EVIDENCE

EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE

Interscambio di Digital Evidence nei Paesi membri dell'UE: il progetto EVIDENCE

Institute of Legal Information Theory and Techniques
Italian National Research Council

Mattia Epifani

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

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

Progetto EVIDENCE : principali dati

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

- Durata: 30 mesi(marzo 2014 – agosto 2016)
- Coordinatore: CNR-ITTIG
- Finanziamneto: € 1,924,589.00 (CSA – Coordination and Support Action)
- Partners
  - CNR-ITTIG, CNR-IRPPS – CNR (Italia)
  - University of Groningen - RUG (Paesi Bassi)
  - International Criminal Police Organization - INTERPOL (Francia)
  - Leibniz University of Hannover - LUH (Germania)
  - Laboratory of Citizenship Science – LSC (Italia)
  - University of Malta – UOM (Malta)
  - Council of Bars and Law Societies of Europe - CCBE (Belgio)
  - Centre of Excellence in Information and Communications Technologies – CETIC (Belgio)
  - Law and Internet Foundation – LIF (Bulgaria)
- Sito web: 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

Progetto EVIDENCE: tema della Call

Nel contesto UE necessità di un **Quadro Comune** che disciplini l'uso delle tecnologie informatiche per la la gestione e lo scambio della prova elettronica nei processi penali

interpretato come

- Necessità di un avere **background comune** per tutti gli attori coinvolti nel ciclo di vita della Prova Elettronica: politici, Forze di polizia, Giudici, Avvocati
- Necessità di fare affidamento su **un livello normativo/giuridico comune** dedicato alla regolamentazione della Prova Elettronica nelle Corti
- Necessità di utilizzare **procedure standard** per l'utilizzo, la raccolta e lo scambio di Prove Elettroniche (attraverso gli Stati Membri dell'UE)

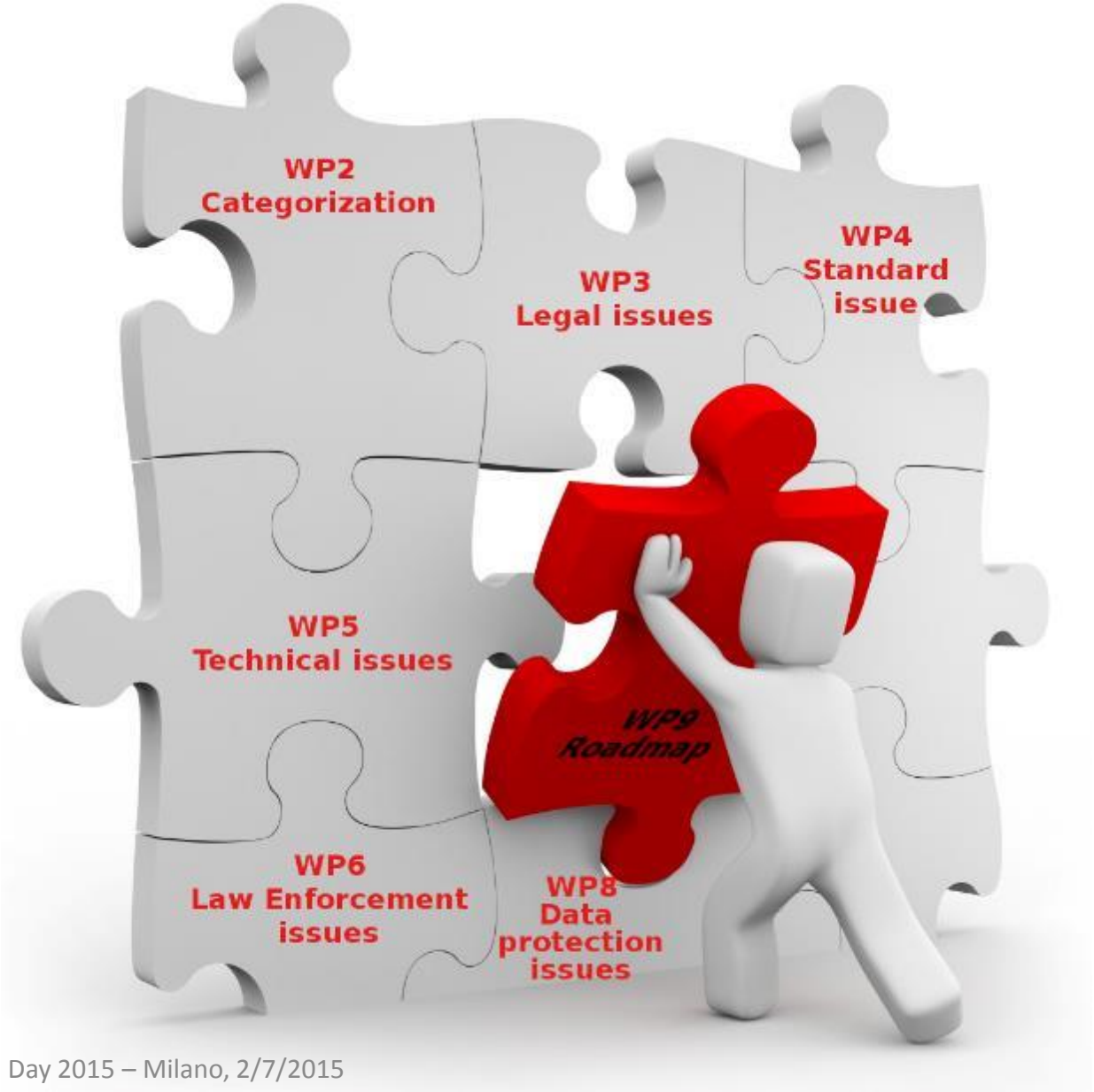
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

Progetto EVIDENCE: Principali obiettivi

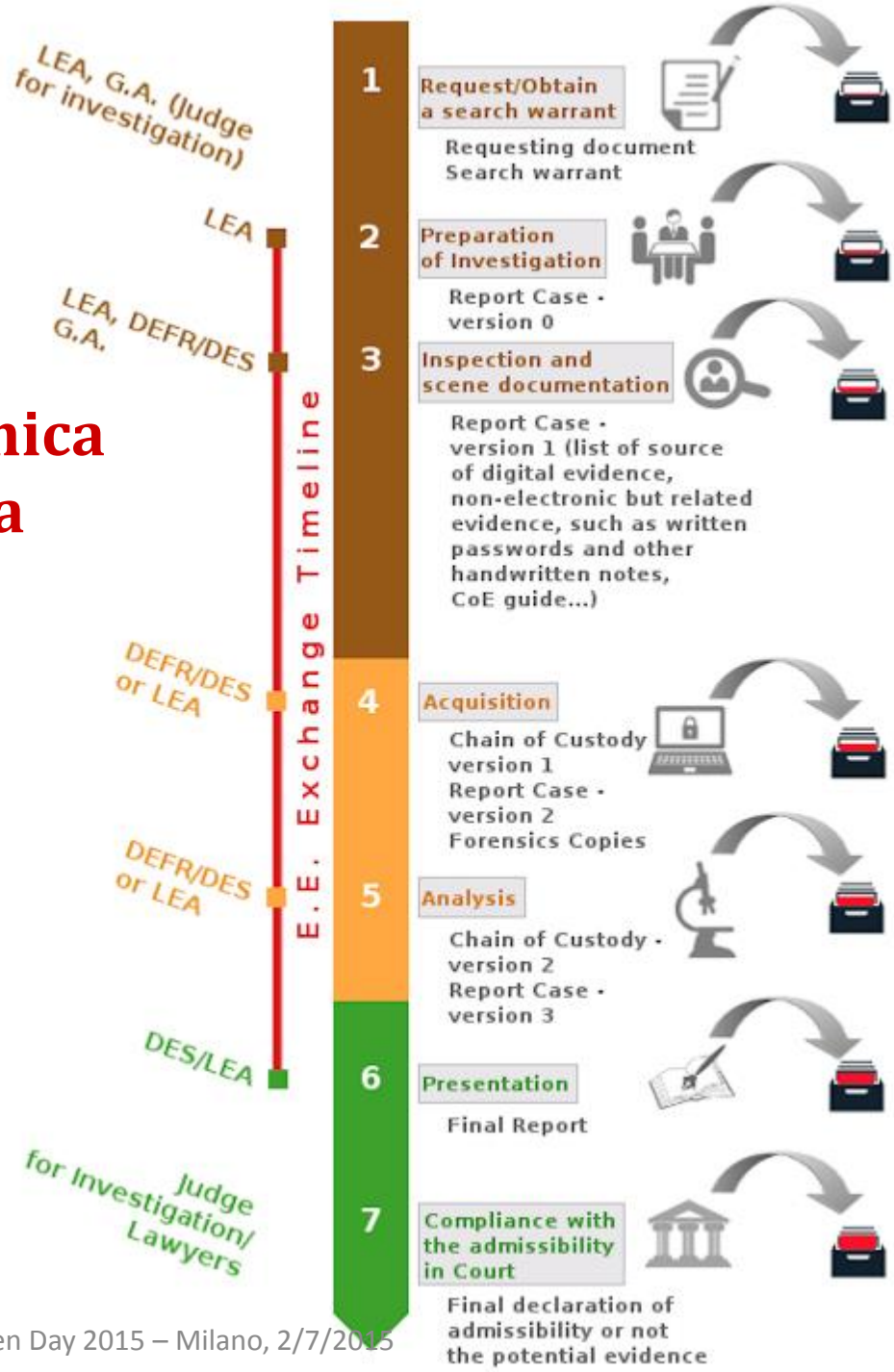
- Sviluppare una **Road Map** (linee guida, raccomandazioni, standard tecnici, un'agenda per futuri progetti di ricerca) al fine di creare un **Quadro Comune Europeo** per l'applicazione uniforme e sistematica delle nuove tecnologie nella raccolta, l'uso e lo scambio di prove
- Proporre delle **Regole** comuni per il trattamento delle **Prove**, sia quelle nate digitali che quelle digitalizzate in momenti successivi, considerando l'eventuale adeguamento delle regole e delle pratiche già esistenti
- Definire le implicazioni operative per le forze di Polizia e le problematiche relative al Trattamento dei Dati (**Privacy)**
- Capire quali siano le condizioni per uno **Scambio** sicuro e coerente di Prove raccolte tramite l'uso delle nuove tecnologie

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



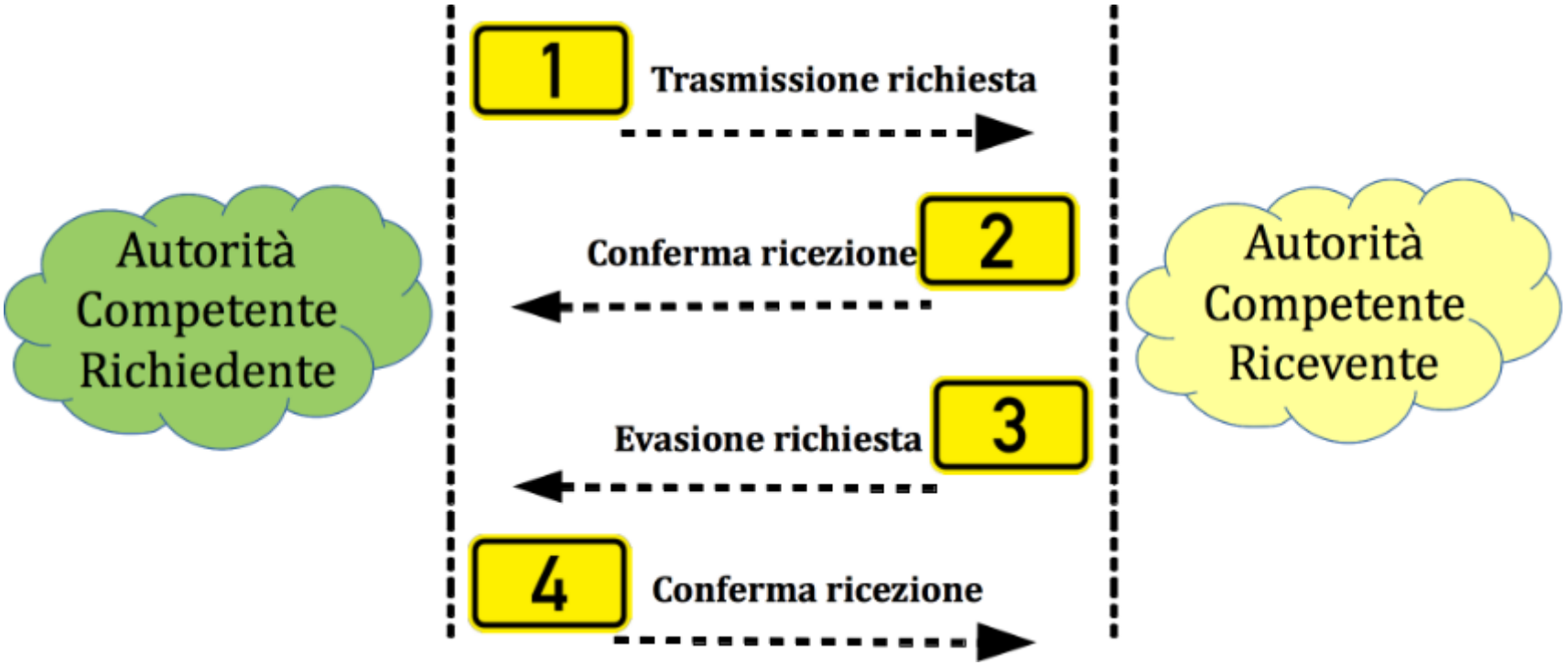
Prova Elettronica
Ciclo di Vita



EVIDENCE
EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE

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

Progetto EVIDENCE: Focus sullo Scambio della Prova



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

Riflessioni dagli incontri con gruppi di esperti

- **Le autorità di polizia richiedono strumenti e poteri investigativi più forti e incisivi**, compresa la possibilità di accedere, da remoto, ai dati memorizzati su una cloud;
- Il Consiglio d'Europa sta pensando ad un ampliamento della Convenzione sul Cybercrime (**Articolo 32 -** Accesso transfrontaliero a dati informatici immagazzinati con il consenso o quando pubblicamente disponibili);
- Alcuni paesi hanno già intrapreso **azioni concrete attraverso specifiche norme sulla materia**, come la Francia;
- L'introduzione di questi maggiori poteri richiede una valutazione di contemporanee **misure di salvaguardia** e dell'impatto sulla **ammissibilità di tali prove tra giurisdizioni diverse**

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

Conclusioni: primi risultati

- Le **sfide** che le autorità di polizia e giudiziarie devono affrontare sono, in larga misura, **simili nei vari paesi dell'UE**

"Un modo per costruire strumenti adatti a combattere il crimine è quello di aumentare la consapevolezza di queste sfide/difficoltà fra i legislatori nazionali e anche nei forum internazionali .Queste difficoltà sono le stesse per tutti I paesi e c'è quindi la necessità di affrontarle insieme."

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

Conclusioni: primi risultati

- **Gli strumenti di anonimizzazione e di crittografia** vengono più spesso indicati come i principali mezzi di intralcio/impedimento/disturbo alle indagini

"Dovrebbe essere possibile tracciare tutto il traffico di rete e dovrebbero essere adottate, a livello internazionale, misure per il controllo dell'utilizzo di TOR o strumenti simili, utilizzati per assicurare la comunicazione anonima su Internet. "

"Obbligare gli Internet Service Providers a fornire gli strumenti per la decodifica dei dati, in caso siano codificati (e.g. WhatsApp, Viber, ecc.)."

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

Conclusioni: primi risultati

- Sono richiesti **poteri investigativi più forti** per affrontare I casi più difficili (e.g. accesso remoto, dati in cloud, hacking, ecc.)

  "Strumenti più potenti per potenziare le intercettazioni su Internet attraverso una collaborazione più estesa ed efficiente fra gli Internet Service Providers.."

- Si auspica una cooperazione internazionale più ampia, forse anche attraverso lo scambio tra databases delle varie autorità.

- Una maggiore armonizzazione/standardizzazione tra le procedure dei vari laboratori forensi, come nel caso dei laboratori per il DNA

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

Conclusioni: primi risultati

- Sono indispensabili procedure MLA più efficienti, soprattutto per quanto riguarda I tempi di esecuzione – la procedura richiederebbe l'utilizzo di mezzi digitali

  "Le autorità di polizia hanno bisogno di maggiore cooperazione e di scambiare prove digitali in maniera più semplice e veloce."

  "There can be a policy measure under which regulators from one country can provide police forces from other country with requested information without MLAT. This can speed-up the investigations of cybercrime."

  "Misure per velocizzare le procedure relative allo scambio sia delle prove digitali che delle informazioni investigative."

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

Digital Forensics Tools Catalogue
Exchange/Sharing - cloud platform
Exchange – metadata and formal languages

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

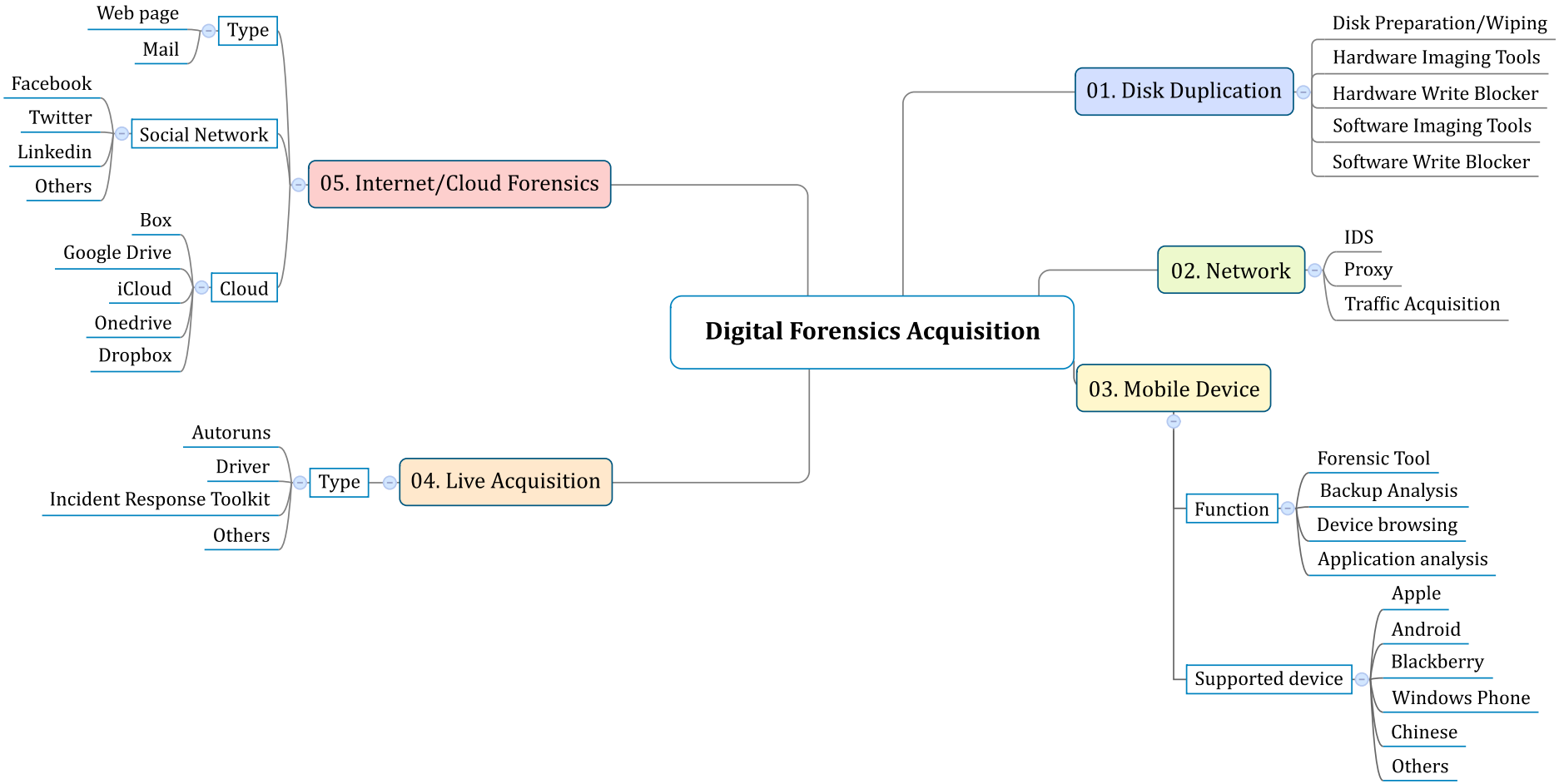
- The most significant digital forensics tools related to:
  - Acquisition: **324**
  - Analysis: **957**
- The total number of software tools collected so far (Jan 2015) is **1.281**

- Organized using a specific **classification**:

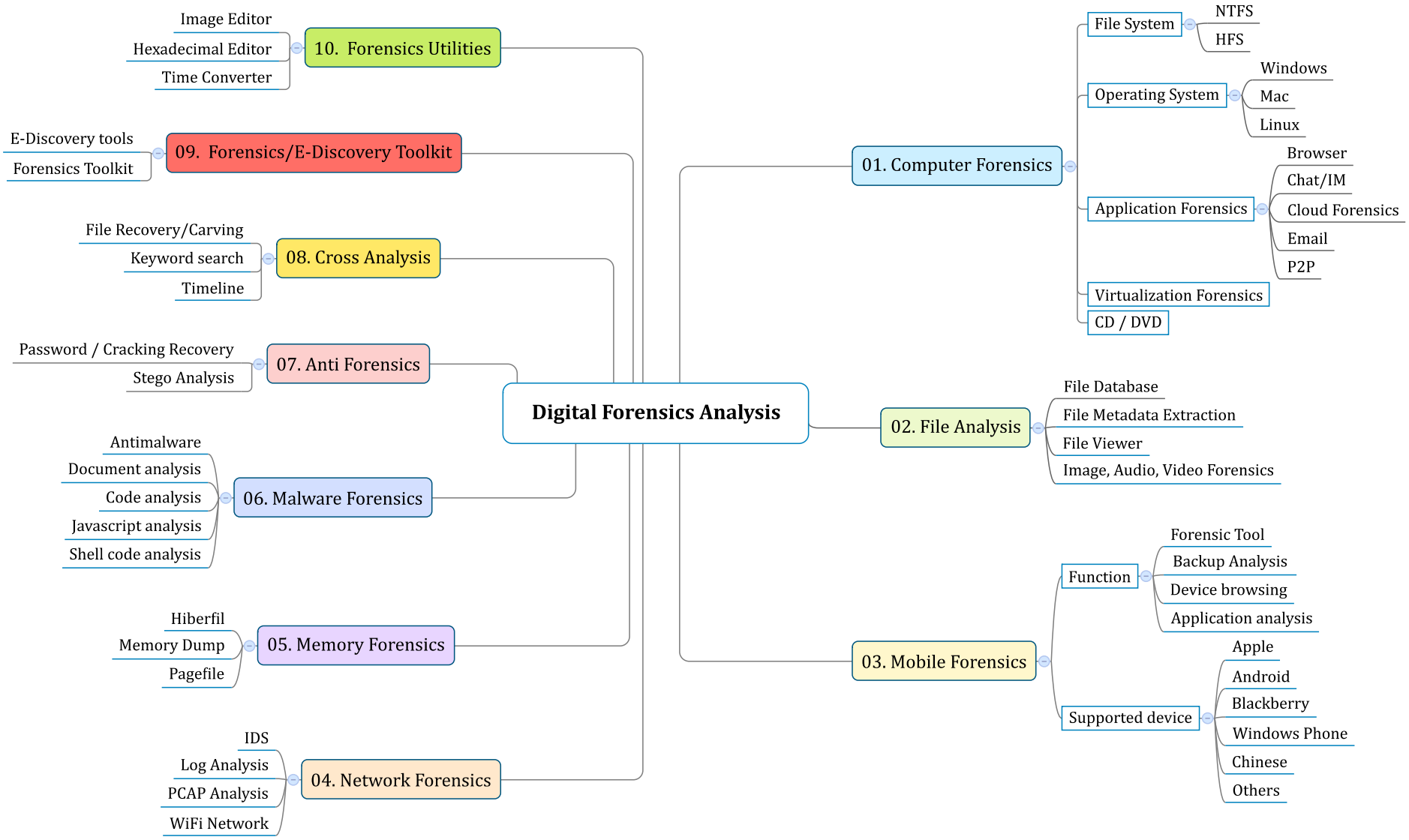
- **Acquisition**
  - 01. Disk duplication
    - 01.01. Write blocker hardware
    - 01.02. Write blocker software
  - …
- **Analysis**
  - 01. Computer Forensics
    - 01.01. File system
    - 01.02. Operating System
  - …

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



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, Questions

- No standard (compared with Acquisition and Analysis)
- It seems mostly human based

- 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?

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 status quo

- In cross-borders criminal cases, cooperation is mostly based upon **international agreement**, for example Convention on Mutual Assistance in Criminal Matters between Member States.
- Independently from the legal framework identified by the EU Member States, the cooperation is mostly **human based.**
- This situation seems similar across countries and, at first glance, the Exchange does not appear based on any electronic means at all.

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
Data held by third-party service providers

- There is a well-established cooperation between judicial authorities and Internet Service Providers (ISP)
- Requested information does not involve personal data (e.g. IP addresses, communication log , etc.) or information does involve personal data (e.g. email accounts, social network profile, messages, etc.)
- Data acquisition is managed through a platform provided by the ISP via web: it is **a real case of Electronic Evidence Exchange**

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: main questions

- No standard (confronted with Acquisition and Analysis)
- Chiefly human based (exception ISPs)

- Exchange within the same country or between countries:
  - What information is exchanged?
  - How the information is exchanged (even taking into consideration privacy/security issues)?
  - Which kind of stakeholders are involved?
  - Which different cases may occur in the Exchange?
- **Have these existing platforms, been already implementing the E.E. Exchange**?
  - **SIENA** by Europol (Secure Information Exchange Network Application)
  - **s-TESTA** by Eurojust (secured Trans European Services for Telematics between Administrations)
  - **NFI** (Netherland Forensics Institute)?

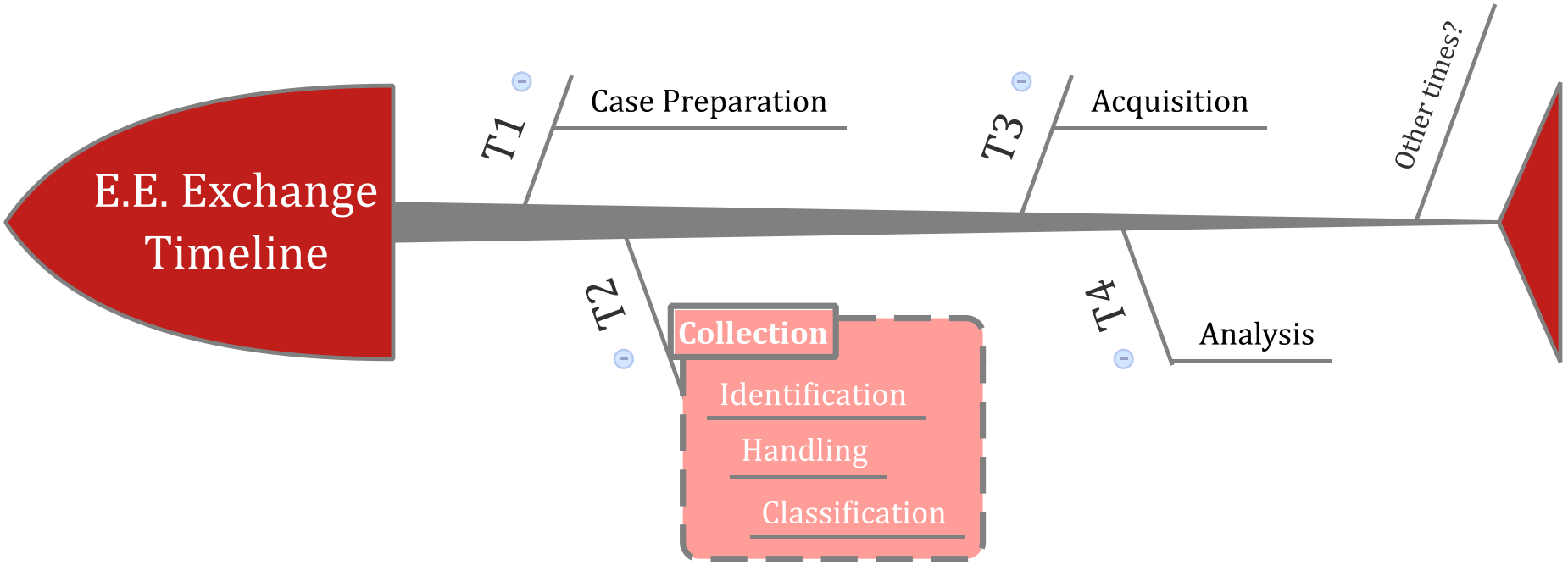
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

Electronic Evidence Exchange, Challenges

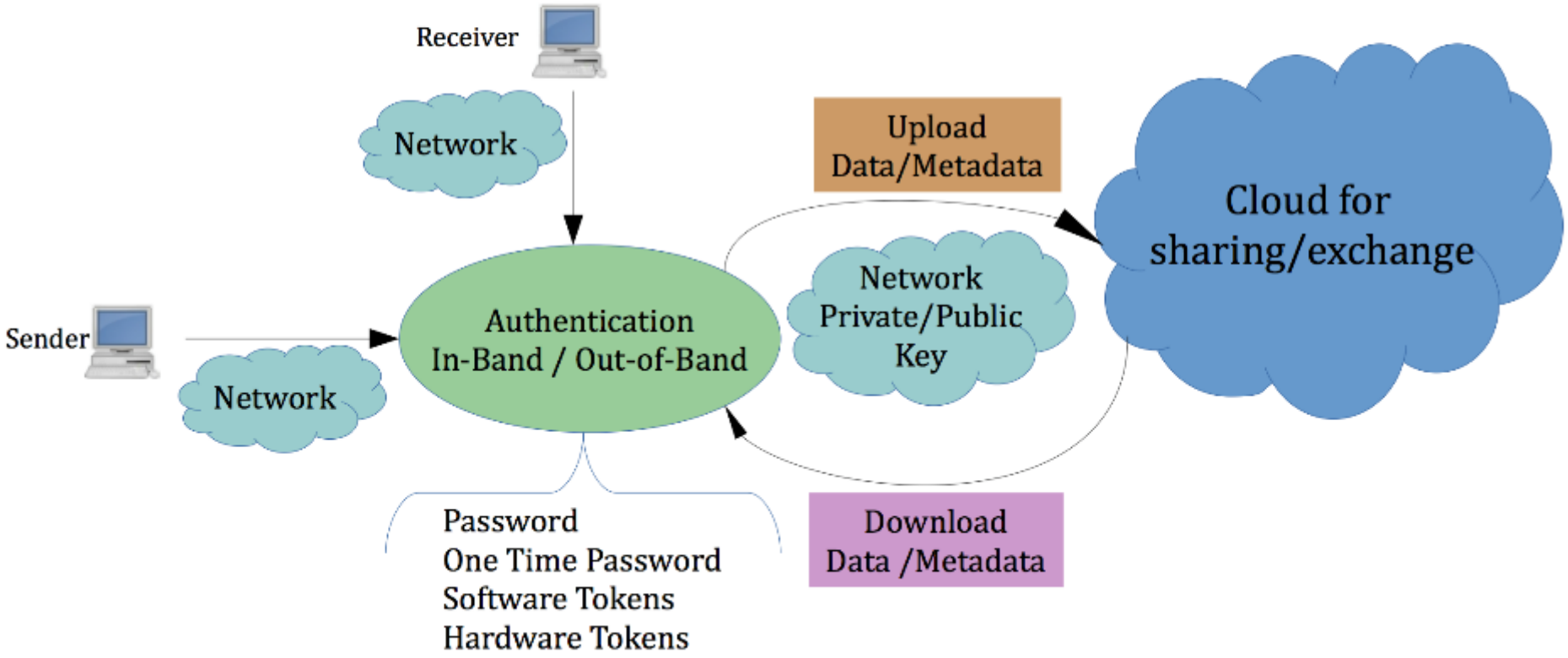
- **Exchange evidence procedures may be slow**. This aspect must be especially born in mind in investigative cases where time is crucial for fighting against serious cross-border and organized crime;
- Exchange evidence procedures may involve **big expenses**, such in case of travelling abroad to take the original/copy source of evidence to be handled;
- Judicial and Police authorities must **invest lots of money to keep up with the development of forensics technology**;
- Exchange trusted procedures are desired

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



- *ISO/IEC 27002 (security controls), 27017 (cloud)*
- *sharing data across different countries/jurisdictions*
- *privacy/security issues and solutions*
- *trusted mechanism*

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

Standard Languages

- Devising a formal standard language to represent the widest range of forensic information and forensic processing results

- The use of standard languages for the information exchange has been dealt in recent scientific contributions, published in 2014 by the European Union Agency for Network and Information Security **ENISA** (Actionable information for Security Incident Response)

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

Formal languages for D.F. information exchanging

- **DFXML** (Digital Forensics XML) by *S. Garfinkel*, aims:
  - tools interoperability
  - compare results produced by different tools
- **CybOX** (Cyber Observable eXpression) *E. Casey and others at MITRE.org*
  - open-source standardized representation of digital observables
  - represent digital actions and objects along with their context, and cover digital forensics information
  - developed with extensibility in mind: new object types can be added to CybOX without altering the core schema
- **DFAX** (Digital Forensic Analysis eXpression) that leverages CybOX for representing the purely technical information
- **UCO** Unified Cyber Ontology provide an abstract layer and express constructs that are common across the cyber domain (Action Lifecycle)

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

Formal languages for D.F. information exchanging: benefits

- **DFXML**, **DFAX**, **CybOX** and **UCO**
- Advantages:
  - Facilitating the **exchange process**
  - Fostering **tools interoperability**
  - Facilitating **tools verification**
- Need:
  - Tools should be able to **create/export** and **read/import** these format in order to guarantee the interoperability between tools and organizations

EVIDENCE
EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE

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

DFAX
(Digital Forensics Analysis eXpression)

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

Digital Forensics Analysis eXpression (DFAX)

- **Leverage CybOX to standardize representation and exchange of digital forensics information**, (Casey, Back, Barnum – DFRWS EU 2015)

- A new standard for **representing and exchanging digital forensics information** (https://github.com/dfax/dfax)

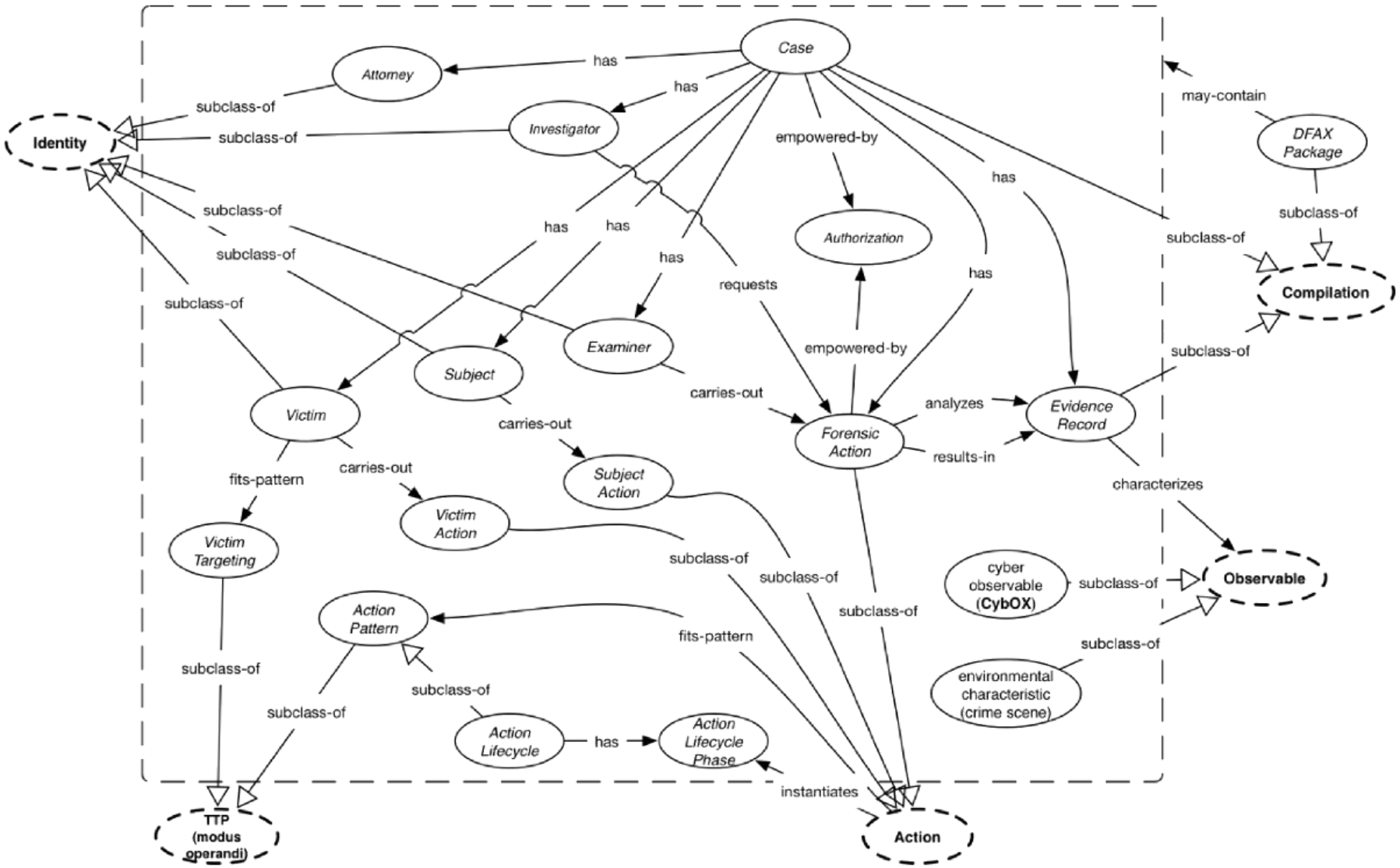
- It incorporates its own structure to represent the **more procedural aspects** of the digital forensics domain, including those for **chain of custody, case management, forensic processing**

- It covers information about:
  - Various roles involved in digital forensics
  - Various actions these roles takes
  - Evidence records resulting from forensic actions
  - Domain specific concepts such as authorizations

EVIDENCE
EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE

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

Digital Forensics Analysis eXpression (DFAX)



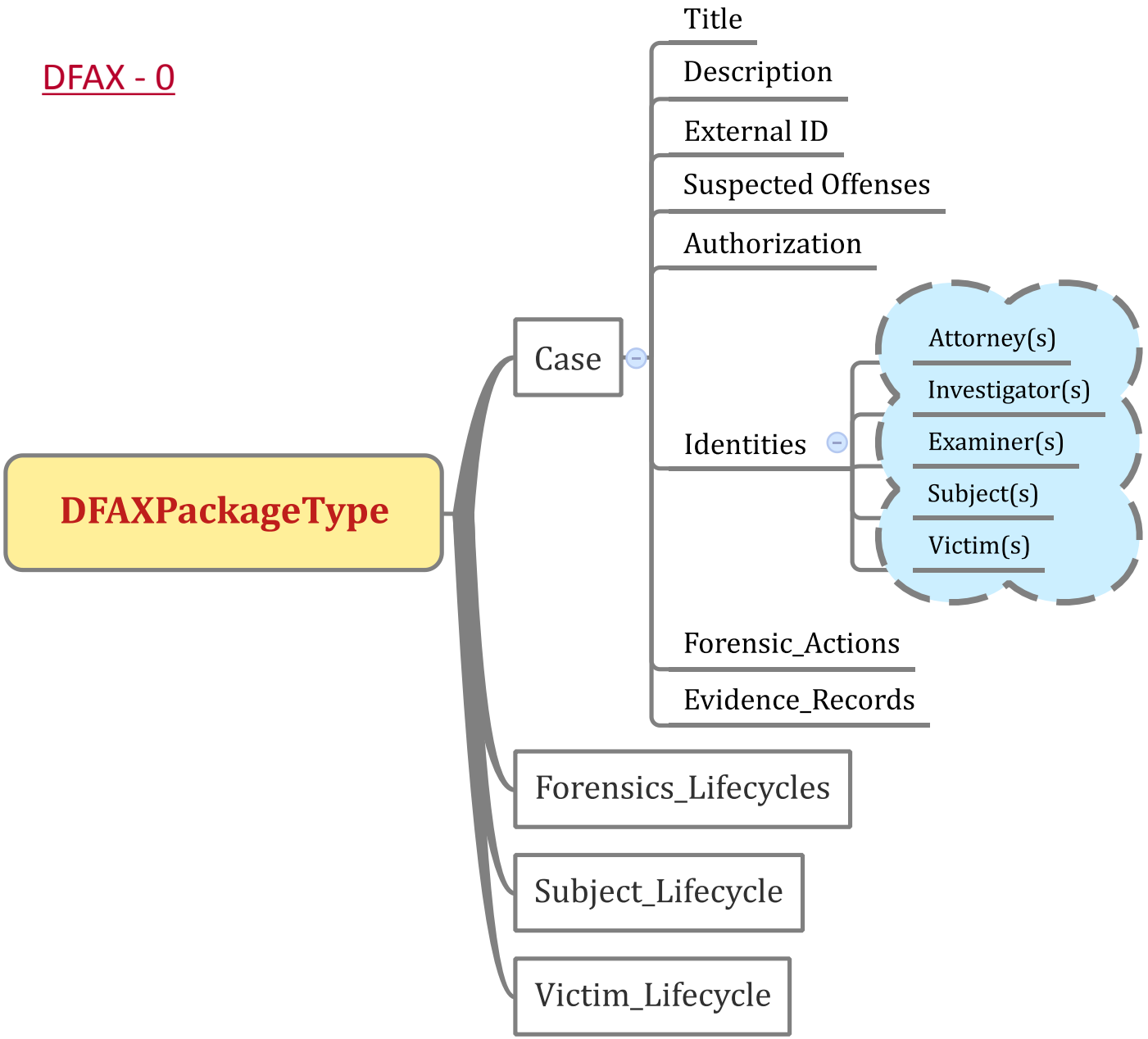
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

