

**CEN**

**CWA 17865**

**WORKSHOP**

March 2022

**AGREEMENT**

---

ICS 07.140

English version

## Requirements and Guidelines for a complete end-to-end mobile forensic investigation chain

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION  
COMITÉ EUROPÉEN DE NORMALISATION  
EUROPÄISCHES KOMITEE FÜR NORMUNG

**CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels**

---

© 2022 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No.:CWA 17865:2022 E

<b>Contents</b>	<b>Page</b>
European foreword.....	5
Introduction .....	7
1 Scope.....	9
2 Normative references.....	9
3 Terms and definitions .....	10
4 Abbreviations .....	12
5 Personnel .....	13
5.1 Competence.....	13
5.2 Impartiality .....	14
5.3 Procedural .....	14
6 Tools.....	14
6.1 Background information .....	14
6.2 Overarching Principles related to the selection and use of Mobile Forensic Tools.....	15
6.3 Tool Fundamentals.....	15
6.4 Methodology .....	16
6.5 Tool Selection .....	17
6.6 Features .....	17
6.6.1 Accessing Data.....	17
6.6.2 Decoding Data.....	18
6.6.3 Data Integrity.....	19
6.6.4 User Knowledge.....	19
6.7 Tool Interoperability .....	19
6.8 Forensic Tool Log .....	20
6.9 Secure Evidential Storage .....	20
6.10 Validation and Verification of Tools.....	21
6.11 Tool Release Notes.....	21
6.12 Risk Register .....	22
6.13 Recommendation for an EU Forensic Testing Body.....	22
7 Processes.....	23
7.1 Background information .....	23
7.2 General requirements .....	23
7.2.1 Impartiality .....	23
7.2.2 Confidentiality.....	23
7.2.3 Auditability.....	24
7.2.4 Repeatability.....	24
7.2.5 Reproducibility .....	24
7.2.6 Justifiability.....	24
7.2.7 Chain of custody.....	25
7.3 Preliminaries.....	25
7.4 First response.....	26
7.5 Recording.....	26
7.6 Labelling.....	26
7.7 Packaging.....	26
7.8 Item transport and storage.....	27

7.9	Lab Work.....	27
7.9.1	Initial inspection phase / device identification.....	27
7.9.2	Instruction and authorisation.....	27
7.9.3	Tool Selection.....	27
7.9.4	Acquisition.....	27
7.9.5	Decoding / Decryption.....	28
7.10	Analysis.....	28
7.10.1	Analytical models.....	28
7.10.2	Live analysis.....	29
7.10.3	Selection of analysis methods.....	29
7.11	Verification and Validation.....	29
7.11.1	Verification of methods.....	29
7.11.2	Validation of methods.....	29
7.11.3	Peer Reviews.....	29
7.12	Reporting of results.....	30
7.12.1	Written reports.....	30
7.12.2	Oral reports at court.....	30
7.13	Exchange of data and archiving.....	31
8	Legal and Ethical Framework.....	31
8.1	General Overview.....	31
8.2	Governance of the evidentiary proceedings.....	36
8.3	Pre-Trial Criminal Proceedings Considerations.....	38
8.3.1	Appropriate logging and protocoling.....	38
8.3.2	Criteria to be met when accessing messages, cloud and sensitive documents.....	38
8.3.3	Importance of the different roles in the criminal procedure – suspect, witness, victim.....	38
8.3.4	Scrutinizing tools and review tools and documenting what tools were used.....	39
8.3.5	Clear audit trails.....	39
8.3.6	Using accessible language to all parties involved in the criminal procedure.....	40
8.3.7	Fair trial implications.....	40
8.3.8	Judicial overview of the process.....	40
8.4	Trial Phase Criminal Proceedings Considerations.....	40
8.5	Prevention of mobile forensics dual-use, misuse, and abuse.....	41
	Annex A (informative) A Good Practice Guide for Mobile Forensic Tool Selection.....	44
A.1	Permissibility.....	44
A.2	Proportionality.....	44
A.3	Validity.....	44
A.4	Security.....	44
A.5	Processes.....	44
A.6	Ethics.....	45
	Annex B (informative) Mobile Forensic Tool – Checklist for Selection.....	46
	Annex C (informative) Mobile Forensic Tool – Risk Register.....	48
	Annex D (informative) Six Steps to Successful to Mobile Validation.....	49
D.1	Step 1: Determine all possible extraction methods for the search authority.....	49
D.2	Step 2: Process the data in more than one tool.....	51

