FEBRUARY 2024 UPDATE

ECTEG

EUROPEAN CYBERCRIME TRAINING AND EDUCATION GROUP

TRAINING CATALOGUE

Funded by
the European Union

Table of Contents

Funded by the European Union

1 Introduction

What is ECTEG?

ECTEG (the European Cybercrime Training and Education Group) is an International Non-Profit Association, funded by the European Commission´s Internal Security Fund (DG HOME).

It gathers Law Enforcement Agencies, Academia and other non profit associations fighting against **cybercrime, cyber-enabled crimes** and conducting **digital crime** education at the national and international levels.

More info

Why is ECTEG an EU-funded initiative?

ECTEG aims to provide a structure where experts can meet to share experiences and specialised knowledge, intending to give the EU Member States and other countries an increased capacity to fight against cybercrime. Its activities also support harmonising cybercrime training across European and international borders.

Funded by the European Union

2 Course Materials: Developments and Updates

Course Developments

With the support of its members, ECTEG contributes to developing electronic evidence training materials and capacity-building tools to support the fight against cybercrime. This also allows its experts community to share the latest investigation techniques, methods and strategies, and to promote the mutual exchange of experiences.

Course Updates

Training materials, especially in fighting cybercrime, must be constantly updated to keep up with the latest technological advances and criminal trends. Experts need to keep abreast of such developments.

At the same time, they need to continuously improve their understanding of how digital evidence is extracted and processed, not relying on proprietary software, but inspecting each piece of information and tooling used in detail.

This improves their investigative and forensic skills and safeguards the due diligence in criminal court case proceedings.

Funded by
the European Union

3 National and International Deployment efforts

Efforts in capacity-building are focused on **enhancing and promoting capacity** at the national and international levels.

At the **national level**, actions aim to encourage the incorporation of ECTEG materials into national LEA curricula sustainably and efficiently.

At an **international level**, the priority is to train all police officers from different countries, resorting also to "Training of the Trainer" models, attending to the needs and gap analysis marked by the international partners and members of ECTEG.

ECTEG Quality Processes

A Quality Management process has been set up to ensure that ECTEG standards and quality are assured throughout the development and delivery of all ECTEG courses.

ECTEG conducts surveys to both trainers and students to gather **continuous feedback** and improve its development processes, training and education offer.

Funded by the European Union

4 Catalogue Content

Available Course Packages

This catalogue contains all available ECTEG course materials:

- **Online courses**: online learning experiences open to medium to large groups of students, with or without trainers.
- **On-site courses**: classroom-based learning experiences for a small cohort of students gathering physically on location, under the guidance of two or more trainers. Some are combined with online *preparation* materials.

This **public information catalogue** can be shared widely within and outside Members’ organisations.

ECTEG **does not** organise courses or training activities: all course materials developed for ECTEG are **free and available only** for **Law Enforcement organisations**[1] involved in IT forensics, fighting cyber-dependent or cyber-enabled crime training processes.

How to request ECTEG course materials

To organise trainings based on ECTEG material, check the requirements and procedures on the ECTEG webpage: htttps://www.ecteg.eu/apply4materials/

[1] If you wish, as an individual, to participate in a training activity, we suggest referring to your national police academy / training center and, as some courses are organised yearly by CEPOL, to your CEPOL national representative.

Funded by the European Union

Online Course Materials

1. **eFIRST**
2. **eCDWI**
   Cryptocurrencies and Dark Web Investigations Online
3. **eCN**
   Introduction to Computer Networks
4. **ePy3**
   Python Programming for Law Enforcement Investigators
5. **eDecrypt**
   Lawful decryption

Funded by
the European Union

eFirst

Cybercrime and Cyber-related crime knowledge base for LEA First Responders

> I was a first responder in the beginning of my career, and I really would have liked to have had this kind of training!
> I am now Head of the Cybercrime Unit of Polícia de Segurança Pública and lead this important project.

Sónia, project leader from Portugal

A first-responders (field police officers without IT expertise) self-paced e-learning package focused on essential IT forensics and IT crime knowledge. The package can also be used to tackle the ever-challenging pre-requisite knowledge required before attending residential training, while providing a common sound reference for all LEA first responders and to all attendees to advanced-level IT forensics courses.

