The Evidence Project: Bridging The Gap In The Exchange Of Digital Evidence Across Europe

By

Maria Angela Biasiotti and Fabrizio Turchi

Presented At

The Digital Forensic Research Conference

DFRWS 2015 EU Dublin, Ireland (Mar 23rd- 26th)

EVIDENCE

EUROPEAN INFORMATICS DATA EXCHANGE
FRAMEWORK FOR COURTS AND EVIDENCE

Bridging the Gap in the Collection, Use and Exchange of Electronic Evidence in Europe

Institute of Legal Information Theory and Technique
Italian National Research Council
Maria Angela Biasiotti
Mattia Epifani,
Fabrizio Turchi

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

Legal Notice: The views expressed in the course of this research are the sole responsibility of the author and do not necessarily reflect the views of European Commission.

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

EVIDENCE Project: Main data

- **European Informatics Data Exchange Framework for Court and Evidence**

- Duration: 30 months (March 2014 - August 2016)
- Coordinator: CNR-ITTIG
- Eu Funding: € 1,924,589.00 (CSA – Coordination and Support Action)
- Partners
  - CNR-ITTIG, CNR-IRPPS – CNR (Italy)
  - University of Groningen - RUG (The Netherlands)
  - International Criminal Police Organization - INTERPOL (France)
  - Leibniz University of Hannover - LUH (Germany)
  - Laboratory of Citizenship Science – LSC (Italy)
  - University of Malta – UOM (Malta)
  - Council of Bars and Law Societies of Europe - CCBE (Belgium)
  - Centre of Excellence in Information and Communications Technologies – CETIC (Belgium)
  - Law and Internet Foundation – LIF (Bulgaria)
- Web site: www.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

EVIDENCE: Topic addressed by the call

- In the European Union context there is a need of a Common Framework regulating the implementation of ICTs in the handle and exchange of electronic evidence in criminal trials

interpreted as

- Need for a **common background** for all actors involved in the Electronic Evidence life-cycle: Policy makers, LEAs, Judges and Lawyers
- Need for a **common legal layer** devoted to the regulation of Electronic Evidence in Courts
- Need for **standardized procedures** in the use, collection and exchange of Electronic Evidence (across EU member States)

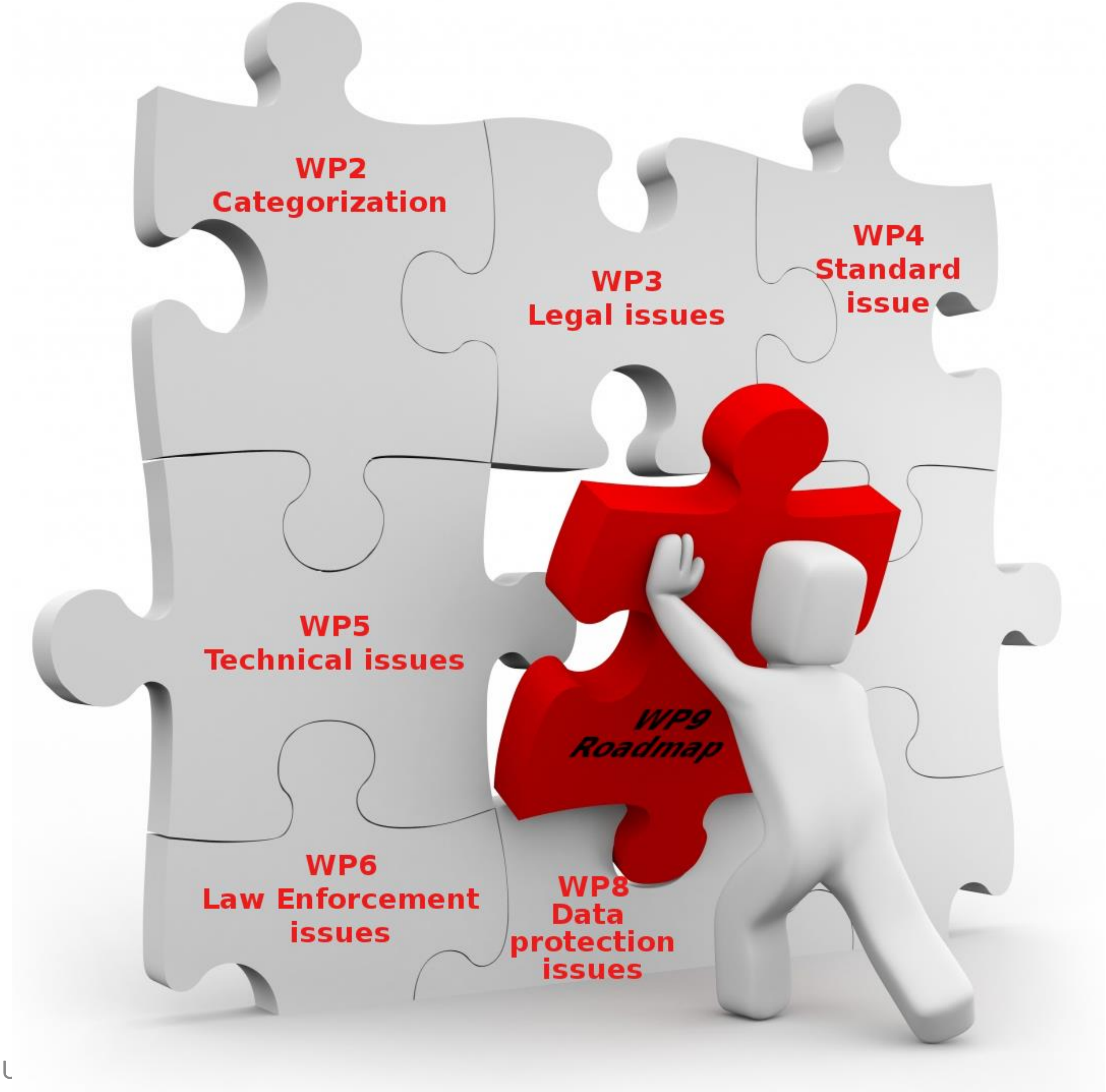
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

EVIDENCE: Main aims

- 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 Rules for treatment of both digitized and born-digital Evidence
- Defining Implications for privacy and ethical issues
- Understanding conditions for a secure and consistent **Exchanging** of Evidence collected by means of new technologies

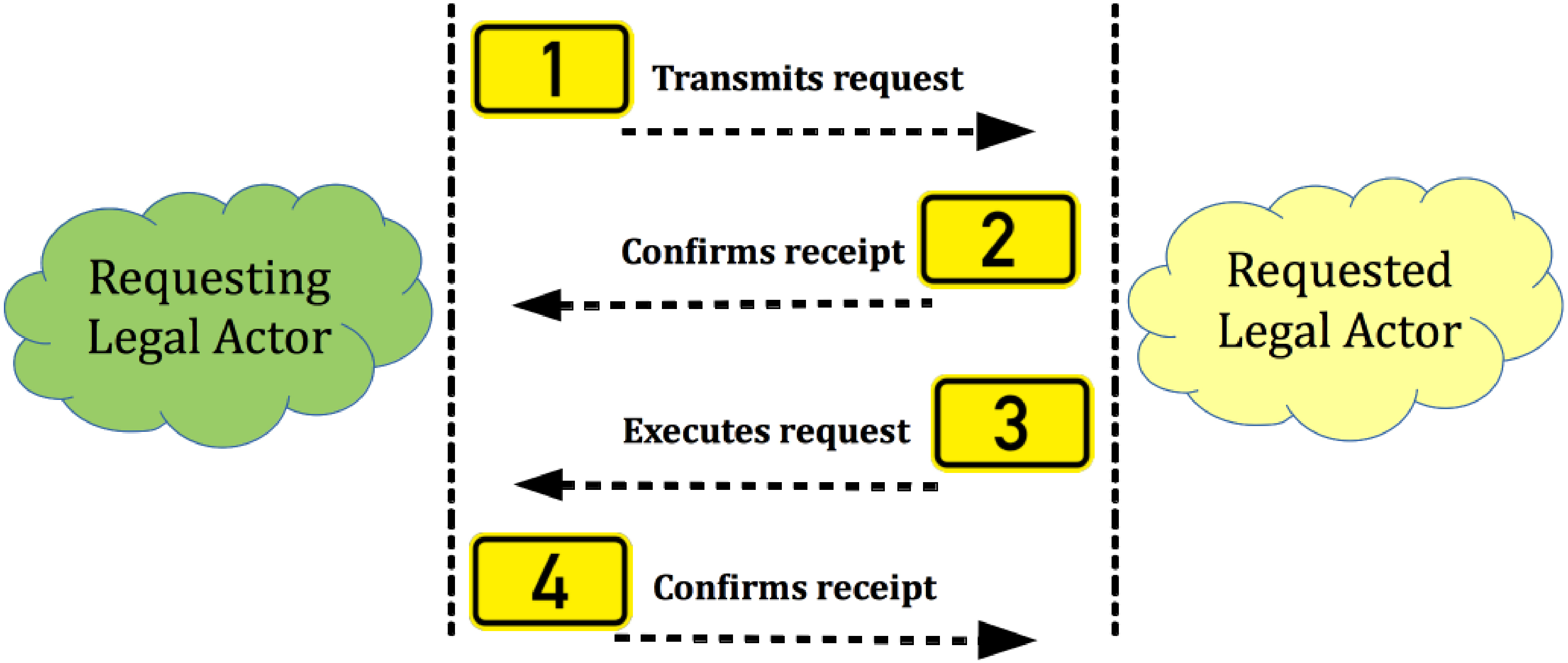
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

EVIDENCE: Road Map



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



Requesting Legal Actor

Requested Legal Actor

1 Transmits request

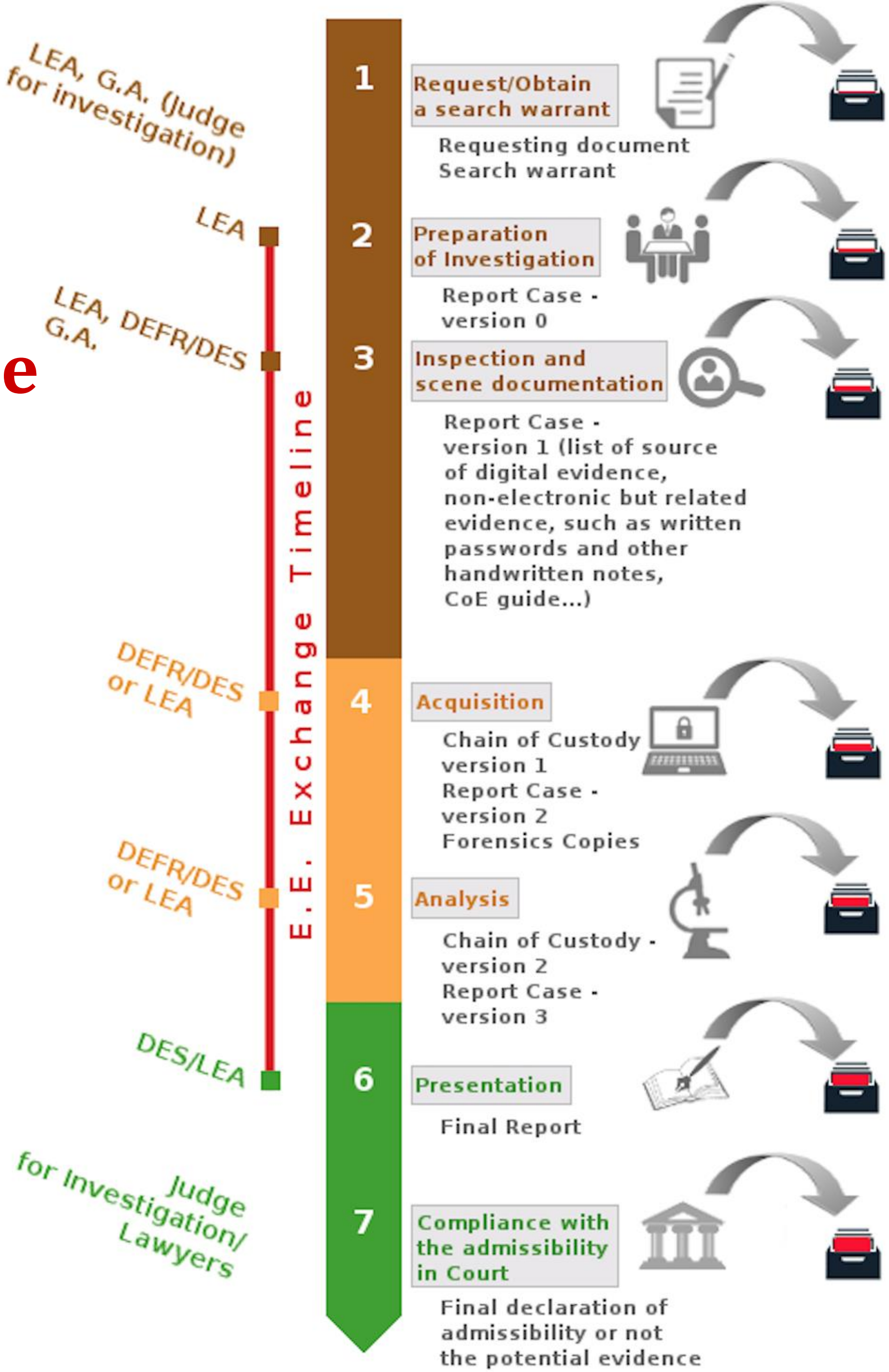
2 Confirms receipt

3 Executes request

4 Confirms receipt

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 …

E.E. Life-Cycle



E.E. Exchange Timeline

LEA, G.A. (Judge for investigation)

1 Request/Obtain a search warrant

Requesting document
Search warrant

LEA

2 Preparation of Investigation

Report Case - version 0

LEA, DEFR/DES G.A.

3 Inspection and scene documentation

Report Case - version 1 (list of source of digital evidence, non-electronic but related evidence, such as written passwords and other handwritten notes, CoE guide...)

DEFR/DES or LEA

4 Acquisition

Chain of Custody version 1
Report Case - version 2
Forensics Copies

DEFR/DES or LEA

5 Analysis

Chain of Custody - version 2
Report Case - version 3

DES/LEA

6 Presentation

Final Report

Judge for Investigation/ Lawyers

7 Compliance with the admissibility in Court

Final declaration of admissibility or not the potential evidence

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

EVIDENCE: Main outcomes

- Comparative analysis of existing legal provisions;
- Identification and specification of those legislative changes that should be promoted at both European and Member State levels;
- Definition of open/widely available standards, assuring the international transfer of evidence;
- Identification of operational and ethical implications for law enforcement agencies;
- Identification of technical developments that should be carried out to sustain all these aspects.

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

EVIDENCE: Completed activities

- **Categorization** of the most relevant concepts in E.E. domain - mind map representation
- **Electronic Evidence** Electronic Evidence is any data resulting from the output of an analogue device and/or a digital device of potential probative value that are generated by, processed by, stored on or transmitted by any electronic device.
  Digital evidence is that electronic evidence which is generated or converted to a numerical format.
- **Prima Facie Size of E.E. Market** - Map of actors
- **D.F. Tools Catalogue** gathered over 1.200 different tools in Acquisition and Analysis processes

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

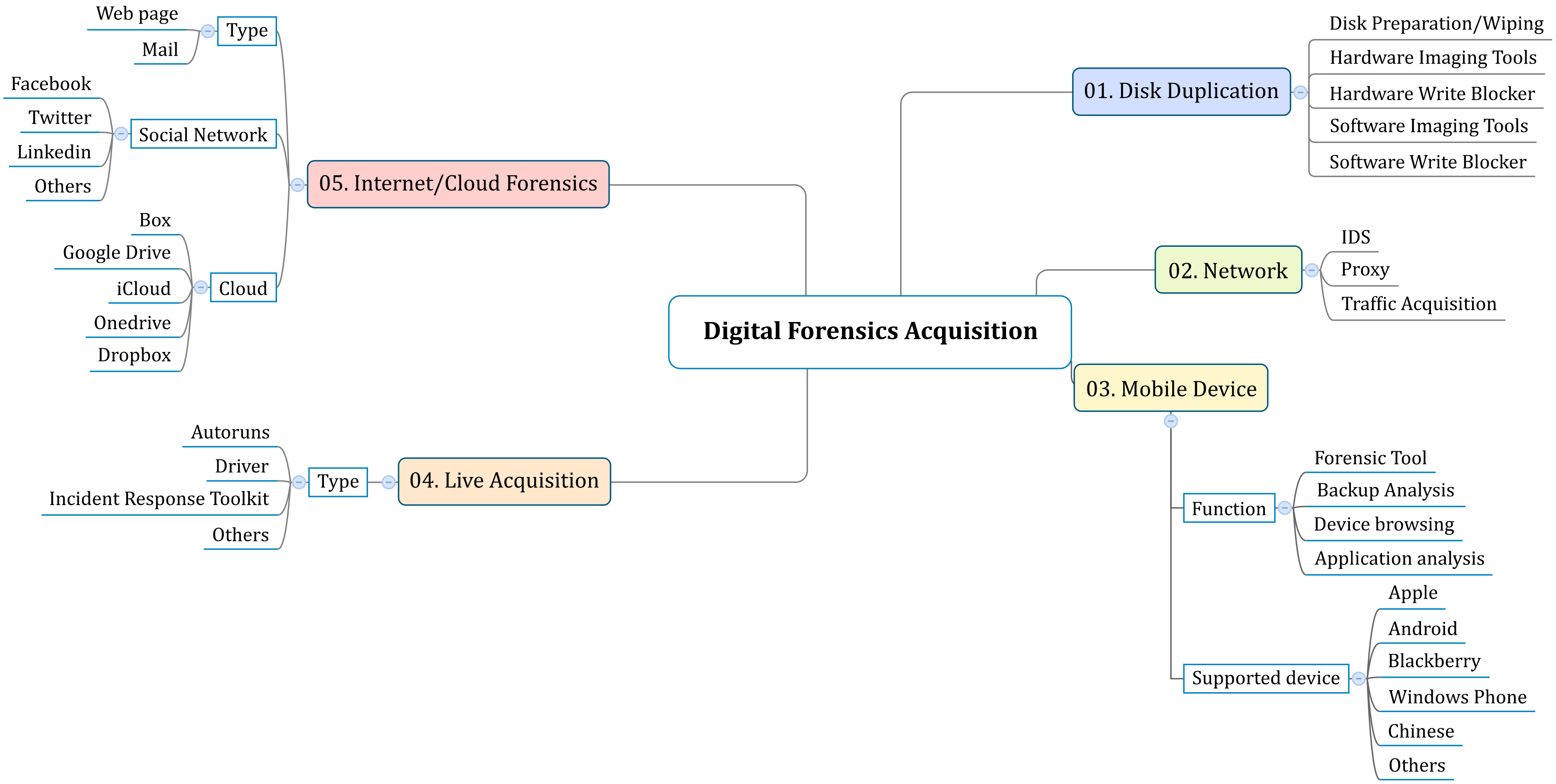
- The most significant digital forensics tools related to:
  - Acquisition: **324**
  - Analysis: **957**
- The total number of software tools collected so far (Jan 2015) is **1.281**

- Organized using a specific **classification**:

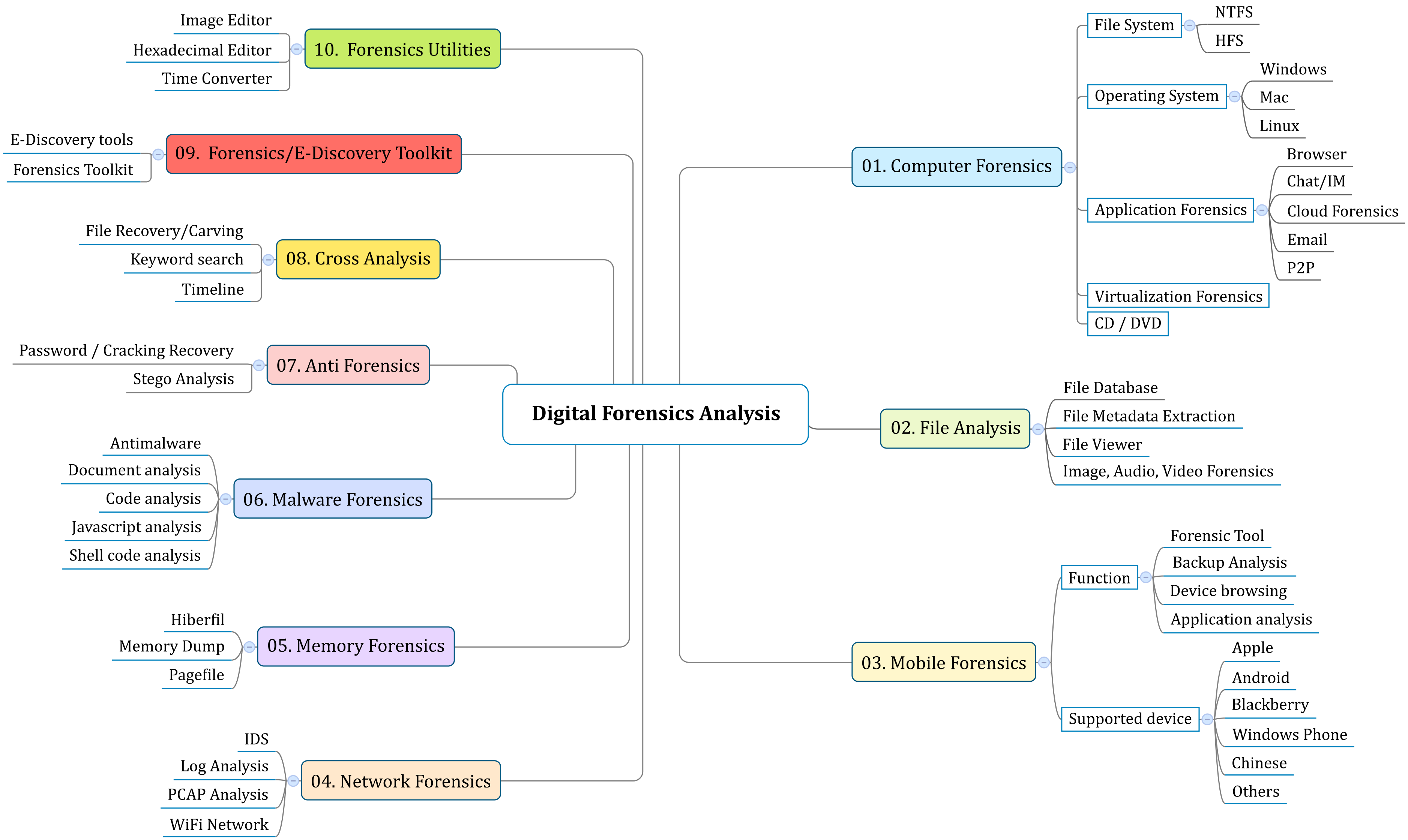
- **Acquisition**
  - 01. Disk duplication
    - 01.01. Write blocker hardware
    - 01.02. Write blocker software
  - …
- **Analysis**
  - 01. Computer Forensics
    - 01.01. File system
    - 01.02. Operating System
  - **…**

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: Acquisition



D.F. Tools Catalogue: Analysis



- Digital Forensics Analysis
  - 01. Computer Forensics
    - File System
      - NTFS
      - HFS
    - Operating System
      - Windows
      - Mac
      - Linux
    - Application Forensics
      - Browser
      - Chat/IM
      - Cloud Forensics
      - Email
      - P2P
    - Virtualization Forensics
    - CD / DVD
  - 02. File Analysis
    - File Database
    - File Metadata Extraction
    - File Viewer
    - Image, Audio, Video Forensics
  - 03. Mobile Forensics
    - Function
      - Forensic Tool
      - Backup Analysis
      - Device browsing
      - Application analysis
    - Supported device
      - Apple
      - Android
      - Blackberry
      - Windows Phone
      - Chinese
      - Others
  - 04. Network Forensics
    - IDS
    - Log Analysis
    - PCAP Analysis
    - WiFi Network
  - 05. Memory Forensics
    - Hiberfil
    - Memory Dump
    - Pagefile
  - 06. Malware Forensics
    - Antimalware
    - Document analysis
    - Code analysis
    - Javascript analysis
    - Shell code analysis
  - 07. Anti Forensics
    - Password / Cracking Recovery
    - Stego Analysis
  - 08. Cross Analysis
    - File Recovery/Carving
    - Keyword search
    - Timeline
  - 09. Forensics/E-Discovery Toolkit
    - E-Discovery tools
    - Forensics 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: structure

- **Tool Name**: it represents the name of the tool assigned by its producer/reseller/developer
- **License type**: it may assume values like Open source, Freeware, Commercial
- **Category**: it is one of the branch of the forensics tools classification. Each tool may belong to more categories
- **Operating System**: it may assume values like: Windows, Mac, Linux, Standalone.
- **Developer**: it is the author of the development of the tool and it may be a person, a community or an organization
- **Url**: the official web site of the tool
- **Test report**: it is the official web address where a well known organization has tested the software and published the results
- **Features**: each Category is connected to a single or multiple features, even though, in some cases, it may not have any features at all.
  Each Feature may assume a single or multiple values.

- On-line D.F. Catalogue

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: collaborative network

- Launched a collaborative network of experts/producers to evaluate/integrate/improve/keep update the content?

- Create a trusted list, about 35, members, of Digital Forensics Experts:
  - LEA (Belgium, France, Greece, Italy, USA)
  - Digital Evidence Specialists (France, Italy, Norway, Spain, USA)
  - Organizations (Netherland Foreniscs Institute, CCIS – Norway, SANS, IISFA, ONIF, …)
  - Invitation letter
  - Feedback and proposal (questionnaire)

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 challenges

- No standard (comparison with Acquisition and Analysis)
- Exchange within the same country or between countries:
  - What information is exchanged
  - How the information is exchanged (even taking into consideration security issues)
  - Which kind of stakeholders are involved
  - Which different cases may occur in the Exchange
  - Pre-analysis / post-analysis exchange cases?
  - It seems mostly human based

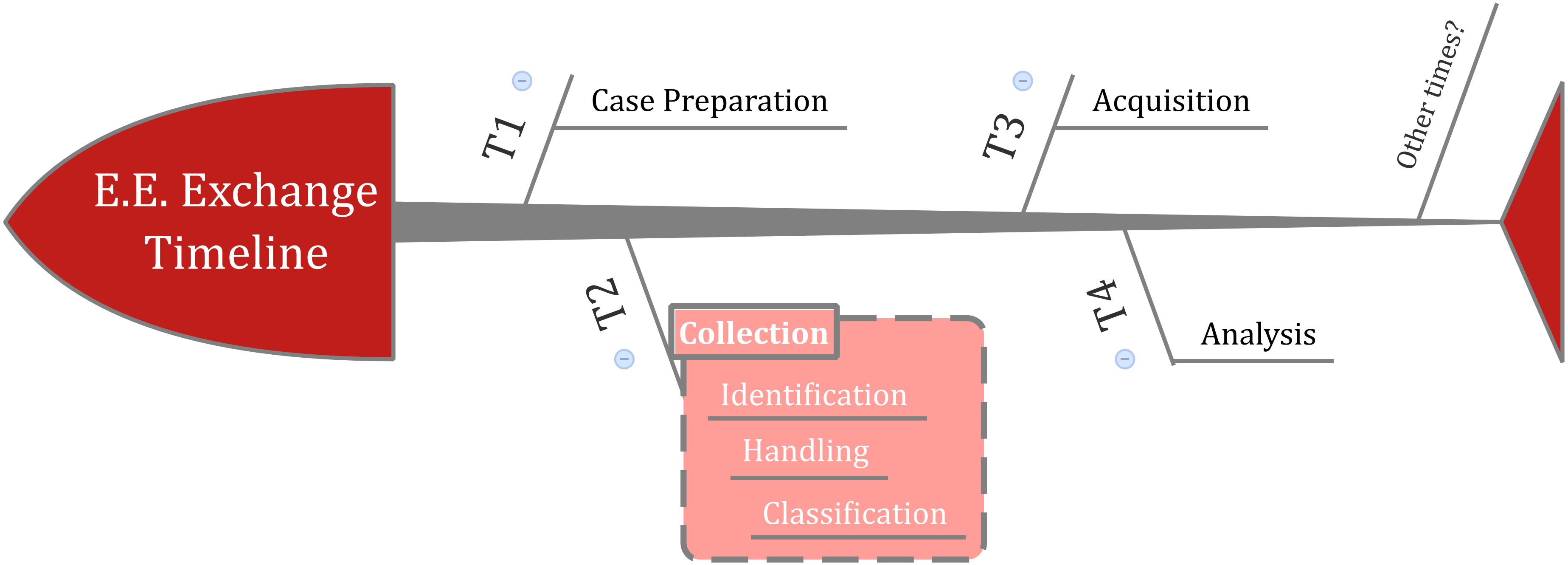
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

