symmetry

MDPI

Article

Scenario-Based Digital Forensics Challenges in Cloud Computing

Erik Miranda Lopez, Seo Yeon Moon and Jong Hyuk Park *

Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 139-743, Korea; erik.miranda@seoultech.ac.kr (E.M.L.); moon.sy0621@seoultech.ac.kr (S.Y.M.)
* Correspondence: jhpark1@seoultech.ac.kr; Tel.: +82-2-970-6702

Academic Editor: Young-Sik Jeong
Received: 13 August 2016; Accepted: 8 October 2016; Published: 20 October 2016

Abstract: The aim of digital forensics is to extract information to answer the 5Ws (Why, When, Where, What, and Who) from the data extracted from the evidence. In order to achieve this, most digital forensic processes assume absolute control of digital evidence. However, in a cloud environment forensic investigation, this is not always possible. Additionally, the unique characteristics of cloud computing create new technical, legal and architectural challenges when conducting a forensic investigation. We propose a hypothetical scenario to uncover and explain the challenges forensic practitioners face during cloud investigations. Additionally, we also provide solutions to address the challenges. Our hypothetical case scenario has shown that, in the long run, better live forensic tools, development of new methods tailored for cloud investigations and new procedures and standards are indeed needed. Furthermore, we have come to the conclusion that forensic investigations biggest challenge is not technical but legal.

Keywords: digital forensics; cloud computing; cloud forensics; challenges

1. Introduction

More and more organisations and individuals are relaying on cloud computing to host their services, applications and data. This proliferation of cloud computing has brought many challenges to forensic investigators as they rarely have physical access to the underlying infrastructure.

The amount of data these cloud providers have from their clients is a very desirable objective for criminals. Additionally, cyber-crooks can use cloud computing as a platform to distribute malware, conduct scams and perform other criminal activity. Thus, investigating cloud related crimes is an arduous but essential task in order to bring criminals to justice.

Law enforcement agencies and private forensic investigators have been demanding solutions to collect data from cloud computing providers. The aim is to be able to conduct forensic investigations in the huge amounts of data that can be found on such platforms. However, many challenges still need to be overcome. This paper will explore the challenges a forensic practitioner might face with a hypothetical case-study scenario.

Our contributions in this paper include:

- Summary of ISO/IEC 27000-series.
- Survey of recent literature in the topic.
- Description of the challenges with a hypothetical scenario.
- Classification of the challenges in technical, legal and architectural issues.
- Solutions for the challenges investigators face.

2. Background

This section focuses on digital forensics and its concepts. The first section defines digital forensics and its applications. Secondly, we present the different types of digital forensic investigations. Then, we explore some of the information security standards, specifically ISO/IEC 27000-series, published by ISO. Assurance for methods, analysis and interpretation of evidence and lastly investigation principles and process are covered.

2.1. Digital Forensics

Digital Forensics (DF), as defined by McKemmish [1], is the "process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable". US-CERT [2] provides a longer and more complete definition: "The discipline that combines elements of law and computer science to collect and analyse data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law". Similar definitions exist but mainly use the same set of keywords. Hence, we can define digital forensics as the discipline that collects, preserves and analyses data in a way that is admissible in court as evidence.

The aim of a forensic investigation is to identify and preserve the evidence, extract the information, document every process, and analyse the extracted information to find answers with respect to the 5Ws (Why, When, Where, What, and Who) [3].

Forensic computing investigation takes place after an incident has occurred and it can assist in a wide range of cases:

- Criminal Damage cases include damage of another's belongings and threats to destroy property [4].
- Industrial Espionage includes patents, inventions and trade secret theft, which is a highly profitable crime.
- Financial Investigations are usually related to economic matters like money laundering and credit card or insurance fraud.
- Corporate Policy Violation includes email abuse, misconduct and employment termination investigations.
- Child Abuse cases are criminal offences such as child grooming and possession of indecent child media content.
- "Defence-in-depth" is an approach to network security. The ability of performing forensic investigations can enhance the overall integrity and survivability of a business infrastructure [2].

As we saw in the last example, digital forensics is not a discipline limited to law enforcement agencies. More and more private organisations are including forensic departments in their teams with the aim of increasing their infrastructure overall security. However, if practiced incorrectly, digital forensics analysis may destroy vital evidence that will automatically be inadmissible in a court of law [2]. Furthermore, the organisation might be liable for such loss of data depending on the legislation. Therefore, it is most important to follow correct methodologies and procedures. We will explore how to deal with such issues shortly on this second section.

2.2. Forensic Investigation Types

There is no one solution for all problems in forensic investigations; therefore, multiple specialisations within computer forensics have arisen. Different specialities focus on specific computing topics: network forensics deals with investigations in network infrastructures; and e-mail forensics, as the name states, investigates e-mail related cases; mobile forensics specialises in handset devices. Figure 1, which is based on Sridhar's [5] research, includes some of the main digital forensics specialities:

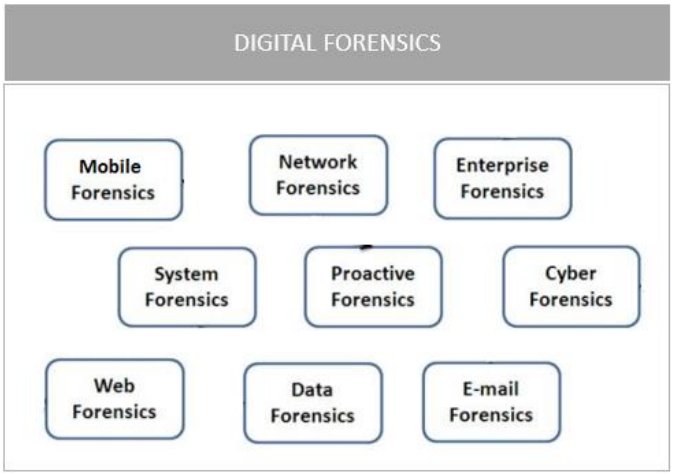

Figure 1. Types of Forensics.

As said earlier, cloud computing makes uses of many different technologies to provide services. This heterogeneity in cloud computing means an investigation in such environment needs to make use of many different forensic investigation types. The application of diverse forensic specialities adds further complexity to an already difficult discipline.

2.3. Challenges

A wide range of challenges in DF exist, from a legal and administrative point of view: lack of standards, lack of international cooperation and "law lag"; and, from the technical side, encryption, anti-forensic tools, data volume and new technologies to mention a few [1]. We will briefly discuss some of them:

- Legal and Administrative Issues

The so-called "law lag" is one of the main legal challenges digital forensics is facing. Laws are always behind technology, as lawmakers fail to keep up with new advancements. Additionally, the difficulty and lengthy process of creating new laws does not help much. The absence of international cooperation, privacy concerns and the need of search warrants are just a few more examples investigators need to deal with. Furthermore, digital forensics is a relatively new discipline thus there is little consistency between industry and courts of law [2], which has led to a lack of standardised processes, training and tools.

Some work is being pushed to deal with legal issues. For example, the European Union is pushing to harmonise evidential standards by the creation of a European Forensic Science Area in order to reduce cross-border problems [6]. Parallel work is being carried out by the International Organization for Standardization with the ISO/IEC 27000, which covers Information Security Management System standards [7]. We will go through some of the most relevant standards within ISO/IEC 27000-series later on.

- Technical Issues

From a technical point of view, encryption, steganography and anti-forensic tools such as "The Onion Router" [8] and "Slacker" [9] add extra complexity to investigations. Forensic professionals also need to keep up with new advancements and technology trends. For example, they are expected to conduct investigations on mobile phones, tablets, network devices and computers, plus deal with different operating systems, software and file systems. Nonetheless, according to most forensic practitioners, the biggest issue they need to deal with is the enormous amount of data they need to examine [10]. Additionally, when dealing with digital evidence, almost every action can modify the

evidence or leave digital traces that may have legal significance. Hence, forensic examinations need to be undertaken by highly qualified staff [1].

