NISTIR 8006

NIST Cloud Computing Forensic Science Challenges

Martin Herman
Michaela Iorga
Ahsen Michael Salim
Robert H. Jackson
Mark R. Hurst
Ross Leo
Richard Lee
Nancy M. Landreville
Anand Kumar Mishra
Yien Wang
Rodrigo Sardinas

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8006

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

NISTIR 8006

NIST Cloud Computing Forensic Science Challenges

Martin Herman
Information Access Division
Information Technology Laboratory

Michaela Iorga
Computer Security Division
Information Technology Laboratory

Ahsen Michael Salim
American Data Technology, Inc.
Research Triangle Park, NC

Robert H. Jackson
Mark R. Hurst
SphereCom Enterprises Inc.
Marshall, VA

Ross Leo
University of Houston-Clear Lake
CyberSecurity Institute
Houston, TX

Richard Lee
Citizens Financial Group
Johnston, RI

Nancy M. Landreville
MELE Associates (Germantown, MD)
and Univ. of Maryland, GC (Adelphi, MD)

Anand Kumar Mishra
Malaviya National Institute of Technology
Jaipur, India

Yien Wang
Rodrigo Sardinas
Auburn University
Auburn, AL

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8006

August 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8006
87 pages (August 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8006

Comments on this publication may be submitted to:

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

All comments are subject to release under the Freedom of Information Act (FOIA).

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 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

cloud computing forensics; digital forensics; forensic science; forensics; forensics challenges.

Acknowledgments

This report is dedicated to the memory of our colleague, collaborator, and friend, Ernesto F. Rojas of Forensic & Security Services Inc., who passed away unexpectedly.

Final Report

This publication was developed by the *NIST Cloud Computing Forensic Science Working Group (NCC FSWG)* chaired by Dr. Martin Herman and Dr. Michaela Iorga. NIST and the co-chairs wish to gratefully acknowledge and thank the members whose dedicated efforts contributed significantly to addressing the public comments to the June 2014 Draft report and to updating and enhancing the publication. We also thank Ramaswamy Chandramouli of NIST and Kim-Kwang Raymond Choo of the University of Texas at San Antonio for reviewing the document and providing feedback.

June 2014 Draft Report

NOTE: The following section acknowledges the initial collaborators and is reproduced exactly as it appeared in the June 2014 draft report.

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. NIST, 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.

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,[1] the NIST Cloud Computing Program (NCCP) has developed the NIST Cloud Computing Standards Roadmap [1] as one of many mechanisms in support of the U.S. Government's (USG's) secure and effective adoption of cloud computing technology[2] 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. The importance of setting standards in close relation with private sector involvement is highlighted in a memorandum from the Office of Management and Budget (OMB), M-12-08 [2], dated January 17, 2012.

With the rapid adoption of cloud computing technology, a 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[3] 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 incident response and internal enterprise operations.

The NIST Cloud Computing Forensic Science Working Group (NCC FSWG) was established to research forensic science challenges in the cloud environment and to develop plans for standards and technology research to mitigate the challenges that cannot be addressed by current technology and methods. The NCC FSWG has surveyed existing literature and defined a set of challenges related to cloud computing forensics. These challenges, along with associated literature, are presented in this document. The document also provides a preliminary analysis of these challenges by including: (1) the relationship between each challenge to the five essential characteristics of cloud computing as defined in the NIST cloud computing model [3], (2) how the challenges correlate to cloud technology, and (3) nine categories to which the challenges belong. In addition, the analysis considers logging data, data in media, and issues associated with time, location, and sensitive data.

---

1 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.

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

3 The NIST definition of cloud computing [3] requires that The Provider's computing resources are pooled to serve multiple Consumers using a multi-tenant model…

Table of Contents

EXECUTIVE SUMMARY ..... **VIII**

1 INTRODUCTION **2**

1.1 DOCUMENT GOALS 2
1.2 AUDIENCE 2

2 OVERVIEW **3**

2.1 CLOUD COMPUTING FORENSIC SCIENCE 3
2.2 DEFINING WHAT CONSTITUTES A CHALLENGE FOR CLOUD COMPUTING FORENSICS 4

3 CLOUD FORENSIC CHALLENGES **5**

3.1 COLLECTION AND AGGREGATION OF FORENSIC SCIENCE CHALLENGES 5
3.2 ANALYSIS AND CATEGORIZATION OF THE CHALLENGES 6
3.2.1 Relevance of Essential Cloud Characteristics *6*
3.2.2 Correlation Between Cloud Technology and Forensic Science Challenges *7*
3.2.3 Categorization of Challenges *8*

4 ADDITIONAL ANALYSIS OF THE CHALLENGES **11**

4.1 ADDITIONAL OBSERVATIONS 12

5 CONCLUSIONS **14**

REFERENCES **15**

APPENDIX A: ACRONYMS **22**

APPENDIX B: GLOSSARY **24**

ANNEX A: CLOUD FORENSIC CHALLENGES **26**

ANNEX B: CSA'S ENTERPRISE ARCHITECTURE (TCI V2.0) **77**

ANNEX C: MIND MAPS **78**

Table of Figures

Figure 1: CSA's Enterprise Architecture 78

Figure 2: Mind Map – Categories and Subcategories 78

Figure 3: Mind Map – Primary Categories 79

Figure 4: Mind Map – Related Categories 80

1 Introduction

Cloud computing has revolutionized the methods by which digital data is stored, processed, and transmitted. One of the most daunting new challenges is how to perform digital forensics in various types of cloud computing environments. The challenges associated with conducting forensics in different cloud deployment models, which may cross geographic or legal boundaries, have 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 methods and practices 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, as well as to provide capabilities for security incident response and internal enterprise operations.

The cloud exacerbates many technological, organizational, and legal challenges already faced by digital forensic examiners. Several of these challenges—such as those associated with data replication, location transparency, and multi-tenancy—are somewhat unique to cloud computing forensics [4], [72]. The NCC FSWG has collected and aggregated a list of cloud forensic challenges (see Annex A) that are introduced and discussed in this document. Future work will involve identifying gaps in technology and standards related to the challenges that need to be addressed and developing possible technological and standards approaches to mitigate these challenges.

1.1 Document Goals

This document is intended to serve as a basis for a dialogue on forensic science concerns in cloud Ecosystems[4] and as a starting point for understanding those concerns (challenges) with the intent of allowing the cloud computing community to identify the technologies and standards that can mitigate these challenges.

1.2 Audience

The primary audience for this document includes digital forensic examiners, developers 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 Consumers—may also be interested in certain aspects of this document.

[4] The term Ecosystems is capitalized here for consistency with the capitalization of cloud-related terms in other NIST publications. Other terms to be capitalized in this report include cloud Actor, Provider, Consumer, Auditor, Broker and Carrier.

2 Overview

This section discusses the characteristics 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 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 law, 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 other than legal and regulatory issues 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 the identification, acquisition, preservation, examination, interpretation, and reporting of potential digital evidence.

NIST defines *cloud computing* 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 [3]. Cloud forensics is a process applied to an implementation of this cloud model.

A number of researchers have defined *cloud forensics* as the application of digital forensic science in cloud environments [4], [72], [73]. Technically, it consists of a hybrid forensic approach (e.g., remote, virtual, network, live, large-scale, thin-client, thick-client, including end-point devices used to access cloud services) to the discovery of digital evidence. Organizationally, it involves interactions among cloud Actors (i.e., Provider, Consumer, Broker, Carrier, 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 [5]:

1. **Search authority.** Legal authority is required to conduct a search and/or seizure of data.
2. **Chain of custody.** In legal contexts, chronological documentation of access and handling of evidentiary items is required to avoid allegations of evidence tampering or misconduct.
3. **Imaging/hashing function.** When items containing potential digital evidence are found, each should be carefully duplicated and then hashed to validate the integrity of the copy.
4. **Validated tools.** When possible, tools used for forensics should be validated to ensure reliability and correctness.
5. **Analysis.** Forensic analysis is the execution of investigative and analytical techniques to examine, analyze, and interpret the evidentiary artifacts retrieved.

6. **Repeatability and reproducibility (quality assurance).** The procedures and conclusions of forensic analysis should be repeatable and reproducible by the same or other forensic analysts [6].
7. **Reporting.** The forensic analyst must document his or her analytical procedure and conclusions for use by others.
8. **Presentation.** In most 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, focuses on carrying out the forensic process *using* a cloud environment. This involves using the cloud to perform examination and analysis of digital evidence [6]

2.2 Defining What Constitutes a Challenge for Cloud Computing Forensics

The numerous challenges for the various stakeholders who share an interest in forensic analysis of cloud computing environments can be broadly categorized into technical, legal, and organizational[5] challenges. These challenges occur when identification and acquisition tasks become impeded or when examination and interpretation by a digital forensic examiner is prevented.

Compared to the challenges of traditional digital forensics, those of cloud forensics are considered to either be unique to the cloud environment or exacerbated by the cloud environment [4]. While the goals of first responders and forensic examiners may be the same in the cloud context as in traditional, large-scale computer and network forensics, distinctive features of cloud computing—such as segregation of duties among cloud Actors, inability to acquire system and network logs, multi-tenancy, and rapid elasticity—introduce unique scenarios to digital investigations. On the other hand, challenges associated with, for example, virtualization, large-scale data processing, and the proliferation of mobile devices and other endpoints are exacerbated in the cloud.

Cloud forensic challenges cannot be solved by technological, legal, or organizational principles alone. Many of the challenges need solutions from all three areas, and scholars and practitioners have been discussing 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.

[5] Organizational challenges involve cloud Actors working together to obtain digital evidence. Cloud Actors include Consumers, Providers, Brokers, Auditors, and Carriers [4].

3 Cloud Forensic Challenges

This section discusses how the NCC FSWG collected and aggregated the challenges and provides an analysis and categorization of those challenges.

3.1 Collection and Aggregation of Forensic Science Challenges

The first step in identifying the challenges that cloud forensic examiners face was to study the existing literature and gather available data on this topic. The data was then aggregated as a collective group effort by the active participants of the NCC FSWG[6] in a meaningful way that allowed for further analysis. 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 two tables (shown in Annex A) that currently list 62 challenges, including challenge descriptions, results of overcoming the challenges, relevance of cloud computing essential characteristics [3], correlations between challenges and functional-capabilities, categories of the challenges, and relevant references in the literature.

