# E-FIRST PROJECT

Law Enforcement training strategy on cybercrime and electronic evidence in the Middle East and North Africa Region

Amman, Jordan
25 September 2019

Carlota Urruela
Universidad Autónoma de Madrid

Funded by the European Commission

ISF-2016-AG-IBA-ECTEG

European Cybercrime Training & Education Group
ECTEG

# ABOUT ECTEG

- European Cybercrime Training and Education Group

- Funded by the European Commission

- Members: European Union and European Economic Area Member States
  law enforcement agencies, international bodies, academia, private industry and experts

- Close cooperation with Europol-EC3 and CEPOL, both members of the advisory group

Funded by the European Commission

ISF-2016-AG-IBA-ECTEG

# ABOUT ECTEG

Some of ECTEG's main aims:

- To support international activities to harmonise cybercrime training across international borders.
- To share knowledge, expertise and find training solutions.
- To promote the standardisation of methods and procedures for training programmes and cooperation with other international organisations.

More information: www.ecteg.eu

Funded by the European Commission

ISF-2016-AG-IBA-ECTEG

European Cybercrime Training & Education Group
ECTEG

POLICIA
JUDICIÁRIA

# eFirst Project

# ABOUT eFIRST

The **“first responders e-learning” package** is an interactive online training course which focuses on essential IT forensics and IT crime knowledge for first responders

It is adapted to different EU languages (+ Arabic and Thai with collaboration of UNODC and the Council of Europe) and the different national legislations.

