



Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN ISO/IEC 27042:2016

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

Informationstechnik - IT-
Sicherheitsverfahren - Leitfaden für die
Analyse und Interpretation digitaler
Beweismittel (ISO/IEC 27042:2015)

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

08/2016



National Foreword

This European Standard EN ISO/IEC 27042:2016 was adopted as Luxembourgish Standard ILNAS-EN ISO/IEC 27042:2016.

Every interested party, which is member of an organization based in Luxembourg, can participate for FREE in the development of Luxembourgish (ILNAS), European (CEN, CENELEC) and International (ISO, IEC) standards:

- Participate in the design of standards
- Foresee future developments
- Participate in technical committee meetings

<https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html>

THIS PUBLICATION IS COPYRIGHT PROTECTED

Nothing from this publication may be reproduced or utilized in any form or by any mean - electronic, mechanical, photocopying or any other data carries without prior permission!

ILNAS-EN ISO/IEC 27042:2016

EUROPEAN STANDARD **EN ISO/IEC 27042**

NORME EUROPÉENNE

EUROPÄISCHE NORM

August 2016

ICS 35.040

English Version

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

Technologies de l'information - Techniques de sécurité
- Lignes directrices pour l'analyse et l'interprétation de
preuves numériques (ISO/IEC 27042:2015)

Informationstechnik - IT-Sicherheitsverfahren -
Leitfaden für die Analyse und Interpretation digitaler
Beweismittel (ISO/IEC 27042:2015)

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

Contents	Page
European foreword.....	3

European foreword

The text of ISO/IEC 27042:2015 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 27042:2016.

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 27042:2015 has been approved by CEN as EN ISO/IEC 27042:2016 without any modification.

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/IEC 2015

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	4
5 Investigation	4
5.1 Overview.....	4
5.2 Continuity.....	5
5.3 Repeatability and reproducibility.....	5
5.4 Structured approach.....	5
5.5 Uncertainty.....	6
6 Analysis	7
6.1 Overview.....	7
6.2 General principles.....	7
6.3 Use of tools.....	8
6.4 Record keeping.....	8
7 Analytical models	8
7.1 Static analysis.....	8
7.2 Live analysis.....	8
7.2.1 Overview.....	8
7.2.2 Live analysis of non-imageable and non-copyable systems.....	9
7.2.3 Live analysis of imageable or copyable systems.....	9
8 Interpretation	9
8.1 General.....	9
8.2 Accreditation of fact.....	9
8.3 Factors affecting interpretation.....	10
9 Reporting	10
9.1 Preparation.....	10
9.2 Suggested report content.....	10
10 Competence	11
10.1 Overview.....	11
10.2 Demonstration of competence.....	11
10.3 Recording competence.....	11
11 Proficiency	12
11.1 Overview.....	12
11.2 Mechanisms for demonstration of proficiency.....	12
Annex A (informative) Examples of Competence and Proficiency Specifications	13
Bibliography	14