DOI: 10.5769/C2013003 or http://dx.doi.org/10.5769/C2013003

Cloud Forensics
BEST PRACTICE AND CHALLENGES FOR PROCESS EFFICIENCY OF INVESTIGATIONS AND DIGITAL FORENSICS

José Antonio Maurilio Milagre de Oliveira
Diretor
Legaltech
São Paulo, Brazil
jose.milagre@legaltech.com.br

Marcelo Beltrão Caiado
Chefe da Divisão de Segurança da Informação
Procuradoria Geral da República
Brasília, Brazil
MarceloBC@pgr.mpf.gov.br

Abstract—**Digital forensics is a relative new science that has many challenges to overcome. This has been especially true since the huge adoption of cloud computing, which has its own characteristics, and the fact that many companies and providers are not well prepared to respond an incident in a proper manner. This paper discusses most common assumptions and principles, and proposes a base process for digital forensics in cloud computing.**

Keywords: cloud computing, cloud forensics, digital forensics, procedures, information security.

I. Introduction

There is no doubt that cloud computing is a phenomenon that tends to change the way of delivering services in Information Technology (IT) and Communication. Since 2009, the U.S. Federal Government has announced measures to implement a massive and complex infrastructure with the launch of Apps.gov, an online storefront for cloud services [1].

In Europe, cloud computing is expected to generate 800,000 jobs. In Brazil, it is noted the advance of the Federal Government with public services, which outlines a strategic plan to drive the adoption of cloud services in the country in a program called "TI Maior", presented by the Ministry of Science, Technology and Innovation [2]. The program discusses issues regarding development, regulatory framework and also aspects related to information security as well.

According to a *Kelton Research* survey [3], 74% percent of companies are already using some cloud computing service. Flexibility, IT environment simplification and costs reduction, are just some of the reasons.

On the other hand, there are no doubts that the growth of technology can also carry risks, involving fraud, incidents and electronic crimes. A survey by *CipherCloud* [4] conducted during the cloud-focused Dreamforce event in San Francisco that drew more than 48,000 attendees, shows that among the biggest concerns of companies, when choosing technologies in the cloud, are data security (66%), data privacy (56%), compliance (34%) and data residency (26%).

In this scenario, it is necessary to devise a process of investigation and digital expertise to be effective and that respects the characteristics of business models involving cloud services and especially in accordance with the legislation or applicable international laws. This is the challenge, considering the characteristics of cloud computing that relativize to the extreme the standards and practices adopted in Computer Forensics.

Put together to the challenge a poor doctrine applied to the subject. Among the first papers that keep a relationship with Computer Forensics and problems in cloud environments, there are the ones published by Wolthusen [5], and by Bebee [6] which proves the need to address these issues urgently, considering the astonishing development of technology.

This paper, showing some of the challenges discussed in the international community, has its bedrock on the design of a proposal for the investigation process and digital forensics in cloud environments. It also presents assumptions, principles and practices to be observed in such expertise areas.

II. Planning Information Security in Cloud Forensics

The success of digital forensics in cloud environments is closely linked with information security planning.

Speculations on information security in cloud environments are increasing, from risk analysis to implementations of controls to ensure security metrics are met.

In fact, some of the worrying foreseeable risks in cloud environments that must be included in a risk assessment for a possible implementation or migration are:

1. Improper access to information: Any form of unauthorized access to sensitive or classified information as confidential;
2. Information leakage: The disclosure of communications, data and trade secrets; and
3. Unavailability of services: Attacks targeted to the structure of cloud computing, which somehow disturb or interrupt the service.

A. Which Elements of Tracking Will be Generated

An important aspect to conjecture is related to the systems auditability. In this context, stakeholders should establish metrics, periodicity, scope and format of logs and other records to be created and maintained.

The adoption of an interface to access data records is also critical, mainly in SaaS service facilities, wherein the customer access to records and physical information is more limited. It may also agree upon a forensic API contract, which allows the actual client to initiate the first response.

Finally, it is important that the CSP (Cloud Service Provider) be obliged to inform the customer in cases involving incidents or attempts immediately and with complete documentation about the incident.

B. Human Resources for Forensics Responses

Forensics responses should be predict in agreements between CSPs and customers, especially detailing the procedure, in which case the answer must be forensic imprint and above of all, indicating internal staff as well as contractors or independent third parties that could follow the examinations. There must be a staff of suitable professionals, incident responders and legal body, which must be in the service level agreement (SLA) and in the contract.