Funded by the European Commission

ISF-2016-AG-IBA-ECTEG

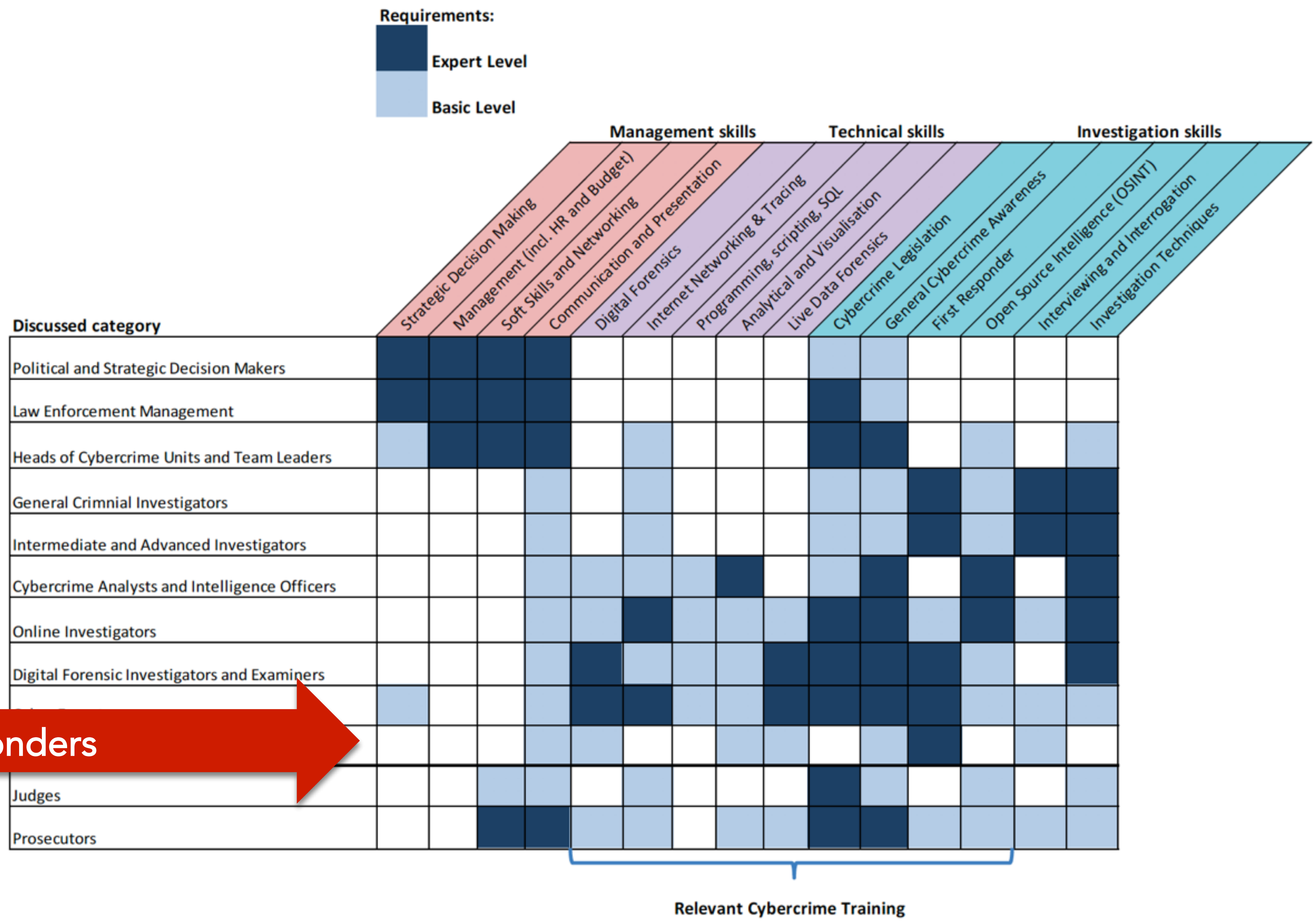
# ABOUT eFIRST

- Definitions, explanations of devices and phenomena.
- Guidelines for search and seizure of electronic evidence.
- Instructions on how to use the FiRST tool.
- Case-Games: Interactive criminal investigations, covering several topics and related to phenomena such as Darkweb and crypto currencies, fake identity on Social Networks, Phishing …
- Quizzes and Tests
- Materials and resources
- …

Funded by the European Commission

ISF-2016-AG-IBA-ECTEG

# ABOUT eFIRST



**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 | | | | ▒ | ■ | ▒ | ▒ | ▒ | ■ | ■ | ■ | ■ | ▒ | | ■ |
| | ▒ | | | ▒ | ■ | ■ | ▒ | ▒ | ■ | ■ | ■ | ■ | ▒ | ▒ | ▒ |
| | | | | ▒ | ▒ | | | ▒ | ▒ | | ▒ | ■ | | ▒ | |
| Judges | | | ▒ | ▒ | | ▒ | | | | ■ | ▒ | | ▒ | | ▒ |
| Prosecutors | | | ■ | ■ | ▒ | ▒ | | ▒ | ▒ | ■ | ■ | ▒ | ▒ | ▒ | ▒ |

**Relevant Cybercrime Training**

First responders

Funded by the European Commission

ISF-2016-AG-IBA-ECTEG

# WHAT IS A 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, who are:

  - Not well skilled on new technologies
  - Not all able to acquire knowledge in English
  - Not available for usual course attendance

