

COMPUTER- FORENSIK HACKS™

*Lorenz Kuhlee
Victor Völzow*



O'REILLY®

Beijing • Cambridge • Farnham • Köln • Sebastopol • Tokyo

009-09.06.06

Inhalt

Vorwort und Danksagungen	IX
Einleitung	XIII
Kapitel 1. Datensicherung	1
1. Woran Sie denken sollten	2
2. So säubern Sie Ihre Backup-Datenträger	5
3. Bevor es zu spät ist – RAM sichern	7
4. RAM sichern trotz Passwortsicherung	9
5. Wenn nichts mehr hilft: Cold Boot	11
6. Weitere flüchtige Daten richtig sichern	16
7. Automatisieren Sie Live-Sicherungen mit Skripten	18
8. So sichern Sie Daten auf der Kommandozeile	21
9. Wenn Sie doch eine GUI bevorzugen	22
10. Vertrauen ist gut, Kontrolle ist besser	25
11. Boot DVDs für die Datensicherung	27
12. Aus der Ferne sichern	29
13. Aus der Ferne sicher sichern	33
14. Wenn Ihnen das Format nicht passt	35
Kapitel 2. Dateisysteme	39
15. Analysieren Sie den Master Boot Record	40
16. Identifizieren Sie verschiedene FAT-Dateisysteme	43
17. Das Prinzip gelöschter Dateien unter NTFS	45
18. Wie Sie Zeitstempel einer Datei validieren	46

19. So identifizieren Sie unter NTFS die Eigenschaften einer gelöschten Datei	49
20. Wie ein Puzzle: Setzen Sie trotz Fragmentierung gelöschte Dateien wieder zusammen	51
21. Wenn Dateien keine Dateien sind	55
22. Der Slack-Bereich	58
23. Welche Daten Sie sonst noch in der MFT finden können	60
24. Schreiben Sie Ihren eigenen MFT-Eintragsparser	62
25. Der Unterschied zwischen Hard- und Soft-Link	70
Kapitel 3. Analyse und Wiederherstellung von Daten	73
26. Zugriff auf Images mit grafischen Helfern	74
27. Binden Sie Images in Ihr System ein	79
28. Finden Sie alte Bekannte	81
29. Retten Sie in wenigen Minuten Dateien mit Freeware unter Windows	83
30. Ausflug in die Welt der Zahlen	89
31. Decodieren Sie Rot13 und Base64	91
32. Entdecken Sie das wahre Gesicht einer Datei	94
33. Erst auspacken, dann suchen	97
34. Wenn Sie doch einmal manuell Carven müssen	99
35. Wenn nichts mehr hilft: Block Hashing	102
36. Keywordsuche mit regulären Ausdrücken	105
37. Volltreffer	108
38. Listen für Forensikläien generieren	113
39. Kopieren nach Dateinamenerweiterung	115
40. Jede Platte hat ihre Geschichte	118
41. Visualisieren Sie Ihre Zeitleiste	123
42. Logfile-Auswertung, Teil 1	128
43. Logfile-Auswertung, Teil 2	132
44. Automatisierte Auswertung von Logfiles	134
45. Analyse der gesicherten RAM-Dumps	136
Kapitel 4. Digitale Spuren in Windows	141
46. Wichtige Verzeichnisse in Windows XP / Vista / 7	142
47. Die Registry-Top-10	144
48. Ihre Goldgrube – MRU-Listen für alle Zwecke	146
49. Welche Programme wurden gestartet?	148
50. So werten Sie Ereignisprotokolle aus	150

51. Reisen Sie in die Vergangenheit	155
52. Finden Sie Spuren in Vorschau Datenbanken	159
53. Sehen Sie, was gedruckt wurde	162
54. Stöbern Sie im Müll	164
55. Passwort vergessen? Kein Problem!	167
Kapitel 5. Digitale Spuren in Linux	173
56. Finden Sie heraus, welches Linux-Derivat vorliegt	174
57. Verschaffen Sie sich einen Partitionsüberblick (Sys V)	176
58. Verschaffen Sie sich einen Partitionsüberblick (BSD)	181
59. Ermitteln Sie installierte Software	182
60. Finden Sie Hinweise auf gelaufene Netzwerkdienste	184
61. Stellen Sie die Netzwerkkonfiguration fest	189
62. Spüren Sie Anomalien bei den Usern auf	190
63. Auf den Spuren des Users	192
64. Stellen Sie Beziehungen grafisch dar	193
65. Analysieren eines LAMP(P)-Servers	196
66. So rekonstruieren Sie eine dynamische Webseite	201
Kapitel 6. Internetartefakte	209
67. So untersuchen Sie SQLite Datenbanken	210
68. Analysieren der Firefox-History	213
69. Sonstige Spuren des Browsers Firefox	216
70. Analysieren der Internet-Explorer-History	220
71. Sonstige Spuren des Browsers Internet Explorer	224
72. Analysieren der Chrome-History	228
73. Sonstige Spuren des Browsers Chrome	230
74. So werten Sie den ICQ-Messenger aus	233
75. Untersuchen Sie den Windows Live Messenger	238
76. Finden Sie Spuren des Skype Messenger	243
77. Analysieren Sie E-Mails von Microsoft Outlook	248
78. Bereiten Sie E-Mails von Windows Live Mail auf	252
79. Analysieren Sie E-Mails im Format mbox	254
80. Der E-Mail auf der Spur	255
81. Finden Sie Spuren im HTML-Quelltext	259
Kapitel 7. Hacking & Co.	263
82. Top-10-Hinweise auf einen Angriff	264
83. So funktioniert WLAN-Hacking	266

84. Typische Suchmuster für Angriffe auf Datenbanken	268
85. Lassen Sie sich Netzwerkverbindungen anzeigen	271
86. Stellen Sie fest, ob ein Webserver leicht angreifbar war	273
87. Der Kammerjäger: Stellen Sie fest, ob sich Malware eingenistet hat	274
88. Überprüfen Sie Ihren Netzwerkverkehr	279
89. PDF Malware-Analyse	282
90. Machen Sie sich die Erfahrung der Profis zunutze	283
Kapitel 8. Virtualisierung	287
91. Nutzen Sie QEMU für die Virtualisierung	289
92. So virtualisieren Sie Ihr forensisches Image	292
93. Richten Sie ein virtuelles Netzwerk ein	293
94. Konvertieren zwischen virtuellen Festplatten	295
95. Blue Screen ade mit OpenGates	297
96. Penetrationstest für Passwörter eines (virtualisierten) Windows-Betriebssystems	299
97. Penetrationstest für Passwörter eines (virtualisierten) Linux-Betriebssystems	303
98. Passwortpenetration mit John the Ripper	306
99. Booten eines Mac OS X-Image	308
100. Eine VM, viele Gesichter	312
Index	315