This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800

FORMOBILE

• FROM MOBILE PHONES TO COURT •

From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices (FORMOBILE)

D3.1 Report on existing practices and standards

DOCUMENT INFORMATION

Deliverable number	D3.1	
Deliverable Name	Report on existing practices and standards	
Work Package	WP3	
Version	1	
Contractual Date of Delivery	*31.01.2020*	
Actual Date of Delivery	06.01.2020	
Type:	**R**: Document, report (excluding the periodic and final reports)	
Dissemination level:	**PU:** Public	
Classification level	Unclassified	
Status	Final	
Main author(s)	Dipl.-Ing. Dr. Karl Grün Dr. Annette Altenpohl Dr. Olga Radchuk Dipl.-Ing. Josef Winkler Dipl.-Ing. Jorg Nachbaur	ASI
Contributor(s)	Rune Nordvik Georgina Louise Humphries Caroline Schlossnickel-Lenz Stephen Collins Coert Klaver Julia Gerstenberg Natalia Jarmuzek Berta Santos	NMPS ZITiS HO NFI HSMW PPHS PJ LIF
Disclaimer	This document reflects only the author's views and not that of the Research Executive Agency. The Research Executive Agency is equally not responsible for any use that may be made of the information contained in this document. This document may not be reproduced or copied without permission. © Copyright in this document remains vested in the Project Partners.	

DOCUMENT CHANGE RECORD

Version	Date	Status	Author(s), reviewer	Description
0.1	22.10.2019	Draft	Author: Olga Radchuk (ASI)	Initial Draft
0.2	20.11.2019	Draft	Author: Olga Radchuk (ASI) Reviewers: LIF, NFI, NMPS, HSMW, PJ	Second draft Changes: • Reference list added • List of additional literature on mobile forensics added to the Annex • Section on non-formal standards removed from the Annex • Section on specific standards moved above the section on general standards • Lack of relevant standards for mobile forensics mentioned in the Conclusion • Abbreviations explained when used for the first time • Explanation on the key words search added to the Methodology • Formatting by HSMW
0.3	09.12.2019	Draft	Author: Olga Radchuk (ASI) Reviewers: ZITiS	Third draft Changes: • 5 ASTM Standards added to the tables 3 and 4
0.4	11.12.2019	Draft	Author: Olga Radchuk (ASI)	Final draft Changes: • Comments with three levels of mobile forensics addressed • Definitions of „first responders", „common laboratories" and „highly specialized laboratories" must be added • Relevance of the specific standards for the three levels of mobile forensics must be added • Title 3.2: removed „Partly relevant"
0.5	20.12.2019	Final Draft	Author: Olga Radchuk (ASI) Reviewers: ZITiS, NMPS	Comments addressed, definitions added
0.6	27.12.2019	Coordinator accepted	Christian Hummert (ZITiS)	Final Review
1.0	06.01.2020	Version submitted to EC	Julia Gerstenberg (HSMW)	Final version

Table of Contents

Executive summary

Development of standards for forensic science is important to enhance the reliability, transparency and confidence in forensic evidence. Standards harmonise work practices to facilitate forensic collaboration of different countries, as well as enable their facilities, in response to cross border investigations.

Standards also facilitate the exchange of forensic results, information and practices, including the sharing of databases, to ensure forensic services are fit for purpose. Standardisation of the processes of collection, analysis, interpretation and reporting of forensic evidence is critical to the validity of evidence. This is especially relevant for the area of mobile forensics, given the variety and rapid evolution of mobile devices, as well as the amount type and constantly growing complexity of data that can be obtained from them and used as evidence in the court.

Consistent and generally accepted standards for mobile forensics within the forensic community may benefit all users of the criminal justice system including members of the public as well as legal and forensic practitioners. Conformance to relevant standards for law enforcement and forensic agencies ensures that methodologies they apply are robust, verifiable and validated, and that training across jurisdictions or countries is consistent. This strongly impacts the quality of evidence and their acceptance by the courts.

It is therefore necessary to get an overview of the global landscape of standardisation in mobile forensics in order to take advantage of existing standardisation activities and to ensure a thorough understanding of the needs and requirements of the involved stakeholders.

The objective of the present document is to analyse the status of current standardisation in mobile forensics and to point towards actions that can increase its effectiveness, ensure inclusion of all relevant stakeholders and their interests and improve the quality of mobile forensics processes and procedures. Further objective of the document is to provide a baseline for subsequent analysis of the topics and processes in mobile forensics that are not addressed by current standardisation activities.

The report is structured around the main scopes of application of standards in the area of mobile forensics starting from collection of any mobile device during criminal investigation to the general requirements for digital investigation. It covers also all requirements that need to be addressed to

successfully and efficiently perform an investigation and present the evidence to law enforcement officials and in the court.

The report reviews relevant standards and outlines the scope of each in effort to help identify the gaps in the areas not properly addressed by ongoing standardisation activities. Gap analysis will be further addressed in the deliverable D3.2: Report on gaps in existing practices and standards, which will align the end users' requirements as identified within the WP1 with the existing standards.

1.Introduction

1.1. Report structure

The report represents the first Work Package 3 (WP3) delivery of the FORMOBILE (From Mobile Phones to Court – A complete FORensic investigation chain targeting MOBILE devices) research project and summarises all applicable standards and best practices that are currently used in mobile forensics.

The report is comprised of three main sections:

Deliverable context and role

This section provides an overview of the FORMOBILE project, purpose, objectives and scope of the WP3 and its role within the project. It also outlines the role of the present deliverable including target audience and document interdependencies.

Mobile forensics standardisation landscape

This section provides a general overview of the standardisation actions undertaken in the area of mobile forensics. It outlines the main standard development organisations and committees responsible for these standards, as well as national and international guidelines, regulations or recommendations used by Law Enforcement Agencies (LEAs). This section includes three sub-sections:

Specific standards in mobile forensics

This section provides information on the existing standards as well as standards under development that are applicable for steps or phases during investigations involving mobile devices (e.g. device seizure and preservation, data acquisition and analysis etc.). The requirements for these steps vary from case to case depending on the device or a type of investigation.

General standards in mobile forensics

This section provides information on the existing standards as well as standards under development that describe general procedures and requirements in mobile forensics. They can be applicable to any investigation (e.g. documentation, reporting etc.) and define the requirements that go above and beyond the investigative process (e.g. characteristics of tools used, training of the personnel, collaboration with external service providers etc.).