Funded by the European Commission

ISF-2016-AG-IBA-ECTEG

# PROJECT TEAM

- “Computer Forensics / Crime LEA experts
- First responders

- 1 pedagogue
- 1 psychologist
- 1 web designer
- 1 coordinator

Funded by the European Commission

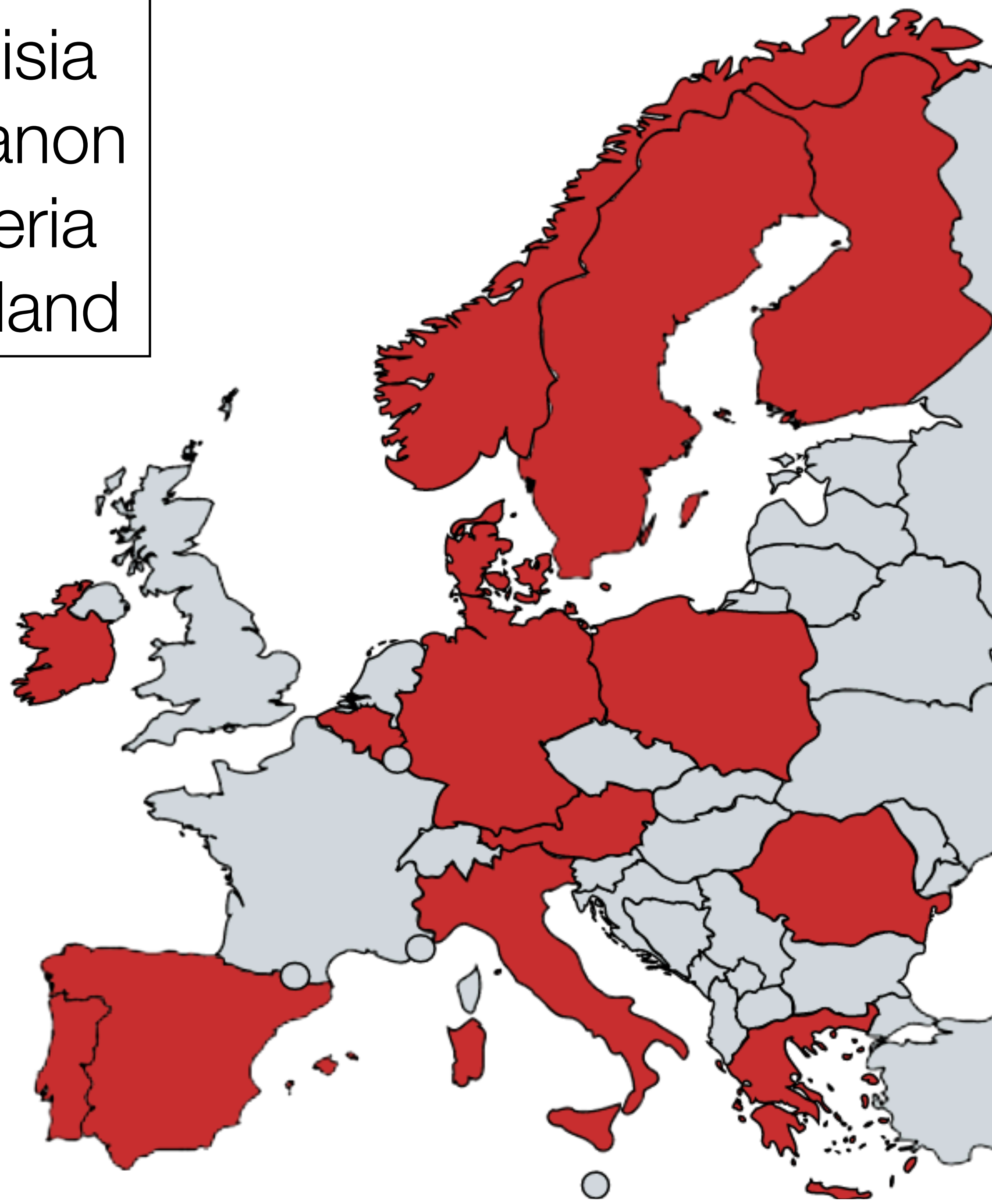
ISF-2016-AG-IBA-ECTEG

# PROJECT TEAM

Portugal
Norway
Spain
Italy
Greece
Germany
Ireland

Belgium
Austria
Denmark
Finland
Sweden
Romania
Poland

+
Morocco
Tunisia
Lebanon
Algeria
Thailand



Funded by the European Commission

ISF-2016-AG-IBA-ECTEG

# ADDRESSED SKILLS AND COMPETENCIES

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

