

DIN EN ISO/IEC 27037

ICS 35.030

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

Information technology –
Security techniques –
Guidelines for identification, collection, acquisition and preservation of digital evidence
(ISO/IEC 27037:2012);
German version EN ISO/IEC 27037:2016

Technologies de l'information –
Techniques de sécurité –
Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves
numériques (ISO/IEC 27037:2012);
Version allemande EN ISO/IEC 27037:2016

Gesamtumfang 53 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (EN ISO/IEC 27037:2016) wurde vom Gemeinsamen Technischen Komitee ISO/IEC JTC 1/SC 27 „IT Security techniques“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird. Auf Grundlage eines CEN/BT-Beschlusses wurde ISO/IEC 27037:2012 im einstufigen Annahmeverfahren (UAP) als EN ISO/IEC 27037:2016 ohne Abänderung übernommen.

Das zuständige deutsche Spiegelgremium ist der Arbeitskreis NA 043-01-27-04 AK „IT-Sicherheitsmaßnahmen und Dienste“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Für die in diesem Dokument zitierten Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO/IEC 27000 siehe DIN ISO/IEC 27000^{*)}

Nationaler Anhang NA (informativ)

Literaturhinweise

E DIN ISO/IEC 27000, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Überblick und Terminologie (ISO/IEC DIS 27000:2015)*

^{*)} In Bearbeitung.

Deutsche Fassung

Informationstechnik —
IT-Sicherheitsverfahren —
Leitfaden für die Identifikation, Mitnahme, Sicherung
und Erhaltung digitaler Beweismittel
(ISO/IEC 27037:2012)

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

Technologies de l'information —
Techniques de sécurité —
Lignes directrices pour l'identification, la collecte,
l'acquisition et la préservation de preuves numériques
(ISO/IEC 27037:2012)

Diese Europäische Norm wurde vom CEN am 19. Juni 2016 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN-CENELEC oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

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 — Leitfaden 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

Europäisches Vorwort

Der Text von ISO/IEC 27037:2012 wurde vom Gemeinsamen Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 27037:2016 übernommen.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Februar 2017, und etwaige entgegenstehende nationale Normen müssen bis Februar 2017, zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 27037:2012 wurde vom CEN als EN ISO/IEC 27037:2016 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (Internationale Organisation für Normung) und IEC (Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Internationale Normen werden in Übereinstimmung mit den Regeln nach ISO/IEC Direktive, Teil 2 erarbeitet.

Die Hauptaufgabe des Gemeinsamen Technischen Komitees ist es, Internationale Normen zu erarbeiten. Internationale Norm-Entwürfe, die von Gemeinsamen Technischen Komitees verabschiedet wurden, werden den Mitgliedsorganisationen zur Abstimmung zur Verfügung gestellt. Für die Veröffentlichung als Internationale Norm wird eine Zustimmung der Mitgliedsorganisationen von mindestens 75% benötigt.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

ISO/IEC 27037 wurde vom Gemeinsamen Technischen Komitee ISO/IEC JTC 1 *Information technology*, Unterkomitee SC 27 *Security techniques* erarbeitet.

Einleitung

Diese internationale Norm bietet einen Leitfaden für spezifische Abläufe bei der Handhabung von potentiellen digitalen Beweismitteln. Diese Prozesse sind: Identifikation, Mitnahme, Sicherung und Erhaltung von potentiellen digitalen Beweismitteln. Diese Prozesse sind bei einer Untersuchung, die darauf ausgelegt ist, die Integrität der digitalen Beweismittel aufrechtzuerhalten, erforderlich — eine akzeptable Vorgehensweise bei der Erhebung von digitalen Beweismitteln, die deren Zulässigkeit vor Gericht und in Disziplinarverfahren sowie in anderen Instanzen unterstützt. Diese Internationale Norm bietet außerdem einen allgemeinen Leitfaden für die Mitnahme von nicht digitalen Beweismitteln, die in der Analysephase von potentiellen digitalen Beweismitteln behilflich sein können.