Non-formal standards for mobile forensics (general and specific)

This section provides information on the manuals, guidelines and other documents that are relevant for the project but do not belong to formal standards. They address various processes within the investigations involving mobile devices and are considered good practices in the area of mobile forensics.

Conclusion

This section contains a summary of the findings from the previous sections and provides a background for the deliverables: D3.2 Gap Report that identifies all gaps in existing practices and standards for mobile forensics, and D3.3 CEN Workshop Agreement (CWA) on mobile forensics that will be the fundament of the novel European mobile forensic standard.

1.2. Objectives of the report

The first aim of this report is to provide a systematic overview of the standardisation landscape, including national and international activities as well as other efforts relevant to the area of mobile forensics (e.g. guidelines, regulations, recommendations etc.).

The second aim of the report is to provide background information for future gap identification and analysis: detection of the gaps between the end user requirements on mobile forensics (D1.1: report that summarises all common problems and needs of the European LEAs in the field of mobile forensics) and the current standardisation landscape.

This report together with the gap analysis will serve as a cornerstone for the CWA, produced in the end of the project.

1.3. Scope of the report

The report identifies national and international standards, guidelines and regulations relevant to the digital investigation process in general and to mobile forensics. This will help set a direction for future standardisation activities.

1.4. Target audience

This report is developed for the FORMOBILE consortium members.

1.5. Methodology

Initial literature review on the topic of digital investigation was conducted by Austrian Standards International (ASI). It identified the broad areas of focus that were further classified according to their scope of application as defined below (general and specific standards).

The content of this report is based on a combination of resources, derived from standards databases of The European Committee for Standardization (CEN), The European Committee for Electrotechnical Standardization (CENELEC), The International Organization for Standardization (ISO), The National Institute of Standards and Technology (NIST), American Society for Testing and Materials International (ASTM) and The European Telecommunications Standards Institute (ETSI), as well as contributions from the consortium partners.

The database search was performed using the following keywords: forensic, investigation, crime, evidence, mobile device, digital investigation. All identified standards were checked for their relevance to the project.

1.6. Areas of focus

The relevant standards are structured according to their scope of application. They are divided into two main groups: standards relevant for steps or phases in the digital investigation process which may be of particular relevance to mobile forensics (specific standards) and standards that outline general requirements for digital investigation (general standards).

Both groups are divided into the following sub-categories that reflect the requirements of digital investigation as well as the steps necessary to follow the chain of custody:

General standards:

1. Terms and definitions
2. Strategy
    2.1. General Digital Forensic Strategy
    2.2. Forensic Readiness Plan for any specific case
3. Requirements for the personnel involved (working on the three levels of mobile forensics, relevant for the project: first responders, common labs, highly specialized labs)
4. Requirements for tools and processes (including management of information)
5. Education and training
6. Involvement of external service providers

Specific standards:

1. Device seizure
2. Data preservation
3. Data acquisition
4. Data examination and analysis
5. Documentation of all investigation steps
6. Reporting
7. Evaluation and sharing of information with other LEAs

1.7. Definitions and abbreviations

1.7.1. Definitions

Standardisation

Standardisation is an activity of establishing, with regard to actual or potential problems, provisions for common and repeated use, aimed at the achievement of the optimum degree of order in a given context [1].

NOTE 1: In particular, the activity consists of the processes of formulating, issuing and implementing standards.

NOTE 2: Important benefits of standardisation are improvement of the suitability of products, processes and services for their intended purposes, prevention of barriers to trade and facilitation of technological cooperation.

Standards can be developed by National, Regional (e.g. European), or International standardisation organisations, by a group of companies (industrial standards, e.g. USB, IEEE) or by companies itself (company standard).

As defined in Regulation (EU) 1025/2012 [2], Article 2a "standard" means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory.

Regulations

A regulation is a document providing binding legislative rules, that is adopted by an authority [3]. For example, when the EU intends to make sure that there are common safeguards on goods imported from outside the EU, it issues a regulation that all imports need to accompany with.

NOTE 1: Regulations are adopted by the European Parliament and the European Council.

Directives

A directive is a legislative act that sets out a goal that all EU countries must achieve [3].

However, it is up to the individual countries to devise their own laws on how to reach these goals. One example is the EU Consumer Rights Directive [4], which strengthen rights for consumers across the EU by eliminating hidden charges and costs on the internet and thus extending the period under which consumers can withdraw from a sales contract.

Common Laboratories

Typically, the laboratory available in a Police District or smaller unit.

First Responders

Personnel that identify and seize the mobile device on the crime scene. Could be normal police officers, but also mobile forensic experts.

Highly Specialized Laboratories

A more advanced laboratory with advanced equipment to carry out specialized tests or perform advanced tasks.

1.7.2. Abbreviations

The following table represents an overview of abbreviations used in connections with standardisation and legislation.

Table 1. Abbreviations

Abbreviation	Description
ASTM	American Society for Testing and Materials
AWI	Approved new Work Item
CD	Committee draft
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CWA	CEN and/or CENELEC Workshop Agreement; standardisation deliverable from a CEN and/or CENELEC workshop
EN	Standard adopted by CEN, CENELEC and/or ETSI
ESO	European Standardisation organisation; The ESO's are CEN, CENELEC and ETSI
ETSI	European Telecommunications Standards Institute
IEC	International Electrotechnical Commission / standards developed by IEC

Abbreviation	Description
IEEE	Institute of Electrical and Electronics Engineers / standards developed by IEEE
ISO	International Standardisation Organisation / standards developed by ISO
LEA	Law Enforcement Agency
NIST	National Institute of Standards and Technology
NSB	National Standardisation Body
SDO	Standards Development Organisation
SR	Special report developed by ESO
TC	Technical committee
TR	Technical report developed by SDO
TS	Technical specification developed by SDO
WD	Working Draft developed by SDO
WG	Working Group to which work is allocated by a Technical committee based on an approved new work item and drafting standardisation deliverables
WP	Work Package

1.8. Key words

CWA, digital investigation, LEA, standardisation, standard, mobile forensics

2. Deliverable context and role

2.1. FORMOBILE overview (abstract)

Mobile devices, especially smartphones represent a unique challenge for law enforcement. Criminal offenders use phones to communicate, coordinate, organise and execute criminal actions. This is especially true for organised crime and terrorist organisations. This development provides new challenges for criminal prosecution and it is vital to empower law enforcement to access the data stored on mobile devices to use it as court evidence in a trustworthy and reliable manner.

