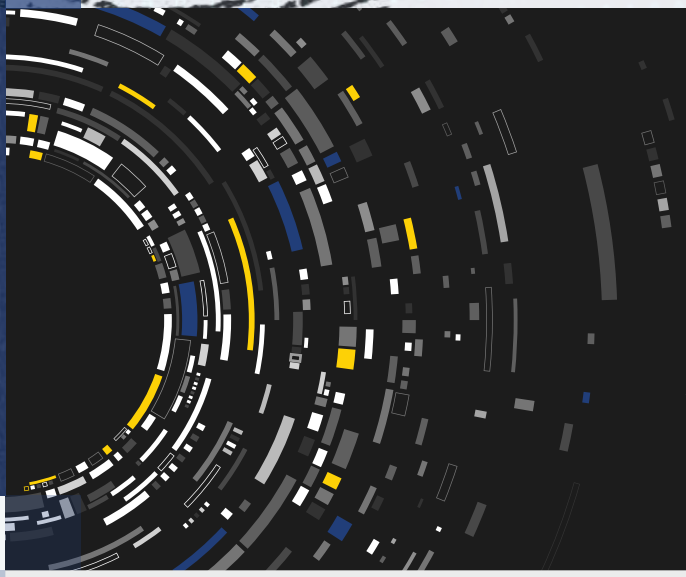
EUROPOL

DIGITAL FORENSICS:
GAP ANALYSIS



Contents

3 **Introduction**

4 **Background**

5 **Gap analysis**

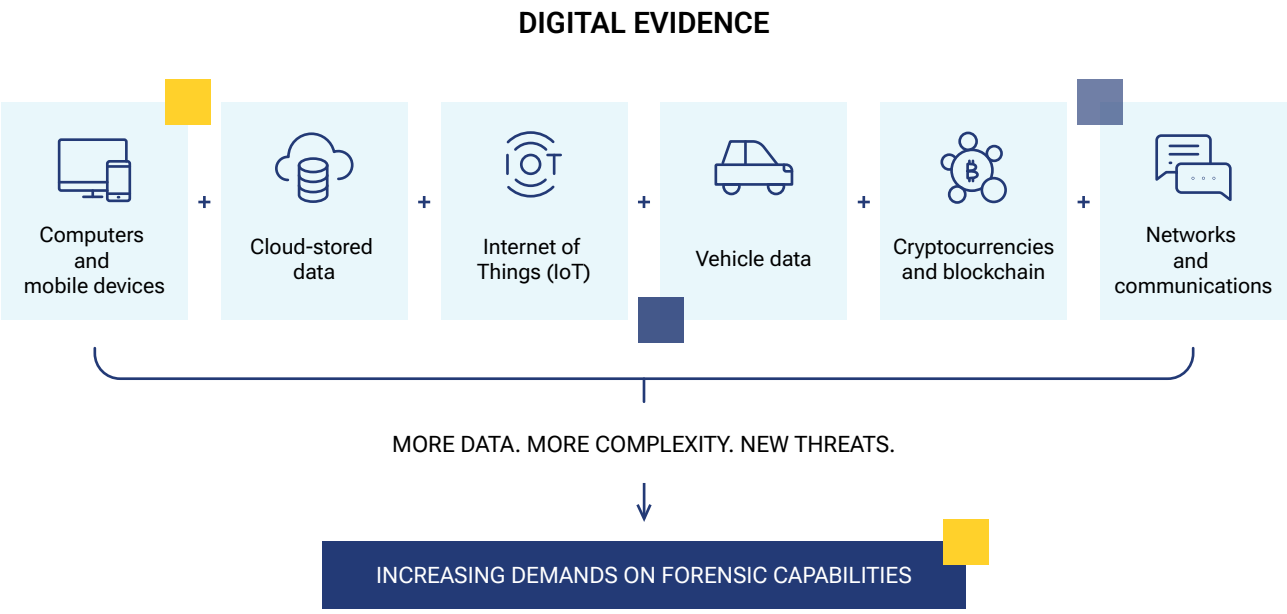
- 5 Digital forensic tools
- 9 Establishing synergies
- 10 Standardisation
- 13 Lack of cooperation with manufacturers
- 14 Shared platforms and tools as a service
- 15 Virtual currencies
- 16 Vehicle forensics
- 18 Internet of Things (IoT)
- 19 Use of artificial intelligence (AI) in forensics
- 21 Training

23 **Conclusions**

Introduction

In an era where digital evidence underpins nearly every criminal investigation, the ability of law enforcement authorities to effectively analyse seized devices has become a cornerstone of modern policing. Digital forensics is no longer a niche capability but a critical operational necessity. However, European law enforcement agencies (LEAs) face mounting challenges in keeping pace with rapid technological advancements, evolving criminal methodologies, and the sheer volume and complexity of digital data. From encrypted communications and cloud-stored evidence, to the proliferation of Internet of Things (IoT) devices and cryptocurrencies, the digital landscape is transforming at an unprecedented rate, often outstripping the tools, skills, and resources available to digital forensic examiners.

Recognising these challenges, the European Commission, in close cooperation with Europol, initiated a comprehensive gap and needs analysis to assess the current state of digital forensic capabilities across EU Member States. This analysis was designed to identify systemic weaknesses, prioritise investment, and foster collaboration in tool development, standardisation, and training. The resulting insights are intended to inform EU-wide strategies that enhance cross-border cooperation, reduce reliance on non-EU commercial solutions, and ensure that law enforcement remains equipped to tackle cyber-enabled crime, terrorism, and other digital threats. By addressing gaps in tool availability, interoperability, and expertise, this report aims to lay the groundwork for a more resilient and unified digital forensic ecosystem—one that safeguards investigative integrity while adapting to the demands of an increasingly digital society.



