CEN

WORKSHOP

AGREEMENT

CWA 17865

March 2022

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

Ref. No.:CWA 17865:2022 E

Contents

Page

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[1)], 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

---

1) 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, *I*nformation 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

Note 1 to entry: In ISO/IEC 30121:2015, 3.3 digital forensics is defined as scientific tasks, techniques, and practices used in the investigation of stored or transmitted binary information or data for legal purposes.

3.5
strategy
<digital forensics> documented objectives defined for the process of proportional examination of digital evidence, in order to support investigations and prosecutions

Note 1 to entry: The strategy helps guide investigators as to the best approach in accordance with current digital forensic science, to support evidential integrity across the criminal justice system, from crime scene to courtroom.

3.6
competence
<mobile forensics> ability, knowledge or skills of people to perform successful, accurate and reliable mobile forensics, as defined by either the organization, policy, standard or accreditation scheme

Note 1 to entry: These requirements should be documented.

3.7
process
set of interrelated or interacting activities that use inputs to deliver an intended result

[SOURCE: ISO 9000:2015, 3.4.1]

3.8
procedure
specified way to carry out an activity or a process

[SOURCE: ISO 9000:2015, 3.4.5]

3.9
file system
<computer forensics> specified method for naming, storing, organizing and accessing files on logical volumes

[SOURCE: ASTM E2916-19e1]

3.10
hash sum
string of alphanumerical values used to substantiate the integrity of digital evidence or for inclusion/exclusion comparisons against known value sets or both

[SOURCE: ASTM E2916-19e1]

3.11
jailbreaking (iOS)/rooting (Android)
activity, which describes modification of an electronic device to remove restrictions imposed by the manufacturer or operator, that can provide access to more data during forensic examinations

3.12
mobile device
any handheld computer device that will have a display screen, providing a touchscreen interface with digital buttons and keyboard or physical buttons along with a physical keyboard

Note 1 to entry: Many such devices can connect to the Internet and interconnect with other devices via Wi-Fi, Bluetooth, cellular networks or near field communication (NFC). Typical devices could be a smartphone, a tablet or wearables.

3.13
mobile device forensics
mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions

[SOURCE: ASTM E2916-19e1]

3.14
forensic acquisition
forensic image is a copy of the electronic data on a device created to generate a trusted copy of the original device data, for examination by a court of law

Note 1 to entry: There are different methods to create forensic images depending on the technology involved.

3.15
physical acquisition
data extracted directly from the device storage area

3.16
logical acquisition
accurate reproduction of information contained within a logical volume (for example, mounted volume, logical drive assignment etc.)

[SOURCE: ASTM E2916-19e1]

3.17
File System acquisition
targeted active files and folders from the file system which may contain remnants of deleted data and non-user data

[SOURCE: CFRS762-Mobile Device Forensics, George Mason University]

3.18
carve
<computer forensics> to extract a portion of data for the purpose of analysis

[SOURCE: ASTM E2916-19e1]

3.19
parsing
process of converting raw data into formatted data structure

Note 1 to entry: A data structure type can be any suitable representation of the information contained in the raw data.

4 Abbreviations

AFU - After First Unlock – term used to describe the state of a modern smartphone wherein the mobile device has been powered on and unlocked at least once but is locked at time of examination.

ASTM - American Society for Testing and Materials.

BFU - Before First Unlock – term used to describe the state of a modern smartphone wherein the mobile device has been powered on, but not yet unlocked at time of examination.

CASE - Cyber-investigation Analysis Standard Expression; a community-developed evolving standard that provides a structured (ontology-based) specification for representing information commonly analysed and exchanged by people and systems during investigations involving digital evidence.

ETSI - European Telecommunications Standards Institute.

EU – European Union

FFS - Full File System

IEC - The International Electrotechnical Commission.

INTERPOL - "The International Criminal Police Organisation – INTERPOL", which is abbreviated to "ICPO–INTERPOL".

ISO - The International Organisation for Standardisation.

JTC - Joint Technical Committee.

LED – Law Enforcement Directive

NIST - National Institute of Standards and Technology. A US government department within the US Department of Commerce who specialises in digital forensic testing of tools.

SC - subcommittee

5 Personnel

5.1 Competence

5.1.1 Personnel shall be competent and duly certified to use the tools and techniques used in their investigations[2]. See 5.3.2.

5.1.2 Requirements for competence should be documented[3]. Reference to already established lists of competences. Requirements for competence should reflect the role of the practitioner.

5.1.3 Training activity should be documented. Records (certificates of attendance, accreditations, etc.) of personnel should be retained.

5.1.4 On the job training[4] should be documented, including what is trained on, when and trained by and authorisation after training is passed, also document the expiry (date) of training. The relevance of the training should be periodically reviewed to determine its validity and suitability.

5.1.5 Personnel should have generic Mobile Device Digital Forensic (tool agnostic) training (basic training should deal with crime-scene[5], chain of custody/evidence topics, basics about types of acquisition, analysis, reporting and court appearance). Technique and tool-oriented training should extend the basic trainings (see also Clause 6.6.4).

---

2) ISO/IEC 17025:2017, Clause 6.2.1

3) ISO/IEC 17025:2017, Clause 6.2.2

4) Like on the execution of internal procedures.

5) Like order of examination (DNA, Fingerprints, digital), bio/chemical hazards

5.1.6 Expiry date of competences should be documented. Some basics of digital forensics do not change very fast. However, the more specific a training is on hardware brands, Operating System specifics, Apps, the more volatile the knowledge is (due to the fast-moving technology in mobile phone devices).

5.2 Impartiality

5.2.1 At all times, agencies procedures on impartiality and avoidance of conflict of interest shall be followed.

5.2.2 If none exist:

a) Personnel should not work on cases where there is a (semblance of a) conflict of interest.

b) When (semblance of a) conflict of interest appears during investigation, work should be transferred to a co-worker or another laboratory[6)].

5.3 Procedural

5.3.1 Procedures and work instructions should be established, documented, shared and updated. Personnel shall work according to them and ensure their correct appliance.

5.3.2 Mobile forensic tools have a variety of capabilities to acquire data from mobile devices. See Clause 6.2, Principle 1 and Clause 7.4 for more details.

6 Tools

6.1 Background information

Mobile forensics is a fast-moving and rapidly evolving scientific area. The constant developments in device hardware, operating systems, apps, app versions and security protections, mean that what was good practice just a few years ago, may now be unsuitable for the latest devices.

For that reason, it is difficult to produce a set of standards with sufficient detail to be relevant, whilst simultaneously being flexible enough to remain valid for the long term. That makes the production of a fixed standard document for mobile forensics very challenging and unproductive.

This document describes good practice and guidance for the selection and use of mobile forensic tools within the wider guidance of this document for personnel and processes. This document is designed to be supplemented with local Standard Operating Procedures, Reference Guides and Work Instructions.

For a quick overview of points to consider when selecting a mobile forensic tool, see:

— Annex A: Good Practice for tool selection;

— Annex B: Checklist for selection;

— Annex C: Mobile Forensic Tool – Risk Register;

— Annex D: Six Steps to Successful to Mobile Validation.

6) See also Clause 7.2.1

6.2 Overarching Principles related to the selection and use of Mobile Forensic Tools

Principle 1: *All reasonable steps should be taken to minimise the risk of changing digitally stored data on a mobile device that could subsequently be relied upon as evidence in court.*

Mobile forensic tools have a variety of capabilities to acquire data from mobile devices. For example, some methods require the installation of agents onto a device; other processes require the jailbreaking or lower level-privileged access of handsets and on occasion, the only way to get the data may require disassembling the device at the chip level. It is essential that persons involved understand the risks of these methods to manage the risk of accidentally overwriting or destroying evidence. This is why training of personnel and the documentation of it are so important to fulfil the requirements.

Principle 2: *A record of all actions taken, and tools applied should be documented and preserved and be made available to the courts if used as evidence.*

It is recommended that data recovered by forensic tools should be corroborated wherever possible, if intended to be used in court. An independent third-party should be able to replicate the processes applied to reach the same results. Such a transparent process helps to validate and verify the evidence being presented in court. It is important that users make a record of their actions and the tools (including the version of the tools) used in an open and accessible audit log trail of what actions were taken to recover the data. Moreover, a log of actions can be produced for court. to provide a definite trail of the steps followed.

Principle 3: *Digital evidence should be securely stored and protected to avoid any risk of subsequent alteration. A forensically sound method should be used to preserve and protect the chain of custody.*

Like all evidence produced in court, there is a need to establish the chain of evidence. The data secured from a mobile device shall be protected from the risk of accidental alteration or interference. The tools used should protect the data and offer a way to check the integrity of the acquired data. In addition, the Laboratory procedures should robustly provide a means to check the integrity of the acquired data. This provides reassurance that the data has not been changed to demonstrate the correct handling of digital evidence. See Clause 8.1 and Clause 8.2.

Principle 4: *Tool users shall be competent to use the tools and able to explain their actions and the implications of those actions on the digital evidence to a court.*

The use of non-forensic tools, such as mobile phone repair tools may be justified if they are the only way to get the data off the device or defeat security protection mechanisms. However, users shall be aware of the risks associated with each technique and be suitably qualified, so that they can adequately explain their actions and defend the processes under cross-examination. Tool users should make investigators and prosecutors aware of the limitations of the digital evidence, as well as its strengths.

6.3 Tool Fundamentals

The scope of work to find truth in data, both exculpatory and inculpatory needs to be defined and undertaken in the context of what is both proportional and reasonable in the circumstances. E.g., in a case that revolves solely a round of abusive chat messages in the last month it would be reasonable to recover all chat messages from the last month. There would be no need (at this point) to recover data from before that date.

Acquisition and analysis of data from devices is often a process of back engineering, either partially or fully automated by a variety of tools. Mobile device operating systems, software, security updates and user applications are regularly modified and keeping up with these changes is a constant challenge for the tool developers.

Due to the volume and complexity of data stored on many digital devices, it is not always possible, nor within scope, to recover all data held on a device for review. It is, therefore, good practice to define a

strategy from the outset for each investigation based on the circumstances of the case and the necessary points to prove.

It is advisable to formulate a plan based around current known tool capabilities to enable the examination to focus on relevant data. As such users shall know and understand the current capabilities and limitations of the forensic tools, they have available at their disposal.

As the tools often extract data in ways the phone manufacturer had not intended, it is not entirely surprising that a tool on its own is unlikely to extract all data that might be present, and investigators may have to do more work to extract and verify the results.

Mobile phones are proprietary embedded electronic devices. Due to the constant volatility that exists within them; for example, memory changes, power cycling, and SSD wear leveling, multiple extractions from the same device will result in non-matching hashes. However, this does not mean that extracted data cannot be relied upon. But it does require an informed understanding of how the technology works. This underlines how essential it is that users understand the tools they are using and be sufficiently trained and qualified to operate them. Users shall be able to adequately explain how the evidence was recovered such that the digital data presented can be relied upon.

Failure to do so can result in perfectly valid mobile forensic evidence being thrown out of court, not because the evidence was unreliable or the tool inaccurate, but because the user was unable to satisfy the court of their understanding of how the tool works[7)].

6.4 Methodology

Adoption and application of standards should not prevent users from complying with national laws, local rules or agency regulations. It is not intended to replace such local guidance, but rather to complement it with a recognised baseline of good practice.

Due to the fragility of digital evidence, it is necessary and important to apply an acceptable methodology to ensure the integrity of the potential evidence. However, due to the rapid changes in the technology, it will not be possible to mandate a specific method or tool type in this guidance document. The only guaranteed factor is change, so it is important to stay up to date on what is currently deemed best practice and the reasons why.

All tools have the potential for error. This is an unavoidable reality, and no digital forensics manufacturer can guarantee their tool is 100 % perfect and accurate. This is particularly the case with mobile device forensics where there are constant and rapid industry changes. The pace of progress demands rapid software updates to cope with new innovations and users shall always satisfy themselves with the reliability of a tool to produce accurate results.

Nevertheless, mandating a prescribed testing and validation regime for every new software release from a mobile forensic tool vendor necessitates a significant burden of work on organisations, which needs to be balanced against their available resources to undertake such testing.

Ideally tool developers should assess the target user requirements when defining feature specifications and ensure that the released features meet their intended purpose. Whilst users should assess whether the methods used, including the use of tools, validate the application purpose.

It is therefore recommended, that users select tools that have been subject to some form of validation testing for accuracy, this may be balanced against risk assessments and available resources to undertake the relevant testing, whether that is through their own organisation's internal procedures or via an independent third-party organisation that can be trusted to publish impartial results. It is important for

---

7) Bevan v. The State of Western Australia [2012] WASCA 153; 43 WAR 233; 224 A Crim R 227: https://jade.io/j/?a=outline&id=269552 (Accessed on 2022-03-01)

organizations to consider the effects of individual environment variables and how that impacts tool use. This is something third party testing may not consider.

NOTE Ideally that would be through the creation of a new European body available for tool testing, similar to those elsewhere in the world. For example, the US National Institute for Science and Technology (NIST)[8].

