**Best Practices Report**

<table>
<thead>
<tr>
<th>Date</th>
<th>23.05.2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dissemination Level</td>
<td>Public</td>
</tr>
<tr>
<td>Responsible partner</td>
<td>Universitat Politècnica de Catalunya</td>
</tr>
<tr>
<td>Editors</td>
<td>Universitat Politècnica de Catalunya, Institut Jožef Stefan</td>
</tr>
<tr>
<td>Authors</td>
<td>Universitat Politècnica de Catalunya, Vrije Universiteit Brussel</td>
</tr>
</tbody>
</table>
Document history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Contributors</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.4</td>
<td>15.04.2018</td>
<td>Pablo López-Aguilar Beltrán</td>
<td>First final draft</td>
</tr>
<tr>
<td>0.5</td>
<td>22.04.2018</td>
<td>Pablo López-Aguilar Beltrán</td>
<td>Second final draft</td>
</tr>
<tr>
<td>0.6</td>
<td>26.04.2018</td>
<td>Pablo López-Aguilar Beltrán</td>
<td>Third final draft</td>
</tr>
<tr>
<td>0.7</td>
<td>28.04.2018</td>
<td>Manel Medina, Pablo López-Aguilar Beltrán</td>
<td>Fourth final draft</td>
</tr>
<tr>
<td>0.8</td>
<td>10.05.2018</td>
<td>Manel Medina, Pablo López-Aguilar Beltrán</td>
<td>Fifth final draft</td>
</tr>
<tr>
<td>0.9</td>
<td>20.05.2018</td>
<td>Manel Medina, Pablo López-Aguilar Beltrán,</td>
<td>Sixth final draft</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lewin Rexin, Sergi Vazquez Maymir, Carlota Urruela</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>23.05.2018</td>
<td>Borka Jerman Blažič, Tomaž Klobučar, Pablo López-Aguilar Beltrán</td>
<td>Final version</td>
</tr>
</tbody>
</table>

Legal Notices

The information in this document is subject to change without notice.

The Members of the LIVE_FOR Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the LIVE_FOR Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

LIVE_FOR is a project funded by the European Union’s Justice Programme (2014-2020). This report reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Contents

LIST OF FIGURES .................................................................................................................. 7
LIST OF ABBREVIATIONS ................................................................................................. 8
EXECUTIVE SUMMARY .................................................................................................. 10

1 INTRODUCTION ............................................................................................................. 11

2 BASIC CONCEPTS ......................................................................................................... 12
  2.1 How does the Internet work? ..................................................................................... 12
  2.2 User / server definition ............................................................................................. 12
  2.2.1 User ..................................................................................................................... 12
  2.2.2 Server .................................................................................................................. 12
  2.3 Information exchange (addresses / ports / protocols) ............................................. 13
  2.3.1 Addresses .......................................................................................................... 13
  2.3.2 Ports .................................................................................................................... 14
  2.3.3 Protocols ............................................................................................................ 14
  2.4 Encryption basic concepts ....................................................................................... 15
  2.4.1 Generic Encryption algorithms ......................................................................... 16
  2.4.2 Hash definition .................................................................................................... 16
  2.5 Log definition and properties .................................................................................. 17
  2.5.1 What is a log? ..................................................................................................... 17
  2.5.2 Log properties .................................................................................................... 19
  2.5.3 Log uses .............................................................................................................. 20
  2.6 Metadata .................................................................................................................. 21
  2.6.1 Types of metadata ............................................................................................... 21
  2.7 Digital evidence ....................................................................................................... 21
  2.7.1 Definition of digital evidence ............................................................................ 21
  2.7.2 Evidence preservation ......................................................................................... 22

3 DIGITAL FORENSICS TECHNIQUES ........................................................................... 23
  3.1 Computer forensics principles ................................................................................. 23
  3.1.1 Forensic readiness ............................................................................................... 23
  3.1.2 Forensic timeline ................................................................................................. 23
  3.2 Legal requirements .................................................................................................. 23
  3.3 Dead acquisition analysis ....................................................................................... 24
  3.3.1 Positive aspects of dead acquisition analysis ..................................................... 25
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.2 Limitations of dead acquisition analysis</td>
<td>25</td>
</tr>
<tr>
<td>3.4 Live forensics</td>
<td>25</td>
</tr>
<tr>
<td>3.4.1 Smartphone live data analysis</td>
<td>26</td>
</tr>
<tr>
<td>3.5 Volatile data definition</td>
<td>26</td>
</tr>
<tr>
<td>3.5.1 Memory dump analysis</td>
<td>27</td>
</tr>
<tr>
<td>4 ADVANCED DIGITAL FORENSICS PROCEDURES AND TECHNIQUES</td>
<td>28</td>
</tr>
<tr>
<td>4.1 Reverse engineering</td>
<td>28</td>
</tr>
<tr>
<td>4.2 Computer forensics tools</td>
<td>29</td>
</tr>
<tr>
<td>4.2.1 Open source tools</td>
<td>29</td>
</tr>
<tr>
<td>4.2.2 Commercial tools</td>
<td>29</td>
</tr>
<tr>
<td>5 CLOUD ENVIRONMENT AND CYBERCRIME</td>
<td>31</td>
</tr>
<tr>
<td>5.1.1 Risk of cloud computing</td>
<td>32</td>
</tr>
<tr>
<td>5.1.2 Benefits of cloud computing</td>
<td>32</td>
</tr>
<tr>
<td>5.2 Cloud services</td>
<td>33</td>
</tr>
<tr>
<td>5.2.1 Cloud software as a service - SaaS</td>
<td>34</td>
</tr>
<tr>
<td>5.2.2 Cloud platform as a service – PaaS</td>
<td>34</td>
</tr>
<tr>
<td>5.2.3 Cloud infrastructure as a service – IaaS</td>
<td>34</td>
</tr>
<tr>
<td>5.3 Cloud management technologies</td>
<td>34</td>
</tr>
<tr>
<td>5.3.1 Virtualization</td>
<td>35</td>
</tr>
<tr>
<td>6 CLOUD FORENSICS PRACTICAL APPROACHES</td>
<td>36</td>
</tr>
<tr>
<td>6.1 Introduction</td>
<td>36</td>
</tr>
<tr>
<td>6.2 Cloud SaaS forensics</td>
<td>36</td>
</tr>
<tr>
<td>6.2.1 Client-based cloud SaaS forensics</td>
<td>36</td>
</tr>
<tr>
<td>6.2.2 API-based forensic cloud</td>
<td>37</td>
</tr>
<tr>
<td>6.2.3 Forensics as a service</td>
<td>38</td>
</tr>
<tr>
<td>6.3 Cloud IaaS forensics</td>
<td>38</td>
</tr>
<tr>
<td>6.3.1 Margarita Shotgun</td>
<td>39</td>
</tr>
<tr>
<td>6.3.2 Aws-IR</td>
<td>39</td>
</tr>
<tr>
<td>6.4 Cloud PaaS forensics</td>
<td>39</td>
</tr>
<tr>
<td>6.5 Practical use case</td>
<td>39</td>
</tr>
<tr>
<td>6.5.1 Scenario</td>
<td>39</td>
</tr>
<tr>
<td>6.5.2 Considerations</td>
<td>40</td>
</tr>
<tr>
<td>6.5.3 Analysis</td>
<td>41</td>
</tr>
<tr>
<td>7 COLLECTING CROSS BORDER EVIDENCE</td>
<td>42</td>
</tr>
</tbody>
</table>
7.1 Introduction ..................................................................................................................... 42
7.2 The legal framework of e-evidence ................................................................................ 42
7.3 Cross border evidence tools in EU members ............................................................... 44
7.4 eCODEX .......................................................................................................................... 44
7.5 EVIDENCE 2 e-CODEX .................................................................................................. 45

8 BEST PRACTICES ON GATHERING E-EVIDENCE ABROAD BY USING THE EIO .......... 47

8.1 Introduction ..................................................................................................................... 47
8.2 Overview of the EIO ........................................................................................................ 47
8.2.1 Background of the EIO ............................................................................................... 47
8.2.2 Definitions and main features of the EIO ................................................................. 47
8.2.3 Judicial decision and judicial authorities ................................................................. 48
8.2.4 Mutual recognition and grounds for return, recourse and refusal: ......................... 48
8.2.5 Scope and electronic evidence ................................................................................... 49
8.2.6 Deadlines .................................................................................................................... 49
8.3 Relation to other instruments ......................................................................................... 50
8.3.1 Instruments of judicial cooperation ........................................................................... 50
8.3.2 Privacy and protection legal framework to cross border access to data and e-evidence ......................................................................................................................... 52
8.3.3 Council of Europe instruments relevant to cross border access to data and e-evidence ......................................................................................................................... 53
8.4 Services providers, e-evidence and the EIO .................................................................... 54
8.4.1 What kind of services do service providers offer when it comes to e-evidence? .... 54
8.4.2 Is direct cooperation with service providers considered voluntary or mandatory? .... 55
8.4.3 Admissibility of e-evidence obtained through voluntary cooperation ..................... 56
8.4.4 Legal nature of Internet protocols .............................................................................. 56
8.5 Guide on the EIO form, Annex A .................................................................................. 57
8.5.1 Section A: Involved states .......................................................................................... 57
8.5.2 Section B: Urgency ..................................................................................................... 58
8.5.3 Section C: Investigative measure(s) to be carried out ............................................. 58
8.5.4 Section D: Relation to an earlier EIO ....................................................................... 59
8.5.5 Section E: Identity of the person concerned .............................................................. 60
8.5.6 Section F: Type of proceedings for which the EIO is issued .................................. 60
8.5.7 Section G: Grounds for issuing the EIO ................................................................. 60
8.5.8 Section H: Additional Requirements for certain measures .................................... 62
8.5.9 Section I: Formalities and procedures requested for the execution ....................... 62
8.5.10 Section J: Legal remedies ........................................................................................ 62
8.5.11 Section K: Details of the authority which issued the EIO ...................................... 62
8.5.12 Section L: Details of the authority which validated the EIO .......................................................... 63
8.6 Guide on the EIO form, Annex B ........................................................................................................... 63
8.6.1 Time limits ......................................................................................................................................... 63
8.6.2 Failure of meeting time limits/Best practice .................................................................................. 63
8.7 Guide on the EIO form, Annex C ........................................................................................................ 64
8.7.1 Article 31 EIO directive ................................................................................................................. 64
8.7.2 Form: Notification of interception of telecommunication without any need of technical assistance ........................................................................................................................................ 64
8.7.3 Best practice ..................................................................................................................................... 65

CONCLUSION ............................................................................................................................................. 66

ANNEX I: DIGITAL EVIDENCE AND INTERNATIONAL STANDARDS ................................................. 67
ISO/IEC 27037:2012 .................................................................................................................................... 67
ISO/IEC 27042:2015 .................................................................................................................................... 67
RFC 3227 .................................................................................................................................................. 70
RFC 4810 .................................................................................................................................................. 71
RFC 4998 .................................................................................................................................................. 72
RFC 6283 .................................................................................................................................................. 72

REFERENCES ............................................................................................................................................. 73
List of figures

Figure 1: User-Server model ........................................................................................................... 13
Figure 2: IPv4 address structure (Wikipedia) .................................................................................. 13
Figure 3: IPv6 address structure (Wikipedia) .................................................................................. 14
Figure 4: TCP header protocol ........................................................................................................ 15
Figure 5: UDP header protocol ........................................................................................................ 15
Figure 6: Hash example .................................................................................................................... 17
Figure 7: Windows Event View example .......................................................................................... 18
Figure 8: Linux logs .......................................................................................................................... 18
Figure 9: Common Log Format example .......................................................................................... 19
Figure 10: Cisco Log Format ........................................................................................................... 19
Figure 11: Ubuntu Log Format ......................................................................................................... 20
Figure 12: Windows Log Format ....................................................................................................... 20
Figure 13: Types of cloud services in front traditional IT ................................................................. 33
Figure 14: Kumodd architectural diagram ......................................................................................... 38
Figure 15: e-Evidence system – proposed solution ........................................................................ 45
List of abbreviations

AES  Advanced Encryption Standard
API  Application Programming Interface
AWS  Amazon Web Services
BCCP  Belgian Code of Criminal Procedure
CAINE  Computer Aided Investigative Environment
CoC  Convention on Cybercrime of the Council of Europe
CJEU  Court of Justice of the European Union
CSA  Cloud Security Alliance
CSP  Cloud Service Provider
DFaaS  Digital Forensics as a Service
DoS  Denial of Service
EAW  European Arrest Warrant
EC  European Commission
ECHR  European Convention on Human Rights
ECS  Electronic communication services
EIO  European Investigation Order
EIOD  European Investigation Order Directive
EJN  European Judicial Network
ENISA  European Union Agency for Network and Information Security
EU  European Union
EXIF  Exchangeable Image File Format
GDPR  General Data Protection Regulation
IaaS  Infrastructure as a Service
ICS  Interpersonal communication service
ICT  Information and communication technology
IP  Internet Protocol
ISP  Internet Service Provider
KVM  Kernel-based Virtual Machine
LAN  Local Area Network
MLA  Mutual Legal Assistance
MLAT  Mutual Legal Assistance Treaty
MS  Member State
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comments</td>
</tr>
<tr>
<td>RPPO</td>
<td>Regulation on the Production and Preservation Orders</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure File Transfer Protocol</td>
</tr>
<tr>
<td>SIFT</td>
<td>SANS Investigative Forensics Toolkit</td>
</tr>
<tr>
<td>TESTA</td>
<td>Trans European Services for Telematics between Administrations</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>XMP</td>
<td>Extensible Metadata Platform</td>
</tr>
</tbody>
</table>
Executive summary

This document presents the best practices that are expected to be followed in cases when application of the EIO directive is applied. Besides the main instruction about application the document provides reasonable introduction to the main knowledge from relevant fields such as digital forensics and cross-border evidences collection from both aspects: technical and legal. This approach is understood by contacted experts to be most useful for the future professional in the respective organizations like prosecutors, judges etc. in cases when the EIO Directive will be applied.

The first chapters define the technical part of this document. It is aimed to facilitate the knowledge needed to carry out a forensic analysis in both traditional computing and cloud environments.

For that purpose, the first chapter is focused on defining basic general concepts such as the functioning of the Internet, the typical topologies of communication networks, how the information exchange process is carried out and which is the definition and use of metadata.

The next two chapters are addressed to the techniques and principles of forensic digital science. They describe the principles of forensic computing, the basic legal requirements needed to carry out the information extraction process properly and the different types of information extraction methods, such as dead acquisition analysis and live forensics methods. Reverse engineering concept is explained and the most complete and well-known tools in this field are listed.

This document also addresses and defines the characteristics of the technologies available behind the cloud environment, as well as carrying out an analysis of the risks and advantages associated with it, since every day more companies and entities migrate their information to the cloud. Some typical practical cases that can be used as a reference are also defined.

One of the characteristics of cloud environments is the difference in terms of geographical location, so the data can be stored in multiple countries with different jurisdictions. This represents a challenge for the EU that needs to develop tools aimed to transfer digital evidences quickly and safely. For that reason, the tools that have been developed so far in this field are analysed.

The legal part is defined in Chapter eight and is aimed to provide a reliable method and a series of best practices on gathering e-evidence abroad by using the EIO. Therefore, this part of the document can be used as a guide to complete properly each of the steps needed in the EIO.

In the Annex, the international standards that can be followed by investigators to carry out a digital forensic analysis of evidence are defined.

It is important that the agents involved in the scope of the Directive and the EIO increase their technical knowledge, their understanding of the main concepts regarding forensic environments in the cloud and enhance their knowledge on filling the EIO and the related procedures.

This document is therefore intended to be used as a guide to allow the most effectiveness and appropriate adaptation to the current situation of the European environment.
1 Introduction

The non-localised nature of cloud computing causes problems in digital forensics procedures and requires LIVE or ON-LINE FORENSICS due to the architecture of the cloud (multi tenancy, distribution and segregation of data), and presents legal challenges related to the integrity and validity of the data collection, evidence control, ownership of the data or the locality of jurisdiction.

LIVE_FOR aims to analyse the current situation in relation to the implementation of Directive 2014/41, the level of understanding among relevant members of the LIVE-FOR target audience, and the judicial relationship between the member countries of the European Union.