Background

On 24 June, the European Commission adopted a Roadmap for lawful and effective access to data for law enforcement purposes[1], to follow up on the recommendations[2] and the concluding report[3] of the High-Level expert Group on access to data for effective law enforcement[4].

The Roadmap sets concrete actions that the Commission has committed to take in six key areas:

- (i) Retention of data by communication service providers.
- (ii) Lawful interception of communications.
- (iii) Digital forensics.
- (iv) Lawful decryption.
- (v) Standardisation.
- (vi) Data analysis through artificial intelligence.

The roadmap also notes that national authorities suffer from a severe lack of resources and capabilities to conduct digital forensics. They struggle to keep up with the need to continuously develop new skills and tools to keep pace with the digital transformation of the society and its related new technologies. Cross-border cooperation among Member States is undermined by the lack of comparable capacities and by the absence of mechanisms for mutually recognising digital forensics experts' skills and expertise. Existing commercial solutions quickly become obsolete, are unaffordable, and are often developed outside the EU. They may also be poorly suited to the needs of Member States' authorities or may not meet EU digital forensics' accountability standards or other legal requirements.

As a result, to strengthen the ability of European law enforcement authorities to perform digital forensics on seized devices, it is necessary to provide targeted funding for projects, both for the research and development of digital forensics tools and for their uptake.

In response to these recommendations, the Commission, in cooperation with Europol, has coordinated this gap analysis of research, development,

1 Roadmap for lawful and effective access to data for law enforcement, accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0349

2 Recommendations of the HLG on Access to Data for Effective Law Enforcement_en.pdf, accessible at https://home-affairs.ec.europa.eu/document/download/1105a0ef-535c-44a7-a6d4-a8478fce1d29_en?filename=Recommendations%20of%20the%20HLG%20on%20Access%20to%20Data%20for%20Effective%20Law%20Enforcement_en.pdf

3 Concluding Report of the HLG on access to data for effective law enforcement_en.pdf, accessible at https://home-affairs.ec.europa.eu/document/download/4802e306-c364-4154-835b-e986a9a49281_en?filename=Concluding%20Report%20of%20the%20HLG%20on%20access%20to%20data%20for%20effective%20law%20enforcement_en.pdf

4 High-Level Group (HLG) on access to data for effective law enforcement, accessible at https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en

deployment maintenance, and uptake of common and/or shared technical solutions for digital forensics.

The findings presented in this document were gathered through a series of consultations, dedicated meetings and surveys with stakeholders and Europol EC3[5] experts. The information gathered was enriched with relevant documents[6] and scientific papers.

For the purpose of this document, digital forensics is defined as: *"… the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony".*

Gap analysis

1. Digital forensic tools

The firs takeaways that can be extracted from the information obtained during the gap analysis exercise are the following.

- The information gathered confirms the common knowledge that **EU companies** occupy a **relatively small share of the market** for commercial digital forensic tools, despite the fact that are significantly cheaper than others. Moreover, EU-made tools are only able to cover a relatively small part of the devices market.
- Some Member States **rely on commercial and open-source tools**, while others indicate that they use exclusively commercial tools. For example, some Member States make use of open-source tools developed in the framework of the EU-funded project FREETOOL[8] and further refined by the European Anti-Cybercrime Technology Development Association in the context of the project Tools4LEAs[9].
- **Open-source initiatives** have developed software on specialised topics. Some rare examples include The SleuthKit (TSK) and its related graphical interface, Autopsy, Wireshark, and Volatility, demonstrating

5 Europol Cybercrime Centre

6 Such as those developed in the context of different projects (CYCLOPES, iLEAD, FORMOBILE)

7 https://csrc.nist.gov/glossary/term/digital_forensics

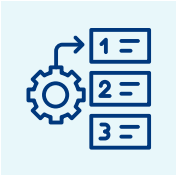
8 https://www.ucd.ie/cci/projects/freetool/

9 https://www.tools4leas.eu/

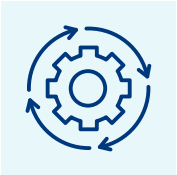
that open-source software can be improved and maintained through contributions from a large community.

- Some **successful examples** in specific targeted areas exist, such as the European Vehicle Forensics Framework (EVFF) for digital forensics analysis of vehicle data. Although in some targeted areas, existing solutions might be too large and complex, while other areas can be covered by one or more simpler tool(s) or through the integration of multiple (smaller) tools.
- **Needs expressed by national LEAs are multiple and diverse**, and therefore might require different kinds of solutions. Some of the needs identified are covered (totally or partially) by tools that are already being used by some end-users. It remains unclear if end-users are aware of the existing solutions and, if so, why existing solutions are not satisfactory.
- Solutions that combine multiple tools can include commercial and open-source modules. **Modularity** allows easier and more agile maintenance and evolution of the overall solution, allowing a more swift response to the sometimes quite rapidly evolving nature of the needs or to the underlying technologies. In some cases, a dedicated library, with **specific** software that can be linked to others, may provide a solution.

Recommendations



Prioritisation: in general, better mechanisms should be created to prioritise the development of digital forensic tools and avoid duplication. Such mechanisms should include shared sets of operational priorities based on threats, a common repository, and national statistics.

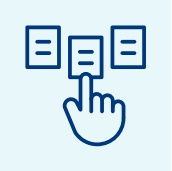


Development and evaluation: due to the technical limitations of commercial software solutions and given the high cost of industry-provided solutions, some law enforcement practitioners develop their own tools. Although the solutions are innovative and useful, they may lack documentation, may struggle to be maintained, and are often limited to a single country or, at times, to the unit where they were developed.

