2101

Informationstechnologie (IT)
Teilgebiet IT-Forensik

Definition des Sachgebiets
Fachliche Bestellungsvoraussetzungen

Stand: 12/2024
Revisionsnummer: 0
Erste Fassung: 12/2024

DIHK Deutsche Industrie- und Handelskammer
IfS

1 Sachgebietseinteilung und Bestellungstenor

Die Informationstechnologie (IT) hat alle Wirtschafts- und Lebensbereiche durchdrungen und besitzt damit eine wichtige Querschnittsfunktion. Fachliche Bestellungsvoraussetzungen müssen daher notwendigerweise sinnvolle Teilgebiete abgrenzen, gleichzeitig aber in geeigneter Weise solche Bereiche zusammenfassen, die von einer/einem einzelnen Sachverständigen abgedeckt werden können.

Sachverständige für das Teilgebiet „IT-Forensik“ sichern und analysieren digitale Spuren und Beweismittel, um schädigende Handlungen und Straftaten gerichtsverwertbar aufzuklären sowie nachzuweisen. Sie werden insbesondere von Ermittlungsbehörden (Staatsanwaltschaften und Kriminalpolizei) beauftragt, um beschlagnahmte Hardware und Daten auszuwerten. Dabei geht es vor allem um die Aufklärung von Straftaten im Bereich der Wirtschaftskriminalität, strafbarem politischem Extremismus, Terrorismus sowie Kinderpornographie. Darüber hinaus werden Sachverständige in der „IT-Forensik“ von privaten und öffentlichen Auftraggebenden mit der Untersuchung von Betriebsstörungen, Sabotage, Spionage und Fehlfunktionen der IT beauftragt.

2 Vorbildung von Antragstellenden

2.1 Studium und praktische Tätigkeit

Erfolgreich abgeschlossenes Studium an einer Hochschule nach dem Hochschulrahmengesetz mit einer Regelstudienzeit von mindestens sechs Fachsemestern in den Fachrichtungen

- Informatik/Wirtschaftsinformatik
- Ingenieurwissenschaften
- Wirtschaftswissenschaften
- Wirtschaftsingenieurwissenschaften
- Physik
- Mathematik bzw. entsprechende Kombinationen

und eine mindestens fünfjährige praktische Tätigkeit, die ihrer Art nach geeignet war, die erforderlichen Kenntnisse zu vermitteln,

oder Nachweis von Erfahrung, Aus- und Fortbildung sowie regelmäßig eine 10-jährige praktische Tätigkeit, die ihrer Art nach geeignet sind, die erforderlichen gleichwertigen Kenntnisse und Kompetenzen zu vermitteln.

2.2 In allen Fällen müssen Antragstellende nachweisen, dass sie in fachverantwortlicher Stellung im Bereich der IT tätig sind und sich mit Themen wie z. B. Zeit, Kosten, Qualität, Markt, Branchenüblichkeit, Stand der Technik, auseinandergesetzt haben. Das erforderliche Erfahrungsniveau wird u. a. durch folgende Tätigkeiten gekennzeichnet:

- Umfassende Systementwicklungen
- Erarbeitung umfangreicher Dokumentationen
- Erarbeitung umfangreicher Pflichtenhefte
- Erstellung von Gutachten oder vergleichbaren schriftlichen Ausarbeitungen.

2.3 Antragstellende sollen eine mindestens dreijährige einschlägige praktische Tätigkeit als Sachverständige/r nachweisen. Diese Tätigkeit darf - vom Zeitpunkt der Antragstellung an gerechnet - nicht länger als ein Jahr zurückliegen.

2.4 Die vorerwähnten Voraussetzungen sind durch Vorlage von fünf selbstverfassten Gutachten nachzuweisen. Die Gutachten müssen die Breite des Sachgebiets abdecken und sollen eine anspruchsvolle Fragestellung aufweisen. Die „Hinweise zum Aufbau eines schriftlichen Sachverständigengutachtens” sind zu beachten.

2.5 Besonderheiten bei der persönlichen Eignungsprüfung

Zusätzlich zur Prüfung der persönlichen Eignung durch die IHK erfolgt in einigen Bundesländern eine Sicherheitsüberprüfung durch die Staatsanwaltschaft oder Polizei. Davon können auch die Mitarbeitenden der/des Sachverständigen betroffen sein. Die Sicherheitsüberprüfungen werden in regelmäßigen Abständen wiederholt. Darüber hinaus kann die Beauftragung in bestimmten Deliktsbereichen von einer vorgeschalteten speziellen Beschulung durch die Staatsanwaltschaft oder Polizei abhängig gemacht werden.

