Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems

Giuliano Giova

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

Summary
Forensic investigators should acquire and analyze large amount of digital evidence and submit to the court the technical truth about facts in virtual worlds. Since digital evidence is complex, diffuse, volatile and can be accidentally or improperly modified after acquired, the chain of custody must ensure that collected evidence can be accepted as truthful by the court. In this scenario, traditional paper-based chain of custody is inefficient and cannot guarantee that the forensic processes follow legal and technical principles in an electronic society. Computer forensics practitioners use forensic software to acquire copies or images from electronic devices and register associated metadata, like computer hard disk serial number and practitioner name. Usually, chain of custody software and data are insufficient to guarantee to the court the quality of forensic images, or guarantee that only the right person had access to the evidence or even guarantee that copies and analysis only were made by authorized manipulations and in the acceptable addresses. Recent developments in forensic software make possible to collect in multiple locations and analysis in distributed environments. In this work we propose the use of the new network facilities existing in Advanced Forensic Format (AFF), an open and extensible format designed for forensic tolls, to increase the quality of electronic chain of custody.

Key words:
Computer forensics, network forensics, chain of custody, distributed evidence management system.

1. Introduction

In a judicial process, evidence is used to demonstrate the truth and, as a consequence, they often affect the outcome of the case. Modern practices grant the judge a good deal of independence in matters relating to the admission of evidence, having as limit that this discretion must be consistent with the law basic principles, fairness, rationality, reasonability, and efficiency. Efficiency should be nearly as important as fairness, but naturally the presentation of evidence remains an adversary process and in process fairness it has been preferred over efficiency. [1].
In U.S., this question is oriented by Federal Rules of Evidences, especially Rule 901. Briefly, it says that evidence admissibility depends on the qualities perceived by judge or jurors. As a consequence, the evidence admissibility is better associated with the existence of a solid chain of custody, which contributes to the fairness, efficiency and reliability of the process. In this way, we consider that digital evidence can't be admitted without chain of custody, because usually it is away from sensory perception.
The U.S. National Institute of Justice (NIJ) defines chain of custody as "a process used to maintain and document the chronological history of the evidence". This means control over the individual's names collecting the evidence and each person or entity subsequently having custody of it, the dates the items were collected or transferred, the agency and case number, the victim's or suspect's name, and a brief description of each item [2].
The production of evidence in the modern digital world is a complex task for these reason we consider essential the, digital evidence should be accepted as valid in court only if the chain of custody can assure exactly what was the evidence, why it was collected and analyzed and how evidentiary data was collected, analyzed and reported. Additionally, the chain of custody must demonstrate exactly where, when and who came into contact with the electronic evidence in each stage of investigation and any manipulation of the evidence [3].
The increasing complexity of forensic science in the digital area leads researchers to claim that traditional computer forensics "is in the edge of a precipice", especially because of the great diversity of electronic devices to be sized and the intensive growth of data amount that must be collected and examined during a digital forensic investigation [4].
This growing complexity makes harder to create and maintain a reliable chain of custody and exposes a wide gap between general evidentiary criteria based on traditional forensic procedures and the scientific community point of view about the risks and conditions necessaries to consider reliable any contemporary digital evidence.

2. Chain of Custody Challenges

The world is experiencing an intense expansion in information and telecommunication utilization. Electronic systems are growing in complexity and diversity,

Manuscript received January 22, 2011
Manuscript revised January 26, 2011

becoming omnipresent, embedded and interconnected. At the same time, there is a severe increase in the quantity of data created into modern societies that are dispersed and flow between servers, personal computers, handhelds, mobile phones, worldwide or personal networks, and any kind of high tech devices.

The US DOJ National Institute of Justice encourages and supports research, evaluation and development projects to improve criminal justice policy and practice. In 2011, it is especially interested in research, technology and tools for digital evidence covering (as in DOJ original text) [5]:

- ✓ Forensic tools for mobile cellular devices: "digital forensic tools used to process evidence from cell phones acquired data from specific locations in the data storage space in the phone's subscriber identity module (SIM) card. Essentially, the tools are designed to 'search' where data with forensic value is expected to be found. This is problematic from a forensic perspective, because data with forensic value can in fact be hidden in other file locations. This problem will grow more acute with the introduction of fourth generation (4G) cell phones. These phones will provide increased data storage capability, while maintaining or reducing the size of the phone, by maximizing the use of the available data storage space. As a result, some of the data storage areas that were not forensically relevant, and which current forensic tools ignore, may become forensically relevant"
- ✓ Data forensics in the cloud computing environment: "Internet-based or Cloud computing is a means of accessing computing resources with minimal infrastructure investment. The accessing of applications and storing of data through the Internet, rather than on the hard drive of a local computer or server, which is what characterizes Cloud computing, is challenging from a forensic perspective. One challenge is that if an application is accessed through the Internet, temporary files with forensic value that would traditionally have been stored on a computer hard drive will be stored within a virtual environment and lost when the user closes the application. With data residing on external servers, the ability to demonstrate that the data obtained is uncompromised also becomes more problematic".
- ✓ Forensic tools for Voice over Internet Protocol (VoIP) communications: "There is a need for forensic tools to extract data with forensic value from computers used for Internet-based telephony, such as call-log data".
- ✓ Forensic tools for vehicle computer systems: "Computers have become an integral component of motor vehicles, including event data recorders (EDRs), or 'black boxes', which can be used for accident investigation".

The DOJ document and other papers discussed in this work reflect the electronic crimes amount and sophistication and electronic life investigation. The evaluation of this kind of evidence requires expertise not commonly known by the judges. Moreover, typical digital evidence can be accessed by first responders, bailiffs, police offices, investigators, expert witnesses, prosecutors, defense attorneys, and may even be corrupted by anonymous people with hidden access to the evidence. For these reasons, courts must be aided by forensic investigators who have strong knowledge and experience in information technology and telecommunications [6].

To be reliable, exams of volatile digital data require ever more a vast technical knowledge, a secure laboratory, updated forensic hardware and software environment, and long deadlines to permit in depth analysis.

Another issue is that today's investigations rely on automated software tools, thus the reliability of investigation outcomes is predominantly determined by the correctness of such tools and their application process. Therefore, the tools used in an investigation must be audited to assure that the tool, techniques and procedures are reliable and function as intended [6].

The technical amplitude makes more difficult to obtain secure and reliable results through any forensic analysis. Recent studies corroborate the perception that the life cycle of digital evidence is getting more complex and each stage increases the probability of a breach that can violate the chain of custody. The result is a scenario where is increasingly difficult for the court to evaluate the evidence and guarantee the integrity of the digital evidence. As a consequence, it is increasingly difficult for the society to accept that digital evidence is genuine and reliable [4].

Usually, courts receive and accept reports created by the practitioners as accurate, at least in principle, but if there is a dispute about the facts during investigation the court interactions will evaluate the question in depth and establish the admissibility and weight of evidences [7].

Knowing the hash code of digital files (digital fingerprint), the location of evidence and the name of practitioners is no longer enough for court. The electronic signature of each object, the *right location* where each piece of digital evidence is handled, the *right time* of access to the evidence, the *correct identity* of all people that had contact with evidence and *complete description* of all transactions is also required. Moreover, there must be accurate logs about digital evidences and these logs must be audited [3].

These reasons compel the courts, trial parties and forensic investigators to require a strong and automated system to maintain chain of custody of digital evidence, a system consistent with a digital society.

This kind of system must serve court and practitioners, but will also interact with the rest of the society. Frequently the first evidences of a crime are discovered during an internal investigation or incident response inside a company.

The IT staff should have the ability to maintain and document digital contents, including its exact location, especially when computer evidence may be presented in court. By not creating and preserving the digital chain of custody, a company is leading itself into an investigation that is compromised from the beginning.
Legislation around the world establishes obligations for all types of business to preserve electronic data that may be relevant to legal matter. In U.S. the Sarbanes-Oxley Act imposes severe penalties and the Securities Exchange Commission rules required data retention for six years. So data must be preserved and maintained in a manner that verifies its authenticity and integrity and also a report is critical to prove a chain of custody [8].
Some modern forensic software describes where every file is located and its many properties, including creation date, last accessed date, and deleted date. That software enforces data authenticity verification using standard algorithms to calculate cyclical redundancy checksum and generating hash values, a unique numerical value based upon the contents contained in original evidence or its image copy. Moreover, modern forensic software adopt the concept of central authentication and grant permission servers, which grant session keys for authorized users and services and monitors all examination activity for chain of custody documentation. Most of those controls are made in real time online mode, over local or wide area networks. There is also other commonly used forensic software that have only elementary functions for chain of custody control, like some forms where the user fills investigator data (like name, address, phone, and e-mail) and case data (like case number and name) [8].
Part of this software adopts open standards for automation, although others use proprietary format to implement chain of custody automation. There are several main forensic formats used by commercially-available or open tools to collect and store both evidence data and chain of custody data. Some tools support other formats, but in general the evidence containers are not interoperable or interchangeable among different tools [9].