Ziel dieser Internationalen Norm ist es, einen Leitfaden für diejenigen Personen bereitzustellen, die für die Identifikation, Mitnahme, Sicherung und Erhaltung von potentiellen digitalen Beweismitteln verantwortlich sind. Zu diesen Personen zählen Ersteinschreiter für digitale Beweismittel (DEFR, en: Digital Evidence First Responder), Spezialisten für digitale Beweismittel (DES, en: Digital Evidence Specialist), Spezialisten für die Reaktion auf einen Vorfall (en: incident response specialists) und Leiter von kriminaltechnischen Laboratorien. Diese Internationale Norm stellt sicher, dass die verantwortlichen Einzelpersonen die potentiellen digitalen Beweismittel auf praktische, weltweit anerkannte Art und Weise handhaben. Diese Vorgehensweise hat zum Ziel, die Untersuchung im Zusammenhang mit digitalen Geräten und digitalen Beweismitteln auf systematische und objektive Weise zu erleichtern und dabei Integrität und Authentizität zu wahren.

Zweck dieser Internationalen Norm ist es außerdem, Entscheidungsträger, die die Glaubwürdigkeit der ihnen vorgelegten digitalen Beweismittel feststellen müssen, mit Informationen zu versorgen. Sie ist für Organisationen geeignet, die potentielle digitale Beweismittel schützen, analysieren und vorlegen müssen. Sie ist für richtungsweisende Stellen von Bedeutung, die Verfahrensweisen bezogen auf digitale Beweismittel erstellen und bewerten, welche häufig Teil einer größeren Beweismenge sind.

Die in dieser Internationalen Norm in Bezug genommenen potentiellen digitalen Beweismittel können aus verschiedenen Arten von digitalen Geräten, Netzwerken, Datenbanken usw. bezogen werden. Diese Internationale Norm bezieht sich auf Daten, die bereits in einem digitalen Format vorliegen. Es ist nicht das Ziel dieser Internationalen Norm, die Umwandlung von analogen Daten in ein digitales Format zu behandeln.

Wegen der leichten Veränderlichkeit von digitalen Beweismitteln ist es notwendig, eine zulässige Vorgehensweise umzusetzen, um die Integrität und Authentizität der potentiellen digitalen Beweismittel sicherzustellen. Diese Internationale Norm fordert nicht den Einsatz bestimmter Werkzeuge oder Methoden. Schlüsselkomponenten, die der Untersuchung Glaubwürdigkeit verleihen, sind die Vorgehensweise während des Prozesses und die Personen, die für die Durchführung der in der Vorgehensweise festgelegten Aufgaben qualifiziert sind. Diese internationale Norm behandelt nicht die Vorgehensweise bei Gerichtsverfahren, Disziplinarverfahren und anderen damit zusammenhängenden Maßnahmen zur Handhabung von potentiellen digitalen Beweismitteln, die nicht explizit unter die Identifikation, Mitnahme, Sicherung und Erhaltung fallen.

Die Anwendung dieser Internationalen Norm erfordert die Einhaltung nationaler Gesetze, Regeln und Verordnungen. Sie sollte keine spezifischen rechtlichen Anforderungen einer Rechtsordnung ersetzen. Stattdessen kann sie als praktischer Leitfaden für jeden DEFR oder DES bei der Untersuchung im Zusammenhang mit potentiellen digitalen Beweismitteln dienen. Sie betrifft nicht die Analyse von digitalen Beweismitteln und ersetzt keine spezifischen Anforderungen einer Rechtsordnung, soweit diese Angelegenheiten wie Zulässigkeit, Beweiskraft, Relevanz und andere rechtlich geregelten Einsatzgrenzen von potentiellen digitalen Beweismitteln vor Gericht betreffen. Diese Internationale Norm darf den Austausch von potentiellen digitalen Beweismitteln zwischen verschiedenen Rechtsordnungen fördern. Um die Integrität der digitalen Beweismittel zu wahren, wird von den Anwendern dieser Internationalen Norm gefordert, dass sie die in dieser Internationalen Norm beschriebenen Verfahrensweisen in Übereinstimmung mit den spezifischen rechtlichen Anforderungen an Beweismittel der jeweiligen Rechtsordnung anpassen und ergänzen.

