Survey on Cloud Forensics

Marco Iannuzzi
marco.iannuzzi@studio.unibo.it
Outline

Cloud Computing
- Definition
- Essential Characteristics
- Service Model

Digital Forensics
- Definition
- ISO 27037
- Digital evidence handling processes
- Case Study: Networked devices

Cloud Forensics
- Definition
- The problems of Cloud Forensics
- Challenge-based approach
- Digital evidence handling processes in Cloud Forensics
- Formal analysis of the challenges
- Case Study
- Conclusion
1. Definition
2. Essential Characteristics
3. Service Model
# The Definitions of Cloud Computing

<table>
<thead>
<tr>
<th>NIST</th>
<th>Gartner</th>
<th>CSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>• [1] Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.</td>
<td>• [2] Cloud computing is a style of computer where scalable and elastic IT-related capabilities are provided ‘as a service’ to multiple external customers using Internet Technologies</td>
<td>• [3] Cloud computing is an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates application and information resources from underlying infrastructure, and the mechanisms used to deliver them. Cloud enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction Through Optimized And Efficient computing</td>
</tr>
</tbody>
</table>

[1] NIST Definition of Cloud Computing, Special Publication (SP) 800-145  
[2] [3] Keyun Ruan, Ibrahim Baggili (PhD), Prof Joe Carthy, Prof Tahar Kechadi University College Dublin, Zayed University, Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis
What is Cloud Computing?

What is cloud computing?

Cloud computing is redefined to include everything we already do.

- Strongly Disagree: 27.16%
- Disagree: 38.27%
- Neutral: 20.99%
- Agree: 7.41%
- Strongly Agree: 0%

Cloud computing is an evolution, not revolution

- Strongly Disagree: 24.17%
- Disagree: 23.46%
- Neutral: 54.32%
- Agree: 18.52%
- Strongly Agree: 0%

Cloud computing is a new way of delivering computing resources, not a new technology

- Strongly Disagree: 10%
- Disagree: 26.25%
- Neutral: 41.25%
- Agree: 20%
- Strongly Agree: 0%

CSA definition

- Strongly Disagree: 9.76%
- Disagree: 25.61%
- Neutral: 37.80%
- Agree: 25.61%
- Strongly Agree: 0%

Gartner definition

- Strongly Disagree: 3.70%
- Disagree: 11.11%
- Neutral: 62.96%
- Agree: 22.22%
- Strongly Agree: 1.91%

NIST definition

- Strongly Disagree: 6.17%
- Disagree: 13.58%
- Neutral: 54.32%
- Agree: 24.69%
- Strongly Agree: 0%

*Keyun Ruan, Ibrahim Baggili (PhD), Prof Joe Carthy, Prof Tahar Kechadi University College Dublin, Zayed University, Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis. (Mar 2011)
Cloud Computing providers

- Dropbox
- iCloud
- Amazon Web Services
- Microsoft Azure
Essential Characteristics

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service
Service Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
Digital Forensics

1. Definition
2. ISO 27037
3. Digital evidence handling processes
4. Case Study: Networked devices
Digital Forensic Science

• The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.
ISO 27037

- The first of a developing family of international standards that seek to create a common baseline for the practice of digital forensics.

- Its intent is to facilitate the usability of evidence obtained in one jurisdiction by a legal process operating in another jurisdiction.

Digital Evidence Handling Processes According to ISO 27037

- ISO 27037 Only addresses the initial steps of the forensics process: identifying, obtaining and preserving potential digital evidence.
Digital Evidence Handling Processes
Identification

- Identification of items that may be or may contain potential digital evidence.
- Digital Evidence physical representation VS virtual representation
Digital Evidence Handling Processes
Collection

- Process of collection of items that contain potential digital evidence.
- Equivalent to the standard law enforcement practice of seizing items containing potential digital evidence under authority of a legal order.
- Removing them to a forensics lab or other facility for processing and analysis.
Digital Evidence Handling Processes

Acquisition

- *Process of creating a copy of data within a defined set.*

- After potential digital evidence is identified, it must either be acquisition.

