Digital Chain of Custody Quality Assessment

Pedro Luis Prospero Sanchez and Giuliano Giova

Escola Politécnica, Universidade de São Paulo, São Paulo, Brazil

Summary
Modern society demands products and services increasingly sophisticated and effective, a desire that has been met through the development of more powerful, reliable and cost-efficient electronic systems. The ubiquity of these systems makes the data often stored in them to be used as evidence to prove the truth of the facts discussed in lawsuits. However, usually, the chain of custody software is insufficient by itself to guarantee the courts the quality of those digital evidences. This paper analyzes the quality gap existing between complex inspected systems and generally a limited procedure is used to document forensic inspections, and then it proposes a method to improve the reliability of the chain of custody.

Key words:
Computer forensics, digital evidence, chain of custody, quality assessment.

1. Introduction

It is up to the court's judges to resolve conflicts judging the causes based on the law and its conviction about the truth of the facts submitted to it, but the identification of these truths has never been a simple task. The rules and methods agreed by the courts and the parties in lawsuits to prove claims have varied widely throughout history, currently the role of technical evidence has grown in the conviction of the judge or the jury. The conviction effectiveness is greater depending on how firmer and clearer is the certainty about the evidence that is submitted to the court.

The term evidence indicates any item that is admitted by the judge in a process, so that, the evidence must be relevant and reliable by relying on sufficient facts or data, by resulting from appropriate methods and by being well assessed from the perspective of forensic sciences [1].

The proportion of evidence presented in digital format to courts increases progressively, due to the revolution brought about in the world by information and communication technologies: there are now over 3 billion Internet users and more than 7 billion mobile phone subscribers, setting the increasing adoption of electronic systems on a day-to-day basis by governments, companies and people [2][3][4].

The trend of evidence virtualization brings striking consequences, as a greater distance between the physical world of the judge and the evidence that inhabits virtual worlds, including the difficulty of finding them among a large mass of data and a greater complexity to their evaluation due to their high volatility, as they can be easily created, modified or destroyed.

In a simplified view, we can characterize the virtual world as a very large environment with virtually no physical limits, where users dynamically interact with multifaceted electronic systems that are in constant transformation.

When there is the prospect of a digital dispute, it can be necessary to identify tiny scattered fragments of this virtual world and then collect and preserve traces to be submitted to the judge in their exact original state, so that they can then be evaluated to establish their relevance and reliability as evidence.

In view of the ubiquity and volatility of these data, it is essential that there is perfect control of the samples collected and the procedures carried out, since any data modification or improper procedure can make the evidence lose its probative value or even lead the judge to mistake. This control is technically called chain of custody.

The US National Institute of Justice (NIJ) defines that the police or security officers who make the initial treatment (first responders) at the place of crime (crime scene) take care of initial verification to assess the situation, recognize potential evidence and identify the necessary resources (walk-through), and then other professionals start acting, such as investigators and forensic examiners (investigators and other responders) in charge of detecting, documenting and retaining potential evidence and samples for comparison (collect) and organization (file case) after being properly identified with labels, containers and others (evidence identifiers).

After the appropriate action, a final examination should be carried out to ensure that the crime scene was effectively and fully processed. All these activities should be recorded in the chain of custody as "the process used to maintain and document the chronological history of the evidence", continuing that record over all the evidence life cycle, as subsequent tests and their submission to the judge [5].

Many countries have laws, technical standards and guidelines, with greater or lesser level of detail in order to provide adequate legal services. The academic world and the industry reach these goals by providing research, methods and tools used by the police and the computer forensics experts to identify, preserve, examine and present evidence to the court.

This paper studies the issues related to the methods used by the experts to choose the best model to be adopted to record the chain of custody in each case, a relevant aspect

Manuscript received April 5, 2016
Manuscript revised April 20, 2016

because it is a central element in the allocation of probative value to the evidence. In this scenario, this paper proposes a method that aims to increase the overall quality of records in chains of custody of digital evidence.

