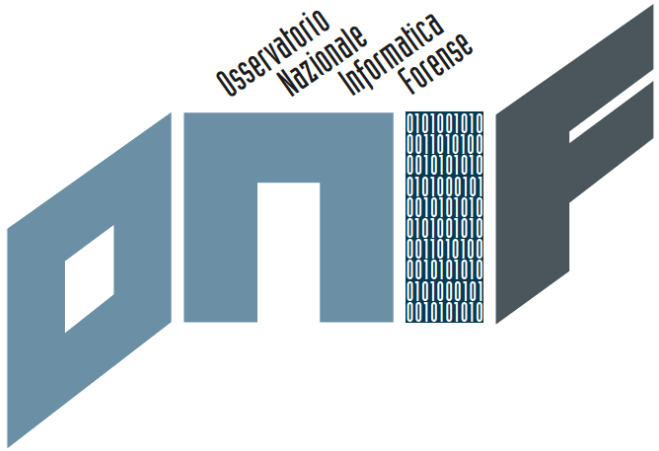


INTERNATIONAL CONFERENCE

Hard Cases of Cross-Border Digital Forensics

Udine, 28 Settembre 2017

Università degli Studi di Udine

DIGITAL INVESTIGATIONS
CURRENT CHALLENGES

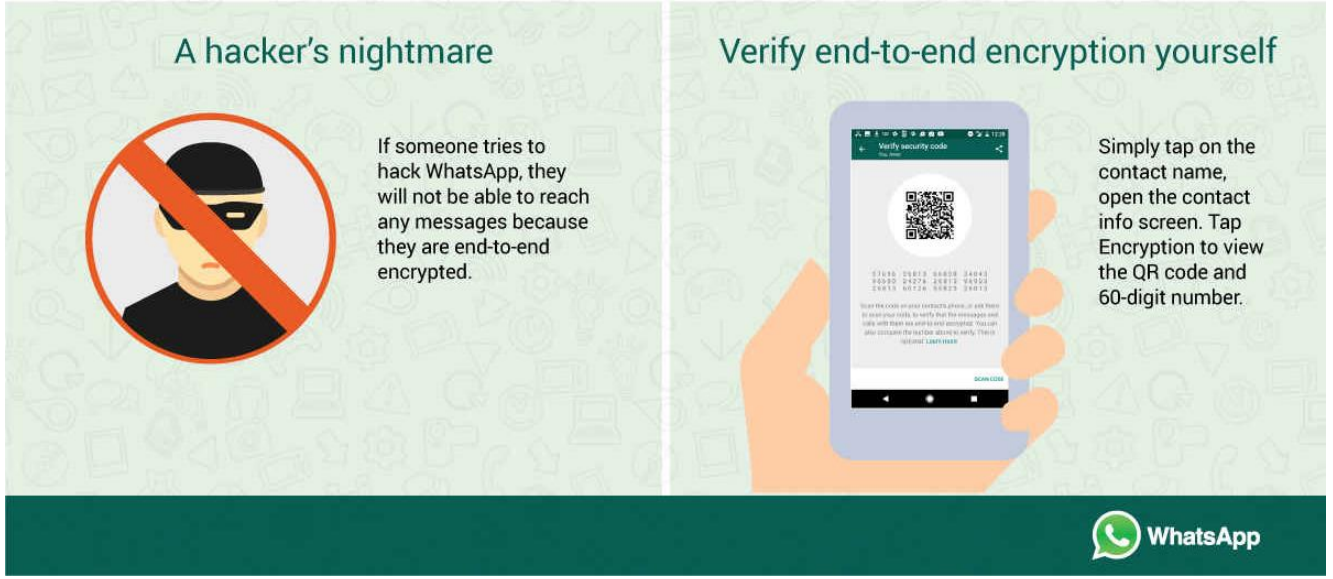
(Some) Current Challenges in Digital Investigations

- ❑ Anonymity and Encryption
- ❑ Accessing data in the Cloud / MLA
- ❑ Data retention
- ❑ Accreditation and Professionalization
- ❑ Digital Evidence Exchange

