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.

This International Standard describes the means by which those involved in the early stages of an investigation, including initial response, can assure that sufficient potential digital evidence is captured to allow the investigation to proceed appropriately.

— ISO/IEC 27038

Some documents can contain information that must not be disclosed to some communities. Modified documents can be released to these communities after an appropriate processing of the original document. The process of removing information that is not to be disclosed is called "redaction".

The digital redaction of documents is a relatively new area of document management practice, raising unique issues and potential risks. Where digital documents are redacted, removed information must not be recoverable. Hence, care needs to be taken so that redacted information is permanently removed from the digital document (e.g. it must not be simply hidden within non-displayable portions of the document).

ISO/IEC 27038 specifies methods for digital redaction of digital documents. It also specifies requirements for software that can be used for redaction.

— ISO/IEC 27040:2015

This International Standard provides detailed technical guidance on how organizations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use.

Security mechanisms like encryption and sanitization can affect one's ability to investigate by introducing obfuscation mechanisms. They have to be considered prior to and during the conduct of an investigation. They can also be important in ensuring that storage of evidential material during and after an investigation is adequately prepared and secured.

— ISO/IEC 27041

It is important that methods and processes deployed during an investigation can be shown to be appropriate. This International Standard provides guidance on how to provide assurance that methods and processes meet the requirements of the investigation and have been appropriately tested.

— ISO/IEC 27043:2015

This International Standard defines the key common principles and processes underlying the investigation of incidents and provides a framework model for all stages of investigations.

The following ISO/IEC projects also address, in part, the topic areas identified above and can lead to the publication of relevant standards at some time after the publications of this International Standard.

— ISO/IEC 27035 (all parts)

This is a three-part standard that provides organizations with a structured and planned approach to the management of security incident management. It is composed of

— ISO/IEC 27035-1

This part presents basic concepts and phases of information security incident management. It combines these concepts with principles in a structured approach to detecting, reporting, assessing, responding, and applying lessons learned.

— ISO/IEC 27035-2

This part presents the concepts to plan and prepare for incident response. The concepts, including incident management policy and plan, incident response team establishment, and awareness briefing and training, are based on the plan and prepare phase of the model presented in ISO/IEC 27035-1. This part also covers the “Lessons Learned” phase of the model.

— ISO/IEC 27035-3

This part includes staff responsibilities and practical incident response activities across the organization. Particular focus is given to the incident response team activities such including monitoring, detection, analysis, and response activities for the collected data or security events.

— ISO/IEC 27044[2)]

This provides guidelines to organizations in preparing to deploy security information and event management processes/systems. In particular, it addresses the selection, deployment, and operations of SIEM. It intends specifically to offer assistance in satisfying requirements of ISO/IEC 27001 regarding the implementation of procedures and other controls capable of enabling prompt detection and response to security incidents, to execute monitoring, and review procedures to properly identify attempted and successful security breaches and incidents.

— ISO/IEC 27050 (all parts)[3)]

This addresses activities in electronic discovery, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of electronically stored information (ESI). In addition, it provides guidance on measures, spanning from initial creation of ESI through its final disposition, which an organization can undertake to mitigate risk and expense should electronic discovery become an issue. It is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities. It is important to note that this guidance is not intended to contradict or supersede local jurisdictional laws and regulations.

Electronic discovery often serves as a driver for investigations, as well as evidence acquisition and handling activities. In addition, the sensitivity and criticality of the data sometimes necessitate protections like storage security to guard against data breaches.

— ISO/IEC 30121:2015

This International Standard provides a framework for governing bodies of organizations (including owners, board members, directors, partners, senior executives, or similar) on the best way to prepare an organization for digital investigations before they occur. This International Standard applies to the development of strategic processes (and decisions) relating to the retention, availability, access, and cost effectiveness of digital evidence disclosure. This International Standard is applicable to all types and sizes of organizations. The International Standard is about the prudent strategic preparation for digital investigation of an organization. Forensic readiness assures that an organization has made the appropriate and relevant strategic preparation for accepting potential events of an evidential nature. Actions can occur as the result of inevitable security breaches, fraud, and reputation assertion. In every situation, information technology (IT) has to be strategically deployed to maximize the effectiveness of evidential availability, accessibility, and cost efficiency

Figure 1 shows typical activities surrounding an incident and its investigation. The numbers shown in this diagram (e.g. 27037) indicate the International Standards listed above and the shaded bars show where each is most likely to be directly applicable or has some influence over the investigative process (e.g. by setting policy or creating constraints). It is recommended, however, that all should be consulted prior to, and during, the planning and preparation phases. The process classes shown are defined fully in this International Standard and the activities identified match those discussed in more detail in ISO/IEC 27035-2, and ISO/IEC 27037.

2) To be published.

3) To be published.