There are legal and technical challenges related to the implementation of Directive 2014/41/EU in regard to cybercrime and cloud computing services. First of all, there certainly is a need to collect data about the intended implementation of the directive by the MS and its alignment with the MS national legal orders, as Directive 2014/41/EU does not consider their differences. Another collection of data is required about educational curriculums for prosecutors and judges regarding the directive and the specific knowledge necessary when deciding on an investigation order for criminal justice purposes in an environment known as cloud computing services. These data need to be analysed to identify the obstacles that delay the implementation and application of the EIO in both aspects: legal and technical. There is also a need to assess the level of awareness of the target groups about the challenges imposed by cybercrime attacks on data and services in cloud computing environments. Based on those findings, the real needs for education and training of the target groups about the recently adopted EU EIO mechanisms and the circumstances for application, and the needs for upgrading the current knowledge of the target group members will be possible to be clearly identified. In that context, the addressing of latest live digital forensic approaches implemented within the volatile cloud environment is required as well. The upgrading of the current university curriculums with programs for judges and prosecutors with contents addressing both needs is also an identified need in the area.

This document clarifies some technical key concepts that are needed for upgrading the knowledge of executive authorities with the latest achievement in relation with Directive 2014/41/EU and live forensic procedures.
2 Basic concepts

2.1 How does the Internet work?

The Internet is a network of devices (computers, mobile phones, etc.) that are connected to each other through cables, waves or other methods that allow exchanging information between one network and another and one device and another, following the same language (TCP protocol). In case a device does not follow that language, it will not be able to exchange information between other devices.

Furthermore, to allow connectivity to the Internet, all devices have to follow a series of rules to be able to access it. It is necessary to assign an ISP (Internet Service Provider) that provides the device an IP address, which is a number that allows the device to be immediately identified in the network. This number is unique, that is, no other device has the same number in the network.

2.2 User / server definition

The User-Server is a distributed system among multiple processors where there are users that request services and servers that provide them.

When using the Internet, there is always a computer called User, which sends requests to another computer/machine called Server.

The main purpose of this communications is:

- Get a web page
- Access an application
- Read an email
- Etc.

2.2.1 User

It is the one that initiates the communication, a service requirement. The initial requirement can be converted into multiple work requirements through networks. The location of the data or applications is completely transparent to the user.

2.2.2 Server

It is an application that offers a service to Internet users. The server receives a request, performs the required service and returns the results. Generally, a server can process multiple requests (multiple users) at the same time.

There are different types of servers, some examples:

- Web servers
- File servers
- Print servers
- Etc.
The Internet is a collection of many different systems, networks, protocols, addresses, ports, services, etc. The smallest network element is our home computer. This computer connects with other devices in a small network controlled by a router. The different networks types are:

- LAN (Local Area Network): every device has unique IP address identifying it. (192.168.1.2)
- WAN (Wide Area Network): The union of many LANs usually belonging to the ISPs (Internet Service Providers). Public IP.
- Network of networks or Internet: set of independent WAN communicating using TCP/IP protocol.

Information exchange is a process used to send or receive information in a network (WAN or LAN) through a mechanism. In order to achieve this transfer, there must be a connection (with or without wire) and a mutual language (protocol) between devices.

The information exchange speed is called bandwidth and is measured in bps, which stands for bits per second.

### 2.3.1 Addresses

The addresses are unique ID numbers for every connected device. The packet switches and the routers use the IP addresses to determine which network section they will use to forward the data. The common IP address version is called IPv4 with 32 bits of information, therefore, there are 4,294,967,296 possible addresses.
However, due to the huge increment of connected systems, a new IP version has been deployed, IPv6, with 128 bits of information, therefore 340.282.366.920.938.463.463.374.607.431.768.211.456 (340 sextillion) possible addresses.

A Typical IPv6 Address For A Device (Host)

![IPv6 Address Structure](Wikipedia)

**2.3.2 Ports**

Every device identified by a unique address has to be able to communicate simultaneously with various applications/services. This is achieved by using logical ports. Information exchange with each service is performed through one or more ports. To define the ports, 16 bits are used, therefore the maximum number of ports is 65536 and we can classify them as:

- Privileged Port: 0-1023, only users with privileges can start services or applications in these ports. They are those used for well-known applications, such as DNS, DHCP, WEB, FTP ...
- Registered ports: 1024-49,151, these ports can be used by any user. You can put any application or service in them.
- Dynamic ports: 49,152-65,534, these ports can also be used by any user. They are usually used by applications in a more dynamic way, so they are opened and closed for short periods of time.

**2.3.3 Protocols**

Protocols, as we have said, are conventions on how and what can be sent over the network. On the Internet the most common ones are:

- **IP protocol**
  
  It provides the mode of transmission of data packets from one end to another, that is to say from one device to another identified by IP addresses, in the simplest way since it does not implement any control mechanism or verification of the ones it sends. Actually, there are two versions of this protocol, IPv4 and IPv6, discussed earlier in this document.

- **TCP protocol**
  
  It stands for Transmission Control Protocol. This is one of the main protocols of Internet. It provides ports and various control mechanisms to ensure the data is received correctly and in order. The vast majority of applications on the Internet (Web, mail, browsers ...) work under this protocol.
The figure below describes TCP header protocol.

![TCP header protocol](image)

**Figure 4: TCP header protocol**

- **UDP protocol**

UDP stands for User Datagram Protocol and it is documented in RFC 768. This protocol does not offer guarantees or any type of control to ensure that the packets sent to the destination arrives and arrives in the correct order. It is a very used protocol for services that do not need specific connections, that is, there is a lot of connection / disconnection, (DNS, DHCP...) or for large volumes of data such as audio or video via streaming.

The figure below describes UDP header protocol.

![UDP header protocol](image)

**Figure 5: UDP header protocol**

### 2.4 Encryption basic concepts

The concept of encryption, applied to information technology, can be understood as the processes to be applied to the data to be protected to prevent it from being visible to third parties, ensuring that both transmission and reception will only be visible by the people whom it is addressed.

The processes that must be used to obtain communications or encrypted data are formed by complex mathematical algorithms that use one or several keys to encode this data, obtaining that only the people who have those keys will be able to visualize the data.

Nowadays, because of the problems of theft of information, passwords, identity theft, more and more, the organizations, institutions and companies are more aware that the use of tools or encryption services are necessary to avoid these incidents and offer more reliable services to its users, as well as its staff in general.
2.4.1 Generic Encryption algorithms

In general terms, we normally use two different methods to perform encryption, each of them is more suitable for some functions or others. These are symmetric key and asymmetric key methods. Next, we explain its operation:

**Symmetric encryption**: The key used to encrypt and decrypt is the same. The disadvantage of this algorithm is the key exchange while the advantage is that the computing calculation is not too high. The most used algorithm that falls within this category is AES.

**Asymmetric encryption**: They use a pair of keys, in such a way that the keys to encrypt and to decrypt are different. This is what is known as a public key system. The private key is owned by the one that decrypts the data, while the public key is the one that you leave available to the users with whom you want to communicate. So, if you want to send an encrypted message and only the person to whom it is directed should see it, you must use his public key to encrypt it and only the person with the private key corresponding to that public key will be able to see it.

This method is also used for electronic signature, and for email, to ensure the authenticity of the person sending the email.

The advantage offered by this method is that it facilitates the distribution of the keys and the disadvantage is that the calculation capacity needed is higher.

One of the most known algorithms is the RSA.

The asymmetric method is generally used to encrypt communications because it is faster and the asymmetric is used to transfer the key.

2.4.2 Hash definition

One of the most effective methods to ensure legal admissibility while preparing to engage a forensic analyst includes the process to generate cryptographic hash values.

A cryptographic hash function is a deterministic procedure (it will always give the same result) that takes an arbitrary set of data and returns a string of fixed-size bits.

A forensic hash is used for identification, verification, and authentication of file data. A forensic hash is a form of a checksum. A checksum is a mathematical calculation, it adds up the assorted bits in a data string and gives us a value.

A forensic hash is the process of using a mathematical function and applying it to the collected data which will give us a unique identifier for the acquired data. If the data is changed it will imply that the new hash will be different, however minimal the change may be.

Examples of checksum algorithms: MD5 (Message Digest 5), SHA-1 (Secure Hash Algorithm 1) and SHA-256. These algorithms are commonly used on forensic image files and also used to validate the integrity of downloaded files (e.g. software, pdf’s documents, etc.) to confirm that those files are the original ones and have not been modified. That is, to ensure the integrity of the data.

MD5 and SHA-1 are less robust, and can generate the same hash value for two different inputs. For the moment, SHA-256 has not been broken. The figure below shows a hash output example:
2.5 Log definition and properties

2.5.1 What is a log?

A log is a record of a server or a computer activity used for statistical purposes as well as backup and recovery. Log files are written by the operating system or other programs for such purposes as recording incoming dialogs, errors and status messages and certain transaction details. Start and stop times of routine jobs may also be recorded. Normally generated in plain text.

Logs allows us to know what happened in an information system and are widely used for:

- Maintenance
- Auditing
- Forensics

Any event can be logged. There is not a standard format, every system/application uses its own.

For example, Event Viewer is a component of Microsoft’s Windows operating systems that lets administrators and users view the event logs on a local or remote machine:
Figure 7: Windows Event View example

Figure 8: Linux logs
2.5.2 Log properties

To be useful, logs have to be generated with a certain granularity. If the granularity is too big we will not be able to establish time relation. Stored logs take a huge amount of disk, so after some time (days, months or years) logs are used to be deleted, as we don’t have infinite disk resources.

To avoid wasting disk space, only the logs regarding relevant events are stored. Most applications can generate information/debugging logs but these are generally disabled.

A good log policy makes it much easier to perform a forensic analysis.

Logs generally belong to the party storing them and can be generated/stored in any point of the information exchange:

- In the user premises
- In the network operator premises
- In the receiver premises

Each party will have its log policy and its applicable regulations regarding log storage and retention.

There are hosting providers who offer what it’s called “bulletproof hosting” which, in fact, is a hosting service, which doesn’t generate/store/provide any logs:

- Placed in countries with very loose regulations regarding logs
- Used by most criminal organizations for its activities

However, we will see those formats that are typically used.

Common Log Format

Is a standardized text file format used by web servers when generating server log files.

![Sample log entry in common.log](image)

**Figure 9: Common Log Format example**

- Other logs

Logs may vary depending on the system that has implemented them. The structure of the logs of some manufacturers is shown below.

![Cisco Log Format](image)

**Figure 10: Cisco Log Format**
Log files have several usage types. They record the user’s activity and especially the server programs (daemons), they are key in investigation processes, and under the control of those who generate them so they can be susceptible to being manipulated. Sometimes the required information can be found by correlating several log files.

They usually include information about the moment in which the event happened.

- **Storage**

Log files can be:

- Stored in the application itself:
  - Log files
  - Databases
- Stored in the operating system:
  - Operating system log files
- Shown by console
  - Printed directly

- **Interpretation**

- Use of forensic software to avoid bugs
- Validation test of the software used

In security, it is usual to correlate several types of logs to obtain information about events. These events can be related to applications.

Some of the most common types of uses related to security are defined below:

- Determine in real time the probability of materializing a threat at any given time
• To know in real time when a threat to the system begins to allow and alert before damage appears
• To know if a threat has been successful or not and determine the real impact on a system
• Determine patterns of the threats, which will be used later to implement new security measures or improve existing ones

2.6 Metadata

Metadata is a fundamental part of forensic analysis. The definition that we can find in the ‘CoE Electronic Evidence Guide’ is: "Metadata, or data about data, consists of information about a file other than the content of the file. The file ‘properties’ can include the date and time that the document was created, when it was last modified and last accessed and by whom. This data can be extremely useful in linking files to individuals”.

That is, they give us additional information about something we already have. Metadata can provide a lot of information, so there are also "anti-forensic" tools that delete or obfuscate them. In the digital world we find them in documents (text, images, photos ...), email, applications, file systems, etc. They can give us information about the owner, creation dates, modification, deletion, printing, formats, device from which it was made if it is a photo, location, etc.

2.6.1 Types of metadata

The different types of data are defined below:

• EXIF (Exchangeable Image File Format): Save technical information about the capture and the image. All the cameras on the market and mobiles store this information (e.g. GPS, Flash, etc.)
• IPTC: Industry standard to store administrative, descriptive and copyright information in images.
• Office documents: large amount of metadata: Author, Keywords, Template, Last modification, Revision number, Program used, Editing time, Last impression, Company, etc.
• XMP (Extensible Metadata Platform), for PDF documents: PDF version, Number of pages, Producer, Modification, date, Creation date, etc.

2.7 Digital evidence

2.7.1 Definition of digital evidence

Since there is not a standard definition about digital evidence, the definition provided by the National Institute of Justice is “Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, a personal digital assistant (PDA), a CD, and a flash card in a digital camera, among other places. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud. However, digital evidence is now used to prosecute all types of crimes, not just e-crime.”
2.7.2 Evidence preservation

Preserving evidence in any situation is very important. Many organizations are not well equipped to handle intrusions or electronic crimes from an operational point of view. The evidence loses its integrity and legal value if it has not been adequately preserved and the chain of custody has not been adequately documented. This happens when an incident is not managed properly or is done in an unstructured way.

For evidence to be admissible in a court, it is essential that the chain of custody be maintained accurately and chronologically. The chain of custody of evidence generally contains information related to:

- Who has had access to the evidence chronologically
- The work that has been done with the evidence (such as disk duplication, virtual memory dump)
- Evidence that the analysis performed is based on exactly identical copies of the original evidence (hash values)

Digital evidence can exist in log formats, file times stamps, contents of memory, browser history, contact lists, cookies, documents, hidden files, images, metadata, temporary files and videos. While not exhaustive, digital evidence can help provide context for the person who does not understand about cybersecurity. The ability to locate and capture evidence depends on the type of data, the skills and experience of the investigators and their tools.

Evidence can be corrupted or overwritten if the system is rebooted or files are accessed inappropriately. Before rebooting a system, it is necessary to download the contents of the disk memory. Any additional analysis must be done on a system image and on copies of the memory that has been dumped (never on the original system).

However, in addition to protecting the evidence it is important to preserve the chain of custody. The term chain of custody refers to the documentation, in detail, the handling and maintenance of the evidence, including the information of the owner, the persons who have accessed it and those who have modified it. This procedure is necessary to satisfy the legal requirements that require a high level of confidence regarding the integrity of the evidence.
3 Digital forensics techniques

3.1 Computer forensics principles

By definition, digital forensics is the “process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable in any legal proceeding (i.e., a court of law), according to D. Rodney McKemmish. The "conduct of a forensic" is based on the investigation of a security incident involving digital information.

The main challenges of this research are:

- Digital evidence is complex.
- The objectivity and knowledge of the experts and judges.
- The nonexistent standardization of tools.

All processes involved in a forensic analysis are aimed at providing digital evidence to help demonstrate that an incident occurred.

We must take into account the "anti-forensic" techniques that we can find applied to the elements to analyse and that basically hinder the possibility of obtaining the evidence. These techniques range from encryption, stenography, or deletion or overwriting of data or metadata.

3.1.1 Forensic readiness

It is what is defined as “the ability of an organization to maximize its potential in the use of digital evidence while minimizing the costs of an investigation”.

The use of digital evidence as a defense requires:

- Monitoring of systems and users: log files, email, network traffic, telephone calls, etc.
- Means (technical, physical and procedural) to ensure data to the eligibility standards.

3.1.2 Forensic timeline

Normally, there is a chain of events preceding the bad event and it is often useful to find out what these events were and what they did. It allows forensics specialists to determine how the attack was done.

3.2 Legal requirements

A forensic investigator must:

- Identify the crime;
- Obtain the evidence;
- Maintain the chain of custody of this evidence;
- Perform a forensic analysis;
- Present the evidence;
- Testify.
It is important to know the legislation to avoid the rejection of evidence in a trial for having broken the law:

- A test is the instrument that the parties have to accredit the facts on which they base their claims
- The moment of presentation of the same depends on the jurisdiction:
  - Civil, Labor or Social, Criminal, Administrative Litigation

### 3.3 Dead acquisition analysis

The dead acquisition allows investigators to access a shutdown system that has to be investigated. When a system is off, the risk of deleting or corrupting files is less than when the system is running. The objective of the investigator is to create an instantaneous image of the files stored on the system disk. This image must be identical to the image from the original disc.

A simple definition of dead acquisition analysis is "to carry out an analysis from a closed computer".

