THE EVIDENCE PROJECT: BRIDGING THE GAP IN THE EXCHANGE OF DIGITAL EVIDENCE ACROSS EUROPE

Maria Angela Biasiotti, Mattia Epifani, Fabrizio Turchi

Institute of Legal Information Theory and Techniques of the Italian National Research of Council

Florence , Italy, 50127

mariangela.biasiotti@ittig.cnr.it, mattia.epifani@ittig.cnr.it, fabrizio.turchi@ittig.cnr.it

ABSTRACT

Based upon the assumption that the very nature of data and information held in electronic form makes it easier to manipulate than traditional forms of data, that all legal proceedings rely on the production of evidence in order to take place and that electronic evidence is no different from traditional evidence in that is necessary for the party introducing it into legal proceedings, to be able to demonstrate that it is no more and no less than it was, when it came into their possession the EVIDENCE Project aims at providing a road map (guidelines, recommendations, technical standards) for realising the missing Common European Framework for the systematic and uniform application of new technologies in the collection, use and exchange of evidence. This road map incorporating standardized solutions aims at enabling all involved stakeholders to rely on an efficient regulation, treatment and exchange of digital evidence, having at their disposal as legal/technological background a Common European Framework allowing them to gather, use and exchange digital evidences according to common standards, rules, practises and guidelines. EVIDENCE activities will also aim at enabling the implementation of a stable network of experts in digital forensics communicating and exchanging their opinions and contributing as well to the building up of a stable communication channel between the public and the private sectors dealing with electronic evidence.

Keywords: digital evidence, digital evidence exchange, metadata, formal languages.

1. THE CONTEXT

All legal proceedings rely on the production of evidence in order to take place. Electronic Evidence is no different from traditional evidence in that is necessary for the party introducing it into legal proceedings, to be able to demonstrate that it is no more and no less than it was, when it came into their possession. In other words, no changes, deletions, additions or other alterations have taken place. The very nature of data and information held in electronic form makes it easier to manipulate than traditional forms of data. When acquired and exchanged integrity of the information must be maintained and proved. Legislations on criminal procedures in many European countries were enacted before these technologies appeared, thus taking no account of them and creating a scenario where criteria are different, uncertain, regulations are not harmonized and aligned and therefore exchange among EU Member States jurisdictions and at transnational level is very hard to be realized. What is missing is a Common European Framework to guide policy makers, law enforcement agencies and judges when dealing with digital evidence treatment and exchange. The EVIDENCE project interpreted this request by defining it as:

- the need for a common background for all actors involved in the Electronic Evidence life-cycle: Policy makers, LEAs, Judges and Lawyers;
- the need for a common legal layer devoted to the he regulation of Electronic Evidence in Courts
- the need for standardized procedures in the use, collection and exchange of Electronic

Evidence (across EU member States).

In response to the above needs and gaps the *EVIDENCE* project aims at providing a *Road Map* (guidelines, recommendations, technical standards) for realizing the missing Common European Framework for the systematic and uniform application of new technologies in the collection, use and exchange of evidence. This *Road Map* incorporating standardized solutions would enable policy maker to realize an efficient regulation, treatment and exchange of digital evidence, LEAs as well as judges/magistrates and prosecutors and lawyers practising in the criminal field to have at their disposal as legal/technological background a Common European Framework allowing them to gather, use and exchange digital evidences according to common standards and rules.

In order to produce this common, unique European way/ approach to the treatment and exchange of electronic evidence, the EVIDENCE project has identified as relevant the following steps:

- Developing a common and shared understanding on what electronic evidence is and which are the relevant concepts of electronic evidence in involved domains and related fields (digital forensic, criminal law, criminal procedure, criminal international cooperation);
- Detecting which are rules and criteria utilized for processing electronic evidence in EU Member States, and eventually how is the exchange of evidence regulated;
- Detecting of the existence of criteria and standards for guaranteeing reliability, integrity and chain of custody requirement of electronic evidence in the EU Member States and eventually in the exchange of it;
- Defining operational and ethical implications for Law Enforcement Agencies all over Europe;
- Defining implications on data Privacy issues;
- Identifying and developing technological functionalities for a Common European Framework in gathering and exchanging electronic evidence;
- Seizing the EVIDENCE market.