2. The chain of custody

As we have seen, the chain of custody is a process used to maintain and document the chronological history of the evidence. There are many possible methods, some of them as simple as a book, or a sheet of paper, which describe events in chronological order. Thus, in summary, it is a procedure very similar to the logbook of a ship, where information is sequentially recorded, regarding the port of origin, distances and measurements of position taken along the way and the events that occur until the arrival at the destination port. In other words, it is the record of the ship's (or evidence's) life cycle. The safety of this process consists in: (i) the obligation to register the activities; (ii) the chronological order in which the records are carried out and (iii) that they are made just when the activity occurs.

These measures give transparency to events that occurred in the handling of evidence and render difficult any attempts to tamper with the documentation of the facts through an unjustified entry, such as a modification or deletion of a text in a logbook or in a chain of custody.

Another security measure to prevent any tampering is to produce a copy of the logbook shortly after having filled an event and deliver them to the court or to trusted third parties.

Such care indicates elementary points of the chronological documentation syntax, but it is also necessary to evaluate semantics issues in order to ensure that each filled description refers to certain potential evidence and to a particular event, not to others. This question is usually resolved by assigning unique and trustable numbers to any object involved in the recorder event. Governments maintain identification services that record and assign, directly or through a concession to the private sector, unique identifiers to people, companies, agencies, sites, buildings, products, vehicles, activities, systems, electronic signatures, banking and so on. In the absence of unique identification, or complementing it, the police, investigators, bailiffs and forensic experts should generate ad hoc identifiers, such as a hash code to identify the content of specific hard disk or file.

It should be noted that often a unique identifier is not sufficient for forensic purposes, for example, the activity documented about an item in a supply chain have to be linked not only to the specific item, but also to the state of that object at the time the forensic activity was carried out. Therefore, even when there is a formal and unique identifier, the event registered in the chain of custody should point to additional controls to ensure the courts the visibility of the evidence state before, during and after any interaction with the crime scene or with any potential evidence.

For example, in a destructive forensic examination of a physical evidence, its chain of custody must contain video recording of such evidence before, during and after forensic procedures.

In the case of a potential digital evidence, it is necessary for the chain of custody of the evidence to show that the hash code is identical before, during and after the forensic activity, safekeeping the complete digital evidence alongside with this hash code. If the forensic procedure involves changes in the evidence, (e.g. to remove encryption from a hard drive), it is necessary that the chain of custody records the hash codes and that there are clones with these codes showing the state of the evidence before, during and after the forensic procedure [6].

Some forensic procedures are even more destructive as the removal of flash memory (Chip-Off) of a mobile phone to clone it directly through a specific machine [7]. A simple hash code calculation is not sufficient to register this kind of event, so the chain of custody must point to other controls that show the condition of the evidence before, during and after the forensic procedure, such as photographic records and measurements from engineering laboratorial instruments.

In some cases, it could be necessary that the documentation of the chain of custody points to analog measures taken by laboratorial equipment such as a multimeter or an oscilloscope, aiming to further ensure the probative value of that potential evidence and ensure the results of tests for the presence or even the absence of data in a solid state memory, for example.

It should also be considered, in this example, whether the Chip-Off procedures and content tests are all performed in the same laboratory with local follow-up of technical representatives of all the parties involved or, rather, the work is carried out in different places, with remote monitoring by the parties or even without any follow-up.

Governments, researchers and the industry provide a wide range of standards, studies, best practices and a wide range of tools to identify, preserve and analyze evidences. However, only a small part of this material relates to the creation and maintenance of chains of custody for digital evidence and even less to the appropriate choice of methods to keep the chain of custody.

Forensic or monitoring software frequently do not cover the entire life cycle of a potential evidence, as occurs with e-discovery and audit tools inside corporations, syslog systems in data centers or call centers, interception systems of telecommunications companies and Internet providers.

3. The Right Choice of Chain of Custody

The main activities carried out by practitioners in computer forensics usually consist in identifying, preserving, analyzing and presenting digital evidence, which must follow to some extent a standardized procedure to meet legal and scientific principles, technical standards and best practices. On the other hand, the characteristics of modern digital society and the complexity of the innovative digital systems make harder to create and maintain a trustworthy set of methods and forensic tools.

Therefore, the review of procedures and the certification itself of the resulting potential evidence depend on the reliability of the chain of custody mechanism. In other words, if the custody record system is reliable, it can be used as a means to assess the procedures performed and the resulting evidence.

