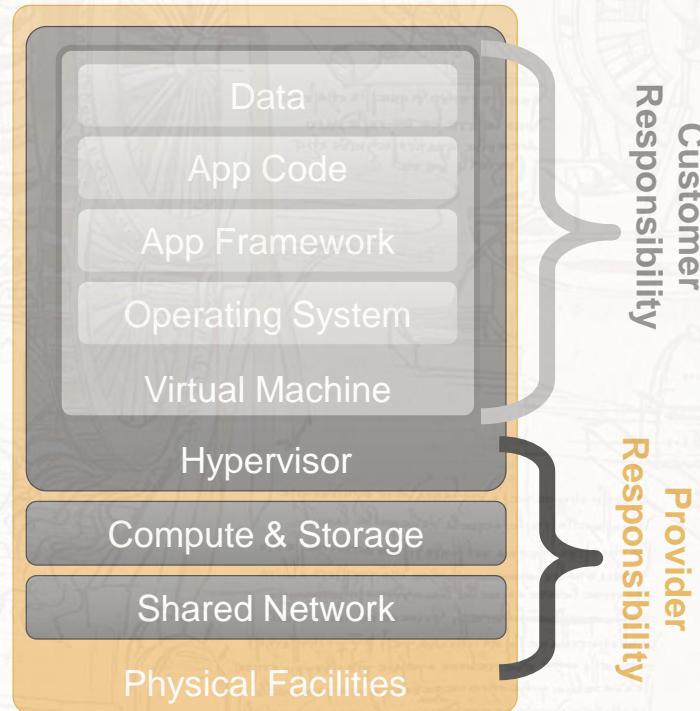
## IaaS

### AWS Shared Responsibility Model

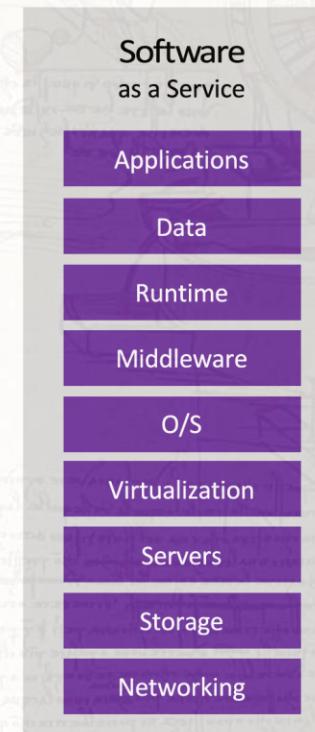
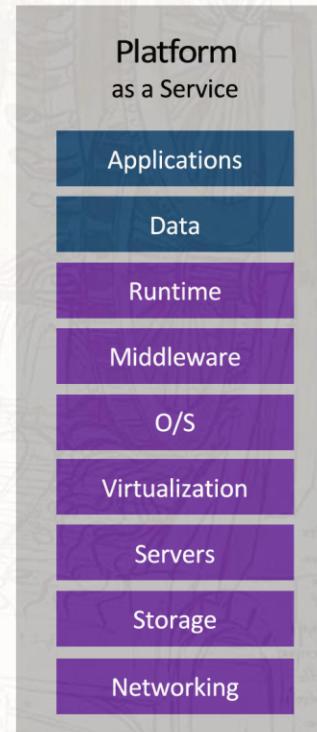
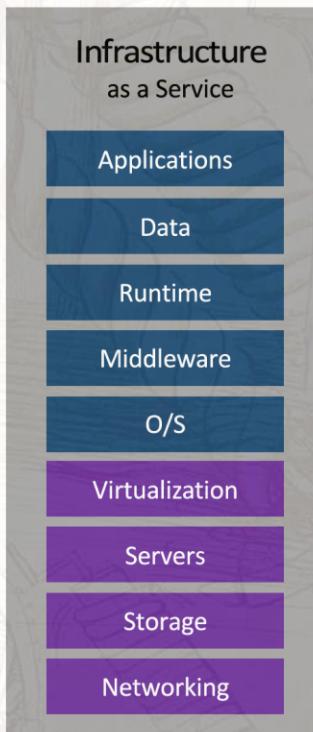
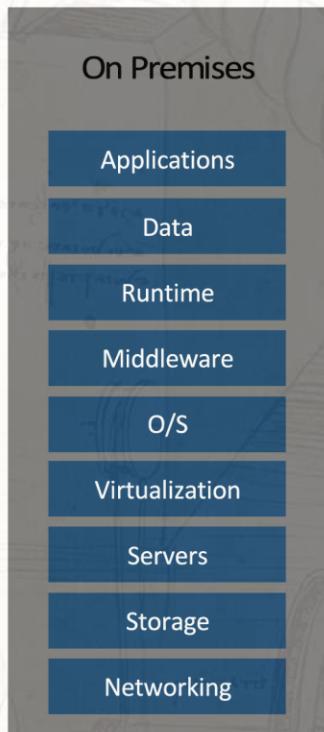
“...the **customer should assume responsibility and management** of, but not limited to, the guest operating system...and associated application software...”

“it is possible for customers to **enhance security** and/or meet more stringent compliance requirements **with the addition of... host based firewalls, host based intrusion detection/prevention**, encryption and key management.”

