World Academy of Science, Engineering and Technology
International Journal of Law and Political Sciences
Vol:11, No:1, 2017

Towards a Proof Acceptance by Overcoming Challenges in Collecting Digital Evidence

Lilian Noronha Nassif

***Abstract*—**Cybercrime investigation demands an appropriated evidence collection mechanism. If the investigator does not acquire digital proofs in a forensic sound, some important information can be lost, and judges can discard case evidence because the acquisition was inadequate. The correct digital forensic seizing involves preparation of professionals from fields of law, police, and computer science. This paper presents important challenges faced during evidence collection in different perspectives of places. The crime scene can be virtual or real, and technical obstacles and privacy concerns must be considered. All pointed challenges here highlight the precautions to be taken in the digital evidence collection and the suggested procedures contribute to the best practices in the digital forensics field.

***Keywords*—**Digital evidence, digital forensic processes and procedures, mobile forensics, cloud forensics.

I. Introduction

DIGITAL evidence can be accepted in a trial provided that it remains reliable since its acquisition. The digital investigator must be prepared even before the crime exists. Prosecutors must understand how technical aspects can influence in the law process; for example, what kind of digital evidence to gather; how long evidence requires preparation and analysis. Smartphones and notebooks are widely used, and frequently they reveal private conversations, photos, and videos. The timing of evidence collection is crucial and the forensic sound tools must be carefully selected in advance.

Digital forensic area is new and several judges still have doubts about understanding the evidence preservation. Standard Operational Procedures (SOP) must be defined and followed during digital evidence gathering phase including the use of specific materials such as antistatic bags and gloves to hold hard drives (HDs), and Faraday bags to hold mobile phones. A Faraday bag blocks electromagnetic signals preventing remote access.

Digital forensics lacks an updated reflection about digital evidence collection challenges. Without a clear understating about the main obstacles, several mistakes can be committed, starting from the crime scene to the forensic laboratory.

This paper presents a detailed list of problems in gathering digital evidence. Prosecutors, policeman, and computer science technicians must have a similar view of problems concerning digital evidence collection. This focus contributes to the continuous improvement of each investigation case.

This article is organized as follows: Section II presents some particularities of digital evidences; Section III presents places where digital evidences can be seized, considering real and virtual sites; Section IV relates challenges in collecting evidence; and Section V concludes the paper.

Lilian Noronha Nassif is with the Public Ministry of Minas Gerais. 30170-008, Belo Horizonte, Brazil University of Minas Gerais State, Belo Horizonte, 30330-050 Brazil (e-mail: lilian.noronha@uemg.br).

II. Digital Evidence

Digital evidence is any information of probative value that is either stored or transmitted in a digital form. Digital evidence types increase continuously. A non-exhaustive list of digital evidence is presented in [1]. Fig. 1 organizes them in groups, according to the similarity of required exams.

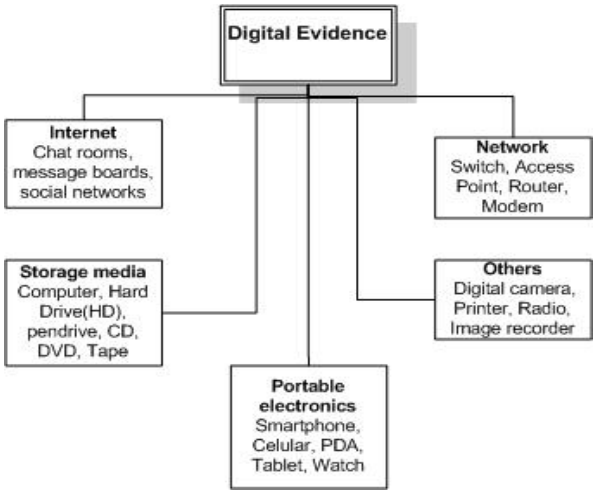

Fig. 1 Digital evidence group example

Storage media and portable electronics deserve a special attention, considering they are frequently the focus of an investigation because of their completeness.

Smartphone is an inseparable accessory nowadays for everyone. It is equipped with all kinds of technology to register photos, conversations, internet navigations, notes, calls, and localizations, for example [2]. All kind of interaction and movement can be gathered from a personal smartphone. This can explain how valuable this digital evidence is, and the careful steps needed to seize it. If smartphone is not properly turned off, and all types of networks were not disconnected, it is possible that all information can be deleted even before it arrives on the forensic laboratory [3].

Instant message (IM) is one of the most important applications used to organize crimes nowadays. Because of privacy communication implemented by cryptography algorithms, IMs, such as WhatsApp, can provide excellent

opportunities for the society, but also can be used by criminals [4].

