ARTICLE:

A proposed electronic evidence exchange across the European Union

By **Maria Angela Biasiotti**

Crime has become global, and almost all crimes involve electronic evidence. A significant problem has become the exchange of data, across jurisdictions and between the domestic participants in the criminal judicial process. Taking this development and the problems into account, the EVIDENCE Project[1] was conceived. The project concluded that the European Union ought to develop a better means to exchange information and evidence relating to crimes quickly from one country to another for the purpose of investigating crime in a timely manner. The exchange becomes crucial in counterterrorism operations and when dealing with global crimes. At the same time, a secure and trusted exchange of information and of electronic evidence relating to crimes is an important element in order to promote judicial cooperation in criminal matters, as well to contribute to an effective and coherent application of EU Mutual Legal Assistance[2] (MLA) and European Investigation Order[3] (EIO) procedures. This paper deals with the electronic evidence exchange in Europe, and more specifically with the new challenges of the implementation of the European Investigation Order Directive – in particular, some of the results of the EVIDENCE Project are discussed. This article will consider some of the conclusions for future activities, with some ideas for the follow-up of the results achieved and the policies promoted by the European Commission.

Tackling terrorism and organized crimes, including cybercrime, can be greatly improved by enabling the efficient, secure and trusted exchange of qualified information and electronic evidence among public prosecutors and law enforcement agencies of Member States, by adopting a standardized language and procedure to foster cooperation in criminal matters. In this context, the challenge is to facilitate the exchange of electronic evidence in the EU framework, making it possible to achieve improved international cooperation in the criminal sector, to include the specific context of EIO and MLA procedures that will allow a strong uniformity and harmonization for investigations procedures.

The present position

Two EU legal Frameworks need to be considered when considering how to enhance judicial cooperation in the criminal field: existing MLA procedures and the new frontier of the EIO. Mutual Legal Assistance consists of 'cooperation between different countries for the purpose of gathering and exchanging information, and requesting and providing assistance in obtaining evidence located in one country to assist in criminal investigations or proceedings in another'.[4] In other words, mutual legal assistance procedures have been designed specifically for the gathering and exchanging of evidence. However, in criminal matters there are no universal instruments governing this cooperation. Moreover, MLA procedures have not been adapted to the realities of today's crimes, which are increasingly global and complex, and adversely affect the potential for rapid and efficient transfers of electronic evidence.

The same reflections need to be considered in relation to the European Investigation Order. Based on the flexibility of the traditional system of mutual legal

[1] European Informatics Data Exchange Framework for Court and Evidence, (funding scheme: CSA (Supporting Action), Call ID FP7-SEC-2013-1; grant agreement no: 608185; duration: 32 months (March 2014 - October 2016); coordinator: Consiglio Nazionale delle Ricerche (CNR-ITTIG), Italy; EU funding: € 1,924,589.00); http://www.evidenceproject.eu; all of the images included in this article formed part of the Project reports, and copyright vests in the Project.

[2] European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 20/04/1959, ETS No.030; Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, Strasbourg, 08/11/1990, ETS No. 141; Council of Europe Convention on the Transfer of Sentenced Persons, Strasbourg, 21 March 1983, ETS No. 112; Mutual assistance in criminal matters between Member States, Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, 2000/C 197/01, OJ C 197, 12.7.2000; Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 8 November 2001, CETS No. 182; Council of Europe Convention on Cybercrime, Budapest, 23 November 2001, ETS 185.

[3] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p. 1–36.

[4] http://ec.europa.eu/justice/criminal/judicial-cooperation/legal-assistance/index_en.htm.

assistance, the EIO is a judicial decision that has been issued or validated by a judicial authority of a Member State (the issuing State) for a specific investigative measure or series of measures to be carried out in another Member State (the executing State) for the purposes of to obtaining relevant evidence. The EIO may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State. Of relevance to the discussion, is that there is no reference to particular procedures or specific means when issuing such requests.

Changes

In June 2016,[5] Ministers of the Justice and Home Affairs Council recommended that MLA procedures should be streamlined, in particular with a view to exchanging electronic evidence. The options available are to develop either decentralized or a centralized approach:

> (i) a central EU portal as an application to process mutual legal assistance and EIO requests with a central storage facility for electronic evidence, or
>
> (ii) a reference implementation of such an application to be installed individually by Member States, providing a reference for the storage facility.

Independently from the approach that the EU will eventually choose, other issues arise, as indicated from the Agenda of the Expert Group Meeting on Principles and Options for an e-evidence exchange platform of 9 November 2016,[6] including the users; security; a location to save the requests and the e-evidence; the functions, including size and translation.

The 'user' perspective needs to be addressed with the aim of catering to as large an audience as possible, and by implementing a tool with a user-friendly back-office to facilitate its and the exchange by the participants; the 'security' relates to sending a request for assistance or exchanging evidence – this should be able to guarantee the validity, integrity and authenticity of the requests, the reply and the electronic evidence transferred; the location of saving the requests and the electronic evidence mainly depends upon the choice of the architecture of the system, whether centralized or decentralized. The capacity to handle and store large electronic documents relates to using alternatives methods to transfer data, perhaps by the prior transfer of a set of metadata describing the electronic evidences available for the request.