*Amazon Web Services:  
Overview of Security Processes*



# Cloud Security Responsibility (Alternative)



*With thanks to  
Troy Larson,  
Azure | MSRC,  
Microsoft Corp.*

# Vacation Responsibility

---

## Backpacking

Entertainment

Lunch & Dinner

Breakfast

Towels

Sheets

Chairs

Bed

Walls

Roof

## RV Rental IAAS

Entertainment

Lunch & Dinner

Breakfast

Towels

Sheets

Chairs

Bed

Walls

Roof

## Hotel PAAS

Entertainment

Lunch & Dinner

Breakfast

Towels

Sheets

Chairs

Bed

Walls

Roof

## Cruise Ship SAAS

Entertainment

Lunch & Dinner

Breakfast

Towels

Sheets

Chairs

Bed

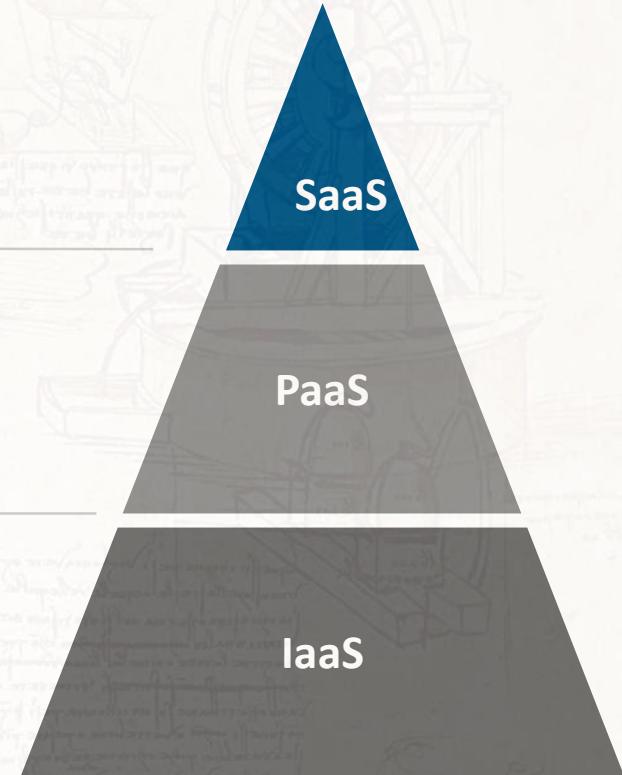
Walls

Roof

*With thanks to  
Troy Larson,  
Azure | MSRC,  
Microsoft Corp.*

# Cloud Forensics Means...

---



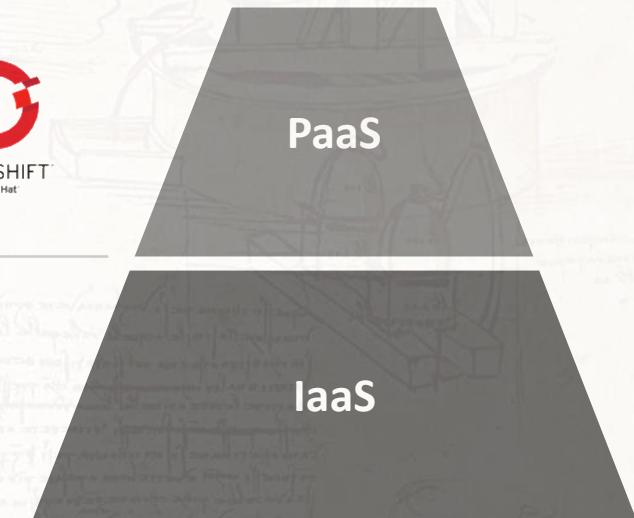
# Cloud Forensics Means...



PaaS



IaaS



# Cloud Forensics Means...



Engine Yard®



PaaS



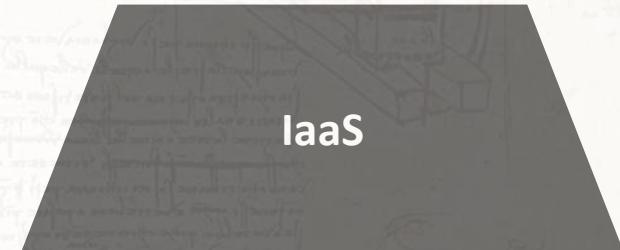
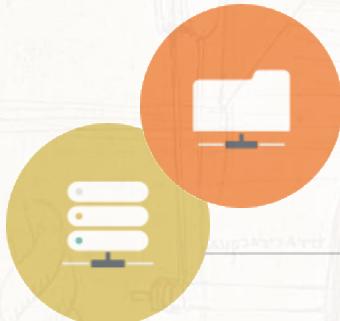
IaaS

# Cloud Forensics Means...

---

Since they won't let me talk for 8hrs

...we'll focus on IaaS today ☺



# 5 Major Challenges

---

1. Data residence
2. Physical acquisition
3. Instance isolation
4. Hypervisor introspection & data integrity
5. Lack of CSP collaboration/support



# Data Residence

---

- Need to know where the data is
- This adds validity to your investigation
- This, in turn, makes your results more credible





# Data Residence: AWS (2008)

---

## Where is my data stored?

Amazon S3 offers storage in the United States and in Europe (within the EU). **You can specify where you want to store your data when you create your Amazon S3 buckets.**

- Source: [https://web.archive.org/web/20081016104719/http://aws.amazon.com/s3/faqs/#Where\\_is\\_my\\_data\\_stored](https://web.archive.org/web/20081016104719/http://aws.amazon.com/s3/faqs/#Where_is_my_data_stored)



# Data Residence: AWS (2013)

---

## Where is my data stored?

Amazon S3 offers storage in the US Standard, US West (Oregon), US West (Northern California), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), South America (Sao Paulo), and AWS GovCloud (US) Regions. You specify a Region when you create your Amazon S3 bucket. ***Within that Region, your objects are redundantly stored on multiple devices across multiple facilities.***

- Source: [https://web.archive.org/web/20130502034405/http://aws.amazon.com/s3/faqs/#Where\\_is\\_my\\_data\\_stored](https://web.archive.org/web/20130502034405/http://aws.amazon.com/s3/faqs/#Where_is_my_data_stored)



# Data Residence: AWS (Now...)

---

## Where is my data stored?

You specify a region when you create your Amazon S3 bucket. ***Within that region, your objects are redundantly stored on multiple devices across multiple facilities. Please refer to Regional Products and Services for details of Amazon S3 service availability by region.***

Source: [http://aws.amazon.com/s3/faqs/#Where\\_is\\_my\\_data\\_stored](http://aws.amazon.com/s3/faqs/#Where_is_my_data_stored)

# Data Residence: Windows Azure (2012)

---



## Location of Customer Data

Microsoft may transfer Customer Data within a major geographic region (e.g., within Europe) for data redundancy or other purposes. For example, Windows Azure Storage geo-replication feature ***will replicate*** Windows Azure Blob and Table data, at no additional cost, ***between two sub-regions within the same major region for enhanced data durability*** in case of a major data center disaster.

