Draft NISTIR 8006

NIST Cloud Computing Forensic Science Challenges

NIST Cloud Computing Forensic Science Working Group
Information Technology Laboratory

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8006

NIST Cloud Computing Forensic Science Challenges

NIST Cloud Computing Forensic Science Working Group
Information Technology Laboratory

June 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie E. May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

National Institute of Standards and Technology Interagency or Internal Report 8006
51 pages (June 2014)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to: Michaela Iorga

Public comment period: *June 23, 2014* through *July 21, 2014*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: nistir8006@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

This document summarizes the research performed by the members of the NIST Cloud Computing Forensic Science Working Group, and aggregates, categorizes and discusses the forensics challenges faced by experts when responding to incidents that have occurred in a cloud-computing ecosystem. The challenges are presented along with the associated literature that references them. The immediate goal of the document is to begin a dialogue on forensic science concerns in cloud computing ecosystems. The long-term goal of this effort is to gain a deeper understanding of those concerns (challenges) and to identify technologies and standards that can mitigate them.

Keywords

Digital forensics; Forensics; Cloud computing forensics; Forensic Science; Forensics challenges

Acknowledgments

This publication was developed by the *NIST Cloud Computing Forensic Science Working Group (NCC FSWG)*, chaired by Dr. Michaela Iorga and Mr. Eric Simmon. The principal editors of this document are Dr. Martin Herman (NIST Senior Adviser) and Dr. Michaela Iorga. The National Institute of Standards and Technology and the principal editors wish to gratefully acknowledge and thank the members whose dedicated efforts contributed significantly to the publication.

The following list (in alphabetical order by last name) includes contributors,[1] internal reviewers of the document and other active members who provided feedback and who have agreed to be acknowledged in this document.

CONTRIBUTORS (document and challenges aggregation):

Josiah Dykstra, Ph.D., Department of Defense
Lon Gowen, Ph.D., United States Agency for International Development
Robert Jackson, SphereCom Enterprises Inc.
Otto Scot Reemelin, CBIZ
Ernesto F. Rojas, Forensic & Security Services Inc.
Keyun Ruan, Ph.D., Espion Group
Mike Salim, American Data Technology, Inc.
Ken E. Stavinoha, Ph.D., Cisco Systems
Laura P. Taylor, Relevant Technologies
Kenneth R. Zatyko, Forensics Technologies & Discovery Services, Ernst & Young LLP

INTERNAL REVIEWERS:

Nancy M Landreville, University of Maryland University College & BRCTC
Kristy M. Westphal, Element Payment Services

OTHER ACTIVE MEMBERS:

Ragib Hasan, Ph.D., Assistant Prof., Dept. of Computer and Information Sciences, Univ. of Alabama at Birmingham
Mark Potter, Danya International
Anthony M Rutkowski, Yaana Technologies

NOTE: All views expressed in this document by the contributors are their personal opinions and not those of the organizations with which they are affiliated.

[1] "Contributors" are members of the NIST Cloud Computing Forensic Science WG who dedicated substantial time on a regular basis to research and development in support of this document.

Executive Summary

The National Institute of Standards and Technology (NIST) has been designated by the Federal Chief Information Officer (CIO) to accelerate the federal government's secure adoption of cloud computing by leading efforts to develop standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders.

Consistent with NIST's mission[2], the NIST Cloud Computing Program (NCCP) has developed *"NIST Cloud Computing Standards Roadmap"* [REF63] as one of many mechanisms in support of the USG's secure and effective adoption of the Cloud Computing technology[3] to reduce costs and improve services. Standards are critical to ensure cost-effective and easy migration, to ensure that mission-critical requirements can be met, and to reduce the risk that sizable investments may become prematurely technologically obsolete. Standards are key elements required to ensure a level playing field in the global marketplace[4]. The importance of setting standards in close relation with private sector involvement is highlighted in a memorandum from the White House; M-12-08,[5] dated January 17, 2012.

With the rapid adoption of cloud computing technology, a new need has arisen for the application of digital forensic science to this domain. The validity and reliability of forensic science is crucial in this new context and requires new methodologies for identifying, collecting, preserving, and analyzing evidence in multi-tenant cloud environments that offer rapid provisioning, global elasticity and broad-network accessibility. This is necessary to support the U.S. criminal justice and civil litigation systems as well as to provide capabilities for security incidence response and internal enterprise operations.

The NIST Cloud Computing Forensic Science Working Group (NCC FSWG) was established to research cloud forensic science challenges in the cloud environment and to develop plans for measurements, standards and technology research to mitigate the challenges that cannot be handled with current technology and methods. The NCC FSWG has surveyed existing literature and developed a set of challenges related to cloud computing forensics. This document presents those challenges along with the associated literature. The document also provides a preliminary analysis of these challenges by including (1) the roles of cloud forensics stakeholders, (2) the relationship of each challenge to the five essential characteristics of cloud computing as defined in the Cloud Computing model, and (3) the nine categories to which the challenges belong.

---

[2] This effort is consistent with the NIST role per the National Technology Transfer and Advancement Act (NTTAA) of 1995, which became law in March 1996.

[3] *NIST Definition of Cloud Computing*, Special Publication (SP) 800-145 [REF65]: "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."

[4] This edition of the standards roadmap focuses on USG cloud computing requirements for interoperability, performance, portability, security, and accessibility. It does not preclude the needs to address other essential requirements.

[5] Principles for Federal Engagement in Standards Activities to Address National Priorities, January 17, 2012 http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08.pdf

Table of Contents

Table of Figures

1 Introduction

Over the past few years, cloud computing has revolutionized the methods by which digital data is stored, processed, and transmitted. With this paradigm shift away from traditional standalone computer devices, workstations and networks to the cloud environment, many technological challenges exist. One of the most daunting new challenges is how to perform digital forensics in the various types of cloud computing environments. Cloud computing, in some respects, is similar to prior computing technologies. However, with the advent of advanced hypervisors (which allow virtual machines) and geographical independence (due to networking advancements), challenges with forensics in these arenas, which may cross geographical boundaries or legal boundaries, become an issue.

NIST carries out many research activities related to forensic science. The goals of these activities are to improve the accuracy, reliability, and scientific validity of forensic science through advances in its measurements and standards infrastructure. As part of these activities, the NIST Cloud Computing Forensic Science Working Group (NCC FSWG) is identifying emerging standards and technologies that would help solve “challenges,” that is, the most pressing problems fundamental to carrying out forensics in a cloud computing environment to lawfully obtain (e.g., via warrant or subpoena) all relevant artifacts.

The cloud exacerbates many technological, organizational, and legal challenges already faced by digital forensics examiners. Several of these challenges, such as those associated with data replication, location transparency, and multi-tenancy are somewhat unique to cloud computing forensics [REF2]. The NCC FSWG collected and aggregated a list of cloud forensics challenges (see Annex B) that are introduced and discussed in this document. Future work will involve developing possible technological approaches to mitigate these challenges, and determining gaps in technology and standards needed to address these challenges.

1.1 Document Goals

This document serves as a basis to begin a dialogue on forensic science concerns in cloud computing ecosystems, and serves as a starting point for understanding those concerns (challenges), with the intent to solve these challenges by identifying technologies and standards to meet those challenges.

1.2 Audience

The primary audience for this document includes digital forensics examiners and researchers, cloud-security professionals, law-enforcement officers and cloud auditors. However, given the breadth and depth of this topic, many other stakeholders, such as cloud policy makers, executives, and the general user population of cloud service consumers may also be interested in certain aspects of this document.

2 Overview

This section discusses the definition of cloud computing forensic science, elaborates on why cloud computing challenges traditional digital forensics methods, and describes what constitutes a challenge for cloud forensics.

2.1 Definition of Cloud Computing Forensic Science

Many experts consider forensic science to be the application of a broad spectrum of sciences and technologies to the investigation and establishment of facts of interest in relation to criminal, civil law, or regulatory issues. The rapid advance of cloud services requires the development of better forensic tools to keep pace. However, the resulting techniques may also be used for purposes outside the scope of law to reconstruct an event that has occurred.

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.

NIST defines *cloud computing* (see [REF65]) as “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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.” Cloud forensics is a process applied to an implementation of this model.

Ruan, et al. [REF2] proposes a working definition for cloud forensics as the application of digital forensic science in cloud environments. Technically, it consists of a hybrid forensic approach (e.g., remote, virtual, network, live, large-scale, thin-client, thick-client) towards the generation of digital evidence. Organizationally it involves interactions among cloud actors (i.e., cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor) for the purpose of facilitating both internal and external investigations. Legally it often implies multi-jurisdictional and multi-tenant situations.

Various process models have been developed for digital forensics, including the following eight distinctive steps and attributes [REF61]:

1. <u>Search authority</u>. In a legal investigation, legal authority is required to conduct a search or seizure of data.
2. <u>Chain of custody</u>. In legal contexts, chronological documentation of evidence handling is required to avoid allegations of evidence tampering or misconduct.
3. <u>Imaging/hashing function</u>. When digital evidence is found, it should be carefully duplicated and then hashed to validate the integrity of the copy.
4. <u>Validated tools</u>. When possible, tools used for forensics should be validated to ensure reliability and correctness.
5. <u>Analysis</u>. Forensic analysis is the execution of investigative and analytical techniques to examine the evidence.
6. <u>Repeatability and reproducibility (quality assurance).</u> The procedures and conclusions of forensic analysis should be repeatable and reproducible by the same or other forensic analysts.
7. <u>Reporting</u>. The forensic analyst must document his or her analytical procedure and conclusions for use by others.
8. <u>Possible presentation.</u> In some cases, the forensic analyst will present his or her findings and conclusions to a court or other audience.

In order to carry out digital forensic investigations in the cloud, these steps need to be applied or adapted to the cloud context. Many of them pose significant challenges. This document is focused on the forensic analysis of artifacts *retrieved* from a cloud environment. A related discipline, which is not addressed here, is carrying out the forensic process *using* a cloud environment. This involves using the cloud to perform examination and analysis of digital evidence [REF68].

2.2 Defining What Constitutes a Challenge for Cloud Computing Forensics

There are numerous challenges for the various stakeholders who share an interest in forensic analysis of cloud computing environments. Challenges to cloud forensics can broadly be categorized into technical, legal, and organizational[6] challenges. Such challenges occur when technical, legal, or organizational tasks become impeded or prevent the examination by the digital forensics examiner.

When comparing cloud forensics challenges to those of traditional digital forensics, we consider cloud forensics challenges to be either unique to the cloud environment, or exacerbated by the cloud environment [REF2]. While the goals of first responders and forensic examiners may be the same in the cloud context in comparison to traditional large-scale network forensics, distinctive features of cloud computing such as segregation of duties among cloud actors, inability to acquire network logs from the load balancer or routers, multi-tenancy, and rapid elasticity introduce unique scenarios for digital investigations. On the other hand, challenges associated with, for example, virtualization, large-scale data processing, and proliferation of mobile devices and endpoints are exacerbated in the cloud.

Cloud forensics challenges cannot be solved by technology, law, or organizational principles alone. Many of the challenges need solutions in all three areas. Technical, legal and organizational scholars and practitioners have begun to discuss these challenges. This report focuses more on the technical challenges, which need to be understood in order to develop technology- and standards-based mitigation approaches.

2.3 Cloud computing forensics stakeholders and their roles

There are many stakeholders involved in cloud forensics activities, including members of government, industry, and academia. One of the biggest challenges in cloud computing is understanding who holds the responsibilities for the various tasks involved in managing the cloud. All responsibilities should be clear at the time of contract signing. Forensics is an area that is particularly prone to misunderstandings since it is often not until a forensic investigation is under way that stakeholders start making assertions about ownership and responsibilities.

