DEIF
High-Efficiency DEIF Savings

ISO/IEC 27042

ISO/IEC 27042:2015 — Information technology — Security techniques — **Guidelines for the analysis and interpretation of digital evidence** *(first edition)*

Abstract

"ISO/IEC 27042:2015 provides guidance on the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility, and repeatability. ..."

[Source: ISO/IEC 27042:2015]

Introduction

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 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.

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

Aside from the standard evidential cont[illegible]ntaining the chain of custody, scrupulous documentation *etc.*), the standard emphasizes the integrity [illegible] analytical and interpretational processes such that different investigators working on the same digital evidence ought to come up with essentially the same results - or at least any differences should be traceable to choices they made along the way. Given the volume, variety and complexity of digital evidence these days, that's quite a challenge, hence the drive for standardization, good practices, common terminology and sound, rational approaches.

The standard touches on issues such as the selection and use of forensic tools, plus proficiency and competency of the investigators.

Status of the standard

The *first* edition was published in **2015** and confirmed unchanged in 2021.

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.

This standard 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 "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. I understand the decision not to integrate this content into ISO/IEC 27037 but a multi-part standard would make more sense to me personally, with an overview part explaining how the jigsaw pieces fit together.

The editors have rejected such a proposal, claiming that it was considered and rejected when the forensics standards development projects were launched. So, sorry valued customers, it seems you will have to buy and correlate multiple standards to accumulate the complete forensics suite in ISO27k.

< Previous standard ^ Up a level ^ Next standard >

Copyright © 2025 IsecT Ltd. Contact us re Intellectual Property Rights