- Is more common in the private sector due to the need to minimize business impact of an ongoing investigation.

- Reducing the impact on other applications.

- Integrity measures to ensure that the copy has not been modified since acquisition.
Digital Evidence Handling Processes

Preservation

- Process to maintain and safeguard the integrity and/or original condition of the potential digital evidence
- Evidence preservation helps assure admissibility in a court of law
- Digital evidence is notoriously fragile, and is easily changed or destroyed, and potential digital evidence may spend a significant period of time in storage before it is analyzed or used in a legal proceeding.
- Strict access controls and appropriate environment controls.
Case Study: Networked devices

- It is difficult to ascertain where the potential digital evidence being sought is stored.

- The data could be located anywhere on the network
Case Study: Networked devices
Identification

Consider the following aspects as a means of identification:

- Device characteristics (observable characteristics)

- Device label (For powered off mobile devices): information obtained from within the battery cavity

- Reverse lookup (In the case of mobile phones): identify the network operator.
Case Study: Networked devices
Physical incident scene search and documentation

- Photographing, videographing or sketching the scene as it appeared upon entry:

- Document the type, brand, model and serial numbers of any digital devices used (and their associated items such as memory cards, sim cards ecc...).

- Identify services to understand dependencies before deciding to disconnecting the device (to protect the potential digital evidence).

- Not turn off or on the devices
Case Study: Networked devices
Collection, acquisition and preservation

- Collect or acquire the potential digital evidence

- Digital evidence copies may not pass standard verification functions such as hashing

- If the devices cannot be disconnected from the network:
  - Live acquisition (Wi-Fi or Bluetooth devices might change pairing information on potential evidential devices...)
  - If he decided to follow an acquisition process, the network devices should be kept running
    - Consider the possibility of sabotage
Cloud Forensics

1. Definition
2. The problems of Cloud Forensics
3. Approach based on challenges
4. Digital evidence handling processes in Cloud Forensics
5. Formal analysis of the challenges
6. Case Study
7. Conclusion

- Cloud computing forensic science is the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation and reporting of digital evidence.

*Keyun Ruan, University College Dublin, Cloud Forensics: challenges & opportunities, 2010*
The problems of Cloud Forensics

Cloud Computing is radically changing how information technology service are created, delivered, accessed and managed

• Exacerbates the Problem for digital forensic activities
• New front for Cyber crime investigation
• Digital Forensics practitioners must extend their expertise and tools
• The amount of forensic data that must be processed is outgrowing the ability to process it in a timely manner

The size of the average digital forensics case is growing of 35% per year
The 3 dimensions of Cloud Forensics
## The 3 dimensions of Cloud Forensics

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Agree or Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical dimension</td>
<td>84%</td>
</tr>
<tr>
<td>Legal dimension</td>
<td>84%</td>
</tr>
<tr>
<td>Organizational dimension</td>
<td>75%</td>
</tr>
<tr>
<td>Social dimension</td>
<td>42%</td>
</tr>
</tbody>
</table>

*Keyun Ruan, Ibrahim Baggili (PhD), Prof Joe Carthy, Prof Tahar Kechadi University College Dublin, Zayed University, Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis. (Mar 2011)*
Challenge-based approach

Technical Dimension
- DATA COLLECTION
- LIVE FORENSICS
- VIRTUALIZED ENVIRONMENTS
- EVIDENCE SEGREGATION

Organizational Dimension
- EXTERNAL DEPENDENCY CHAINS
- INTERNAL STAFFING
- SERVICE LEVEL AGREEMENTS

Legal Dimension
- MULTIPLE JURISDICTIONS AND TENANCY
Data Collection

• Identifying, labeling, recording and acquiring forensic data

• Client/side or server/side

• Access to forensic data varies considerably based on the cloud model that is implemented

• Service Level Agreements
Live Forensics

- Live Forensics in Digital Forensics Versus Live Forensics in Cloud Forensics

- The problem of deleted data
Live Forensics – Possible Solutions...