E.E. Exchange/Sharing Platform

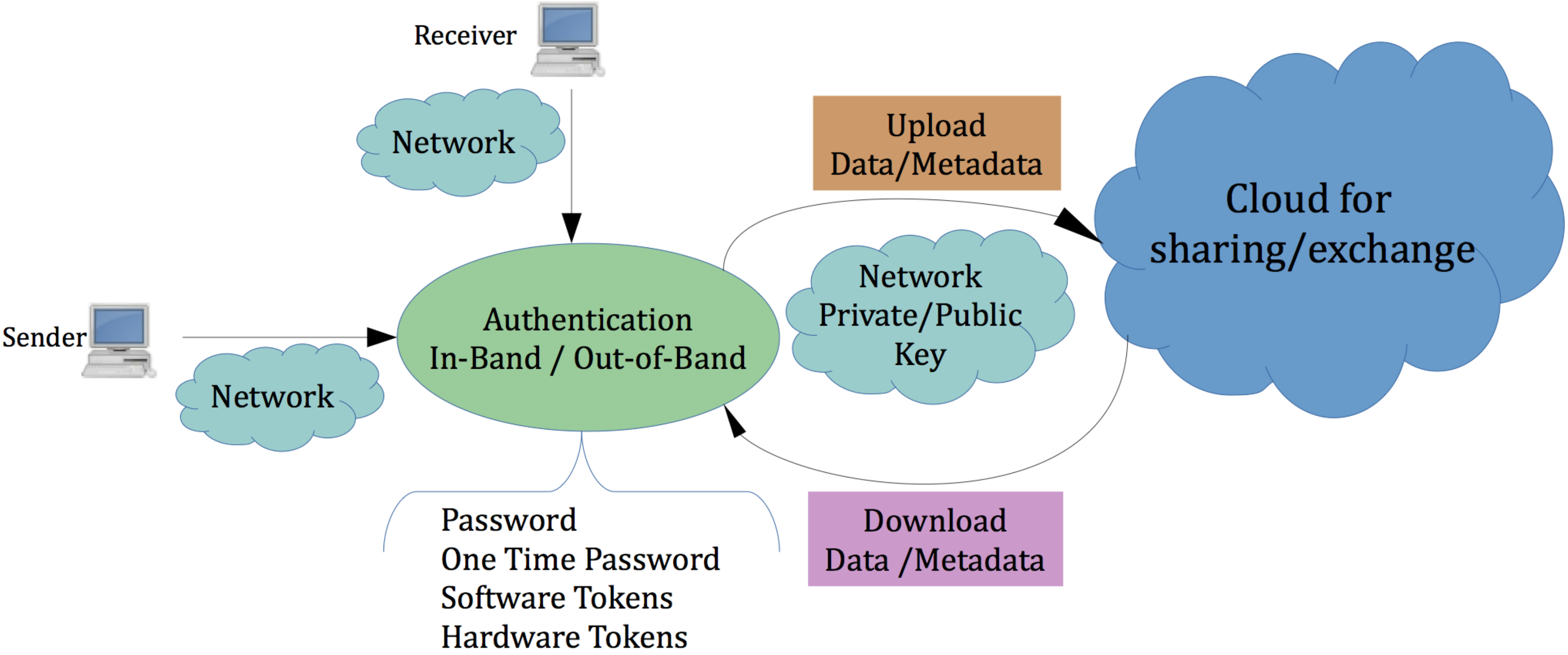
- Exchange timeline
- Platform general architecture (draft proposal)
- Use Cases and metadata
  - Use Case 0: Case Preparation
  - Use Case 1: Source of evidence
  - Use Case 2: E.E. Acquisition/Forensic Copy
  - Use Case 3: Analysis
    a) Single file
    b) File set
    c) Output tool report
    d) Final report
- Already existing standards (CyBox, DFXML, STIX, Cybex)

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

E.E. Exchange: when may it take place?