Course aims: identifying and seizing potential electronic evidence (including "live data" forensics); gaining awareness and basic knowledge on digital forensics, cybercrime, the Internet and its services, encryption, dark web and cryptocurrencies and other topics.
Several criminal phenomena are explained to assist victims of crimes facilitated by the use of new technologies when taking a complaint and starting a criminal case.

The package is available in many EU languages and can be adapted to national legislation and guidelines.

Level: Beginner

Flexible study, approx. 60 hours of self-learning material

Law Enforcement First Responders, Law Enforcement Officers or judicial authorities

Online, self-paced and interactive

Theoretical chapters, Serious Games, Quizzes for Self-Assessment

Funded by
the European Union

eCDWI

Cryptocurrencies and Darkweb Investigations

This course on Cryptocurrency and Dark Web Investigations was developed for Law Enforcement officers dealing with investigations of all types of criminal phenomena (drugs, weapons, cybercrime) facilitated by cryptocurrency and/or the Dark Web.

It covers various topics, such as introductions to anonymity and encryption, cryptocurrency basics and seizing, and the Dark Web criminal landscape.

Developed and maintained with the support of

EMPACT CEPOL

Level: Beginner

2 weeks (10 working days)

Law Enforcement Investigators

Online self-paced with instructor-led live sessions

Theoretical material with illustrations, screencasts, examples, how-to instructions, self-check exercises, graded tests.

Funded by the European Union

eCN

Introduction to Computer Networks

This course gives an overview of computer networking and data communication topics.

Starting with a simple example of a user surfing on a website, the course explains how all network parts interact and make this possible. Opensource software tools are used to observe each component's behaviour and reflect on how it may be compromised.

A set of guided labs facilitates the acquisition of knowledge.

A PDF Manual is available.

Level: Beginner

Flexible, approximately one to two weeks

Digital Forensics Examiners

Self-paced, only available in English.

Theoretical chapters, Practical Exercises, Labs

Funded by
the European Union

ePy3

Python Programming for Law Enforcement Investigators

The course teaches Law Enforcement investigators Python programming language skills (without any prerequisite of having prior programming experience) and how to apply them in cybercrime investigations and digital forensic examinations.

The course aims to build knowledge and skills such as programmatic problem solving, code reuse, user input validation and file input and output; text processing and database analysis; retrieving data from online sources, and developing solutions for scraping and monitoring websites.

The acquired skills allow to improve the use of existing digital forensic software by addressing limitations and introducing some automation and batch processing.

Developed with the support of osce

Level: Intermediate

2 -12 weeks flexible study

Law Enforcement Investigators and Digital Forensics Examiners

Self-paced / Trainer-led webinars

Theoretical Classes, Practical Exercises, Quiz, Coding Assignments

Funded by
the European Union

eDecrypt

> We made several pilots of the Decrypt course, to assess the content and receive feedback from all participants.
> This was the best way, in my mind, to enrich the course and make it suitable for all students.

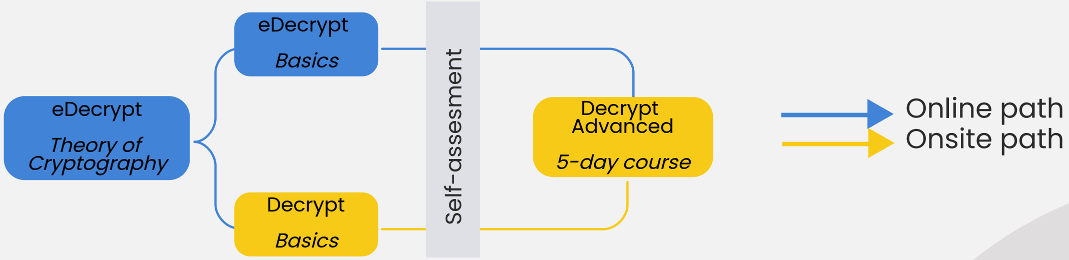
Developer and Trainer from France

Lawful decryption

These course materials aim to provide a sustainable training package to allow EU Member States' law enforcement agencies to enhance their lawful decryption capacity building at the regional and national level.

eDecrypt tackles the essential skills needed to retrieve keys and passwords necessary to decrypt evidence lawfully. One of its modules, Decrypt Basics, is available both on-site and as an online module. To provide the required cryptographic background for the course, a tailored, exercise-rich introduction is offered in the module "Theory of Cryptography".