1) How to deal with cloud computing

It may be that physical access to the affected device is thousands of miles away from the client, which is why it is important, in the contract, to establish where, physically, the customer wants their data to be, choosing a location with greater forensic maturity and more suitable legislation.

2) Consolidated standards

When detailing the procedure that the human resources will perform, it is essential the adoption of consolidated standards in the community, among which we can mention:

- SAS 70 certification;
- RFC 3227: Guidelines for Collection and evidence Archiving;
- NIST SP 800 86: Guide to Integrate into Techniques Forensic Incident Response;
- ISO / IEC 27037: Guidelines for identification, collection, acquisition, and preservation of digital evidence;
- ISO / IEC 27041: Guidelines for the analysis and interpretation of digital evidence (DRAFT); and
- ISO / IEC 27043: Digital evidence investigation principles and processes (DRAFT).

C. Cooperation in Multi-jurisdiction Cases

The Safety Plan must be designed by knowing how the customers data physical division is performed, considering legal aspects and privacy of each cloud shadow, detailing clearly contacts of response teams and details of the legislation of the countries in cases of incidents.

This preliminary step is critical to the success of any forensic analysis, because in case of any incident, the expert must make the data segregation, which is not an easy task, without having the minimum information. It is important to mention that the cloud provider must present the customer and determine the liability of third parties which are also used to provide the service.

It is therefore confirmed that CSPs and customers need to establish forensic capabilities so that we can reduce the information security related risks in cloud environments.

Best Practices for cloud computing security should be observed when designing, hiring, establishing metrics and service levels across multiple CSPs and customers.

Internationally, the Cloud Security Alliance (CSA), has a good practice guide for information security implementation in cloud environment [7]. Likewise, the European Network and Information Security Agency also has important recommendations on the subject [8].

III. Digital Investigations In Cloud Forensics

A forensic response process to incidents regarding cloud computing should be provided in the Security Management System and agreed with service providers and everyone in the supply chain, considering the maturity of the implemented security as well. There is no doubt that the success of a forensic response process is closely linked with the maturity of information security applied to the cloud structure and especially the willingness of such service providers. Rarely, in an investigation of this nature, there will be the traditional and classic option to seize the equipment.

The digital forensics is an area for identification, preservation, collection and analysis of digital evidence and artifacts (those, when relevant to the case), in the scope of presenting the materiality of an incident (showing whether the event actually happened or not) and mainly by indicating

the source of the incident. This is a science in its infancy, with few more than ten years of groundbreaking research.

Among the fronts of digital forensics, we can identify the *post-mortem,* where analysis have addressed commonly content of discs, recovery, carving, e-discovery, among others, and the live one, which seeks volatile content such as memory, kernel, processes, network states, data that is totally or partially impaired with the shutdown of the equipment.

Nonetheless, cloud computing has elasticity as one of its essential characteristics. The term elasticity refers to the idea of an environment that can be easily extended, according to customer demand.

Cloud forensics, in this context, would be one of the specializations of Digital Forensics, target to the analysis of cloud environments, involving investigations related to incidents, fraud and computer crimes. To Keyun Ruan [9], from the Centre for Cybercrime Investigation, of University College Dublin, cloud forensics would be linked to network forensics, which in turn would be linked to digital forensics. To the authors network forensics techniques could be tailored to cloud computing environments.

Nonetheless, access to data on disk (raw) or snapshot structures will often be essential for understanding what happened to the compromised system, given the elasticity of the cloud service models. We also cannot fail to conjecture the intimate connection with Database Forensics, as sometimes the expert must act in this instance, seeking records from unauthorized modifications of data stored in the cloud.

When we think of cloud, we imagine a model, on demand, in which access is allowed to a shared pool of configurable resources, including but not limited to networks, servers, storage, applications and services. For the forensic expert, initially it will be mandatory in the identification phase, to determinate if it is really a cloud environment or any other form of web service, or even a VPS or VPN. A mistake in the identification of the service, will certainly lead to investigations failure, which may violate standards and best practices.

From the perspective of Computer Forensics, virtualization services on a single physical server brought several points and questions to be addressed by the research community. The ease of deleting data has always been one of the issues pertaining to virtualization. On the other hand, it may be stated that the cloning bitstream (physical) would be facilitated by copying the file that represents the virtual disk.

