EVIDENCE

EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE

EVIDENCE and beyond

Institute of Legal Information Theory and Technique
Italian National Research Council

Mattia Epifani
EVIDENCE Project

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

Consiglio Nazionale delle Ricerche

university of groningen

Leibniz Universität Hannover

GA No. 608185

LSC

01.03.2014 – 31.10.2016

ocetic
Your Connection to ICT Research

EU funding: € 1,924,589.00

promoting law & justice - European lawyers - Les avocats européens pour le droit & la justice -
CCBE

INTERPOL

UNIVERSITY OF MALTA
L-Università ta' Malta

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

The Process: Electronic Evidence Life Cycle (1/2)

1 Before the incident occurs

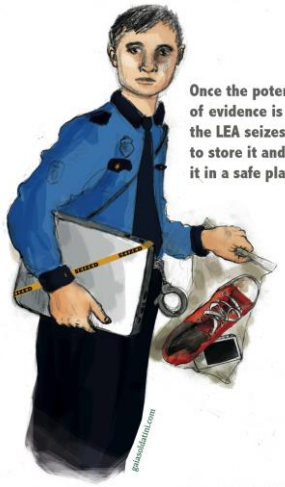
2 Crime scene

The Law Enforcement Agency (LEA) arrives at the crime scene and delimits it in order to prevent non-authorized access.

3 Inspection and scene documentation

The LEA inspects the crime scene in order to identify potential sources of evidence.

4 Seizure of potential source of evidence



Once the potential source of evidence is identified, the LEA seizes it in order to store it and analyse it in a safe place.

5 Request of a specialist intervention

The LEA requires the intervention of a Digital evidence first responder (DEFR) to analyse the content of the potential source of evidence.

6 Investigation

The DEFR makes a forensic copy of the potential evidence and starts its analysis.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

The Process: Electronic Evidence Life Cycle (2/2)

7 Presentation before Court

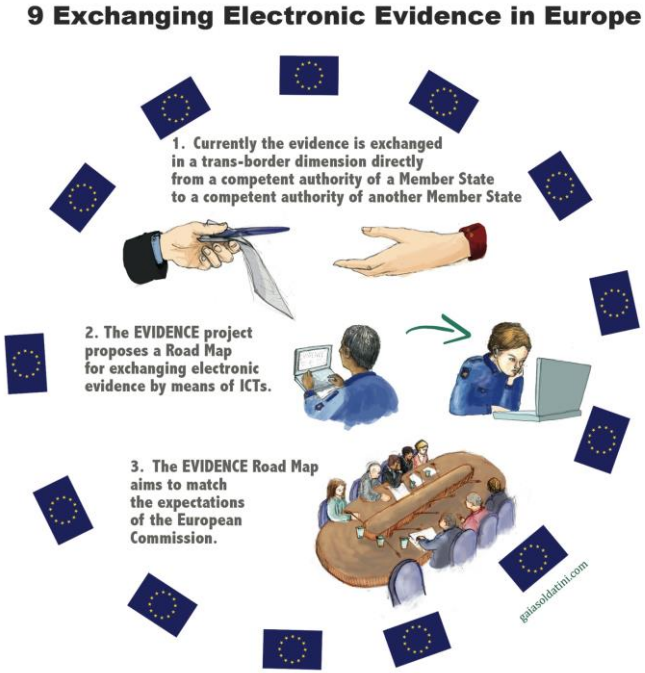
The report case together with the copy of the source of evidence and other relevant documents are given to the judicial authority

8 Admissibility in Court

The potential electronic evidence is admitted in court, if all the legal and technical requirements are met.

