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

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.

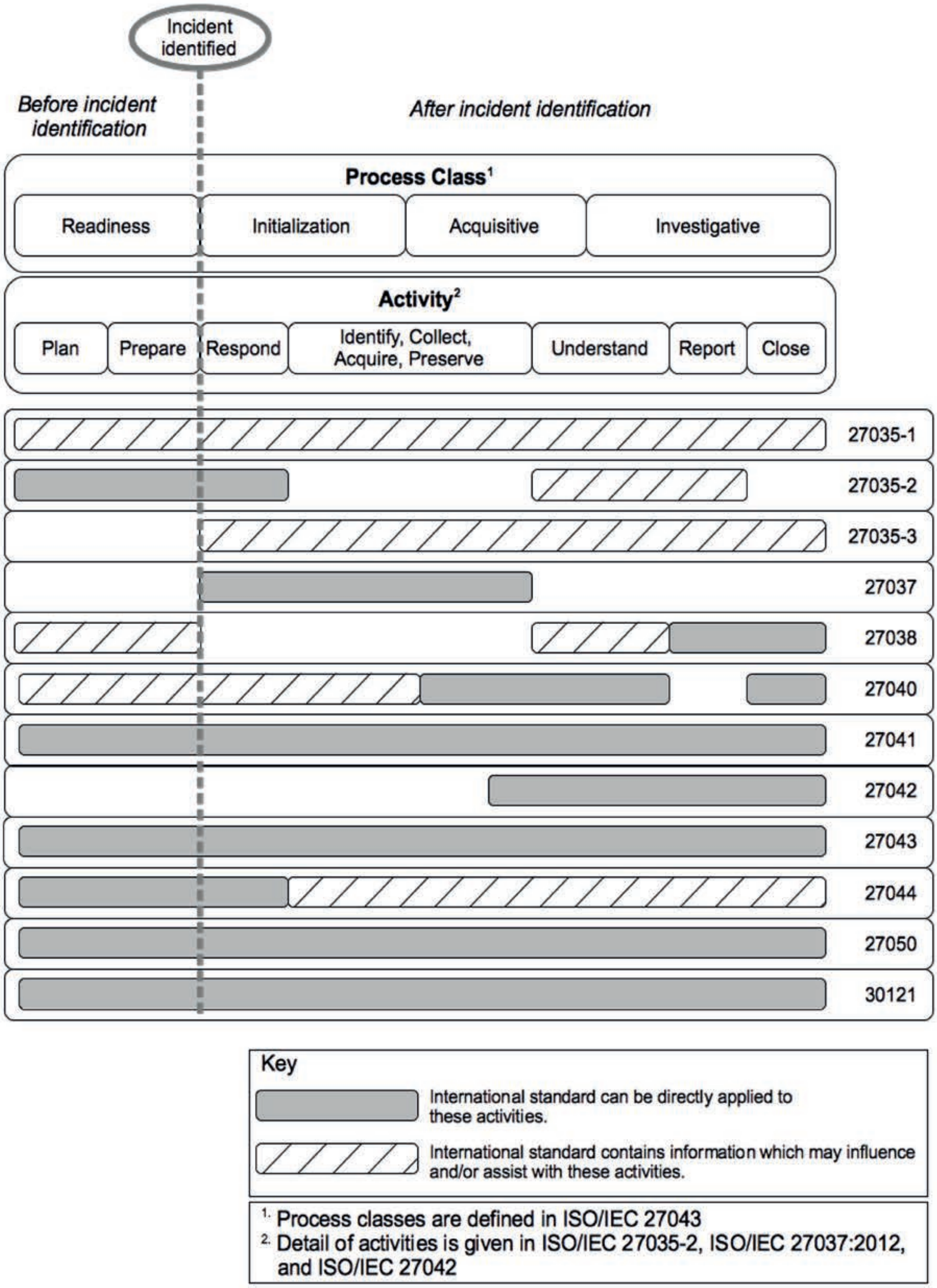
Incident identified
Before incident identification
After incident identification
Process Class[1]
Readiness
Initialization
Acquisitive
Investigative
Activity[2]
Plan
Prepare
Respond
Identify, Collect, Acquire, Preserve
Understand
Report
Close
27035-1
27035-2
27035-3
27037
27038
27040
27041
27042
27043
27044
27050
30121
Key
International standard can be directly applied to these activities.
International standard contains information which may influence and/or assist with these activities.
1. Process classes are defined in ISO/IEC 27043
2. Detail of activities is given in ISO/IEC 27035-2, ISO/IEC 27037:2012, and ISO/IEC 27042

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.

