Cybercrime Capacity Building
a cooperative process

Making the UK and Europe a safer place to live and work online
Canterbury, 12 January 2018

Nikon FE2
produced from 1983 to 1987
still working and useable today

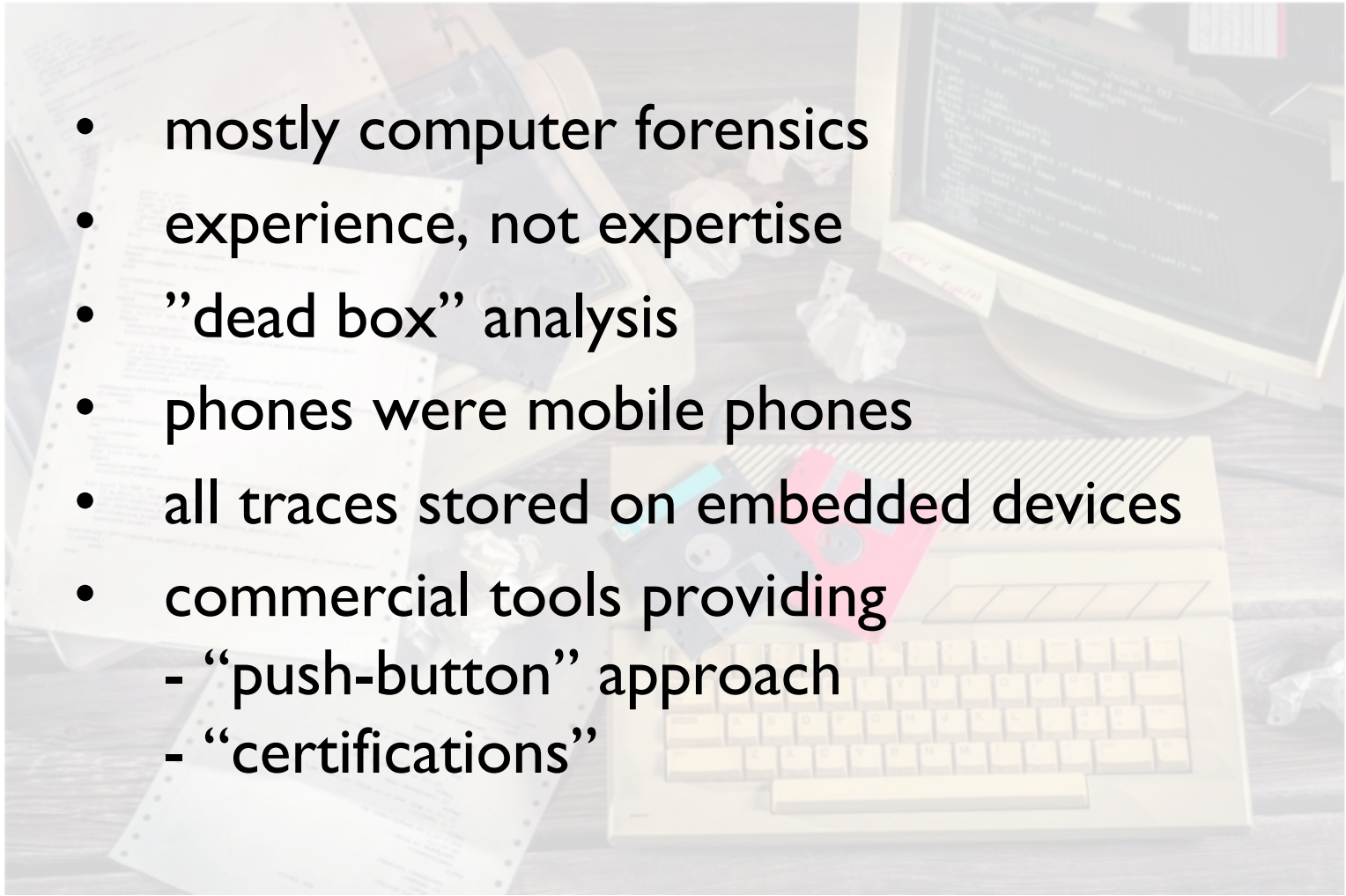
obsolescence ?

Sony digital mavica
produced in 1997
still working and useable today
if you find:

- a floppy disk
- batteries

knowledge obsolescence ?