Auch wenn diese Internationale Norm keine forensische Bereitschaft (en: forensic readiness) behandelt, kann eine angemessene forensische Bereitschaft die Identifikations-, Mitnahme-, Sicherungs- und Erhaltungsprozesse von digitalen Beweismitteln deutlich unterstützen. Die forensische Bereitschaft ist das Erreichen einer angemessenen Fähigkeit einer Organisation, mit der sie digitale Beweismittel identifizieren, mitnehmen, sichern, erhalten, schützen und analysieren kann. Während die in dieser Internationalen Norm beschriebenen Prozesse und Aktivitäten grundlegend reaktive Maßnahmen sind, die für die Untersuchung eines Vorfalls (en: incident) nach dessen Eintreten eingesetzt werden, ist die forensische Bereitschaft ein proaktiver Prozess, bei dem versucht wird, solche Ereignisse im Voraus zu planen.

Diese Internationale Norm ergänzt ISO/IEC 27001 und ISO/IEC 27002 sowie insbesondere die Anforderungen an die erforderlichen Maßnahmen bei der Sicherung von potentiellen digitalen Beweismitteln durch Bereitstellung zusätzlicher Umsetzungsregeln. Des Weiteren findet diese Internationale Norm Anwendung in Kontexten, die nicht im Zusammenhang mit ISO/IEC 27001 und ISO/IEC 27002 stehen. Diese Internationale Norm sollte in Verbindung mit anderen Normen zu digitalen Beweismitteln und zur Untersuchung von Informationssicherheits-Vorfällen (en: security incidents) gelesen werden.

Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für die Identifikation, Mitnahme, Sicherung und Erhaltung digitaler Beweismittel

1 Anwendungsbereich

Diese Internationale Norm bietet einen Leitfaden für spezifische Tätigkeiten bei der Bearbeitung von digitalen Beweismitteln, wozu die Identifikation, Mitnahme, Sicherung und Aufrechterhaltung von beweiskräftigen digitalen Beweismitteln zählt. Diese Internationale Norm liefert einen Leitfaden für Personen im Hinblick auf übliche Situationen, die während des Bearbeitungsprozesses von digitalen Beweismitteln eintreten und unterstützt Organisationen bei deren Disziplinarverfahren und erleichtert den Austausch von digitalen Beweismitteln zwischen Rechtsordnungen.

Diese Internationale Norm enthält Hinweise für folgende Geräte und/oder Funktionen, die unter verschiedenen Umständen zum Einsatz kommen:

- digitale Speichermedien, die in handelsüblichen Computern verbaut sind, wie Festplatten, Floppy Disks, optische Datenspeicher und magneto-optische Disketten (MO-Disks), Datenträger mit vergleichbaren Funktionen;
- Mobiltelefone, persönliche digitale Assistenten (PDA, en: Personal Digital Assistants), persönliche elektronische Geräte (PED, en: Personal Electronic Devices), Speicherkarten;
- mobile Navigationssysteme;
- digitale Foto- und Videokameras (einschließlich CCTV);
- handelsübliche Computer mit Netzwerkanschlüssen;
- auf TCP/IP und anderen Protokollen basierende Netzwerke;
- Geräte mit vergleichbaren Funktionen, wie in den vorstehenden Punkten genannt.

ANMERKUNG 1 Die vorstehende Auflistung der Geräte ist eine exemplarische Liste und erhebt keinen Anspruch auf Vollständigkeit.

ANMERKUNG 2 Die Umstände umfassen die vorstehend genannten Geräte, die in unterschiedlichen Varianten vorliegen können. Beispielsweise kann ein Automobilsystem ein mobiles Navigationssystem enthalten, einen Datenspeicher und ein sensorisches System.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/TR 15801, *Document management — Information stored electronically — Recommendations for trustworthiness and reliability*

ISO/IEC 17020, *Conformity assessment — Requirements for the operation of various types of bodies performing inspection*

ISO/IEC 17025:2005, *General requirements for the competence of testing and calibration laboratories*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000, ISO/IEC 17020, ISO/IEC 17025, ISO/TR 15801 und die folgenden Begriffe.

3.1

Sicherung

(en: acquisition)

Prozess zur Erstellung einer Kopie von Daten innerhalb eines festgelegten Bereiches

ANMERKUNG Das Ergebnis der Sicherung ist eine Kopie von potentiellen digitalen Beweismitteln.