The HD is another important digital evidence that can be physically removed from the desktop or notebook for posterior analysis on the forensic laboratory. However, investigators usually do not get volatile information during a seizing procedure. Volatile information contains system time, logged-on users, open files, network information, command history, process memory, for example. These information can be acquired if the computer is encountered turned on [3].

Digital evidences usually are seized after other investigations phases, such as, wiretapping. However, after digital evidence seizing, everyone involved are alarmed. The digital evidence seizing is important to validate some investigations and must be treated with extreme care. After this phase, the investigated tend to eliminate all kind of proofs, and digital evidence can be the last chance for a succeed case.

III. Places to Seize Digital Evidence

Investigators can collect evidence on site and online and can send evidence to the forensic laboratory. When an investigator collects evidence on site, the investigator is physically present at the crime scene. When an investigator collects evidence online, the investigator is acquiring data by using a network or by extracting data from the cloud. At lab, more precisely, at the forensic laboratory, investigators can extract all kind of information from a digital evidence previously seized. Section IV presents the challenges involved for each location.

When seizing computers on site, they can be turned on, and in these cases, it is possible to get volatile data from the Random Access Memory (RAM). Also it is recommended to photograph the screen. Fig. 2 summarizes where evidence collection takes place.

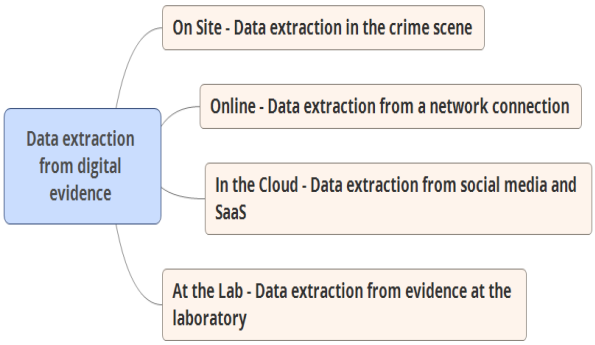

Fig. 2 Digital evidence data extraction

In some cases, it is possible to acquire the image from the evidence on site. This procedure does not remove the evidence from the original place and a bit-stream copy of the evidence and its hash function are send to the forensic laboratory for posterior analysis.

IV. Challenges to Seize Digital Evidence

This section presents challenges according to the different locations where digital evidence is gathering, as presented at Fig. 2.

A. Challenges in Collecting Evidence on Site

When investigators arrive at the crime scene, they have to make decisions about how to collect evidences. Some challenges are presented as:

- **Impossibility of physical removal**. If the hardware platform is big, probably it is impossible to remove the evidence from the site. In this case, the evidence mirror or some data selection must be done on site.
- **Disk size**. An evidence copy demands a disk of the same size if no compression is used. Sometimes it is difficult to calculate previously the amount of disks necessary to mirror an evidence.
- **Quantity of evidence**. If the quantity of evidence available in the crime scene is numerous, the investigator must have several equipment of the same type, for example, several disk clone tools.
- **Collection time**. The evidence collection time can be restricted. This challenge is increased by the difficulties already presented above, for example, the time is short, the evidence size is big, and it is impossible to remove the evidence from the crime scene.
- **Connectivity**. The investigator needs to interact with the evidence using a wireless or wired connection. A great variety of cables must be available to integrate the forensic equipment to the digital evidence. This is particularly difficult for cellular phones because of non-standard interoperability.

These challenges must be combined for each case. In addition, the hardware platform must be considered, for example: High and medium computer platforms (mainframe, blade, and virtualization), low computer platform (desktop, laptop, and tablet), and cellular.

B. Challenges in Collecting Evidence Online

Collecting online evidence presents several challenges as described as:

- **Throughput**. In the online evidence acquisition, the investigator copies all information from the suspect equipment by using a network. Nevertheless, the network throughput is inferior to local data acquisition, making the process slower than acquisition on site.
- **Data change**. During the online data acquisition, the local user can modify data. Such situation can result in disk image problems because files could be in use during the copy.
- **Machine disconnection**. The online data acquisition can be interrupted anytime if the suspect machine is disconnected from the network for any reason. This incident results in an abrupt process cancelation.
- **Data collection recognition.** During data acquisition, the local user can realize that a remote copy is taking place, and consequently, he can modify his behavior. He can delete or modify files, block remote access, or turn the

evidence off, for example. This can hinder a reliable data acquisition.

- **Network problems.** When the online acquisition occurs in a local network, the massive data transfer between the investigator equipment and the suspect machine can degrade the network performance. Other users of the same network can face problems in usual activities such as low latency to access internet, open a remote document, or print a file.