D.3	Step 3: Deep dive forensics: Where the push button stops and forensic examinations begin .....	52
D.4	Step 4: Validation (Types: Visual, cross-tool, call detail records, CCTV, carving, replication).....	52
D.5	Step 5: Reporting/Sharing your findings.....	53
D.6	Step 6: Education.....	54
	Annex E (informative) Forensic Information Report Template.....	55
E.1	General.....	55
E.2	Forensic Information Report.....	55
7.3	Analysis Interpretation.....	62
7.4	Review and Validation.....	62
	Annex F (informative) Governance implications of the use of Artificial Intelligence in mobile forensics .....	64
	Bibliography.....	65

## European foreword

This CEN Workshop Agreement (CWA 17865:2022) has been developed in accordance with the CEN-CENELEC Guide 29 “CEN/CENELEC Workshop Agreements – A rapid way to standardization” and with the relevant provisions of CEN/CENELEC Internal Regulations - Part 2. It was approved by a Workshop of representatives of interested parties on 2022-02-22, the constitution of which was supported by CEN following the public call for participation made on 2021-01-28. However, this CEN Workshop Agreement does not necessarily include all relevant stakeholders.

The final text of this CEN Workshop Agreement was provided to CEN for publication on 2022-03-01.

Results incorporated in this CWA received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 832800 (project FORMOBILE).

The following organizations and individuals developed and approved this CEN Workshop Agreement:

1. Agentur für Innovation in der Cybersicherheit (Germany)
2. APWG European Union Foundation (Spain)
3. Athena Research Centre (Greece)
4. CCL-Forensics Ltd (UK)
5. Cellebrite (Israel)
6. Central Office for Information Technology in the Security Sector (Germany)
7. COMISARIA GENERAL DE POLICÍA CIENTÍFICA - DIRECCIÓN GENERAL DE LA POLICÍA (Spain)
8. DigiFors GmbH (Germany)
9. Dr. Malvika Mehta (consultant)
10. East Midlands Special Operations Unit (UK)
11. Europol
12. Foundation for Research and Technology - Hellas (Greece)
13. Home Office (UK)
14. International Justice Analysis Forum (Germany)
15. Kriminalistika OÜ (Estonia)
16. Law and Internet Foundation (Bulgaria)
17. Magnet Forensics (Canada)
18. Malta Police Force (Malta)
19. Mittweida University of Applied Sciences (Germany)

20. MSAB (Sweden)
21. Netherlands Forensic Institute (The Netherlands)
22. Norwegian Police University College (Norway)
23. Polish Platform of Homeland Security (Poland)
24. Stadtpolizei Zürich (Switzerland)
25. StAG srl (Italy)
26. Timelex (Belgium)
27. University of Adelaide, School of Electrical and Electronic Engineering (Australia)
28. University of Lausanne, Ecole des Sciences Criminelles (Switzerland)
29. University of South Wales, Faculty of Computing, Engineering and Science (UK)
30. University of Zagreb, Faculty of Transport and Traffic Sciences, Department for Information and Communication Traffic (Croatia)

Attention is drawn to the possibility that some elements of this document may be subject to patent rights. CENCENELEC policy on patent rights is described in CEN-CENELEC Guide 8 “Guidelines for Implementation of the Common IPR Policy on Patent”. CEN shall not be held responsible for identifying any or all such patent rights.

