ISO/IEC 27037

Search

● Search this site

Home | ISO27k standards | FREE ISO27k Forum | FREE ISO27k Toolkit | FREE ISO27k FAQ | DONATE!

ISO/IEC 27000
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27006
ISO/IEC 27007
ISO/IEC TS 27008
ISO/IEC 27010
ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC 27019
ISO/IEC 27021
ISO/IEC TS 27022
ISO/IEC TR 27024
ISO/IEC TS 27028
ISO/IEC TR 27029
ISO/IEC 27031
ISO/IEC 27032
ISO/IEC 27033
ISO/IEC 27034
ISO/IEC 27035

< Previous standard ^ Up a level ^ Next standard >

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

Abstract

> *"ISO/IEC 27037:2012 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. It 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. ISO/IEC 27037:2012 gives 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. The above list of devices is an indicative list and not exhaustive."*
>
> *[Source: ISO/IEC 27037:2012]*

Introduction

This standard provides guidance on identifying, gathering/collecting/acquiring, handling and protecting/ preserving digital forensic evidence *i.e.* "digital data that may be of evidential value" for use in court.

The fundamental purpose of the ISO27k digital forensics standards is to promote good practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organisations and jurisdictions may well retain certain methods, processes and controls, it is hoped that standardization will (eventually) lead to the adoption of similar if not identical approaches internationally, making it easier to compare,

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

combine and contrast the results of such investigations even when performed by different people or organisations and potentially across different jurisdictions.

One of the most critical issues in forensic investigations is the acquisition and preservation of evidence in such a way as to ensure its integrity. As with conventional physical evidence, it is crucial for the first and subsequent responders (defined as “Digital Evidence First Responders” and “Digital Evidence Specialists”) to maintain the chain of custody of all digital forensic evidence, ensuring that it is gathered and protected through structured processes that are acceptable to the courts. More than simply providing integrity, the processes must provide assurance that nothing untoward can have occurred. This requires that a defined baseline level of information security controls is met or exceeded.

Digital forensic evidence can come from any electronic storage or communications media such as cellphones, computers, iPod's, video game consoles *etc*. By its nature, digital forensic evidence is fragile - it can be easily damaged or altered due to improper handling, whether by accident or on purpose.

Prior to the release of ISO/IEC 27037, there were no globally-accepted standards on acquiring digital evidence, the first step in the process. Police have developed their own national guidelines and procedures for the acquisition and protection of electronic evidence. However, this creates issues when cross-border crimes are committed since digital forensic evidence acquired in one country may need to be presented in the courts of another. Tainted evidence that *may* have been acquired or protected without the requisite level of security may be legally inadmissible.

Scope and purpose

The standard provides detailed guidance on the identification, collection and/or acquisition, marking, storage, transport and preservation of electronic evidence, particularly to maintain its integrity. It defines and describes the processes through which evidence is recognized and identified, documentation of the crime scene, collection and preservation of the evidence, and the packaging and transportation of evidence.

The scope covers ‘traditional’ IT systems and media rather than vehicle systems, cloud computing *etc.* The guidance is aimed primarily at first responders.

Every country has its own unique legislative system. A crime committed in one jurisdiction may not even be regarded as a crime in another. The challenge is to harmonize processes across borders such that cybercriminals can be prosecuted accordingly. Therefore, a means to allow and facilitate the exchange and use of reliable evidence (*i.e.* an international standard on acquiring digital evidence) is required.

“Digital evidence”, meaning information from digital devices to be presented in court, is interpreted differently in different jurisdictions. For the widest applicability, the standard will avoid using jurisdiction-specific terminology. It will not cover analysis of digital evidence, nor its admissibility, weight, relevance *etc*. It also will not mandate the use of particular tools or methods.

Structure and content

Status of the standard

The *first* edition was published in **2012** and confirmed unchanged in 2018.

Related standards

This standard concerns the initial *capturing* of digital evidence.

ISO/IEC 27041 offers guidance on the *assurance* aspects of digital forensics *e.g.* ensuring that the appropriate methods and tools are used properly.

ISO/IEC 27042 covers what happens *after* digital evidence has been collected *i.e.* its analysis and interpretation.

ISO/IEC 27043 covers the broader *incident investigation* activities, within which forensics usually occur.

ISO/IEC 27050 (in 4 parts) concerns *electronic discovery* which is pretty much what the other standards cover.

British Standard BS 10008:2008 “Evidential weight and legal admissibility of electronic information.

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799

Specification.” may also be of interest.

Personal comments

I don’t understand why SC 27 maintains several distinct forensics standards, covering different aspects of forensics, when they are in reality complementary parts of the same process. A properly structured multi-part standard would make more sense to me, with an overview part explaining how the jigsaw pieces fit together.

< Previous standard ^ Up a level ^ Next standard >