Collezione di Giustizia Penale

dedicata a Massimo Nobili
e diretta da Marcello L. Busetto, Alberto Camon, Claudia Cesari,
Enrico Marzaduri, Daniele Negri

7

Each volume published in this series has been approved by the directors and – with the exception of conference proceedings – submitted for double blind peer review in accordance to the series' regulation. The regulation and the records pertaining to the review of each book are kept by the publisher and by the directors.

DIGITAL FORENSIC EVIDENCE

TOWARDS COMMON EUROPEAN STANDARDS IN ANTIFRAUD ADMINISTRATIVE AND CRIMINAL INVESTIGATIONS

edited by
Michele Caianiello and Alberto Camon

Wolters Kluwer CEDAM

Printed by GECA s.r.l. - Via Monferrato, 54 - 20098 San Giuliano Milanese (MI)

This publication was funded by the European Union's HERCULE III programme.

Table of contents

LAURA BARTOLI-GIULIA LASAGNI

THE HANDLING OF DIGITAL EVIDENCE IN ITALY

Katalin Ligeti-Gavin Robinson

THE HANDLING OF DIGITAL EVIDENCE IN LUXEMBOURG

LORENA BACHMAIER WINTER

THE HANDLING OF DIGITAL EVIDENCE IN SPAIN

Laura Bartoli-Giulia Lasagni

ANTIFRAUD INVESTIGATION AND DIGITAL FORENSICS: A COMPARATIVE PERSPECTIVE

Michele Caianiello

CONCLUSIVE REMARKS
ANTIFRAUD INVESTIGATIONS AND RESPECT FOR FUNDAMENTAL RIGHTS FACED WITH THE CHALLENGE OF E-EVIDENCE AND DIGITAL DEVICES

Raffaella Brighi-Michele Ferrazzano

DIGITAL FORENSICS: BEST PRACTICES AND PERSPECTIVE

Overview: 1. Introduction, issues, and goals. – 2. Digital forensics. – 3. Standards and guidelines. – 3.1. International standards and guidelines. – 3.2. Overview of guidelines, best practices and soft regulation of DEVICES' Partners. – 3.3. Guidelines on Digital Forensic Procedures for OLAF Staff – 4. Digital forensics expert: roles and skills. – 5. Main steps in digital investigations. – 6. The digital forensics lab: tools, facilities, and requirements. – 7. The big amount of data: technical requirements versus privacy. – 8. Conclusions: recommendation and perspective.

1. *Introduction, issues, and goals*

This contribution aims to conduct a technical investigation on the methodological requirements for the processing of digital evidence, with specific reference to anti-fraud procedures. In this context, from a digital forensic perspective, our research focuses on two aspects. The first one aims to identify the minimum criteria that need to be met in all the stages while processing digital evidence in order to obtain reliable evidence, as well as the skills needed by those who work on digital evidence and the characteristics required for the facilities (e.g. labs) entrusted with digital investigations. The second aspect relates to the amount of digital data that need to be gathered and brought to court in order to have meaningful evidence, while protecting the privacy of the individual in relation to the data stored in digital devices – this strictly related to the defence right of those who are subject to investigation. On this topic, the work sets out an alternative method for selecting the digital data, in such a way as to balance the two competing goals of ensuring complete investigations while respecting the privacy of those investigated, as provided by

the Guidelines on Investigation Procedures for OLAF Staff at § 15.3 [1].

In the practice of trial procedure, the peculiar structure of digital data engenders the illusion that what is digitally represented is indisputable, as is the meaning ascribable to such representation. This prompts us to uncritically believe that a digital exhibit is suited to support the judge's logico-probative reasoning.

Digital data is a representation that uses a binary sequence of bits that are not human-understandable. Therefore, it requires a series of operations through which a transformation is realized that may lead to different results (displayed as text on a screen or as a video, or again as an image printed on paper) [2]. Without interpretation, data cannot have any meaning [3].

By its nature, digital data is: "immaterial", requiring a suitable support to store on, such as a CD-ROM, hard disk, or flash drive; "volatile": it can easily be dispersed; "corruptible," meaning that it can be modified anonymously or involuntarily; "reproducible" without any limit on the number of copies that may potentially be made of it.

Digital evidence may be characterized as any data that (a) is allocated somewhere on a digital device or sent across computer systems of telecommunications networks and (b) can have some relevance in the outcome of a judicial process [4].

Every data useful to support or reject a theory about the way an

---

[1] Available at: *ec.europa.eu/anti-fraud/investigation-guidelines-olaf-staff_en*.

[2] For an introduction to the relationship between concepts of "data" and "information" see G. CONTISSA, *Information technology for the law*, Giappichelli, Torino, 2017, p. 73 ff.

[3] J. SOWA, *Conceptual Structures: Information Processing in Mind and Machine*, Addison-Wesley, Reading, MA, 1984.

[4] Both properties are included in the well-known definitions of digital evidence on which the technical-scientific community converges: the definition by the Standard Working Group on Digital Evidence – «Digital evidence is any information of probative value that is either stored or transmitted in a digital form»; and the definition by International Organisation of Computer Evidence – «Digital evidence is an information stored or transmitted in binary form that may be relied upon in court». A summary definition, which seems to cover every relevant aspect and also includes the concept of electronic evidence, was recently developed in 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)): «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

offence was committed or to establish intent or an alibi can be considered digital evidence.

During a trial, the way digital data has been collected or stored is often challenged. This is owed to the fact that these activities necessarily require to deal with intangible material invisible to those with no specific competence in the area in question (an example could be a *log file* containing traces of illicit activity).

Neglect, lack of skill, or inappropriate methods can all result in the judge reasoning on data that have been misidentified or improperly collected or stored, leading to flawed expert opinions and reports.

As happens with any type of evidence, including digital evidence, the burden of demonstrating that the evidence is truthful and authentic falls on the party who introduces it. The use of digital evidence is constantly increasing, and it is therefore possible that courtrooms use, more and more, to keep copies of emails, digital photographs, word-processing documents, electronic spreadsheets, GPS tracking data, audio files, and digital videos.

Traditionally and historically, evidence has been presented either in tangible form (paper documents, printed photographs, and so on) or on the basis of witness or expert testimony. Digital evidence is obtained from devices that process digital data either locally (in the device itself) or within a computer network (typically the Internet). Like other kinds of evidence, digital evidence needs to be reliable and to preserve its integrity, meaning that it must be shown without alteration or tampering. Herein, then, lies the key challenge posed by digital evidence: because electronically represented data is intangible, it more easily lends itself to being altered or doctored than traditional sources of information, and these alterations are often difficult to perceive, detect, and document – all of which makes it necessary to use specific methods and technical procedures if digital data is to qualify as reliable and thus achieve the status of evidence proper.

Because recourse to digital evidence raises the issues that come up with scientific evidence, it becomes necessary to construct an epistemological framework [5] through which there is the need to define methodological standards and technical tools suited to

---

any electronic device. Digital evidence is that electronic evidence that is generated or converted to a numerical format».

[5] See S. Haack, *Legalizzare l'epistemologia. Prova, probabilità e causa nel diritto*, Egea, Milan, 2015; Id., *Six Signs of Scientism*, in *Logos & Episteme*, 3 (2012), i. 1, p. 75 ss.

guarantee the procedural certainty and transparency to cope with the increasing complexity of services in the ICT sector, as well as with the internationalization of investigations involving digital data.

Considering the foregoing, it will come useful to go through the list of the main characteristics by which digital evidence is distinguished:

intangibility: a digital bit does not present itself in any physical form, making it necessary to find for it an adequate support capable of storing so that it can subsequently be accessed;

alterability: digital data is binary (its value being either 0 or 1), making it possible to alter it anonymously, often without leaving behind any traces of such alterations, and as a result its processing needs to be done implementing appropriate measures by which to store and safeguard it;

change owing to regular use or mishandling: digital data can undergo change even as a result of "regular usage" (simply by booting up a computer), such that it is processing for evidentiary purposes needs to be subject to specific methods by suitably trained personnel;

volatility: once digital evidence is altered, it is no longer possible to restore it to its previously stored value; in addition, there are circumstances in which digital data can easily be dispersed owing to the characteristics of the support that stores it (consider, for example, the digital data contained in the RAM memory of a system that gets shut down while executing some process);

potentially unlimited reproducibility: any digital data can be copied to other devices with memory capacity, the only limit here being the amount of storage space available in these devices; it is worth noting, in this connection, that if a copy is made using the appropriate methods, it will not alter the original data, making it therefore possible to use copies that for all intents and purposes are originals.