There are usually four stages related to traditional digital forensics:

- **Collection**: Search, seizure and acquisition of information in a forensic manner. The main actions are the duplication of the forensic disk and the collection of random evidence, such as CDs, documents and other information.
- **Examination**: This stage aims to identify and extract relevant data for the specific case. Analysis of the file system and extraction of all relevant information must be carried out.
- **Analysis** is the process of using the identified data in a way that demonstrates that the actions performed on the computer were performed by one or more individuals. This stage involves searching, consulting and correlating existing data.
- **Reporting** is the last stage in which the investigator collects all the information and writes a complete report on the findings, describing in detail the used procedure.

It is fundamental that all of the steps described above are carried out in the appropriate manner. Otherwise, the information collected will no longer have any value. The report written by the investigator must indicate the reason for the analysis of the system, the procedures used and the conclusions obtained. The report must achieve the following objectives:

- Describe accurately the details of the incident
- Be understandable to decision makers
- Be able to withstand a barrage of legal scrutiny
- Be unambiguous and not open to misinterpretation
- Can be easily referenced
- Contain all the information required to explain the conclusions reached
- Offer valid conclusions, opinions or recommendations when necessary
- Created in a timely manner

For many years, traditional forensic science has been the only means used to obtain digital evidence or carry out an investigation based on information extracted from computers. It is a relatively simple procedure. However, this technique has several advantages and disadvantages.
3.3.1 Positive aspects of dead acquisition analysis

Under normal circumstances, the possibility of forensic investigators overwriting or modifying information is quite low. Normally, they take enough precautions to ensure that the computer is not modified during the data copying process.

It should be said that when a computer is turned off, the data that is currently in use may be lost (the memory that stores data in use is called RAM). This supposes that a large part of the relevant information is not found when doing the analysis with the computer turned off. However, nowadays there are memories that store the data in use for a certain period after turning off the computer. This gives the investigator a chance to obtain information stored in RAM for a short period of time.

3.3.2 Limitations of dead acquisition analysis

There are several problems related to traditional forensic science. Those most relevant are described below.

- In response to the effectiveness of forensic analysis, cybercriminals have resorted to the widespread use of cryptography. This means that in many cases, examiners can not obtain the necessary information because the information is encrypted.
- The need to acquire data related to the network (from available ports) has grown exponentially. This type of information is volatile and is lost in case the computer shuts down which, as mentioned above, is the basis of traditional digital forensic analysis.
- Modern computers have increasingly greater capacity to store information. This fact, together with the complex and advanced techniques used by cybercriminals, means that research based on traditional forensic science is slow and complex. The log files also tend to increase in size and dimension, which further complicates an investigation.
- Forensic analysis is not the optimal method to acquire volatile data. Although modern RAMs give a margin of time in which volatile data is not erased, this time is often not enough to make an adequate acquisition.

Due to the many limitations of traditional forensics, forensic acquisition is an alternative that is used very frequently. This allows forensic professionals to access a large amount and variety of information that would otherwise have been lost in traditional forensic analysis. The next section addresses this acquisition mode.

3.4 Live forensics

The live forensic acquisition method is similar to the dead forensic acquisition method. It is carried out when the computer is turned on and developed in response to the deficiencies of traditional forensic acquisition techniques, taking into account the retention of volatile data and a countermeasure for files encrypted in a live system.

When the systems are turned on, the information should be acquired according to the order of volatility, from higher to lower volatility. The degree of volatility has, in general, two levels:

- Information about the RAM memory, partitions and swap files, network processes and the running operating system;
- Information of the files and data systems contained in the sectors of the devices by blocks.

In the case of virtualized environments, in which each of the virtual machines will be formed by several files, such as the hardware configuration of the computer, the one used for the memory and
one or more physical or virtual disks. Here, the information to be obtained will be the virtual hard disks and a dump of the part of the RAM used by this environment. In this way, once all the configuration files of the virtual machine and the virtual disks have been obtained, it should be able to reproduce the original environment for analysis.

When mobile devices are manipulated, they must be properly isolated, so that they do not come into contact with wireless networks that can accidentally manipulate the data contained within them, for which devices known as Faraday cages will be used.

The analysis methodology consists on cloning the accessible parts of the SIM card and entering the clone of the card in the terminal. Once the terminal is turned on, a low-level copy of the data contained in its internal memory will be made. If any specific terminal model is not supported by the forensic tools available, the information that can be read on the screen can be transferred to the report or proceed as in the case of the systems turned off.

Once the data analysis process has been completed, neither the battery nor the original SIM card should be inserted again and, as always, the hash of all extracted information should be calculated.

### 3.4.1 Smartphone live data analysis

According to the document from ENISA “Mobile threats incident handling”, “mobile forensics refers to digital forensics relating to recovery of data or digital evidence from a mobile device (i.e. mobile phones, as well as other digital devices such as tablets and GPS devices)”.

The recommendations to be taken into account when performing a forensic digital in the phone and that are expressed in this guide are:

- **Data acquisition**: It must be done with the mobile phone turned on, because if it is not, the memory cannot be accessed. If you have additional SD cards, we must also collect that data.

- **Chain of custody**: There are certain points that we must monitor in the forensic analysis of mobile phones because they can make it difficult to maintain the chain of custody. These points are:
  
  - Most forensic tools available usually require installing extra software on the mobile;
  - There is no easy way to stop reading only ISO file systems, which must be monitored not destroy information or modify it;
  - If there is malware, it can erase the entire device or delete certain files if it is able to detect that kind of analysis.

- **Forensic network analysis**: Surely there will be needs to analyse both the Wi-Fi network and the cellular network. If the Wi-Fi network is company-owned, then it will be easy to acquire the data, standardized network forensic tools will be used. But as regards the cellular network, it will be necessary to take into account the ISPs and obtain a court order to access this information.

### 3.5 Volatile data definition

There are two types of storage, the persistent (hard drives) and the volatile data storage.

As the word indicates, non-persistent data is usually stored in volatile devices, which have the characteristics of being quite fast. This type of data is ideal for storing information where the period
of existence is short. When the process that generates these data ends, the data dies and remain inaccessible.

The information that these volatile data can give in a forensic investigation can be very useful, therefore, when a forensic analysis is carried out, maintaining the system and the processes in progress until obtaining the evidence is crucial.

There are two main types of volatile data:

- Volatiles, properly said, the data that we can take out of the system while it is running: network connections, processes in execution, characteristics of processes...

- Transient data: data that is generated or used by the applications during a period of time. For example, necessary data to access information that disappears when the application ends. Session cookies are type of transient data, or encrypted volumes mounted with a key that allows the accessibility. However, if these data are dismantled, even though they are physically available, it will not be possible to access the information.

All devices, from computers, mobile phones, servers or virtual servers have volatile storage; this is what is called RAM (Random Access Memory). The RAM is the area where the data that the computer uses in a precise moment is stored. It is a temporary storage area because the data and programs that are running, disappear when the machine is restarted.

The forensic analysis of the memory can be performed from the following components:

- RAM memory of the equipment
- CrashDumps Memory of virtual machines
- Hibernation files

3.5.1 Memory dump analysis

Memory dump analysis is a forensic technique that consists of dumping all the data stored in the memory and related devices (swap) in order to analyse it using the most appropriate tools and obtain information about the system and running applications.

Swap space is used by the system to swap chunks of memory between the RAM and the disk when there is no sufficient space in the RAM memory. During the forensics, Swap files may be found in a disk partition or in a file in the file system.

Some tools to memory dump analysis:

- For Windows Systems: FTK Imager, Mandiant Memoryze or Windd.
- For Linux Systems: Memdump, dd copying device fmem.
4. Advanced digital forensics procedures and techniques

4.1 Reverse engineering

Software reverse engineering are techniques used to follow the source code of a program. The reasons for using this technique are varied:

- Identify malicious or erroneous content in the program.
- Adapt it to meet certain requirements.
- Find out how it works or how it performs certain functions.

If we use reverse engineering for the purpose of copying or duplicating programs, it may constitute a violation of copyright. For that, some software licenses specifically prohibit reverse engineering.

According to the article from "security affairs", there are some main steps to carry out software reverse engineering:

1- Attaching a debugger

The debugger is one of the basic tools of reverse engineering.

The debugger is very useful for testing programs, it helps us detect errors, allows us to pause the program step by step to see everything it do. That is a very good reverse engineering tool.

Some known debuggers are:

- For Windows: WinDBG and OllyDBG
- For Mac OS / iOS: llbd
- For Linux: gdv, dbx or GVD.

Evidently, there are techniques to avoid the use of a debugger and obtaining the code, the licensed and licensed software will protect you to avoid it.

2- Researching functioning

With a debugger, it is possible to see what this software piece changes.

Investigating aspects related to software such as the resources it uses (network, system, functions ...) is another typical technique when performing reverse engineering. Some tools to carry out this research are:

- Windows: Process Monitor, APIMonitor, TCPViewer or PortMon.
- Linux: Top, Dnotify, Tcpdump or Netstat.

3- Disassembling

Disassembling is one of the main techniques to actually perform reverse engineering, since disassembling involves restoring the source code. Obviously, in order to carry out disassembly, the compiler language, the rules for the construction of codes and the details of software architectures have to be known.

Some known disassemblers are: OllyDBG, Relyze or Capstone for Windows and zydis, Capstone or edb for linux.
4.2 Computer forensics tools

The goal of computer forensics is to perform crime investigations by using evidence from digital data to find who was the responsible for that crime.

To help the realization of forensic analysis of computers there are a whole series of tools, oriented to different areas (database forensics tools, disk and data capture tools, file viewers, network forensics tools...) and described below. These tools were recommended by the Infosec Institute⁴:

4.2.1 Open source tools

- **CAINE**
  
  CAINE (Computer Aided Investigative Environment) is the GNU/Linux live distribution created for digital forensics. The main features that CAINE offers are: an interoperable environment that supports the digital researcher during the four phases of digital research, an easy-to-use graphical interface and an almost automatic generation of the final report.

  Read more about it: [http://www.caine-live.net/](http://www.caine-live.net/)

- **SANS Investigative Forensics Toolkit – SIFT**
  
  The SIFT workstation is made up of a set of open source forensic tools designed to help perform forensic analysis.

  It is one of the most used open source tools. It has the advantage that it is updated very frequently with what is always available with the latest forensic tools.


4.2.2 Commercial tools

- **EnCase**
  
  EnCase Forensic is one of the most used commercial tools, offering great flexibility. It can be used to acquire data from a wide variety of devices, such as smartphones, tablets and GPS and offers us the possibility of generating reports on the results obtained.

  More information: [https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx](https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx)

- **Cellebrite UFED**
  
  Cellebrite's UFED solutions are a set of high-level tools that help researchers, quickly and efficiently, to capture the evidence of both mobile devices and cloud services.

  Along with EnCase it is one of the most used forensic tools trading platforms.

  More information: [http://www.cellebrite.com](http://www.cellebrite.com)

- **X-Ways Forensics**
  
  X-Ways Forensics is the forensic edition of WinHex. It is an integrated, powerful and affordable forensic computer environment with numerous forensic features that make it a powerful tool with a multitude of features: disk analysis, free space capture, slack space, space between partitions and text, which creates a table fully detailed unit content with all existing and deleted files and directories and even alternative data streams (NTFS), Bates numbering files and more like image gallery, file preview, calendar / timeline visualization, etc. It also serves as a low-level image creation and cloning tool that creates true mirrors
(including all free spaces) and reads most disk formats and media types and supports drives and files of virtually unlimited size.

All features and further details are described in: https://www.x-ways.net/
5 Cloud environment and cybercrime

Cybercrime represents a high expense and risk for any society, weakens confidence in the information and communication technologies environment and threatens international peace and stability. Military conflicts and political disagreements are increasing and are supported by cyber-attacks. Trillions of security incidents happen every year and millions of attacks on computer systems every day. Cybercrime is therefore undoubtedly one of the most important concerns of governments, societies and individuals. The estimated cost of cybercrime in the European Union is around 15 billion euros per year.

It should therefore be noted that the criminal judicial authorities face the problem that the evidence in relation to any of the crimes we have mentioned above is stored in electronic format and in cloud environments.

In addition, the entry into the market of IoT devices is a new window of opportunity for cybercrime, which suggests that it will increase in the coming years.

In general terms, the data required in judicial investigations are classified into three groups:

- Subscriber information
- Data traffic
- Data content

The main problem to obtain this data, necessary to carry out a criminal investigation, happens when the data is stored in cloud environments. Cloud computing (also called "cloud environment") is a model that allows access to the network and on demand, to a shared group of configurable computing resources (networks, servers, storage, applications and services) that can be provided by a relatively agile, fast and simple way.

The cloud model is composed of five essential characteristics:

- Service available on demand
- Wide access to the network
- Sharing of resources
- Quick elasticity
- Custom service

It offers three differentiated services:

- “Cloud Software as a Service” (SaaS)
- “Cloud Platform as a Service” (PaaS)
- “Cloud Infrastructure as a Service” (IaaS)

These services can be deployed following four different models:

- Private cloud
- Community cloud
- Public cloud
- Hybrid cloud

The cloud environment presents a substantial change in the way in which, until now, the data has been worked on, since they no longer remain in specific devices or in closed networks and they are treated in a distributed way through different services, suppliers, locations and jurisdictions.
All this implies a series of new complex challenges for the judicial authorities, mainly due to the volatility of the data, the independence of the jurisdictions and the maintenance of the chain of custody of the digital evidences. In addition, it is not always clear whether the cloud service provider is considered the "controller" of the data or the "processor" of the data.

In this context, the main problem of cloud services lies in the difficulty of carrying out forensic analysis procedures due to their decentralized nature. This presents a series of legal challenges related to the integrity of the data, the control and ownership of the evidence collected and the jurisdictional differences that exist in the different member countries of the European Union.

5.1.1 Risk of cloud computing

In terms of information security, the cloud environment must be able to protect data in the cloud, as well as ensuring that governance, risk management and compliance are addressed in an integrated environment. NIST\textsuperscript{9} describes the following risks related to the cloud environment:

- **Insulation failure**: a characteristic of cloud computing are shared resources. Although it is not commonplace, the failure mechanisms that separate storage, memory, routing and reputation among different tenants can create risks.
- **Data protection**: It can be difficult for users to verify the data management procedures of the cloud provider.
- **Unsafe or incomplete data deletion**: Due to multiple leases and the reuse of hardware resources, there is a greater risk that the data is not completely removed, appropriately or in a timely manner.
- **Malicious insider**: cloud architects have high-risk roles. A malicious intern could cause a great degree of damage.

These risks can lead to various types of threats. The following CSA\textsuperscript{10} list describes the main threats of cloud computing:

- Data breaches
- Data loss
- Account hijacking
- Insecure application programming interfaces (APIs)
- Denial of Service (DoS)
- Malicious insiders
- Abuse of cloud services
- Insufficient due diligence
- Shared technologies issues
- System and Application Vulnerabilities
- Advanced Persistent Threats (APTs)

5.1.2 Benefits of cloud computing

Although cloud computing is attractive to attackers because of the massive concentrations of data, cloud defences can be more robust, scalable and cost-effective. The European Union Agency for Network and Information Security (ENISA) provides the following top security benefits of cloud computing:
• **Scalability**: Technology in the cloud allows reallocating resources quickly and effectively. An example of this is the filtering and modelling of traffic, authentication and encryption as defensive measures.

• **Cost-effective**: The measures adopted are cheaper when they are implemented on a large scale. Concentration or resources provide a cheaper physical perimeter and control of physical access and easier and cheaper application of many security-related processes.

• **Timely and effective updates**: Updates can be quickly extended through a homogeneous platform.

• **Audit and evidence**: In theory, cloud computing can provide forensic images of virtual machines, which can result in a decrease in the time required to carry out the process of gathering information in a forensic investigation.

### 5.2 Cloud services

Cloud service providers (CSPs) are companies that offer network services, infrastructure or commercial applications in the cloud. Cloud services are hosted in a data center where companies or people using network connectivity are able to access.

It is mandatory to understand some cloud forensics concepts, since the complexity of cloud forensics depends on the cloud service models (SaaS, PaaS or IaaS) and on the deployment model (private or public cloud).

Different service models were described briefly in the basic concepts chapter of this document. However, the key elements that affect investigations between different service models, following some NIST criteria are described with some detail.

![Figure 13: Types of cloud services in front traditional IT](image)
5.2.1 **Cloud software as a service - SaaS**

Software distribution model where a company provides the maintenance, support and operation that the user will use during the time he hired the service. The user will use the system hosted by that company, which will maintain the user's information in their systems and provide the necessary resources to exploit that information.

