Exploring Cloud Incidents

1 Introduction

The use of cloud computing technologies is gaining increased popularity and quickly becoming the norm. At the same time, the cloud service providers (CSP) are not always able to keep up the pace with new technologies. This also affects forensic analysis of incidents in these systems. Nowadays, events caused by malicious activities are becoming more and more frequent and, therefore, digital forensics activities are becoming a necessity. Even though this necessity is identified as a challenge, digital forensics on cloud remains a complex topic.

The specific characteristics of a cloud-based environment can raise a number of technological, organizational and legal challenges (the definition of these dimensions of analysis for the cloud forensics is explained below) that digital forensics investigators usually don't face while obtaining digital evidence in traditional IT environments.

1.1. Scope and objectives

With this paper, ENISA aims to give an overview of the current status of the forensic analysis techniques and processes of cloud incidents.

Specifically, the objectives of this paper are:

- To identify and analyse the current technical, legislative, organisational challenges or any other kind of limitations that could hamper a sufficient and seamless investigation of cloud incidents.
- To present an overview of the techniques, approaches and good practices for the forensic analysis of incidents in the Cloud, based on a desktop research.
- To provide advice and good practices (in particular related to SLAs and security measures) on how to make cloud forensic analysis more effective.

1.2. Target Audience

This document is addressed to:

- cloud providers and cloud customers, to enhance their knowledge on existing approaches and techniques;
- law enforcement agencies and governmental authorities, to improve their expertise on the matter;
- cloud security professionals to make them aware of the challenges they might face when conducting forensic analysis in cloud environments.

Specifically, the document aims at informing both cloud providers and cloud customers on cloud forensics challenges; it also provides insight on the current approaches to cloud security professionals and law enforcement agencies. Additionally, the document addresses some of the key challenges and concludes on how cloud service providers, law enforcement agencies and cloud security experts could invest on cloud forensics within the EU Member States.

2. Approaches for Cloud forensics

The term "Cloud Forensics" refers to the ability of reconstructing and analysing past cloud computing events (cloud based cybercrimes or incidents) by applying suitable practices, techniques and methods. This process can be divided into the stages depicted in the Figure 1:

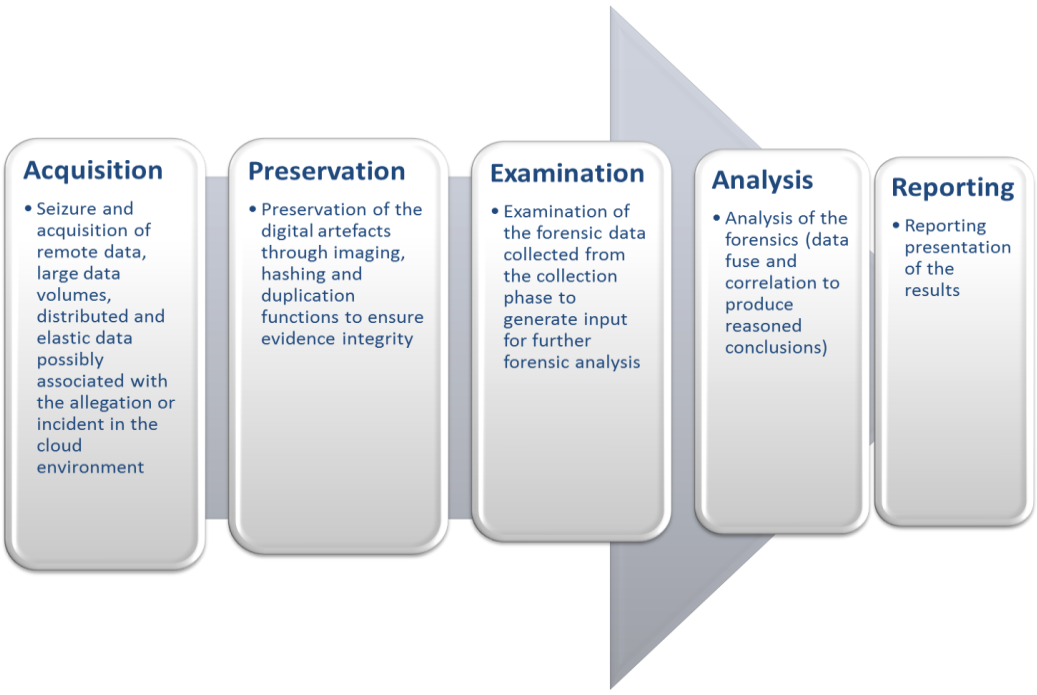

Figure 1 Cloud forensics stages

A cloud incident[1] is a breach of security in the cloud environment that has an impact on the operation of network and information system core services, which public administrations and market operators provide.

2.1. Literature review

Based on the literature review, the main factors that render forensic investigation on cloud harder than traditional investigations are the following:

- Legal issues including multiple ownership, multiple jurisdictions, and multiple tenancies;
- Limited access to remote and distributed physical infrastructure and storage;
- Lack of physical control and physical location of data;
- Lack of collaboration from the cloud provider(s);
- Segregation of duties among cloud actors;
- Difficulties in accessing and analysing the log data / lack of transparency of log data to the consumer;
- Proliferation of mobile devices and endpoints.

1 ENISA; Cloud Security Incident Reporting, Framework for reporting about major cloud security incidents

The complexity of cloud forensics depends on:

a. The cloud service models: in the IaaS model, customers may easily have access to data, while in the SaaS model customers may have little to no access to data required for cloud forensics;
b. The deployment model: in private clouds, provider-side artefacts should not be segregated among multiple tenants, while in public clouds, the segregation is mandatory.

The following table tabulates some of the key elements that affect investigations between different service models, based on the relevant literature[2] [3] [4]

SERVICE MODEL	CUSTOMER	PROVIDER
SaaS	• Client does not have a deep view of the system and its underlying infrastructure • Single sign-on (SSO) access control should be requested • The client has to contribute to the forensic process, e.g. by implementing Proofs of Retrievability (POR)	• Logging tools should run on the provider infrastructure • Providers may not give access to the IP logs of clients accessing content or to the metadata of all devices
PaaS	• Core application is under the control of the customer • The customer has no direct control of the underlying runtime environment • Logging mechanisms and additional encryption can be implemented	• Some CSPs provide diagnostic features that offer the ability to collect and store a variety of diagnostics data in a highly configurable way.
IaaS	• IaaS instances provide much more information that could be used as forensic evidence than the PaaS and SaaS models. • Some examples are: the ability of the customer to install and set up the image for forensic purposes, to execute the snapshot of virtual machine; RFC 3227 contains several best practices applicable to a IaaS useful for responding to a security incident especially in the case of live investigating systems.	• Virtual IaaS instances, in many cases do not have any persistent Storage (Persistent data has to be stored in long time storage) and volatile data might be lost. • Providers may be reluctant to provide forensic data such as recent disk images because of privacy issues that arise. • Some problems may arise from the unclear situation regarding how the provider handles the termination of client contracts and from the inability of the client to verify that the sensitive data stored on a virtual machine has been deleted exhaustively.

Table 1 Investigation in the different service models

2 Technical Challenges of Forensic Investigations in Cloud Computing Environments, D. Birk

3 Cloud forensics: An overview, Keyun Ruan, Prof. Joe Carthy, Prof. Tahar Kechadi, Mark Crosbie

4 Forensic Investigation in Cloud Computing Environment, Agreeka Saxena, Gulshan Shrivastava, Kavita Sharma

2.2. Procedures for cloud forensics

There are three potential types of forensics in the cloud environment: before incident, live, and post incident[5].