The project is now at its halfway mark and step 1-5-7 are completed whilst step 2-3-4-6 are on the way to produce final assessment.

2. PRELIMINARY REMARKS ON THE CONCEPT OF ELECTRONIC EVIDENCE

Before going for any kind of classification the very first issue at stake has been to set the right scenario and to fix the range and scope of the categorization task with respect to the Project aims and goals. In this sense, our aim is to develop a framework for the application of new technologies in the collection, use and exchange of evidence between Courts of the EU Member states. So, the main keywords to be considered are: Source of Evidence, Authenticity, Evidence, *ICT* and Exchange.

The use of *ICT* associated with evidence is often described utilizing two main expressions: Electronic Evidence and Digital Evidence. Is the first one different from the second or are they just synonyms?

We know for sure that both electronic and digital evidence originate from the so called sources of evidence and that there is a specific need to carry on a forensics analysis in order to identify the evidence itself. We are also aware of the fact that these sources might be electronic, or non electronic and that in the latter case it can acquire the status of "digital/electronic evidence " if digitized.

The analysis of the most significant sources of information demonstrated that there is no uniform use of the terms that identify this domain. Indeed, both digital evidence and electronic evidence are accepted terms in the scientific community. For instance the International Standard Document, ISO/IEC 2703, "Guidelines for identification, collection, acquisition, and preservation of digital evidence", prefers the term digital evidence, because it refers to data that is already in a digital format and does not cover the conversion from analogical data into digital one. On the other hand, authoritative sources such as the Council of Europe have opted for the term Electronic evidence in the recently published "Electronic evidence guide" (Council of Europe, 2013).

Moreover there are many different definitions of “Electronic/Digital Evidence”, each of them highlighting some, but not all, essential features. The following are the main definition we have collected/analysed so far (Mason, 2012):

- any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi (Carrier, 2006);
- digital evidence is any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi (Casey, 2011).

None of the above cited definitions of digital evidence or electronic evidence matched our needs, therefore we finally decided to adopt the following original definition:

Electronic Evidence is any data resulting from the output of an analogue device and/or a digital device of potential probative value that are generated by, processed by, stored on or transmitted by any electronic device. Digital evidence is that electronic evidence which is generated or converted to a numerical format.

Therefore, the *EVIDENCE* Project activities are based upon its own core definition, capable, in our opinion to catch all various sides, challenges of Electronic Evidence, relying on its very general abstraction level.

Based upon this definition our statement is that within the Electronic Evidence category both those evidence that are “born digital” and “not born digital” but that may have become such during their life-cycle are to be included.

As a matter of fact electronic evidence and digital evidence in our conceptualization do coincide (see Figure 1). Therefore, we will assume that semantically speaking Electronic Evidence is the broader class including both those records “born digital” as well as those ones “not born digital” but digitized afterwards. Once the digitization process has been carried out the Evidence becomes “electronic” even if it was originally “non electronic” or analogical.

Figure 1 depicts the relationship between the Electronic Evidence and the other forms in which it may appear, with a specific focus on:

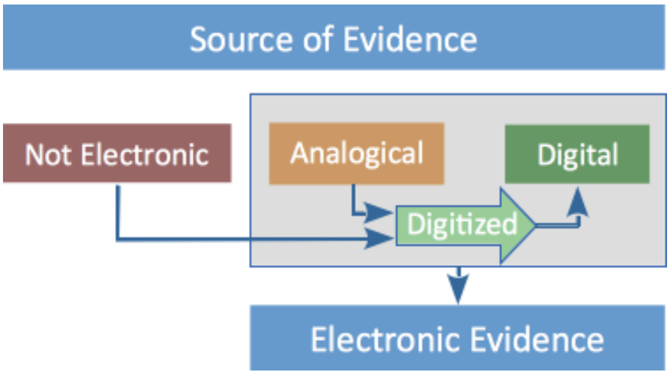

Figure 1: From Sources of Evidence to Electronic Evidence

- Not Electronic items that should be digitized, and therefore are afterwards treated as they were born-digital, once the authenticity is assured as related to the original one;
- Electronic items - some sort of analogical form, which, as in the case of the Not Electronic items, should be digitized.

In the same *Figure 1* it is to be noted that:

- Arrows represent the process of transformation needed to generate the transition from "Non Electronic" or from "Analogical" to Digital items.
- Lines show that no process is needed and that the evidence is per se electronic.

Of course the transition from Analogical or Not Electronic to Electronic is not an essential step; it may happen but is not mandatory. In this way we can include every type of evidence present in paper documents, objects, court hearings with witnesses and other, that, due to the increasing use of ICT, are frequently objects of digitization. Therefore, we prefer to use the term Electronic evidence that in our opinion comprises a larger range of items/potential evidence.

3. ELECTRONIC EVIDENCE LIFE CYCLE

Starting from the relevant concepts extracted both manually and semi-automatically, this step of the project was focused on the identification and classification of the building blocks of the conceptual model oriented to the description of the Electronic Evidence domain. The structuring is mainly based upon the electronic evidence life-cycle as described in *Figure 2*. Having clarified starting point of the conceptualization and the choice of the term preferred for the categorization, it is worthwhile to describe which is the flow to which actions are referred in the digital forensics domain. Therefore a brief description of the digital forensics procedures will outline the process used to manage electronic evidence. The very first milestone starts with an incident, an unlawful criminal, civil or commercial act, and sets the scene for the electronic evidence life-cycle scenario. Indeed an artefact or a record enters into the forensic process only if an incident forces it to do so. Otherwise, for all of its natural lifespan the artefact or record will remain outside the forensic process and thus forensically irrelevant – though it may continue to be very relevant to its user or owner.

