
Dirk Labudde · Michael Spranger
(Hrsg.)

Forensik in der digitalen Welt

Moderne Methoden der forensischen
Fallarbeit in der digitalen
und digitalisierten realen Welt

 Springer Spektrum

Inhaltsverzeichnis

1	Einführung	1
	Dirk Labudde, Frank Czerner und Michael Spranger	
1.1	Forensik – ein aktueller Ein- und Rückblick und der CSI-Effekt	1
1.2	Forensik im System der Wissenschaften	5
1.3	Tatort in der modernen Forensik	7
1.3.1	Der moderne Tatortbegriff	7
1.3.2	Moderne Formen der Spurensicherung	12
1.3.3	Zusammenwachsen von virtueller und realer Welt	14
1.4	Aufgaben und Ziele der forensischen Wissenschaft	16
1.5	Spuren als Beweismittel und deren Beweiswürdigung im Strafprozess	20
	Literatur	22
2	Biometrie und die Analyse digitalisierter Spuren	25
	Dirk Labudde	
2.1	Einleitung	25
2.1.1	Die Identifikation – Wer bin ich?	26
2.1.2	Die Verifikation – Bin ich der, für den ich mich ausbebe?	26
2.2	Biometrie	26
2.2.1	Historischer Streifzug durch die Biometrie in der Forensik	27
2.2.2	Biometrie und das Locard'sche Prinzip	28
2.3	Biometrische Merkmale	30
2.4	Ausgewählte Analyseverfahren	33
2.4.1	Der Fuß als biometrisches Merkmal im Prozess der Digitalisierung	33
2.4.2	Iriserkennung	36
2.5	Fingerabdruckanalyse	39
2.5.1	Der Fingerabdruck als biometrisches Merkmal	39
2.5.2	Technologien zur Aufnahme des Fingerabdrucks	40
2.5.3	Matching	49
2.6	Ausgewählte Forensische Datenbanken	52
2.6.1	DNA-Analysedatei (DAD)	52

2.6.2	Violent Crime Linkage Analysis System (ViCLAS)	52
2.6.3	Integrated Ballistic Identification System (IBIS)	53
2.6.4	Paint Data Query (PDQ)	53
2.6.5	SoleMate	54
2.6.6	TreadMate	54
2.6.7	Automatisches Fingerabdruckidentifizierungssystem (AFIS) . .	54
2.6.8	Eurodac-System	55
	Literatur	55
3	Computergestützte Gesichtswerteil- und Tatortrekonstruktion	59
	Sven Becker und Dirk Labudde	
3.1	Computergestützte forensische 3D-Gesichtswerteilrekonstruktion . . .	59
3.1.1	Einleitung	59
3.1.2	Historische Entwicklung	62
3.1.3	Voraussetzungen, Faktensammlung und Recherchen	62
3.1.4	Klassische Methoden der Gesichtswerteilrekonstruktion . . .	65
3.1.5	Computergestützte Methode der Gesichtswerteilrekonstruktion mittels Open-Source-Software	66
3.2	Studie am Beispiel eines Schädelknochen	69
3.2.1	Hintergründe zum ausgewählten Fall	69
3.2.2	Prozessüberblick	70
3.2.3	Digitalisierung des Schädelknochen	71
3.2.4	Punktwolkenerzeugung und Oberflächenrekonstruktion mittels VisualSfM und CPMVS	71
3.2.5	Modellnachbearbeitung und Editierung mittels MeshLab	74
3.2.6	Positionierung anatomischer Werteilmarker und Rekonstruktion ausgewählter Gesichtswerteile	74
3.3	Schlussfolgerung und Ausblick	78
3.4	Computergestützte Rekonstruktion von Tatorten und Großschadensereignissen	79
3.4.1	Einleitung	79
3.4.2	Studie einer Tatortrekonstruktion an einem historischen Mordfall	80
3.4.3	Unterstützung der Rekonstruktion durch Einsatz moderner unbemannter Flugobjekte	81
	Literatur	86
4	DNA-Phänotypisierung	89
	Anne-Marie Pflugbeil, Karlheinz Thiele und Dirk Labudde	
4.1	DNA-Analytik im forensischen Alltag	89
4.2	Von der Spur zum DNA-Profil	90
4.2.1	Workflow	90
4.2.2	DNA-Marker in der Forensischen Molekulargenetik	92