6.5 Tool Selection

There are some key considerations in tools selection which should be considered. Depending on the situation a variety of different tools may be used for the various stages of the process.

a) Features

- Accessing Data.
- Decoding Data.
- Data Integrity.

b) User Knowledge

- Data Sets.
- Dependencies and Limitations.

6.6 Features

6.6.1 Accessing Data

Naturally one of the most important considerations is whether the tool will enable users to get access to the data in the first place. This is also, very often one of the greatest determinates of the purchase price of such tools.

The cost of the tool investment should be balanced by the overall capabilities and the needs of the particular investigation. For example, if the tool is limited to just one extraction function on just one particular device type, which requires users to purchase other tools to review and analyse the data, then those total costs shall be taken into consideration to understand the overall true value and benefits of a particular mobile forensic tool.

Attention should be given that some products may assume users have access to other common digital forensic tools, so it is good practice to check exactly which tools are needed throughout the complete investigation chain, before selecting suitable products. Comparisons can be challenging due to the constant evolving nature of devices and operating systems.

Equally, it is vital that practitioners are aware of any limitations with the products, to make a fair comparison and informed decision on the best tool for the case presented. For example, certain capabilities to overcome security protocols on mobile devices and access data, are very sensitive to multiple variables such as the exact hardware model, operating system version, current state of the device (e.g., BFU/AFU) and last known security patch, to be successful. Users should ensure that they have all the necessary and relevant information available, when a tool is selected for the task.

Another consideration for tool selection is the extraction method capabilities. Logical acquisitions of mobile device data may result in limited recovery of application and user data. Physical and File System

8) US Department of Homeland Security: Test Results for Mobile Device Acquisition: US National Institute for Science & Technology (NIST)

acquisitions often result in a richer set of collected data and provide the examiner with the opportunity to carve additional artifacts from the device memory which may not have been automatically decoded by the tool, for example, deleted data or system log files. Practitioners should consider the risks associated with exploitation and extraction techniques via vulnerabilities such as jailbreaking, rooting, Emergency DownLoad (EDL), Joint Test Action Group (JTAG) and others (see also Clause 6.9).

Practitioners should consider the use of dedicated tools for specialist work. For example, cloud services, drones, vehicle entertainment units and game consoles may require dedicated technology or licenses. The total number of available tools continues to grow, and regular assessment of the various options is recommended good practice.

The speed of acquisition and duration of the extraction is another important factor to take into consideration and balanced against the type and volume of data expected to be recovered. Different extraction techniques will vary by device and tool and the impact of the time taken to extract data may be a relevant consideration for some users.

6.6.2 Decoding Data

Accessing the raw data alone is not usually sufficient enough for mobile forensic practitioners. Tools need to balance different user requirements. Very few examiners have the necessary time to read the raw binary hex files to carve out artifacts. The vast majority of users rely on a tool to make some form of automated decoding. Therefore, the decoding capability of tools is very important, because of the data enrichment value it can offer and the time it can save users. The ability to quickly review what has been recovered and then determine whether there is anything of evidential value on the device is a significant factor for consideration in tool selection.

Many users tend to focus on accessing the data as their priority and often overlook the quality of the decoding of a tool. This is a significant oversight, given that most investigators will only have enough time to review what is automatically decoded and presented to them by the tool. It should not be assumed that the data presented by the tool will always be a complete record of everything stored on the mobile device. Equally, it should not be assumed that every mobile device extraction from the same source of mobile device will present the same data regardless of the tool used. A simple comparison test between different mobile forensic tools should soon debunk this assumption. It should be understood that mobile forensic tools often produce different results when comparing the outputs of their decoding. So, all other things being equal, practitioners should ensure that the tool of choice decodes most data in the most reliable way. Users should understand that no tool can guarantee to recover and decode all data stored on a device, practitioners should seek to ensure the relevant data artifacts have been decoded. This is why verification and validation of data recovered by tools is important.

While the recovered raw data may be the same and available in all the extraction data sets, an ability of a forensic tool to decode and present this information is a separate matter. Tools rely on the understanding of vendors' software engineers of the latest data formats and storage techniques, which are constantly changing.

Good practice is to undertake comparison tests between tools with similar capabilities on known devices, with known data for specific applications, to measure variances in the ‘decoded’ data presented based from the same acquisition. The speed of development and frequency of updates in smartphones means that the way in which data is recorded and stored is changing all the time and it is an endless task for tools to keep up to date.

NOTE It is for this reason that the creation of a new European Forensic Testing Body is advocated as explained in clause 6.13.

The capabilities of a forensic tool, the specific operating system present, and the type of device being examined determine what types of artifacts can be recovered and identified. The automated decoding and search capabilities of a tool can play a significant role in the discovery of relevant artifacts.

Time harmonisation is another factor often overlooked during the consideration for tool selection. If users anticipate analysing the contents of several different mobile devices, it is vital to understand whether there is consistency in the way that date and time formats are decoded and presented by the tool. Many mobile devices store date and time in different formats, which are determined by hardware, operating system and regions. Normalizing variable dates and time stamps from several different mobile devices for an accurate timeline comparison is essential. On a mobile device, some timestamps may come from the device's internal clock, while other timestamps may come from the network and a good understanding of how time stamps work in each case is critical.

EXAMPLE Are these two artifact timestamps identical 2021/01/03 15:37 and 2021/01/03 15:37 UTC+02:00

6.6.3 Data Integrity

The greater the capabilities of tools are, the more the forensic examiner benefits from all the programming experience and knowledge built into the tool. Nevertheless, regardless of how capable a tool is, users should be capable of presenting the evidence in court and producing a quality forensic report which could be subject to cross examination.

NOTE An example for a forensic information report template is provided in Annex E.

Getting past security and encryption to acquire the data is important. Equally so is the importance of good decoding, but ultimately all that effort should be geared towards producing evidence which is of a quality and reliability that is acceptable to the court.

The Chain of custody (Clause 7.2.7) for handling evidence is critical in investigations and users shall be able to prove the origin and provenance of the evidence presented. Regarding chain of evidence, it is important to demonstrate that the data has not been interfered with or altered in any way from the moment data is first acquired, until the day it is ultimately used in court trial.

If users take the time to acquire the data, decode it and then prepare a detailed report to present the evidence at court, then it is vital to ensure that the data can be relied upon to be an accurate representation of the original digital evidence stored on the mobile device. For example, visual ID of IMEI, IMEI, DNA/Fingerprint on SIM card, battery, memory card should appear in the report. Often there is an obligation of proof required on users to prove that the data has not been altered or interfered with in any way.

6.6.4 User Knowledge

It is important to distinguish between the admissibility of mobile data as evidence and the admissibility of expert opinion about the interpretation of the digital evidence. These are two separate topics.

In relation to the use of a forensic tool, to satisfy the court that the digital evidence can be admitted – it is vital that the examiner can demonstrate competence. That competence should relate to both the use of the tool, satisfying the court that the tool was functioning correctly and that the results can be relied upon as an accurate record of data stored on the device, relevant to the case in question (See also Clause 5.1.5).

Certified training is essential, not only to ensure knowledge on the use of the tools to the examination but also to ensure credibility on court. Mobile Forensic Tools are often expensive investments, so it would be a significant oversight not to also invest in user education. More details about this can be found in Clause 5 on Personnel.

The principles detailed in Clause 6.2 act as a helpful summary guide and the sections that follow will provide further insight on how to ensure the integrity of digital evidence.

6.7 Tool Interoperability

Tools selected for mobile forensics should, wherever possible, support the concept of openness in terms of data exchange between other forensic tools and support standard industry file formats. It is preferable,

where possible, to extract/decode data from the same mobile device by multiple tools due to variable support levels.

For example, the CASE file output: https://caseontology.org/index.html. This aids in the verification of data that has been extracted using different forensic tools and allows for easier and clearer results comparisons (see also Clause 7.13).

Practitioners should ensure the selected tool has the required features to be able to export data to other formats for ingestion into other tools for further processing.

6.8 Forensic Tool Log

It is recommended that tools used for forensic processes, wherever possible, maintain an automated audit secure log of the processes and procedures undertaken. Ideally, this should record (see also Clause 7.2.3):

— Tool software version used.

— Mobile device model examined.

— Details of the precise techniques applied to obtain the data (e.g., connection type, extraction process used, agent required).

— Indications of any extraction or decoding errors encountered.

— Open transparency to ensure fairness in any subsequent trial.

— Date and time of tool execution.

— Any specific hardware/platform system details

— Operator ID (where possible).

If the items above are not logged automatically by the tool, they can be recorded in a worksheet, notes or other method.

It is important that a third party can track the same processes used and achieve the same results. For this to happen, a properly documented sequence of processes needs to have been recorded contemporaneously, and those same records need to be accessible by all parties. This forensic tool log is meant to supplement all organisations local procedures, laws and chain of custody records.

6.9 Secure Evidential Storage

There are some fundamental legal requirements applicable in most courts across the globe when it comes to digital evidence. Whilst the precise specifications vary in different jurisdictions, some general principles can be adopted internationally.

Original digital evidence in this context refers to the raw data acquired from the mobile device and excludes subsequent decoding. It is imperative to validate, using the original digital evidence that the digital signature mechanisms have not changed, and the integrity of the data remains intact. It is recommended that a working copy of the original digital evidence is used for subsequent examination.

One such principle is that of secure preservation of the digital media and devices holding the digital evidence as far as is practicably possible. Therefore, due diligence is required to ensure the tool selected for the examination process is capable of safely preserving the evidence. This can be achieved either through a secure evidential container for the data, or through verification that the data presented in court matches the original evidence, so there can be no allegation of tampering or altering the evidence produced at court. The use of logs and timestamps together with digital signature mechanisms and secure

hash functions (it is recommended to use SHA-256 or multiple algorithms), can all help to establish a secure chain of evidence for digital evidence presented at court.

It shall be ensured that the tool has suitable methods to protect the integrity of the evidence. Where possible, users should select a tool with a secure methodology to protect data, together with an open, accessible audit trail of forensic processes applied to the device, that can be read and understood by an independent party if necessary.

6.10 Validation and Verification of Tools

Validation and verification testing can provide some degree of assurance that a tool performs to the required specifications. However, it can never be guaranteed that a tool will always operate with 100 % accuracy in all circumstances and instead it should be treated as an indicator of suitability for a function.

Mobile devices present special challenges for the validation of tools, techniques, and procedures. These challenges include rapid development cycles, undocumented operating and file systems, the overwhelming diversity of hardware devices, firmware revisions, and the need for narrowly specialised tools and methods.

It is not practical to test every combination of mobile forensic tool version and device type. It is best practice, at a minimum, to test those subsets of a functionality of the tools that are relevant to its expected use.

Validation testing should be performed whenever new, revised, or reconfigured tools, techniques or procedures are introduced into the forensic process.

For the validation and verification of forensic tools, this guidance refers to the definitions established in ISO/IEC 17025:2017:

— Validation – Verification, where the specified requirement is fit for intended use.

— Verification – Provision of objective evidence that a given item fulfils a specified requirement.

Requirements are conditions or capabilities needed to be present to use the tool for a particular purpose.

Example of verification: If the tool is being verified for support for chat messages in a specific app, then testing would involve starting with data with known results, processing that dataset with the tool, and ensuring that the results from the tool match the expected results.

Example of validation: If the organisation has a process (method) defined in their standard operating procedure, the tool will be tested to ensure that it complies with the requirements of the given procedure demonstrating that the tool functions in the use case intended by the lab.

NOTE These definitions for verification and validation differ from the definitions used in the software development process as forensic tools used in forensic labs should constitute full software releases as opposed to software in development. For tools being developed by the lab it is suggested that verification and validation using the definitions from IEEE, 1990 be followed throughout the development lifecycle.

6.11 Tool Release Notes

Professional manufacturers should conduct thorough testing of their forensic tools.

Manufacturer release notes can be very helpful in identifying where previous issues have been solved, bugs fixed, and new or improved capabilities incorporated which may need testing. This can help users to assess the potential impact on previously extracted data and decide whether new validation testing is necessary.

Detailed records should be kept of tests undertaken including dates and version numbers for future reference in case of any challenges in court proceedings that may be raised years later[9].

6.12 Risk Register

Vendors should provide guidance on how users can best leverage their tools during a forensic extraction.

While several tools could be used to perform a mobile forensic extraction, guidance should be provided as to how users best select the appropriate tool or extraction option within that tool as well as the expected dataset upon successful extraction.

Maintenance of a risk register which includes assessments of risk and any suspected uncertainties for available tools can assist in that process.

A tool could start with a blank entry but be viewed as a potential risk; for example, if it is brand new and has not yet been evaluated in any detail.

The risk register should also include any temporary or potentially permanent changes made to the device to include jailbreaks, roots, and software agents that may be introduced to the device during extractions. Where possible, the vendor should prompt the user with options to "opt out" of anything that could be considered a risk.

It should be noted that users may have access to a limited number of tools and the best on the market may not be available. When this occurs, a tool may be chosen because it is the only tool available that can produce any form of result or is the only tool accessible to that user. Equally, there could be situations where the only way to gain access to the data on a mobile device is to use alternative technology and tools not originally intended for the digital forensic market, for example mobile phone repair tools, flashing software, and hacker boxes to unlock devices. In such circumstances the need for tool knowledge, testing and validation still remain. Whatever tools are selected, maintaining contemporaneous detailed records of their use and risks involved is advised as good practice for any subsequent court proceedings.