Before incident: In the cloud environment, it is important for the customer and the CSP to have prior agreement on the actions they have to take for forensics in case of an incident. Before incident is considered the most valuable type of forensics because such provisioning activities tackle most of the technical issues. This type of analysis falls under the responsibility of the CSP who has to carry out some preliminary actions: examples include tracking of the activity records, regular and detection of suspicious of abnormal behaviour, collection of activity logs, collection of support machinery (hypervisor) logs and collection of logs from other tenants (the latter implies careful planning for information sharing and anonymization). A common practice, well documented and detailed in all stages, is to monitor the network (before incident - provisioning) and try to turn each case into a traditional network forensics procedure when an incident occurs. CISOs can handle many incidents more efficiently and effectively if these provisional actions and controls have been adopted into the procedures of the CSP in order to support forensics activities. These preventive controls can be included in the contract between customers and providers to support the forensic analysis of incidents.

Live: Live forensic acquisition aims at capturing forensic data from a live and running system before switching off the power. In general live forensic acquisition is usually carried out to acquire volatile data (memory, process, network information acquired in order of volatility) that will be lost with traditional forensic acquisition (dead forensics). Due to the nature of cloud systems (cloud system cannot be easily 'switched off', networking for the remote access of the infrastructure, etc.), live forensic acquisition capability is essential but also very expensive.

Post incident: After an incident, the investigators acquire a logical and physical image of each artefact. In such cases it is recommended to have the mapping of the entire environment used by the victim, both the dedicated and the shared environment, if any and if allowed.

2.3. Traditional approaches

The main features of forensic approaches used in cloud based environments are remote acquisition and triage capabilities, applied on the target virtual machine deployed in the IaaS model. In both SaaS and PaaS models, the ability to access the virtual instance for gathering evidential information is highly limited or almost impossible: the investigator will have to rely on the evidence provided by the CSP and the device.

The tools currently available are actually the ones used in traditional investigations. In particular, network forensic tools are used to capture data (information, logs, etc.) on IaaS, as IaaS instances provide more information for forensic evidence in case of an incident than the PaaS and SaaS models do[6].

In the SaaS model, the customer does not have any control of the underlying operating infrastructure or even the application that is provided. For the support of forensics analysis, the customer has to buy specific services from the providers (for example logging and trace activities application, access control toolkit) to create useful information for the analysis.

In the PaaS model, it might be possible to implement logging mechanisms at the application layer to help the forensic investigation. However, the customer has not direct control of the underlying environment and the data acquisition for collecting evidence depends strongly on the prior agreement with the CSPs.

5 Cybercrime and Cloud Forensics: Applications for Investigation Processes, K. Ruan

6 Technical Challenges of Forensic Investigations in Cloud Computing Environments, D. Birk

3. Challenges in forensics for cloud incidents

In this paper, we have followed a specific approach to identify the challenges of cloud forensics in the EU. In order to contextualize the specific European landscape we report briefly some essential pointers that are specific in the EU policy context:

- The EU data protection Directive 95/46/EC[7] imposes stringent dispositions with regards to the processing of personal data and on the free movement of such data. At the same time, not all member states have adopted the EU data protection directive, resulting in the fragmentation of national data protection legislation. With the General Data Protection Regulation, which includes new data protection requirements that should be implemented by MS, this becomes even more complex.
- In case of forensic analysis that requires cross-border data access and exchange, the lack of collaboration mechanisms between the EU law enforcement agencies and the fragmentations in a multitude of national regulations, make the coordination between the law enforcement agencies problematic and the roles and responsibilities of the actors involved in this type of investigations unclear.
- There is a lack of specific guidelines or references in cross-European level for forensics investigations tailored to the characteristics of cloud computing infrastructure.
- The big cloud services providers are mainly based outside the EU where the laws regulating privacy and data protection are different from the EU, as are the regulations regarding multi-jurisdictions' and cross border investigations.
- No certification exists for tools, practices and training related to cloud forensic investigations.