From the agenda, it seems that the EU is already looking forward considering at least two EU funded projects that might help in realizing the platform: The E-Codex initiative and the EVIDENCE Project Roadmap. The first could provide the necessary infrastructure for the trusted and secure exchange of requests and evidence, whilst the latter could provide the methodology and the formal language to enable the trusted and secure exchange to take place.

Furthermore, it is also necessary to improve cooperation with the Internet Service Providers (ISPs), through the development of a common framework to request specific categories of data, such as the use of identical forms and tools.[7]

The effectiveness of MLA and EIO procedures rely on the implementation of such a secure and trusted method of exchanging electronic evidence among the relevant agencies, a number of which ought to be involved with implementing such an exchange, such as:

> (i) Public prosecutors, judges, lawyers and law enforcement agencies who regularly deal with crimes with a substantive amount of electronic evidence.
>
> (ii) Policy makers at national and European level, because of the need to provide the legal basis for the exchange of electronic evidence.
>
> (iii) Ministries of Justice of EU Member States, who need to facilitate and put in place appropriate measures to facilitate the exchange.

[5] European Council of the European Union, Luxembourg, 9 June 2016, Council conclusions on improving criminal justice in cyberspace, http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace .

[6] 16 11 09 Experts' meeting on the setting up of a reliable and secure e-platform for the European Investigation order on Mutual Legal Assistance (MLA) in http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=636&NewSearch=1&NewSearch=1 .

[7] European Council of the European Union, Luxembourg, 9 June 2016, Council conclusions on improving criminal justice in cyberspace, http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace .

(iv) EU bodies and agencies such as EUROJUST, EUROPOL, OLAF-Digital Forensic Unit and the Data Protection Office.

(v) International Institutions, such as INTERPOL and the International Criminal Court.

(vi) Digital forensic software companies and ISPs.

Some electronic evidence issues

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, the integrity of the data must be maintained and proved, i.e. demonstrated that the electronic evidence has not been altered since the time it was created, stored or transmitted. Legislation on criminal procedures in many European countries was enacted before the use of electronic evidence, although many Member States have amended their legislation to accommodate the new form of evidence. However, some issues remain, and include, but are not limited to, the following:

(i) In certain countries there are defined rules as to admissibility of evidence in legal proceedings, while in other countries admissibility is flexible.

(ii) Legislation and policies may negatively affect an investigation. For example, privacy and data protection laws in some Member States may prevent the collection of evidence, and varied data retention periods across jurisdictions may complicate investigations.

(iii) Legislation may furthermore not sufficiently address the realities of modern investigations, especially when it comes to evolving new technologies.[8]

The EVIDENCE project conclusions

The EVIDENCE Project concluded with the following results:

(i) The categorization of electronic evidence.

(ii) A survey on the legal position in handling and exchanging electronic evidence in Europe.

(iii) A survey on the technical position in handling and exchanging electronic evidence in Europe, along with a proposal for the representation of data and meta data involved in the exchange process.

(iv) A plan for realising a Common European Framework for the Exchange of Electronic Evidence. The plan provides a brief overview of the legal issues; considerations relating to standards; technical aspects; law enforcement requirements; the nature of the market, and data protection issues, and the challenges these topics pose. The aim of the Common European Framework for the Exchange of Electronic Evidence is to improve the efficiency of investigations and judicial procedures while maintaining adequate safeguards aimed at protecting relevant fundamental human rights and respecting clear standards of conduct.

The description of the activities carried out under the EVIDENCE Project that are relevant to this article, including proposals for the future, are set out below.

Electronic evidence semantic structure: categorization

The EVIDENCE Project concerns the collection, preservation, use and exchange of electronic evidence within the various stages of the evidence lifecycle. By the collection of electronic evidence, we mean the process of gathering items that contain potential electronic evidence in the widest sense, including search, seizure, interception and any other forms of gathering evidence by law enforcement agencies, but also capture of evidence by the private sector and any other forms of gathering potential electronic evidence. Once the evidence is collected, it needs to be preserved before it can be used during the trial. Preservation is the process of maintaining and safeguarding the integrity and original condition of the potential electronic evidence, meaning that it needs to be stored in a secure way in order to safeguard against alteration, and access to the evidence needs to be restricted to persons authorised to process the evidence. Once the trial starts, the electronic evidence needs to be used, meaning that the evidence needs to be analysed and a final document or report needs to be produced and

[8] See EVIDENCE Deliverable 3.1 – Overview of existing legal framework in the EU Member States: http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-1-411.pdf and EVIDENCE Deliverable 3.2 – Status quo assessment and analysis of primary challenges and shortcomings: http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-2-412.pdf.

presented before the court. At any point during the electronic evidence lifecycle, it will be necessary to provide copies of the evidence to the various competent authorities including, law enforcement agencies, digital evidence professionals, courts, etc. To distinguish between the interchange of electronic evidence within a country and cross a border, we refer to the first one as transfer, and to the latter as an exchange. A transfer may occur between different agencies in the same country. An exchange may take place between competent national authorities of different countries (cross-border exchange) in the field of cooperation in criminal matters.