For the purposes of this document, a list of stakeholders in cloud forensics is presented in Annex A. The table in this Annex introduces the stakeholders in the left-most column and provides a description of each stakeholder in the right-most column. The central columns identify the Cloud Actors as defined in NIST SP 500-292 [REF64]. The roles played by each cloud stakeholder in the cloud ecosystem are identified. The list provided in Annex A is not comprehensive. It was created based on the analysis of the forensics challenges the authors collected and aggregated as part of this study.

[6] Organizational challenges involve challenges dealing with cloud actors (see Annex A) working together to obtain digital evidence. The cloud actors include consumer, provider, broker, auditor and carrier [REF2].

3 Cloud Forensics Challenges

This section discusses how the NCC FSWG collected and aggregated the challenges, as well as the steps taken to perform a preliminary analysis of the challenges.

3.1 Collection and Aggregation of Challenges

The first step towards identifying the challenges that cloud forensics practitioners are facing was to study the available literature and gather available data on this topic. The data was then aggregated in a meaningful way that permits further analysis.

The data was gathered and aggregated as a collective group effort by the active participants of the NCC FSWG. These active participants represent many key cloud ecosystem stakeholders, including government, private industry, and academia, both domestically and internationally. The methodology for gathering the data was as follows:

- Perform a literature search. Most of these sources are listed in the References Section (Section 8).
- Obtain input from a variety of stakeholders in the group.
- Have various group discussions among the participants through scheduled conference calls as well as emails.

The data gathered was inserted into a spreadsheet (shown in Annex B) that currently lists 65 challenges, together with challenge descriptions, categories, cloud computing essential characteristics [REF65], and relevant references. (Note that the last column in the spreadsheet lists references that discuss each challenge.)

To better assist with a focused discussion and formal analysis of the challenges, a "normalized syntax" was developed with which to express each challenge. This "normalized syntax" is described later in this section.

The cloud forensic science challenges were aggregated in a spreadsheet referred to as the "Cloud Forensics Challenges" spreadsheet. The major objectives of the spreadsheet are:

- Identify the major challenges in conducting digital forensics procedures where the evidence resides in a cloud computing environment. While there are challenges in conducting any digital forensics procedure, the essential characteristics of cloud computing systems enumerated in Section 3.2 provide many challenges that are not encountered, or encountered to a lesser degree, in more traditional computing models.
- Establish a common vocabulary for communicating challenges between stakeholders. There are many stakeholders in cloud forensics including, but not limited to, cloud Consumers, cloud Providers, first responders, forensics examiners, and law enforcement. As a result of this diverse set of stakeholders, a common "language" is needed to allow effective communication of the challenges between the various groups.
- Create an on-going dialogue among stakeholders to define potential technology and standards mitigation approaches to the forensics challenges faced in the cloud computing environment. The challenges identified in the Cloud Forensics Challenges spreadsheet are certainly not comprehensive. As the spreadsheet continues to evolve, the long term objective is to identify potential technology and standards mitigation approaches and to determine technology and standards gaps to address the challenges.

To achieve these objectives, we developed a formula for a normalized sentence syntax that allows expression of all cloud forensics challenges in a common format. Figure 1 contains the normalized formula.

Normalized challenge [formula]:

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

Figure 1: Normalized Formula for Expressing Cloud Computing Forensics Challenges

This formula is comprised of four "variables:"

- *Actor/Stakeholder* – This variable [a noun] identifies the stakeholder(s) who is affected by the challenge that has been identified. Examples of stakeholders include cloud consumers, investigators, first responders, etc.
- *Action/Operation* - This variable [a verb] identifies the activity that the stakeholder would like to perform. Examples of actions include decrypting, imaging, gaining access, etc.
- *Object of This Action* – This variable identifies the specific item upon which the action is to be performed. Examples of objects include data, audit logs, time stamps, evidence, etc.
- *Reason* – This variable identifies the primary challenges that the stakeholder faces in order to perform the specified action on the object.

In Annex B, the normalized description of each challenge is shown in the sixth column. Taken as a whole, the 65 items identified by the Cloud Forensics Challenges spreadsheet represent many of the major challenges that are being faced in performing digital forensics in the cloud environment based on the collective experience of the NCC FSWG. The NCC FSWG hopes that by initiating this dialogue, the experience of other professionals can be drawn upon to further refine and update this product.

3.2 Data Analysis

The NCC FSWG has attempted to keep the challenges generic without taking on the multitude of differences in architectures between the many products that proliferate the cloud computing family of offerings.

To assist in organizing the cloud forensics challenges, each challenge was correlated to one or more of the five essential characteristics of the cloud computing model as defined in *The NIST Definition of Cloud Computing* [REF65]. These characteristics, which are identified in the second column of the challenges spreadsheet in Annex B, include:

- **On-demand self-service -** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad network access -** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- **Resource pooling -** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but

may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

- **Rapid elasticity -** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service -** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

A review of the Annex B challenges reveals that a majority of the issues are technical in nature, with a major secondary group that is framed by legal and organizational issues. The technical issues revolve around the differences between the operating framework of cloud computing and traditional datacenter physical computing. The legal and organizational issues reflect primarily the crossing of national borders through the manner in which cloud providers store customer information for operational redundancy, cost and reliability.

To facilitate a more detailed understanding and analysis of the challenges identified, they have been organized into the mind map shown in Annex C. The mind map provides a graphic depiction of the relationship between items (in this case challenges) and was used to provide structure and to classify the challenges into categories. The highest level of the mind map (presented in blue text) represents the complete set of the challenges that were identified in Annex B.

To assist in a meaningful analysis, the challenges were then categorized into the following nine major groups (presented in red text in the mind map). The categories and associated descriptions below provide a summary of the contents of Annex B. Some of the challenges lie in more than one category because, as will be described, a challenge may be part of a "primary category" and also part of a different "related category." Refer to Annex B for the details.

- **Architecture (e.g., diversity, complexity, provenance, multi-tenancy, data segregation, etc.) --** Architecture challenges in cloud forensics include dealing with variability in cloud architectures between providers; tenant data compartmentalization and isolation during resource provisioning; proliferation of systems, locations and endpoints that can store data; accurate and secure provenance for maintaining and preserving chain of custody; infrastructure to support seizure of cloud resources without disrupting other tenants; etc.
- **Data collection (e.g., data integrity, data recovery, data location, imaging, etc.) --** Data collection challenges in cloud forensics include locating forensic artifacts in large, distributed and dynamic systems; locating and collecting volatile data; data collection from virtual machines; data integrity in a multi-tenant environment where data is shared among multiple computers in multiple locations and accessible by multiple parties; inability to image all the forensic artifacts in the cloud; accessing the data of one tenant without breaching the confidentiality of other tenants; recovery of deleted data in a shared and distributed virtual environment; etc.
- **Analysis (e.g., correlation, reconstruction, time synchronization, logs, metadata, timelines, etc.) --** Analysis challenges in cloud forensics include correlation of forensic artifacts across and within cloud providers; reconstruction of events from virtual images or storage; integrity of metadata; timeline analysis of log data including synchronization of timestamps; etc.
- **Anti-forensics (e.g., obfuscation, data hiding, malware, etc.) --** Anti-forensics are a set of techniques used specifically to prevent or mislead forensic analysis. Challenges in cloud forensics include the use of obfuscation, malware, data hiding, or other techniques to compromise the integrity of evidence; malware may circumvent virtual machine isolation methods; etc.

- **Incident first responders (e.g., trustworthiness of cloud providers, response time, reconstruction, etc.) --** Incident first responder challenges in cloud forensics include confidence, competence, and trustworthiness of the cloud providers to act as first-responders and perform data collection; difficulty in performing initial triage; processing a large volume of forensic artifacts collected; etc.
- **Role management (e.g., data owners, identity management, users, access control, etc.) --** Role management challenges in cloud forensics include uniquely identifying the owner of an account; decoupling between cloud user credentials and physical users; ease of anonymity and creating fictitious identities online; determining exact ownership of data; authentication and access control; etc.
- **Legal (e.g., jurisdictions, laws, service level agreements, contracts, subpoenas, international cooperation, privacy, ethics, etc.) --** Legal challenges in cloud forensics include identifying and addressing issues of jurisdictions for legal access to data; lack of effective channels for international communication and cooperation during an investigation; data acquisition that relies on the cooperation of cloud providers, as well as their competence and trustworthiness; missing terms in contracts and service level agreements; issuing subpoenas without knowledge of the physical location of data; seizure and confiscation of cloud resources may interrupt business continuity of other tenants; etc.
- **Standards (e.g., standard operating procedures, interoperability, testing, validation, etc.) --** Standards challenges in cloud forensics include lack of even minimum/basic SOPs, practices, and tools; lack of interoperability among cloud providers; lack of test and validation procedures; etc.
- **Training (e.g., forensic investigators, cloud providers, qualification, certification, etc.) --** Training challenges in cloud forensics include misuse of digital forensic training materials that are not applicable to cloud forensics; lack of cloud forensic training and expertise for both investigators and instructors; limited knowledge by record-keeping personnel in cloud providers about evidence; etc.

Once the challenges were grouped into their primary categories, it was determined that several challenges could logically be grouped into subcategories (presented in green text in the mind map). For example, “Data Integrity” and “Data Recovery” were determined to be two important subcategories of the “Data Collection” category because multiple data collection challenges could be logically grouped into these subcategories. Annex C.1 is the mind map that represents these categories and subcategories. Once all of the categories and subcategories were identified, each of the challenges in the spreadsheet in Annex B was analyzed in relationship to the other challenges and mapped into the appropriate category (and subcategory, if appropriate). These challenges (presented in black text in the mind map) are the end nodes for each path through the mind map.

During this preliminary analysis, it was also discovered that while every challenge could be logically grouped into a primary category, many of the challenges overlapped into other categories. Within the spreadsheet in Annex B, the latter challenges are identified to belong to one or more “related categories.” To make a distinction between primary categories and related categories in the mind map, different node background colors were selected. A challenge’s primary category is depicted by a green node background (Annex C.2 shows the primary categories), while a challenge’s related category is depicted by an orange background (Annex C.3 shows the related categories).

4 Preliminary Analysis

Our study examined 65 different challenges related to cloud computing forensics. This section provides additional insight into the nature of these challenges.

In traditional computer forensics, due to the centralized nature of the information technology systems, investigators can have full control over the forensic artifacts (e.g., router logs, process logs, hard disks). However, in a cloud ecosystem, due to the distributed nature of the information technology systems, control over the functional layers varies among cloud actors depending on the service model. Therefore investigators have reduced visibility and control over the forensic artifacts. For example, cloud consumers have the highest level of control over the functional stack in an IaaS cloud model and the least level of control in an SaaS cloud model. Because of this difference in control, evidence collection varies according to the service model [REF60].

An important source of forensic analysis is logs, many of which may be available in cloud computing environments but may be hard to access or aggregate due to the segregation of duties among actors and lack of transparency of log data for the consumer. Three examples of such logs are audit logs, security logs, and application logs. Audit logs are the records of interactions between services and the underlying operating system. Security logs trace users to actions, identifying the particular user who took an action on a particular date at a particular time. Application logs record activity generated by the applications along with errors and other operational faults of the applications.

In cloud computing, when there is a potential need for forensic artifacts at the hypervisor/virtual machine monitor (VMM) layers, additional complexity arises from the architecture of the cloud ecosystem. Just as there can be significant differences in how Windows, Linux, and other operating systems create and handle events, there are different architectures and configurations for hypervisors/VMMs from the different manufacturers and each has its own event definition and logging (or lack thereof). Cloud computing can present a challenge to the acquisition of artifacts if, for example, the creation and migration of a virtual path or virtual asset needs to be ascertained across several platforms or providers.