DFAX Schema

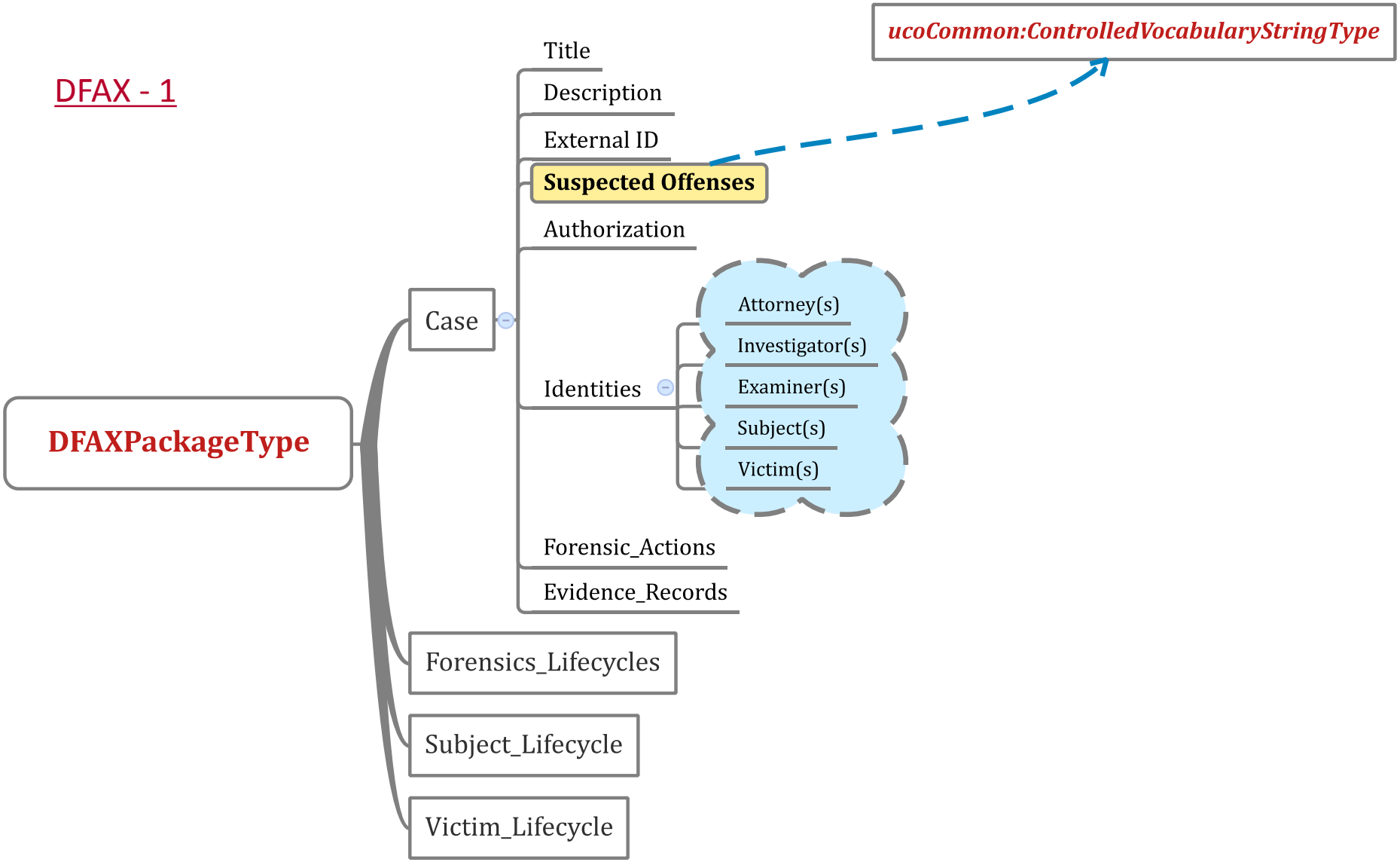
- Based on two XML Schema (XSD)
  - **dfax_core.xsd**
  - **uco_common.xsd**
- DFAX Core defines the "core" of DFAX
- UCO_Common = **Unified Cyber Ontology**
  - Express concepts/constructs that are common across the cyber domain
    - Identity
    - Date and Time
    - Action(s)
    - Observable(s)
    - Platform(s)
    - Tools(s)
    - Error(s)
    - …

ding from the European
rogramme for research,
ıd demonstration under
ıt agreement No608185

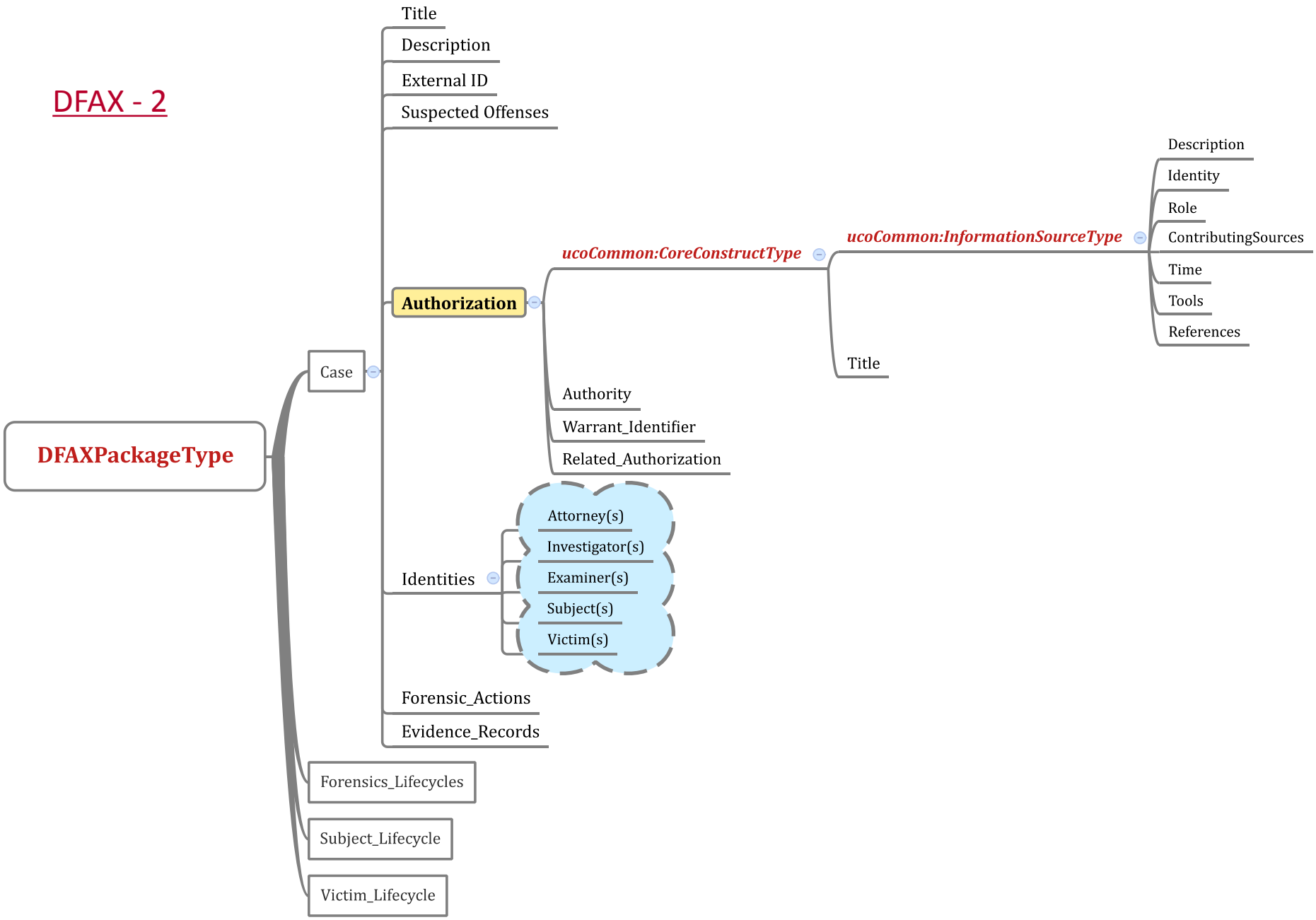
DFAX - 0



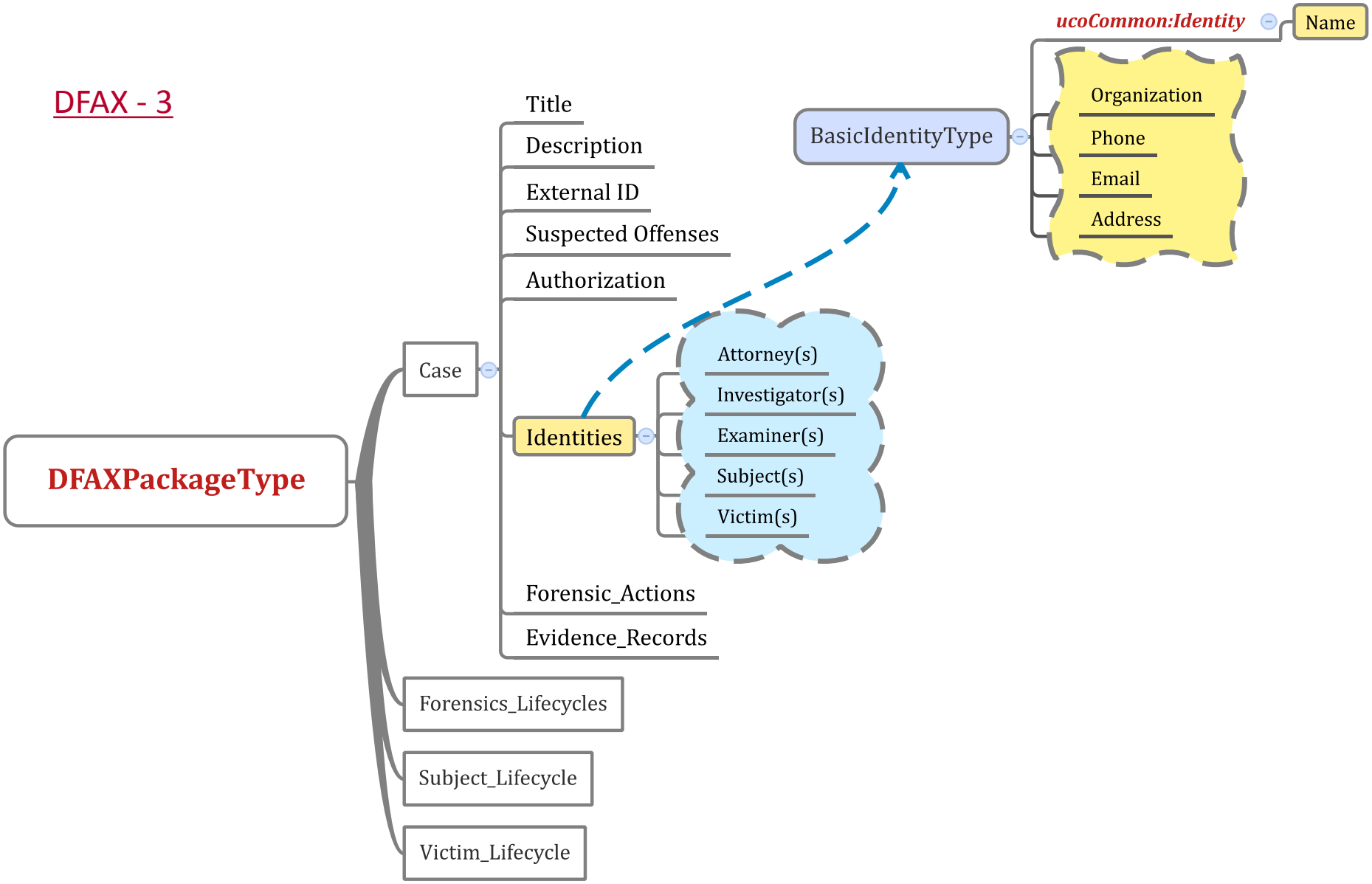
DFAX - 1


ucoCommon:ControlledVocabularyStringType
DFAXPackageType
Case
Title
Description
External ID
Suspected Offenses
Authorization
Identities
Attorney(s)
Investigator(s)
Examiner(s)
Subject(s)
Victim(s)
Forensic_Actions
Evidence_Records
Forensics_Lifecycles
Subject_Lifecycle
Victim_Lifecycle