One of the main aims of the project was to develop a common and shared understanding on what electronic evidence is, together with the relevant concepts (digital forensics, criminal law, criminal procedure, criminal international cooperation) as well as to draft a proposed 'standard process' occurring when a crime occurs.

A definition of electronic evidence needs to be is broad enough to include all kinds of evidence regardless of their origin. This was a particularly important for the aim of the EVIDENCE Project, which focused on the exchange, as well as on the harmonized handling of electronic evidence within a common European framework. Based on these premises, the following definition is proposed:

> 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.

The term data includes any analogical or digital item, because these items may be the output of analogue devices or data in digital form.

Forms of electronic evidence

Evidence comes in different forms. The EVIDENCE Project concerns electronic evidence. The figure below shows the different types of evidence. The first type is physical or traditional (not electronic) evidence such as a murder weapon or the bloodstain of the victim, which may be digitised, for example, by taking a digital photograph of the murder weapon. The second type is analogical evidence, that is evidence formed in an analogue form (videotape or vinyl), which may be digitised and entered into a digitisation process acquiring digital status. The third type of evidence is digital evidence, that is, evidence originally in digital form as created by any digital device (computer or computer like-device). The EVIDENCE Project considers all these forms of evidence as 'electronic evidence', taking into account that at the end of the process they can be labelled as electronic regardless of their origin.

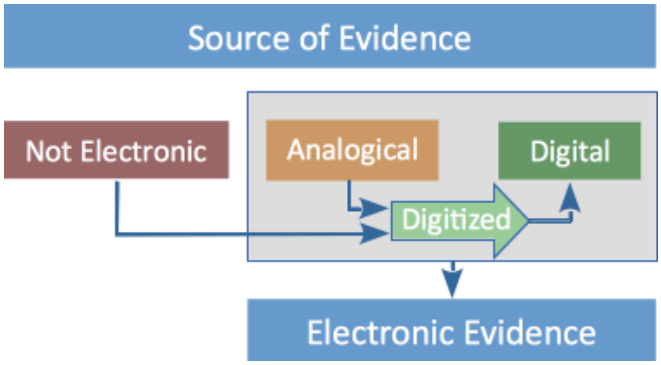

Figure 1

Electronic evidence includes, but it is not limited to, digital evidence. The aim of the project was to create a broader category that comprises all types of evidence and the various handling processes independently from the method by which it was created.

The electronic evidence life cycle

The process of handling electronic evidence can be divided in several phases. The first phase includes the identification, collection and anti-contamination precautions (searching the scene, collecting the evidence, packaging and labelling and creating documents reporting the activities performed at every step) of electronic evidence. In the second phase, the acquisition of the source of evidence takes place, determining which items are most likely to serve the purposes of the investigation, which are the most time sensitive, which are most at risk of being lost or corrupted, including the identification of similar issues. During the third phase, the findings are evaluated and interpreted. The fourth phase includes the presentation of the results in a report, which should include factual findings, interpretation, and expert opinion. The report and presentation are essential steps in the electronic evidence lifecycle, because the court will examine the report that should contain all relevant findings as well as technical and non-technical explanations of the case and its issues. During each of the phases involved in handling

electronic evidence, it is essential to guarantee the preservation of the evidence: every precaution must be taken when collecting evidence, because any break in the process or improper handling of a procedure could spoil the probative value of the evidence, potentially making it inadmissible. The same principle applies to documenting procedures. Everything must be documented: how the evidence was found, its condition, model and serial numbers, markings, etc. The exchange may happen in different phases of the electronic evidence lifecycle. Figure 2 illustrates the different phases of electronic evidence.

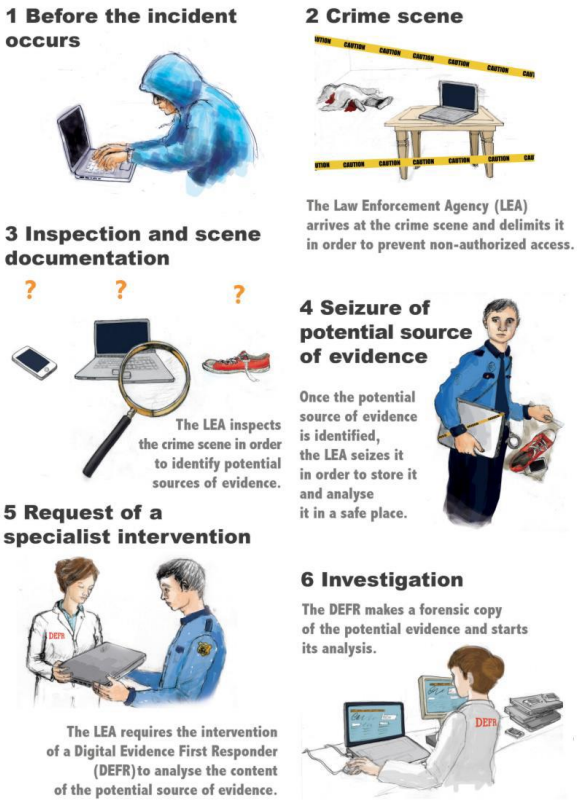

Figure 2

On the basis of the life-cycle outlined above, eight different concepts have been identified by the EVIDENCE Project. The concepts have been organized and classified as follows:

(i) Crime is an act, default or conduct prejudicial to the community, for which the person responsible may, by law, be punished by a fine or imprisonment.