Funded by the European Commission

ISF-2016-AG-IBA-ECTEG

# NATIONAL VERSIONS

- Based on the main workspace and then translated content in national language

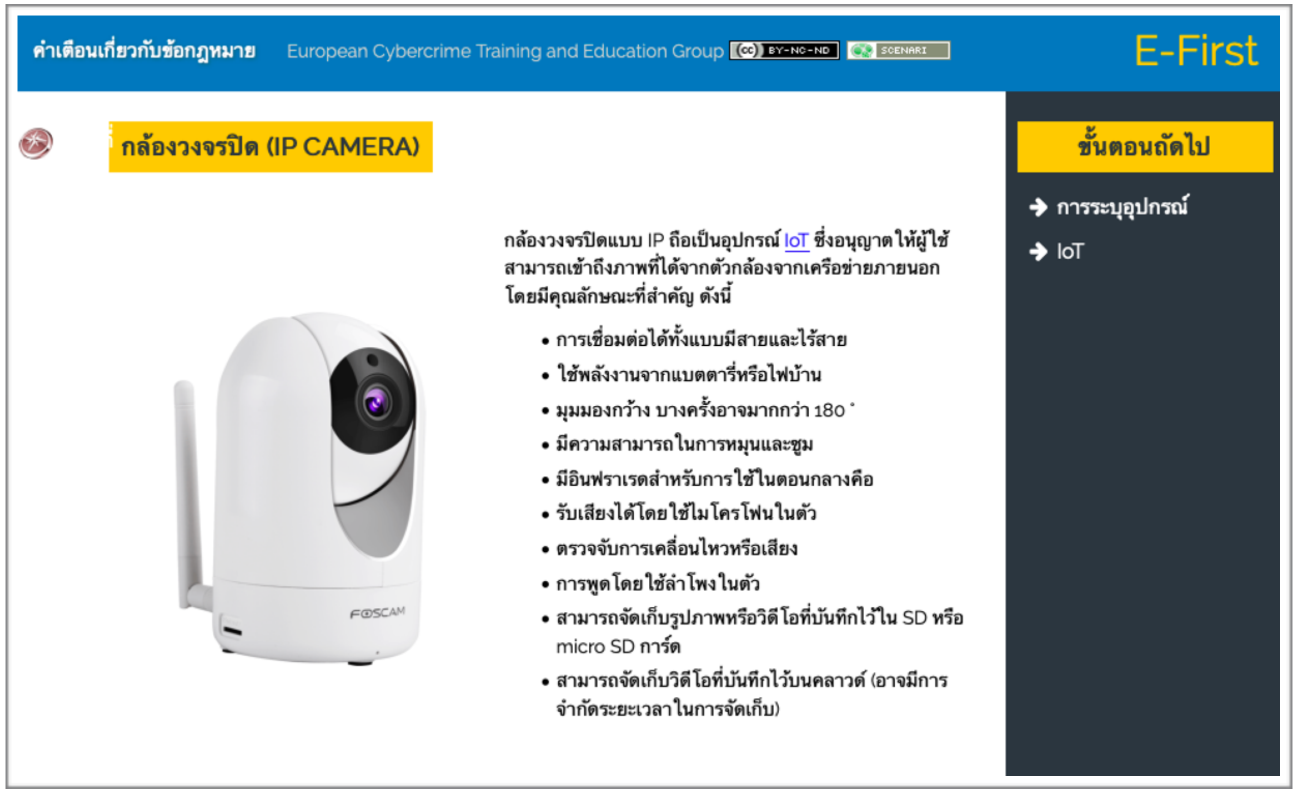
- Adds national level documents

    - Legislation - Directives
    - Guidelines
    - Standardised forms
    - Specific Contact Data and processes

- All content may be customised / modified

Funded by the European Commission

ISF-2016-AG-IBA-ECTEG



คำเตือนเกี่ยวกับข้อกฎหมาย European Cybercrime Training and Education Group BY-NC-ND SCENARI E-First