Projects suffer from a lack of instruments and infrastructure. Some examples include a platform to develop and customise LLM and AI solutions, and common datasets (which each project currently has to build each time). Another is an environment to test newly developed tools. Such an environment would allow tool developers to assess the target user requirements when defining feature specifications and ensure that the released features meet their intended purpose. Users would also be able to assess whether the methods used, including the use of tools, validate the application's purpose.

Existing services are offered by the Europol Innovation Lab in regards to tool testing such as the Research and Innovation Sandbox and should be more broadly communicated and advertised to reach a larger community of developers. In addition, the Commission will continue its efforts to bridge research and development with uptake via dedicated projects, and to support the European Anti-Cybercrime Technology Development Association (EACTDA)[10].

Licensing: intellectual property (IP), intellectual property rights (IPR), and software licenses are an essential part of any software development and/or usage scenario. As any software solution almost always includes various software components (Software Bill of Materials - SBOM), each of them with its own IP/IPR/license, end-users may own some of the IP (if they developed all or part of the software). However, in most cases they will not own the IP of the whole SBOM, and third-party components are used/included whose IP is not owned by the developer(s). The IPR/licenses of the whole software tool's /solution's entire SPOM must be respected. IP owners can license their IP using one or more licenses. Where non-commercial, cost-free software is concerned, strong-copyleft licensed software is to be avoided. **Model licensing agreements** should be available for developers to ensure that IP ownership is respected and that tools can be used and distributed under favourable conditions (e.g. cost-free for law enforcement).



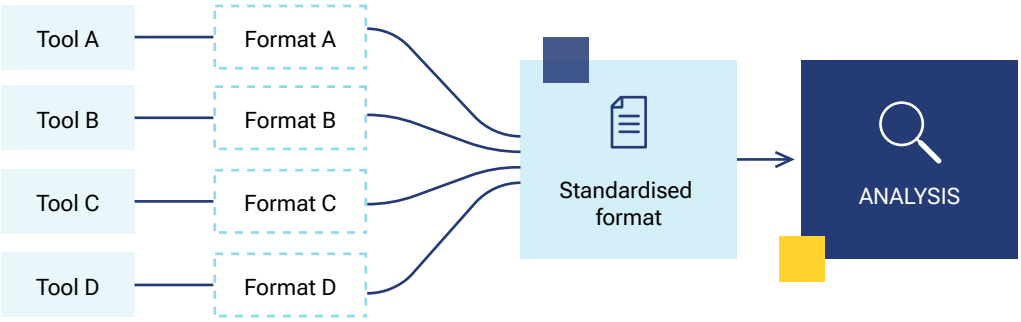
Selection: a catalogue of existing and available tools consolidated in a manner that allow LEAs to identify the solution that matches their specific need is still missing. This would facilitate a more precise gap analysis and the definition of which tools are to be developed by whom (for example, open source, free tools would complement commercial tools). Such a catalogue should be complemented by an assessment of the different functionalities, allowing for a comparison between different tools and for the selection of the most appropriate ones. Currently, digital forensic tools validation practices are highly fragmented. Each country applies its own criteria and methodologies for tool testing, resulting in reduced interoperability. Guidelines for selection can be developed to partially close this gap (see for instance the 'Mobile Forensic Tool – Checklist for Selection'[11]) and result in a uniform SOP for law enforcement, aligned with existing standards. Ideally an interactive AI based solution should exist to enable a straightforward identification of the most accurate tool by hands-on practitioners.

Data format: commercial solutions often use proprietary formats which hamper the ability of LEAs to integrate those tools in a sequence of data treatments; for example, when the application of several analytics to a specific set of evidence is

10 https://www.eactda.eu/index.html

11 "Requirements and Guidelines for a complete end-to-end mobile forensic investigation chain" CEN-CENELEC Ref. No.:CWA 17865:2022

required. As a consequence, digital forensics examiners often lose a lot of time preparing data that needs to be processed. More generally, the lack of standardised formats limits the ability to efficiently use modules in a pipeline. A recent initiative led by EACTDA aims at proposing, in a systematic manner, modules to provide interoperability between all tools developed by the association. Nevertheless, more efforts are required to promote the definition, implementation, and use of a standard data format and interoperable solutions.



Beyond that, standardising digital forensic data formats through recognised Standards Development Organisations (SDOs) such as the European Telecommunications Standards Institute (ETSI) is essential to the replacement of proprietary architectures with automated, multi-tool pipelines. This technical alignment could directly inform the EU's Rolling Plan for ICT Standardisation[12] by translating policy objectives for cross-border electronic evidence sharing into practical, operational realities. Adopting unified handover schemas, similar to the frameworks established by ETSI Technical Committee for Lawful Interception (TC-LI) facilitates secure, automated data exchange across diverse systems and jurisdictions. Furthermore, SDO-backed formats embed a structured, machine-readable chain of custody directly into the data, safeguarding its integrity and ensuring it remains legally admissible in court.

Distribution and uptake: it is important to provide law enforcement authorities with a one-stop-shop for accessing open-source tools, which are not necessarily publicly available. The Europol Code Repository (ECR) and the Europol Tool Repository (ETR) already provide a secure, LEA exclusive platform for sharing non-commercial, cost-free software developed by Europol, the European Commission's Joint Research Centre, European law enforcement agencies, academia, and non-profit research organisations.

In this area, procedural and operational guidelines including the available tools produced by EUROPOL would support the uptake of these tools. For example, an operational and interactive map, where the practitioners could consult and directly open the link to the tool and documentation when necessary

12 EC, Rolling Plan on ICT Standardisation, source: https://digital-strategy.ec.europa.eu/en/policies/rolling-plan-ict-standardisation ; accessed: 17/07/26

for an investigation. Mechanisms providing maintenance, support, and updates, are important, and require adequate funding and resources. When practitioners are presented with the choice between commercial tools that include support for installation, management, updates, and training courses, and free, open-source tools which do not include clear support, they typically opt for the former.