The major objectives of these tables are to:

- 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 are encountered to a lesser degree in more traditional computing models.
- Create an ongoing dialogue among stakeholders to define potential technology- and standards-based approaches to the mitigation of forensic challenges faced in the cloud computing environment. The challenges identified in the Cloud Forensic Challenges tables (Annex A) are certainly not comprehensive and will continue to evolve. The long-term objectives are to identify technology and standards gaps related to the challenges that need to be addressed and to develop possible technological and standards approaches to mitigate those challenges.

Taken as a whole, the items identified by the Cloud Forensic Challenges tables represent many of the major challenges that arise while 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 information.

[6] These active participants represent numerous key cloud Ecosystem stakeholders, including government, industry, and academia, both domestically and internationally.

3.2 Analysis and Categorization of the Challenges

Once the forensic science challenges were collected and aggregated, a multi-dimensional analysis and categorization of these challenges were performed to identify each one's cloud-based root cause and to organize them in categories that are agnostic to cloud Providers or cloud service models.

3.2.1 Relevance of Essential Cloud Characteristics

The NCC FSWG intended to keep the challenges generic and, therefore, disregarded the myriad architectural differences among the many cloud computing family of offerings when analyzing the aggregated challenges.

Additionally, the team targeted only the digital forensic challenges unique to or exacerbated by the cloud environment. To assist in filtering out the challenges that do not have a cloud-based root cause, the team analyzed each challenge through the lens of the five *essential characteristics of the cloud computing model* as defined in The NIST Definition of Cloud Computing [3]. These characteristics are used to identify whether a challenge has a cloud-based root cause. Table 2 of Annex A captures this analysis in the third column, which identifies the characteristics most relevant to each challenge. The *essential characteristics of the cloud computing model* are reproduced below:

- **On-demand self-service:** A Consumer can automatically and unilaterally provision computing capabilities, such as server time and network storage, as needed without requiring human interaction with each cloud 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 Consumer generally has no control over or knowledge of 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 data center). Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to rapidly scale 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.

3.2.2 Correlation Between Cloud Technology and Forensic Science Challenges

To better understand the correlation between the cloud forensic science challenges and their cloud-based root cause, the NCC FSWG analyzed each challenge's relationship to the cloud functional capabilities (cloud processes or solutions) identified in the Cloud Security Alliance's (CSA's) Enterprise Architecture (EA) [9]and leveraged by the NIST Cloud Security Reference Architecture (CSRA) [10].

The CSA's EA, reproduced in Annex C, Fig. 1, covers the following domains:

a. Business Operations and Support (BOSS) – has capabilities associated with cloud IT services to support an organization's business needs.
b. Information Technology Operation & Support (ITOS) – has capabilities associated with managing the cloud IT services of an organization.
c. Security and Risk Management (S & RM) – has capabilities associated with safeguarding cloud IT assets and detecting, assessing, and monitoring cloud IT risks.

The CSA's EA also identifies the corresponding data grouping into the following service layers:

d. Presentation Services – has capabilities associated with the end user interacting with a cloud IT solution.
e. Application Services – has capabilities associated with the development and use of cloud applications provided by an organization.
f. Information Services – has capabilities associated with storage and the use of cloud information and data.
g. Infrastructure Services – has capabilities associated with core functions that support the cloud IT infrastructure, such as facilities, hardware, networks, and virtual environments.

Altogether, there are 347 functional capabilities listed within these categories.

The correlations between the forensic challenges and these functional capabilities were examined by determining the relationship between a particular forensic challenge and a particular functional capability (all possible pairs of challenges and capabilities were considered) and by labeling the challenge (as describe below) based on the functional capabilities affected.

The relationship was determined by:

1. Clarifying what it means for a *challenge to be overcome* (see Annex A, Table 1, column 5 that identifies *what would be the result if the challenge were, in fact, overcome?*) and
2. Answering the question, *If the challenge were overcome, would that make it easier to conduct a cloud forensic investigation on the considered functional capability?*[7]

Analysis of the correlation between the forensic science challenges and the functional capabilities constitutes the foundation for labeling each challenge based on the functional capabilities affected by the challenge. Each challenge is labeled along a generic-to-specific axis (see Annex A, Table 2, column 4). A challenge is labeled *generic* if it applies to most of the

[7] The results of this analysis will be presented in a future NIST publication.

capabilities. A challenge is labeled *specific* if it applies to a limited set of capabilities. A challenge is labeled *quasi* if it falls somewhere between *generic* and *specific.*

3.2.3 Categorization of Challenges

A review of the Annex A 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 data center computing. The legal and organizational issues primarily reflect the crossing of national borders and legal jurisdictions by the manner in which cloud Providers store cloud Consumer's information for operational redundancy, cost, and reliability.

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

To assist in a meaningful analysis, the challenges are 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 A. 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 A, Table 2 for the details.

- **Architecture (e.g., diversity, complexity, provenance, multi-tenancy, data segregation).** 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
- **Data collection (e.g., data integrity, data recovery, data location, imaging).** 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 of 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
- **Analysis (e.g., correlation, reconstruction, time synchronization, logs, metadata, timelines).** 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

- **Anti-forensics (e.g., obfuscation, data hiding, malware).** Anti-forensics are a set of techniques used specifically to prevent or mislead forensic analysis. Anti-forensic 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
- **Incident first responders (e.g., trustworthiness of cloud Providers, response time, reconstruction).** 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 collected forensic artifacts
- **Role management (e.g., data owners, identity management, users, access control).** 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
- **Legal (e.g., jurisdictions, laws, service level agreements, contracts, subpoenas, international cooperation, privacy, ethics)**. 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
- **Standards (e.g., standard operating procedures, interoperability, testing, validation).** 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
- **Training (e.g., forensic investigators, cloud Providers, qualification, certification).** 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

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 on 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 logically be 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 Annex A was analyzed in relationship to the other challenges and mapped into the appropriate category (and subcategory, if appropriate). These challenges (presented in black text on 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 Table 2 in Annex A, the latter challenges are identified as belonging to one or more related categories. The primary and related category information is represented in the mind maps shown in Annex C. Different node background colors were selected for primary and related categories. 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 Additional Analysis of the Challenges

The study examined challenges related to cloud computing forensics, and this section provides additional insight into the nature of these challenges.

In traditional computer forensics, the centralized nature of IT systems allows investigators to have full control over the forensic artifacts (e.g., router logs, process logs, hard disks). However, in a cloud Ecosystem, the distributed nature of IT systems dictates that control over the functional layers varies among cloud Actors depending on the cloud service model. Therefore, investigators have a lower level of visibility and control over the forensic artifacts. For example, cloud Consumers have the highest level of control over the functional stack in an Infrastructure as a Service (IaaS) model and the least level of control in a Software as a Service (SaaS) model. Because of this difference in control, evidence collection varies according to the service model [11].

Important sources of forensic analysis are 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 the lack of transparency of log data for the Consumer. Three examples of such logs are audit, security, and application logs. Audit logs are the records of interactions between services and the underlying operating system. Security logs trace users to actions by 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.

When there is a potential need for forensic artifacts at the hypervisor/virtual machine monitor (VMM) layers in cloud computing, additional complexities arise 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 different manufacturers, and each has its own event definition and logging (or lack thereof). Another level of variability and complexity is added by the fact that the quantity and quality of log data for cloud products are often configurable by the cloud Providers and/or Consumers [6]. 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 virtual platforms or cloud Providers.

To perform forensic analysis using logs with integrity on which all stakeholders can rely, the logs must be trusted [12]. Differences in log formats, decentralization of logs among different layers, lack of accessibility to logs, the multi-tenancy nature of clouds, and the need to preserve 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 because of several possible factors, including:

1) The identification of the cloud Provider and its partners, which 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 identities are used
3) The ability of the forensic examiner to gain access to the desired media

4) The ability to obtain assistance from the cloud infrastructure/application Provider service staff
5) An understanding of the topology, proprietary policies, and storage systems within the cloud.
6) The examiner's ability to complete a forensically sound image of the media once access is obtained
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 (e.g., 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 forensic investigator's ability to obtain keys for decryption
12) The storage system no longer being local
13) Often no way to link given evidence to a particular individual other than by relying on the cloud Provider's word, although there may be evidence in the client endpoint that can link the individual to evidence in the cloud [6]

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 first responders, law enforcement, and court systems while assuring cloud Providers that there will be minimal or no 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 cost of travel. In essence, this will involve electronically moving forensic images and metadata from the cloud Provider to a forensics lab. Potential approaches include a documented process for the remote, programmatic collection of evidential data like the one proposed in [6] or even performing the forensics in a scientifically sound manner in the cloud itself.

4.1 Additional Observations

During preliminary analysis, some common topics were identified 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 included here to provide additional insight into the challenges.

- **Time –** Time is frequently a critical issue as it relates to time synchronization and the possible disappearance of evidence that is not quickly found, as Zimmerman and Glavach [13] point out. Once the information source is identified, do all involved entities have the time synchronized using a consistent time source such as Network Time 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. In addition to using NTP to ensure that all server time is synced, the issue of time

zones used in timestamps must be addressed in cloud forensics. Not all systems use Coordinated Universal Time (UTC) timestamps; when recorded in local time, the time zone offset must be collected from the server. Additionally, if evidence is not found quickly enough, it may be overwritten or lost in some other manner. Some example challenges in Annex A related to time include FC-05 (Timestamp synchronization), FC-14 (Real-time investigation intelligence processes not possible), FC-30 (Data available for a limited time), and FC-53 (International cloud services).

- **Location –** Locating digital media can be a time-consuming process in cloud environment cases. Both backup and redundant storage are important, and an understanding of the topology will aid in identifying physical locations of media storage. Locating the evidence can be a big hurdle. As pointed out by Zimmerman and Glavach [13], 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. When forensic data is collected on a physical resource, the justification for collecting that data on that particular resource must be shown by showing the validity of the logical to physical mapping. This is critical since all components – computing, network and storage are virtualized in the cloud. Some example challenges in Annex A related to location include FC-17 (Multiple venues and geo-locations), FC-25 (Decreased access and data control), FC-27 (Locating evidence), FC-37 (Additional evidence collection), FC-48 (Physical data location), and FC-60 (Decoupling user credentials & physical location).
- **Sensitive data –** Sensitive data theft cases (insider, outsider, and both working together) are an important issue. According to CIO.com [14], the U.S. Commission on Intellectual Property estimates over $300 billion in annual losses to U.S. companies due to theft. The pervasive personal use of cloud computing environments by employees 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 A related to sensitive data include FC-39 (Selective data acquisition), FC-56 (Confidentiality and Personally Identifiable Information [PII]), FC-61 (Authentication and access control), and FC-07 (Use of metadata).