- Memory snapshot
- Timeline of an event
- Key aspect in digital evidence handling: Repeatable.
Evidence Segregation

- Segregate resources during investigations without breaching the confidentiality of the other tenants that share the infrastructure

- Storage is highly virtualized. Physical disk devices may be virtualized as a set of logical units presented to a cloud user (or a server supporting a cloud user) with RAID level, cache settings, etc.

- Units may even be transparently moved from place to place based on global performance
Evidence Segregation – Possible Solution...

- Procedures and tools must be developed to physically locate forensic data with specific timestamps while taking into consideration the juris-dictional issues
Virtualized Environments

- Virtualization reduced IT costs
- The logical units may even be transparently moved from place to place based on global performance and availability issues
- Cloud computing provides computational redundancy by replicating and distributing resources.
- Instances of servers run as virtual machines monitored and provisioned by a hypervisor
Virtualized Environments – Possible Solution...

- Create non-intrusive system snapshots on live systems or plugging into the hypervisor to record data on the OS kernel level.
ORGANIZATIONAL DIMENSION
<table>
<thead>
<tr>
<th>Cloud Forensics Stakeholders</th>
<th>Consumer</th>
<th>Provider</th>
<th>Broker</th>
<th>Auditor</th>
<th>Carrier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Enterprise Customer</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>An organizational user of Cloud services</td>
</tr>
<tr>
<td>Cloud End-User (Employee of Enterprise Customer)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>An individual user of cloud services who is a member of an Enterprise Customer organization</td>
</tr>
<tr>
<td>Cloud Individual Customer</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>An individual user of cloud services who is not consuming those services as a member of an Enterprise Customer organization</td>
</tr>
<tr>
<td>Cloud Service Vendor</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>Provider of cloud services</td>
</tr>
<tr>
<td>Communication Services Vendors</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>Provide data transport between Cloud consumers and Cloud providers</td>
</tr>
<tr>
<td>Third-party, Independent Assessors</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>Independent of consumers and providers, they determine whether services being provided comply to SLA</td>
</tr>
<tr>
<td>State Regulators</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>Regulatory bodies with public oversight responsibilities, typically appointed by State or Local Governments (or at a broader level, County or Province or Parish, etc.)</td>
</tr>
<tr>
<td>Federal Regulators</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>Regulatory bodies with public oversight responsibilities, typically appointed by the Federal Government</td>
</tr>
<tr>
<td>Federal Agencies (including Federal Legal Court)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>U.S. Federal Agencies (or on a broader level, National Government agencies)</td>
</tr>
<tr>
<td>State Agencies (including Legal Courts)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>State Agencies with public oversight responsibilities (or at a broader level, Provincial or Regional Agencies)</td>
</tr>
<tr>
<td>Academia/Research Organizations</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Recognized universities, colleges, and research organizations that operate forensic laboratories or conduct cloud forensics research</td>
</tr>
</tbody>
</table>
External Dependency Chains

- Chain of cloud service Providers
- Dependencies on other CSPs
- Investigations of each individual link in the dependency chain
SLA - Service Level Agreements

- CSP’s forensic support obligations depend on the service model
- Different service models provide different capabilities for the customer in terms of digital forensics
- SLA omit important terms regarding forensic investigations
  - But SLA is essential for specifying CSP responsibilities associated with forensic investigations
- CSPs are generally unwilling to increase transparency
SLO - service level objective

- Required forensic functionality must be specified in service level objectives (SLOs) incorporated into the service level Agreements.

- SLOs may include requirements for notification, identification, preservation, and access to potential evidence sources.
SLO - service level objective

- SLOs determine the way that CSPs address forensic investigations, including the process for identification and preservation of potential evidence and access to data.