To perform forensic analysis using logs with the integrity on which all stakeholders can rely, the logs must be trusted [REF67]. Decentralization of logs among different layers, accessibility of logs, the multi-tenancy nature of clouds, and preserving the chain of custody make log analysis challenging in clouds. Additionally, the use of logs in hypervisors is not well understood and presents a significant challenge to cloud forensics.

The identification, collection, and preservation of media can be particularly challenging in a cloud computing environment given several possible factors, including:

1) Identification of the cloud provider and its partners. This is needed to better understand the environment and thus address the factors below.
2) The ability to conclusively identify the proper accounts held within the cloud by a consumer, especially if different cyber personas are used.
3) The ability of the forensics examiner to gain access to the desired media.
4) Obtaining assistance of the cloud infrastructure/application provider service staff.
5) Understanding the topology, proprietary policies, and storage system within the cloud.
6) Once access is obtained, the examiner’s ability to complete a forensically sound image of the media.
7) The sheer volume of the media.
8) The ability to respond in a timely fashion to more than one physical location if necessary.

9) E-discovery, log file collection and privacy rights given a multi-tenancy system. (How does one collect the set of log files applicable for this matter versus extraneous information with possible privacy rights protections?)
10) Validation of the forensic image.
11) The ability to perform analysis on encrypted data and the collector's ability to obtain keys for decryption.
12) The storage system no longer being local.
13) There is often no way to link given evidence to a particular suspect other than by relying on the cloud provider's word.

Standards and technologies need to be developed to address these challenges. For example, forensic protocols need to be developed that can be adopted by the major cloud Providers. These protocols must adequately address the needs of the first responders and court systems while assuring the cloud Providers no disruption or minimal disruption to their service(s). On the technology front, an example of a current need is the ability to lawfully perform remote digital forensics collections that will lower the costs of travel. In essence, this will involve moving forensic images electronically from the cloud Provider to a forensics lab. Better yet would be performing the forensics in a scientifically sound manner in the cloud itself.

4.1 Additional Observations

During the preliminary analysis, we found some common topics in these challenges, each of which overlaps several of the categories enumerated in the mind map. These topics appear to be orthogonal to those categories, and are therefore included here to provide additional insight into the challenges.

- **Time –** Time is frequently a critical issue as related to time synchronization and the possible disappearance of evidence if not found quickly. Zimmerman and Glavach [REF53] point out, "Once the information source is identified, do all involved entities have time synchronized via a consistent time source such as Network Timing Protocol (NTP). If a forensic expert has a difficult time convincing your legal counsel that the time stamps from client-side log files match time stamps on provider-side log files, the forensics will be difficult to defend." Also, if evidence is not found quickly enough, it may be overwritten or lost in some other manner. Some example challenges in Annex B related to *time* include Challenge #5 (Timestamp synchronization), Challenge #14 (Real-time investigation intelligence processes not possible), Challenge #30 (Data available for a limited time), and Challenge #53 (International cloud services).
- **Location –** Locating the digital media can be a time consuming process in cloud environment cases. An understanding of the topology will aid in identifying physical locations of media storage. Both back-up and redundant storage are important. The legal venue can add to the complexity and is an important item to address early on. Locating the evidence can be a big hurdle. As pointed out in Zimmerman and Glavach [REF53], "before network or computer forensics can begin, the network or computer must be 'found.' There may only be traces of a virtual machine (VM) because the VM may reside on dispersed, internationally-located physical drives." Some example challenges in Annex B related to *location* include Challenge #17 (Multiple venues and geo-locations), Challenge #25 (Decreased access and data control), Challenge #27 (Locating evidence), Challenge #37 (Additional evidence collection), Challenge #48 (Physical data location), and Challenge #60 (Decoupling user credentials & physical location).
- **Sensitive data –** Sensitive data theft cases (insider, outsider, and both working together) is an important issue. According to CIO.com [REF69], the U.S. Commission on Intellectual Property estimates over $300B in annual losses to U.S. companies due to theft. The pervasive use of cloud computing environments by employees for personal use could heighten the risk of insider theft given the low cost storage arrays available and low cost high-speed bandwidth to move data. The intrusion

threat has grown for all systems connected to the Internet. Some example challenges in Annex B related to *sensitive data* include Challenge #39 (Selective data acquisition), Challenge #56 (Confidentiality and Personally Identifiable Information (PII)), Challenge #61 (Authentication and access control), and Challenge #7 (Use of metadata).

5 Conclusions

This document highlights many of the forensic challenges in the cloud computing environment for the digital forensics practitioner, the cloud Providers, law enforcement, and others. We provide a definition of cloud computing forensics to scope this area. We discuss cloud forensics stakeholders and their roles. In our approach, we list 65 challenges using a formula of four variables of actor/stakeholder, action/operation, object of action, and reason. We examined recent research papers and involved the international community. Our categories of challenges include architecture, data collection, analysis, anti-forensics, incident first responders, role management, legal issues, standards, and training.

As pointed out in [REF47], "more research is required in the cyber domain, especially in cloud computing, to identify and categorize the unique aspects of where and how digital evidence can be found. End points such as mobile devices add complexity to this domain. Trace evidence can be found on servers, switches, routers, cell phones, etc. Digital evidence can be found at the expansive scenes of the crime which includes numerous computers as well as peripheral devices…To aid in this quest, digital forensics standards and frameworks for digital forensics technologies are required now more than ever in our networked environment."

The NCC FSWG will continue its efforts and will initiate more dialogue among the stakeholders. The next steps include (1) further analysis of the cloud forensics challenges, (2) prioritizing the challenges, (3) choosing the highest priority challenges and determining gaps in technology, standards and measurements to address these challenges, and (4) developing a roadmap to address these gaps.

6 Acronyms

Selected acronyms and abbreviations used in the guide are defined below.

CIO	Chief Information Officer
IATAC	Information Assurance Technology Analysis Center
IEEE	Institute of Electrical and Electronics Engineers
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
NTP	Network Timing Protocol
NCC FSWG	NIST Cloud Computing Forensic Science Working Group
NTTAA	National Technology Transfer and Advancement Act
PII	Personally Identifiable Information
SOP	Standard Operating Procedure
SP	Special Publication
U.S.	United States
USG	U.S. Government
VM	Virtual Machine
VMM	Virtual Machine Monitor

7 Glossary

Challenges	A challenge, for this paper, is currently a difficult or impossible task that is either unique to cloud computing or exacerbated by it.
Cloud computing	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. This cloud model is composed of five essential characteristics, three service models, and four deployment models. – "The NIST Definition of Cloud Computing," NIST SP 800-145, September 2011.
Cloud Provider	The entity (a person or an organization) responsible for making a service available to interested parties. – "US Government Cloud Computing Technology Roadmap Volume II Release 1.0," NIST SP 500-293, November 2011.
Digital forensics	The process used to acquire, preserve, analyze and report on evidence using scientific methods that are demonstrably reliable, accurate, and repeatable such that it may be used in judicial proceedings. – "SWGDE Digital Forensics as a Forensic Science Discipline," Version 1.0, February 6, 2014.
Forensics	The use or application of scientific knowledge to a point of law, especially as it applies to the investigation of crime. – "SWGDE and SWGIT Digital and Multimedia Evidence Glossary," Version 2.7, April 8, 2013.
Imaging	The process used to obtain a bit by bit copy of data residing on the original electronic media. This process allows the investigator to review a duplicate of the original evidence while preserving that evidence. -- "Computer Forensics: Digital Forensic Analysis Methodology." 01/2008 Volume 56, number 1, DOJ.
Virtual machine	A virtual data processing system that appears to be at the disposal of a particular user, but whose functions are accomplished by sharing the resources of a real data processing system. – "*ISO/IEC 2382-1:1993, Information technology — Vocabulary — Part 1: Fundamental terms.*"
Virtualization	The simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine. – "Guide to Security for Full Virtualization Technologies," NIST 800-125, January 2011.

8 References

REF1 Ruan, K. 'Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey results', Digital Investigation, March 2013.

REF2 Ruan K., J. Carthy, T. Kechadi, M. Crosbie, (2011) ‘Cloud Forensics’, 7th IFIP Advances in Digital Forensics VII, G. Peterson and S. Shenoi (eds), vol. 361, pp. 35-46.

REF3 Ruan K., Carthy, J. (2012) ‘Cloud Computing Reference Architecture and its Forensic Implications: a Preliminary Analysis’, Proceedings of the 4th International Conference on Digital Forensics & Cyber Crime, Springer Lecture Notes, October 25-26, Lafayette, Indiana, USA.

REF4 ‘Mapping ISO27037 to Cloud Computing Environments’, Cloud Security Alliance, Cloud Forensics Working Group, June 2013.

REF5 Ruan K., James I.J., Carthy, J., Kechadi, T. (2012) ‘Key Terms for Service Level Agreement to Support Cloud Forensics’, Advances in Digital Forensics VIII, Springer, pp. 201-212.

REF6 Ruan, K. (2013) ‘Designing a Forensic-enabling Cloud Ecosystem’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF7 Crosbie, M. (2013) ‘Hack the Cloud: Ethical Hacking and Cloud Forensics’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF8 Cohen F. (2013) ‘Challenges to Digital Forensic Evidence in the Cloud’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF9 Adams R. (2013) ‘The Emergence of Cloud Storage and Need for a New Digital Forensic Process Model’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF10 Ferguson-Boucher K. and Endicott-Popovsky B. (2013) ‘Forensic Readiness in the Cloud: Integrating Records Management and Digital Forensics’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF11 Barrett D. (2013) ‘Security Architecture and Forensic Awareness in Virtualized Environments’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF12 Dykstra J. (2013) ‘Seizing Electronic Evidence from Cloud Computing Environments’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF13 Orton I., Alva A., Endicott-Popovsky B. (2013) ‘Legal Process and Requirements for Cloud Forensic Investigations’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF14 Gonsowski D. (2013) ‘Compliance in the Cloud and Implications on Electronic Discovery’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF15 Spyridopoulos T. and Katos V. (2013) ‘Data Recovery Strategies for Cloud Environments’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF16 Didone D. and J.G.B. de Queiroz R. (2013) ‘Forensics as a Service’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF17 Marturana F., Tacconi S. and Italiano G. (2013) ‘Forensics as a Service’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF18 Shende R.G.J. (2013) ‘Forensics as a Service’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF19 Ruan K., Carthy, J. (2012) ‘Cloud Forensic Maturity Model’, Proceedings of the 4th International Conference on Digital Forensics & Cyber Crime, Springer Lecture Notes, October 25-26, Lafayette, Indiana, USA.

REF20 James J.I., Shosha A.F., Gladyshev P. (2013) ‘Digital Forensic Investigation and Cloud Computing’, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

REF21 Grobauer B., Schreck T. (2010) 'Towards Incident Handling in the Cloud: Challenges and Approaches ' Siemens CERT, Munich.

REF22 Grivas S.G., Kumar, T.U., Wache H. (2010) 'Cloud Broker: Bringing Intelligence into the Cloud - An Event-based Approach', 2010 IEEE 3rd International Conference on Cloud Computing, pp. 544-545.

REF23 Fowler B. (2009) 'Securing a Virtual Environment.' http://www.infosecwriters.com/text_resources/pdf/BFowler_VIrtual_Environment.pdf

REF24 Chen Y., Paxson V., Katz R.H., (2010) 'What’s new about cloud computing security.' Electrical Engineering and Computer Sciences, University of California at Berkeley, Technical Report No. UCB/EECS-2010-5, January 20, 2010, http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

REF25 Decker M., Kruse W., Long B., Kelly G. (2011) 'Dispelling Common Myths of Live Digital Forensics.' https://www.dfcb.org/docs/LiveDigitalForensics-MythVersusReality.pdf

REF26 Creeger M. (2010) 'Moving to the Edge: A CTO Roundtable on Network Virtualization.'