5 Conclusions

This document highlights many of the forensic challenges in the cloud computing environment for digital forensic examiners, cloud Providers, law enforcement, and others. The information in this document was developed as a result of examining recent research papers and involved the international community. It provides a definition of cloud computing forensics to scope this area and describes the relationship of each challenge to the five essential characteristics of cloud computing. The document also discusses how the challenges correlate to cloud technology by considering their relationship to the Cloud Security Alliance's Enterprise Architecture. The categories of challenges include architecture, data collection, analysis, anti-forensics, incident first responders, role management, legal issues, standards, and training. Finally, the results of overcoming each challenge are provided.

As pointed out in [15], 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. This was also echoed in a more recent literature survey [74], which also identified a number of cloud forensic research and operational challenges, such as the need for a forensic-by-design framework that allows integration of forensic tools into the development of cloud physical system to mitigate risks and enable forensic capabilities.

The NCC FSWG will continue its efforts and initiate more dialogue among stakeholders. The next steps include: (1) further analyzing the cloud forensic challenges, (2) prioritizing the challenges, (3) developing a Cloud Forensics Reference Architecture, (4) choosing the highest priority challenges and determining the corresponding gaps in technology and standards that need to be addressed, and (5) developing a roadmap to address these gaps.

References

[1] Hogan M, Liu F, Sokol A, Tong J (2011) NIST Cloud Computing Standards Roadmap. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 500-291. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=909024

[2] Executive Office of the President (2012), Principles for Federal Engagement in Standards Activities to Address National Priorities, January 17, 2012 https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2012/m-12-08_1.pdf

[3] Mell P, Grance T (2011) The NIST Definition of Cloud Computing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-145. https://doi.org/10.6028/NIST.SP.800-145

[4] Ruan K, Carthy J, Kechadi T, Crosbie M (2011) Cloud Forensics. 7th IFIP Advances in Digital Forensics VII, G. Peterson and S. Shenoi (eds), vol. 361, pp. 35-46.

[5] Zatyko K (2007) Commentary: Defining Digital Forensics. Forensic Magazine, January 2, 2007.

[6] Martini B, Choo KR, (2014) Remote Programmatic vCloud Forensics: A Six-Step Collection Process and a Proof of Concept. Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 24–26 September 2014.

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

[8] Liu F, Tong J, Mao J, Bohn RB, Messina JV, Badger ML, Leaf DM (2011) NIST Cloud Computing Reference Architecture (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 500-292. https://doi.org/10.6028/NIST.SP.500-292

[9] Cloud Security Alliance, Trusted Cloud Initiative, Enterprise Reference Architecture, https://downloads.cloudsecurityalliance.org/initiatives/tci/TCI_Reference_Architecture_v2.0.pdf

[10] NIST SP 500-299: Cloud Security Reference Architecture (draft 1) , renumbered to NIST SP 800-200 (draft 2): https://github.com/usnistgov/CloudSecurityArchitectureTool-CSAT/blob/master/Documents/NIST%20SP%20800-200-SRA_DRAFT_20180414.pdf

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

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

[13] Zimmerman S, Glavach D, (2011) Cyber Forensics in the Cloud. Information Assurance Technology Analysis Center (IATAC), IA newsletter, Vol 14, No 1, Winter 2011.

[14] Corbin K, (2013) 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

[15] Zatyko K, Bay J, (2012) The Digital Forensics Cyber Exchange Principle, Forensics Magazine. 81. 13-15.

[16] SWGDE Digital and Multimedia Evidence (Digital Forensics) as a Forensic Science Discipline, Version 2.0, September 5, 2014. https://drive.google.com/file/d/1OBux0n7VZQe7HSgObwAtmhz5LgwvX0oY/view

[17] SWGDE Digital and Multimedia Evidence Glossary, Version 3.0, June 23, 2016. https://drive.google.com/file/d/1ZZwOqgVOWo6qDeoJqv6VKafY2i1RJI2B/view

[18] Computer Forensics: Digital Forensic Analysis Methodology. January 2008, Volume 56, number 1, Department of Justice, USA. https://www.justice.gov/sites/default/files/usao/legacy/2008/02/04/usab5601.pdf

[19] ISO/IEC 2382-1, Information technology - Vocabulary - Part 1: Fundamental terms, 1993. https://www.iso.org/standard/7229.html

[20] Scarfone K, Souppaya M, Hoffman P (2011) Guide to Security for Full Virtualization Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-125. https://doi.org/10.6028/NIST.SP.800-125

[21] Carrier BD, (2006) Risks of live digital forensic analysis. Communications of the ACM Volume 49, No 2, , 56-61, Feb. 2006, http://doi.acm.org/10.1145/1113034.1113069.

[22] Bilby D, (2006) Low Down and Dirty: Anti-Forensic Rootkits. Fourth Annual RuxCon Conference (RuxCon 2006), Sydney, Australia.

[23] Lu R, Lin X, Liang X, Shen XS, (2010) 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), ACM, pp. 282–292.

[24] Ruan K, (2013) Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey results, Digital Investigation, March 2013.

[25] Spyridopoulos T, Katos V, (2012) Data Recovery Strategies for Cloud Environments, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2012.

[26] Fowler B, (2009) Securing a Virtual Environment, http://www.infosecwriters.com/text_resources/pdf/BFowler_VIrtual_Environment.pdf

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

[28] Grivas SG, Kumar TU, Wache H, (2010) Cloud Broker: Bringing Intelligence into the Cloud - An Event-based Approach, IEEE 3rd International Conference on Cloud Computing, pp. 544-545.

[29] 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, 2012 Lafayette, Indiana, USA.

[30] Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing, Cloud Security Alliance, Incident Management and Forensics Working Group, June 2013. https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf

[31] Ruan K, James IJ, Carthy J, Kechadi T, (2012) Key Terms for Service Level Agreement to Support Cloud Forensics, Advances in Digital Forensics VIII, Springer, pp. 201-212.

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

[33] Grispos G, Storer T, 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.

[34] Marty R, (2011) Cloud application logging for forensics, ACM Proc., Symposium on Applied Computing (SAC11), Taichung, Taiwan. ACM, pp. 178–184, March 2011.

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

[36] Ruan K, (2013) Designing a Forensic-enabling Cloud Ecosystem, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2013.

[37] Anderson J, Rainie L, (2010) The future of cloud computing, Pew Research Center, https://www.pewresearch.org/internet/2010/06/11/the-future-of-cloud-computing.

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

[39] 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 2013.

[40] Anderson R, Barton C, Bohme R, Clayton R, van Eeten JG, Levi M, Moore T, Savage S, (2012) Measuring the Cost of Cybercrime, Workshop on the Economics of Information Security (WEIS). http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

[41] EC Council (2017) Ethical Hacking and Countermeasures: Attack Phases. 2nd Edition. EC-Council Press.

[42] Lemos R, (2010) Cloud-Based Denial Of Service Attacks Looming, Researchers Say, DEFCON 2010. https://www.darkreading.com/attacks-breaches/cloud-based-denial-of-service-attacks-looming-researchers-say/d/d-id/1134121

[43] 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.

[44] Decker M, Kruse W, Long B, Kelly G, (2011) Dispelling Common Myths of "Live Digital Forensics," http://dfcb.org/wp-content/uploads/2018/05/myth-of-live-forensics.pdf

[45] 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 2013.

[46] Kortchinsky K, (2009) CLOUDBURST: A VMware Guest to Host Escape Story, BlackHat USA 2009, Las Vegas, https://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf

[47] Adams R, (2012) The Emergence of Cloud Storage and Need for a New Digital Forensic Process Model, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed., IGI Global, 2012.

[48] Chen Y, Paxson V, Katz RH, (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

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

[50] Choo KR, (2010) Cloud computing: Challenges and future directions. Trends & Issues in Crime and Criminal Justice, No 400: 1–6, Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi400

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

[52] 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 2013.

[53] Dykstra J, Sherman AT, (2013) Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform, Digital Investigation, Volume 10, Supplement, pp. S87-S95, August 2013, https://www.sciencedirect.com/science/article/pii/S174228761300056X

[54] Dykstra J, (2012) Seizing Electronic Evidence from Cloud Computing Environments, Cybercrime and Cloud Forensics: Applications for Investigation Processes, IGI Global, December 2012.

[55] Dykstra J, Riehl D, (2012) Forensic Collection of Electronic Evidence from Infrastructure-as-a-Service Cloud Computing, Richmond Journal of Law and Technology, http://jolt.richmond.edu/wordpress/?p=463 .

[56] Muniswamy-Reddy K, Macko P, Seltzer M, (2010) Provenance for the cloud. In Proceedings of the 8th USENIX conference on File and storage technologies (FAST10). USENIX Association, Berkeley, CA, USA, 15-14, 2010.

[57] 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, pp. 1–7, 2011.

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

[59] Kirsten, FB, Convery N, (2011) Storing Information in the Cloud – A Research Project. Journal of the Society of Archivists, 32:2, 221-239, https://www.tandfonline.com/doi/abs/10.1080/00379816.2011.619693

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

[61] James JI, Shosha AF, Gladyshev P, (2013) Digital Forensic Investigation and Cloud Computing, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ed. Ruan K, IGI Global, December 2013.

[62] Grobauer B, Schreck T, (2010) Towards Incident Handling in the Cloud: Challenges and Approaches, CCSW '10: Proceedings of the 2010 ACM workshop on Cloud computing security workshop October 2010, 77–86 https://doi.org/10.1145/1866835.1866850

[63] Anthes G, (2010) Security in the cloud, Communications of the ACM 53(11): 16-18, November 2010, DOI: 10.1145/1839676.1839683

[64] Creeger M, (2010) Moving to the Edge: A CTO Roundtable on Network Virtualization. Communications of the ACM, August 2010. https://doi.org/10.1145/1787234.1787251

[65] 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

[66] CIO Council & Chief Acquisition Officers Council, (2012) Creating Effective Cloud Computing Contracts for the Federal Government. https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/cloudbestpractices.pdf

[67] Cloud Security Alliance, Legal Information Center, (2013) What Rules Apply to Government Access to Data Held by US Cloud Service Providers. https://cloudsecurityalliance.org/artifacts/government-access-to-data-held-by-us-cloud-service-providers/

[68] Hooper C, Martini B, Choo KR, (2013) Cloud computing and its implications for cybercrime investigations. In: Australia, Computer Law and Security Review 29(2): 152–163.