With cloud computing, we have other issues to be considered. While the cloud become an object of studies by hackers and crackers, in its various instances, from the hypervisor (which manages the resources for virtual machines) to the interface layers, there is also concern about the use of public and private cloud providers as anti-forensic technique. Criminals could be using this technique for improperly accessing virtual spaces, practicing crimes or hosting shells, botnets, access to resources for deep-web, trojans among others. As an example, the Pirate Bay is operating from cloud-hosting providers around the world to escape from authorities [10].

By the other hand, there is the concept of *data abundance* involving artifacts, where screening sample techniques need to be applied to prevent that the forensic never ends.

In this context, the digital investigator must bear in mind that the cloud within the practice of computer incident may be used as:

- Object: When the virtual server in the cloud is the target of cybercriminals, being directly attacked, such as in a denial of service;
- Environment: When the cloud is the environment in which a digital crime is committed, such as unauthorized modification or deletion of data;
- Weapon: When the cloud is one of the tools used to commit crimes or stores digital planning or artifacts that might lead authorship of a possible computer crime. This context is also when cloud is used as anti-forensic technique for stealth connection or attribution of authorship to an innocent person, or even the use of botnets;

In above cases, sometimes customers and cloud providers are at litigation, where an expert will be appointed to evaluate eventual failure in service delivery, which might has generated losses or accountabilities.

Still, it should be noted that forensic investigations in cloud environments will take place in the following interesting prospects:

- Research: Full investigation of violations of law and policy, or even suspicious transactions, rebuilding events and collaborating with authorities and sponsors of expertise in collecting and analyzing evidence; Using from network techniques such as packet capture techniques to disk (dead) capture, and data recovery, encrypted and using stenography;
- Prevention: Through the log monitoring, event correlation and anticipation of supposed incidents; Working in conjunction with the incident response team;
- Compliance: Helping companies and organizations meet the requirements and best practices involving security and response to incidents involving cloud computing;

According to [11], a good research method should always consider different sources of evidence, not only the provider but also the customer terminals, using methods like data fusions for collection and data correlation.

IV. Cloud Forensics Principles

Although there are much disagreement in regard to assumptions, principles and practices for investigative analysis in the clouds, some assumptions have been consolidated in the international community researchers. Those assumptions are features that need to be considered always in such analyzes. We present some of the most important ones.

A. Consider the Technical, Organizational and Legal Dimensions

Before starting to work on a cloud environment, the expert should divide the initial design of the project in three dimensions: the technical, which will map the entire structure to be analyzed; the organizational, where he will understand the business model, service features, and will map the called dependency chain and human structure for incident response and customer service; the legal, which he will assess the legal issues related to data and to orient the computer examination as evidence acceptance in court, establishing the chain of custody, among others.

B. Consider the Logical and Physical Dimensions

The expert must completely review the structure, in each forensic analysis, understanding the physical dimension that hosts the logical area of the client, and mainly identify which are the physical and logical constraints to access the assets. Seldom, in an examination in such environments, the expert will have full access to the physical dimension, whereas this dimension is considered by many providers their business secret.

C. It Might not Exist Media Control and Access to Physical Infrastructure

The principles, frameworks and best practices are usually based on the assumption that the storage media is always in investigator's control. This changes with cloud computing. Some concepts brought by the principles of the Association of Chief Police Officer (ACPO) of England, and Investigative Process Model (Dip Model) from Digital Forensics Research Conference (DFRS), are put in check when the environment is in the cloud. It must be noted that these frameworks are well regarded by the community in digital investigations.

The non-physical infrastructure must also be characteristics of multi-tenants and multi-ownerships clouds, where information can be stored in different asset owners or where a single physical disk can concentrate data from numerous other clients. In case of access, one could think of privacy violation.

D. Elastic Tools, Elastic Cloud

The community should look for tools that fit the elasticity of the cloud.

E. Provider Cooperation is Essential

Despite some models of services in the cloud facilitate customer access to information and metadata, it is also known that it is virtually impossible to perform an examination in cloud environment without any cooperation.

V. Proposed Process for Cloud Forensics

A process for responding to incidents involving forensic cloud computing should be provided in the Security Management System and agreed with service providers and third parties in the chain of dependence, including the possibility of simulations.

Digital forensics has not been seen as an easy task in cloud computing devices. According to Gartner: "cloud services are especially difficult to investigate, because data access and data from multiple users can be located in several places, spread across a number of servers that change all time” [12].