6.13 Recommendation for an EU Forensic Testing Body

Whilst independent testing of forensic tools is highly recommended, the effort and expense involved to do so should not be underestimated. This includes both software and hardware tools. It is an extremely time-consuming process that prevents law enforcement users from undertaking their primary role of 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 to test a tool across a broad range of functionality.

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 function. Manufacturers issue almost monthly updates to their tools, which places a tremendous burden on agencies to conduct regular and repeated testing for each and every update.

To avoid significant duplication of effort by all the individual law enforcement agencies across Europe, it is highly recommended that the European Union considers establishing an independent test body that can be relied upon to conduct such independent testing on their behalf. The cost savings alone in terms of the time saved would surely make this a worthwhile investment.

---

[9] Danish Police software tool error: https://politi.dk/rigspolitiet/nyhedsliste/orientering-om-fejl-i-softwarevaerktoej/2020/04/30 (Accessed on 2022-03-01)

7 Processes

7.1 Background information

The rapid development of mobile devices makes this CWA a living document and has consequences for the CWA. The CWA covers the whole investigation chain from the first appearance of the mobile device as potential digital evidence until the presentation in court.

It will support quality management (as an internal structure) in the law enforcement agencies and forensic laboratories within the European Union.

7.2 General requirements

Digital evidence shall be precise and accurate to be accepted in the court. Digital evidence is fragile in nature and shall be handled properly and carefully.

7.2.1 Impartiality

7.2.1.1 Within the organisation, its personnel, all activities, and any policies regarding impartiality shall be documented.

7.2.1.2 Any information obtained during the forensic process should not influence the impartiality thereof. Information obtained during the forensic process that potentially impacts the impartiality shall be recorded.

7.2.1.3 Any activities shall be undertaken impartially, structured, and managed to safeguard impartiality and eliminate any room for bias of results.

7.2.1.4 Digital Forensics Management shall be committed to and responsible for impartiality.

Any pressures to compromise the impartiality of the laboratory activities like commercial, financial or other pressures shall be excluded systematically.

7.2.1.6 The identification of any risks to impartiality shall be an on-going process. This includes risks that arise from activities, relationships of laboratories, or relationships of personnel. However, those relationships need not entail a risk to impartiality.

7.2.1.7 In case of identification of a risk to impartiality, the laboratory shall demonstrate means to eliminate or minimise such risk.

7.2.2 Confidentiality

7.2.2.1 Within the organisation, its personnel, and all activities any policies regarding confidentiality shall be documented.

7.2.2.2 Only those with lawful authority or dully authorized should be able to access evidence or pieces of evidence.

7.2.2.3 If a release of information is required by law or authorised by contractual arrangements, the subject or individual affected shall, unless prohibited by law, be notified of the information supplied.

7.2.2.4 With the exception of explicit requirements by law, personnel, including any committee members, contractors, personnel of external bodies, or individuals acting on behalf of the laboratory, shall keep confidential all information obtained or created during the performance of laboratory activities.

7.2.2.5 It is suggested to use standard handling codes to facilitate and simplify the practical use of information, and to enable the option of adding specific conditions on the use of information, if and when appropriate.[10)]

7.2.3 Auditability

All processes and performed actions shall be documented in a way that an independent assessment to evaluate all activities performed is possible. Any independent assessor shall be able to justify the decision-making process in selecting a given course of action. The assessor shall be able to determine whether appropriate scientific methods, techniques or procedures were followed.

7.2.4 Repeatability

Repeatability is established when the same results are produced under the following conditions:

a) examining the same evidence,

b) using the same procedure under the same conditions,

c) at any time after the original examination.

Any trained forensic practitioner should wherever possible be able to repeat the examination described in the documentation and arrive at the same results without guidance or interpretation.

For some mobile device forensic techniques, especially in chip-off or jailbreaking, some limitations apply.

7.2.5 Reproducibility

Reproducibility is established when the same results are produced under the following conditions:

a) Using the same evidence to examine.

b) Using a different procedure under different conditions.

c) The examination can be repeated at any time after the original examination.

The individual responsible for the reproduction shall be informed about the applicable conditions. For some mobile device forensic techniques, especially in chip-off, some limitations apply.

7.2.6 Justifiability

All actions, methods and procedures in handling and examination of potential digital evidence on mobile devices shall be justified. The justification should be documented by demonstrating that the decision was the best choice to get most potential digital evidence from the mobile device.

---

10) Europol suggests the following Handling Codes:

Code H0: "This information may only be used for the purpose of preventing and combating crimes in line with the ECD and any other applicable law"

Code H1: "This information must not be used as evidence in judicial proceedings without the permission of the provider."

Code H2: "The provider must be consulted before this information is used and/or disseminated."

Code H3: "Other restrictions and comments:" can be marked to describe all other possible restrictions, permissions or purposes of transmission. Restrictions, permissions or purposes can form part of the 'Terms of Use' as mentioned on top of this page. (legal basis: Article 14 Europol Council Decision, 2009/371/JHA)

7.2.7 Chain of custody

In any forensic examination of mobile devices all persons that are in contact with the device shall be able to account for all the acquired data and the mobile device at the time it is within the custody of the agency or laboratory. The chain of custody record is a document identifying the chronology of the movement and handling of the potential digital evidence. It should also include known relevant information about the state of the device, including known changes of state (e.g., power on/off, SIM present, flight mode, battery charge level, damage, packaging, biohazard/body fluids/DNA/fingerprints/on-screen content etc/current date and time/updates to software/current running apps, etc.). The document shall be instituted from the collection of the device. This shall be accomplished by tracing the history of the item from the time it was first identified, collected and acquired up to the present status and location (see also Clause 8.3.1).

The chain of custody is a document that details and records the personnel responsible for handling the potential evidence at any point in time of the investigation. The amount of detail necessary in the chain of custody document varies per jurisdiction.[11)] The chain of custody shall be maintained throughout the lifetime of the potential evidence and preserved for an appropriate period after the end of lifetime. The document shall be protected against manipulations and data loss (see also Clause 6.3 on Tool Fundamentals).

7.3 Preliminaries

Before a forensic examination of mobile devices starts, a request of lawful authority for service is needed. The request for service shall

a) be documented;

b) contain reasons for the forensic examination;

c) contain concise, clear, and explicit questions or tasks;

d) contain state information of the device, including operational state, physical state, hazards that may pose a risk to the examiner, and other forensic traces which shall be preserved during examination;

e) specify whether all or only specific data is to be examined; and

f) specify whether the destruction or modification of the device during examinations is permitted.

State law may allow exceptions such as lockout situations or threat to life, etc.

The request for service shall be carefully checked and reviewed by the forensic examiner. The check shall include the following questions:

— Are the reasons for the forensic examination reasonable?

— Are the requested procedures established and relevant?

— Is the communication with the customers ensured and rules established?

If there are severe doubts in the legality of the request of service, it shall be rejected. If there are missing information or small errors, correction or modification is permissible if the requestor agrees. Before

---

11) See https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf (Accessed on 2022-03-01)

starting the examination, it is recommended to contact the initiator to manage expectations and make them aware of possible risks.

7.4 First response

The forensic value of the evidence of the mobile device shall not be reduced by the first responder and everything shall be done to preserve the evidence to minimise the impact on the investigation.

Nevertheless, while it is not possible to totally preserve all evidence for mobile phones, it is necessary to manage the risks associated to the investigations.

In any case:

a) Damage of digital and physical evidence shall be avoided.

b) Data changes shall be avoided where possible.

c) The state of the device on/off should not be changed (see also Clause 7.7).

7.5 Recording

All relevant information of the evidence shall be recorded (see also Clause 7.2.7). This includes:

a) A unique, permanent identifier of the item.

d) A description of the item and the in-situ situation (where appropriate photos should be included).

e) The state of the device (on/off).

f) The state of the connectivity of the device (flight mode on/off, connected to service and or WLAN).

g) Lock codes if available (these shall be requested from all persons connected to the mobile device), noting that some devices have self-destructing pin codes.

h) Any useful related accessories, SIM cards, packaging or documentation that could assist the investigation.

7.6 Labelling

All evidence shall be uniquely, consistently labelled with a unique identifier. The label shall not be changed during the whole examination.

7.7 Packaging

All evidence shall be packed safely for transportation.

The package shall not alter the evidence. If there is additional forensic evidence like DNA, fingerprints, etc., this shall be considered. In some cases, faraday bags or similar devices blocking connections may be useful. As the circumstances require the device shall be provided with electricity.

The use of Faraday bags shall be considered if the device has been seized in a "switched on" mode to help prevent (remote and/or external) interference to mobile devices; an alternative approach is switching the device to flight mode, if first responder is competent to do this.

NOTE Information about the use of Faraday bags is available at https://www.staff.hs-mittweida.de/~engler/FORMOBILE/CWA/FORMOBILE_LIVEFLOW.pdf.

7.8 Item transport and storage

All evidence shall be transported and stored safe. There shall be provisions to prevent access of third parties to the evidence.

The evidence shall be preserved and protected to avoid alteration by any influences.

As the circumstances require, the device may require power, and controlled or blocked connections to networks.

Procedures for handling operating devices and controlled connection of devices shall be in place.

7.9 Lab Work

The forensic examination of mobile device evidence starts with an initial inspection phase, an authorisation phase, the selection of appropriate tools, then the process of acquisition, decoding and data analysis.

7.9.1 Initial inspection phase / device identification

The first step of the lab work is an initial inspection phase. In this phase, the mobile device shall be identified. This can be done:

a) via the IMEI (considering the possibility that some devices, especially clones can have fake IMEI stickers printed on them which do not match the electronic IMEI stored in the device).

b) by comparing the device to reference devices.

Identification can be difficult with fake phones (counterfeit products) or very new devices. In addition to the type of the device, also the operating system and the OS version and the Firmware version should be determined where possible. The process of identification shall be documented (model, serial number, and any other valid information, including taking pictures of the device and checking the quality of the pictures right after taking them).

Furthermore, this initial inspection phase serves to preserve the evidence. It should include the detection of defects and potential device manipulations. The forensic experts shall determine whether there are vulnerable data, volatile data or expiration periods. They shall decide whether the device has to be examined immediately or whether the device can be examined later.

7.9.2 Instruction and authorisation

The handling of the device including the reporting should be discussed in agreement with the requestor of the examination. A forensic strategy shall be selected and authorised by the requestor.

7.9.3 Tool Selection

Before examination, the tools to be used in the process shall be identified Tool restrictions can be

a) defined by external regulations and legal permission;

b) dependent on the request of service;

c) dependent on the device to be examined.

In any case, the tools selection criteria need to be justified and documented (see also Clause 6.5).

7.9.4 Acquisition

The quality of the forensic image of the mobile device evidence is of outstanding importance for the evidential value of the complete forensic examination (see also Clause 6.6.1). The following guidance is

recommended to secure the maximum amount of potential evidence, that supports the defined strategy (see Clause 6.3). Different considerations should apply for victims and witness devices to balance data privacy (see Clause 8). Therefore, there are the following requirements to the forensic acquisition:

a) Physical image: Whenever feasible a physical image of the mobile device should be acquired. This means that every sector of the non-volatile memory of the mobile device is duplicated.

b) The possibility of acquiring volatile memory (RAM) should be considered.

c) File system/logical Images should be acquired if a physical acquisition is not possible or only limited data is to be examined.

d) Error handling: All read errors during acquisition should be recognised and documented.

e) Completeness of the image: The forensic image should be complete. This includes that all persistent memories built into the mobile device or connected to the mobile device should be acquired as completely as possible.

f) Prevention of alteration: The forensic image shall not be altered after acquisition (for example by making image read only and calculating a cryptographic hash). All decoding or analysis work should be performed on a copy of the image.

In many mobile devices, some of the user data is stored on cloud servers or physically separated from the device itself. It shall be ensured that this data is acquired appropriately too, if legally permissible and feasible. If backups of the device are legally available and accessible on cloud servers or external storage these should also be acquired.

7.9.5 Decoding / Decryption

In many mobile devices, the stored user data or part of the data is encrypted. Before analysis, the data shall be decrypted with appropriate tools if possible.

Other data is plain text but encoded in various ways; this is for example true for time stamps. Encoded data shall be decoded properly to be analysed (see also Clause 6.6.2).

7.10 Analysis

After acquisition, decryption, and decoding, the user data shall be analysed appropriately, to extract evidence from the mobile device. All evidence shall be evaluated objectively to determine its meaning and relevance to the case. Errors and oversights that may have already been made shall be identified. Evidence gathered by others shall be assessed regarding its reliability and significance before being relied upon.

Basic goals of forensic analysis of mobile devices address fundamental issues such as where the device came from, who used it in the past, how it was used, what data it contained, whether a password was necessary, or whether other access restrictions apply.