However, customers can choose to disable this feature.

- Source: <https://web.archive.org/web/20120510055557/https://www.windowsazure.com/en-us/support/trust-center/privacy/>

# Data Residence: Windows Azure (2013)

---



## Location of Customer Data

Microsoft may transfer Customer Data within a major geographic region (e.g., within Europe) for data redundancy or other purposes. For example, Windows Azure replicates Blob and Table data between two sub-regions within the same major region for enhanced data durability in case of a major data center disaster.

• Source: <https://web.archive.org/web/20130512060355/http://www.windowsazure.com/en-us/support/trust-center/privacy/>

**Where'd the “customers can choose to disable this feature” part go?**

# Data Residence: Windows Azure

---



## You know where your customer data is located

Microsoft maintains an ever-expanding network of cloud-scale datacenters in locations around the globe, and verifies that each meets strict security requirements. As a Microsoft Cloud customer, you will know the location where your data is stored. ***Each Microsoft cloud service has its own location policies for customer data.***

- Source: <https://www.microsoft.com/en-us/TrustCenter/Privacy/default.aspx> & <https://www.microsoft.com/en-us/TrustCenter/Privacy/You-are-in-control-of-your-data>



# Data Residence: GCE (2013)

**Do I have the option of using a regional data center in selected countries?**

Yes, Google Compute Engine offers datacenter options in Europe and within the United States. These datacenter options are designed to provide low latency connectivity options from those regions, however ***at this time selection of datacenter will make no guarantee that project data at rest is kept only in that region.***

- Source: <https://web.archive.org/web/20130429150332/https://developers.google.com/compute/docs/faq>



Google Compute Engine

# Data Residence: GCE (2014)

## Do I have the option of using a regional data center in selected countries?

Yes, Compute Engine offers data centers in the United States, Europe, and Asia. These data center options are designed to provide low latency connectivity options from those regions.

- Source: <https://web.archive.org/web/20140913123317/https://developers.google.com/compute/docs/faq>

Where'd the “*project data at rest is kept only in that region*” part go?



# Data Residence: GCE (2016)

**Do I have the option of using a regional data center in selected countries?**

Yes, Compute Engine offers data centers in the United States, Europe, and Asia. These data center options are designed to provide low latency connectivity options from those regions. ***For specific region information, including the geographic location of regions, see Regions and Zones.***

- Source: <https://developers.google.com/compute/docs/faq>

**No mention of where your data *might* be located since 2013...**

# Multi-Cloud Data Residence?

---



# Physical Acquisition

---

- Unless you own the cloud architecture...
- Or have the bent the CSP to your will...
- You may be stuck with snapshots and/or logical imaging



# Image Acquisition: AWS

---

- There are 3+ ways that I know of
  1. Snapshot the EBS volume, mount, and copy locally
  2. Have AWS ship you the data from S3 on physical device
  3. Use AMI Tools to compress, encrypt, and sign a snapshot





# Image Acquisition: AWS EBS

---

- Launch a clean Amazon Linux AMI
- Stop the instance of the root volume you wish to capture
- Detach the `/dev/sda1` volume
- Create a snapshot of the now detached `/dev/sda1` volume
- Attach the `/dev/sda1` volume to the new AMI as `/dev/sdf` (don't mount)



# Image Acquisition: AWS EBS

---

- Create a new EBS volume the same size as the root volume you wish to capture
- Attach this new volume as /dev/sdg
- Then use these commands:
  - sudo mkfs -t ext3 /dev/sdg
  - sudo mkdir /vol1
  - sudo mount /dev/sdg /vol1
  - sudo chown ec2-user /vol1
- Use dd to make an image of /dev/sdf
  - sudo dd if=/dev/sdf | gzip -c > /vol1/sda1.img.gz



# Image Acquisition: AWS EBS

- Create a new EBS volume the same size as the root volume you wish to capture
- Attach this new volume as /dev/sdg
- Then use these commands:
  - sudo mkfs -t ext3 /dev/sdg
  - sudo mkdir /vol1
  - sudo mount /dev/sdg /vol1
  - sudo chown ec2-user /vol1
- Use dd to make an image of /dev/sdf
  - sudo dd if=/dev/sdf | gzip -c > /vol1/sda1.img.gz

A screenshot of a forum post titled "Re: Creating a forensic image". The post is by "Lance@AWS" on January 5, 2012, at 6:39 PM, in response to a post from "Albatross Digital, LLC". The message content is:

Hi Albatross Digital,

If I understand your need correctly, I would consider using dd to make an image of the EBS root volume (ie.. /dev/sda1) you wish to capture.



# Image Acquisition: AWS S3

---

- Amazon provides a service to export data from S3 onto a physical device and ship it to the requestor
- Customer must provide the storage device and is billed \$80 per storage device handled plus \$2.49 per data-loading hour
- In EBS or S3 methods it is impossible to verify the integrity of the forensic disk image\*

Source: J. Dykstra, A.T. Sherman / Digital Investigation 9 (2012) S90–S98

# Image Acquisition: AWS S3 + AMI Tools

---



- ec2-bundle-vol
  - Creates a bundled AMI by **compressing, encrypting and signing** a snapshot of the local machine's root file system
- ec2-migrate-bundle
  - Copies a bundled AMI from one Region to another
- ec2-download-bundle
  - Downloads the specified bundles from S3 storage

# Dykstra/Sherman Experiment

---

- Experiment by J. Dykstra, A.T. Sherman
  1. Manual installation of EnCase Servlet and FTK Agent
  2. Used VM introspection for complete drive image
  3. AWS Export process (ship a drive)