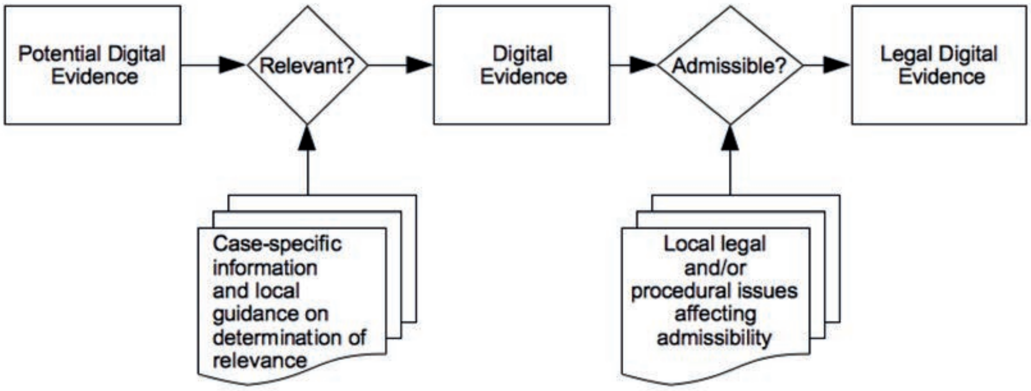
Potential Digital Evidence
Relevant?
Digital Evidence
Admissible?
Legal Digital Evidence
Case-specific information and local guidance on determination of relevance
Local legal and/or procedural issues affecting admissibility

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.

[SOURCE: ISO/IEC 27037:2012, 3.17]

3.18
reproducibility
property of a process to get the same test results on a different testing environment

Note 1 to entry: Different testing environment means different computer, hard drive, operator, etc.

[SOURCE: ISO/IEC 27037:2012, 3.18]

3.19
spoliation
act of making or allowing change(s) to the potential digital evidence that diminishes its evidential value

[SOURCE: ISO/IEC 27037:2012, 3.19]

3.20
validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

[SOURCE: ISO/IEC 27004:2009, 3.17]

3.21
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: Verification only provides assurance that a product conforms to its specification.

[SOURCE: ISO/IEC 27004:2009, 3.18, Modified – Original note was removed, Note 1 to entry has been added.]

3.22
verification function
function which is used to verify that two sets of data are identical

[SOURCE: ISO/IEC 27037:2012, 3.25, Modified – Notes were removed.]

3.23
work instruction
detailed descriptions of how to perform and record a process

[SOURCE: ISO/TR 10013:2001, 3.1, Modified - changed from plural to singular, task changed to process.]

4 Symbols and abbreviated terms

CPD	continuing professional development
SMTP	simple mail transfer protocol

5 Investigation

5.1 Overview

The primary purpose of an investigation is to develop understanding of an incident. Prior to the conduct of an investigation, it may not be possible to determine what action, if any, will be taken once the understanding has been developed. Investigation can result in improved remediation, improvements to security measures and controls for the future, disciplinary action against personnel or civil or criminal court proceedings against those responsible for the incident.

Because the final outcome can be difficult to determine during the initial stages of the investigation it is important that the investigation is carried out in a manner which is inherently reliable and which produces digital evidence which has reliable provenance.

This can be achieved by competent investigators using examinations which are composed of validated analytical processes, in which they are proficient, and ensuring that every item of digital produced can be traced back to the source of potential digital evidence from which it is derived.

5.2 Continuity

As discussed in ISO/IEC 27037:2012, proper recording of the chain of custody and processes applied to potential digital evidence, helps to ensure that there can be no allegations that spoliation has occurred as a result of tampering by some unknown party. This is achieved by having rigorous and complete records of all processes applied in order to produce digital evidence from a source of potential digital evidence. Use of contemporaneous notes is highly beneficial in this regard as notes taken during the process tend be more accurate than notes and records produced some time after the events which they describe.

5.3 Repeatability and reproducibility

Digital evidence which has been produced by methods which do not satisfy the principles of repeatability and reproducibility are highly susceptible to challenge and can call into question the competence and proficiency of the investigative team which uses them. While it may be necessary to devise new methods during an investigation, in order to address new technology or a previously unknown investigative need, the application of proper validation (see ISO/IEC 27041) can assist with demonstration that methods reliably and reproducibly produce results which satisfy an investigative need (see also Figure 1).

5.4 Structured approach

Investigators have a duty to ensure that they report their findings as fully and impartially as possible. In order to achieve this, a structured approach to investigation, which should be carried out by competent and proficient investigators, should be adopted with potential digital evidence sources being subjected to examinations, made up of individual analyses appropriate to the devices and data under investigation.

This structure is shown in Figure 3 and more detail of analysis, interpretation, reporting, competence and proficiency is given in the next clauses.

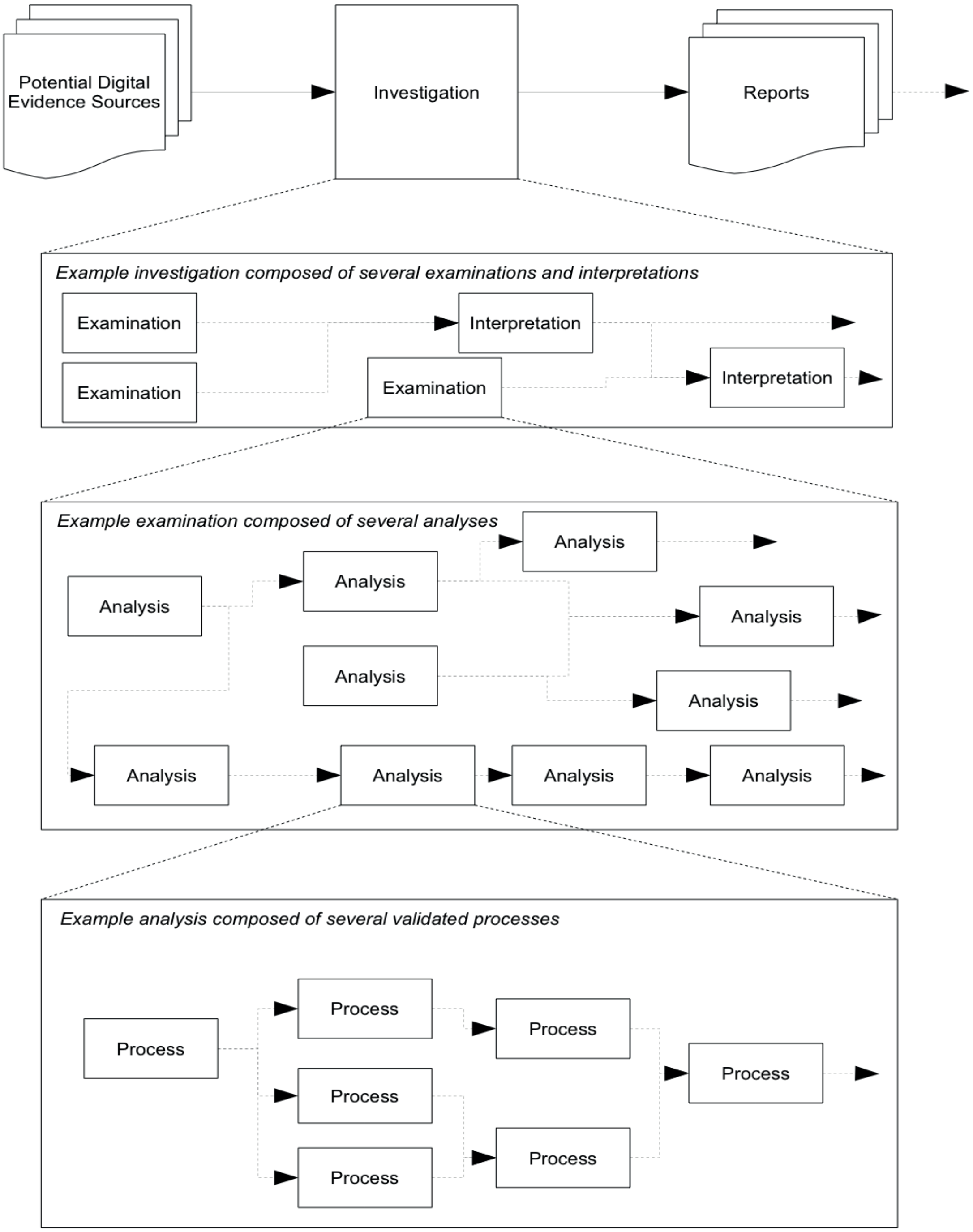
Potential Digital Evidence Sources
Investigation
Reports
Example investigation composed of several examinations and interpretations
Examination
Examination
Interpretation
Examination
Interpretation
Example examination composed of several analyses
Analysis
Analysis
Analysis
Analysis
Analysis
Analysis
Analysis
Analysis
Analysis
Analysis
Example analysis composed of several validated processes
Process
Process
Process
Process
Process
Process
Process

Figure 3 — Structure of a typical investigation

5.5 Uncertainty

Investigators should be aware of areas of uncertainty in findings. Uncertainty should be considered inversely proportional to the quality and quantity of evidence in support of a hypothesis.

In some situations the presence of a single item of digital evidence may be sufficient for the purposes of the investigation (e.g. possession of a restricted document by an unauthorised user), whereas, in other circumstances, a larger body of evidence may be required to substantiate the investigators' hypothesis (e.g. possession of a large collection of illegal material).

Where possible, additional guidance should be obtained from the client. (See also Clause 8).

6 Analysis

6.1 Overview

Analysis is required as many of the meaningful digital artefacts are latent in their native form (e.g., the remnants of a deleted file in free space that must be carved out of free space and reconstructed). As noted below, analysis must make use of validated processes (as defined by ISO/IEC 27041) be performed by competent personnel and be scrupulously documented to establish traceable and defensible provenance for information.

6.2 General principles

Analysis relates to the identification and evaluation of digital evidence from sources of potential digital evidence. It is likely to be an iterative process as each item of digital evidence identified can lead to the re-consideration of other digital evidence. Identification and evaluation can only be carried out in the presence of sufficient contextual information to allow the investigator to make informed decisions about each item under consideration (e.g. information about the suspected incident, the system under consideration and the nature of the sources of potential digital evidence being examined).

Investigators and their support staff must, therefore, be competent to carry out their roles in the analysis. Competence may be defined in terms of the individual processes they will carry out, or as a set of well-defined competencies against which they can be assessed.

Processes used to carry out the examination of items of potential digital evidence should be fully validated (see ISO/IEC 27041) for their role(s) in the investigation.

Processes used should not change the contents of any sources of potential digital evidence under examination. Where there is a chance of damage to potential digital evidence, appropriate measures should be taken to minimize the likelihood, or the effects, of any such damage (e.g. using a write blocker to minimize the chance of inadvertently modifying the contents of an evidentiary hard disk drive). However, if the occurrence of such damage is inevitable or strictly necessary, the investigative team should be competent to explain the effects of any actions taken which may have resulted in damage, as well as the reasons for such actions and damage.

If a member of the investigative team believes that he/she has found evidence of another incident, he/she should inform the investigative lead of this fact and await further instructions. Investigative leads informed of such evidence should consult with appropriate authorities before allowing the investigation to proceed. If any observed damage to potential digital evidence occurs then this should be stated in the (final) report.

NOTE 1 In many jurisdictions, exceeding the authority of one's investigative mandate may render all results (not just those relevant to the newly discovered incident) unusable in legal and administrative proceedings.

Members of the investigative team should bear in mind their locally mandated obligations in respect of impartiality. Where such obligation exists and if, during the course of investigating a premise, the investigative team finds evidence disproving the premise, or which supports or suggests a counter-premise, this should be reported together with the supporting evidence.

An independent investigator, unconnected with the analysis and interpretation, should be able to examine the processes and decisions made by the original investigative team and achieve the same results. For this to happen, a properly documented sequence of atomic processes (normally defined within the context of separate validated processes), which have been recorded in contemporaneous notes, should have been followed with appropriately detailed records kept.

NOTE 2 When using this International Standard, the user assumes that potential digital evidence has been gathered in accordance with the recommendations of ISO/IEC 27037:2012 and that steps similar to those described in ISO/IEC 27037:2012 will be used to preserve potential digital evidence during analysis.

6.3 Use of tools

Tools (combinations of software, hardware and firmware) can be of great help in the analysis process. Selection of tools should be based on the agreed requirements and the processes (see ISO/IEC 27041) which make up the analysis. The user should be competent to use the tools in the context of the relevant process.

Processes involving new tools should be capable of passing validation and confirmation prior to deployment. Users should take account of this prior to adopting new tools. For the selection of tools for use in validated processes, the procedure specified in ISO/IEC 27041 should be followed.

NOTE The concept of validation requires consideration of the intended use of the tool. Hence the requirement is solely to validate the process for the manner in which it will be used in the investigation. A tool which is known to be flawed may still be used, providing the process in which the tool participates can be shown to be fit for its intended use.

6.4 Record keeping

Throughout the analysis, each person carrying out any process should keep accurate and detailed contemporaneous notes of their actions and the results of those actions, in addition to chain of custody record, described in ISO/IEC 27037:2012. These should be sufficiently detailed to allow another similarly competent person to repeat those actions and achieve the same results. The notes should include details of relevant information received and decisions taken, including reasons for the decision.

7 Analytical models

7.1 Static analysis

Static analysis should normally be carried out on a copy of the original potential digital evidence (as described in ISO/IEC 27037:2012) to avoid accidental digital evidence spoliation or obfuscation.

Static analysis is the examination of potential digital evidence, by inspection only, in order to determine its value as digital evidence (e.g. by identifying artefacts, constructing event timelines, examining file contents and deleted data, etc.). Potential digital evidence will be inspected in raw form and interpreted through the use of appropriate processes (e.g. by loading into appropriate viewers) but executable code will not be executed.

This method of analysis is particularly appropriate for the analysis of consequential data (e.g. contents of log files, contents of network packets, contents of memory dumps) and meta-data (e.g. file permissions and timestamps). In some cases, however, it may not be possible for investigators to gain a full understanding of the significance of potential digital evidence from static analysis alone (e.g. intrusion or data exfiltration by means of malware).

7.2 Live analysis

7.2.1 Overview

In some circumstances it may be necessary or beneficial to examine a live version of the potential digital evidence in order to gain proper understanding. This can be particularly useful when dealing with systems such as instant messaging, smartphones/tablets, network intrusion, complex networks, encrypted storage devices or suspected polymorphic code.

Two distinct forms of live analysis exist:

a) live analysis of systems which cannot be imaged or copied; and

b) live analysis of systems which can be imaged or copied.

7.2.2 Live analysis of non-imageable and non-copyable systems

Where it is not possible, for technical or operational reasons (e.g. unique hardware, adverse effect on business), or where there can be a significant risk of loss of potential digital evidence when imaging or copying is attempted (e.g. attempting to copy data from a live storage device using tools present on the suspect system) it may be necessary to carry out a live analysis on a system without first following the steps recommended in ISO/IEC 27037:2012.

In these circumstances, the investigator(s) should take great care to minimise the risk of damage to potential digital evidence and should ensure that they have a full and detailed record of all processes performed. Investigative leads should ensure that any person required to carry out a live analysis is fully competent to do so and able to explain their processes and any alterations to data, potential digital evidence or systems which may have occurred as a result of their actions.

7.2.3 Live analysis of imageable or copyable systems

Where a system can be imaged or copied, it can be appropriate, or necessary, to examine that system, by directly interacting with or observing it in operation. In such circumstances, investigators should take care to emulate, in hardware or software, the original environment as closely as possible by using verified (see ISO/IEC 27041) virtual machines, copies of original hardware or even the real original hardware in order to allow live analysis. Where emulation is to be used, care should be taken to ensure that the emulation is as close as possible to the original system. Steps should be taken to ensure that any changes required to allow the copy to run in the emulator do not materially change the operation of the system and the potential digital evidence under analysis.

NOTE Care in using emulation is also required when dealing with suspected malware infection as some malware variants can detect that they are being executed in a virtual environment and modify their behaviour or refuse to run.

8 Interpretation

8.1 General

The objective of interpretation is to derive meaning from digital evidence by performing an evaluation of data and analysing it in the context of the circumstances. Interpretation, through processes of examination and analysis involves finding facts and in some cases, augmenting facts with opinion. It may require repetition of analysis or potential digital evidence collection depending on the results of interpretation.

The investigative team should remember that their primary responsibility is to provide a fair and accurate interpretation of the facts as they determine them.

8.2 Accreditation of fact

When assessing evidence care must be taken to distinguish facts that have been found and information that has been inferred.

EXAMPLE The presence of an extant file on a device is a fact. If that file was an attachment to an email in an inbox, it can be inferred that the file was created on the device due as a result of being received in an email; hence this is inferred information. If the file was, however, found in a user-created directory with a user-specified filename, it can be inferred that the user made a conscious decision to create or save the file. Inferences about files, such as these, can be corroborated by examining other parts of the filesystem to obtain additional information.

Distinctions between facts and inferred information need to be kept in mind and care taken that all the facts required to support any inference are in place and themselves verified. When reporting facts and inferred information, the distinction between the two needs to be stated and the logical process that has occurred in any inference be clear and repeatable.

8.3 Factors affecting interpretation

Interpretation of any digital evidence is dependent on the information available about the context of creation of that item of digital evidence. To be able to carry out a proper interpretation, the investigative team may require information from persons involved in the day to day running of the system(s) which are under investigation. Care should be taken, however, to test the reliability of any such information provided and to ensure that assigned probative value reflects that reliability.

The investigative team will also require information about the purpose of the investigation and a definition of the scope of their work, including the purpose and target audience of the final report.

During analysis and interpretation, the investigative team should take account of the quality of available potential digital evidence (e.g. completeness, source and original purpose, possibility of evidence obfuscation measures being deployed).

The goal of the interpretation stage is to produce an explanation of the facts found during the analysis, within the context provided to the investigative team. If there is more than one reasonable explanation, then alternate explanations should also be reported. If the contextual information changes, the interpretation may also have to change. If facts lend themselves to more than one interpretation, all of them - or at least the more plausible - should be presented as a result of the analysis stating, if possible, their respective likelihoods.

9 Reporting

9.1 Preparation

Prior to commencing the investigation, the nature and purpose of the final report should be ascertained by the investigative lead. This should be used to guide the investigative process and may consist of a set of questions to be answered, an indication of the likely readers of the report and details of any constraints and limitations which apply to the investigation. The investigative lead should prepare a documented investigative strategy or plan in order to assist in determination of resources, selection of processes and tools and to give guidance to the investigative team.

Reports should contain all information required by applicable local policy or legislation. Some suggested content is given in 9.2.

The use of report templates, with standardized format, drop-down selection lists and placeholders for common text with associated descriptions of the text which is likely to appear, may assist in ensuring that sufficient information is included in reports.

9.2 Suggested report content

If local policy or legislation do not define the report contents, it is suggested that reports should contain, at a minimum:

- a clear statement of the writer’s qualifications or competence to participate in the investigation and produce the report;
- a clear statement of the information provided to the investigative team prior to the investigation commencing (including the nature of the report to be produced);
- the nature of the incident under investigation;
- the time and duration of the incident;
- the location of the incident;
- the objective of the investigation;
- the members of the investigative team, and their roles and actions;

- the time and duration of the investigation;
- the location of the investigation;
- factual details of the digital evidence found during the investigation;
- any damage to potential digital evidence that has been observed during the investigation and its impact on the further investigative steps;
- limitations of any analysis undertaken (e.g. incomplete data sets, operational/time constraints); and
- a list of processes used including, where appropriate, any tools used.

Some reports may also contain:

- An interpretation of the digital evidence as it is understood by the investigator (e.g. an account of how an external attack may have proceeded and led to the presence of digital evidence found). If more than one interpretation is possible, all plausible and likely interpretations should be included with an indication of their relative likelihoods. The interpretation may be given as an opinion if necessary.
- Conclusions.
- Recommendations for further investigative or remedial work.

When a report contains one or more opinions, the writer should clearly distinguish between facts and opinions, and give a justification for any opinions stated.

In some cases, report design can be carried out in the readiness and initialization process classes (see ISO/IEC 27043). Where appropriate, the template design process can be validated using the framework described in ISO/IEC 27041.

10 Competence

10.1 Overview

All steps involved in the investigation of an incident should be carried out by persons who are demonstrably competent to complete the tasks assigned to them. They should be sufficiently familiar with, and experienced in, the tools, methods and techniques which they will use to be able to carry them out with minimal supervision and should also be able to recognize the limits of their own abilities. Should an investigator recognize their own limitations, the issue should be referred to a more senior or competent individual for appropriate action to be taken.

A non-competent person's involvement in an investigation may adversely affect the results of that investigation, resulting in delays in completion or incorrect conclusions being reached.

An example competence definition is in given in Annex A.

10.2 Demonstration of competence

Competence should be measured against a set of core skills identified for the processes involved in the investigation as they are assigned to each person conducting a part of the investigation. Objective evidence of the person's qualifications and experience should be sought. These can take the form of formal competence tests or certification, academic qualifications, job history, evidence of active participation in CPD events such as conferences, training courses, or development of new tools, methods, techniques, processes or standards.

10.3 Recording competence

A person's competence should be reviewed at regular intervals in order to ensure that the person's record of competence is accurate. The review should take account of new areas and levels of competence which have been achieved and should also “retire” those competences which are no longer relevant for the person in question, either because the skills and knowledge involved are no longer relevant or because they have not had the opportunity to practice them sufficiently since the last review was conducted.

If a person’s competence in a particular area is not sufficient for their role in an investigation, steps should be taken to increase that level of competence through appropriate CPD activity as soon as possible.

11 Proficiency

11.1 Overview

A competent investigative team can be considered proficient when, given a sample of potential digital evidence, its analysis produces equivalent results to those produced by another competent investigative team using a similar analysis.

Records which demonstrate the proficiency of an investigative team assist in showing that the analyses used are accurate, reliable, reproducible and appropriate.

11.2 Mechanisms for demonstration of proficiency

Proficiency can be demonstrated through participation in an appropriate proficiency testing process (ISO/IEC 17043:2010), overseen by an independent third party. In such a process all investigative teams will be supplied with the same samples for analysis. The expected results of the analyses will be predicted by the independent third party and the independent third party will be responsible for comparing the results from all participating investigative teams against the predicted results and the results produced by all other investigative teams in the test group.

Investigative teams which produce equivalent results for the supplied samples will be considered equally proficient in the analyses used to produce those results.

NOTE Among proficient investigative teams which produce equivalent results, the conclusions issued in the report may not always be equivalent.

Proficiency tests should be repeated at regular intervals in order to show that proficiency is maintained.

If no suitable independent third party test is available, an investigative team may approach other investigative teams directly to establish a testing scheme suitable for their own needs. Such a scheme should, ideally, be subjected to independent scrutiny to ensure it is appropriate.

Annex A
(informative)

Examples of Competence and Proficiency Specifications

A.1 Example Competence Specification

General competence	**Analysis of *sendmail* server incidents**
Specific competencies	Able to — locate, parse and interpret sendmail log files — locate, parse and interpret user mailboxes — locate, parse and interpret SMTP headers found in mail messages — locate, parse and interpret sendmail configuration files — describe common sendmail failure modes and common exploits in relevant versions of sendmail

A.2 Example Proficiency Specification

General proficiency	**Analysis of sendmail incidents**
Specific proficiencies	— Successfully identify and extract relevant records from — logfiles — user mailboxes — mail messages — configuration files — core files — Successfully identify and attribute interactions with other software, systems and users

Bibliography

[1] ISO/IEC 17024:2003, *Conformity assessment — General requirements for bodies operating certification of persons*

[2] ISO/IEC 17025:2005, *General requirements for the competence of testing and calibration laboratories*

[3] ISO/IEC 17043:2010, *Conformity assessment — General requirements for proficiency testing*

[4] ISO/IEC 27004:2009, *Information technology — Security techniques — Information security management — Measurement*

[5] ISO/IEC 27035:2011, *Information technology — Security techniques — Information security incident management*

[6] Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3ed. New York: Academic Press, 2011.

ICS 35.040

Price based on 14 pages