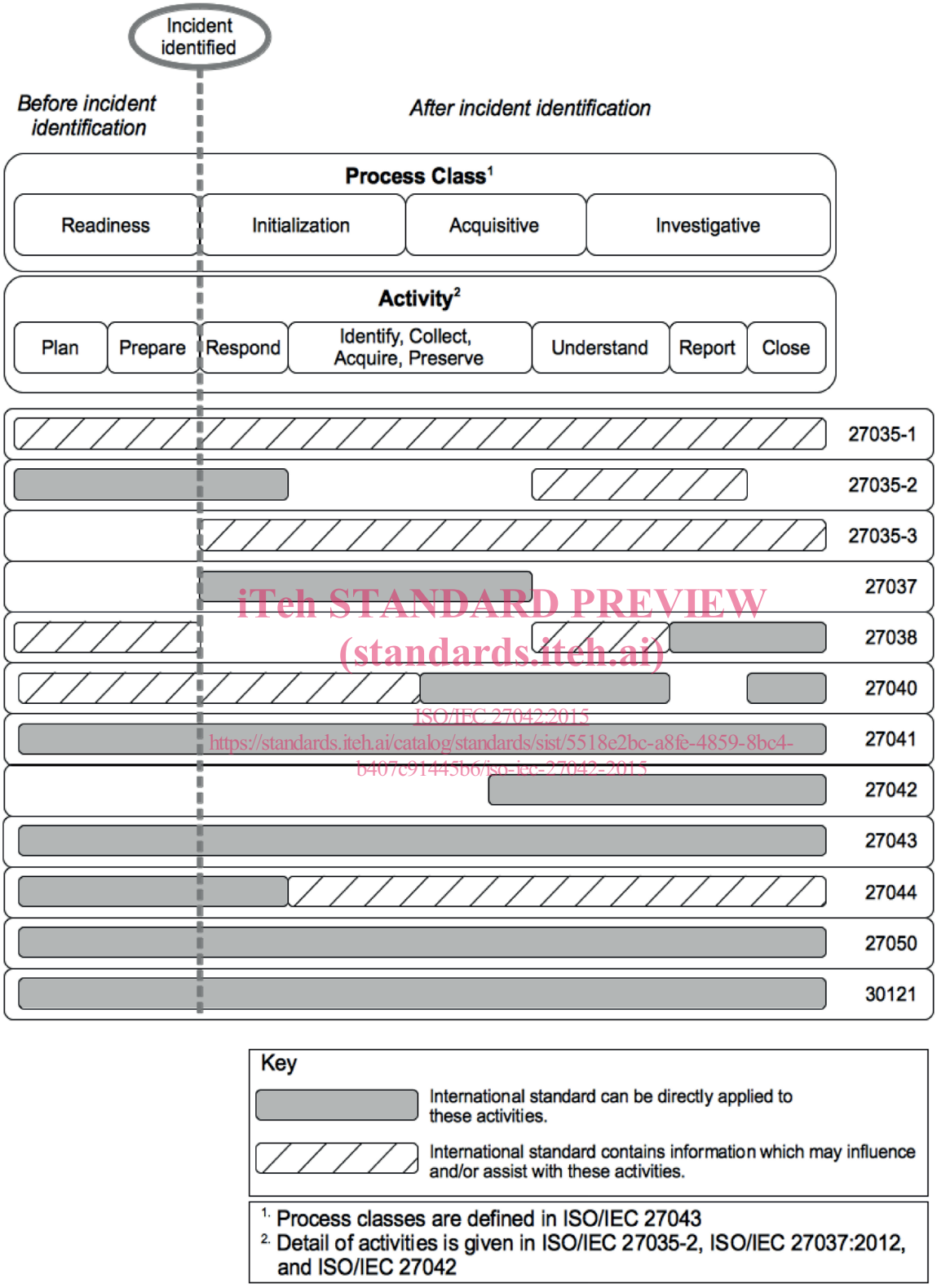

Figure 1 — Applicability of standards to investigation process classes and activities

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

1 Scope

This International Standard provides guidance on the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility, and repeatability. It encapsulates best practice for selection, design, and implementation of analytical processes and recording sufficient information to allow such processes to be subjected to independent scrutiny when required. It provides guidance on appropriate mechanisms for demonstrating proficiency and competence of the investigative team.

Analysis and interpretation of digital evidence can be a complex process. In some circumstances, there can be several methods which could be applied and members of the investigative team will be required to justify their selection of a particular process and show how it is equivalent to another process used by other investigators. In other circumstances, investigators may have to devise new methods for examining digital evidence which has not previously been considered and should be able to show that the method produced is "fit for purpose".

Application of a particular method can influence the interpretation of digital evidence processed by that method. The available digital evidence can influence the selection of methods for further analysis of digital evidence which has already been acquired.