3. Problem Setting

In general terms, the admission of computer evidence in U.S. is governed by Federal Rule Evidence 901 as a general document admission, but must be considered other governmental guides and norms about electronic evidence and search and seizure. The USA Patriot Act resulted in a number of significant changes to various Federal statutes governing the searching and seizing of computers and the gathering of electronic evidence [10]. The Canada Evidence Act specifically addresses the authentication of computer evidence. Other countries in the world have its own legislation and rules about recommended forensic measures, which naturally are related to their own law enforcement infrastructure and to a particular set of forensic tools and expertise [8].
In the nongovernmental area there is a similar situation, each company has its own corporate policies for incident response and particular procedures to deal with computer investigation. Some companies have operations and affiliates in several countries worldwide, which may oblige the collection and investigation of sparse digital evidence under different authorities and laws. In this case, related evidences from different countries may be collected with incompatible forensic tools, each one specific of the local affiliate or the local law enforcement agency. Also, many transactions to be investigated occur among different companies or individuals around the world, since a main characteristic of the Internet is that most transactions in the World Wide Web overcome geographical or political boundaries and its related infrastructure [8].
This scenario circumscribes the objective of this work: to review difficulties and formulate suggestions to make a more reliable chain of custody of digital evidence, making it more consistent to courts necessities regardless of country, company or tool where digital evidence is collected.
Within this objective, this work explores gaps between the traditional chain of custody and the modern studies point of view about the risks and requirements concerning reliability of contemporary digital evidence. This paper also aims to contribute to the discussion about the trend to establish a worldwide standard more suited to maintain chains of custody throughout the lifecycle of digital evidence and helps the improvement of new versions of chain of custody software. This work will not define or select any standard itself, because this is a mission outside of its scope.

4. Approaching Digital Forensics Reality and Chain of Custody

Traditional chain of custody is mainly based on filling in paper forms or electronic forms the name of investigators, a concise description of the evidence under examination and some kind of hash code. Modern forensic software adds better evidence description, electronic user identification, digital signature and automatic audit trail.
However, there is still a great distance from the usual chain of custody software to the effective court questions and users, this is, the digital doubts of first responders, bailiffs, police offices, investigators, expert witnesses, prosecutors, and defendants.
Pollit [11] has made an *ad hoc* review of principal digital forensic process models, focusing on the evolution of digital forensics process scientific basis, concluding that the area is experiencing a rapid transformation and the

process models definitions are becoming more robust. Based on Pollit's research, we have identified some relevant points related to the process model, the admission of evidence in a court and the chain of custody:

- ✓ In 2000, Noblet, et al. [12] presented a study about the relation between the investigation motives and the requirements of forensic science;
- ✓ In 2001, the Digital Forensic Research Workshop DFRWS[13]appointed a consensus that digital forensics is a process with "some reasonability";
- ✓ In 2002, Reith, Carr and Gunsch [14] presented a process model with 9 main steps: identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence;
- ✓ In 2003, Carrier and Spafford [15] presented the Integrated Digital Investigation Process that maps the digital investigative process to the physical investigative process, with 17 phases in 5 groups: readiness, deployment, physical crime scene investigation, digital crime scene investigation, and review phases;
- ✓ In 2003, Stephenson [16] starting from Digital DFRWS framework, developed a process model for incidents root cause analysis with 9 steps: collecting evidence, analysis of individual events, preliminary correlation, event normalizing, event deconfliction, second level correlation (consider both normalized and non-normalized events), timeline analysis, chain of evidence construction, and corroboration;
- ✓ In 2003, Carrier [17] concluded that no software is perfect and therefore each analysis tool will have an associated tool implementation error based on its history, value useful to evaluate result reliability;
- ✓ In 2003, Mocas [18] found out that there are multiple contexts for digital forensics, such as law enforcement context, a military context and a business system security context, and therefore studied in a legal setting what properties are desirable on evidence and process;
- ✓ In 2004, Baryamueeba and Tushabe [19] suggested a modification to Carrier and Spafford's model of 2003 inserting two additional phases to avoid inconsistencies in the investigation, getting the isolation of scenes into primary crime scene (the computer) and the secondary crime scene (the physical crime scene);
- ✓ In 2004, Beebe and Clark [20] stated that previous process models were single tier, but real process tends to be multi-tiered, therefore introduced an objectives-based framework looking for technology neutrality and wide user community applicability;
- ✓ In 2004, Carrier and Spafford [21] added new elements to the digital forensic framework: events and event reconstruction;
- ✓ In 2004, Pollitt [22] stated that forensics is not a single process, in fact is a set of tasks grouped into functions related to the process that is being applied (role) and bound by constraints;
- ✓ In 2005, Ruibin, Yun and Gaertner [23] proposed a method to bind computer intelligence to the current computer forensic framework and a case-relevance concept to measure the importance of any information to a given case;
- ✓ In 2006, Erbacher, Christensen and Sundberg [24] stated that network forensics is not a linear process because have multiple feedback loops;
- ✓ In 2006, the National Institute of Standards and Technology (NIST) published the Guide to Integrating Forensic Techniques into Incident Response [25] defining the basic forensic process having four phases: collection, examination, analysis, and reporting.