[69] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2015-2020, February 2016. https://www.cisco.com/c/dam/m/en_in/innovation/enterprise/assets/mobile-white-paper-c11-520862.pdf.

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

[71] Ferguson-Boucher K, Endicott-Popovsky B, (2013) Forensic Readiness in the Cloud: Integrating Records Management and Digital Forensics. Cybercrime and Cloud Forensics: Applications for Investigation Processes, IGI Global, https://www.igi-global.com/chapter/forensic-readiness-cloud-frc/73960

[72] Quick Q, Martini B, Choo KR, (2014) Cloud Storage Forensics, Syngress Publishing / Elsevier.

[73] Martini B, Choo KR, (2011) An integrated conceptual digital forensic framework for cloud computing, Digital Investigation 9(2), pp. 71-80.

[74] Manral B, Somani G, Choo KR, Conti M, Gaur MS, (2020) A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions, ACM Computing Surveys 52(6): 124:1-124:38, https://doi.org/10.1145/3361216

Appendix A: Acronyms

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

API	Application Programming Interface
BNA	Broad Network Access
BOSS	Business Operation Support Services
CIO	Chief Information Officer
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
EC2	Elastic Compute Cloud
FC	Forensic Challenge
G	Generic
G8	Group of Eight
IaaS	Infrastructure as a Service
IATAC	Information Assurance Technology Analysis Center
IEEE	Institute of Electrical and Electronics Engineers
INTERPOL	International Criminal Police Organization
IP	Internet Protocol
ITL	Information Technology Laboratory
ITOS	Information Technology Operation and Support
MS	Measured Service
N/A	Not Applicable
NCC FSWG	NIST Cloud Computing Forensic Science Working Group
NCCP	NIST Cloud Computing Program
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
NTP	Network Time Protocol
NTTAA	National Technology Transfer and Advancement Act
OD	On-Demand Self-Service

OMB	Office of Management and Budget
PaaS	Platform as a Service
PII	Personally Identifiable Information
PSK	Pre-Shared Key
Q	Quasi
RAM	Random Access Memory
RE	Rapid Elasticity
RP	Resource Pooling
S	Specific
SaaS	Software as a Service
S&RM	Security and Risk Management
SOP	Standard Operating Procedure
SP	Special Publication
SPAN	Switched Port Analyzer
SRA	Security Reference Architecture
TAPS	Test Access Port
TCP	Transmission Control Protocol
US	United States
USB	Universal Serial Bus
USG	United States Government
UTC	Coordinated Universal Time
VM	Virtual Machine
VMM	Virtual Machine Monitor
WPA	Wi-Fi Protected Access

Appendix B: Glossary

Challenge	For this paper, a currently difficult or impossible task that is either unique to cloud computing or exacerbated by it
Cloud Auditor	A party that can conduct an independent assessment of cloud services, information system operations, performance, and security of the cloud implementation [8]
Cloud Broker	An entity that manages the use, performance, and delivery of cloud services and negotiates relationships between Cloud Providers and Cloud Consumers [8]
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers [8]
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 [3]
Cloud Consumer	A person or organization that maintains a business relationship with and uses service from Cloud Providers [8]
Cloud Provider	The entity (a person or an organization) responsible for making a service available to interested parties [8]
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 [16]
First responder	A person who provides a rapid initial response to any IT incident or event that may require further investigation. Examples of such events include security threats, cyber-attacks and other illegal activities.
Forensic science	The use or application of scientific knowledge to a point of law, especially as it applies to the investigation of crime [16]
Forensic examiner	A person who is an expert in acquiring, preserving, analyzing, and presenting digital evidence from computers and other digital media. This evidence may be related to computer-based and non-cyber crimes, including security threats, cyber-attacks, and other illegal activities.
Imaging	The process used to obtain a bit by bit copy of data residing on the original electronic media; allows the investigator to review a duplicate of the original evidence while preserving that evidence [18]

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 [19]
Virtualization	The simulation of the software and/or hardware upon which other software runs; this simulated environment is called a virtual machine (Adapted from [20])

Annex A: Cloud Forensic Challenges

Table 1: Cloud forensic challenges

The following table captures, in no particular order, the cloud-specific forensic challenges identified through extensive literature research.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-01	Deletion in the cloud	Recovering data deleted from the cloud (by either the Provider, Consumer, or attacker) and attributing that data to a specific user	Deletion in the cloud is often based on the deletion of nodes pointing to information in virtual instances. Pathways for retrieval of the deleted information are dependent on cloud Providers offering sufficiently sophisticated mechanisms for access. Once the data is recovered, it remains a challenge to attribute specific data items to an individual user given the fact that cloud-based storage is a shared service in a multi-tenant environment.	If this challenge were overcome, it would be easier to recover deleted data and to attribute that recovered data to a specific user.
FC-02	Recovering overwritten data	Recovery of deleted data that has been overwritten by another user in a shared virtual environment	Recovery of data marked as deleted (i.e., for which the nodes pointing to it are deleted) is difficult if the data is overwritten by another user in a shared virtual environment. Note: Data can be overwritten by the same user or another user. If the latter, attributing ownership is difficult.	If this challenge were overcome, it would be easier to recover deleted data that has been overwritten and to attribute that recovered data to a specific user.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-03	Evidence correlation	Evidence correlation across cloud Providers	Correlation of activities across multiple cloud Providers is a challenge. A primary reason is lack of interoperability.	If this challenge were overcome, the investigator could correlate evidence from different cloud Providers.
FC-04	Reconstructing virtual storage	Reconstruction of virtual storage in cloud environments from physical disk images	In some cloud environments, imaging of media has an added level of complexity that could cause damage to the original media.	If this challenge were overcome, an investigator could reconstruct virtual storage from all of the relevant physical disk images, making it easier to produce reliable forensic evidence associated with the data stored on the physical disks.
FC-05	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 since 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.	If this challenge were overcome, it would be possible to achieve timestamp synchronization across the cloud environment relevant to the investigation (as may be needed for, e.g., correlation of evidence and timeline determination).

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-06	Log format unification	Unification of log formats	Unified means of collecting and exporting log data have 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 without a standardized interface and export format. Furthermore, proprietary or unusual log formats of one party can become major roadblocks in joint investigations.	If this challenge were overcome, the investigator could unify log formats (as may be needed for, e.g., evidence correlation or log analysis).
FC-07	Use of metadata	Use of metadata	The use of metadata (as an authentication method) may be in peril since common fields (e.g., 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 concerns. Entities that maintain information in the cloud should consider the impact of the cloud on metadata, understand what metadata the cloud Provider preserves, and identify whether it can be readily accessed for e-discovery purposes. However, cloud computing can offer additional metadata that would not be available in non-cloud cases (e.g., login events to the cloud environment, versioning information, and file integrity data).	If this challenge were overcome, an investigator would have access to persistent metadata fields (as may be needed to, e.g., highlight usage patterns, establish timelines, event correlation, and point to gaps in the data and events). Note: authentication is not appropriate for this challenge.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-08	Log capture	Capture and timeline analysis of logs	Log capture is difficult in cloud environments and complicates forensic timeline analysis, review, and event correlation for DHCP log data.	If this challenge were overcome, the investigator could perform forensic timeline analysis of network logs involving dynamically assigned IP addresses.
FC-09	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.	If this challenge were overcome, there would be validated standards and specifications that support interoperable forensic techniques and tools (i.e., interoperable across different Providers). This would provide more reliable, consistent, and comprehensive forensic tools.
FC-11[8]	No single source for criminals	No single point of failure for criminals	There is no single source that would allow criminals to be caught in a straightforward manner, no one computer in a group that holds all 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, obtain compute services from a second cloud Provider, and route all of their communications through a third Provider (e.g., an email provider).	If this challenge were overcome, the investigator can link all accounts of the same user on different clouds, allowing for the ability to acquire, combine, and analyze forensic data from multiple Providers used by the user.

[8] FC-10, FC-20, and FC-57 are deleted from the final document because the Working Group considered them to be obsolete challenges at the time of publication. Subsequent work derived from this document used the initial FC numbers, so the initial numbering system has been maintained for compatibility and traceability.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-12	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 steppingstone approach to exploitation also applies to the cloud space. Forensic 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 that enable an attacker to compromise the chosen target.	If this challenge were overcome, it would be easier and faster to detect a malicious act.
FC-13	Criminals' access to low-cost computing power	The cloud offers computing power that would otherwise be unavailable to criminals with small budgets and/or limited resources	Cloud computing offers computing power that would otherwise be unavailable to criminals with small budgets and/or limited resources. 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.	If this challenge were overcome, criminals would not have easy access to cloud computing for criminal activities.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-14	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, in many cases, special legal means must be applied 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.	If this challenge were overcome, the investigator could collect real-time intelligence about evidence, allowing the ability to perform real-time forensic investigation (i.e., collect data and forensic artifacts in a real-time, rapidly changing cloud environment).

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-15	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 another guest or to 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.	If this forensic challenge were overcome, it would make forensic investigations easier by effectively tracing the movement and isolating the location of malware that has transitioned from its original infection point to other areas of the virtual environment.
FC-16	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 tenant's resources or applications.	If this challenge were overcome, it would be easier for investigators to confidently attribute all changes that originate from cloud management portal applications to a specific user, resulting in the investigator knowing when an unauthorized user has gained control, reconfigured, or deleted another tenant's resources or applications.
FC-17	Multiple venues and geolocations	Access to computer and network resources involve expanded scope and, possibly, more than one venue and geolocation	Geolocation unknowns can impact the chain of custody, finding evidence, and identifying resources that are required for access to the system.	If this challenge were overcome, knowing the location of the venues or geolocations would make it easier to find the evidence and identify resources to maintain the chain of custody.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-18	Lack of transparency	Lack of transparency triggers lack of trust and difficulties of auditing	The cloud's operational details (architecture and implementation) aren't transparent to users.	If this challenge were overcome, the cloud's operational details would become more transparent, making it easier to collect forensic evidence that is accurate, complete, traceable, auditable, and forensically sound.
FC-19	Criminals can hide in the 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.	If this challenge were overcome, cells of the criminal organizations would be discoverable, making it easier for the forensic investigator to identify forensic evidence.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-21[9]	Potential evidence segregation	Segregation of potential evidence in a multi-tenant system	Segregation of forensic data in an infrastructure shared by multiple users (i.e., multi-tenant environment) is needed. Technologies used for provisioning and deprovisioning resources are constantly being improved. It is a challenge for cloud service Providers and law enforcement agencies to segregate resources during investigations without breaching the confidentiality of other tenants who share the infrastructure.	If this challenge were overcome, it would be easier for the investigator to access forensic evidence of one tenant in a way that preserves the confidentiality/privacy of other tenants.
FC-22	Boundaries	Boundaries	Because of the elastic nature of cloud computing and the inherent complications of multi-tenant environments, system boundaries are often difficult to define.	If this challenge were overcome, it would be easier to focus the scope of the investigation within appropriate boundaries and ensure that the forensic information collected is relevant to the investigation.
FC-23	Secure provenance	Secure provenance	Provenance is a record of the history of an item. In the context of cloud computing, secure provenance refers to establishing the chronology of ownership, custody, or location of data. Establishing these characteristics in a cloud environment is challenging due to multi-tenancy and the elastic nature of the cloud.	If this challenge were overcome, it would be easier for the investigator to guarantee the ownership, custody, location, or actions taken on forensic evidence.

