**Beat: News**

# New Analysis Highlights Gaps in Police Tools, Training and Resources

**Europe's Digital Evidence Challenge**

Brussels, 16.10.2026, 16:27 Time

**USPA NEWS -** A new analysis from the European Commission and Europol has highlighted the difficulties facing law enforcement authorities as they work to recover and examine digital evidence. Published on 16 October, the assessment identifies gaps in technology, specialist knowledge and resources, alongside the need for stronger cooperation across the European Union.

A mobile phone, a connected vehicle or information stored in the cloud can hold vital clues to a criminal investigation. Messages, location records and other digital traces may help investigators establish what happened, identify those involved or test an account of events.

However, finding that information and turning it into reliable evidence requires specialist tools and expertise. The new analysis examines how European law enforcement can respond to an increasingly complex technological environment, drawing on consultations, surveys, expert meetings and contributions from Europol's European Cybercrime Centre.

Keeping Pace with Technological Change

Digital forensics involves recovering, preserving and examining information from electronic devices and systems. Its value extends well beyond offences committed online: evidence held on a device can also help investigators understand events in the physical world.

The European Commission says national authorities lack sufficient resources and capabilities in this field. Investigators must continually develop their skills and update their tools as technology changes, placing pressure on services already dealing with demanding workloads.

Uneven capabilities also affect cooperation between member states. Where specialist knowledge or technical capacity is limited, authorities can struggle to work effectively with colleagues across borders. The assessment brings these needs together to help guide future European action.

Making Tools Work Together

Standardisation and interoperability are among the analysis's central themes. In practical terms, this concerns whether forensic tools and working methods can support consistent examination and allow information to be used effectively across different systems.

For an investigation involving several countries, technical compatibility matters. Teams need to understand how material has been recovered, what procedures were followed and what limitations apply to the results.

A common approach can help make that process clearer. It can also support the sharing of expertise, allowing authorities to learn from work carried out elsewhere rather than repeatedly tackling the same technical problems in isolation.

The wider Commission roadmap includes developing an EU approach to standardisation in digital forensics, alongside support for forensic tools through European funding and cooperation with private organisations.

Evidence Beyond the Seized Device

Cloud services, connected household equipment and modern vehicles create further challenges. These are identified as key areas in the assessment, reflecting the growing range of technologies that investigators may encounter.

A seized device may provide only part of the picture. Relevant information could also be associated with an online account, a remote

service or another connected system. Investigators therefore need to establish where potential evidence exists and how it can lawfully be obtained.

Different technologies also produce different kinds of records. Understanding what those records mean, how they were generated and whether they are complete is essential before drawing conclusions.

This makes specialist knowledge particularly valuable. The presence of a digital record does not automatically explain who created it, why it exists or how it relates to an alleged offence.

Cost and Access to Specialist Technology

Affordability is another concern. According to the Commission, existing commercial solutions are often developed outside the EU, can be unaffordable and do not always match Member States' requirements.

The findings will help shape future Commission activity, including initiatives and projects supported through the Internal Security Fund.

For authorities considering new technology, the purchase price is only one part of the practical question. Tools must remain useful as devices, software and services change. Staff also need the knowledge to operate them properly and interpret their findings.

Investment therefore needs to consider the working life of a forensic capability, including training, maintenance and continued technical development.

Artificial Intelligence and Human Judgement

Artificial intelligence is also part of the discussion. The Commission's wider roadmap envisages supporting AI tools that can help authorities filter and analyse large quantities of seized data.

Such technology offers potential assistance with demanding analytical tasks. However, identifying a possible connection is different from establishing its significance.

An automated result still needs careful examination. Investigators must consider context, check the underlying material and recognise the possibility of errors. Forensic findings must be capable of meaningful scrutiny, particularly when they contribute to decisions affecting an individual's liberty or reputation.

Training from the First Response to the Courtroom

The assessment also identifies training and expertise gaps among first responders and legal professionals.

That focus recognises that digital evidence passes through several hands. The first person encountering a device may need to recognise its potential relevance and seek specialist assistance. Later, prosecutors and other legal professionals must understand what the examination establishes and where uncertainty remains.

Clear communication between technical specialists and the justice system is therefore essential. A detailed forensic result is useful only if its meaning and limitations can be explained accurately.

Effective Investigations and Fundamental Rights

The analysis follows the Commission's June 2025 roadmap on lawful and effective access to data, which sets out work on forensic capability, cooperation and technical development.

The Commission's stated approach requires access to data to be necessary, proportionate and grounded in clear law, with independent oversight and effective remedies. It also recognises the importance of privacy, data protection and secure digital systems.

For Europe's law enforcement authorities, the challenge is both technical and organisational. Better tools need skilled people,

sustained support and procedures that produce dependable evidence. The value of this analysis will ultimately lie in how effectively its findings are translated into practical improvements across member states.

**Article online:**
https://www.uspa24.com/bericht-27285/new-analysis-highlights-gaps-in-police-tools-training-and-resources.html

**Editorial office and responsibility:**
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): Daren Frankish

**Exemption from liability:**
The publisher shall assume no liability for the accuracy or completeness of the published report and is merely providing space for the submission of and access to third-party content. Liability for the content of a report lies solely with the author of such report. Daren Frankish

**Editorial program service of General News Agency:**
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com
Official Federal Reg. No. 7442619