

Inhaltsverzeichnis

1	Ein Mac OS Lab aufsetzen	19
1.1	System Integrity Protection deaktivieren.....	19
1.2	Einen Übungs-Account einrichten.....	19
1.2.1	Einen neuen Benutzer-Account erstellen	20
1.2.2	Gatekeeper-Funktionalität deaktivieren	21
1.3	Programme im Mac OS Lab installieren	22
1.3.1	Java SE.....	22
1.3.2	Xcode	22
1.3.3	Fuse.....	23
1.3.4	Mac Ports.....	23
1.3.5	Homebrew	23
1.3.6	Libewf.....	24
1.3.7	Xmount.....	24
1.3.8	Sleuth Kit.....	25
1.3.9	SQLite-Browser	25
1.3.10	Hex-Editoren	25
1.3.11	Github	25
1.3.12	Python	25
1.4	Den Übungs-Account wieder löschen	26
2	Wichtige Hintergrundinformationen.....	27
2.1	Das Betriebssystem Mac OS.....	27
2.2	Appelution in Cupertino.....	28
2.2.1	Apple-Betriebssystem-Modelle	31
2.3	Mac OS X intern	31
2.3.1	Historie der Mac-OS-X-Versionen	32
2.3.2	Darwin – das Grundgerüst von Mac OS	37
2.4	Die Mac-OS-Architektur	38
2.4.1	HFS+	39
2.4.2	HFS+ case-sensitive	39
2.4.3	/bin	40
2.4.4	/sbin.....	40
2.4.5	/usr	41
2.4.6	/etc.....	41
2.4.7	/dev.....	41
2.4.8	/tmp	41
2.4.9	/var	41
2.4.10	/Applications	42
2.4.11	/Developer	42
2.4.12	/Library	42

2.4.13	/Network	42
2.4.14	/System	43
2.4.15	/Users	43
2.4.16	/Volumes	43
2.4.17	/Cores	43
2.4.18	Apple EFI.....	46
2.4.19	Launchd.....	50
2.4.20	Prozesse und Threads.....	51
2.4.21	Mach-O-Binaries	53
2.4.22	Bundles und Packages	55
2.4.23	Applications.....	56
2.4.24	Frameworks.....	56
2.5	Mac-OS-Sicherheitskonzepte.....	57
2.5.1	Code Signing.....	57
2.5.2	Sandboxing.....	57
2.5.3	Gatekeeper	58
2.5.4	File Quarantine.....	59
2.5.5	System Integrity Protection	59
2.5.6	XPC.....	60
2.6	Zusammenfassung	61
2.7	Übung: Mac-OS-Handling	62
3	Das Mac-OS-Dateisystem im Fokus.....	67
3.1	Solid State Disks	68
3.2	GUID-Partitionsschema.....	70
3.2.1	GUID Partition Table	70
3.2.2	Analyse der GUID Partition Table.....	75
3.2.3	Zusammensetzen von Fusion-Drive-Laufwerken	77
3.3	Hierarchical File System Plus (HFS+)	78
3.3.1	Speichersystematik.....	80
3.3.2	HFS+ Special Files	81
3.3.3	Extraktion von HFS+ Special Files.....	82
3.3.4	Volume Header.....	83
3.3.5	Allocation File	86
3.3.6	B-Baum-Struktur	87
3.3.7	Catalog File	95
3.3.8	Extents Overflow File	100
3.3.9	Attributes File.....	100
3.3.10	Journal	103
3.3.11	Dateikomprimierung.....	103
3.3.12	Hardlinks	105
3.3.13	Mac-OS-Zeitstempel.....	107
3.4	Apple File System (APFS)	108
3.4.1	Flexible Partitionen	109
3.4.2	Dateisystem-Snapshots.....	111
3.4.3	Dateien und Verzeichnisse klonen	112
3.4.4	Verschlüsselung.....	112
3.4.5	Eine APFS-Volume erstellen	113