3 Allgemeines

Antragstellende müssen zum Nachweis der besonderen Sachkunde Kenntnisse in den jeweils angegebenen Vertiefungsgraden nachweisen:
Grundkenntnisse (G)
Vertiefte Kenntnisse (V)
Detailkenntnisse (D)

Die in Ziffer 4 - 6 angegebenen Beispiele dienen lediglich zur Erläuterung. Sie erheben keinen Anspruch auf Vollständigkeit.

4 Rechtsgrundlagen

4.1 Die „Allgemeinen Rechtskenntnisse Sachverständigentätigkeit“ in der jeweils gültigen Fassung sind Bestandteil dieser Bestellungsvoraussetzungen.

4.2 Die folgenden Gesetze und Verordnungen müssen bekannt sein:

a) einschlägige versicherungsrechtliche Vorschriften (G)
b) einschlägige Vorschriften des Ordnungswidrigkeitenrechts (G)
c) einschlägige Vorschriften des Strafrechts (§§ 11 Abs. 3, 174, 176ff, 182, 184 a-d, 201a, 202 a-c, 206, 263a, 266b, 268, 269, 270 StGB) (G)
d) weitere einschlägige Straftatbestände aus UWG, UrhG, HGB, AO) (G)
e) Telekommunikationsgesetz (TKG, insbesondere Überwachung der Telekommunikation) (G)
f) Datenschutzgesetze (V)
g) Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI- Kritisverordnung - BSI-KritisV) (G)
h) Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) (G)

4.3 Strafrechtliche und kriminalistische Kenntnisse

a) Verfahrensweisen im Ermittlungsverfahren (G)
b) Beauftragung im Ermittlungsverfahren (G)
c) Auswertungsmöglichkeiten und Beweisverwertungsverbote (G)
d) Aussageverweigerungsrechte) (G)
e) Täterterminologie (V)

5 Allgemeine Fachkenntnisse

Von Antragstellenden wird erwartet, dass sie das gesamte Spektrum ihres Sachgebietes kennen und aufgrund ihrer Fachkenntnisse ihre Tätigkeit systematisch vornehmen und nachvollziehbar beschreiben und bewerten können.
Zu den im Folgenden dargestellten allgemeinen Fachkenntnisse können unter Ziffer 6 weitere Spezialkenntnisse gefordert sein.

5.1 Hardware

a) Physik, Elektrotechnik, Werkstoffkunde, Messtechnik, Mathematik (G)
b) IT-Sicherheit (V)

5.1.1. Bauelemente (G)

Aufbau, Wirkungsweise und Dimensionierung wesentlicher elektrischer und elektronischer Bauelemente (passive, aktive, elektromechanische und elektrochemische Bauelemente)

5.1.2. Baugruppen/Geräte (G)

Technologie, Aufbau und wesentlichen Funktionen von Baugruppen und Geräten der Informationstechnologie

5.1.3. Netzwerktechnik (G)

Übertragungsverfahren, Topologien, Komponenten der Netzwerktechnik

5.1.4. Allgemeine Computerhardware

a) Computer (Rechnerorganisation, Rechnerarchitektur) (V)
b) Peripheriegeräte (Speichersysteme, Datenein- und -ausgabegeräte) (V)
c) Sensoren und Sicherheitsmodule (V)
d) Energieversorgung und Elektrotechnik (im Zusammenhang mit Hardwarekomponenten und Datenübertragung) (G)

5.2 Software

5.2.1 Informationstechnik

a) Modellierung (Abstraktion, Graphen, Automaten, Strukturen, Prozesse, Berechenbarkeit) (G)
b) Querschnittsverfahren (IT-Sicherheit (V), Qualitätssicherung(G))
c) Programmierparadigmen (G)
d) Algorithmen (G)

5.2.2 Softwareengineering

a) Programmiersprachen (V)
b) Datenstrukturen und Datenbankdesign (D)
c) Systemarchitekturen (G)
d) Schnittstellen (V)
e) Entwicklungsumgebungen (G)

5.2.3 Systemsoftware

a) Betriebssysteme (G); MS Windows, Linux, UNIX , iOS, Android, Mac OS, Symbian (V)
b) Virtualisierungssysteme ((G); VMware, Virtual PC, Citrix) (V)
c) Datenbankmanagementsysteme (DBMS) (Datenbankgrundlagen, Datenbankmodelle, Abfragesprachen, Transaktionsverwaltung, Datenintegrität, Data Warehouses) (V)