- The proportion of relevant evidence available as “accessible sources of evidence” is determined by the terms of the SLA.
SLO - service level objective

- Webserver logs
- Application server logs
- Database logs
- Guest operating system logs
- Host access logs
- Virtualization platform logs and SaaS portal logs
- Network captures
- Billing records

- Webserver logs
- Application server logs
- Guest operating system logs
- Host access logs
- Virtualization platform logs
- Network captures
- Billing records
- Management portal logs

- Cloud or network provider perimeter network logs
- Logs from DNS servers
- Virtual machine monitor (VMM) logs
- Host operating system logs
- API logs
- Management portal logs
- Packet captures
- Billing records
### Agreement Importance

<table>
<thead>
<tr>
<th>Agreement</th>
<th>Very Unimportant</th>
<th>Unimportant</th>
<th>Neutral</th>
<th>Important</th>
<th>Very Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>An agreement on the recording of the chain of custody among all parties in an investigation</td>
<td>1.52%</td>
<td>7.58%</td>
<td>48.48%</td>
<td>42.42%</td>
<td></td>
</tr>
<tr>
<td>Tools provided, techniques supported, access granted regarding forensic investigation should be included in the SLA (Service Level Agreement)</td>
<td>4.48%</td>
<td>16.42%</td>
<td>47.76%</td>
<td>29.85%</td>
<td></td>
</tr>
<tr>
<td>An agreement on the division of responsibilities among all parties involved (cloud organizations, law enforcement, etc.) in cases of investigation</td>
<td>4.48%</td>
<td>19.40%</td>
<td>49.25%</td>
<td>26.87%</td>
<td></td>
</tr>
<tr>
<td>An agreement on the access and control over forensic data at all levels between cloud organizations</td>
<td>1.52%</td>
<td>24.24%</td>
<td>42.42%</td>
<td>31.82%</td>
<td></td>
</tr>
</tbody>
</table>

*Keyun Ruan, Ibrahim Baggili (PhD), Prof Joe Carthy, Prof Tahar Kechadi University College Dublin, Zayed University, Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis. (Mar 2011)*
Multiple Jurisdictions And Tenancy

- Each Jurisdiction imposes different requirements regarding data access

- Absence of a worldwide regulatory body

- Terms that can be included in the SLA in order to support forensic investigations:
  - Technical key terms,
  - Organizational key terms,
  - Legal key terms
  - Auditing key terms
Multiple Jurisdictions And Tenancy

- Lack of legislative mechanism facilitating evidence retrieval involving confidential data
- Lack of forensic expertise
- Exponential increase of digital (mobile) devices accessing the Cloud
- Segregation of forensic data in an infrastructure shared by multiple users (multitenant environment)
- Simple role management (e.g., admin, user) makes it difficult to categorize suspects
- Lack of law/regulation and law advisory
- Decreased access to and control over forensic data at all levels from customer side
- Investigating external chain of dependencies of the cloud provider (e.g., a cloud provider can use the service from another provider)
- Lack of international collaboration and legislative mechanism in cross-country data access and exchange
- Ineffective encryption key management makes it easier to lose the ability to decrypt forensic data stored in the Cloud
- Single points of failure

*Dr. Keyun Ruan University College Dublin, Designing a Forensic-enabling Cloud Ecosystem, 2013
Multiple Jurisdictions And Tenancy

Amazon S3

- Amazon S3 offers storage in the US Standard, US West (Oregon), US West (Northern California), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), 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.