2. *Digital forensics*

The aim of *digital forensics* [6] is to apply scientific and analytic

[6] On the subject: B.D. CARRIER, *Defining digital forensic examination and analysis tool using abstraction layers*, in *International Journal of Digital Evidence*, 1(2003), i. 4, p. 1-12; E. CASEY *Foundations of digital forensics*, in ID. (ed.) *Digital*

techniques to digital data stored on digital devices or moving across a digital network, so as to identify, process, and preserve such data, in such a way that it can be assessed as evidence at trial. Digital forensics thus answers the need for the technical and methodological rigor required by the legal process, and it defines best practices for managing digital evidence.

From the standpoint of digital forensics, any digital evidence needs to satisfy the following criteria [7] if it is to qualify as such:

integrity: this means that none of the activities done using the data can alter it, except where acquiring the data makes it necessary to resort to procedures that entail changes, which in turn will have to be kept to a minimum [8];

authenticity: digital data must present itself in the same condition in which it was originally acquired;

completeness: digital data needs to be acquired along with its context, in such a way as to make it possible to properly assess its probative value by either of the two parties concerned (those who bring it in as evidence in support of the claims they are making, and those who need to defend themselves against those claims);

reliability: digital data can not reveal itself to have been altered, and at any rate it must provide all the guarantees needed to forestall any doubt that may arise as to its authenticity and truthfulness;

pertinence: digital data needs to speak to the case for which it is brought in as evidence;

adequacy: digital data needs to be gathered in a manner that is

---

evidence and computer crime, 3rd ed. Academic, Waltham, 2011; L. DANIEL, *Digital forensics for legal professionals. Understanding digital evidence from the warrant to the courtroom*, Syngress, Amsterdam, 2012; J. HENSELER, *Computer crime and computer forensics*, in *The encyclopaedia of forensic science*, Academic, London, 2000; S. MASON, *Electronic evidence*, 3rd ed., Lexis Nexis Butterworths, London, 2012. See also M. POLLIT, *A History of Digital Forensics*, in K.P. CHOW-S. SHENOI (eds.), *Advances in Digital Forensics VI,* Boston, Springer, 2010, pp. 3-15. In Italy, one of the first definitions of the discipline and its scientific approach is presented in C. MAIOLI, *Dar voce alle prove: elementi di informatica forense*, in *Crimine virtuale, minaccia reale*, Franco Angeli, 2004 and in C. MAIOLI, *Introduzione all'informatica forense*, in P. POZZI (eds.) *La sicurezza preventiva dell'informazione e della comunicazione*, Franco Angeli, 2004. For an in-depth examination of the main areas of Digital forensics see also C. MAIOLI (ed.), *Questioni di Informatica forense*, Aracne, 2015.

[7] See, among all, E. CASEY, *Digital evidence and Computer Crime. Forensics Science, Computers and the Internet*, 3rd ed., Academic Press, 2011.

[8] In the Italian legal system, the acquisition of data susceptible to being altered in the process is governed by Article 360 of the Code of Criminal Procedure. See *infra*, L. BARTOLI-G. LASAGNI, *The handling of digital evidence in Italy*, §§ 2-3.

adequate to its purpose if its informational contribution is to be appreciable;

documentation: each step in the process needs to be documented in accordance with the *chain of custody* paradigm [9], following the lifecycle of digital evidence. That means that every step in the handling of digital data must be recorded chronologically, so as to make it possible to track and protocol the full journey the evidence makes from the moment it is identified to the moment it reaches trial, thereby guaranteeing a transparent process and the integrity of its outcome. Any expert, including an independent one or one the court appoints at a later time, needs to be able to repeat all the operations carried out during the digital investigation, and needs to be able to do so solely by looking at the chain of custody and having a copy of the data in hand.

It can be observed that in standardizing the manner of carrying out digital forensics operations, lawmakers across all countries have placed greater emphasis on the result that is to be achieved than on the method to be followed in working toward that result: the fear has been that if technical procedures are etched in the law itself, that would not have acted as a safeguard but, in the long run, would instead have led to contrary and distortion effects owing to the discipline's constant evolution and to the peculiarities distinctive to each case.

Until October 2012, the methods were set out in some sector-specific best practices aimed to outline the paradigms of technical procedure in digital forensics, this through a method that allows to (a) capture evidence without altering or damaging the original device; (b) authenticate the exhibit and the (bitstream) image [10] that

---

[9] To the need for documentation, the *best practices* give an answer with the North American institute, already used for particular types of physical goods, of the "chain of custody". This term alludes, in our system, to a complex of procedural rules and technical regulations which – with the ultimate aim of guaranteeing the genuineness and integrity of the finds and the traceability of the operations – impose the meticulous documentation of every step taken by the digital data from the moment of acquisition to their entry into the process. On this subject, see L. BARTOLI-C. MAIOLI, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in *Informatica e diritto*, 2015, i. 1-2, p. 139-151. On the implementation of computable models for the chain of custody, please refer to R. BRIGHI-V. FERRARI, *Digital evidence and procedural safeguards: potential of blockchain technology*, in *Ragion Pratica*, 50 (2018), i. 2, p. 329.

[10] A bit stream image (or a forensic copy, or bit-to-bit copy) is the bit-by-bit copy of digital data in one digital data storage device to another digital data storage device, either in clone mode or in image mode. With this methodology, exact cloning is

has been captured; (c) guarantee that the findings of fact can be repeated; (d) analyze the original data without modifying it; and (e) ensure that the fact-finding activities are as impartial as possible.

From the standpoint of digital forensics, then, the digital nature of the evidence makes it necessary to take two elements into account.

(i) The first is an *objective element*, and it consists in following sector-specific standards and guidelines. There is a twofold criterion that is doubtlessly useful in enabling information technology to effectively interface with the law: for one thing, the chosen standards should not force the use of any specific technology that practitioners must commit to indefinitely; and, for another, the operating procedures and investigative methods supported by the standard must be ones in wide use among digital forensics experts.

(ii) A *subjective element*, consisting in the skillset the forensics expert applies to digital data from the moment the digital evidence in question is detected. This is an essential element, considering that a legal proceeding can be seriously undercut by ignorance of the duties and responsibilities assumed under the law governing the handling of digital data, and considering the legal consequences of mishandling such data, as well as by failure to use the techniques the law prescribes for such handling.

In practical terms, however, the development and implementation of common procedures comes up against two limits, one having to do with technology – particularly as concerns the media on which data is stored and the "technological habitat" in which the device in question works and is put to use – the other owed instead to the subjective element, meaning the subjectivity that individuals bring to their activity, as well as the aims pursued through that activity: for law enforcement, the aim will be to acquire the elements needed to advance their investigation, all the while preserving the authenticity of the evidence so acquired; for the judiciary, the aim will be to connect those discoveries to criminally relevant facts; for the court-appointed or party-appointed expert, the aim will be to check that the procedures followed in obtaining the evidence at hand are consistent with a proper exercise of the right to defence.

---

performed without loss of data in the destination and without alteration of data in the source. See below, § 5.

3. *Standards and guidelines*

Digital forensics experts have several guidelines at their disposal, each laying out principles and methods for the proper handling of digital evidence.

In order to provide technical and methodological rules for the collection and the handling of digital evidence in antifraud procedures, the research was focused on: (a) the selection of the main international standards and guidelines, in view of the international recognition they have gained and of their relevance to antifraud, (b) the overview of guidelines and best practices recommended by partners, and (c) the exam of *Guidelines on Digital Forensic Procedures for OLAF Staff* (2016), treated as a point of reference for the final recommendations.

3.1. *International standards and guidelines*

The main international standards and guidelines, selected in view of the international recognition they have gained and of their relevance to antifraud, are the following.

ISO/IEC International Standards. Since 2012, the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC) have put out technical standards forming a coherent corpus serving as a useful reference point for digital investigations in all areas in which such investigations occur. These standards therefore cover not only criminal but also civil procedure, as well as investigations carried out internally within government agencies and private organizations alike, and whose findings may therefore never end up in a courtroom. ISO standards are (i) international, (ii) independent of the law in force in each single country, and (iii) independent as well of the instruments and technologies that may be used in complying with them (*technical neutrality*). In particular, the ISO/IEC standards relevant for the purpose of this research are the following: (1) ISO/IEC 27037 «Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence»; (2) ISO/IEC 27041 «Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method»; (3) ISO/IEC 27042 «Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence»; (4) ISO/IEC 27043 «Information technology – Security techniques – Incident investigation principles

and processes»; (5) ISO/IEC 27050 «Information technology – Security techniques – Electronic discovery».

