Inhaltsverzeichnis

1	**Einführung in die IT-Forensik: Spurensuche im digitalen Zeitalter**	1
1.1	**Cybercrime-Vorfälle**	5
1.2	**Der Begriff „IT-Forensik"**	5
1.3	**Die Begriffe „Digitale Spur" und „Digitales Artefakt"**	7
1.4	**Die W-Fragen in der IT-Forensik**	10
1.5	**Die Begriffe „Gerichtsfestigkeit" und „Gerichtsverwertbarkeit"**	11
1.6	**Teilgebiete der IT-Forensik**	15
1.7	**Die Bedeutung der Zeit**	16
1.8	**Was ist Anti-Forensik?**	18
1.9	**Modelle der IT-Forensik**	19
1.9.1	SAP-Modell (Secure, Analyse, Present)	19
1.9.2	BSI-Modell	21
1.9.3	EDRM-Modell	23
1.9.4	NIST-Modell	25
1.9.5	Casey-Modell	26
1.9.6	CERT-Taxonomie	27
1.9.7	MITRE ATT&CK-Framework	28
1.9.8	Vergleich der Modelle und das pSAP-Modell	28
1.9.9	pSAP-Modell	30
1.10	**Lerninhalte zusammengefasst**	31
1.11	**Reflexionsfragen**	32
2	**Vorbereitung (pSAP: prepare)**	35
2.1	**Strategische Vorbereitung**	36
2.1.1	Forensik-Koffer	39
2.1.2	Writeblocker	41
2.1.3	Forensik-Software	44
2.2	**Operationale Vorbereitung**	45
2.3	**Identifizierung relevanter Datenquellen**	45
2.3.1	Datenquellen-Übersicht	45
2.3.2	RAID-Systeme	48
2.3.3	Cloud- und virtuelle Systeme	49
2.4	**Datenquellen nach Nutzerinteraktion**	51
2.5	**Datensammlung von flüchtigen und persistenten Daten**	55
2.5.1	Persistente, Semipersistente und flüchtige Daten	55
2.5.2	Live-Forensik	57
2.5.3	Post-Mortem-Forensik	58
2.5.4	Post-Live-Forensik	59
2.6	**Transport von zu sichernden Geräten**	59
2.7	**Planung einer automatisierten Analyse**	60
2.8	**Lerninhalte zusammengefasst**	61
2.9	**Reflexionsfragen**	62

3	**Datensicherung (pSAP: Secure)**	63
3.1	**Allgemeine Regeln**	64
3.1.1	Technische Sicherungsreihenfolge	64
3.1.2	Imaging und Hashwertbildung	65
3.1.3	Datenformate für IT-forensische Images	68
3.2	**Sicherung von flüchtigen Daten**	70
3.2.1	Hauptspeichersicherung	71
3.2.2	Cold-Boot-Vorgehen	72
3.2.3	Software	74
3.3	**Sicherung von lokalen Datenträgern**	75
3.4	**Sicherung von Daten auf mobilen Geräten**	84
3.4.1	Datenspeicher	84
3.4.2	Physische Extraktion	86
3.4.3	Filesystem-Extraktion	88
3.4.4	Logische Extraktion	89
3.4.5	Screen Capturing	90
3.5	**Sicherung von Daten in RAID- und virtuellen Systemen**	90
3.5.1	RAID-Systeme	90
3.5.2	Virtuelle Systeme	91
3.6	**Lerninhalte zusammengefasst**	94
3.7	**Reflexionsfragen**	96
4	**Datenauswertung (pSAP: Analyse)**	97
4.1	**Strategisches Vorgehen**	99
4.2	**Technische Grundlagen**	103
4.2.1	Aufbau von Datenträgern	103
4.2.2	Dateisysteme	104
4.2.3	Zeit- und Datumsangaben	106
4.2.4	Gelöschte Daten, File Carving, Sonderbereiche	107
4.3	**Analyse-Tools**	113
4.4	**Aggregation, Strukturierung und Reduktion der Daten**	118
4.5	**Analyse von Systemdaten**	122
4.5.1	Windows-Auswertung	123
4.5.2	Unix-Auswertung	124
4.6	**Analyse von Anwenderdaten**	125
4.6.1	Analyse von E-Mails	125
4.6.2	Analyse von Texten	127
4.6.3	Analyse von Bildern	129
4.6.4	Analyse von Audios	131
4.6.5	Analyse von Videos	132
4.6.6	Analyse von Kryptowährungen	133
4.7	**Analyse von Mobiltelefonen**	136
4.8	**Analyse von Netzwerkdaten**	141
4.9	**Lerninhalte zusammengefasst**	144
4.10	**Reflexionsfragen**	146

5 **Erstellung von forensischen Berichten (pSAP: Present)** ... 147
5.1 **Schreibstil** ... 148
5.2 **Tagesprotokoll** ... 149
5.3 **Protokollierungstechniken** ... 151
5.4 **Timeline** ... 152
5.5 **Abschlussdokumentation** ... 156
5.5.1 IT-forensischer Bericht ... 156
5.5.2 IT-forensisches Gutachten ... 156
5.6 **Lerninhalte zusammengefasst** ... 164
5.7 **Reflexionsfragen** ... 166

6 **Forensische Analyse von Datenbanken** ... 167
6.1 **Aufbau und Analyse von relationalen Datenbanksystemen** ... 170
6.1.1 Welche Datenbanken existieren? ... 173
6.1.2 Wie sieht die Struktur einer Datenbank aus? ... 174
6.1.3 Wie erhält man systeminterne Informationen? ... 177
6.1.4 Zusammenfassung ... 183
6.2 **Exkurs: SQL-Injektion-Angriffe** ... 183
6.3 **Prozess der Datenbank-Forensik** ... 186
6.3.1 Infrastruktur-Szenarien ... 186
6.3.2 Die W-Fragen in der Datenbank-Forensik ... 189
6.3.3 Datenbankartefakte ... 190
6.3.4 Vorgehensweise in der DB-Forensik ... 191
6.4 **Spezialfall: Analyse von SQLite-Datenbanken** ... 199
6.4.1 Datenbankartefakte ... 200
6.4.2 Datenspeicherung ... 201
6.4.3 Identifikation von Nutzern ... 201
6.5 **Lerninhalte zusammengefasst** ... 205
6.6 **Reflexionsfragen** ... 206

7 **Informationsgewinnung aus öffentlichen Quellen (OSINT)** ... 207
7.1 **OSINT-Quellen** ... 212
7.2 **OSINT-Suchtechniken** ... 214
7.2.1 Klassifikation von Suchmaschinen ... 214
7.2.2 Aufbau von Suchmaschinen ... 215
7.2.3 Suchmaschinen Hacking und Dorking ... 218
7.3 **OSINT-Tools** ... 220
7.4 **Deepweb- und Darkweb-Recherche** ... 222
7.5 **Systematische OSINT-Recherche** ... 224
7.6 **Lerninhalte zusammengefasst** ... 230
7.7 **Reflexionsfragen** ... 230

8 **Ausblick auf die Zukunft der IT-Forensik** 233
8.1 **Herausforderungen** 234
8.2 **Techniken der Zukunft** 235

Serviceteil
Literatur 240
Stichwortverzeichnis 247