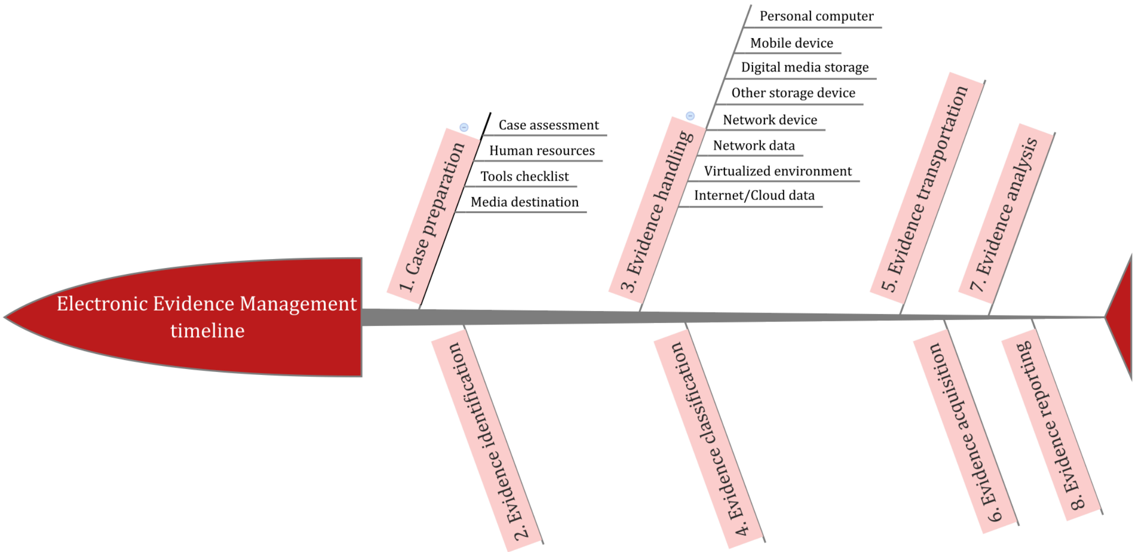

Figure 2: Electronic Evidence management timeline/life cycle

The phases we have taken into consideration are chiefly based on already existing investigative process models and ISO 27043 that represents a point reference with the aim of creating a harmonized model on the basis of about other existing models.

The digital evidence management timeline/life-cycle consists of six main different phases, regarding the handling of electronic evidence, starting from the incident event:

- Case Preparation: this is the first step of the digital evidence management timeline and it comprises organizational, technical and investigative aspects
- Evidence Identification: this is the step consisting of examining/studying the crime scene in order to preserve, as much as possible, the original state of the digital/electronic devices that are going to be acquire.
- Evidence Handling: this is the step where it is defined which specific standard procedures are to be followed, based on the kind of device is being handled.
- Evidence Classification: this is the step consisting of identifying the main features and the status of the device, taking notes about Case ID, Evidence ID, Seizure place/date/made by/ Evidence type, picture, status, etc.
- Evidence Acquisition: this is one of the most critical phase within the digital evidence handle processes: the forensics specialist must take care of the potential digital evidence in order to preserve its integrity during the following processes till to the presentation before a Court.
- Evidence Analysis: this is a process heavily affected by the kind of case under investigation, the type of evidence to be handled and the features related to each of the evidence to be examined (e.g. installed operating system, type of file system, etc.).
- Evidence Reporting: this is one of he most critical steps. After the completion of identification, acquisition and analysis activities digital evidence specialists have to complete their job producing a report with all the activities carried out and the outcome achieved. The report must contain all details to allow the specialists to testify before a Court only relying on that document.

The investigation process model depicted in *Figure 2* represents a simplified view of the whole process, because some concurrent processes have not been represented, such as Obtaining authorization, Documentation, Managing information flow, Preserving chain of custody, Preserving digital evidence. Furthermore it's not a sequential flow, it may be circular in some points and it might have back up to certain steps, Such example could be:

- The analysis can reveal that some references to data sources have not been acquired.
- During the acquisition phase it might be possible to reconsider the acquisition plan to include more data sources.
- During presentation some questions may arise requiring further analysis in order to provide satisfactory answers.

More and more evidence may be generated in the course of most court hearings with witnesses being recorded and their testimony entered into the official court record, irrespective of whether a case is criminal or civil. Furthermore in our specific view once the reporting phase is accomplished, the electronic evidence may open to the scenario of Electronic Evidence Exchange. In this case the further step dedicated to the Presentation may take place before a National Court or before another EU Member State.