The overarching objective of FORMOBILE is to establish a complete end to end forensic investigation chain, targeting mobile devices. To achieve this goal three objectives will be pursued. Novel tools shall be developed that include the acquisition of previously unavailable mobile data, unlocking mobile devices, as well as the decoding and analysis of mobile data. Based on the definition of requirements of law enforcement and legal and ethical issues a new mobile forensics standard shall be developed. With the developments of the new standard and the new tools, training for police and criminal prosecution will be established, providing the end users with the latest knowledge in a novel and an innovative curriculum to ensure a quality standard of investigations.

The European Union (EU) has developed as a Security Union, building on the European Agenda on Security [5]. This aims to ensure that people live in an area of freedom, security and justice, without internal frontiers. To strengthen digital forensics in the context of criminal investigations is crucial to achieve this vision. FORMOBILE contributes to the fight against virtually all forms of crime. This is because mobile devices are widely used in crimes, especially in the arrangement of conspiracies. Yet, there are crimes more closely related to mobile devices; this includes child abuse and emerging forms of cybercrime. To fight crime effectively, law enforcement must be empowered to access all evidence stored on mobile devices.

2.2. FORMOBILE Consortium

Table 2. FORMOBILE Consortium

No.	Name of participant organisation	Short name	Type	Country
1	Mittweida University of Applied Sciences (coordinator)	HSMW	Uni	DE
2	Netherlands Forensic Institute	NFI	Public Body	NL
3	Micro Systemation AB	MSAB	SME	SE
4	Austrian Standards International	ASI	NSB	AT
5	Central Office for Information Technology in the Security Sector	ZITiS	Public Body	DE
6	Home Office	HO	LEA	UK
7	Spanish National Police	ESMIR	LEA	ES
8	The Polish Police Regional Headquarters in Poznan	KWPP	LEA	PL
9	Malta Police Force	MPF	LEA	MT
10	Portuguese Judicial Police	PJ	LEA	PT
11	Delft University of Technology	TUD	Uni	NL
12	University of Patras	UPat	Uni	EL
13	Foundation for Research and Technology Hellas	FORTH	Research Org.	EL
14	Norwegian Ministry of Justice and Public Safety	NMPS	Public Body	NO
15	Law and Internet Foundation	LIF	NGO	BG
16	Polish Platform for Homeland Security	PPHS	NGO	PL
17	time.lex	TLX	SME	BE
18	Strane Innovation	SI	SME	FR
19	Kyrgyz State Technical University named after I. Razzakov	KSTU	Uni	KG

2.3. WP3: Development of the forensic standard for mobile phones

2.3.1. Objectives of the work package and tasks

The overarching objective of the WP3 is development of a CWA that can be immediately applied by LEAs and serve as a forerunner for a new European standard in mobile forensics.

The objective of the Task 3.1 (Identification of existing practices and standards) is to provide an overview of current standardisation activities in the area of IT security in general with a special focus on mobile forensics, including existing standards, standards under development, as well as regulations, guidelines and directives. The present report fulfils this objective and represents the deliverable D3.1 Report on existing practices and standards.

The objective of the Task 3.2 (Gap analysis of existing practices and standards) is to reveal the gaps between the end user requirements (common problems and needs of the European LEAs in the field of mobile forensics) and the content of the standards in order to integrate the missing information into the CWA.

The objective of the Task 3.3 (Definition of the European mobile forensic standard) is to develop and publish the CWA that addresses the project needs and can be immediately integrated by end users (LEAs) into their chain of custody.

2.3.2. Role of WP3 in the FORMOBILE context

The CWA will be based on the requirements derived from the work performed in WP1 (Definition of law enforcement agencies requirements and application tests), WP2 (Legal and ethical issues) and WP7 (Training for law enforcement agencies) as well as key findings from stakeholder reviews, input and background material/information.

WP1: The collected data from the WP1 questionnaire will contain the end user requirements from LEAs covering the requirements of all three layers of forensic laboratories. They will be compared against the existing standards in order to identify the gaps.

WP2: The CWA will be validated in the WP2 to ensure its legal compliance.

WP7: The CWA will provide a background for the methodology of the training, developed within the WP7. It will serve as best practice guidelines in mobile forensics for all three levels (first responders, common labs, highly specialized labs) and ensure compliance of the training with the requirements of the end users.

2.3.3. Deliverable interdependencies

This document is the first out of three deliverables within the WP3 and serves as the basis for the development of the CWA. It will provide the background for the following two deliverables (D3.2 Gap Report summarising gaps in existing practices and standards for mobile forensics and D3.3 CEN Workshop Agreement on mobile forensics).

3. Mobile forensics standardisation landscape

The search identified a total of 56 standards from the European and international standardisation bodies as listed in the tables 3 and 4 in the following sections.

Of the 56 standards, 41 are international standards jointly developed by ISO and IEC, 14 European standards developed by ETSI and 1 national standard developed by NIST in the USA, as well as several of non-formal standards (e.g. guidelines, directives, policies etc.).

The research demonstrates that ISO (on an international level) and IEC (on European level) have been very active in developing a large part of the standards relevant for mobile forensics. The committees working on such standards include ISO/IEC JTC 1 Information technology, ISO/TC 272 Forensic sciences and ISO/CASCO Committee on conformity assessment. Many NSBs in Europe adopt these standards in lieu of developing their own.

On the European level, standardization in digital investigation is being conducted at ETSI in the area of Lawful Interception, covering cloud services, interfaces, wireless internet access, architecture of IP networks to name a few. Despite the extensive work conducted so far, the standards issued by ETSI are only partly relevant for the particular area of digital investigation and do not address the issues the FORMOBILE project is working on.

In the USA, NIST Computer Security Resource Center (CSRC) works on cybersecurity and information security. It has published Guidelines on Mobile Device Forensics that also lay within the scope of this report.

The next two sections consider standards identified in analysis and outline the relevance and scope of each in relation to mobile forensics. The additional literature on mobile forensics is listed in the Annex.

3.1. Specific standards for digital (mobile) forensics

This section covers the standards, specific for various aspects of digital (mobile) forensics procedures.