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

# Introspection & Data Integrity

---

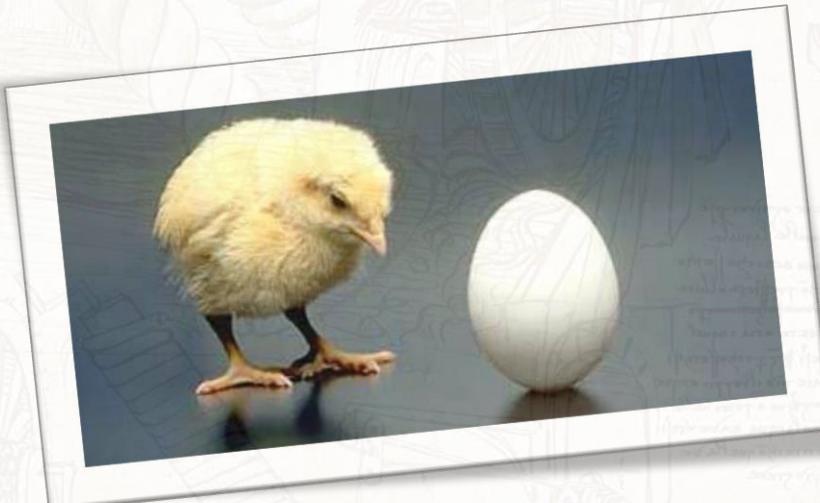
- Introspection is not new
  - First introduced by T. Garfinkel and M. Rosenblum in *A Virtual Machine Introspection Based Architecture for Intrusion Detection*
- Way to look into current state of the guest virtual machine
  - e.g. covert, low-level access to read find processes and threads, recover files mapped in memory, and extract information about the Windows registry



# Introspection & Data Integrity

---

- Enabled by provider
- Transparent to tenant and server instance
- Great for forensic acquisition
  - but hard to prove integrity



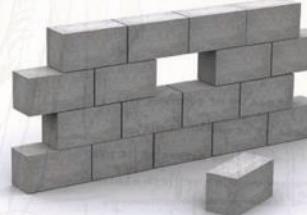
# Instance Isolation

---

- **Several conditions must be met in order for a cloud instance to be successfully isolated:**
  - **Location:** The physical location of the instance is known
  - **Incoming & Outgoing Blocking:** The instance is blocked from sending/receiving communications to/from the outside world



Source: Waldo Delport and Martin Olivier - *Isolating Instances In Cloud Forensics*



# Instance Isolation

---

- **Several conditions must be met in order for a cloud instance to be successfully isolated:**
  - **Collection:** Evidence from the instance can be gathered
  - **Non-Contamination:** Evidence from the instance is not contaminated by the isolation process
  - **Separation:** Information unrelated to the incident is not part of the isolation process

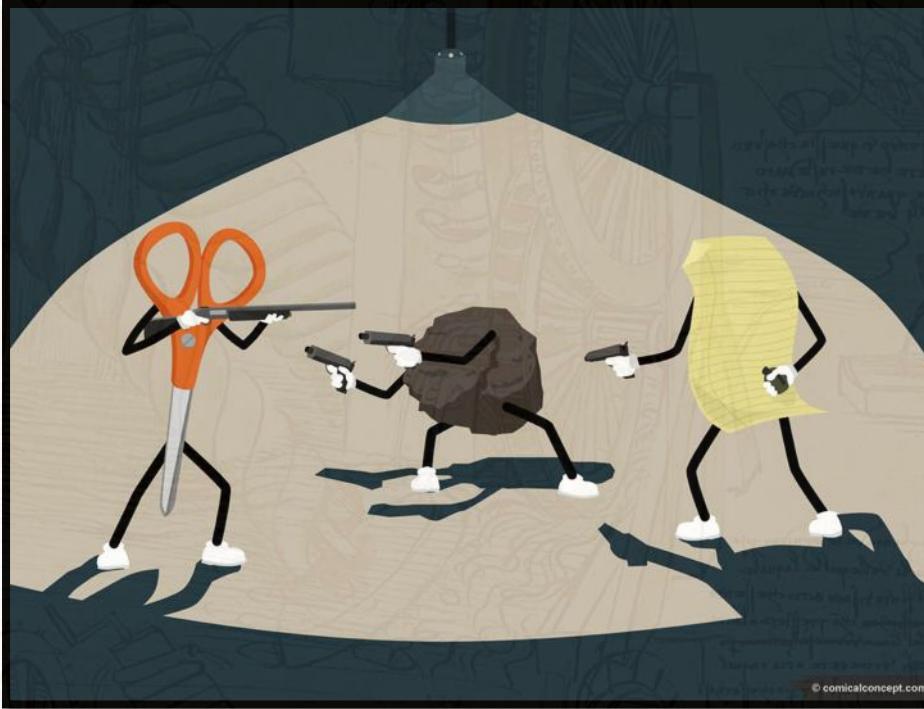


Source: Waldo Delport and Martin Olivier - *Isolating Instances In Cloud Forensics*



# CSP Collaboration/Support

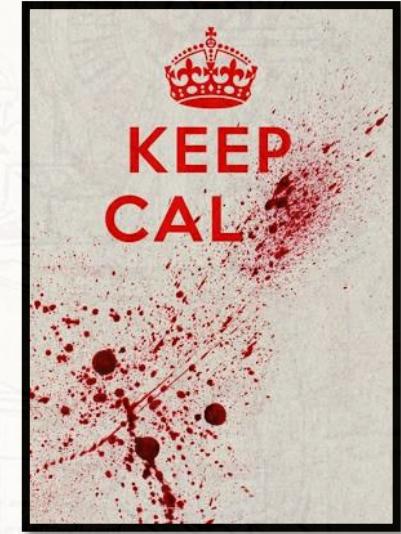
---



# CSP Collaboration/Support

---

- Most providers have people that can help
- Contracts should indicate level of effort...
  - That you're expected to exert
  - That they're willing to exert
- Ask for:
  - Samples/examples of past investigations
  - Methodologies employed
  - Credentials of staff
  - Interviews with CSP team members