Therefore, to depict the cloud forensics status in the EU landscape we have defined these three dimensions:

- The **technical dimension** refers to the specific features of the cloud computing model that are to be considered in the forensic investigations in the cloud computing environment.
- The **organizational dimension** refers to the aspects related to the coordination of parties involved in the forensic investigations in the cloud computing environment.
- The **legal dimension** regards the legal aspects and issues between the parties involved in the forensic investigations in the cloud computing environment, the legislative frameworks as well as the legal issues of the acquisition of digital evidence in the cloud computing environment.

The table below outlines the three dimensions as well as the challenges of forensic analysis per dimension.

TECHNICAL	ORGANISATIONAL	LEGAL
Forensic data collection	Organisational structure for each cloud organisation	Multi-jurisdiction and multi-tenancy
Elastic, static and live forensics	Chain of Dependencies of CSPs and cloud applications	Service Level Agreement
Evident segregation of resource pooling environment		
Investigations in virtualized environments		
Proactive preparations of measures for forensic investigations		

7 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Table 2 Characterization of the three dimensions identified in the forensics of cloud incidents in the EU

Due to the multi-tenant nature of Cloud, a number of additional *horizontal challenges* that might affect the cloud forensics have been identified in this analysis. Specifically, these challenges are not directly linked to the dimensions identified above, but they might belong to one or more of the dimensions or be related to more generic/high-level issues.

3.1. Technical challenges

Forensic data collection in a cloud environment is defined as the process of identifying, labelling, recording, and acquiring forensic data from the possible sources of data in the Cloud[8] and is actually the first critical stage of the post -incident analysis. In particular, the experts consulted within the context of this study, highlighted that forensic data collection in the case of cloud based environments is usually more complex than in traditional investigations, particularly given

a. the remote nature of the evidence,
b. the lack of physical access and
c. the distributed and dynamic nature of the cloud model that makes it difficult to demonstrate the integrity and authenticity of the evidence acquired.

It is important to stress that seizure and acquisition of digital artefacts is a critical step in the forensic process, on which the other steps are highly dependent. The issues encountered in this initial phase of the process can affect its next phases by preventing and/or interrupting the execution of the investigations. Most of the interviewees, based on their experience in specific investigation practices and forensics activities, have agreed that technical challenges have been almost always less relevant than legal and organizational ones, which are considered as the most difficult to overcome. Some of the technical characteristics of cloud computing, such as the resource pooling using multi-tenancy model and virtualization of resources, are well known in traditional investigations. However, in a cloud environment such features are actually enhanced and they might prevent the practices of forensics in some cases. Given the specific characteristics of the cloud, the post incident investigation activities become more complex. In particular the following features can be translated to some cloud-specific challenges for forensic analysis:

Multi-tenancy. Multi-tenancy of systems is not a new challenge in the forensic investigations but, in the case of Cloud, it is exacerbated by the rapid elasticity of the cloud resources that increases the complexity of the data acquisition. Most forensics procedures and tools developed over the years focus on physical acquisition and extraction of images. However, in cloud environments, if the CSP is not providing the specific feature then the forensic process is almost impossible. Additionally, physical acquisition might be a challenge even for the CSP if the tenant has released the resources which are then reused by other tenant in a different fragmentation scheme.

Dynamic nature. In cloud, the resources are allocated dynamically. This attribute of cloud hampers the accurate segregation of the resources under investigation. This is a significant challenge for the investigators and the Law Enforcement Agencies (LEA) as confidentiality of other tenants sharing the infrastructure must be taken into account.

Volatile data. It was always a challenge for digital forensics investigators to acquire the volatile data in memory. The same applies to the data stored in the cloud instances that do not have persistent storage synchronization. Additionally, in cloud instances, volatile data might be lost after attacks that are able to force the shutdown of the

8 Cloud forensics: An overview, Keyun Ruan, Prof. Joe Carthy, Prof. Tahar Kechadi, Mark Crosbie.

cloud instances. Attackers entirely compromising the acquisition of volatile data from virtual IaaS instances could abuse this vulnerability.