Table 3. Key specific standards

No.	Title	Scope
1	NIST Special Publication 800-101, Guidelines on Mobile Device Forensics	The guide provides basic information on mobile forensics tools and the preservation, acquisition, examination and analysis, and reporting of digital evidence present on mobile devices.
2	ISO 21043-2:2018 Forensic sciences — Part 2: Recognition, recording, collecting, transport and storage of items	Specifies requirements for the forensic process focusing on recognition, recording, collection, transport and storage of items of potential forensic value. It includes requirements for the assessment and examination of scenes but is also applicable to activities that occur within the facility. It also includes quality requirements.
3	ISO/CD 21043-3 Forensic Sciences — Part 3: Analysis	Under development
4	ISO/CD 21043-4 Forensic Sciences — Part 4: Interpretation	Under development
5	ISO/CD 21043-5 Forensic Sciences — Part 5: Reporting	Under development
6	ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence	Provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value. Provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organisations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions. Provides guidance for the following devices and circumstances: • Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto optical disks, data devices with similar functions; • Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards; • Mobile navigation systems;

		• Digital still and video cameras (including CCTV); • Standard computer with network connections; • Networks based on TCP/IP and other digital protocols, and Devices with similar functions as above.
7	ISO/IEC 27038:2014 Information technology — Security techniques — Specification for digital redaction	Specifies characteristics of techniques for performing digital redaction on digital documents. It also specifies requirements for software redaction tools and methods of testing that digital redaction has been securely completed.
8	ISO/IEC 27042:2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence	Provides guidance on the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility, and repeatability. It encapsulates best practice for selection, design, and implementation of analytical processes and recording of sufficient information to allow such processes to be subjected to independent scrutiny when required. It provides guidance on appropriate mechanisms for demonstrating proficiency and competence of the investigative team.
9	ISO/IEC 27050 Information technology — Security techniques — Electronic discovery	Group of standards (27050-1 to 27050-3) dealing with Electronic Discovery: • Part 1: Overview and concepts • Part 2: Guidance for governance and management of electronic discovery • Part 3: Code of practice for electronic discovery Guides discovering pertinent Electronically Stored Information (ESI) or data by one or more parties involved in an investigation or litigation, or similar proceeding. The group: • provides an overview of electronic discovery; • defines related terms and describes the concepts; • identifies other relevant standards (e.g. ISO/IEC 27037) and how they relate to, and interact with, electronic discovery activities; provides requirements and guidance on activities in electronic discovery, including, but not limited to, identification, preservation, collection, processing, review, analysis and production of ESI.
10	ASTM E 2825 Standard Guide for Forensic Digital Image Processing	Provides digital image processing guidelines to ensure the production of quality forensic imagery for use as evidence in a court of law. Briefly describes advantages, disadvantages, and potential limitations of each major process.

3.2. General standards for IT security

Many standards in mobile forensics may apply to several areas of focus, as outlined in the section 1.6 This section seeks to provide an overview of general standards relevant for forensic strategy, terms and definitions, requirements for personnel and its education and training, tools and processes, as well as external service providers.

Table 4. Key general standards

No.	Title	Scope	Relevance
1	ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories	Specifies the general requirements for the competence, impartiality and consistent operation of laboratories. It is applicable to all organisations performing laboratory activities, regardless of the number of personnel.	Highly accepted standard in traditional forensic disciplines and required by law for DNA and fingerprint investigations in many EU countries. Partly adopted and useful for digital forensics.
2	ISO 21043-1:2018 Forensic sciences — Part 1: Terms and definitions	Defines terms used in the ISO 21043 series of standards.	Relevant
3	ISO/IEC 30121:2015 Information technology — Governance of digital forensic risk framework	Provides a framework for Governing bodies of organisations (including owners, board members, directors, partners, senior executives, or similar) on the best way to prepare an organisation for digital investigations before they occur. This International Standard applies to the development of strategic processes (and decisions) relating to the retention, availability, access, and cost effectiveness of digital evidence disclosure.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
4	ISO/IEC 24745:2011 Information technology — Security techniques — Biometric information protection	Provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. Additionally, it provides requirements and guidelines for the secure and privacy-compliant management and processing of biometric information. It specifies: • analysis of the threats to and countermeasures inherent in a biometric and biometric system application models;	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics

No.	Title	Scope	Relevance
		• security requirements for secure binding between a biometric reference and an identity reference; • biometric system application models with different scenarios for the storage of biometric references and comparison; guidance on the protection of an individual's privacy during the processing of biometric information.	
5	ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements	Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
6	ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls	Provides guidelines for organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment(s). It is designed to be used by organisations that intend to: • select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001; • implement commonly accepted information security controls; develop their own information security management guidelines	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
7	ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance	Provides explanation and guidance on ISO/IEC 27001:2013	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
8	ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring,	Provides guidelines intended to assist organisations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001:2013, 9.1. It establishes: • the monitoring and measurement of information security performance;	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics

No.	Title	Scope	Relevance
	measurement, analysis and evaluation	• the monitoring and measurement of the effectiveness of an information security management system (ISMS) including its processes and controls; the analysis and evaluation of the results of monitoring and measurement	
9	ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management	Provides guidelines for information security risk management. This document supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
10	ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems	Specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021-1 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
11	ISO/IEC TS 27008:2019 Information technology — Security techniques — Guidelines for the assessment of information security controls	Provides guidance on reviewing and assessing the implementation and operation of information security controls, including the technical assessment of information system controls, in compliance with an organisation's established information security requirements including technical compliance against assessment criteria based on the information security requirements established by the organisation. Offers guidance on how to review and assess information security controls being managed through an Information Security Management System specified by ISO/IEC 27001.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
12	ISO/IEC 27009:2016 Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements	Defines the requirements for the use of ISO/IEC 27001 in any specific sector (field, application area or market sector). It explains how to include requirements additional to those in ISO/IEC 27001, how to refine any of the ISO/IEC 27001 requirements, and how to include controls or control sets in addition to ISO/IEC 27001:2013, Annex A. It ensures that additional or refined requirements are not in conflict with the requirements in ISO/IEC 27001.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
13	ISO/IEC 27010:2015	Provides controls and guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organisational and inter-	Only relevant as general IT standard. Not really relevant