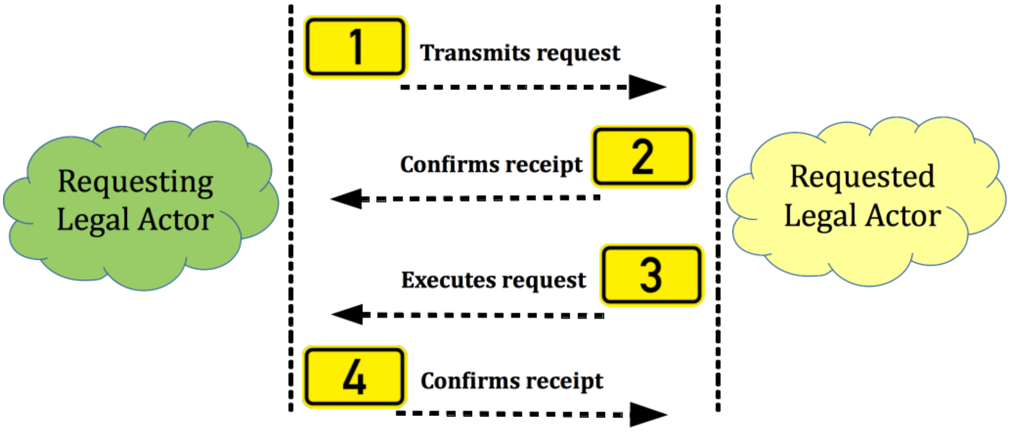

Figure 3: Overview of exchange data between Legal Authorities

Figure 3 outlines at a high level of description the exchange process that takes place between the Requesting and Requested Legal Authorities involved in the case after the analysis or interpretation is completed.

4. MID-TERM RESULTS

In order to produce the Road Map a specific set of objectives have been considered essential and a group of mid-term results have been achieved.

4.1 ELECTRONIC EVIDENCE DOMAIN CATEGORIZATION

It has been developed, within the activities carried out in the *Categorization* work package[6], a common and shared understanding on what electronic evidence is and which are the relevant concepts of electronic evidence in involved domains and related fields such as digital forensic, criminal law, criminal procedure and criminal international cooperation.

A mind map representation of the whole categorization is visible via the following address:

http://www.evidenceproject.eu/categorization.

4.2 LEGAL ISSUES PRELIMINARY RESULTS

On of the main goal of the project, addressed by the *Legal Issues* work package[7], is the identification of a legal framework in the EU Member States, governing the implementation of new technologies in processing evidence, including trans- border exchange. Some general consideration have been achieved on the basis of a pilot comparative study:

- There is no comprehensive international or European legal framework relating to e-evidence, only few relevant legal instruments (e.g.: Cybercrime Convention);
- Although some regulation exists at national level, rules vary considerably even among countries with similar legal traditions (e.g. on admissibility issues);
- It has been gradually developing an interpretative evolution of the national criminal laws so to apply (also) to e-evidence (amendments to existing norms);
- There has been a increase in knowledge and expertise of actors involved in the handling of e-evidence, but lack of specific standards is still missing;
- Several national data protection laws have been modified as a consequence of the introduction of antiterrorism measures;
- Different Laws and practices of member states contribute to create a situation of legal and practical

[6] The activities have been developed by the CNR-ITTIG (Italy) and CNR-IRPPS (Italy), partners of the Evidence project.

[7] The activities have been developed by the University of Groningen (The Netherlands), partner of the Evidence project.

uncertainty.

4.3 DATA PROTECTION ISSUES

Another crucial goal of the project, addressed by the *Data Protection Issues* work package[8], is the identification of data protection issues and remedies regarding the process of gathering and using electronic evidence.

The following general consideration have been determined:

Secondary law: there is no valid regulations addressing data protection issues related to the collection of electronic evidence

Conventions: Cybercrime Convention contains procedural regulations on the collection of electronic evidence and data protection safeguards

European Convention on Mutual Assistance in Criminal Matters addresses the exchange of evidence

Art. 82 (2) TFEU: The EU has a legal competence to harmonise particular aspects of criminal procedure law such as:

- admissibility, which includes rules on means of collecting electronic evidence;

This competence could be used to set up a minimum standard of privacy safeguards to be established in relation to the use of certain means of collecting electronic evidence.

Moreover in most domestic legal frameworks rather few and not necessarily sufficient and/or congruent privacy safeguards related to electronic evidence exist. Such examples could be:

- Procedural Law: Structure and Rules - very few definitions of electronic evidence exist;
- Cross-Border Scenarios & International Law - in Cloud computing environments legal issues are not sufficiently or not at all addressed by law;
- Investigative Measures - Existing rules often apply both to physical and electronic evidence
- Admissibility - Not regulated specifically

4.4 DIGITAL FORENSICS TOOLS CATALOGUE

Starting from the Digital Evidence life-cycle shown in *Figure 2*, there are already standards for many of phases depicted. In particular for the acquisition and investigative processes the ISO 27043, ISO 27037 and ISO 27042 represent points of reference. In composing the overview of existing standard for the handling of electronic evidence, within the activities related to the *Standard Issues* work package[9], a huge number of digital forensics tools have been gathered and there has been created a *Digital Forensics Tools Catalogue*, concerning tools for the Acquisitive and Analysis phases as described at different levels of details by the ISO/IEC standards, above mentioned.

