Inhaltsverzeichnis

1 **Android und mobile Forensik** ... 15
- **1.1 Einleitung** ... 15
- **1.2 Android-Plattform** ... 16
- 1.2.1 Geschichte von Android ... 17
- 1.2.2 Googles Strategie ... 22
- **1.3 Linux, Open-Source-Software und Forensik** ... 25
- 1.3.1 Eine kurzer historischer Abriss zu Linux ... 26
- 1.3.2 Linux in VirtualBox installieren ... 27
- 1.3.3 Linux und Forensik: Grundlegende Befehle ... 31
- **1.4 Das Android Open Source Project (AOSP)** ... 42
- 1.4.1 AOSP-Lizenzen ... 42
- 1.4.2 Entwicklungsprozess ... 43
- 1.4.3 Der Wert von Open Source in der Forensik ... 45
- 1.4.4 Herunterladen und Kompilieren des AOSP ... 46
- **1.5 Internationalisierung** ... 47
- 1.5.1 Unicode ... 47
- 1.5.2 Tastaturen ... 48
- 1.5.3 Custom Branches ... 49
- **1.6 Android Market** ... 50
- 1.6.1 Apps installieren ... 51
- 1.6.2 App-Statistiken ... 54
- **1.7 Android-Forensik** ... 54
- 1.7.1 Herausforderungen ... 55
- **1.8 Zusammenfassung** ... 56
- **1.9 Referenzen** ... 56

2 **Android-Hardwareplattformen** ... 59
- **2.1 Einführung** ... 59
- **2.2 Überblick über Kernkomponenten** ... 59
- 2.2.1 CPU ... 60
- 2.2.2 Baseband/Radio ... 60
- 2.2.3 Speicher (RAM und NAND-Flash) ... 60
- 2.2.4 GPS ... 61
- 2.2.5 Drahtloses Netzwerk (WLAN und Bluetooth) ... 62
- 2.2.6 SD-Karte ... 62
- 2.2.7 Bildschirm ... 62
- 2.2.8 Kamera ... 63
- 2.2.9 Tastatur ... 63

2.2.10 Batterie ... 64
2.2.11 USB ... 64
2.2.12 Sensoren ... 65
2.2.13 Lautsprecher/Mikrofon ... 65
2.3 Überblick über verschiedene Gerätetypen ... 65
2.3.1 Smartphone ... 66
2.3.2 Tablet ... 66
2.3.3 Netbook ... 66
2.3.4 Google-TV ... 67
2.3.5 Fahrzeuge (In-Board) ... 67
2.3.6 GPS ... 67
2.3.7 Andere Geräte ... 67
2.4 ROM und Boot-Loader ... 68
2.4.1 Power-On und On-Chip Boot ROM Code Execution ... 69
2.4.2 Boot-Loader (IPL/SPL) ... 69
2.4.3 Linux-Kernel ... 70
2.4.4 Der Init-Prozess ... 71
2.4.5 Zygote und Dalvik ... 73
2.4.6 System-Server ... 74
2.5 Hersteller ... 75
2.6 Android Updates ... 75
2.6.1 Angepasste Benutzeroberflächen ... 76
2.6.2 Aftermarket-Android-Geräte ... 77
2.7 Spezifische Geräte ... 77
2.7.1 T-Mobile G1 ... 78
2.7.2 Motorola Droid ... 78
2.7.3 HTC Incredible ... 79
2.7.4 Google Nexus One ... 80
2.8 Zusammenfassung ... 81
2.9 Referenzen ... 81

3 Android Software Development Kit (SDK) und die Android Debug Bridge (ADB) ... 83
3.1 Einleitung ... 83
3.2 Android-Plattformen ... 83
3.2.1 Android-Plattform-Highlights bis Version 2.3.3 (Gingerbread) ... 86
3.3 Software Development Kit (SDK) ... 90
3.3.1 SDK Release History ... 90
3.3.2 SDK-Installation ... 90
3.3.3 Android Virtual Devices (AVD; Emulator) ... 100
3.3.4 Architektur des Android-Betriebssystems ... 104
3.3.5 Dalvik-VM ... 106
3.3.6 Entwicklung von nativem Code ... 106
3.4 Android-Sicherheitsmodell ... 107
3.5 Forensik und das SDK ... 109

3.5.1 Ein Android-Gerät mit einer Workstation verbinden 109
3.5.2 USB-Schnittstellen 112
3.5.3 Einleitung zur Android Debug Bridge (ADB) 119
3.6 Zusammenfassung 121
3.7 Referenzen 121

4 Android-Dateisysteme und -Datenstrukturen 123
4.1 Einleitung 123
4.2 Data in the Shell 123
4.2.1 Welche Daten gespeichert werden 124
4.2.2 Verzeichnisstruktur der Datenablage von Apps 124
4.2.3 Wie Daten gespeichert werden 125
4.3 Speichertypen 146
4.3.1 RAM 146
4.3.2 NAND-Flash 149
4.4 Dateisysteme 154
4.4.1 Die Dateisysteme rootfs, devpts, sysfs und cgroup 156
4.4.2 proc 159
4.4.3 tmpfs 160
4.4.4 Extended File System (EXT) 163
4.4.5 FAT32/VFAT 163
4.4.6 YAFFS2 164
4.5 Eingebundene Dateisysteme 177
4.5.1 Eingebundene Dateisysteme 177
4.6 Zusammenfassung 181
4.7 Referenzen 181

