

American National Standard

INCITS/ISO/IEC 27037:2012[2014]

(ISO/IEC 27037:2012, IDT)

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

Developed by



Where IT all begins



INCITS/ISO/IEC 27037:2012[2014]

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.

Date of ANSI Approval: 6/25/2014

Published by American National Standards Institute,
25 West 43rd Street, New York, New York 10036

Copyright 2014 by Information Technology Industry Council
(ITI). All rights reserved.

These materials are subject to copyright claims of International Standardization Organization (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), and Information Technology Industry Council (ITI). Not for resale. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ITI. All requests pertaining to this standard should be submitted to ITI, 1101 K Street NW, Suite 610, Washington DC 20005.

Printed in the United States of America

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

Reference number
ISO/IEC 27037:2012(E)



This is a preview of "INCITS/ISO/IEC 27037...". Click [here](#) to purchase the full version from the ANSI store.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

This is a preview of "INCITS/ISO/IEC 27037...". Click here to purchase the full version from the ANSI store.

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative reference.....	1
3 Terms and definitions.....	2
4 Abbreviated terms	4
5 Overview.....	6
5.1 Context for collecting digital evidence	6
5.2 Principles of digital evidence.....	6
5.3 Requirements for digital evidence handling.....	6
5.3.1 General.....	6
5.3.2 Auditability.....	7
5.3.3 Repeatability.....	7
5.3.4 Reproducibility.....	7
5.3.5 Justifiability	7
5.4 Digital evidence handling processes	8
5.4.1 Overview.....	8
5.4.2 Identification.....	8
5.4.3 Collection	9
5.4.4 Acquisition.....	9
5.4.5 Preservation.....	10
6 Key components of identification, collection, acquisition and preservation of digital evidence	10
6.1 Chain of custody.....	10
6.2 Precautions at the site of incident	11
6.2.1 General.....	11
6.2.2 Personnel	11
6.2.3 Potential digital evidence	12
6.3 Roles and responsibilities	12
6.4 Competency.....	13
6.5 Use reasonable care	13
6.6 Documentation	14
6.7 Briefing	14
6.7.1 General.....	14
6.7.2 Digital evidence specific	14
6.7.3 Personnel specific.....	15
6.7.4 Real-time incidents	15
6.7.5 Other briefing information	15
6.8 Prioritizing collection and acquisition	16
6.9 Preservation of potential digital evidence.....	17
6.9.1 Overview.....	17
6.9.2 Preserving potential digital evidence.....	17
6.9.3 Packaging digital devices and potential digital evidence.....	17
6.9.4 Transporting potential digital evidence.....	18
7 Instances of identification, collection, acquisition and preservation	19
7.1 Computers, peripheral devices and digital storage media	19
7.1.1 Identification.....	19
7.1.2 Collection	21

This is a preview of "INCITS/ISO/IEC 27037...". [Click here to purchase the full version from the ANSI store.](#)

7.1.3	Acquisition	25
7.1.4	Preservation	29
7.2	Networked devices	29
7.2.1	Identification	29
7.2.2	Collection, acquisition and preservation	31
7.3	CCTV collection, acquisition and preservation	33
Annex A (informative)	DEFR core skills and competency description	35
Annex B (informative)	Minimum documentation requirements for evidence transfer	37
Bibliography		38

This is a preview of "INCITS/ISO/IEC 27037...". [Click here to purchase the full version from the ANSI store.](#)

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*.

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 (DEFs), 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 DEF 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 is a preview of "INCITS/ISO/IEC 27037...". [Click here to purchase the full version from the ANSI store.](#)

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.