The *Catalogue* represents the overview of forensics tools for handling digital evidence, generally accepted in the EU member states. The *Catalogue*, in its current version 1.0 dated February 2015, comprises over 1.200 tools divided into two main branches: Acquisition and Analysis.

The Digital Forensics Catalogue is visible via the following URL: *http://wp4.evidenceproject.eu*

4.5 MARKET SIZE MAP OF ACTORS

Another relevant goal of the project, addressed by the *Market Size* work package[10], is the identification and classification of the main types of actors involved in the "social arena" of electronic evidence.

There are two type of actors having a direct interest in electronic evidence:

- *Process Actors*: public and private actors involved in handling the electronic evidence;
- *Context Actors*: actors providing technical solution and assistance in this field.

Furthermore there are nine typological areas of *Process Actors*, in turn comprising a total of 40 types of actors:

- Public law enforcement and Intelligence

[8] The activities have been developed by the Leibniz Universität Hannover (Germany), partner of the Evidence project.

[9] The activities have been developed by the CNR-ITTIG (Italy), partner of the Evidence project

[10] The activities have been developed by the Laboratory of Citizenship Sciences (Italy), partner of the Evidence project.

agencies (e.g. Law enforcement officers, Detectives, Intelligence agencies);

- Actors of legal criminal trial (e.g. Judges, Prosecutors, Lawyers, etc.);
- Notaries;
- Public register actors (e.g. Business register actors , Civil acts register actors, Landregister actors, etc.);
- Forensic examiners (e.g. Fraud examiner, Forensic laboratory staff member, Digital Evidence First Responder, etc.);
- Private investigators;
- Hardware producers (e.g. Hardware producers for Computer Forensics, for Mobile Forensics, etc.);
- Technology/software producers (e.g. Software houses that produce complete commercial toolkits for forensic analyses, that make software for specific commercial analyses, etc.);
- Service providers (e.g. Major consulting firms, Associated professional studios, etc.).

Finally ten typological areas of *Context Actors*, in turn containing twenty six types of actors, can be enumerated:

- Specialized International Organizations (e.g. UN agencies concerned with justice and technological innovation, etc.);
- Law making bodies (e.g. European organizations, National governments);
- Technological innovation actors linked to the Internet (e.g. Internet service providers, Cloud technology providers);
- Legal and forensic associations and networks (e.g. General legal and forensic associations and networks, Associations and networks concerned with issues linked to new technologies);
- Research bodies, associations and networks (e.g. Organizations and associations concerned with Internet and ICT , Academic institutions concerned with ICT, etc.);
- Actors involved in the field of human rights (e.g. Civil rights organizations, Privacy protection organizations, etc.);
- The media (e.g. Traditional and Social media, etc.);
- Enterprises interested in the proper functioning of justice (e.g. Individual firms, Business associations);
- Transnational projects (e.g. Digital forensics research projects and training);
- Other actors collecting evidence (e.g. Public and Private actors that collect data / potential evidence).

5. ELECTRONIC EVIDENCE EXCHANGE STAUS QUO OVERVIEW

As far as the Exchange process (see *Figure 3*) is concerned, there is no standard published or proposed, furthermore it represents one of the essential points of the *EVIDENCE* Project that aims to facilitate and foster the exchange between different authorities and across the EU Member States. The project aims at defining functional specifications for exchanging digital evidence, in such way that no matter what forensic tool is being used by an examiner, the results of his or her examination must be verifiable by another examiner, independent of the tool being used as long as the tools are comparable in specification and function.