Cybercrime fighting early times



- mostly computer forensics
- experience, not expertise
- ”dead box” analysis
- phones were mobile phones
- all traces stored on embedded devices
- commercial tools providing
  - “push-button” approach
  - “certifications”

The digital evidence as an exception

- Difference between technical evidence and expert evidence ?
  - Live data forensics needs to take decisions
  - Chip-of is sometimes destructive
  - Cloud storage and IoT challenges
  - Cyber attacks and networks
- Reproducibility is not possible anymore
- Traces without interpretation are often useless

Anatomy Lesson of Dr. Nicolaes Tulp
Rembrandt – 1632
Mauritshuis – The Hague

Do we need specialists ?

- To explain « How »
  - To investigation lead and magistrate
  - To react to cyber attacks
  - In front of court and jury
- To keep “in house” excellence
  - Following IT evolution
  - Be part and contribute in a network
- To explain “Why”
  - Suspects profiling
  - In front of court and jury

Why is it a challenge ?

- Specialists and experts are needed
  - to solve real world criminal cases
  - to advise management and law makers
  - to create and update course materials
  - to transfer their knowledge as trainers
- Priorities are set at national level
  - short-term approach
  - siphon off phenomenon

What's an expert staying in his/her corner ?

- Expert of the corner !
  - how to address technology evolution ?
  - how to address crime evolution ?
  - how to check hypothesis