Many other different process models and frameworks have resulted from an increasing amount of researches that have been made during the last decade about digital forensics process.

The consolidation of study's results shows that does not exists a mature and operational chain of custody framework suited for real heterogonous and unstable digital process, especially due to the inexistence of a really standard and stable process model.

This work have as target to approach chain of custody frameworks with the real digital forensics process or, in other words, to join the real controls about tasks and persons that accesses evidence with controls made by chain of custody software.

To show in more detail our study, we will use as base some recent researches. In 2010, Ćosić et Miroslav [3] [21] proposed a conceptual digital evidence management framework (DEMF) to improve the chain of custody of digital evidence in all phase of investigation.

His studies recommend a process using hash code for fingerprint of evidences (what), hash similarity to changes control (how), biometric identification and authentication for digital signing (who), automatic and trusted time stamping (when), GPS and RFID for geo location (where). Those controls can be implemented through a database to record activities done by first responders, forensic investigators, court expert witness, law enforcement personnel, and police officers.

With this approach, the chain of custody model becomes closer to the real word than the old fill in the blanks used by traditional forensic procedures and software.

Köhn, Eloff and Olivier [7] have proposed a paradigm for modeling forensic processes using the Unified Modeling Language (UML). They have defined a digital forensic process model (DFPM) derived from Krause model and combined with U.S. DOJ reference for evidence of

computer-related crimes. In essence, the process model shows five main activities:

- ✓ collect
- ✓ authenticate
- ✓ examine
- ✓ analyze
- ✓ report

In [7]) authors also show five main role players:

- ✓ first responder
- ✓ investigator
- ✓ prosecutors
- ✓ defense
- ✓ court

Certainly, there can be several variations of this model according to each country, legislation, court organization, type of legal case, and many other factors, but in all cases the modeling approach can furnish a conceptual scheme to better know the players and the activity interconnected and involved with digital evidences.

The simplified process model from [7] can be compared with the several formats used in the forensic software to maintain the chain of custody.

Digital evidence can be stored in open or proprietary formats. The CDESF working group [22] surveyed in 2006 the following disk image main formats: raw, AFF, DEB (Qinetiq), EnCase, Expert Witness, gfzip, ProDiscover and SMART. Raw format doesn't store metadata; some of the other formats can store metadata in the same file as the evidence, others in separate files.

Most formats can store a limited number of metadata, like case name, evidence name, examiner name, date, place, and hash code to assure data integrity. Other formats allow the storage of arbitrary metadata, specially the Advanced Forensic Format (AFF) and Gfzip format [22]. Since it is an open, configurable and expansive format, this work selected AFF as a base to advance the study about chain of custody, but the same study can be applied to other formats.

5. The Advanced Forensic Format

In 2006, Garfnkel et al. [23] defined the Advanced Forensic Format (AFF) as a file format and container to store digital evidence in a single archive containing both a sector-to-sector copy of original data stored as an image and arbitrary metadata that implicitly refers to that image and its content.

Metadata can be system metadata, like sector size or device serial number. Metadata can also be user-specified, such as identification of forensic computer, the user of the forensic software, software configuration or department name.