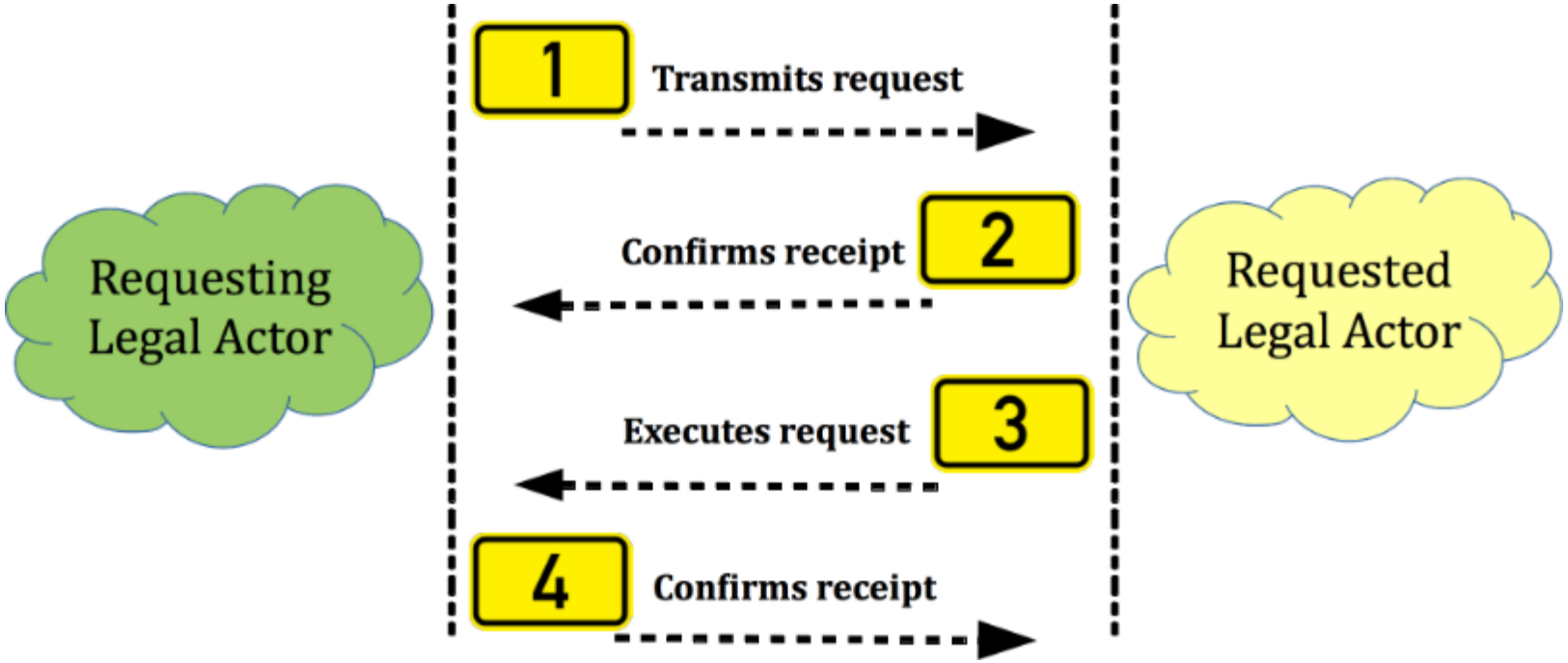
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

The Goal: Harmonize this process in the EU Member States



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

EVIDENCE: Focus on E.E. Exchange



The process of *transferring* an E.E. or/and a Source of Evidence, in the specific field of criminal investigation or criminal trial collaboration, from a requested (sending) legal actor to a requesting (receiving) legal actor in a different country (*across EU Member States*), according to a specific set of standard rules …

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

Methodology: How to Harmonize this process in the EU Member States?

- **Harmonizing the Treatment for Harmonizing the Exchange**

- Creating a **common background** for all actors involved in the Electronic Evidence life-cycle: Policy makers, LEAs, Judges and Lawyers (same practises and aligned guidelines)

- Creating a **common legal layer** devoted to the regulation of Electronic Evidence in Courts (same rules)

- Creating **standardized procedures** in the use, collection and exchange of Electronic Evidence (across EU Member States)(same methodologies/standards/tools)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

EVIDENCE Solution: The way to the EU Common Framework

- Developing a **Road Map** (guidelines, recommendations, technical standards, research agenda) for creating a **Common European Framework** for the systematic, aligned and uniform application of new technologies in the collection, use and exchange of evidence
- Drafting/assessing **Rules for the treatment of electronic evidence**
- Defining implications for **privacy** and operational issues
- Understanding conditions for a secure and consistent **Exchanging** of Evidence collected by means of new technologies