3.2

zugewiesener Speicherplatz

Bereich auf einem digitalen Speichermedium, einschließlich des Primärspeichers, der zur Speicherung von Daten, einschließlich Metadaten, genutzt wird

3.3

Mitnahme

Prozess zur Sammlung von physischen Elementen, die potentielle digitale Beweismittel enthalten

3.4

digitales Gerät

elektronische Anlage zur Verarbeitung oder Speicherung von digitalen Daten

3.5

digitale Beweismittel

Informationen oder Daten, die in binärer Form gespeichert oder übertragen werden und die im Sinne eines Beweismittels als relevant befunden werden dürfen

3.6

digitale Beweismittelkopie

Kopie des digitalen Beweismittels, die erstellt wurde, um die Verlässlichkeit des Beweismittels aufrecht zu erhalten, indem sowohl das digitale Beweismittel als auch die Verifizierungsmaßnahmen eingeschlossen sind, wobei die Verifizierungsmethode entweder in die zur Verifizierung verwendeten Werkzeuge eingebettet sein oder eigenständig vorliegen kann

3.7

Ersteinschreiter für digitale Beweismittel

DEFR

(en: Digital Evidence First Responder)

Person, die dazu befugt, ausgebildet und qualifiziert ist, um als Erste am Untersuchungsort (en: incident scene) tätig zu werden und die Mitnahme und Sicherung von digitalen Beweismitteln vorzunehmen und dabei die Verantwortung für die Handhabung dieser Beweismittel trägt

ANMERKUNG Befugnis, Ausbildung und Qualifikation sind die vorausgesetzten Anforderungen, die notwendig sind, um verlässliche digitale Beweismittel zu erbringen, wobei jedoch individuelle Gegebenheiten dazu führen können, dass eine Person nicht alle drei Anforderungen erfüllt. In diesem Fall sollten die vor Ort geltenden Gesetze, organisationsbezogene Vorgaben und die individuellen Gegebenheiten berücksichtigt werden.

3.8

Spezialist für digitale Beweismittel

DES

(en: Digital Evidence Specialist)

Person, die die Aufgaben eines DEFR übernehmen kann und über besondere Fachkenntnisse, Fähigkeiten und Fertigkeiten verfügt, um eine Vielzahl an technischen Fragen zu beantworten

ANMERKUNG Ein DES kann spezielle Kompetenzen besitzen, wie zum Beispiel Zugang zu Netzwerken, RAM-Zugriff, Ausführen von Systemsoftware oder Kenntnisse über Großrechner (Mainframes).

3.9

digitales Speichermedium

Gerät, auf dem digitale Daten aufgezeichnet werden können

[angepasst aus ISO/IEC 10027:1990]

3.10

Beweiserhaltungseinrichtung

sichere Umgebung oder ein Ort, in der bzw. an dem die mitgenommenen oder gesicherten Beweismittel gespeichert oder gelagert werden

ANMERKUNG 1 zum Begriff Eine Beweiserhaltungseinrichtung sollte frei von Magnetfeldern, Staub, Schwingungen, Feuchtigkeit oder anderen Umwelteinflüssen sein (wie extreme Temperaturen oder Luftfeuchte), die die potentiellen digitalen Beweismittel in der Einrichtung schädigen können.

3.11

Hash-Wert

Bit-Kette als Ergebnis einer Hash-Funktion

[ISO/IEC 10118-1:2000]

3.12

Identifikation

Prozess, der die Suche nach, das Erkennen und die Dokumentation von potentiellen digitalen Beweismitteln umfasst

3.13

Imaging

Prozess zur Erstellung einer bit-weisen Kopie eines digitalen Speichermediums

ANMERKUNG 1 zum Begriff Die bit-weise Kopie wird auch als physische Kopie bezeichnet.

BEISPIEL Beim Imaging-Prozess einer Festplatte würde der DEFR auch die Daten kopieren, die zuvor gelöscht worden sind.

3.14

Peripheriegerät

Gerät, das an ein digitales Gerät angeschlossen ist, um dessen Funktionalität zu erweitern

3.15

Erhaltung

Prozess zur Aufrechterhaltung und Sicherung der Integrität und/oder des Originalzustands von potentiellen digitalen Beweismitteln

3.16

Verlässlichkeit

Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen

[ISO/IEC 27000:2009]

3.17

Wiederholbarkeit

Eigenschaft eines durchgeführten Prozesses, die gleichen Prüfergebnisse in derselben Prüfumgebung zu erhalten (derselbe Rechner, dieselbe Festplatte, dieselbe Verfahrensweise usw.)