[9] FC-10, FC-20, and FC-57 are deleted from the final document because the Working Group considered them to be obsolete challenges at the time of publication. Subsequent work derived from this document used the initial FC numbers, so the initial numbering system has been maintained for compatibility and traceability.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-24	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 to it, and whether leakage or contamination of the data was possible. If data is stored in a cloud to which multiple users and cloud service Providers potentially have access, associating the data to the subject beyond a reasonable doubt is a challenge.	If this challenge were overcome, it would be easier for the investigator to verify who had continuous ownership and access to forensic evidence.
FC-25	Decreased access and data control	Decreased access and control of data at all levels by cloud Consumers	In every combination of cloud service and deployment models, the cloud Consumer faces the challenge of decreased access to forensic data. Decreased access to forensic data means that cloud Consumers 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 abstract data locations from Consumers to facilitate data movement and replication.	If this challenge were overcome, it would be easier for investigators who work through cloud Consumer accounts to know and obtain access to physical locations of data in these accounts.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-26	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.	If this challenge were overcome, it would be easier for investigators to obtain evidence in situations involving multiple chains of dependencies through multiple cloud systems.
FC-27	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 the results are questionable due to the lack of knowledge of all locations of data storage.	If this challenge were overcome, it would be easier to quickly locate relevant data in response to an e-discovery request.
FC-28	Data location	Data location	There are many uncertainties in dealing with transparency in the cloud and distribution boundaries for retrieval due to multiple tenants in multiple data centers.	If this challenge were overcome, data locations in multiple data centers would be discoverable, thus making it easier to retrieve that data.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-29	Imaging, isolating, and collecting data	Locating and collecting cloud-based data for forensic investigations	The mirroring of large volumes of data over multiple machines in different jurisdictions and the lack of transparent, real-time information about data locations introduce difficulties in collecting data for forensic investigations. Complicating this challenge is the fact that the cloud Application Programming Interfaces (APIs) are often the only way to access certain data and metadata, and these APIs are not always developed with forensic use in mind.	If this challenge were overcome, it would be easier to locate and collect constantly moving cloud-based data for forensic investigations.
FC-30	Data available for a limited time	Data associated with deallocated virtual machine (VM) instances may only be available for a limited time	It is difficult to identify the data 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 deallocated, investigators would not know whether evidential traces or the entire VM instance could be recovered.	If this challenge were overcome, it would be easier to collect evidential information from a deallocated VM.
FC-31	Locating storage media	Identifying storage media where artifacts, log files, and other evidence may be found	In the cloud, a computer instance may not have local persistent storage since all storage occurs through an object store held remotely.	If this challenge were overcome, it would be easier to identify remote storage media where relevant evidence may be found.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-32	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 may be exceeded. If too little is identified, exculpatory or inculpatory evidence may be missed. Commonly missed evidence include network logs from related network components. In most cloud computing environments, most of the evidence and, in particular, 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 authentication and authorization data and procedures 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.	If this challenge were overcome, it would be easier to locate all relevant forensic data in response to any forensic request.
FC-33	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.	If this challenge were overcome, it would be easier to recover deleted data and overwritten deleted data.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-34	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 changing as it is being collected. Therefore, after acquisition, it is impossible for a third party to verify that the data collected is correct because the data is no longer the same as it was 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, thereby changing its contents. Even inserting a USB key into a running suspect system will alter the system. Therefore, live data forensics usually rely on the suspect system, which [21] claims cannot be trusted. Rootkits or other malware in the suspect system can provide various anti-forensic functions, resulting in unreliable evidence [22]. Additionally, data residing in a VM is volatile since after terminating a VM, all the data may be lost. Volatile data of a VM includes all of the logs stored in that VM (e.g., SysLog, registry logs, and network logs).	If this challenge were overcome, it would be easier to establish the veracity and reliability of data collected in a volatile state from a live, running cloud computing system.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-35	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, hypervisor, or file system is used in order to accurately understand the environment.	If this challenge were overcome, it would make the collection of evidence in forensic investigations easier by enabling the investigator to fully understand (with confidence) all of the logical and physical aspects of the system.
FC-36	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 service Providers, the details of how drafts are turned into deliverable messages were unavailable, leading to an inability to prove whether or not a draft was ever sent (and, more obviously, whether it was ever transmitted or received).	If this challenge were overcome, the investigator would have access to the details of application processes, thus making it easier to obtain relevant evidence.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-37	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 since 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.	If this challenge were overcome, collecting additional evidence after initial evidence collection or in areas not immediately evident from the original crime scene would be easier to perform.
FC-38	Imaging the cloud	Imaging the cloud	Imaging all evidence in the cloud is impractical while partial imaging may have legal implications 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.	If this challenge were overcome, it would make forensic investigations easier by simplifying the process for cloud imaging while also protecting the admissibility of evidence by establishing greater confidence in the imaging process.
FC-39	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.	If this challenge were overcome, it would be easier to use selective data acquisition techniques (thus saving time and resources) to acquire relevant forensic data.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-40	Cryptographic key management	Cryptographic key management	Difficulties in identifying, maintaining, and effectively recovering keys makes it easier to lose the ability to decrypt forensic data stored in the cloud.	If this challenge were overcome, it would make forensic investigations easier by preserving cryptographic keys that are required in order to access encrypted forensic evidence.
FC-41	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.	If this challenge were overcome, forensic data would be more reliable, complete, and attributable to the correct owner due to better trust boundaries between users.
FC-42	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 can occur 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 the control of multiple parties. Thus, opportunities for faults and failures are extended in the cloud.	If this challenge were overcome, the faults and failures that contribute to the quality and integrity of evidence would decrease in the context of multiple parties, multiple computers, multiple locations, etc.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-43	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 through some other means (e.g. cryptographic hashes, hardware roots of trust, etc.).	If this challenge were overcome, the integrity and trustworthiness of forensic data would be improved in the context of multiple layers of cloud abstraction and the cumulative trustworthiness of the layers.
FC-44	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 Provider may be more concerned with restoring service than with preserving evidence. Further, the Provider may begin its own investigation into an incident without taking proper precautions to ensure the integrity of potential evidence. In more severe cases, Providers may not report or cooperate in the investigation of incidents for fear of reputational damage.	If this challenge were overcome, it would make forensic investigations easier by ensuring that cloud Providers treat a compromised cloud environment as a crime scene in order to preserve the veracity, integrity, and admissibility of essential forensic evidence.
FC-45	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 explicitly stated in the agreement.	If this challenge were overcome, it would make forensic investigations easier by clearly delineating cloud Provider responsibilities for preserving and providing timely access to relevant forensic information.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-46	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 their respective jurisdictions.	If this challenge were overcome, it would improve the ability of investigators to obtain forensic data in varying jurisdictions.
FC-47	Reliance on cloud Providers	Reliance on cloud Providers	Although data acquisition may frequently be done without assistance from the cloud Provider (e.g., with user credentials), it often relies on the cooperation of cloud Providers, typically in compliance with legal processes. However, since cooperation may be limited by the Provider's resources and number of employees, an ever-increasing number of cooperation requests becomes a problem.	If this challenge were overcome, cloud Providers would be better equipped, in terms of physical and human resources, to provide assistance to forensic investigators in forensic data collection.
FC-48	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.	If this challenge were overcome, physical data locations would be known, making it easier to specify subpoenas and collect complete evidence.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-49	Port protection	Port protection	Because of the distributed nature of the cloud computing environment, identifying and accessing the ports to scan using SPAN or TAP is a challenge.	If this challenge were overcome, it would be easier for a forensic investigator to collect network traffic, which could contain relevant forensic evidence, in real time.
FC-50	Transfer protocol	Transfer protocol	TCP/IP v6 dumps, Windows dumps, and TCP segment deciphering are important forensic tools that may be unavailable in some cloud environments.	If this challenge were overcome, it would be easier for a forensic investigator to have access to dumps of TCP/IP network traffic, which could contain relevant forensic artifacts.
FC-51	e-discovery	e-discovery	The location of data in cloud environments is often uncertain. Therefore, completing e-discovery requests within a reasonable timeframe, as well as assuring that the requests have been completed, is often a challenge.	If this challenge were overcome, completion of the e-discovery request in a reasonable time frame would be assured.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-52	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.	If this challenge were overcome, it would be easier for the investigator to access and exchange data across international boundaries.
FC-53	International cloud services	Lack of definition of the scope for acquiring data that is stored on a cloud service in a different country from that of the investigator	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 of the scope of the acquisition of data in a foreign country via remote connections depends on the laws and regulations of the host country. This challenge limits the investigator's ability to begin a live analysis of the suspect system. Requiring a formal international request to access data from another country may result in significant delays.	If this challenge were overcome, it would be easier and more straightforward for investigators to obtain live, real-time data on international cloud services.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-54	Jurisdiction	Jurisdiction	Many cloud systems operate in multiple countries and regions, and each jurisdiction has specific legal frameworks governing the release, protection, and acceptable use of data. While various international bodies have attempted to adopt treaties for law enforcement to collect and exchange forensic data, there is no universal agreement between countries that addresses jurisdictional issues when cloud data is stored in multiple countries.	If this challenge were overcome, there would be mechanisms in place that provide agreements between jurisdictions, thereby empowering investigators and law enforcement officers to obtain necessary data pertaining to their investigations.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-55	International communication	International communication	Cloud computing blurs physical, policy, and jurisdictional boundaries. 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. Often, law enforcement prefers faster, informal channels to begin an international investigation rather than traversing such networks.	If this challenge were overcome, investigators would achieve timely and effective communication and cooperation at an international level.
FC-56	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 mechanisms facilitating evidence retrieval involving confidential data.	If this challenge were overcome, access to confidential data pertaining to investigations would be available to investigators while also maintaining the privacy and confidentiality of all other tenants and businesses.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-58[10]	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 the use of unique identities may inhibit the ability to positively identify a subject.	If this challenge were overcome, the investigator could link all of an individual's accounts and positively identify the person as the owner of the account.
FC-59	Fictitious identities	Criminals can create entire fictitious identities online to link to their cloud accounts, creating excess noise' for the forensic investigator to analyze	Most cloud Providers will require a name, address, and credit card to register an account. A criminal can trivially obtain credit card numbers and 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.	If this challenge were overcome, the investigator could link all of the accounts of an individual and positively identify the real person - the owner of the account.