Starting from the assumption that the company already knows the risks involved in a cloud environment, we have to define a process for the forensic response time, which not only restore services but mainly produces scathing evidence of what occurred in a system, and can be considered in court. Among the steps we propose for an investigation and digital forensics in a cloud environment, there are:

A. Map Technical, Organizational and Legal Dimensions

This is the first step, i.e., before the expert establish an effective plan for forensic analysis, one should divide the assessment into three tabs, and in it, sort and collect all available information, contacts, norms and rules.

At this stage it is important that the expert consider the following, as it will give needed information to advance in the examination:

1. Review the contract, SLA and Security Policy; (cases involving cessation activities, deletion or exclusion, any zero knowledge encryption system, cooperation with authorities), among others; and
2. Assess whether cloud computing characteristics are present (or if we are dealing with other similar services)

As stated by [13], the back-end is generally a three-tier arrangement, comprising: physical machines and storage, virtual machines and a SLA layer (Figure 1). The SLA is responsible for the monitoring of the service contract to ensure

its fulfillment in real-time. All layers should be considered by any expert when evaluating the service contract.

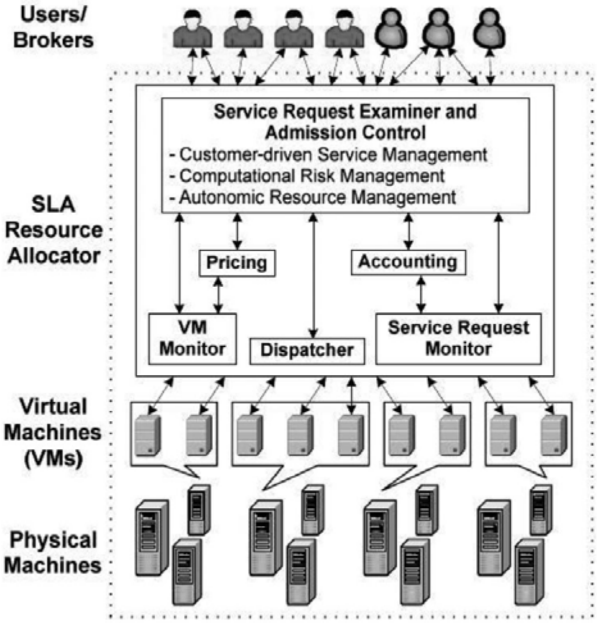
Users/ Brokers
SLA Resource Allocator
Service Request Examiner and Admission Control
- Customer-driven Service Management
- Computational Risk Management
- Autonomic Resource Management
Pricing
Accounting
VM Monitor
Dispatcher
Service Request Monitor
Virtual Machines (VMs)
Physical Machines

Figure 1: Cloud Computing Layers [13]

The expert must also evaluate organizational configuration or development platform models, which may be:

1. Private Cloud: Infrastructure is operated only by the organization that owns the cloud.;
2. Community Cloud: The cloud is shared by many organizations, because they have a common goal, and is administered by the community;
3. Public Cloud: It contains information from more than one user / customer, maintained by a organization provider; and
4. Hybrid Cloud: Composition involving two or more models, also called *virtual private cloud*. Sometimes used for load balancing in different clouds.

For digital forensics it is important to know the ways of configuring a cloud service, since this will directly impact on the path of data that can be collected as evidence. It should be noted that data stored in the cloud can be stored in one or more distributed physical locations, making the determination as to which law should be enforced or even the procedure and framework applied. This is a complicated issue and that needs to be addressed by the expert.

In addition to the organizational setting, the expert should evaluate the service model supplied by the provider being analyzed. As it is known, there are three basic levels of services involving cloud computing models, namely:

1. SaaS (Software as a Service), where the client can use applications available by the provider cloud, and the interaction is commonly done through web-browsers. As an example, there is the Google Apps suite of applications;
2. PaaS (Platform as a Service), where there is the availability of an application programming interface (API) so that customers can create and host applications. Commonly there is the provision of a development platform; and
3. IaaS (Infrastructure as a Service), which is the assignment of virtualized computing resources such as processing power, memory and storage.

It is critical to identify the service model so that we can prepare the process of digital forensics, considering the variants of each service. The collection is directly influenced by the models of service delivery. In IaaS-based platforms, there is more interaction between the client and platform, which will result on a greater possibility of collecting data for forensic examination, that may not occur in PaaS and SaaS models. Typically, on SaaS and PaaS platforms the expert will not have control of the hypervisor, which would be very important in an investigation.

Another advantage of investigating IaaS environments is related to the fact that in such a model, it is usually possible to make a snapshot analysis, supported by all popular hypervisors like Xen, VMware ESX and Hyper-V. Furthermore, processes need not to be interrupted for forensic analysis, generating no downtime or SLA violations.