The user has the ability to use the provider’s applications that run on their infrastructure. It is possible to access applications from various user devices thanks to an interface (web browser for example). The user does not administer or control the underlying infrastructure of the cloud.

5.2.2 **Cloud platform as a service – PaaS**

PaaS model is a cloud services category that provides a platform and environment that allow developers to create applications and services that work through the internet. PaaS services are hosted in the cloud, and users can access them simply through their web browser. The PaaS model allows users to create software applications using tools provided by the provider. Services can be preconfigured functionalities to which users can subscribe, choosing the functions they wish to include to solve their needs and discarding those they do not need. Thus, the packages can vary from a simple environment that is handled with the mouse and does not require any kind of knowledge or special installation by the user side, until the provision of infrastructure options for advanced development.

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

5.2.3 **Cloud infrastructure as a service – IaaS**

Infrastructure as a service usually works through a virtualization platform. Instead of acquiring servers, space in data centre or network equipment, users buy all these resources from an external service provider. A fundamental difference with virtual hosting is that the provisioning of these services is done completely through the web.

The capacity that is given to the user is the possibility of providing processing, storage, networks and other fundamental computing resources where the user can implement and execute arbitrary software, which can include operating systems and applications. The user does not manage or control the underlying infrastructure of the cloud, but has control over operating systems, storage, deployed applications and possibly limited control of selected network components (e.g., host firewalls).

5.3 **Cloud management technologies**

Cloud management platforms are a variety of integrated products that provide tools for the management of public, private and hybrid cloud environments. All of that cloud managers must have minimum required tools providing self-service interfaces, system images provisioning, metering and billing, and some degree of workload optimization. Then, more advanced managers may also include integration with external network resources, service catalogues, tools supporting the configuration of storage and network resources and provide advanced monitoring for improved “guest” performance and availability.
5.3.1 Virtualization

Virtualization consists of creating an environment equivalent to a physical one using software tools, for example, servers, computers, networks, applications, etc. That’s why you can talk about virtual servers, virtual applications....

Virtualization offers us the advantage of being able to run several virtual machines on a physical server. To carry out the management of the different machines that will coexist, another layer of software is needed, called hypervisor, which is in charge of making the communication between the server hardware (disks, memory, network and CPU) and the virtual machines.

Some of the most common virtualization tools are:

- **VirtualBox**
  VirtualBox has many followers thanks to the combination of a very attractive model. It has a free price service, multiplatform support and a large number of functions that make running and maintaining virtual machines simple. The descriptions and parameters of virtual machines are completely stored in plain text XML files to facilitate portability and easily share folders. Its "Guest Additions" function, available for Windows, Linux and Solaris virtual machines, makes VirtualBox intuitive and easy to use, allowing the user to install software on the virtual machine that grants additional privileges to the host computer to, among other tasks, share files, share units and peripherals.

- **Parallels**
  Although the Mac version is best known of its virtual machine software, Parallels also runs virtualization on Windows and Linux. Thanks to optimization in Intel and AMD chips, Parallels software has a direct link to the hardware of the host computer with selective focus. When you enter the virtual machine to work, the host machine automatically gives you the processing power. The software also offers peripheral support functions, synchronization, clipboard sharing and shared folders.

- **VMware**
  VMware is one of the best-known virtualization platforms. For desktop users it comes in two main forms: VMware Player and VMware Workstation. VMware Player is a free platform, focused on occasional users who do not need advanced or business solutions. VMware Workstation includes all the features of VMWare Player-easy virtual machine creation, and many other capabilities such as the possibility of cloning machines, taking multiple snapshots of the guest operating system, repeating changes made, etc.

- **QEMU**
  QEMU is focused on Linux machines and is a powerful virtualization tool built on the KVM (Kernel-based Virtual Machine) system. The system executes guest code directly on the host’s hardware, can emulate machines on all types of hardware with dynamic translation, and supports automatic resizing of virtual disks. In addition, it can run on hosts without administrative privileges. Unlike most emulators, QEMU does not require administrator access to run, which makes possible to build portable virtual machines based on USB memories.
6 Cloud forensics practical approaches

6.1 Introduction

Due to the different types of cloud services (SaaS, IaaS and PaaS) that already exist and their different implementations (public, hybrid and private), different practical approaches may be needed when performing a forensic investigation in cloud environments.

The main point of decision about which techniques to apply depends directly on what limitations exist for acquiring the information. The available data for the investigation can also depend of the type of cloud and its implementation.

The first step thus, is to obtain information of the cloud and its operator (CSP – Cloud Service Provider). Some points to consider are:

- Where does the CSP operate?
- Which are its SLAs (Service Level Agreements) on multi jurisdiction and multitenancy?
- Which security measures or services does it implement?

By doing this the investigator can obtain a more objective view of the possibilities for investigation, for example, how many data may be able to obtain, in which way, how long will it take, etc.

It is also possible to have several kinds of clouds (and CSPs) involved, in which case cloud forensics could be quite more complex.

Depending on the cloud implementation we can still apply classical forensic techniques. These may be used in private clouds or owned parts of hybrid clouds, since the investigator can access the infrastructure directly. In that case, practically none of the access limitations mentioned before apply. Still, the data availability limitations could be present, depending on the access control measures the private operator has implemented. Nevertheless, this section will focus on the public cloud forensics, including the public parts of a hybrid cloud.

We can talk about 3 scenarios focusing on the 3 types of clouds. For any of them, it is always possible to ask the CSP to provide as much information as it is available, and to perform a classical forensic process over these data. The next subsections describe alternative actions to carry on when this is not an available choice for any reason.

6.2 Cloud SaaS forensics

This is the highest level of abstraction in the cloud services offer. It consists of directly offering a service, such as email, or multimedia or document edition, storage, etc...

One of the most frequent usage is expected to be with the cloud storage services, as they are a very well-known and widely used services offered by many companies such as Amazon, Dropbox, Google, Microsoft or Apple. Cloud storage offers remote storage, a user can access the space from any browser or from clients that may have been installed on mobile devices or on computers.

6.2.1 Client-based cloud SaaS forensics

When using these services, temporal copies of the files are stored locally, in the devices used for accessing them. These temporal copies may be valid evidence and it is not necessary to directly access the information in the cloud.
One practical approach may be the following:

- Access the computer
- Acquire a disk image
- Analyse the image for gathering stored files information, browser metadata, etc...

The paper “Digital forensic investigation of cloud storage services” provides great detail of the possibilities of this method.

Although this is a good approach, the required physical access to the devices related with the investigation, may represent serious limitations. The main one is that possibly not all the data stored in the cloud are present in the physically accessible devices, either because no access to the data has been made from the device, or because they have been deleted. In this last situation evidence of presence of the data in the device can yet be obtained but not necessarily the data itself.

The other serious limitation is that other versions of the data may exist in the cloud but not on the devices. Usually, lack of synchronization may make some of the device versions to be old ones. But sometimes, there can also exist newer versions, crafted in other devices, not available to the investigators neither in the accessed devices, nor in the cloud.

These limitations make necessary another approach to data analysis from a client device.

### 6.2.2 API-based forensic cloud

Some cloud services provide an API (Application Programme Interface) to directly acquire the content of a cloud drive storage. This permits access with a lower level of abstraction than the client front-end and is, therefore, appropriate for forensic processing.

One of the most important parts of API-based forensic is that APIs use to be well-defined and have a detailed documentation, so this allows for formal and precise approach to forensics tool development and testing. Additionally, developing the drivers for the API is much easier than reverse engineering and software tools are easy to use too.

All queries to these APIs have to be authenticated but, since the investigator has access to the client device, credentials are available in the client applications.

These are some API-based forensic tools:

#### 6.2.2.1 Kumod

It is an acquisition tool that queries the target cloud drive and obtains a list of files with their metadata and place it an appropriately structured local file system tree.

It can be used via command line or with a web GUI, and both allow filters on data acquisition.
6.2.2.2 UFED

It is an extraction and analysis software, which uses the user credentials from popular cloud services. UFED extracts and analyses the data of the desired cloud service through the service provider’s API and shows all the data (of any cloud service) in a unified format, which helps forensic experts to look at the common connections and correlate critical evidences.

Furthermore, extracted data is hashed separately, which allows comparing data against its origin, and UFED can generate and share PDF reports of all the data acquired.

6.2.3 Forensics as a service

DFaaS (Digital Forensics as a Service) offers a centralized capacity for data that can be shared amongst all investigators.

This service-based approach has the capacity of collecting, examining, storing and analysing the amount of data by detectives and forensic experts through a web application or some interfaces.

All of those platforms allow running automated tools, analysing data using visualization tools, integrating data sources or building a network of contact, which makes it possible to identify, classify, organize and compare the traces.

6.3 Cloud IaaS forensics

In an IaaS environment, the forensic analysis is made at multiple layers. This is because this type of architecture is similar to any machine, but it can only be accessed remotely, and moreover, it has a virtualization layer that obligates forensic experts to use a different acquisition activity for every layer.

One possible advantage is that the administrator of the infrastructure may have placed/contracted additional security/monitoring measures that will provide more information.
Despite these details, the forensic process can be performed in a very similar way as a classical one, by using the appropriate tools, and considering the virtualization environment restrictions.

In the following sections, some tools that may aid performing this kind of forensic investigation are presented. The readers interested to obtain more detailed information about them, should refer to the paper “Hardening AWS Environments and Automating Incident Response for AWS Compromises” written by the team behind Threat Response, a cloud cybersecurity company.

### 6.3.1 Margarita Shotgun

This tool allows obtaining memory images of both on premises and AWS instances. The acquisition of the memory is done remotely. It is only necessary to configure certain parameters (server IP, administrator password, etc) of the instance that contains the memory wanted. To carry out the copy of the memory, the connection must be made through SSH (encrypted).

This tool is highly efficient since it works in parallel. That means that the copy is made very quickly obtaining high quantity of information.

### 6.3.2 Aws-IR

This tool can be used to effectively collect cloud evidence under AWS (Amazon Web Services) IaaS environments. This tool can be used to carry out an instance duplication in order to analyse it in a fast way. It can also perform additional processes that may reduce the success of an attack. Therefore, this tool is aimed to collect evidences while mitigating possible attacks.

Some of these processes are:

- Filter or cut the active links of the attacker
- Disable access to this compromised instance by changing the access key

### 6.4 Cloud PaaS forensics

This environment is similar to SaaS and data has to be provided by the CSP. On the other hand, it allows the administrators of the platform to implement access control facilities, when possible, that may help during forensic investigations.

### 6.5 Practical use case

In this section we present a use case for a forensic analysis of a mail service provided as SaaS. It is a simplification of the use case provided in the first LIVE_FOR educational workshop in Brussels, Belgium.

#### 6.5.1 Scenario

The Banker Martin Miller (M), a citizen of your country, is suspected to support a criminal organisation (O) by taking care of the organisation’s payments. There are strong grounds for believing that the O is involved importing drugs, mostly cocaine, importing counterfeited products and organising a network of forced prostitutions by smuggling of Asian women. O is poised to use violence and murders for achieving their interests.

Your national criminal police office became aware of M and his involvement in O by a telephone call monitored in another crime case, which is not related to the present case. Your police authority contacted you in your legal function and proposed the initiation of investigation proceedings.
Regarding to police’s information, M is living in Brussels and is taking care of the transactional proceedings of O, including wage payments of O’s members. Therefore, he holds information about the most important leaders of O. Furthermore, it is highly likely that M is trying to hide the incomes and sources of financing of the O by money laundering, investing money in companies and properties. It is alleged that M uses complex business activities, including complex accounting schemes, to conceal the true purpose of the criminal organisation.

In addition to that, the police know that M does not have any physical hard copies at his place, as he tries to act very confidential by not creating any evidence. He mentioned during the forenamed phone call, that he has a “clean” computer, meaning all documents and transaction scripts are stored in the cloud service WOLK, a Dutch internet service provider. Further investigations revealed that the company’s servers are located in Belgium. The servers are property of WOLK and not owned by another company. Open source investigations showed, that M is using the email-address mmiller@wolk.nl for various internet services, therefore it can be reasonably assumed, that this address is also used as access data to the cloud service.

M has previously been convicted of money laundering related to corruption offences in the construction industry in your country. After the serving of his sentence, he moved to Brussels to work in the financial sector.

### 6.5.2 Considerations

This case, as mentioned before, is related to a cloud service provided as SaaS. There are two possible main approaches depending on the possibility of acquiring the device.

**Is it possible to obtain M’s computer?**

- **yes**
  - Obtain the device and perform:
    - Traditional forensics looking for temporal copies of the data
    - AND/OR
    - Obtain credentials and perform API based forensics

- **no**
  - Ask WOLK for the service data and perform the forensic analysis on it
As the measures to be taken if the possibility of acquiring the device has been described in previous sections, here, the forensic analysis methods over the data provided by the CSP will be presented.

### 6.5.3 Analysis

First of all, the integrity of the evidence has to be checked. The tools used will depend on the verification method but the most common ones are hashes. Depending on the type of hash the proper functions will be used to recalculate the function and compare the result with the provided signature. Examples of these tools are `md5sum` and `sha1sum` (not safe anymore) or `sha256sum` utilities in Linux systems.

Next, depending on the nature of the evidence files, the adequate tools have to be chosen. In this scenario, as there are e-mail files involved, the two most common file formats are PST and mbox.

There are tools or libraries for dealing with both formats for example:

- For PST: `libpst`, `libff`, `pst2gmail`
- For mbox: `grepmail`, `mairix`

Also consider that the main forensic analysis frameworks such as OSForensics, Encase, Autopsy, etc... have built in capabilities to manage those formats so using one of them is also valid and, in many ways, advisable.

Once the adequate tools for working with the evidence have been selected the analysis has to be performed always over a copy of the original file to avoid evidence corruption.

Considering the context of the analysis, the investigator will be allowed to explore all the available data freely or to perform bounded searches related to the case. In case bounded searches have to be performed, the first step is to develop a keyword list related to the case and do searches only of the terms included in it. Always, every step along with its motivations has to be well documented.
7 Collecting cross border evidence

7.1 Introduction

The European project "Overview of existing legal framework in the EU Member States" carries out a study on the legal framework of the European Union, which analyses those points that may have in common the different jurisdictions of the EU member countries, to arrive to a common framework that can be applied in specific areas. Regarding digital evidence, the project points out that there is no comprehensive international or European legal framework specifically related to electronic evidence. The parties involved in an investigation rely on the national laws of the member states regarding the collection, preservation, use and exchange of electronic evidences. These national criminal laws were drafted years ago, and therefore at the time did not contemplate the existence of the Internet, new technologies and the derivate problems in the current scope and scenario. Some countries have been adapting their legislation to include such deployments, but others are based on traditional laws that also apply to electronic evidence. Therefore, there are great differences in each of the member states’ legislations, which make difficult the handling of transnational electronic evidences difficult. In certain countries, traditional investigation powers may be general enough to apply to the evidence. However, in other countries traditional procedural laws may not cover specific issues related to electronic evidence, which make additional legislation necessary. Admissibility rules exist in the Court in some countries, while in other countries eligibility may be flexible. There is no doubt that a clear scope of application of the powers and a sufficient legal authority is necessary to carry out the actions needed.

Although there is no comprehensive international or European legal framework related to electronic evidence, there is a series of legal documents and international and European legal instruments that are relevant to electronic evidence. One of the most relevant instruments is the European Investigation Order (EIO) introduced by the Directive 2014/41 to which this project refers. This instrument can be used to stimulate the exchange of digital evidence among member states, where with appropriate procedures, the evidence can be recognized in different courts from different member’s jurisdictions.

The EIO improves the existing EU laws that cover this field, since it establishes strict deadlines for the collection of the requested evidence. It also limits the reasons for rejecting such requests and reduces paperwork by introducing a single standard form for authorities to request assistance when they seek evidence.

7.2 The legal framework of e-evidence

As of today, there is currently not an adopted definition nor categorization at international or EU level that determines what the notion of electronic evidence (e-evidence) comprises in the field of criminal investigations.