2.4. Investigation Activities

According to ISO/IEC 27037 and 27042, there are seven main activities in a forensic investigation [10,11]. The first two activities focus on readiness, before an incident happens; the rest are carried out after the incident happens. Figure 2 was extracted from ISO/IEC 27041 [12] and represents the activities before and after an incident has been identified.

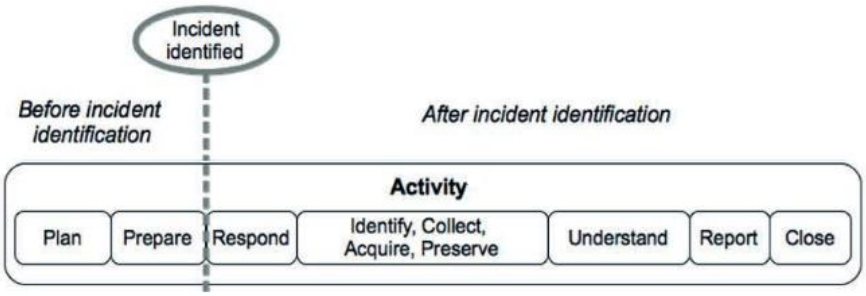

Figure 2. Investigation activities from ISO/IEC 27041 [13].

- *Plan*: A scenario-based planning approach tailored to the investigators needs is recommended. The idea is to plan scenarios that investigators might face.
- *Prepare*: Forensic practitioners should put all essential services in place in order to support future cases. This includes preparing tools, techniques and safeguards.
- *Respond*: This is when the incident has happened and the forensic practitioners start determining the scope of the event like what the situation is, the nature of the case and its details. This step is important because helps determining the characteristics of the incident and defining the best approach to carry out the investigation.
- *Identify*: Here is where the investigators start gathering information about the specific event or incident. Notes describing the systems to be analysed, their network position and general configurations may be taken at this stage.
- *Collect*: This third step, after the incident has been identified, aims to maximise the collection of evidence as well as minimising the impact to the victim. Recording of the scene is also included on this step.
- *Acquire*: The most important task here is to maintain the integrity of the evidence and provide assurance that the evidence has not been changed. This is carried out by maintaining a chain of custody of all evidence, ensuring that they have been collected and protected by legally acceptable processes.
- *Preserve*: Isolation, securing and preservation of the original evidence is comprised in this step. The main aim is to prevent any cross-contamination.
- *Understand*: In this step, investigators need to determine the significance of reconstructed data and draw conclusions.
- *Report*: Here a summary, explanation of findings and conclusions are reported. The reports should be written such that they are legally admissible. In addition, a 3rd forensic investigation team should reach the same conclusions following the investigation steps in the report.
- *Close*: In the last step, practitioners need to ensure evidence is returned to rightful owner or securely stored if needed.

2.5. ISO/IEC Standards

The International Organization for Standardization (ISO) is an independent, non-governmental international organisation responsible for creating international standards by bringing together experts who share their knowledge and develop specifications for products, services and systems [13]. The main objectives of standards are to make things work, support innovation, provide solutions and facilitate international trade [13].

In this section, we explore some of the information security standards, specifically ISO/IEC 27000-series, published by ISO. Table 1 shows the ISO/IEC 27000-series.

Table 1. ISO/IEC 27000-series.

Standard	Description	Activity
27037 [11]	Guidelines for identification, collection and/or acquisition and preservation of digital evidence	*Respond*, *Identify*, *Collect*, *Acquire*, *Preserve*
27038 [14]	Specification for digital redaction	*Report*, *Close*
27040 [15]	Storage security	*Collect*, *Preserve*, *Close*
27041 [12]	Guidance on assuring suitability and adequacy of investigation methods	*All activities*
27042 [16]	Guidelines for the analysis and interpretation of digital evidence	*Understand*, *Report*, *Close*
27043 [17]	Investigation principles and processes	*All activities*

ISO/IEC 27037 provides guidelines for those involved in the early stages of investigations. The main aim is to ensure that sufficient potential evidence is identified and collected as well as it is preserved appropriately.

ISO/IEC 27038 describes the process of redaction. Redaction refers to the action of removing or modifying information that is not to be disclosed. Care needs to be taken to permanently remove the information so there is no way of being recovered. This standard also specifies requirements for redaction in software.

ISO/IEC 27040 gives detailed technical guidance on how to mitigate risk in data storage. Security storage includes guidelines for data in transit as well as what to do during the lifetime of media and after end of use. This is important for forensic investigators as security mechanisms like encryption can affect the ability to investigate the evidence. Hence, considerations need to be taken prior to and during the investigation. Additionally, the same guidelines can be applied to prevent contamination when storing the collected evidence. As explained earlier, this is critical to avoid making the evidence inadmissible in court.

ISO/IEC 27041 provides assurance that the investigative process used is suitable for the case under examination. In addition, it explains complicated processes and reduces them into smaller parts to aid in the improvement of simple investigation procedures.

ISO/IEC 27042 explains the methods and processes to be used during an investigation in order to evaluate, interpret and report the evidence correctly and effectively.

ISO/IEC 27043 defines the principles and process classes underlying the investigation. Most importantly, it provides a framework model for all stages of investigations.

2.6. Cloud Computing

Cloud computing is simply a marketing term for the delivery of hosted services over the Internet. Instead of deploying and managing a physical IT environment in order to host applications and data, organisations rely on remote and virtualised environments, usually managed by third parties [18].

New name, same old technology: cloud computing offers diverse benefits such as scalability, flexibility and readily available services [19]. Services are based on Pay-As-You-Go (PAYG) and if it works, the resources will scale dynamically with increasing (or decreasing) demand, thus providing great scalability. Flexibility benefit refers to the ability of using the computer resources you need when you need them, shortening IT projects and overall cost. New business opportunities are easier and quicker to implement by simply utilising readily available cloud services. These are just a few examples why cloud computing is an increasing popular choice for businesses and organisations.

Like everything in life, cloud computing also comes with some drawbacks. The availability of the service is arguably one of the most important obstacles for the adoption of such technology [20]. Service delivery depends on the ISP (Internet Service Provider) and cloud provider. When outages happen, service will simply be interrupted. Data confidentiality and privacy are two other big issues [20]. How the data are protected and who has access to them are main concerns. For example, European customers might think twice before choosing a US cloud provider, as the USA Patriot Act can give access to the data to US law enforcement agencies without a warrant [21].

Cloud computing uses three main levels of service that differ on the services that are delivered to the end user [22]:

- Software as a Service (SaaS): Providers offer access to their applications that are hosted on their own servers and consumers make use of them [22]. Common examples include file storage, social networking and email.
- Platform as a Service (PaaS): Here cloud providers offer a platform where consumers deploy and run their applications [22]. The underlying hardware, network and tools are provided by the cloud service. Examples include Google App Engine [23] and Windows Azure [24].
- Infrastructure as a Service (IaaS): Consumers buy raw computing and storage space and they can control and manage the underlying infrastructure like the operating systems, software and network [22]. Examples are Amazon EC2 and Rackspace Cloud Services.

Cloud services can be categorised by their organisational deployment: Private, the infrastructure is provisioned exclusively to a single organisation for private use [22]. Community is used by a specific community of organisations that share common concerns [22]. When the infrastructure is for open use, it is considered public [22]. Hybrid refers to the combination of two or more distinct cloud infrastructure [22].

2.7. The Trouble with Cloud Forensics

The aim of digital forensics is to extract information to answer the 5Ws from the data extracted from the evidence. In order to achieve this, most digital forensic processes assume absolute control of digital evidence [18]. However, in a cloud environment, forensic investigators might not have absolute control of the evidence.