7.10.1 Analytical models

Forensic analysis requires reliable and scientific analytical models. Otherwise, mobile device forensic analysts face the challenges of unjustified forensic conclusions or that the findings are speculations without concrete scientific support. In the absence of a scientific analytical model there is a risk that forensic results will vary from analyst to analyst.

All evidence shall be reviewed by qualified personnel before being submitted to a court (see also Clause 5.3.2 and ISO 9001:2015, Clause 7.2).

7.10.2 Live analysis

In some cases, it is necessary to analyse the mobile device live; this means there is no acquisition or decryption step, but data is analysed on the running device itself. Live analysis bears the danger that the data on the device is altered; therefore, a post-acquisition analysis is preferable. If live analysis is used every step on the device shall be documented carefully including an exact time stamp. The documentation shall contain photos or ideally a video recording of the displayed preferences and results. Modifications on the device shall be limited to a minimum and appropriately documented.

7.10.3 Selection of analysis methods

Selected methods and procedures shall be appropriately defined, established, and kept up to date. If necessary, a laboratory may choose to utilise a procedure that is not specified where no alternatives are available. In such a case, the usage shall be documented and justified. New methods shall be properly developed.

7.11 Verification and Validation

All laboratories shall use only appropriate methods and procedures for all laboratory activities.

All supporting documentation, such as manuals, standards, instructions, or reference data, which is relevant for the methods or procedures shall be kept up to date and shall be available to the personnel.

7.11.1 Verification of methods

All laboratories shall verify that methods can be properly performed before introducing them. Records of the verification shall be retained. If the method is revised, the verification shall be repeated.

Deviations from methods for any laboratory activity shall occur only if the deviation is documented and technically justified.

7.11.2 Validation of methods

All laboratories shall follow a deviation process for non-standard methods used, ensuring the impact on the evidence can be documented, justified, verified and validated. This is also necessary for laboratory developed methods and standard methods used outside their intended scope or otherwise modified. If the method is altered, the validation process shall be repeated. All known limitations of methods shall be documented and communicated to the customers and the court.

The performance of the laboratory shall be compared with other labs regularly.[12)] This can be done through proficiency tests, ring trials or interlaboratory comparison.

All validation should be performed on independent data that has been carefully created through a documented process. In addition, tool version information shall be included. Independent test data should be exchanged via the forensic laboratories within the EU. If the creation of independent test data is not possible or very time-consuming post hoc validation is possible. On occasions the validation can be actioned against the results of reverse engineering of applications.

7.11.3 Peer Reviews

Not only the written reports but the whole process of the forensic analysis from the first responder to the oral presentation at the court should be peer reviewed regularly. The process can be reviewed as a whole or in segments.

---

12) See ISO/IEC 17025:2017, Clause 7.7.2.

7.12 Reporting of results

No data or report should be released before review and authorisation. The review and authorisation shall be performed by a competent person other than the person who conducted the forensic analysis. For the review and authorisation process the reviewer shall gain full access to all relevant data and the examined devices itself. Records of the review should be kept. If the reporter and the reviewer do not reach a common conclusion, a documented escalation procedure shall be followed.

The report should indicate whether the findings were validated. For non-validated findings, a disclaimer should be in place.

EXAMPLE A possible disclaimer could be: "There is the possibility that there are data within the exhibit(s) which have not been extracted by the process(es) used. Further validation work of the process(es) used will not be undertaken unless the material is reasonably challenged by a party or if new information indicates that the material may be incomplete or inaccurate. Should this be the case, the issue must be brought to the attention of the laboratory. The exhibit(s) may have to be resubmitted for validation work or even a further examination."

The tool versions shall be included as they also update frequently, and the amount of data parsed may change by the time the trial arrives.

All relevant data are provided accurately in the reporting; all records are kept.

Requirements for an investigation may differ in and across member states, this can depend on the receiver of the reporting (state attorney, defence, court).

7.12.1 Written reports

For all written reports, standard templates should be used whenever available. All fields in the template should be labelled in one official national language and English.

The written report should be stated in clear, simple and comprehensive language suitable for non-technical experts (see also Clause 8.3.6). The language used should minimise the "digital gap" between digital evidence presented at court by technical experts on the one hand and judges, prosecutors and defence attorneys on the other hand. All technical terms used shall be explained in a glossary of terms (this glossary should also be written in one official national language and English). All technical procedures and methodologies applied shall be explained including possible limitations and data changes or modifications during the forensic investigation chain.

All laboratories shall have a standard audit process for written reports. The report shall allow the reader to independently review the reliability of methods used in the production of digital evidence, and the validity of digital evidence presented at court.

For further information see Clause 8.3 and Clause 8.4.

NOTE An example for a forensic information report template is provided in Annex E.

7.12.2 Oral reports at court

The oral report should be stated in clear, simple and comprehensive language suitable for non-technical experts (see also Clause 8.3.6). The language used should minimise the "digital gap" between digital evidence presented at court by technical experts on the one hand and judges, prosecutors and defence attorneys on the other hand. All technical procedures and methodologies applied shall be explained including possible limitations and data changes or modifications during the forensic investigation chain.

The oral report shall allow the audience to independently review the reliability of methods used in the production of digital evidence, and the validity of digital evidence presented at court.

For further information see Clause 8.3 and Clause 8.4.

7.13 Exchange of data and archiving

All data analysed that influenced the report shall be archived. Regulations for the duration of archiving are appointed in state regulations and should allow for any appeal process periods. For every data exchange the rules of confidentiality apply (see Clause 7.2.2).

For some countries, there are also regulations for the formats to store data. If no regulations apply it is recommended to consider the Cyber-Investigation Analysis Standard Expression (CASE) as a standard digital forensic format (see also Clause 6.7).[13)]

8 Legal and Ethical Framework

8.1 General Overview

A general overview should be made of the legal requirements pertaining to mobile forensic investigations. Such an overview should be created in each jurisdiction by the competent authority and needs to be reviewed periodically. It is aimed at ensuring the legality and lawfulness of any actions taken. It should include:

a) Applicable procedural rules, defined by the applicable criminal procedural law, including the practical and administrative requirements imposed by these rules, this also includes rules on jurisdiction and competence:

   1) Rules on seizure – refers to the formal seizure of a mobile device by LEAs to secure evidence during the investigation stage of the criminal proceedings. Typically, different rules exist for devices that have been formally seized in comparison to devices that have not formally been seized. National/ Local rules also differ in scope and content, including different views on whether it is allowed to search a mobile device without its prior seizure and/or to copy data from it. Also important are the rules related to the exercise of judicial control over the seizure of a mobile device, and the existing practice and case law. This shall be mapped as well. There are likely also some limits to the seizure (e.g., personal data considerations; attorney-client privilege) that should be considered. Another aspect to be acknowledged is the notification of the concerned person about the seizure. With regard to the various parties (accused, suspect, witness, victim) of the proceeding the procedures related to seizure usually differ.

   2) Rules on accessing correspondence – in accordance with Art.8 European Convention of Human Rights the private and family life, and the confidentiality of personal correspondence should be respected. Because of this, accessing private correspondence from mobile devices should be considered only when necessary, proportionate and relevant. Relevant national/ local rules and case law should be mapped and followed, provided they also follow this principle of proportionality. The potential involvement of third parties (e.g. persons who are not implicated) should be considered as part of the proportionality test.

   3) Rules on accessing data in transit/ data in the cloud – clear rules should be established when accessing cloud data from a mobile device in accordance with European and International law, national and local law and practices. Rules, approaches and procedures in general, and actions in a specific case relating to the issue of accessing data in transit and data in the Cloud, especially when located outside their own jurisdiction, should be made explicit and be documented. This is particularly important during the pre-trial proceedings when investigative actions might be exercised without judicial control. Due to the deluge of information usually available on cloud

13) See: https://caseontology.org

services, the right to privacy, protection of personal data and principle of proportionality should be considered as most likely some amount of the data is irrelevant.

4) The rules of procedure when accessing information residing outside the jurisdiction – the existing instruments for cross-border judicial cooperation and exchange of evidence in criminal matters (e.g. European Investigation Order & Mutual Legal Assistance Treaties) should be duly considered. The respective rules should be followed as it will facilitate the collection and transfer of evidence across borders. These rules specify the timeframe for the procedure as well as the responsible authority in each country. It should be noted that the different existing instruments apply in different situations under various circumstances.

5) The rules of procedure when collecting evidence to-be transferred in another jurisdiction – the relevant mechanisms (mentioned above) for cooperation and mutual recognition of judicial decisions should be taken into account. Furthermore, the European Commission proposal on European Production and Preservation Orders (April 2018) aiming to facilitate and enhance the procedures of obtaining electronic evidence by judicial and law enforcement authorities from different Member States should be followed up.

6) Rules on reliability of the evidence –throughout Europe, there is currently little case law or specific rules on this, so likely national/ local, and case law on the matter will be limited or non-existent. What is needed at the very least are forensic copies/back-ups to work on (to be able to prove that evidence was not altered/has not lost its integrity) and a due professional approach (audit trail etc.) to guarantee authenticity and reliability of evidence and to establish the chain of custody, including who has performed which actions, at what time, and for what purpose (explicability and auditability of actions). Courts should set some basic requirements for quality and reliability of the investigation process (including the presentation of mobile evidence, in particular). In particular, the process and its results should allow for a third party to repeat the process and reproduce the results. The right to a fair trial and the principle of equality of arms should be duly considered in this context. A clear and established process, complemented by clear, concise, complete, understandable and transparent reporting will help the defence (and the judge) to review the evidence. If guidance is present, LEAs should ensure to follow it closely. Absent such guidance, LEAs should provide for this by themselves, which can be done by adhering to other sections of this standard and making information about this available to the other procedural parties. Whether national or local guidance exists or not, any reports about mobile forensic examinations should aim to prove the reliability of the evidence by giving sufficient information so as to enable all procedural parties to review the evidence, thereby aiming to close the digital gap between forensic experts and the prosecution, judiciary and defence. Any national/ local rules falling short of this mark should be complemented by LEAs to reach this goal.

b) Applicable human rights (right to a fair trial, right to privacy, and right to non-discrimination) and requirements flowing from those rights should be considered and specific procedures for the investigation to respect these requirements should be drawn up and use to foster an organizational culture and reflex of respect for human rights.

1) To support the right to a fair trial, the tools should come with guidelines not only for IT-forensic experts but also for the legal practitioners involved (prosecution, defence and the court), which would also allow the latter to understand the major functionality and possible limits of the respective tool. Provided that the digital data from mobile phones and cloud services concerned should be understood by the abovementioned legal practitioners (usually textual data, pictures, audio, video, but also some meta data), tools used by LEAs should be accompanied with review tools which allow not only judges and prosecutors, but also criminal defence lawyers to access and research these data independently. If no review tools are available, the data shall be made

available in another way, with due respect for the rights of the defence, i.e., giving them a real and fair chance to review the data. If access to all data is not feasible, the defence should at least have a say in selection relevant materials and should be facilitated in making an informed selection. In assessing whether the principle of equality of arms was respected, the resources of the defence, its level of specialization, and all other circumstances of their access (place, time, limits, accessibility, etc.) to the evidence shall be taken into account. Evidence that does not meet minimum fair trail guarantees shall be declared inadmissible.

2) One of the main considerations in the use of mobile forensic tools, already mentioned in relation to the legal overview above, is that of ethics and fundamental rights. The Charter of Fundamental Rights of the European Union is a source of primary law and it is legally binding on all EU Member States and the European Convention on Human Rights is binding on all states that have signed up to it including the whole of the EU. Any national/ local laws that include such provisions are also binding. The main fundamental rights that may be impacted by the use of a mobile forensic tool are mainly the right to fair trial, privacy, data protection, and non-discrimination. All these shall be duly considered. A specific point of attention relates to the potential use of Artificial Intelligence (AI) components in mobile forensics tools, e.g. for the visualization of data and advanced search and filtering options assisting the mobile forensic practitioner. Such tools may have an additional impact on human rights and shall in addition follow ethical rules and principles, such as human control and oversight, quality and accuracy assurance, security, privacy and data governance, transparency, non-discrimination and fairness, societal and environmental well-being and accountability.

3) By its very nature, the data recovered from a mobile device is often of sensitive nature about identifiable individuals. Thus, the use of a mobile forensic tool can present a significant intrusion of privacy due to the fact that various types of personal data are inevitably present in a mobile phone and, if the principle of data minimisation is not complied with and the data is processed beyond the purposes of the investigation, the amount of processed data is too excessive or irrelevant, and there is an unclear use of powers by the LEAs, a breach of the right to privacy can take place. While this right is not absolute, a proportionality test to balance the importance of the right to privacy with the need to conduct a successful investigation is strictly necessary before any data processing takes place. By its very nature, the data recovered from a mobile device often reveals sensitive details about identifiable individuals. Thus, the use of a mobile forensic tool can present a significant intrusion of privacy due to the fact that various types of sensitive personal data are inevitably present in a mobile phone. If the principle of data minimisation is not complied with appropriately, and data is processed beyond the purposes of the investigation (i.e., data is excessive or irrelevant to the investigation), a breach of the right to privacy of individuals can take place (both of the suspect or owner of the device, but also of others whose data is on the device). While this right is not absolute, a proportionality test to balance the importance of the right to privacy with the need to conduct a successful investigation is strictly necessary before any data processing takes place. Investigations should access data based on reasonable lines of enquiry and reasonably defined hypotheses. These may change during the investigation. For some investigations it may be needed to access all data, but for many investigations a granular approach (only certain types of data, only a given timeframe, etc.) is more appropriate. This also applies to the decision on which devices to acquire (e.g. only the mobile phone of the suspect vs. all devices from all people linked to the suspect, including witnesses or victims). Such a granular approach is also required by data protection law, in particular the data minimization principle.