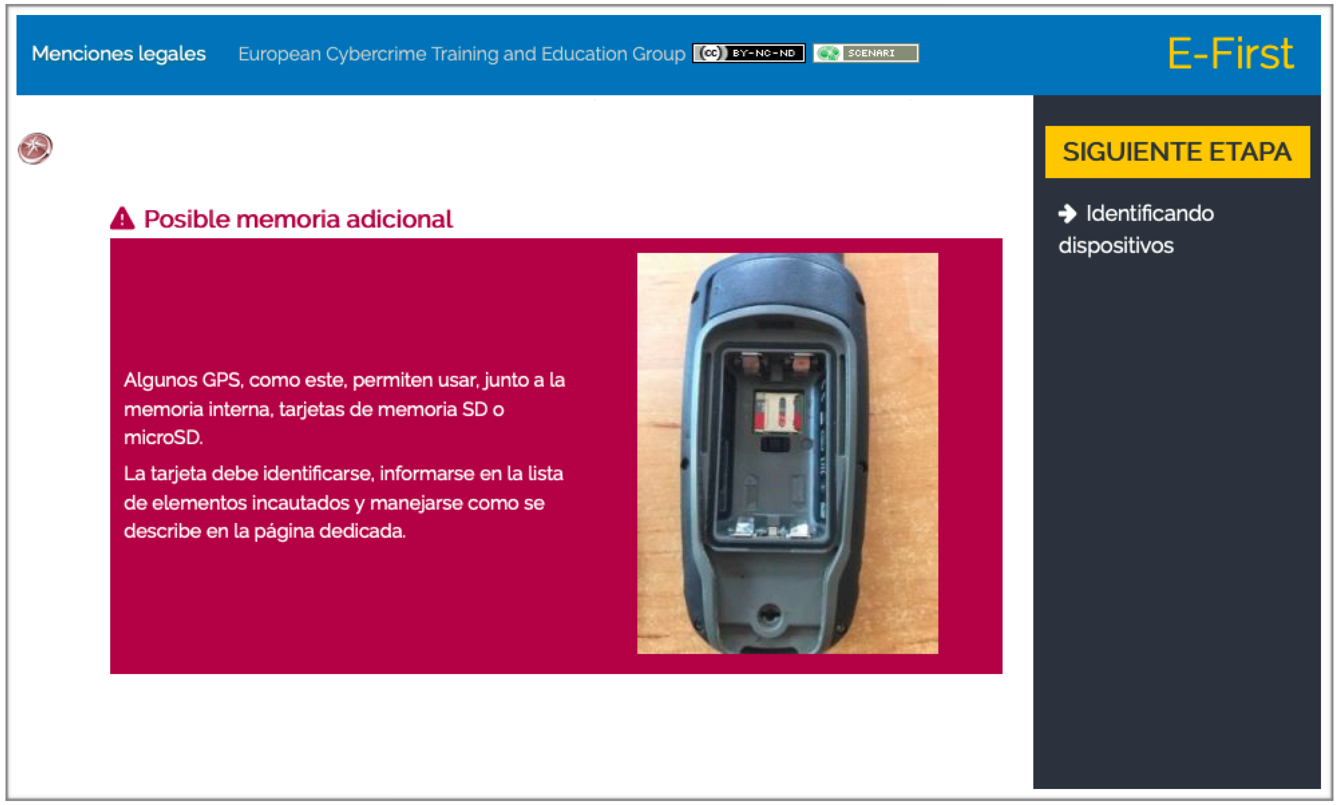
## กล้องวงจรปิด (IP CAMERA)

กล้องวงจรปิดแบบ IP ถือเป็นอุปกรณ์ IoT ซึ่งอนุญาตให้ผู้ใช้สามารถเข้าถึงภาพที่ได้จากตัวกล้องจากเครือข่ายภายนอก โดยมีคุณลักษณะที่สำคัญ ดังนี้

- การเชื่อมต่อได้ทั้งแบบมีสายและไร้สาย
- ใช้พลังงานจากแบตตารี่หรือไฟบ้าน
- มุมมองกว้าง บางครั้งอาจมากกว่า 180 ˚
- มีความสามารถในการหมุนและซูม
- มีอินฟราเรดสำหรับการใช้ในตอนกลางคืือ
- รับเสียงได้โดยใช้ไมโครโฟนในตัว
- ตรวจจับการเคลื่อนไหวหรือเสียง
- การพูดโดยใช้ลำโพงในตัว
- สามารถจัดเก็บรูปภาพหรือวิดีโอที่บันทึกไว้ใน SD หรือ micro SD การ์ด
- สามารถจัดเก็บวิดีโอที่บันทึกไว้บนคลาวด์ (อาจมีการจำกัดระยะเวลาในการจัดเก็บ)

ขั้นตอนถัดไป

- การระบุอุปกรณ์
- IoT



Menciones legales European Cybercrime Training and Education Group BY-NC-ND SCENARI E-First