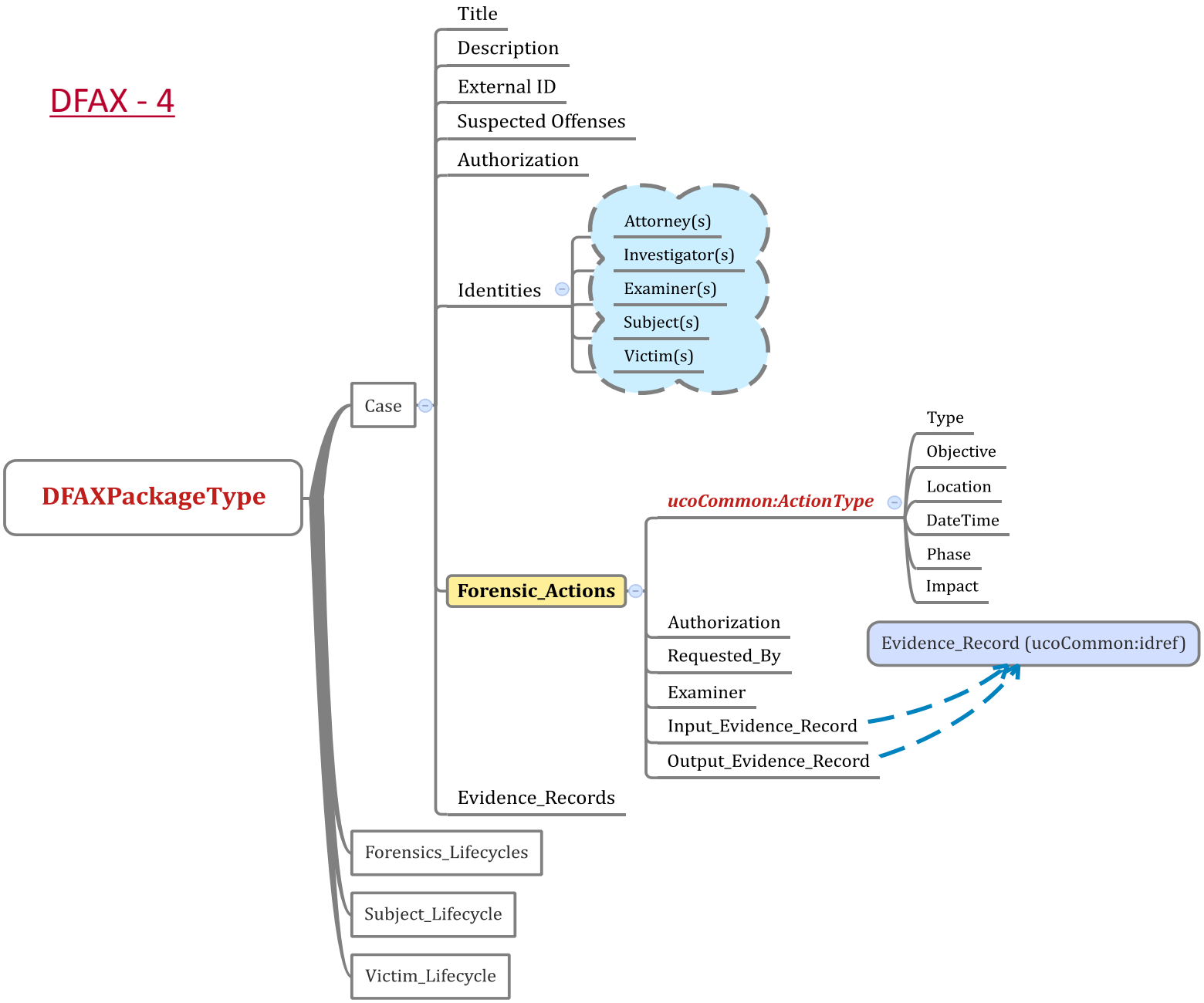
DFAX - 2


DFAXPackageType
Case
Title
Description
External ID
Suspected Offenses
Authorization
ucoCommon:CoreConstructType
ucoCommon:InformationSourceType
Description
Identity
Role
ContributingSources
Time
Tools
References
Title
Authority
Warrant_Identifier
Related_Authorization
Identities
Attorney(s)
Investigator(s)
Examiner(s)
Subject(s)
Victim(s)
Forensic_Actions
Evidence_Records
Forensics_Lifecycles
Subject_Lifecycle
Victim_Lifecycle

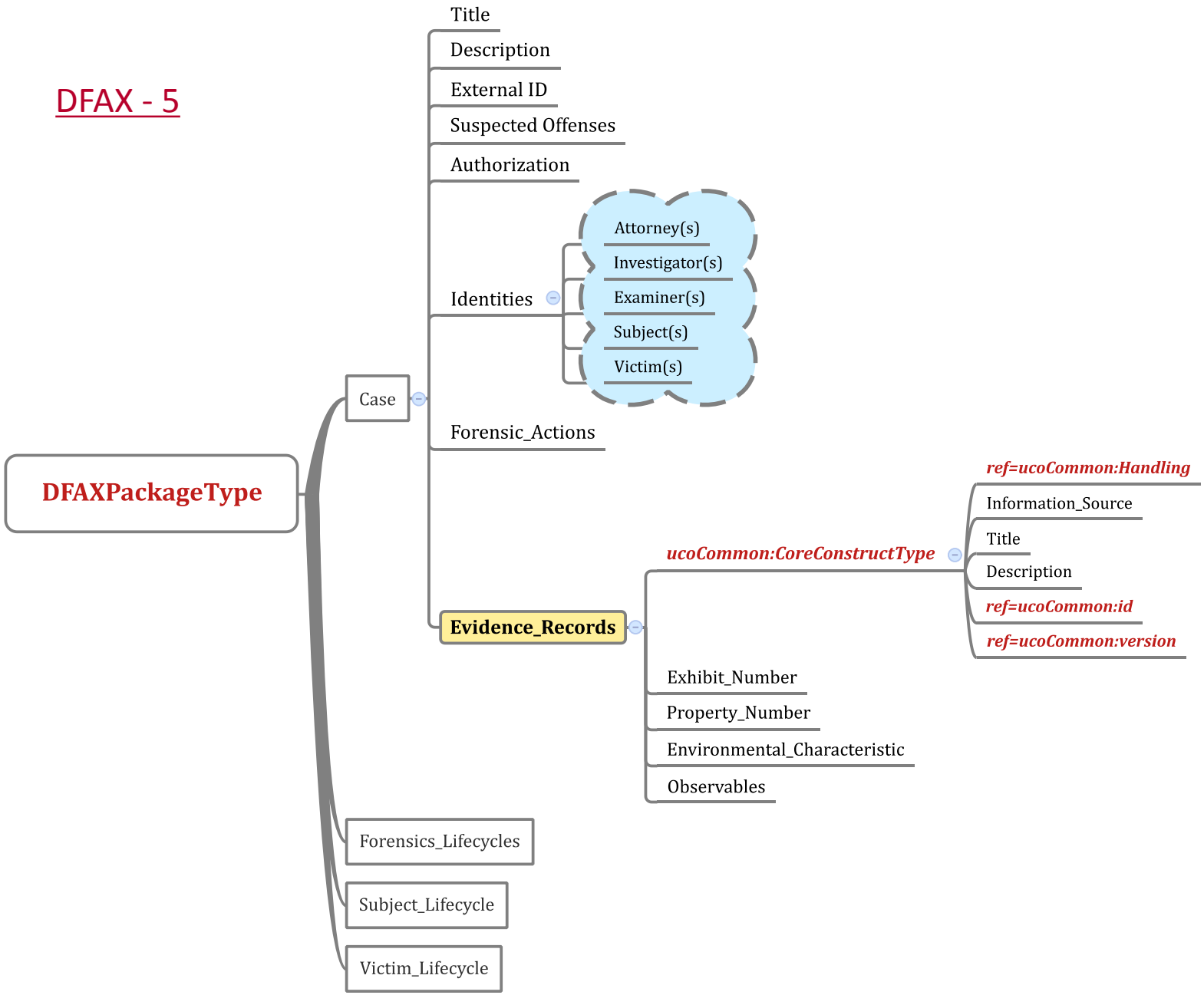
DFAX - 3


DFAXPackageType
Case
Title
Description
External ID
Suspected Offenses
Authorization
Identities
Attorney(s)
Investigator(s)
Examiner(s)
Subject(s)
Victim(s)
BasicIdentityType
ucoCommon:Identity
Name
Organization
Phone
Email
Address
Forensic_Actions
Evidence_Records
Forensics_Lifecycles
Subject_Lifecycle
Victim_Lifecycle

DFAX - 4

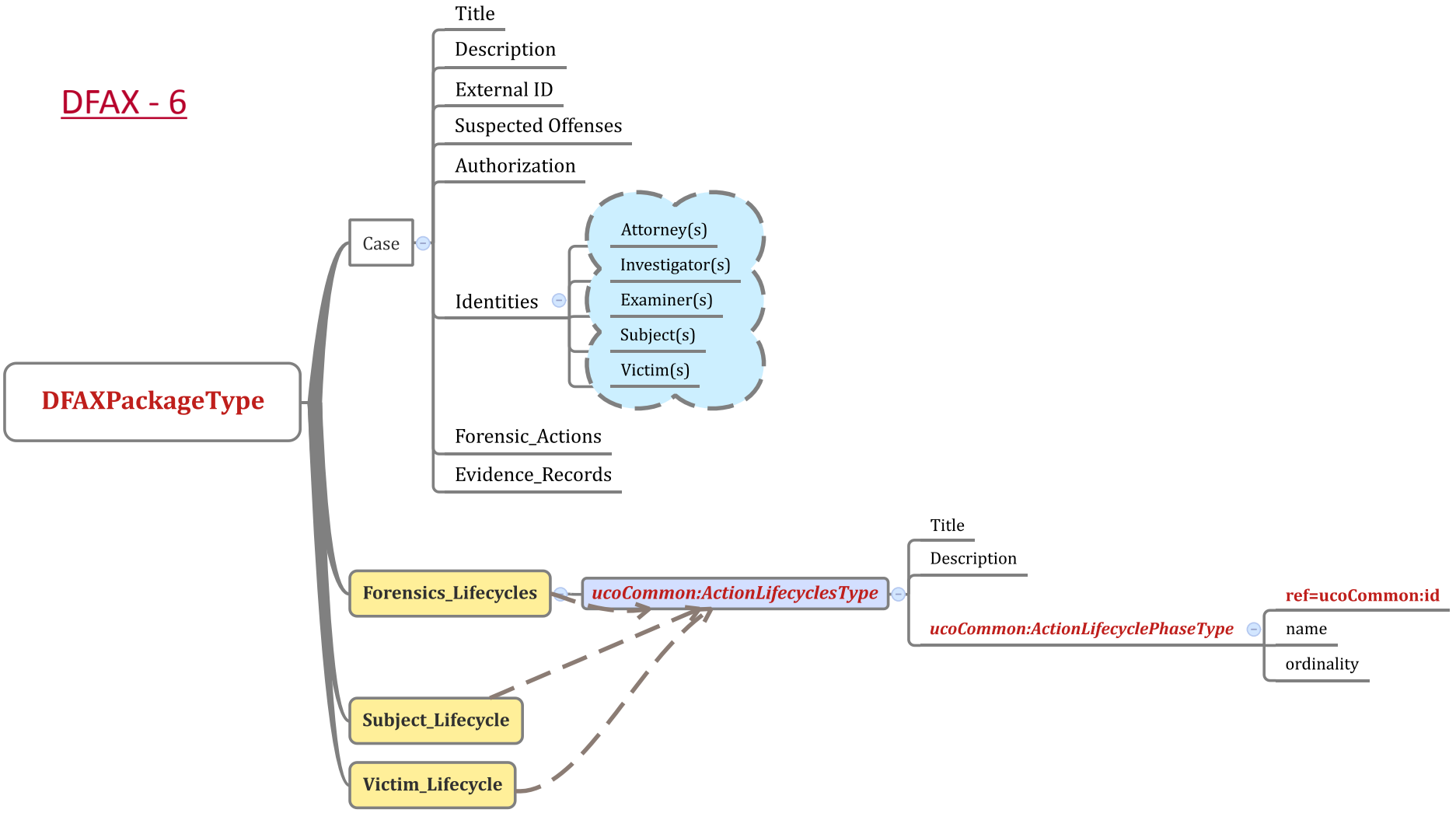

DFAXPackageType
Case
Title
Description
External ID
Suspected Offenses
Authorization
Identities
Attorney(s)
Investigator(s)
Examiner(s)
Subject(s)
Victim(s)
Forensic_Actions
ucoCommon:ActionType
Type
Objective
Location
DateTime
Phase
Impact
Authorization
Requested_By
Examiner
Input_Evidence_Record
Output_Evidence_Record
Evidence_Record (ucoCommon:idref)
Evidence_Records
Forensics_Lifecycles
Subject_Lifecycle
Victim_Lifecycle

DFAX - 5



ıropean
ɛsearch,
ɲ under
608185

DFAX - 6


DFAXPackageType
Case
Title
Description
External ID
Suspected Offenses
Authorization
Identities
Attorney(s)
Investigator(s)
Examiner(s)
Subject(s)
Victim(s)
Forensic_Actions
Evidence_Records
Forensics_Lifecycles
ucoCommon:ActionLifecyclesType
Title
Description
ucoCommon:ActionLifecyclePhaseType
ref=ucoCommon:id
name
ordinality
Subject_Lifecycle
Victim_Lifecycle