Data deletion. Data deletion procedures are in place by the CSP for privacy reasons[9] and for the elasticity of the cloud resources. The recovery of deleted data in a shared and distributed virtual environment is more difficult if the CSP has not implemented efficient mechanisms for the retrieval and the limitation of data in terms of backups and data retention.

Cumulative trust issues across Cloud layers. Cloud environments are structured in multiple layers (Network, Physical Hardware, Host OS, Virtualization, Guest OS, Guest application) and this introduces more trust issues than in traditional investigation where the target machines are physically controlled/owned by the customers[10]. The data forensic acquisition techniques vary according to the level of trust required for each layer. For example, the acquisition technique that follows a remote forensic software takes place in the layer of the Guest application. This technique requires to trust that the Guest OS, Virtualization, Host OS, Physical Hardware and Network (all the previous layers) to produce accurate and error free evidence data.

Cloud and time synchronization dynamics. The collection and analysis of evidence entails the correlation and the event-based reconstruction of information from dispersed sources of the digital environment under investigation and requires the association of timestamps with each event or data item of interest in order to reconstruct a sequence of events. The definition of time-lining[11] of the file creation, access, and modification times over cloud resources is an issue for the rapid dynamics of the cloud environment and for the accurate time synchronization requested. In the cloud environment, the data is distributed across the world, and when reconstruction of the data and the actions is required, the time synchronization is a critical issue as timestamps must be synchronized using protocols (e.g. NTP) that synchronize machines located across different locations.

Unification of different data format of the logs. A similar issue to time synchronization is the distribution of logs among different layers of the cloud stack and the different data format of the logs. It is an issue inherited by network forensics that makes accessibility and acquisition of logs more complex. Unification of log formats in cloud forensics requires at least common dictionaries, synchronized clocks and unifying console.

Lack of cloud-specific tools. The lack of cloud-specific and certified tools has often been perceived as an obstacle for the development of foundation of mature cloud forensics technology. The development of such tools should evolve together with cloud technology and should provide suitable and standard solutions for the digital evidence collection overcoming the specific technical challenges of the investigations in the cloud environment.

Encryption of data. Data encryption may cause some technical challenges because the decryption of large amounts of data is time and resources intensive. This challenge is exacerbated by the fact that in the Cloud in case of investigations that require large volumes of data to be decrypted.

Re-usable and shareable resources. Due to the constant re-use of resources (i.e. IP addresses), some of them might be blacklisted due to an abuse case. The next tenant that gets the IP is also considered black listed due to the

9 Directive on privacy and electronic communications (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ 2002 L 201).

10 Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and Evaluating Tools, Trust, and Techniques, J. Dykstra, A. Sherman

11 Cloud Computing: Pros and Cons for Computer Forensic Investigations Denis Reilly, Chris Wren, Tom Berry

previous owners' malicious use. The whitelisting process is more difficult in cloud environments and can lead to whole ranges of IPs being blocked due to slow response of CSP fixing the issue.

User Accountability. Cloud resources can be used by many tenants during a short period of time (e.g. over a year). Tracking of the use of each resource by a user is critical in a forensics investigation; for instance a public IP address used in an attack/abuse can be held by many users during a year, therefore, who is responsible for a specific time, which space was allocated to which user at the time in order to extract evidence, and other similar queries might arise.

3.2. Organisational challenges

The complexity of forensics and investigations in a cloud environment is strictly related to the organisational challenges. The experts noted that these types of challenges are actually the most relevant (compared to the technical and legal ones) and that might affect investigations in a very severe manner. The most prominent organisational challenges are the following:

Evidence collection. In practice, forensic investigations in the case of cloud computing environments always involve at least two parties, the CSP and the cloud customer. However, the dependency on the CSP for the forensic data collection is strongly dominant since it affects the starting phase to execute the investigation.

Limited collaboration. Investigators can collect forensic evidence themselves remotely from the source (time consuming operation), but in most cases investigations require evidence retrieval from physical locations on the premises of the providers. In both cases, without the provider's cooperation, it is almost impossible to perform the investigation and obtain any information; additionally, in most cases the time needed for the data acquisition may be longer than in traditional investigations. When the investigator is in law enforcement, cloud providers (in some countries) might be obliged to cooperate and facilitate the investigation.