Over years of use, Cohen et al. [24] have observed problems to be corrected in the first version of AFF standard (AFF1). They also perceived an intense evolution in the digital forensic processes. One of the changes was that some practitioners started to work in distributed environments. Analysis began to be made at multiple locations and performed by different individuals. This kind of necessity was contemplated in 2009 by a new version called Advanced Forensic Format 4 (AFF4).

The AFF4 version extends preceding AFF model and functionalities to support multiple data sources, logical evidence and several others improvements. The most important improvements for this work are the possibility to store arbitrary metadata and the support for forensic workflow.

6. Resource Description Framework (RDF)

As demonstrated, a chain of custody software can be closer with reality if the format used allows the creation and maintenance of arbitrary metadata about fingerprint of evidences (what), procedures (how), digital signing (who), time stamping (when), and geo location (where). Although storing metadata is not enough to have an effective chain of custody software system, a method to define and manipulate metadata is necessary.

The Resource Description Framework (RDF) is a XML-based standard and language, created by World Wide Web Consortium (W3C) to facilitate processes execution among different devices. Enables encoding, exchange and use of device metadata having both human-readable and machine-processable vocabularies.

RDF use Universal Resource Identifier (RDI) to identify objects, such as metadata, as explained in The Internet Society RFC3986, RFC4395 and others. Each object identified by a URI can be also described by a Universal Resource Name (URN), its name, and a Uniform Resource Locator (URL), its location.

With this approach we get the interchangeability of metadata created by different resources and in any location, a basic concept for Semantic Web [25].

7. Chain of Custody with AFF4 and RDF

Over the last years, researchers have proposed several solutions on the use of AFF4 and RDF resources to improve digital forensics process model or software. As explained above, they improved also the chain of custody functionalities, as an indirect consequence.

This work complements those studies demonstrating that AFF4 and RDF can be better explored to improve chain of custody reliability in digital investigations.

We propose the use of AFF4 or similar metadata flexible schema in conjunction with strong RDF descriptions having the objective of furnish sets of frameworks to automate the interaction between the real world and most of chain of custody software, providing in this way support to both human-readable and machine-processable forensic

controls. Moreover, this approach can bring facilities to let forensic software closer to worldwide broad and highly diversified digital investigation schemes, maintaining the overall reliability [25].

AFF4 and similar frameworks can store arbitrary metadata and these metadata can represent a great amount of real world objects. Uses the technology called Universal Resolver (UR) suited to resolve external references to forensic objects and facilitating universal visibility of evidence and sharing evidence among different instances on computer network.

Access and manipulation of AFF4 evidence over the network can be done with the HTTP protocol, making easier to share whole evidences files or part of them, as byte range. Those characteristics are especially important for remote investigations and to implement an effective distributed system to manage evidence, what is adequate to a great and diversified roll of digital forensics processes [24].

To demonstrate in more detail this approach, this work selects the DEMF framework, defined by Ćosić and Bača [21], as a model to ensure the security of a chain of custody. In a simplified vision, author's framework can be presented as:

```
DEMF = f {fingerprint_of_file,          //what
          biometrics_characteristic,    //who
          time_stamp,                   //when
          gps_location,} ;              //where
```

(1)

It is clear that this framework is focused on interactions with the real world devices, such as GPS, time stamp generators, biometrics devices, and hash code automatic calculators, leaving chain of custody closer with real world and aiding digital evidence to be better accepted and understood by court.

This criterion is a core point of our study, because modern chain of custody will be reliable only if real world facts were accurately represented into a chain of custody. This means the forensic system should capture environmental data directly from the appropriated transducers.

In our example, such solution will be feasible if DEMF or similar schema should be implemented in expansible open format such as AFF4 and if, in same environment, the RDF should be used to manage many arbitrary metadata that directly interact with real world and remote transducers.

Differently of what (possibly) occurs with Expert Witness Format (EWF) and other proprietary formats, the AFF format can store great amount of properties (metadata) related to the forensic image and its environment, such as acquisition date, sector size, and many other proprieties. This solution should be based on AFF version 4, not on AFF1, because the new version is a redesign of the earlier architecture and extended it format toward a global evidence management [12].