2. Establishing synergies

There is a need to **create and ensure the sustainability of subject-matter expert communities** in various fields with corresponding goals and objectives. These expert networks should be multidisciplinary and benefit from the contribution of non-LEAs experts, where relevant. Existing communities should also be supported. The new Joint Research Centre (JRC) Security Campus, launching in September 2026[13], could pioneer this support by facilitating developer meetings.

The objectives of such communities would be to:

- **Build and sharing of knowledge and expertise.**
- **Facilitate the development of project proposals and contributions to ongoing projects.**
- **Allow for a holistic approach to capacity building, covering research, development, and training.**
- **Establish de facto standardisation in the medium term.**

These communities should be maintained and stimulated by projects, volunteers, the European Commission, Europol, and the JRC, depending on their specificities. They should also be provided with virtual and physical collaborative spaces to coordinate, cooperate and meet. Some examples of activities that can incentivise the creation and maintenance of such activities would be the development of workshops, sprints, and training activities, where the organisers manage the funding and logistics.

Communication across communities is equally important and dedicated mechanisms should be put in place, starting with an overview of existing

13 Security Research & Innovation Campus, Joint Research Centre, https://joint-research-centre.ec.europa.eu/scientific-activities/jrc-security-research-innovation-campus_en

communities. This would facilitate project integration and favour the creation of 'project families', for example in the area of mobile forensics.

3. Standardisation

Despite the existence of standards such as **ISO/IEC 27037**[14] **and ISO/IEC 27042**[15], the rapid evolution of **cloud computing, IoT systems, and cross-border investigations means that current standardisation efforts, supported by common taxonomy, remain incomplete,** particularly regarding **chain-of-custody documentation and forensic evidence acquisition in modern digital environments.** Below are examples of some of the challenges to standardisation efforts, categorised by the applicable context:

1 **Cloud forensics** (in cloud environments)

- Data may be distributed across multiple physical locations.
- Investigators do not control the hardware.
- Evidence may be volatile or automatically deleted.
- Investigators must rely on cloud service providers to forensically image user data.

Maintaining a **reliable chain of custody becomes difficult when the evidence is gathered by third parties or across jurisdictions.**[16] Additionally, forensic investigators often cannot create full disk images of cloud systems, or may not have access to logs or infrastructure-level artifacts.[17]

2 **IoT & emerging technology** (e.g., vehicle forensics)

Traditional digital forensic standards were designed for physical devices such as computers, mobile phones and hard drives. However, modern investigations increasingly involve: IoT devices (smart home systems, industrial sensors, etc.), drones, and connected vehicles.

These systems may:

- lack forensic interfaces;
- send data to external cloud platforms;
- generate evidence distributed across many systems.

14 ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence, https://www.iso.org/standard/44381.html

15 ISO/IEC 27042:2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence, https://www.iso.org/standard/44406.html

16 Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges, https://www.mdpi.com/1424-8220/24/2/433

17 Interpol review of digital evidence for 2019–2022 - ScienceDirect, https://www.sciencedirect.com/science/article/pii/S2589871X22000985

Research shows that **the absence of standardised cloud-forensics frameworks for data acquisition can undermine the reliability and admissibility of evidence.**[18]

3 **Chain-of-custody management in complex digital investigations** (e.g., mobile forensics, virtual currency forensics)

Chain of custody ensures that digital evidence:

- has not been altered;
- is traceable through every handling step;
- can be trusted in court.

However, digital evidence often moves through many entities, including:

- first responders,
- forensic laboratories,
- investigators,
- prosecutors,
- cloud providers.

Researchers note that **current chain-of-custody processes are still largely manual,** which can create risks of errors or missing documentation, thus standards should be adapted regarding chain-of-custody management.[19]

Challenge:	Why standardisation is needed:
Cloud forensics	Evidence is distributed across providers and jurisdictions.
IoT and emerging technologies	Lack of forensic acquisition standards.
Chain-of-custody management	Complex evidence handling across organisations.

As a complement to possible standardisation efforts, it is important to develop **standard operating procedures and best practices.** Such documents already exist at national and international levels, but there is no mechanism currently in place to share these documents.

EU forensic testing body: tools being developed by law enforcement or those that are open-source and cost-free, need to be tested, evaluated and

18 Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation, https://www.researchgate.net/publication/377242721_Digital_Forensics_Challenges_in_Cyberspace_Overcoming_Legitimacy_and_Privacy_Issues_Through_Modularisation

19 [1807.10359] B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics, https://arxiv.org/abs/1807.10359

validated to facilitate uptake and deployment. The same applies to proprietary, commercial tools, for which validation procedures are not uniformly standardised and results may not be easily reproduced. Validation may take the form of distributed mechanisms, where different communities contribute to evaluation and validation. Independent testing of forensic tools is highly recommended. However, the effort and expense involved here should not be underestimated.

Testing, evaluation and validation is required for both software and hardware tools. It is an extremely time-consuming process that prevents law enforcement users from conducting their primary role: investigating crime. It is also very costly to acquire a suitably wide range of representative mobile devices and populate them with sufficiently variable examples of data in order to test a tool across a broad range of functionalities.

