# A case study on digital forensics in the cloud

Fabio Marturana
Computer Science, Systems and Production Dept.
University of Rome "Tor Vergata", Italy
marturana@libero.it

Gianluigi Me
Computer Science, Systems and Production Dept.
University of Rome "Tor Vergata", Italy
me@disp.uniroma2.it

Simone Tacconi
Postal and Communications Police
Ministry of the Interior, Italy
simone.tacconi@interno.it

*Abstract*— **Cloud computing and cloud forensics are probably the two most popular and debated IT topics in recent years, implying relevant technological and economic opportunities, the former, and open issues such as the ability to perform digital investigations in the cloud, the latter. In cloud forensics, the distributed nature of data processing in the cloud and the lack of physical access to digital artifacts on the server side represent, indeed, a serious concern for investigators and stakeholders, as traditional approaches to evidence collection and recovery may be no longer applicable. In this paper we discuss technical aspects of digital forensics in cloud computing environments and present results of a case study about user-cloud interaction, aimed at assessing whether existing digital forensics techniques are still applicable to cloud investigations. We conclude proposing a new methodology for automatic cloud-based artifact categorization as a future work.**

***Keywords: cloud computing, digital forensics, cloud forensics, SaaS applications***

## I. Introduction

Cloud computing and the pervasiveness of the Internet are radically changing the way how information technology services are created, delivered, accessed and managed. This new service delivery paradigm has the potential to become one of the most transformative developments in the history of computing, following the footsteps of mainframes, minicomputers, PCs (Personal Computers), and smartphones [1]. The National Institute of Standard and Technology (NIST) has defined cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [2].

Cloud computing can be used for a wide variety of tasks such as sharing documents, photos and files, synchronizing calendars, and contact lists and providing access to programs such as photo editing tools and word processors on devices with limited RAM, CPU and storage capacity. Other benefits offered by cloud paradigm include: greater data security and availability (i.e. the theft of a device leaves the data still available in the cloud), logical security as software patches are applied by the Cloud Service Provider (CSP) and lower storage and processing hardware costs [3].

### *A. Technical background*

Digital forensics is the application of scientifically derived and proven methods aiming at preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence extracted from high-tech devices, maintaining a documented chain of evidence, for presentation in courts [4]. Digital forensics is thus considered the main framework of methodologies and tools available to investigate digital artifacts.

A definition of cloud forensics is provided in [5] where it is defined as a cross-discipline between cloud computing and digital forensics. Cloud forensics is associated with a multi-dimensional model with *organizational*, *legal* and *technical implications*. The *technical dimension* involves a set of tools and procedures to carry out the forensic process in cloud computing environments; The *organizational dimension* recommends to define a structure of internal staffing, provider-customer collaboration, and external assistance fulfilling the specific incident response roles; The *legal dimension* deals with regulations and agreements which have to be developed to secure that forensic activities will not breach any laws or regulations under any jurisdictions where the data resides in, throughout the investigation [5].

Fundamental cloud computing characteristics are: broad network access, rapid elasticity, measured service, on demand self-service and resource pooling. Cloud architecture relies mainly on three core technologies: web applications and web services, virtualization, and cryptography. According to the aforementioned NIST definition [2], services in the cloud are provided according to the following basic models: *Infrastructure as a Service (IaaS)*, *Platform as a Service (PaaS)* and *Software as a Service (SaaS)*. In particular, with *IaaS* an entire operating system, applications, and storage are remotely available to users whereas, with *PaaS*, users are assigned the tools to build and host web

978-0-7695-4810-4/12 $26.00 © 2012 IEEE
DOI 10.1109/CyberC.2012.26

IEEE computer society

applications on a remote machine, and with *SaaS* turn-key applications and data based on a remote machine are made available to users [6], [7].

The NIST introduces, further, four possible cloud deployment models: *Public*, *Private*, *Hybrid* and *Community* cloud [2]. Being available on the cloud and regardless of the device used, a pool of available resources such as applications, processes and services can be rapidly deployed, scaled and provisioned, on demand. As a consequence, cloud computing enables tasks formerly carried out by well-rounded computers and servers to be performed on a pocket device such as a smartphone.

### *B. Motivation*

Since cloud computing appears to be an emerging challenge to digital investigations, it is crucial to understand the impact that the cloud will have on forensic tasks and how existing techniques, tools and methodologies would cope in cloud scenarios. As a consequence, being the emerging field of cloud forensics in its infancy, an urgent need is arising to define new methods and related tools that can be used to conduct digital investigations in cloud environments.

Motivated by the aim of understanding opportunities and limitations of traditional digital forensics techniques applied to the cloud, we have built a case study based on a set of popular *SaaS* cloud applications, to see if captured IP packets and traces found on the local device, extracted with openly available forensic tools, where sufficient to prosecute the offender in court. We excluded in advance the option of making a request to seize a cloud server in the foreign jurisdiction as it is a time consuming activity, with limited added value from a technical standpoint.

### *C. Paper outline*

The outline of the remainder of the paper is as follows: we mention the challenges of cloud computing in Section II and describe the outline of the conducted case study in Section III, discussing relevant results in Section IV. We finally draw the conclusion of our research in Section V and suggest possible future research scenarios in Section VI.

## II. Challenges of cloud computing

Recently the spread of high-tech and cybercrimes related to the diffusion of cloud computing, where everything runs virtualized in a variety of geographically distributed data centers, has led to significant changes in traditional digital investigations. Malware and botnets are often delivered “as a service” to criminal start-up organizations at a very low cost, according to a *“Crimeware-as-a-Service”* paradigm. Cybercriminals and terrorists are likely to take advantage of any new technology to commit crimes. Cloud computing technology can be used, indeed, to propagate a terrorist ideology, disseminate information, facilitate communication, or for an attack against computer systems and networks.

Further, cloud computing may be even considered an anti-forensic strategy carried out by criminals to hide themselves and to confuse, hinder, delay or even stop investigations as evidentiary material could be distributed over several servers in different geographic locations and in a multi-jurisdiction and multi-tenancy environment which can be provisioned and unallocated in minutes.

In this regards, cloud services may be especially difficult to investigate, because logging and data for multiple customers data may be co-located and spread across an ever-changing set of hosts and data centers, as Gartner states.

From an investigator standpoint, moreover, one of the main problems of cloud forensics is that users are less likely to store local copies of documents on the hard drives of their computers and other electronic devices, given the security, synchronizing, and sharing benefits offered by the cloud. Interaction with remote documents is normally made through a web browser doing away with the need to have a word processor installed on the local device, as many devices aimed at interacting with cloud networks have no local hard drive. As a consequence, in a cloud environment, investigators are likely to find scarce evidentiary material by analyzing local artifacts with traditional digital forensics.

Another important challenge of the cloud, experienced by investigators during incident handling, is the lack of physical access to the cloud servers, which narrows the windows of possible investigative solutions to the following three options: to try to recover data fragments from seized local devices known to have interacted with the cloud, to try to eavesdrop network traffic between local devices and the cloud network or to make a request to a court in the foreign jurisdiction to seize evidence directly from the cloud server. In the latter case, law enforcement should employ official channels to acquire the original data on the cloud server issuing a formal request to the relevant court in the foreign jurisdiction, with a long wait time before acquisition of the original data could be undertaken. During this period the cloud account owner may have securely deleted all evidentiary material and overwritten it to permanently delete the data. By analyzing client devices, on the other hand, it depends on the used model (e.g. *IaaS, PaaS, SaaS*) if and where potential evidence could be extracted. With regards to *SaaS* applications, indeed, a Web browser on the client side may be the only application that communicates with the service in the cloud. Hence, in an exhaustive forensic investigation, evidentiary material gathered from the browser environment should be taken into great consideration [7].

## III. Case Study Outline

In this paper we have built a case study, designed according to cloud working principles, to show that, searching local artifacts, it is possible to find interesting evidentiary material about the user-CSP interaction. In this regards, we have selected and analyzed document editing and photo sharing *SaaS* applications, such as *Google Documents, Flickr and PicasaWeb*, to demonstrate that potential evidence may be found in logs and temporary files, internet cache, navigation history, downloads and cookies of the Web browsers.

We have also analyzed *Dropbox*, a popular file sharing *SaaS* application which may work both as a Web based cloud application, as *Google Documents, Flickr and PicasaWeb*, or as a traditional, locally installed software which stores a copy of the server data in a synched local folder when users interact with the cloud servers. In the latter case, if an Internet connection is available, *Dropbox* connects to the cloud to check for file updates and change the local copy accordingly to ensure that it reflects the current state of the server data and vice versa. It is possible, thus, to acquire a copy of data as it exists in the cloud by simply retrieving data or fragments from local hard drives and without the need to access the server directly.

In this regards, we engineered five test scenarios, numbered from 1 to 5, whose preliminary steps were establishing a connection with the cloud service and creating a user account. In each scenario, we performed the tests listed below, each labeled with a unique sequence number and a description of the performed action:

*Scenario 1 - Dropbox accessed via Web browser:*

- Test 1.1: logging on www.dropbox.com,
- Test 1.2: uploading a word document,
- Test 1.3: opening or downloading a word document,
- Test 1.4: deleting a word document.

*Scenario* 2 - *Google Documents accessed via Web browser:*

- Test 2.1: logging on docs.google.com,
- Test 2.2: creating a word document,
- Test 2.3: uploading a word document,
- Test 2.4: opening a word document,
- Test 2.5: deleting a word document.

*Scenario 3 - PicasaWeb accessed via Web browser:*

- Test 3.1: logging on picasaweb.google.com,
- Test 3.2: uploading an image file,
- Test 3.3: opening an image file,
- Test 3.4: deleting an image file.

*Scenario 4 - Flickr accessed via Web browser:*

- Test 4.1: logging on flickr.com,
- Test 4.2: uploading an image file,
- Test 4.3: opening an image file,
- Test 4.4: deleting an image file.

*Scenario 5 - Dropbox client installation with local synched folder:*

- Test 5.1: installing Dropbox client software on the local hard drive,
- Test 5.2: saving a file in the Dropbox local folder,
- Test 5.3: opening a file in the Dropbox local folder,
- Test 5.4: deleting a file in the Dropbox local folder.

In scenarios 1 to 4, in particular, we tested the cloud services against the three most popular Web browsers (i.e. *MS Internet Explorer, Mozilla Firefox and Google Chrome*) on the client side. We recorded and analyzed the browser activity (i.e. cache, cookies, navigation history and downloads) and captured the network traffic accordingly, to recover data fragments of the interaction between the local device and the cloud.

Finally, in the last scenario, we tested the *Dropbox* service against a set of traditional forensics tools to verify its presence in the list of installed programs or in the process list and to find evidentiary material in the local file system by analyzing the file access timeline, the list of deleted or recently accessed files etc..

All tests were performed twice, the former using *live* forensics tools on a powered on laptop computer running *Windows 7 Home Edition 64 bit* and the latter with *post mortem* forensics tools on a physical image of its hard disk.

With regards to scenarios 1 to 4, moreover, we have tested the cloud services against the following Web browser versions:

- MS Internet Explorer 8.0.7601.17514,
- Mozilla Firefox 11.0,
- Google Chrome 18.0.1025.168 m,

against the following openly available Nirsoft *live* forensics tools, on the powered on system:

- SmartSniff v1.91,
- IECacheView v1.460,
- IECookiesView v1.74,
- IEHistoryView v1.65,
- MozillaCacheView v1.51,
- MozillaCookiesView v1.36,
- MozillaHistoryView v1.42,
- ChromeCacheView v1.35,
- ChromeCookiesView v1.02 ,
- ChromeHistoryView v1.05,
- CurrProcess v1.13,

and finally against *Internet Evidence Finder v4.0* from *JAD software* (not free of charge), used as *post mortem* forensics tools on the physical image of the local hard disk, as a cross-check.

As far as the last scenario is concerned, we have first analyzed the powered on system with the following openly available *Nirsoft live* forensics tools:

- WhatInStartup v1.33,
- RegScanner v1.85,
- CurrProcess v1.13,
- WinPrefetchView v1.10
- RecentFilesView v1.15,
- SearchMyFile v1.82,

and then we have searched the physical image of the local hard disk with *Sleuthkit, Autopsy* and *Log2Timeline*.

## IV. Case Study Results and Discussion

This section summarizes results of the tests carried out in scenarios described in Section III.

The following is a list of inspected local folders and Web browsers databases which, for brevity, we will refer to hereafter by their nicknames, indicated within brackets:

- Users\..\AppData\Local\Microsoft\Windows\Cookies *(IE_cookies),*
- Users\..\AppData\Local\Microsoft\Windows\History *(IE_history),*
- Users\..\AppData\Local\Microsoft\Windows\Temporary Internet Files *(IE_cache),*
- Users\..\AppData\Roaming\Mozilla\Firefox\...\cookies.sqlite *(MF_cookies),*
- Users\..\AppData\Roaming\Mozilla\Firefox\...\places.sqlite *(MF_history),*
- Users\..\AppData\Local\Mozilla\Firefox\...\cache *(MF_cache),*
- Users\..\AppData\Local\Google\Chrome\User Data\Default\Cookies *(GC_ cookies)*
- Users\..\AppData\Local\Google\Chrome\User Data\Default\History *(GC_history),*
- Users\..\AppData\Local\Google\Chrome\User Data\Default\Cache *(GC_cache).*

### *A. Scenario 1 - Dropbox accessed via Web browser:*

The usage of SmartSniff to eavesdrop the connection has been of scarce utility as *Dropbox* server provided a secure HTTPS connection, encrypted via SSL on TCP port 443.

In *test 1.1*, we found cookies from *www.dropbox.com* in IE_cookies, MF_cookies and GC_cookies and traces of the login phase in some HTTP and HTTPS url in IE_history, MF_history and GC_history, attesting that *Dropbox* login page was accessed at list once.

In *test 1.2*, upon uploading a word document on *Dropbox* server, the *…dropbox.com/upload* url was saved in IE_history whereas no traces of the file upload were found in MF_history and GC_history.

In *test 1.3*, upon opening or downloading a word document, four HTTPS url reporting the actual filename in url title were saved in IE_history and a copy of the file was stored in IE_cache; Two HTTPS url reporting the actual filename in url title were saved in MF_history and a copy of the file was stored in the *\Users\...\AppData\Local\Temp* folder; No url were saved in GC_history whereas a copy of the file was stored in GC_cache.

In *test 1.4*, upon deleting a word document from Dropbox, no traces of the user-CSP interaction were found locally.

### *B. Scenario 2 - Google Documents accessed via Web browser:*

The usage of *SmartSniff* to eavesdrop the connection has been of scarce utility as *Google Documents* server provided a secure HTTPS connection, encrypted via SSL on TCP port 443.

In *test 2.1*, we found cookies from *account.google.com,* and *google.com* in IE_cookies, MF_cookies and GC_cookies and traces of the login phase in some HTTP and HTTPS url in IE_history, MF_history and GC_history, attesting that *Google Documents* logon page was accessed at list once.

In *test 2.2*, upon creating a word doc in *Google Documents*, an HTTPS url reporting the actual filename in url title were saved in MF_history and GC_history whereas Internet Explorer leaved no traces. In IE_cache, MF_cache and GC_cache, we found icons, generic files and JavaScript files used by the browser to interact with the server.

In *test 2.3*, upon uploading a word document on *Google Documents*, no traces of the user-CSP interaction were found locally.

In *test 2.4*, upon opening a word document, an url was saved in MF_history and GC_history, whose title reported the complete name (with extension) of the opened file. No traces were found in IE_history, IE_cache, MF_cache and GC_cache.

In *test 2.5*, upon deleting a word document on *Google Documents*, no traces of the user-CSP interaction were found locally.

### *C. Scenario3 - PicasaWeb accessed via Web browser:*

The usage of *SmartSniff* to eavesdrop the connection has been of scarce utility as *Google PicasaWeb* server provided a secure HTTPS connection, encrypted via SSL on TCP port 443.

In *test 3.1*, we found cookies from *account.google.com* and *google.com* in IE_cookies, MF_cookies and GC_cookies and traces of the login phase in some HTTP and HTTPS url in IE_history and MF_history, attesting that *Google PicasaWeb* login page was accessed at list once. With regards to Google Chrome, in particular, two HTTPS url reporting the actual username in the title were saved in GC_history, attesting that *Google PicasaWeb* user account was accessed at list once. For each photo album that we created on the server, a cover image was saved in IE_cache, MF_cache and GC_cache.

In *test 3.2*, upon uploading an image file on Google PicasaWeb, we found an HTTPS url in IE_history, and MF_history, attesting that *Google PicasaWeb* upload page was accessed at list once. With regards to Google Chrome, in particular, a url reporting the actual username, as an HTTPS parameter, were saved in GC_history. Finally, for each image that we uploaded on *Google PicasaWeb*, a correspondent image file was saved in IE_cache, MF_cache and GC_cache.

In *test 3.3*, upon opening an image file from *Google PicasaWeb*, we found an HTTPS url in IE_history, MF_history and GC_history, whose title reported the name of the album the photo belongs to. With regards to Google Chrome, in particular, it was possible to find the image in its original dimension in GC_cache.

In *test 3.4*, upon deleting an image file on *Google PicasaWeb*, no traces were found in IE_history and

MF_history. With regards to Google Chrome, in particular, an HTTPS url, whose title reported the name of the album the deleted photo belonged to, were saved in GC_history.

### D. Scenario 4 - Flickr accessed via Web browser:

With the exception of the authentication stage in which *Flickr* server provided a secure HTTPS connection, encrypted via SSL on TCP port 443, the usage of *SmartSniff* to eavesdrop the connection has been of great utility as the web connection between the user and cloud server was in the clear.

In *test 4.1*, we found cookies from flickr.com and yahoo.com as well, in IE_cookies, MF_cookies and GC_cookies, as we used a yahoo account to authenticate to *Flickr*; Traces of the login phase were found in some HTTP url in IE_history, MF_history and GC_history, attesting that *Flickr* login page was accessed at list once. Personal images displayed in the home page after the authentication were saved in IE_cache, MF_cache and GC_cache.

In *test 4.2*, upon uploading an image file on *Flickr* server, the *…flickr.com/photos/upload* url was saved in IE_history, MF_history and GC_history whereas we found a copy the of the album web page the photo belongs to in IE_cache and MF_cache.

In *test 4.3*, upon opening an image, an url was saved in IE_history, MF_history and GC_history, whose title reported the name (without extension) of the opened file. In IE_cache and GC_cache it was a copy of the opened file whereas, in MF_cache, a copy of a web page pointing to the opened file was saved.

In *test 4.4* upon deleting an image file, a copy was stored in IE_cache, MF_cache and GC_cache; With regards to Internet Explorer, two url were saved in IE_history, whose title reported the partial name (without extension) of the deleted file.

### E. Scenario 5 - Dropbox client installation with local synched folder:

In *test 5.1* we performed both a *live* analysis of the powered on laptop computer to check for:

- the presence of *Dropbox* folders synched with the server,
- registry keys attesting installation of the *Dropbox* client,
- *Dropbox* software in the list of installed applications,
- The presence of *Dropbox* synchronization process in the list of running processes,
- a dropbox.pf file in Windows prefetch directory, attesting that *Dropbox* was executed at list once,
- files recently accessed and *Dropbox* synchronization logs,

and a *post mortem* analysis of the physical image of the local hard disk to check for:

- the presence of *Dropbox* folders synched with the server and related files,
- *Dropbox* synchronization logs,
- the timeline of recently opened, modified and deleted file by *Dropbox*.

In *tests 5.2, 5.3 and 5.4*, we performed a *post mortem* analysis of the physical image of the local hard disk to check for:

- the *Dropbox* synchronization logs,
- the list of files recently opened, modified and deleted by *Dropbox* and related timeline.

All the tests of the current scenario were successful as it was possible to reconstruct all user activities by performing both *live* and *post mortem* analysis.

## V. Conclusion

In this paper we have described our point of view about the emerging challenges of cloud computing to digital forensics and related countermeasures.

The research question that we addressed in this work was the following: *"is it possible to analyze cloud environments with traditional digital forensics procedures and how existing techniques, tools and methodologies would cope in cloud scenarios?"*.

In this context, we conducted a forensic investigation on a cloud environment [8], after building a practical case study, in which we have analyzed some popular *SaaS* applications to demonstrate that, upon sharing files, photos and document in the cloud, evidentiary material may be found in logs and temporary files, saved locally by Web browsers.

We have inspected, therefore, local folders and Web browsers databases with traditional *live* and *post mortem* forensic methods and tools to cross-check the retrieval of potential evidence, concerning the user-CSP interaction.

We have also analyzed *Dropbox*, a popular file sharing *SaaS* application which may work both as a Web based cloud application or a traditional, locally installed software which stores a copy of the server data in a synched local folder. Our aim was to verify that it was possible to acquire a forensic copy of data as it exists in the cloud by simply retrieving data or fragments from local hard drives.

The outcome of the case study outlined above was surprising as we have been able to collect interesting evidentiary material of the user-Cloud interaction from local artifacts or eavesdropping network connections without the need to access the cloud server directly.

An important aspect to point out is finally the possibility, offered by most Web browsers, to surf the cloud anonymously (i.e. deleting navigation data upon quitting the browser) which could be considered an anti-cloud forensics technique. As a consequence, it will be necessary to investigate, in the future, if the adoption of forensic techniques for deleted file retrieval and timeline creation could overcome or mitigate this problem.

## VI. Future work

The spread of high-tech and cybercrimes in the cloud, related to the worldwide diffusion of low-cost mobile devices (i.e. PDAs, tablets, handsets and smartphones), providing mobile access to email and documents, with CPU, RAM and storage capacities exceeding traditional desktop or laptop systems, will increased vertically over the coming years. With cloud computing growing more complex and a wide variety of private, hybrid, and public cloud-based systems and infrastructure already in use, moreover, the lack of physical access to the cloud servers will make it even more difficult to isolate evidentiary material with traditional forensic methods. As a consequence, the standardization of new cloud forensics techniques will certainly be the most serious challenge of cloud computing over the coming years.

In this regards, novel ideas aimed at identifying, at an early stage of investigations, the typical crime-related fingerprints when searching artifacts in the cloud, are welcome as they could provide new pieces of information to current investigative techniques.

Digital forensics is constantly supported by new methods and tools to retrieve evidence effectively. A new research field, called triage, which allow to rank groups of artifacts and quickly identify the most relevant ones from crime's perspective has recently emerged. Triage is based on Machine Learning theory and has two main applications, called *live* and *post mortem*, which differ in the way they are implemented. In this regards, it is important to refer to the work done in [9],[10],[11] and [12], as far as computer and mobile forensics are concerned, as it may be also applied to cloud forensics.

A possible future work could be, indeed, to analyze user artifacts and user-CSP interactions with Machine Learning algorithms with the aim of matching well-known crime-related patterns. As a result of the application of such triage-based techniques, cloud forensics investigations' complexity could decrease significantly.

In this regard, interested readers who may want to try their own triage-based implementations should spend some time to identify the features related to the crime/s they want to analyze and collect a consistent set of categorized cloud artifacts related to one of the aforementioned crime/s. It is important to mention that categorization success depends on the accuracy adopted when creating the training-set which is the core of the whole process. The higher the number of analyzed artifacts (i.e. the training samples) is, indeed, the better the model is able to categorize new artifacts.

## Acknowledgment

The paper is based on a research carried out in collaboration with the Carabinieri Corps and the Computer Forensics Unit of the Italian Postal and Communications Police, Ministry of the Interior.

## References

[1] R. Perry, E. Hatcher, R.P. Mahowald, S.D. Hendrick. Force.com Cloud platform drives huge time to market and cost savings. White paper, IDC. 2009. Retrieved June 22, 2012, from http://www.salesforce.com/fr/assets/pdf/whitepapers/whitepaper-idc-force-roi-study.pdf.

[2] J. P.Mell, T.Grance. The NIST definition of cloud computing. In Recommendations of the National Institue of Standard and technology, Special Publication 800-145. 2011.

[3] C.P. Garrison. Digital forensics for Network, Internet, and cloud computing. Syngress Publishing, 2010.

[4] Digital Forensic Research Workshop (DFRWS). A roadmap for digital forensic research. 2001. Retrieved April 20, 2012, from http://www.dfrws.org/dfrws-rm-final.pdf.

[5] K. Ruan, J. Carthy, T. Kechadi, M. Crosbie. Cloud forensics: An overview. In proceedings of 7th IFIP International Conference on digital forensics, Advances in digital forensics, Vol. 7, Springer, 2011.

[6] N. Antonopoulos, L. Gillam. Cloud computing. Principles, Systems and Applications. Published by Springer-Verlag, 2010.

[7] D. Birk. Technical Challenged of Forensic Investigations in cloud computing Environments. 2011. Retrieved May 10, 2012, from http://www.zurich.ibm.com/~cca/csc2011/submissions/birk.pdf.

[8] D. Barrett. Virtualization and forensics a digital forensic investigator's guide to virtual environments. Syngress Publishing, 2010.

[9] F. Marturana, R. Bertè, G. Me, S. Tacconi. Mobile Forensics "triaging": new directions for methodology. In Proceedings of VIII Conference of the Italian Chapter of AIS (ITAIS 2011) Rome, Italy, Springer, 2011.

[10] F. Marturana, R. Bertè, G. Me, S. Tacconi. A quantitative approach to Triaging in Mobile Forensics. In Proceedings of International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, (TRUSTCOM 2011) Changsha, China, pages 582-588, 2011.

[11] F. Marturana, R. Bertè, G. Me, S. Tacconi. Data mining based crime-dependent triage in digital forensics analysis. In Proceedings of 2012 International Conference on Affective Computing and Intelligent Interaction (ICACII 2012) and IERI Lecture Notes in Information Technology, 2012, in press.

[12] F. Marturana, R. Bertè, G. Me, S. Tacconi. Triage-based automated analysis of evidence in court cases of copyright infringement. In Proceedings of First IEEE International Workshop on Security and Forensics in Communication Systems (SFCS 2012), in conjunction with IEEE ICC, Ottawa, Canada, 2012, in press.