[10] FC-10, FC-20, and FC-57 are deleted from the final document because the Working Group considered them to be obsolete challenges at the time of publication. Subsequent work derived from this document used the initial FC numbers, so the initial numbering system has been maintained for compatibility and traceability.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-60	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 to a physical entity in order to prove the physical ownership of the data attributed to the cloud username.	If the challenge were overcome, coupling of the cloud username and credentials to the physical person using the account would be resolved. In this way, the forensic investigator could verify the physical person using the username and the credentials.
FC-61	Authentication and access control	Authentication and access control	Access control in cloud environments is somewhat difficult and may not meet data protection regulations.	If this challenge were overcome, it would be easier to implement data protection regulations that allow forensic investigators to determine whether the account was used by authorized or unauthorized entities.
FC-62	Testability, validation, and scientific principles not standardized	Testability, validation, and scientific principles for cloud forensics tools have not been standardized across the industry	While various countries and standards bodies have attempted to create standards for computer-based forensic tools, test and validation processes for cloud forensic hardware, software, policies, and techniques have not been standardized. This lack of standardization brings into question the reliability and forensic soundness of the evidence acquired by these tools.	If this challenge were overcome, there would be more forensic techniques, tools, and methods validated for accuracy and repeatability. The result would be accurate and repeatable forensic methods that could be used by the investigator.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-63	Lack of standard processes & models	Lack of standard processes and models	There is no single process for digital forensics. Although various process models have been proposed, there is no single accepted standard, and the majority of organizations are creating their own SOPs, which may or may not be based on an existing process model.	If this challenge were overcome, there would be more validated standard procedures and best practices, and it would be easier to perform sound forensic investigations that can be defended in courts.
FC-64	Limited knowledge of logs and records	Custodians and individuals responsible for record keeping in cloud Provider companies might have limited knowledge of which logs and records might be sought after as evidence	Unlike a traditional computing environment to which the forensic 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 the testimony of representatives of the Provider. In many cases, these individuals are custodians of the records but do not have detailed knowledge of technologies or actual records that might be found if sought after. Indeed, companies benefit from not keeping such records or having custodians with only limited knowledge.	If this challenge were overcome, custodians in cloud Provider companies would have adequate knowledge about forensically meaningful data (logs and records) in their cloud systems and the relevance of such data to forensic investigations, thus making it easier to aggregate all forensic artifacts pertaining to an investigation.

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-65	Cloud training for investigators	Lack of training materials that educate investigators on cloud computing technology and cloud forensic operating policies and procedures	Most digital forensic training materials are outdated and not applicable to cloud environments. The lack of knowledge about cloud technology may interfere with remote investigations where systems are not physically accessible and where 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, few standard operating policies are in place for cloud forensics, which makes the nature of the approach more trial and error than scientific.	If the challenge were overcome, forensic investigators would have better training and the necessary cloud training materials to make their investigations easier and more sound.

Table 2: Categorization of cloud forensic challenges

Legend:

Cloud Essential Characteristics:	**Challenge/Functional-Capabilities Correlation:**
OD = On-demand self-service BNA = Broad network access RP = Resource pooling RE = Rapid elasticity MS = Measured service	S = Specific Q = Quasi G = Generic

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-01	Deletion in the cloud	RP/MS	S (specific to capabilities where stored data needs to be both recovered and attributed to a user; also deals with a narrow aspect of forensics, namely deletion and attribution)	Architecture	Data Collection (Data Recovery)	[23]
FC-02	Recovering overwritten data	OD/BNA/RP/RE	S (specific to capabilities where stored data needs to be both recovered and attributed to a user; also deals with a narrow aspect of forensics, namely deletion and attribution)	Architecture	Data Collection (Data Recovery)	[24], [4], [25], [26]
FC-03	Evidence correlation	RE	S (specific to when evidence correlation across multiple Providers is involved)	Analysis	N/A	[24], [4], [27], [28]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-04	Reconstructing virtual storage	OD/RP/RE	Q (can apply to many but not most or all capabilities)	Analysis	Incident First Responders (Reconstruction)	[4], [29], [25]
FC-05	Timestamp synchronization	RP/RE/MS	S (only applies when multiple time sources are involved)	Analysis (Metadata Logs)	N/A	[24], [4], [30], [31], [32], [33]
FC-06	Log format unification	RP/RE/MS	Q (applies when logs are involved, which is for many capabilities but not all or most)	Analysis (Metadata Logs)	N/A	[24], [4], [31], [28], [34]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-07	Use of metadata	OD/BNA/RP/RE/MS	Q (applies only where metadata are involved and the persistence thereof is an issue)	Analysis (Metadata)	N/A	[27], [35]
FC-08	Log capture	OD/BNA/RP/RE/MS	S (only applies to network logs involving dynamically assigned IP addresses)	Analysis (Metadata)	N/A	[24], [4], [34]
FC-09	Interoperability issues among Providers	RE	G (applies to most capabilities)	Architecture	Standards (Interoperability)	[24], [4], [29], [36], [37], [38]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-11	No single source for criminals	OD/BNA/RP/RE	S (only applies when multiple clouds are involved)	Architecture	Data Collection	[39], [40]
FC-12	Detection of the malicious act	OD/BNA/RP/RE	Q (applicability is limited to capabilities that may be vulnerable to steppingstone attacks)	Architecture	N/A	[39], [41], [15]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-13	Criminals access to low cost computing power	OD/BNA/RP/RE/MS	G	Architecture	N/A	[39], [42]
FC-14	Real-time investigation intelligence processes not possible	OD/BNA/RP/RE	S (only applies when real-time forensics are employed)	Architecture	N/A	[24], [4], [29], [31], [36], [43], [44]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-15	Malicious code may circumvent VM isolation methods	RP	S (applies only to hypervisor or guest-to-guest attacks)	Architecture	Anti-Forensics	[4], [29], [45], [25], [26], [46]
FC-16	Errors in cloud management portal configurations	RP/MS	S (applies only to hypervisor management portal attacks)	Architecture (Multi-Tenancy)	Role Management (Identity Management)	
FC-17	Multiple venues and geolocations	BNA/RP/RE/MS	G (forensics on most capabilities involves clouds with multiple geolocations)	Architecture	Data Collection	[24], [4], [29], [30], [31], [36], [32], [47], [15]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-18	Lack of transparency	OD/RP/RE/MS	G (applies to most capabilities)	Architecture	Data Collection	[24], [4], [29], [31], [43], [48], [49]
FC-19	Criminals can hide in cloud	OD/BNA/RP/RE	G (applies the same way to most capabilities regardless of the nature of the capability; however, it only applies when the attack is by a cell-based criminal organization)	Architecture	Legal (Contract / SLA) Role Management (Identity Management)	[39]
FC-21	Potential evidence segregation	OD/RP/RE	G (applies the same way to most capabilities regardless of the nature of the capability)	Architecture (Data Segregation) (Multi-Tenancy)	Data Collection	[24], [4], [29], [36], [43], [50], [51]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-22	Boundaries	OD/BNA/RP/RE	G (applies the same way to most capabilities regardless of the nature of the capability)	Architecture (Multi-Tenancy)	Data Collection	[48]
FC-23	Secure provenance	OD/BNA/RP/RE	G (applies the same way to most capabilities regardless of the nature of the capability)	Architecture (Provenance)	N/A	[23]
FC-24	Data chain of custody	OD/BNA/RP/RE /MS	G (applies the same way to most capabilities regardless of the nature of the capability)	Architecture (Provenance)	N/A	[24], [4], [29], [31], [36], [32], [52], [43]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-25	Decreased access and data control	OD/BNA/RP/RE/MS	G (applies to most capabilities)	Data Collection	N/A	[24], [4], [31], [50], [53]
FC-26	Chain of dependencies	OD/BNA/RP/RE/MS	Q (applies only to capabilities that could be spread across multiple Providers, usually involving applications [e.g., Netflix or Facebook])	Data Collection	N/A	[24], [4], [31]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-27	Locating evidence	OD/BNA/RE/RP/MS	S (deals with e-discovery)	Data Collection	N/A	[24], [4], [29], [31], [32], [54], [27], [48], [44], [55]
FC-28	Data location	OD/RP/RE/MS	G (applies in much the same way regardless of the nature of the capability being investigated)	Data Collection	N/A	[24], [4], [29], [30], [31], [32], [47], [45], [54], [52], [27], [25], [43], [55]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-29	Imaging, isolating, and collecting data	OD/BNA/RP/RE/MS	G (deals with any data in files and databases when system incorporates mirroring)	Data Collection	N/A	[24], [4], [56]
FC-30	Data available for a limited time	OD/BNA/RP/RE/MS	S (deals specifically with deallocated VMs and recovery of information from them)	Data Collection	N/A	[25], [57], [6]
FC-31	Locating storage media	OD/BNA/RP/RE/MS	Q (deals with remote storage media, which applies to many capabilities)	Data Collection	N/A	[24], [4], [29], [32], [47], [54], [52], [27], [25]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-32	Evidence identification	OD/BNA/RP/RE/MS	G (identifying evidence applicable everywhere)	Data Collection	N/A	[32], [50], [58], [6]
FC-33	Dynamic storage	OD/BNA/RP/RE/MS	S (refers specifically to recovering deleted data)	Data Collection	N/A	[48], [59]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-34	Live forensics	OD/BNA/RP/RE/MS	S (deals specifically with volatile data and live forensics)	Data Collection	Architecture	[24], [4], [29], [31], [36], [43], [44], [60]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-35	Resource abstraction	OD/BNA/RP/RE/MS	G (the need to know information about the cloud system to do forensics applies generically)	Data Collection	Architecture	[49], [6]
FC-36	Application details are unavailable	MS	S (limited to applications)	Data Collection	Architecture	[32]
FC-37	Additional evidence collection	OD/RP/RE/MS	G (also same issue in non-cloud)	Data Collection	Architecture	[32], [49]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-38	Imaging the cloud	OD/BNA/RP/RE/MS	Q (applies to imaging, which is not general but can be more broad than specific)	Data Collection	Architecture	[24], [4], [30], [45], [25], [50], [60]
FC-39	Selective data acquisition	OD/BNA/RP/RE/MS	G (could apply to almost any capability)	Data Collection	Incident First Responders	[61], [62]
FC-40	Cryptographic key management	OD/BNA/RP/RE/MS	S	Data Collection	Legal (Privacy)	[24], [4], [29], [31], [43], [63]
FC-41	Ambiguous trust boundaries	OD/BNA/RP/RE/MS	G (many ways that boundary of trust can be ambiguous)	Data Collection (Data Integrity)	N/A	[25], [64], [60]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-42	Data integrity and evidence preservation	OD/BNA/RP/RE/MS	G (this can apply to nearly any capability with very few exceptions)	Data Collection (Data Integrity)	Architecture	[32], [11]
FC-43	Root of trust	OD/BNA/RP/RE/MS	Q (only applies to capabilities that are affected by this abstraction)	Data Collection (Data Integrity)	Legal	[62], [48], [64], [60]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-44	Competence and trustworthiness	OD/BNA/RE	G (could apply to almost any capability)	Incident First Responders	Legal (Contract / SLA)	[62], [48], [64], [65], [50], [60]
FC-45	Missing terms in contract or SLA	OD/BNA/RP/RE /MS	Q (applicable only to capabilities where forensic data can be provided by Provider)	Legal (Contract / SLA)	N/A	[24], [4], [31], [66]
FC-46	Limited investigative power	OD/BNA/RP/RE	Q (only applicable where jurisdiction is an issue; when it is an issue, this is generic)	Legal	N/A	[24], [4], [54], [55]
FC-47	Reliance on cloud Providers	RP/RE/MS	G (could apply to almost any capability)	Legal	N/A	[24], [4], [29], [30], [54], [52], [62], [53]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-48	Physical data location	RE	S (only applies where physical location is relevant and subpoenas are involved)	Legal	N/A	[24], [4], [29], [31], [47]
FC-49	Port protection	BNA/RP/RE/MS	S (very specific)	Legal	Data Collection	