On the 17 of April 2018 the European Commission (EC) proposed new rules in the field of cross border access to electronic evidence by police and judicial authorities (hereinafter the EC Proposals). The EC Proposals included a Regulation on European and Preservation Orders for electronic evidence in criminal matters and a Directive on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

In its impact assessment (IA of the EC Proposals) the EC acknowledges the existence of different types of e-evidence and proposes a conceptualization of the e-evidence based on existing legal definitions provided in instruments such as the Council of Europe Convention on Cybercrime and the e-Privacy regulation proposal. Consequently, the EC has opted for a flexible conceptualization of e-evidence based on typologies of data and the type of service provider that generates the data.
As an example, the Proposed Regulation on the Production and Preservation orders for electronic evidence (RPPO Proposal), defines e-evidence in the context of the instrument as “evidence stored in electronic form by or on behalf of a service provider at the time of the receipt of a production or preservation order certificate, consisting in stored subscriber data, access data, transactional data and content data (Article 2 of the RPPO Proposal).

The following scheme illustrates the definitions of the different types of data as identified in the RPPO proposal.

<table>
<thead>
<tr>
<th>Types of data</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content data</td>
<td>Any stored data in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data.</td>
</tr>
<tr>
<td>Subscriber data</td>
<td>Any data pertaining to:</td>
</tr>
<tr>
<td></td>
<td>a) the identity of a subscriber or customer such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone, or email;</td>
</tr>
<tr>
<td></td>
<td>b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of service, excluding passwords or another authentication means used in lieu of a password that are provided by a user, or created at the request of a user;</td>
</tr>
<tr>
<td>Access data</td>
<td>Data related to the commencement and termination of a user access session to a service, which is strictly necessary for the sole purpose of identifying the user of the service, such as the date and time of use, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the user of a service, data identifying the interface used and the user ID. This includes electronic communications metadata as defined in point (g) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications];</td>
</tr>
<tr>
<td>Transactional data</td>
<td>Data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, unless such data constitutes access data. This includes electronic communications metadata as defined in point (g) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications];</td>
</tr>
</tbody>
</table>

The explanatory memorandum of the RPPO acknowledges that all the types of data described above contain personal data and therefore are embraced by the safeguards offered by the EU legal framework (see section 3.1.2). This said the proposal considers a different treatment in terms of
conditions for access given the distinct impact the processing of types of data might have on the fundamental right of individuals.

7.3 Cross border evidence tools in EU members

The deliverable “First Evidence Exchange Application Prototype” of the European project “European Informatics Data Exchange Framework for Courts and Evidence” specifies some of the characteristics of the communication systems of Eurojust, Europol and Interpol.

As it is defined, these organizations have systems that run on top of secure networks. The secure dedicated lines that exist between these judicial and law enforcement organizations in Europe use VPN tunnels that are commonly used in other organizations and add a layer of security to information exchange systems. These systems are available only to authorized users. These organizations implement point-to-point data exchange systems defined below:

- In terms of networks, a secure network TESTA-NG (Trans European Services for Telematics between Administrations) is used and provided by the European Commission for organizations that must exchange information based on it. Each TESTA-NG node is encrypted and connected to the network that exchanges data with other nodes in the network.

- Eurojust also operates on TESTA-NG and has a secure network connection based on VPN to communicate with the judicial authorities of the member states. These communications are secure message delivery (email services), secure file transfer (SFTP), video streaming services, public key infrastructure and other data services.

- INTERPOL’s i-24/7 and I-link systems, provide communication links between law enforcement agencies in all member countries and are also based on VPN tunnels over leased lines.

- The SIENA system at EUROPOL is a message exchanging system similar to an e-mail system. It is accompanied by the Large File Exchange system, a secure file transfer service (SFTP) for large files and has also been deployed over a leased line. SIENA is available also to Eurojust as it is used as the integration of information exchange systems between Europol and Eurojust.

However, there is not a common platform that allows all member states implicated in the EIO to handle digital evidences in a simple and quick way. For this reason, a new platform aimed to be used by all members to share and transfer digital evidences is being developed.

7.4 eCODEX

As specified in the report "Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace", throughout several meetings, the majority of the Member States expressed the option to use e-CODEX as a tool for the secure transmission of data. For this reason, a specific project team is being created that includes representatives from all the Member States, since the establishment of the system requires (parallel) work by the Member States and the Commission. At a meeting held on March 13, 2017, the member states discussed the organization of the project and concluded that the system could be operational by the summer 2019. It is hoped that the creation of this platform, together with the form, will facilitate cooperation and the exchange of information between the judicial authorities of the Member States, allowing them to obtain electronic evidence more quickly and effectively, while meeting the necessary security requirements combined with friendly user interface.
The platform will allow identifying the relevant authority more quickly, completing the form more easily and transmitting it more quickly and safely, as is currently the case. In addition, the tool can be used to send back the requested evidence. In this way, the process should be faster and, to a certain extent, less complex and less resource-intensive. The use of the IT platform will also increase the transparency of the process, allowing the collection of statistics and improving information regarding its procedure. However, the benefits of these solutions will be limited to the EU Member States participating in the EIO. The process of mutual recognition, including deadlines, will not change, which means that the process will remain long and require more resources compared to direct cooperation with service providers.

Figure 155: e-Evidence system – proposed solution

7.5 EVIDENCE 2 e-CODEX

There is an ongoing project fruit of the evolution of the success of two prior projects that were co-funded by the EU: e-CODEX and Evidence. This project is led by the Italian National Research Centre (CNR) in partnership with 17 other organizations (including the European Lawyers Foundation and the Ministries of Justice of some Member States).

The EVIDENCE2eCodex project prepares interested parties to implement changes in the handling of electronic evidence and in the electronic exchange of such evidence.

The goal is to share with both legal and IT practitioners the availability of working instruments for digital cooperation in those European Investigation Order (EIO) cases that include digital evidence by:

- Create an instrument with legal validity to carry out digital evidence exchanges related to Mutual Legal Assistance (MLA) and EIO procedures through e-CODEX;
- Provide communities that deal with the legal and technological fields involved with ‘ready-to-use’ information on EIO, digital evidence and e-CODEX;
- Develop a case that serves as an example of how electronic evidence can be shared through e-CODEX in a secure and standardized way to support MLA and EIO cases;
• Develop a theoretical approach in "large file handling" first, if possible, followed by a specification for practical implementation, since digital evidence could come in "large size";

• Produce an action plan and guidelines for implementation at EU level of a "real life" example.

The project officially started on 15th February 2018 and will run for 18 months.
8 Best practices on gathering e-evidence abroad by using the EIO

8.1 Introduction

This chapter addresses legal aspects concerning the use of the EIO to obtain cross-border access to electronic evidence. The content of the best practices is greatly influenced on the input shared by practitioners and other individuals who participated in the events organized by LIVE_FOR.

It is not the purpose of this chapter, to provide a thorough analysis of the European Investigation Order as an instrument for judicial cooperation but again, to present a set a compilation of experiences, questions and answers exchanged by judicial and law enforcement from different Member States when willing to access e-evidence using an EIO.

8.2 Overview of the EIO

8.2.1 Background of the EIO

The Directive 2014/41/EU regarding the European Investigation Order (hereinafter EIOD) was adopted by the Parliament and the Council of the European Union on 3rd April 2014. From 22 May 2017, the Directive replaced the corresponding provisions of the following conventions applicable between the Member States bound by this Directive (art 34 of the EIOD)

a) European Convention on Mutual Assistance in Criminal Matters of the Council of Europe of April 1959, as well as two additional protocols, and bilateral agreements concluded pursuant to article 26 thereof

b) Convention Implementing the Schengen Agreement

c) Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and its protocol

In addition, the EIOD replaces the Council Framework Decision 2008/978 /JHA on the European Evidence Warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters and it also replaces those provisions of the Framework decision 2003/577/JHA regarding the freezing of evidence (see recitals 25 and 26 of the EIOD).

As of today (May 2018) Austria, Czech Republic, Luxembourg, and Spain have not yet adopted the Directive. On the other hand, Denmark and Ireland opted out from it adoption and as a result will continue to use Mutual Legal Assistance Treaties (hereinafter MLATs) to carry out judicial cooperation.

8.2.2 Definitions and main features of the EIO

As described in its explanatory memorandum the EIO aims to overcome the complexity and fragmentation, which the system of mutual legal assistance represents. It is supposed to do so by replacing with a single instrument the different rules and systems for the obtaining of all kinds of evidence.

Article 1.1 of the EIOD defines the EIO as “a judicial decision which has been issued or validated by a judicial authority of a Member State (“the issuing State”) to have one or several specific investigative measure(s) carried out in another member State (“The executing State”) to obtain evidence in accordance with this Directive”.
The EIO is therefore a judicial decision enforceable in the Union that is issued or validated by the judicial authority of a Member State and executed in another Member State on the basis of the principle of mutual recognition (Article 1 of the EIOD). As novelties the EIOD introduces a procedure of cooperation with deadlines, a standardised form and a determined number of grounds for which an executing state might refuse a request.

### 8.2.3 Judicial decision and judicial authorities

The EIOD Directive identifies as authorities capable of issuing and/or validating an EIO (Article 2(2) of the EIOD):

- Judges
- Courts
- Investigative judges and/or
- Public prosecutors competent in the case concerned

This is consistent with the CJEU’s interpretation of the term judicial authority according to which these “are not limited to designating only the judges or courts of a Member State, but may extend, more broadly, to the authorities required to participate in administering justice in the legal system concerned”.

Contrary to what occurs in the Council Framework Decision 2002/584/JHA on the European Arrest Warrant (hereinafter EAW), the EIO provides detail on the meaning and scope of the term “judicial authority”. By embracing not only to courts or judges, the EIO leaves the door open to be used by other authorities outside the judiciary, such as police, insofar a subsequent validation is performed by an authority identified as such in article 2.2 of the EIOD. In order to prevent that the validation proceeding turns into a purely bureaucratic and void procedure, the EIOD requires the issuing authority to perform an assessment of the necessity and proportionality of the investigative measure requested prior its submission.

As a result, flexibility in the form is compensated with scrutiny in its substance, by imposing the involvement of issuing authorities and its obligation to validate the observation of the conditions for issuance and transmission as stated in article 6.1 of the EIOD (Article 2.c (ii) of the EIOD). In particular, in its article 6 the Directive indicates that an EIO might only be submitted when:

a) It is **necessary** and **proportionate for the purpose** of the proceedings referred to in article 4 taking into account the rights of the suspected or accused person. According to the EJN contact Points, failure to comply with this requirement cannot, on a regular basis, represent a ground for refusal. If doubts concerning the necessity of the measures requested in the EIO, executing authorities should ask for clarifications and additional information to the issuing authority. The lack of detail in describing the offence or the wideness of the investigative measure requested might result in a question of proportionality and necessity.

b) The investigative measure (s) indicated in the EIO **could have been ordered** under the same conditions in a similar **domestic case**.

### 8.2.4 Mutual recognition and grounds for return, recourse and refusal:

While based on the principle of mutual recognition, the EIO also incorporates the flexibility of traditional system of MLAT (Recital 6 of the EIOD) and thus the executing states enjoys margin of
manoeuvre when receiving a request via an EIO. In particular, the Directive offers the executing authority the possibility to:

a) Return the EIO to the issuing state in those cases where an executing authority receives an EIO which has not been issued by an issuing authority from those specified in Article 2 (c) (Article 9(3) of the EIOD).

b) Recourse to a different type of investigative measure from that requested (Article 10 of the EIOD) in those cases where:
   a. The investigative measure does not exist under the law of the executing state
   b. The investigative measure would not be available in a similar domestic case

c) Not-recognise or not-execute the measure when it refers to one of the listed grounds that allow doing so. In its article 11 the EIO identifies the following grounds to refuse execution:
   a. Immunity or privilege under the law of the executing state
   b. National security interests
   c. The EIO does not relate to a criminal proceeding and the investigative measure would not be authorised in a similar domestic case.
   d. Its execution would be against the principle of ne bis in idem.
   e. The conduct on which the EIO is issued is not an offence in the Executing State
   f. Substantial grounds to believe its execution is incompatible with fundamental rights and legal principles shrined in article 6 TEU and the Charter.39
   g. The conduct for which the EIO is issued is not one of the 32 listed in Annex D and does not constitute an offence under the law of the Executing State.
   h. The use of investigative measures indicated in the EIO is restricted to a list or category of offences in the Executing State, which does not include the offence covered by the EIO.

8.2.5 Scope and electronic evidence

The EIOD is applicable to any investigative measures directed to the gathering of any type of evidence, including electronic evidence (hereinafter e-evidence), in criminal proceedings, except for in the case of joint investigation teams (Article 3 of the EIOD).

The Directive provides for specific rules for e-evidence in two cases:

- Requests for the identification of persons holding a subscription of a specified phone number or IP addresses (article 10.(2).e of the EIOD).40
- Requests of interception of telecommunications (Article 30 of the EIOD).

By criminal proceedings the EIOD refers to those that are brought by judicial and administrative authorities. In case of the latter, this will only apply insofar they give raise to proceedings before courts with criminal jurisdiction (Article 4 of the EIOD).

8.2.6 Deadlines

The EIOD establishes a principle of celerity and equivalence of priority to domestic cases for the recognition and execution of EIO requests (Article 12 of the EIOD). The obligation to address both actions is delimited in two stages:
• Upon receipt of the EIO, the executing authority has 30 days for its recognition.
• Once lapsed that first period, the executing authority then has 90 to carry out its execution.

In regard to provisional measures article 32(2) states that the executing authority shall decide and communicate a decision within 24 hours of receipt of the EIO.

Whenever the seriousness of the offence or other particularly urgent circumstances requires it, issuing authorities might request that such time limits to be shortened (Article 12(2) of the EIOD). However, this will remain at the discretion and capacity of the executing authority (Article 12. (5) and 12(6) of the EIOD).

In the context of requests for access of e-evidence stored by service providers, once the executing authority has received the order and recognise it within the 30 fist days, then it has 90 more to forward a domestic production order to the service provider under its national legal framework. At that point the service provider will collect the evidence and send it back to the executing authority, which after reviewal of the evidence obtained, can re-assess the suitability for its transmission to the issuing state.

8.3 Relation to other instruments

The EIO substitutes the conventions referred in article 34 of the EIOD, but only regarding the “corresponding provisions” found in that specific convention and without any further explanation on which are those provisions (art 34 of the EIOD). It is therefore unclear the way in which the EIO articulates with the rest of conventions on those clauses not strictly replaced by the EIOD.