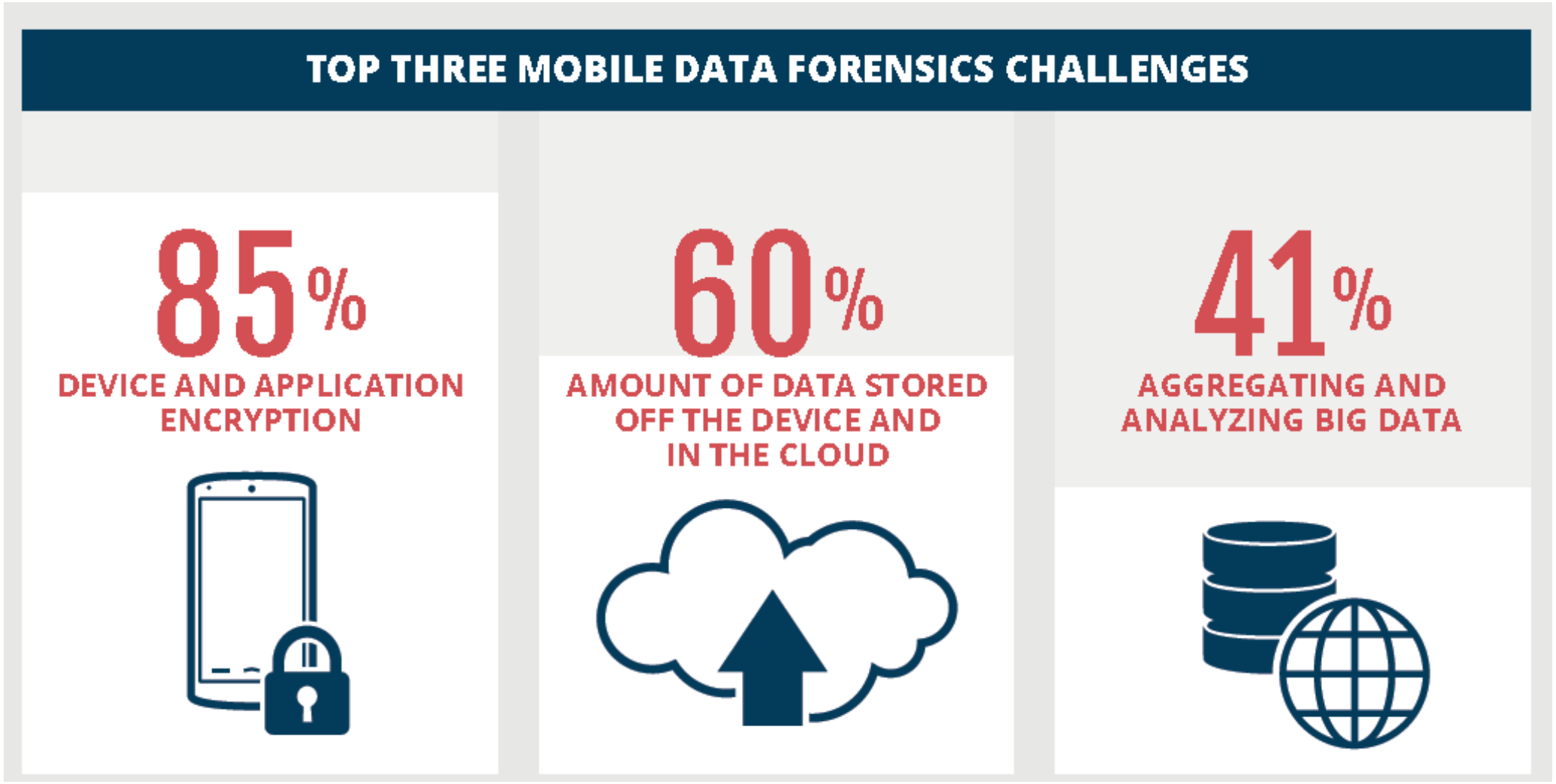
Anonymity and Encryption

- More and more devices and applications are using **anonymization** and **encryption**
- **Anonymization**: hard/impossible to trace back an action to an IP address
  - The Onion Router
  - VPNs
- **Encryption**: used both in transit and on devices making harder/impossible to
  - Intercept data
  - Extract data during a (post mortem) digital forensics investigation