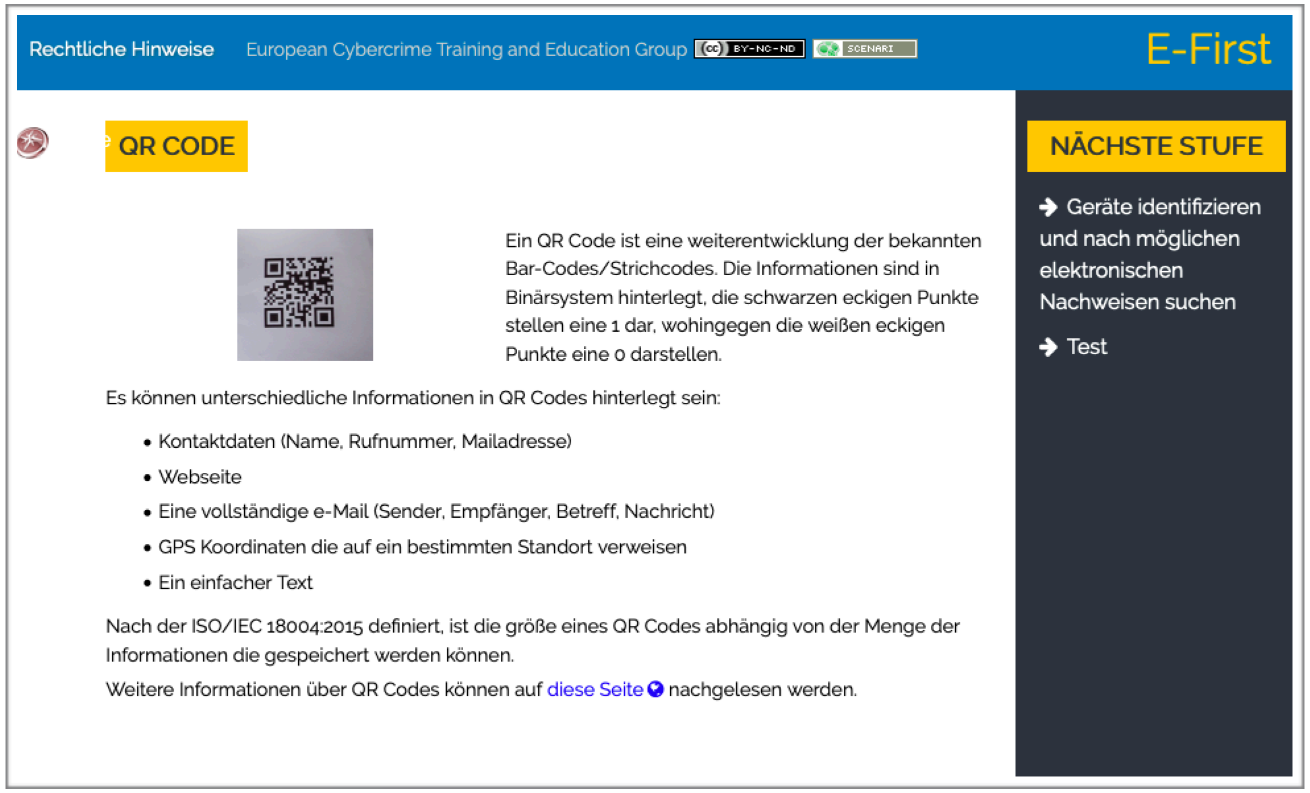
### Posible memoria adicional

Algunos GPS, como este, permiten usar, junto a la memoria interna, tarjetas de memoria SD o microSD.

La tarjeta debe identificarse, informarse en la lista de elementos incautados y manejarse como se describe en la página dedicada.

SIGUIENTE ETAPA

- Identificando dispositivos



Rechtliche Hinweise European Cybercrime Training and Education Group BY-NC-ND SCENARI E-First

## QR CODE

Ein QR Code ist eine weiterentwicklung der bekannten Bar-Codes/Strichcodes. Die Informationen sind in Binärsystem hinterlegt, die schwarzen eckigen Punkte stellen eine 1 dar, wohingegen die weißen eckigen Punkte eine 0 darstellen.

Es können unterschiedliche Informationen in QR Codes hinterlegt sein:

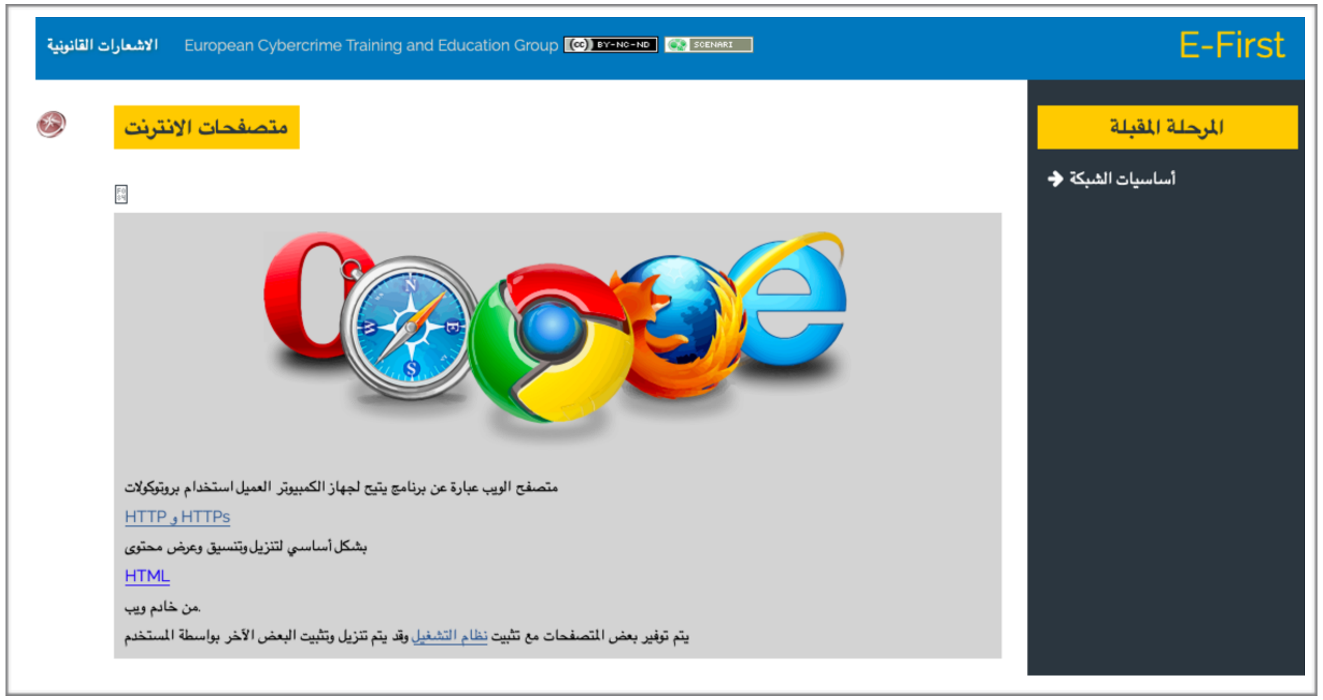
- Kontaktdaten (Name, Rufnummer, Mailadresse)
- Webseite
- Eine vollständige e-Mail (Sender, Empfänger, Betreff, Nachricht)
- GPS Koordinaten die auf ein bestimmten Standort verweisen
- Ein einfacher Text

Nach der ISO/IEC 18004:2015 definiert, ist die größe eines QR Codes abhängig von der Menge der Informationen die gespeichert werden können.

Weitere Informationen über QR Codes können auf diese Seite nachgelesen werden.

NÄCHSTE STUFE

- Geräte identifizieren und nach möglichen elektronischen Nachweisen suchen
- Test



