INTERNATIONAL STANDARD

ISO/IEC 27042

First edition
2015-06-15

Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'analyse et l'interprétation de preuves numériques

Reference number
ISO/IEC 27042:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

Introduction

General

This International Standard provides guidance on the conduct of the analysis and interpretation of potential digital evidence in order to identify and evaluate digital evidence which can be used to aid understanding of an incident. The exact nature of the data and information making up the potential digital evidence will depend on the nature of the incident and the digital evidence sources involved in that incident.

When using this International Standard, the user assumes that the guidance given in ISO/IEC 27035-2 and ISO/IEC 27037:2012 has been followed and that all processes used are compatible with the guidance given in ISO/IEC 27043:2015 and ISO/IEC 27041[1].

Relationship to other standards

This International Standard is intended to complement other standards and documents which give guidance on the investigation of, and preparation to investigate, information security incidents. It is not a comprehensive guide, but lays down certain fundamental principles which are intended to ensure that tools, techniques, and methods can be selected appropriately and shown to be fit for purpose should the need arise.

This International Standard also intends to inform decision-makers that need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyse, 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.

This International Standard describes part of a comprehensive investigative process which includes, but is not limited to, the following topic areas:

- incident management, including preparation, and planning for investigations;
- handling of digital evidence;
- use of, and issues caused by, redaction;
- intrusion prevention and detection systems, including information which can be obtained from these systems;
- security of storage, including sanitization of storage;
- ensuring that investigative methods are fit for purpose;
- carrying out analysis and interpretation of digital evidence;
- understanding principles and processes of digital evidence investigations;
- security incident event management, including derivation of evidence from systems involved in security incident event management;
- relationship between electronic discovery and other investigative methods, as well as the use of electronic discovery techniques in other investigations;
- governance of investigations, including forensic investigations.

These topic areas are addressed, in part, by the following ISO/IEC standards.

- ISO/IEC 27037

[1] To be published.