Furthermore, in regard to countries in the EU that are not signatories of the EIOD the specific applicable instruments will need to be assessed. Consequently, authorities from member states bound by the EIO should consider its use jointly with other MLAT mechanisms:

8.3.1 Instruments of judicial cooperation

<table>
<thead>
<tr>
<th>Requests between signatory parties of the EIO Directive</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The Benelux Treaty 1962</strong></td>
<td><strong>Scope</strong>: Treaty concerning extradition and mutual assistance in criminal matters between the Kingdom of Belgium, the Grand Duchy of Luxembourg and the Kingdom of the Netherlands.</td>
</tr>
<tr>
<td></td>
<td><strong>Reference to e-evidence:</strong></td>
</tr>
<tr>
<td></td>
<td>- No explicit reference</td>
</tr>
<tr>
<td><strong>Naples II Convention of 1997</strong></td>
<td><strong>Scope</strong>: Convention on close cooperation between EU customs administrations.</td>
</tr>
<tr>
<td></td>
<td><strong>Reference to e-evidence:</strong></td>
</tr>
<tr>
<td></td>
<td>- No explicit reference</td>
</tr>
<tr>
<td></td>
<td>- Could be used jointly with the EIO in specific cases, by requiring customs to seize a property which might contain e-evidence.</td>
</tr>
<tr>
<td><strong>The Benelux Police Treaty 2004</strong></td>
<td><strong>Scope:</strong> concerning cross-border police intervention</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td><strong>Reference to e-evidence:</strong></td>
<td><strong>No explicit reference</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Council Framework Decision 2006/960/JHA of 18 December 2006</strong></th>
<th><strong>Scope:</strong> Decision simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reference to e-evidence:</strong></td>
<td><strong>No explicit reference</strong></td>
</tr>
<tr>
<td></td>
<td><strong>See article 2(d) on the definition of intelligence.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Council Decision 2008/615/JHA of 23 June 2008 (Prüm)</strong></th>
<th><strong>Scope:</strong> Decision on cross-border police and judicial cooperation between European Union (EU) countries in criminal matters.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Electronic-evidence:</strong></td>
<td>The instrument comprises the exchange of information regarding: i) the automated access to DNA profiles, dactyloscopic data and certain national vehicle registration data; ii) supply of data in relation to major events; iii) supply of information in order to prevent terrorist offences; iv) other measures for stepping up cross-border police cooperation</td>
</tr>
</tbody>
</table>

### Requests by Member States party of the EIOD to Denmark or Ireland

<table>
<thead>
<tr>
<th><strong>Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union</strong> and its Protocol 2001.</th>
<th><strong>Status:</strong> In force, only relevant regarding requests issued to Denmark</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope:</strong> to supplement the provisions and facilitate the application between the Member States of the European Union, of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and its additional protocol and the provisions on mutual assistance in criminal matters of the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985</td>
<td><strong>Reference to e-evidence:</strong> While the EU 2000 Convention does not have any specific provision concerning e-evidence it might be relevant insofar its purpose is to foster Member States assistance in criminal matters, which indirectly might also include e-evidence.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Council of Europe European Convention on Mutual Assistance in Criminal Matters from 4 April 1959 + Protocol 1978</strong></th>
<th><strong>Status:</strong> In force, only relevant regarding requests issued to Ireland.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope:</strong> The Contracting Parties undertake to afford each other, in accordance with the provisions of this Convention, the widest measure of mutual assistance in proceedings in respect of offences the punishment of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting Party (article 1.1).</td>
<td><strong>Electronic-evidence:</strong> No specific provision, on the other hand, the convention allows the Member Parties to request by means of rogatory letters the production of evidence under specific requirements.</td>
</tr>
</tbody>
</table>

| **Schengen Implementation Convention 19 June 1990** | **Scope:** Based on that provided in the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at their common borders. The Convention aims to fulfil the resolve expressed in that Agreement to |

---

1. Scope: concerning cross-border police intervention
2. Reference to e-evidence: No explicit reference
3. Scope: Decision simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.
4. Reference to e-evidence: No explicit reference
5. Scope: Decision on cross-border police and judicial cooperation between European Union (EU) countries in criminal matters.
6. Electronic-evidence: The instrument comprises the exchange of information regarding: i) the automated access to DNA profiles, dactyloscopic data and certain national vehicle registration data; ii) supply of data in relation to major events; iii) supply of information in order to prevent terrorist offences; iv) other measures for stepping up cross-border police cooperation
7. Status: In force, only relevant regarding requests issued to Denmark
8. Scope: to supplement the provisions and facilitate the application between the Member States of the European Union, of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and its additional protocol and the provisions on mutual assistance in criminal matters of the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985
9. Reference to e-evidence: While the EU 2000 Convention does not have any specific provision concerning e-evidence it might be relevant insofar its purpose is to foster Member States assistance in criminal matters, which indirectly might also include e-evidence.
10. Status: In force, only relevant regarding requests issued to Ireland.
11. Scope: The Contracting Parties undertake to afford each other, in accordance with the provisions of this Convention, the widest measure of mutual assistance in proceedings in respect of offences the punishment of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting Party (article 1.1).
12. Electronic-evidence: No specific provision, on the other hand, the convention allows the Member Parties to request by means of rogatory letters the production of evidence under specific requirements.
13. Scope: Based on that provided in the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at their common borders. The Convention aims to fulfil the resolve expressed in that Agreement to
abolish checks at their common borders on the movement of persons and facilitate the transport and movement of goods at those borders

**Electronic-evidence: No explicit reference**
The Convention contemplates the obligation by the member states to assist each other for the purposes of preventing and detecting criminal offences (Article 39). Despite it does not explicitly refers to e-evidence the, the Convention establishes a tool for police cooperation, the Schengen Information System (SIS), and a secure system for the exchange of police information.

---

**Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence**

**Status:** In force, only relevant regarding requests issued to **Ireland**.

**Scope:** The purpose of the Framework Decision is to establish the rules under which a Member State recognise and execute in its territory a freezing order issued by a judicial authority of another Member State in the framework of criminal proceedings (Article 1 of the FD).

**Electronic-evidence:** the instrument only refers to the preservation of existing evidence, it thus cannot be used to produce e-evidence that is unknown to the issuing state.

---

**Requests issued by MS bound by the EIO to Norway, Iceland, Switzerland, Liechtenstein**

- Council of Europe European Convention on Mutual Assistance in Criminal Matters from 4 April 1959 + Protocol 1978
- Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union and its Protocol 2001: only relevant regarding requests issued to **Norway and/or Iceland**.
- 19 June 1990
- Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union (without the protocol): only relevant regarding requests issued to **Switzerland and/or Liechtenstein**

---

**8.3.2 Privacy and protection legal framework to cross border access to data and e-evidence**

The access by law enforcement to personal data represents an interference with the right to privacy as described in article 7 of Charter of Fundamental Rights of the European Union (hereinafter the Charter) and with the right to the protection of personal data guaranteed by article 8 of the Charter. Pursuing article 52(i) of the same instrument, any limitation on the exercise of the rights and freedoms recognised in the Charter must 1) be provided by law, 2) respect the essence of those rights and freedoms, 3) be subject to the principle of proportionality and 4) be necessary and genuinely meet the objectives of general interest recognised by the EU.

The limitations of the rights to privacy and data protection for data processed by service providers offering services such as electronic communication services, information society services are contemplated in the EU legal framework:

- Article 23 of the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**General Data Protection Regulation, GDPR**).
• Article 15 of the Directive 2002/58/EC (ePrivacy Directive) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)\textsuperscript{53}.

Data protection in the police and criminal justice sector is specifically subject to the regime established by the Directive (EU) 2016/680 (Police Directive) concerning the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

8.3.3 Council of Europe instruments relevant to cross border access to data and e-evidence

Besides EU legislation the Council of Europe provides instruments that might also be relevant to the cross-border access and exchange of e-evidence by EU Member states, especially given the fact that as has been stated, not all Member States have yet transposed the EIO Directive\textsuperscript{55}. In that regard, of particular relevance is the Council of Europe Convention on Cybercrime\textsuperscript{56} (hereinafter Budapest Convention), which harmonizes criminal substantive elements in the area of cybercrime, sets out domestic procedural measures to investigate and prosecute criminal offences (Article 2 and 11 of the CC) and determines the safeguards and conditions how investigations and prosecution ought to be carried.

Under the Budapest convention country members are obliged to adopt legislative and other measures necessary to establish the powers and procedures governing the offences referred in the Convention and for the collection of e-evidence (Article 14 of the Budapest Convention)\textsuperscript{57}.

These powers and measures are at the same time subject to conditions and safeguards ensuring an adequate protection of human rights and liberties as described in the Council of Europe European Convention on Human Rights\textsuperscript{58} (hereinafter ECHR) while also take into account the principle of proportionality (Article 15 of the Budapest Convention).

In particular the Budapest Convention includes the following cross border access measures relevant to e-evidence:

- Expedited preservation of stored computer data (Article 16)
- Expedited preservation and partial disclosure of traffic data (Article 17)
- Production order (Article 18)
- Search and seizure of stored computer data (Article 19)
- Real-time collection of traffic data (Article 20)
- Interception of content data (Article 21)

According to article 23 of the CC, the Parties are bound to “co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.”\textsuperscript{59}

All EU member States are signatory parties of the Budapest Convention; however, Ireland and Sweden have not ratified it. To that effect, from the two MS that opted out from the EIO, access requests to Denmark can be performed on the basis of the Budapest Convention while in the case of Ireland that would not be case and thus, will need to rely on Council of Europe European Convention on Mutual Assistance in Criminal Matters from 4 April 1959 and its Protocol from 1978\textsuperscript{60}.
Relation of the Budapest Convention (CoC) and the EIO

The relation between these two legal instruments (EIO Directive and CoC) is considered as essential for mutual cooperation between member states in cases that involve digital evidence.

It is clear that the relation between the EIO Directive and other bilateral and multilateral legal instruments is addressed in the article 35 of the EIO Directive, according to which such legal instruments may continue to apply in cases when especially they strengthen the aims of the Directive, simplify or facilitate gathering of evidence and provide sufficient level of safeguards in performing these acts. All three conditions specified in the art. 29 of the CoC are met in relation to the EIO article 32. This suggests that countries should follow procedures laid down in the art. 32 of the EIO Directive, as the approach is introducing higher effectiveness in cases when the rules from the art. 29 of the CoC apply. However, in cases where these two provisions may be contradictory, the Directive should apply and the Directive article should have higher priority.

Another consequence of the existence of art. 29 of the CoC is that all states that are implementing this Convention should be able to respond to the freezing order issued pursuant to the art. 32 of the Directive, since provisions allowing such procedural measure have to be already in place.

8.4 Services providers, e-evidence and the EIO

A recurrent discussion during the LIVE_FOR workshops refers to how data requests to private companies offering internet services in the EU are carried. In order to gather e-evidence within the EU, police and judicial authorities can either use traditional judicial cooperation tools such as the EIO and MLATs or rely on the direct cooperation with service providers. The following section will address access requests directly addressed to service providers.

8.4.1 What kind of services do service providers offer when it comes to e-evidence?

National criminal courts are not bound to the definitions offered in the EU directives. In this respect, in the Yahoo! v Belgium case the Belgian Supreme Court (Court de Cassation) by judgment on 18 January 2011 provided an autonomous interpretation the notion of service provider of electronic communications based on the Belgian Code of Criminal Procedure (BCCP). This position, which was later on ratified also by the Court de Cassation in 2015, considered that the BCCP had to be interpreted in a broader sense than that set by e-Privacy Directive and defined a provider of electronic communication service as “anyone that provides services of electronic communications, including among other things the transmission of communications data”.

The argument was also sustained by the Correctional Court of Mechelen (also in Belgium), which considered that Skype qualified as an Electronic Communication Service provider insofar it provided “a software that supports communications over the internet.”

The recent European Commission’s Directive Proposal on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, offers a structured description of service providers in the context of criminal investigations. In that regard, article 2(2) of the proposed Directive defines service providers as any natural or legal person that provides one or more of the following categories of services: i) electronic communications services; ii) information society services; iii) internet domain name and IP numbering services such as IP address providers.

- Electronic communication services (ECS): the definition distinguishes between providers of three types of services:
  - Internet access service means a publicly available electronic communication service that provides access to the internet, and thereby connectivity to virtually
end points of the internet, irrespective of the network technology and terminal equipment used (Article 2(2) of the Regulation (EU) 2015/2120).

- **Interpersonal communications service (ICS):** Interpersonal communications services are services that enable interpersonal and interactive exchange of information, covering services like traditional voice calls between two individuals but also all types of emails, messaging services, or group chat. At the same time, ICS comprise two categories of ICS: i) Number Based (N-B ICS) and ii) Number-Independent.

- **Services consisting wholly or mainly in the conveyance of signals,** including telecommunications services such as transmission services in networks used for the provision of machine-to-machine services and broadcasting. With respect to machine-to-machine (M2M) communications the status quo is confirmed and clarified: only the transmission element continues to fall within the scope of the ECS definition whereas M2M services at the applications layer remain outside the scope.

- **Providers of information society services** embrace “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services,” for which the storage of data is a defining component of the service provided to the user such as social networks, online marketplaces and other hosting service providers (Article 2 (2) b of the Proposal Directive).

- **Providers of names and numbering services for the internet** such as IP addresses, domain name registries, domain name registrars and related privacy and proxy services. (Article 2 (2) c of the Proposal Directive)

### 8.4.2 Is direct cooperation with service providers considered voluntary or mandatory?

Daily practice shows that criminal investigations more often than not rely on reaching service providers outside the framework of MLAT’s or mutual recognition instruments. Member States have different approaches when it comes to consider the obligation of service providers established in another country to comply with a request carried by their own national authorities.

- **Voluntary:** Austria, Romania, Sweden, Hungary, Netherlands, Greece, Czech Republic, Denmark, Finland, Slovenia, Italy, Estonia, Luxembourg, Malta, Bulgaria.
- **Mandatory:** Belgium, Cyprus, Spain, Portugal, United Kingdom, France, Lithuania.

When data is requested under an EIO or MLAT’s instruments, the solicitude is carried between two public authorities, conversely, in the case of direct cooperation with foreign service providers the dialogue is between a public and a private entity. As a result, it results questionable private parties’ obligations concerning deadlines, form of execution or confidentiality.

It is also worth noting that a great number of member states do not provide a legal basis for service providers established in their territory to respond to direct requests of law enforcement authorities from another EU member State. Only the domestic law of Spain and France permit such direct cooperation between a service provider established in their territory and law enforcement from other EU member states. The lack of a specific legal framework for these requests, either from the requesting state and from that of the requested state, results in legal controversies when it comes to enforcement, even in those cases when the cooperation from the service provider is considered mandatory by the requesting authority.

A prominent example of this issue can be found again in the case Yahoo v Belgium, where the Belgian Cassation Court understood that the failure to comply by Yahoo! (a company based in the
U.S.) with the petition made by Belgian authorities represented an offence committed on the Belgian territory and thus was subject to punishment in accordance with the provisions of the Belgian Laws. The Court stated that "the criminal offence established in article 46bis, § 2, section 4 of the Code of Criminal Procedure, [was] committed at the place where the requested information must be received". In that line, the Court considered that the failure to comply with a request enforced compliance with the measure took place in Belgium and thus its sanctioning needed to be understood purely in domestic terms.

To further ground the relation between the company and the Belgian jurisdiction, the Court held that Yahoo actively participated in the economic activity of Belgium as it used national domain names (“www.yahoo.be”), the localisation of service language, the targeted advertising based on the location of the users of its services and finally that the service was accessible for those users in Belgium.

8.4.3 Admissibility of e-evidence obtained through voluntary cooperation

Depending on national legislations, evidence obtained via voluntary cooperation with service providers located in another Member States might have its admissibility at Courts challenged. This will depend on the specific provisions of the national legislation from the specific Member State requesting the data.

The majority of Member States do not constrain admissibility to the existence of legal provisions specifically allowing it, this is the case of: Austria, Romania, Hungary, Belgium, Cyprus, Ireland, Denmark, Spain, Finland, Portugal, Italy, Estonia, France, Luxembourg, Malta, Sweden. Conversely Poland, Greece, United Kingdom and Bulgaria do not allow it by domestic laws. In the cases of Romania, Slovakia, Netherlands, Lithuania, Czech Republic, Germany, Slovenia, admissibly is subject to stringent conditions.

8.4.4 Legal nature of Internet protocols

In its judgment of 19 October 2016 in the Court of Justice of the European Union (CJEU) dealt with the issue of legal nature of Internet Protocol addresses (IP addresses). The Court first defined IP addresses as “series of digits assigned to networked computers to facilitate their communication over the internet (paragraph15). It then drew a distinction between two types of IP's, namely dynamic and static IP addresses:

- **Static IP addresses**: series of digits permanently allocated to a particular network interface of a particular device.
- **Dynamic IP addresses**: dynamic IP are a series of digits temporally assigned to a device by the ISP, typically each time the device connects to the Internet.

The main difference between static and dynamic IP addresses relies on the fact that dynamic IP’s change each time a new connection to the internet is performed. Consequently, while in the case of static IP addresses there is no doubt on the personal character of the data, obtaining information from dynamic IP addresses had been often regarded as to be less sensitive and thus accepted that its access is less restrictive. In relation to that, the Court acknowledged that dynamic IP addresses cannot be regarded on its own as personal data, insofar it does not directly reveal the identity of the natural person or person(s) using a specific device at the time an internet access occurs (paragraph38). However, the CJEU considered that dynamic IP addresses, when combined with additional data hold by ISPs, could be indeed regarded as data relating to an “identifiable natural person” in light of article 2 of the Data Protection Directive 95/46.
In that regard, the CJEU concluded that “a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.”

IP addresses enable law enforcement authorities to obtain valuable information for their investigations such as the location of Internet Service Provider to which a user is connected. In the case of dynamic IP addresses, while they do not allow to trace a specific computer, they can lead to requests to ISP’s to provide the personal information of the subscriber using them at a specific time. As a result, insofar IP addresses either dynamic or static are considered personal data, they will require the issuance of a warrant for its production.

In a similar vein, the European Court of Human Rights has recently ruled that requests for subscriber information linked to dynamic IP addresses are susceptible of raising privacy issues capable of engaging the protection of article 8 of the Convention. In that regard in Benedik v Slovenia the Court stated that the obtaining by the police, without a court order, of subscriber information associated with the dynamic IP address in order to connect the computer usage to a location and, potentially, to a person, falls with the scope of the notion of “private life” as provide in Article 8 of the ECHR.