On the other hand, the ideal is that SaaS and PaaS interfaces offer or implement an additional interface with the purpose of compliance and forensics. Through the API, clients should receive information about events in their environments [14]. Another alternative may be the compression and encryption of logs that could be sent to third-party servers, preventing the possibility of a shutdown or volatile data destruction.

B. Identify Outlining Stages of Computer Forensics that Will be Overcome and Correlate Them to the Propositions

In this phase the expert will create tabs in his project with all phases of Computer Forensics: a) Identification, b) Preservation, c) Collection, d) Examination, e) Analysis f) Presentation. Within these tabs, he must employ assumptions that are consensus in the research community, as discussed in Part 3 of this work. We must recall that the expert should always be updated with new assumptions, principles and rules.

C. Identify Outlining Stages of Computer Forensics and Propositions with Technical, Organizational and Legal Results

At this point, we propose a data fusion. The expert will merge Computer Forensics phases, given the assumptions related to an examination of this nature, with the result of the mapping of technical, organizational and legal frameworks applied to the case. The result will be a matrix, where the researcher will have assumptions, data and characteristics to be examined at each stage of the forensic examination.

Having this information, the expert can then devise the best strategy for forensic investigation, beginning the execution of his expert activity. Among the criteria that will emerge and that will guide the work, we list:

1) Identification

The detection of an incident in a cloud environment may differ according to the model adopted for the services. The adoption of cloud in Intrusion detection systems can be implemented by the user in the IaaS or even by the CSP in cases involving SaaS or PaaS. At this time the expert will interact with the professional´s provider for mapping the incident and the extent of damage. It will be identified which access the provider offers to the customer in the event of an investigation. Also, it will be identified if the provider is performing regular snapshots or even object auditing and multiple backups.

2) Preservation

The preservation of evidence in cloud environments is not so peaceful. Implementing preservation techniques may require isolating cloud resources, which can cause performance degradation for other clients. From the best practices, providers should isolate the physical disk connected to an incident. The problem is that data from other customers that share resources could also be copied.

Under the existing frameworks, identifying electronic stored information, commonly sets up procedures considering that the evidence is in the possession of the investigator. In cloud, the providers are in custody of such information. Client control is more difficult. The client can indeed control his data, but do not always have access to the metadata server he uses, and which are fundamental in a computer investigation.

Another issue that needs to be revised in the process of preservation is the chain of custody. In SaaS or PaaS models the customer may not be the first to have contact with the evidence, then the provider shall be responsible for this preservation task, involving the allocation of knowledgeable first responders.

In the conventional model, the chain of custody must start when the researcher has access to physical media. For companies, the challenge remains to implement contracts that allow the investigator access to the evidence, sometimes in a physical way, and not just with network access, or even a chain of custody that begins with the provider and then is transferred to the client.

3) Collection

The challenge of collecting is to have access to data. The investigator may have access to data, or copy over the network, or rely on the CSP team. The evidence collection in cloud environments proposes new challenges to experts, especially due to the lack of tools to assist them with agility. It should initially be pointed out the challenge to the expert who will handle increasing amounts of data, with the storage capacity growth and low cost of such devices. An investigation in a virtualized environment can become extremely costly in the collection phase, due to the existing devices. The elasticity (involving the ability to scale capacity according to the requirements), which is characteristic of the cloud, increases this problem.

One way to minimize this fact is to use screening models, as the model called Screening (CFFTPM) [15] a framework that has been growing among the research community worldwide (Figure 2).

The collection also will deal with the following questions:

1. Multi-jurisdiction: Data can be stored in physical locations with different jurisdictions. One must respect the jurisdiction of where the data resides;
2. Limited access to physical media: For legal or even business strategy, the expert may have limited access to media, needing a further court order;
3. Dead Forensics or Live Forensics: The memory capture and other states might be limited to an interface available to the customer. Similarly, it is virtually impossible to shutdown a machine to remove the disc or boot via live CD, common practices in traditional digital forensics. The expert should establish remote collection strategies.

