Introduction

Biasiotti, Maria Angela; Cannataci, Joseph A.; Mifsud Bonnici, Jeanne Pia; Turchi, Fabrizio

Published in:
Handling and Exchanging Electronic Evidence Across Europe

DOI:
10.1007/978-3-319-74872-6_1

Chapter 1
Introduction: Opportunities and Challenges for Electronic Evidence

Maria Angela Biasiotti, Joseph A. Cannataci, Jeanne Pia Mifsud Bonnici, and Fabrizio Turchi

Abstract Beyond the different and varied rules that each Member State adopts regarding the admissibility and development of evidence, including digital evidence, elements that in any case must be guaranteed are its relevance and its authenticity with respect to the case being examined. However, these requirements are far from easy to achieve, taking into account some peculiar characteristics of digital evidence, for example, its fragility (easily alterable, damageable and destructible) and its immateriality, namely, the difficulty in associating particular evidence to a physical object: Often it is confused with the device that contains it and therefore closely linked to the concepts of changeability and volatility. This means that the lifecycle of digital evidence must always be accompanied by documentation, always kept up to date, constituting the so-called chain of custody, i.e., the document that describes in detail what happens to digital evidence from the moment in which it was identified as evidence until its presentation before the judge in the trial phase, more specifically, the person who took possession of it to preserve its authenticity, when, where and how, and in what manner. The issue of digital evidence is necessarily interdisciplinary in that it affects different areas: the law in its national, European and international forms, digital forensics, computer science, sociology of law and diplomatics. The latter discipline, perhaps the least known among those mentioned, is focused on "studying the forms that official, legally probative or even constitutive documentation has taken over time".

M. A. Biasiotti (✉) · F. Turchi
CNR, Institute of Legal Information Theory and Techniques, Florence, Italy
e-mail: mariangela.biasiotti@ittig.cnr.it; fabrizio.turchi@ittig.cnr.it

J. A. Cannataci · J. P. Mifsud Bonnici
University of Groningen, Security, Technology and e-Privacy (STeP), Groningen, The Netherlands
e-mail: j.a.cannataci@step-rug.nl; g.p.mifsud.bonnici@step-rug.nl

M. A. Biasiotti et al. (eds.), *Handling and Exchanging Electronic Evidence Across Europe*, Law, Governance and Technology Series 39,
https://doi.org/10.1007/978-3-319-74872-6_1

1.1 The Current Scenario

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, processed, stored or transmitted using any electronic device. Digital evidence is that electronic evidence that is generated or converted to a numerical format.

This definition, proposed by the Evidence project[1] is important because it clarifies the various definitions proposed in recent years and also resolves some of their ambiguities. It takes stock of the concreteness of electronic evidence and demonstrates the profound interdisciplinary character hiding behind this issue.

The definition of electronic evidence introduced above has a broader application than other proposed descriptions, for example, by the Standard Working Group on Digital Evidence[2] or by the International Organisation of Computer Evidence,[3] as it includes both evidence that is born digital, and that which in the course of its life is transformed and then stored or exchanged in electronic form.

In today's modern technological society, every type of investigation potentially has a digital dimension, i.e., a significant part of the relevant information for the case investigated, if not all, can be traced back to and extracted from the digital devices of the parties involved, whether they be victims, suspects or their families.

It is now clear that each of us leaves digital traces everywhere, and these traces can, in the future, be potential evidence in an investigation or a course case.

From a legal point of view, one of the most important results of this phenomenon is that the use of new technologies in the justice sector is emerging in an ever more pervasive and wide-ranging manner, in Europe. After starting the process of computerisation of civil and administrative judicial systems in the various EU Member States, and because of the big push by the European Commission and the Council of Europe towards the computerisation of the justice sector (e.g., the e-Justice program[4] and its portal), the criminal process is also feeling the need to use information technology for the management of procedures and activities connected to investigations and legal proceedings.

In a recent paper in December 2016, the EU Council adopted conclusions to improve the efficiency of criminal justice in cyberspace. Among other things, the document refers to the creation of a secure and trustworthy online portal for the exchange of digital evidence in the context of the imminent entry into force of the European investigation order and mutual legal assistance procedures.

[1] The European Evidence project, European Data Informatics Exchange Framework for Courts and Evidence, is a project financed by the European Commission as part of the 7th Framework Programme (Grant Agreement 608185), www.evidenceproject.eu.

[2] "Digital Evidence is any information of probative value that is either stored or transmitted in a digital form".