3.18

Reproduzierbarkeit

Eigenschaft eines Prozesses, die gleichen Prüfergebnisse in einer anderen Prüfumgebung zu erhalten (anderer Rechner, andere Festplatte, anderer Bearbeiter usw.)

3.19

Minderung der Beweiskraft

Durchführen oder Zulassen von Änderungen an potentiellen digitalen Beweismitteln, wodurch deren Beweiswert verringert wird

3.20

Systemzeit

Zeit, die von der Systemuhr generiert und vom Betriebssystem verwendet wird, und nicht die Zeit, die vom Betriebssystem errechnet wurde

3.21

Verfälschen

Vorgang der vorsätzlichen Durchführung oder Genehmigung von Änderungen an den digitalen Beweismitteln (d. h. absichtliche oder zielgerichtete Minderung der Beweiskraft)

3.22

Zeitstempel

zeitabhängiger Parameter, der einen Zeitpunkt im Hinblick auf einen gemeinsamen Zeitbezug bezeichnet

[ISO/IEC 11770-1:1996]

3.23

nicht zugewiesener Speicherplatz

Bereich auf einem digitalen Speichermedium, einschließlich des Primärspeichers, der nicht vom Betriebssystem zugewiesen ist und der für die Speicherung von Daten, einschließlich Metadaten, zur Verfügung steht

3.24

Validierung

Bestätigung durch Beibringen eines objektiven Nachweises, dass die Anforderungen für einen spezifischen Verwendungszweck oder eine spezifische Anwendung erfüllt worden sind

[ISO/IEC 27004:2009]

3.25

Verifizierungsfunktion

Funktion, die verwendet wird, um zu verifizieren, dass zwei Datensätze identisch sind

ANMERKUNG 1 zum Begriff Zwei unterschiedliche Datensätze sollten mithilfe der Verifizierungsfunktion keine Übereinstimmung ergeben.

ANMERKUNG 2 zum Begriff Verifizierungsfunktionen werden in der Regel mit Hash-Funktionen wie MD5, SHA1 usw. umgesetzt, wobei jedoch andere Methoden ebenfalls angewendet werden dürfen.

3.26

flüchtige Daten

Daten, die besonders anfällig für Veränderung sind und leicht modifiziert werden können

ANMERKUNG 1 zum Begriff Eine Änderung kann das Abschalten der Stromversorgung oder Einfluss durch ein Magnetfeld sein. Zu den flüchtigen Daten zählen ebenfalls Daten, die sich ändern, wenn sich der Systemstatus ändert. Beispiele sind im RAM gespeicherte Daten und dynamische IP-Adressen.

4 Abkürzungen

AVI	Audio Video Interleave
CCTV	Videouberwachungsanlage (en: Closed Circuit Television)
CD	Compact Disk
DNS	Desoxyribonukleinsäure
DEFR	Ersteinschreiter für digitale Beweismittel (en: Digital Evidence First Responder)
DES	Spezialist für digitale Beweismittel (en: Digital Evidence Specialist)
DVD	Digital Video/Versatile Disk
ESN	elektronische Seriennummer (en: Electronic Serial Number)
GPS	globales Positionsbestimmungssystem (en: Global Positioning System)
GSM	globales System für mobile Funkkommunikation (en: Global System for Mobile Communication)
IMEI	International Mobile Equipment Identity
IP	Internetprotokoll (en: Internet Protocol)
ISIRT	Informationssicherheitsnotfallteam (en: Information Security Incident Response Team)
LAN	lokales Netzwerk (en: Local Area Network)
MD5	Message-Digest Algorithm 5
MP3	MPEG Audio Layer 3
MPEG	Expertengruppe für bewegte Bilder (en: Moving Picture Experts Group)
NAS	netzgebundener Speicher (en: Network Attached Storage)
PDA	persönlicher digitaler Assistent (en: Personal Digital Assistant)
PED	persönliches elektronisches Gerät (en: Personal Electronic Device)
PIN	persönliche Identifikationsnummer (en: Personal Identification Number)
PUK	PIN-Entsperrschlüssel (en: PIN Unlock Key)
RAID	redundante Anordnung unabhängiger Festplatten (en: Redundant Array of Independent Disks)
RAM	Direktzugriffsspeicher (en: Random Access Memory)
RFID	Identifizierung mithilfe elektromagnetischer Wellen (en: Radio Frequency Identification)
SAN	Speichernetzwerk (en: Storage Area Network)
SHA	sicherer Hash-Algorithmus (en: Secure Hash Algorithm)
SIM	Teilnehmer-Identitätsmodul (en: Subscriber Identity Module)
USB	universeller serieller Bus (en: Universal Serial Bus)
UPS	unterbrechungsfreie Stromversorgung (en: Uninterruptible Power Supply)
USIM	universelles Teilnehmer-Identitätsmodul (en: Universal Subscriber Identity Module)
UV	Ultraviolett
WLAN	kabellose Netzwerkverbindung (en: „Wi-Fi“ Wireless Fidelity)