Specifically, the factors that make the role of the CSP important are mainly related to the following:

- In the distributed architecture of the cloud model, data is stored in different host machines and located in the data centres across the world. Information about machines, credentials, logs and encryption keys is managed on the provider side.
- The procedure of evidence acquisition conducted on the target machines has to be fully supported by the CSP: the investigators collect the evidence directly from the target sources together with the providers and are not allowed to "touch" or operate on any of the CSP systems and machines.
- Even third parties could be engaged in the forensics investigations if the CSPs have data located on contracted third parties, increasing the complexity on the organization aspects of the forensics activities.
- CSPs and investigators do not usually follow any common standard or procedures to acquire image/find traces/get history logs, which increases the complexity of the design and organization of the activities of the forensic investigations.
- In the case of cross-border incidents the collaboration between the CSPs and law enforcement becomes even more crucial and complex: in the worst case, if the law enforcement bodies or the CSP of one of the involved countries does not collaborate it is almost impossible to proceed with the investigation. In cross border incidents the legal procedures are slower as they might "hit" in legal obstacles and gaps on legislation between countries.

Responsibilities based on the deployment model. Finally, there are still significant differences in the complexity of the forensics investigations depending on the cloud deployment models. In general, the more control the customer has on the cloud environment, the fewer organizational challenges the investigator will face. In the case of IaaS, where the consumer has complete control over a guest operating system running on a virtual machine (VM)

and the provider retains control and responsibility for the hypervisor (HV) down to the physical hardware in the data centre, the organizational issues are weaker than in the other deployment models. More challenges arise in the SaaS case, where the owner of the data has no control over the infrastructure and without the full collaboration of the CSP the owner of the data cannot access the needed information (logging, data, metadata, hashes, root hashes etc.).

3.3. Legal challenges

With regards to the legal challenges for cloud forensics the most important ones that were highlighted by the experts are analysed below.

Cross-border and multi-jurisdictional issues

Cross-border and multi-jurisdictional challenges are common to almost any cloud deployment model. However in cases where the host machines and data centres of the CSPs are located around the world, more legal issues are likely to emerge considering the time constraints that characterise the investigations. Specifically, the experts have underlined the following:

a. Cross-national legislations and collaboration mechanisms or channels between law enforcements, CERTs and public authorities that can facilitate the exchange of data for the forensic investigations are not well developed.
b. Formal requests issued during cross-border investigations to allow access to data stored remotely are conditional to the local legislation. Access is granted only after preliminary analysis realised by the responsible authorities of the countries in which the data resides.
c. There is no specific regulation governing the CSP obligations in terms of standard operating procedures, the standard actions the CSP has to take in case of investigations to which request the CSP has to comply, the timing for that (e.g. immediately, in a week, in a month), and finally the instructions on how data logs should be kept, managed and stored in order to provide evidence.
d. There are currently no agreements among cloud providers, law enforcement and customers to collaborate on investigations when necessary.
e. For law enforcement dealing with international investigations, legal access to data is still one of the most relevant challenges. A number of different issues might occur: the concept of locality of the law enforcement mandate (national or regional), the national legislations which do not allow some categories of information to be transferred abroad, privacy aspects related to sensitive information, and finally the presence of consulting authorities or institutions (as centres of expertise).
f. International cyber policies and laws must progress to help and solve the issues surrounding multi-jurisdiction investigations.

On the other hand, for the private sector, the cross-border and multi-jurisdictional issues can be managed in a better way, as the access and exchange of data for investigations is performed exclusively by the CSP that is the owner of the data.

SLAs regarding forensics

In most cases, forensic activities and services provisions are not included in SLAs. During the negotiation phase, the customers are not always aware of the relevance of forensics activities, while, the providers often lack transparency in defining what is and what is not included in the contract in terms of forensics services. SLAs that clearly define the forensic process could eliminate most of the organizational issues that hamper an investigation.