Microsoft Azure

- 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.
Internal Staffing

- Most Cloud Forensics investigations are conducted by traditional digital forensics expert
  - Using conventional network forensic procedures and tools
  - Scarcity of technical and legal expertise with respect to cloud forensics
Digital Evidence Handling in Cloud Forensics

Potential digital evidence should be treated according to the following principles:

- Minimize handling
- Account for any changes and document actions taken
- Comply with local rules of evidence
- Do not take actions beyond your competence
Digital Evidence Handling in Cloud Forensics Identification

It is recommended that customers identify the additional data sources unique to the cloud service model. Specifically:

- SaaS - application level logs like authorization errors, accounting (who did what, when)
- PaaS - application specific logs available ideally via an API, patch status, authentication errors, operating system exceptions and warnings, anti-malware software warnings, …
- IaaS - system level logs, Infrastructure: hypervisor events and logs, unencrypted RAM snapshots, Intrusion detection and firewall events, network events, storage logs, backups

...
Digital Evidence Handling in Cloud Forensics Collection

- Acquisition should usually be preferred over collection to avoid impacts to parties not involved in the matter and the gathering of irrelevant information.

- Collection of digital evidence can often only be performed by the CSP and not by the tenant.
Items normally thought of as physical (hard drives, server memory, etc.) will be logical items (a virtual hard disk file, a file that contains the contents of server memory for a suspended virtual machine, etc.)

Acquisition must focus on these logical items rather than the physical containers where they reside.
The chain of custody must be preserved as well, which is challenging in multi-geographical and multi-jurisdictional environments.
formal analysis of the challenges
“normalized syntax”

1. Identify the major challenges in conducting digital forensics procedures where the evidence resides in a cloud computing environment

2. Establish a common vocabulary for communicating challenges between stakeholders

3. Dialogue among stakeholders to define standards.
Normalized Formula for Expressing Cloud Computing Forensics Challenges

Normalized challenge [formula]:

For an [actor/stakeholder], [action/operation] applicable to [object of this action] is challenging because [reason]

This formula is comprised of four “variables”:

1. **Actor/Stakeholder**: who is affected by the challenge that has been identified.
2. **Action/Operation**: The activity that the stakeholder would like to perform.
3. **Object of This Action**: The specific item upon which the action is to be performed.
4. **Reason**: The primary challenges that the stakeholder faces in order to perform the specified action on the object.

*NIST Cloud Computing Forensic Science Working Group Information Technology Laboratory, NIST Cloud Computing Forensic Science Challenges, June 2014*
<table>
<thead>
<tr>
<th>Challenge</th>
<th>Description</th>
<th>Normalized [FORMULA]:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributing deleted data to a specific user.</td>
<td>Deletion in the cloud is often based on the deletion of nodes pointing to information in virtual instances. Whether the deletion of the information (which is actually held on physical hard drives) has been fully achieved needs to be assessed and proven. Likewise, pathways for retrieval are dependent on cloud providers offering sufficiently sophisticated mechanisms for access.</td>
<td>For <strong>forensics examiners</strong>, identifying and attributing data that is deleted in the cloud to a specific user is a challenge because the sheer volume of data and users constantly operating in a cloud environment limits the amount of backups that the cloud Provider will retain. AND/OR For <strong>forensics examiners</strong>, identifying and attributing data that is deleted in the cloud to a specific user is a challenge because cloud Providers may not implement sufficient methods for retrieving information on deleted data in an Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) delivery models.</td>
</tr>
<tr>
<td>Recovery of deleted data before it may be overwritten.</td>
<td>Recovery of data marked as deleted (for which the nodes pointing to it are deleted) is difficult since it gets overwritten by another user in a shared virtual environment.</td>
<td>For all stakeholders, recovering deleted data that is overwritten by another user is a challenge because in a shared virtual environment there may not be a snapshot in time (e.g., backup) or other record that contains an image of the data before it was overwritten.</td>
</tr>
<tr>
<td>Synchronization of timestamps</td>
<td>Accurate time synchronization has always been an issue in network forensics, and is made all the more challenging in a cloud environment as timestamps must be synchronized across multiple physical machines that are spread across multiple geographical regions, between the cloud infrastructure and remote web clients including numerous end points.</td>
<td>For analysts, correlating the observables with disparate timestamps is challenging because timestamps may be inconsistent between many sources.</td>
</tr>
<tr>
<td>Challenge</td>
<td>Description</td>
<td>Normalized [FORMULA]:</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Access to computer and network resources involve expanded scope and may involve more than one venue and geo-location</td>
<td>Access to computer and network resources involve expanded scope and may involve more than one venue and geo-location</td>
<td>For all investigators, managing the scope of collection is challenging because distributed data collection and chain of custody from a wide range of sources or geo-location unknowns can cause various jurisdictional issues.</td>
</tr>
<tr>
<td>Chain of custody of data</td>
<td>Because of the distributed, multi-layered nature of cloud computing, the chain of custody of data may be impossible to verify. Without strict controls it may be impossible to determine exactly where the data was stored, who had access, and whether leakage or contamination of data was possible. If data is stored in a cloud where multiple users and cloud Providers potentially have access, associating the data to the suspect beyond a reasonable doubt is a challenge.</td>
<td>For law enforcement and courts, ensuring proper chain of custody of data is a challenge because the distributed, shared infrastructure of cloud computing makes identifying and validating a chain of custody difficult.</td>
</tr>
<tr>
<td>Data location</td>
<td>There are many uncertainties dealing with transparency in the cloud and distribution boundaries for retrieval due to multiple tenants in multiple data centers.</td>
<td>For all stakeholders, data collection of target data is challenging due to the flexibility cloud providers have in moving data between data centers and geographic regions.</td>
</tr>
</tbody>
</table>
Case Study