4.3	Phänotypisierung – DNA als biometrisches Merkmal	95
4.3.1	Phänotyp	95
4.3.2	Phänotypisierungssysteme	96
4.4	Relevante Datenbanken	101
4.5	Rechtliche Aspekte	102
4.6	Anwendung in der Gesichtswerteilrekonstruktion	103
4.7	Zusammenfassung und Ausblick	104
	Literatur	106
5	Digitaler Tatort, Sicherung und Verfolgung digitaler Spuren	113
	Dirk Pawlaszczyk	
5.1	Einleitung	113
5.2	Tatort, Digitale Spuren und Datenquellen	114
5.3	Sicherung digitaler Spuren	118
5.3.1	Live-Response-Akquise	119
5.3.2	Post-mortem-Akquise	125
5.3.3	Datenrekonstruktion mittels Carving	137
5.3.4	Kategorisierung und Filterung der Datenartefakte	140
5.4	Verfolgung digitaler Spuren im Netz	142
5.4.1	Analyse und Rekonstruktion des Browsercaches	143
5.4.2	Tatort Cloud	147
5.4.3	Der Messengerdienst WhatsApp	150
5.4.4	Open Source Intelligence: Tatort soziale Netzwerke	153
5.4.5	Verfolgung von Zahlungsströmen im Bitcoinnetzwerk	156
5.5	Fazit und Ausblick	164
	Literatur	165
6	Textforensik	167
	Michael Spranger und Dirk Labudde	
6.1	Einleitung	167
6.2	Analyse unstrukturierter digitaler Daten	170
6.3	Charakteristik forensischer Texte	172
6.4	Entwicklung einer Kriminalitätsontologie	172
6.4.1	Ontologie-basierte Informationsextraktion	172
6.4.2	Repräsentation von Wissensmodellen	174
6.4.3	Forensisches Ontologiemodell	175
6.5	Ansätze der forensischen Textanalyse	177
6.5.1	Pipeline zur ausführlichen Analyse	177
6.5.2	Identifikation forensischer Rollen	179
6.5.3	Lösungsansatz für das Problem der versteckten Semantik	179
6.6	Kategorisierung forensischer Texte	182

6.7	Forensische Kurznachrichtenanalyse	186
6.7.1	Einleitung	186
6.7.2	Charakteristik inkriminierter Kurznachrichten	187
6.7.3	Eine neue Methode zur Klassifikation forensischer Kurznachrichten	188
6.7.4	Detektion zusammenhängender Konversation	190
6.7.5	Bewertung von Konversationen	193
6.7.6	Erzeugung eines Wörterbuches	195
	Literatur	196
7	Malware Forensics	199
	Christian Hummert	
7.1	Einleitung	199
7.2	Charakteristik – Einteilung von Malware	201
7.2.1	Verbreitung und Wirkung	201
7.2.2	Innere Systematik	203
7.3	Forensische Untersuchung von Malware	203
7.3.1	Belauschen von Malware	203
7.3.2	Inhaltliche Analyse	205
7.4	Malware Antiforensics	206
7.4.1	Kompression von Executables	207
7.4.2	Verschlüsselung von Executables	207
7.4.3	Obfuskation	208
7.4.4	Anti-Debugging Techniken	209
7.5	Malware Anatomie	210
	Literatur	212
8	Audioforensik	215
	Hartmut Luge	
8.1	Einleitung	215
8.2	Überblick zu den Teilgebieten der akustischen Forensik	216
8.2.1	Phonetische Stimmerkennung und Stimmenvergleich (Voice Identification)	216
8.2.2	Nebengeräusche und Geräuscherkennung (Sound Identification)	217
8.2.3	Geräuschsynthese und Beurteilung (Audibility Analysis)	217
8.2.4	Hör- und Sprachverständlichkeitsverbesserung und phonetische Textanalyse (Intelligibility Enhancement)	217
8.2.5	Manipulations- und Echtheitsanalyse (Authenticity Analysis)	218
8.2.6	Zeit-Ereignis-Analyse (Event Sequence Analysis)	218
8.3	Formate und Verfahren der technischen Audioforensik	219
8.3.1	Audioformate und Übertragungskanal	219
8.3.2	Manipulation und Echtheit von Audioaufzeichnungen	222