Although the Workshop parties have made every effort to ensure the reliability and accuracy of technical and nontechnical descriptions, the Workshop is not able to guarantee, explicitly or implicitly, the correctness of this document. Anyone who applies this CEN Workshop Agreement shall be aware that neither the Workshop, nor CEN, can be held liable for damages or losses of any kind whatsoever. The use of this CEN Workshop Agreement does not relieve users of their responsibility for their own actions, and they apply this document at their own risk. The CEN Workshop Agreement should not be construed as legal advice authoritatively endorsed by CEN/CENELEC.

This CWA has been proposed by the FORMOBILE European Project (funding from the European Commission’s Horizon 2020 – The Framework Programme for Research and Innovation (2014 - 2020) under Grant Agreement No 832800).

## Introduction

Mobile devices, especially smartphones represent a unique challenge for law enforcement. Due to their wide use, they underpin many criminal investigations. For instance, one may find critical evidence in a smartphone of a victim who is in no position to unlock the device. Moreover, criminal offenders, organised crime and terrorist organisations use mobile devices for various purposes, which introduces many challenges for criminal prosecution. Determining how the data got onto the mobile device is not always simple as these devices often sync and share data with other digital media and cloud services. Law enforcement need not only to access the data stored on mobile devices, but also provide it as court evidence in a trustworthy and reliable manner.

The overarching objective of Horizon 2020 project FORMOBILE is to establish a complete end-to-end forensic investigation chain that targets mobile devices and includes an appropriate standard. Adherence to the standards during all steps of investigation in this field is of critical importance for the evidence being regarded as reliable and acceptable to the court. Development of such a standard is of the utmost importance to secure the successful outcome of an investigation. Despite the relatively large number of standards and non-formal standardisation documents, relevant for IT security and digital investigation, there is a lack of specific standards for mobile forensics in general and especially in the areas, relevant for the FORMOBILE project.

Several European and international standardisation bodies work on the standardisation in the area of digital forensics, including ISO and IEC<sup>1)</sup>, NIST, ETSI and ASTM. The standards, developed by these organisations do not explicitly address the topic of mobile forensics in digital investigations. This standard is aimed to complement existing standards from these organisations. Currently, they are only partly relevant for the FORMOBILE Project and do not provide a holistic approach to the processes of mobile forensics. A significant amount of the reference documents, used as standards in mobile forensics, are best practices and guidelines.

There are current policies and initiatives at national, European as well as international level to introduce consistent and generally accepted standards for mobile forensics within the forensic community. This may benefit all users of the criminal justice system including members of the public as well as legal and forensic practitioners. This CWA can be immediately applied by Law Enforcement Agencies (LEAs) and serve as a forerunner for a new European Standard in mobile forensics.

Several European initiatives and regulations, relevant for the area of digital investigations, includes the Council of Europe's Convention on Cybercrime (The Council of Europe, 2001), Directive of the European Parliament and of the Council regarding the European Investigation Order (Council, 2014), INTERPOL Global guidelines for digital forensics laboratories (INTERPOL, 2019).

In Europe, there is no unified legal framework for the processes of acquisition, collection, processing, storage or exchange of digital data, which may result in evidence acceptable to the courts of law in different countries. Within these countries, the processes usually conform to national law and regulations, but those regulations and laws may not be consistent or enable transfer for evidential purposes between countries. Despite mutual recognition, implemented across various countries, a lot of issues remain open that allow judges to determine the admissibility of electronic data as evidence.

There is a growing need for LEAs and other organisations dealing with mobile forensics to have a consistent European standard which ensures that evidence presented for the court are regarded as reliable. This is extremely important for unification of the investigative process across law enforcement

---

<sup>1)</sup> This includes ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, incl. ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence; ISO/IEC JTC 1/SC 37 Biometrics; ISO/IEC JTC 1/SC 40 IT Service Management and IT Governance.

in different countries and for a successful outcome of the investigation. LEAs, national and international forensic laboratories of different levels, organisations working in the area of mobile forensics as well as independent experts are among the beneficiaries of this CEN Workshop.