3.4.6	Partitionsschema	115
3.4.7	Container-Superblock	117
3.4.8	Volume Header.....	117
3.4.9	Forensische Ansätze.....	120
3.4.10	Ausblick auf das APFS	123
3.5	Übung: Partitionen und Dateisystem.....	124
4	Forensische Analyse von Mac OS	131
4.1	Stand der Forschung.....	131
4.2	Modelle der Digitalen Forensik.....	132
4.3	Der investigative Prozess nach Casey.....	132
4.3.1	Der investigative Prozess für Mac-Computer.....	135
4.4	Live Response	135
4.4.1	Maßnahmen bei eingeschalteten Mac-Computern.....	136
4.4.2	Vertrauenswürdige Binaries.....	137
4.4.3	Sammlung volatiler Daten (Triage)	138
4.4.4	Virtuelle Maschinen	139
4.5	Übung: Live Response	140
4.5.1	RAM-Sicherung.....	145
4.5.2	Logische Sicherung	147
4.6	Post-Mortem-Analyse	147
4.6.1	Forensische Abbilder von Datenträgern.....	148
4.6.2	Live-CD/-DVD oder bootbarer USB-Stick.....	150
4.6.3	Sicherung von MacBooks mit NVMe-Controllern	152
4.6.4	Sicherung über die Recovery-Partition	154
4.6.5	Target Disk Mode.....	155
4.6.6	FileVault 2 und Fusion Drive.....	155
4.6.7	Open-Firmware-Passwort.....	156
4.6.8	Disk Arbitration	156
4.7	Sicherungsstrategien für Mac-Computer	157
4.8	Übung: Sicherung erstellen.....	158
4.8.1	Sicherung mit dd/dcfldd.....	158
4.8.2	Sicherung mit ewfacquire	159
4.8.3	Sicherung mit dem FTK Imager	159
5	Kategorisierung digitaler Spuren	161
5.1	Persistente Spuren	161
5.2	Mac-spezifische Formate	162
5.2.1	Property List Files	162
5.2.2	NSKeyedArchiver-Format	163
5.2.3	SQLite.....	166
5.2.4	Analyse von SQLite.....	169
5.2.5	Disk Images	178
5.2.6	Forensische Abbilder mounten	180
5.3	System- und lokale Domäne	181
5.3.1	Systeminformationen	181
5.3.2	Nutzerkonten	184
5.3.3	Netzwerkeinstellungen	185

14 *Inhaltsverzeichnis*

5.3.4	Software-Installationen	186
5.3.5	Drucker	189
5.3.6	Keychains	190
5.3.7	Firewall	192
5.3.8	Launch Agents	193
5.3.9	Launch Daemons.....	194
5.3.10	Freigaben.....	195
5.4	Nutzer-Domäne	201
5.4.1	Nutzer-Account-Informationen	202
5.4.2	Papierkorb	204
5.4.3	Zuletzt genutzte Objekte.....	205
5.4.4	Dock	206
5.4.5	Spaces.....	207
5.4.6	Anmeldeobjekte von Nutzern.....	209
5.4.7	SSH	210
5.4.8	Apps	211
5.4.9	Kontakte	211
5.4.10	Kalender	213
5.4.11	Mail	214
5.4.12	Safari.....	217
5.4.13	Fotos.....	218
5.4.14	Nachrichten	219
5.4.15	FaceTime.....	221
5.4.16	Notizen	221
5.4.17	Continuity	223
5.4.18	Siri.....	224
5.4.19	Applikationen von Drittanbietern	225
5.5	Netzwerk-Domäne	226
5.6	Zusammenfassung	226
6	Informationen aus Log-Dateien	227
6.1	Log-Dateien des Betriebssystems	227
6.1.1	Nutzer-/Account-Informationen	227
6.1.2	Software-Installationen	228
6.1.3	Filesystem Check.....	228
6.1.4	Storage Manager	228
6.1.5	WiFi.log.....	229
6.1.6	System.log	229
6.1.7	Periodische Log-Dateien	231
6.1.8	Apple System Logs	232
6.1.9	Audit-Logs.....	233
6.1.10	Unified Logging	235
6.2	Log-Dateien der Nutzer-Domäne	245
6.2.1	Verbundene iOS-Geräte	245
6.2.2	FaceTime-Verbindungen	246
6.2.3	Übersicht	246