[3] "Digital evidence is an information stored or transmitted in binary form that may be relied upon in court".

[4] See also e-justice.europa.eu/home.do?action=home&plang=en&init=true.

In fact, digital evidence is assuming strategic importance not only for so-called cybercrimes (as they have been defined in the Budapest Convention of 2001, ratified in Italy by Law 48/2008), but also for common crimes, in which digital traces can represent a significant potential source of evidence for investigators and judicial authorities.

Beyond the different and varied rules that each Member State adopts regarding the admissibility and development of evidence, including digital evidence, elements that in any case must be guaranteed are its relevance and its authenticity[5] with respect to the case being examined. However, these requirements are far from easy to achieve, considering some peculiar characteristics of digital evidence, for example, its fragility (easily alterable, damageable and destructible) and its immateriality, namely the difficulty in associating particular evidence to a physical object: often it is confused with the device that contains it and therefore closely linked to the concepts of changeability and volatility.

This means that the lifecycle of digital evidence must always be accompanied by documentation, always kept up to date, constituting the so-called chain of custody, i.e., the documentation that details how digital evidence was handled from the moment it was identified as evidence until its presentation to judge in the trial phase. More specifically, chain of custody tracks who took possession of evidence to preserve and maintain its authenticity, when, where and how, and in what manner.

The issue of digital evidence is necessarily interdisciplinary in that it affects different areas: the law in its national, European and international forms, digital forensics, computer science, sociology of law and diplomatics. The latter discipline, perhaps the least known among those mentioned, is focused on "studying the forms that official, legally probative or even constitutive documentation has taken over time" (Valenti, 1961).

Concerning the issue of digital evidence, it becomes important where it deals with contemporary records and even digital documents (Duranti, 1998).

Furthermore, dealing with digital evidence means addressing the separate reality that surrounds it. This means basing oneself not only on studies and analyses on a theoretical level but also on the experience of those who routinely work with this particular type of evidence in real life, and also managing the variety of actors involved in various capacities in the lifecycle of electronic evidence. Constant and open dialogue with these actors is crucial in this area, especially given the continued and rapid evolution of technology. Comparing design ideas, operational proposals and practical needs that are waiting to be fulfilled, if done directly by the stakeholders concerned, can only produce a shared and efficient outcome for all parties involved.

The following entities are to be considered among the main stakeholders involved in various ways and with different roles in the domain of electronic evidence:

- Communities involved in the processing and/or exchange of electronic evidence: the Digital Forensics Research Workshop (DFRWS), the Netherlands Forensic

[5] ISO/IEC 27043:2015, Incident investigation principles and processes.

Institute—NFI, the National Institute of Standards and Technology—NIST, academic/scientific community of the INTERPARES project.
- European organisations and agencies: Eurojust, Europol, OLAF—European Anti-Fraud Office.
- International institutions: Interpol, International Criminal Court—ICC and European Council.
- Forensic software companies: Cellebrite, Oxygen Forensics, Magnet Forensics, Microsystemation (MSAB).
- The major Internet service providers and large software companies: Apple, Facebook, Google, Microsoft, Samsung and Yahoo.
- Prosecutors, judges and police forces of various European Union Member States.

There are, then, various European projects connected with subjects complementary to that of digital evidence: LASIE, e-Crime, GIFT, Mapping, SIIP, e-Codex, e-Sens, EA-Fit Tools, and others. Strengthening relations and synergies among the various players is an ambitious challenge, but success would make it possible to address common problems in a systematic and shared manner, developing solutions that can stimulate the future work of policy makers.

1.2 Digital Forensics

The concept of digital evidence is inextricably linked to digital forensics,[6] the discipline that deals with the recognition, preservation, acquisition and analysis of digital information, with the objective of addressing forensic questions relevant to the legal inquiry being carried out.

Digital forensics is definable not only about techniques and tools for the extraction of investigative information in accordance with certain technological standards,[7] but above all focuses on the study of the scientific processes, procedures, technologies and rules to use, develop, adapt or propose to improve the results achievable while at the same time better protecting the integrity of digital evidence.

Recent developments in digital forensics, as a profession and as a scientific discipline, have grown out of efforts by organizations that support criminal justice to address the growing prevalence of crimes committed through the use of new technologies. Consequently, groups of specialists for investigations into cybercrime have been establish on a national level in Europe, the United States and other countries. Furthermore, in some countries specific training programmes on digital forensics were developed, aware that the spread and pervasiveness of digital devices requires that every police officer have solid basic training in dealing with electronic evidence.