Given that many agencies across Europe use the same tools, it would be extremely cost-effective to avoid individual testing and process duplication within each agency, and instead centralise this testing function. It is highly **recommended that the European Union considers establishing an independent test body that can be tasked with conducting such independent testing on their behalf.** The cost savings alone in terms of the time saved would surely make this a worthwhile investment.[20]

20 "Requirements and Guidelines for a complete end-to-end mobile forensic investigation chain" CEN-CENELEC Ref. No.:CWA 17865:2022

4. Lack of cooperation with manufacturers

Manufacturers, many of whom operate outside the EU, are often reluctant to provide LEAs with information on data extraction. Remaining up to date with data extraction techniques can also be problematic due to:

- new devices being frequently introduced on the market;
- devices being subject to regular software updates;
- devices quickly becoming obsolete or upgraded;
- some devices being more popular in the EU compared with the U.S. and therefore not being prioritised by the industry;
- the majority of new devices having advanced security measures enabled by default.

Reliance on device-specific vulnerabilities for forensic acquisition is increasingly unsustainable due to their inconsistent reliability and lack of guaranteed success. Furthermore, the introduction of such vulnerabilities into devices poses significant security risks, as they may be exploited by malicious actors. While proprietary tools can facilitate access, their high cost and exclusive nature limit scalability and practical applicability in law enforcement operations.

One possible approach to addressing data access challenges could involve manufacturers retaining a key (or a partial key) to unlock their devices, but strictly under legally justified circumstances.

Creating a 'best practices' guide base on market leading IoT devices has been identified as a priority. This guide would include:

- the device specifications;
- forensic examination guidelines;
- details of the suite of tools that is needed for data extraction.

The guide should include the above while respecting the confidentiality of intellectual property, including patents, trade secrets and software copyrights of companies.

5. Shared platforms and tools as a service

Although not directly accessible by the Member States, the Europol Decryption Platform is available as a service for the most challenging cases. It adequately complements existing capacities at national levels. Other aspects of digital forensics, such as data analysis, could also be provided through direct access to a shared and common platform. Hansken[21], the open digital-forensics-as-a-service platform developed by the Netherlands Forensics Institute (NFI) could serve as a model to develop such services at EU level. The European Darkweb criminal Activity Monitoring and Analysis platform (EU DAMA), developed by the JRC and offered free of charge to LEAs in Member States, is another example of a solution that could serve such approach.

Agentic AI programming solutions, customised to the requirements of law enforcement, could be developed by creating a dedicated platform that provides direct access to a community of law enforcement developers. This community would collectively contribute to `dedicated platform, for instance, creating thematic skills libraries and in turn, enhance AI agentic programming solutions. In addition, some Member States with specific digital forensic capabilities could offer these as a service, ensuring more sustainable maintenance and development.

21 https://www.hansken.nl/

6. Virtual currencies

For cryptocurrency tracing and analysis, Member States primarily rely on well-known tools. The market is widely dominated by American companies, which poses a **sovereignty problem**: sensitive data is shared with American companies. Only a few agencies have deployed on-premise versions of these well-known tools.

Price is a significant issue: annual licences for these tools are expected to drastically increase in the coming years, obliging several Member States to discontinue their use. Europol provides services to national authorities, but it would be impossible for the Agency to replace national subscriptions entirely. The same applies on a national level, where central or federal cybercrime units provide services to local units.

For some investigations involving cryptocurrencies, it is necessary to analyse transactions in blockchain systems. Such analysis requires access to historical data, which is currently available on just one commercial company. This creates a de facto dependency on that company, which has licensing fees, therefore forcing LEAs to prioritise investigations to avoid budgetary issues.

Lack of interoperability poses obstacles to investigations: outputs of existing commercial tools are proprietary and cannot be imported in, or used in conjunction with, other tools.

Practitioners are used to overreliance on commercial tools and are not always able to correctly interpret the obtained results. This is already leading to cases being dismissed by courts due to an absence of reliable evidence. Two cases arose in France in recent months. There is a need to **build expertise** beyond the use of commercial tools in order to ensure the correct interpretation of the analysis. For this reason, Europol has built a new capacity building approach: The [Block]Chain of Evidence (BoE). It was piloted in the Europol HQ, in partnership with EUROJUST, during the summer of 2026.

7. Vehicle forensics

Across Europe, end-users report the following common gaps:

- **difficulties in data acquisition and analysis** due to the use of proprietary data formats and a lack of standardisation between vehicle manufacturers;
- increasing use of **encryption, secure systems** and **cloud-based** storage, which limits direct access to relevant data;
- insufficient **availability and effectivity of forensic tools**, often limited to non-European vehicles, leading to a reliance on manual processes;
- limited **cooperation with manufacturers**, which restricts access to telematics, backend data and system logs;
- **legal and regulatory gaps**, including a lack of harmonised European frameworks and restrictions on certain investigative techniques.

In terms of priorities, end-users particularly emphasise:

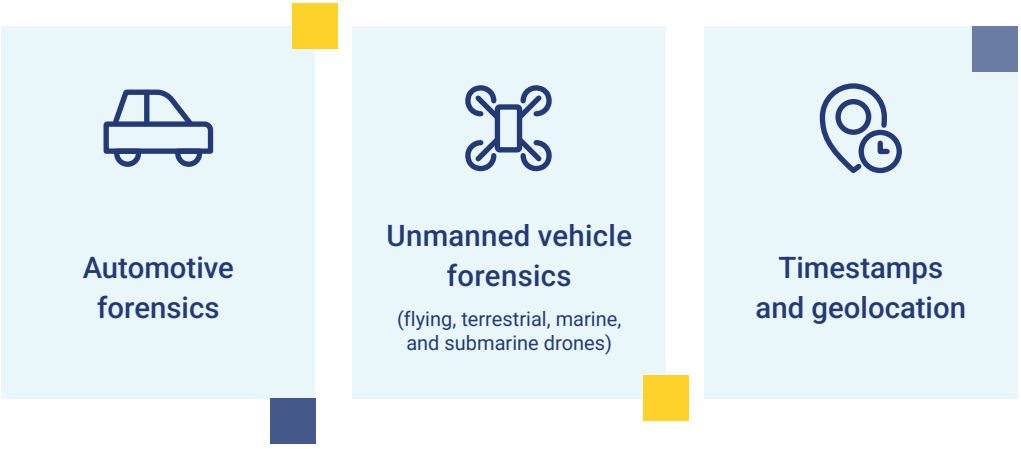
- The creation of a centralised European vehicle system database
- development of automated and user-friendly tools for data acquisition, extraction and analysis
- improved capabilities to access live, encrypted and remote, cloud-based data
- strengthening cooperation with manufacturers
- investment in specialised training and dedicated forensic units