See the suggested Training path, showing also the continuing Decrypt Advanced (on-site):



Level: Intermediate

Approx. 30 hours

Law enforcement w/basic experience in decryption

Self-paced, online

Theoretical classes and exercises, including Capture the Flag challenges

Funded by the European Union

On-site Course Materials

1 **DFI**
Digital Forensic Investigator

2 **LDF**
Live Data Forensics

3 **MIN**
Malware Investigations

4 **AWFSF**
Advanced Windows File Systems Foreniscs

5 **NF**
Networks Forensics

6 **Decrypt Advanced**
Lawful decryption

7 **CyberEx**

Funded by the European Union

DFI

DFI

DIGITAL FORENSIC INVESTIGATOR

Digital Forensic Investigator

> It was the best opportunity to increase my Linux commands level. The first e-learning part starts from no background and reaches, let's say, a 20% level. The onsite part was more practical, with a lot of exercises and challenges. With the support of the trainers we succeeded in learning everything!

Madalina, participant from Romania

The course introduces participants to Open Source Digital forensics software, file systems, data carving, evidential digital artefacts, computer forensic strategies and data forensics, based on practical exercises on a realistic criminal investigation scenario.

An e-learning set of activities prepares students to attend a two-week classroom course, with practical exercises focusing on basic usage of the Linux command line interface. This approach reduces the quantity of theory on the onsite course and makes it more practical.

After completion of the training activity, the participants shall be able to, among other: explain and apply the rules of forensics and reporting, use a forensic distribution of the Linux operating system for basic tasks, acquire and access forensically digital evidence, recover deleted files, apply basic file carving tasks.

Level: Intermediate

Approx 20 hours self-paced e-learning and 10 days on-site course

Law enforcement agencies (LEA) cybercrime investigators and digital forensics examiners

Self-paced e-learning followed by a trainer-led on-site practical course

Theoretical classes, exercises, practical scenario-based criminal case

Funded by
the European Union

LDF

Live Data Forensics

This theoretical and practical course aims to introduce Live Data Forensics and the use of Live Forensic investigative techniques.

It covers Live Forensic techniques on running computer systems, concentrating on aspects such as acquiring volatile data, acquiring Cloud and Remote Storage and analysing Memory to determine the next steps.

It does not cover portable Devices (smartphones, etc.) or Server Environments Embedded Systems (e.g. IoT, Automotive IT).

Level: Beginner

14 hours of e-learning and one week on-site course

Law enforcement staff handling running computers in searches

Self-paced e-learning followed by a trainer-led on-site course

Videos, theoretical classes, exercises, practical scenarios

Funded by
the European Union

wMIN

Malware Investigations

This course handles the basics of malware analysis for Windows Portable Executables.

It aims to obtain information from the malware analysis process that will help identify criminals and their infrastructure: it will give the participants a better view of extracting or gaining information from a piece of malware, while discovering where to get this information and the tools to achieve it.

It is not a course on reverse-engineering malware or the disassembly of binary files.

Level: Intermediate

Max 19 hours of e-learning and one-week on-site

Law enforcement with experience in forensic analysis

Self-paced e-learning followed by a trainer-led on-site course

Theoretical classes and exercises

Funded by
the European Union

AWFSF

Advanced Windows File System Forensics

Windows File Systems are the most often encountered in computer digital forensics.

Aiming to provide advanced knowledge on NTFS and exFAT file systems, the course will contribute to a better understanding of the existing digital forensic tools' limitations, identify and recover hidden pieces of evidence, and improve the reporting accuracy as well as the timeline and suspect's behaviour profiling.

Participants should have a sound understanding of digital forensics, covered in the DFI course.