REF27 Computing Research Association (2003) 'Four Grand Challenges in Trustworthy Computing.'

REF28 Convery N. (2010) 'Cloud computing toolkit: guidance for outsourcing information storage to the cloud.' http://www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf

REF29 Convery N. (2010) 'Storing information in the cloud.' http://www.drnicoleavena.com/storage/articles/Cloud_computing_report_final-1.pdf

REF30 Choo K. R. (2010) 'Cloud computing: challenges and future directions.' http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi400.html

REF31 Cisco (2013) 'Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2013-2018.'

REF32 CIO Council & Chief Acquisition Officers Council (2012) 'Creating Effective Cloud Computing Contracts for the Federal Government.'

REF 33 Barnhill, D.S. (2010) 'Cloud Computing and Stored Communications: Another Look at Quon v. Arch Wireless,' 25 Berkeley Tech. L.J. 621. Available at: http://scholarship.law.berkeley.edu/btlj/vol25/iss1/25

REF34 Pew Research Center (2010), 'The future of cloud computing'.

REF35 Dykstra J, Riehl D. Forensic Collection of Electronic Evidence from Infrastructure-as-a-Service Cloud Computing. Richmond Journal of Law and Technology 2012;19. Available at: http://jolt.richmond.edu/wordpress/?p=463.

REF36 Cloud Security Alliance Legal Information Center, What Rules Regulate Government Access to Data Held by US Cloud Service Providers.

REF37 Pearson, S. Privacy, Security and Trust in Cloud Computing. In: Privacy and Security for Cloud Computing, Computer Communications and Networks, S. Pearson and G. Yee (eds.), Springer (2012).

REF38 Reynolds, E. and Greenway, M. "Minimize the risk of your cloud-based services." HP White Paper 4AA4-0150ENW, 2012. http://h20195.www2.hp.com/V2/GetPDF.aspx%2F4AA4-0150ENW.pdf

REF39 LU, R., LIN, X., LIANG, X., AND SHEN, X. S. Secure provenance: the essential of bread and butter of data forensics in cloud computing. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10) (New York, NY, USA, 2010), ACM, pp. 282–292.

REF40 Grispos , G., Storer, T., and Glisson, W. (2012) Calm before the storm: the challenges of cloud computing in digital forensics. International Journal of Digital Crime and Forensics, 4 (2), pp. 28-48.

REF41 EU Council Ethical Hacking and Countermeasures Attack Process Steps. https://www.eccouncil.org/Certification/certificate-series/ehs-attack-phases

REF42 Reilly, D., Wren, C., and Berry, T. "Cloud Computing: Pros and Cons for Computer Forensic Investigators." International Journal Multimedia and Image Processing (IJMIP), Volume 1, Issue 1, March 2011.

REF43 R. Marty, "Cloud application logging for forensics," Proc. of the 2011 ACM Symposium on Applied Computing (SAC'11), Taichung, Taiwan. ACM, March 2011, pp. 178–184.

REF44 Almulla, S., Iraqi, Y. and Jones, A. "Cloud forensics: A research perspective." 2013 9th International Conference on Innovations in Information Technology (IIT), 2013.

REF45 Kashi Venkatesh Vishwanath and Nachiappan Nagappan, Characterizing Cloud Computing Hardware Reliability, http://research.microsoft.com/pubs/120439/socc088-vishwanath.pdf

REF46 Measuring the Cost of Cybercrime, Anderson Ross et al, http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

REF47 Zatyko, Ken and Bay, John. The Digital Forensics Cyber Exchange Principle, http://www.dfinews.com/articles/2012/02/digital-forensics-cyber-exchange-principle#.Uq83puLEqrU

REF48 Lemos, R. Cloud-Based Denial Of Service Attacks Looming, Researchers Say. Available at http://www.darkreading.com/smb-security/167901073/ security/perimeter-security/226500300/index.html, 2010. Last accessed August 4, 2010.

REF49 Kortchinsky, K. (2009). CLOUDBURST: A VMware Guest to Host Escape Story. Retrieved from http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf.

REF50 Dykstra J, Sherman AT. (2011) Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies.Proceedings of the 2011 ADFSL Conference on Digital Forensics Security and Law, ASDFL, pp. 191–206.

REF51 Kaufman, L. Can public-cloud security meet its unique challenges? Security Privacy, IEEE 8, 4 (July-Aug. 2010), pp. 55–57.

REF52 Lu, R., Lin, X., Liang, X., and Shen, X. S. Secure provenance: the essential of bread and butter of data forensics in cloud computing. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS ’10) (New York, NY, USA, 2010), ACM, pp. 282–292.

REF53 Zimmerman, S. and Glavach, D. “Cyber Forensics in the Cloud.” Information Assurance Technology Analysis Center (IATAC), IAnewsletter, Vol 14, No 1, Winter 2011

REF54 Josiah Dykstra, Alan T. Sherman, Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform, Digital Investigation, Volume 10, Supplement, August 2013, pp. S87-S95.

REF55 Kiran-Kumar Muniswamy-Reddy, Peter Macko, and Margo Seltzer. 2010. Provenance for the cloud. In Proceedings of the 8th USENIX conference on File and storage technologies (FAST'10). USENIX Association, Berkeley, CA, USA, 15-14.

REF56 Hay B, Nance, K Bishop, M. Storm clouds rising: security challenges for IaaS cloud computing. 44th Hawaii International Conference on system Sciences–HICSS 2011, Kauai, Hawaii USA; 2011, pp. 1–7.

REF57 Birk, D.; Wegener, C., "Technical Issues of Forensic Investigations in Cloud Computing Environments," 2011 IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), pp.1-10, 26 May 2011.

REF58 Dykstra, J., Sherman, A.T. Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and Evaluating Tools, Trust, and Techniques. Digital Investigation 2012; 9, Supplement: S90–S98. The Proceedings of the Twelfth Annual DFRWS C.

REF59 Gary Anthes. 2010. Security in the cloud. Commun. ACM 53, 11 (November 2010), pp. 16-18.

REF60 S. Zawoad and R. Hasan "Digital Forensics in the Cloud", The Journal of Defense Software Engineering (CrossTalk), Sept 2013, Vol. 26, No 5, pp. 17-20.

REF61 Zatyko, K. (2007). Defining Digital Forensics, Forensic Magazine.

REF62 P. Henry, J. Williams and B. Wright, The SANS Survey of Digital Forensics and Incident Response, July 2013. https://blogs.sans.org/computer-forensics/files/2013/07/sans_dfir_survey_2013.pdf

REF63 Hogan, M., Liu, F., Sokol, A., and Tong, J. "NIST Cloud Computing Standards Roadmap", NIST SP 500-291, National Institute of Standards and Technology, July 2011.

REF64 F. Liu, J. Tong, J. Mao, R. B. Bohn, J. V. Messina, M. L. Badger, D. M. Leaf, NIST Cloud Computing Reference Architecture (NIST SP 500-292), National Institute of Standards and Technology, U.S. Department of Commerce (2011). http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

REF65 P. Mell and T. Grance, The NIST definition of cloud computing (NIST SP 800-145), National Institute of Standards and Technology, U.S. Department of Commerce (2011).http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

REF66 Carrier, B. D. "Risks of live digital forensic analysis." Communications of the ACM Volume 49, No 2, Feb. 2006, 56-61. DOI http://doi.acm.org/10.1145/1113034.1113069.

REF67 S. Zawoad and R. Hasan "Towards Building Proofs of Past Data Possession in Cloud Forensics", Academy of Science and Engineering Journal 2012, Vol. 1, Issue 4, pp. 195-207.

REF68 Buchanan,W., J. Graves, N. Bose, R. Macfarlane, B. Davison, and R. Ludwiniak, "Performance and student perception evaluation of cloud-based virtualized security and digital forensics labs." In HEA ICS Conference, 2011.

REF69 K. Corbin, "Economic Impact of Cyber Espionage and IP Theft Hits U.S. Businesses Hard," CIO.com, July 2013. http://www.cio.com/article/736132/Economic_Impact_of_Cyber_Espionage_and_IP_Theft_Hits_U.S._Businesses_Hard.

REF70 D. Bilby, "Low Down and Dirty: Anti-Forensic Rootkits." Fourth Annual RuxCon Conference (RuxCon 2006), Sidney, Australia, 2006.

Annex A - Stakeholders

MAPPING OF CLOUD FORENSICS STAKEHOLDERS TO CLOUD ACTORS (AS DEFINED IN NIST REFERENCE ARCHITECTURE [REF64]) IN THE CONTEXT OF A CLOUD FORENSIC INVESTIGATION (In answer to the question: "Would this Cloud Actor ever play this Role in a Cloud Forensic investigation?").						
	Stakeholder's Role as CLOUD ACTORS					
Cloud Forensics Stakeholders	CONSUMER	PROVIDER	BROKER	AUDITOR	CARRIER	Description
Cloud Enterprise Customer	X	X	X			An organizational user of Cloud services
Cloud End-User (Employee of Enterprise Customer)	X					An individual user of cloud services who is a member of an Enterprise Customer organization
Cloud Individual Customer	X					An individual user of cloud services who is not consuming those services as a member of an Enterprise Customer organization
Cloud Service Vendor	X	X	X	X	X	Provider of cloud services
Communication Services Vendors		X			X	Provide data transport between Cloud consumers and Cloud providers
Third-party, Independent Assessors				X		Independent of consumers and providers, they determine whether services being provided comply to SLA
State Regulators	X			X		Regulatory bodies with public oversight responsibilities, typically appointed by State or Local Governments (or at a broader level, County or Province or Parish, etc.)
Federal Regulators	X			X		Regulatory bodies with public oversight responsibilities, typically appointed by the Federal Government
Federal Agencies (including Federal Legal Court)	X	X	X	X		U.S. Federal Agencies (or on a broader level, National Government agencies)
State Agencies (including Legal Courts)	X	X	X	X		State Agencies with public oversight responsibilities (or at a broader level, Provincial or Regional Agencies)
Academia/Research Organizations	X	X				Recognized universities, colleges, and research organizations that operate forensic laboratories or conduct cloud forensics research
Third-party IAM Service Vendors	X		X			Businesses that offer identity and access management (IAM) services as part of the cloud ecosystem
Testing and Certification Vendors	X			X		Recognized cloud forensics testing and certification organizations, etc.
Law Enforcement Agents				X		Self explanatory
Forensic Laboratory	X			X		Specialized facility equipped to perform forensics work, either for Law Enforcement or other forensics applications