5 Überblick

5.1 Kontext für die Mitnahme von digitalen Beweismitteln

Digitale Beweismittel können für den Einsatz in vielen verschiedenen Szenarien erforderlich sein. Bei jedem dieser Szenarien liegt ein unterschiedliches Gleichgewicht der Einflussfaktoren Beweiskraft, Aktualität der Analyse, Wiederherstellung von Systemen und Kosten für die Mitnahme der digitalen Beweismittel vor. Aus diesem Grund wird von Organisationen gefordert, einen Priorisierungsprozess durchzuführen, der die Anforderungen ermittelt und ein Gleichgewicht zwischen Beweiskraft, Aktualität und Systemwiederherstellung schafft, bevor der DEFR beauftragt wird. Ein Priorisierungsprozess umfasst die Bewertung des verfügbaren Materials, um den möglichen Beweiswert sowie die Reihenfolge, in der die potentiellen digitalen Beweismittel mitgenommen, gesichert oder erhalten werden sollten, zu bestimmen. Die Priorisierung wird durchgeführt, um das Risiko, dass die Beweiskraft potentieller digitaler Beweismittel vermindert wird, auf ein Mindestmaß zu verringern, und um die Beweiskraft der gesammelten potentiellen digitalen Beweismittel auf ein Höchstmaß zu steigern.

5.2 Grundsätze der digitalen Beweisführung

In den meisten Rechtsordnungen und Organisationen wird die digitale Beweisführung von drei wesentlichen Grundsätzen gesteuert: Relevanz, Verlässlichkeit und Vollständigkeit. Diese drei Grundsätze sind dabei für alle Untersuchungen wichtig und nicht nur bei digitalen Beweismitteln, die in Gerichtsverfahren zulässig sind. Digitale Beweismittel sind relevant, wenn es darum geht, eine Frage eines spezifischen Falls zu belegen oder zu widerlegen. Auch wenn die ausführliche Definition von „Verlässlichkeit“ in den verschiedenen Rechtsordnungen unterschiedlich ausgelegt wird, ist die allgemeine Bedeutung dieses Grundsatzes, „sicherzustellen, dass das digitale Beweismittel ist, was es vorgibt zu sein“, weit verbreitet. Nicht immer ist es notwendig, dass der DEFR alle Daten mitnehmen oder eine vollständige Kopie des digitalen Originalbeweismittels anfertigen muss. Vielmehr bedeutet das Konzept der Vollständigkeit in vielen Rechtsordnungen, dass der DEFR ausreichend potentielle digitale Beweismittel sammeln muss, um die Untersuchungsgegenstände angemessen prüfen oder untersuchen zu können. Dieses Konzept zu verstehen ist für den DEFR von großer Bedeutung, um den Aufwand ordnungsgemäß priorisieren zu können, wenn gleichzeitig Zeit und Kosten zu berücksichtigen sind.

ANMERKUNG Der DEFR sollte sicherstellen, dass die Mitnahme von potentiellen digitalen Beweismitteln gemäß den vor Ort geltenden Gesetzen und den sich aus den spezifischen Umständen ergebenden Vorschriften erfolgt.

Alle vom DEFR und DES zu verwendenden Prozesse sollten vor ihrem Einsatz validiert worden sein. Falls die Validierung extern erfolgt, sollte der DEFR oder der DES verifizieren, dass die Validierung für den spezifischen Einsatz der Prozesse und für die Umgebung und Gegebenheiten, unter denen die Prozesse durchgeführt werden, angemessen ist. Der DEFR oder DES sollte außerdem

- a) alle Maßnahmen dokumentieren,
- b) eine Methode bestimmen und anwenden, mit der die Fehlerfreiheit und Verlässlichkeit der Kopie der potentiellen digitalen Beweismittel im Vergleich zur Originalquelle festgestellt werden kann und
- c) erkennen, dass der Vorgang der Erhaltung von potentiellen digitalen Beweismitteln nicht immer eingriffsfrei erfolgen kann.