Best Practice Manual for the Forensic Examination of Digital Technology (ENFSI, 2015). The European Network of Forensic Science Institutes (ENFSI)[11] was Established in 1995. Today it comprises 37 European countries, including most of the EU member states. As a network of experts, ENFSI is devoted to the purpose of sharing knowledge and experiences and coming to mutual agreements in the field of forensic science, including the domain of digital evidence. For this purpose, the ENFSI encourages all the laboratories that are part of the network to comply with best-practice and international standards in order to ensure quality and competence. The Best Practice Manual (BPM) for the Forensic Examination of Digital Technology (2015) provides frameworks for procedures, quality processes, and training processes for forensic examinations in IT. It is focused on providing guidance for forensics laboratories having to comply with international and local regulatory standards. Particularly section 4 defines the characteristics an IF laboratory needs in compliance with the ENFSI code of conduct. It sets criteria for (i) the composition of the digital forensics unit (section heads/operations managers, technical experts; analysts, assistants), (ii) the equipment, (iii) the reference material, (iv) the workplace setting and environment; and (v) the archival practices. The BMPs addresses all the phases of digital investigations, from the methods for handling items (physical seizure, protection, the transportation and archiving of digital evidence), through to the case assessment and the examination and reconstruction of events, and including the evaluation, interpretation, and presentation of findings.

Electronic Evidence Guide (EEG, Council of Europe, 2013). The Electronic Evidence Guide (EEG), developed by the Council of Europe, is intended for use by law-enforcement and judicial authorities only to support and guide them in identifying and handling electronic evidence using methods that will ensure that the authenticity of evidence will be maintained throughout the process. The EEG has been prepared with a special focus on the fight against cybercrime. It also covers state-of-the-art technology such as mobile

[11] ENFSI is the EU's regulatory agency that sets the standards to be used in forensics labs. Its operating protocols are therefore in use by Europol as well as other EU agencies doing forensic work. A list of associated laboratories may be found at *enfsi.eu*.

devices and cloud storage and has a section on live-data forensics, raising awareness of how important it is to be able to capture volatile data.

Electronic evidence: A basic guide for first responders (ENISA, 2014). The guidelines issued by the European Union Agency for Network and Information Security (ENISA) [12] have been developed with a view to supporting and shoring up collaboration between Computer Emergency Response Teams (CERTs) and law enforcement, and are designed to help CERTs in their task of supporting law enforcement in gathering evidence. To this end, the guidelines integrate the welter of material that exists on the topic of digital forensics, often written from a law-enforcement perspective, so as to provide CERTs with guidance in an area that is often new to them, in such a way that they can deal with potential digital evidence and the evidence-gathering process. The guidelines touch the different phases first responders encounter when performing digital forensics or electronic evidence gathering and describe how they should act before and while arriving at the scene, what they should keep in mind when performing memory forensics, etc. Then, a CERT first responder can deal with gathering of electronic evidence in an appropriate way and have a good communication with law enforcement.

Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (2019). The Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (2019) [13] are the first international instrument designed to address issues arising in specific relation to electronic evidence in civil and administrative proceedings. Like other international standards for the handling of digital evidence, these guidelines deal with the use, collection, seizure, transmission, storage, and preservation of digital evidence. They also address awareness-raising, training, and education. It is worth pointing out § 4 of these guidelines, with their emphasis on due process rights [14].

---

[12] Electronic evidence: a basic guide for first responders (ENISA, 2015), online at *enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders*.

[13] Online at *search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c*.

[14] On this subject see *infra*, L. BARTOLI-G. LASAGNI, *The handling of digital evidence in Italy*, § 4.

Particularly relevant are the following guidelines, developed at the national level, but widely turned to at the international level as well.

Guidelines on Digital forensics (NIST – National Institute of Standards and Technology, USA, 2014). The NIST [15] Guidelines on Digital forensics [16] (2014) provide basic information about digital devices and forensics tools designed for the preservation, acquisition, examination, analysis, and reporting of digital evidence stored on digital devices. They primarily focus on mobile devices, including personal digital assistants (PDAs), smartphones, and tablets with cellular-voice capabilities. They are intended for forensic examiners, response-team members handling a computer security incident, and organizational-security officials investigating employee-related incidents. They assume a working knowledge of traditional digital forensics methods.

Good Practice Guide for Computer-Based Electronic Evidence (ACPO – Association of Chief Police Officers, UK, 2012). The ACPO guideline Good Practice Guide for Computer-Based Electronic Evidence (2012) is primarily written for law-enforcement personnel who may need to deal with digital evidence. This guideline was first released in the late 1990s. Since then, there have been five iterations; some of the changes include an update in document title. The guide is essential reading for anyone involved in the field of digital forensics. The latest version has been updated to include more than just evidence from computers. It sets out some shared principles as follows:

Principle 1: no action taken by law-enforcement agencies, persons employed within those agencies, or their agents should change data which may subsequently be relied upon in court.

Principle 2: in circumstances where someone finds it necessary to access original data, they must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: an audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: the person in charge of the investigation has overall

[15] NIST - National Institute of Standards and Technology, USA.
[16] All guidelines are available on NIST website *nist.gov*.

responsibility for ensuring that the law and these principles are adhered to.

Particularly relevant for our topic here is § 7.1, addressing "Training and Education". The guidelines underline that training in digital investigation significantly differs from usual police training. Owing to the rapidly changing environment of technology, there is a requirement for the continuous but essential retention and updating of skills [17].

3.2. *Overview of guidelines, best practices, and soft regulation of DEVICES' Partners*

The analysis of *National reports* from DEVICES' Partners points out that international standards are the common reference base for professionals who work in digital forensics area. Some countries (or better, local law enforcements, agencies, or corporations) recognize them in local guidelines or soft rules, others do not.

In Spain [18], Law enforcement agents (LEA) in the criminal investigation and IT experts in private digital investigation (for companies, for labour proceedings, for internal investigations within the obligations set out in CCL compliance programmes, etc.) follow the same protocols, guidelines and standards, and mainly the UNE standards, [19] which are certified by AENOR (Asociación Española de Normalización y Certificación), very similar to ENFSI and ISO international standard. All forensic analysis requires a quality control of the acquisition of the data or samples that will be subject to forensic analysis, which implies the traceability of the chain of custody. Within the UNE standards, there is a detailed description on what are the processes and information to be checked at the examination stage and reflected in the report. The standard describes a list of data, actions and processes that should be included, although the list does not pretend to be exhaustive: the practioner can collect other data and perform other actions. Further the information provided by the relevant police unit (*policía científica*) to Project's partner National legal expert confirms that they prepare

[17] See below § 4.

[18] See *infra*, L. BACHMAIER WINTER, *The handling of digital evidence in Spain*, § 3.1.

[19] UNE is the acronym for Una Norma Española. UNE is in fact an ISO member standardisation body.

their reports and expert opinions following the already mentioned standards.

In Germany [20], at the federal level, a standard for digital investigations have been set with the Guidelines on "IT forensics" by German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik-BSI). The guidelines explain the use of IT forensics and are designed both as a basic guide, which allows a deeper understanding of the matter, and a reference work for the solution of practical problems. The guidelines are mainly addressed to system operators, i.e. the private corporations. However, the principles established within the guidelines and a part of their contents are relevant also for law enforcement investigations in State Criminal Police Offices. Furthermore, the BSI Guidelines are the main reference work for defence lawyers to challenge digital evidence. The various State Criminal Police Offices follow also standards based on guidelines adopted by the respective authorities (not public). Guidelines may also exist for the prosecution services, which again may differ widely among institutions.

In Italy [21], the main standard in use by LEA and by IT forensics Expert of private company are ISO standards and the other international guidelines mentioned in § 3.1. The Guardia di Finanza (or GdF) – a militarized law-enforcement agency under Italy's Economy and Finance Ministry responsible for dealing with financial crimes and smuggling – produce the circular n. 1/2018, an internal document released on the agency's website, [22] entitled «Operating Manual on Tax Evasion and Tax Fraud» and runs to 1,251 pages across four volumes. It has introduced the role of the "Computer Forensics and Data Analyst" (CFDA), a qualified practitioner responsible for identifying, collecting, and acquiring digital evidence. GdF provides specific training for first responders, this in keeping with international standards in digital forensics like ISO/IEC 27037 – Annex A.

Finally, the Dutch and the Luxemburgian [23] National Reports do

---

[20] See *infra*, S. GLESS-T. WAHL, *The handling of digital evidence in Germany*, § 3.2.2.

[21] See *infra*, L. BARTOLI-G. LASAGNI, *The handling of digital evidence in Italy*, § 2.

[22] Available at: *gdf.gov.it/documenti-e-pubblicazioni/circolari/circolare-1-2018-manuale-operativo-in-materia-di-contrasto-allevasione-e-alle-frodi-fisca*.

