

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

Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für die Identifikation, Mitnahme, Sicherung und Erhaltung digitaler Beweismittel (ISO/IEC 27037:2012); Deutsche Fassung EN ISO/IEC 27037:2016

Inhalt	Seite
Europäisches Vorwort.....	4
Vorwort.....	5
Einleitung.....	6
1 Anwendungsbereich.....	8
2 Normative Verweisungen.....	8
3 Begriffe.....	9
4 Abkürzungen.....	12
5 Überblick.....	13
5.1 Kontext für die Mitnahme von digitalen Beweismitteln.....	13
5.2 Grundsätze der digitalen Beweisführung.....	13
5.3 Anforderungen an die Handhabung von digitalen Beweismitteln.....	13
5.3.1 Allgemeines.....	13
5.3.2 Auditierbarkeit.....	14
5.3.3 Wiederholbarkeit.....	14
5.3.4 Reproduzierbarkeit.....	15
5.3.5 Begründbarkeit.....	15
5.4 Prozesse zur Handhabung von digitalen Beweismitteln.....	15
5.4.1 Überblick.....	15
5.4.2 Identifikation.....	16
5.4.3 Mitnahme.....	16
5.4.4 Sicherung.....	17
5.4.5 Erhaltung.....	18
6 Schlüsselkomponenten bei der Identifikation, Mitnahme, Sicherung und Erhaltung von digitalen Beweismitteln.....	18
6.1 Obhutskette.....	18
6.2 Vorkehrungen am Untersuchungsort.....	19
6.2.1 Allgemeines.....	19
6.2.2 Personal.....	20
6.2.3 Potentielle digitale Beweismittel.....	20
6.3 Rollen und Verantwortlichkeiten.....	21
6.4 Kompetenz.....	21
6.5 Anwendung angemessener Sorgfalt.....	22
6.6 Dokumentation.....	22
6.7 Einsatzbesprechung (en: briefing).....	23
6.7.1 Allgemeines.....	23
6.7.2 Spezifische Einsatzbesprechung für digitale Beweismittel.....	23
6.7.3 Personalbezogene Einsatzbesprechung.....	24
6.7.4 Zeitkritische Vorfälle (en: Real-time incidents).....	24
6.7.5 Sonstige Besprechungsinformationen.....	24
6.8 Priorisierung der Mitnahme und Sicherung.....	25
6.9 Erhaltung von potentiellen digitalen Beweismitteln.....	26
6.9.1 Überblick.....	26

6.9.2	Erhalten von potentiellen digitalen Beweismitteln	26
6.9.3	Verpacken von digitalen Geräten und potentiellen digitalen Beweismitteln	26
6.9.4	Transport von potentiellen digitalen Beweismitteln	28
7	Phasen der Identifikation, Mitnahme, Sicherung und Erhaltung	28
7.1	Computer, Peripheriegeräte und digitale Speichermedien	28
7.1.1	Identifikation.....	28
7.1.2	Mitnahme.....	31
7.1.3	Datensicherung.....	35
7.1.4	Erhaltung	40
7.2	Netzwerkgeräte	40
7.2.1	Identifikation.....	40
7.2.2	Mitnahme, Sicherung und Erhaltung	42
7.3	Mitnahme, Sicherung und Erhaltung von Daten aus Videoüberwachungsanlagen (en: CCTV-Systemen).....	45
Anhang A (informativ) Beschreibung von Schlüsselqualifikationen und Kompetenzen des DEFR.....		47
Anhang B (informativ) Mindestanforderungen an die Dokumentation für den Transfer von Beweismitteln		50
Literaturhinweise		51

Bilder

Bild 1	— Leitfaden für die Entscheidung über die Mitnahme oder Sicherung von potentiellen digitalen Beweismitteln	31
Bild 2	— Leitfaden für die Mitnahme von eingeschalteten digitalen Geräten	32
Bild 3	— Leitfaden für die Mitnahme von ausgeschalteten digitalen Geräten.....	34
Bild 4	— Leitfäden für die Sicherung von eingeschalteten digitalen Geräten.....	36
Bild 5	— Leitfaden für die Sicherung von ausgeschalteten digitalen Geräten	38

Tabellen

Tabelle A.1	— Beispiele für Kompetenzbeschreibungen.....	47
Tabelle A.2	— Kompetenzdefinition.....	49