According to Eurostat, in 2014 almost 20% of EU enterprises were using cloud computing services [25]. This number is expected to greatly increase as Amazon alone reported revenue of $7.88B in Q4 2015, up 69% over 2014 report [26]. This growth in popularity of cloud computing has significant implication when investigating in this environment as investigations become more complex.

2.8. Defining What Constitutes a Challenge

Each challenge will be classified into three categories: technical, legal and architectural. We have already presented technical and legal concepts. The first one refers to challenges created when collecting and analysing evidence, recovering data, and preserving integrity. The second one consists of issues created by legal restrictions, privacy concerns and jurisdictional difficulties. Architectural is the third group for the unique challenges found exclusively in cloud computing environment.

Our first step towards identifying forensic cloud computing challenges was to study the available literature and data on the topic. Then, we consider a simple but common forensic investigation case

to find the challenges we would encounter in such investigation and find out the biggest challenge category. We define the "biggest challenge" as a challenge that could bring the forensic investigation to a complete halt. For us, a qualitative method to analysis is preferred over a quantitative approach; hence, we consider the "biggest challenge" group not the group with the most challenges but the group that could potentially completely stop the investigation if one of its challenges were not overcome. Finally, we discuss open issues and where more work needs to be done.

3. Related Work

In this third section of the paper, we explore current work and available literature on cloud forensic challenges. Our search criteria include papers exclusively focused on this topic and no older than five years.

Martini and Choo [27] reviewed some of the most important technical publications. They argue that many of the challenges have already been explained but little evidence-based research to provide technical solutions exists. They also mention that ensuring the laws keep pace with the advancements in technology is needed.

Ruan et al. [28] conducted a survey amongst 257 international digital forensic experts and practitioners. Their survey included key questions on cloud forensics ranging from definitions, challenges, opportunities and missing capabilities. According to the results, more than 80% of the respondents strongly agreed in the following four challenges: (1) Jurisdiction (90%); (2) Lack of international collaboration and legislative mechanism in cross-nation data access and exchange (85%); (3) Lack of law/regulation and law advisory (81%); and (4) investigating external chain of dependencies of the cloud provider (80%). Although the results might be incomplete due to half of the respondents not finishing the survey, it can clearly be seen that forensic practitioners consider legal challenges the bigger issue in cloud forensics.

Alqahtany et al. [29] examined the challenges in cloud forensics by researching current literature. They divided the challenges by forensic investigation stages and identified a total of 13 issues. Additionally, they explored technical solutions and current research proposals to address such challenges. They concluded that dependence in cloud providers, time analysis and evidence correlation for multiple sources, cross border issues, lack of control of the environment and jury's technical comprehension are the main open issues that need further attention and effort.

Zawoad and Hasan [30] also examined the cloud forensics issues, investigated current available solutions to address them and concluded with open issues that need further work. However, the authors suggest Digital Forensics-as-a-service (DFaaS) as a solution to facilitate cloud investigations. They argue that if cloud services provided forensics-as-a-service, their customer would not need to implement any forensic schemes; thus making forensics cost effective for small and medium enterprises.

The National Institute of Standards and Technology (NIST) provides a comprehensive list of challenges practitioners face when investigating cloud environments [31]. NIST lists a total of 65 challenges, which are divided into technical, legal and organisational challenges. The main objective of the paper was to understand those concerns and identify standards and technologies to address them. However, the paper is a work in progress and, at the time of writing our paper, it does not provide solutions yet.

Quick's work focused his research on cloud storage data [32]. His motivation was that criminals are storing illicit data in cloud hosting providers, which is difficult to recover because the data of interest can be distributed, virtualised or transient. According to him, those are the biggest challenges when investigators need to recover data and prove the ownership and interaction of the files in cloud storage. As such, Quick developed a digital forensic analysis framework and conducted a research on popular cloud storage servers. His research concluded that vast amount of data remnants can be found from browsers and client software, and this data can be beneficial for law enforcements when investigating cloud storages.

Ab Rahman et al. [33] also argued that virtualisation of the data and their geographical location are the main concerns when investigating cloud storages. He and his team proposed an integrated cloud incident handling model for cloud investigations, which was successful in collecting residual or remnant data from client applications in a case study. The authors are planning to deploy the model in a real-world setting to validate it.

Many other studies have been done to overcome other challenges. Quick and Choo [34] wondered if data collection in cloud storage changes the data or its metadata. Their research concluded that their approach left everything unchanged and noted the importance of investigating timestamps. Daryabar et al. [35] also focused their efforts on understanding the alterations on the data and timestamps changed caused by mobile apps. Quick and Choo [36] also investigated how to deal with large volume of data, one of the main challenges by most of the literature reviewed, and provided a novel solution to reduce the data in forensic subset files. Cahyani et al. [37] examined the suitability of forensic tools to investigate cloud environments. Mobile forensics is an essential part in cloud investigations and Cahyani and team worked specifically on Windows phone devices. They concluded that tools for acquisition on such devices remains limited. On a similar topic, Do et al. [38] explained that general-purpose mobile toolkits cannot keep up with the ever increasing number of models, makes and firmware in mobile devices. They argue that general-purpose toolkits might not obtain all the relevant data and that it is infeasible for a practitioner to be familiar with every device. Teing et al. [39] provided a methodology for Peer-to-peer (P2P) investigations. They demonstrated that although files were fully encrypted, it is possible to retrieve crucial cloud metadata like the IDs and IP addresses of the peer nodes. Table 2 shows the summary of challenges identified in literature.

Table 2. Summary of challenges identified in literature.

Challenge	References
Jurisdiction	[28–31]
Lack of international collaboration	[28,30,31]
Lack of law/regulation and law advisory	[27,28,31]
Investigating external chain of dependencies of the cloud provider	[28,31]
Dependence in cloud providers	[29–31]
Time analysis and evidence correlation for multiple sources	[29–31]
Lack of control of the environment	[29,31]
Jury's technical comprehension	[29]
Large volume of data	[30,31]
DFaaS	[30]
Chain of custody	[30,31]
Crime scene reconstruction	[30]
Tools	[27,30,31,37–39]
Log visualisation	[30,31]
Virtualisation	[32,33]
Geographical location	[32,33]
Data and metadata changes	[34,35]

Although papers and articles pointing out the challenges in cloud forensics exist, few of them fully describe the challenges or provide solutions to overcome them. We believe there is a need for a study on the challenges with a hypothetical case scenario investigation and even a bigger need to provide specific solutions to each concerns.

4. Case Study

Here we present a hypothetical case study of a cloud-based crime. The aim is to illustrate the challenges listed in Section 2 with a case study and provide solutions to the issues. The hypothetical crime has been assigned to Police Chief Wiggum:

> Snake Jailbird is a criminal who traffics with stolen goods and sells them on a website hosted in a cloud provider. He pays his cloud provider, Krusty Cloud, with different stolen credit cards. Police have learnt about the website and need to prosecute the criminal.

The incident has been identified so the investigation will skip the first two activities and start with respond phase.

- **Respond:** Here forensic practitioners start determining the scope of the event.Action: PC Wiggum has already been briefed on the case and the details. He knows the investigation will need to be carried out in a cloud environment and as such the first thing to do is to find out where Krusty Cloud is registered to confirm if he has jurisdiction to investigate the case. Then, he will need to apply for a search warrant.
  - Challenge: Extraterritorial Jurisdiction (ETJ)

EJT is used to describe the ability of international tribunals to hear a case [40]. If the cloud provider is in the country of the investigation, investigators may obtain a search warrant; if the server is abroad, investigators may need to collect the data through international cooperation. However, it is not always clear who has jurisdiction. Going back to our example, let us suppose Wiggum is a police chief from Country A, the same applies to our fictional criminal, Snake. Now, let us also assume Krusty Cloud is registered in Country B but has all its servers in Country C. Who has jurisdiction in this case? Country A, because prosecutor and accused are residents in this country; Country B, because Krusty HQ (Head Quarter) is registered there; or Country C, because the servers and the data are physically located there?