(ii) Sources of electronic evidence: comprise any physical, analogical and digital device (computer or computer like device) capable of creating information that may have a probative value in legal proceedings.

(iii) A process is a series of actions or steps taken in order to achieve a particular end within the electronic evidence lifecycle.

(iv) Electronic evidence is any information (comprising the output of analogue devices or data in digital form) of potential probative value that is manipulated, generated through, stored on or communicated by any electronic device.

(v) A requirement represents principles or rules related both to legal rules and handling procedures that are necessary, indispensable, or unavoidable to make potential electronic evidence admissible in legal proceedings.

(vi) A 'stakeholder' (interested party) includes people or organizations having a concern in or playing a specific role in the electronic evidence lifecycle.

(vii) A rule contains a set of explicit or understood regulations or principles governing conduct or procedures for the identification, collection, preservation, analysis, exchange and presentation of electronic evidence in a cross border and national dimension.

(viii) Digital forensics is the application of forensic science to electronic evidence in a legal matter.

These main classes have been hierarchically structured in sub-classes that may be easily updated and maintained. The concepts are directly linked to the class they refer to according to the EVIDENCE Project conceptual model developed from the perspective of the life-cycle of electronic evidence.[9] All concepts and definitions relevant for the EVIDENCE Project can be found in the categorisation of the EVIDENCE Project.

[9] The structure is conceived as a conceptual map, and all the definitions and notes of the categorization may be viewed at http://www.evidenceproject.eu/categorization/. The whole semantic structure formalised in Simple Knowledge Organization System (SKOS) is a standard way to represent and support the categorization activities. SKOS has the advantage of expressing knowledge organization systems in a machine-understandable way within the framework of the semantic web, and is illustrated at http://evidence-project.herokuapp.com/en/hierarchical_concepts.html.

Legal analysis

The introduction and the extensive use of information technology has generated new forms of crimes or new ways of perpetrating them, as well as new types of evidence.[10] Although all kinds of evidence have to be handled according to criminal (procedural) laws, electronic evidence needs additional and specific methods of handling in order to maintain its authenticity and integrity. What is missing is a Common European Framework to guide policy makers, law enforcement agencies and legal authorities when dealing with the treatment and exchange of electronic evidence. There is a need for a common legal framework and standardised procedures regulating the collection, preservation, use and exchange of electronic evidence.

European legislation adds important value to the national legal systems creating a common framework to provide for criminal activity. Dealing with crime can be more efficient by adopting minimum standards for electronic evidence in the criminal field as well as in the cybercrime area. A number of guidelines and technical standards have been prepared by various agencies regarding electronic evidence.[11] These guidelines and standards are aimed at providing support and guidance in handling and examining electronic evidence. Many guidelines and best practices set out the necessary competencies and knowledge in order to fill the gap of standardised procedures across agencies, as well as the lack of specific legislation governing the use, collection, analysis and exchange of electronic evidence.

In order to gather specific information on criminal procedural rules across European countries, a bespoke questionnaire was designed that allowed the project to conduct a survey in 13 Member States, namely: Belgium, Bulgaria, Croatia, Denmark, Finland, Germany, Hungary, Italy, The Netherlands, Poland, Spain, Sweden and United Kingdom. This set of 13 Member States was considered a fair representation of 'families of law' and of different regions of Europe (i.e. common law/civil law; Nordic countries/Southern countries/Eastern Europe/Central Europe, etc.). In addition, the EVIDENCE Project conducted research on the legislation and practices currently in place in the European Union Member States concerning the collection, preservation and exchange of electronic evidence. This analysis, together with the answers received from the questionnaire, enabled the members of the project to write a report dealing with an overview of the legislative provisions existing at the European level; and at the level of the Member States on the collection, preservation and exchange of electronic evidence with the aim of identifying challenges and shortcomings.

It was obvious from the analysis and the questionnaire[12] that there is no comprehensive international or European legal framework relating to (electronic) evidence.[13] There is a reliance on national law when it comes to the collection, preservation, use and exchange of (electronic) evidence. While it is true that some countries have adapted their legislation to accommodate electronic evidence, others rely on traditional laws and apply them to electronic evidence. There are thus significant differences in national legislation and approaches, which makes the handling of electronic evidence difficult across jurisdictions. Evidence rules vary considerably even amongst countries with similar legal traditions. In certain countries, traditional investigative powers might be general enough to apply to electronic evidence, while in other countries traditional procedural laws might not cover specific issues regarding electronic evidence, making it necessary to have additional legislation. In all cases, legislation requires a clear scope of application of powers and sufficient legal authority for actions.

While there is no comprehensive international or European legal framework relating to electronic evidence, a number of international and European legal instruments and policy documents are relevant to electronic evidence. This includes the EU legal framework and guidelines, and the legal instruments and documents by the Council of Europe.

