DIN EN ISO/IEC 27042:2016-12 (E)

Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence (ISO/IEC 2 7042:2015)

Contents

Page

European foreword ... **3**

Foreword ... **4**

Introduction ... **5**

1 Scope ... **9**

2 Normative references ... **9**

3 Terms and definitions ... **9**

4 Symbols and abbreviated terms ... **12**

5 Investigation ... **12**
5.1 Overview ... 12
5.2 Continuity ... 13
5.3 Repeatability and reproducibility ... 13
5.4 Structured approach ... 13
5.5 Uncertainty ... 14

6 Analysis ... **15**
6.1 Overview ... 15
6.2 General principles ... 15
6.3 Use of tools ... 16
6.4 Record keeping ... 16

7 Analytical models ... **16**
7.1 Static analysis ... 16
7.2 Live analysis ... 16
7.2.1 Overview ... 16
7.2.2 Live analysis of non-imageable and non-copyable systems ... 17
7.2.3 Live analysis of imageable or copyable systems ... 17

8 Interpretation ... **17**
8.1 General ... 17
8.2 Accreditation of fact ... 17
8.3 Factors affecting interpretation ... 18

9 Reporting ... **18**
9.1 Preparation ... 18
9.2 Suggested report content ... 18

10 Competence ... **19**
10.1 Overview ... 19
10.2 Demonstration of competence ... 19
10.3 Recording competence ... 19

11 Proficiency ... **20**
11.1 Overview ... 20
11.2 Mechanisms for demonstration of proficiency ... 20

Annex A (informative) **Examples of Competence and Proficiency Specifications** ... **21**

Bibliography ... **22**