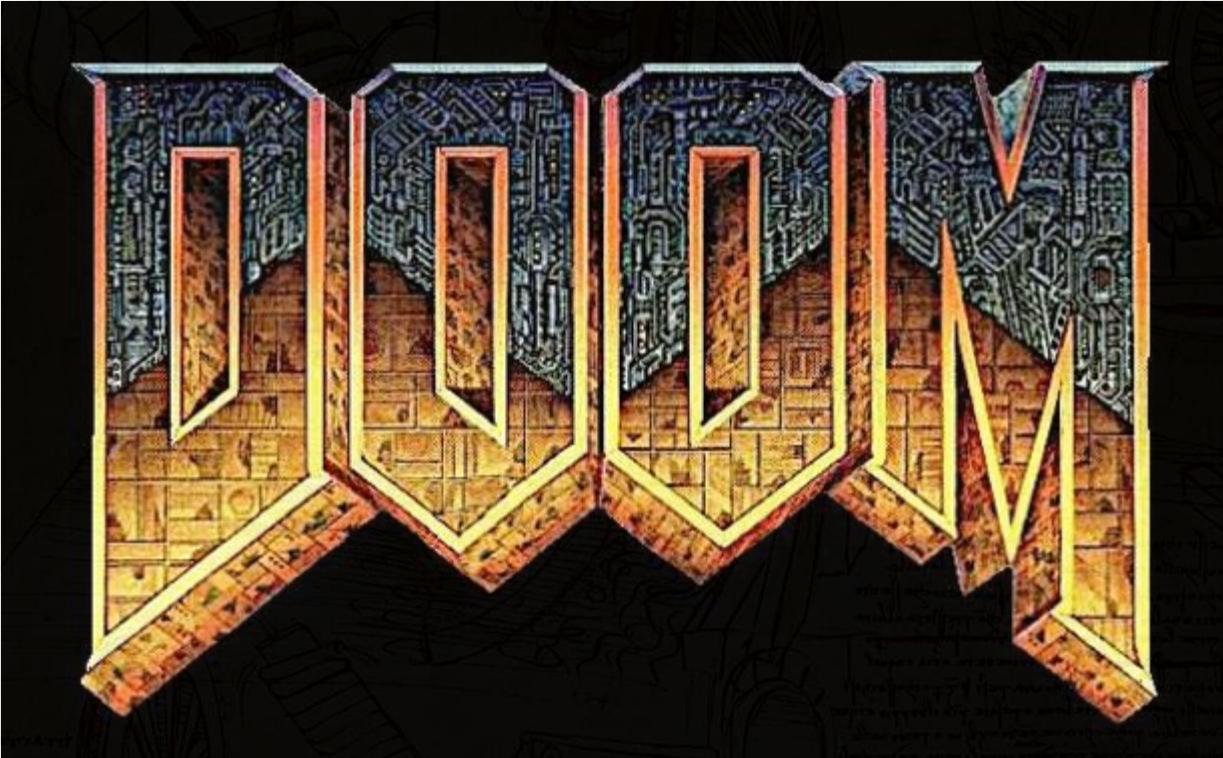


# How Existing Forensics/IR Tools Can Help

...And What They Can Do Better

# It's Not All...

---



# And It's Not All Gloom...

---



# New Architecture, Similar Tools

- Your old tools and techniques may still work
  - Some, but not all



REDLINE

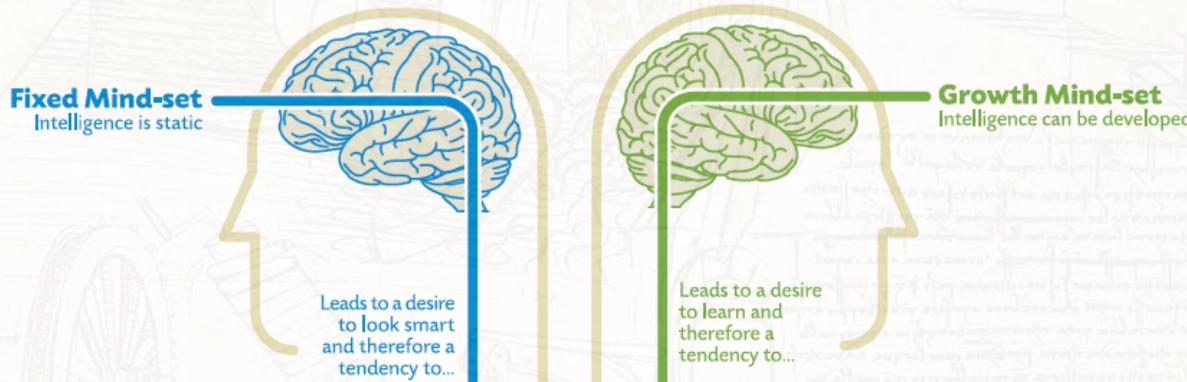


ARSENAL RECON

# Not Just Technical Challenges

---

- Biggest challenge is mindset
- Need to grow comfortable with
  - Storing images/data/ off-site (a.k.a. *The Cloud*)
  - Processing off-site (a.k.a. *The Cloud*)
  - Launching off-site analysis consoles in...you guessed it, *The Cloud!*



# Existing Tools Can Be Used...

---

- e.g. NBDServer
  - Serves the (XP, Win 7, Win 2008) server as a read-only network block device
  - Also possible to use this tool (w/Volatility or Rekall) to image the Windows system RAM across the network to your client

# Existing Tools Can Be Used...

---

```
[server] nbdserver.exe -c 192.168.2.197 -f  
\\.\PHYSICALDRIVE0 -n0
```

```
[client] modprobe nbd
```

```
[client] nbd-client 192.168.2.157 60000 /dev/nbd0
```

# This starts the client, tells it to look for the server on 192.168.2.157, use port 60000 and create the new network block device as /dev/nbd0.

```
[client] f1s -f ntfs -m C: -r /dev/nbd0 > test.fls
```

# NBD-Server Advances

---

- <https://github.com/yoel/nbd>
  - Latest commit [3c610bd](#) 8 days ago
- <https://github.com/reidrac/swift-nbd-server>
  - This is a NBD server for OpenStack Object Storage (Swift)
  - Latest commit [dafc44a](#) on Mar 30, 2016
- <https://github.com/psychomario/PyPXE>
  - Pure Python2 PXE (DHCP-(Proxy)/TFTP/HTTP/NBD) Server
  - Latest commit [6cc6b51](#) on Dec 22, 2016

**NBD**

Network Block  
Device

# F-Response Cloud Connector

- F-Response 4.0.4
  - The new Cloud Connector
  - Let's you 'mount'
    - Amazon S3 Buckets
    - HP, Rackspace Cloud Containers
    - Windows Azure Blob Storage Containers



# F-Response Cloud Connector

---

- F-Response 4.0.4
    - The new Cloud Connector
    - Let's you 'mount'
      - Amazon S3 Buckets
      - HP, Rackspace Cloud Containers
      - Windows Azure Blob Storage Containers
  - F-Response (as of 3/21/16)
    - Let's you 'mount'
      - Amazon S3 & Microsoft Windows Azure Blob Storage
      - Box.com & Dropbox
      - Gmail (OAuth) & Google Apps for Business Drives
      - HP Helion & Rackspace Cloud Files
      - Office 365 email, OneDrive, and Sharepoint
- 
- [www.leocybersecurity.com](http://www.leocybersecurity.com)

# Finally!!!

F-Response Universal now available on Amazon EC2

Apr/22/2015



We are very pleased to announce that F-Response Universal, our newest and most comprehensive version of F-Response is now available as a Amazon EC2 Machine Image (AMI).

We've been working with multiple customers to refine the Amazon EC2 process and present a clean and simple way for new customers looking to stand up F-Response Universal in the Amazon cloud.

REF: <https://www.f-response.com/blog/f-response-univ-on-ec2>

# Chad Tilbury's Blog Post

Like many great inventions, the idea behind F-Response is so simple and elegant it is hard not to punish yourself for not thinking of it. Using the iSCSI protocol to provide read-only mounting of remote devices opens up a wealth of options for those of us working in geographically dispersed environments. I have used it for everything from remote imaging to fast forensic triage to live memory analysis. F-Response is vendor-neutral and tool independent, essentially opening up a network pipe to remote devices and allowing the freedom of using nearly any tool in your kit. The product is so good, I really wouldn't blame them for just sitting back and counting their money. Luckily, counting money gets boring fast, so instead the folks at F-Response have kept innovating and adding value. Their latest additions are new "Connector" tools: Database, Cloud, and Email.



Chad Tilbury  
@chadtilbury

REF: <http://forensicmethods.com/fresponse-cloud-forensics>

# AccessData Joins The Party

---

Wednesday, November 01, 2017 (11:51:29)

## AccessData's AD Lab Becomes First Forensics Platform Available On AWS And Azure

[AccessData Group](#) today announced that its AD Lab centralized investigations platform is now the first product in its category to be available to users in a cloud-based environment.

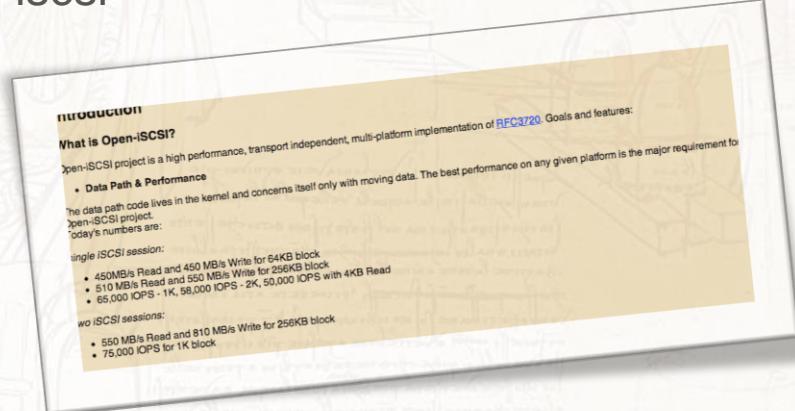
REF: <https://www.forensicfocus.com/News/article/sid=3011/>

[www.leocybersecurity.com](http://www.leocybersecurity.com)

# I Once Had An Idea...

---

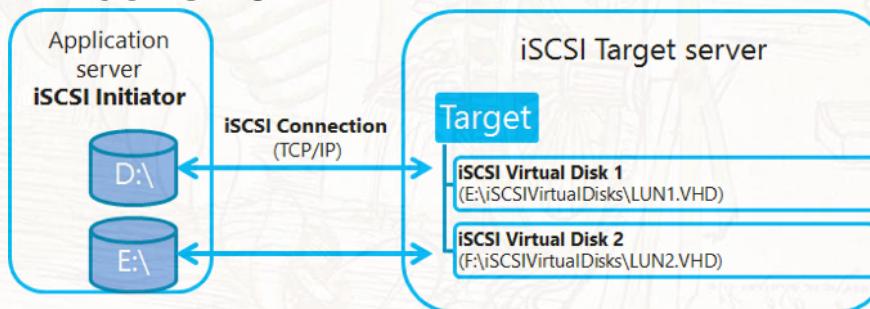
- It went something like this...
  - “It would be great if someone built me (and everyone else doing forensics) a client-server architecture based on the Open-iSCSI protocol”
  - <https://github.com/mikechristie/open-iscsi>
  - <http://www.open-iscsi.org/>