In order to establish requirements for uniform regulation of electronic evidence, the similarities and differences of the national legal frameworks have been assessed by the EVIDENCE Project in order to

[10] The content of this paragraph is related to deliverable D3.1 – Overview of existing legal framework in the EU Member States, and deliverable D3.2 – Status quo assessment and analysis of primary challenges and shortcomings, prepared by the University of Groningen, a partner of the EVIDENCE project.

[11] For a list, see Appendix 1 in Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017).

[12] See Deliverable 3.1: http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-1-411.pdf .

[13] But see the Draft Convention on Electronic Evidence, published in the 2016 issue of the journal.

identify the major challenges and shortcomings of the legal frameworks within the EU Member States which include legal and data protection issues, problems with law enforcement in particular as regards cross-border cases when evidence needs to be exchanged, and technical issues as regards training and technical capabilities. Effective legislation and law enforcement should include an effective legal framework, access to investigative tools and techniques, training and technical capabilities and best practices policies that ensure proportionality between the protection of privacy and legitimate crime prevention and control. In considering whether or not harmonisation should take place, the current rules on the collection, preservation and use and exchange of electronic evidence were reflected upon, and the following categories of requirements were identified:

(i) Legal basis and uniform definitions, concepts and standards;

(ii) Common and specific rules, definitions, standards and procedures of collection;

(iii) Guidelines for preservation and use;

(iv) Specific investigative measures;

(v) Admissibility based on mutual trust;

(vi) Regulation of cloud computing;

(vii) Transfer of electronic evidence;

(viii) Provisions to regulate the role of private sector participants;

(ix) Transfer of actionable intelligence from intelligence agencies and law enforcement agencies and vice-versa;

(x) Effective cross-border regulation;

(xi) Joint Investigation Teams.

Investigative measures dealing with electronic evidence can affect the suspect's fundamental rights, especially in a digital environment, which allows the gathering of (personal) information through different channels. Consequently, there has to be a balance between effective law enforcement on the one hand and proper protection of citizens' fundamental rights on the other hand. A European legal framework that comprehensively addresses data protection issues relating to the collection of electronic evidence does not exist. There is a need to include specific safeguards in the current legislative frameworks to address the shortcomings. From a data protection perspective, the Common European Framework for the Exchange of Electronic Evidence should also seek to provide for rules on minimum data protection standards that need to be met during the life-cycle of electronic evidence. This applies to both privacy and data security, in particular safeguards against the alteration of electronic evidence. Non-binding guidelines regarding privacy safeguards and data security rules on a practical level are necessary in order to achieve an adequate level of data protection.

The technology

Tools

The EVIDENCE Project provided an overview of existing standards for the treatment and exchange of electronic evidence, taking into consideration tools that are thoroughly tested and generally accepted in the computer forensics field in the context of the EU Member States. The project also set out the lifecycle of electronic evidence, which highlights the main processes of the investigation phase in which potential electronic evidence is identified, collected, and acquired and then safely preserved. A Digital Forensics Tools Catalogue was subsequently developed,[14] which can become a point of reference within the forensic community. This will help digital evidence professionals to determine the most suitable tool for their case and to identify a similar or comparable tool for conducting a dual-tool validation.

Metadata

One of the main objects of the project was to identify and propose a standard for the representation of data and metadata involved in the digital evidence exchange. The requirement for a standard language to represent a broad range of forensics information and the processing of results is an increasing need within the forensics community.

On the basis of the information gathered during meetings, interviews, questionnaires with digital evidence professionals, members of the judiciary and police authorities, (and also considering the little scientific literature published on this subject), it seems that, at present, the exchange process is chiefly human based. In cross-borders criminal cases, cooperation is based upon international agreement or letters rogatory to the foreign court and, at first glance, the exchange does not appear to be based on

[14] wp4.evidenceproject.eu.

any electronic means. In most cases, the forensic copy of the original source of evidence is exchanged: a judicial or police authority from an EU Member State A (requesting authority) will make a request to an EU Member State B (requested authority) to generate a forensic copy, based on mutual trust between the two competent authorities. When the procedures have been completed, the authority of country A will instruct a person to travel to country B, take a forensic copy of the evidence, and take it to a specialized forensic laboratory located in country A.

Furthermore, when it comes to the proposed Common European Framework for the Electronic Evidence Exchange, a group of questions are to be born in mind:

(i) What information should be exchanged?

(ii) When may the exchange take place?

(iii) How can the information be exchanged, taking into consideration security issues?

(iv) When the amount of electronic evidence is vast, how should it be dealt with?

(v) Which agencies should be involved?

There are already existing platforms for the information exchange (Secure Information Exchange Network Application (SIENA/UMF) by Europol; s-TESTA/EPOC IV (European Pool against Organised Crime) by Eurojust; I-24-7 by Interpol; Hansken system by the Netherlands Forensic Institute), but, none of them use a detailed structure related to digital forensics information for exchanging data. For this reason, the EVIDENCE Project proposed another information model for the representation of electronic evidence. The proposal for the representation of data and metadata involved in an electronic evidence exchange consists of:

(i) A set of data and metadata for describing all actions (i.e. tasks), participants (e.g. subjects, victims, authorities, examiners, etc.), tools (i.e. digital tools for carrying out different forensics processes), digital and physical objects involved in the investigative case (e.g. hard disk, smartphone, memory dump, etc.) and objects relationships (e.g. Contains, Extracted From, etc.).