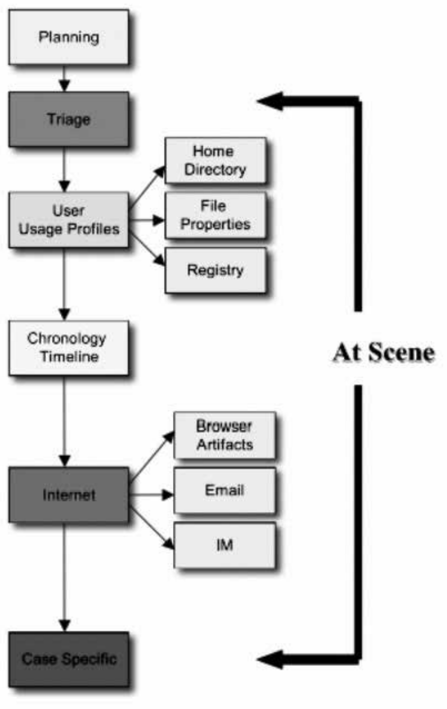

Figure 2: CFFTPM Phases

Commonly, the expert would be performing the imaging of the disc, through duplication bitstream equipment or a command like dd. This changes in cloud, where an interface apparently on a single disk is divided into multiple physical disks. The challenge for the expert is to know each

segment that composes the target and are interesting for the investigation, cloning the devices (defining the start and end clusters) and then have the capability to concatenate them in a investigation environment. Thus, the expert will have to deal with the concept of distributed multi-tenant. A good example of this is Google GFS [16].

It is mandatory for the contractors to predict, therefore, not only the logical access cloud interface, but also situations where physical access is essential. A proposal to collect data that proportionally respects neighbors in the clouds should be among the team's Cloud Service Provider and customers discussions.

If on one hand, cloud providers are striving to provide security to data in the clouds, on the other, such security involving encryption and data traffic can become an enemy in time of investigation involving cyber crimes. The implementation of *zero knowledge system*, a concept that allows all data to be encrypted before being sent to the clouds, may cripple an investigation. There will be the need of a covenant involving the exchange of keys, if the encryption is performed by the client, otherwise the provider should be legally liable. A negative example comes from Google, that to ensure the privacy of users, assures that when a user deletes their data, they are in fact deleted and the pointers of the replicators are also eliminated, which can be a challenge.

On the other hand, in the cloud, we can think about a certain persistence of data, which is an advantage, because unless the customer has administrative access, it becomes difficult to perform a complete deletion of data. Hence, it is important to know the persistence in the form of backups and other data provided by the CSP.

In this sense, the European Union encourages union members to apply the *Data Retention Directive* of 2006 [17], which in Article 5 stipulates communication providers to retain certain data about users, userid, allocated IP, time and date of the communication and time of login and logoff systems. The challenge is whether the legislation includes providers of cloud computing services. We will soon have the first legal signs on the topic.

A proposed solution to the problem of the constant inability of the expert to have physical contact with the evidence to be collected, can be called *organizational cooperation*, where the provider would be responsible for the extraction of forensic image of physical disk or partition, or at least virtual machine created for the client by handling the hypervisor. There should be exceptionally careful when handling the hypervisor, which can be compared to a kernel of the operating system. It will be usual for cloud providers to provide snapshots of the disk and client memory. Good practice recommends that this generation be documented and assisted by an expert for the customer, so it can be used as digital evidence in court. This approach will ensure that the hypervisor was reliable.

Important to remember, in these cases the researcher is not the first to have contact with the evidence and the chain of custody is created by the provider. It is clear and undisputed that cloud providers need to know the procedures of digital forensics, mainly relying on human resources prepared for such tasks.

Despite the cloud provider contract predicting the possibility of going to an expert for the collection of physical evidence, sometimes it would be needed someone from the provider to run the task. This is because we are dealing with different platforms, trade secrets, proprietary technologies, among other logistical issues that make it important that wherever possible the client's expert should be acting in conjunction or can follow the expert's provider in executions of tasks in operation.

It must be reminded that the legal limitation involving the location of each provider can compromise the legitimacy of the collected data.

It is, finally, another good practice to be implemented in providers, the automated generation of hashes of snapshots, dated, the virtual disks, as well as existing files, serving as a basis for comparison after the data is capture by the expert. The investigator then, at the stage of examination, must extract the hashes from snapshots computed by CSP after collection, and compare them by checking the matching.

Other important issues in the collection are:

1. In *live* collection, the expert should consider all endpoints, and the generation of the timeline of events should consider time synchronization, which is difficult and demands specific tools;
2. The expert must pay attention to the segregation of the evidence - collecting information logs from multiple clients can generate legal liability;
3. He should assess whether the system already has a solution to generate hash files from cloud, as well as if provides support for remote binary copy; and
4. The expert should evaluate if the system being examined offers versioning of erased or overwritten files / objects, and how it is possible to access these mirrors.