However, if the chain of custody system is not reliable, it will be useless for the intended purpose, so probative value cannot be assigned to the evidence produced. Consequently, the quality of the chain of custody software is essential to the acceptability of potential evidence by the court.

The paradigm proposed here does not refer to an absolute quality assessment, but only to simple comparative evaluation of the main characteristics of the chain of custody and the inspected system.

For example, it may not be necessary to use a complex and complete online chain of custody software to record the arrest and transport to the laboratory of a theater ticket found on a table, in such cases the usual chain forms may be sufficient custody, as suggested by various government agencies.

On the other hand, it appears to be reckless the use of a form like this to register the chain of custody of the survey and data collection in a large ERP system or in a big cloud service.

The calculation of the hash code of a resulting container of data is insufficient, since demonstrating that the container remains preserved does not ensure that the previous procedures performed in the management system or in the big cloud service are correct and that there was no manipulation of data before or during their placement in the container.

In cases like these, the custody registration process is certainly required to be much broader and powerful. It is a similar context when systems generate data continuously and automatically with possible forensic purpose.

For instance, when a banking system registers transactions in a current account related with money laundering, or when the infrastructure systems of a telecommunications operator meet judicial orders of interception or the monitoring by the police of a website with illicit trade with court authorization. In these examples it will not be enough that the chain of custody record is a mere form, an effective and possible complex chain of custody system is required.

Thus, it is necessary to propose a model that is as simple and objective as possible, in a way that can be used in day-to-day by computer forensics investigators, respondents and the experts to comparatively evaluate the system to be inspected and the chain of custody tracking system that they intend to use to meet the legal obligations and best practices.

The cited research and presented examples demonstrate that the choice of method to be used to document the chain of custody of evidence given depends on the specification of the evidence and the procedures to be performed [8].

4. Problem to Solve

Scientific research brought significant contributions to the definition of the main procedures and techniques necessary to conduct forensic examinations on digital devices. The most relevant studies show four or five phases:

(i) preparation;
(ii) collection and preservation;
(iii) examination and analysis;
(iv) presentation and reporting;
(v) disseminating the case, having small differences in the number and types of activities in each phase [9].

Numerous authors contributed to the study of each activity, evaluating and indicating the best techniques to be used depending on the complexity and volatility of the digital world, emphasizing those which propose analytical models that help in the study of the crime scene [10].

Due to the increasing size and complexity of the cyber world, these tasks have depended increasingly on the aid of forensic software that automate processes and support the work of forensics investigators and experts in computer forensics.

However, a universal forensic software which applies to all (or nearly all) digital investigations. is not available.

Moreover, the increasing complexity of new and diversified devices requires specific and specialized forensic tools.

The literature has numerous studies on verification and validation of forensic software, detailing and testing its main functions such as collecting evidence, conducting research for keywords and presentation of results. However, there are no wider studies about the quality and usability of the chains of custody functions inside forensic software.

The majority of chain of custody modules are developed by the manufacturer of each forensic software and, therefore, its coverage is limited to its own procedures. To illustrate, a powerful tool built to collect hard drive and pendrive data, usually cannot help when the practitioner is

collecting data from network, even when he is using the same forensic computer.
Thus, it follows that the functions to ensure the chain of custody quality are segmented and sparse in several manual or automatic tools [11], requiring the investigator to perform ad hoc choices to compose a range of tools that tries to meet all the needs of each research scenario, then seeking to prevent any gaps that hinder or impede the ensuring of proper probative value to the evidence obtained.
The second problem identified is the lack of actually accepted and practical methods to assist the investigator in the task of choosing rationally their day-to-day proper composition tools for chain of custody record.

5. Proposed Model

The literature study indicates that the methods to evaluate the chain of custody are in an advanced stage in other areas of knowledge.
The highlights are the national and international standards, methods and tools used in DNA testing and handling of products such as nuclear materials, hardwoods, gemstones and several others. Frequently those modern tools use mapping techniques in their chain of custody controls [12].
Computer forensics also uses mapping techniques, inherited from its use in electronic engineering. There are studies using the technique to evaluate crime scenes [10], digital research processes [9] and to evaluate the quality of forensic software [13].
However, even if this technique is suitable for any fast processes or functions examinations, we have not found a large use of it in forensic software [14].
In such context, this paper proposes the use of mapping technique as practical innovation to ensure adequate chain of custody controls when the practitioner performs searches and seizures.
With this scope, it is proposed the adoption of the present mapping technique to:

(i) Map the target environment where the practitioner will conduct search and seizure (“Target Map”);
(ii) Map the chain of custody tool that the practitioner intends to use in a particular forensic work (“Custody Map”);
(iii) Compare both maps to determine gaps and overlaps ("Overlap Map"), and use results to confirm if the planned scheme will ensure an adequate chain of custody.
(iv) If there is a map of expected traces or potential evidences, the practitioner can also compare the “Trace Map" suggested by [15] with Overlap Map to ensure the adherence of the choice made.

Thus, the proposed process includes, in summary, the activities shown in Figure 1.

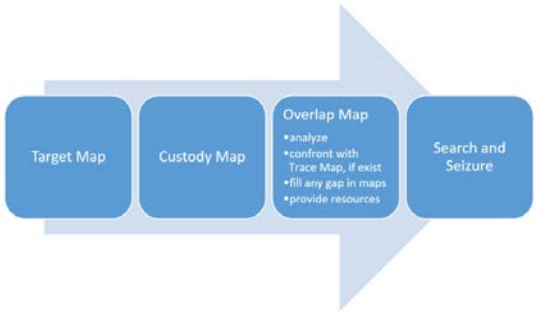

Figure 1: Proposed mapping process

Each map must be constructed starting from its highest level (top-level map) and be detailed only to the extent needed.
Ditto for the comparison of maps, which should be performed at the highest level possible within the objectives of this proposal, seeking to ascertain:

a) If the chain of custody model to be adopted ensures the possibility of registration of all forensic events of interest to technical research;
b) If the technology adopted in the chain of custody model is compatible with the technology and size of the environment to be surveyed;
c) If this model is suitable from the point of view of the effort required for the records.

Thus, we propose a method that primarily assists choosing the best model for the chain of custody and secondly provides criteria and additional documents to the court and the parties to better assess the probative quality of the evidence.

6. The Method: Comparative Mapping

Maps were born with the graphical representation of the celestial sphere and the surface of the terrestrial globe, but soon this method was used in other areas of knowledge to make the creation of clear representations easy.
More recently the technique has been used to map information in order to quickly communicate its categories and structures by means of short, clear, understandable and self-explanatory texts.
In order to build a map, the activities of identifying, categorizing, interrelating and sequencing and presenting graphically information are carried out, providing a simple and modular tool to present concepts, structures, functions and processes [13].
The proposed method adopts function mapping to identify the higher level functions that the investigator notes in the research target environment.
Then, it uses techniques of breakdown, i.e. the division of a complex system into more readily apparent and understandable parts, but this breakdown should be done

only until there is visibility of the main types of systems or components that can be of forensic interest during the inspection of the environment.
The functional breakdown strategy is already widely used in computer science (decomposition paradigm), being used at this time to show the higher-level functions, the main processes, the involved areas and the main objects handled by the target system.

7. Target Environment Map (Target Map)

Mankind generates and stores unprecedented amount of data, a factor that makes more complex and laborious any research on digital medium.
For this reason, it is essential that the researcher seeks to be informed in advance about the target environment and uses the obtained information to better plan his research actions, especially when it is necessary to conduct a judicial inspection without prior notice, to collect and preserve evidence of interest for the legal proceedings that are found on site. [15]
Thus, based on the information that the investigator obtains about the main processes of interest and infrastructure resources that they use, he must mount the map of the target environment, adopting a model similar to that suggested in Figure 2.
The choice of processes to be used depends on the goals, usually established by the authority who ordered the search and seizure, and the target technical infrastructure predictable from the preliminary surveys conducted by the investigator on the Internet for public information such as resumes of employees or any information disclosed about the target.
In a real case, the map may be more or less detailed, depending on the particular characteristics of each case.
Still referring to the map of Figure 2, once established the key processes and structure components, the investigator establishes the dependency relationships between these elements from the perspective of the procedures to be carried out during the inspection of the target site. For instance, the investigator may foresee that to determine a sales-related fraud he will need to inspect both the current data stored in the company's database, as well as the old data stored on a backup tape library. In this example, he will mark on the map the respective relationships.

