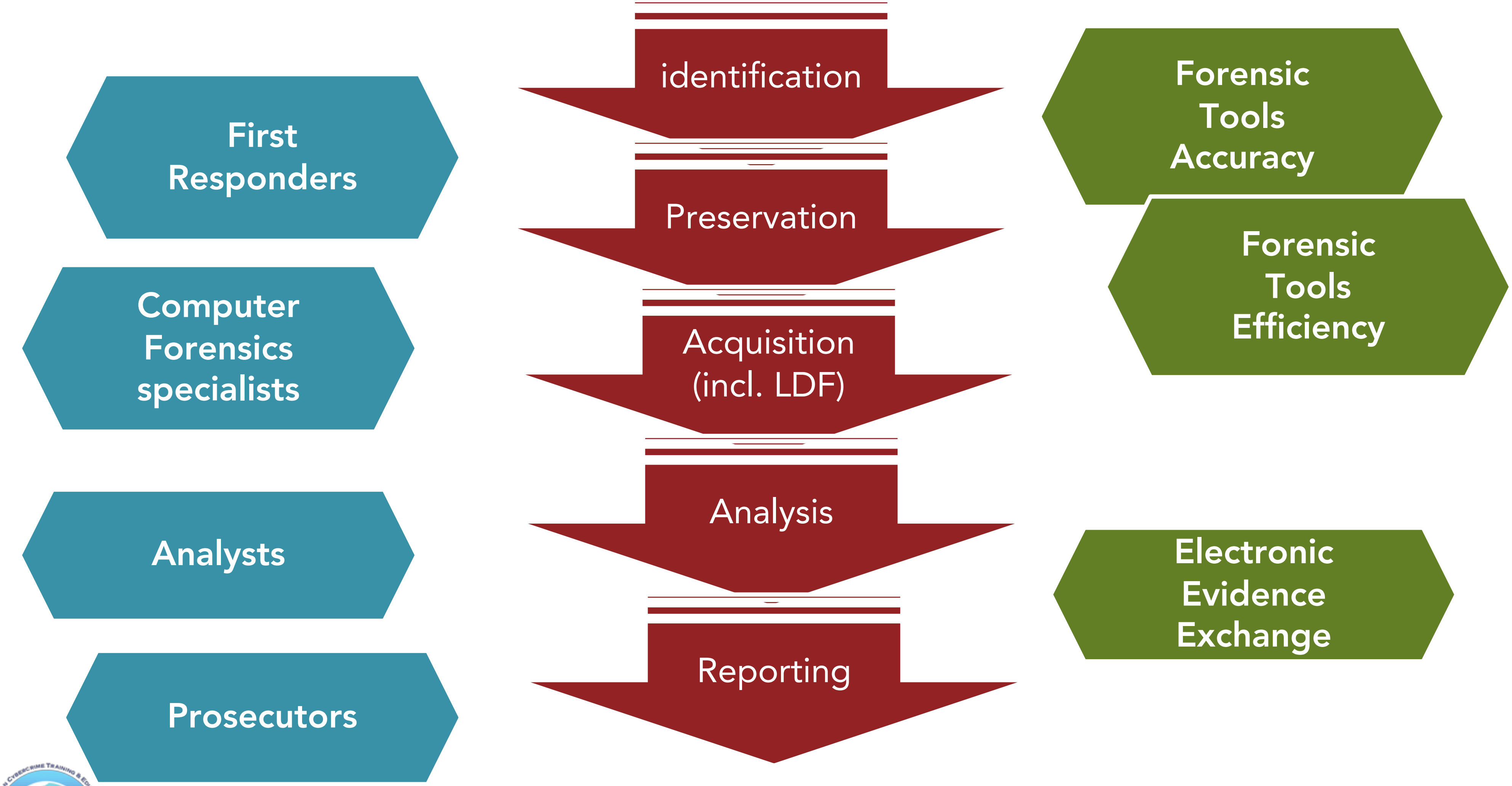
Electronic Evidence
Role of the First Responder in an IoT world

Yves Vandermeer, MSc
ECTEG Chair
Norwegian Police University College

Actors and Tools



First Responder ?