4) Examination and Analysis

The timestamping should be considered in the collection phase and also in the analysis phase. A knowledge process involving all jurisdictions should be adopted and timestamps applied to services. The community challenge is to design tools to automate this correlation.

Once the collection phase is overcome, by far one of the most problematic stages involving cloud environments, frameworks and practices for analysis can be applied to the analysis of computer artifacts. Many open source tools, data carving, pattern matching, and filtering are recommended, like The Coroners Toolkit, Foremost, Xplico, Autopsy, among others, contained in Linux Forensic distributions, can assist the expert work. Under proprietary software, EnCase and FTK should be considered. Dykstra and Sherman [18], performed one of the first research involving data collection tests in the cloud with tools like FTK and Encase, in an IaaS environment.

In investigations where network traffic packets were collected, Xplico or Wireshark filters can be used for session reconstruction and even content decoding.

The analysis of evidence in cases involving cloud is similar to analysis of evidence in digital forensics and may involve:

- Processes;
- Memory;
- Files;
- E-mails;
- Logs;
- Network traffic; and
- Web data.

Regarding the logs, it is the expert´s task to be familiar with the most used platforms, knowing the way they are generated, so he can use a parser efficiently, detailing his report in an effective way.

5) Presentation

In this proposal, the presentation phase may consist of legal appraisal or a simple briefing or draft of what happened. It can be used in legal form by a lawyer or even used by the expert for the defense of their findings in court. The forensic reports also work as an input in process improvement and continuous corporate improvement.

The four Daubert Principles [19] (guidelines for acceptance of scientific evidence) should be considered in the presentation of results involving investigations in cloud environment:

1. The key question is know whether the theory can be tested, namely the theory must be tamper-proof. The CSP must maintain evidence for the time agreed;
2. The results should be subject to review by other experts;
3. When applying a determined known technique, the Court must consider the potential rate of error, and the existence and maintenance of standards and controls on their operation; and
4. It should be rated the degree to which the theory and technique is generally accepted by the scientific community. In Computer Forensics this is a difficult task, considering that discussions on international best practices are just starting, which is critical to the advancement in the area.

Nonetheless, it is highly recommended that cloud Provider's technicians sign along the client´s expert report, ensuring uniformity of opinions and avoiding exploitation thesis as self defense on the argument that the provider was unaware or did not recognize what was performed by investigators.

VI. Conclusions and Future Works

There is no doubt that Computer Forensics in cloud environments is still embryonic and needs to become more mature to be able to equate the efficiency of an investigation with respect to privacy, fundamental rights and guarantees and SLAs between providers and other customers.

It is known that the frameworks, practices and principles, wide discussed and consolidated in the community of Computer Forensics, are not explained in their entirety or accuracy and must promptly be derived, revised and adapted in the design of a minimum standard that meets the concepts, service models and configurations of cloud computing.

Within the present work, a proposal for preliminary e-discovery processes and Computer Forensics was shown, involving cloud environments, not exhaustive and stony, which can be adapted to meet the changing technology and the characteristics of each cloud environment, besides of cases that may be presented.

While many challenges exist in digital research of cloud environments, it is true that the contractual relations are identified as one of the solutions to the problem, and there is urgent need for international regulations. The Computer Forensics must be provided in terms of services, ensuring rights and duties between clients and providers. This is a negotiation that should be made between the parties. Computing is a key element, considering that the elements of compliance in providing cloud services to grow. In Brazil the PL 5344/2013 [20], presented by Mr. Ruy Carneiro, wants to regulate the relationship between users and companies of this type of service.

An example that is worth to mention is the city of Los Angeles, who adopted an e-mail system to 30,000 employees in 2009, hiring Google services [21]. In this contract there are predictions that Google can fix the city in case the system is broken and city data exposed. On the other hand, the Gmail service offered to individual customers, allows Google to processes personal information on servers in the United States and other countries, which can be a deterrent in the face of an investigation involving such servers.

As it can be deduced, considering that bargaining power may be greater on small providers, an expert can find relevant information to an investigation more easily on these cases.

Some issues that can and should be contractually defined are: a) data collection amount and frequency, b) where the information will be stored, c) interface for access to data pertaining to the incident, d) ways that virtual disk images will be provided, e) hash format of the files, f) who handles the evidence on the side of the CSP, g) restrictions on certain datacenter storage locations, which contain no laws on privacy and security, or that do not cooperate in investigations, among other issues that can troubleshoot data spoliation or deterring investigations involving data in the cloud;

From the technical view providers may consider creating automated systems that collect and preserve ESI (Electronic Stored Information) pertaining to customers, for cases involving incidents. Other issues that must be considered in the technical side are: a) Ability to capture specific packages in relation to client servers b) Potential access to routers and other network components c) Segmented access to Firewall record; d) Access to the service hops, e) Creating an instance for log storage.