Different countries have different rules when carrying out overseas investigations. For example, The Brussels I Regulation [41] describes the rules to determine if European Union Member States have jurisdiction in cases with links to other European Union countries. In other cases, most countries have legal assistance treaties with other countries [42]. These treaties are designed to formalise law enforcement assistance and may be applied to forensic investigations that involve overseas cloud providers. However, if police failed to gain jurisdiction over the case or failed to get help from other states, the investigation might come to a complete halt and the case may even be dropped. Hence, stronger cooperation between countries to overcome legal differences and practices is needed.

  - Challenge: Search Warrant

A search warrant is a court order that authorises law enforcement officers to search a person or location for evidence and seize it. Although search warrants vary between countries, essentially the search warrant must describe what needs to be seized with reasonable particularity. In a cloud investigation, the search warrant should include a description of the information that needs to be seized and where it is located [43]. In our hypothetical case, PC Wiggum needs to describe that he needs website files and any other information related to the criminal like payment details and personal information. Additionally, the location of the data needs to be noted with reasonable particularity. This adds many complications, as the data are likely to be replicated in multiple servers and probably in different foreign datacentres. Hence, the warrant should not include its physical location but be served to the data custodian, the cloud provider [43]. Forensic investigators need strong training in legal matters to successfully obtain a search warrant.

- **Identify:** Here is where the investigators start gathering information about the specific event or incident.Action: PC Wiggum needs to take notes of the systems to be analysed, their configuration and networks. However, he might not have physical access to the systems and may need to rely on the competence of the cloud staff.
  - Challenge: No physical access

The lack of physical access is a challenge identified in all the reviewed literature. This is because physical access to the cloud servers is not feasible for investigators as the exact location of where the

data are stored cannot be determined. Forensic practitioners might be able to track suspect's activities in the cloud, which will be explained in further detail in the collection stage. On the other hand, in some cases, investigators may need to ask for help to cloud providers and rely on their competence. Which brings us to the next challenge.

- Challenge: Competence and trustworthiness

In some cases, forensic investigator will need to turn to cloud providers for help. This means that practitioners need to rely on the competence of cloud providers' staff and trust them. Furthermore, this may make the admissibility of the evidence hard [44]. To solve this, forensic investigators should work with the cloud providers hand to hand, provide them proper documentation and ensure forensic procedures are followed.

- **Collect:** In this step, practitioners aim to maximise the collection of evidence as well as minimising the impact to the victim.Action: PC Wiggum has requested Krusty Cloud for cooperation and now he needs to locate the data to start collecting it. However, data collection in cloud cases comes with many challenges.
  - Challenge: Data Location and Collection

As said, no physical access is possible as it is usually unfeasible to pin point the exact location of the data. This means investigators might not able to create a forensic copy of the media storing the evidence. For example, Google have developed the Google File System (GFS) for data storage and allows users to access, create and modify their data [45]. When using their storage, it might seem that the data are stored in a single location; however, data are stored in multiple physical locations. Still, PC Wiggum might be able to extract remnant data from the suspect's browsers, handsets and client software [32,33]. Another option is to track the suspect's activities like file accesses and modifications, data transmissions and other information [46]. For example, practitioners should keep in mind that it is possible to retrieve crucial cloud metadata like the IDs and IP addresses of the peer nodes from the client software in P2P investigations, as demonstrated by Teing et al. [39]. User profiling using behavioural characteristics has been started to be implemented in intrusion detection systems. For example, Peng et al. [47] reviewed different user profiling methods that determine users' actions and behaviour to track them. Although their work focused on intrusion detection, same techniques could be applied for profiling and tracking a suspect; hence making it possible to know where their data might be located. However, finding the files of a specific user is an arduous task because of the main characteristics of cloud environments, multi-tenancy and resource sharing.

- Challenge: Multi-tenancy and resource sharing

Two of the main characteristics of cloud environments are multi-tenancy and resource sharing. The first one means that a single system serves multiple users. The second one refers to the sharing of the same hardware and software resources between users. This makes data location even harder because law enforcements need to seize the specific portion of the media where the suspect's data are stored. Referring to the cloud provider for assistance can help investigators with this challenge; however, as we have discussed earlier, this creates its own challenges in competence and trustworthiness.

- Challenge: Large and changing systems

Cloud service providers need large infrastructures to be able to keep the ability of their services. Additionally, as we explained earlier, resources are shared between different users which means the systems are always changing. Hence, collaboration from cloud providers is needed because they are the ones who know how the system works. On the other hand, investigators will need to use live forensic techniques as described on volatility challenge later on.

- **Acquire:** The most important task here is to maintain the integrity of the evidence and provide assurance that the evidence has not been changed while it is being acquired.Action: PC Wiggum needs to start acquiring the identified evidence without compromising or contaminating it.
  - Challenge: Massive volume of data

Nowadays, we hold many devices that are able to store data. As such, we keep large volumes of data across many storage media such as USB sticks, mobile memory and external hard drives. This problem exponentially increases in cloud investigations as a user can have Terabytes of data at their disposal. Data mining techniques can be applied to deal with this issue. For example, deviation detection can help in fraud or digital forgery investigations [48]; entity extraction can identify personal information in large datasets or databases [49]; and classification may be used to trace spam [50]. Additionally, techniques to collect data from social networks such as Facebook and Twitter can be used—and have already been used—to deny or confirm criminal alibis [51]. For example, PC Wiggum could check Snake's Facebook profiles to link him with other suspects or known criminal and find out what he has been up to. Some tools exist collect and link data from social networking platforms, and the discipline has been called Social Networking Forensics. This relatively new discipline is useful to find out the suspect's activities and his connections with other potential suspects.

In addition, investigators should also explore suspect's smartphones, tablets and personal computers. Cloud providers allow users to store large amounts of data and files and also offer a diverse number of services; hence, large amount of useful information is likely to be found on such devices. For example, Chung et al. [52] proposed new procedures for investigating handset devices running on Windows, Mac and Android. Their procedures allowed them to investigate users' traces that were later used to track their actions and recover files. Therefore, investigating suspect's smartphones can lead to a more precise investigation.

  - Challenges: Volatility

Volatility refers to the loss of content in memory or storage when the power is turned off. This is a big issue from a forensic point of view because if the server goes down, all processes in memory and CPU will disappear. This problem increases in complexity when the case involves Virtual Machines (VM). For example, IaaS VM have no persistent storage; therefore, all volatile data may be lost if the VM goes down [46]. Much literature has been written to address this challenge, and specialised tools already exist to retrieve volatile data. However, we would also suggest implementing Digital Forensics-as-a-Service (DFaaS) in cloud environments. Such technique allows collecting, acquiring and examining the evidence in the cloud instead of local machines. This would reduce complexity in forensic investigations, which would lead to a reduction in cost and time [53]. Although some proposals exist to develop further DFaaS, its implementation rate is far from ideal. Many trust issues arise when cloud providers' cooperation is needed [44], as we have already discussed. However, we believe such technology would be invaluable in cloud forensics as demonstrated by van Baar et al. on their study in the Netherlands [54].

  - Challenge: Chain of Custody

Chain of custody is a document that keeps a track of the evidence at all time by giving detailed history of the logs. Chain of custody is one of the most reliable methods for showing the authenticity of evidence and it is importance should not be underestimated as a weak or inexcusably lax report will make the evidence inadmissible in court [55]. This is a challenge not only forensic practitioners face but all investigators and prosecutors. As such, training and legal advice is a must for a legally acceptable chain of custody.

- **Preserve:** Isolation, securing and preservation of the original evidence is comprised in this step. The main aim is to prevent any cross-contamination.Action: The collected evidence needs to be protected from any contamination. PC Wiggum must ensure that the original evidence is not altered in any way.