On the basis of the information gathered so far, it seems that, at the moment, in cross-borders criminal cases, cooperation is mostly based upon international agreement or letter rogatory to the foreign Court. Independently from the legal framework identified by the EU Member States, the cooperation is mostly human based where the electronic evidence exchange is carried out between judicial stakeholders from a source EU authority to another judicial authority in the target EU member state. This approach is similar across countries and, at first glance, the Exchange does not appear based on any electronic means at all.

In most cases the forensics copy of the original source of evidence is exchanged: a judicial/police authority from an EU member state A (requested authority) requests an EU member state B (requesting authority) to generate a forensics copy, based on mutual trust between the two competent authorities. Later the exchange of the forensic copy will be attained on human based: the authority from country A instructs someone to take the copy or the copy is delivered by a secure courier to the requested authority . In any case it has to emphasize that no electronic means is involved in the exchange process.

To facilitate human cooperation, institutions such as *EuroJust*, *EuroPol*, *InterPol* put in place systems or platform in order to communicate/share relevant information.

There are two different cross-borders cooperation levels:

• the judicial cooperation based, almost exclusively, via the regular international procedures for mutual assistance in criminal matters, regulated by strict procedures, time-consuming and unpredictable, but the only way for an evidence exchange,

• the investigation cooperation simpler and quicker but only for operational, technical information or coordination activities. During investigations there may be an information exchange that cannot be used during the trial over the pleading stage.

In many cases judicial authorities act relying on international agreement established through *Eurojust* to coordinate investigations and prosecutions between the EU Member States when dealing with cross-border crime.

The exchange of the electronic evidence should take place in a secure environment, relying on a service for exchanging the evidence in a secure manner. In order to achieve this goal such a service will rely on digital certificates in order to certify the proprietary of a public key. This would allow any judicial authorities (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the certified public key.

6. ELECTRONIC EVIDENCE EXCHANGE: EXISTING PLATFORMS

There are already existing platforms for the information exchange, but, for confidential reasons it has almost been impossible to collect detailed information about their architecture and the kind of information exchanged. The main important system in the evidence exchange is: *SIENA*, that stands for Secure Information Exchange Network Application. It is a secure communication system managed by *Europol,* dedicated to the EU law enforcement community and based on *Universal Message Format* (*UMF*) standard . *SIENA* is used for exchanging personal information related to the crime areas within the mandate of *Europol*, including EU restricted information.

7. ELECTRONIC EVIDENCE EXCHANGE: PROPOSED STANDARDS

The requirement upon a standard language to represent a broad range of forensics information and processing result has become an increasing need within the forensics community. For the electronic evidence exchange a similar need has to be addressed even though the aim of the exchange may address different issues, for example malware analysis, relevant artifacts exchange, tools result comparison. Research activities conducted in this field have been used to develop and propose many languages.

CybOX (Cyber Observable eXpression) is one of the most important languages that have been recently proposed. It has been devised along with other related languages, by Mitre.org such as CAPEC (Common Attack Pattern Enumeration and Classification), STIX (Structured Threat Information eXpression) and TAXII (Threat Automated eXchange of Indicator Information).

The use of standard languages for the information exchange has been dealt in recent scientific contributions, published in 2014, by the European Union Agency for Network and Information Security (ENISA) and in particular Actionable information for Security Incident Response and in Standards and tools for exchange and processing of actionable information .

Another relevant resource is a recent document (Casey, 2014), that proposed *DFAX* (*Digital Forensic Analysis eXpression*), that leverages *CybOX* for representing the technical information.

8. ELECTRONIC EVIDENCE EXCHANGE CHALLENGES

The regular international procedures for mutual assistance in criminal matters are time-consuming and unpredictable, but they represent, at the moment, the only way for the evidence exchange. Nevertheless the current situation may pose obstacles for fighting against serious cross-border and organized crime especially in investigative case where time is crucial.

