EUROPOL

FORENSICS

Using state-of-the-art science to solve and prevent crimes

Forensics, or forensic science, involves applying the latest scientific methods to investigate and fight crimes in a range of areas. To this end, Europol provides forensic support to law enforcement agencies across the EU.

The crimes Europol thus helps fight include:

euro counterfeiting

illicit drug production

payment card fraud

cybercrime

FIGHTING COUNTERFEITING

Europol is the EU's central office for combating euro counterfeiting. The support it provides includes:

> forensic support to determine the origin of materials and devices used for the manufacturing of fake currency;
> expert support and training on how to protect the euro from counterfeiting.

TACKLING THE PRODUCTION OF ILLICIT DRUGS

Europol experts help to dismantle illicit production sites and to collect evidence in EU Member States. They also carry out technical investigations on custom-made and industrial equipment seized from drug production and storage units.

Europol also has in place a number of forensic systems that it uses in the fight against illicit drugs:

> The Europol Illicit Laboratory Comparison System (EILCS) processes photographic and technical information on synthetic drugs.
> The Europol Synthetic Drug System (ESDS) includes information on modi operandi and significant seizures. This enables the identification of matches between seizures.
> The Europol Specific Means of Concealment (ESMC) system contains information on the concealment methods used to transport cocaine.

FIGHTING CYBERCRIME

The European Cybercrime Centre (EC3) offers its advanced digital forensics tools and platforms to investigations and operations in Member States, thus enabling a collective EU response to cybercrimes that:

> are committed by organised groups;
> generate large criminal profits such as online fraud;
> cause serious harm to the victim such as online child sexual exploitation;
> involve attacks on critical infrastructure and information systems in the EU.

PAYMENT CARD FRAUD

J-CAT

Europol's Joint Cybercrime Action Taskforce (J-CAT) has also supported several high-profile cybercrime operations against organised crime networks active in payment fraud.

Payment card fraud is highly profitable. It increasingly involves card-not-present transactions: the unauthorised use of credit or debit data to make purchases remotely, including via e-commerce websites. The tools criminals use to commit payment card fraud include:

> cloned cards

- counterfeit cards
- card readers and writers.

In response, Europol and its partners have their own arsenal of forensic-support tools, including:

- radio-frequency meters
- motorised card readers
- contactless card readers
- test cards.

OTHER TOOLS

A variety of other forensic-analysis tools are available to assist EU law enforcement authorities, including the Universal Forensic Extraction Device (UFED), a stand-alone mobile forensic kit that can extract data from 95 % of all mobile phones.

TRAINING

Europol regularly offers training to law enforcement authorities from within and outside the EU on a range of forensic techniques and best practices. Topics covered include:

- payment card fraud forensics and investigations:
  - skimming equipment and electronics
  - card-not-present and card-present fraud
  - ATM malware

- open-source IT forensics
- best practices in decryption
- combating online sexual exploitation of children

The courses on open-source forensics are offered in partnership with the European Cybercrime Training and Education Group (ECTEG), which supports the international harmonisation of cybercrime training.

The courses on decryption are offered in partnership with the European Commission's Joint Research Centre (JRC), which is known as the EU science hub.

These courses are important occasions for learning and knowledge-sharing, but they also strengthen professional ties that will help future investigations.

Source URL: https://www.europol.europa.eu/activities-services/services-support/forensics