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

The paths to the Roadmap

In order to produce the Roadmap the following objectives were achieved as considered essential:

- DEVELOPED a common and shared understanding on what electronic evidence is and which are the relevant concepts of electronic evidence in involved domains and related fields (digital forensic, criminal law, criminal procedure, criminal international cooperation) – **EVIDENCE CATEGORISATION**

- DETECTED which are rules and criteria utilized for processing electronic evidence in EU Member States, and eventually how is the exchange of evidence regulated; **STATUS QUO ANALYSIS**

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

The paths to the Roadmap

- DETECTED of the existence of criteria and standards for guaranteeing reliability, integrity and chain of custody requirement of electronic evidence in the EU Member States and eventually in the exchange of it- **EVIDENCE FORENSIC TOOLS CATALOGUE**
  EVIDENCE STANDARD PROPOSAL FOR A FORMAL LANGUAGE

- Defined and understood the needs of law enforcement, prosecution services and the judiciary

- Identified data protection and privacy requirements in Europe on the use and exchange of electronic evidence

- IDENTIFIED and DEVELOPED technological functionalities for a Common European Framework in gathering and exchanging electronic evidence- **EVIDENCE PROOF OF CONCEPT**

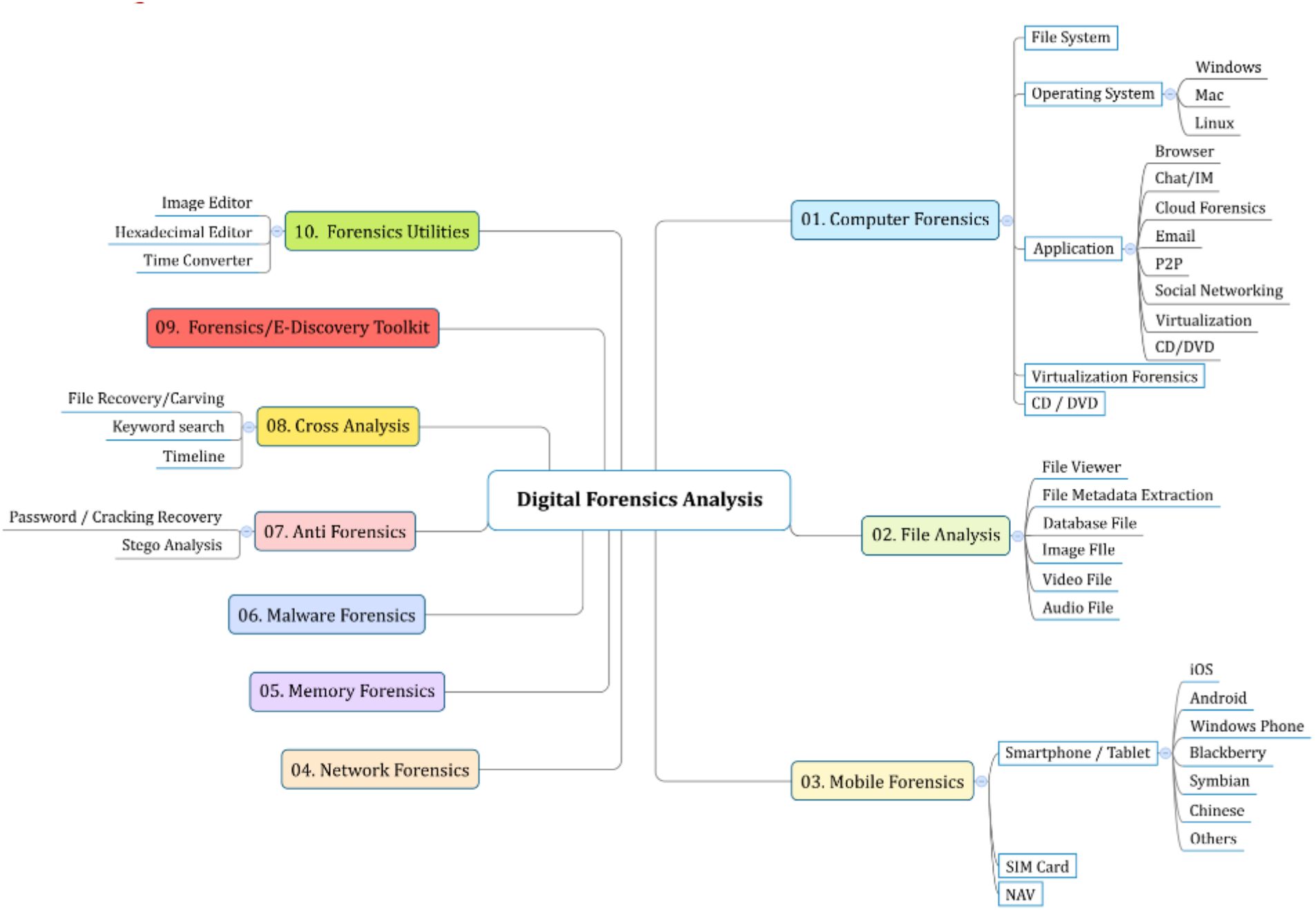
- Sized the EVIDENCE market **- EVIDENCE MAP OF ACTORS**

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

D.F. Tools Catalogue: main data

- The most significant digital forensics tools related to:
  - Acquisition: **461**
  - Analysis: **1.031**
- The total number of software tools collected so far is **1.492**
- Organized using a specific **classification**:

- **Acquisition**
  - 01. Disk duplication
    - 01.01. Write blocker hardware
    - 01.02. Write blocker software
  - …
- **Analysis**
  - 01. Computer Forensics
    - 01.01. File system
    - 01.02. Operating System
  - …


Digital Forensics Analysis
01. Computer Forensics
File System
Operating System
Windows
Mac
Linux
Application
Browser
Chat/IM
Cloud Forensics
Email
P2P
Social Networking
Virtualization
CD/DVD
Virtualization Forensics
CD / DVD
02. File Analysis
File Viewer
File Metadata Extraction
Database File
Image FIle
Video File
Audio File
03. Mobile Forensics
Smartphone / Tablet
iOS
Android
Windows Phone
Blackberry
Symbian
Chinese
Others
SIM Card
NAV
04. Network Forensics
05. Memory Forensics
06. Malware Forensics
07. Anti Forensics
Password / Cracking Recovery
Stego Analysis
08. Cross Analysis
File Recovery/Carving
Keyword search
Timeline
09. Forensics/E-Discovery Toolkit
10. Forensics Utilities
Image Editor
Hexadecimal Editor
Time Converter

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

D.F. Tools Catalogue on WEB

wp4.evidenceproject.eu

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

Electronic Evidence Exchange: status quo

- **No existing standard**
- Chiefly **human based**
- Exception: data obtained by third parties (i.e. ISPs) are exchanged in electronic format, but without a common standard

- What information needs to be exchanged?
- When may the exchange take place?
- How the information can be exchanged?
- Which kind of stakeholders are involved?
- How to generate **trust** among all potential stakeholders?