This International Standard provides a common framework, for the analytical and interpretational elements of information systems security incident handling, which can be used to assist in the implementation of new methods and provide a minimum common standard for digital evidence produced from such activities.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2013, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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

ISO/IEC 27041[4)], *Information technology -- Security techniques -- Guidance on assuring suitability and adequacy of incident investigative method*

3 Terms and definitions

For the purposes of this document, the terms and definitions in ISO/IEC 27000:2013 and the following apply.

4) To be published.

3.1
analysis
evaluation of *potential digital evidence* (3.15) in order to assess its relevance to the investigation

Note 1 to entry: *Potential digital evidence* (3.15), which is determined as having relevance, becomes *digital evidence* (3.5).

Note 2 to entry: See also Figure 2.

3.2
client
person or organization on whose behalf the investigation is to be undertaken

3.3
competence
ability to apply knowledge and skills to achieve intended results

[SOURCE: ISO/IEC 17021:2011, 3.7]

3.4
contemporaneous notes
contemporaneous record
written record of actions taken and decisions made, produced at the same time or as soon afterwards as is practically possible, as the actions and decisions it records

Note 1 to entry: In many jurisdictions, it is necessary for contemporaneous notes to be handwritten in non-erasable in a tamper-evident notebook to assist with issues of non-repudiation and admissibility.

3.5
digital evidence
information or data, stored or transmitted in binary form which has been determined, through the process of analysis, to be relevant to the investigation

Note 1 to entry: This should not be confused with *legal digital evidence* (3.14) or *potential digital evidence* (3.15).

Note 2 to entry: See also Figure 2.

[SOURCE: ISO/IEC 27037:2012, 3.5, modified – Note 1 and Note 2 to entry added, definition adapted to distinguish between evidence relating to the incident under investigation and other non-relevant information or data.]

3.6
emulate
accurately imitate, or perform in the same way as, another application or environment

3.7
examination
set of processes applied to identify and retrieve relevant potential digital evidence from one or more sources

3.8
evidence obfuscation
effect of an operation performed on potential digital evidence which results in the digital evidence being hidden or obscured in some way

Note 1 to entry: This can be the result of a deliberate or coincidental action and can or cannot result in spoliation of the digital evidence.

3.9
interpretation
synthesis of an explanation, within agreed limits, for the factual information about evidence resulting from the set of examinations and analyses making up the investigation

3.10
investigation
application of examinations, analyses, and interpretation to aid understanding of an incident

3.11
investigative lead
person leading the investigation at a strategic level

3.12
investigative team
all persons involved directly in the conduct of the investigation

3.13
investigator
member of the investigative team, including the *investigative lead* (3.11)

3.14
legal digital evidence
digital evidence (3.5) which has been accepted into a judicial process

Note 1 to entry: See also Figure 2.

3.15
potential digital evidence
information or data, stored, or transmitted in binary form which has not yet been determined, through the process of analysis, to be relevant to the investigation

Note 1 to entry: The process of analysis determines which of the *potential digital evidence* is *digital evidence* (3.5)

Note 2 to entry: See also Figure 2.

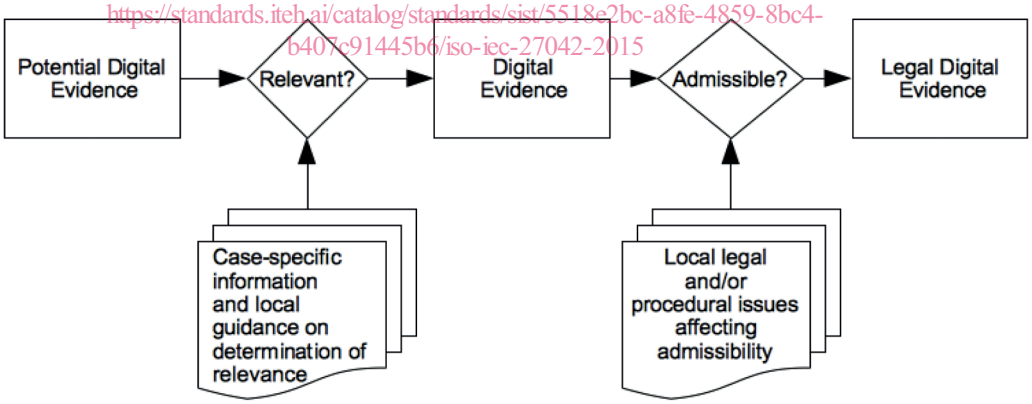

Figure 2 — Digital evidence status transitions

3.16
proficiency
ability of an investigative team to produce results equivalent to those of a different investigative team given the same sources of potential digital evidence

3.17
repeatability
property of a process conducted to get the same test results on the same testing environment

Note 1 to entry: Same testing environment means the same computer, hard drive, mode of operation, etc.