Example: WhatsApp Encryption



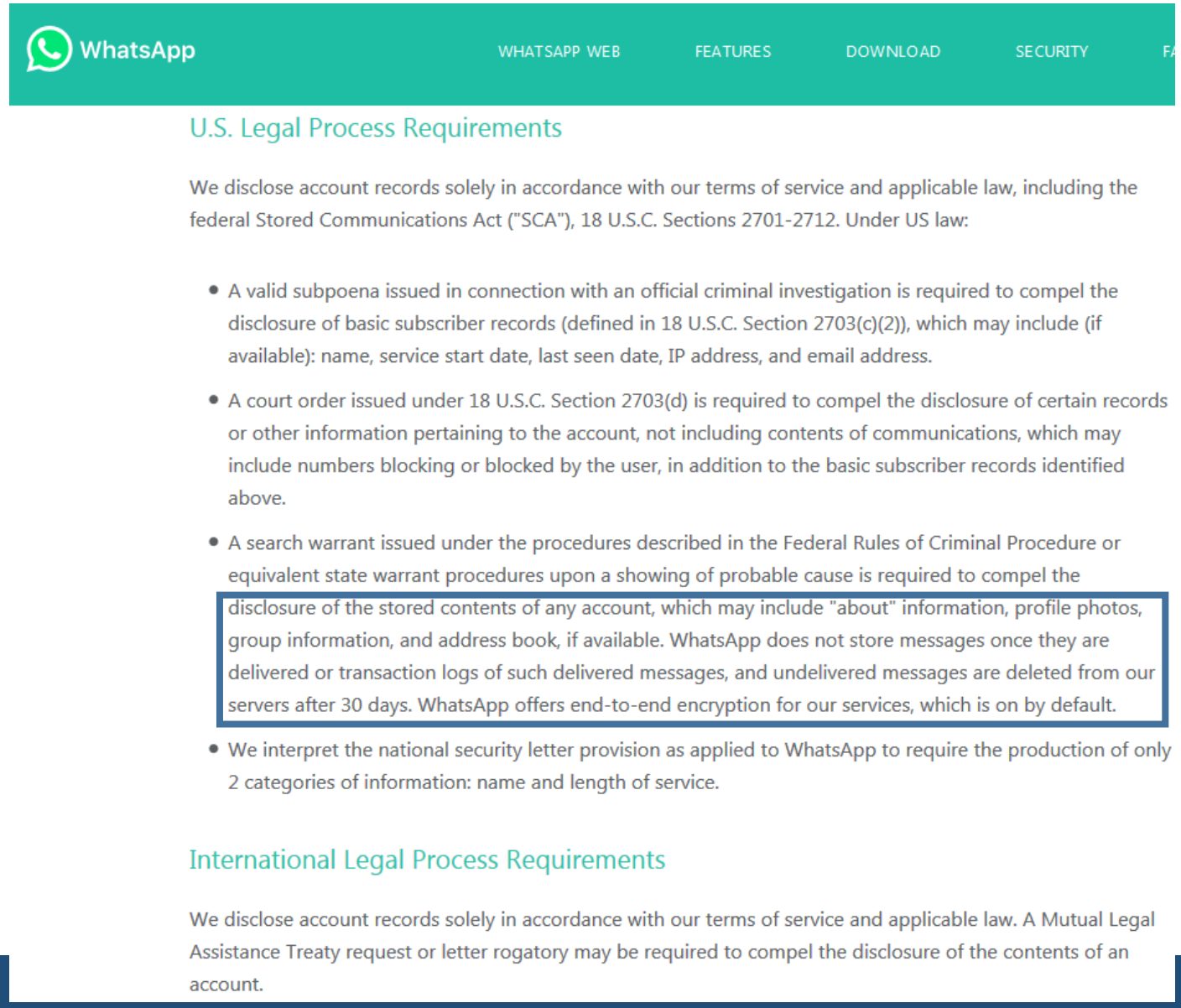
Mobile Forensics Challenges
(Source: CELLEBRITE Survey 2015)



Anonymity and Encryption: solutions?

- Backdoor?
- Malware/Trojan installed on the device?
  - Remotely
  - Manually
- Provider cooperation?

Example: WhatsApp stored contents



WhatsApp

WHATSAPP WEB FEATURES DOWNLOAD SECURITY FA

U.S. Legal Process Requirements

We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712. Under US law:

- A valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703(c)(2)), which may include (if available): name, service start date, last seen date, IP address, and email address.
- A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include numbers blocking or blocked by the user, in addition to the basic subscriber records identified above.
- A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include "about" information, profile photos, group information, and address book, if available. WhatsApp does not store messages once they are delivered or transaction logs of such delivered messages, and undelivered messages are deleted from our servers after 30 days. WhatsApp offers end-to-end encryption for our services, which is on by default.
- We interpret the national security letter provision as applied to WhatsApp to require the production of only 2 categories of information: name and length of service.

International Legal Process Requirements

We disclose account records solely in accordance with our terms of service and applicable law. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account.