- Each police officer
  - On the field (patrol, house search)
  - At the office, when taking victim's complaint
  - During the investigation

- >=1,5 millions Law Enforcement users only in EU
  - Not well skilled on new technologies
  - Not all able to acquire knowledge in English
  - Not available for usual course attendance

Dedicated tool(s)

- Live Data Forensics
  - Memory acquisition
  - Essential Information
    - Encryption
    - Cloud
    - Crypto currencies wallet
- FREETOOL project

FREETOOL
Free Reliable Tools for Investigating Cybercrime

Training Competency Framework

Requirements:

■ **Expert Level**

▒ **Basic Level**

Discussed category	**Management skills**				**Technical skills**					**Investigation skills**					
	Strategic Decision Making	Management (incl. HR and Budget)	Soft Skills and Networking	Communication and Presentation	Digital Forensics	Internet Networking & Tracing	Programming, scripting, SQL	Analytical and Visualisation	Live Data Forensics	Cybercrime Legislation	General Cybercrime Awareness	First Responder	Open Source Intelligence (OSINT)	Interviewing and Interrogation	Investigation Techniques
Political and Strategic Decision Makers	■	■	■	■						▒	▒				
Law Enforcement Management	■	■	■	■						■	▒				
Heads of Cybercrime Units and Team Leaders	▒	■	■	■		▒				■	■		▒		▒
General Crimnial Investigators				▒		▒				▒	▒	■	▒	■	■
Intermediate and Advanced Investigators				▒		▒				▒	▒	■	▒	■	■
Cybercrime Analysts and Intelligence Officers				▒	▒	▒	▒	■		▒	■		■		■
Online Investigators				▒	▒	■	▒	▒	▒	■	■	▒	■	▒	■
Digital Forensic Investigators and Examiners				▒	■	▒	▒	▒	■	■	■	■	▒		■
Cyber Experts	▒			▒	■	■	▒	▒	■	■	■	■	▒	▒	▒
	▒			▒	■	■	▒	▒	■	■	■	■	▒	▒	▒
Judges			▒	▒		▒				■	▒		▒		▒
Prosecutors			■	■	▒	▒		▒	▒	■	■	▒	▒	▒	▒

First responders

Relevant Cybercrime Training

Skills and competences

- **Identify** and **seize** items with potential electronic evidence
- Take urgent measures to preserve (electronic) traces
- Live Data Forensics whenever needed
- Understanding the importance of electronic evidence
- Welcome & correctly support victims
- Protect evidence integrity
- Case specific victim aid & advice
- Contribute to citizen awareness
- Prevention

ef1
POLITIE-POLICE
POLITIHØGSKOLEN
Politie
Polizeiakademie Hessen
Cyber Science Center
Polisen
Swedish Police
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
EUROPOL
EC3
CEPOL

e-First

Project : E-learning first responders

- Driver : ECTEG & Portuguese Judicial Police
- Deliverables :
  - E-learning in seven EU languages
  - Opt-in update tool
- Planning :

Phase I	English only	September 2018
Phase II	+14 languages	Spring 2019

The project team

- « Computer Forensics / Crime » LEA experts
- First responders
- 1 pedagogical expert
- 1 psychologue
- 1 web designer
- 1 coordinator