(ii) Formal languages for representing all the elements above cited in a standard way.

(iii) A platform for implementing the exchange process in terms of functionalities, together with a recommendation for an integration with existing platforms already in place and run by European or International public bodies.

The project compared the standard language that has been developed in the last year by the forensics community. On the basis of the study conducted on digital forensics standards, it was concluded that the combination of the recent languages (CybOX, DFAX[15] and the Unified Cyber Ontology (UCO)) represent the most suitable standards to represent data and metadata related to an evidence exchange for a variety of reasons:

1. They have been developed in the cyber security environment, but they include a number of essential elements representing digital forensics information.

2. They permit the description of technical, procedural and judicial information.

3. They have been developed with the intention of being adaptable to the development of technology, and they permit the introduction of new elements to include forensics information not yet envisaged.

4. They use the Unified Cybersecurity Ontology that permits the description of actions, people and their relationships.

4. They are open source.

5. They already contain a structure for representing a wide range of forensics information.

The EVIDENCE Project also produced and implemented a Proof of Concept (PoC) application on the digital evidence exchange, to include a support for maintaining a detailed continuity of evidence (also called a chain of custody). The proposed architecture follows the reasoning of the goal-oriented analysis, and takes into account the results of the analysis of existing systems used by Eurojust and INTERPOL. The implementation of the PoC (application and library) is designed to fill the gap of capturing the investigation actions performed during the lifecycle of a criminal investigation. The PoC facilitates this process by providing a structure that guides the forensic

[15] https://github.com/DFAX/dfax .

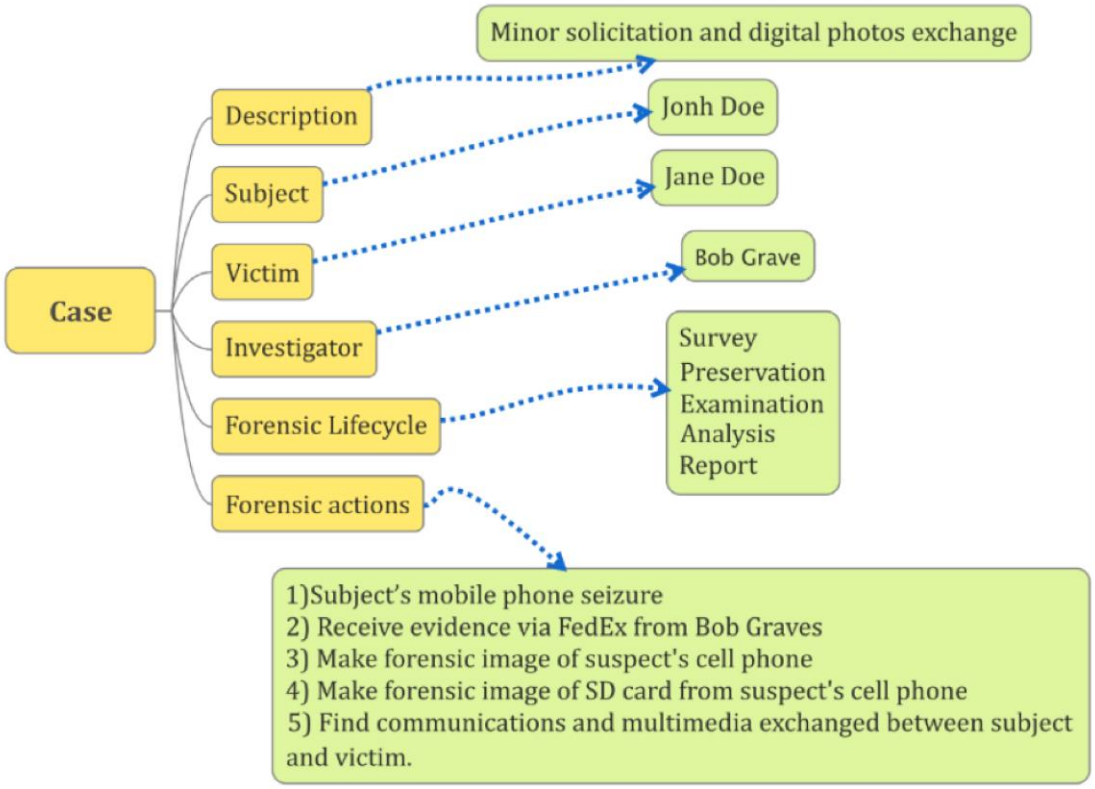

Figure 3: is a representation in CybOX/DFAX of a minor solicitation and digital photograph exchange

investigators and a representation language that enables serialisation of the investigation metadata, and includes packaging, sharing, and the reproducibility of results and the facilitating of the exchange of digital evidence in general. Additionally, the integration of this technology with digital evidence exchange mechanisms can be facilitated by using a structure representation language that has been approved by the forensics community. The aim of the PoC is not to replace or attempt to compete with existing systems, but rather to fill the gaps of functional and data format heterogeneity of existing systems by using standard, semantically rich protocols such as the DFAX language.