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-50	Transfer protocol	BNA/MS	S (same as FC49)	Legal	Data Collection	
FC-51	e-discovery	OD/BNA/RP/RE/MS	S (applies to e-discovery only)	Legal	Data Collection	[24], [4], [27], [55]
FC-52	Lack of international agreements & laws	OD/BNA/RP/RE/MS	Q (applicable only when international boundaries are an issue but generic otherwise)	Legal (Jurisdiction)	N/A	[24], [4], [36], [52], [67]
FC-53	International cloud services	BNA/RP/RE/MS	S (only applies for live, real-time data across international boundaries)	Legal (Jurisdiction)	N/A	[62]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-54	Jurisdiction	RP	Q (only applies when jurisdiction is an issue, and then it is generic)	Legal (Jurisdiction)	N/A	[24], [4], [29], [30], [31], [36], [32], [47], [54], [52], [43], [61], [55], [68]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-55	International communication	OD/BNA/RP/RE/MS	Q (applicable only when international boundaries are an issue but generic otherwise)	Legal (Jurisdiction)	N/A	[24], [4], [29], [31], [32], [47], [52], [61], [69]
FC-56	Confidentiality and PII	RP/MS	S (limited to PII, confidential, or sensitive data)	Legal (Privacy)	N/A	[36], [52], [70]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-58	Identifying account owner	OD/BNA/RP/RE/MS	S (applicable only to capabilities which are concerned with account ownership)	Role Management (Identity Management)	N/A	[24], [4], [31], [43]
FC-59	Fictitious identities	OD/BNA	S (applicable only to capabilities which are concerned with account ownership)	Role Management (Identity Management)	N/A	
FC-60	Decoupling user credentials & physical location	BNA	S (applicable only to capabilities which are concerned with account ownership)	Role Management (Identity Management)	N/A	[25]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-61	Authentication and access control	RP	S (applicable only to capabilities which are concerned with data classification and access control)	Role Management (Identity Management)	N/A	[24], [4], [29], [31], [43], [48]
FC-62	Testability, validation, and scientific principles not standardized	OD/BNA/RP/RE/MS	G (applies to most capabilities)	Standards	N/A	
FC-63	Lack of standard processes & models	OD/BNA/RP/RE/MS	G (applies to most capabilities)	Standards (No Single Process)	N/A	[24], [4], [36], [47], [43], [61]

FC ID	Short Title	Relevance of Essential Cloud Characteristics	Labeling of Challenge/Functional-Capabilities Correlation	Primary Category (Subcategory)	Related Category (Subcategory)	References
FC-64	Limited knowledge of logs and records	MS	Q (applies to many capabilities but not all or most [e.g., not as much applicability to BOSS])	Training	N/A	[71]
FC-65	Cloud training for investigators	OD/BNA/RP/RE/MS	G (applies to most capabilities)	Training (Qualification and Certification)	Standards (No Single Process)	[24], [4], [31], [32]

Annex B: CSA's Enterprise Architecture (TCI v2.0)