4) Data protection is critically important to consider, including data protection by design and default and the use of data protection impact assessment to assess data protection consequences of methods, procedures and tools. The reputational damage, loss of public confidence and financial costs for violating data protection laws can be significant – which reinforces the

importance of protecting personal privacy of individuals.[14] Practitioners should be sure to check that digital forensic data is stored in a protected format at all times and not an easily accessible manner, when considering the issue of data protection and integrity for presentation in court.

5) Further, the implementation of the requirements and guidelines set out in this CWA in Clause 5 (Personnel), Clause 6 (Tools), and Clause 7 (Processes), are aimed at supporting the respect for fundamental rights and freedoms including the right to a fair trial and non-discrimination. Ultimately, digital forensics and forensic tools have to support these principles, otherwise the security provided by a court of law following due process will be compromised. The right to a fair trial and equality of arms in the context of access to electronic evidence in criminal proceedings has also been the focal point of the European Court of Human Rights' case of Rook v Germany.[15] Ensuring sufficient transparency within the mobile forensic tools themselves is of primary importance to avoid the occurrence of possible bias which may produce discriminatory results based on sensitive characteristics, contrary to the European Convention of Human Rights and the Charter of Fundamental Rights of the European Union. In addition, transparency helps create the possibility for effective scrutiny and helps bridge the digital gap between forensic specialists and the courtroom participants. Thus, any mobile forensic tool should be designed from the outset as inherently objective and transparent and this should be validated by both tool providers and users, and any known issues or errors should be disclosed. Human oversight in this regard is needed.

c) Applicable substantive rules on data protection (EU) (Law Enforcement Directive)[16], including:

1) Data processing principles: legal basis (legal ground), fairness, data minimisation (data shall not be excessive to the purposes, which may impose granular extraction/acquisition of data), purpose limitation (including appropriate re-use and sharing of data), accuracy, security, storage limitation, integrity and confidentiality, data mishandling measures etc.

2) Essential data protection principles and tools of the Law Enforcement Directive, such as compliance data protection by design and default and the use of Data Protection Impact Assessments (DPIA).

3) Data subject rights, including right to information and any restrictions to data subject rights that might be applicable through national law.

4) Law Enforcement Directive's obligation for a different treatment of data stemming out of fact and data stemming out of opinion.

5) The Law Enforcement Directive's requirements to distinguish and differentiate between the different categories of data subjects -witnesses, accused, victims.

---

[14] The Investigation Report by the Information Commissioner's Office on Mobile phone data extraction by Police forces in England and Wales, June 2020, emphasised that inconsistent approaches and standards of compliance by forces increase the risk that public confidence is undermined, see p. 8.

[15] Rook v Germany, 1586/15, [2019] ECHR 593.

[16] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

6) The Law Enforcement Directive's obligation to log activities.

7) Additionally, applicable EU Member State law, e.g. in relation to the processing of special categories of data (biometric data, health data, political opinions, etc). Special safeguards may be needed here.

d) Applicable Court of Justice of the European Union. and European Court of Human Rights case law.

e) Applicable national/ local rules with regard to existing privilege (medical, psychological, religious, attorney-client) and the criteria when such could be overridden by the interest of the ongoing investigation.

f) Applicable national/ local case law.

g) Other applicable national or international law. In particular, in relation to the use of instances of Artificial Intelligence (AI) in mobile forensics, this may in the future include the AI act, as such instances may qualify as high-risk AI systems.

NOTE Classification rules for high-risk AI systems are set in the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Act (COM/2021/206 final).

h) Other rules and principles of law, as applicable (proportionality as a general principle, the correct handling of indecent images and abuse materials which should not be distributed electronically etc.).

The overview should be heavily influenced by local law and hence these are only minimum principles to be included.

The overview should be applied throughout the investigation and preceding every next step (including in particular when using more intrusive functionalities, tools, methods or techniques) to ensure compliance with applicable laws and regulations and to safeguard the admissibility of the evidence before a court of law and to ensure compliance with legal and ethical rules, avoiding potential liability, unwanted legal consequences and loss of reputation. This means that before every next step a legal check shall be conducted, which means that it should be considered:

— Whether additional steps are required to comply with applicable criminal procedure, e.g., a court order.

— Whether this step is permissible under data protection law and in full compliance with the principles of data protection law, including legality, data minimisation and strict necessity for the pursued purpose (purpose limitation) "and tools used should be ensured".

— Whether there are any human rights, ethical and data privacy considerations to impact the decision.

— Whether there are any other elements to be considered that may impact the admissibility of the evidence.

— Whether other legal or ethical requirements prohibit or limit this step.

— Whether the step is proportional to the investigation and aims pursued, both in terms of investigative actions as such and in terms of privacy intrusion.

The decision, especially when deciding to move forward, should be documented.

Since legal requirements are often complex and nuanced, and may moreover vary heavily between jurisdictions (of which more than one may be relevant in any given investigation), it is highly advisable:

— to have the overview for the own jurisdiction (especially with regards to data protection law and human rights aspects) to be drafted or at least verified by external legal experts;

— to have the international aspects of the overview drafted or at least verified by external legal experts;

— to have an overview drafted or at least verified by external legal experts for other relevant jurisdictions;

— to seek external legal advice when dealing with new issues or jurisdictions;

— to seek external legal advice whenever unsure about the course of action.

8.2 Governance of the evidentiary proceedings

The legal overview should be complemented by or include a governance method for the evidentiary proceedings, i.e., a method relating to how information and digital evidence resulting from that information is processed and dealt with, from the moment it is gathered, to its presentation to the court, especially by means of what information is included in reports and/or expert testimonies on behalf of the prosecution, which are submitted to the court.

The evidentiary governance should encompass every step of the process of evidence gathering, processing and analysis to be fully comprehended by all involved parties and stakeholders. This means that different professionals (IT forensics experts, law enforcement officials, prosecutors, defence lawyers, judges) involved within the process should understand each other as a part of a holistic and integrated approach to the criminal proceedings, rather than as individual and independent phases. The goal should be that from the acquisition of the data on the mobile device all the way to the presentation of evidence in court, both the process and the outcomes should be transparent to all involved parties. That requires awareness of various parties involved and capability to present the acquired data and information, and the conclusion in terms of evidentiary value, in a simple and clear manner. Such governance is a necessary pre-condition to have a truly fair trial and a proper administration of justice in any country which adheres to the rule of law. The lack of understanding from any of the parties (usually the defence lawyers and judges and, to an extent, the prosecution as well), in terms of how forensic experts and law enforcement gathered and processed the evidence and what potential issues and pitfalls there could be, make them unable to review the evidence and hence there is the inherent risk of unfair and incorrect judgments. Hence, all parties shall understand the process and its outcomes and shall know what certain data is able to prove in which scenarios. All involved shall know what to look for to review the information. In practice it means:

— Be aware whether the mobile device has been lawfully seized.

— Be knowledgeable about the techniques of acquisition of data from mobile devices, including if and what measures have been taken to prevent obtaining unnecessary data (e.g., related to third parties or not relevant to the concerned case).

— Be knowledgeable about the steps of processing and analysing that data.

— Be familiar with the potential setbacks that may occur throughout the mobile forensic process, potential errors and uncertainties.

— Know how to interpret the results and their level of assurance/certainty. How reliable is the evidence and what can it prove, and to which degree of certainty?

Law enforcement and the prosecution have a prime responsibility in making this a reality as they are placed in the best position to bring about a common understanding. It may be counterintuitive to fight

for better possibilities for the court and the defence to review law enforcement's own work, but a fair trial demands this.

Information and digital evidence governance as a concept is part of this standard to help deal with the fact that mobile forensics by definition involves the processing of large quantities of digital data and complex technical processes, which are not readily understandable to non-experts, and hence leave potential issues with the right to a fair trial as explained before. Information and digital evidence governance aim to help remedy this situation by creating a shared means of control over the process and of reviewing the process followed by law enforcement afterwards in the courtroom. Such an information governance process should:

— Be holistic, encompassing both IT, legal and ethical perspectives to provide an integrated approach towards data and information processing.

— Document all steps and relevant considerations.

— Lead to an accurate, clear and concise report to be used in Court while enabling all relevant parties in the process to understand what has happened to the information, what the information seeks to prove, and what potential issues and pitfalls are, so that they can review the information presented to the Court.

— Ensure reliable and accurate, authentic and admissible evidence with good probative value.

— Ensure security of the information, which includes its confidentiality and integrity, both internally and externally (e.g., need to know basis access to guarantee internal confidentiality vs. measures to protect against unwanted disclosure to third parties and security measures to protect against accidental alteration by staff vs. intentional alteration by a maleficent third party).

— Be in line with the relevant ethical principles: accountability, responsibility, transparency, non-discrimination, fairness, privacy, confidentiality, inclusiveness, lawfulness, compatibility and others.

— Consider big data and Artificial Intelligence as they influence digital data and information processing., especially in terms of the potential privacy and discrimination issues that may be present when using such techniques. Information about governance implications of the use of Artificial Intelligence in mobile forensics is provided in Annex F.

Thus, the governance of the evidentiary proceedings in the context of mobile forensics requires a more comprehensive and complex approach than the traditionally known chain of custody to enable full and effective judicial control. This is due to the specific digital environment, the gap in knowledge between the courtroom participants and the mobile forensics practitioners and the volatility of mobile evidence. To elaborate ethical principles enshrined within the legal framework and the deployed technological standards by experts within the criminal prosecution a clear and structured comprehension of the 'evidence lifecycle' is necessary. Particularly, for data extracted from mobile devices and the cloud a dedicated, a specific approach is needed.

Any law enforcement agency implementing this standard should implement a suitable governance method for information and digital evidence resulting from that information. Next to what has already been presented, a suitable governance method should in particular take into account also the considerations presented in Clauses 8.3, 8.4 and 8.5 below.

NOTE In the context of the FORMOBILE project, a task force has produced a guidance document aimed at the legal practitioners at a trail (the judge, defence and prosecution) to enable them to ask the right questions about the evidence governance framework and evidence gathering approach employed by the LEAs and forensic practitioners. The document is aimed more broadly at electronic evidence but has been drafted specifically with mobile forensics in mind as well. It contains elements so legal practitioners can employ a checklist of requirements to verify that the approach followed by the LEA or forensic practitioner satisfies the requirements for the proper

administration of justice, due process and a fair trial, enabling real and effective scrutiny of specialized electronic evidence by non-experts. This document can provide useful guidance for LEAs and forensic practitioners as well, as they are the ones who shall satisfy the requirements in practice through their evidence governance framework. The document is available at https://formobile-project.eu/.

8.3 Pre-Trial Criminal Proceedings Considerations

Special attention should be given to limits imposed by applicable legal requirements, which circumscribe the permissible scope of the investigation. Such limits may include confidential suspect/client communications or certain materials requiring a special warrant, for example.

8.3.1 Appropriate logging and protocoling.

All information relevant to the case needs to be appropriately logged, stored and protocoled so that evidence can be subsequently challenged.[17)] More specifically, rules on data decryption, decoding, further use of the extracted mobile device contents and alteration of data during the investigation need to be established so that data extraction is appropriately and responsibly carried out. Logging and protocoling is regarded a procedural guarantee in the scope of the pre-trial phase of the investigation (see also Clause 7.2.7).

8.3.2 Criteria to be met when accessing messages, cloud and sensitive documents.

Suitable criteria shall be set up for accessing messages, cloud data, and sensitive documents so that the right to privacy is protected and all the guarantees are in place to make sure that no excessive and disproportionate amount of private data is processed. In addition to defining the threshold for when to access these documents at all in the first place, appropriate limits shall be defined to the specific data that can be retrieved, accessed and analysed in the first place, and then included as part of the trial proceedings. Recent case law establishes that retrieval of data by the relevant authorities is to be executed only upon written request and on the respective national/ local legal basis.[18)] To collect the requested information, the requirement of necessity shall first be fulfilled, which means that there shall be ground for initial suspicion for the offence.[19)] Furthermore, the specific type of crime needs to be taken into account as well, as additional limitations, such as obtaining a specific court order, may need to be overcome beforehand.

With regards to limiting the amount of data, the extraction of data shall also be proportional and as granular as possible, that is, not to allow for a bulk extraction of all data but only for specific information, relevant to the case. Granularity can be expressed by only obtaining certain types of data, only acquiring certain sources (e.g. devices, accounts) or limiting the acquisition to a given time frame.

8.3.3 Importance of the different roles in the criminal procedure – suspect, witness, victim.

Prior to accessing personal information, a balancing exercise shall be performed, taking account the right to privacy of the data subject but also their different role in the criminal procedure: suspect, witness or victim. With regards to victims and witnesses, the privacy of the data subject needs to be interpreted more strictly. In case of the suspect/accused, their rights to remain silent and not to incriminate themselves shall be respected. Furthermore, evidence cannot be obtained through coercion or oppression, and against the will of the accused to incriminate them, which would be a violation of the

---

17) Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, Article 7.

18) Case 50001/12, Breyer v. Germany, [2020] ECLI:CE:ECHR:2020:0130JUD005000112.

19) Ibid.

right to a fair trial[20], therefore information cannot be compelled from the suspect/accused without their express consent or a warrant/judicial order.[21] While the right to privacy of the suspect/accused can more easily be restricted than that of victims and witnesses, a suitable proportionality test is still necessary to determine whether the personal data in question is pertinent to the specific case. In all instances, the least intrusive measures by the relevant authorities need to be taken so that no violation of the right to respect for private and family life of the victim, defendant and any third parties concerned occurs and so that any impact remains as limited as possible.[22] Information sharing rules

The sharing of the forensic evidence shall be first duly authorised and on a need-to-know basis. This is required for the purposes of establishing a secure chain of custody and ensuring the integrity of the evidence (that it has not been tampered with since first obtained), as well as protecting the fundamental rights of all parties to the investigation.

8.3.4 Scrutinizing tools and review tools and documenting what tools were used

It is of primary importance to clearly take into account the purpose and scope of the specific tools used in the mobile forensic examination and for further processing the resulting digital evidence. The technical capabilities of the tools shall be examined and documented and should be validated before use. The goal is that not only the forensic experts understand capabilities and shortcomings of different tools on the market, but also the other procedural parties, enabling them to review the evidence produced by such tools by means of asking relevant questions. For this reason, reports should also mention what tools were used and any particularities relating to those tools should be shared with all procedural parties. Additionally, the output from the tools needs to be comprehensive enough so that the prosecution, the defence and the court can adequately assess the results and the relevancy/admissibility of the evidence. If there is a gap, this can be bridged through accompanying results with sufficient guidance in reports. Certain tools also offer review tools to facilitate access and understanding by other procedural parties. The presence and functionalities of such review tools should be a relevant factor in selecting which tools to use. The selection of tools thus can help create transparency, which is necessary to comply with the right to a fair trial and the corresponding principle of equality of arms.

Scrutiny of tools also generally requires the embedding of all the relevant legal and data protection considerations into the design or acquisition criteria of the tools. Next to the aforementioned all-important transparency and information governance enabling a fair trial, tool selection should also ensure that all other legal requirements are met, e.g., enabling granular extraction of data and "need to know" access, provide detailed logging of actions, etc.

8.3.5 Clear audit trails

The existence of clear auditability as an organisational accountability measure is required and it shall describe the methods and tools used for gathering the evidence and processing it, delineate the chain of custody, provide details on the general quality of the processed data, and, in the case of data sharing between entities, whether consent for sharing the relevant information was required and obtained.[23] Clearly established audit trails help ensure the reliability of the overall investigation process. Audit trails also should enable that actions taken can be explained and reviewed.

---

[20] Case 19187/91 Saunders v. United Kingdom, [1996] ECLI:CE:ECHR:1996:1217JUD001918791.

[21] Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, Recital (27).

[22] Case 26419/10, Saint-Paul Luxembourg S.A. v. Luxembourg [2013].

[23] "Universal principles of data ethics" - 12 guidelines for developing ethics codes, www.accenture.com/DataEthics

8.3.6 Using accessible language to all parties involved in the criminal procedure.

To bridge the so-called digital gap between legal practitioners (judges, prosecutors and the defence), on the one hand, and IT forensic experts on the other, as well as to ensure the rights to a fair trial (including the principle of equality of arms), presumption of innocence and defence, any findings shall be presented in accurate, clear, concise, understandable, and easily accessible language. This increased transparency will lead to better common understanding of the evidence by all involved parties, but especially by the relevant legal practitioners involved. Using such accessible language will be beneficial to the quality, relevancy and admissibility of the evidence and shall contribute to preventing miscarriages of justice. (See also Clause 7.12.1and Clause 7.12.2.)

8.3.7 Fair trial implications

The right to a fair trial and the principle of equality of arms are protected by human rights legislation[24)] and entail the right to an equal opportunity of both parties in criminal proceedings to present their cases. This inevitably means that a proper access to the case file[25)], including to a copy of all the original forensic evidence, shall be provided to them, thus also providing better transparency and complying with the right to a defence, as well as contributing to the proper administration of justice. Furthermore, Art .7 of Directive 2012/13 also requires that all material evidence related to the specific case is made available to all suspected or accused individuals and their lawyers for the purposes of preparing a defence. Evidence should be provided in a manner that allows the defence to effectively review it, taking into account its real resources. Evidence that breaches the requirement for a fair trial risks being made inadmissible.

8.3.8 Judicial overview of the process

Judicial scrutiny is crucial to ensure greater transparency, fair trial and the proper administration of justice. Judicial oversight is also of primary importance as it can ensure the reliability and admissibility of the digital evidence in court, and that the pre-trial criminal process has not infringed upon the data subject's rights.

A dedicated checklist that covers the whole process should thus be followed to ensure that the overall investigation has been conducted in compliance with the applicable EU and national/ local legal, ethical and data protection frameworks from beginning to end. This should be part of the jurisdictional overview. Breach of the right for fair trial has the risk of the evidence being made inadmissible.

8.4 Trial Phase Criminal Proceedings Considerations

The legal overview and governance method shall also take into account the requirements of the trial phase of the criminal proceedings. The first important provision shall be the general rules on admissibility of evidence applicable before the relevant courts. These may depend on the jurisdiction involved but, in general such include at least:

1) Relevance: the gathered evidence shall be related to the facts under dispute.

2) Authenticity: the gathered evidence should be proven to be accurate and collected from a reliable source. This includes the fact that the evidence has been collected following the chain of custody and hence could be shown to not have been tempered with (integrity) and there should be transparency on the methods and tools used.

---

24) European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 6; Charter of Fundamental Rights of the European Union, Article 47.

25) Ocalan v. Turkey, 46221/99, Council of Europe: European Court of Human Rights, 12 March 2003.

The legal overview and the information governance method should also contain general requirements derived from law and good practice in terms of due diligence and reasonable care, such as the rules applicable to ensure secure preservation and transport of media, evidence, and investigation results, which may help show the value of the evidence to the court.

The processing of the forensics data shall take place on a strict need-to-know basis, with the relevant experts that access parts of the data being logged in and their access being strictly confined to the administration of justice purposes. It is recommended that the prosecution provides ad-hoc authorisations on the introduction of certain data as evidence in the trial proceedings.

In some jurisdictions the court can be assisted by experts with scientific, technical, or other expert knowledge in their assessment of the case at hand and the evidence presented before it. To ensure that the interpretation of the evidence presented by an expert witness for the prosecution will be admissible and effective, the legal overview should also list the requirements for such an expert opinion, depending on the applicable legal requirements, but at least including:

a) Whether and how the tools, theories and techniques employed by the expert have been tested, including whether they have been published or peer reviewed.

b) Whether there are known error rates to report.

c) Whether the tool, theory, or technique employed is based on (internationally) recognised standards and/or whether they enjoy widespread acceptance.

d) Any other objective limits that are relevant to understand the presented interpretation of the underlying evidence.

e) The qualifications and experience of the expert relevant to the task at hand[26].

The legal overview should also consider obligations at the end of the process, such as the necessity of notification of the results of the investigation to the subject of the investigation, as well as what happens after the case has been tried, such as rules on data retention and on safe deletion of evidence.

It shall also contain applicable rules concerning sharing/transmitting evidence.

8.5 Prevention of mobile forensics dual-use, misuse, and abuse

An additional, but equally important, factor to consider is the control of use and accessibility of mobile forensic tools and technology. For example, some of the tools are so powerful in their capabilities to defeat encryption and security protocols that they are defined as ‘dual-use’ and fall under export control regulations. This means their applications for civilian use could equally be applied in a military context and therefore need careful control as to whom has access to them and for what purpose. This highlights the seriousness of the potential for abuse and misuse of these powerful tools. Hence, even if the tools are used by legitimate and authorized users, there is still a need to ensure that the capabilities of the tools are not misused. The following risks should be taken into account to identify potential dual-use:

— communicate/exchange data in an inappropriate manner (time; relevant stakeholders);

— unclear and non-comprehensive distribution of tasks/obligations among staff members to avoid duplication of data;

26 Daubert v. Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579 (1993), https://www.law.cornell.edu/supct/html/92-102.ZS.html (Accessed on 2022-03-01)

— lack of pre-defined requirements about the type of data that will be collected and the ways this data will be analysed;

— inconsistent and unsystematic collection of data;

— inaccurate identification of used data;

— no specific purpose for using the data. To ensure integrity of acquired data all aspects related to data collection, ownership, storage, protection, analysis, sharing and reporting should be duly considered.

This is why, professionals should duly consider dual-use, misuse and/or abuse of mobile forensics data as specific ethical concerns. To minimise these risks some mitigation safeguards shall be put in place within the context of mobile forensics and throughout the various steps of the process. In particular, during the acquisition of data from the mobile devices (a due care of the deployed tools, techniques and proper training of professionals to be considered), when unlocking mobile devices (the used methods), decoding and analysis of mobile data which may involve materials, methods, technologies or generates knowledge that could be misused for unethical purposes.

With regard to that, certain risks should be taken into account during the research and elaboration phase of the tools for mobile forensics. For instance: disclosing data in an inappropriate way, lack of clear rules and procedures about collection and analysis of the data and/or no clear purpose for using the data. Users should check that this is appropriately covered when approving tools for use.

Export control under the applicable EU law and its implementation by the Member States plays an important role to contribute to international and regional security and stability, and to restrict that these tools and technology are used in countries where serious violations of human rights have been established or for internal repression.[27)] These powerful tools should be used by lawfully authorised agencies in states which have a record of respecting human rights, where the rule of law is upheld and there are remedies available in respect of an alleged breach. Further, and regardless of whether a mobile forensic tool falls under a control in the list of dual-use items published by the Wassenaar Arrangement and implementing lists[28)] the use and purchase of mobile forensic tools from manufactures should be preceded by vetting to ensure they regulate sales of their technology and such vetting should include an appropriate human rights due diligence ("HRDD") and ethical considerations.[29)] Mobile forensic tools should only be used by end-users complying with the aforementioned legal and ethical rules and requirements.

In addition, the misuse and/or abuse of the mobile forensics data itself is to be considered by any end-user. To do that, the following aspects should be considered: whether the data, knowledge and technologies concerned can harm people if modified, what might be the consequences if the latter (e.g. collected data) serve any other purpose than the intended one and what might happen if third parties have access to that data. Results from mobile forensics are vulnerable to misuse mainly due to the fact that it encompasses data, procedures, knowledge and materials which could be misinterpreted and/or misused to stigmatise, discriminate against, harass or intimidate people, if not handled properly.

---

27) See e.g. Article 6 of Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment.

28) See for example Category 4 (Computers) or Category 5 (Telecommunication and "information security") in Annex 1 (List of Dual Use Items) of Council Regulation (EC) No 428/2009 of 5 May setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

29) Proposal by the EU Commission for mandatory human rights due diligence legislation with an enforcement mechanism is contemplated in 2021. See also Study on due diligence requirements through the supply chain - Final Report, January 2020 focusing on due diligence requirements to identify, prevent, mitigate and account for abuses of human rights.

Furthermore, it involves technologies that might infringe fundamental rights. This is why appropriate security policies and measures and a governance framework are of primary importance. In many countries, cyber security and data protection law, amongst others, will impose specific requirements for this. Still, it is a general principle of best practice, even absent of any specific legal obligations.

Annex A
(informative)

A Good Practice Guide for Mobile Forensic Tool Selection

A.1 Permissibility

Do practitioners have lawful permission, authority, or consent to use the forensic tool?

A mobile device often contains considerable amounts of data and falls within the definition of 'Personal Data' under the Law Enforcement Directive and the General Data Protection Regulation.[30)] Users should ensure they have lawful authority to recover data, which require adherence to the criminal justice legislation and applicable data protection laws. Users should ensure they have lawful authority to recover data.

A.2 Proportionality

Is the use of the tool proportional and justified?

Given the possible intrusions into privacy, can practitioners take steps to ensure that only evidential data which is necessary is recovered? Does the tool have the functionality to help limit the intrusion to specific time or dates to aid investigators?

A.3 Validity

Is the use of the tool valid in the circumstances?

A mobile forensic tool is not always the only option to recover evidence. For example, if the case needs to establish the time and date of a telephone call – consider the use of Call Data Records from the network operator as an alternative and reliable source of evidence. Ensure the use of tools is reasonable, necessary, and proportional in the given circumstances.

A.4 Security

Can practitioners rely on the evidence produced by the tool?

Ensure the tool has protection mechanisms built in to prevent accidental alteration or deletion of digital data. Ideally, select a tool purpose-built for forensics where possible that has an established record and can demonstrate a secure chain of custody for the evidence produced.