One of the main challenges is that the electronic evidence exchange standards require the involvement of a range of different agencies in order to be a success. From a strictly technical point of view, it will be helpful to convince the important agencies in forensics tools development to extend and adapt their software to this new standard.

The way forward

The Common European Framework for the application of new technologies in the collection, preservation, use and exchange of electronic evidence cannot be effective without enhancing technical standards. The way forward should include recommendations for a standard electronic exchange platform and language to represent a wide range of forensic information and processing methods. This includes a standard for representing data and metadata involved in the exchange process and formal languages for their representation. It also introduces a cloud platform for implementing the exchange process, which includes features such as cryptographic control and malware protection. The research carried out by this project also points to the increasing need in the forensics community to provide for the trustworthiness, integrity, efficiency and security of digital forensic tools.

Law enforcement and operational challenges

Law enforcement agencies operate in a field of patchwork solutions (as regards cross-border access to data, data retention, etc.). While the industry continues to push boundaries, law enforcement agencies have to manoeuvre their way through a highly uncertain and politically sensitive landscape that to a certain extent suffers from legal lacunae. Among other things, in an increasingly globalised online environment, the collection and exchange of electronic evidence is hampered by out-dated and lengthy MLA practices that are no longer adapted to today's realities. The legal lacunae hampers the cooperation of international law enforcement. For example, the invalidation[16] of the EU Data Retention Directive,[17] as well as a lack of international consensus regarding cross-border access to data, has led to some uncertainty for law enforcement agencies investigating crimes in the online environment. The need for modernisation efforts in the field of international police and judicial cooperation are therefore necessary. The legal lacunae would mostly be addressed by legal solutions.

Apart from legal solutions, digital forensics urgently needs to obtain a professional status. Digital evidence practitioners have expressed an interest for their field of expertise to reach a level of professionalism and recognition. This would, however, require a reassessment of the potential regulation of digital forensics professions to ensure that practitioners meet a certain standard. Furthermore, as these practitioners often rely on automated digital forensic tools for the acquisition and analysis of digital evidence, these tools should ideally be subject to validation procedures to ensure that they are fit-for-purpose.[18] Lastly, there are currently no universal standards applicable to digital forensic laboratories in particular, thus it is also worth considering the development of an accreditation procedure to ensure digital forensic laboratories meet certain pre-determined quality levels.

As law enforcement is not the sole participant within the digital evidence domain, the importance of ensuring all relevant agencies are included in discussions cannot be understated. Therefore, the collaboration between law enforcement agencies and other participants also needs to be addressed, and it will be necessary to continue developing best practices in recognition of the fact that trusted collaboration with other participants is of the essence in this field. Finally, it is also important to ensure prosecutors and magistrates understand the digital evidence process and digital evidence generally, thereby potentially alleviating prosecutors from unnecessarily burdensome requests for further or additional analysis.

The future

While certain practitioners might fear that standardisation efforts may hamper innovation, there is an overall consensus that the proposals by the EVIDENCE Project are only the beginning of a lengthy standardisation process. In addition, practitioners often rely on automated digital forensic tools for the acquisition and analysis of digital evidence. It is suggested that these tools should be subject to validation procedures.[19] Furthermore, there are no universal standards applicable to digital forensic laboratories. The development of an accreditation procedure to ensure digital forensic laboratories meet certain pre-determined quality levels would aid in achieving a universal standard.

The EVIDENCE Project: the future[20]

The EVIDENCE Project identified a number of challenges as regards the collection, preservation, use and exchange of electronic evidence from different perspectives, and provides a number of objectives for addressing these challenges. The objectives include conducting further research and enhancing law enforcement, legislation, policies, trust, technical standards and digital forensics. These have been

[16] http://curia.europa.eu/juris/documents.jsf?num=C-293/12.

[17] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L105, 13.4.2006, p. 54–63.

[18] For case law in relation to forensic tools, see 6.45 – 6.55 in Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017).

[19] See paragraph *Digital Forensics Tools Validation* in EVIDENCE Deliverable D4.1 – Overview of Existing Standard for Treatment and Exchange of Electronic Evidence: http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d4-1-413.pdf .

[20] The paragraph is inspired by the deliverable D9.2 – Roadmap, prepared by the University of Groningen, partner of the EVIDENCE project, available at http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d9-2-426.pdf . Some parts have been faithfully taken from the original document.

divided into a number of actions, which need to be addressed on a short, medium or long term in order to reach the objectives. All actions need to start as soon as possible and preferably at the same time.

The short term solutions (expected to be addressed in 2 – 3 years) address two objectives: enhanced law enforcement and further research. Enhancing law enforcement is the major objective of the Roadmap (as referred to in the project), taking into consideration that law enforcement agencies are the most important participants involved with electronic evidence. Most of the law enforcement challenges will primarily find a solution through legislation and policy decisions. However, there are also other measures that can be taken in order to enhance law enforcement. This includes improving the MLA procedure in the short term by improving international coordination and joint investigation teams.