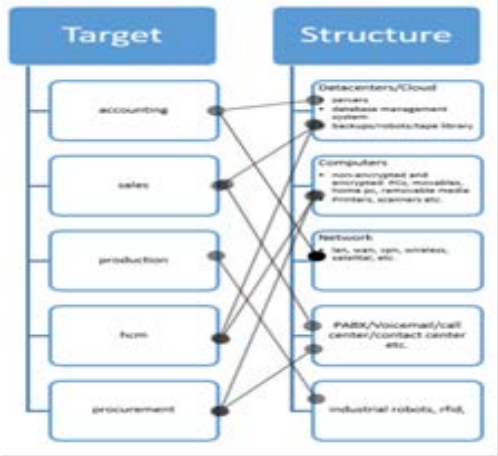

Figure 2: Target Map

8. Custody Map

The next step is to map the intended chain of custody framework necessary to ensure the value of the evidence. For this step, the investigator initially indicates on the map the major tools and forensic methods he wants to use not only in the search and seizure, but also in other stages of the forensic work, as shown on the left side of Figure 3. Next, he must map the key chain of custody functions that he intends to use in each forensic tool, by marking on the diagram the relationship between the tool and the custody function.
The investigator must also indicate and highlight on this map the possible existence of evidence whose chain of custody records are not guaranteed by each forensic tools. Therefore, in such cases the investigator must also indicate which alternative method he intends to adopt in these cases.

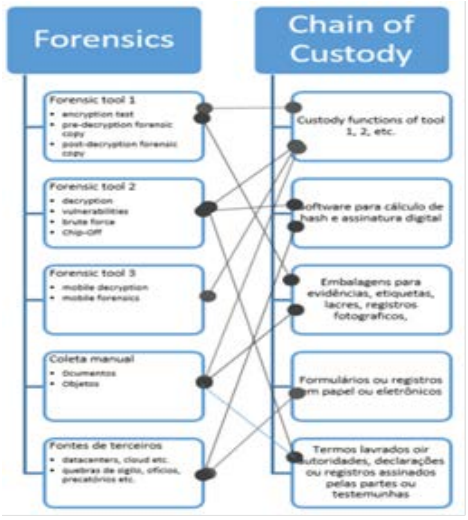

Figure 3: Custody Map

Therefore, the Custody Map must indicate the tools and methods of the forensic collection that one intends to adopt and which are the corresponding chain of custody records that ensure their probative value of the potential evidence when they are submitted to the court.

9. Overlap Map

The next step of the proposed method is to compare the Target Environment Map with the Custody Map. In order to do this, the two maps should be put side by side, so the researcher may indicate on the map the relationships between the components of the structure and the forensic tools or methods to be used in the identification, collection and preservation of potential evidence, as shown in the example of Figure 4. As a final result, the map indicates the relationship between the functions that are the subject of legal proceedings and the chain of custody of the component responsible for ensuring the probative value of the collected and examined evidence.

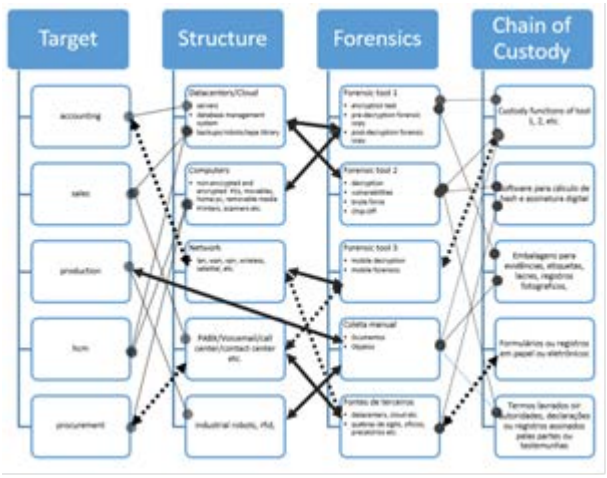

Figure 4: Overlap Map

With the final map mounted, the investigator shall then decide whether there is consistency between: (i) the evidences that he needs to collect in each function in the target environment, (ii) and the possibility to create an accurate chain of custody. At this moment, he should seek any gaps about evidences not properly protected by chain of custody records, as indicated by the dashed lines in Figure 4, and any possible overlapping records that can mean lost time during the survey, due to the resources spent generating redundant chain of custody records. After that study, the investigator can confront it with Trace Map, if it exists, for an agile final quality verification.