- Challenge: Make a forensic copy

Before the examination of the evidence starts, the forensic investigator needs to make a forensic image, a bit-by-bit image of the evidence. The original evidence must not be used at all and must be kept securely to keep its integrity intact. The aim is to limit access to the evidence and prevent contamination during the examination. However, as we have been explaining, it is not always possible to locate where the data are stored, or they might be stored in multiple locations, data might change while in use or data might disappear if the power goes off. Additionally, the amount of data can be very large. Hypervisors offer snapshot capabilities, which is usually enough to collect the necessary information [56]. Major virtualisation products like Citrix [57], Proxmox [58] and VMware [59] offer this feature. A snapshot creates an instance of a virtual machine that can be later used for examination. The main advantage is that services do not need to be powered down; however, investigators need to know where the data are stored.

- Challenge: Data Integrity

Making sure that the integrity of the evidence has not been compromised is vital to bring a case to justice. If evidence has purposely or unwittingly been modified, the judge will not accept it and the case might be dropped. In order to keep integrity intact, investigators need to work on copies of the forensic image created in the early stages of the investigation. Furthermore, the investigator in charge needs to ensure that the chain of custody is being followed. However, in cloud computing cases, data needs to be collected using live forensic techniques that might alter the data itself if not performed correctly. Therefore, familiarity in live forensics and skills using the tools is a must for practitioners wanting to investigate cloud cases.

- **Understand:** In this step investigators need to determine the significance of reconstructed data and draw conclusions.Action: Now that PC Wiggum has the evidence, he needs to examine it and draw conclusions. However, he will need to decrypt files and recover any deleted data.
- Challenge: Recovery of deleted data

Forensic practitioners often are able to recover deleted files from storage devices such as hard drives, USB sticks and mobile phones. However, in cloud computing, recovery of the data is a challenging task due to the volatility and resource sharing characteristics of this environment. Investigators may refer again to cloud providers and request backups or file repositories to obtain deleted files. Previous snapshots of VM might also contain useful information. However, this might be insufficient because critical information might be ignored. Roussev and McCulley [60] demonstrated by analysing Google Docs that much can be learned from reviewing a document's revisions since its creation, as any modifications can be undone. Therefore, checking the suspect's hand devices is always a good practice as they may also hold copies of the deleted data.

- Challenge: Cryptography

More and more providers are offering encryption to their customers to protect their data. For example, Google Drive encrypts data at transmission level with HTTPS and Perfect Forward Secrecy (PFS) at service level. The 2048 RSA encryption keys are also used for validation and key exchange [61]. Cloud providers might be able to assist accessing the data in the investigation. However, if the criminals encrypt their files using other tools like TrueCrypt or Encrypt, investigators may need to force the suspect to divulge the password or brute-force it. Investigators may check for other weakness points to find out the password. Browsers have the capability of storing passwords and their repository is usually easy to crack. Additionally, suspect's mobile phone or other devices may hold the passwords or even a copy of the encrypted file itself if auto-synchronisation is enabled.

- Challenge: Data correlation issues

Investigators usually correlate multiple sources of evidence to confirm the results of the investigation [56]. In our case-scenario, PC Wiggum would trace Snake's payments and contact the credit card company used for paying the cloud service. Data mining techniques can once again be used to help identifying correlations. For example, correlation techniques can be used to link criminals with each other, find their personal data, identify their daily routines, etc. Tracking individuals through their postings on online news, social media or opinion websites may also create data correlation issues as multiple providers would need to be investigated. Peng et al. [62] provided a solution to this by using a bit-level n-gram based analysis, which helps identifying individuals from linguistic profiles. Peng et al. [47] also researched on user profiling. Although their work is focused on intrusion detection, same techniques can be applied for profiling and tracking a suspect through its behaviour. However, evidence correlation across multiple cloud providers is still a difficult task [31]. Investigators need to contact all providers involved and deal with different technologies and environments, which brings us to the next challenge.

○ Challenge: Lack of interoperability

Lack of interoperability between cloud providers is another challenge faced by forensic investigators [31]. Providers often use different architectures and technologies and each one may need different approach to locate and collect the evidence. This means that investigators need to trust the providers once again, creating more challenges in competence and trustworthiness.

○ Challenge: Partial evidence

Conducting examinations with partial evidence is real risk. Incomplete data may create false positives and might draw to wrong conclusions. Most legal systems work under Blackstone's formulation, which is the principle that "It is better that ten guilty persons escape than that one innocent suffer". Therefore, partial or incomplete evidence may be inadmissible in court. This means that if forensic practitioners failed to collect and acquire all the required evidence, they may need to start the identification, collection and acquisition processes again.

- **Report:** Here, a summary, explanation of findings and conclusions are reported.Action: PC Wiggum needs to produce investigation reports including what he has found and his conclusions. Additionally, he needs to include his investigation steps so a reviewer can come to the same conclusion. Once he has everything ready, he needs to bring his findings to court.

○ Challenge: Investigation report

Investigation reports are not limited to cloud cases and should be produced for any forensic investigation. They should be written so that they are legally admissible and include descriptions of the results and conclusions. Similarly, a 3rd forensic investigation team should reach identical conclusions following the examination steps in the report. Good writing skills in technical matters with knowledge of legal jargon should be included in the forensic practitioners training.

○ Challenge: Choosing the right court

Although this might not seem as a real challenge, it is not always easy to decide about the court where the case is to be brought to. In cloud computing, it is not always clear where the crime has been committed as the evidence could be located in different physical locations. In these cases, legal assistance is advised before deciding about the court.

- **Close:** In the last step, practitioners need to ensure evidence is returned to rightful owner or securely store if neededAction: PC Wiggum might need to return any seized evidence and securely delete or store as needed.

○ Challenge: Evidence return and Secure deletion

Returning of the evidence is not always needed, as hardware might not have been collected for examination. However, evidence data might need to be deleted according to each jurisdiction's laws

in privacy and data management. Data should be securely removed in such a way that it would be infeasible to recover them. Forensic practitioners need legal advice and training to know what to do with the data depending on the law.

5. Results

In the Table 3, we have listed the challenges PC Wiggum has faced during his cloud investigation. In addition, we have also included the solutions we provided earlier that will address or at least help addressing the issues.

Table 3. List of identified challenges and suggested solutions.

Challenge	Category	Potential Solution
Respond		
Extraterritorial jurisdiction	*Legal*	Stronger international cooperation
Search warrant	*Legal*	Legal training
Identify		
No physical access	*Architectural*	Ask cloud provider for cooperation
Competence and trustworthiness	*Architectural*	Provide documentation and Ensure forensic procedures are followed
Collect		
Data location and collection	*Architectural*	Mobile forensics and Data Profiling
Multi-tenancy and resource sharing	*Architectural*	Ask cloud provider for cooperation
Large and changing systems	*Architectural*	Cloud provider knowledge and Live forensics
Acquire		
Massive volume of data	*Technical*	Data Mining and Social Networks Forensics and Mobile forensics
Volatility	*Architectural*	Live Forensics and DFaaS
Chain of custody	*Legal*	Training and Legal advice
Preserve		
Make a forensic copy	*Architectural*	Snapshots
Data integrity	*Technical*	Live forensic training
Understand		
Recovery of deleted data	*Architectural*	Backups and Repositories and Snapshots and Mobile forensics
Cryptography	*Technical*	Brute-force and Mobile forensics
Data correlation issues	*Technical*	Data mining and User Profiling
Lack of interoperability	*Architectural*	Cloud provider cooperation
Partial Evidence	*Legal*	Return to early stages of investigation
Report		
Investigation report	*Legal*	Training
Choosing the right court	*Legal*	Legal advice
Close		
Evidence return and Secure deletion	*Legal*	Legal training and Legal advice

Cloud providers usually have datacentres in different countries and this can lead to *extraterritorial jurisdiction* restrictions [63]. Additionally, there is no guarantee that the foreign country in question will cooperate. In order to overcome extraterritorial jurisdiction restrictions, stronger international cooperation, like The Brussels I Regulation [41], is needed. Even when jurisdictional restrictions do not apply, investigations may be put on hold by enforcers' limited investigative power, for example, by not being successful on getting a *search warrant*. Officers need legal training to produce a successful search warrant. On the other hand, civil investigations might come to a completely halt when they face jurisdictional obstacles as they will not obtain a search warrant.