However, SLAs with clearly defining terms and conditions to enable general forensic readiness in the Cloud, are not usually in place. Moreover, terms and conditions on segregation of duties between CSP and cloud customers are

quite often not included in SLAs. Even if these clauses are included, the respective terms and their meaning are, in many cases, not clear to the customers.

To facilitate forensics activities, the CSPs should define the terms and conditions in the contracts. General agreements describing clauses like data access and procedures for forensics, as well as roles and responsibilities should be included in the SLAs to address most of the practical issues encountered in the investigations. Examples of clauses to be negotiated in advance are the following:

- Type of access granted by the CSP to the customers/investigators and authentication method for eligible investigators;
- The apportionment of roles and responsibilities between the CSP and the cloud customer regarding forensic analysis ;
- Procedures to follow in the forensic investigations;
- Time of delivery of the data;
- Type of metadata and type of logging (depending on the deployment models) that will be collected;
- Cost related items (What extra costs are defined in case of incidents? Are the costs related to forensics standard fees or extra costs?);
- Who can gain access to data collected and under what conditions.

Finally, with regard to the SLA a recommendation has been provided by one of the interviewees: Metrics (Service Level Objectives) to be included in the SLA could facilitate the forensics activities, and in particular metrics on implementation of logs and procedures, metrics on the effectiveness of incident resolution and metrics of efficiency of incident resolution.

Chain of custody

In a legal context, the chronological documentation of evidence handling is required to avoid allegations of evidence tampering or misconduct (*chain of custody*).

In traditional IT investigations, the copy of the hard disk of the targeted machine is used as evidence in court. In the Cloud environment, the distributed, multi-tenancy and the elastic nature of the cloud makes it more difficult for the investigators to prove that the data presented to the court are those of the persecutor. No tool exists at the moment that can solve this issue.

However, in practice, this problem is tackled by adhering to good practices; for instance, in the UK and IE, the evidence collected in the cloud and provided by the prosecution has been admitted after proving to the court that investigators had carefully and transparently executed standards procedures and good practices.

3.4. Horizontal challenges

In the context of this paper several horizontal challenges have also been identified as issues related to one or more of the dimension already defined:

1. One of the most relevant issues that might affect cloud forensics activities, especially in the case of critical information investigations, is the **time-to-detect and time-to-respond**. The time of occurrence of an incident and the actual start-up of the investigation activities, as well as the time spent to complete the evidence collection, are always crucial. The start of the data collection might be delayed due to a series of issues, as described above (mainly organizational) and any delay in having access to the machines/data might invalidate the whole process; given the dynamic nature of the distributed environment, changes can occur at any time:

like in any investigation, the delay in collecting evidence might have a strong impact on the results of the prosecution.

2. A second major issue is related to the **cost and effort (resources)** needed to conduct the investigation from all parties involved (CSP, law enforcement, client, third party, etc.). In most cases, the cost of investigations is incurred only by the customer (if forensic services have not been included earlier in the SLAs contract) and it is translated as extra cost to cover unforeseen activities. As customers actually want to have cost-effective cloud computing solutions, especially if they are just moving to the cloud and have limited digital security awareness, in most cases they are not very keen on including additional services (insurance, basic forensic features, etc.) in the contract to avoid cost increase (risk of unforeseen costs).
3. Finally, CSPs do not typically provide **standard features** (e.g. logging, monitoring, etc.) to support forensics in common cloud infrastructures that could minimize the cost of ownerships of the infrastructure exploiting economy of scale. For example, the IP logging that is actually one of the most expensive and crucial features needed for the investigations, is not included in the services that the providers offer to the customer. The cost of the investigation (also in terms of effort and manpower) might increase due to the regulation, which in most of the EU countries, does not impose specific obligations for the CSP to provide the data needed for the investigations.

