INTERNATIONAL STANDARD

ISO/IEC 27037

First edition
2012-10-15

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

Reference number
ISO/IEC 27037:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27037 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

This International Standard provides guidelines for specific activities in handling potential digital evidence; these processes are: identification, collection, acquisition and preservation of potential digital evidence. These processes are required in an investigation that is designed to maintain the integrity of the digital evidence – an acceptable methodology in obtaining digital evidence that will contribute to its admissibility in legal and disciplinary actions as well as other required instances. This International Standard also provides general guidelines for the collection of non-digital evidence that may be helpful in the analysis stage of the potential digital evidence.

This International Standard intends to provide guidance to those individuals responsible for the identification, collection, acquisition and preservation of potential digital evidence. These individuals include Digital Evidence First Responders (DEFRs), Digital Evidence Specialists (DESs), incident response specialists and forensic laboratory managers. This International Standard ensures that responsible individuals manage potential digital evidence in practical ways that are acceptable worldwide, with the objective to facilitate investigation involving digital devices and digital evidence in a systematic and impartial manner while preserving its integrity and authenticity.

This International Standard also intends to inform decision-makers who need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyze and present potential digital evidence. It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

The potential digital evidence referred to in this International Standard may be sourced from different types of digital devices, networks, databases, etc. It refers to data that is already in a digital format. This International Standard does not attempt to cover the conversion of analog data into digital format.

Due to the fragility of digital evidence, it is necessary to carry out an acceptable methodology to ensure the integrity and authenticity of the potential digital evidence. This International Standard does not mandate the use of particular tools or methods. Key components that provide credibility in the investigation are the methodology applied during the process, and individuals qualified in performing the tasks specified in the methodology. This International Standard does not address the methodology for legal proceedings, disciplinary procedures and other related actions in handling potential digital evidence that are outside the scope of identification, collection, acquisition and preservation.

Application of this International Standard requires compliance with national laws, rules and regulations. It should not replace specific legal requirements of any jurisdiction. Instead, it may serve as a practical guideline for any DEFR or DES in investigations involving potential digital evidence. It does not extend to the analysis of digital evidence and it does not replace jurisdiction-specific requirements that pertain to matters such as admissibility, evidential weighting, relevance and other judicially controlled limitations on the use of potential digital evidence in courts of law. This International Standard may assist in the facilitation of potential digital evidence exchange between jurisdictions. In order to maintain the integrity of the digital evidence, users of this International Standard are required to adapt and amend the procedures described in this International Standard in accordance with the specific jurisdiction's legal requirements for evidence.

Although this International Standard does not include forensic readiness, adequate forensic readiness can largely support the identification, collection, acquisition, and preservation process of digital evidence. Forensic readiness is the achievement of an appropriate level of capability by an organization in order for it to be able to identify, collect, acquire, preserve, protect and analyze digital evidence. Whereas the processes and activities described in this International Standard are essentially reactive measures used to investigate an incident after it occurred, forensic readiness is a proactive process of attempting to plan for such events.

This International Standard complements ISO/IEC 27001 and ISO/IEC 27002, and in particular the control requirements concerning potential digital evidence acquisition by providing additional implementation guidance. In addition, this International Standard will have applications in contexts independent of ISO/IEC 27001 and ISO/IEC 27002. This International Standard should be read in conjunction with other standards related to digital evidence and the investigation of information security incidents.

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

1 Scope

This International Standard provides guidelines for specific activities in handling digital evidence, which are identification, collection, acquisition and preservation of digital evidence that may be of evidential value. This International Standard provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.

This International Standard gives guidance for the following devices and/or functions that are used in various 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.

NOTE 1 The above list of devices is an indicative list and not exhaustive.

NOTE 2 Circumstances include the above devices that exist in various forms. For example, an automotive system may include mobile navigation system, data storage and sensory system.

2 Normative reference

The following referenced documents are indispensable for the application 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/TR 15801, *Document management — Information stored electronically — Recommendations for trustworthiness and reliability*

ISO/IEC 17020, *Conformity assessment — Requirements for the operation of various types of bodies performing inspection*

ISO/IEC 17025:2005, *General requirements for the competence of testing and calibration laboratories*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions in ISO/IEC 27000, ISO/IEC 17020, ISO/IEC 17025 and ISO/TR 15801, as well as the following apply.

3.1
acquisition
process of creating a copy of data within a defined set

NOTE The product of an acquisition is a potential digital evidence copy.