Law enforcement agencies have *no physical access* to the storages, networks and servers in the cloud. Even if the cloud provider agrees to cooperate, civil investigators depend on the *competence and trustworthiness* of cloud staff. This can be overcome by providing complete documentation and ensuring that forensic procedures are followed by the provider.

Main characteristics of cloud computing are *multi-tenancy and resource sharing* [63], which mean that the same system might be shared and used by many different users. Investigators need to find out which portion of the media need to seize when investigating a particular user and they also have to be sure that they have collected everything needed. The collaboration of the cloud provider may come handy here as well as user profiling techniques. Additionally, cloud computing environments are *large and changing systems*, adding even more complexity. The use of live forensic techniques and cloud provider's expertise on their own environment is crucial. Furthermore, criminals can use the cloud to hide by using different providers, thus increasing the difficulty of finding the *data location* [31] and carrying out its *collection*. In this case, investigators should start tracking file access and modification times and communications. Additionally, they could extract remnant data from browsers and client software.

Practitioners also have to deal with the *massive volume of data* users hold and to add further complications, in a cloud environment forensic investigators have no physical access or control to the media or network where the evidence resides [31]. Diverse data mining techniques are available to deal with large volume of data. Additionally, social network forensics and handsets investigation can help with this issue. Cloud systems are continuously running and the providers will likely not turned off the machines when collecting the evidence. This means investigators need to use live forensic techniques to acquire data from running applications, processes or network transmissions. However, live forensics has its own difficulties because of the *volatility* of the data, which means data can be modified when collecting it. A *chain of custody* is one of the most critical aspects in any investigation. Therefore, training and legal advice on how to maintain the chain is a must.

Once forensic practitioners have collected the evidence, they need to *create a forensic image* before understanding the evidence. However, as earlier mentioned, it is not always possible to locate where the data are stored, or data might change while in use or disappear completely. Cloud environments usually consist of virtual machines or containers and the hypervisors were these guest machines are hosted have snapshot facilities. These snapshots can be used as forensic copies.

Lack of interoperability between cloud providers is another challenge faced by forensic investigators [31]. Providers often use different architectures and technologies and each one may need different approach to locate and collect the evidence. Once again forensic practitioners may need the help of the cloud provider. Furthermore, *recovery of deleted data* before they are overwritten is an even more complex task in cloud environments because the system is still up and running. Recovering the data from backups, repositories, previous snapshots or other handsets can solve this hassle. However, forensic practitioners sometimes must execute code to collect the data, especially when using live forensics, which might potentially change the evidence [64]. Thus, exhaustive training in live forensics will help protecting *data integrity*.

While examining the evidence, the data might be encrypted so investigators need to deal with *cryptography* in order to extract the data. It is always a good idea to check the suspect's phones or tablets for unencrypted files or passwords. If this fails, brute-force might help with the decryption if the encryption key length is not too long. *Data correlation* across multiple cloud providers is difficult [38] but data mining and user profiling techniques can help. Another issue is that the acquired evidence might be incomplete or forensic practitioners may have obtained *partial evidence*, which can lead to a false accusation or dismissed the case all together. When this happens, investigators should return to the early stages of the investigation to collect and acquire the missing bits.

Then, investigators need to produce *investigation reports* and *decide which court to choose*. Although this might seem trivial, in cloud computing cases, it is not always clear where the crime has been

committed as the evidence can be located in multiple physical countries. Thus, legal training and advice is suggested.

Finally, two more actions need to be taken: *the evidence return and secure deletion*. In cloud investigations, returning of the evidence might not be necessary as hardware might not have been collected during the investigation. However, evidence data might need to be deleted according to each jurisdiction's laws in privacy and data management. Data should be securely removed in such a way that it would be infeasible to recover them. Legal training and advice are recommended here too.

We have identified a total of 20 challenges—seven legal, nine architectural and four technical—and provided potential solutions to overcome them. A list of the challenges and respective solutions can be found on Table 3. For technical challenges, data mining, mobile forensics and social networking forensics can aid. For architectural challenges, the use of mobile forensics, live forensics, Digital Forensics as a Service and cloud tailored techniques such as snapshots is invaluable. In addition, despite the trustworthiness issues that the collaboration and knowledge of the cloud provider might cause, their help in the case should not be overlooked. In order to overcome legal challenges, stronger international cooperation, legal advice and training are needed. This means practitioners need to have an understanding in mobile and social networking forensics, legal terms as well as data mining techniques if they want to succeed in cases where a cloud investigation is needed.

6. Discussion

Current forensic tools and techniques often require powering off devices or to attach digital forensic devices on the incident scene physical host. This might be sufficient for most cloud cases but is not ideal. Thus, in the long run, specialised processes and tools for cloud environments are needed; however, there is a lack of standards and procedures, tools and training.

Much work is being done to improve cloud investigations and we have included most of them as potential solutions. For example, researchers are focusing their efforts on extracting cloud storage information from client cloud software such as Dropbox and Google Drive [32,33,35], social networking applications such as Facebook, Twitter and Google+ [65], and different mobile devices [37,38]. Other researchers are working on techniques to deal with the large amount of data found on the cloud. Digital Forensic Data Reduction and the Quick Analysis methodology have the potential to pinpoint relevant evidence in a timely manner [66]. As earlier presented, data mining techniques [47–49] are also being applied to investigate large amount of data. Virtualisation of data and services poses more issues for practitioners but they can make use of snapshot functionalities, recover data from backups or use remote programmatic process, which can collect evidence and ensure no potential evidence is missed [67].

Conversely, cloud services could develop and implement automated forensic frameworks to their own systems like Digital Forensic-as-a-Service, where cloud providers could offer resources for forensic purposes exclusively. The implementation of this forensic alternative would make remote acquisition easier, quicker, cheaper and more trustworthy. This obviously raises a few questions: Who would pay for this service? Who would have the authority or jurisdiction to access the investigation reports? What about user privacy? More importantly, will the court trust it?

The system to be investigated can be configured as a virtualisation cloud system. Hence, the acquisition of the data from the system needs to be tailored to such technology. Investigators may use the snapshot feature available in most virtualisation technologies. However, this might be insufficient because critical information might be ignored. For example, much can be learned from reviewing an online document's revisions since its creation, as any modifications can be undone. Additionally, investigators might be able to find useful information on the suspect's PC or mobile devices thanks to the synchronisation between cloud and other devices.

On the other hand, log data related to cloud services can be acquired by examining the suspect's portable devices such as tablet, laptop or mobile phone. This is where mobile forensics comes handy

as discussed earlier and explored on [37,38]. Furthermore, social networking forensics may be applied to find out the suspect's activities and his connections with other potential suspects.

Nevertheless, we have come to the conclusion that forensic investigations biggest challenge is not technical—researchers and engineers are working on the technical issues and eventually we will have the needed models, frameworks and tools to investigate in the cloud—but legal. The reviewed literature also identified the similar legal aspects and Ruan et al. [28] survey amongst international digital forensic experts and practitioners shows that they consider legal challenges the bigger issue as well in cloud forensics. If legal challenges are not overcome, the investigation is likely to come to an early halt or be disregarded completely in a court of law. This is why we consider legal matters the most challenging group.