In this scenario, although not exhaustive, the first lines to design a model for process efficiency of investigations and digital forensic in the cloud were presented. They can be extended to model specific processes for each one of the different cloud computing technologies.

REFERENCES

[1] V. Kundra, "Streaming at 1:00: In the Cloud". The White House - Office of Social Innovation and Civic Participation. http://www.whitehouse.gov/blog/Streaming-at-100-In-the-Cloud), September 15, 2009.

[2] TI Maior – Programa estratégico de Software e Serviços de Tecnologia da Informação. http://timaior.mcti.gov.br/

[3] Kelton Research, "Global Survey: Has Cloud Computing Matured?". Third Annual Report, Executive Summary, Avanade Research & Insights (http://www.avanade.com/Documents/Research%20and%20Insights/FY11_Cloud_Exec_Summary), June 2011.

[4] CipherCloud, "Data security and privacy stopping cloud implementations", in press.

[5] S.D. Wolthusen, "Overcast: Forensic Discovery in Cloud Environments", In: Proceeding of the 5th International Conference on IT Security Incident Management and IT Forensics (IMF '09), Sttugart, pp. 3-9, 2009

[6] N. Beebe, "Digital Forensic Research: The Good, the Bad and the Unaddressed", In: G. Peterson and S. Shenoi (Eds.), Advances in Digital Forensics V, IFIP AICT 306, Springer, pp. 17-36, 2009.

[7] Cloud Security Alliance (CSA), "Security Guidance for Critical Areas of Focus In Cloud Computing v3.0", 2011.

[8] European Network and Information Security Agency (ENISA), "Cloud Computing - Benefits, risks and recommendations for information security", 2009.

[9] Keyun, R., Carthy, J., Kechadi, T., Crosbie, M. "Cloud Forensics", IN: G. Peterson and S. Shenoi (Eds.), Advances in Digital Forensics VII, 7th IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, January 31 – February, 2011, Revised Selected Papers, Spring, pp. 35-46, ISBN 978-642-24211-3, 2011.

[10] S. Anthony, The Pirate Bay moved for the cloud to evade police" (http://www.extremetech.com/computing/ 138037-the-pirate-bay-moves-to-the-cloud-to-evade-the-police), October, 2012.

[11] S. Satpathy, S. Pradhan and B. Ray, "Digital Investigation Tool Based on Data Fusion in Management of Cyber Security Systems", International Journal of Information Technology and Knowledge Management, July-December 2010, Volume 2, No. 2, pp. 561-565.

[12] Gartner Inc., "Cloud Computing – Key Initiative Overview", 2010.

[13] VIVEK School of ERP. Cloud Computing. http://acharyavivek.blog.co.in/2010/04/12/cloud-computing-2/, 2010.

[14] D. Birk, C. Wegener, "Technical Issues of Forensic Investigations in Computing Environments", IEEE/SADFE 2011, 6th International Workshop on Systematic Approaches to Digital Forensic Engineering (in conjunction with IEEE Security and Privacy Symposium), Oakland, CA, USA, 2011

[15] M. Rogers, J. Goldman, R. Mislan, T. Wedge, "Computer Forensics Field Triage Process Model", Conference on Digital Forensics, Security and Law, 2006.

[16] S. Ghemawat, H. Gobioff, S. Leung, "The Google File System", 19th ACM Symposium on Operating Systems Principles, Lake George, NY, October, 2003.

[17] Directive 2006/24/EC of the European Parliament and the Council, 15 March 2006.

[18] J. Dykstra, A. Sherman, "Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and Evaluating Tools, Trust and Techniques", Digital Investigation 9:S90—S98, 2012.

[19] S. Richard P. In: "FOR 508 Advanced Computer Forensic Analysis and Incident Response, workbook day 5 - Computer Crime US", SANS Institute, May, 2010.

[20] Projeto de Lei 5344/2013. http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=570970

[21] S. David, "Los Angeles Adopts Google Email System for 30,000 City Employees" (http://latimesblogs.latimes.com/technology/2009,10/city-council-votes-to-adopt-google-email-system-for-30000-city-employees), September, 2009.