ISO/IEC 27042:2015-06 (E)

Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 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)ExamplesofCompetenceandProficiencySpecifications 13

Bibliography 14