

DIN EN ISO/IEC 27037:2016-12 (E)

Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012)

Contents		Page
European foreword		4
Foreword		5
Introduction		6
1 Scope		8
2 Normative reference.....		8
3 Terms and definitions.....		9
4 Abbreviated terms		11
5 Overview.....		13
5.1 Context for collecting digital evidence		13
5.2 Principles of digital evidence.....		13
5.3 Requirements for digital evidence handling.....		13
5.3.1 General.....		13
5.3.2 Auditability.....		14
5.3.3 Repeatability.....		14
5.3.4 Reproducibility.....		14
5.3.5 Justifiability		14
5.4 Digital evidence handling processes		15
5.4.1 Overview.....		15
5.4.2 Identification.....		15
5.4.3 Collection		16
5.4.4 Acquisition.....		16
5.4.5 Preservation.....		17
6 Key components of identification, collection, acquisition and preservation of digital evidence		17
6.1 Chain of custody.....		17
6.2 Precautions at the site of incident.....		18
6.2.1 General.....		18
6.2.2 Personnel		18
6.2.3 Potential digital evidence		19
6.3 Roles and responsibilities		19
6.4 Competency.....		20
6.5 Use reasonable care		20
6.6 Documentation		21
6.7 Briefing		21
6.7.1 General.....		21
6.7.2 Digital evidence specific		21
6.7.3 Personnel specific.....		22
6.7.4 Real-time incidents		22
6.7.5 Other briefing information		22
6.8 Prioritizing collection and acquisition		23
6.9 Preservation of potential digital evidence.....		24
6.9.1 Overview.....		24
6.9.2 Preserving potential digital evidence.....		24
6.9.3 Packaging digital devices and potential digital evidence.....		24
6.9.4 Transporting potential digital evidence.....		25

7	Instances of identification, collection, acquisition and preservation	26
7.1	Computers, peripheral devices and digital storage media	26
7.1.1	Identification.....	26
7.1.2	Collection	28
7.1.3	Acquisition	32
7.1.4	Preservation.....	36
7.2	Networked devices	36
7.2.1	Identification	36
7.2.2	Collection, acquisition and preservation	38
7.3	CCTV collection, acquisition and preservation	40
Annex A	(informative) DEFR core skills and competency description.....	42
Annex B	(informative) Minimum documentation requirements for evidence transfer	44
Bibliography	45