5 Geräte-, Daten- und App-Sicherheit unter Android 183
5.1 Einleitung 183
5.2 Ziele und Angriffsvektoren von Datendiebstahl 184
5.2.1 Android-Geräte als Ziel 185
5.2.2 Android-Geräte als Angriffsvektor 193
5.2.3 Datenspeicher 194
5.2.4 Aufzeichnungsgeräte 194
5.2.5 Umgehen von Netzwerkkontrollen 194
5.2.6 So richtig heimtückische Methoden 195
5.3 Sicherheitsbetrachtungen 195
5.3.1 Sicherheitsphilosophie 195
5.3.2 US Federal Computer Crime Laws and Regulations 197
5.3.3 Open Source versus Closed Source 199
5.3.4 Verschlüsseltes NAND-Flash 201
5.4 Individuelle Sicherheitsstrategien 202
5.5 Unternehmensweite Sicherheitsstrategien 204
5.5.1 Policies (Sicherheitsrichtlinien) 204
5.5.2 Passwort-/Pattern-/PIN-Lock 205

5.5.3 Remote-Wipe von Geräten (Fernlöschung) ... 206
5.5.4 Upgrade auf aktuelle Software ... 207
5.5.5 Fernverwaltungs-Features ... 208
5.5.6 Anwendungs- und Geräte-Audit ... 210
5.6 Sicherheitsstrategien in der App-Entwicklung ... 211
5.6.1 Sicherheitstests mobiler Anwendungen ... 211
5.6.2 Strategien der App-Sicherheit ... 213
5.7 Zusammenfassung ... 220
5.8 Referenzen ... 220

6 Techniken der Android-Forensik ... 223
6.1 Einleitung ... 223
6.1.1 Untersuchungsvarianten ... 223
6.1.2 Unterschied zwischen logischen und physischen Techniken ... 224
6.1.3 Modifikation des Zielgerätes ... 225
6.2 Vorgehen für die Handhabung eines Android-Geräts ... 227
6.2.1 Sicherstellen des Gerätes ... 227
6.2.2 Isolierung vom Netzwerk ... 228
6.2.3 Umgehen des Passwortschutzes ... 232
6.3 Images von Android-USB-Speichern erstellen ... 240
6.3.1 SD-Karte versus eMMC ... 241
6.3.2 Wie man forensische Images von SD-Karte/eMMC erstellt ... 242
6.4 Logische Techniken ... 248
6.4.1 ADB Pull ... 249
6.4.2 Backup-Analyse ... 250
6.4.3 AFLogical ... 251
6.4.4 Kommerzielle Anbieter ... 259
6.5 Physische Techniken ... 298
6.5.1 Hardwarebasierte physische Techniken ... 299
6.5.2 Softwarebasierte physische Techniken und Privilegien ... 302
6.5.3 AFPhysical-Technik ... 310
6.6 Zusammenfassung ... 316
6.7 Referenzen ... 317

7 Android-Apps und forensische Analyse ... 319
7.1 Einleitung ... 319
7.2 Analysetechniken ... 319
7.2.1 Timeline-Analyse ... 319
7.2.2 Dateisystemanalyse ... 322
7.2.3 File-Carving ... 325
7.2.4 Strings (Zeichenketten) ... 328
7.2.5 Hex: Ein guter Freund des Forensikers ... 330
7.2.6 Android-Verzeichnisstrukturen ... 337
7.3 FAT-Forensik-Analysen ... 344
7.3.1 FAT-Timeline-Analyse ... 345

7.3.2 Zusätzliche FAT-Analysen ... 353
7.3.3 Anmerkungen eines FAT-Analysten ... 355
7.4 YAFFS2-Forensik-Analysen ... 358
7.4.1 YAFFS2-Timeline-Analyse ... 362
7.4.2 YAFFS2-Dateisystem-Analyse ... 369
7.4.3 YAFFS2-File-Carving ... 372
7.4.4 YAFFS2-String-Analyse ... 374
7.4.5 Anmerkungen eines YAFFS2-Analysten ... 376
7.5 Android-App-Analyse und Referenz ... 380
7.5.1 Nachrichten (SMS und MMS) ... 381
7.5.2 MMS-Helper-App ... 382
7.5.3 Webbrowser ... 383
7.5.4 Kontakte ... 389
7.5.5 Medienscanner ... 391
7.5.6 YouTube ... 393
7.5.7 Cooliris Mediengalerie ... 395
7.5.8 Google Maps ... 397
7.5.9 Gmail ... 402
7.5.10 Facebook ... 405
7.5.11 Adobe Reader ... 407
7.6 Zusammenfassung ... 408
7.7 Referenzen ... 409

Stichwortverzeichnis ... 411