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

CybOX Objects

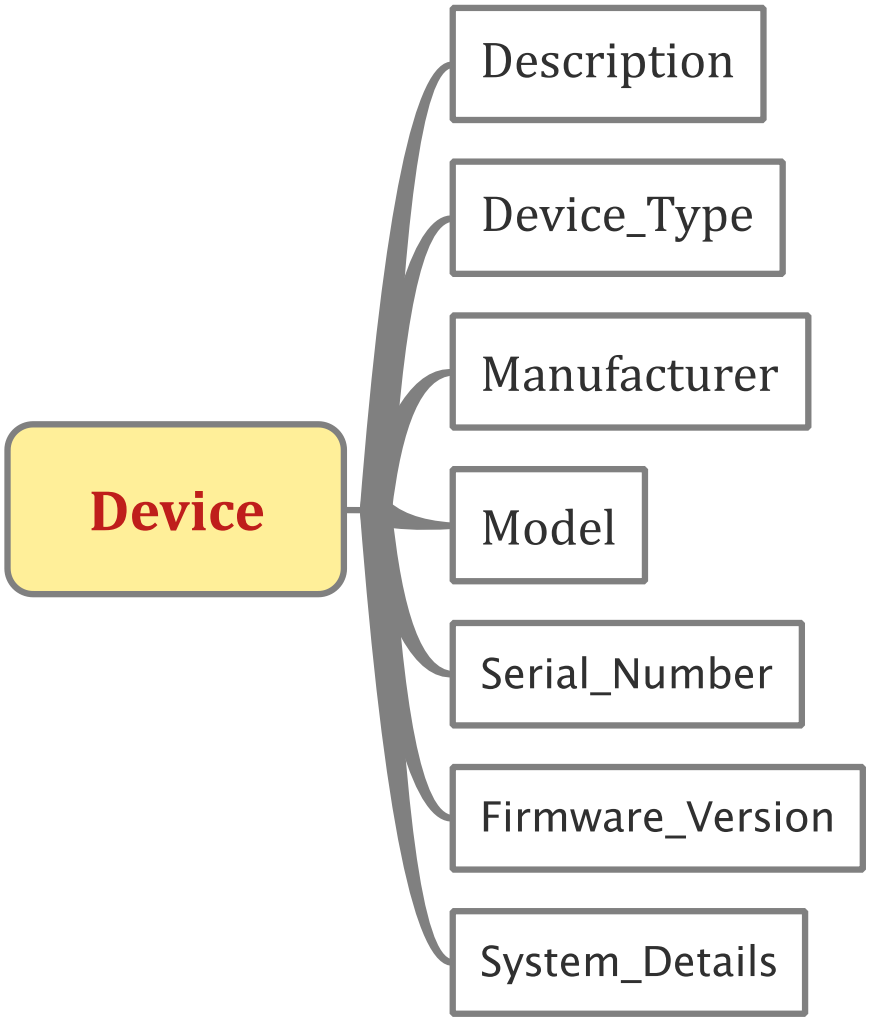
- Every object is described by an **XSD schema**, composed by **Elements** and **Complex Types**

- Some examples, useful in Digital Forensics

Object Name	Description
Device	Characterize a specific Device
Disk	Characterize a Disk Drive
Disk Partition	Characterize a single partition of a disk drive
Volume	Characterize generic disk volumes
WinVolume	Characterize Windows disk volumes
File	Characterize a single generic file
System	Characterize a computer system as a combination of both hardware and software

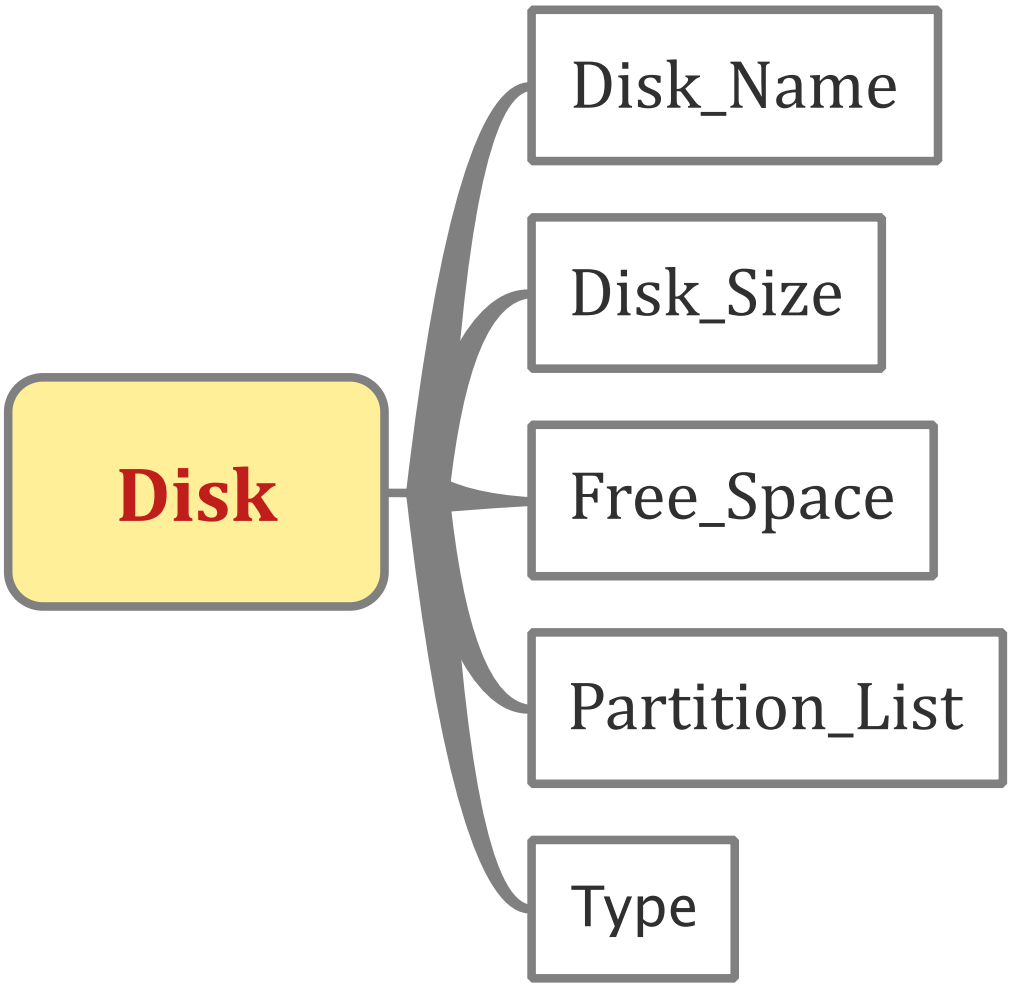
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

CybOX Objects: Device



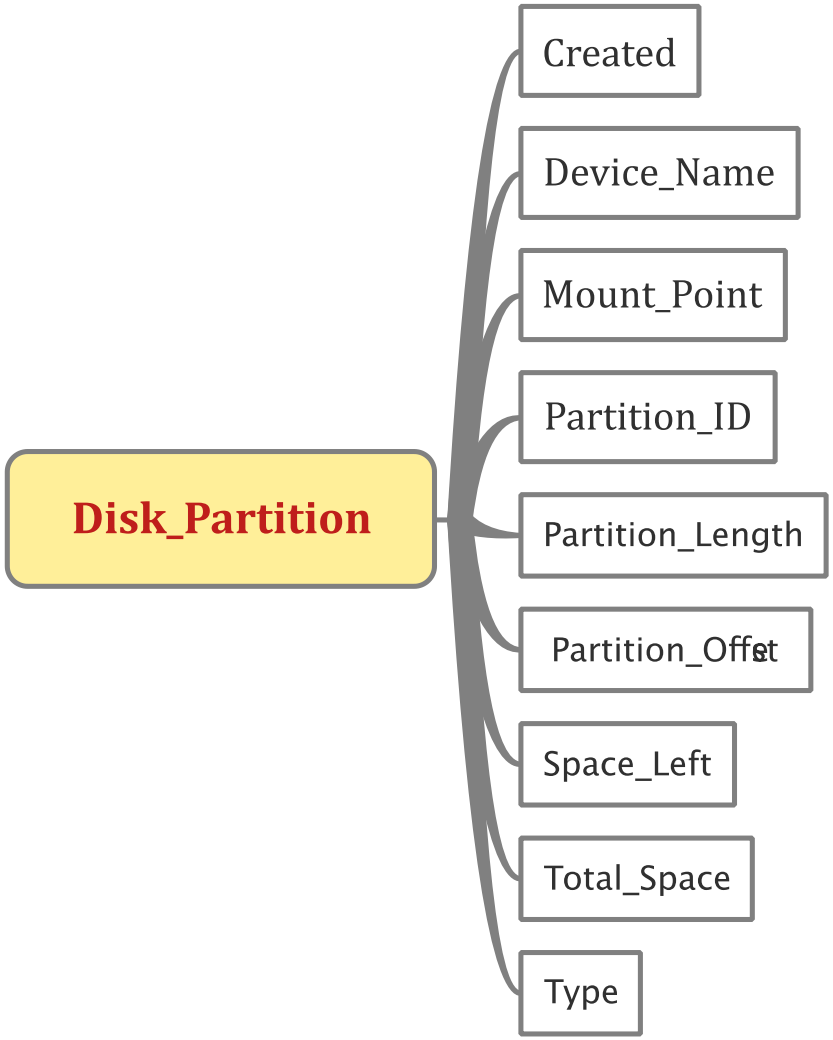
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

CybOX Objects: Disk



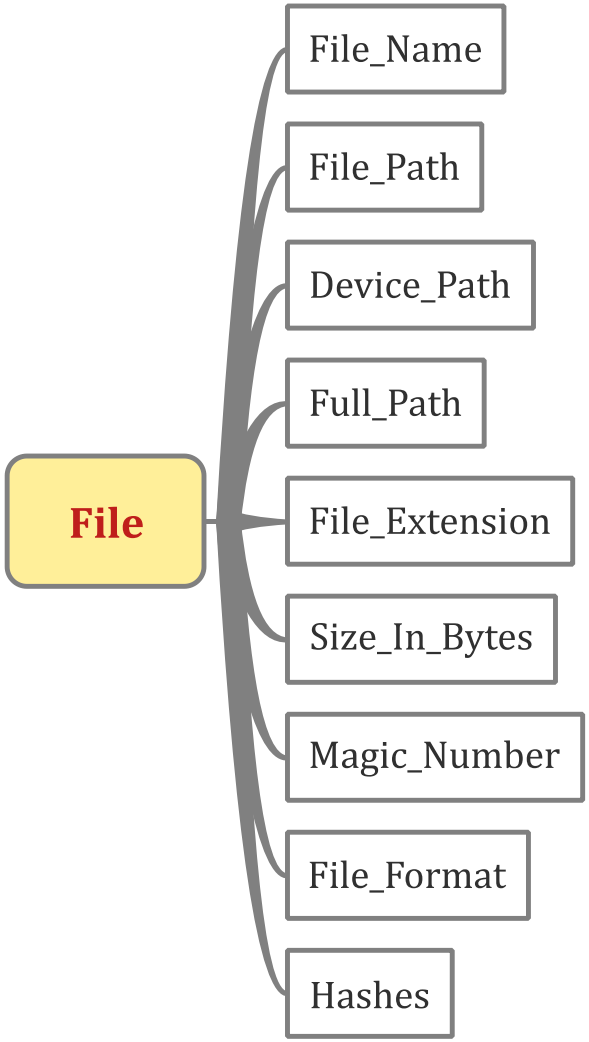
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No608185

CybOX Objects: Disk_Partition



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

Cybox Objects: File



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

Other Useful CybOX Objects

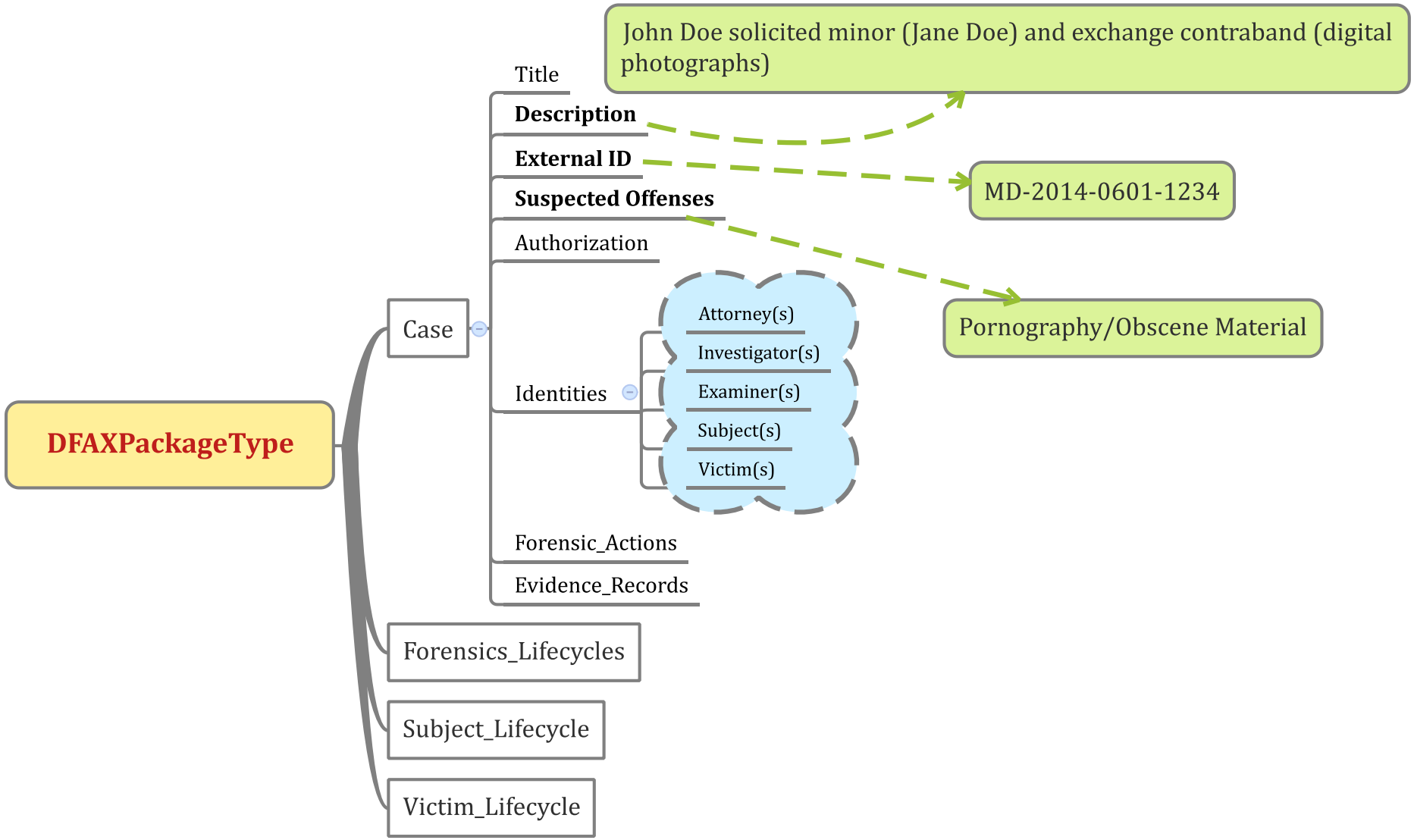
Object Name	Description
Archive File	Characterize an archive file
PDF File	Characterize structural and metadata information regarding a single PDF file
Image File	Characterize an image file
Email Message	Characterize an email file
WinFile	Characterize Windows files
WinExecutableFile	Characterize Windows PE (Portable Executable)
WinEventLog	Characterize entries in the Windows Event Log
WinPrefetch	Characterize entries in Windows Prefetch files
WinRegistryKey	Characterize windows registry objects (Keys and Keys/Values)
URLHistory	Characterize a stored URL History on a particular web browser