765 ## Annex B - Cloud Forensics Challenges

	Relevance of Essential Cloud Characteristics OD=On-demand self-service; BNA=Broad network access; RP=Resource pooling; RE=Rapid elasticity; MS=Measured service	Short Title (for inclusion in the Mind Map)	Challenge	Description	Normalized [FORMULA]: For a [actor/stakeholder (e.g., consumer)], [action/operation] applicable to [object of this action] is challenging because [reason]	Primary Category (Sub-category)	Related Category (Sub-category)	References
1	RP/MS	Deletion in the cloud	Attributing deleted data to a specific user.	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.	For forensics examiners, 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 forensics examiners, 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..	Architecture	Data Collection (Data Recovery)	REF39
2	OD/BNA/RP/RE	Recovering overwritten data	Recovery of deleted data before it may be overwritten.	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.	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	Architecture	Data Collection (Data Recovery)	REF2, REF1, REF15, REF23

					overwritten.			
3	RE	Evidence correlation	Evidence correlation across multiple cloud Providers	Correlation of activities across cloud Providers is a challenge; interoperability is an issue	For investigators, correlation of activity is a challenge because there is no interoperability between cloud Providers.	Analysis	N/A	REF2, REF1, REF14, REF22
4	OD/RP/RE	Reconstructing virtual storage	Liability and reconstruction of virtual storage in cloud environments from physical disk images	Imaging of media has an added level of complexity in some cloud environments which could cause damage to the original media and add the risk of being sued.	For all investigators and courts, reconstruction of virtual images or storage is challenging because these reconstruction algorithms need to be validated or developed.	Analysis	Incident First Responders (Reconstruction)	REF2, REF3, REF15
5	RP/RE/MS	Timestamp synchronization	Synchronization of timestamps	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.	For analysts, correlating the observables with disparate timestamps is challenging because timestamps may be inconsistent between many sources.	Analysis (Metadata Logs)	N/A	REF40, REF1, REF2, REF4, REF5, REF8
6	RP/RE/MS	Log format unification	Unification of log formats	Unification of log formats has been a traditional issue in network forensics. This challenge is exacerbated in the cloud because it is extremely difficult to unify log formats or make them convertible to each other from the massive resources available in the cloud. Furthermore, proprietary or unusual log formats of one party can become major roadblocks in joint	For analysts, analyzing logs is a challenge due to the lack of unification in log formats that triggers a significant amount of additional work to convert between log formats, and because it can also result in lack and/or omission of essential data.	Analysis (Metadata Logs)	N/A	REF43, REF1, REF2, REF5, REF22

				investigations.				
7	OD/BNA/RP/RE/MS	Use of metadata	Use of metadata	The use of metadata (as an authentication method) may be in peril since common fields (such as creation date, last modified date, last accessed date, etc.) may be changed as the data is migrated to and within the cloud. Metadata may also be changed during the collection process, giving rise to both authentication challenges and spoliation worries. Entities that maintain information in the cloud should consider the impact of the cloud on metadata, and understand what metadata the cloud provider preserves and whether it can be readily accessed for e-discovery purposes.	For all stakeholders, authenticating with metadata within a cloud environment is a challenge because the data may change or not be preserved for e-discovery purposes and the data moves into and within the cloud.	Analysis (Metadata)	N/A	REF42, REF14
8	OD/BNA/RP/RE/MS	Log capture	Timeline analysis of logs	Forensic timeline analysis of logs for DHCP log data and log review with correlation.	For investigators, review of DHCP logs is a challenge because there is no consistency from one cloud Provider to another on how they collect log data.	Analysis (Metadata)	N/A	REF43, REF1, REF2
9	RE	Interoperability issues among providers	No interoperability among providers	Identifying commonalities and major differences between architectures can lead to more efficient, effective, and consistent collection of forensic evidence.	For investigators/law enforcement/analysts, the collection and preservation of forensic evidence is challenging because there is a lack of interoperability among providers and there is lack of control from the customer's perspective into the proprietary architecture and/or the technology used.	Architecture	Standards (Interoperability)	REF44, REF1, REF2, REF3, REF6, REF34

10	RP/RE	Single points of failure	Single points of failure	As has been demonstrated by outages, cloud computing has single points of failure that could adversely impact the ability to acquire useful evidence.	For some investigators, evidence acquisition is a challenge because of the adverse impact of single points of failure.	Architecture	Data Collection	REF45, REF7
11	OD/BNA/RP/RE	No single point of failure for criminals	No single point of failure for criminals	There is no single point of failure allowing criminals to be caught in a straightforward manner; no one computer in a group that holds all of the data necessary for the forensic investigator to reconstruct the information about the crime. A criminal organization can choose one cloud provider as a storage solution (e.g., Dropbox), obtain compute services from a second cloud provider (e.g., Amazon EC2), and route all of their communications through a third (e.g., Gmail or Pastebin).	For all investigators, collection and analysis of data from distributed and disparate sources is challenging because perpetrators can use services from different providers.	Architecture	Data Collection	REF46, REF7
12	OD/BNA/RP/RE	Detection of the malicious act	Detection of the malicious act	Attacks on computer systems are typically performed through sequences of incremental steps where each step in an attack exploits what would appear to be a small vulnerability. This "stepping stone" approach to exploitation also applies in the cloud space. Forensics investigators will not find a single "ah-ha" moment where an attack is launched and a system is compromised. Instead, they will likely find a series of small changes made across dozens of systems and applications to enable an attacker to penetrate a cloud.	For all stakeholders, detecting the steps of a criminal attack on the cloud is challenging because such attacks may comprise many seemingly benign steps across disparate systems.	Architecture	N/A	REF47, REF7, REF41

13	OD/BNA/RP/RE/ MS	Criminals access to low cost computing power	The cloud offers computing power that would otherwise be unavailable to criminals with small budgets	Cloud computing offers computing power that would otherwise be unavailable to criminals with small budgets. Google's AppEngine was used as a command-and-control network for a botnet in 2009. Password cracking the cloud is already offered as a service by one security firm, and the Amazon EC2 computer service was used by a security researcher to crack Wifi WPA-PSK passwords.	For all stakeholders, identifying criminal activities is challenging because the cloud provides computing power at lower cost, empowering unpredictable attacks that would be unpractical outside a cloud environment.	Architecture	N/A	REF48, REF7
14	OD/BNA/RP/RE	Real-time investigation intelligence processes not possible	Intelligence processes for real-time investigation are often not possible in the cloud environment	Data that is not stored in storage media cannot be seized; it can only be collected in real time by placing sensors into the real-time environment. The manner in which such evidence is identified must be different from that in which evidence resides in a desktop or within a disk. This sort of evidence must be identified by an intelligence process and special legal means must be applied in many cases to collect it. In most cloud environments, such intelligence is hard to come by, and most providers do not want to reveal the specifics of their operations. Such operations often change quickly with time, and many parties may be involved. For example, a cloud infrastructure may be composed of leased time on hundreds of systems around the globe, owned and operated by scores of different providers. With records spread across such an infrastructure, even knowing where to look to place sensors is enormously problematic.	For investigators and examiners, investigating real-time incidents in the cloud is challenging because intelligence processes to enable such investigations are often not possible when collaborating/interacting with cloud Providers or other actors.	Architecture	N/A	REF1, REF2, REF3, REF19, REF6, REF5, REF25

15	RP	Malicious code may circumvent VM isolation methods	Malicious code may circumvent virtual machine isolation methods, and interfere with the hypervisor or other guest virtual machines	Vulnerabilities in server virtualization allow an attacker to escape from a guest virtual machine to either another guest or the hypervisor itself. Ensuring that a compromised virtual machine stays isolated requires comprehensive security in the hypervisor and the software that interacts with the virtual machine.	For the investigator/evidence collector, acquiring forensically sound evidence is challenging because malicious code may circumvent virtual machine isolation methods and may interfere with the hypervisor or other guest virtual machines.	Architecture	Anti-Forensics	REF49, REF2, REF3, REF11, REF15, REF23
16	RP/MS	Errors in cloud management portal configurations	Configuration errors in cloud management portals may result in an unauthorized user being able to reconfigure or delete another user's cloud computing platform	Vulnerabilities in management portal applications provided by cloud Providers may be exploited by an unauthorized individual to gain control, reconfigure, or delete another cloud tenants resources or applications.	For the investigator/evidence collector, determining the source of an unauthorized change to a user's cloud computing environment is challenging because multiple individuals are simultaneously using the same cloud management portal.	Architecture (Multi-Tenancy)	Role Management (Identity Management)	
17	BNA/RP/RE/MS	Multiple venues and geo-locations	Access to computer and network resources involve expanded scope and may involve more than one venue and geo-location	Geo-location unknowns can impact the chain of custody in finding evidence and identifying resources that are required for access to the system.	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.	Architecture	Data Collection	REF47, REF1, REF2, REF3, REF4, REF5, REF6, REF8, REF9
18	OD/RP/RE/MS	Lack of transparency	Lack of transparency triggers lack of trust and difficulties of auditing	The cloud's operational details aren't transparent enough to users.	For the investigator/evidence collector, collecting accurate, complete, traceable, audible and forensically sound evidence is challenging because of multiple levels of computation outsourcing and lack of transparency.	Architecture	Data Collection	REF50, REF1, REF2, REF3, REF5, REF19, REF24

19	OD/BNA/RP/RE	Criminals can hide in cloud	The distributed nature of cloud computing enables a criminal organization to maintain small "cells" of operation, with no one cell knowing the identity of any others	Data partitioning allows each cell in the criminal organization to preserve its anonymity while still sharing information on likely victims and the results of any criminal activities. Thus individual members of such an organization may be unaware of the identities of other members.	For all stakeholders identifying "cells" of criminal organizations is challenging because the distributed nature of cloud computing enables the operations of segregated cells of criminal organizations with no one cell knowing the identity of any others; therefore identifying and associating the cells may be difficult.	Architecture	Legal (Contract / SLA) Role Management (Identity Management)	REF7
20	OD/BNA/RP/RE/ MS	Cloud confiscation and resource seizure	Cloud confiscation and resource seizure	Confiscation of cloud resources can often affect the business continuity of co-tenants.	For investigators, confiscation and seizure of cloud resources to acquire evidence may pose a challenge because the business continuity of other tenants may be adversely affected.	Architecture	Legal (Jurisdiction)	REF35, REF1 ,REF2, REF3, REF5, REF12
21	OD/RP/RE	Potential evidence segregation	Segregation of potential evidence in a multi-tenant system	Segregation of forensic data in an infrastructure shared by multiple users (multi-tenant environment) is needed. Technologies used for provisioning and de-provisioning resources are constantly being improved. It is a challenge for cloud Providers and law enforcement agencies to segregate resources during investigations without breaching the confidentiality of other tenants who share the infrastructure.	For providers and investigators, accessing the data of one tenant without breaching the confidentiality of other tenants is challenging because existing technologies to do so are not effective enough.	Architecture (Data Segregation) (Multi-Tenancy)	Data Collection	REF51, REF1, REF2, REF3, REF6, REF19, REF30
22	OD/BNA/RP/RE	Boundaries	Boundaries	System boundaries need to be defined	For all stakeholders, protection of system boundaries is challenging because it is difficult to define system interfaces.	Architecture (Multi-Tenancy)	Data Collection	REF24

23	OD/BNA/RP/RE	Secure provenance	Secure provenance	Ensuring chain of custody by secure provenance for data capture	For law enforcement, ensuring proper chain of custody and security of data, metadata, and possibly hardware is a challenge because it may be difficult to determine ownership, custody, or accurate location.	Architecture (Provenance)	N/A	REF52
24	OD/BNA/RP/RE/ MS	Data chain of custody	Chain of custody of data	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.	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.	Architecture (Provenance)	N/A	REF8, REF1, REF2, REF3, REF5, REF6, REF13, REF19
25	OD/BNA/RP/RE/ MS	Decreased access and data control	Decreased access and control of data at all levels by cloud consumers	In every combination of cloud service model and deployment model, the cloud customer faces the challenge of decreased access to forensic data. Access to forensic data varies considerably based on the cloud model that is implemented. Decreased access to forensic data means that cloud customers generally have little or no control - or even knowledge - of the physical locations of their data. In fact, they may only be able to specify location at a high level of abstraction, typically as an object or container. Cloud Providers intentionally hide data locations from customers to facilitate data movement and replication.	For all investigators, gaining access to forensic data is a challenge because there is decreased access and control at all levels for all consumers.	Data Collection	N/A	REF54, REF1, REF2, REF5, REF30