Some areas require further research before they can be addressed in the Common European Framework, because there are too many uncertainties regarding these topics. A better understanding of these challenges is necessary in order to provide clear and effective legal, policy, technical and other recommendations which can be included in the Common European Framework. This includes research into constitutional limitations, data retention, the negative effect of legislation, crypto-currencies, the internet of things, cloud computing, technical solutions for admissibility, improving investigative techniques and best practices.

The medium term solutions (expected to be addressed in 3 – 4 years) address four objectives: enhanced legal provisions, enhanced exchange, enhanced trust and enhanced technical standards. Enhancing certain legal provisions, in particular investigative measures that pose a particular challenge, should be addressed as soon as possible. There is a general lack of specific investigative measures, and not all methods sufficiently cover the specific nature of electronic evidence..[21] A more specific legal basis to collect electronic evidence is necessary, in particular in order to avoid admissibility issues in cross-border cases[21] A common European framework for the systematic and uniform application of new technologies in the collection, use and exchange of electronic evidence should include specific, clear and precise investigative measures regarding the collection of electronic evidence. This includes a legal distinction between physical and electronic evidence, lawful interception, computer-assisted search, seizure and preservation and storage. These specific investigative measures need to be addressed in order to provide more clarity, legal certainty and authority for law enforcement agencies in certain areas.[21]

The long term solutions (expected to be addressed in 5 – 6 years) provided in the Roadmap address four objectives: enhanced legal framework, enhanced policies, enhanced law enforcement and a more professional status in the field of digital forensics.

The proposed actions cannot be addressed without the support of all everyone involved. It is not sufficient to enhance legislation and technical standards. For the Common European Framework to be effective, enhanced trust is necessary, in particular enhanced trust in the judiciary, referring to the fact that specific solutions for those people involved in the treatment and exchange of electronic evidence should be enhanced by putting in place specific actions directed to training, education[22] and including electronic evidence in the syllabus for lawyers and judges.[23]

It is important to stress that no one action alone will solve the ensemble of challenges identified by the EVIDENCE Project. The actions need to be taken together for changes to be more effective.

Conclusions

When we started working on the activities of the EVIDENCE Project, there were few who were sufficiently knowledgeable about the topic to have a good understanding of the nature of the problems with electronic evidence. The approach was to be aware of the different challenges and gaps and try to

[21] See the EVIDENCE deliverable D9.2 – Roadmap (already cited above) based on the deliverables D6.1 – 'Overview of the existing mechanisms and procedures for the collection, preservation and exchange of electronic evidence by law enforcement agencies within the European Union and beyond' and D6.2 – 'Status quo assessment and analysis of primary challenges and shortcomings', prepared by INTERPOL, but not public.

[22] Denise H Wong, 'Educating for the future: teaching evidence in the technological age' (2013) 10 *Digital Evidence and Electronic Signature Law Review* 16, and Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice' (2013) 10 *Digital Evidence and Electronic Signature Law Review* 23.

[23] Stephen Mason, 'A framework for a syllabus on electronic evidence', (2013) 10 *Digital Evidence and Electronic Signature Law Review* 7.

recommend suitable solutions from interdisciplinary perspective, bringing into the scope of the project a significant number of organizations:

> Communities involved in electronic evidence handling and exchanging: DFRWS, DFAX/CybOX communities, NIST, INTERPARES
>
> EU institutions: EUROJUST, EUROPOL, COE Cybercrime Convention, OLAF-Digital Forensics Unit and DPO
>
> International institutions: INTERPOL, ICC
>
> Digital forensic software companies: Cellbrite, Oxygen Forensics, Magnet Forensics
>
> ISPs: Facebook, Yahoo, Microsoft, Google, Apple and Samsung.
>
> Public prosecutors, judges and law enforcement agencies
>
> EU Projects: LASIE Project, e-Crime, GIFT, MAPPING, SIIP, e-Codex
>
> Others: Netherlands Forensic Institute; University of Lausanne, Ecole des Sciences Criminelles; National Criminal Investigation Service; Norway, European Cybercrime Training and Education Group; IISFA-International Information Systems Forensics Association; interPARES Community; DFRWS-Digital Forensics Research Workshop group

The effect of the Project was significant.[24] To build on the success of the Project, it is necessary for institutions to begin to put into effect the work undertaken during the project, such as providing for pilot schemes with a view to generating that necessary awareness to render the exchange of electronic evidence in the EIO and MLA context. Once its effectiveness is established in this context, it can be implemented across EU Member States.

Maria Angela Biasiotti is a Researcher at ITTIG-CNR. She has a degree in Law and holds a PhD in Information Technologies and Law at the Faculty of Law, Bologna University. She is a Visiting Professor in Legal Informatics at the Law Faculty of the University of Pisa, and coordinated the EVIDENCE Project.

http://www.ittig.cnr.it/persone/ricerca/maria-angela-biasiotti/

[24] The EVIDENCE Project will be part of the DG Home Annual Report as a 'success story'; a brief description of the Project will be published in the CORDIS website in six languages. Both these publications are forthcoming.