No.	Title	Scope	Relevance
	Information technology — Security techniques — Information security management for inter-sector and inter-organisational communications	sector communications. It provides guidelines and general principles on how the specified requirements can be met using established messaging and other technical methods. Is applicable to all forms of exchange and sharing of sensitive information, both public and private, nationally and internationally, within the same industry or market sector or between sectors.	for LEA's that deal with digital forensics
14	ISO/IEC 27013:2015 Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	Provides guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for those organisations that are intending to either • implement ISO/IEC 27001 when ISO/IEC 20000-1 is already implemented, or vice versa, • implement both ISO/IEC 27001 and ISO/IEC 20000-1 together, or integrate existing management systems based on ISO/IEC 27001 and ISO/IEC 20000-1.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
15	ISO/IEC 27014:2013 Information technology — Security techniques — Governance of information security	Provides guidance on concepts and principles for the governance of information security, by which organisations can evaluate, direct, monitor and communicate the information security related activities within the organisation.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
16	ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	Provides guidelines for information security controls applicable to the provision and use of cloud services by providing: • additional implementation guidance for relevant controls specified in ISO/IEC 27002; • additional controls with implementation guidance that specifically relate to cloud services. Provides controls and implementation guidance for both cloud service providers and cloud service customers.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
17	ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public	Establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics

No.	Title	Scope	Relevance
	clouds acting as PII processors	Specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment(s) of a provider of public cloud services.	
18	ISO/IEC 27021:2017 Information technology — Security techniques — Competence requirements for information security management systems professionals	Specifies the requirements of competence for ISMS professionals leading or involved in establishing, implementing, maintaining and continually improving one or more information security management system processes that conforms to ISO/IEC 27001.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
19	ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity	Describes the concepts and principles of information and communication technology (ICT) readiness for business continuity and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organisation's ICT readiness to ensure business continuity. It applies to any organisation (private, governmental, and non-governmental, irrespective of size) developing its ICT readiness for business continuity program (IRBC), and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions. It also enables an organisation to measure performance parameters that correlate to its IRBC in a consistent and recognised manner.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
20	ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity	Provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection (CIIP). It covers the baseline security practices for stakeholders in the Cyberspace. It provides: • an overview of Cybersecurity, • an explanation of the relationship between Cybersecurity and other types of security, • a definition of stakeholders and a description of their roles in Cybersecurity, • guidance for addressing common Cybersecurity issues, and a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics

No.	Title	Scope	Relevance
21	ISO/IEC 27033 Information technology — Security techniques — Network security	Group of standards (27033-1 to 27033-6) dealing with Network Security: • Part 1: Overview and concepts • Part 3: Reference networking scenarios — Threats, design techniques and control issues • Part 4: Securing communications between networks using security gateways • Part 5: Securing communications across networks using Virtual Private Networks (VPNs) • Part 6: Securing wireless IP network access It is relevant to anyone involved in owning, operating or using a network.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
22	ISO/IEC 27034 Information technology — Security techniques — Application security	Group of standards (27034-1 to 27034-7) dealing with Application Security: • Part 1: Overview and concepts • Part 2: Organisation normative framework • Part 3: Application security management process • Part 5: Protocols and application security controls data structure • Part 6: Case studies • Part 7: Assurance prediction framework Is applicable to in-house developed applications, applications acquired from third parties, and where the development or the operation of the application is outsourced.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
23	ISO/IEC 27035 Information technology — Security techniques — Information security incident management	Group of standards (27035-1 to 27035-2) dealing with Information security incident management: • Part 1: Principles of incident management • Part 2: Guidelines to plan and prepare for incident response Applicable to all organisations, regardless of type, size or nature. Organisations can adjust the guidance given in this part of ISO/IEC 27035 according to their type, size and nature of business in relation to the information security risk situation.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
24	ISO/IEC 27040:2015 Information technology — Security techniques — Storage security	Provides detailed technical guidance on how organisations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes:	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics

No.	Title	Scope	Relevance
		• the security of devices and media, • the security of management activities related to the devices and media, • the security of applications and services, security relevant to end-users during the lifetime of devices and media and after end of use.	
25	ISO/IEC 27041:2015 Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method	Provides guidance on mechanisms for ensuring that methods and processes used in the investigation of information security incidents are "fit for purpose". It encapsulates best practice on defining requirements, describing methods, and providing evidence that implementations of methods can be shown to satisfy requirements. It aims to: • provide guidance on the capture and analysis of functional and non-functional requirements relating to an Information Security (IS) incident investigation, • give guidance on the use of validation as a means of assuring suitability of processes involved in the investigation, • provide guidance on assessing the levels of validation required and the evidence required from a validation exercise, give guidance on how external testing and documentation can be incorporated in the validation process.	Relevant for LEA's who do analysis of acquired data. For instance, the 'I have been hacked' defence in Child Exploitation cases. The methods used by the LEA need to be proved 'fit for purpose'.
26	ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes	Provides guidelines based on idealised models for common incident investigation processes across various incident investigation scenarios involving digital evidence. This includes processes from pre-incident preparation through investigation closure, as well as any general advice and caveats on such processes. The guidelines describe processes and principles applicable to various kinds of investigations, including, but not limited to, unauthorised access, data corruption, system crashes, or corporate breaches of information security, as well as any other digital investigation.	Relevant
27	ISO/IEC TS 29003:2018 Information technology — Security techniques — Identity proofing	Provides guidelines for the identity proofing of a person, specifies levels of identity proofing, and requirements to achieve these levels. Is applicable to identity management systems.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
28	ISO/IEC 29100:2011	Provides a privacy framework which: • specifies a common privacy terminology;	Only relevant as general IT standard. Not really relevant

No.	Title	Scope	Relevance
	Information technology — Security techniques — Privacy framework	• defines the actors and their roles in processing personally identifiable information (PII); • describes privacy safeguarding considerations; and • provides references to known privacy principles for information technology. Is applicable to natural persons and organisations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.	for LEA's that deal with digital forensics
29	ISO/IEC 29101:2018 Information technology — Security techniques — Privacy architecture framework	Defines a privacy architecture framework that: • specifies concerns for ICT systems that process PII; • lists components for the implementation of such systems; • provides architectural views contextualising these components. Is applicable to entities involved in specifying, procuring, architecting, designing, testing, maintaining, administering and operating ICT systems that process PII.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
30	ISO/IEC 29151:2017 Information technology — Security techniques — Code of practice for personally identifiable information protection	Establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of personally identifiable information (PII). In particular, it specifies guidelines based on ISO/IEC 27002, taking into consideration the requirements for processing PII that may be applicable within the context of an organisation's information security risk environment(s).	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
31	ISO/IEC 29191:2012 Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication	Provides a framework and establishes requirements for partially anonymous, partially unlinkable authentication.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
32	ISO/IEC TS 30104:2015 Information Technology — Security Techniques — Physical Security Attacks, Mitigation Techniques and Security Requirements	Addresses the following topics: • a survey of physical security attacks directed against different types of hardware embodiments including a description of known physical attacks, ranging from simple attacks that require minimal skill or resources, to complex attacks that require trained, technical people and considerable resources;	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics

No.	Title	Scope	Relevance
		• guidance on the principles, best practices and techniques for the design of tamper protection mechanisms and methods for the mitigation of those attacks; • guidance on the evaluation or testing of hardware tamper protection mechanisms and references to current standards and test programs that address hardware tamper evaluation and testing. Applicable for product developers designing hardware security implementations and testing or evaluation of the final product.	
33	ISO/IEC 30107 Information technology — Biometric presentation attack detection — Part 1: Framework	Group of standards (30107-1 to 30107-3) dealing with presentation attack detection (PAD): • Part 1: Framework • Part 2: Data formats • Part 3: Testing and reporting • Part 4: Profile for testing of mobile devices (under development) Biometric data can be easily obtained directly from a person, online, or through existing databases and then used to create spoofs (or fakes) to mount an attack. The presentation of a biometric spoof (e.g. a facial image or video of a person on a tablet or a fake silicone or gelatine fingerprint) to a biometric sensor can be detected by methods broadly referred to as PAD. The group: • provides a foundation for PAD through defining terms and establishing a framework through which presentation attack events can be specified and detected so that they can be categorised, detailed and communicated for subsequent decision making and performance assessment activities; • defines data formats for conveying the mechanism used in biometric PAD and for conveying the results of presentation attack detection methods; establishes principles and methods for performance assessment of PAD mechanisms as well as reporting of testing results from evaluations of PAD mechanisms.	Only relevant as general IT standard. Not really relevant for LEA's that deal with digital forensics
34	ETSI TS 101 331 V1.5.1 (2017-03) Lawful Interception (LI); Requirements of Law Enforcement Agencies	Gives guidance for lawful interception of telecommunications in the area of co-operation by network operators, access providers, and service providers. It provides a set of requirements relating to handover interfaces for the interception by law enforcement and state security agencies. Requirements regarding telecommunications	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on

No.	Title	Scope	Relevance
		services provided from areas outside national boundaries are not fully developed yet and therefore only some preliminary requirements have been annexed for information. The present document describes the requirements from a Law Enforcement Agency's (LEA's) point of view.	lawfully seized (mobile) devices.
35	ETSI ES 201 158 V1.2.1 (2002-02) Telecommunications security; Lawful Interception (LI); Requirements for network functions	The present document describes the general requirements of Network Operators (NWOs), Service Providers (SvPs) and Access Providers (APs) relating to the provision of lawful interception, with particular reference to the Handover Interface (HI). The provision of lawful interception is a requirement of national law, which is usually mandatory. From time to time, a NWO and/or SvP and/or AP will be required, according to a lawful authorisation, to make available results of interception, relating to specific identities, to a specific LEA.	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on lawfully seized (mobile) devices.
36	ETSI TS 101 671 V2.15.1 (2006-11) Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic	The present document is step 3 of a three-step approach to describe a generic Handover Interface (HI) for the provision of lawful interception from a Network Operator, an Access Provider or a Service Provider (NWO/AP/SvP) to the Law Enforcement Agencies (LEAs). The provision of lawful interception is a requirement of national law, which is usually mandatory for the operation of any telecommunication service. Step 1 contains the requirements for lawful interception from a users' (LEAs) point of view and is published in TS 101 331. Step 2 describes the derived network functions and the general architecture (or functional model) and is published in ES 201 158. The present document specifies: • the generic flow of information as well as the procedures and information elements, which are applicable to any future telecommunication network or service; • the network/service specific protocols relating to the provision of lawful interception at the Handover Interface (HI), for the following networks/services: switched circuit and packet data	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on lawfully seized (mobile) devices.
37	ETSI TR 102 519 V1.2.1 (2014-02) Lawful Interception (LI);	Provides an overview of the issues and challenges regarding the Lawful Interception of Public Internet Access by means of Wireless LAN technology as defined in the IEEE 802.11 [i.2] specification and possible approaches for dealing with these issues, considering different architectures and business models.	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on

No.	Title	Scope	Relevance
	Lawful Interception of public Wireless LAN Internet Access		lawfully seized (mobile) devices.
38	ETSI TS 102 656 V1.3.1 (2017-03) Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data	Gives guidance for the delivery and associated issues of retained data of telecommunications and subscribers. It provides a set of requirements relating to handover interfaces for the retained traffic data and subscriber data by law enforcement and other authorised requesting authorities. The present document describes the requirements from a Law Enforcement Agency's (LEA's) point of view.	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on lawfully seized (mobile) devices.
39	ETSI TS 102 657 V1.23.1 (2019-08) Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data	Is based on requirements from ETSI TS 102 656 [2]. The present document contains handover requirements and a handover specification for the data that is identified in national legislations on Retained Data. The present document considers both the requesting of retained data and the delivery of the results. It defines an electronic interface.	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on lawfully seized (mobile) devices.
40	ETSI TR 103 657 V1.2.1 (2011-12) Lawful Interception (LI); Retained data handling; System Architecture and Internal Interfaces	Elaborates on RD system architecture and assigns and describes internal interfaces to specific services and functional entities on the CSP (Communications Service Provider) side. It provides guidance on implementation issues that CSPs have to deal with. The present document contains: • A reference model in the network operator and communication service provider domain. • A high-level description of Internal Network Functions and Interfaces. • Application of the reference model to some typical CSPs.	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on lawfully seized (mobile) devices.
41	ETSI TR 101 567 V1.1.1 (2016-01) Lawful Interception (LI); Cloud/Virtual Services for Lawful Interception (LI) and Retained Data (RD)	Provides an overview of Cloud/virtual services and studies. This includes Lawful Interception (LI) and Retained Data (RD) aspects of these services in the converged Cloud/virtual service environment, the challenges and obstacles of complying with those obligations, what implementations can be achieved under existing ETSI LI standards and what new work may be required to achieve needed Lawful Interception capabilities.	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on lawfully seized (mobile) devices.

