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 understanding 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.

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.

![Digital Evidence Group Example](image)

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.

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 collection in the cloud services, and discussed in
and GoGrid [12].
provisioning of infrastructural resources, usually virtual
[9] and Google App Engine [10]. IaaS refers to on-demand
operating system support and software development
[8]. The PaaS offers platform layer resources, including
examples of SaaS include Google Drive [7] and Rackspace
SaaS provides on-demand applications over the Internet. Some
a service (PaaS), and infrastructure as a service (IaaS) [6]. The
three categories: Software as a service (SaaS), platform as
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] 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
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.

V. CONCLUSION

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