C. Challenges in Collecting Evidence in the Cloud

Data collection in the cloud is harder than on site data acquisition and online data acquisition. Cloud computing is defined as a model for convenient access to remote shared resources [5].

The cloud forensics is defined as a subset of network forensics since it is based on extensive network access. The evidence data acquisition in the cloud can be applied in cloud services and in social media. The challenges in evidence collection of each one are described in the following.

1. Cloud services

The business model available for clouds offers services with different resource controls. The main cloud types are grouped into three categories: Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) [6]. The SaaS provides on-demand applications over the Internet. Some examples of SaaS include Google Drive [7] and Rackspace [8]. The PaaS offers platform layer resources, including operating system support and software development frameworks. Some examples of PaaS include Windows Azure [9] and Google App Engine [10]. IaaS refers to on-demand provisioning of infrastructural resources, usually virtual machines. Some examples of IaaS include Amazon EC2 [11] and GoGrid [12].

The following presents important challenges faced during evidence collection in the cloud services, and discussed in more details by [13]:

- **Volatile data**. In the IaaS, user can turn off the Virtual Machine and as a consequence, all volatile data will be lost. Although data can be synchronized in a persistent storage, usually users do not contract this service, mainly when they want to explore this vulnerability.
- **Trust in the Service Provider**. When the investigation issues a subpoena to a service provider to gather information about a user, some trust problems occurs. The technician that works at Internet Service Provider (ISP), SaaS, PaaS and IaaS will be the responsible to gather the information. Nevertheless, usually he is not a forensic investigator and it is not possible to guarantee his integrity in a court of law.
- **Third part privacy**. In a cloud structure, many users can share the same physical resources. The HD image in the cloud may violate the privacy of other users. It is necessary to prove that suspect data are not mixed with other users.
- **Log problems**. Different logs in a computer environment can help in a crime scene reconstruction. However, gathering different logs in the cloud sometimes can be impossible. The log problems are related to the volatility of logs in virtual machines, several log tiers (database, operating system, network), several people accessing logs (development, network administrators), and the lack of a standard log format.
- **Chain of custody**. The chain of custody in the cloud is questionable because multiple people may have access to the evidence and the process depends on the service provider.
- **Cross border law**. The data storage of a service provider can be distributed worldwide. The attacker may access the cloud computing service from one country and data may be stored in a data center in another country. Different laws may apply to this situation, and the investigator must acquire data considering all these aspects.

2. Social Media

Data in social media can be a valuable source of information during an investigation. Nevertheless, it is difficult to gather evidence in a way to be accepted in court. Some studies and real cases are helping to define the best practices for this situation.

According to [12], the main social media types are classified in the following groups:

1) Social networks: This service consists in a user profile that interacts private and publicly with others (e.g. Facebook and LinkedIn);
2) Media sharing: This service allows a user to upload videos and photos and share with others (e.g. Youtube, Instagram);
3) Activity tracking: This service allows a user to record certain activities such as visiting a determined place (e.g. FourSquare);
4) Blogs and microblogs: A blog works like a diary and a microblog works like short updates to anyone subscribed to receive it (e.g. Twitter);
5) Social news: This service allows a user to share items or links to news articles (e.g. Digg);
6) Discussion forums: Forums are created about a specific topic of common interest for a group and participants can discuss openly;
7) Reviews: This service allows a user to participate in the comment section (e.g. TripAdvisor).

The following presents important challenges of collecting social media evidence discussed in [13]-[16]:

Although information in social media is public, the user can configure his profile to restrict the access of unknown people. Most users allow friends to access their posts. The court may reject the evidence if an investigator pretends to be a friend to get information from the suspect. This behavior may involve dishonesty, fraud, deceit, or misrepresentation.

- **Privacy concerns**. An employer cannot request the employee password in social media even if the employee is under a professional misconduct investigation. Only the relevant information for the investigation must be

accessed.

- **Privacy and social media policies**. Employers must define an explicit social media policy for their employees that describe which content belongs to the employer. This can avoid a reasonable expectation in the privacy for different interactions of the employee, such as, a personal email sent from work computers or the establishment of professional connections in LinkedIn.
- **Data change and data manipulation**. Users can easily delete information from their social media profile. Unfortunately, users can also be victim of data manipulation on their own social media space. In [15], investigators are oriented to record what they are seeing on the social media by using tools such as Camtasia [17] and Screencast-O-Matic [18]. It is also important to ensure that data were not manipulated after this recording. Therefore, the investigator must identify himself, record day and time, explain the purpose of the investigation, and send the recording to several people, including his boss, the attorney and a third party company capable of auditing activities [15].