As we have seen, there is a lack of standards and jurisdictional issues. Cloud forensic standards are not a priority yet. After many years, the forensic community has not even agreed on standards for traditional forensics. Fortunately, the European Forensic Science Area, NIST and ISO/IEC 27000 are working on producing standards for both traditional and/or cloud forensics.

From the jurisdictional point of view, there is not much international cooperation. If the cloud provider is in the country of the investigation, investigators may be able to easily obtain a search warrant; if the server is abroad, investigators may need to collect the data through international cooperation, making the process difficult. As such, cross-border investigations are time consuming and extremely expensive, and only lawyers and criminals seem to benefit from cross-border offences. Consequently, we need stronger international cooperation to address this issue. Perhaps a common international law for forensic investigations might be a solution, though it would be naïve to think most countries would agree on it. Conversely, perhaps, involving INTERPOL, which currently 190 states are members [68], in international cases could be a solution. However, what happen with civil or private investigations? Do cloud service provider cooperate in a no criminal cases? Do they allow private external investigator on their own systems? Clearly, more work needs to be done on this subject.

7. Future Work

In our analysis we have argued that legal obstacles is the biggest challenge group in cloud forensics because failing to overcome any of its challenges, the investigation is very likely to come to a complete stop. However, as engineers, our knowledge in law is quite limited. This is the reason we would like to focus our efforts somewhere else. We are aware of the limitations of using a hypothetical case and this is why we are planning to use a real-life case for our future research. We believe such scenario will help us validate our findings, discover new challenges and provide a better understanding of the current state of cloud forensics. Additionally, a real-life scenario could give us the opportunity to further explore Digital Forensics as a Service. We believe such framework is the future for cloud forensics as it can process and investigate high volume of data automatically. Digital Forensics as a Service products are starting to be being used, like the Xiraf project funded by the Dutch Government [54], and their popularity are on the rise. Cloud computing is continuously changing and evolving which means work to adapt cloud forensics is a never ending task.

8. Conclusions

More and more businesses and individuals are relaying on cloud computing for their data, applications and services. This increase of cloud computing use has brought many challenges to forensic investigators. Unlike traditional forensic computing investigations, cloud environments are shared between multiple users and the systems are usually located in multiple physical locations. This means law enforcement agencies may not have physical access to the servers, networks and media devices.

Our hypothetical case scenario has shown that although current forensic techniques might be sufficient for most cloud investigations, in the long run, better live forensic tools, development of new methods tailored for cloud investigations like Digital Forensic as a Service and new procedures and

standards are indeed needed. Furthermore, we have come to the conclusion that forensic investigations biggest challenge is not technical but legal. Law enforcement agencies' power restrictions and the need for advice and legal training seem to be overlooked. Moreover, jurisdictional restrictions and lack of international cooperation are making cross-border investigations both expensive in time and cost. Consequently, stronger international cooperation for cloud forensics is needed.

Acknowledgments: This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2016-H8601-16-1009) supervised by the IITP (Institute for Information & communications Technology Promotion).

Author Contributions: Erik Miranda mainly wrote the paper; Seo Yeon Moon researched the related works; and Jong Hyuk Park supervised the paper work, reviewed, made comments, etc.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. McKemmish, R. *What Is Forensic Computing?*; Australian Institute of Criminology: Canberra, Australia, 1999.
2. United States Computer Emergency Readiness Team (US-CERT), Computer Forensics. Available online: https://www.us-cert.gov/sites/default/files/publications/forensics.pdf (accessed on 14 May 2016).
3. Kruse, W.G., II; Heiser, J.G. *Computer Forensics: Incident Response Essentials*, 14th ed.; Pearson Education: Indianapolis, IN, USA, 2010.
4. UK Legislation, Criminal Damage Act 1971. Available online: http://www.legislation.gov.uk/ukpga/1971/48/contents (accessed on 8 May 2016).
5. Sridhar, N.; Bhaskari, D.L.; Avadhani, P.S. Plethora of cyber forensics. *Int. J. Adv. Comput. Sci. Appl.* **2011**, 2, 110. [CrossRef]
6. Council of the European Union. ENFOPOL 413 COPEN 342. Available online: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2017537%202011%20INIT (accessed on 21 May 2016).
7. International Organization for Standardization, ISO/IEC 27000:2016. Available online: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66435 (accessed on 18 May 2016).
8. TOR Project. Available online: https://www.torproject.org/ (accessed on 11 May 2016).
9. Metasploit. Available online: https://www.metasploit.com/ (accessed on 11 May 2016).
10. Al Fahdi, M.; Clarke, N.L.; Furnell, S.M. Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. In Proceedings of the Information Security for South Africa, Johannesburg, South Africa, 14–16 August 2013; pp. 1–8.
11. ISO/IEC 27037:2012. *Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*; The International Organization for Standardization (ISO); The International Electrotechnical Commission (IEC) ISO/IEC: Geneva, Switzerland, 2012.
12. ISO/IEC 27042:2015. *Guidelines for the Analysis and Interpretation of Digital Evidence*; The International Organization for Standardization (ISO); The International Electrotechnical Commission (IEC) ISO/IEC: Geneva, Switzerland, 2015.
13. ISO/IEC 27041:2015. *Guidance on Assuring Suitability and Adequacy of Incident Investigative Method*; The International Organization for Standardization (ISO); The International Electrotechnical Commission (IEC) ISO/IEC: Geneva, Switzerland, 2015.
14. International Organization for Standardization, about ISO. Available online: http://www.iso.org/iso/home/about.htm (accessed on 17 June 2016).
15. ISO/IEC 27038:2014. *Specification for Digital Redaction*; The International Organization for Standardization (ISO); The International Electrotechnical Commission (IEC) ISO/IEC: Geneva, Switzerland, 2014.
16. ISO/IEC 27040:2015. *Storage Security*; The International Organization for Standardization (ISO); The International Electrotechnical Commission (IEC) ISO/IEC: Geneva, Switzerland, 2015.
17. ISO/IEC 27043:2015. *Incident Investigation Principles and Processes*; The International Organization for Standardization (ISO); The International Electrotechnical Commission (IEC) ISO/IEC: Geneva, Switzerland, 2015.
18. Grispos, G.; Storer, T.; Glisson, W.B. Calm before the storm: The Challenges of cloud computing in digital forensics. *Int. J. Digit. Crime Forensics* **2012**, *4*, 28–48. [CrossRef]
19. Catteddu, D. Cloud computing: Benefits, risks and recommendations for information security. In *Web Application Security*; Springer: Berlin/Heidelberg, Germany, 2010; p. 17.

20. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.H.; Konwinski, A.; Lee, G.; Patterson, D.A.; Rabkin, A.; Stoica, I.; et al. *Above the Clouds: A Berkeley View of Cloud Computing*; University of California at Berkeley: Berkeley, CA, USA, 2009.
21. Bush, G.W. *USA Patriot Act 2001 (H.R. 3162)*; The U.S. Congress: Washington, DC, USA, 2001; pp. 107–156.
22. Mell, P.; Grance, T. The NIST definition of cloud computing. *Commun. ACM* **2010**, *53*, 50.
23. Google, Google App Engine Documentation. Available online: https://cloud.google.com/appengine/docs (accessed on 5 May 2016).
24. Microsoft, Microsoft Azure. Available online: https://azure.microsoft.com/en-gb/ (accessed on 5 August 2016).
25. Eurostat, Cloud Computing-Statistics on the Use by Enterprises. Available online: http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises (accessed on 18 May 2016).
26. Amazon, Quarterly Results. Available online: http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-reportsother (accessed on 18 May 2016).
27. Martini, B.; Choo, K.-K.R. Cloud forensic technical challenges and solutions: A snapshot. *IEEE Cloud Comput.* **2014**, *1*, 20–25. [CrossRef]
28. Ruan, K.; Carthy, J.; Kechadi, T.; Baggili, I. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digit. Investig.* **2013**, *10*, 34–43. [CrossRef]
29. Alqahtany, S.; Clarke, N.; Furnell, S.; Reich, C. Cloud forensics: A review of challenges, solutions and open problems. In Proceedings of the 2015 International Conference on Cloud Computing (ICCC), Riyadh, Saudi Arabia, 27–28 April 2015; pp. 1–9.
30. Zawoad, S.; Hasan, R. Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. Available online: https://arxiv.org/abs/1302.6312 (accessed on 5 February 2013).
31. Quick, D.; Martini, B.; Choo, K.-K.R. *Cloud Storage Forensics*; Syngress Publishing: Amsterdam, The Netherlands, 2013.
32. Ab Rahman, N.H.; Cahyani, N.D.W.; Choo, K.-K.R. Cloud incident handling and forensic-by-design: Cloud storage as a case study. *Concurr. Comput. Pract. Exp.* **2016**, in press. [CrossRef]
33. Quick, D.; Choo, K.-K.R. Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? *Digit. Investig.* **2013**, *10*, 266–277. [CrossRef]
34. Daryabar, F.; Dehghantanha, A.; Choo, K.-K.R. Cloud storage forensics: MEGA as a case study. *Aust. J. Forensic Sci.* **2016**, 1–14. [CrossRef]
35. Quick, D.; Choo, K.-K.R. Big forensic data reduction: Digital forensic images and electronic evidence. *Clust. Comput.* **2016**, *19*, 723–740. [CrossRef]
36. Cahyani, N.D.W.; Martini, B.; Choo, K.-K.R.; Al-Azhar, A.K.B.P. Forensic data acquisition from cloud-of-things devices: Windows smartphones as a case study. *Concurr. Comput. Pract. Exp.* **2016**, in press. [CrossRef]
37. Do, Q.; Martini, B.; Choo, K.-K.R. A cloud-focused mobile forensics methodology. *IEEE Cloud Comput.* **2015**, *2*, 60–65. [CrossRef]
38. National Institute of Standards and Technology (NIST). *Cloud Computing: Forensic Science Challenges*; NIST Cloud Computing Forensic Science Working Group Information Technology Laboratory: Gaithersburg, MD, USA, 2014.
39. Teing, Y.-Y.; Dehghantanha, A.; Choo, K.-K.R.; Yang, L.T. Forensic investigation of P2P cloud storage services and backbone for IoT networks: BitTorrent Sync as a case study. *Comput. Electr. Eng.* **2016**, in press. [CrossRef]
40. Stigall, D.E. Ungoverned spaces, transnational crime, and the prohibition on extraterritorial enforcement jurisdiction in international law, Notre Dame J. Int'l & Comp. L. 1, 2013. Available online: http://ssrn.com/abstract=2211219 (accessed on 5 August 2016).
41. Regulation (EC) No 44/2001. 2000. Available online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:en:HTML (accessed on 5 August 2016).
42. Doyle, C. *Extraterritorial Application of American Criminal Law*; DIANE Publishing: Collingdale, PA, USA, 2010.
43. Dykstra, J. Seizing electronic evidence from cloud computing environments. In *Cybercrime and Cloud Forensics: Applications for Investigation Processes*; IGI Global: Hershey, PA, USA, 2013; pp. 156–185.
44. Dykstr, J.; Sherman, A.T. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digit. Investig.* **2012**, *9*, S90–S98. [CrossRef]
45. Ghemawat, S.; Gobioff, H.; Leung, S.-T. The Google file system. *ACM SIGOPS Oper. Syst. Rev.* **2003**, *37*, 29–43. [CrossRef]

46. Damshenas, M.; Dehghantanha, A.; Mahmoud, R.; Shamsuddin, S.B. Forensics investigation challenges in cloud computing environments. In Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, Malaysia, 26–28 June 2012; pp. 190–194.
47. Peng, J.; Choo, K.-K.R.; Ashman, H. User profiling in intrusion detection: A review. *J. Netw. Comput. Appl.* **2016**, *72*, 14–27. [CrossRef]
48. Mahdian, B.; Saic, S. Using noise inconsistencies for blind image forensics. *Image Vis. Comput.* **2009**, *27*, 1497–1503. [CrossRef]
49. Sindhu, K.K.; Meshram, B.B. Digital forensics and cyber crime datamining. *J. Inf. Secur.* **2012**, *3*, 196–201. [CrossRef]
50. De Vel, O.; Anderson, A.; Corney, M.; Mohay, G. Mining e-mail content for author identification forensics. *SIGMOD Rec.* **2001**, *30*, 55–64. [CrossRef]
51. The New York criminal law blog, criminal found via facebook. Available online: http://newyork criminallawyersblog. com/2010/03/assault-criminal-who-was-found-via-facebook-is-back-in-ny.html (accessed on 19 May 2016).
52. Chung, H.; Park, J.; Lee, S.; Kang, C. Digital forensic investigation of cloud storage services. *Digit. Investig.* **2012**, *9*, 81–95. [CrossRef]
53. Wen, Y.; Man, X.; Le, K.; Shi, W. Forensics-as-a-service (FaaS): Computer forensic workflow management and processing using cloud. In Proceedings of the Fourth International Conference on Cloud Computing, GRIDs, and Virtualization, Valencia, Spain, 27 May–1 June 2013; pp. 208–214.
54. van Baar, R.B.; van Beek, H.M.A.; van Eijk, E.J. Digital forensics as a service: A game changer. *Digit. Investig.* **2014**, *11*, S54–S62. [CrossRef]
55. Giannelli, P.C. Chain of custody and the handling of real evidence. *Am. Crim. Law Rev.* **1982**, *20*, 527–568.
56. Birk, D.; Wegener, C. Technical issues of forensic investigations in cloud computing environments. In Proceedings of the 2011 IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), Oakland, CA, USA, 26 May 2011; pp. 1–10.
57. Citrix, xenserver: Understanding snapshots. Available online: http://support.citrix.com/article/CTX122978 (accessed on 2 August 2016).
58. Proxmox, live snapshots. Available online: https://pve.proxmox.com/wiki/Live_Snapshots (accessed on 2 August 2016).
59. VMware, understanding virtual machine snapshots. Available online: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180 (accessed on 2 August 2016).
60. Roussev, V.; McCulley, S. Forensic analysis of cloud-native artifacts. *Digit. Investig.* **2016**, *16*, S104–S113. [CrossRef]
61. Google, security. Available online: https://support.google.com/work/answer/6056693?hl=en (accessed on 1 August 2016).
62. Peng, J.; Choo, K.-K.R.; Ashman, H. Bit-level n-gram based forensic authorship analysis on social media: Identifying individuals from linguistic profiles. *J. Netw. Comput. Appl.* **2016**, *70*, 171–182. [CrossRef]
63. Ruan, K. *Cybercrime and Cloud Forensics: Applications for Investigation Processes: Applications for Investigation Processes*; IGI Global: Hershey, PA, USA, 2012.
64. Jones, R. *Safer Live Forensic Acquisition*; University of Kent: Canterbury, UK, 2007.
65. Norouzizadeh Dezfouli, F.; Dehghantanha, A.; Eterovic-Soric, B.; Choo, K.-K.R. Investigating social networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms. *Aust. J. Forensic Sci.* **2016**, *48*, 469–488. [CrossRef]
66. Quick, D.; Choo, K.-K.R. Big forensic data management in heterogeneous distributed systems: Quick analysis of multimedia forensic data. *Softw. Pract. Exp.* **2016**, in press. [CrossRef]
67. Martini, B.; Choo, K.-K.R. Remote programmatic vCloud forensics: A six-step collection process and a proof of concept. In Proceedings of the 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, China, 24–26 September 2014; pp. 935–942.
68. INTERPOL, member countries. Available online: http://www.interpol.int/Member-countries/World (accessed on 4 August 2016).