[23] See *infra*, K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxemburg*, § 1.

not recognize any specific (public) guidelines, or soft regulation or checklist of operation carrying out digital investigation.

3.3. *Guidelines on Digital Forensic Procedures for OLAF Staff*

The relevance of OLAF investigations in the European antifraud legal framework, coupled with OLAF's close cooperation with national authorities, makes the *Guidelines on Digital Forensic Procedures for OLAF Staff* (2016) the starting point for our study on the development of common standards for digital investigations in the EU and a term of comparison for all the involved Member States.

These guidelines, issued by the European Anti-Fraud Office (OLAF), are intended for use by its staff for the purpose of identification, acquisition, imaging, collection, analysis, and preservation of digital evidence. The aim of these Guidelines is to establish rules for conducting digital forensic operations in a manner that ensures the integrity of the evidence and of the chain of evidence, so that the evidence may be admissible in administrative, disciplinary, and judicial procedures.

These guidelines are modelled on ISO and ACPO technical standards, but taking a dual approach, at once technical and legal. In this respect the OLAF Guidelines stand apart from strictly technical standards, in virtue of their relating the technical requirements to the specific EU provisions in which they find their legal basis.

Due to the fact that these guidelines do not merely regulate the technical aspects of an IT investigation, OLAF's guidelines provide for the involvement of various professional staff: the first is the investigator, who is generally responsible for conducting the investigation and is familiar with the legal aspects; then, the involvement of the Digital Evidence Specialist (DES)[24] is also required, who is permanently integrated into OLAF's staff and has specific technical knowledge in the digital field. Further actors may be involved in the digital investigation, including the Legal Advice Unit, the consultant of the subject concerned by the investigation, and the (possible) national authorities involved. There is a clear separation of roles between the investigator and the expert who deals with the management of the IT data, which also means the setting

[24] Competence, skills, and role of the digital evidence specialist is examined in depth in § 4.

up of standard models for the discussion between the IT expert and the investigator.

The guidelines describe the sequence of operations that DES has to perform (see below, § 5), from the identification of potential digital evidence to the acquisition and transport to analysis activities, in accordance with the main international technical standards but discounting, compared to the latter, the lack of a certain technical precision. OLAF's operations are characterized by the drafting of specific Reports [25], i.e. summary documents containing the activities carried out relevant for the preparation of an accurate chain of custody. During investigations, a file (*case file*) is kept up to date through an information system called Case Management System, which tracks all the actions taken, the operators involved, and the information collected.

OLAF also has a forensic laboratory where forensic analysis activities take place (see below, § 6). The data collected by DES are transferred to the servers of the forensic laboratory and constitute the so-called "forensic work file", a file that is stored on the laboratory server for the time necessary to carry out the investigations.

For analysis, the investigator must submit a request to DES about the subject of the data search; he cannot require an indiscriminate apprehension of the data without stating a logical criterion to guide the choice of what to extract and what not.

DES will only provide those files that match the Investigator's query: all other data will be stored on the server and will not be visible to the Investigator. The step is of crucial importance, and from an organizational and technical point of view it represents a remarkable step forward, totally unparalleled, for example, by our system. DES shall also prepare a separate Report, called the "Digital Forensic Examination Report": it summarizes the results of all the operations carried out by DES, and lists all the information provided to the Investigator as a result of the analysis. The Digital Forensic Examination Report will also be included in the investigation file (CMS casefile).

In conclusion, the guidelines provide both for the compliance with specific technical measures and the provision of adequate facilities, as well as the guarantee of the legal requirements of proportionality.

On the technical side, however, we cannot fail to point out that

[25] Digital forensic Operation Report, Digital forensic examination report and the Operational Analysis Report.

although the OLAF guidelines are in compliance with the main technical reference standards, they lack technical precision and accuracy in several steps (see in this respect below, § 5). Technical integration is necessary because they do not tell us how DES should proceed in practice, nor which programs she should use, but this is left to other sources that are not mentioned. On the other hand, the aim of the guidelines is not to provide an accurate technical manual to inspire the work of DES (as EEG or ENSI guidelines) nor to indicate in general the technical objectives to be achieved (as the ISO/IEC standards): The aim is to show to the investigator the limits imposed by technology, and to DES the aims and safeguards that the law requires of his work. In short, the guidelines are that common knowledge hub that technicians and jurists should jointly know, without prejudice to the specific areas of specialist knowledge that each maintains.

4. *Digital forensics expert: roles and skills*

International technical standards, as well as many best practices developed nationally, insist on the importance of the technical personnel entrusted with digital forensics activities, devoting specific sections to defining roles and skills for such personnel. The required degree of technical skill is high, and it needs to be rounded out with an understanding of the applicable law if these technicians are to be able to properly handle digital evidence. Availability to advanced IT tools is not sufficient.

The ISO/IEC 27037 standard singles out two professional figures: the Digital Evidence First Responder (DEFR) – an «individual who is authorized, trained and qualified to act first at an incident scene for handling digital evidence» – and the Digital Evidence Specialist (DES), whose preparation is normally deeper and more specific in comparison with the DEFR, and who may «handle a wide range of technical issues». In addition to providing a specific table with the different skills required for different purposes (Annex A, ISO/IEC 27037), the standard underscores on multiple occasions that practitioners need to have technical as well as legal training. It is up to each jurisdiction to define the criteria required to qualify as a DEFR or a DES, and in these roles, practitioners need to demonstrate the ability to do investigative work (sec. 6.4 ISO/IEC 27037).

Even greater specificity can be found in the ENFSI guidelines,

according to which forensics experts mut be tested regularly to assess their ability; also laboratories are regulated more strictly and are periodically reviewed with regard to the quality of the tools and their adequacy.

ENFSI places emphasis on testing not only the theoretical understanding that practitioners have of the subject matter, but also their practical, hands-on abilities, which is done by giving them a simulated IT problem that they are then asked to solve.

Under the impulse of international standards, some local authorities have defined the role and skills of personnel authorized to work in digital investigations.

The ACPO guidelines highlight that the general principle for training in digital investigation differs significantly from the principle governing police training, in which connection it refers us to the *ACPO Good Practice and Advice Guide for Managers of e-Crime Investigation*.

In Italy, GdF Circular n. 1/2018 introduced a specific figure, qualified and trained in Computer Forensics and Data Analysis (CFDA). Professionals in this role are part of the staff of the judicial police, and they are uniquely qualified to acquire and analyze digital evidence, access the data of multinational groups that share data across branches. Owing to the peculiarities a tax audit involves at the initial phase, in which digital evidence is acquired and assessed, the GdF General Command has also launched courses designed to train first responders in line with the international standards covering the same subject matter.

The National reports by the Legal experts involved in DEVICES' Project show that if digital evidence is important for the case and special analytical expertise is necessary, technical operations and analysis may be carried out by special IT forensics Units within the LEA (e.g. the IT Forensics Unit of the *Policía científica* in Spain)[26]. Police officers who want to specialize in IT forensics may get additional training and qualifications. Training is refreshed and competences re-assessed periodically. In the Netherlands specifications on the training and the necessary expertise are given in a Ministerial Decision. Specific training courses and certifications

[26] See *infra*, L. BACHMAIER WINTER, *The handling of digital evidence in Spain*, §§ 2-3; L. BARTOLI-G. LASAGNI, *The handling of digital evidence in Italy*, §§ 2-3; S. GLESS-T. WAHL, *The handling of digital evidence in Germany*, § 3.1; K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxembourg*, § 2.

are required, for example, to identify system weaknesses and to modify codes in order to access automated systems (OSCP) and to collect data from wireless networks and circumvent the restrictions of these wireless networks (OSW). Members of the technical team must possess some legal knowledge as well. Although there is no strict separation between a DEFR and a DES, the police officer who is present at the "acquisition" phase (regularly a seizure of an object/of data) is usually different from the one who does a "technical analysis". In Germany and in the Netherlands the specialists at the special units are not handling the case, i.e. they do not make conclusions on the analyzed data. Their work is more or less limited to "data preparation", but the investigator handling the case has to choose what data need to be processed.

The OLAF Guidelines likewise provide that a digital investigation should always involve a professional specifically trained in digital forensics: this is the Digital Evidence Specialist (DES), a member in the OLAF staffs bringing «specialised technical expertise to perform digital forensic operations and to prepare related reports». The DES supports the investigator, who leads the investigation, is responsible for it, and knows all its legal implications. The OLAF Guidelines prohibit the investigator from interacting with anything that may prove useful as digital evidence, so much so that if anyone should come forward with a device on their own accord, the inspector may not accept it. Only the DES is authorised to do so and to copy the contents stored on a device; this in order to avoid tampering and to preserve the chain of custody. On the other hand, DESs may only be involved in the digital operations that fall within their purview, and they are neither acquainted with the broader investigative context nor are they to take any interest in the concrete case at hand. As we will see, this can prove limiting if the need should arise to accord priority to certain operations over others or to select the material that is relevant to the investigation.