No.	Title	Scope	Relevance
42	ETSI TR 103 690 V1.1.1 (2012-02) Lawful Interception (LI); eWarrant Interface	The present document presents a high-level description of an interface mechanism - the eWarrant Interface - for receipt of requests for measures producing real-time or stored information by an issuing authority possessing lawful authorisation to initiate such a request. The eWarrant Interface is a generic, extensible interface intended to be fully compatible with all existing kinds of requests for these purposes - as well as support future ones, including local requirements and languages or character sets.	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on lawfully seized (mobile) devices.
43	ETSI TS 103 120 V1.3.1 (2019-05) Lawful Interception (LI); Interface for warrant information	Defines an electronic interface between two systems for the exchange of information relating to the establishment and management of lawful required action, typically Lawful Interception. Typically, this interface would be used between a Communications Service Provider on one side and a Government or Law Enforcement Agency who is entitled to request a lawful action on the other side. The present document is a specific and detailed example of one particular Warranty interface for eWarrants.	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on lawfully seized (mobile) devices.
44	ETSI TS 103 280 V2.3.1 (2019-04) Lawful Interception (LI); Dictionary for common parameters	Defines a dictionary of parameters that are commonly used in multiple TC LI specifications. Aside from defining a dictionary, the present document aims to provide technical means for other specifications to use.	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on lawfully seized (mobile) devices.
45	ETSI TR 103 304 V1.1.1 (2016-07) CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services	Proposes several scenarios focusing on today's ICT and develops an analysis of possible threats to Personally Identifiable Information (PII) in mobile and cloud-based services. It also presents technical challenges and needs derived from regulatory aspects (lawful interceptions). It consolidates a general framework, in line with regulation and international standards, where technical solutions for PII protection can be plugged into.	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on lawfully seized (mobile) devices.
46	ETSI TS 102 677 V1.1.1 (2019-07) Lawful Interception (LI); Dynamic Triggering of Interception	Defines an architecture for the lawful interception of dynamically allocated flows in a secondary communications domain, triggered by the activity of permanent identities in a primary domain. Dynamic triggering as defined in the present document is intended to be able to handle a service that is handled by more than one CSP or network (for example one CSP handling the communication set up and another CSP handling the content exchange).	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on lawfully seized (mobile) devices.

No.	Title	Scope	Relevance
47	ETSI TS 101 158 V1.3.1 (2014-02) Telecommunications security; Lawful Interception (LI); Requirements for network functions	Describes the general requirements of Network Operators (NWOs), Service Providers (SvPs) and Access Providers (APs) relating to the provision of lawful interception, with reference to the Handover Interface (HI).	Only relevant in the field of Lawful Interception. Not really relevant for LEA's that deal with digital forensics on lawfully seized (mobile) devices.
48	ASTM E 2678 Standard Guide for Education and Training in Computer Forensics	Provides information to improve and advance computer forensics through the development of model curricula consistent with other forensic science programs.	Only relevant as general computer forensics training standard. Not really relevant for LEA's that deal with digital forensics
49	ASTM E 2917 Standard Practice for Forensic Science Practitioner Training, Continuing Education, and Professional Development Programs	Provides foundational requirements for the training, continuing education, and professional development of forensic science practitioners to include training criteria toward competency, documentation, and implementation of training, and continuous professional development. This information is intended for forensic science service providers to help establish a training framework with program structure and content; for forensic science practitioners as they acquire and maintain their knowledge, skills, and abilities (KSAs); and for training programs to manage and support the continuous development of their employees. This practice outlines minimum training criteria and provides general information, approaches, and resources for all disciplines.	Only relevant as general forensic science training standard.
50	ASTM E 3046 Standard Guide for Core Competencies for Mobile Phone Forensics	Identifies the core competencies necessary for the handling and forensic processing of mobile cellular (cell) telephones (phones). It applies to both first responders and laboratory personnel. Different levels of cell phone analysis are discussed as well as the basic skills required at each of these levels.	Relevant
51	ASTM E2916 Standard Terminology for Digital and Multimedia Evidence Examination	Represents a compilation of terms and corresponding definitions used in the examination of digital and multimedia evidence to include the areas of computer forensics, image analysis, video analysis, forensic audio, and facial identification.	Relevant

3.3. Non-formal standards for mobile forensics (general and specific)

This section covers the non-formal standards, including guidelines, manuals, best practices and other documents.

Table 5. Key non-formal standards (general and specific)

No.	Title	Scope
1	SHAFFER, John S. **Cell phone forensics in a correctional setting: Guidebook**. Washington, DC: Corrections Technology Center of Excellence, National Law Enforcement and Corrections Technology Center, 2014.	The Guidebook was developed for the National Institute of Justice (NIJ). It provides correctional administrators with a brief, yet comprehensive and informative, view of cell phone forensic technologies. It reviews the evolving role of cell phone forensics in correctional institutions and presents issues to consider when acquiring and implementing these technologies. It also addresses the opportunities and challenges involved in selecting technologies and implementing them in correctional settings.
2	SOMMER, Peter. **Digital Evidence. Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers**. The Information Assurance Advisory Council (IAAC), 2012.	The purpose of this guide is to make directors, managers and their professional advisors aware of the issues involved in collecting, analysing and presenting digital evidence. It covers the following topics among others: • The need for digital evidence and forensic readiness planning • Risk scenarios • Good evidence • E-disclosure
3	**Best Practice Manual for the Forensic Examination of Digital Technology**. European Network of Forensic Science Institutes (ENFSI), 2015	The Manual aims to provide a framework for procedures, quality principles, training processes and approaches to the forensic examination. The aim is to provide a bridge between the requirements of international and local regulatory standards, and the actual implementation within each member's laboratory environment.
4	WILLIAMS, Janet. **ACPO good practice guide for digital evidence**. Metropolitan Police Service, Association of chief police officers, GB, 2012.	The purpose of this document is to provide guidance not only to assist law enforcement but for all that assists in investigating cyber security incidents and crime. It covers the following topics: • The principles of digital evidence • Plan • Capture • Analyse • Present • General topics