8.3.3	Formantanalyse und Spracherkennung	225
8.3.4	Sprachverschlüsselung	231
	Literatur	238
9	Methoden des maschinellen Lernens und der Computational Intelligence zur Auswertung heterogener Daten in der digitalen Forensik	239
	Tina Geweniger, Marika Kaden und Thomas Villmann	
9.1	Einleitung	239
9.2	Datenstrukturen und Datenähnlichkeit	240
9.2.1	Daten und Datenstrukturen in der Forensik	240
9.2.2	Datenähnlichkeit – mathematische Beschreibung	241
9.3	Aufgabenstellungen in der Datenanalyse	243
9.4	Prototypbasierte Methoden der CI zum Clustern und Klassifizieren	244
9.4.1	Prototypbasierte Clusteralgorithmen	245
9.4.2	Prototypbasierte Klassifikation – Lernende Vektorquantisierer	255
9.4.3	Andere Verfahren zum Clustern und Klassifizieren – Bemerkungen	259
	Literatur	260
10	Digitale Forensik zwischen (Online-)Durchsuchung, Beschlagnahme und Datenschutz	265
	Frank Czerner	
10.1	Einleitung	265
10.2	Daten und Dateien als Gegenstände einer Durchsuchung und Beschlagnahme?	266
10.3	Beschlagnahme und Durchsuchung bei E-Mails, SMS etc.	268
10.4	Kopieren von Daten (Image) als eingriffsschwächeres Äquivalent zur Beschlagnahme eines Rechners?	270
10.5	Problem der Begrenzung von Durchsuchung und Beschlagnahme auf verfahrensrelevante Datenbestände versus Amtsermittlungsgrundsatz im Strafprozess	271
10.6	Durchsuchung und Beschlagnahme von Daten und der „Kernbereich privater Lebensgestaltung“	273
10.7	Durchsuchung und Beschlagnahme auch bei Nichtbeschuldigten?	276
10.8	Formalia bei der Anordnung und Durchführung von Durchsuchung und Beschlagnahme	276
10.9	Telekommunikationsüberwachung gemäß § 100a StPO	276
10.9.1	Rechtliche Qualifizierung einzelner Phasen im E-Mail-Verkehr	277
10.9.2	Voraussetzungen und Möglichkeiten der Telekommunikations- überwachung gemäß § 100a StPO	281
10.9.3	Anordnung und Durchführung der Telekommunikationsüber- wachung	284

10.10 Quellen-Telekommunikationüberwachung	286
10.11 Speicherung von Verkehrsdaten für eine spätere Strafverfolgung	287
10.12 Online-Durchsuchungen zugunsten effektiver Strafverfolgung?	288
10.12.1 Online-Durchsuchung im geltenden Strafprozess	288
10.12.2 Notwendigkeit einer Legitimierung von Online-Durchsuchungen im Strafverfahren	291
10.13 Online-Durchsuchung zur terroristischen Gefahrenabwehr: Ermittlungsbefugnisse nach dem BKAG und dem ATDG	293
10.14 Die rechnerexterne Datenspeicherung im World Wide Web: Cloud Computing	295
10.15 Daten auf Servern außerhalb des Hoheitsgebietes der Bundesrepublik Deutschland	297
Literatur	298
Ausgewählte Rechtsnormen (Auszug)	301
Glossar	313
Sachverzeichnis	317