26	OD/BNA/RP/RE/ MS	Chain of dependencies	Chain of dependencies in multiple cloud systems	Cloud Providers and most cloud applications often have dependencies on other cloud Providers. For example, a cloud Provider that provides an email application (SaaS) may depend on a third-party provider to host log files (i.e., PaaS), which in turn may rely on a partner who provides the infrastructure to store log files (IaaS). A cloud forensic investigation thus requires investigations of each individual link in the dependency chain.	For all investigators, performing investigations and accessing evidence are a challenge, because the dependencies of multiple cloud systems requires investigations of each individual link in the dependency chain.	Data Collection	N/A	REF1, REF2, REF5
27	OD/BNA/RE/RP/ MS	Locating evidence	Locating evidence in a large and changing system	E-discovery is a critical component in cloud computing and essential for locating data that may be requested in a subpoena. However, the time frame for responses and the thoroughness of results are questionable due to the lack of knowledge of all locations of data storage.	For all investigators, locating and collecting data is challenging because data may quickly change or disappear and requestors lack knowledge of where and how data are stored.	Data Collection	N/A	REF35, REF1, REF2, REF3, REF5, REF8, REF12, REF14, REF24, REF25
28	OD/RP/RE/MS	Data location	Data location	There are many uncertainties dealing with transparency in the cloud and distribution boundaries for retrieval due to multiple tenants in multiple data centers.	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.	Data Collection	N/A	REF35, REF1, REF2, REF3, REF4, REF5, REF8, REF9, REF11, REF12, REF13, REF14, REF15, REF19

29	OD/BNA/RP/RE/MS	Imaging and isolating data	Data mirroring and tracking the movement of data	Data mirroring over multiple machines in different jurisdictions, as well as the lack of transparent, real-time information about data locations introduces difficulties in forensic investigations.	For first responders, imaging media and isolating a moving data target is challenging in a cloud environment because of the main characteristics of the cloud such as elasticity, automatic allocation/de-allocation of resources, redundancy and multi-tenancy.	Data Collection	N/A	REF55, REF1, REF2
30	OD/BNA/RP/RE/MS	Data available for a limited time	Data associated with newly created virtual machine instances may only be available for a limited time	No research has been conducted on determining what data is associated with removed VM instances. If a new VM instance is created and either compromised or used to attack, evidential traces may be available in the VM. If the VM instance is then de-allocated, investigators currently do not know whether evidential traces or the entire VM instance could be recovered.	For all stakeholders, forensic data collection and preservation of virtual machines is a challenge because standard practices and tools do not yet exist.	Data Collection	N/A	REF56, REF15
31	OD/BNA/RP/RE/MS	Locating storage media	Identifying storage media where artefacts, log files and other evidence may be found	In the cloud, a computer instance may not have local persistent storage as all storage occurs through an object store held remotely. Thus the operational security model of the application, which assumes a secure local log file store, is now broken when moved into a cloud environment.	For all stakeholders, locating storage in the cloud with certainty is challenging because locating, with certainty, storage requires a thorough understanding of the cloud architecture and implementation.	Data Collection	N/A	REF1, REF2, REF3, REF8, REF9, REF12, REF13, REF14, REF15

32	OD/BNA/RP/RE/ MS	Evidence identification	Sources/traces of evidence are generated differently compared to non-cloud environments and pose challenges for evidence identification	The first step in gathering evidence is identifying possible sources of evidence for collection. It is fairly common that identified evidence includes too little or too much information. If too much is identified, then court-mandated search and seizure limitations maybe exceeded. If too little is identified, exculpatory or inculpatory evidence may be missed. Commonly missed evidence comes in the form of network logs from related network components. In most cloud computing environments, most of the evidence, and particularly most of the redundant traces, are either not available or are not generated or stored in the same way as they would be in traditional non-cloud environments. User-based login and controls are typically in the application rather than in the operating system, so records tend to be limited to whatever the application designer decided to do.	For investigators and examiners, identifying sources/traces of evidence is challenging because they are either not available or are not generated or stored in the same way as they are in traditional non-cloud environments.	Data Collection	N/A	REF57, REF8, REF30
33	OD/BNA/RP/RE/ MS	Dynamic storage	Dynamic storage	Some cloud Providers dynamically allocate storage based on the current needs of the user. As data is deleted from the system, the storage is re-allocated to optimize data reads and storage use.	For all stakeholders, data collection of evidence is a challenge because of the dynamic allocation of storage, and systems that scavenge storage after an item is deleted.	Data Collection	N/A	REF24, REF29

34	OD/BNA/RP/RE/MS	Live forensics	Live forensics is common in cloud environments, but many challenges remain	When evidence is collected in a cloud environment, the suspect system is still running and data is likely to be changing as it is being collected. Therefore it is impossible for a third party to verify, after acquisition, that the data collected is correct because the data is no longer the same as at the time of acquisition. When conducting live data forensics, the processes used in data acquisition will result in changes to the system. In order to collect volatile evidence, the suspect computer must remain on, and the suspect operating system must be used to access the needed data. For example, when retrieving information from RAM a program must be loaded into the running memory, changing its contents. Even just inserting a USB key into a running suspect system will alter the system. Therefore, live data forensics usually relies on the suspect system. Carrier [REF66] claims that the suspect system cannot be trusted. Rootkits or other malware in the suspect system can provide various anti-forensic functions, resulting in unreliable evidence [REF70]. Also, data residing in a VM are volatile, as after terminating a VM, all the data may be lost. Volatile data of a VM includes all the logs stored in that VM, e.g., SysLog, registry logs, and network logs.	For forensics examiners, verifying the validity and integrity of data collected is a challenge because the data within the cloud is volatile and constantly changing and live forensics tools will make changes to the suspect system.	Data Collection	Architecture	REF58, REF1, REF2, REF3, REF5, REF6, REF19, REF25

35	OD/BNA/RP/RE/ MS	Resource abstraction	Resource abstraction	In cloud computing, abstract resources are made available to cloud consumers. This is often desirable to consumers who do not want to know how the cloud is implemented, but the lack of transparency makes forensics challenging. The forensic investigator may need to know what hardware, what hypervisor, what file system, etc. are used in order to accurately understand the environment.	For the investigators/evidence collectors, discovering evidence and acquiring the evidence in a forensically sound manner is challenging because the resources are abstracted and the information regarding cloud architecture, hardware, hypervisor, and file system type is not available to accurately understand the environment.	Data Collection	Architecture	REF50
36	MS	Application details are unavailable	Private and confidential details of cloud-based software/applications used to produce records are typically unavailable to the investigator	For example, in a particular criminal case involving email through cloud Providers, the details of how drafts are turned into deliverable messages were unavailable, leading to the inability to prove whether or not a draft was ever sent (and more obviously whether it was ever transmitted or received).	For investigators and examiners, obtaining details of a software/application under question hosted in the cloud is challenging because such details might very likely be unavailable.	Data Collection	Architecture	REF8
37	OD/RP/RE/MS	Additional evidence collection	Additional collection is often infeasible in the cloud	Relevant forensic information is often located in places not immediately evident from the original crime scene. In traditional digital forensics, for cases where evidence is stored for long periods and can be identified as missing in a timely fashion, the problem can usually be mitigated by additional collection. But in cloud environments, such collection is often infeasible as specific locations of content are unknown, the volumes may be very high, and the protocols and mechanisms used to exchange information may be non-standard and poorly or not documented.	For investigators and examiners, collecting additional evidence is challenging because collection is often infeasible as specific locations of content are unknown, the volumes may be very high, and the protocols and mechanisms used to exchange information may be non-standard and poorly or not documented.	Data Collection	Architecture	REF50, REF8

38	OD/BNA/RP/RE/ MS	Imaging the cloud	Imaging the cloud	Imaging all evidence in the cloud is impractical while partial imaging may have legal implication in the presentation to the court, this leads to the suggestion that forensic acquisition processes and tools should be an integrated part of the cloud functionality, instead of a bolt-on service	For forensics examiners, law enforcement, and the courts, imaging evidence in the cloud is a challenge because imaging all evidence in the cloud is impractical while partial imaging may have legal implication in the presentation to the court.	Data Collection	Architecture	REF58, REF1, REF2, REF4, REF11, REF15, REF30
39	OD/BNA/RP/RE/ MS	Selective data acquisition	Selective data acquisition	Selective data acquisition implies a preliminary analysis, or some prior knowledge, to reduce the overall dataset in which an investigator is interested. Some investigators focus on data sources that they believe are likely to provide the richest sources of information, but justifiable exclusion remains a challenge.	For forensic examiners, performing a selective data acquisition is a challenge because prior knowledge about relevant data sources is often difficult to obtain in a cloud environment.	Data Collection	Incident First Responders	REF20, REF21
40	OD/BNA/RP/RE/ MS	Cryptographic key management	Cryptographic key management	Ineffective encryption key management makes it easier to lose the ability to decrypt forensic data stored in the cloud	For all investigators, decryption of data is a challenge because the ephemeral nature of cloud resources (flexibility, elasticity, volatility, always changing, etc.) and the scale of the systems may cause ineffective key management and the loss of the ability to decrypt data needed for forensic investigations.	Data Collection	Legal (Privacy)	REF59, REF1, REF2, REF3, REF5, REF19
41	OD/BNA/RP/RE/ MS	Ambiguous trust boundaries	Ambiguous trust boundaries between users can cause questionable data integrity	The use of cloud services, especially of multi-tenant environments, may increase risk to the integrity of data, both at rest and during processing.	For investigators/evidence collectors, obtaining non-corrupted, complete set of data for forensic evidence poses a challenge in multi-tenant cloud environments because not all vendors implement vertical isolation for consumers' data	Data Collection (Data Integrity)	N/A	REF58, REF15, REF26

42	OD/BNA/RP/RE/MS	Data integrity and evidence preservation	Responsibility for quality of evidence, evidence admissibility, faults and failures in data integrity and digital preservation is shared among multiple actors and the opportunities for such faults and failures are higher in the cloud context	Digital evidence that is presented in court is admitted or rejected based on the relative weights of probative and prejudicial value. Faults occur either intentionally or accidentally and consist of missed content, contextual information, meaning of content, process elements, relationships, ordering, timing, location, corroborating content, consistencies, and inconsistencies. In the cloud, the faults may extend to multiple computers in multiple locations under control of multiple parties. Thus opportunities for faults and failures are extended in the cloud.	For all stakeholders, maintaining quality of evidence, evidence admissibility and integrity of data and preserving evidence is challenging because faults and failures in data integrity are shared among multiple parties, and the chance for such faults and failures increases in cloud environments due to the sharing of data/responsibilities.	Data Collection (Data Integrity)	Architecture	REF60, REF8
43	OD/BNA/RP/RE/MS	Root of trust	Root of trust	Cloud implementations have multiple layers of abstraction, from hardware to virtualization to guest operating systems. The integrity and trustworthiness of forensic data is dependent on the cumulative trustworthiness of the layers that could potentially manipulate or compromise data integrity. Further, users must now trust cloud providers, unless integrity can be guaranteed another way (e.g. cryptographic hashes, hardware roots of trust, etc.).	For all investigators, determining the trustworthiness and integrity of cloud forensics data is a challenge because of the dependence on the cumulative integrity of multiple layers of abstraction throughout the cloud system.	Data Collection (Data Integrity)	Legal	REF58, REF21, REF24, REF26
44	OD/BNA/RE	Competence and trustworthiness	Competence and trustworthiness of the cloud Provider as an effective, immediate first-responder	When an incident occurs on the side of the cloud Provider, the cloud Provider may be more concerned with restoring service than with preserving evidence. Further, the cloud Provider may begin its own investigation into an incident without taking proper precautions to ensure the integrity of potential evidence. In more severe cases, cloud Providers may not report or cooperate in investigation of incidents for fear of	For all stakeholders confidence, competence, and trustworthiness of cloud providers acting as first-responders is a challenge because the goals and priorities of the cloud providers may differ from those of the investigators.	Incident First Responders	Legal (Contract / SLA)	REF58, REF21, REF24, REF26, REF28, REF30

				reputational damage.				
45	OD/BNA/RP/RE/ MS	Missing terms in contract or SLA	Missing terms in contract or Service Level Agreement	Requirements that the cloud provider maintain and/or produce pertinent evidence within specified time constraints may not be specified in the agreement.	For all stakeholders, lack of forensic related terms in cloud contracts is challenging because it could inhibit the generation and collection of existing appropriate data as well as generating potentially appropriate data.	Legal (Contract / SLA)	N/A	REF1, REF2, REF5, REF32
46	OD/BNA/RP/RE	Limited investigative power	Limited investigative power	In civil cases, there may be limited investigative power given to investigators or consulting firms to legally obtain data under the respective jurisdictions.	For investigators and consulting firms, obtaining data for civil cases under the respective jurisdictions is challenging because they often have limited investigative powers.	Legal	N/A	REF35, REF1, REF2, REF12
47	RP/RE/MS	Reliance on cloud providers	Reliance on cloud providers	Data acquisition today relies almost exclusively on cooperation of cloud providers, often in compliance with legal processes. Cooperation may be limited by the number of employees and other resources at the provider, and does not scale.	For all investigators, acquiring cloud forensics data is challenging because it relies on the cooperation of the cloud Providers, which may be limited due to limited provider resources.	Legal	N/A	REF54, REF1, REF2, REF3, REF4, REF12, REF13, REF21