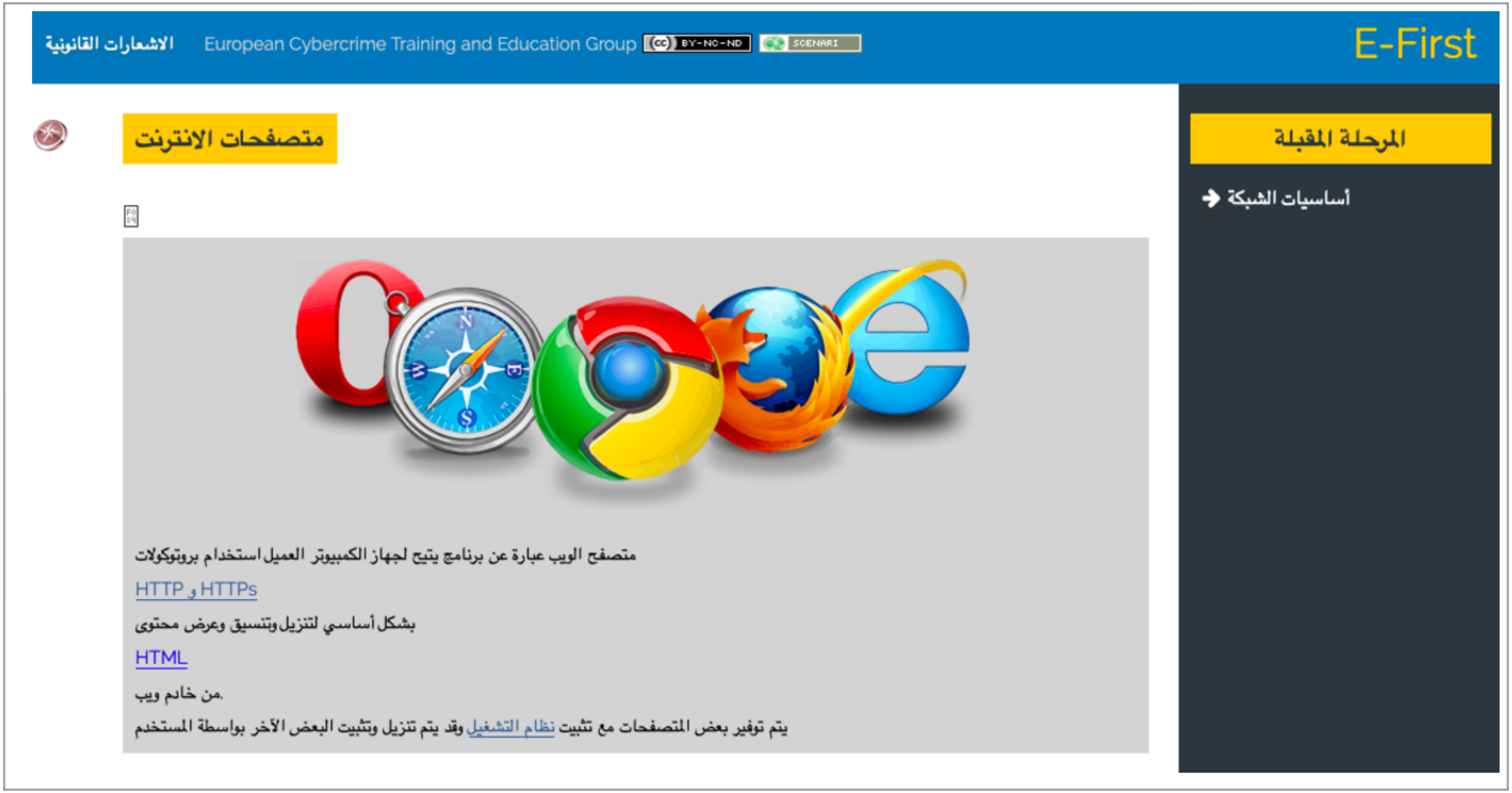
الاشعارات القانونية European Cybercrime Training and Education Group BY-NC-ND SCENARI E-First

## متصفحات الانترنت

متصفح الويب عبارة عن برنامج يتيح لجهاز الكمبيوتر العميل استخدام بروتوكولات
HTTP و HTTPs
بشكل أساسي لتنزيل وتنسيق وعرض محتوى
HTML
من خادم ويب.
يتم توفير بعض المتصفحات مع تثبيت نظام التشغيل وقد يتم تنزيل وتثبيت البعض الآخر بواسطة المستخدم

المرحلة المقبلة

- أساسيات الشبكة



## متصفحات الانترنت

متصفح الويب عبارة عن برنامج يتيح لجهاز الكمبيوتر العميل استخدام بروتوكولات

HTTP و HTTPs

بشكل أساسي لتنزيل وتنسيق وعرض محتوى

HTML

من خادم ويب.

يتم توفير بعض المتصفحات مع تثبيت نظام التشغيل وقد يتم تنزيل وتثبيت البعض الآخر بواسطة المستخدم

# HOW TO OBTAIN eFIRST?

- Restricted to Law Enforcement Agencies
- Freely available from ECTEG
  - To be installed on your local (national) web server
  - Apache server (or equivalent)
- Win-win approach
  - Contribute to quality improvement
  - Provide usage stats

Funded by the European Commission

ISF-2016-AG-IBA-ECTEG

# HOW TO OBTAIN eFIRST?

## Contact:

Carla Pagès

*carla.santos@pj.pt*

Yves Vandermeer

*yves.vandermeer@ecteg.eu*

Funded by the European Commission

ISF-2016-AG-IBA-ECTEG