Another improvement proposed in our work is the adoption of technologies like Web Ontology Language (OWL) and Resource Description Framework (RDF) in the direction of an expansible architecture to automate forensic procedures in an environment of the Semantic Web. This additional proposal complements studies from other researchers in order to automate collection tasks and evidence analysis. Among them it is necessary to highlight the structure of the Advanced Forensic Format (AFF) proposed by Garfinkel et al. [16] in 2006, extended in 2009 with the AFF4 version which currently has supported multiple data sources and logical evidence. In 2010, Ćosić and Bača [17] proposed the Digital Evidence Management Framework (DEMF) which applies the vision Five W`s and one H (who, what, when, where, why, and how) to the chain of custody connected to digital signatures and real data such as geolocation to record the handling of evidences. In 2012, Garfinkel et al. [18] grounded on the chain of custody concept (CoC) presented the electronic chain of custody (e-CoC) which aims to replace the paper form for a framework based on Semantic Web technologies from OWL and RDF. In the same direction, Gayed et. al. [18] proposed a method to represent and integrate digital evidences from various sources, they suggest a pragmatic and simple ontology to model evidence from different sources such as images of hard drives or capture of packets on networks. Thus, a parser captures the evidences and generates dynamic assertions representing those objects and associating them to their respective classes. After, an aggregate view makes up a knowledge base Web Ontology Language (OWL). Thus, the researcher can use the standard consultation language Resource Description Framework (RDF) to carry out consultations and transactions with the modeled heterogeneous evidences, allowing the discovery of complex patterns and relationships. Considering these studies, our model proposes the adoption of a forensic tool to automatize the creation and use of Target Map, Evidence Map and Overlap Map considering OWL, RDF and other mentioned formats in the direction of a Semantic Web application.

10. Results and Discussion

The proposed method provides a quicker, wider and more objective method to improve the choice of a better chain of custody mechanisms, through:

a) Agile way to map targets and systems submitted to judicial investigations.
b) Agile way to map forensics tools and, especially, the chain of custody functions and methods.
c) Effective visual format to communicate with both computer forensics investigators and courts.
d) Wider vision about chain of custody gaps and overlaps than those provided by each forensic tool.
e) Faster preview of oversights and errors that could jeopardize the probative value of evidence.

f) Easier way to view overlaps that mean waste of resources, as time and space, due to the unnecessary generation of redundant chain of custody records.
g) Support the planning of computer forensic activities.
h) Support for the rational choice of forensic tools and mechanism of chains of custody.
i) Support for better execution of forensic procedures.
j) Support for the protection of the chain of custody.
k) Strengthening of the probative value of evidence.

The proposed model provides a simple solution to the problem mentioned in the introduction chapter of this paper and fills a gap since there are not in the literature effectives solutions about an agile and visual approach to confront the evidences that are intended to be collected with the tools that will be used to assure the forensic value of the chain of custody.

Examining the literature, it indicates that some authors, as in [10], propose the use of network maps to represent in details the procedures, tasks and sub-tasks that the investigator intends to carry out at the crime scene, but differ from the proposed model because they embrace much more details, impractical in the context, have different goals and do not consider as a priority the quality of the chain of custody and the communication with the law operators.

11. Conclusions and Future Works

The proposed method fulfills the need to assist computer forensics investigators in their responsibility to ensure the probative value of the evidence they collect, preserve, analyze and present in court, and presents a visual and easy way to understand the main technical elements for law operators to assess the probative value of the evidence they receive in judicial processes.

As a development, the authors suggest the incorporation of this model into the formats adopted by leading forensic tools, as well as to create an OWL and RDF based model designed to the widest and automatic integration with forensic software applications.