No.	Title	Scope
5	**Guidance: Method validation in digital forensics**. Forensic Science Regulator, 2016	Provides guidance and advice on validation stages and how the process can be applied within the digital forensic sciences.
6	**Global Guidelines for Digital Forensics Laboratories**. Interpol, 2019	The document outlines the procedures for establishing and managing a Digital Forensics Laboratory (DFL) and provides technical guidelines for managing and processing electronic evidence. These Guidelines should be seen as a template document that can be used by countries when considering developing their digital forensics capability. The advice given is intended to be used at both the strategic and tactical levels, in accordance with national legislation, practice, and procedures.
7	**Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition**. Scientific Working Group on Digital Evidence (SWGDE), 2019	This document provides best practices for the collection, preservation, and acquisition of evidence from mobile devices. The collection and preservation of data from mobile devices is performed in the field, as well as the lab. Increasingly, field personnel are also performing acquisitions. This document provides best practices for the three functions that are likely to be needed by field personnel. The intended audience is personnel qualified to collect, preserve, or acquire digital evidence.
8	**SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence**. Scientific Working Group on Digital Evidence (SWGDE), 2010	The purpose of document is to recommend minimum testing requirements for commonly used forensic tools and procedures. Organisations may exceed these minimums based on operational needs or policies. Testing is often referred to as validation or verification testing. This document addresses testing to evaluate whether a tool or procedure performs as expected and to understand the limitations of tools.
9	**Best Practices for Collection of Damaged Mobile Devices**. Scientific Working Group on Digital Evidence (SWGDE), 2016	The purpose of this document is to describe the best practices for the collection of damaged mobile devices (e.g., smart phones, tablets, feature phones).
10	**Best Practices for Digital Evidence Acquisition from Cloud Service Providers**. Scientific Working Group on Digital Evidence (SWGDE), 2019	The purpose of this document is to provide guidance for acquiring digital evidence from a cloud service provider.
11	**Recommended Guidelines for Validation Testing**. Scientific Working Group on Digital Evidence (SWGDE), 2014	The purpose of this document is to provide guidance for validation testing, required to demonstrate that examination tools (hardware and software), techniques and procedures are suitable for their intended purpose.
12	**Best Practices for Chip-Off**. Scientific Working Group on Digital Evidence (SWGDE), 2016	This document describes best practices for acquiring data contained within a device by removing the flash memory chip from the printed circuit board (PCB) and directly reading the data from the chip.
13	**Best Practices for Mobile Phone Forensics**. Scientific Working Group on Digital Evidence (SWGDE), 2016	The purpose of this document is to describe the best practices for mobile phone forensics. This document provides basic information on the logical and physical

No.	Title	Scope
		acquisition of mobile phones. The intended audience is either examiners in a lab setting or first responders who encounter mobile phones in the field.
14	**Core Competencies for Mobile Phone Forensics**. Scientific Working Group on Digital Evidence (SWGDE), 2016	This document provides an outline of the knowledge and abilities all practitioners of mobile phone forensics should possess. The following elements provide a basis for training and testing programs. This basis is suitable for certification, competency and proficiency testing.
15	**Best Practices for Examining Mobile Phones Using JTAG**. Scientific Working Group on Digital Evidence (SWGDE), 2015	The purpose of this document is to describe best practices for acquiring data contained within a mobile device using a Joint Test Action Group (JTAG) boundary scan technique as defined in IEEE 1149.1-2013, IEEE Standard for Test Access Port and Boundary-Scan Architecture.
16	**Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges**. Cybercrime Division, Directorate General of Human Rights and Rule of Law Council of Europe, 2014	The purpose of the Guide is to provide support and guidance to criminal justice professionals on how to identify and handle electronic evidence in such ways that will ensure its authenticity for later admissibility in court.
17	**NIST Special Publication 800-202 (Quick Start Guide for Populating Mobile Test Devices)**	This guide provides procedures for documenting and populating various data elements typically found within the contents of a mobile device, e.g., mobile phone, tablet, etc. The guide discusses techniques and considerations for preparing the internal memory of a mobile device for use in testing a mobile forensic tool.
18	**Smart Phone Tool Specification (NIST)**	This paper defines requirements for mobile device applications capable of acquiring data from 51 smart phones operating over a Global System for Mobile communication (GSM) network and a 52 Code Division Multiple Access (CDMA) network, and test methods used to determine whether a specific tool meets the requirements for producing measurable results.

4.Conclusions

Standardisation is a very important tool to ensure that the evidence acquired during the investigative process are valid and accepted during the trial. It is of special importance for the procedures in mobile forensic due to very quick development of mobile devices and related technologies. Standardisation allows for quick adjustment of the necessary forensic procedures and in many cases saves the time needed to obtain evidence.

This deliverable within the WP3 Task 3.1 provides an overview of existing standards and the ongoing standardisation work in a wide area of relevance to the FORMOBILE project. We identified 61 standards, among them – 41 international standards developed by ISO and IEC, 14 European standards developed by ETSI, 5 international standards developed by ASTM International and 1 national standard developed by NIST in the USA. Of them, 51 standards belong to the general area of focus, whereas only 10 standards describe procedures in mobile forensics. In addition, we identified 18 non-formal standards (e.g. guidelines, directives, policies etc.). It must be emphasized that despite the relatively large number of standards, relevant for IT security, there is a lack of specific standards for mobile forensics in general and especially in the areas, relevant for the FORMOBILE project. However, adherence to the standards during all steps of investigation in this field is of critical importance for the evidences being regarded as reliable and accepted for the court, and development of such standard is of utmost importance to secure the successful outcome of the investigation.

This overview provides a baseline for the next deliverable within the WP3, D3.2: Report on gaps in existing practices and standards. While the list of identified standards is not exhaustive, this report can serve as a reference on the key standards in mobile forensics for the consortium members as well as for any expert working in the area of digital investigation.

5.References

1. https://www.iso.org/standard/39976.html
2. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:0033:EN:PDF
3. https://europa.eu/european-union/eu-law/legal-acts_en
4. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0083
5. https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en

List of Tables

Annex. Additional literature on mobile forensics

No.	Title	Authors ISBN
1	Android Security Internals: An In-Depth Guide to Android's Security Architecture 1st Edition	Nikolay Elenkov 9781593275815
2	Learning Android Forensics	Oleg Skulkin, Donnie Tindall, Rohit Tamma 978-1-78913-101-7
3	Learning iOS Forensics - Second Edition	Mattia Epifani, Pasquale Stirparo 1785882082
4	Mobile Forensic Investigations	Lee Reiber 978-1-260-13509-1
5	Practical Mobile Forensics	Rohit Tamma, Oleg Skulkin, Heather Mahalik, Satish Bommisetty 978-1-78883-919-8