7	Hack the Mac	249
7.1	Mac-OS-Nutzerpasswörter	249
7.1.1	Cracking des Nutzerpassworts mit Dave Grohl.....	251
7.1.2	Cracking des Nutzerpassworts mit Hashcat	252
7.2	FileVault 2 – Full Disk Encryption.....	256
7.2.1	FileVault2-Cracking mit JtR – EncryptedRoot.plist.wipekey.....	259
7.2.2	FileVault2-Cracking mit JtR – Image-Datei	264
7.3	Mac-OS-Keychains cracken	266
7.3.1	Angriff auf den Nutzerschlüsselbund mit JtR.....	266
7.4	Verschlüsselte Disk Images.....	267
7.4.1	Angriff auf eine verschlüsselte DMG-Datei mit JtR	268
7.4.2	Angriff auf eine verschlüsselte Sparsebundle-Datei mit JtR	268
7.5	Übung: Analyse und Cracking – Teil 1	268
7.5.1	Szenario	268
7.5.2	Lösung: Szenario.....	270
7.5.3	Fortsetzung des Szenarios.....	273
7.5.4	Lösung: Fortsetzung des Szenarios	273
8	Anwendungsanalyse unter Mac OS.....	275
8.1	Tools zur Anwendungsanalyse	275
8.1.1	Mac OS: Aktivitätsanzeige	275
8.1.2	List open Files: lsof.....	277
8.1.3	Fs_usage.....	277
8.1.4	Xcode: Instruments	278
8.1.5	DTrace.....	280
8.1.6	FSmonitor	280
8.1.7	DaemonFS	281
8.2	Modell zur Analyse von Applikationen unter Mac OS	281
8.3	Anwendungsanalyse der Nachrichten-App.....	283
8.3.1	Analyseumgebung.....	283
8.3.2	Anwendungsanalyse der Nachrichten-App	283
8.3.3	Ansätze für eine forensische Analyse	304
8.3.4	Zusammenfassung	305
9	Random-Access-Memory-Analyse	307
9.1	Stand der Forschung.....	308
9.2	Struktur des RAM-Speichers	308
9.3	Tools zur Sicherung und Analyse.....	311
9.4	RAM-Analyse mit Volatility.....	312
9.5	Volatility-Plugin vol_logkext.py.....	314
9.6	Zusammenfassung	317
10	Forensische Betrachtung der Mac-Technologien	319
10.1	Versions	319
10.2	Spotlight.....	326
10.2.1	Analyse von Spotlight.....	327
10.2.2	Spotlight als Werkzeug.....	329
10.3	Time Machine.....	333
10.3.1	Time-Machine-Spuren auf zu sichernden Rechnern	334

16 Inhaltsverzeichnis

10.3.2	Allgemeine Struktur eines gemounteten Time-Machine-Backups	337
10.3.3	Struktur eines lokalen Backups	344
10.3.4	Analyse von Time-Machine-Backups	345
10.4	iCloud	350
10.4.1	iCloud-Spuren unter Mac OS	353
10.4.2	iCloud-Daten sichern	360
10.5	iOS-Backups.....	361
10.6	Übung: Cracken eines verschlüsselten iOS-Backups	368
10.7	Übung: Angriff auf die Manifest.plist.....	368
10.8	Übung: Analyse und Cracking – Teil 2	369
10.8.1	Suchen mit Spotlight.....	369
10.8.2	Fortsetzung des Szenarios	371
10.8.3	Lösung: Suchen mit Spotlight	371
10.8.4	Lösung: Fortsetzung des Szenarios	372
11	Advanced Terminal im forensischen Umfeld	373
11.1	Basiskommandos	373
11.2	Tastaturfunktionen	374
11.3	Spezielle Kommandos	374
11.3.1	Suche nach Dateien: locate	374
11.3.2	Suche nach Dateien: find.....	375
11.3.3	Grep.....	376
11.4	Mac-OS-Kommandos	377
11.4.1	Anzeige von erweiterten Metadaten	377
11.4.2	Anzeige und Konvertierung von Plist-Dateien	378
11.5	Scripting-Grundlagen	379
11.6	Übung: Advanced Terminal	380
12	AppleScript, Automator, OS X Server	381
12.1	Ein kurze Einführung in AppleScript	381
12.2	Automator und relevante Arbeitsabläufe	383
12.2.1	Workflow: Copy Files.....	386
12.2.2	Workflow: Kalenderdaten parsen	387
12.2.3	Workflow: Kontakte parsen	388
12.2.4	Dienst: Dateiliste erstellen	389
12.2.5	Dienst: MD5-Hashliste erstellen.....	391
12.2.6	Programme: Versteckte Dateien anzeigen und ausblenden.....	391
12.2.7	Programme: Diskarbitration Daemon aktivieren und deaktivieren.....	392
12.3	Mac OS als vollwertiges Serversystem	393
12.3.1	OS-X-Server-Upgrade über den App Store.....	393
12.3.2	Grundlegende OS-X-Server-Einstellungen.....	394
12.3.3	Dateifreigaben innerhalb eines Mac-Netzwerks.....	395
12.3.4	Digitale Spuren zu eingerichteten Diensten.....	395

Literaturverzeichnis	397
Kapitel »Wichtige Hintergrundinformationen«.....	397
Kapitel »Das Mac-OS-Dateisystem im Fokus«.....	400
Kapitel »Forensische Analyse von Mac OS«	401
Kapitel »Kategorisierung digitaler Spuren«	402
Kapitel »Informationen aus Log-Dateien«.....	404
Kapitel »Hack the Mac«	405
Kapitel »Anwendungsanalyse unter Mac OS«.....	405
Kapitel »Random-Access-Memory-Analyse«.....	406
Kapitel »Forensische Betrachtung der Mac-Technologien«.....	407
Kapitel »AppleScript, Automator, OS X Server«	407
Stichwortverzeichnis.....	409