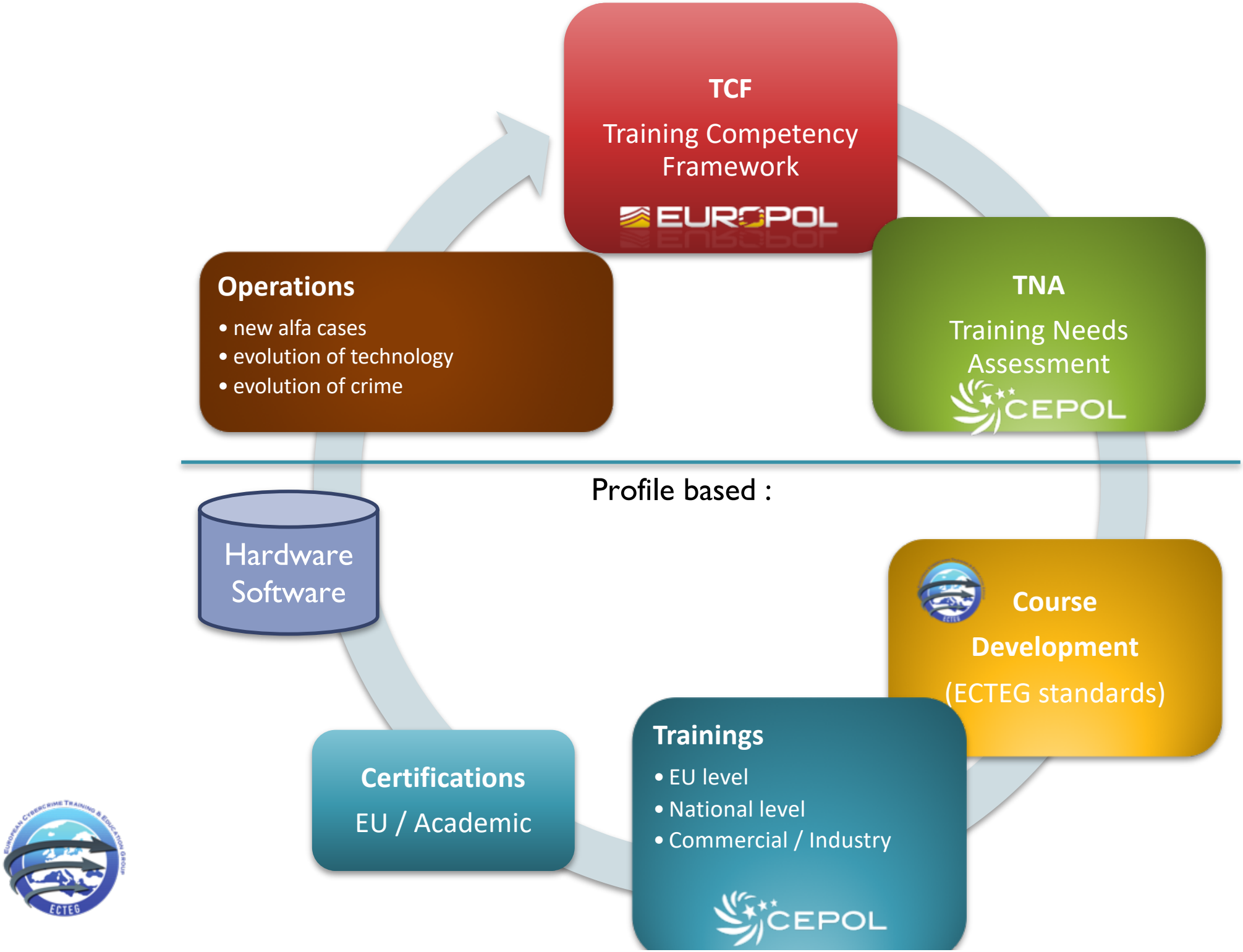
International approach solution

- sharing resources
  - experts
  - course materials
- organising EU level trainings