Accessing data in the Cloud / Data retention / MLA Procedures

- The big players have a fundamental role!
  - **Google, Facebook, Apple, Microsoft, Samsung, Yahoo!, Linkedin, Twitter**
- Each provider has its own guidelines!
- Transparency Reports
- Need to modify MLA Procedures to improve access to data stored in other jurisdictions
- **Relevant activities made by the COE Cloud Evidence Group**
  - http://www.coe.int/en/web/cybercrime/ceg

Cloud Evidence Group

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

16 September 2016
Strasbourg, France

T-CY (2016)5
Provisional

Cybercrime Convention Committee (T-CY)

Criminal justice access to

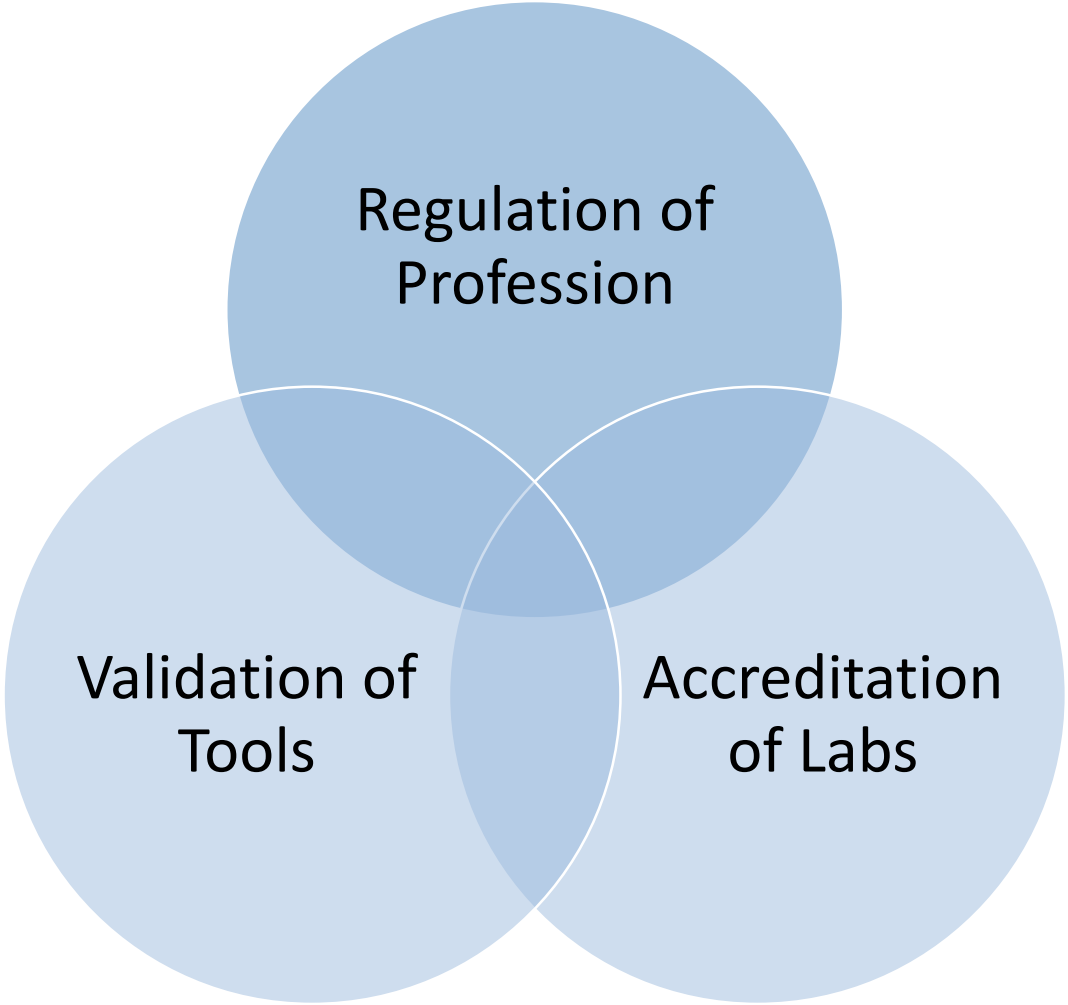
electronic evidence in the cloud:

Recommendations for consideration by the T-CY

Final report of the T-CY Cloud Evidence Group

Professionalization of Digital Forensics

EVIDENCE
EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE



Professionalization of Digital Forensics

- **Regulation of Digital Forensics Professions**
  - Require a strong **standardised knowledge basis**
    - Strong understanding of underlying IT concepts
  - **Continued training**
    - Continuous technological developments – need to remain up to date
  - Certification by an **independent certification board**
    - Regional or international board with nationally accredited bodies?

- **Validation of digital forensics tools**
- **Accreditation of digital forensics labs**
  - Guidelines for digital forensics labs
  - But **demonstration of conformity with standards** counts towards accreditation

Training in Digital Forensics: why?