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

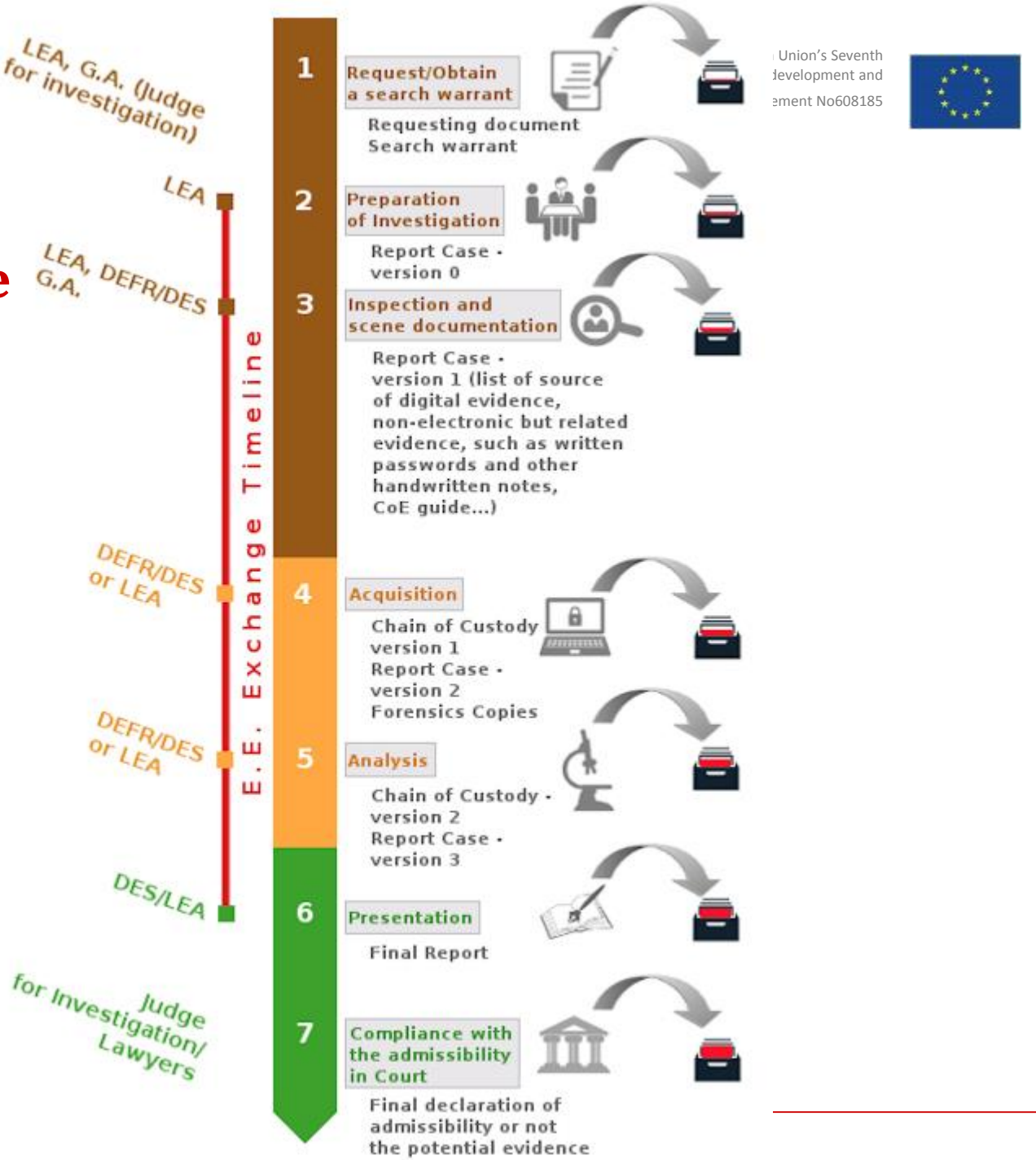
Electronic Evidence Exchange: what?

- Information about the **people** involved (both technical and legals)
- Surroundings information about **legal authorization**
- Information about the used **process/lifecycle**
- Information about the **chain of custody**, by identifying who did what, when and where
- **Actions** performed by people
- Information about the **source of evidence** and the **digital evidence** obtained during the process
- Complete descriptions of the identified **objects** inside the digital evidence
- Relationships between **objects**

EVIDENC
EUROPEAN INFORMAT
FRAMEWORK FOR CO

Union's Seventh
development and
ement No608185

E.E. Life-Cycle (when?)