8.5  Guide on the EIO form, Annex A

8.5.1  Section A: Involved states

Section A demands the involved member states.

8.5.1.1  Issuing state

You can check the implementation of the EIO Directive in your national law here: EJN table of implementation.

Regarding to the responsibility of your authority for issuing EIOs within in your domestic system, watch your national law implementing the EIO directive.

8.5.1.2  Executing state

First prejudice for using the EIO is the implementation of the Directive in the requested state. As the time limit of implementation is expired in May 2017, you can issue investigative measures in all EU member states which opted into the directive. Only Denmark and Ireland opted out.

Several member states have not implemented the EIO Directive yet. Nonetheless, you can issue investigative measures in these member states by using the EIO form. Those countries will treat your EIO like Mutual Legal Assistant requests, thus the internal procedures in the executing states will not comply with the EIO directive.

The current state of implementation in the executing state can be found in the aforementioned table provided by EJN.

If you contact a country which is no EU member state, you cannot use the instrument of the EIO. For this purpose, check if you have any bilateral agreements or international agreements signed by both your country and the requested country, e.g. for the gathering of e-evidence the Budapest Convention on Cybercrime.
8.5.2 Section B: Urgency

8.5.2.1 Grounds for urgency

Regarding to Article 9 of the EIO directive, the executing authority has to recognise the receipt of the EIO and executing it as it would be a national case. The investigative measures should be carried out with the same celerity as in a national case. Therefore, the issuing state can request an urgent execution of the issued measures if the issuing authority names reasonable grounds for the urgency. One possible ground for urgent action is the risk of the destruction of evidence. In cases of electronic evidence and its characteristics of short time availability, requesting urgent execution can be called appropriate to ensure e-evidence will not be destroyed before.

8.5.2.2 Best practice

Nonetheless, the urgency of measures aiming or the gathering of e-evidence, is not given by default due to its nature.

The assessment of the priority of the issued measure has to take the concrete case in particular into consideration. Therefore, make sure to specify within section B why urgency is particularly in your case needed naming the risks of which e-evidence could be destroyed when and what the impact on your case would be. Of course, repeating the same reasons for every EIO, might not help to induce to that urgency.

8.5.3 Section C: Investigative measure(s) to be carried out

The EIO is deliberately wide ranging in order to take into account the differing roles of the Law Enforcement Authorities in the various European Union member states. According to Article 3 EIO Directive, the EIO shall cover “any investigative measure” except for measures listed in Article 3 EIO Directive.

The EIO makes specific reference to a number of investigative measures. However, some of the measures could be not available to your country because your own domestic law does not allow for it.

Generally speaking, you can ask for anything that you can lawfully do in your country. If any measure can be lawfully authorised under your domestic law, you can now ask for it to be carried out in another participating state. However, some measures such as the interview of a willing witness can be catered for under police cooperation in most countries and it is favourable to use this route in the first instance on the occasions that it is available in your specific case.

8.5.3.1 Description of the required measures

Fill in the free field boxes describing the envisaged measures.

8.5.3.2 Ticking boxes

Additionally, search for the relevant measure(s) in the list and tick the boxes.

8.5.3.3 Best practice: Relation description/boxes

How to complete the form: The form cannot be altered: Some of your colleagues might be tempted to delete or modify the form. That is not how the form works. The titles and sections shall be left as they are, for the specific reason that the form is common. Therefore, deletion of certain gaps or boxes is not allowed.

How to fill section C: The filling of the section C can be done with bullet points. Describe what measure you would like to request the executing state to execute. In case the requested measure also appears as one of those listed in the list of measures you should also tick the adequate box.
8.5.3.4 **Best practice: Banking information**

Requesting banking information: You should include certain information which might be relevant for the execution or the gathering of information. For instance, for banking information, you would ask for the identification of an account number. Additionally, you would request information about the transactions within a certain period of time, also including if you need both incoming and outgoing transactions or only one of both. Ask for all the beneficiaries of the account or existence of power of attorneys for that bank account. Specify your requested as much as possible to receive the relevant evidence.

8.5.3.5 **Best practice: Provisional measures**

From a legal point of view, you can use the EIO for provisional measures like freezing of data, email accounts or telecommunication data. For transferring the frozen e-evidence, you must send a second EIO to the executing state which takes the legal requirements of your own country into account, especially if the approval of a judge is prescribed. Hence, the last box of Section C can be ticked in case of preliminary requests for provisional measures.

Many practitioners do still rely on the Budapest Convention on Cybercrime of the Council of Europe from 2001. This international treaty serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty.

Procedures of the Budapest Convention under article 29 – Expedited preservation of stored computer data are well implemented and highly efficient in several EU member states when quick freezing of stored data is needed. Additionally, next to the EU member states, further countries like the US have ratified the Budapest Convention. Therefore, make sure to check if well working procedures under the Budapest Convention are implemented in your country and take into consideration to use this instrument in case of needed expedited preservation.

8.5.3.6 **Necessity and proportionality assessment**

Furthermore, explain the necessity and proportionality assessment for requesting a specific measure:

For instance, if you request email content, always include the following information:

- Why do you need the content?
- Why is it necessary to receive that information?
- Why is it proportional to access the emails?

There is a lot of evidence gathering that might require the assessment of an investigative judge. The prosecutor will request the judge’s permission to access data, intercept or any further measure and attach the decision to the EIO. Take into consideration, that prosecutors can ask for some information, but many information are exclusively decreed by judges.

8.5.4 **Section D: Relation to an earlier EIO**

8.5.4.1 **EIO supplementing an earlier EIO**

Especially in large cases, you might issue several measures over a longer period. Therefore, you must make sure that you refer to an earlier EIO by filling in Section D.
8.5.4.2 EIO addressed to another MS in the same case

Furthermore, you might contact various countries within one case. Also state the involvement of other states in Section D. Take into consideration to use European coordination possibilities by reaching out to your national contact point of the European Judicial Network (EJN) or your National Desk at Eurojust (especially if you consider using Coordination Meetings or Coordination Centres).

8.5.5 Section E: Identity of the person concerned

Section E asks for detailed information about the person(s) concerned.

8.5.5.1 Best practice: How far to go into detail?

The issuing authority must provide the executing authority with detailed and complete information about the person who the measures identified in the EIO are addressed to. Every detail is important as the related instrument of the EAW has shown (both instruments are based on the principle of Mutual Recognition).

Note: Legal persons might also be the target of an EIO, if they are involved in the criminal activities. It is therefore important to define the status of legal persons, for instance companies, pointing out if they are witnesses or suspects in the specific case.

8.5.5.2 Best practice: Special requirements if executing state shall request ISPs

For facilitating the work, whenever possible the issuing authority should provide the address of the companies the measure will affect, especially when speaking about ISPs. If the issuing authority knows the ISP and its contact information, such information should be mentioned in the form.

8.5.6 Section F: Type of proceedings for which the EIO is issued

8.5.6.1 Meaning of the different types

Section F names four different types of proceedings the EIO can be issued in. The standard ticked box in criminal investigations will be box a).

8.5.6.2 Best practice: Examples when not to tick box a)

Criminal and Administrative proceedings: It is important to remind that most of the time the EIO is used to issue measures in criminal investigations but in other countries it can also be used for administrative/further minor criminal issues. Hence, the EIO allows to be issued for other matters rather than criminal investigation.

Such a different matter can be found for instance in the German preventive law: in cases that the German police has information but does not have enough to launch a criminal investigation there is a special law (preventive law), on the basis of which investigations can be initiated. The nature of those would be considered administrative.

8.5.7 Section G: Grounds for issuing the EIO

Section G is one of the most important sections of the EIO form. Compared to the former rogatory letters, this section is the main part, which should be structured and minimised to the relevant information about the criminal proceedings. The issuing state needs to argue why the issued measure must be executed by referring to its domestic law.

8.5.7.1 Summary – What to include

Section G.1 names the following points which must be included:
• summary of the underlying facts
• a description of offences charged or under investigation
• the stage the investigation has reached
• the reasons for any risk factors
• any other relevant information

Provide the executing state with an efficient overview of your criminal investigations carried out so far. Explaining the background briefly, do not go too much into detail if it is not relevant. Describe the charged/investigated offences carefully.

8.5.7.2 Legal classification and list of offences

Name the legal classification of the offence(s) under your domestic law.

Additionally, you have to tick the relevant boxes in Section G.3, if the offence can be subsumed under one of the listed points. All named offences will be punishable in the issuing state by a custodial sentence or detention order of a maximum of at least three years under most of European Member states’ law systems. Thus, the dual criminality in both countries, the issuing and executing, is ensured.

8.5.7.3 Grounds for refusal, article 11 (1) EIO directive

Additionally, purpose of this section is also to check, if there is any ground for refusal according to article 11 (1) EIO directive. Most relevant grounds for refusal are:

• Non bis in idem, article 11 (1) (d) EIO directive

National courts cannot proceed against the responsible parties of crimes within in the other member state’s jurisdiction if the second state’s tribunal has already pronounced sentence for the same crimes.

• Breach of fundamental rights, article 11 (1) (f) EIO directive

Article 11 (1) (f) EIO directive refers to article 6 TEU and the Charter of Fundamental Rights. Article 6 TEU constitutes the principles of respecting human and fundamental rights. Therefore, an issued measure can be refused, if the execution would be a breach of fundamental rights. Highly relevant is for instance the right to privacy and data protection, article 7 and 8 of the Charter. Infringements of the right to privacy and data protection have to be justified according to the data protection legal framework, paying special attention to the Police and Justice Data Protection Directive82. The EIO directive prescribes the need of a legal implementation of the EIO directive from a data protection point of view referring to the former data protection legal framework of the EU and the CoE in article 20. As the new data protection legal framework, including GDPR and Police and Justice Directive, comes into force on 25th of May 2018, member states must follow these advanced legal provisions.

• Dual criminality, article 11 (1) (g) EIO directive

Offences must be punishable under the domestic law of the executing state under the conditions named in article 11 (1) (g) EIO directive. If the offence is listed in annex D of the EIO directive, dual criminality can be reasonably assumed.

• Costs, article 21 EIO directive
If costs exceed the normal appropriate amount, the executing authority should contact the issuing authority for negotiations about cost sharing.

**8.5.7.4 Speciality of article 10 EIO directive**

Whenever the requested measure does not refer to those listed in section G.3 of 32 crimes, the executing state is entitled to refuse performing the measures. However, according to article 10 there are some measures that cannot be refused in any circumstance, such as the identification of phone numbers and IP addresses.

**8.5.8 Section H: Additional Requirements for certain measures**

Section H lists several measures which require additional notification responsibilities, certain information or further details to be followed. For the specific purpose of this document, section H.3. is the most relevant one.

**8.5.8.1 Section H.3: provisional measures**

If the issuing authority requests the freezing of money, it will have to choose whether the same is to be used as evidence or for confiscation purposes.

For realising the money freezing, the specific section on information on bank accounts and financial information must be filled in.

**8.5.8.2 Interception of communications**

If it comes to the measure of intercepting telecommunications, first consideration is whether technical assistance of the executing state is needed to realise the interception.

If assistance is needed, this state has to issue the measure via the EIO by using the normal procedure.

If technical assistance is not required, the state has to notify the other member state that would be normally involved in the interception or that is attempted to intercept communications of a target that is in its territory. For such a notification ANNEX C of the EIO directive must be used.

**8.5.9 Section I: Formalities and procedures requested for the execution**

Certain measures may require certain formalities and procedures, for instance times of searching of suspects’ homes, deletion responsibilities within interception of communications, protection of maximum privacy or further specialties of national codes of procedural criminal law. Those formalities shall be listed and well explained in section I to ensure the recognition of all evidence in front of court in the end of the criminal proceeding.

**8.5.10 Section J: Legal remedies**

Suspects have the right to ask for legal remedies during the whole investigations. This means, that both, legal remedies of the issuing and the executing states are available for the suspect. Therefore, all involved authorities and states have transparently to inform the suspect about what legal remedy can be provided in the specific country.

**8.5.11 Section K: Details of the authority which issued the EIO**

Tick the type of authority which issued the EIO. Issuing authority is any judicial authority in compliance with article 2 of the EIO directive, which is defined by the domestic law of the issuing state.
8.5.12 Section L: Details of the authority which validated the EIO

Name the authority which validated the EIO.

For questions about the impact of the function of the validating authority on the validity of the evidence gathering of evidence, especially if it is a different authority from that allowed to carry out the procedures that in the issuing state, check point 3.3.: (Section C) of the document.

8.6 Guide on the EIO form, Annex B

Purpose of annex B of the EIO directive is the confirmation of the receipt of an EIO by the executing state. Required information for confirmation are details about the time of reception of the EIO, the receiving authority, (if applicable) the competent authority the EIO has been transmitted to and (if needed) further information for the issuing authority.

8.6.1 Time limits

One of the core improvements of the EIO directive are new time limits for recognition as well as execution. According to article 12, time limits and conditions are:

- An EIO should be treated with the same celerity as domestic cases. (article 12 (1) EIO directive).
- Shortening of time limits are possible under specific conditions listed in article 12 (2) EIO directive
- 30 days to decide on the recognition or the execution of the EIO. (Need for decision on recognition depends on the domestic law/implementation law of the EIO directive.) (article 12 (3) EIO directive).
- Time limit can be extended for another 30 days under the conditions of article 12 (5) EIO directive.
- Execution of the issued investigation measures must be carried out without delay, no later than 90 days after the decision about recognition or execution. (article 12 (4) EIO directive).

Starting point of the time frame is the receipt of the competent executing authority: Therefore, domestic proceedings in the executing state transmitting the EIO does not count into the time frame.

8.6.2 Failure of meeting time limits/Best practice

If the executing member states does not meet the aforementioned time limits, for the time being no consequences are apparent.

Nonetheless, experts’ experiences show, that the timeframes are doable and considered as an huge improvement of the EIO. Additionally, also the direct contact between authorities via annex B of the EIO directive provides enhancement.

What happens when the executing state argues that there are no resources to execute the EIO?

The best option for the issuing authority would be to raise a case to Eurojust via its national desk. The issuing state could request to prioritise the evidence considered more volatile.
If there is no other way, an alternative could be to request to secure the evidence under the Budapest convention. Possibly, it would not be the same executing authority, as it would only concern the freezing. The executing state could incur in a breach of the Directive when securing evidence pursuing article 32 of the Directive Provisional measures.

Moreover, legally speaking it is impossible to not comply with execution deadlines: If the executing state cannot respect the deadlines established by the EIO, then it will have to communicate such circumstance to the issuing state. Whenever the executing authority faces difficulties in performing the tasks requested, those should be communicated to the issuing state in order to find a solution.

In such a situation, the executing state could ask the issuing state to provide resources such as judges or forensics teams to aid in the execution of the investigatory measures.

8.7 Guide on the EIO form, Annex C

As explained in section 8.3.8.2 of this document, member states must notify other member states in cases of interception of telecommunication without technical assistance under the conditions of article 31 EIO directive.

8.7.1 Article 31 EIO directive

Conditions of article 31 EIO directive:

- Purpose of carrying out an investigative measure.
- Authorised interception of telecommunications by the competent authority of one Member State (the ‘intercepting Member State’).
- Communication address of the subject of the interception specified in the interception order is being used on the territory of another Member State (the ‘notified Member State’)
- No technical assistance of the notified member state is needed to carry out the interception

Consequence:

The intercepting Member State shall notify the competent authority of the notified Member State of the interception.

Point in time of notification:

- prior to the interception in cases where the competent authority of the intercepting Member State knows at the time of ordering the interception that the subject of the interception is or will be on the territory of the notified Member State;
- during the interception or after the interception has been carried out, immediately after it becomes aware that the subject of the interception is or has been during the interception, on the territory of the notified Member State.

8.7.2 Form: Notification of interception of telecommunication without any need of technical assistance

For notifying the other member state use annex C. Information required are contact details of the competent intercepting authority, point in time of the interception/duration, identity of the
concerned person and a description/legal description of the case comparable to Section G of annex A.

Tick the boxes in section (V) according to the point in time of your notification of interception.

As mentioned in annex C, the notified member states must, if it has any reasons, object to the interception or use of any already intercepted material within 96 hours after receiving the notification.

### 8.7.3  Best practice

#### 8.7.3.1  Consequence if you do not fulfil this obligation of notification

Non-fulfilment of notification obligations is a national law issue. In most cases, using the intercepted material in legal proceedings should work, however it depends on the national law.