A.5 Processes

Can tool users follow a prescribed workflow to adhere to agreed standards?

Where possible, users should consider tools that allow for a comprehensive set of guidance notes whilst performing a device extraction. Ideally, that information should be used to guide practitioners through a pre-defined workflow to ensure best practice.

---

30) European Commission – What is Personal Data? https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

A.6 Ethics

Does the tool manufacturer respect international laws, fundamental rights and technology export controls?

The selection of a tool should involve vetting of the manufacturer and the contemplated business relationship, including whether the manufacturer is subject to export control that restricts the use of such powerful tools in countries which use it for internal repression or other serious violations of human rights, and taking due account of other relevant business conduct aspects as part of a HRDD and ethical considerations.

(It should also be noted that the European Commission intends to propose mandatory human rights due diligence legislation with an enforcement mechanism in 2021).

Annex B
(informative)

Mobile Forensic Tool – Checklist for Selection

No	Function	Description
1	Extraction of mobile phone data	The tool shall be able to access and read data from mobile devices, SIM Cards, memory cards and related mobile tech.
2	Quick and intuitive extraction process	The tool should be able to handle large data volumes and not slow down investigations and be easy to use to aid training processes.
3	Ability to process standard forensic file formats	The tool shall be able to both ingest and export forensic file formats to support verification of mobile data in other tools.
4	Understood to be forensically sound	The tool shall operate with forensic soundness, not altering sources and preserving metadata on extracted items.
5	The tool shall provide auditing functionality	There is a need for a range of tool process information to be gathered to inform users and allow for independent verification.
6	Ability to process structured data formats	Mobile device investigations will involve data contained within databases e.g., SQL, Plists, the tool chosen should be able to handle this.
7	Ability to extract and present geospatial data	Modern smartphone data is often geotagged or contains geo location data which can assist in investigations.
8	Ability to extract and present temporal info	Some files recovered will have time information in terms of metadata, but some files will also contain timestamped entries such as chat logs.
9	Facilitate tagging / categorising items	A key part of review is being able to assign items to different categories to assist future investigation work.
10	Filter by keyword	The tool shall give the user the ability to search information based on case knowledge which will include key words.
11	Ability to identify source of relevant data	Once an investigator has identified an artifact as relevant to the case, it shall be able to be linked back to the original source.
12	Present understandable reports	The tool should produce reports about the case, both during the investigation and as reports for formal court documents.
13	Ability to recover smartphone app data	The tool should be able to extract and/or parse structured data from mobile apps.

No	Function	Description
14	Scripting capabilities	The tool should be able to allow users to perform specific operations for the extraction and processing of the data in user-defined batches.

Annex C
(informative)

Mobile Forensic Tool – Risk Register

Please use this document to record and monitor known issues, risks or behaviours related to mobile forensic tools that need to be considered by examiners:

No	Tool and Version No	Risk Title	Details	Examiner Entry	Date
1	Product X version Y	Failure to detect altered file extensions of artifacts	Via logical examination it has been noted that this tool does not detect when a suspect deliberately alters the file extension to disguise them. This is relevant particularly to Child Sexual Abuse investigations, where a known method is to disguise data by deliberately altering the file extension. For example, changing a picture file name from 'Bad_Picture.jpg' to 'Bad_Picture.pdf' to avoid detection. Hidden pictures like this will not be reported by this tool via logical extraction.	Officer Smith 1234	1st Jan 2020
2	Product Z version A	Interference with other forensic tools on same PC	This version is known to interfere with other digital forensic tools operating on the same Windows computer as it will lock out available USB ports. This often is misreported as the other tools fail to acquire a mobile device, whereas it is in fact caused by this tool failing to release USB port drivers when finished.	Professor Jones	1st April 2020
3	Product B version C	Case File Data Protection not working as expected	Review of recent NIST Report information testing this tool reports that it fails to detect a deliberate attempt to modify the case data after extraction. Careful attention needs to be given to securing data if this tool is used for extraction purposes to verify results.	Supervisor Roberts	1st July 2020

Annex D
(informative)

Six Steps to Successful to Mobile Validation

D.1 Step 1: Determine all possible extraction methods for the search authority

a) It is necessary to ensure that the seizure is legally authorized via consent, warrant, title, etc.

b) Think before you start and consider the order of extraction. Time is often the critical factor and there are cases when you may need to review some data manually (which may take just a few seconds) and only then make a decision which method to use.

   1) Learn as much as possible about the target device to be able to choose the most appropriate extraction method and tool(s). For many devices, several different methods exist, and they often complement each other. Evaluate all possible risks for each, and start with the safest method and work to the most comprehensive (which may be the most risky), if time allows. It may be helpful to have a logical acquisition even if full file system can be obtained.

   2) Keeping the device powered on and network isolated increases the chances of accessing the device, so please try to accommodate that. Note that some devices will turn on when plugged in, enabling them to be remotely wiped when they connect to network.

   3) Read the tools or vendors product guides and help files. They contain lots of useful information that will help you deciding the way forward with your seized device.

   4) If the device is not supported by your tools, contact the vendors and ask if there is a possible solution coming in future planned release.

   5) For eDiscovery cases be mindful of necessary upstream ingestion needs, and possible conversion(s) necessary from forensic tools. Keep in mind this may not only apply to eDiscovery investigations.

   6) Ideally, interact with the device as little as possible prior to carrying out any extraction, given the possibility of triggering database changes, altering logs and usage records. Ensure that interaction with the target device which may change settings or data is necessary, proportionate, and deliberate.

   7) Understand that exploits and specialized techniques are often required to recover data from smartphones. Be aware that some exploits will require the device to be restarted several times.

   8) Understand what each extraction method will obtain from the device. Read the tool support notes wherever possible.

   9) If data is not extracted, double-check all the connections and power. If still unsuccessful attempt to extract with another tool or another extraction method. Additionally, it may make sense to continue research and request support for devices that are not easily extracted from a vendor. If support is updated, additional extractions can then be obtained.

c) Obtain extractions from external components of the mobile device.

1) UICC (SIM) cards - remove after the extraction of the device and acquire separately using your tool of choice.

2) SD cards and the like should be acquired inside the device first and then should be removed, write-protected and acquired outside of the device, assuming time allows.

   — In the instance of adoptable or encrypted storage, it will need to be acquired through the device.

d) If legally authorized, extract cloud data.

1) Explain to the judge/attorneys/client why cloud data is just as relevant as the data on the device.

2) Social media and applications store data in the cloud that may not be accessible on the device.

3) Data recovered from a smartphone may lead to the discovery of possible cloud data and potential keys enabling access to cloud repositories.

4) Try to obtain warrant for data from Online providers if the data is relevant to your investigation.

5) Be aware that acquiring cloud data can raise alarms on the suspect's account. Act quickly once started.

e) If using an acquisition technique that is either new, unconventional or known to be unreliable, begin with a less invasive acquisition (such as a logical) so that in the event of a technique going wrong you are not left with nothing.

1) Understand if the tool or method is using native extraction methods.

2) If proprietary methods are used by the tools, make sure you understand how the tool functions and ask the vendor, where needed. When possible, test the methodology on an exemplar device before attempting the method on evidence. This may not always be possible.

3) Understand the configuration options that have been set for your extractions. (i.e. options settings that have been selected for the extraction, since this will impact not only how you acquire the data, but how you will review the data).

f) Obtain acknowledgment (preferably written) from the investigator in charge (ideally after consultation with prosecutors) and/or device owner if you believe there is a potential for device bricking, warranty invalidation, or physical damage to the device.

1) If a method has not been tested and publicly researched, try the method on a test device.

2) Obtain all extractions possible before attempting an extraction that could potentially damage a device. In some instances, it is advantageous to wait for an extraction method to be developed before attempting a methodology that could cause permanent physical damage to the device.

g) Use more than one tool or method to extract data that may be the focal point or key artifact of the crime. Understand that mobile log and system data (clock, etc.) constantly changes (user created artifacts should not change assuming the device is properly isolated), and two data extractions may not be exactly the same, nor necessary.

h) Always check which applications are installed on the device and determine the level of support your chosen tools offer.

1) Different levels of extraction and support exist depending on device, chipset, OS version, and application version.

2) Document the versions of tools used to ensure your report stands valid based upon the level of support for applications at the time of examining the evidence.

3) Be aware that processes such as application downgrade may be necessary to recover data, changing application versions and requiring restarts of the device.

4) Manual verification may be required to ensure all applications are accounted for.

D.2 Step 2: Process the data in more than one tool

a) Make sure you update your tools regularly. Be sure to read the release notes and check if the added support fixes a bug or provides the necessary support for your device.

   1) Updating tools and verifying the updates can take extended periods of time.

   2) When tools update, new bugs may be introduced. Make sure you verify against old versions or correlate artifacts to other tools and scripts to ensure data is being presented as expected.

b) Compare artifact results across more than one tool for anything that is considered essential evidence, whether exculpatory or inculpatory. These artifacts should be your priority for validation. Refer to D.3 step 3 when data is inconsistent. (Native application artifacts, contacts, calls, messages, browser, images).

   1) Make sure you know how the tool you are using will represent the data. Ask if you aren't sure if the tool is decoding and aggregating data or not.

   2) Be sure to check the source of the data if there are any discrepancies between tools.

   3) Different tools might parse different data types from same application.

   4) Most tools support import of extractions from other tools and are able to decode them. Use it to verify your primary tools findings, this can be done after the device is returned to confirm your findings.

   5) Verify the duplicated data between different tools and concatenate data from the tools to give the most accurate representation of the application data.

   6) Combine the results of different tools for tricky cases where different techniques can give additional results: carving, data evasion techniques, secure messaging that can leave remnants on the device, etc.

   7) Make sure you reference and refer to CASE and FORMOBILE guidance.

c) Learn the intricacies of your tools.

   1) Be familiar with how your tools deduplicate, filter and show results.

   2) Be familiar with how keyword searching works in your tools so that you understand the results.

   3) Be familiar with file formats and how they are represented by the tools.

4) Be familiar with the way your tool handles timestamps (default time zone, automatic conversion or not, etc.). Be aware that not all applications store all timestamps related to the device time. Mobile apps can utilize time offsets that are not related to UTC or the time zone of the device.

d) If available, know your tool's capabilities to parse unsupported application's data in a semi-automatic way, but understand the limitations and deep dive where necessary.

e) Make sure your tool settings are correct to recover deleted artifacts, parse unsupported applications, provide connections, etc. Make sure to verify after every update.

f) Compare the list of installed applications to the list of applications supported by the tool(s) you are using.

D.3 Step 3: Deep dive forensics: Where the push button stops and forensic examinations begin

a) Do the artifacts make sense?

1) Are they legible?

2) Does the timeframe correlate to the crime?

3) Are they contextual?

b) Compare to the source/device.

c) Do not forget removable media (UICC (SIM) and MicroSD Cards).

d) Manually verify key artifacts on the handset and photograph them or use a tool to photograph them – what is the time set to?

1) It is wise to note the time zone for where the device was derived and the time zone of your lab (i.e. Device seized in Eastern Time but sent to a lab in Central Time).

e) Leverage community tools and scripts.

f) Create sample files for keyword searching to ensure the tools are properly showing results.

g) Work closely with investigators on the case to help develop timelines and filters.

h) Take your time and research - always ask for help, when needed. Avoid reinventing the wheel without at least being aware existing research has already been done.

i) Make sure you understand all potential application data sources and data formats, so you can extract and analyse data unsupported by your toolset.

D.4 Step 4: Validation (Types: Visual, cross-tool, call detail records, CCTV, carving, replication)

a) Follow the source file for the artifact.

1) The source should be identified and reported if the artifact is important to your investigation.

2) The source file should be followed and verified for critical evidence.

3) The source should be provided for future validation/verification purposes.

4) On encrypted devices, tracing the data to its source hex data, is not trivial. Be prepared to answer questions on why decoded data cannot be viewed in hex viewer in the raw data dump. The same might apply on translation layers as well.

b) Examine databases, plists and relevant files in their native format or in a file viewer. This should be done after an extraction has been obtained.

c) Validate timestamps - are the timestamps shown in the device local time or UTC? Cross check for daylight saving time, time zone changes, time sync, etc.

1) Know where the timestamp comes from (handset vs mobile network).

2) Time zones can be tricky. Make sure you do not assume the user stayed in one location.

3) Make sure your tool is extracting relevant timestamps. Verify on the device, if necessary.

d) Don't fear Hex and know how to keyword search in Hex. If you are not familiar with looking at raw data with Hex viewers, find training that will further your understanding in this area. This applies to other structures found on mobile devices.

e) Reach out for support and to get your questions answered (there is no stupid question as the field is wide and changing rapidly). Be sure to use tool vendors support for any product-specific questions you have.

f) Reach out for community support.

g) Create test data to replicate your findings when the data may cause confusion. Even more important when cross time zone data exists, you are reporting on/researching a non-supported application or when you have found "the smoking gun" and want to be sure to corroborate using all available sources of information.

h) Take ample notes pertaining to validation steps taken.

i) Retain all research and documentation created should it be required to be provided or referred to at a later stage by a third party.

j) Ensure understanding of recovered data. Not all recovered data is user deleted.