AFF4 user-specific metadata functionalities [24] will be used by means of a RDF framework [21]. In simple terms, RDF statements should be used to describe object properties as a tuple, since all metadata can be reduced to a tuple notation [24]. The general format is:

SUBJECT ATTRIBUTE VALUE (2)

Real world objects can be described through a Universal Resource Name (URN), such as:

- ✓ ISBN-10 and ISBN-13 of Federal Rules of Evidence Manual:
  urn:isbn10: 0327159219
  urn:isbn10: 978-0327159216

- ✓ IETF's RFCs:
  urn:ietf:rfc:5832
  urn:ietf:rfc::2442

Using URN in AFF4 environment we get the following example [24]:

urn:aff4:83a3d6db-85d

In [24], Cohen, et al. describes the use of distributed evidence management system AFF4 based in a fictitious company having offices in two distinct cities, each one with its own forensic computer laboratory connected via WAN.

In our work, we explore a similar example, but not only in a fictitious company. Expanding the use of RDF and adopting frameworks like DEMF defined by Ćosić and Bača [21], it is possible to extend those functionalities to the court environment.

This approach will permit a direct interaction between the forensic system and first responders, bailiffs, police offices, investigators, expert witnesses, prosecutors, and defense attorneys, as illustrated in the following simplified diagram.

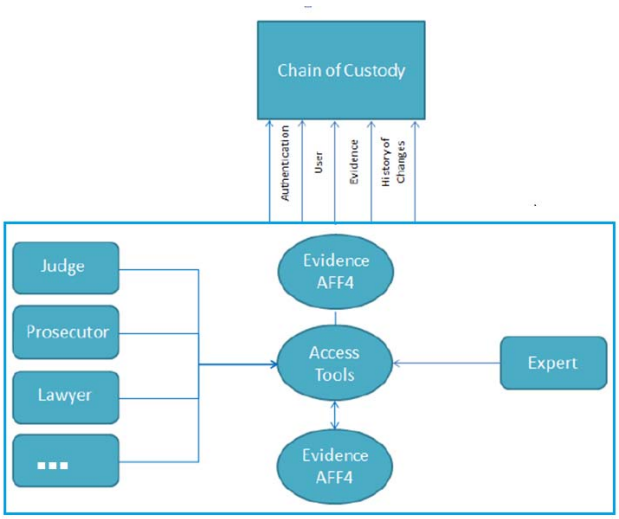

Figure 1: Simplified block diagram

The sample block diagram can be used to design a simplified UML, as follow.

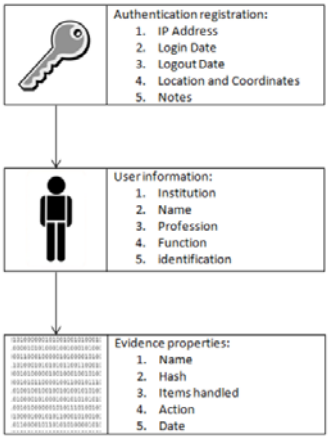

Figure 1: Simplified UML

Starting from these models, the RDF implementation is represented, in a free form, as follows:

```
rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
<!--xmlns:aff4="http://192.168.0.1/evidence01/docs/aff4.xml#" -->>
        <rdf:Description rdf:about="urn:aff4:98a6dad6-4918
        aff4/evidence01.aff4">
            <aff4:access>
                <aff4:ip>192.168.1.20</aff4:ip>
                <aff4:dateLogin>1294230200</aff4:dateLogin>
                <aff4:dateLogout>1294230800</aff4:dateLogout>
                <aff4:location>Washington, DC USA</aff4:location>
                <aff4:coordinatesNorth>385342</aff4:coordinatesNor
                th>
                <aff4:coordinatesWest>770211</aff4:coordinatesWest
                >
                <aff4:note>Change reports.</aff4:note>
            </aff4:access>
            <aff4:user>
                <aff4:institution>International Law
                Institute</aff4:institution>
                <aff4:name>Willians</aff4:name>
                <aff4:profession>Lawyer</aff4:profession>
                <aff4:function>Prosecutor</aff4:function>
                <aff4:idType>America Bar Association</aff4:idType>
                <aff4:idNumber>25365XX</aff4:idNumber>
            </aff4:user>
            <aff4:evidence>
                <aff4:name>Evidence01</aff4:name>
                <aff4:type>AFF4</aff4:type>
                <aff4:hash>db64e67f5b41bbc0f3728c2eae4f07eb</aff
                4:hash>
            </aff4:evidence>
            <aff4:history>
                <aff4:item>
                    <aff4:name>report03.rtf</aff4:name>
                    <aff4:fullPath>AFF4:CaseExample0001/Reports/r
                    eport03.rtf</aff4:fullPath>
                    <aff4:date>1294230300</aff4:date>
                    <aff4:action>delete</aff4:action>
                    <aff4:field>all</aff4:field>
                </aff4:item>
                <aff4:item>
                    <aff4:name>report04.rtf</aff4:name>
                    <aff4:fullPath>AFF4:CaseExample0001/Reports/r
                    eport04.rtf</aff4:fullPath>
                    <aff4:date>1294230550</aff4:date>
                    <aff4:action>copy</aff4:action>
                    <aff4:field>all</aff4:field>
                </aff4:item>
            </aff4:history>
        </rdf:Description>
</rdf:RDF>
```

