< Previous standard ^ Up a level ^ Next standard >

ISO/IEC 27043:2015 — Information technology — Security techniques — **Incident investigation principles and processes** *(first edition)*

Abstract

"ISO/IEC 27043:2015 provides guidelines based on idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence. ..."

[Source: ISO/IEC 27043:2015]

Introduction

The fundamental purpose of the digital forensics standards ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042, ISO/IEC 27043 and ISO/IEC 27050 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 standardisation will (eventually) lead to the adoption of similar if not identical approaches internationally, making it easier to compare, combine and contrast the results of such investigations even when performed by different people or organisations and potentially across different jurisdictions.

Scope and purpose

The standard concerns the principles behind, and the forensic processes involved in, investigating incidents.

Status of the standard

The *first* edition was published in **2015** and confirmed unchanged in 2020.

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

Related standards

ISO/IEC 27037 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.

This standard 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 "Evidential weight and legal admissibility of electronically stored information (ESI), Specification." may also be of interest.

Personal comments

I am puzzled why SC 27 publishes and maintains several distinct forensics standards covering different aspects of forensics, when they are in reality complementary parts of the same process. A multi-part standard would make more sense to me, with a "part 1" overview explaining how the jigsaw pieces fit together.

< Previous standard ^ Up a level ^ Next standard >

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