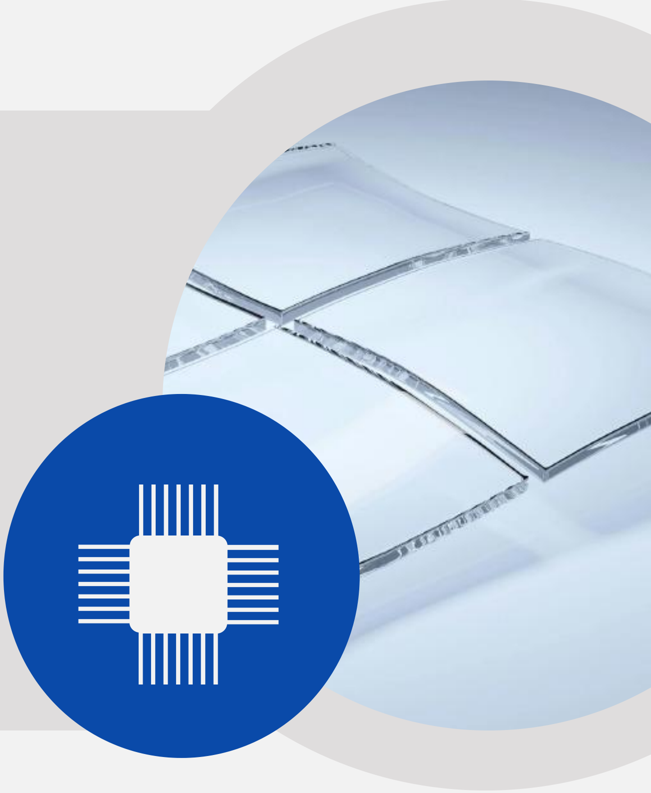
Level: Advanced

5 days on-site

Law Enforcement Investigators and Digital Forensics Examiners

Trainer-led

Theoretical Classes, Practical Exercises, Quizzes



Funded by
the European Union

NF

Networks Forensics

The course aims to provide general and practical knowledge of Networks Forensics at an intermediate level. The eCN course is recommended as its baseline.

Some topics, among others, are how to obtain information for network analysis and acquire valuable evidence during an investigation.

Training will encompass latest best practices, technologies and techniques available to Law Enforcement specialists.

Level: Intermediate

On-site, 5 Days

Digital forensics examiners and Cybercrime Investigators

On-site course, materials in English

Theoretical class, Exercises, Labs

Funded by
the European Union

Decrypt Advanced

Lawful decryption

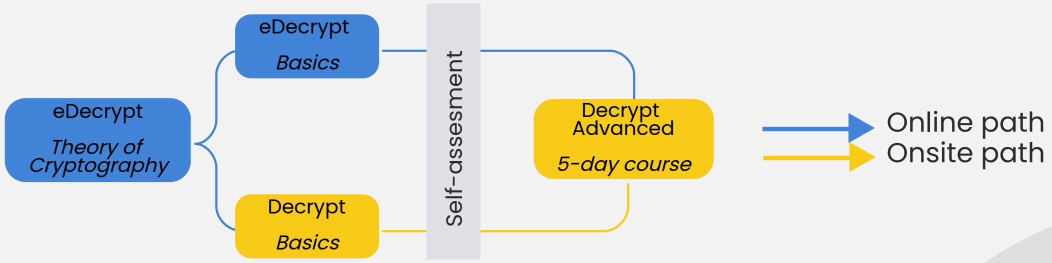
> Using knowledge gained in this course,
> I managed to open an encrypted
> container in a murder case.
> Thanks to everybody involved
> in teaching!

Participant from Germany

These course materials aim to provide a sustainable training package to allow EU Member States' law enforcement agencies to enhance their lawful decryption capacity building at the regional and national level.

Sequel to eDecrypt, **Decrypt Advanced** dives into more sophisticated strategies for handling encrypted evidence in a lawful manner. The materials include topics such as technical and background information, but the course is founded on hands-on activities, like solving exercises and "capture-the-flag" competitions to challenge the students and transfer skills.

See the suggested Training path, showing also the preceding eDecrypt (online):



Level: Advanced

One-week on-site

Law enforcement with experience in decryption

Trainer-led on-site course

Theoretical classes and exercises, including Capture the Flag challenges

Funded by
the European Union

CyberEx

Cyber Incident Response

A training product available for cyber-investigators who are the first to arrive on the scene and must preserve all possible traces and evidence, particularly the digital forensic traces that were generated, using all the new technologies.

It focuses on traces that can be found on hardware itself but also on other devices with which they communicate (printers, scanners, GPS cars/GSM, Fit-bit, gaming consoles, remote controls of garage doors and fixtures).

Developed with the support of circl

Level: Intermediate

10 days on-site

Law Enforcement Investigators and Digital Forensics Examiners

Trainer-led

Theoretical Classes, Practical Exercises, Quizzes

Funded by
the European Union

Upcoming developments

eFirst (update)

Estimated Sept 2024

DFI (update)

Estimated end 2024

Malware (update)

Estimated end 2024

CTF - Capture the Flag

Estimated 2025

MacOS Advanced

Estimated mid 2025

And more to come!...

Funded by
the European Union

Funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.