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

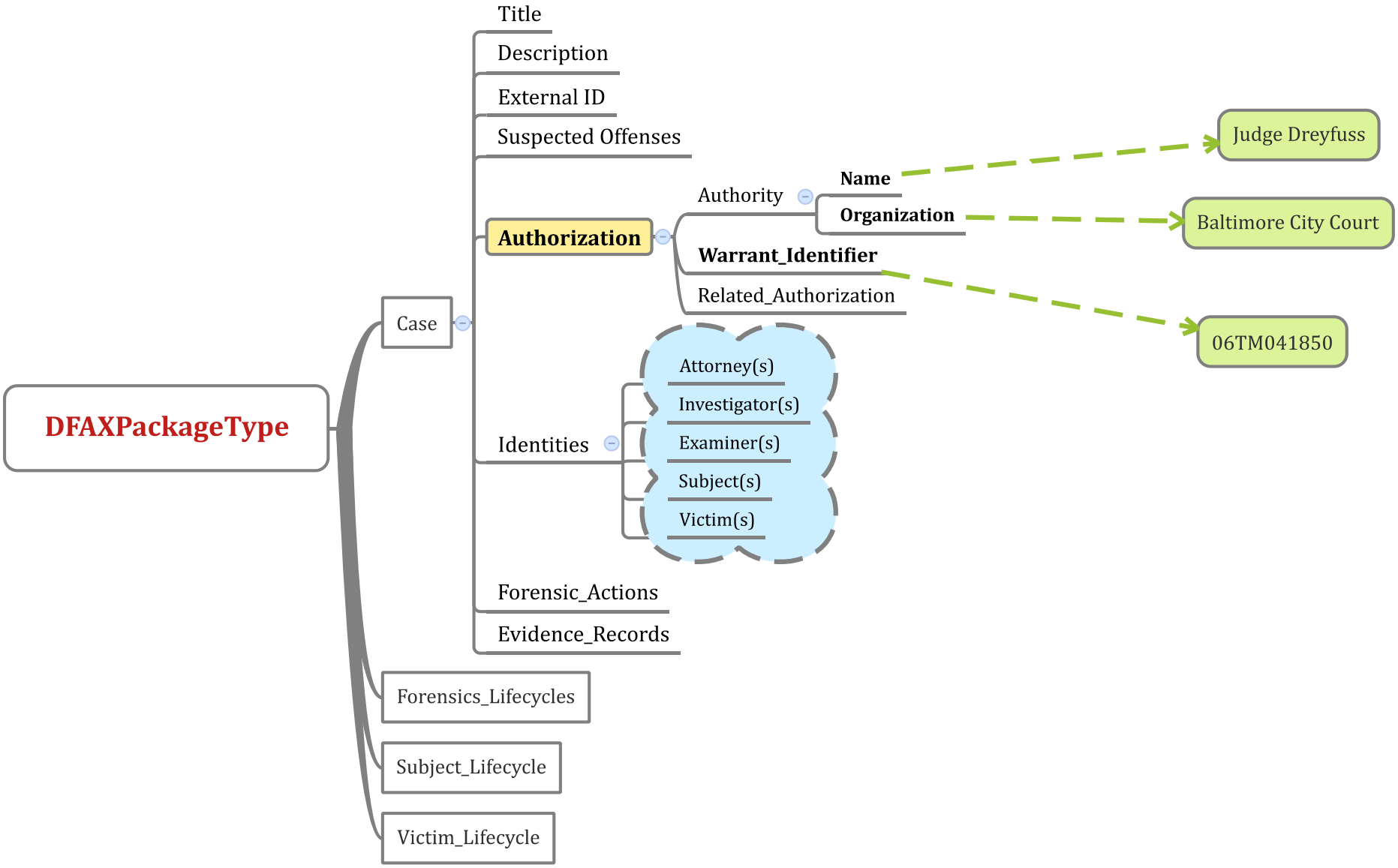
Basic example

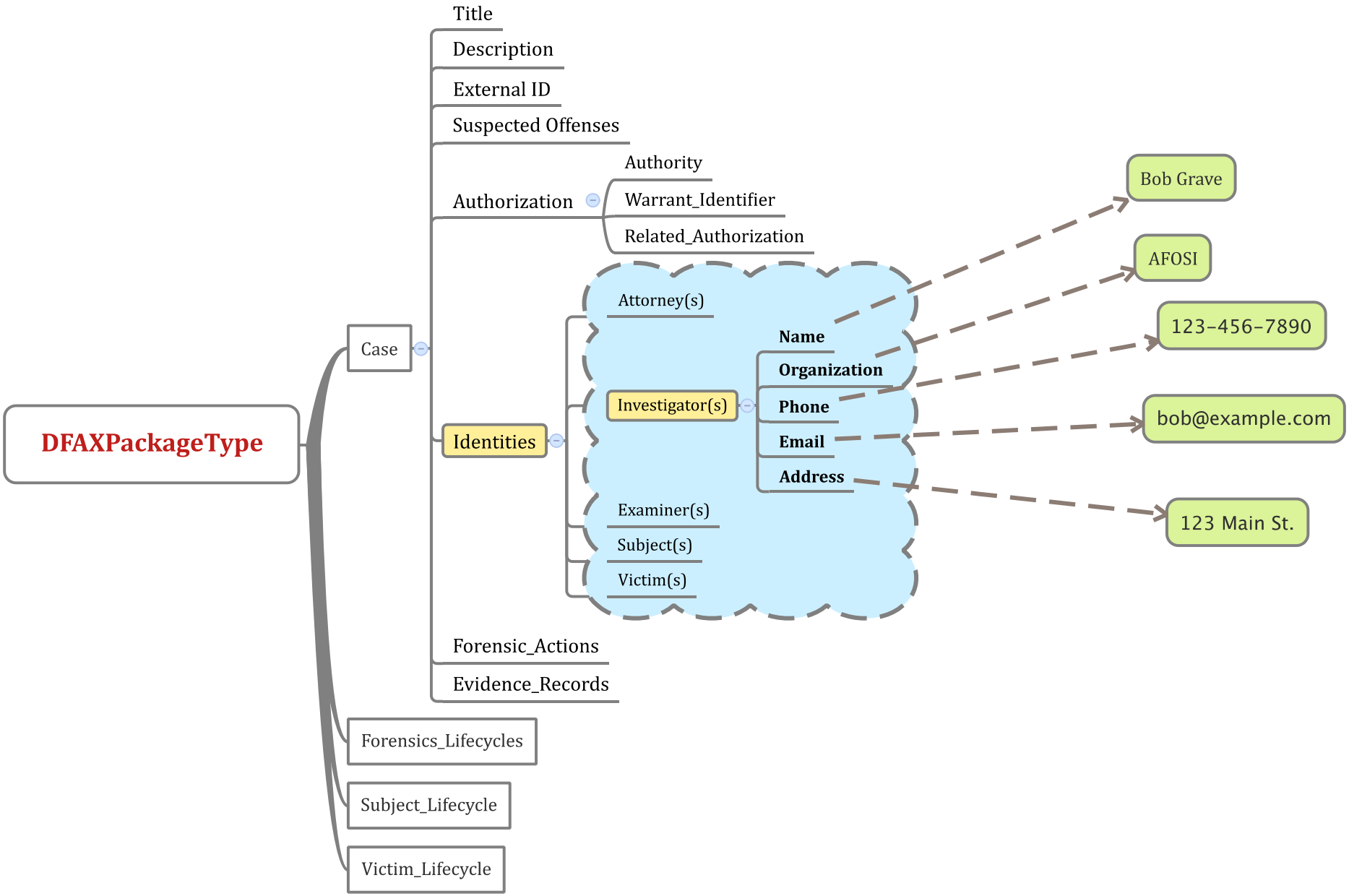
- **Case**
  - Minor solicitation and digital photos exchange
- **Identities**
  - Autority (*judge Dreyfuss*)
  - Investigator (*Bob Grave*)
  - Examiner
  - Subject (*Jonh Doe*)
  - Victim (*Jane Doe*)
- **Forensic Lifecycle**
  1. Preparation
  2. Preservation
  3. Examination
  4. Analysis
  5. Report
- **Forensics Actions**
  - Subject's mobile phone seizure
  - Device examination to find communications between the Subject and the Victim

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

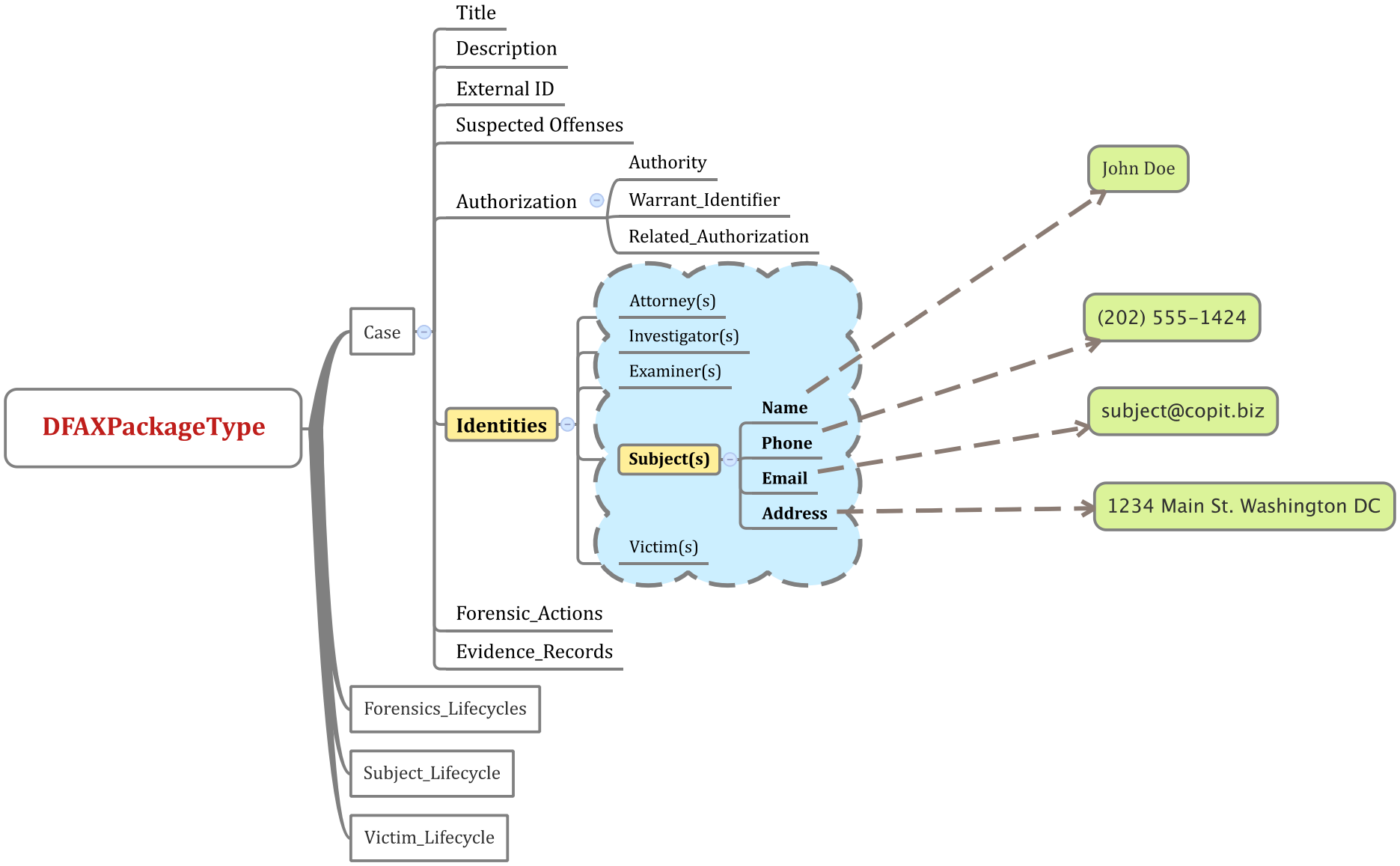


This project has received funding from the European Union's Seventh Framework Programme for research,