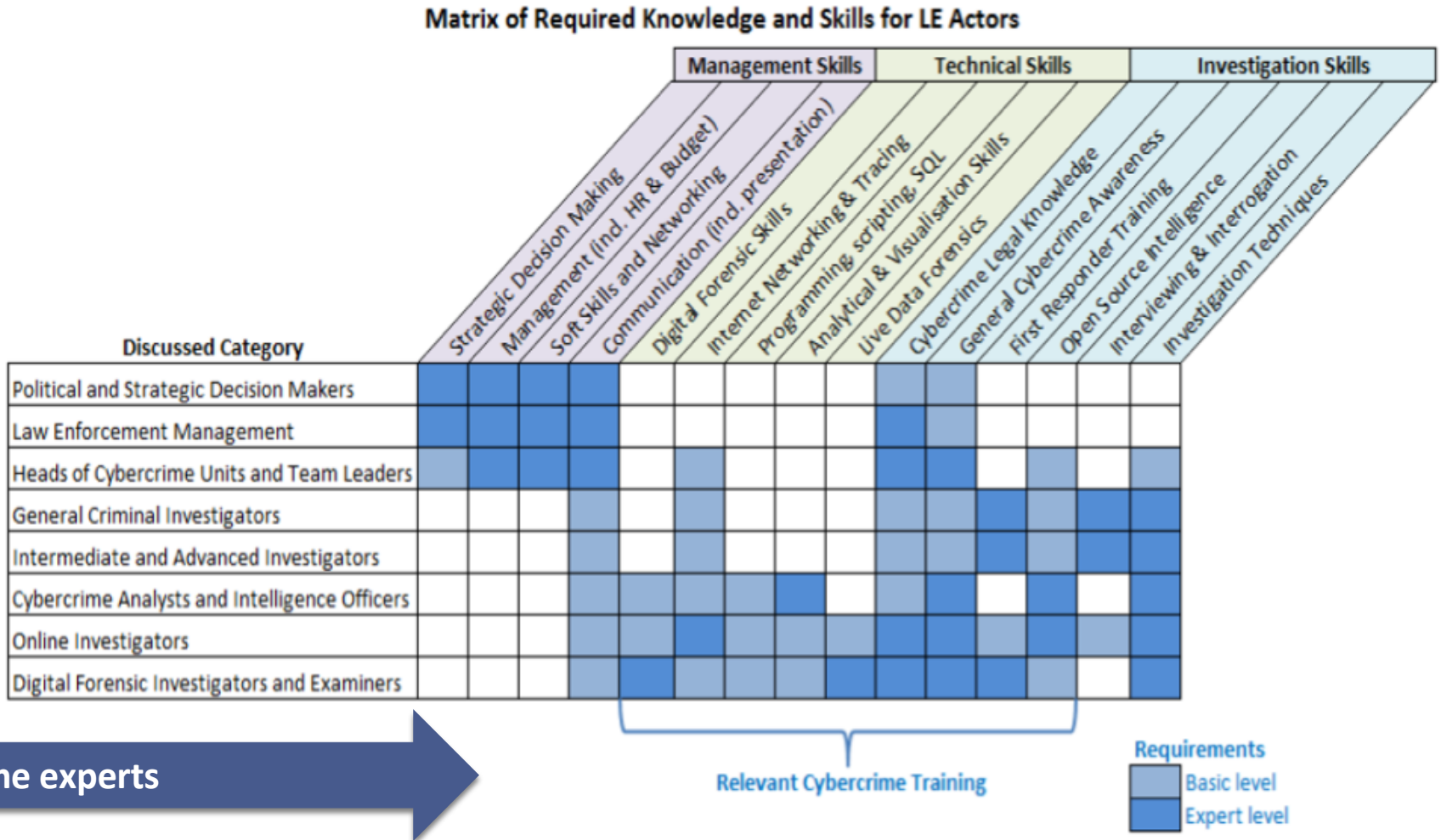
→ standards

sustainable networking

IT crime Training Governance Model


TCF
Training Competency Framework
EUROPOL
TNA
Training Needs Assessment
CEPOL
Operations
• new alfa cases
• evolution of technology
• evolution of crime
Profile based :
Hardware
Software
Course Development
(ECTEG standards)
Trainings
• EU level
• National level
• Commercial / Industry
CEPOL
Certifications
EU / Academic

Training Competency Framework



Cyber crime experts

First responders

ECTEG working on five components:

- Training based on needs
- Addressing soft skills too
- Create a sustainable expert network
- Collaboration with the academic world
  - Research and Development
  - Detect new trends
  - Certify skills and competences
- Implementation of a quality process

ECTEG ?

- Since 2001,
  informal working group starting with a few members from EU Law Enforcement and Universities

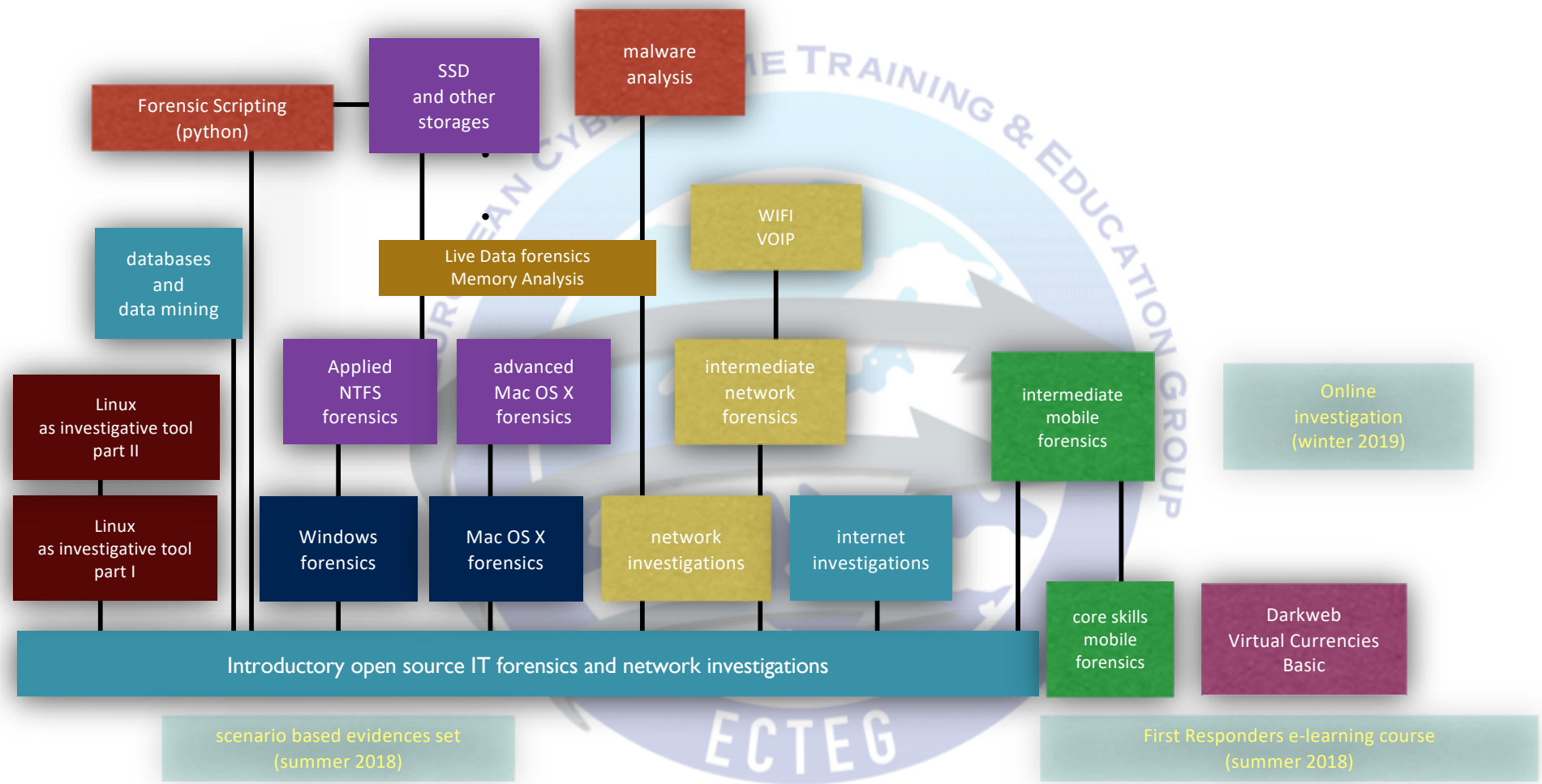
- Nov 2016,
  became officially
  International Non Profit Association