5.2.4 Einsatz und Betrieb von Software und Systemen

Standardsoftware (branchenübergreifende Lösungen, branchenspezifische Lösungen, ERP- Systeme, E-Commerce-Lösungen) (G)
Systemintegration und Betrieb von Schnittstellen (G) Konfigurationsmanagement (G)
Systemmonitoring (V) Protokollierung (V)

6 Spezialkenntnisse im Bereich IT-Forensik

6.1 Kenntnisse

a) Grundsätzliche Prinzipien der IT-Forensik (Grundlegende Definitionen und Vorgehensweisen, Nature of Evidence, Locard’sche Regel, Spurentheorie, Prozessmodelle, übliches Nutzerverhalten) (D)
b) Kryptologie (Grundlagen, Prinzipien, Verfahren, Anwendungen, Sicherheit, Erkennung von verschlüsselten Daten, mögliche Verfahren zur Passwortentschlüsselung) (V)
c) Hashwerte (z.B. SHA256, SHA256-3 und alte Verfahren wie MD5) (V)
d) Schlüsselwortsuche vs. Indexsuche (inkl. reguläre Ausdrücke) (V)
e) Gängige Datentypen und Codierungen (INTEGER, FLOAT, DOUBLE, BYTE/STRING/VARCHAR, ARRAY, BOOLEAN, RECORD) (G)
f) Unterschiedliche Codierungen von Zeitstempeln und Zeitzonen (G)
g) Zeichensatzkodierung und Binärdaten-Encoding (V)
h) Digitale Signaturen und Schlüsselverwaltungssysteme (V)
i) Übliche Betrugsansätze und Erscheinungsformen der Cyberkriminalität (Schadsoftware/Malware/Ransomware, Spam, Phishing, DDoS-Angriffe) (D)

6.2 Prozesse und Vorgehensweisen

a) Planung und Durchführung von Sicherstellungsmaßnahmen (D)
b) Untersuchung von Daten mit Hilfe spezialisierter Werkzeuge (D)
c) Aufbereitung der Erkenntnisse (Inhalt, Darstellungsformen, Trennung von Tatsachen und Ableitungen) (D)
d) Chain of Custody Dokumentation (D)
e) Vorgehen für die Sicherstellung laufender Systeme (inkl. Netzwerktrennung) (D)
f) Lagerung, Schutz und Zugang zu Originalbeweismitteln - Verwaltung von Asservaten (V)
g) Erkennen von Beweismittelmanipulationen und -fälschungen bzw. Bewertung der Fälschbarkeit von elektronischen Beweismitteln (betrifft alle Arten von elektronischen Spuren) (D)

6.3 Datenspiegelung und Archivierung

a) Hard- und softwarebasierte Schreibschutzsysteme (PATA, SATA, SCSI, USB, SAS, NVME, Speicherkarten) (V)
b) Planung von Datensicherungsmaßnahmen und Strategie bei Vor-Ort-Beweissicherungen (V)
c) Gängige forensische Datenspiegelungsformate (V)
d) Protokollierung von Lesefehlern und Verifikation der Datenintegrität (D)
e) Sicherung flüchtiger Speicherbereiche (D)

6.4 Auswertung von Netzwerkverkehr

a) Grundlagen Datenübertragung und Vernetzung (Konzepte, Möglichkeiten und Verfahren zur Verbindung von Standorten, Daten- und Telekommunikation) (G)
b) IP-Adressen und deren Verschleierung (Dynamische IP-Adressenzuweisung durch Provider, Open-Proxy, Anonymisierungsnetzwerk TOR, Hidden Services, VPN-Anbieter, CDN/Cloudflare) (V)
c) Netzwerk-Topologien (V)
d) Netzwerkprotokolle und -Basisdienste (IPv4 u. IPv6, TCP, UDP, DNS, DHCP, SMTP, POP, IMAP, HTTP(S)) (V)
e) Auslesen und Sichern von Netzwerkverkehr (Wireshark, tcpdump, Port Mirroring) (V)