3.2
allocated space
area on digital media, including primary memory, which is in use for the storage of data, including metadata

3.3
collection
process of gathering the physical items that contain potential digital evidence

3.4
digital device
electronic equipment used to process or store digital data

3.5
digital evidence
information or data, stored or transmitted in binary form that may be relied on as evidence

3.6
digital evidence copy
copy of the digital evidence that has been produced to maintain the reliability of the evidence by including both the digital evidence and verification means where the method of verifying it can be either embedded in or independent from the tools used in doing the verification

3.7
Digital Evidence First Responder
DEFR
individual who is authorized, trained and qualified to act first at an incident scene in performing digital evidence collection and acquisition with the responsibility for handling that evidence

NOTE Authority, training and qualification are the expected requirements necessary to produce reliable digital evidence, but individual circumstances may result in an individual not adhering to all three requirements. In this case, the local law, organizational policy and individual circumstances should be considered.

3.8
Digital Evidence Specialist
DES
individual who can carry out the tasks of a DEFR and has specialized knowledge, skills and abilities to handle a wide range of technical issues

NOTE A DES may have additional niche skills, for example, network acquisition, RAM acquisition, operating system software or Mainframe knowledge.

3.9
digital storage medium
device on which digital data may be recorded

[Adapted from ISO/IEC 10027:1990]

3.10
evidence preservation facility
secure environment or a location where collected or acquired evidence is stored

NOTE An evidence preservation facility should not be exposed to magnetic fields, dust, vibration, moisture or any other environmental elements (such as extreme temperature or humidity) that may damage the potential digital evidence within the facility.

3.11
hash value
string of bits which is the output of a hash-function

[ISO/IEC 10118-1:2000]

3.12
identification
process involving the search for, recognition and documentation of potential digital evidence

3.13
imaging
process of creating a bitwise copy of digital storage media

NOTE The bitwise copy is also called a physical copy.

EXAMPLE When imaging a hard drive, the DEFR would also copy data that has been deleted.

3.14
peripheral
device attached to a digital device in order to expand its functionality

3.15
preservation
process to maintain and safeguard the integrity and/or original condition of the potential digital evidence

3.16
reliability
property of consistent intended behaviour and results

[ISO/IEC 27000:2009]

3.17
repeatability
property of a process conducted to get the same test results on the same testing environment (same computer, hard drive, mode of operation, etc.)

3.18
reproducibility
property of a process to get the same test results on a different testing environment (different computer, hard drive, operator, etc.)

3.19
spoliation
act of making or allowing change(s) to the potential digital evidence that diminishes its evidential value

3.20
system time
time generated by the system clock and used by the operating system, not the time computed by the operating system

3.21
tampering
act of deliberately making or allowing change(s) to digital evidence (i.e. intended or purposeful spoliation)

3.22
timestamp
time variant parameter which denotes a point in time with respect to a common time reference

[ISO/IEC 11770-1:1996]

3.23
unallocated space
area on digital media, including primary memory, which has not been allocated by the operating system, and which is available for the storage of data, including metadata

3.24
validation
confirmation, through the provision of objective proof, that the requirements for a specific intended use or application have been fulfilled

[ISO/IEC 27004:2009]

3.25
verification function
function which is used to verify that two sets of data are identical

NOTE 1 No two non-identical data sets should produce an identical match from a verification function.

NOTE 2 Verification functions are commonly implemented using hash functions such as MD5, SHA1, etc., but other methods may be used.

3.26
volatile data
data that is especially prone to change and can be easily modified

NOTE A change can be switching off the power or passing through a magnetic field. Volatile data also includes data that changes as the system state changes. Examples include data stored in RAM and dynamic IP addresses.

4 Abbreviated terms

AVI	Audio Video Interleave
CCTV	Closed Circuit Television
CD	Compact Disk
DNA	Deoxyribonucleic Acid
DEFR	Digital Evidence First Responder
DES	Digital Evidence Specialist
DVD	Digital Video/Versatile Disk

ESN	Electronic Serial Number
GPS	Global Positioning System
GSM	Global System for Mobile Communication
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
ISIRT	Information Security Incident Response Team
LAN	Local Area Network
MD5	Message-Digest Algorithm 5
MP3	MPEG Audio Layer 3
MPEG	Moving Picture Experts Group
NAS	Network Attached Storage
PDA	Personal Digital Assistant
PED	Personal Electronic Device
PIN	Personal Identification Number
PUK	PIN Unlock Key
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RFID	Radio Frequency Identification
SAN	Storage Area Network
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
USB	Universal Serial Bus
UPS	Uninterruptible Power Supply
USIM	Universal Subscriber Identity Module
UV	Ultraviolet
Wi-Fi	Wireless Fidelity