Additionally, the intercepting member state will often become aware of the interception of a target on foreign territory during the analysis of the intercepted data afterwards. Thus, the subsequent notification shall be lawful.

#### 8.7.3.2  Transfer of interception data

The notified state might ask for the data to be transferred directly to it during the execution in the intercepting member state. However, in some member states the intercepting authority must first check the data. Consequently, the notified member state has no control of what data is transferred anymore, which might infringe domestic law.

Reacting to such issues, technical and legal solutions for direct transmission are analysed in the International (LI) Data-Exchange in real time based on mutual legal assistance (INTLI) project run by the German Federal Criminal Police Office (Bundeskriminalamt).
Conclusion

The new technologies in the field of computing represent a wide range of advantages for most of the citizens and the Society. Communication between agents is instantaneous and access to information (if it is not restricted) is almost immediate and independent of the location of any request. The volume of data that is generated is increasing and the growing trend seems to be exponential.

However, the exponential increase in the volume of data generated, together with the decentralization of the systems, points to a paradigm shift and opens a wide window of new possibilities in the field of cybercrime.

The European Investigation Order introduced in Directive 2014/41/EU seeks to adapt to this new paradigm and aims to streamline the management and handling of digital evidence in all (and among all) Member States of the European Union.

To ensure the success of the project and to be able to carry out an effective response to the current challenges, it is important that the agents involved in the scope of the Directive and the EIO, increase their technical knowledge and understanding of the main concepts regarding forensics and cloud environments.

Furthermore, it is also necessary to increase their knowledge on the writing and the procedures used in the field of the EIO, to facilitate the effective handling and response of all the agents involved in its processing.

This document is aimed to be used as a guide of best practices to allow the adaptation to the current situation to be effective and appropriate to the reality of the European environment.
Annex I: Digital evidence and international standards

The international standards that can be followed by investigators to carry out a digital forensic analysis of evidence are defined below:

ISO/IEC 27037:2012

The ISO / IEC 27037: 2012 standard "Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence" is a standard for the identification, collection, acquisition and preservation of digital evidence. The ISO / IEC 27037: 2012 standard provides guidelines for specific activities such as identification, collection, acquisition and preservation of potential computer evidence that may have probative value. This standard provides, to the investigator, guides regarding the process of handling digital evidence, as well as is also used as a guide the procedures for the exchange of digital evidence between jurisdictions (a court can, send digital evidence to another, maintaining the chain of custody of said evidence).

The ISO / IEC 27037: 2012 standard includes guidelines for the conservation of evidence and the chain of custody for digital storage devices, such as hard drives, USB memories, optical and magnetic disks, mobile phones, PDAs, memory cards, navigation systems by satellite, surveillance cameras (CCTV), computers with connection to the network, networks based on the TCP / IP protocol or similar, etc.

The main principles of the standard are listed below:

- **Methodology of the process**: the evidence must be acquired using a non-intrusive or minimally intrusive method.
- **Audit of the process**: the procedure followed and the generated documentation must be able to be audited by investigators other than those who acquired the evidence, with a traceability of the collection process of the same.
- **Reproduction of the process**: the procedure should be able to be repeated by investigators outside those who executed it for the first time, starting from the same premises and obtaining the same results.
- **Defense of the process**: the procedure must be able to be defended, demonstrating the adequacy of the tools used in it.

Furthermore, the treatment of the evidence for each type of device is as follows:

- **Identification**: location of evidence, whether physical or logical
- **Acquisition**: collection of evidence or its forensic copy, as well as documentation associated with it
- **Preservation**: preservation of the evidence as an unaltered element, so that it can be admitted as evidence, that is, retaining its chain of custody

ISO/IEC 27042:2015

intervention, from its identification (potential digital evidence), through its analysis (digital evidence), until it is accepted as evidence in a court (digital legal evidence).

The definitions provided by the standard for its use in the realization of a forensic analysis are listed below:

- **Potential digital evidence**: information identified as possible digital evidence, that is, that has not yet been analysed, stored in a physical medium, or transmitted through the network in binary format.

- **Digital evidence**: information identified as digital evidence, after its corresponding forensic analysis using the appropriate tools, stored in a physical medium, or transmitted through the network in binary format.

- **Digital legal evidence**: information identified as digital evidence that has been accepted in a judicial proceeding (evidence or piece of evidence, according to legal terminology).

- **Research**: application of exams, analysis and interpretations of potential digital evidence until it becomes legal digital evidence.

- **Examination**: set of procedures that are applied to identify and recover a potential digital evidence from one or several sources.

- **Analysis**: evaluation of the potential digital evidence in order to assess its possible importance in an investigation.

- **Interpretation**: synthesis and documentation to explain, within its scope, the facts carried out in the examinations and analysis made during the investigation.

The standard also presents analytical models that investigators can use, which are divided into the following categories:

- **Static analysis**: it is an analysis of the potential digital evidence (content of files, deleted data, etc.), in order to determine if it can be considered digital evidence. It should be examined raw and procedures used to avoid altering the potential digital evidence.

- **Live analysis**: it is an inspection of potential digital evidences in active systems, like RAM memories, mobile phones, tablets, networks, etc. The analysis must be done hot. In turn, the live analysis is divided into:
  
  - **Live analysis of systems that cannot be copied** or it is not possible to get an image of them: the risk for the investigator to analyse this type of systems is evident, since the potential digital evidence, can be lost by not being able to perform a copy of it. Therefore, it is very important to minimize the risk of the analysis and keep a record of all the procedures performed.
  
  - **Live analysis of systems that can be copied** or you can get an image of them: this type of systems must be analysed interacting with them directly, being extremely careful when making software or hardware emulations and using certified virtual machines, or even the real environments to obtain results closer to reality.

As well, ISO / IEC 27042: 2015, defines certain indications or guidelines that the investigators should include in their report, unless there are judicial indications against them. These guidelines are the following:

- **Qualifications of the investigator**
• Initial information available to the investigator and his team
• Nature of the incident that is going to be investigated by the investigator
• Date, time and duration of the incident
• Place of incident
• Research objectives
• Members of the research team supervised by the investigator
• Date, time and duration of the investigation
• Place of investigation
• Facts supported by digital evidence and found during the investigation
• Damage to digital evidence and its implications in the following stages of the research process
• Limitations of all analysis performed
• Detail of processes and tools used
• Interpretation of digital evidence by the investigator
• Conclusions
• Recommendations for future research

On the other hand, the standard emphasizes that the facts must be totally separated from the opinions of the investigator, in such a way that said opinions must be founded and be supported by the facts that arise from the digital evidences investigated. The investigator cannot include, therefore, in the report, any type of judgment or assertion that is not based on purely scientific facts.

Finally, the standard concludes with certain indications for investigators, who talk about the training and maintenance of the skills required to execute the activities leading to the management of digital evidence with due quality. These indications are:

• Definition of professional competence as an ability to obtain a result from the application of knowledge.
• The incompetence of a person can damage the investigation.
• The professional competence of an investigator must be measured and identified with metrics such as: university degrees, exams, certifications, curriculum, professional experience, continuous training, attendance at training events such as congresses, symposia or conferences, etc. In many European member states, according to the Civil and Criminal Procedure Laws, the investigator must have the official degree corresponding to the matter of the exercise, being the case of Engineering or Computer Engineering.
• The professional competence of an investigator should be measured periodically and in regular periods, including new areas of knowledge.
• An investigator will be considered competent when the results of his investigations are equivalent to those of another investigator.

• Independent third parties must validate professional competence.

**RFC 3227**

The RFC (Request for Comments) 3227 is a document that includes the main guidelines for the collection and storage of digital evidence, constituting a real standard for the collection and storage of evidence. RFC 3227 defines a process for collecting evidence that helps the investigator to acquire and catalogue digital evidence.

The process affects the acquisition of an image of the system that should be acquired as reliable as possible, making detailed notes that include dates and indicating if the local time or UTC time is being used, minimizing the changes in the information that is being collected (eliminating if possible the external agents that could execute these changes), prioritizing the collection on the analysis, collecting the information in order of volatility (that is, collecting first the information of the caches memories and the main memory -RAM- and , later, collecting the information from the secondary memory -hard disks-, followed by the USB memories and, finally, the optical units, system logs and documents).

The investigator, according to this standard, should try by all means to lose the least possible information, taking the best decision with respect to whether the evidence should be extracted from the running (turned on) computers that have been inspected (always before notary public or authority to record the process), or disconnect the machine from the network in order to avoid activating any computer program designed to eliminate information from the physical units connected to the computer, either remotely (panic button), or on a scheduled basis. It is necessary to add that this disconnection will cause the demagnetization of the caches and of the main memory, whose information will be irretrievably lost, which is why it is necessary to analyse and decide *in situ* what is the best option according to what the Investigator perceives in the different systems intervened.

The information provided by the programs of the system should also be ignored, since they may have been compromised. Programs that modify the metadata of the system files should not be executed.

In addition, the investigator must pay attention not to violate, under any circumstances, the privacy of individuals, complying at all times with the criteria of the European Union, which protects the privacy of the individual. It is also necessary to pay attention to the compromised information of the organization, since it may be the case that formulas, plans, or any other type of assets subject to the laws of industrial property are stored.

Therefore, the collection of evidence must follow the principles of:

• **Admissibility**: the evidence must be admissible by a Court of Justice.

• **Authenticity**: it must be possible to link the evidence to the incident or offense.

• **Completeness**: the test must be complete, not partial.

• **Reliability**: the process of collecting the evidence should not be questioned, so the chain of custody must be kept in an absolutely scrupulous manner, in order to prevent the Court not to admit the evidence.

• **Credibility**: the evidence must be easily understandable by the Court that will evaluate it.
The standard also defines a procedure for collecting evidence, which should be as detailed as possible, unambiguous and minimizing the amount of decision making necessary during the collection process. Thus, it is defined that the process must be transparent, in such a way that all the methods used for the collection of the test must be reproducible, which means that the procedure must be forensic (from the Latin forensis, "public and notorious"), as well as the duty of using standard methods.

A list should be created with all the systems involved in the incident, in order to subsequently collect the evidence, establishing a list of the evidences that are more likely to be admitted, taking all precautions for the collection of evidence.

For each computer system, the corresponding order of volatility must be obtained in each of its memories, disconnecting each system to avoid alterations in the evidence, and gathering the evidence with the necessary forensic tools. It is also necessary to record the degree of synchronization of the system clock and, while collecting evidence, to investigate the possibility of what other elements may be considered evidence. In addition, it is necessary to document each step and collect in a document the people involved in the procedure, taking note of who was there and what each of them was doing, as well as their observations and reactions. Finally, it is necessary to calculate the summaries or hash codes for each of the evidences, without altering them, in order to initiate a chain of custody procedure of the evidence.

On the other hand, the evidence archiving procedure defines how the evidence should be stored. The evidence must be clearly protected and well documented. Thus, the investigator will most likely need the help of a notary who grant public faith to the generation act of the chain of custody by calculating the hash code corresponding to the proof. In addition, documentation must be generated that leads to a clear description of how the evidence was found, how it was manipulated and who has custody of who is the evidence at every moment, detailing the changes that occur in the custody of it.

Access to stored evidence should be limited and a documentation is needed about the people who will have permission to access them, as well as custody changes that occur in the tests. It would also be convenient to implement a mechanism that detects unauthorized access to tests.

All the programs that the investigator needs to carry out the forensic analysis of the tests, must be prepared in advance in "read-only" optical media, such as CDs or DVDs, and must include at least one program from each of the following typologies:

- A program for the examination of processes
- A program to examine the state of the system
- A program for making copies bit by bit
- A program to calculate checksums or hash codes
- A program for the generation of basic images and to analyse these
- A script to automate the collection of evidence

In addition, the investigator must be prepared to ensure the authenticity and reliability of the tools used.

---

**RFC 4810**

RFC 4810 defines a standard that must be followed for the preservation of information so that the existence of certain files, created at a certain moment, can be tested, as well as its integrity from
the moment of its creation until the moment when it is presented as evidence by the investigator. Similarly, the RFC defines what type of file systems can support this type of scenario and what requirements they must meet.

Finally, the RFC defines the way in which a digital signature must be able to be verified after having elapsed an indeterminate time since the generation of it.

**RFC 4998**

RFC 4998 defines a standard that must be followed for the preservation of information, including digitally signed information, in order to prove its existence and integrity during a period of time that may be undefined. The RFC defines what type of file systems can support these scenarios and what requirements must be met by an Evidence Registry, in which a computer expert is supported, to guarantee the existence of such information, in order to avoid being repudiated.

**RFC 6283**

RFC 6283 defines a standard to demonstrate the existence, integrity and validity of information, including digitally signed information, for indefinite periods of time. The RFC also defines the XML language extensible language syntax, as well as the processing rules, which must be followed for the creation of full evidence of long period information in order to avoid its repudiation.
References

4 McKemmish, D. Rodney. Computer and Intrusion Forensics, USA, 2003
6 Mobile threats incident handling handbook by ENISA: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/Mobileincidenthandlinghandbook.pdf
8 Computer forensics tools: http://resources.infosecinstitute.com/computer-forensics-tools
10 https://cloudsecurityalliance.org/group/top-threats/#_overview
12 Digital forensic investigation of cloud storage services: https://www.sciencedirect.com/science/article/pii/Sr742287612000400?via%3Dihub
15 Open Source Incident Response Toolkit: https://www.threatresponse.cloud/
16 Python installable command line utility for mitigation of instance and key compromises: https://github.com/ThreatResponse/aws_ir
17 Overview of existing legal framework in the EU Member States by EVIDENCE project: : http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-1-411.pdf
21 Ibid [P 53] Impact Assessment
24 In that regard in its article 2 (i) the RPPO allows the production of subscriber data and access data to be requested by judges, courts, investigative judges and prosecutors, while a production orders for transactional and content data excludes prosecutors from its issuing (Article 2(2) RRPO). In relation to that differential procedural treatment, the WP 29 already expressed its doubts in its statement from November 2017, and reminded that “metadata may reveal very sensitive data, in line with the considerations of the ECJ in Digital Rights Ireland and Tele 2/ Watson”.


27 Web of e-CODEX project: [https://www.e-codex.eu/](https://www.e-codex.eu/)

28 Web of EVIDENCE project: [http://www.evidenceproject.eu/](http://www.evidenceproject.eu/)


- Webserver analysis Handbook by ENISA: [https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exec3_forensic_analysis_iii-handbook](https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exec3_forensic_analysis_iii-handbook)


31 Council Framework Decision 2008/978/JHA, on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters

32 Council Framework Decision 2003/577/JHA, on the execution in the European Union of orders freezing property or evidence

33European Judical Network (EJN), Status of Implementation <accesible at [https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120>](https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120>)


35 Ibid. Art. 1

36 Case C-452/16 Openbaar Ministerie v Krzysztof Marek Poltorak [2016] Para 33

37 Council Framework Decision 2002/584/JHA, on the European arrest warrant and the surrender procedures between Member States
38 Useful tools and information for the practical application of the European Investigation Order (EIO) Directive. Extracts from Conclusions of Plenary meetings of the EJN concerning the practical application of the EIO, Brussels, 8 December 2017

39 The obligation to respect fundamental rights is thus twofold, as it is found first on the assessment carried by the issuing authority prior submission and then also by the executing authority upon receipt.

40 Executing authorities will always have to respond to measures requiring the identification of persons holding a subscription of a specified phone number or IP address.


43 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al33051


45 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008D0615


47 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800656ce


54 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG

55 While signatory parties, Ireland and Sweden have not yet ratified the Cybercrime Convention; source : Chart of signatures and ratifications of Treaty 185 < accessible at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures >

56 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

57 Council of Europe, Convention on Cybercrime [2001] Preamble

58 https://www.echr.coe.int/Documents/Convention_ENG.pdf

59 Ibid [Art 23]

60 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800656ce


70 Ibid


72 Ibid (para 8)

73 Ibid (para 9)


75 Case C-582/14 Breyer [2016]

76 Benedik v Slovenia App no 62357/14 (ECtHR, 24 April 2018) [para 119]

77 https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120

78 https://www.coe.int/en/web/conventions/full-list-/conventions/rms/0900001680081561

79 https://www.ejnforum.eu/cp/practitioners/contact-points

80 http://www.eurojust.europa.eu/Practitioners/operational/Pages/coordination-meetings.aspx

81 http://www.eurojust.europa.eu/Practitioners/operational/Pages/eurojust-coordination-center.aspx

82 Directive 2016/680