48	RE	Physical data location	Physical data location	Because physical locations of data are unknown (due in part to lack of local storage and access to the hardware), there are difficulties in specifying and responding to subpoenas. This can inhibit collection of evidence by a first responder, particularly dynamic evidence. Therefore acquisition of forensic images is preferred over seizure of servers from a data center which is not feasible due to the conflict with privacy rights of other tenants.	For law enforcement and courts, specifying on a subpoena the physical location(s) of data is challenging because the requestor often does not know where the data is physically stored.	Legal	N/A	REF1, REF2, REF3, REF5, REF9
49	BNA/RP/RE/MS	Port protection	Port protection	Scanning of ports using SPAN or TAPS is a challenge.	For investigators, scanning of ports is challenging because cloud Providers do not provide access to the physical infrastructure of their networks.	Legal	Data Collection	
50	BNA/MS	Transfer protocol	Transfer protocol	There is a need to ensure the capability of TCP/IP v 6 dumps and Windows dumps including TCP segment deciphering.	For investigators, dumping of TCP/IP network traffic is a challenge because cloud Providers do not provide access to the physical infrastructure of their networks.	Legal	Data Collection	
51	OD/BNA/RP/RE/MS	E-discovery	E-discovery	There are extensive challenges in response time to an e-discovery request because of location uncertainty of data and the need for assurance of completion of the request.	For all stakeholders, response time for e-discovery is challenging because of location uncertainty of the data and the uncertainty about whether all relevant data were discovered.	Legal	Data Collection	REF35, REF1, REF2, REF14
52	OD/BNA/RP/RE/MS	Lack of international agreements & laws	Lack of international agreements and laws	There is a lack of international collaboration and legislative mechanisms in cross-nation data access and exchange.	For all stakeholders, gaining access to and exchanging data is challenging because of lack of international collaboration and lack of cross-nation legislative mechanisms.	Legal (Jurisdiction)	N/A	REF36, REF1, REF2, REF6, REF13

53	BNA/RP/RE/MS	International cloud services	There has been very little definition of what to do if data is stored on a non-national cloud service that is currently connected while the investigator begins a live analysis of the suspect system.	If the data is accessible, an investigator may save a considerable amount of time by acquiring the data from the connected service rather than waiting for international requests. However, authority on this matter is not always clear. A lack of definition on the scope of acquisition of data on non-national remote connections sometimes depends on the country, and many times depends on the investigator's preliminary analysis of the remotely stored data as well as the likelihood of receiving the data if an international request was made.	For all investigators, real-time, live access to data on international cloud services is challenging because of lack of definition and agreements dealing with authority to access the data.	Legal (Jurisdiction)	N/A	REF21
54	RP	Jurisdiction	Jurisdiction	A growing number of inter-connected devices can be exploited from almost anywhere in the world, but law enforcement still struggle with the concept of jurisdiction in an online world without borders, sometimes resulting in illegal, or at least questionable, cross-border actions by law enforcement	For all investigators, legal access to data is challenging because questions of international jurisdiction have not been worked out.	Legal (Jurisdiction)	N/A	REF35, REF1, REF2, REF3, REF4, REF5, REF6, REF8, REF9, REF12, REF13, REF19, REF20

55	OD/BNA/RP/RE/MS	International communication	International communication	Cloud computing blurs physical, policy, and jurisdictional boundaries globally. However, law enforcement at a global level has yet to find effective, timely, and efficient international communication and cooperation channels. Conferences such as the International Symposium on Cybercrime Response specifically discuss international law enforcement communication and collaboration efforts. Global law enforcement communication channels, such as INTERPOL's I-24/7 network or the G8 24/7 network, connect many countries, but are limited by their structure and bureaucracy. Many officers have found the global networks to be somewhat effective if the request is not overly urgent. However, these networks have failed to address real-time requests for help from countries under DDoS attack. Many times, law enforcement will prefer faster, informal channels to begin an international investigation, rather that traversing such networks.	For law enforcement, achieving timely and effective communication and cooperation at an international level when dealing with an investigation in a multi-jurisdictional cloud is challenging because mechanisms and networks for such communication are often slow and inefficient.	Legal (Jurisdiction)	N/A	REF2, REF1, REF2, REF3, REF5, REF8, REF9, REF13, REF20, REF31
56	RP/MS	Confidentiality and PII	Concern for confidentiality and personally identifiable information (PII)	Cloud computing has significant implications for the privacy of personal information as well as for the confidentiality of business and governmental information; there is a lack of legislative mechanism facilitating evidence retrieval involving confidential data.	For all stakeholders, maintaining confidentiality of cloud data is challenging because of lack of legislation governing the conditions under which such data can be accessed by investigators.	Legal (Privacy)	N/A	REF37, REF6, REF13

57	BNA/RP/RE/MS	Reputation fate sharing	"Reputation fate sharing"	Reputation does not virtualize well. One customer can impact the reputation of the cloud provider and all co-hosted users. A spammer using the cloud Provider's IP range may get these IP addresses blacklisted. This could potentially disrupt service of legitimate cloud customers if they are later assigned IP addresses that have been blacklisted.	For legal/ethical cloud consumers and cloud providers, rehabilitating the reputation affected by illegal/unethical activities of some cloud consumers is challenging because the dynamic, automatic assignment of resources (e.g., IP addresses) might cause the assignment of resources that have been blacklisted due to the illegal/unethical activities of some cloud consumers to other legal/ethical cloud consumers. Such an assignment affects the legal/ethical cloud consumer's activities and overall cloud provider's reputation, and ultimately business.	Legal (Ethical)	N/A	REF38, REF20
58	OD/BNA/RP/RE/MS	Identifying account owner	Role management makes it difficult to identify suspect	Insufficient granularity of user/process identities and/or the lack of policy enforcement requiring use of unique identities may inhibit the ability to positively identify a suspect.	For all investigators, positively identifying the owner of an account is challenging because the technology or policy does not support sufficient identification of the owner of the account.	Role Management (Identity Management)	N/A	REF1, REF2, REF5, REF19
59	OD/BNA	Fictitious identities	Criminals can create entire fictitious identities online to link to their cloud accounts, creating excess "noise" for the forensic investigator to analyze	For example, most cloud providers will require a name, address, and credit card to register an account. A criminal can trivially obtain credit card numbers, and then create fake profiles on existing legitimate social media websites to make his/her cloud identity appear to have a corresponding equivalent in the "real world." A forensic investigator is then faced with the daunting challenge of obtaining data on the criminal identity from multiple online entities, many of which are geographically spread around the world.	For all investigators, determining the actual identity of a cloud user (legitimate or illegitimate) is challenging because criminals can enter fictitious identities.	Role Management (Identity Management)	N/A	

60	BNA	Decoupling user credentials & physical location	Decoupling between cloud user credentials and physical users	Due to the decoupling between cloud user credentials and physical users, network-type metadata plays a significant role in the data acquisition process. A challenge is how to bind a cloud username with a physical entity in order to prove the physical ownership of the data attributed to the cloud username.	For forensics examiners, positively attributing a cloud user's credentials to a physical user is a challenge because there is no mandatory non-repudiation methods implemented in the cloud and sophisticated encryption and network proxy services may raise questions as to the validity of network-type metadata.	Role Management (Identity Management)	N/A	REF15
61	RP	Authentication and access control	Authentication and access control	Access control in cloud environments is somewhat difficult, and may not meet data protection regulations.	For forensics examiners (and other pertinent actor), positively identifying the entities that accessed data without being authorized (as opposed to the actors who were authorized to access the data) is challenging because the authentication and access control to users' cloud accounts may not meet data protection regulations.	Role Management (Identity Management)	N/A	REF1, REF2, REF3, REF5, REF19, REF24
62	OD/BNA/RP/RE/ MS	Testability, validation, and scientific principles not addressed	Testability, validation, and scientific principles have not been widely addressed	Test and validation processes for cloud forensics hardware, software, policies, and techniques have not been created.	For law enforcement and courts, using and/or collecting results from tested and validated tools and techniques is challenging because test beds, test processes, validated techniques, and trained test engineers specializing in cloud environments are rare.	Standards	N/A	
63	OD/BNA/RP/RE/ MS	Lack of standard processes & models	Lack of standard processes and models	"The reality is that there is no single process for digital forensics." Various process models have been proposed, however there is no one accepted standard, and the majority of organizations are creating their own SOPs, which may or may not be based on an existing process model.	For forensics examiners, law enforcement, and the courts, establishing standard procedures and best practices for investigations in the cloud is a challenge because standards and procedures in cloud forensics are much less mature than in traditional forensics and far from being widely adopted.	Standards (No Single Process)	N/A	REF1, REF2, REF6, REF9, REF19, REF20

64	MS	Limited knowledge of logs and records	Custodians and individuals responsible for record keeping in cloud provider companies might have limited knowledge on what logs and records might be sought for as evidence	Unlike a traditional computing environment to which the forensics examiner might have access to perform experiments, in the cloud, the details of what logs are produced, what other records are produced and/or kept, and where they might be found are opaque except through testimony of representatives of the provider. In many cases, these individuals are custodians of the records, but don't have detailed knowledge of technologies or actual records that might be found if sought. Indeed, companies benefit from not keeping such records or having custodians with only limited knowledge.	For all stakeholders, trusting records/logs kept in cloud environments is challenging because custodians and individuals responsible for these operations might have only limited knowledge and may not be qualified for evidence preservation.	Training	N/A	REF10
65	OD/BNA/RP/RE/ MS	Cloud training for investigators	Lack of training materials that educate investigators on cloud computing technology and cloud forensics operating policies and procedures.	Most digital forensic training materials are outdated and are not applicable in cloud environments. The lack of knowledge about cloud technology may interfere with remote investigations where systems are not physically accessible and there is an absence of proper tools to effectively investigate the cloud computing environment. Operating system virtualization permits the implementation of many different operating systems that share the same underlying platform resources. This includes the sharing of operating system and security software as well as hardware. Moreover, only few standard operating policies are in place for cloud forensics making the approach more trial and error than scientific.	For forensics investigators/evidence collector, getting trained in cloud computing technology and forensics operations in cloud environments are challenging because most digital forensic training materials are outdated and do not address cloud environments.	Training (Qualification & Certification)	Standards (No Single Process)	REF1, REF2, REF5, REF8