The presented method reveal that the use of RDF facilities together with AFF4 flexible metadata and its distributed evidence management is a strong tool to improve the chain of custody reliability, especially because this system should be based on real world transducers, such as GPS, motion detectors, environmental recorders, time-stamp generators, biometric identification and digital signatures.
The proposed method is, as an indirect consequence, an essential to the design and development of a really functional distributed evidence management and chain of custody control system. The solution should also adhere to the semantic web layered architecture.
This approach complements previous work led by others researchers, as described, improving chain of custody process model and software.

8. Conclusion

In this work we have presented a synthesis of scientific and technical studies regarding to the importance of metadata and the chain of custody to bring more reliable digital evidences to the court. We have explored the potential of AFF4 format and RDF structure to improve an

expansible open format that can reduce the distance between the actual *de facto* formats and the court and society needs.

This research is only at an initial stage and there are a number of tasks to be done and problems to be solved in future studies, such as:

(i) identify the main characteristics for a worldwide chain of custody control;
(ii) specify a common standard forensic format for chain of custody, considering AFF4, EWF and other formats;
(iii) implement an experimental chain of custody wide range solution using semantic web methods and technologies to support courts and practitioners and, also, allow machines to understand the meaning in chain of custody matter;
(v) integrate digital forensics software with the proposed chain of custody software.

AFF4 creators [26] explain that the world has been in a "Golden Age of Digital Forensics", but this is coming to an end. In the future digital forensics must be more efficient, and better coordinated as a team effort.

The approach suggested in this work increases the feasibility and reliability of distributed digital evidence system.

References

[1] BRIDGE, W. J. Burdens Within Burdens at a Trial Within a Trial. Boston College Law Review, 1982. ISSN Volume 23 Issue 4 Number 4.

[2] NATIONAL INSTITUTE OF JUSTICE. U.S. National Institute of Justice. Crimes Scene Guides, 2011. Avalible at: <http://www.ojp.usdoj.gov/nij/topics/law-enforcement/investigations/crime-scene/guides/glossary.htm>. Acessed in: Jan 2011.

[3] ĆOSIć, J.; BAčA, M. A Framework to (Im)Prove Chain of Custody in Digital Investigation Process. Proceedings of the 21st Central European Conference on Information and Intelligent Systems. [S.l.]: [s.n.]. 2010. p. 435-438.

[4] TURNER, P. Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags). Digital Forensic Research Workshop (DFRWS). New Orleans, LA: [s.n.]. 2005. p. 1-8.

[5] U.S. DEPARTMENT OF JUSTICE (DOJ), OFFICE OF JUSTICE PROGRAMS (OJP), NATIONAL INSTITUTE OF JUSTICE (NIJ). Solicitation: Electronic Crime and Digital Evidence Recovery. National Criminal Justice Reference Service, 2011. Avalible at: <http://www.ncjrs.gov/pdffiles1/nij/sl000957.pdf>. Acessed in: 2011.

[6] GUO, Y.; SLAY, J.; BECKETT, J. Validation and verification of computer forensic software tools - Searching Function. Digital Investigation, 2009. S12-S22.

[7] KÖHN, M.; ELOFF, H. P. J.; OLIVIER, M. UML Modeling of Digital Forensic Process Models (DFPMs). ISSA 2008 Information Security Innovative Mind Conference. [S.l.]: Proceedings. 2008.

[8] PATZAKIS, J. M. Maintaining The Digital Chain of Custody. Password - The ISSA Journal, Oak Creek/U.S., p. 14-15, 2003. ISSN February 2003.

[9] GARFINKEL, S. L. et al. Advanced Forensic Format: An Open, Extensible Format For Disk Imaging. [S.l.]: [s.n.], Cap. Chapter 2.