The **European Vehicle Forensics Framework (EVFF)** is a collaborative initiative aimed at enhancing the forensic capabilities of law enforcement and judicial authorities in Europe. It is a modular software framework that facilitates the analysis of data from vehicle infotainment system images. It focuses on the examination, preservation and analysis of digital evidence from modern vehicles to support criminal investigations. The modular architecture of the EVFF enables project contributors to develop and integrate their modules. The framework consists of three modules: mounters, extractors, and reporters. However, EVFF does not support acquisition. To ensure comprehensive forensic workflows, the framework should be complemented by other solutions for data acquisition.

The EVFF is developed by European law enforcement experts working together under the aegis of the Commission Joint Research Centre and Europol. The tool is freely available to Member States and Schengen Associated Countries LEAs on the Europol Tools Repository (ETR).

The European Cybercrime Training and Education Group (ECTEG) is developing a dedicated training course on vehicular forensics[22]. The course, which should be available at the beginning of 2027, addresses the challenges of recovering digital evidence or data stored in a vehicle's modules, networks, and messages sent across operating systems. It focuses on two types of vehicles: manned vehicles (such as a car, with people inside it operating its controls) and unmanned vehicles (such as a drone that can be controlled remotely, operating without a person onboard). Both types of vehicles are used to commit crimes, leaving digital traces that can be of paramount importance to investigators.

To assist LEAs in their investigations, ECTEG and its experts are creating a set of course modules covering:



The modules include theoretical and practical training, such as securing and preserving a vehicle at a crime scene, acquiring data, and awareness of vehicle data sources and networks, all while ensuring practitioners' security.

22 https://www.ecteg.eu/projects/vehicular-forensics/

8. Internet of Things (IoT)

Compared to the mobile telecommunication device market, the market for IoT devices is characterised by a much greater number of different products, with no operating system standardisation.

Looking at home automation tools as an example, there are many different communication protocols between IoT devices and third-party devices sold to create a single point of control for a house. Additionally, most home automation solutions only offer cloud storage for a limited period. Home security cameras, for instance, store recorded events on the solution provider's servers, usually located in another country, making the acquisition of such evidence more complex, potentially delayed, or even impossible.

For each domain, new initiatives and software/hardware solutions are developed, creating new financial and educational challenges for specialised law enforcement units.

Currently, there are no specialised tools, techniques or best practices for the analysis of data collected from IoT devices. Each IoT device normally needs to be investigated using a number of different techniques and tools, which do not typically provide all the required functions. Bespoke data analysis tools are often developed in house for each of the different operating systems, which requires a significant number of resources. Therefore, different tools are often needed to extract data.

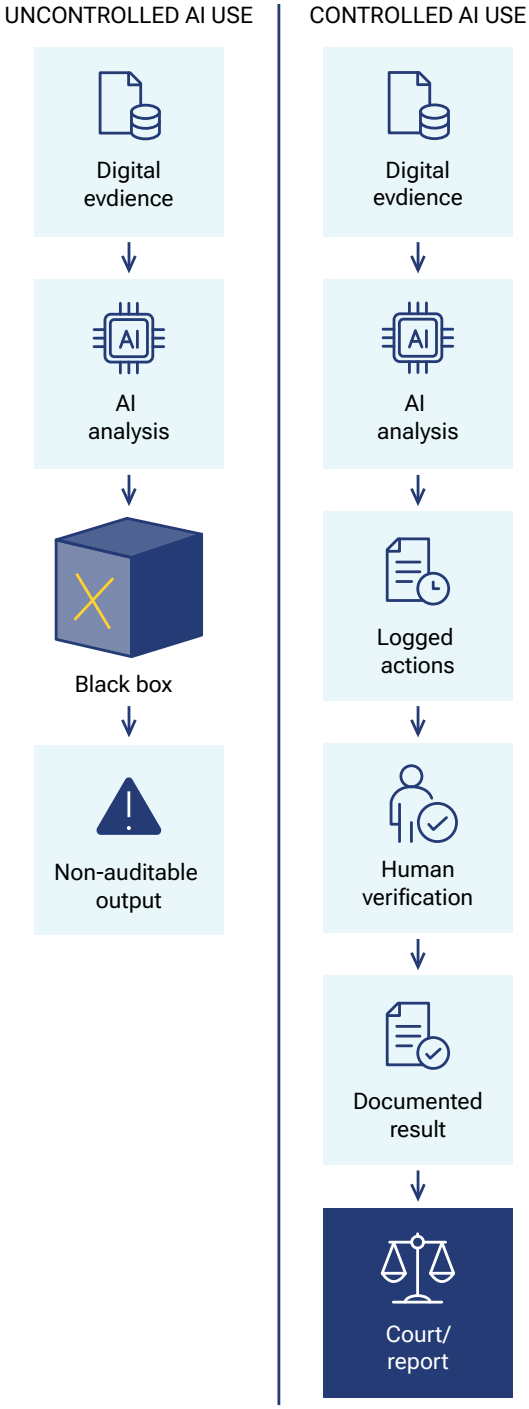
Functions should include (but not be limited to) acquisition, federation, review/analysis, targeted extraction, translation, and token expiration. Data visualisation tools integrating the capability to visually correlate data between different IoT devices would be extremely useful for investigations. If the digital evidence is presented in an easily understandable way, it could prove useful during subsequent prosecutions. Encryption issues related to the acquisition of data in the cloud[23] and lack of expertise[24] were also indicated as relevant challenges in this area.