6.5 Datenträger, Dateisysteme und Datenrettung

a) Gängige Dateisysteme (FAT, exFAT, NTFS, ReFS, EXT2, EXT3, EXT4, XFS, ReiserFS, APFS, HFS) (V)
b) Gängige Dateisystemverschlüsselungen (Luks, Bitlocker, TrueCrypt/VeraCrypt, Steganos etc.) (V)
c) Physische Datenrettungsmethoden (V)
d) Logische Datenrettungsmethoden (D)
e) Dateiattribute (Zugriffsrechte, Eigenschaften, MACE-Zeitstempel) (D)
f) Spuren der Datenlöschung (D)

g) Sicheres Löschen von Daten (D)
h) Solid-State-Drive-Verhalten (TRIM, Wear Leveling, Garbage Collection, Over- Provisioning, Bad Block Replacement) (V)
i) Spezielle Speicherbereiche von Datenträgern (Bootsektor, Partitionstabellen, HPA-Host Protected Area, DCO Device Configuration Overlay) (V)
j) Volume Shadow Copies, Restore Points, Volume Snapshots (V)
k) Enterprise-Storage (insb. SAS, SAN, NAS, iSCSI, Fiberchannel, RAID) (V)

6.6 Auswertung von Datei-, Verzeichnis- und Datenträgerverweisen und -zugriffsspuren

a) LNK-Dateien, Jumplists, Recent File Lists, Shellbags, Listen zuletzt verwendeter Dateien in Konfigurationsdateien oder -Datenbanken (V)
b) Zuordnung von Dateizugriffsspuren über Volume Name, Volume Serial Number und Zeitstempel (V)
c) USB Device Peering Analyse (Vendor und Product ID, Unique Serial Number, Drive Letter, First-, Last- Time-Connected and Last Removal) (V)

6.7 Auswertung von Dateiinhalten (u.a. Bilder, Videos und Audioaufnahmen)

a) Zuordnung von Bildern und Videos zu Aufnahmegeräten, -orte und -zeiten (V)
b) Deduplizierung und Auffinden bekannter Dateiinhalte anhand von Hashwerten (D)
c) Near-Duplicate-Detection mittels robuster Hashwerte (rHash, PhotoDNA) (V)
d) Zentrale und verzeichnisweise Vorschaubilddatenbanken (V)
e) Gängige Mediendateiformate (JPG, BMP, PNG, HEIC, WebP, AVI, MOV, MPEG, VOB, 3GP etc.) (V)
f) Zentrale Datenbanken zur Speicherung von Zusatzinformationen (V)
g) Möglichkeiten und Erkennung von KI-generierten „deep fakes“ (D)

6.8 Auswertung von Chatsystemen

a) Gängige Chatsysteme (z.B. Skype, ICQ, WhatsApp, Telegram, Knuddels, Kik, Viber, SnapChat, Facebook Messenger, Instagram, Threema, Signal, SMS/MMS etc.) (V)
b) Chatverlaufsprotokolle bzw. -datenbanken (XML-Dateien, SQLite-Datenbanken, JSON- Dateien, Textdateien, etc.) (V)
c) Abgleich von Dateien mit Dateiübertragungsprotokollen (V)

6.9 Auswertung von E-Mail-Nachrichten

a) E-Mail-Container-Datenbanken (Thunderbird-MBox-Format, Outlook PST-, OST- und NST-Dateien) (V)
b) E-Mail-Server-Datenbanken (z.B. MS Exchange) (V)
c) E-Mail-Client-Anwendung vs. Webmailer Nutzungsspuren (V)
d) E-Mail-Header-Analyse (Adressierung, Übertragungsverlauf, Signaturverfahren, Nachrichtenverschlüsselung) (D)

6.10 Auswertung von Internetbrowsernutzungsspuren

a) Bekannte Browservarianten (WebKit = Safari, Chrome, Opera und Edge; Gecko = Firefox und TOR; etc.) (V)
b) Auswertbare Nutzungsspuren (u.a. Verlauf, Cache, Lesezeichen, Form-History, Cookies, Login Daten) (V)
c) Privater Browsing-Modus (V)
d) Abgleich von Dateien mit Downloadspuren (V)
e) Internetsuchmaschinen-Nutzung (Suchbegriffe und Reverse-Bildersuche) (V)

6.11 Auswertung von P2P- und F2F-Tauschbörsen

a) Gängige Tauschbörsen-Programme und -Netzwerke (eMule/aMule, Shareaza, MLDonkey, Frostwire, Bittorrent, Gigatribe, etc., ed2k-, Gnutella-, Bittorrent-Netzwerk) (V)
b) Tauschbörsen-Protokoll- und Konfigurationsdateien (u.a. known.met, Partfiles, Suchbegriffseingaben, Tauschverzeichniskonfiguration, Up- und Downloadraten und -Einstellungen, Statistikdaten, Vorschaudateien, Dateihashwerte) (V)
c) Überwachungsmethoden von Tauschbörsennetzwerken (V)