Furthermore, when it comes to Electronic Evidence Exchange, a group of questions are to be born in mind:

- What information should be exchanged?
- When may the exchange take place?
- How the information could be exchanged, even taking into consideration security issues?
- Which kind of stakeholders are involved?

The present situation raises three main issues:

- exchange evidence procedures may be slow. This aspect must be especially born in mind in investigative cases where time is crucial for fighting against serious cross-border and organized crime;
- exchange evidence procedures may involve big expenses, such in case of travelling abroad to take the original/copy source of evidence to be handled;
- Judicial and Police authorities must invest lots of money to keep up with the development of forensics technology.

In order to address the issues a possible solution could be using a cloud environment , centralized or distributed, for exchanging/sharing evidence where the users could be competent authorities (e.g. judicial, police, etc.) but private subjects as well. This platform could speed up the exchange procedures and it could avoid, except for special cases, travelling abroad to take the original source of evidence. Moreover, through a digital platform, a wider cooperation could be put in place and, for example, specific technical support could be requested through the same digital platform, from a police authority to another located in a different EU member state. A more developed technological cooperation among the involved authorities could optimize costs and better distribute resources.

9. CONCLUSIONS

At the moment, there is no standard for the exchange and it is mostly human based. Only in case of data held by third-parties there is a well-established cooperation between judicial authorities and Internet Service Providers (ISP). In this context the exchange is managed through platforms provided by ISPs via web. This scenario may pose serious issues:

- exchange evidence procedures may be slow: it must be especially born in mind in investigative cases where time is crucial for fighting against serious cross-border and organized crime;
- exchange evidence procedures may involve big expenses, such as in the case of traveling abroad to take the original/copy source of evidence to be handled;
- Judicial and Police authorities must invest lots of money to keep up with the development of forensics technology: expenses related to software updating and keeping up personnel competencies;
- exchange desperately needs trusted procedures and environments between involved stakeholders

So the way forward for the electronic evidence exchange would be introducing a cloud environment to be used from judicial and police authorities and by private stakeholders in order to speed up the process, optimize costs and foster a more developed cooperation and trust among the involved competent authorities. Moreover, using this platform could be possible to carry out an electronic evidence exchange using specific meta data along with the data related to the source of evidence. This meta data, expressed in an open standard language could describe the digital evidence in a unique way and be used by software companies/producers to represent the widest range of forensic information and forensic processing results in order to share structured information between independent tools and organizations.

REFERENCES

Carrier, B. (2006). Hypothesis-Based Approach to Digital Forensic Investigations. Center for Education and Research in Information Assurance and Security. Purdue University.

Casey, E. (2011). Digital Evidence and Computer Crime. Forensic Science, Computers, and the Internet. Elsevier, Third Edition.

Casey, E., Back, G., Barnum, S. (2015). Leveraging CybOX to standardize representation and exchange of digital forensic information. Digital Investigation, 12S, 102-110. Elsevier.

Council of Europe. (2013). Electronic Evidence Guide. Retrieved on February 2015 from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp

Daniel, L., Daniel, L. (2011). Digital Forensics for Legal Professionals. Syngress Media Inc.

ISO/IEC 27037. (2012). Guidelines for identification, collection, acquisition and preservation of digital evidence. Retrieved on March 2015 from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44381

ISO/IEC 27043. (2015). Incident investigation principles and processes. Retrieved on March 2015 from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44407

Garfinkel, S. L. (2012). Digital forensics XML and the DFXML toolset. Digital Investigation. Elsevier.

Mason, S. (2012). Electronic Evidence, third edition. LexisNexis Butterworths.

Peterson, G., Sujeet, S. (2012). Advances in Digital Forensics VIII, Editors: Peterson, Gilbert, Shenoi. Springer.