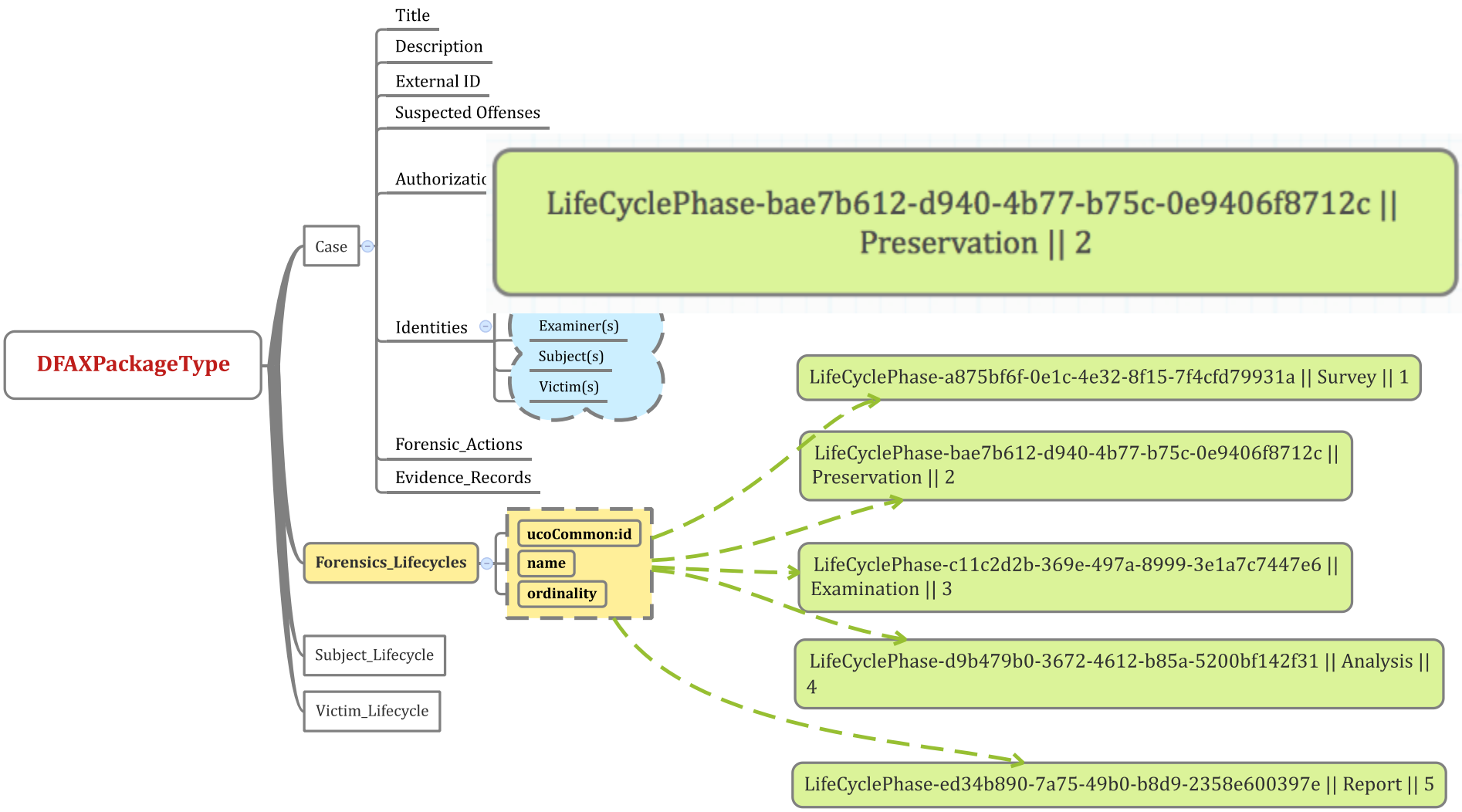

DFAXPackageType
Case
Title
Description
External ID
Suspected Offenses
Authorization
Authority
Warrant_Identifier
Related_Authorization
Identities
Attorney(s)
Investigator(s)
Name
Organization
Phone
Email
Address
Examiner(s)
Subject(s)
Victim(s)
Forensic_Actions
Evidence_Records
Forensics_Lifecycles
Subject_Lifecycle
Victim_Lifecycle
Bob Grave
AFOSI
123-456-7890
bob@example.com
123 Main St.

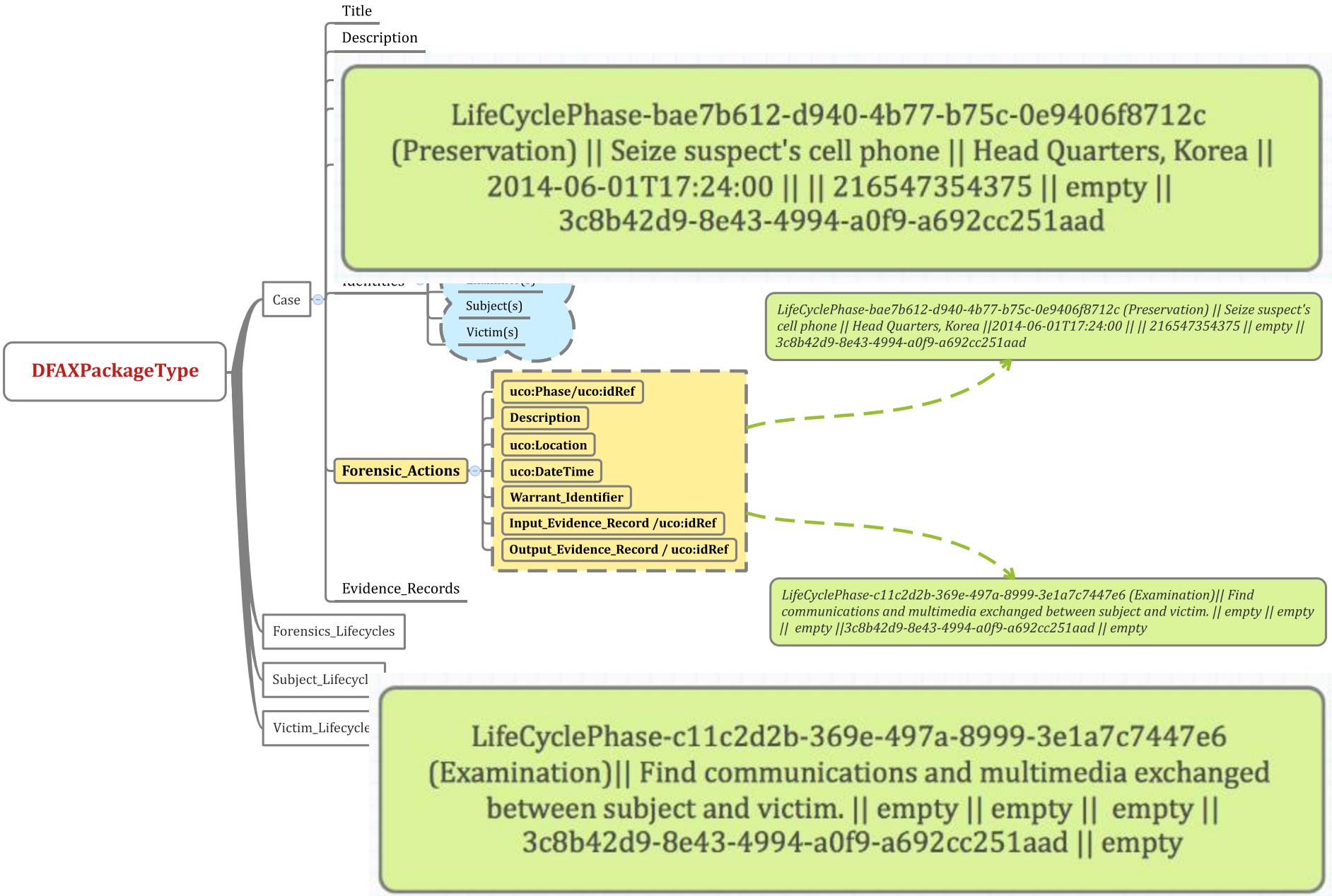
This project has received funding from the European Union's Seventh Framework Programme for research,



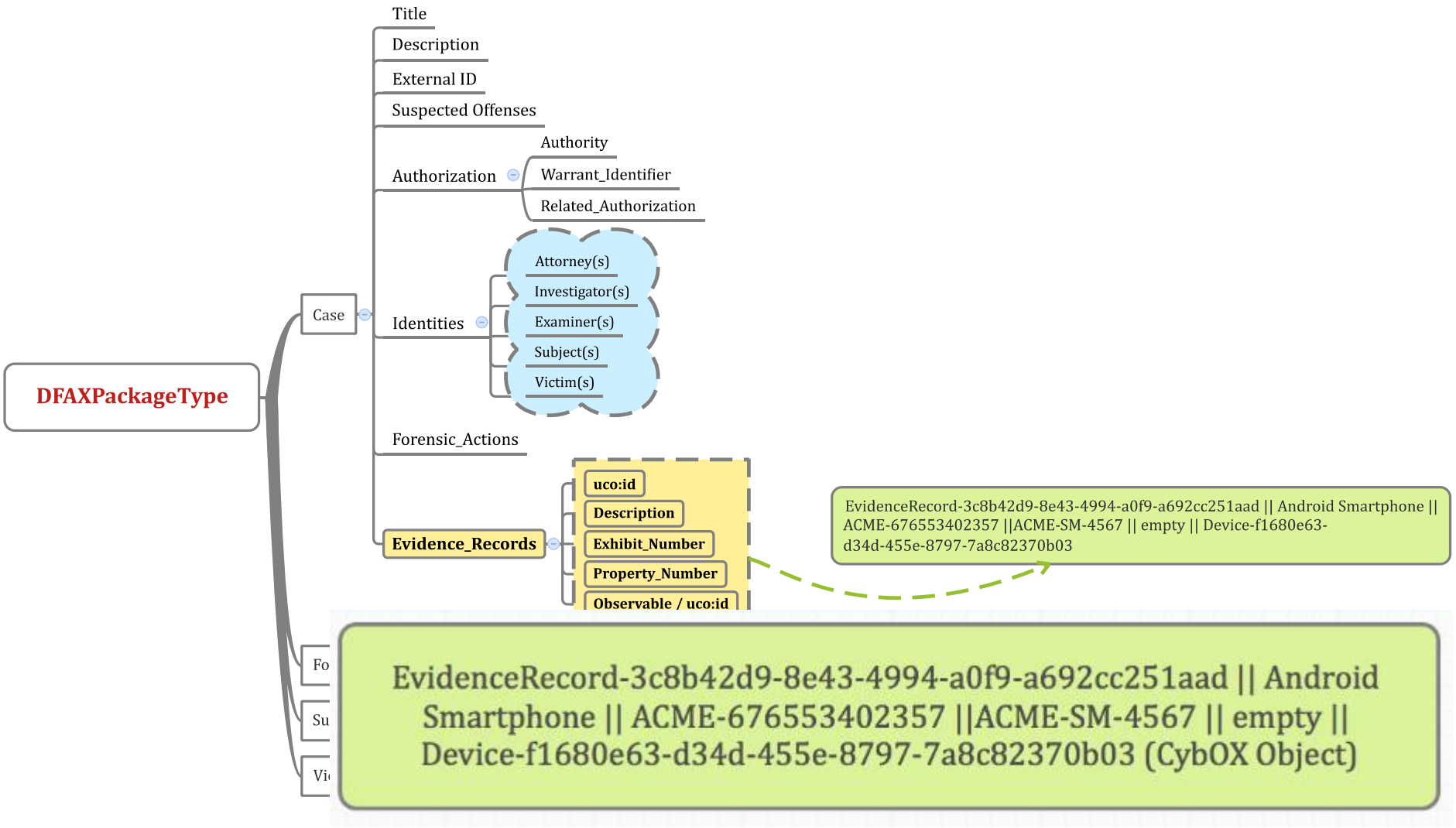
EVIDENCE
EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE

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




Title
Description
LifeCyclePhase-bae7b612-d940-4b77-b75c-0e9406f8712c (Preservation) || Seize suspect's cell phone || Head Quarters, Korea || 2014-06-01T17:24:00 || || 216547354375 || empty || 3c8b42d9-8e43-4994-a0f9-a692cc251aad
Case
Subject(s)
Victim(s)
DFAXPackageType
LifeCyclePhase-bae7b612-d940-4b77-b75c-0e9406f8712c (Preservation) || Seize suspect's cell phone || Head Quarters, Korea ||2014-06-01T17:24:00 || || 216547354375 || empty || 3c8b42d9-8e43-4994-a0f9-a692cc251aad
uco:Phase/uco:idRef
Description
uco:Location
uco:DateTime
Forensic_Actions
Warrant_Identifier
Input_Evidence_Record /uco:idRef
Output_Evidence_Record / uco:idRef
Evidence_Records
LifeCyclePhase-c11c2d2b-369e-497a-8999-3e1a7c7447e6 (Examination)|| Find communications and multimedia exchanged between subject and victim. || empty || empty || empty ||3c8b42d9-8e43-4994-a0f9-a692cc251aad || empty
Forensics_Lifecycles
Subject_Lifecycl
Victim_Lifecycle
LifeCyclePhase-c11c2d2b-369e-497a-8999-3e1a7c7447e6 (Examination)|| Find communications and multimedia exchanged between subject and victim. || empty || empty || empty || 3c8b42d9-8e43-4994-a0f9-a692cc251aad || empty

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



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

Formal/Standard Languages: next steps

- Try to convert our case study to DFAX structure
- Extending DFAX structure:
  - Have all possible steps been taken into consideration in the DFAX Evidence_LifeCycle element?
  - Is it possible to describe the Acquisition stage in terms of:
    - Source of evidence (input)
    - Forensic acquisition (output)
    - Hashing
    - Used tool
  - Are all possible forensics cases thoroughly described/covered by CybOX Objects? (LNK, Jumplist are missing)

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

Standard languages for E.E. Exchanging: why?

- They are open source
- Each possible stakeholder can be involved, even private ISPs
- Standard languages like CybOX and DFAX have been developed with extensibility in mind in order to represent a variety of digital objects, the relationships between them, and also the events associated with them. Therefore it is adaptable to the fast-pace development of technology

EVIDENCE
EUROPEAN INFORMATICS DATA EXCHANGE
FRAMEWORK FOR COURTS AND EVIDENCE

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!

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

INTERPOL