# Windows 2008 R2 ++

---

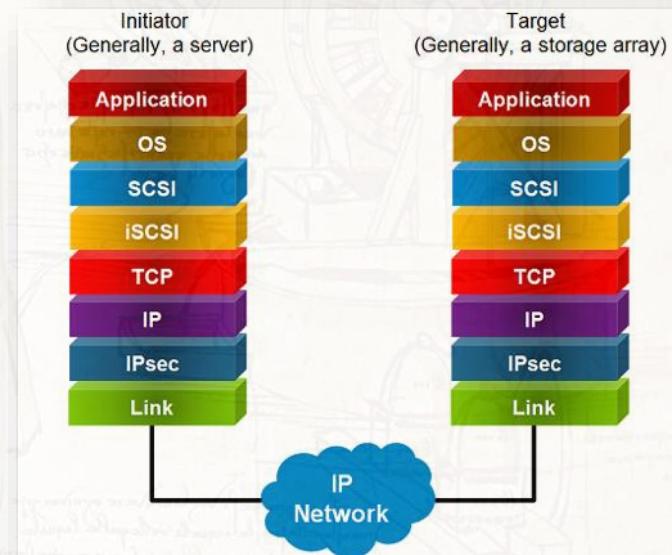
- The iSCSI Target in Microsoft Windows Server
  - Downloadable in Windows 2008 R2
  - Standard in Windows 2012



- Fantastic walkthrough and PowerShell scripts to configure
  - <http://www.lazywinadmin.com/2013/07/create-iscsi-target-using-powershell-on.html>

# iSCSI Initiator Clients

- OS X
  - iSCSI Initiator for OS X
    - <https://github.com/iscsi-osx/iSCSIInitiator>
- FreeBSD
  - FreeBSD iSCSI Initiator
    - <https://github.com/oberstet/iscsi>
- Linux (Ubuntu)
  - open-iscsi
    - <https://help.ubuntu.com/lts/serverguide/iscsi-initiator.html>

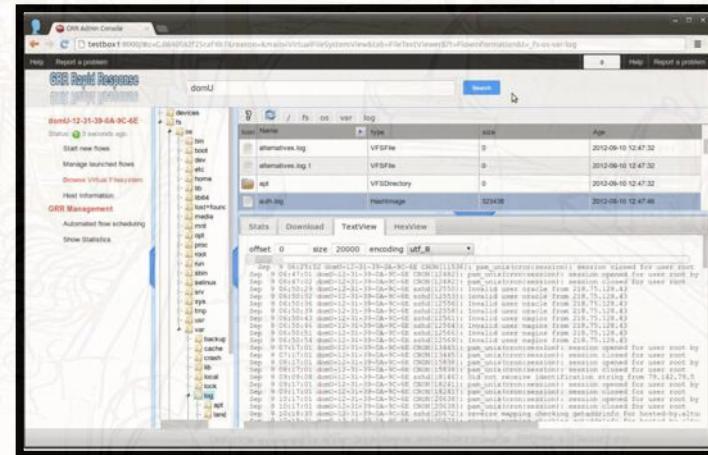


# GRR

- GRR Rapid Response
  - Remote live forensics for incident response
  - Was in its infancy back in 2011/2012

## Why GRR?

- Tell me if this machine is compromised
  - (while you're at it, check 20000 of them)
- Joe saw something weird, check his machine
  - (p.s. Joe is on holiday in Cambodia and on 3G)
- Why did a packet containing "fooooo" go from A to B?
  - (by the way, we're not sure what A was)
- Forensically acquire 25 machines for analysis
  - (p.s. they're in 5 continents and none are Windows)



The screenshot shows the GRR Admin Console interface. On the left, there's a file browser window titled 'domU' showing various system logs like 'alternatives.log', 'alternatives.log.1', 'nft', and 'wtmp'. On the right, a large window displays a log of network traffic. The log table has columns for 'offset', 'size', 'encoding', and 'hex'. The log entries show various network packets, with some specific ones highlighted in yellow. One entry highlights a packet from IP 210.75.128.43 to port 22, with the hex dump showing '0x041501 4e454d45 00000000 00000000'. The log also includes a note about 'invalid user oracle'.

# GRR

---



- Much more mature now
  - Cross-platform support for Linux, OS X and Windows clients
  - Live remote memory analysis using open source memory drivers for Linux, OS X and Windows via the Rekall memory analysis framework
  - Powerful search and download capabilities for files and the Windows registry
  - Secure communication infrastructure designed for Internet deployment
- <https://github.com/google/grr>

# Other Tools

---

- <http://wirespeed.io/> (now known as <https://evimetry.com/>)
  - “Wirespeed gives you the ability to analyse evidence without the delays of traditional acquisition, regardless of whether your target device is local, or across the internet.”
- <https://github.com/google/turbinia/>
  - OSDFCon submission by Cory Altheide & Johan Berggren entitled “*Turbinia: Cloud-scale forensics*”
- <https://www.brimorlabs.com/tools/>
  - Live Response Collection – Allosaurus Build
    - Automated tool that collects volatile data from Windows, OSX, and \*nix based operating systems

# ThreatResponse: The New Hotness?

---

- ThreatResponse
  - “A Free Open Source Security Suite for Hardening and Responding in AWS.”
  - <http://www.threatresponse.cloud>

## ThreatResponse Suite



AWS\_IR CLI

AWS\_IR automates your incident response with zero security preparedness assumptions. It can handle key and host compromises and collects all pertinent data in an S3 bucket along with the ThreatResponse Web workstation.



Incident Pony™

Incident Pony is a first of its kind case management and Incident Response orchestration tool specifically designed for AWS. By wrapping our open source tools in a web front-end we've made it even easier to manage incidents in your cloud.



Margarita Shotgun

Command line utility that works with or without Amazon EC2 instances to parallelize remote memory acquisition.

1. Load the appropriate module from the ThreatResponse kernel module warehouse
2. Acquire the memory by streaming to an S3 bucket using multi-part upload over ssh

# ThreatResponse: The New Hotness?

ThreatResponse

Acquire Analyze Advise

### Process and Analyze Assets for cr-16-071619-cdd5

The ThreatResponse interface displays three main asset types: MEMORY (blue), DISK (red), and LOGS (pink). Below these, a section titled 'Disks' shows a table for 'Snapshots for us-west-2'. The table includes columns for 'Id', 'Instance', 'Volume', and 'Processed'. Four rows are listed, each with an 'ADD' button next to it.