Annex C - Mind Maps

Annex C.1: Categories and Subcategories

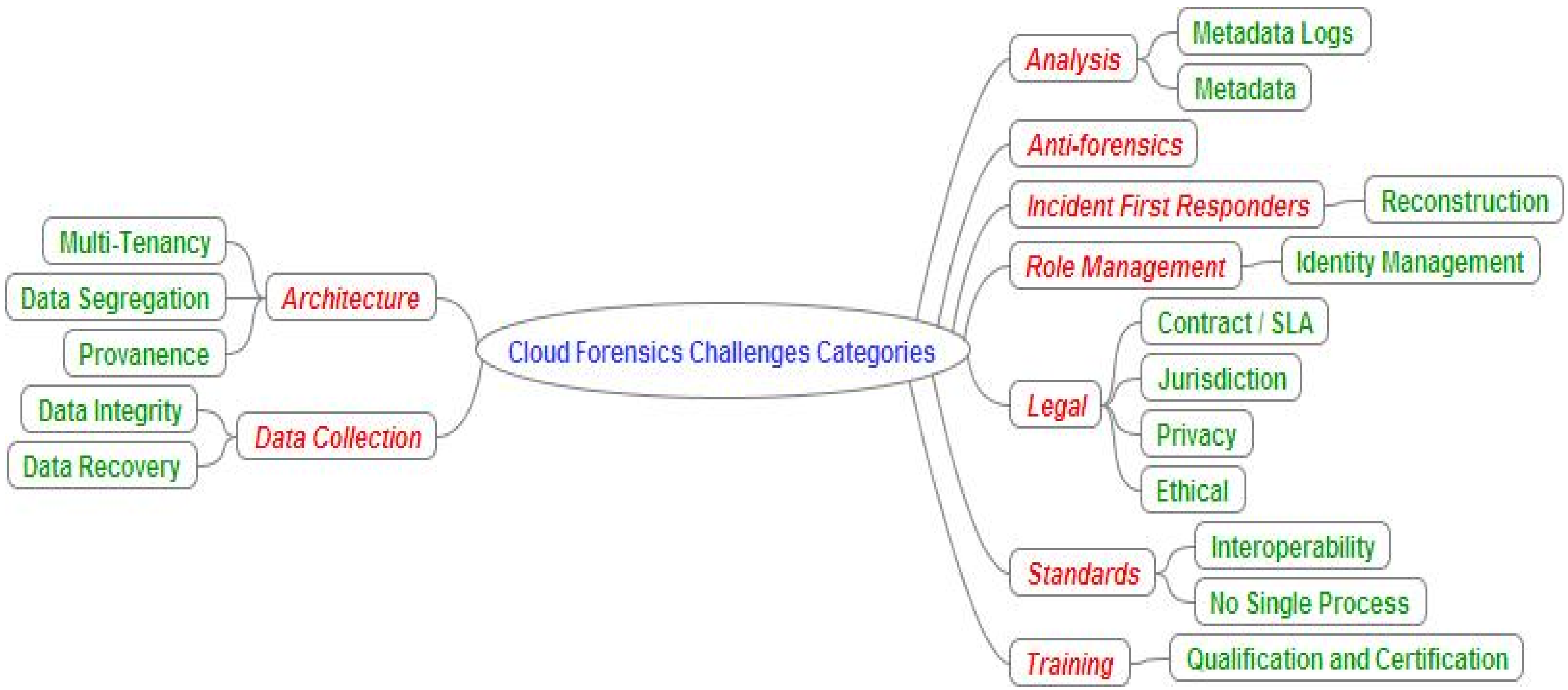

Figure 2: Mind Map – Categories and Subcategories

Annex C.2: Primary Categories

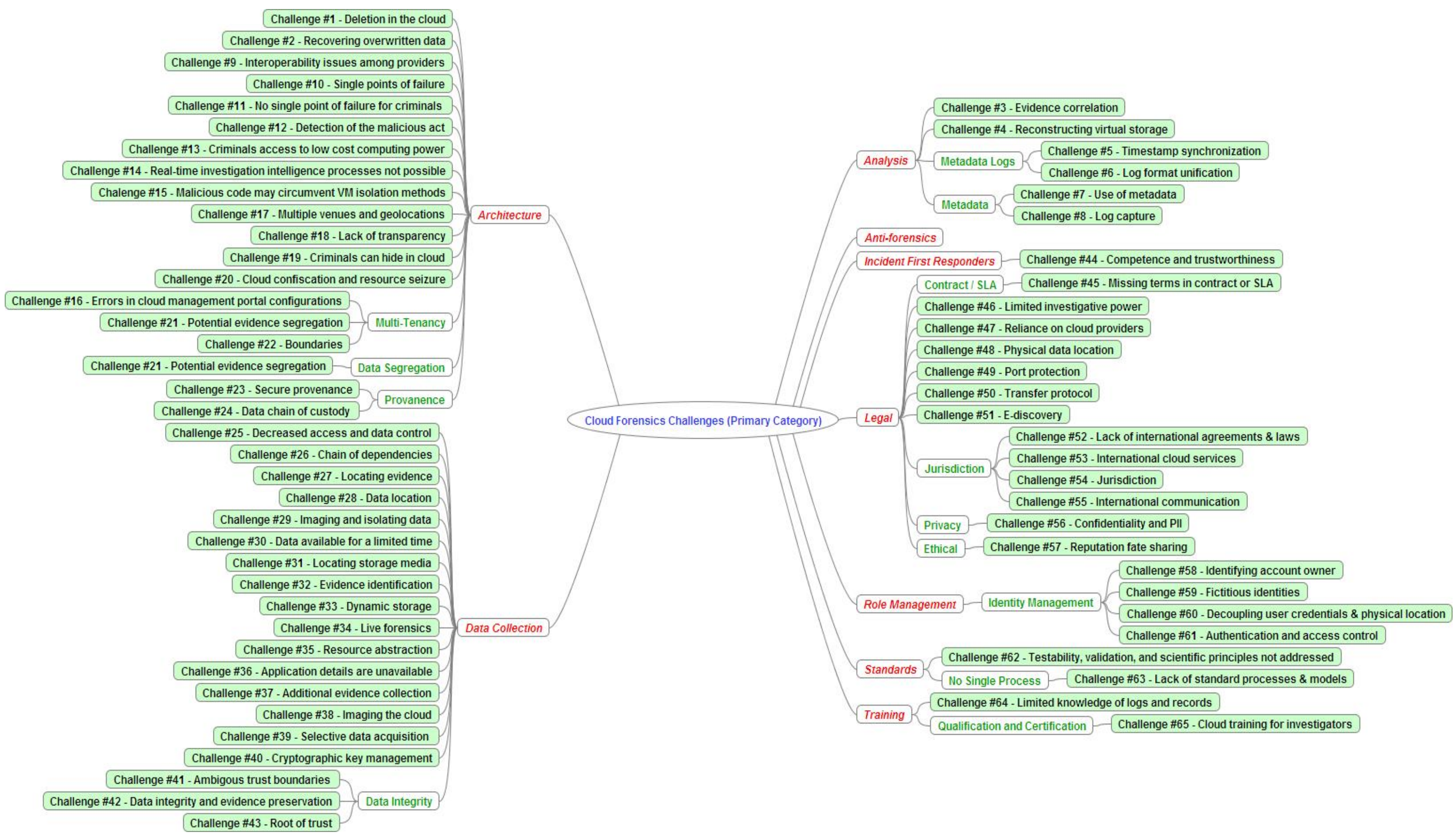

Figure 3: Mind Map – Primary Categories

Annex C.3: Related Categories

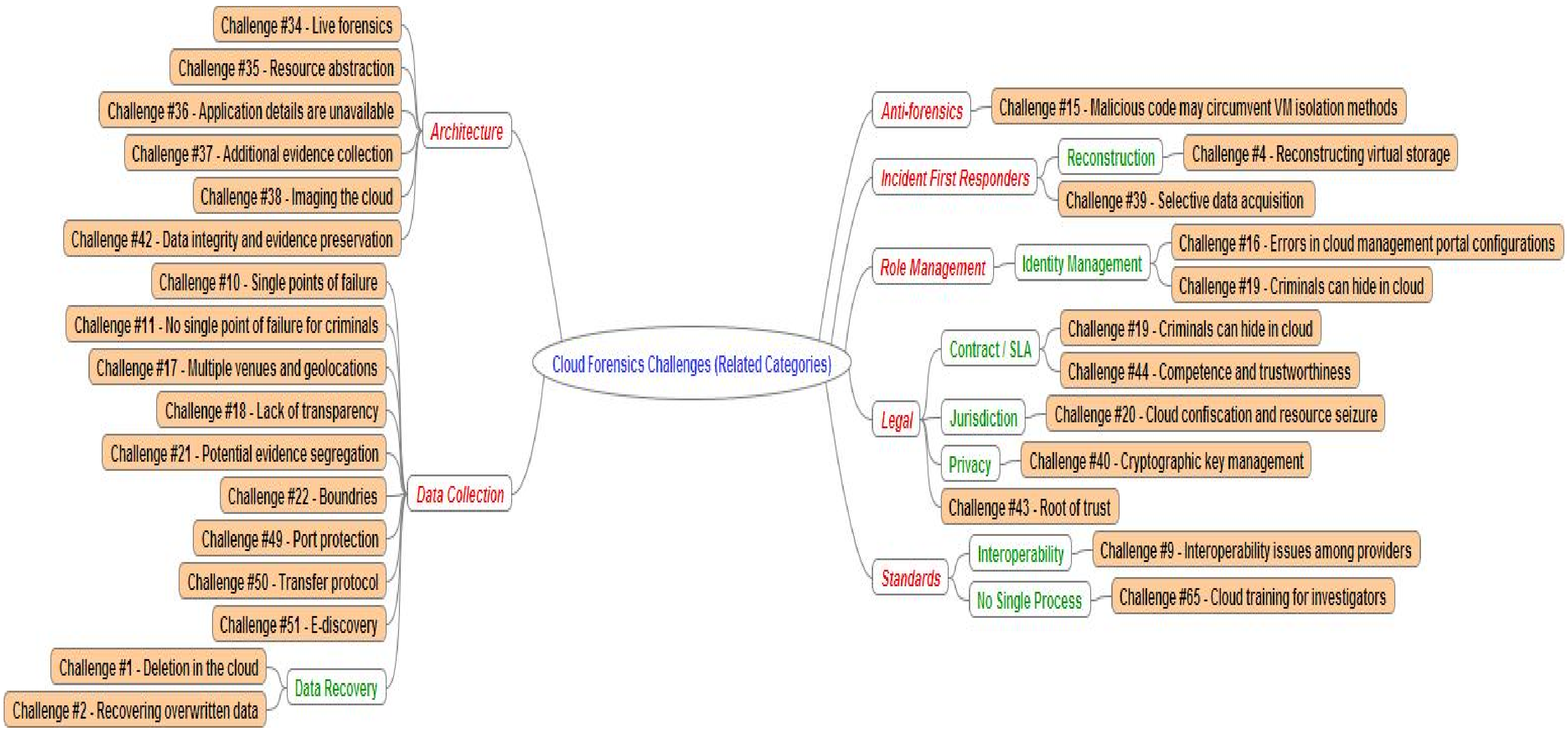

Figure 4: Mind Map – Related Categories