4. Conclusions

In concluding this paper, we present recommendations based on evidence collected and on the challenges presented above. These recommendations can enforce cloud security and the process of cloud forensics analysis. To align them with the challenges these recommendations are classified in technical, organisational or legal; keep in mind however that one recommendation might be able to satisfy more than one challenge or on the other hand that one challenge might need a combination of recommendations to reach an adequate solution.

Technical

For Cloud Service Providers

- Solving the issues deriving from the multi-tenant nature of the cloud model, CSP could provide specific tools to enable access and guarantee access control from and for other tenants.
- CSPs need to adopt and implement efficient mechanisms for the retrieval of data, for backups and to implement a data retention policy.
- Specific training activities focused in forensic analysis of cloud incidents as an essential element to support the effective execution of investigations and cloud forensics should be widely promoted within a CSP. This can extend also to the organisational dimension.

For law enforcement agencies and policy makers

- LEAs and policy makers should develop or use specific certified tools to support the activities of the forensics analysis.

- LEAs and policy makers should support the development of standard procedures and guidelines on forensics analysis, that will facilitate the presentation of the evidence in a jury as robust proof of a methodical and certified process of acquisition of data in such a complex environment as that of the cloud;

- LEAs should invest more on education and training on specific tools and methodologies, create common bodies of knowledge and conduct exercises and scenarios (to test also collaboration between stakeholders involved). Specifically, training requirements for CERTs and investigators professionals (that should have the ability to understand technical challenges of the cloud and grasp the specificities of the business model is essential) could be fulfilled with vertical training actions on the specific aspects of cloud technologies.

Organisational

For Cloud Service Providers

- CSP should identify and indicate a “point of contact” for the forensic investigations (responsible for execution of the activities to be realized by the CSP in order to support and assist the forensic investigation activities, main reference for the customer in case an incidents happens and forensics activities are about to begin);
- The CSP should enhance collaboration with LEAs and other public institutions to formulate the procedure in conducting forensic analysis in case of cloud incidents. This should explain under which circumstances and following which procedure CSP can enable the forensics investigation.

For law enforcement agencies and policy makers

- Policy makers should identify and define specific policies and guidelines for Security Operations Centres at EU level to achieve incident notification and incident collaborative resolution.

- Rules and procedures should be proposed at EU level to facilitate the cooperation between the different actors (CSP, customers, third parties that might all belong to different countries each with its own regulation) and law enforcement EU bodies.
- Forensic investigation should be part of the national cyber security exercises and part of the national SOPs.

Legal

For Cloud Service Providers

- As per the SLA or contract, the CSP should ensure quick and dependable access to the information/data needed at any time during the investigation through specific and documented procedures.

For law enforcement agencies and policy makers

- Transnational agreements and/or procedures to regulate the multi-jurisdiction investigation would support a quick and correct execution of activities during the forensic process.
- Chain of custody challenges should be resolved at a national level through specific guidelines created by the policy makers (this should be covered also in the case of cross national cases).

Acknowledgments

We would like to thank the experts who participated in the interviews[12] and provided their expertise and useful comments on earlier drafts of this document: Neha Thethi (BH Consuilting), Cosimo Anglano (UNIUPO), Ludo Block (Grant Thornton NL), Jose Manas (UPM), Raj Samani (McAfee), Olivier Caleff (ANSSI), Toomas Lepik (CERT-EE), Hellenic Academia (UNIPI).

Special thanks for the contribution to Lauri Palkmets (ENISA) and Alexandros Zacharis (ENISA).

This work has been done in collaboration with CNIT (under the ENISA tender F-COD-13-C24), and in particular with the experts Maria Cristina Brugnoli, Federico Morabito, Emiliano Casalicchio and Giuseppe Bianchi.

Authors

Dimitra Liveri, Christina Skouloudi

Contact

For contacting the authors please email to resilience@enisa.europa.eu

For media enquires about this paper, please email to press@enisa.europa.eu.

12 The interviews have been conducted online after the consent of the participants.