As such, the primary purpose of this document is to provide recommendations for a complete forensic investigation chain targeting mobile devices that covers good practices for the mobile phone forensic chain, tools for the acquisition, recovery, analysis and visualisation of data, as well as the necessary training required to effectively use the new tools and successfully follow the good practices. These broad topics are covered in the following clauses addressing the three areas of critical importance: Personnel (Clause 5), Tools (Clause 6) and Processes (Clause 7).

This CWA seeks to document good practice guidance for the correct and necessary processes, competencies and methods required to ensure the admissibility of the evidence. It provides a set of guidelines that fit within the wider context of digital forensic investigations for law enforcement in general at the level of specificity, necessary to keep these guidelines meaningful, whilst simultaneously avoiding such detail that make them quickly obsolete.

The guidance in this document is designed to specifically address the specialism of mobile forensics. It is intended to be complementary to existing related standards within the digital forensics sphere. It is not intended to replace or override existing guidance or good practice specific to other digital forensics areas.



## 1 Scope

This CEN Workshop Agreement (CWA) focuses on the Personnel, Tools, Processes and Legal and Ethical framework specific for mobile forensics and including the following topics:

- a) Competencies;
- b) device seizure;
- c) data preservation;
- d) data acquisition;
- e) data examination and analysis;
- f) documentation of all investigation steps;
- g) reporting;
- h) evaluation and sharing of information with other LEAs; and
- i) legal and ethical considerations.

In addition to the process-related issues, the document covers requirements for new curriculum for training of LEA officers, security practitioners and criminal prosecution experts to ensure that the evidence from mobile devices is court-approved across national borders.

It is recognised that national laws and good practices applied at LEAs vary not only between different European countries but also within these countries. This CWA offers a collection of building blocks covering different aspects of mobile forensics allowing for adjustments based on national laws and regulations as well as internal rules and codes of conduct. It allows LEAs from different countries to accommodate their available technical solutions, at the same time offering a standardised collection of procedures and requirements.

It should be explicitly stated that it is not possible to cover all the possible related topics for mobile forensics. Detailed subject matters and specialisms such as Cloud Forensics, Cell Site Analysis, Interception of Communications are excluded. Similarly, the rules and regulations about chain of custody in general, plus guidance for transmission of evidence across national boundaries are excluded from this standards document.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 21043-2:2018, *Forensic sciences — Part 2: Recognition, recording, collecting, transport and storage of items*

ISO/IEC 17025:2017, *General requirements for the competence of testing and calibration laboratories*

ISO/IEC 27037:2012, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

ISO/IEC 27041:2015, *Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method*

ISO/IEC 27042:2015, *Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*

ISO/IEC 27043:2015, *Information technology — Security techniques — Incident investigation principles and processes*

ISO/IEC 27050 (all parts), *Information technology — Security techniques — Electronic discovery*

ASTM E2916-19 — *Standard Terminology for Digital and Multimedia Evidence Examination*

### **3 Terms and definitions**

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

#### **3.1 chain of custody**

responsibility for or control of materials and associated data as they move through each step of a process

Note 1 to entry: In NIST SP 800-72 chain of custody is defined as process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

[SOURCE: ISO 20387:2018, 3.12, modified with Note to entry added]

#### **3.2 chain of evidence**

process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence

Note 1 to entry: The “sequencing” of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner. Rationale: Sufficiently covered under chain of custody.

Note 2 to entry: This definition is derived from CNSSI 4009 Committee on National Security Systems (CNSS) Glossary.

Note 3 to entry: This definition also relates to potential evidence, not yet accepted as evidence by court.

#### **3.3 conflict of interests**

conflict of interest arises when a person involved in the investigation has a private interest that may affect the impartial and objective performance of his or her powers or duties

#### **3.4 digital forensics**

use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal