STN	**Informačné technológie. Bezpečnostné metódy. Návod na identifikáciu, zber, získavanie a zachovanie digitálnych dôkazov (ISO/IEC 27037: 2012).**	**STN EN ISO/IEC 27037**
		36 9762

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 01/17

Obsahuje: EN ISO/IEC 27037:2016, ISO/IEC 27037:2012

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 27037

August 2016

ICS 35.040

English Version

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

Technologies de l'information - Techniques de sécurité - Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques (ISO/IEC 27037:2012)

Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für die Identifikation, Sammlung, Erhebung und Erhaltung der digitalen Beweissicherung (ISO/IEC 27037:2012)

This European Standard was approved by CEN on 19 June 2016.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN ISO/IEC 27037:2016 E

Contents

Page

European foreword

The text of ISO/IEC 27037:2012 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has been taken over as EN ISO/IEC 27037:2016.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2017, and conflicting national standards shall be withdrawn at the latest by February 2017.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27037:2012 has been approved by CEN as EN ISO/IEC 27037:2016 without any modification.

INTERNATIONAL
STANDARD

ISO/IEC
27037

First edition
2012-10-15

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

ISO/IEC 27037:2012(E)

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27037 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

v

ISO/IEC 27037:2012(E)

Introduction

This International Standard provides guidelines for specific activities in handling potential digital evidence; these processes are: identification, collection, acquisition and preservation of potential digital evidence. These processes are required in an investigation that is designed to maintain the integrity of the digital evidence – an acceptable methodology in obtaining digital evidence that will contribute to its admissibility in legal and disciplinary actions as well as other required instances. This International Standard also provides general guidelines for the collection of non-digital evidence that may be helpful in the analysis stage of the potential digital evidence.

This International Standard intends to provide guidance to those individuals responsible for the identification, collection, acquisition and preservation of potential digital evidence. These individuals include Digital Evidence First Responders (DEFRs), Digital Evidence Specialists (DESs), incident response specialists and forensic laboratory managers. This International Standard ensures that responsible individuals manage potential digital evidence in practical ways that are acceptable worldwide, with the objective to facilitate investigation involving digital devices and digital evidence in a systematic and impartial manner while preserving its integrity and authenticity.

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

The potential digital evidence referred to in this International Standard may be sourced from different types of digital devices, networks, databases, etc. It refers to data that is already in a digital format. This International Standard does not attempt to cover the conversion of analog data into digital format.

Due to the fragility of digital evidence, it is necessary to carry out an acceptable methodology to ensure the integrity and authenticity of the potential digital evidence. This International Standard does not mandate the use of particular tools or methods. Key components that provide credibility in the investigation are the methodology applied during the process, and individuals qualified in performing the tasks specified in the methodology. This International Standard does not address the methodology for legal proceedings, disciplinary procedures and other related actions in handling potential digital evidence that are outside the scope of identification, collection, acquisition and preservation.

Application of this International Standard requires compliance with national laws, rules and regulations. It should not replace specific legal requirements of any jurisdiction. Instead, it may serve as a practical guideline for any DEFR or DES in investigations involving potential digital evidence. It does not extend to the analysis of digital evidence and it does not replace jurisdiction-specific requirements that pertain to matters such as admissibility, evidential weighting, relevance and other judicially controlled limitations on the use of potential digital evidence in courts of law. This International Standard may assist in the facilitation of potential digital evidence exchange between jurisdictions. In order to maintain the integrity of the digital evidence, users of this International Standard are required to adapt and amend the procedures described in this International Standard in accordance with the specific jurisdiction's legal requirements for evidence.

Although this International Standard does not include forensic readiness, adequate forensic readiness can largely support the identification, collection, acquisition, and preservation process of digital evidence. Forensic readiness is the achievement of an appropriate level of capability by an organization in order for it to be able to identify, collect, acquire, preserve, protect and analyze digital evidence. Whereas the processes and activities described in this International Standard are essentially reactive measures used to investigate an incident after it occurred, forensic readiness is a proactive process of attempting to plan for such events.

This International Standard complements ISO/IEC 27001 and ISO/IEC 27002, and in particular the control requirements concerning potential digital evidence acquisition by providing additional implementation guidance. In addition, this International Standard will have applications in contexts independent of ISO/IEC 27001 and ISO/IEC 27002. This International Standard should be read in conjunction with other standards related to digital evidence and the investigation of information security incidents.

INTERNATIONAL STANDARD

ISO/IEC 27037:2012(E)

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

1 Scope

This International Standard provides guidelines for specific activities in handling digital evidence, which are identification, collection, acquisition and preservation of digital evidence that may be of evidential value. This International Standard provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.

This International Standard gives guidance for the following devices and/or functions that are used in various circumstances:

— Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto optical disks, data devices with similar functions,

— Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards,

— Mobile navigation systems,

— Digital still and video cameras (including CCTV),

— Standard computer with network connections,

— Networks based on TCP/IP and other digital protocols, and

— Devices with similar functions as above.

NOTE 1   The above list of devices is an indicative list and not exhaustive.

NOTE 2   Circumstances include the above devices that exist in various forms. For example, an automotive system may include mobile navigation system, data storage and sensory system.

2 Normative reference

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

ISO/TR 15801, *Document management — Information stored electronically — Recommendations for trustworthiness and reliability*

ISO/IEC 17020, *Conformity assessment — Requirements for the operation of various types of bodies performing inspection*

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

ISO/IEC 27037:2012(E)

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

koniec náhľadu – text ďalej pokračuje v platenej verzii STN