ISO/IEC 27037:2012-10 (E)

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

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
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