NOTE For more information see https://www.nist.gov/publications/standardization-file-recovery-classification-and-authentication.

D.5 Step 5: Reporting/Sharing your findings

a) Highlight evidence relevant to the investigation.

b) Explain your findings - know and understand what you are reporting.

c) Consider data privacy concerns and subsets reports when passed to third parties.

d) Provide opinions only when required or legally permitted, if appropriate. And annotate or appropriately mark said comments as opinions.

e) Make sure you validate what you report.

   1) Even a quick validation works.

   2) If possible, have a colleague review the narrative report as a sanity check.

f) Take and keep notes to be prepared for testifying in court sometimes years after your investigation.

g) Set the expectations for your report.

h) eDiscovery clients may require specific output for their reports.

i) Where possible, share your findings within your organization or the Digital Forensics and Incident Response (DFIR) community via a blog or whitepaper.

D.6 Step 6: Education

a) Digital Forensics and Incident Response (DFIR) is a fast-moving field and what we practiced yesterday may differ from today (powering devices down and removing battery, removing UICC (SIM) cards vs keeping devices in a powered-on state. We need to adapt.).

b) Stay as current as possible.

   1) Take Training - Vendor training, Vendor-neutral training, self-training, in person or online/on-demand.

   2) Be familiar with all relevant case law in your jurisdiction and know when you are in 'setting new precedent' territory.

   3) Create a list of active researchers and follow them.

   4) If possible, share your own research with the community. If you have faced this issue/question, there is a good chance others will or already have.

   5) Participate in capture the flag (CTF) challenges where test data is provided to enhance your skills in the form of a game/challenge.

   6) Ask the DFIR community for help.

Annex E
(informative)

Forensic Information Report Template

E.1 General

This Annex provides an example for a Forensic Information Report Template.

E.2 Forensic Information Report

Date of Report:	Click or tap here to enter text.
Report provided by:	Click or tap here to enter text.
Organisation:	Click or tap here to enter text.
Contact Person:	Click or tap here to enter text.
Case Number:	Click or tap here to enter text.

Appendix to Report (if any):	Click or tap here to enter text.

The forensic information contained in this report is based on the information provided at the time and initial findings and / or assessment of a crime scene and exhibit(s). A record of all actions taken and tools applied during the forensic investigation is documented and preserved in this report in an open and accessible audit log trail and made available to the courts if used as evidence.

1 Case Information

1.1 General Information

Case Number:	Click or tap here to enter text.
Request Number:	Click or tap here to enter text.
Date of Request:	Click or tap here to enter text.
Contact Person:	Click or tap here to enter text.
Suspects:	Click or tap here to enter text.

1.2 Material to be examined

Material received from:	
Via:	Click or tap here to enter text.
Date Received:	Click or tap here to enter text.
Exhibit 1:	Click or tap here to enter text.
Exhibit 2:	Click or tap here to enter text.
Exhibit 3:	Click or tap here to enter text.

1.3 Requested Examination

Click or tap here to enter text concerning the requested examination case and questions to be answered.

1.4 Received Information

Click or tap here to enter text concerning the received information to the case.

2 Personnel and Competence

Reporting Officer:	Click or tap here to enter text.
Certification(s):	Click or tap here to enter text.
Training activity(s):	Click or tap here to enter text.
Qualification(s):	Click or tap here to enter text.
Expiry date of competences:	Click or tap here to enter text.

3 Initial Inspection Phase and Device Identification

	Exhibit 1	**Exhibit 2**	**Exhibit 3**
Date of inspection	Click or tap here to show calendar.	Click or tap here to show calendar.	Click or tap here to show calendar.
Time of inspection	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Initial inspection			
Mobile device model	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Unique permanent identifier / label	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Description of the device	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Packaging	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Accessories	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Damages	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Device manipulations	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
State of device (on / off)	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Flight mode (on / off)	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Connected to service (yes / no)	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Connected to Wi-Fi (yes / no)	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

	Exhibit 1	**Exhibit 2**	**Exhibit 3**
SIM present (yes / no)	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
ICCID	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Memory card present (yes / no)	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Battery charge level	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Running apps / software	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Known changes of state	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Vulnerable data	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Volatile data	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Expiration periods	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Lock codes / PIN	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Device Identification			
Serial Number	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Visual ID of IMEI	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
IMEI	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Phone number	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Operating system	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
OS version	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Firmware version	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Decision			
Device has to be examined immediately	☐	☐	☐
OR			
Device can be examined later	☐	☐	☐

Pictures of the exhibits:

4 Instruction and Authorisation

The handling of the device including the reporting was discussed in agreement with the requestor of the examination as per 1.3 Requested Examination and 1.4 Received Information. A forensic strategy was selected and authorised by the requestor.

5 Tools Selection

The following tools and methods were selected as appropriate for the requested examination and as per requirements of the case and used for inspection and acquisition of the devices' content:

Exhibit 1: Click or tap here to define device.			
Name of the tool / software	**Version of the tool / software**	**Use case / purpose**	**Is the tool validated?**
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	☐ Yes ☐ No
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	☐ Yes ☐ No
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	☐ Yes ☐ No

Exhibit 2: Click or tap here to define device.			
Name of the tool / software	**Version of the tool / software**	**Use case / purpose**	**Is the tool validated?**
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	☐ Yes ☐ No
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	☐ Yes ☐ No
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	☐ Yes ☐ No

Exhibit 3: Click or tap here to define device.			
Name of the tool / software	**Version of the tool / software**	**Use case / purpose**	**Is the tool validated?**
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	☐ Yes ☐ No
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	☐ Yes ☐ No
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	☐ Yes ☐ No

6 Acquisition and Accessing of Data

6.1 Acquisition Method and Process

Exhibit 1: Click or tap here to define device.		
Date of extraction process	Start time of extraction process	End time of extraction process

Click or tap here to show calendar.	Click or tap here to enter text.	Click or tap here to enter text.
Techniques to obtain data		
Connection(s) type Click or tap here to enter text.	Operator ID Click or tap here to enter text.	Agent required Click or tap here to enter text.
Extraction process used		
Click or tap here to enter text.		
Extraction errors		
Click or tap here to enter text.		
Specific hardware / platform system details		
Click or tap here to enter text.		

Exhibit 2: Click or tap here to define device.		
Date of extraction process Click or tap here to show calendar.	Start time of extraction process Click or tap here to enter text.	End time of extraction process Click or tap here to enter text.
Techniques to obtain data		
Connection(s) type Click or tap here to enter text.	Operator ID Click or tap here to enter text.	Agent required Click or tap here to enter text.
Extraction process used		
Click or tap here to enter text.		
Extraction errors		
Click or tap here to enter text.		
Specific hardware / platform system details		
Click or tap here to enter text.		

Exhibit 3: Click or tap here to define device.		
Date of extraction process Click or tap here to show calendar.	Start time of extraction process Click or tap here to enter text.	End time of extraction process Click or tap here to enter text.
Techniques to obtain data		
Connection(s) type Click or tap here to enter text.	Operator ID Click or tap here to enter text.	Agent required Click or tap here to enter text.
Extraction process used		

Click or tap here to enter text.
Extraction errors
Click or tap here to enter text.
Specific hardware / platform system details
Click or tap here to enter text.

6.2 Acquisition Results

Following results were obtained and material generated during the acquisition phase:

Exhibit 1: Click or tap here to define device.			
Physical image Click or tap here to enter text.	Logical image Click or tap here to enter text.	Volatile memory (RAM) Click or tap here to enter text.	Cloud server data Click or tap here to enter text.
Additional information (optional)			
Click or tap here to enter text.			

Exhibit 2: Click or tap here to define device.			
Physical image Click or tap here to enter text.	Logical image Click or tap here to enter text.	Volatile memory (RAM) Click or tap here to enter text.	Cloud server data Click or tap here to enter text.
Additional information (optional)			
Click or tap here to enter text.			

Exhibit 3: Click or tap here to define device.			
Physical image Click or tap here to enter text.	Logical image Click or tap here to enter text.	Volatile memory (RAM) Click or tap here to enter text.	Cloud server data Click or tap here to enter text.
Additional information (optional)			
Click or tap here to enter text.			

6.3 Decoding and Decryption

Exhibit 1: Click or tap here to define device.
Decoding performed on: Click or tap here to enter text.
Decoding / decryption errors

Click or tap here to enter text.
Decoding and decryption results
Click or tap here to enter text.

Exhibit 2: Click or tap here to define device.
Decoding performed on: Click or tap here to enter text.
Decoding / decryption errors
Click or tap here to enter text.
Decoding and decryption results
Click or tap here to enter text.

Exhibit 3: Click or tap here to define device.
Decoding performed on: Click or tap here to enter text.
Decoding / decryption errors
Click or tap here to enter text.
Decoding and decryption results
Click or tap here to enter text.

7 Analysis and Evidence

7.1 Analysis Methods

To accommodate the questions mentioned in 1.3, forensic analysis of the extracted data was done as described below:

Click or tap here to describe your analysis methods.

7.2 Analysis Results

All date and time information in this chapter is based on the local time zone of: Click or tap here to enter time zone.

	Exhibit 1	**Exhibit 2**	**Exhibit 3**
Origin of exhibit	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Usage	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Data Content	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

Access restrictions	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

7.2.1 Question 1 Examination Request

Click or tap here to describe your analysis results regarding question 1 of examination request.

7.2.2 Question 2 Examination Request

Click or tap here to describe your analysis results regarding question 2 of examination request.

7.2.3 Question 3 Examination Request

Click or tap here to describe your analysis results regarding question 3 of examination request.

7.2.4 Question 4 Examination Request

Click or tap here to describe your analysis results regarding question 4 of examination request.

7.3 Analysis Interpretation

7.3.1 Question 1 Examination Report

Click or tap here to describe your analysis interpretation regarding question 1 of examination request.

7.3.2 Question 2 Examination Report

Click or tap here to describe your analysis interpretation regarding question 2 of examination request.

7.3.3 Question 3 Examination Report

Click or tap here to describe your analysis interpretation regarding question 3 of examination request.

7.3.4 Question 4 Examination Report

Click or tap here to describe your analysis interpretation regarding question 4 of examination request.

7.4 Review and Validation

The methods used, processes and results in this report have been reviewed by:

Reviewer:	Click or tap here to enter text.
Certification(s):	Click or tap here to enter text.
Training activity(s):	Click or tap here to enter text.
Qualification(s):	Click or tap here to enter text.
Expiry date of competences:	Click or tap here to enter text.

The findings in the report were validated as follows:

Click or tap here to enter text.

Disclaimer for non-validated findings: *(optional, if needed)*

There is the possibility that there are data within the exhibit(s) which have not been extracted by the process(es) used. Further validation work of the process(es) used will not be undertaken unless the material is reasonably challenged by a party or if new information indicates that the material may be incomplete or inaccurate. Should this be the case, the issue shall be brought to the attention of the laboratory. The exhibit(s) may have to be resubmitted for validation work or even a further examination.

8 Additional Information

Click or tap here to enter text.

11 Conclusion

Click or tap here to enter text.

ANNEX: Glossary of Terms

Abbreviation / Term	Description

Annex F
(informative)

Governance implications of the use of Artificial Intelligence in mobile forensics

ISO/IEC 38507 provides guidance for members of the governing body of an organization to enable and govern the use of Artificial Intelligence (AI), in order to ensure their effective, efficient and acceptable use within the organization.

When using Artificial Intelligence in mobile forensics, the governance process should ensure the following:

— Human control and oversight shall be possible.

— The AI shall produce results that are accurate, reliable and reproducible and do not introduce inaccuracies or mistakes. This shall be verified.

— The AI shall be secure and threat resilient and a risk management approach shall be in place.

— The AI shall support the implementation of privacy requirements, data protection rules and good data governance.

— The AI and its functionality shall be as transparent as possible. Transparency includes elements such as traceability, explainability and explicability of the functioning and understandability and interpretability of the results.

— The AI shall provide guarantees in relation to supporting non-discrimination and fairness in the administration of justice, respecting the diversity present in society.

— The broader societal and environmental impact of the AI shall be considered.

— The AI shall allow and/or support measures of accountability, such as logging of events, actions and results and should enable an audit trail of what has happened.

Bibliography

[1] ISO/IEC 30121, *Information technology — Governance of digital forensic risk framework*

[2] ISO/IEC 38507, *Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations*

[3] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

[4] ISO 9001, *Quality management systems — Requirements*

[5] ISO 20387, *Biotechnology — Biobanking — General requirements for biobanking*

[6] Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings

[7] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters

[8] Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings

[9] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[11] INTERPOL. (2019). Global guidelines for digital forensics laboratories. https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

[12] INTERPOL. (2021). Guidelines for digital Forensics – First responders - Best practices for search and seizure of electronic and digital evidence https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

[13] NIST SP 800-72, *Guidelines on PDA Forensics*

[14] The Council of Europe. (2001). Convention on Cybercrime. Budapest: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[15] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Act (COM/2021/206 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[16] Validation and verification of software:
https://www.complianceonline.com/resources/software-verification-and-validation-overview-and-must-have-documents.html