D. Challenges in Collecting Evidence at the Lab

Data extraction at the forensic laboratory seems to be the easier place to extract data. However, if inadequate procedures were taken during acquisition, investigators probably will not succeed in data extraction.

Important challenges faced during evidence collection at the lab are presented as:

- **Locked devices:** Every day, the number of people that lock their smartphones is increasing. If the smartphone is a new version of iPhone, the probability to unlock the device at the lab is very low. In these cases, the police approach to seize this kind of evidence on site is very important. One chance can be to get the iPhone directly unlocked from the owner and proceed with the unlock mechanism on the device.
- **HD I/O error:** HD is a sensible device and physical impacts can result in I/O errors. This kind of error does not allow the investigator to make a proper image of the original HD. This type of problem can be avoided if the HD is properly transported from the site to the forensic laboratory.
- **Turned on smartphone:** Some smartphones have a sensitive button to turn it on and off. Usually, several smartphones are seized in a same case and are sent to the forensic lab in a same bag. If the smartphone is turned on unwittingly during the transportation, it can be erased remotely. In this case, the investigator will not be able to extract data when the evidence arrives at the laboratory.

V. Conclusion

Digital forensics still faces several challenges concerning digital evidence collection phase. Different virtual and real locations can be considered the crime scene. Technical obstacles and legal frontiers must be considered to preserve and accept the digital proof in a court.

This paper presented several challenges to seize digital evidence in virtual and real places. The same difficulty must be shared between prosecutors, investigators, and police involved in the apprehension of digital evidences.

Forensics processes must follow standards and must be optimized continuously. The first phase to understand the problem is to characterize them properly. This paper contributes to this elucidation and describes systematically all challenges in the crucial forensic phase of collecting evidence, thereby increasing preparation procedures and success in the digital evidence preservation.

References

[1] Technology Working Group for Investigative Uses of High Technology. Investigative uses of technology: Devices, tools, and techniques. NIJ Special Report NCJ213030. Washington, DC: National Institute of Justice (2007).
[2] IDC. Available at http://www.idc.com/prodserv/smartphone-os-market-share.jsp. (Accessed: 30 Sep 2016).
[3] Electronic CSI, A Guide for First Responders, 2nd Edition, National Institute of Justice, (2008).
[4] Zhang, Li, Xu, Chao, Pathak, Parth H., Mohapatra, Prasant. Characterizing Instant Messaging on Smartphones. Volume 8995. Lecture Notes in Computer Science pp 83-95. 2015
[5] Mell, P., Grance, T. "Draft NIST working definition of cloud compuing-v15", 21. Aug (2009).
[6] Zhang, Q., Cheng, L. Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Application. 1(1), 7-18. (2010)
[7] Google. Google Drive. Available at https://drive.google.com (Accessed 08 Jan 2015).
[8] Rackspace. Focus on your business. Available at http://www.rackspace.com (Accessed 03 Jan 2015).
[9] Azure. Windows azure. Available at http://www.windowsazure.com (Accessed 10 Jan 2015).
[10] GAE. Google App Engine. Available at http://appengine.google.com (Accessed 10 Jan 2015).
[11] Amazon. Amazon Elastic Computing Cloud. Available at htt://aws.amazon.com/ec2 (Accessed 10 Jan 2015).
[12] GoGrid. Cloud Hosting, Cloud Computing and Hybrid Infrastructure from GoGrid. Available at http://www.gogrid.com (Accessed 09 Jan 2015).
[13] Zawoad, S., Hasan R. Cloud Forensics: A meta-Study of Challenges, Approaces, and And Open Problems. arXiv preprint arXiv:1302.63.12, pp 1-15, (2013).
[14] Bosack et al. Social Media Evidence: Ethical and Practical Considerations for Collecting and Using Social Media Evidence in Litigation. Corporate Conseul CLE Seminar (2014)
[15] Murphy, J., Fontecilla, A. Social Media Evidence in Criminal Proceedings: An Uncertain Frontier.Richmond Journal of Law & Technology. Volume XIX, Issue 3. 2013
[16] How to Gather Social Media Evidence. Avoid Legal Disasters and Win More Cases. Available at http://i-sight.com/how-to-gather-social-media-evidence. (Accessed: 10 Nov 2014).
[17] Camtasia. Available at http://www.techsmith.com/camtasia.html (Accessed: 03 Jan 2015).
[18] Screencast-O-Matic. Available at http://screencast-o-matic.com/ (Accessed: 05 Jan 2015).