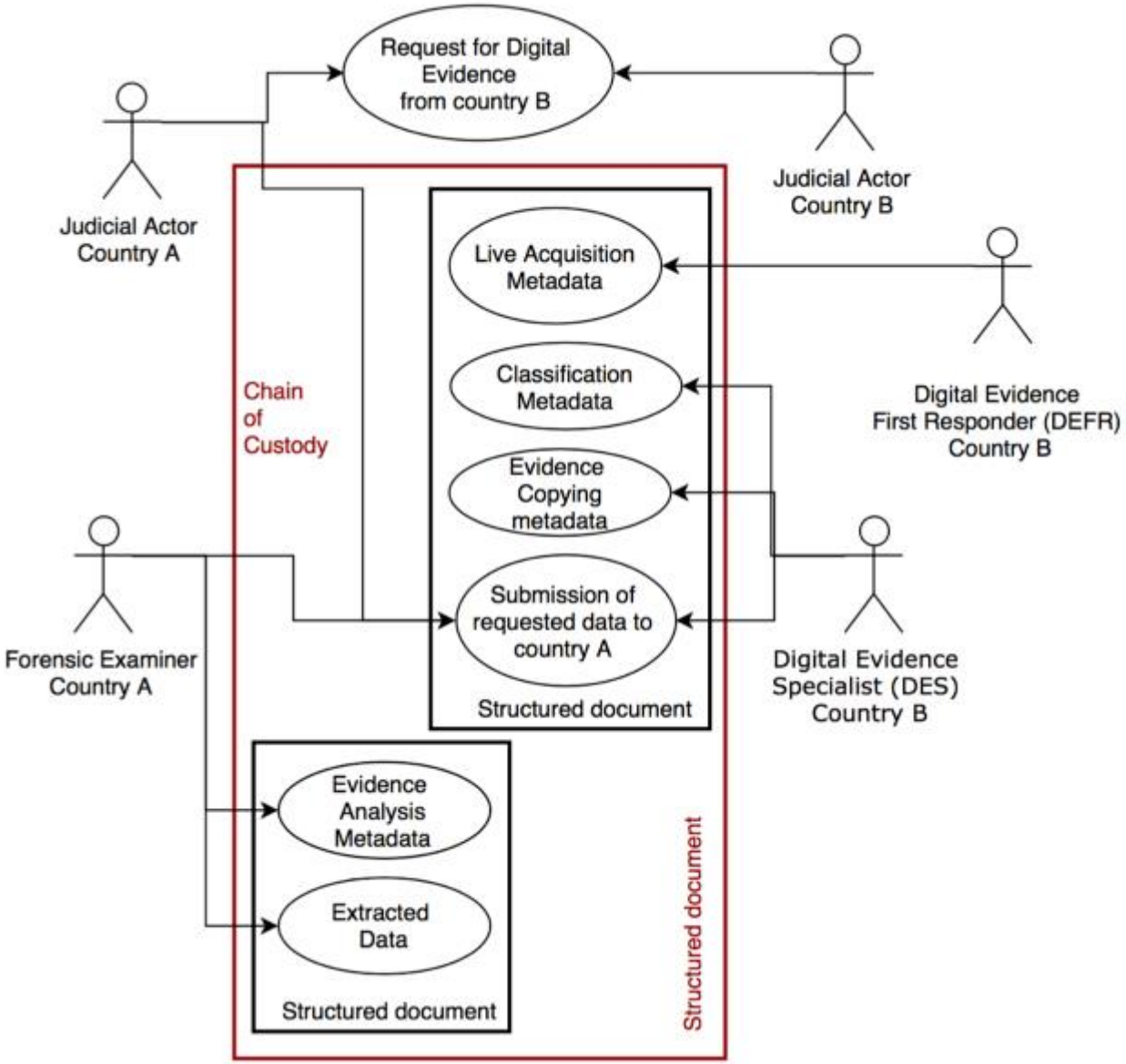
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

Electronic Evidence Exchange: how?

- Developing a formal standard language to **represent the widest range of forensic information and forensic processing results and include legal requirements**
- **Implementing the exchange on already existing platform or create a specific platform for the Exchange?**
- *Advantages*
  - Facilitating the **exchange process**, including legal requirements data (e.g. how results are obtained)
  - Forensics **tools interoperability**
  - Forensics **tools verification**
- *Needs*
  - **Agreement on the language structure among various actors** (i.e. forensics tools manufacturers to extend/adapt their tools)
  - **Trust between stakeholders**

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

EVIDENCE WORKFLOW Packaging



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

How do we meet the Future challenges ?

- Facilitating the Evidence Exchange process in the context of **the EIO and the MLA procedures**
- Introducing **a standard for the representation of the Electronic Evidence (data and metadata), along with legal requirements** data (e.g. how results are obtained and which rules applied)
- **Sharing and linking of information (Eoghan Casey) through technical and automatic mechanisms**
- Including **Services providers** and **Digital Forensics hardware/software devolper** in the loop