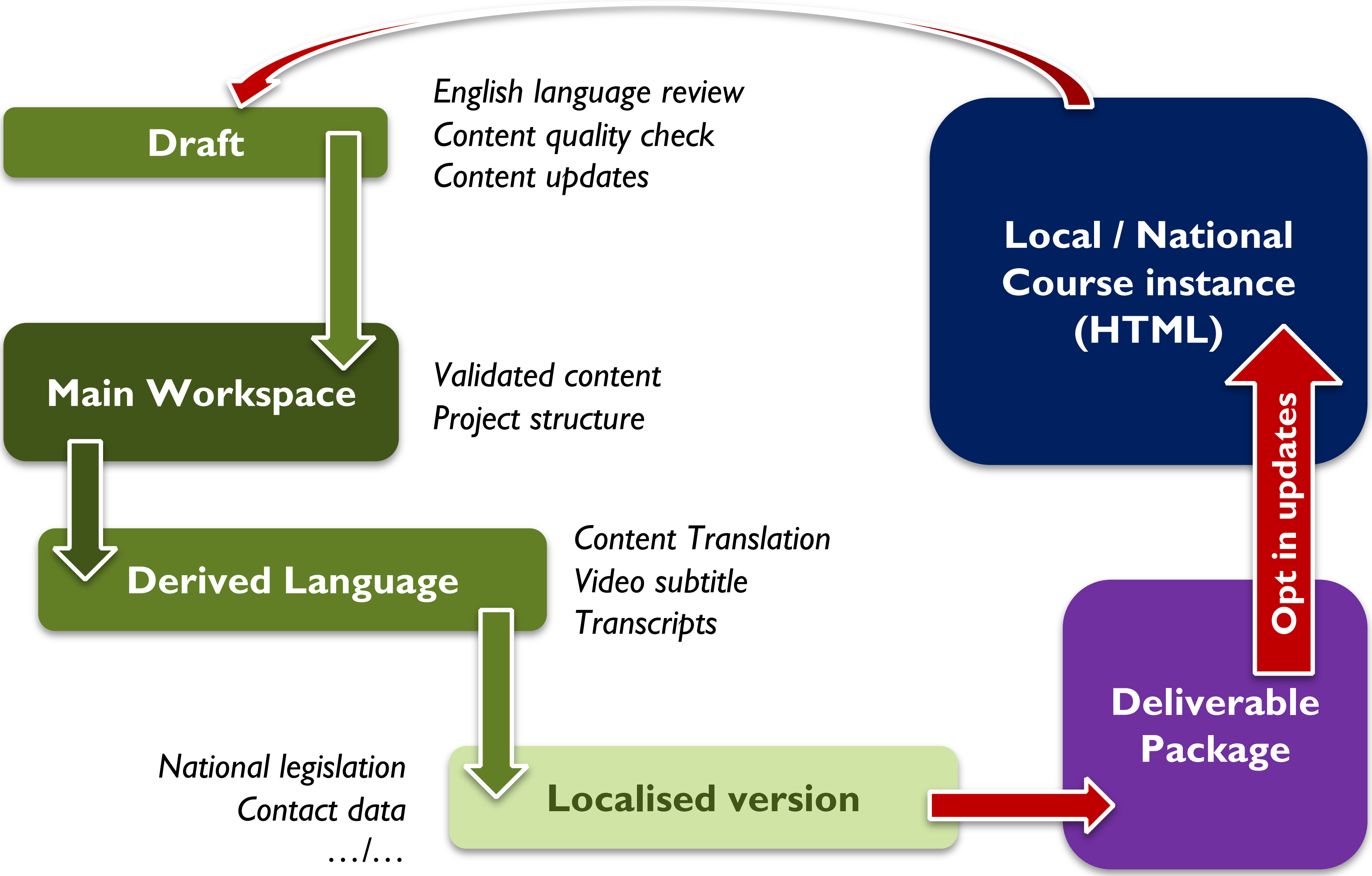
English
Portuguese
Norwegian
Spanish
Italian
Greek
German
French

Dutch
Polish
Danish
Finnish
Swedish
Arabic
Thai

The project architecture

- Based on open source Scenari e-learning development software (*www.scenari.org*)
- Running on dedicated server
  - Linux server
  - Scenari server package
  - Open office

The project architecture


Draft

English language review
Content quality check
Content updates

Main Workspace

Validated content
Project structure

Derived Language

Content Translation
Video subtitle
Transcripts

National legislation
Contact data
…/…

Localised version

Deliverable Package

Opt in updates

Local / National Course instance (HTML)

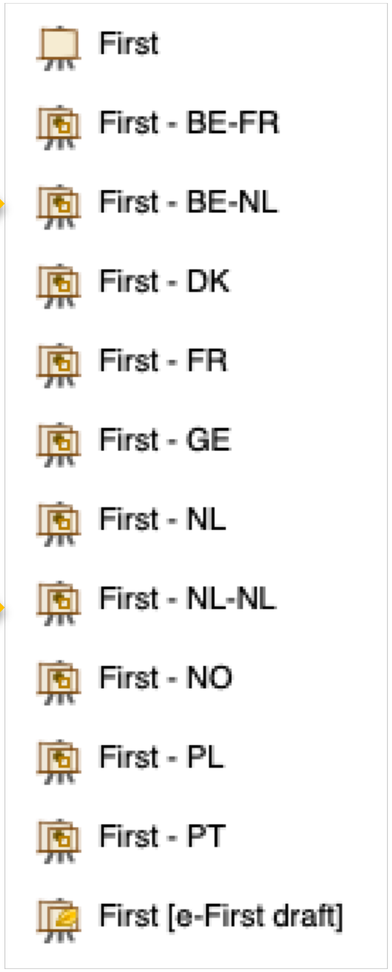
Localisation approach

Draft (input)

Master (validated)

Language specific (derived)

Country specific (derived)