LOG2TIMELINE ALL			
Snapshots for us-west-2			
ID	Instance	Volume	Processed
snap-a3d00be1	Instance Missing	vol-49c159c9	<button>ADD</button>
snap-acf4f3ea	Instance Missing	vol-3ec058be	<button>ADD</button>
snap-52b3ce08	Instance Missing	vol-71cf48f8	<button>ADD</button>
snap-c68d7c98	Instance Missing	vol-1fcf579f	<button>ADD</button>

timeSketch

Overview Explore Stories Views Timelines

### Search

11 events (0.007s)

Date	Event Description	Details
2015-09-18T07:54:38+00:00	User: shutdown Computer Name: 3.16.0-44-generic Terminal: system boot PID: 0 Terminal_ID: 32382 Status: RUN_LVL IP Address: localhost Exit: 0	[Start Time] [Content Modification Time]
2015-09-16T20:25:54+00:00	User: dean Computer Name: 192.168.1.11 Terminal: pts/0 PID: 16304 Terminal_ID: 808416116 Status: USER_PROCESS IP Address: 192.168.1.11 Exit: 0	[Start Time] [Content Modification Time]
2015-09-16T20:25:54+00:00	User: N/A Computer Name: localhost Terminal: pts/0 PID: 16304 Terminal_ID: 0 Status: DEAD_PROCESS IP Address: localhost Exit: 0	[Start Time] [Content Modification Time]
2015-09-06T17:13:26+00:00	User: dean Computer Name: 192.168.1.11 Terminal: pts/0 PID: 16304 Terminal_ID: 808416116 Status: USER_PROCESS IP Address: 192.168.1.11 Exit: 0	[Start Time] [Content Modification Time]
2015-08-29T13:26:49+00:00	User: deanfrom 10.0.8.6:52673 using authentication method: publickey ssh pid: 6944	[Content Modification Time]
2015-08-29T13:26:53+00:00	User: dean Computer Name: 192.168.1.11 Terminal: pts/0 PID: 6754 Terminal_ID: 808416116 Status: USER_PROCESS IP Address: 192.168.1.11 Exit: 0	[Content Modification Time]
2015-08-29T13:22:53+00:00	User: dean Computer Name: 192.168.1.11 Terminal: pts/0 PID: 6754 Terminal_ID: 808416116 Status: USER_PROCESS IP Address: 192.168.1.11 Exit: 0	[Content Modification Time]
2015-08-29T13:22:45+00:00	User: dean Computer Name: 192.168.1.11 Terminal: pts/0 PID: 6754 Terminal_ID: 808416116 Status: USER_PROCESS IP Address: 192.168.1.11 Exit: 0	[Content Modification Time]
2015-08-29T13:22:05+00:00	User: dean Computer Name: 192.168.1.11 Terminal: pts/0 PID: 6666 Terminal_ID: 808416116 Status: USER_PROCESS IP Address: 192.168.1.11 Exit: 0	[Content Modification Time]
2015-08-29T13:20:36+00:00	User: dean Computer Name: 192.168.1.11 Terminal: pts/0 PID: 5959 Terminal_ID: 808416116 Status: USER_PROCESS IP Address: 192.168.1.11 Exit: 0	[Content Modification Time]

# Continued Evolution Required

---

- Cloud presents challenges
- Cloud also presents opportunities



# Advantages Of Conducting Forensics/IR

In Cloud Environments

# Advantages (now and future)

- Automated instance isolation
- On-demand forensic workbenches
- Automated timeline generation
- Dynamic analysis ‘workers’
- Distributed file carving
- Multi-cloud analysis



# More Information

---

- NIST
  - Special Publication 800-86 - Guide to Integrating Forensic Techniques into Incident Response
    - <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>
  - Cloud Computing Forensic Science Working Group (NCC-FSWG)
    - <http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudForensics>
      - ***Moving at the speed of NIST*** – © 2016, Andrew Hay

# More Information (Continued...)

---

- Introduction of iSCSI Target in Windows Server 2012
  - <https://blogs.technet.microsoft.com/filecab/2012/05/21/introduction-of-iscsi-target-in-windows-server-2012/>
- Cloud Forensics Bibliography
  - [http://www.forensicswiki.org/wiki/Cloud\\_Forensics\\_Bibliography](http://www.forensicswiki.org/wiki/Cloud_Forensics_Bibliography)
- SANS Digital Forensics and Incident Response Blog
  - <https://digital-forensics.sans.org/blog>

# More Information (Continued...)

---

- Forensics in AWS: an introduction
  - <https://blyx.com/2016/03/11/forensics-in-aws-an-introduction/>
- How I learned to stop worrying and love the cloud: Azure Forensics for the Security Responder
  - <https://blogs.msdn.microsoft.com/azuresecurity/2015/08/14/how-i-learned-to-stop-worrying-and-love-the-cloud-azure-forensics-for-the-security-responder/>

# Summary

- Cloud forensics and incident response require an open mind
- Cloud can be used to help with complex investigations
- Tools continue to evolve to better handle dynamic environments





# Thank You

---

## Questions?

[www.leocybersecurity.com](http://www.leocybersecurity.com)

-  **Andrew Hay, CTO**  
**LEO Cyber Security**  
 [+1.415.940.9660](tel:+14159409660)  
 [andrewsmhay@leocybersecurity.com](mailto:andrewsmhay@leocybersecurity.com)  
 [@andrewsmhay](https://twitter.com/@andrewsmhay)
  
-  **LEO Cyber Security**  
6211 West NW Highway,  
Suite #2103,  
Dallas, TX 75225  
 [+1.469.844.3608](tel:+14698443608)  
 [www.leocybersecurity.com](http://www.leocybersecurity.com)