- EU funding

ECTEG course packages

- Full courses packages available for free and **LEA only**
  - trainer manual
  - trainer presentations
  - student manual
  - practicals / fake suspect artefacts .. (including virtual machines)
  - exams

ECTEG training materials



ECTEG course development standards

- Integration in the ECTEG framework
- Synergy with other projects (education, R&D)
- Modularity
- Education instead training only
- Knowledge and practical
- No tool dependant
- Exercises using open source tools
- International experts on topics
- English, localised whenever needed and possible
- Pilot courses

Project : crimes scenarii

POLITIHØGSKOLEN

- Project driven by NUCP (Norway)
- Deliverable : crime scenario, with associated set of evidences to support all training modules
  - Computer Forensics
  - Network Forensics
  - Computer crime (cyber attacks)
- Documentation
- Support for all modules, including non ECTEG projects becoming ECTEG products

Project : Online investigators

- Driven by UCD (Ireland) based on a previous project slightly adapted
- Covers the TCF profile
- Deliverables :
  3 weeks training package with on-line resources
- Pilot : 2018 : 3 x 1 week with exercises in between
- Synergy with :
  - Existing initiatives in EC3 on good practices and tools
  - Certification deployment project

Project : E-learning first responders

- Deliverables :
  - 7 EU languages e-learning packages (incl. Norwegian, Spanish & Portuguese)
  - Reference network of contributors around EU
  - Updating tools (opt-in and pull)
- Availability
  - English : Spring 2018
  - +6 additional EU languages : Winter 2018

Funded by European Commission

Global Cybercrime Certification Project

- Using Training Competency Framework as backbone
  (profile based certification)
- Unlinked from the training
- Checking competences and skills
  - Theory & practice by academic partners
  - Internship for most profiles
- Limited validity 5 ≃ 3 years
- Transition from existing ones (*i.e. IACIS*)
- Compatible with academic degrees (bachelor, master)

Advantages

- Mutual recognition of expertise levels
- Valorisation of practitioners
- Harmonisation through EU
  - Profiles harmonisation
  - Defining procedures and standards
  - Practitioners network
  - Career path
  - Training attendees prerequisites
- Support to national structures
  - Addressing capacity building issues

Step forward – model implementation

- Already advised when :
  - Creating new profiles
  - Creating new training packages
- Governance board
  - Europol, CEPOL, Eurojust, ECTEG, EUCTF, …
  - Certifying body
  - Accreditation bodies organising certifications
- Certification organised by accredited bodies :
  - Implementation checked by governance board members

Applying for ECTEG materials

- Law Enforcement
- Academic Institution
  with letter of support from LEA

- Attendees may only be from Law Enforcement

- www.ecteg.eu/apply4materials/
  - application for materials
  - includes some commitements

contact data

Canterbuty Christchurch University

Dr. Abhaya Induruwa

abhaya.induruwa@canterbury.ac.uk

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

www.ecteg.eu

Yves Vandermeer

yves.vandermeer@ecteg.eu

twitter : @ecteg