EVIDENCE
EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE

- To be a good digital forensics analyst, an **IT technical background it is not sufficient**
- There is a **need of specialized training and continuous update** of competences, because technology moves very fast
- It is **impossible to find an expert for every single specific sub-field of digital forensics**
- Training is needed for
    - Law Enforcement
    - Private sector consultants
    - Legal (judges, public prosecutors, lawyers)

Training for Judges, Public Prosecutors and Lawyers

- Courses on digital evidence/digital forensics

  - to be included into standardised curriculum at law school
  - to be included into continued training for lawyers
  - to be included into mandatory training for magistrates
    - Example of best practice: Magistrates Course in Belgium (LEAs/Prosecution/Magistrates)

Accreditation of DF Experts/Labs

- **No standard view/organization around European countries**
- Most relevant:
  - **Nederlands Register Gerechtelijk Deskundigen (NL)**
    - Standards Digital Forensics (2016)
  - **Forensics Science Regulator (UK)**
    - «Certification, registration and assessment of digital forensic experts: The UK experience» (Sommer, Digital Investigation, 2011)
    - Forensic science providers: codes of practice and conduct
    - Digital forensic services: codes of practice for forensic service providers (2014)
    - Method validation in digital forensics (2016)
  - **NIST**
    - Recommendations for the accreditation of Digital and Multimedia Forensic Science Service Providers (2016)

Electronic Evidence Exchange: status quo

EVIDENCE
EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE

- **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?

Electronic Evidence Exchange: what?

EVIDENCE
EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE

- 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**

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**

EVIDENCE
EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE

EU FORENSIC EXPERTS CALL FOR ACTION ON NEW CYBER INVESTIGATION STANDARD

12 May 2017

Press Release

Industry has taken on board the issue, responding positively to this new digital forensic standard

Under the umbrella of Europol's European Cybercrime Centre (EC3), a number of the EU's leading digital forensic experts have called for the adoption of the Cyber-investigation Analysis Standard Expression (CASE) as a standard digital forensic format at a meeting hosted at the Agency's headquarters in The Hague on 11 and 12 May 2017.

A digital forensic specialist routinely uses software tools to extract, parse and analyse information on a hard drive or a mobile phone. So far, it was not possible to aggregate the digital in a standardised way, meaning that for each and every tool the investigators had to match the data extracted with the tool specification. This made the process time-consuming and costly.

Cyber-investigation Analysis Standard Expression (CASE) bridges this gap. On the occasion of the expert meeting, EC3's Forensic Lab was able to convince the vast majority of the market leaders to adopt this open-source data format for forensics. This event is a game changer in the specialised field of forensic analysis, as key laboratories and services have repeatedly called for the implementation of such a standard in the past.

CASE is a community-developed standard format, defined as a profile of the Unified Cyber Ontology (UCO). As such, CASE leverages contextually relevant components of the UCA; extending, constraining or renaming them as appropriate. CASE is specified at a semantic level and supports various serialisations, its default serialisation being JSON-LD.

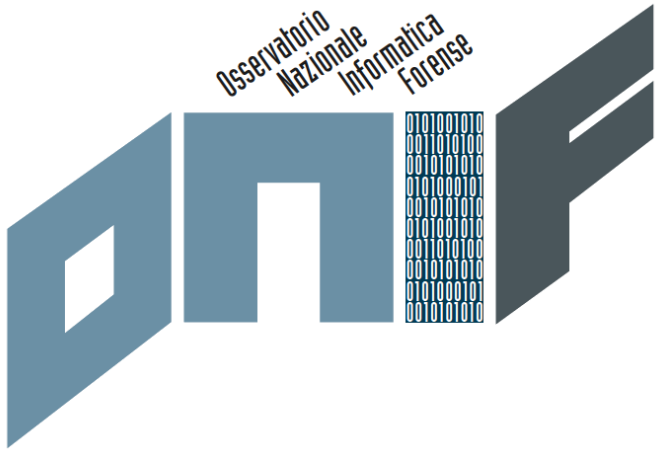
After discussions with the market leaders, EC3 is happy to announce that the following industries companies are currently looking into implementing the standard:

EVIDENCE
EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE

After discussions with the market leaders, EC3 is happy to announce that the following industries companies are currently looking into implementing the standard:

- Access data
- Cellebrite
- Guidance software
- I2 – IBM
- Magnet forensic
- Mercure
- Mobile edit
- Network miner
- Nuix
- Oxygen
- Volatility
- XRY

DFRWS 2018 EU



INTERNATIONAL CONFERENCE

Hard Cases of Cross-Border Digital Forensics

Udine, 28 Settembre 2017

Università degli Studi di Udine

GRAZIE PER L'ATTENZIONE!

www.onif.it

info@onif.it