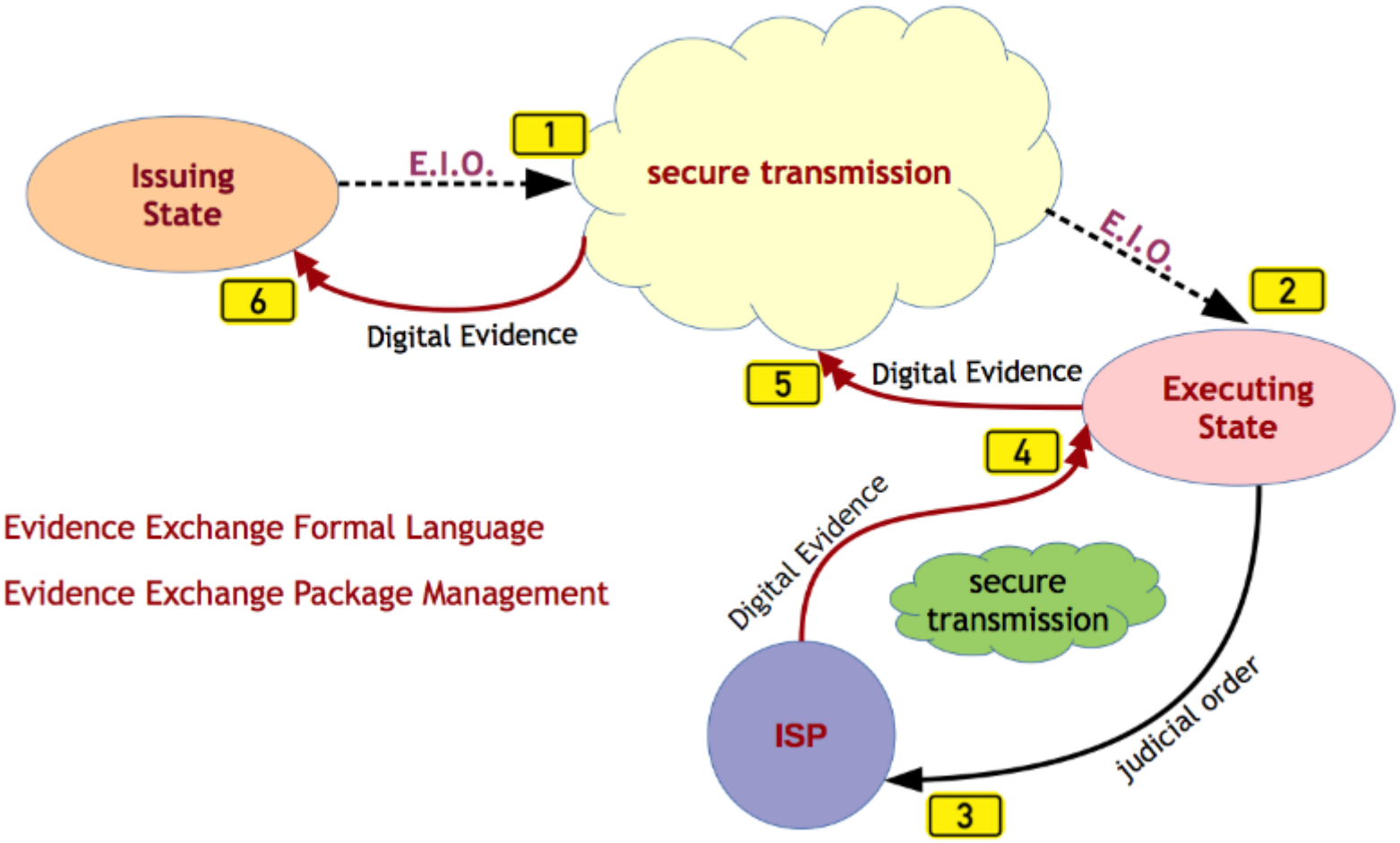
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

Which tools/means are we going to use?

- Using a **formal/standard language (EVIDENCE proposal) for representing the Evidence to be exchanged**.
- A common and standard format for representing the broadest possible range of cyber-investigation domains, including digital forensic science, incident response, and counter terrorism
- e-Codex platform, S-Testa, SIENA, E24/7, and others..
- Information systems already in place led by an European Public Organization (?)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

A possible scenario



Evidence Exchange Formal Language

Evidence Exchange Package Management

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

Thank you for your kind attention!

Questions?