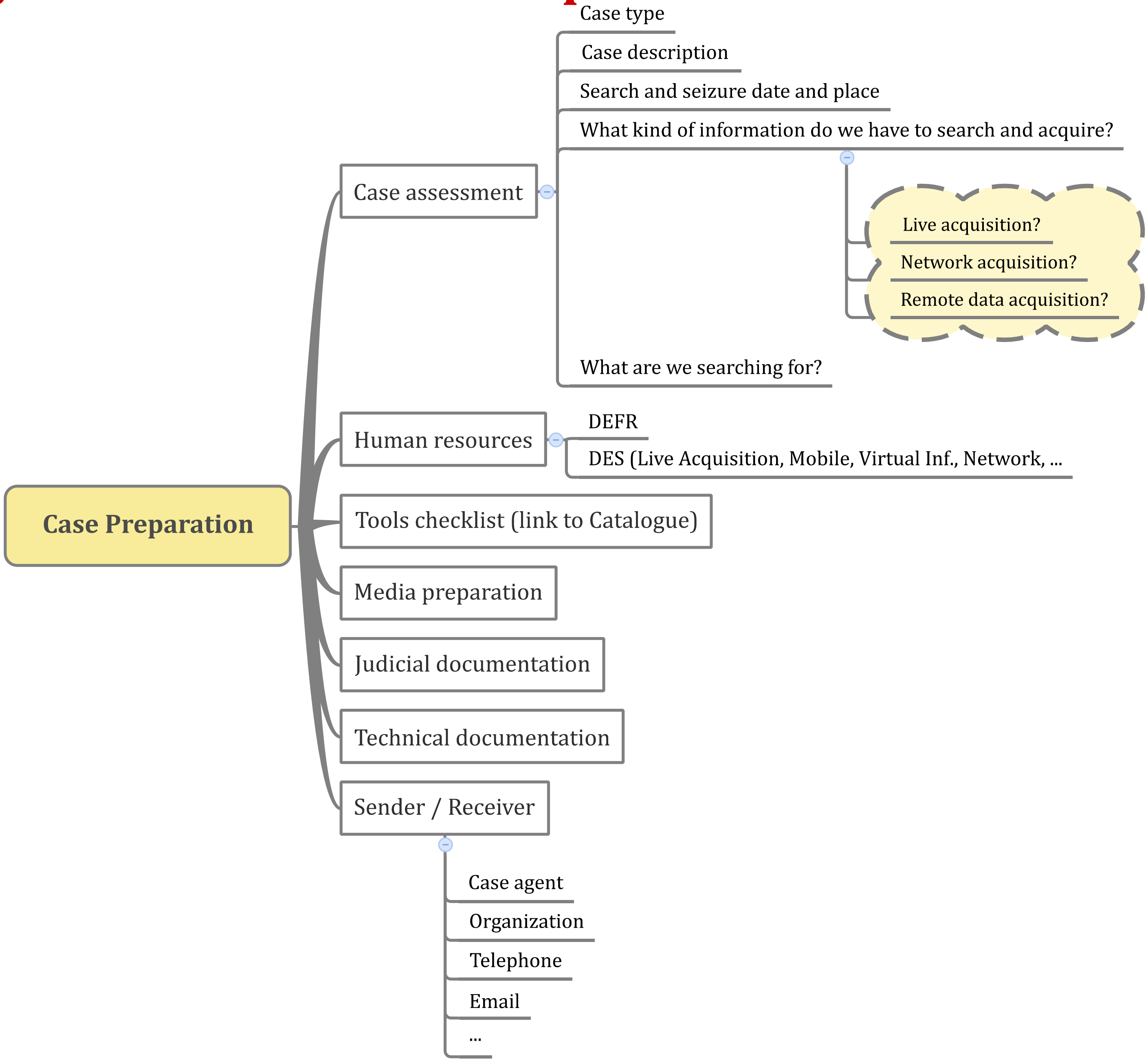


Electronic Evidence Exchange/Sharing Platform



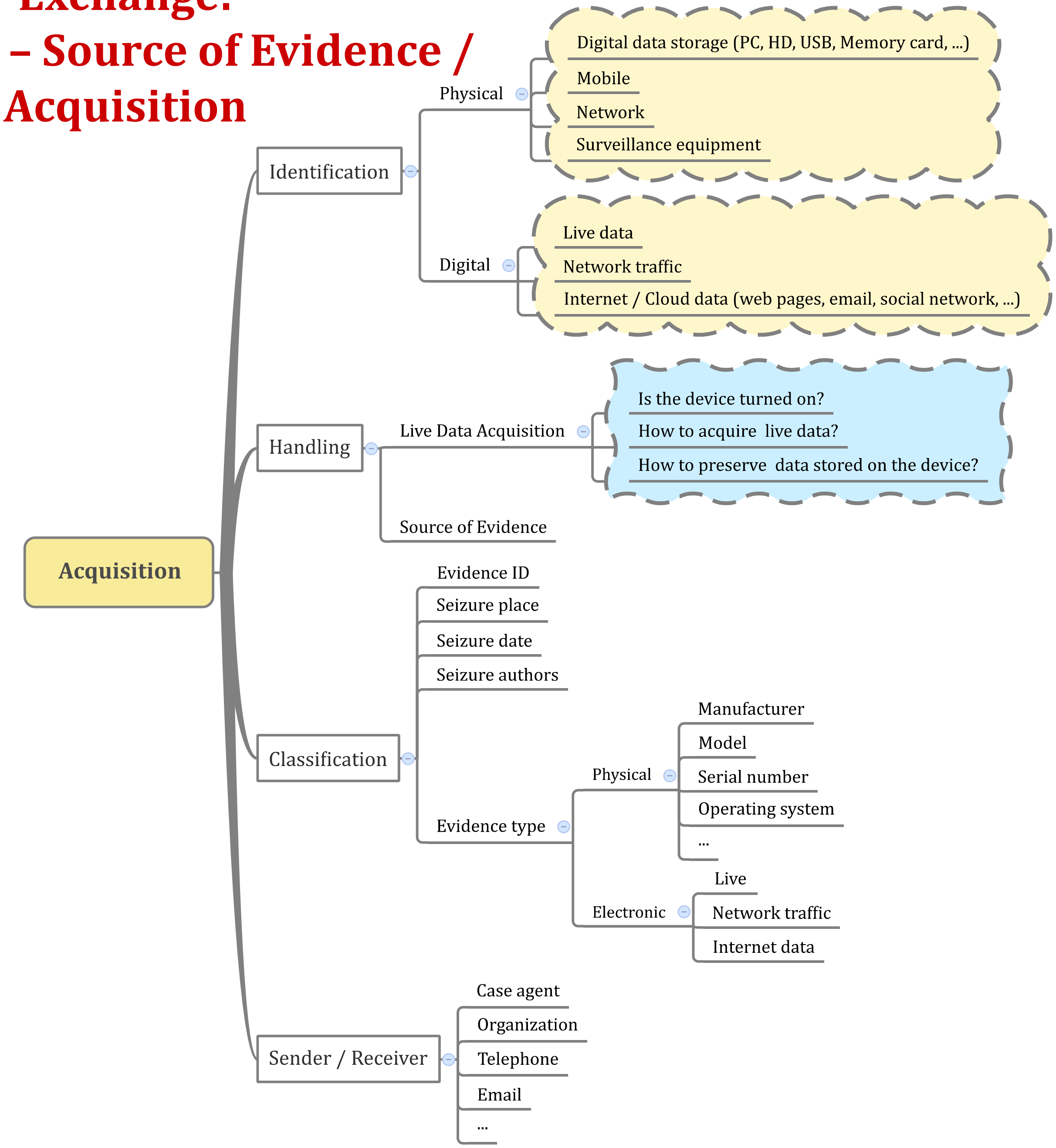
- *sharing data across different countries/jurisdictions*
- *privacy/security issues and solutions*
- *trusted mechanism*