First

First - BE-FR

First - BE-NL

First - DK

First - FR

First - GE

First - NL

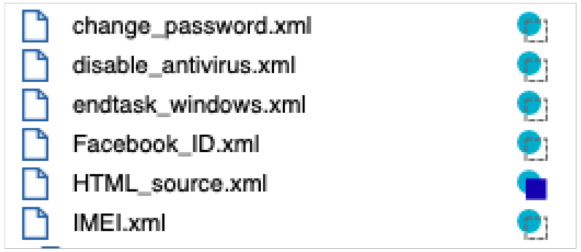
First - NL-NL

First - NO

First - PL

First - PT

First [e-First draft]



change_password.xml

disable_antivirus.xml

endtask_windows.xml

Facebook_ID.xml

HTML_source.xml

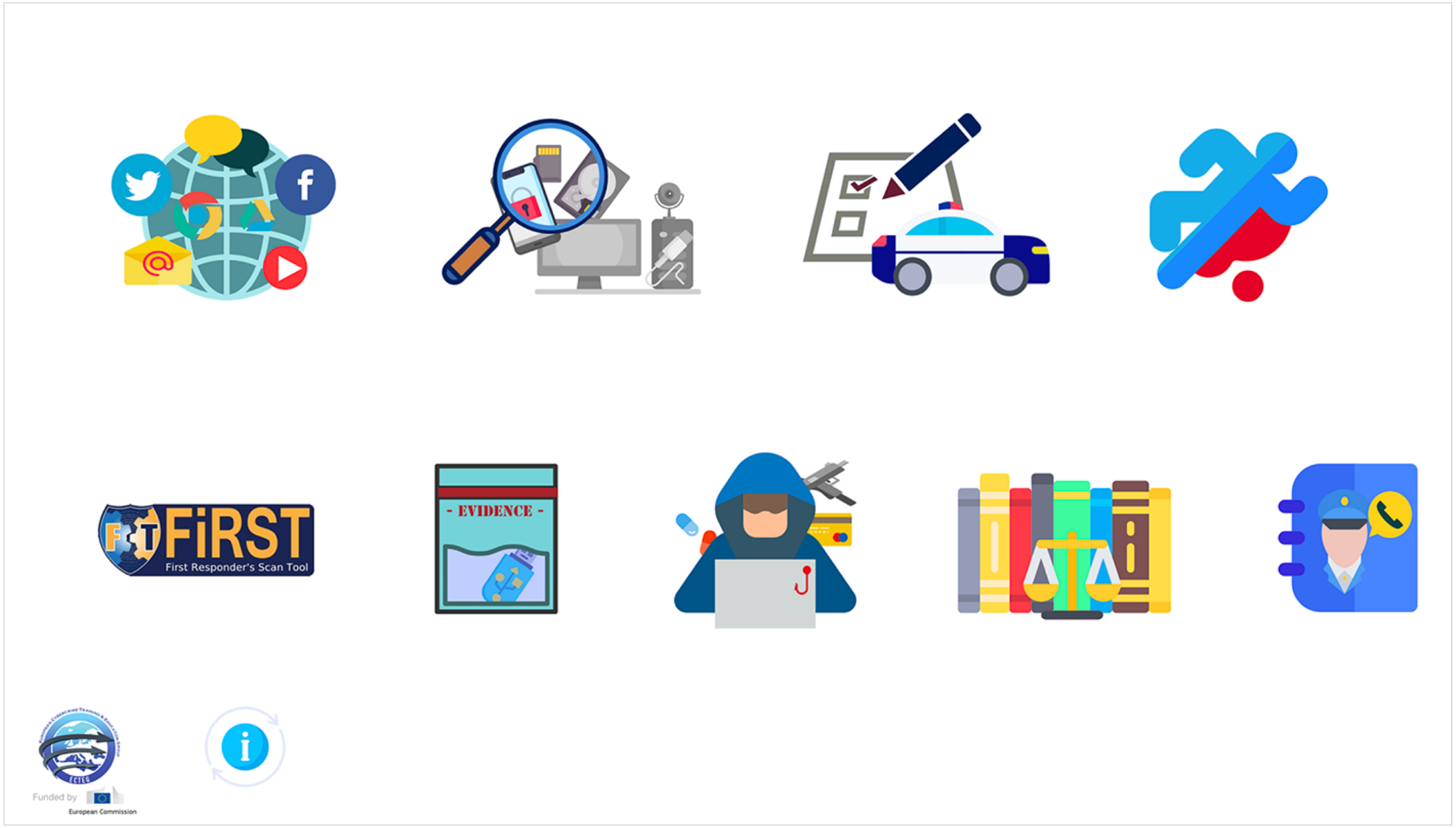
IMEI.xml

Project management

- Versioning
- Viewing and Editing rights
  - By Workspace
  - On some specific items
- Reuse of existing resources
  - Other ECTEG projects
  - Europol communication materials
  - …/…