[6]Following is a brief and non-exhaustive bibliography on the subject: Carrier (2003, 2006), Casey (2011), Daniel (2012), Henseler (2000), Mason (2012), and Richardson (2009).

[7]ISO/IEC 27037:2012, Guidelines for identification, collection, acquisition, and preservation of digital evidence, ISO/IEC 27042:2015, Guidelines for the analysis and interpretation of digital evidence, etc.

Originally digital forensics concerned a single discipline, currently indicated by the name computer forensics, which mainly focused on the computer as a source of evidence. In the last 20 years, the technological evolution has gradually shifted towards mobile devices, connectivity has assumed a global dimension and the use of increasingly newer and more complex devices and systems is spreading: just consider for example the development of so-called IoT—Internet of Things devices like the Smart Watch, Smart TV, Smart Home, the growing use of cloud storage systems, the use of virtual currencies (like Bitcoin) and the Dark Net. People are therefore moving away from traditional devices towards a completely interconnected world where digital traces left by each person are on the rise, locally recorded on different devices or remotely in the cloud even beyond national borders. This rapid and continuous technological evolution has resulted in the equally rapid development of the sub disciplines of digital forensics, outlined, although not exhaustively, in the following list:

- computer forensics: discipline that includes software tools for the forensic analysis of file systems, operating systems, applications. In particular, there are numerous tools to manage the sources of evidence generated by the use of applications. Some of these include tools for various types of analysis: for digital traces generated by the use of browsers, for chat configuration and log files, configuration files related to cloud storage, email archives, data and configuration files relating to peer-to-peer applications, data and configuration files related to social networks (Facebook, LinkedIn, Twitter, etc.).
- Mobile forensics, for the analysis of mobile devices.
- Network forensics, for the analysis of network traffic.
- Memory forensics, for the analysis of RAM memory and hibernation files.
- Malware forensics, for the analysis of malware.

The need felt by law enforcement in this specific area is to increase confidence through the preparation of rules and procedures established by law, and a set of guarantees associated with the acquisition and analysis of digital evidence. In this regard, it would seem particularly important to render the relatively young field of digital forensics more professional. Digital forensic professionals have expressed an interest in their field of expertise reaching a level of professionalism and recognition similar to that achieved in the field of DNA analysis. However, this requires a review of the potential regulation of digital forensic professions to ensure that operators meet a certain standard. Moreover, as these professionals 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 they are fit for the purpose. Finally, there are currently no universal standards applicable to digital forensic laboratories, so it is therefore appropriate to consider the development of an accreditation procedure to ensure that laboratories meet predetermined levels of quality.

Of equal importance in digital forensics appears to be the need to “build bridges” between police forces and other stakeholders, including the private sector and the judiciary. Therefore, the cooperation between all these stakeholders is of particular

importance. In the end, the acquisition of technical skills is critical for prosecutors and judges, so they can understand the processes behind the collection and analysis of digital evidence.

Further, it is also necessary to address the issue of the relationship with the companies that produce the tools that are used for the acquisition and analysis of digital evidence. On this front, it is necessary to stimulate dialogue with these producers, leading to the adoption of a standard language that, above all, supports interoperability of the results produced by the various tools and systems.

1.3 Legal Framework in Europe

At the European level, there is still neither a unified legal framework nor shared rules that make it possible to handle digital evidence and its possible exchange in a uniform manner across the Member States.

Currently, evidence is exchanged in transnational contexts from the competent authority of one Member State to the competent authority of another Member State. However, there are no specific rules that systematically and clearly regulate the collection, storage, processing and exchange of electronic evidence.

Among the most urgent needs felt by the various parties involved in the lifecycle of digital evidence, particularly worthy of mention are:

- A uniform European regulation regarding digital evidence, first in terms of acquisition and admissibility.
- A common perception, even regarding the reliability of digital evidence, held by all stakeholders (police, judges, lawyers, forensic specialists, etc.).
- Greater cooperation and greater mutual trust among the forces that fight crime, especially when it involves different countries.
- Common investigation and criminal procedures to counteract or prevent the globalisation of crime.
- Secure and reliable tools that ensure the integrity and authenticity both in the transmission and the reception of the request and the evidence itself.

The lack of common rules is all the more problematic considering evidence and the person committing the crime may be located outside the borders of a particular State, raising issues of territoriality.

To overcome these difficulties, it is necessary to promote and develop international cooperation between judicial and police authorities of the different States, especially considering the differences in legal systems and methods of investigation.

At a European level, there are a limited number of legal instruments that can be directly or indirectly relevant to the collection, storage, processing and exchange of electronic evidence. Most of them have been implemented by the various Member States, but often in different ways, according to their own legal systems and traditions.

Although initiatives have been promoted to overcome legal gaps, including by the European Union and the Council of Europe, there are still many limitations. Given that the specific nature of electronic evidence and the rapid evolution of both technology and of crimes committed using it, it is essential to activate an action plan for creating a single legal framework on a European level for the collection, processing and exchange of electronic evidence.

This European framework should be a compromise between the need to ensure efficient police investigations and respect for the fundamental rights of every citizen, on which the new technologies have a major impact.

1.4 The Volume

The volume collects all the efforts made during the EVIDENCE project to create the knowledge and the necessary awareness on this topic. It is also emblematic of the huge network of stakeholders with whom the Project got in contact with and established a solid relation and connection. Therefore, the volume collects contributions by those who have played a leading role in the project activities, as well as by representatives of the different institutions engaged in the growth of the awareness on this topic from a European and International perspective.

It can be affirmed that almost all the stakeholders involved in the handling and exchanging of electronic evidence have contributed to this Volume. Their perspectives, according the specific roles played, are described and shared with the largest community.

The volume is divided into four parts.

The first part is devoted to provide the context of interest of the Volume and to set the scene of the Electronic Evidence handling and exchange scenario at European and international level. It comprises a brief introduction of the editors of the manuscript where some relevant points are emphasised. This chapter is followed by the contribution by M.A. Biasiotti who sets the scene of the Electronic Evidence Treatment and Exchange in Europe, summarises the actions taken by the European Union concerning the processing and exchange of electronic evidence, and also gives account both of the provisions for Mutual Legal Assistance (MLA) and European Investigation Order (EIO), as well as actions carried out by the Council and the European Commission through working groups, emphasising the important innovative contribution resulting from the on-going initiatives and projects.

The second part hosts contributions of authors offering an international perspective and view of how electronic evidence is treated in those contexts outside European Union, mainly international. In this part A. Seger, briefly reports on the important process in which the Council of Europe is engaged with the Cloud Evidence Group and describes the way the Council of Europe, Cybercrime Convention is currently dealing with the e-evidence and access to data in the cloud, whilst Eoghan Casey et al., present the new frontier of digital forensics by describing the evolution of expressing and exchanging cyber-investigations data and

metadata in a standardised form. This part is concluded by F. Cajani, who gives an overview of the matters not yet solved regarding communications, interception systems and electronic data detained on foreign servers, mainly involving Internet Service Providers.

The third part hosts contributions by representatives of the various institutions dealing with the electronic evidence treatment and exchange from a practical point of view in the context of criminal field, with the aim to trace the operational scenario and give the practitioners point of view. The first contribution by S. Berghs et al., from INTERPOL, describes the operational scenario of their institution, specifically focusing on the work related to the treatment and exchange of electronic evidence; the contribution by H. Ilyoung, from International Criminal Court, provides an introduction to the activities and challenges of digital forensics in international criminal investigations, and draws attention to requirements for more international cooperation, awareness improvement, standard establishment and the need for a joint effort at solving technical issues; D. Drewer and J. Ellermann, from EUROPOL, describe how the online environment represents a challenge for privacy and the suppression of crime in the context they work for; finally X. Tracol, from EUROJUST offers argues about the use of MS PowerPoint presentation by prosecutors and attorneys during the criminal trials.

The last part describes the effort and the success results and story of the activities carried out during the EVIDENCE project reporting on the results achieved. S. Avveduto et al., describe the categorisation realised for the electronic evidence domain with a specific perspective in the criminal field; J. Mifsud Bonnici et al., report on the analysis of the legal scenario existing in the EU when dealing with the treatment and exchange of electronic evidence; F. Turchi and M. Epifani present the building up process for creating the first Digital Forensic Tools Catalogue, whilst N. Forgò et al., analyse the specific data protection issues arising with the treatment and exchange of electronic evidence in the EU, D. Mezzana describes the social arena of all actors involved in the electronic evidence chain also considering facilitating factors and obstacle in the process of implementing the change needed to pave the way to the electronic evidence exchange in Europe; F. Turchi and E. Epifani gives details of the proposal and the need to adopt a formal standard language when exchanging electronic evidence and describe benefit of such proposal; and N. Matskanis et al. present the Environment realised to allow the exchange process in Europe by adopting the proposal achieved under the EVIDENCE project. A. Tsvetkova stresses the work needed to manage and render successful a EU funded project where experts from different background and different expertise are put together and must find a way to collaborate and to integrate their knowledge. Finally J. Mifsud Bonnici, J. Cannataci and M.A. Biasiotti present the EVIDENCE Road map to the future realisation of a common legal Framework in Europe dealing with the treatment and exchange of electronic evidence.

1.5 Final Reflections

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

Even actors directly involved in the treatment of electronic evidence by default (public prosecutors, law enforcement agencies (LEAs) and judges) demonstrated significant gaps and challenges in their knowledge and training. The status quo at the beginning of the EVIDENCE project was "I know electronic evidence exists, I know I cannot make it without but I don't know how to deal with it and treat and handle it without compromising it…".

We realised that fragmentation cannot only be found in the legal framework, but is also reflected by the vast number of actors involved. On an international level there are several actors involved, such as Interpol, Eurojust, Europol and its EC3 cybercrime centre and Joint Cybercrime Action Taskforce (J-CAT), CEPOL and ENISA. However, when we look at a national level the number of actors involved in one way or another becomes numerous. Certain public and private actors providing technical solutions and assistance have a direct interest in electronic evidence. These are process actors that make up the supply and demand for technologies and services. Other type of actors are context actors and play an indirect role in electronic evidence in a broader political, social or economic context.

Considering this vast number of actors involved, one of the issues is that these actors are not always in agreement considering the different interests involved and that they do not always coordinate with each other. Other obstacles include mistrust within the judiciary, lack of necessary competences and professionalisation, cultural differences, lack of governance and functional difficulties. Solutions to address these issues include mandatory training and education, certification, building bridges between the private and public sector, raising awareness, validation of digital forensic tools, etc.

The Impact of such an initiative was very big. The added value realised by the results of the Project to its context is emphasised by the many positive reactions and feedback received from the electronic evidence community and from the European Commission as well. Since the beginning of the project, in 2014, in two and a half years we have been able to generate awareness, stimulated the debate, opening/setting up a dialogue and creating specifically a network and community, also merging into the EVIDENCE initiative one the various communities and stakeholders belonging to different disciplines and domains.

It is now clear that it is necessary to establish a common European framework for the processing and exchange of digital evidence to effectively counter crime, which is increasingly international, be it terrorism or cybercrime.

All the actors at a European level, like Eurojust, Europol, the European Commission, the magistrates and the police forces, now seem convinced that it is of vital interest to achieve the exchange of evidence in legal matters. Because the evidence comes in the form of information of a certain type, chain of custody, integrity and authenticity must be ensured, both of the request and of the response that will be given. Once again, the obstacle to be overcome together for the implementation of a digital platform that will enable exchange is and remains the lack of "trust". It all revolves around the ability to develop and deploy operational, political, legal and technological tools that are able to feed and cultivate this simple but fundamental relational concept.

The many meetings with the experts, often behind closed doors, and the many contributions gathered in this volume make us very hopeful.

References

Carrier BD (2003) Defining digital forensic examination and analysis tool using abstraction layers. Int J Digit Evid 1(4):1–12

Carrier BD (2006) A hypothesis-based approach to digital forensic investigations. CERIAS technical report 2006-06. www.cerias.purdue.edu/assets/pdf/bibtex_archive/2006-06.pdf

Casey E (2011) Foundations of digital forensics. In: Casey E (ed) Digital evidence and computer crime, 3rd edn. Academic, Waltham

Daniel L (2012) Digital forensics for legal professionals. Understanding digital evidence from the warrant to the courtroom. Syngress, Amsterdam, p 368

Duranti L (1998) Diplomatics. New uses for an old science. Scarecrow, Lanham, p 186

Henseler J (2000) Computer crime and computer forensics. In: The encyclopedia of forensic science. Academic, London

Mason S (2012) Electronic evidence, 3rd edn. Lexis Nexis Butterworths, London, p 934

Richardson J (ed) (2009) Archbold: criminal pleading, evidence and practice. Sweet & Maxwell, Thomson Reuters, London

Valenti F (1961) Il documento medievale. Nozioni di diplomatica generale e di cronologia, Modena, Società Tipograca Editrice Modenese, p 226