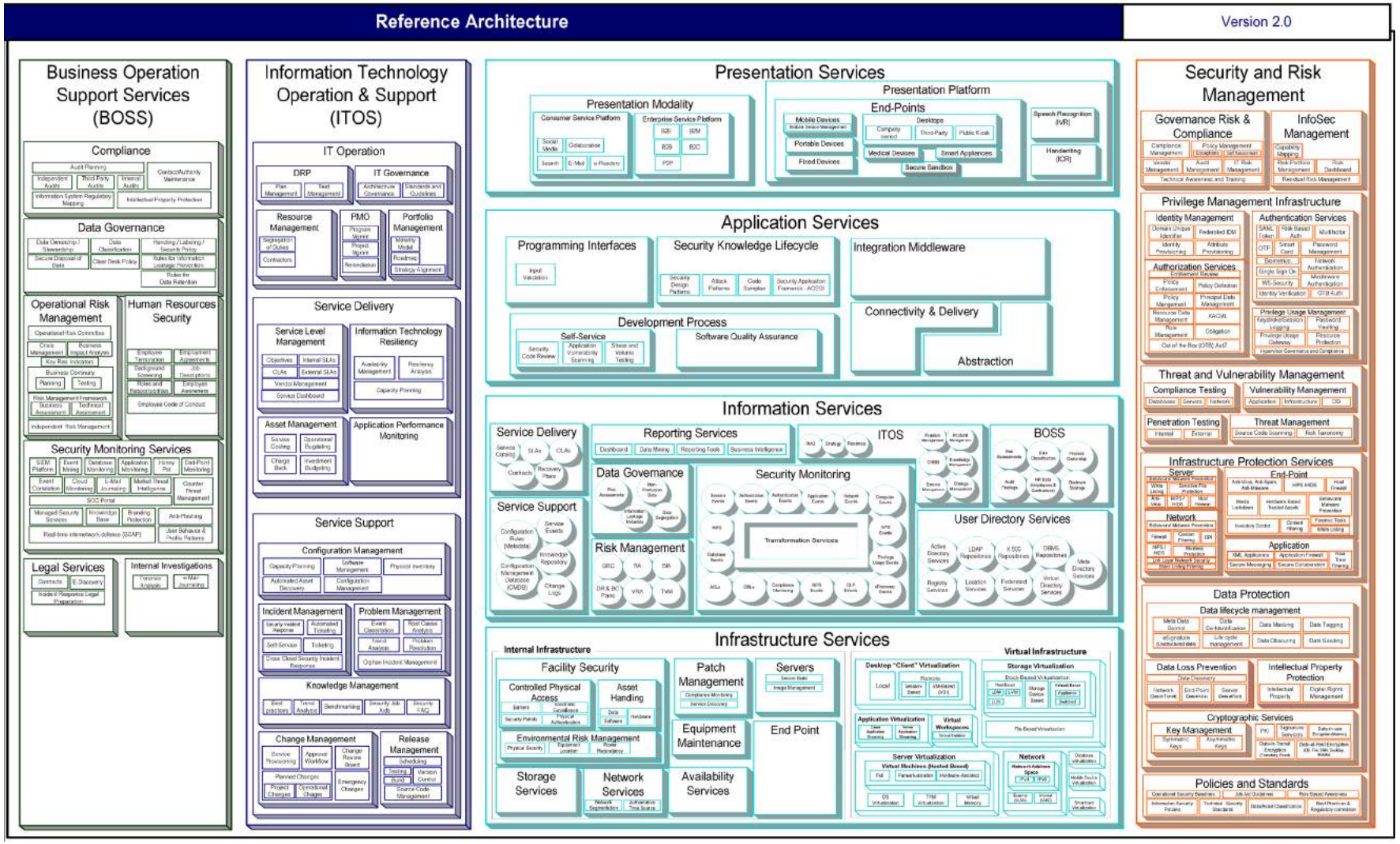

Figure 1: CSA's Enterprise Architecture

Annex C: Mind Maps

Annex C.1: Categories and Subcategories

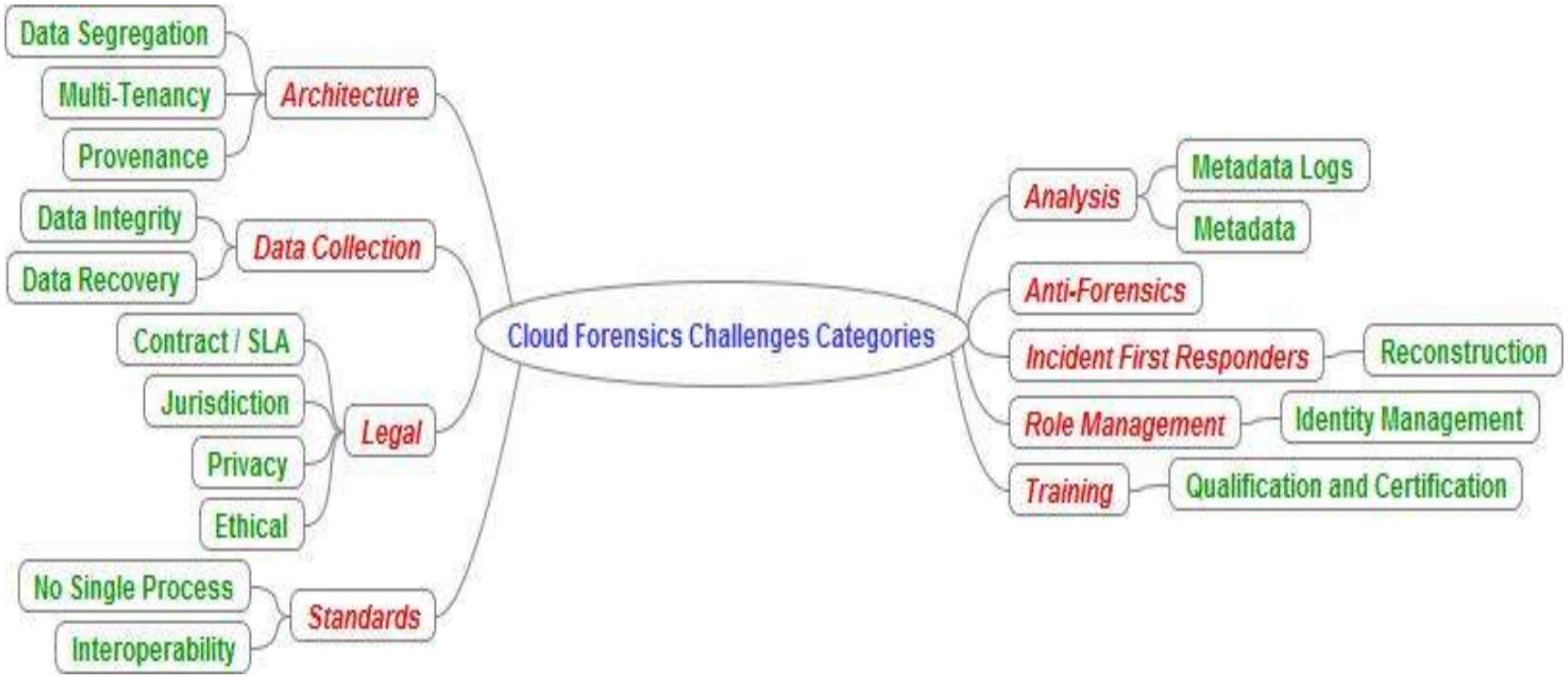

Figure 2: Mind Map – Categories and Subcategories

Annex C.2: Primary Categories

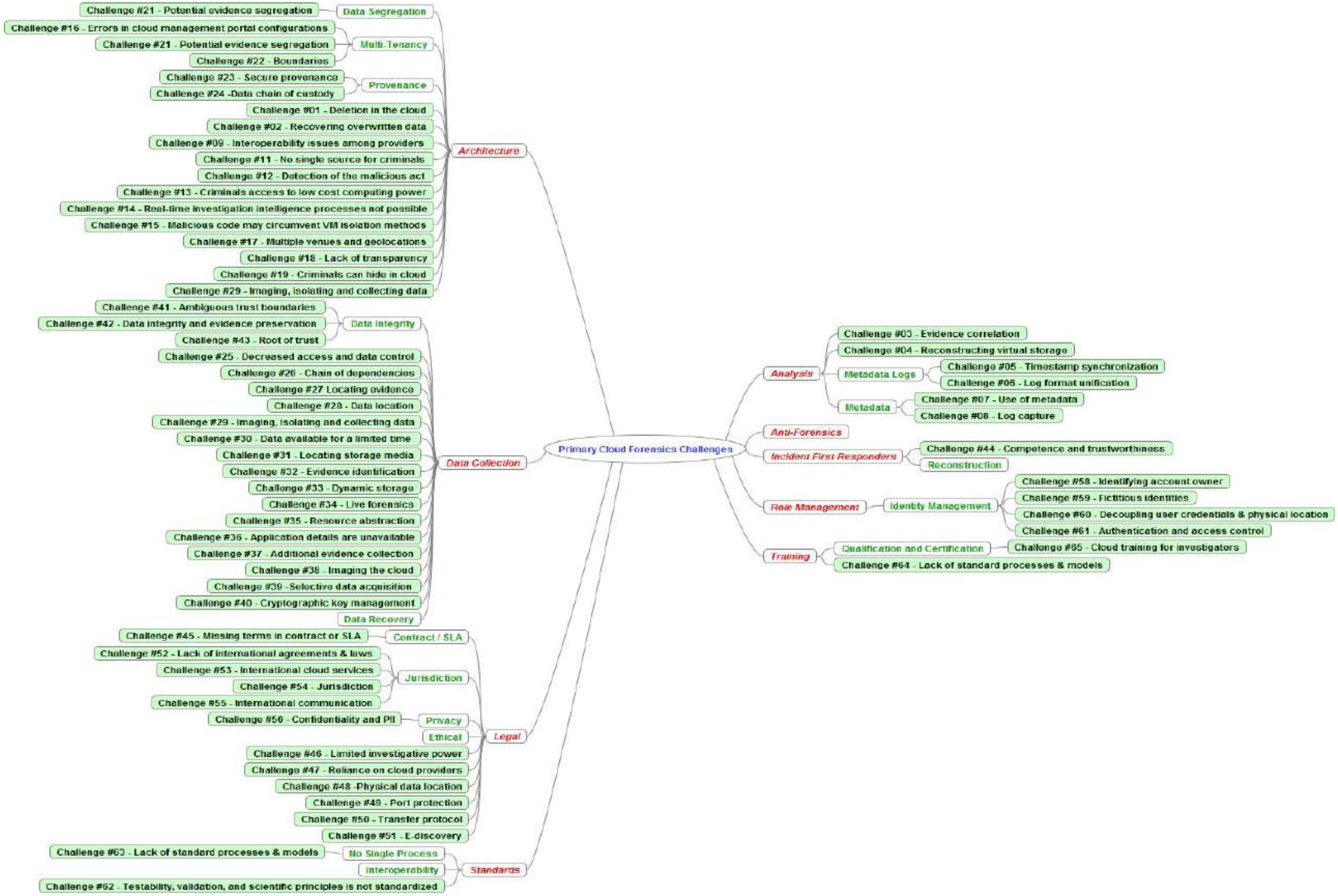

Figure 3: Mind Map – Primary Categories

Annex C.3: Related Categories

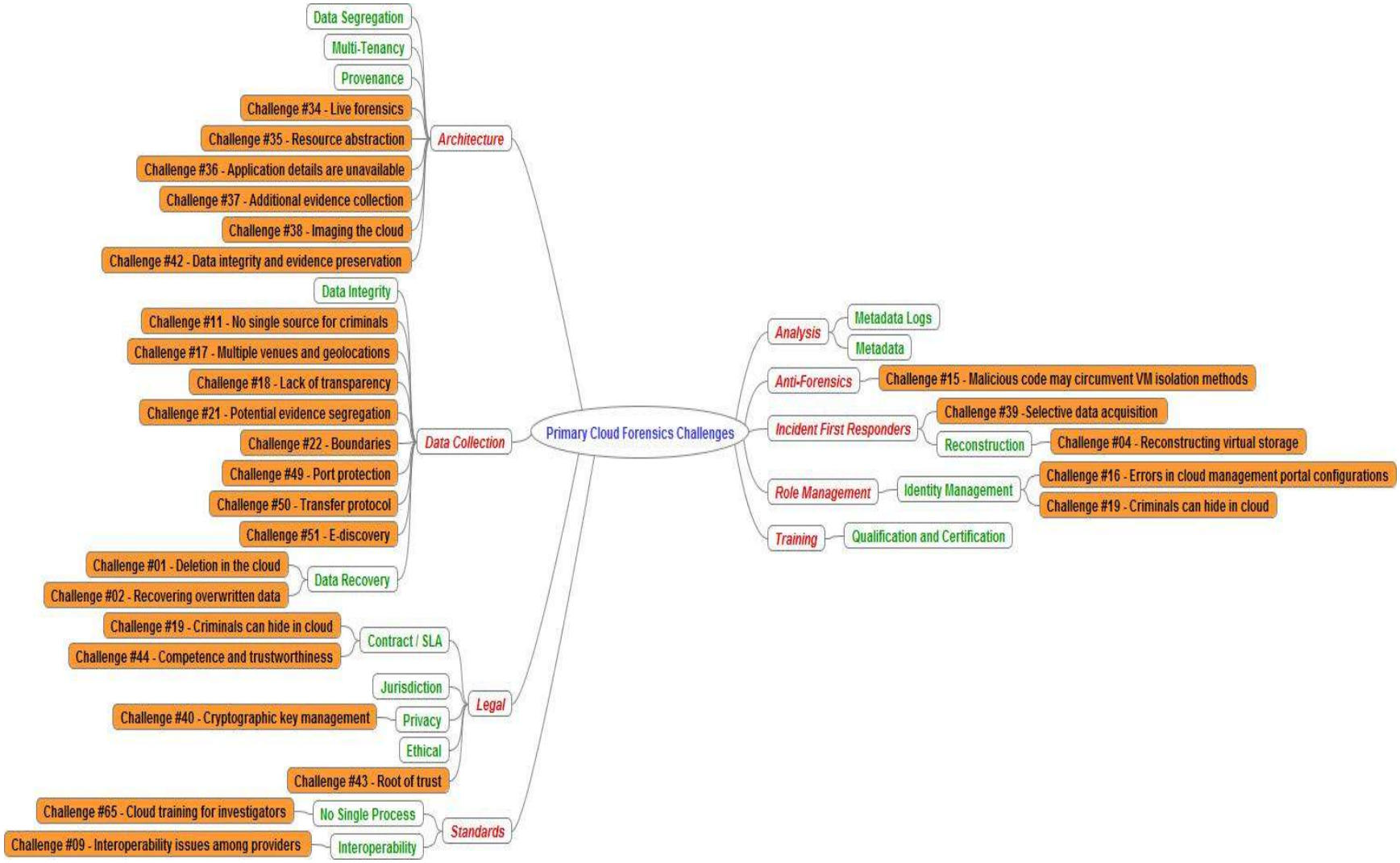

Figure 4: Mind Map – Related Categories