The project content

- A knowledge base
  - Interactive
  - Multi media
  - Including « Electronic Evidence Guide » from the CoE
  - Including Europol-EC3 materials
  - Referring to the FiRST software *(FREETOOL project)*
- Serious gaming part


FiRST
First Responder's Scan Tool
- EVIDENCE -
Funded by European Commission

Phase 2 – May 2019

- Adding new phenomena
- Adding interactive gaming cases
- Sync scripts (on demand updates)
- SCORM compatibility
- Localisation in +14 EU languages
    - Support from the Council of Europe
    - Support from UNODC
- Adding national legislation, contact points, …

Outcomes

- Reaction against new phenomenon facilitated (usually 2 weeks)
- Harmonisation of the terminology
  - Inside LEA community (national & international)
  - Magistrates and prosecutors
  - Citizens and law makers
- Identification of human resources
- Course materials available for advanced courses

What’s next ?

- Updating phenomenons
- Additional languages

- Version for prosecutors ?
- Version for general citizen awareness ?

- New domains:
  - Decryption awareness
  - Automotive basics

Obtaining e-first ?

- English package **freely** available from ECTEG
  - Accessible on the ECTEG Moodle
  - Or to be installed on your local web server
    - Apache server (or equivalent)
    - **Works without internet connexion**
- Win-win approach
  - Contribute to quality improvement
  - Provide usage stats

Electronic Evidence Exchange

- Cyber crime don’t know borders
- Electronic Evidence content is sometimes partially unknown
- Some standards needed

So what's your idea of a perfect date?
YYYY-MM-DD
I find other formats a bit confusing

(some) References

- Council of Europe – Electronic Evidence Guide
- Biasiotti, M.A. et al. (2018) Handling and Exchanging Electronic Evidence Across Europe.
- Mason, S. & Seng, D. (2017) Electronic Evidence. HeinOnline.
- Nickson M. Karie, S.M.K. (2017) Digital Forensic Readiness in Organizations: Issues and Challenges. Journal of Digital Forensics, Security and Law, Vol 12
- James, J.I. & Gladyshev, P. (2013) Challenges with automation in digital forensic investigations.
- James, J.I. & Jang, Y.J. (2013) An Assessment Model for Cybercrime Investigation Capacity.
- Shah, M.S.M.B., Saleem, S. & Zulqarnain, R. (2017) Protecting Digital Evidence Integrity and Preserving Chain of Custody. Journal of Digital Forensics, Security and Law
- Garrie, D.B. (2014) Digital forensic evidence in the courtroom: Understanding content and quality. Nw. J. Tech. & Intell. Prop
- Eoghan Casey, S.B., Ryan Griffith, Jonathan Snyder, Harm van Beek, Alex Nelson (2017) Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language.

contact data

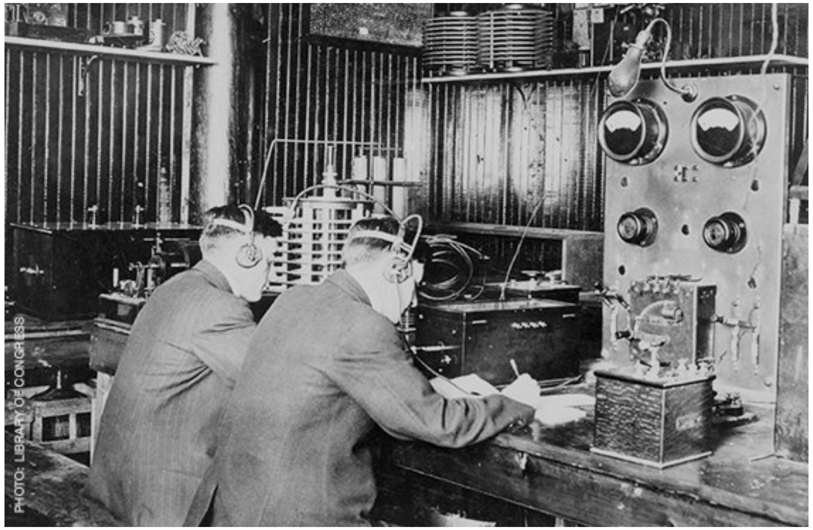


PHOTO: LIBRARY OF CONGRESS

European **C**ybercrime **T**raining and **E**ducation **G**roup

www.ecteg.eu

Yves Vandermeer

yves.vandermeer@ecteg.eu

twitter : @ecteg