It should at any rate be observed that because OLAF is equipped with its own investigative tools, it is fully compliant with the applicable technical standards, and it is also in a position to audit its own work.

It should further be underscored that the periodical quality check improves if carried out by internal personnel, that are part to the same administrative structure. This is an added value because OLAF does not need to rely on external experts and practitioners that may not have the same experience with the justice system and with OLAF's work.

Digital forensics operators in Italy are a broad and diverse group today, with professionals whose training varies considerably, and some may even not have the skills necessary for the role that is entrusted to them in a trial. The problem lies in the fact that there is no specific job qualification, making it possible for anyone to enter the job market even with a rudimentary understanding of the subject matter.

Here we report some data providing a snapshot of the Italian landscape in this regard. In light of the data provided by ONIF (the country's National Digital Forensics Observatory), 72,6% of legal forensics consultants hold a higher-education degree, and only 40,3% of those in this pool hold a degree in information technology or a related field. As concerns training and continuing professional development, 45% has not gone completed any specifically designed university programme, 78% has no professional certification in the field. More than that, the tools of continuing professional development in large part consist of a combination of textbooks, dedicated websites, mailing lists, and social networks, thereby stripping the training down to its bare minimum. As for professional bodies, 53% of digital forensics experts are unregistered, either because there is no such specific body or because there are no degrees through which to gain access to the profession, as is the case with some programmes offered under the old curriculum. The professional body with the highest number of registered members is the engineering society. Of all interviewees, 42% were registered with an association of expert witnesses for the court in whose jurisdiction they were working, but there were also cases in which someone might be registered with more than one court – an option that the law does not in theory allow. Only 30% of the professionals interviewed were covered by professional liability insurance – although, to be fair, there is no legal requirement to obtain such coverage [27].

The National reports of DEVICES' Legal experts show that in other countries some level of quality is ensured by professional associations or lists of computer forensic experts. In Spain, the expert evidence presented by the defendant or any other private party in the criminal procedure needs to be prepared by an IT expert with the relevant training and registered in the official association. These associations are public institutions guaranteeing the

[27] ONIF Survey 2015, *La professione del consulente tecnico informatico in Italia*, Rome, 28 April 2016, *onif.it*.

professional quality/degrees and standards, both technical as deontological [28]. In Germany, if a court or public prosecutor wants to appoint an expert (*Sachverständiger*), they can resort to lists of experts provided for by the Chamber of Industry and Commerce (IHK). A certification of the expertise is not required by law. Bigger firms have, however, a certification by the German Federal Office for Information Security (BSI) [29]. There is no register for digital forensics experts in Luxemburg, but the website of the Luxembourg Ministry of Justice maintains lists of experts assermentés, with a handful self-described as specialising in IT and/or cybercrime [30].

The best setting, however, seems to be the Dutch one: the Register of Court Experts (NRGD) guarantees and promotes the quality of the contribution that court experts make to the legal process, and it could well serve as an example to other legal systems. The NRGD was the first register of forensic experts, established under the Experts in Criminal Cases Act of 2010 and managed by an independent Board of Court Experts. Although anyone can work as forensic expert even if they are not registered in NGRD, the registration gives experts recognition.

From the foregoing analysis of existing standards and experiences we can distil the following essential characteristics that anyone should embody in the role of forensic expert:

a capacity to do the job in a manner that is independent, impartial, conscientious, competent, and trustworthy;

proper and transparent conduct in relating to all the parties who have a stake in the case at hand;

an ability to communicate competently with all the other parties involved in the proceedings in a professional role;

confidentiality in using the data and information that one gains access to over the course of an investigation, in keeping with all applicable laws;

constantly staying up to date by completing training programs, attending conferences and seminars, and reading the literature (books, papers, journal articles, blogs);

using tools and techniques which the scientific community recognizes as suited to the task of acquiring digital evidence and guaranteeing its integrity, in compliance with all applicable laws;

---

[28] See L. BACHMAIER WINTER, *National Report: Spain*, § 4.

[29] See *infra*, S. GLESS-T. WAHL, *National Report: Germany*, § 3.1.

[30] See *infra*, K. LIGETI-G. ROBINSON, *National Report: Luxemburg*, § 2.

using proven scientific methods, or other methods whose reliability can be verified, when analyzing or interpreting data (e.g., verifying results by using different methods or using accepted datasets when establishing correlations between different data points), all in keeping with applicable laws;

applying the methods that international guidelines set out for the most common activities (e.g., search and seizure, transfer of devices, data acquisition) and for best practices concerning all activities in which it proves impossible to guarantee that evidence will not be altered (e.g., data captured from smartphones or from systems with a running task), all in compliance with the law;

the ability to properly handle situations for which there are no well-established practices and techniques (e.g., when dealing with data stored on remote devices, or on an Internet server, or on non-standard devices), an ability that will have to be maintained by hands-on experience and by continuously keeping up to date on the latest developments in the field;

the ability to provide clients with verifiable reports (whether oral or written) fully and clearly explaining the basis for the task that needs to be assigned, as well as any other aspect of one's personal experience and background which may be pertinent to the same task.

Finally, it is worth mentioning the question of the digital forensic expert's relation to service providers: the seizure of data from the latter bypasses almost all of the technical and methodological guarantees set out in international standards, for it is entirely up to the service provider to guarantee the quality of the data it collects and hands over to the authorities.

5. *Main steps in digital investigations*

On the basis of the standards that have been considered in this research project, we can identify the main steps of the digital investigation process.

Digital investigations are defined as the «use of scientifically derived and proven methods towards the identification, collection, transportation, storage, analysis, interpretation, presentation, distribution, return, and/or destruction of digital evidence derived from digital sources, while [...] preserving digital evidence, and maintaining the chain of custody» (ISO/IEC 27043). It comprises several steps and two main phases (Figure 1).

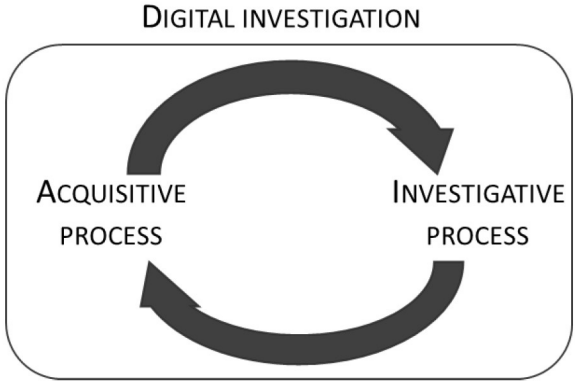

Figure 1 – Digital investigation process

Its two mains phases consist of the processes of (Phase one) acquiring data and (Phase two) using it for an investigation. The output of the acquisition process is input for the investigative process. Sometimes, the output of investigative process can suggest other activities that require a new acquisitive process. And so on, until the end of the investigation.

"Phase one" is the Digital Evidence [initial] Handling Process, which includes identification, collection, acquisition, and preservation of potential digital evidence. As the name suggests, the acquisition process is the process through which data is acquired or captured. In the OLAF guidelines, this is referred to as the "digital forensics operation", which the Digital Evidence Specialist (DES) carries out using forensic equipment and software tools. Its aim is to locate, identify, collect, and/or acquire and preserve any and all data which may be relevant to an investigation, and which may be used as evidence in administrative, disciplinary, or judicial procedures.

"Phase two", investigative process (which the OLAF guidelines call "operation analysis"), is concerned with analyzing the evidence, interpreting the results of the analysis, reporting the results of the interpretation, and presenting these results in a court of law, with the use of specific analytical tools and techniques by which to establish links between pieces of information.

Each phase is composed of steps (Figure 2) that must be sequentially followed in each digital investigation.

However, there are some precise factors that require a case-by-case assessment of the operations to be performed. These factors include the following: the digital device is turned on or off; the system cannot be removed because it provides a critical service or

because it is in the network and therefore cannot be physically reached; legal reasons why the digital device may not be acquired.

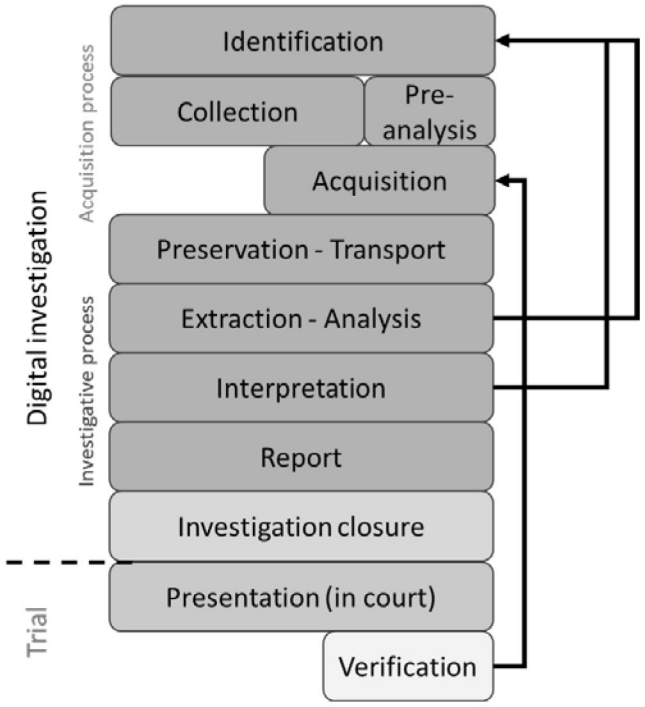

Figure 2 – Main phases of a digital investigation

The acquisition process comprises five main steps, in which the digital evidence is (1) identified, (2) collected and sometimes preliminarily analyzed, (3) acquired, (4) preserved, and (5) transported.

A point of discussion about this process is the one related to its repeatability: all of these steps are particularly critical because any mishandled operation in this phase could cause data to be altered or lost along the way, thereby making it impossible to verify or repeat the results of the investigation.

All the technical standards require that a complete and accurate record must be kept of each operation, even by photographing or filming the activity.

In terms of protection of the chain of custody and documentation of the activities, it is also necessary to highlight the EEG guidelines that require the documentation of the scene on which the IT technicians operate, as well as photos and videos to trace the state of

computer systems at the access. If possible, a 360° recording of the environment can be useful.

By that, all the activities, movements, and choices operated by the technicians are implicitly documented, so this substantial documentation can well support the accuracy of the acquisition process.

In the same direction, the ISO/IEC standards suggest documenting by any means possible both the status of the places prior to the operations and the procedures for completing the operations [31]. Also, the ENISA guidelines clearly indicate the obligation to register and document the performance of the activities [32].

The first activity, as mentioned, consists in identifying potential digital evidence. The Digital Evidence First Responder (DEFR) or Digital Evidence Specialist (DES) should search for items that may contain digital data relevant to the incident: computers, devices (scanner, printer, GPS tool), storage media, and networked devices [33].

This is not a simple task: physical devices or virtual spaces must be identified (as cloud-computing repositories). The devices can also be very small. The DEFR needs to also look for power cables, SIM cards, etc. If the DEFR does not identify the data correctly, it may thereafter never be recoverable.

In identifying data (step 1), the DEFR should establish priorities in the collection or acquisition of potential digital evidence, this depending on how volatile the data is and on its relevance to the investigation. In this case, however, who is carrying out IT activities must grasp the reason why the evidence is being collect or acquired. The OLAF Guidelines make it a requirement to exclude all data that is not relevant to the investigation.

The next step (2) is to decide whether to collect the digital devices or acquire the digital data. Collection is the process of removing electronic devices from their location and taking them to a forensics laboratory in order to subsequently make a forensic copy. The entire process needs to be documented from packaging to transportation.

Acquisition (step 3) involves creating a copy of data and

---

[31] ISO IEC 27037 par. 6.2.1; par. 7.2.1.2.

[32] Par. 2.1.2, *Digital forensics Handbook, Document for teachers* (ENISA), September 2013, available at *enisa.europa.eu*.

[33] For a practical guide on technical aspects see, among all, D.R. HAYES, *A Practical Guide to Digital Forensics Investigations*, 2nd ed., Pearson, 2021; B. NELSON-A. PHILIPS-C. STEUART, *Guide to computer forensics and investigations*, 6th ed., Cengage, 2018.

documenting the activities performed. The DES can make an image copy or clone [34] using dedicated software [35] or dedicated hardware [36]. All best practices require at least two copies in order to ensure that no physical damage is done to hard drives or logical damage to data.

Best practices require verifiable copies using hash functions of all bits contained within each media item. The DEFR should use the most appropriate method.

Returning on the technical gaps in the OLAF guidelines, it is worth pointing out that they do not indicate an order of priority for the acquisition of digital media, even if all international standards do so. For example, RAM must be acquired before non-volatile data: this is a common rule, shared by any standard as well as by the scientific community.

The ISO/IEC 27037 standard dedicates an entire paragraph to the topic of acquisition priorities of digital evidence.

The EEG guidelines do not directly express priority rules, but they clearly favour the prioritization of the volatile data, since they impose not to turn off a turned-on computer.

Moreover, OLAF guidelines do not suggest the usage of the least invasive software for the acquisitions [37].

The main criteria to collect or acquire data, dictated by international standards, include: the volatility of potential digital evidence; encryption applied to an entire disk or volume where passphrases or keys may reside as volatile data in RAM memory or in external tokens; legal requirements; resources such as storage size, availability of personnel, and time limits; the ability to seize a device.

---

[34] The bit-stream copy by clone is a mechanical copying of the single bits to a blank target support, creating a perfect clone of the source. In the imaging copy process, a file (or a set of files) is created and it represents the exact sequence of bit, useful to reconstruct the source. The main pros of the image are the possibility of making multiple copies on the same target, as well as the usage of a compression algorithm that reduces the disk usage.

[35] This kind of software includes dd Linux command or commercial products like FTK Imager, Encase, and Xways.

[36] Complete acquisition in over a short period can be accomplished by forensic duplicators like Tableau TD3 and Logicube Falcon. These are fully featured, fully forensic duplicators that offer an ideal combination of ease of use, reliability, and ultra-fast forensic imaging of hard disks and solid-state drives.

[37] The EEG guidelines demand (§ 3.4.2) the usage of the less invasive software, suggesting one instead of others, because of the less memory requirement for the execution.

In this context, a pre-analysis will often be carried out in order to identify the data that may be relevant.

During pre-analysis, some operations may damage the original data, and the verification process cannot be performed. That is made up for by photographically documenting the activity and providing a basis for each choice. The practitioner should be able to explain the effects of any actions taken.

Generally, technical standards require that all data stored on all devices be integrally captured (by making a copy of the entire image), for it is only by looking at how the single data point is consistent with the rest of its data environment that it may be determined whether the data has been altered. In some circumstances, partial or selective copies of the data are allowed, as for example when the quantity of the data to be captured makes it impracticable to capture the entire image on a hard disk. However, where this latter method is used, investigators need to be sure that all relevant data has been captured. In short, the rule is: seize everything, capture the data partially only when technical constraints do not allow for the complete collection. At the same time, the law requires that the personal sphere of those under investigation be encroached upon as little as possible, while refraining from capturing whatever data is not strictly necessary to establish the facts.

We should point out that the OLAF Guidelines do not permit the collection of physical devices, so what the DESs should do instead is only make copies of the data that is stored on them. Moreover, DES can analyze in preview data to decide if she must acquire all data, some data or nothing, according to the investigation requirements.

The issues related to the balance between the principle of proportionality and technical requirements for completeness are the subject of the next section.

The last two phases (step 4 and step 5) in the acquisition process concern the methods of transporting and storing the devices and the copies acquired, as well as maintaining and safeguarding the integrity and original condition of potential digital evidence, so as to be able finally to analyze the evidence.

The OLAF Guidelines require data to be stored in the CSM case management system in the forensic laboratory. This repository must follow robust security policies.

We can conclude that all the operations in the acquisition process are critical and potentially unrepeatable.

The investigative process starts from the acquired material and is aimed at analyzing the evidence and interpreting and presenting the

results. Each operation can therefore be repeated starting from the forensic copy.

A close collaboration is required between the skilled technician and the investigator who has a full and accurate grasp of scope of the investigation.

In the extraction and analysis phase, the digital evidence extracted from the source equipment is identified and evaluated. Specialized software is often used to discover digital data, as the volume of data that needs to be analyzed can be vast. Here we have a first point to discuss. Should tools used be validated? How can we really verify result if forensic software is not open source? [38].

Interpretation is the step where an investigator infers information from facts. The aim is to derive meaning from digital evidence, evaluating it in the context of circumstances. For example, a file being contained in a device is a fact. If the file was saved with a user-specified filename, it would be reasonable to infer that the user was deliberate in making that choice. The goal is to explain the facts detected over the course of the analysis.

In this phase there are circumstances that may make it necessary to go back to the initial step, where the data was identified. For example, if an analysis reveals that some of the data are missing from the system being analyzed but may be found elsewhere, then the entire procedure will have to be repeated on another device [39].

In our opinion it is particularly difficult at this stage to separate technical skills from investigative ones: both are important and need to be integrated.

Finally, the two final steps, reporting and presentation, are going to lead to the closing of the investigation.

---

[38] The issue on the usage of open-source software in digital forensics, especially in acquisition and analysis phases, is a well-known topic in the literature. In fact, if software whose source code is secret is used, a scholar has observed that «there seems to be a deficit of protection for the defence, since the latter, unable to check the correctness of the program's operation, may not be able to verify the activities carried out by investigators. Also, for this reason, exclusive use of open-source programs is desirable, with countless advantages for all procedural actors, including the possibility of verifying the activities carried out on the data even after years, given the easy availability of the software itself»: L. MARAFIOTI, *Digital evidence e processo penale*, in *Cass. pen.*, 2011, p. 4509. See also E. HUEBNER-S. ZANERO, *Open Source Software for Digital Forensics*, Springer, New York, 2010.

[39] Consider a scenario in which an email is found that brings into the conversation a third party who may in turn come under investigation, along with all the devices held by this person.

In particular, the reporting should contain all the documentation acquired or produced during analysis. It needs to contain scientific explanations in order to make possible to verify all the assumptions made during the investigation, moreover it must specify the tools and method used. The report should be written in a clear, concise, and unambiguous manner. The report is also the basis of the presentation, whose main purpose is to offer a live demonstration of the results obtained.

In the final verification phase, an independent expert or one of the other authorized parties must be able to inspect the activities carried out by the DEFR and the DES: all the operations they have gone through need to have been documented, so as to make it possible to determine whether all the appropriate methods, techniques, and scientific procedures have been used. One of the tools that has traditionally been used to reconstruct the way these technicians have worked in arriving at a given result – and so a tool that makes it possible to review the work done on the data, and to do so even at a distance of several years – is an open source software. But numerous competing proprietary software products have since come onto the market: we have reached a point where the key element in any verification lies in the ability to reproduce the same results by different means or methods. The OLAF Guidelines do not comment on this point, but generally a verification can make it necessary to backtrack all the way to the acquisition phase.

6. *The digital forensics lab: tools, facilities, and requirements*

It is no less important to digital investigations that *specialized labs* be set up where digital evidence can be managed. This includes the ability to create *virtual environments* which are remote from the places where investigations are conducted, and which also make it possible to automate certain phases in the forensic process of managing, storing, analyzing, and interpreting data. These labs can store large amounts of data, effect secure communications, carry out authentications on several levels, and check access based on one's role. And they are also equipped with forensic tools for managing cases, enable multiple virtual machines to share the same hardware. A centralized digital forensics laboratory provides investigators with the advanced tools they need for their work, making the best use of resources and skills, and bringing down the cost of forensic investigations.

First labs were created about a decade ago, but they came up against the limitations of technology and the challenges faced in getting the courts to admit evidence that had not been gathered in any of the traditional ways. But then came the surge in cybercrime. In response, an international legal framework was developed that could act as a support, and governments began to call for a more effective use of forensic science. It is against that background that many new initiatives followed and flourished, with the development of shared platforms and virtual labs in various sectors of forensic science [40], and with the adoption of methods that can be applied on a large scale.

Forensic investigations in real time can bring multiple advantages, and the uptake of this approach has the potential to make the criminal justice system much more effective. Consider live forensics, for example, where a power outage can cause the loss of volatile memory containing critical data, especially in cases involving encrypted devices (using encryption passwords), extensive memories, or the use of anti-forensics techniques [41].

However, the use of forensic tools of this kind also raises some issues: best practices require to continually test the hardware and software tools used in examinations, and most examiners unfortunately lack the skills necessary to validate them.

Even so, once these problems are overcome under a proper system of governance, the growth of cloud and virtual environments suggests that digital forensics labs will in the future be increasingly centralized and not constrained within geographic boundaries.

A digital forensics lab must have the following features: a surveillance system, to monitor the premises for unauthorized access and break-ins; access control; a fire-control system; reinforced windows, doors, and walls to prevent break-ins; a sufficient number power sockets, fuses, breakers, and current load; anti-static flooring; a radio-jamming system; a cooling system, because overheating can lead to loss of data and may damage hardware; off-site data storage backup, so that in the event of disaster, the offsite storage can be

[40] From 2012 to 2017, the European Forensic Genetics Network of Excellence (EUROFORGEN-NoE) built a virtual forensic genetics lab with partners from nine countries (scientists, scholars, law enforcement officials, and members of the judiciary) who collaborate in criminal investigations involving issues of privacy and the protection of minors.

[41] Anti-forensics is a set of techniques that can be used to conceal digital evidence and thus thwart the work of investigators trying to find it.

used to gain access to critical data; and archival long-term data storage. A digital forensics lab also needs some common facilities, like a reception area, one or more evidence-storage rooms, an evidence-processing area and laboratory, a personal space, and a briefing space[42]. Obviously, a digital forensics laboratory must be technologically equipped with several kinds of hardware and software for forensics acquisition and analysis, along with mobile kits for work outside the lab itself.

As said, OLAF has its own forensic laboratory. The laboratory is an isolated and protected space, the internal network is isolated from the Internet and Intranet. Access to the laboratory is limited only to specified people and after identification, and the entrance is under video surveillance.

OLAF has a lot of digital forensics hardware and software, and trained operators, so it does not need to rely on third parties for the performance of its activities of acquisition, analysis, and reporting. That is perfectly coherent with the international scientific recommendations, which insist on both the importance of the staff and the instruments.

The COVID-19 pandemic has further highlighted the importance of smart working. Even if most DESs are already equipped with laptops that they can bring into the field, the transition to smart working is not so easy. It is true that most of the analytical work can be done remotely, but digital forensics laboratories need policies and standard operating procedures to govern what DES can and cannot do from home. They include: ensuring employees harden their home networks, updating router firmware and changing Wi-Fi passwords regularly; having a virtual private network (VPN) available, in order to secure data in transit. Moreover, no original device must leave the lab space, but only forensic copies in encrypted devices, tracking everything and returning them; workstations must be encrypted and locked when DES is not working, to avoid access to sensitive data by people in the home environment. Another necessary requirement is the strong coordination among forensic experts and lab managers, who are in charge of ensuring the respect of the policies (for example, new purchases or replacements for broken technology).

---

[42] See the INTERPOL Global Guidelines for Digital Forensics Laboratories, available at *interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf*.

Anyway, some operations can only be performed in a lab, like identification and acquisition phases. So, to ensure that the lab work is being done without unnecessarily risking the examiners' safety, the team must identify the member who can go to the lab during a targeted time frame on a given day each week. That examiner must work from a list of needs. All laboratories should make these rules on their own.

7. *The big amount of data: technical requirements versus privacy*

Modern investigative activities are increasingly dependent on the interpretation of huge quantities of digital data of various kinds. This makes it very time-consuming to extract and analyze data, with great computing power, and moreover it makes the process extremely sensitive, owing to the risk that the confidentiality or secrecy of the information being analyzed may be compromised. This brings a dual aspect into the picture. The first one is tied to the need to ensure that digital investigations are effective and efficient, as well as that the necessary data is acquired in its entirety. The second one is instead tied to the right to dignity in what concerns one's digital life, a consideration that is moreover inseparable from the confidentiality or secrecy of all the information that coexists in virtual spaces. The issue therefore arises as to how to delimit the scope of an investigation, and in which phases, in the effort to find all the information that is relevant to the case at hand, all the while excluding all private and irrelevant data from the scope of the analysis and interpretation.

This issue is particularly relevant specifically in connection with the antifraud effort. As anticipated in Section 3.2, the OLAF Guidelines seem to veer away from the benchmark technical standards, at least in part, by taking a more considered approach. OLAF's general rule is that an investigation needs to proceed with a complete forensic acquisition of data, as the technical standards require, but that, if possible, the DES and the investigator need to have it in their discretion to display a preview of the data so as to assess whether to only acquire part of it. The 2013 *Guidelines on Investigation Procedures for OLAF Staff* a sort of general operating manual, also require at Article 15 that the digital forensic examination and analysis of the data collected in a digital forensic investigation be *limited to extracting data that is necessary and relevant to the same investigation* (§ 15.3). As explained *supra*, § 3.3, the DES has to extract and hand over to the investigator only the data that are pertinent to the

investigation. Indeed, in order to extract data from the forensics lab, the investigator must submit a written request to the DES specifying the exact object of the data search, meaning that the investigator cannot ask for a blanket acquisition of data, but must define a logical criterion in light of which to decide what to extract and what to leave out. The DES will produce in read-only format exclusively those files that meet the search criteria specified by the investigator: all other files will remain in the lab.