[10] UNITED STATES DEPARTMENT OF JUSTICE. Electronic Evidence and Search & Seizure Legal Resources. United States Department of Justice, 2011. Avalible at: <http://www.justice.gov/criminal/cybercrime/>. Acessed in: 2011.

[11] POLLITT, M. M. An Ad Hoc Review of Digital Forensic Models. Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07). [S.l.]: IEEE Computer Society. 2007.

[12] NOBLETT, M. G.; POLLITT, M. M.; PRESLEY, L. A. Recovering and Examining Computer Forensic Evidence. Forensic Science Communications, v. 2, n. 4, October 2000.

[13] DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS). A Road Map for Digital Forensic Research. Report From the First Digital Forensic Research Workshop (DFRWS). Utica, New York: [s.n.]. 2001.

[14] REITH, M.; CARR, C.; GUNSCH, G. An Examination of Digital Forensic Models. International Journal of Digital Evidence, 2002.

[15] CARRIER, B.; SPAFFORD, E. H. Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, 2003.

[16] STEPHENSON, P. Modeling of Post-Incident Root Cause Analysis. International Journal of Digital Evidence, 2003.

[17] CARRIER, B. Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. International Journal of Digital Evidence, 2003.

[18] MOCAS, S. Building Theoretical Underpinnings for Digital Forensics. Digital Forensic Research Workshop 2003. Cleveland: [s.n.]. 2003.

[19] BARYAMUREEBA, V.; TUSHABE, F. The Enhanced Digital Investigation Process. Digital Forensic Research Workshop 2004. Baltimore, Maryland: [s.n.]. 2004.

[20] BEEBE, N. L.; CLARK, J. G. A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. Digital Forensic Research Workshop 2004. Baltimore, Maryland: [s.n.]. 2004.

[21] CARRIER, B. D.; SPAFFORD, E. H. An Event-Based Digital Forensic Investigation Framework. Digital Forensic Research Workshop 2004. Baltimore, Maryland: [s.n.]. 2004.

[22] POLLITT, M. M. A Framework for Digital Forensic Science - Six Blind Men from Indostan. Digital Forensic Research Workshop 2004. Baltimore, Maryland: [s.n.]. 2004.

[23] CHAN KAI YUN, T.; RUIBIN, G.; GAERTNER, M. Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework. International Journal of Digital Evidence.

[24] ERBACHER, R. F.; CHRISTIANSEN, K.; SUNDBERG, A. Visual Forensic Techniques and Processes. Proceedings of the 9th Annual NYS. Albany: [s.n.]. 2006. p. 72-80.

[25] NATIONAL INSTITUTE OF STANDARDS AND

TECHNOLOGY. Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology. [S.l.]. 2006. (NIST Special Publication 800-86).

[26] ĆOSIć, J.; BAčA, M. Do we have a full control over integrity in digital evidence life cycle. 32nd International Conference on Information Technology Interfaces. Dubrovnik/Cavtat: Proceedings of ITI 2010. 2010. p. 429-434.

[27] COMMON DIGITAL EVIDENCE STORAGE FORMAT WORKING GROUP. Survey of Disk Image Storage Formats. Digital Forensic Research Workshop (DFRWS). [S.l.], p. 1-18. 2006.

[28] GARFINKEL, S. L. et al. Disk Imaging with the Advanced Forensic Format, Library and Tools. Research advances in digital forensics - second annual IFIP WG 11.9 international conference on digital forensics. Springer: [s.n.]. 2006.

[29] COHEN, M.; GARFINKEL, S.; SCHATZ, B. Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow. Digital Investigation, 2009. S57-S68.

[30] MILLER, E. An Introduction to the Resource Description Framework. D-Lib Magazine, n. May 1998, p. 1-8, 1998. ISSN ISSN 1082-9873.

[31] GARFINKEL, S. L. Digital forensics research: The next 10 years. Digital Investigation. S64-S73.

Giuliano Giova received the B.S degree in Economics from Centro Universitário Álvares Penteado. He now stays in Escola Politécnica da Universidade de São Paulo to obtain the M.S in Electronic Engineering. His research interest includes electronic digital systems, computer science and engineering forensics. He is director of Instituto Brasileiro de Peritos em Comércio Eletrônico e Telemática (Brazilian Expert Witness Institute for Electronic Commerce and Telematics). He is member of IEEE.