5.3 Anforderungen an die Handhabung von digitalen Beweismitteln

5.3.1 Allgemeines

Die in 5.2 dargelegten Grundsätze können wie folgt eingehalten werden:

- Relevanz: Es sollte die Möglichkeit bestehen, aufzuzeigen, dass das gesicherte Beweismaterial für die Untersuchung relevant ist, d. h. dass es wertvolle Informationen zur Unterstützung der Untersuchung des jeweiligen Vorfalls enthält und dass es gute Gründe für deren Sicherung gab. Durch Audits und

Begründungen sollte der DEFR in der Lage sein, die umgesetzten Verfahren zu beschreiben und zu erläutern, wie die Entscheidung zur Sicherung jedes Beweismittels getroffen wurde.

- **Verlässlichkeit:** Alle Prozesse, die bei der Bearbeitung von potentiellen digitalen Beweismitteln eingesetzt werden, sollten überprüfbar und wiederholbar sein. Die Ergebnisse aus der Anwendung solcher Prozesse sollten reproduzierbar sein.
- **Vollständigkeit:** Der DEFR sollte darauf achten, dass ausreichend Beweismaterial erfasst worden ist, um eine ordentliche Untersuchung durchführen zu können. Der DEFR sollte in der Lage sein, durch Audits und Begründungen eine Angabe darüber zu machen, wie viel Beweismaterial insgesamt betrachtet worden ist und welche Verfahren dabei angewendet wurden, um zu entscheiden, wie viel und welches Beweismaterial zu erheben ist.

ANMERKUNG Das Beweismaterial kann durch Sicherung der Daten- und/oder Mitnahme des Beweismittels erhoben werden.

Es gibt vier grundlegende Aspekte bei der Bearbeitung von digitalen Beweismitteln: Auditierbarkeit, Begründbarkeit und entweder Wiederholbarkeit oder Reproduzierbarkeit, abhängig von den jeweiligen Gegebenheiten des Einzelfalls.

5.3.2 Auditierbarkeit

Für einen unabhängigen Gutachter oder andere befugte interessierte Parteien sollte die Möglichkeit bestehen, die durchgeführten Tätigkeiten des DEFR oder DES zu bewerten. Dies wird durch eine angemessene Dokumentation aller vollzogenen Maßnahmen ermöglicht. Der DEFR und der DES sollten in der Lage sein, den Entscheidungsfindungsprozess bei der Auswahl einer bestimmten Vorgehensweise zu begründen. Vom DEFR und DES durchgeführte Prozesse sollten für ein unabhängiges Gutachten zur Verfügung stehen, um zu bestimmen, ob eine geeignete wissenschaftliche Methode, Technik oder ein geeignetes wissenschaftliches Verfahren eingehalten wurde.

5.3.3 Wiederholbarkeit

Die Wiederholbarkeit gilt als sichergestellt, wenn unter folgenden Bedingungen die gleichen Untersuchungsergebnisse erzielt werden:

- durch Einsatz derselben Messverfahren und Messmethoden;
- durch Einsatz derselben Messgeräte und unter denselben Messbedingungen;
- wenn die Prüfergebnisse jederzeit nach der ursprünglichen Prüfung wiederholt werden können.

Ein ausreichend befähigter und erfahrener DEFR sollte in der Lage sein, alle in der Dokumentation beschriebenen Prozesse durchzuführen und dabei ohne Anleitung oder Interpretation die gleichen Ergebnisse zu erzielen. Der DEFR sollte sich dessen bewusst sein, dass es zu Situationen kommen kann, in denen es nicht möglich sein könnte, den Test zu wiederholen, z. B. wenn eine Original-Festplatte kopiert und anschließend wieder in Gebrauch genommen wurde oder wenn ein Untersuchungsobjekt einen flüchtigen Speicher umfasst. In diesem Fall sollte der DEFR sicherstellen, dass der Sicherungsprozess verlässlich ist. Um die Wiederholbarkeit sicherzustellen, sollten eine Qualitätskontrolle und eine Dokumentation des Prozesses erfolgen.