6.12 Auswertung von Cloudstorages und Cloudanwendungen

a) Cloudstorage Anbieter (Dropbox, Amazon Cloud, MEGA, OneDrive, Box, Google Drive) (V)
b) Synchronisationsverzeichnisse (On Demand Streaming vs. Lokale Offline Kopie) (V)
c) Protokolldaten (filecache.dbx, sync_history.db, sync.db, streemsfs.db) (V)
d) Auswertung von Auditlogs und Erzeugen von eDiscovery-Exporten (z.B. MS 365 Plattform, AWS, Google Cloud) (V)

6.13 Spiegelung und Auswertung von Mobilgeräten

a) Mobilgeräte-Betriebssysteme (iOS, Android) (V)
b) Auslesemethoden (Physical, Advanced Logical, Logical, iCloud-Backup, iTunes-Backup, Kies/Smart Switch) (V)
c) Gerätezugangssperren und -Passwörter (D)
d) Geopositionsdaten (Funkzelle, WLAN-Hotspots, GPS) (V)
e) Geräteidentifikationsmerkmale (SIM, IMEI, IMSI, ICCID, Apple-ID, Gerätename) (G)
f) Mediendateienspeicherung (DCIM, Android Gallery 3D, Anwendungsverzeichnisse) (V)
g) Ereignisprotokolldaten (Health-Data, WLAN-Verbindungen, Call-Logs, Benachrichtigungen, Batteriestatus, etc.) (V)

6.14 Auswertung von Betriebssystem- und Programmnutzungspuren und Konfigurationen

a) Betriebssystemkonfigurationen (Windows-Registrierungsdatenbanken, /etc Verzeichnis) (V)
b) Nutzerzuordnung (Computername, eingetragener Besitzer, eingetragene Onlinekonten, registrierte E-Mail-Adressen, Nutzerkontoname und -passwort) (V)
c) Nutzeranmeldungen (Kontoerstellung, letzte An- und Abmeldungen, lokal und remote, letzter Shutdown) (V)
d) Installationsverlauf (Betriebssystemversion und -updates, installierte Anwendungen) (V)
e) Netzwerkkonfigurationen (Interfaces, WLAN SSID, Domain, MAC, Drahtgebunden, Drahtlos, VPN, Mobilfunk) (V)
f) Programmausführungsnutzungsspuren (Prefetch, bash_history, SRUM, UserAssist, etc.) (V)
g) Betriebssystemereignisanzeige (Windows Event Logs, /var/log/) (V)
h) Anwendungsforensik – Methoden und Techniken zur Analyse von Spuren auch unbekannter Anwendungen (V)

6.15 Fallbezogene Auswertungsstrategien und -analysen

a) Beschreibung zielführender Datensicherungs- und Auswertungsstrategien, Abhängigkeit von konkreten Fallkonstellationen (V)
b) Umgang mit unbekannten bzw. neuartigen Systemen und Anwendungen (V)

7 Technische Ausstattung

Sachverständige müssen über eine angemessene IT-Ausrüstung und die gängige Software verfügen, die es ihnen erlaubt, Programme, Komponenten, Geräte und Rechner (auch im Verbund) zu prüfen. Sie müssen mit der Bedienung und den Funktionen der Systeme auf Hard- und Software-Ebene vertraut und in der Lage sein, Systeme selbst einzurichten. Sachverständige müssen mit dieser Ausrüstung Sachverhalte zuverlässig dokumentieren können.

8 Räumliche Voraussetzungen

Die Überlassung inkriminierten Materials zu Auswertungszwecken wird in bestimmten Deliktsbereichen von der Erfüllung sicherheitstechnischer Voraussetzungen bei den Büroräumen abhängig gemacht. Hierbei sind gesteigerte Anforderungen an die Einbruchsicherheit zu stellen, wie auch an Vorkehrungen zur Verhinderung des unbefugten Zutritts während der Bürozeiten (Zugangskontrollen, intern gesicherte Bereiche) sowie an die Sicherung von Asservaten vor unberechtigtem Zugriff. Die Sicherheitsüberprüfung erfolgt gegebenenfalls durch die Staatsanwaltschaft oder Polizei und kann in regelmäßigen Abständen wiederholt werden.