23 See section 3 "Standardisation"

24 See section 8 "Training"

9. Use of artificial intelligence (AI) in forensics

To ensure the integrity and reliability of digital forensic examinations, it is crucial to establish a controlled platform for AI-driven forensics. Without structured oversight, there is a significant risk of uncontrolled, ad-hoc AI systems being deployed, which could compromise the chain of custody, and the reproducibility and admissibility of evidence. AI must be used transparently, with full traceability, documentation, and manual verification where necessary, to maintain trust in investigative outcomes and compliance with legal frameworks.



Following there is a list of considerations to address when introducing AI in digital forensics examinations:

- While traditional forensics is based on the chain of custody and repeatability, AI is based on probability and context. Therefore, the structured logging of every action performed by AI is necessary.
- Artificial Intelligence is highly effective in generating investigative leads. However, any analysis should remain repeatable and, where necessary, manually verified.
- AI-driven processes should be traceable and documented to ensure reproducibility in court. If a file is analysed, it should remain unaltered by AI. If modifications are unavoidable, they must be documented and ideally be reversible.
- AI cannot be used in black box fashion (based solely on inputs and outputs without knowledge of its process), because it often generates a non-auditable answer/output, even if it is statistically accurate. For example, a 99 % accurate AI response is still not usable if the reasoning and steps behind it cannot be demonstrated.
- AI may produce varying outputs due to differences in training models. However, this is not an issue if an analyst can manually reproduce the AI's steps.
- Anti-forensic techniques, used by threat actors, can confuse AI and lead to incorrect outputs. Ad-hoc modifications of input data directly affects the output.
- The usage of AI must comply with the AI Act[25], GDPR[26], ISO/IEC standards, and the NIST AI RMF framework[27].

25 Regulation - EU - 2024/1689 - EN - EUR-Lex, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

26 Regulation - 2016/679 - EN - gdpr - EUR-Lex, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

27 NIST AI Risk Management Framework (AI RMF), https://www.nist.gov/itl/ai-risk-management-framework

10. Training

Training resources should be developed by multidisciplinary communities, comprising law enforcement officials and academics. The development of training materials should involve both digital forensics experts and tactical investigators, to ensure that training enables a valuable connection between the different actors of the investigative chain. Training should aim at developing knowledge and expertise of investigators, independently of the technical solutions used, therefore it should be **tools agnostic**. At the same time, training courses should include relevant references to available tools that are not well known by practitioners, and free of charge to EU LEAs.

Training courses should be targeted and tailored to different audiences such as first responders, experts, trainers, prosecutors, and the judiciary.

First responders (possible online or self-paced): front-line officers can sometimes underestimate the importance of data that can be collected from IoT devices and often do not have the relevant knowledge on what to seize and submit for further analysis.

Experts (face-to-face): it is important to have table-top exercises integrated into this type of training, utilising different levels of expertise such as local or central units. Exchange programmes for experts could also be of benefit, to increase knowledge sharing and interoperability.

Trainers: at EU level, it is necessary to support a train-the-trainers approach, so that the competencies can then be disseminated domestically. Moreover, knowledge sharing spaces and exchange programmes are important to supplement and complement training activities.

Prosecutors and the judiciary, so they can effectively understand, evaluate and present digital evidence in court.

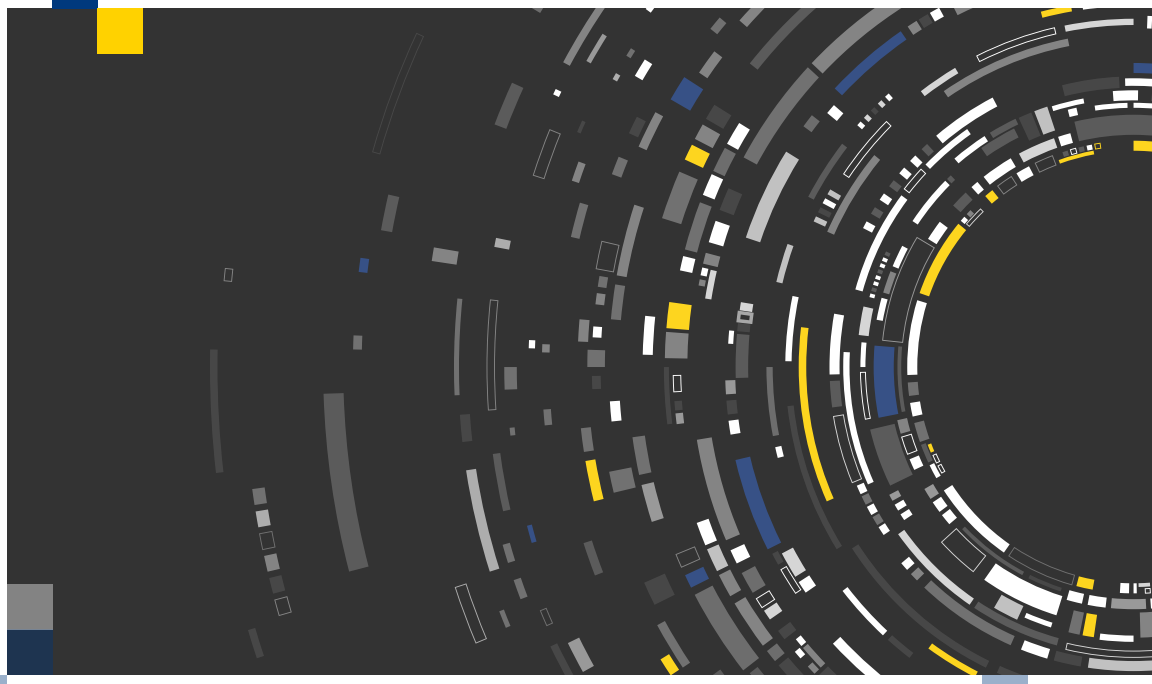
Training should be designed as a cohesive, multi-tiered framework, ensuring that courses for different audiences are complementary and progressively build upon one another. In this context, CEPOL is establishing an Expertise Development Training Modality (EDTM) focused on lawful decryption; a two-year pilot programme aimed at strengthening decryption expertise and training capacity across Member States. The EDTM will deliver a structured curriculum comprising online webinars, basic and advanced training modules, as well as train-the-trainers courses to empower national trainers. Additionally, the programme will facilitate dedicated exchange programmes,