Exchange: Use Case 0 – Case Preparation

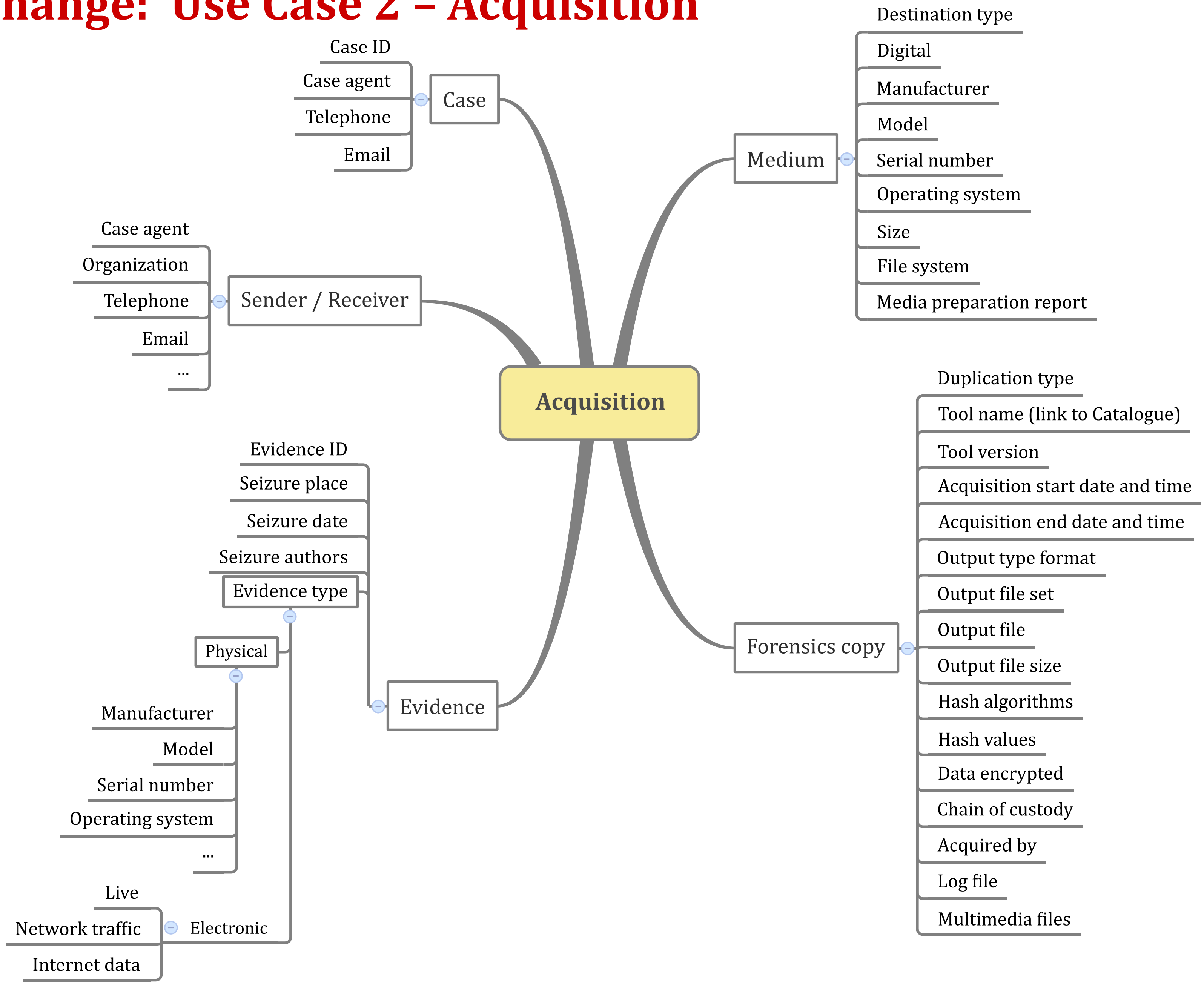


- Case Preparation
  - Case assessment
    - Case type
    - Case description
    - Search and seizure date and place
    - What kind of information do we have to search and acquire?
      - Live acquisition?
      - Network acquisition?
      - Remote data acquisition?
    - What are we searching for?
  - Human resources
    - DEFR
    - DES (Live Acquisition, Mobile, Virtual Inf., Network, ...
  - Tools checklist (link to Catalogue)
  - Media preparation
  - Judicial documentation
  - Technical documentation
  - Sender / Receiver
    - Case agent
    - Organization
    - Telephone
    - Email
    - ...

Exchange:
Use Case 1 – Source of Evidence / Acquisition



Exchange: Use Case 2 – Acquisition



- Acquisition
  - Case
    - Case ID
    - Case agent
    - Telephone
    - Email
  - Sender / Receiver
    - Case agent
    - Organization
    - Telephone
    - Email
    - ...
  - Evidence
    - Evidence ID
    - Seizure place
    - Seizure date
    - Seizure authors
    - Evidence type
      - Physical
        - Manufacturer
        - Model
        - Serial number
        - Operating system
        - ...
      - Electronic
        - Live
        - Network traffic
        - Internet data
  - Medium
    - Destination type
    - Digital
    - Manufacturer
    - Model
    - Serial number
    - Operating system
    - Size
    - File system
    - Media preparation report
  - Forensics copy
    - Duplication type
    - Tool name (link to Catalogue)
    - Tool version
    - Acquisition start date and time
    - Acquisition end date and time
    - Output type format
    - Output file set
    - Output file
    - Output file size
    - Hash algorithms
    - Hash values
    - Data encrypted
    - Chain of custody
    - Acquired by
    - Log file
    - Multimedia files

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

Thanks for your attention!

mariangela.biasiotti@ittig.cnr.it
mattia.epifani@ittig.cnr.it
fabrizio.turchi@ittig.cnr.it