References

[1] B. Carrier, “Open Source Digital Forensics Tools: The Legal Argument,” 2002.
[2] B. SANOU, “ICT Facts & Figures. The world in 2015.,” ITU 150 AÑOS (1865 - 2015), 2015. [Online]. Available: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.
[3] FBI, “2014 Internet Crime Report,” 2015.
[4] Symantec, “Internet Security Threat Report 2016,” vol. 19, no. April, 2013.
[5] N. I. of Justice, “Crime Scene Investigation: Guides for Law Enforcement | National Institute of Justice.” [Online]. Available: http://www.nij.gov/topics/law-enforcement/investigations/crime-scene/guides/pages/glossary.aspx. [Accessed: 16-Apr-2016].
[6] Y. Prayudi and Azhari, “Digital Chain of Custody : State Of The Art,” Int. J. Comput. Appl., vol. 114, no. 5, pp. 1–9, 2015.
[7] SWGDE, “SWGDE Best Practices for Collection of Damaged Mobile Devices,” 2006.
[8] G. Giova, “Improving Chain of Custory in Forensic Investigation of Electronic Digital Systems,” Int. J. Comput. Sci. Netw. Secur., vol. 11, no. 1, pp. 1–9, 2011.
[9] S. R. Selamat, R. Yusof, and S. Sahib, “Mapping Process of Digital Forensic Investigation Framework,” J. Comput. Sci., vol. 8, no. 10, pp. 163–169, 2008.
[10] H. I. Bulbul, H. G. Yavuzcan, and M. Ozel, “Digital forensics: An analytical crime scene procedure model (ACSPM),” Forensic Sci. Int., vol. 233, no. 1–3, pp. 244–256, 2013.
[11] G. Giova, “Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems,” Int. J. Comput. Sci. Netw. Secur., vol. 11, no. 1, pp. 1–9, 2011.
[12] J. Aguilar, T. Barnes, J. Browne, B. A. Hamilton, Y. Burney, J. Byrd, R. Mcelroy, A. Denmark, L. Hartman, and G. Matheson, “Forensic Science Laboratories : Handbook for Facility Planning , Design , Construction , and Relocation.”
[13] Y. Guo, J. Slay, and J. Beckett, “Validation and verification of computer forensic software tools-Searching Function,” Digit. Investig., vol. 6, no. SUPPL., 2009.
[14] Robert E. Horn, “Information Mapping,” Train. Bus. Ind., vol. 11, no. 3, pp. 1–10, 1974.
[15] Selamat Siti Rahayu, N. H. Hassan, Y. Robiah, and M. F. Abdollah, “A Forensic Traceability Index in Digital Forensic Investigation,” J. Inf. Secur., vol. 04, no. 01, pp. 19–32, 2013.
[16] S. L. Garfinkel, D. J. Malan, K.-A. Dubec, C. C. Stevens, and C. Pham, “Advanced Forensic Format: An Open, Extensible Format for Disk Imaging,” Adv. Digit. Forensics II FIP Int. Conf. Digit. Forensics, vol. 222, pp. 17–31, 2006.
[17] J. Ćosić and M. Bača, “A framework to (Im)Prove „Chain of Custody“ in Digital Investigation Process,” Proc. 21st Cent. Eur. Conf. Inf. Intell. Syst., pp. 435–438, 2010.
[18] T. F. Gayed, H. Lounis, and M. Bari, “Cyber Forensics : Representing and (Im) Proving the Chain of Custody Using the Semantic web,” Cogn. 2012 Fourth Int. Conf. Adv. Cogn. Technol. Appl., no. Im, pp. 19–23, 2012.

Pedro Luis Prospero Sanchez is an electrical engineer, PhD and livre-docente in Electrical Engineering by the Polytechnic School of the University of São Paulo. Holds a degree in law from the Law School of the University of São Paulo and is an Associate Professor of the Electronic Systems Engineering Department of the Polytechnic School of the University of São Paulo, where he leads the area of education and research in Legal Engineering, Science and Forensic Technology. Is the coordinator of the Group of Legal Engineering, Science and Forensic Technology of the University of São Paulo.

Giuliano Giova is a B.Sc. in Economics by Centro Universitário Álvares Penteado and a M.Sc. in Electronic Engineering by the Polytechnic School of the University of São Paulo. He is now a PhD student in the Polytechnic School of the University of São Paulo. His research interests include electronic digital systems, computer science and engineering forensics. He is the director of Instituto Brasileiro de Peritos em Comércio Eletrônico e Telemática (Brazilian Expert Witness Institute). He is a member of IEEE.