1. Polly stores contraband images in the cloud.
2. He uses a pre-paid credit card.
3. His cloud-hosted website shares the images.

- Law enforcement discovers the website and wants to terminate the service and prosecute the criminal.
Case Study

*Josiah Dykstra, Digital Forensics for IaaS Cloud Computing, June 2012
Experiment 1 (Guest OS)

- Launch and “hack” a virtual machine in EC2
- Use EnCase and FTK agents to acquire disk images remotely
- Use Fastdump, FTK Imager, Memoryze to acquire memory images remotely
- Analyze data to determine success
Experiment 2 (Virtualization)

- Launch and “hack” a virtual machine on a local cloud
- Use introspection to inject an EnCase agent to acquire disk image
- Create virtual machine snapshot and analyze “live” offline
- Analyze data to determine success
Experiment 3 (Host OS)

- Launch and “hack” a virtual machine in EC2
- Use AWS Export to obtain a disk image
- Analyze data to determine success
Conclusion:
When do we start as investigators?

- Jurisdictions
- Ownership
- SLA
- Chain of Cloud Service Provider
- Segregation & multiple tenants
- Cloud Model
- Forensic Tool
Current state

- Software and tools that doesn’t have the flexibility for the investigators to build and customize the desired analysis workflow for specific forensic dataset
Solution:
Digital Forensic as a Service (FaaS)

- Cloud Computing infrastructures
- Dynamic workflow and Large forensic dataset
- Platform with sharing software on-demand
- Different interface for Investigators, collaborators, developers
<table>
<thead>
<tr>
<th>Pro</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Software on-Demand</td>
</tr>
<tr>
<td>• Forensic App Store</td>
</tr>
<tr>
<td>• Storing Forensics Data</td>
</tr>
<tr>
<td>(Metadata of the file)</td>
</tr>
<tr>
<td>• Flexibility</td>
</tr>
<tr>
<td>• Workflow based on users' requests’</td>
</tr>
<tr>
<td>• Web based portal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Against</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security</td>
</tr>
<tr>
<td>• Privacy</td>
</tr>
<tr>
<td>• Service Continuity</td>
</tr>
<tr>
<td>• Network dependence</td>
</tr>
</tbody>
</table>
Thank you!

Marco Iannuzzi
marco.iannuzzi@studio.unibo.it

[2] Dr. Keyun Ruan University College Dublin, Designing a Forensic-enabling Cloud Ecosystem, 2013 (http://www.cirrus-project.eu/sites/default/files/content-files/articles/Ruan_0.pdf)