This last example, too, underscores the need to set out clear limits to the admissibility into evidence of forensic copies; if the entire collection enters the case file, the parties could consult it and gain access to data that are not pertinent to the legal proceedings. Note that in making a forensic copy, the aim is to make sure that the data being copied is not altered: it is not to produce the copy itself as the result of an investigation.

This is a critical point, and it means that the forensic copy is to be understood as a tool supporting the work of the digital forensic expert.

It is clear that when the parties are not involved in the fact-finding process, a forensic copy also becomes the probative element from which to start in carrying out that process. But how to proceed when the parties have the option of taking part in the process?

A forensic copy contains a huge quantity of data, and most of it will often bear no relevance to the technical investigation.

Take any case of any kind (child pornography, fake invoicing, intellectual property infringements): the data that are relevant to the fact in dispute, no matter what their quantity is, will only amount to a fraction of the data stored on the digital device being examined.

The figure below (n. 3) illustrates the entire process that runs from the acquisition of data to the analysis and selection of pertinent files.

Figure 3 – The process of identification of relevant files

Along with the relevant data, there will be a huge quantity of data that the parties concerned – the owner of the device, its user, or third parties whose data may be stored in it – would reasonably expect not to be captured, disclosed or taken into account: this includes projects, patents pending, family albums, and intimate messages, among other examples.

However, the need for confidentiality must be balanced against the need to preserve the integrity of the data for which a forensic copy is required.

In reality, the forensic copying of data is an operation that is instrumental to the subsequent data-analysis phase, in which it will be necessary to select pertinent data.

This brings into focus an interesting method by which to meet both of these two competing needs, and it rests on the idea of an impartial technician (a court-appointed or party-appointed expert) entrusted with reviewing all the data so as to select the pertinent data and leave out all data that is not pertinent.

The culling of such data can be done in an extremely granular way, looking at the files one by one, often with a great expenditure of resources (both time and money), or it can be done by applying objective selection criteria, which may also be used in combination. This can be done, for example, by searching for files having identical hashes or filtering a search by date, keyword, filetype, or interlocutor [43].

If these data-analysis activities are carried out adversarially, the parties involved who are bound by an oath of confidentiality would be in a position to assess the pertinence of the data that has been captured, requesting that only the data that are strictly necessary be introduced as evidence, and that all other data be "destroyed" [44].

---

[43] A variety of filtering tools are available. These include open-source tools like Autopsy, the search tools built into operating systems, and more advanced proprietary analytics tools like Xways, FTK, Nuix or Intella.

[44] This selection must take place in the presence of both parties, in a closed hearing, out of the public eye, otherwise it would lose its effectiveness. The immediate destruction of not relevant data to protect confidentiality may appear risky (errors or omissions would be impossible to remedy, and changes in the prosecution's line could be hard to face without the original set of data). However, it has nothing different from the excerpt of an intercepted conversation, or from the restitution of previously seized items (a car, a flat...). A compromise could be the maintenance of a sort of "safe storage of the forensic copy", under lock and key, to be able to access the entire collection in case it should be necessary.

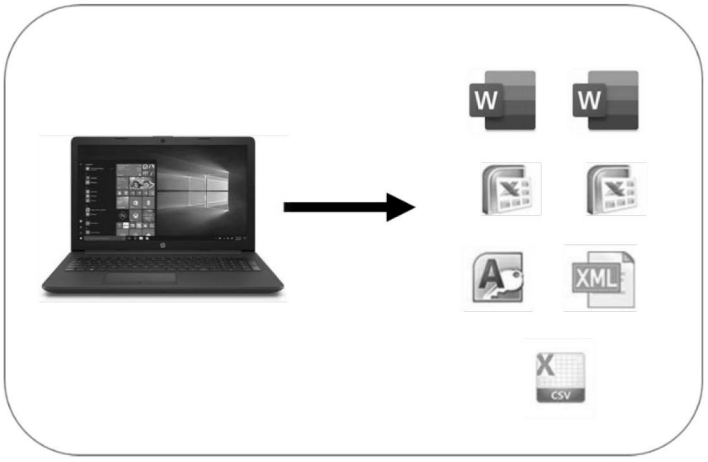

Figure 4 – Exemplification of the selection of data that is limited to what is relevant

The figure above (n. 4) illustrates the result of a selection process omitting all the intermediate passages, including the making of a forensic copy that would not be presented at trial because all concerned parties were able to contribute to the adversarial selection of the relevant files.

It is worth noting that, in Italy, this model is already in wide use in some kind of cases, for instance: in proceedings involving copyright infringement, where it would be unreasonable to grant access to the counterpart's industrial secrets. We are also beginning to see the first cases of this model being used in criminal proceedings in Italy in which a prosecutor, pursuant to Article 360 of the Code of Criminal Procedure [45], tasks an expert with performing a non-repeatable technical ascertainment, and is asked by the defence – as it is its right – to proceed with a special evidentiary hearing (*incidente probatorio*). At that point it will be up to the judge of the evidentiary hearing to appoint an impartial expert witness to task with analyzing the data, always respecting the fundamental tenets of an adversarial procedure. The forensic copy is thus only an intermediate working tool that gets destroyed once the data is selected as evidence, thereby requiring greater precision in describing the data that have survived the process of selection.

[45] In this case, the defence can only assist and express observations but has no right to veto respect the activity of the expert witness.

Under the proposed method, the prosecutor should perform a non-repeatable ascertainment (except if the "safe storage of the forensic copy" is implemented) enabling the counterpart to actively participate in the selection process. This choice clearly means that those findings need to be disclosed and that is why the selection is fundamental to protect the privacy.

It is furthermore evident that this way of selecting the evidence requires the investigating expert to have a proper appreciation of the criteria under which the proceedings are to be carried forward, which not infrequently places experts in a position where they have to make decisions about the parties' conflicting claims (with one party asserting that the data is relevant to the case, the other denying such a claim). Nor should it be discounted, finally, that the process of joint selection of the evidence can significantly delay the process, beyond what it would take for an independent analysis of the data, which can be verified and challenged at a later stage by re-examining the forensic copy.

8. *Conclusions: recommendation and perspective*

Taking account of the inherent features of digital evidence, we have used the methodological approach of digital forensics to outline a minimal set of activities for the proper handling of digital evidence within the framework of the technical and methodological standards that serve as a benchmark in the sector. We have further analyzed the roles and qualifications of the professional figures entrusted with digital investigations, identifying a skillset for the digital forensic expert. In our opinion it is particularly difficult to separate technical skills from investigative ones, indeed both are important and need to be integrated.

What emerges from the research is the pressing need to train and certify those to whom these activities are entrusted, and to invest in the infrastructure and research needed to support them. This includes building specialized labs for handling digital findings, and we described the characteristics these labs should have, even considering the experience of COVID-19 and the perspective of smart working, that need to be considered in the OLAF guidelines [46]. Furthermore, we suggest other additions in the next

[46] In the guidelines, only a physical isolated and protected laboratory is foreseen.

version of OLAF guidelines: for instance, they would be substantially improved by emphasizing the issue of the reproducibility of the analysis, which means that the results should be reached by different means or methods that those employed in the first place. The Guidelines could also be more helpful if they could guide the expert through the acquisition process, in particular, by establishing priorities. Moreover, they could be updated in order to respond to the technological progress, in particular reference to the cloud solutions (virtual machines, cloud storage...), which radically change the approach in the phases of identification, collection and acquisition. The Guidelines could also establish significant reliability thresholds by pay more attention to verifiable reports (both oral and written) that explain fully and clearly what was done and why, justifying the choice, especially when it comes to the information disclosed by service providers (included cloud service providers), since it is entirely up to the service provider to guarantee the quality of data collected and delivered to the authorities.

Finally, it was pointed out that the selection of data that may be relevant to the investigation – where the national legal system allows it – makes it necessary to take antifraud measures so as to properly address the typical problem of unsecured data stored on digital devices and virtual spaces. Considering the continuous increase of memories and the amount of data produced by citizens (also extraneous to the case), this is a proposal to safeguard personal data that are unrelated to the investigation. This is also an important requirement in Guidelines on Investigation Procedures for OLAF Staff at § 15.3. In this connection, we propose an alternative selection method by which to balance the competing desiderata calling for investigations at once complete and confidential. This highlights the need to achieve synergy between the different partiests and processes involved in an investigation: this is key to ensuring due process and to obtaining scientifically valid and highly reliable factual finding.