enabling practitioners to refine their skills through peer learning and collaborative engagement.

Development and delivery of training should be continuous and should keep pace with technological innovation. For instance, IoT device types receive regular software updates and are constantly upgraded. New IoT devices are regularly being introduced on the market and there is no standardisation of data formats. It is therefore very difficult for LEAs to keep up to date with the new technologies, and this presents a number of challenges.

In addition to - or through integration with - training, data visualisation libraries, a practical field guide for practitioners (SOP) and a priority list of IoT devices of interest could assist with the effective collection of relevant data at the crime scene.

Lack of standardised procedures and recognition of digital forensics expertise across EU Member States hinders cooperation and investigations[28]. Processes or guidelines should be developed and adopted to capture competencies and skills. **Documentation** of training (certificates, expiry dates) is mandatory. **On-the-job training** must be recorded, noting authorisation and validity periods.



28 European Parliament, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI%282025%29775879

Conclusions

This gap analysis underscores the urgent need for a coordinated, EU-wide strategy to strengthen digital forensic capabilities across EU Member States. While significant progress has been made in certain areas, systemic challenges persist – ranging from tool fragmentation and lack of interoperability, to resource constraints and evolving criminal methodologies. The following conclusions and strategic priorities are critical to addressing the identified challenges, and to ensuring law enforcement remains equipped to combat crime effectively:

Standardisation and interoperability

Data formats: The lack of standardised data formats and interoperable tools remains a significant bottleneck, leading to inefficiencies, duplicated efforts, and reduced cross-border cooperation. Proprietary formats used by commercial tools hinder seamless integration and analysis pipelines, wasting valuable investigative time.

Chain of custody and evidence integrity: Current processes are often manual, error-prone and ill-suited for complex digital forensic examinations, for example cloud forensics and IoT. Standardised frameworks are necessary to ensure evidence integrity and admissibility in court.

AI in Digital Forensics

AI as Tool: AI offers transformative potential for investigative leads, automation, and data analysis, but its use must be traceable, reproducible, and compliant with legal frameworks (AI Act, GDPR, ISO/IEC Standards).

Addressing critical gaps in tools, expertise and cooperation

Tool Development: EU-developed tools, such as those developed under the Tools4LEAs and FREETOOL projects, are underutilised despite being cost-effective and aligned with EU Standards. Commercial tools dominate the field of digital forensics, often at high cost and with limited interoperability.

Testing and Validation: The absence of a centralised EU testing body leads to duplicated efforts, wasted resources, inconsistent validation, and delayed deployment of tools.

Expertise and training

Skills shortage: Law enforcement agencies struggle to keep pace with technological advancements (e.g. encryption, virtual currencies, IoT), leading to a reliance on both commercial tools, and gaps in the manual interpretation of results.

Standardised competencies: Fragmented training programmes and lack of a common European certification undermines the effectiveness and credibility of digital forensic examiners.

First responders: Front line officers and legal professionals often lack awareness on the potential of digital evidence or how to handle it (e.g. vehicles, cloud data).

Cooperation with manufactures and cross-border collaboration

Manufacturer engagement: the reluctance of manufacturers to provide data extraction methods or forensic interfaces exacerbates access challenges.

Funding and Governance

Targeted investment: digital forensics require sustained funding and a prioritisation mechanism for tool development, training and infrastructure.

Conclusion

The digital forensic landscape in EU Member States is at a crossroads. Without coordinated, strategic action, the gaps in standardisation, tool development, AI governance, and training will widen, leaving law enforcement agencies ill-equipped to tackle evolving digital threats. By prioritising standardisation, EU-made solutions, AI transparency, and shared platforms, the EU can build a resilient, unified forensic ecosystem that ensures investigative integrity, legal compliance and technological sovereignty.

Headquartered in The Hague, the Netherlands, Europol supports the 27 EU Member States in their fight against terrorism, cybercrime and other serious and organised forms of crime. We also work with many non-EU partner states and international organisations. From its various threat assessments to its intelligence-gathering and operational activities, Europol has the tools and resources it needs to do its part in making Europe safer.

DIGITAL FORENSICS: GAP ANALYSIS

PDF | ISBN 978-92-9414-156-9 | DOI: 10.2813/7161293 | QL-01-26-023-EN-N

Neither the European Union Agency for Law Enforcement Cooperation nor any person acting on behalf of the agency is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2026

© European Union Agency for Law Enforcement Cooperation, 2026

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the copyright of the European Union Agency for Law Enforcement Cooperation, permission must be sought directly from the copyright holders.

While best efforts have been made to trace and acknowledge all copyright holders, Europol would like to apologise should there have been any errors or omissions. Please do contact us if you possess any further information relating to the images published or their rights holder.

Cite this publication: Europol, Digital forensics: gap analysis, Publications Office of the European Union, Luxembourg, 2026.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu