



Computer & Literatur Verlag GmbH

PC-FORENSIK

von Christoph Willer



Bibliographische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Herausgebers ist es nicht gestattet, das Buch oder Teile daraus in irgendeiner Form durch Fotokopie, Mikrofilm oder ein anderes Verfahren zu vervielfältigen oder zu verbreiten. Dasselbe gilt für das Recht der öffentlichen Wiedergabe.

Der Verlag macht darauf aufmerksam, daß die genannten Firmen- und Markenzeichen sowie Produktbezeichnungen in der Regel marken-, patent-, oder warenzeichenrechtlichem Schutz unterliegen.

Die Herausgeber übernehmen keine Gewähr für die Funktionsfähigkeit beschriebener Verfahren, Programme oder Schaltungen.

1. Auflage 2012

© 2012 by C&L Computer und Literaturverlag
Zavelsteiner Straße 20, 71034 Böblingen
E-Mail: info@cul.de
WWW: <http://www.CuL.de>

Coverdesign: Hawa & Nöh, Neu-Eichenberg, <http://www.hn-grafik.de>
Redaktionelle Ergänzungen: Jörg Braun
Redaktionelle Überarbeitung: Rosa Riebl
Satz: C&L Verlag
Druck: Kössinger AG, Schierling, <http://www.koessingerag.de>
Printed in Bavaria

Dieses Buch wurde auf chlorfrei gebleichtem Papier gedruckt

ISBN 978-3-936546-60-6

INHALT

Vorwort	13
----------------------	-----------

Kapitel 1	
Arbeiten vor Ort	15

1.1	Objekte der Computerforensik.....	18
1.1.1	Server und nicht vernetzte Computer.....	18
1.1.2	Externe Speicher- und Sicherungssysteme	20
1.1.3	Mobiltelefone	20
1.1.4	Sonstige Geräte.....	20
1.2	Werkzeugkoffer.....	21
1.2.1	Auswertecomputer	22
1.2.2	Externer Speicher.....	26
1.2.3	Fotoapparat	28
1.2.4	Forensik-Software	29
1.3	Die Daten des PCs.....	30
1.3.1	Daten im Arbeitsspeicher	36
	Windows-RAM auslesen.....	37
	Hiberfil.sys	39
	Pagefile.sys	39
	Linux-RAM auslesen.....	41
1.3.2	Daten auf Festplatten.....	41
	Notebook-Festplattensicherung	44
	Desktop-Festplattensicherung	44
	Server-Festplattensicherung	46
1.3.3	Daten auf externen Datenträgern.....	47

Kapitel 2

Analysevorbereitung49

2.1 Auswerte-System anschließen.....	52
2.1.1 Ausgebaute Festplatte.....	52
2.1.2 Nicht ausgebaute Festplatte.....	54
2.2 Datenträger sichern	57
2.2.1 Image-Formate	58
2.2.2 Festplatten unter Linux sichern	60
Mit dd	60
Mit dcfldd	64
Prüfsumme über Image legen	65
Images zurückschreiben	66
EnCase-Images	66
Images defekter Datenträger.....	69
Images mit grafischen Werkzeugen	72
2.2.3 Festplatten unter Windows sichern	76
Mit FTK-Imager	76
Mit X-Ways Forensic Browser	79
2.2.4 CDs und DVDs sichern.....	80
2.3 Image verifizieren	86
2.3.1 Prüfsummen berechnen.....	86
2.4 Datums- und Zeitstempel ermitteln	88
2.4.1 Zeitzonen	90
2.4.2 Zeitstempel des Dateisystems.....	94

Kapitel 3

Images vorbereiten97

3.1 Images einhängen	97
3.1.1 Linux	97
CD-Images.....	98
Beliebiges Datenträger-Image.....	99
3.1.2 Windows	102
CD-Images.....	102
Festplatten-Image	103
3.2 Datenträgerrettung.....	107

Kapitel 4

Daten suchen..... 113

- 4.1 Dateiformate..... 117**
 - 4.1.1 Bild-/Grafikformate 123
 - Bitmapformate 124
 - Vektorgrafikformate 129
 - 4.1.2 Videoformate und Sound 130
 - 4.1.3 Kompositformate 134
 - Word Binary File Format..... 134
 - OLE-Container..... 136
 - 4.1.4 Dateicontainer 139
 - Archive 140
 - Virtuelle Maschinen 140
 - Verschlüsselte Container..... 142
 - 4.1.5 Beschreibende Formate 142
 - Postscript..... 143
 - Portable Document Format..... 146
 - Hypertext Markup Language 147
 - 4.1.6 XML-Formate 150
 - Ecma Office Open XML File Format 151
 - Microsoft Office 2003 XML 155
 - Open Document Format 156
 - 4.1.7 Textformate 158
 - 4.1.8 Datenbankformate 161
 - 4.1.9 Ausführbare Dateien und DLLs..... 166
- 4.2 Suchbereiche 168**
 - 4.2.1 Dateien 169
 - 4.2.2 Datenträger 171
 - Festplattenaufteilung 172
 - Partitionsanfang 178
 - Dateisysteme..... 182
 - Gelöschte Partitionen 216
 - 4.2.3 Sonderbereiche 224
 - Flüchtiger Speicher 224
 - Slackspace..... 226
 - Reservierte Festplattenbereiche 227
- 4.3 Suchverfahren..... 234**
 - 4.3.1 Gelöschte Dateien 234
 - Headersuche mit scalpel..... 236

4.3.2	Im Dateisystem	241
	Suchen mit find	241
	Erkennen mit file	247
4.3.3	In Wiederherstellungspunkten	248
4.3.4	Im Windows-Papierkorb	250
	rifiuti.....	251
	rifiuti2.....	253
	X-Ways Trace.....	255
4.3.5	Windows-Registrierdatenbank.....	256
	Die Dateien der Registrierdatenbank	257
	Die Schlüssel der Registrierdatenbank.....	261
	Auswertungen	268
4.3.6	Bilder	278
	Digitalkamera.....	279
	Gesichtserkennung	284
	Vorschaubilder.....	286

Kapitel 5

Datenanalysen.....293

5.1	Dateien vergleichen	293
5.1.1	Einfache Dateivergleiche	293
5.1.2	Dateivergleiche	297
5.1.3	Dokumentinhalte vergleichen	298
5.2	Dateien durchsuchen	303
5.2.1	Textdateien durchsuchen	304
5.2.2	Speicherdumps auswerten	309
5.2.3	Dateien in Dateien auswerten	312
	Modifizierte Audiodatei	314
	Modifizierte Bilddatei	314
	Steganographie-Programme	315
5.2.4	Dokument-Metadaten auswerten	318
	Audio- und Bilddateien	318
	Office-Dokumente	319
5.2.5	Eventlogs auswerten	335
	Ereigniseinträge	335
	Sonstige Protokolldateien	339

Kapitel 6	
Verschlüsselung	341
6.1 Werkzeuge	343
6.1.1 Hardware	343
6.1.2 Software	344
Ophcrack	344
Cain&Abel	347
SamInside	349
Elcomsoft Password Recovery Bundle	350
Elcomsoft Advanced EFS Data Recovery	352
Password Recovery Tool Kit/Distributed Network Attack	354
Passware	354
Mail PassView	355
Dialupass	356
AsteriskLogger	357
PasswordFox	358
NetworkPasswordRecovery	359
Ultimate BootCD	359
6.2 Passwort-Ermittlungsverfahren	360
6.2.1 Social Engineering	360
6.2.2 Brute-Force-Attacke	362
6.2.3 Wörterbuch-Attacke	362
Individuelle Wörterbücher	363
Wörterbuch aus Festplatte	365
6.2.4 Rainbow-Tabellen	365
6.3 Formen der Verschlüsselung	367
6.3.1 Einzeldateien	368
GnuPG-Dateien	368
PGP-Dateien	369
Office-Dokumente	369
6.3.2 Container	370
Archiv-Dateien	370
E-Mails	371
EFS-Dateien	371
TrueCrypt- und FreeOTFE-Container	372
6.3.3 Vollverschlüsselung	374
6.3.4 BIOS-Passwort	377
6.3.5 Festplatten-Passwort	377
6.3.6 Netzwerk- und Router-Passwörter	379

Kapitel 7

Online-Aktivitäten381

7.1 E-Mails	381
7.1.1 Aufbau von E-Mails	382
Formate.....	382
Verschlüsselte E-Mails	384
7.1.2 E-Mail-Auswerteprogramme	385
7.1.3 E-Mail-Dateien suchen und durchsuchen.....	394
7.1.4 E-Mail-Clients.....	397
Mozilla Thunderbird.....	397
Outlook Express.....	399
Outlook.....	404
Windows Mail.....	407
T-Online.....	408
7.1.5 Webmail	409
7.1.6 Mailserver suchen.....	411
7.2 Browser.....	411
7.2.1 Suchbegriffe suchen	411
7.2.2 Internet-History.....	412
7.2.3 Cookies.....	421
7.3 Kommunikationsplattformen	423
7.3.1 Soziale Netze	424
Benutzerdaten.....	425
Facebook-Passwort	425
Personenbeziehungen	427
Blogeinträge.....	428
7.3.2 Chat.....	428
Chat-Programme suchen	430
Chat-Passwörter suchen	431
Gelöschten Chat-Mitschnitt suchen	433
Chat-Kontaktdaten suchen	438
7.3.3 Skype	441
7.4 Filesharing	443
7.4.1 Download-Clients suchen	448
7.4.2 BitTorrent	450
7.4.3 Gnutella/Limewire.....	451
7.4.4 Gnutella/BearShare	452

Kapitel 8
Netzwerk-Forensik..... 453

- 8.1 Netzwerk-Grundlagen..... 454**
- 8.2 Netzwerk-Programme 459**
 - 8.2.1 Basis-Netzwerkkonfiguration..... 459
 - 8.2.2 Netzwerk-Teilnehmer..... 460
 - 8.2.3 Weg eines IP-Pakets..... 463
 - 8.2.4 Namen und IP-Adressen 464
 - Umgekehrte Namensauflösung 465
 - dig..... 470
 - host 473
 - 8.2.5 Netzwerkverkehr mitschneiden 473
 - Daten sammeln mit tcpdump..... 474
 - Logs auswerten 477
 - Grafische Auswertungen..... 478
 - Netzwerkstatistiken 480

Kapitel 9
Dokumentation..... 481

- 9.1 Tagesprotokolle 481**
 - 9.1.1 Protokollaufbau 482
 - 9.1.2 Arbeitsschritte mitschneiden 483
- 9.2 Abschlussbericht..... 490**
 - 9.2.1 Aufbau 491

Anhang: Checklisten 495

Stichwortverzeichnis..... 499

Vorwort

Die ganze Branche des gerichtsverwertbaren Auswertens von Datenträgern ist hierzulande noch ziemlich neu und befindet sich im Entwicklungsstadium. Naturgemäß gibt es aus diesem Grund für die Computerforensik noch nicht allzu viele brauchbare Bücher, erst recht nicht in Deutsch.

Weil ich als Forensiker praktisch nicht auf Fachbücher zurückgreifen konnte und die Informationen im Internet spärlich, ungeordnet und oft falsch sind, fing ich an, mir meine gesamten Notizen auf Hunderten von Zetteln, die ich mir in den letzten fünfzehn Jahren als Gedankenstütze notiert und aufbewahrt hatte, für eine Dokumentation zusammenzustellen. So wurde aus meinen ersten Aufzeichnungen ein kleiner praktischer Leitfaden, der mir die tägliche Arbeit in der IT-Forensik erleichtern sollte. Ich verfeinerte diesen Leitfaden, nutzte ihn für Schulungen und stellte ihn auch ausgewählten Kollegen zur Verfügung. Der Leitfaden wuchs und wuchs, jeden Tag gibt es Veränderungen in der Computerwelt, Betriebssysteme kamen und gingen, Ermittlungsmöglichkeiten kamen hinzu, andere wurden von der Technik überholt.

Irgendwann kam mir die Idee, meine Dokumentation in einem Buch festzuhalten. Als ich das erste Mal diesen verwegenen Gedanken hatte, verwarf ich ihn gleich wieder, um ihn aber doch irgendwo im Hinterkopf reifen zu lassen. Mutig schrieb ich verschiedene Verlage an, um anzufragen, ob ein Interesse an so einem Buch bestünde.

Frau Riebl von C&L war die erste, die auf die Anfragen antwortete, und in einigen E-Mails und Telefonaten entwickelte sich in lockerem Umgangston ein gewisses Vertrauensverhältnis. Die Bedingungen waren schnell ausgehandelt, ich blieb beim C&L Verlag hängen, aber dann begann es erst richtig! Ich hatte ja keine Ahnung, auf was ich mich da eingelassen hatte! Von der kleinen Arbeitshilfe zum systematisch aufbereiteten Buch, das gleichzeitig zum Lernen und Nachschlagen dienen soll, ist es in Wirklichkeit ein großer Schritt, den ich komplett unterschätzte, und die anfangs auf ein halbes Jahr ausgelegte

Projektdauer verlängerte sich auf ein Vielfaches. Anfangs wollte ich alles gegenüber der Familie geheimhalten und erst das fertige Buch präsentieren, aber aufgrund des Arbeitsumfangs war das längst nicht mehr möglich.

Teilweise gingen mir die Themen gut von der Hand, aber ab und zu musste mir Frau Riebl einen Dämpfer versetzen. Ihre Korrekturen waren in grüner Schrift, ich konnte nach ein paar Monaten keine grüne Farbe mehr ertragen. Mit Anmerkungen wie *Stenografie?? Unser Buch braucht Fließtext!*, aber auch *Dies ist kein Roman!* oder *Hatten Sie keine Lust, hierzu was zu schreiben?* (natürlich in GRÜN!) musste sie mich ab und zu wieder aufs richtige Pferd setzen. Dies hatte ich auch nötig, nahezu alle Anmerkungen waren sinnvoll, es dauerte jedoch ein Weilchen, bis ich das einsah. Vielen Dank dafür an Frau Riebl mit ihrer Geduld und Hartnäckigkeit, aber auch danke für die vielen Hilfen, Ratschläge und Ergänzungen, die mir diese erfahrene Lektorin und Verlegerin an die Hand gab und damit wichtige Beiträge zu diesem Buch leistete. Ich bin froh, ihre Betreuung erfahren zu haben.

Natürlich war auch das Privatleben der letzten Jahre durch das Schreiben des Buches sehr beeinträchtigt, meine Lebensgefährtin hatte es nicht leicht, zu oft hatte ich keine Zeit für gemeinsame Unternehmungen. Vielen Dank auch für ihr liebevolles Verständnis!

Sehr viele angenehme und lehrreiche Erfahrungen kann ich mit dem Schreiben dieses Buches verbinden, so war regelmäßig Verlass auf die internationale Forensik-Community in verschiedenen Foren. Einige Softwarehersteller unterstützten mich mit ihren Produkten. Danke an sie und auch an alle die, von denen ich Informationen übernehmen durfte, speziell an Hans-Peter Merkel und Frau Fiona Meg Riessler und die vielen anderen Quellen, die hier nicht genannt werden können. Recht herzlichen Dank auch an meinen ersten externen Leser Andreas Rieb, der mir eine große Hilfe war.

Ich selbst konnte während der Recherchen zu diesem Buch mein Wissen ebenfalls erweitern, verfeinerte Suchtechniken und Ermittlungsmöglichkeiten und kam auf neue Ideen.

Nun wünsche ich mir, dass Sie, die Leser dieses Buchs, es ebenfalls als lehrreich empfinden, dass neue Kollegen in der IT-Forensik damit den Einstieg in diesen schweren Bereich finden, und dass die fortgeschrittenen Kollegen es als empfehlenswertes Nachschlagewerk ansehen. Hoffentlich kann ich Ihnen neue Techniken zeigen oder Sie auf Ideen bringen, was im jeweiligen Fall noch möglich sein könnte, ihn zu lösen und die gesetzten Ziele zu erreichen.

Ihr

Christoph Willer

EDV-Sachverständiger und Certified Forensic Computer Examiner (CFCE)

Kapitel 1

Arbeiten vor Ort

Bei vielen Straftaten, in unzähligen Zivilgerichtsverfahren und zunehmend auch in außergerichtlichen Auseinandersetzungen sind Computer, Mobiltelefone, PDAs und sogar komplette Netzwerke nicht mehr wegzudenkende Tatwerkzeuge oder Beweismittel. Die Disziplin der Computerforensik – oder IT-Forensik – fasst die verschiedenen Verfahren zur Aufdeckung und Sicherung der vielfältigen in elektronischen Systemen vorhandenen Spuren zusammen. Der, der auf verdächtigen Geräten Spuren sucht, ist der Forensiker. Er muss professionell ausgebildet sein, schreibt Gutachten und unterstützt die Behörden. Er wird üblicherweise dann tätig, wenn er von einem Richter einen konkreten Auftrag vorliegen hat. Die Landeskriminalämter, das Bundeskriminalamt, die Bundespolizei und das Bundesamt für Sicherheit in der Informationstechnik sind nur einige Beispiele von öffentlichen Dienststellen, die IT-Forensik-Labore unterhalten. Auch größere Unternehmen haben inzwischen ihre eigenen Labore eingerichtet und Techniker für diese Spezialgebiete intensiv ausgebildet.

Heute sind aber nicht nur die Behörden, sondern auch viele Unternehmen Nachfrager forensischer Leistungen. Weil sie immer mehr Ziel von Angriffen werden, beauftragen sie oft zuerst einen Forensiker mit der Ermittlung von digitalen Spuren, bevor sie sich an die Polizei wenden. Oft gehen nämlich die Angriffe von Innentätern aus, die sich erlaubterweise im gleichen PC-Netzwerk wie ihre Opfer aufhalten. Es sind neidische oder neugierige Mitarbeiter, die durch ihre Machenschaften die Kollegen in Mißkredit bringen oder auch »nur« Informationen über sie einholen wollen.

Aber auch die Vorstände von Unternehmen verstoßen immer wieder gegen das Bundesdatenschutzgesetz (BDSG) und andere Gesetze und kommen in die Schußlinie der Medien, wenn sie ihre Mitarbeiter in besonderer Weise überwachen und in den Verdacht geraten, sie auszuspionieren. Sie überwachen und protokollieren den E-Mail-Verkehr und das Internet-Surfverhalten

der Mitarbeiter, lesen Daten von ihren Computern aus, orten Firmenfahrzeuge, installieren Kameras, gleichen Finanzdaten ab, speichern Krankheitsdaten und hören Telefonate ab. Wenn der Verdacht besteht, dass diese Praktiken gegen geltendes Recht verstoßen, wird ein Forensiker hinzugezogen, der versuchen muss Spuren zu finden, die dem Richter Aufschluss darüber geben, ob die Aktivitäten legal waren oder gegen das Gesetz verstoßen. Dem Forensiker steht keine Beurteilung zu, er muss nur suchen und dokumentieren.

In diesem Buch für Techniker geht es darum, wie man zu neugierigen oder kriminellen Zeitgenossen auf die Schliche kommt. Es wird gezeigt, wie die Spuren, die sie auf IT-Geräten hinterlassen, gefunden werden können und welche elektronischen Beweismittel für widerrechtliche Machenschaften es neben dem PC sonst noch gibt. Dabei sollen einerseits Einsteiger in die Materie angesprochen und angeleitet werden, aber auch erfahrene IT-Forensiker können sicherlich die eine oder andere Idee aufgreifen und umsetzen.

Natürlich hilft das Buch auch dann, wenn der Leser keinen Auftrag einer öffentlichen Institution für eine Fahndung in der Tasche hat, sondern »nur« sein Passwort für den Computerzugang vergessen hat oder wichtige Daten retten muss, die mit dem versehentlichen Löschen einer Partition erst mal verschwunden zu sein scheinen. Die Methoden sind nämlich teilweise die gleichen.

Einige der Lösungen der Computer-Forensik überschneiden sich also mit dem Bereich der Datenrettung. Datenrettung hat zum Ziel, Daten, die – aus welchen Gründen auch immer – verloren geglaubt sind, wieder sichtbar zu machen, sie möglichst zu restaurieren und dem Anwender wieder zur Verfügung zu stellen, so dass er weiterhin mit ihnen arbeiten kann und ein eventuell eingetretener Schaden minimiert oder eliminiert wird.

Die Computer- oder IT-Forensik bezeichnet dagegen die gerichtsverwertbare, systematische Analyse von IT-Geräten und die damit verbundene Aufbereitung der Daten. Sie deckt die Spurensuche, Beweismittelsicherung und die Rekonstruktion von Abläufen an IT-Geräten ab, die in mögliche kriminelle oder auch nur moralisch bedenkliche Handlungen einbezogen waren oder einfach nur nicht gemäß ihrer vertraglichen Bestimmung genutzt wurden. Auch dabei werden unter anderem Daten wiederhergestellt, aufbereitet und zur Verfügung gestellt. Das Anwendungsspektrum ist aber breiter. Der Forensiker muss auch Fragen beantworten können, unter welcher Benutzererkennung welche Dateien zu einem bestimmten Zeitraum auf einem PC angelegt wurden, wann jemand Kenntnis von bestimmten Aktionen hatte, mit wem jemand Kontakt hatte, zu welchen Zeitpunkten bestimmte E-Mails gesendet wurden, welche Online-Aktivitäten auf dem PC durchgeführt wurden, auf welche USB- oder Netzwerklaufwerke zugegriffen wurde und vieles mehr.

Viele Verfahren in der Datenrettung und PC-Forensik gleichen sich also, jedoch ist der oberste Grundsatz der IT-Forensik die Gerichtsverwertbarkeit (was sie von der reinen Datenrettung unterscheidet). Das heisst zum einen,

dass die Beweise juristisch einwandfrei erhoben, aufbewahrt und nachgewiesen werden müssen, zum anderen aber auch, dass es zu jedem späteren Zeitpunkt eines Verfahrens möglich sein muss, aufgrund einer eventuell erforderlichen neuerlichen Untersuchung des Original-Beweismaterials zum gleichen Ergebnis zu kommen. Das Original-Beweismaterial darf also nicht verändert werden.



Bild 1.1: Schreibschutzmodule gibt es für IDE-, SATA-, SCSI- und USB-Anschluss

Die Unveränderlichkeit des Beweismaterials – in anderen Bereichen der Forensik längst eine Selbstverständlichkeit, niemand käme auf die Idee, in Asservatenkammern aufbewahrte Beweismittel zu verändern – stellt bei einem Computer eine besondere Herausforderung dar, da bei jedem Start zum Beispiel eines Windows-Systems die Datums-/Zeitstempel von zirka tausend(!) Dateien verändert werden.

Geht man von dem Grundsatz »Im Zweifel für den Angeklagten« aus, könnte ein Angeklagter mit diesem Wissen also argumentieren, während der Untersuchung seien nachweislich Datums-/Zeitstempel von Dateien verändert worden, es sei nicht bestimmbar, was sonst noch verändert wurde und damit sei auch nicht ausgeschlossen, dass ihm sogar Beweismaterial untergeschoben wurde. Das darf in einem ordnungsgemäßen Verfahren natürlich

nicht passieren. Vorgreifend sei erwähnt, dass der Forensiker aus diesem Grund von jedem betroffenen Datenträger zunächst mit Hilfe eines speziellen Hardware-Schreibschutzmoduls ein bit-identisches Abbild erzeugen muss. Seine Eigenschaften müssen dann protokolliert und mit dem Original verglichen werden. Gearbeitet wird dann nur noch an diesem Abbild. So kann im Ernstfall nachgewiesen werden, dass das originale Beweismaterial nicht verändert wurde.

1.1 OBJEKTE DER COMPUTERFORENSIK

1.1.1 Server und nicht vernetzte Computer

Im Fokus der forensischen Untersuchung stehen in der Regel die Computer. Dies können je nach Fall umfangreiche Serversysteme, vernetzte Arbeitsplätze oder – sehr häufig – alleinstehende Computer ohne eine Netzwerkanbindung in einem Privathaushalt oder im mobilen Einsatz sein.

Unterschiede in der forensischen Vorgehensweise und in den Untersuchungsmöglichkeiten ergeben sich dabei weniger aus der Art des zu untersuchenden Systems, als vielmehr aus der Ausgangssituation. So kann beispielsweise im einen Fall nur die Recherche in großen Datenbankbeständen auf einem Server von Relevanz sein¹, im anderen Fall geht es vielleicht um die Aufdeckung und Analyse von Handlungen an einem oder mehreren Computern.

Der Forensiker muss Kenntnisse in verschiedenen Betriebssystemen mitbringen, denn auf den verdächtigen Rechnern sind oft unterschiedliche Betriebssysteme installiert. Insbesondere bei Servern wird es sich meist um Unix-/Linux-Systeme handeln, bei den Arbeitsplatz-Computern stellen dagegen Windows-Systeme immer noch den größten Teil der Asservate dar. Wenngleich sich auch die genutzten Werkzeuge unterscheiden (müssen), sind die grundsätzlichen Möglichkeiten und Vorgehensweisen, die in diesem Buch vornehmlich am Beispiel Windows XP und Vista vorgestellt werden, doch ähnlich. Im Zweifelsfall kann dem Forensiker eine analoge Anwendung auf die andere Plattform weiterhelfen.

Netzwerkkarten

Netzwerkkarten sind aus Sicht der Computer-Forensik wichtig, weil sie eine weitgehend eindeutige Adresse aufweisen, die sogenannte MAC-Adresse. Sie wird übermittelt, wenn der PC seine IP-Adresse anfordert. Das kann

¹ Auf die Recherche in Datenbanken wird in diesem Buch nicht weiter eingegangen werden, da die individuellen Gegebenheiten von Datenbanksystemen immer eine Einzelfallbetrachtung bedingen. Außerdem kann eine derartige Recherche nur in Zusammenarbeit mit einem auf das jeweilige System eingearbeiteten Datenbank-Administrator geleistet werden.

wichtig sein, wenn es darum geht festzustellen, ob Netzwerkverbindungen bestehen oder bestanden haben.

Ein Computer kann mehrere Netzwerkkarten und somit MAC-Adressen besitzen, neben den internen Netzwerkkarten für den Kabelzugang (Ethernet) und einer WLAN-Karte kann ein Laptop beispielsweise auch mit einer PCMCIA-Netzwerkkarte ausgerüstet sein.

»Weitgehend eindeutig« bedeutet, dass die MAC-Adressen zunächst vom Hersteller abhängig sind und diese angehalten sind, pro Kontinent die MAC-Adresse jeweils nur einmal zu vergeben. MAC-Adressen sind eine fast(!) einzigartige sechs Byte (48 Bit) große hersteller-abhängige Kennung einer Netzwerkkarte. Sie wird üblicherweise in hexadezimaler Schreibweise dargestellt, beispielsweise als 00:0C:29:99:5D:8F.

Die ersten drei Byte der Adresse beschreiben in der Regel den Hersteller, wobei allerdings gilt, dass in virtuellen Maschinen MAC-Adressen frei gewählt werden können.

Beispiele:

- 00:50:8B Compaq Computer Corp.
- 00:07:E9 Intel Corp.
- 00:60:2F Cisco Systems, Inc
- 00:15:F2 AsusTek Computer Inc
- 00:0C:29 VMWare, Inc

MAC-Adressen können softwaremäßig ausgelesen werden, am einfachsten unter Linux mit *ifconfig* und unter Angabe der gewünschten Netzwerkkarte:

```
# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:19:db:f8:d2:09
          inet addr:192.168.0.8  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:169  errors:0  dropped:0  overruns:0  frame:0
          TX packets:149  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17827 (17.4 KiB)  TX bytes:15328 (14.9 KiB)
          Interrupt:42  Base address:0xe000
```

Unter <http://www.techzoom.net/lookup/check-mac.en> findet man einen Online-MAC-Adressdekodierer, mit ihm können MAC-Adressen hinsichtlich ihrer Herstellerfirma aufgelöst werden. So kann man beispielsweise eine MAC-Adressen schnell daraufhin überprüfen, ob vielleicht ein Fabrikat vorliegt, das sich offiziell gar nicht im Bestand der Firma befindet.

Entgegen einer weit verbreiteten Meinung können MAC-Adressen auch verändert oder gefälscht werden. Unter Linux ist das wieder mit *ifconfig* leicht möglich:

```
# ifconfig eth0 down
# ifconfig eth0 hw ether neue_MAC-Adresse
# ifconfig eth0 up
```

1.1.2 Externe Speicher- und Sicherungssysteme

Neben den Computern selbst sind oft auch externe Speichersysteme wie beispielsweise Network Attached Storages (NAS), Storage Area Networks (SANs) oder einfache Wechselfestplatten und Sicherungsmedien (USB-Sticks, CDs, DVDs, Zip-Laufwerke und vieles mehr) zu untersuchen. Auch bei Providern genutzter Online-Speicherplatz oder WLAN-fähige externe Festplatten müssen untersucht werden, ein Verdächtiger könnte ja Datenbestände außerhalb seiner direkten Sphäre verstecken, beispielsweise auf einer Festplatte, die in einem anderen Geschoss oder bei einem Nachbarn steht, und auf die er aus der Ferne mit seinem PC zugreifen kann.

1.1.3 Mobiltelefone

iPhones, Blackberrys und alle anderen Smartphones und Telefone besitzen mittlerweile eine große Speicherkapazität. Müssen Mobiltelefone und PDAs untersucht werden, ist in erster Linie darauf zu achten, dass ihre Ladegeräte und Netzkabel ebenfalls sichergestellt sind.

Bei Mobiltelefonen war es in der Berufspraxis des Autors mehrfach der Fall, dass Verdächtige versuchten, den Speicher des Geräts zu manipulieren, indem sie pausenlos anriefen oder Kurzmitteilungen sandten, um so die Liste der letzten Anrufe zu überschreiben. Würde das Telefon aber ausgeschaltet, bestünde die Gefahr, dass man – wegen einer (noch) nicht bekannten PIN – nicht oder nicht zeitgerecht an darauf befindlichen Daten gelangt. Sichergestellte Mobiltelefone sollten deswegen (spätestens in der Asservatenkammer) in Alufolie eingewickelt oder in spezielle forensische, abstrahlgeschützende Behältnisse gelegt werden, um den Empfang zu stören.

1.1.4 Sonstige Geräte

Das Repertoire der möglichen Beweismaterialien ist noch lange nicht erschöpft: Digitale Kameras und deren Speicherkarten können ebenso wie MP3-Player, Playstations oder eine Xbox an einen PC angeschlossen und Daten darauf versteckt werden. Selbst moderne Musiker-Keyboards wurden schon als Datenverstecke genutzt, enthalten sie inzwischen ja auch schon lange handelsübliche Festplatten mit einer Kapazität von Hunderten von Gigabyte.

Weitgehend unbekannt ist, dass neben den Computern und ihren typischen externen Speichern auch viele moderne Peripheriegeräte wie Kopier-, Fax- oder Multifunktionsgeräte eine handelsübliche Festplatte enthalten können oder unter Umständen aufgrund von Netzwerkfähigkeit eigene Dateispei-

cher anlegen. Auch solche Geräte können also mögliches Beweismaterial darstellen und müssen entsprechend untersucht werden.

Auf Papiaerausdrucken hinterlegen manche Drucker an einer bestimmten Stelle ein mit dem bloßen Auge unsichtbares Wasserzeichen, in dem Drucker- und Dateinformationen in Pixelanordnungen versteckt werden, was es möglicherweise erlaubt, die Herkunft eines Ausdrucks nachzuvollziehen. Gleiches gilt für Digitalkameras, in denen sich der digitale Fingerabdruck jedoch in individuellen Pixelbesonderheiten des in der Kamera befindlichen CCD-Kamerachips findet.

Wichtige Hinweise in Strafrechtsfällen kann die Auswertung eines Navigationssystems liefern; die zuletzt gesuchten Ziele, zu einem bestimmten Zeitpunkt eingespeicherte Punkte oder gefahrene Routen können in manchen Fällen durchaus zur Aufklärung von Sachverhalten beitragen. Dabei kann es sich einerseits um stationäre oder mobile Navigationsgeräte handeln, andererseits um softwarebasierte Routenplaner auf dem Computer oder im Internet.

1.2 WERKZEUGKOFFER¹

Um einen verdächtigen PC auseinandernehmen zu können, muss der Forensiker eine Reihe von handelsüblichen Werkzeugen mit vor Ort bringen beziehungsweise im Labor vorliegen haben. Zum Öffnen von Computern und Laptops, dem Ausbau von Festplatten und dem Arbeiten am offenen Computer sind ein Feinmechaniker-Schraubendrehersatz (Kreuz-/Schlitz- und Torx-Schraubendreher), ein Magnetschraubendreher, falls mal eine Schraube ins Gehäuse fällt, eine Spitzzange und eine Pinzette nötig.

Ein essentieller Bestandteil des Werkzeugkoffers sind alle Sorten von Kabeln und Adaptern. Der Datenretter oder Computer-Forensiker wird immer wieder vor Situationen stehen, in denen sein Auswerte-PC in irgendeiner Weise zu einem bestehenden System kompatibel sein muss. Ihre Zahl nimmt ständig zu, benötigt werden unterschiedliche USB- und Firewire-Kabel in allen Variationen, Bluetooth-Adapter, SATA-, eSATA-, IDE-, SCSI-, Y-Kabel für die interne Stromversorgung in den Desktopcomputern, mehrere Netzwerkkabel, Crossover-Netzwerkkabel oder ein entsprechender Adapter, Monitorkabel, Kaltgerätestecker, WLAN-Karten, iPhone-/iPod-USB-Adapter und so weiter. Damit man bestimmt das richtige Kabel vor Ort dabei hat, sollte man sich – soweit möglich – im voraus über die zu erwartende Situation informieren.

¹ Teile dieses Kapitels wurden vom Autor bereits im Aufsatz »Computerforensik – Technische Möglichkeiten und Grenzen« in der Zeitschrift »Computer und Recht«, Ausgabe 9/2007 veröffentlicht. Dem Verlag Dr. Otto Schmidt KG, Köln, wird herzlich für die Freigabe gedankt.

1.2.1 Auswertecomputer

Die beschlagnahmten Datenträger beziehungsweise Images werden auf einem Auswertecomputer untersucht. An seiner Ausstattung darf nicht gespart werden! Zwar ist gute Hardware nach wie vor teuer, doch man wird bei der Arbeit zweifelsfrei von der Geschwindigkeit eines modernen Computers und mehrerer Prozessoren profitieren.

Einige Firmen haben sich sogar auf die Herstellung von Forensik-Computern spezialisiert, beispielsweise MH-Service in Karlsruhe. Es werden mehrere Varianten von Auswertecomputern angeboten, vom Laptop über einen gut ausgestatteten Labor-Auswertecomputer bis hin zu tragbaren Computern, die nahezu dem Labor-Auswertecomputer gleich gestellt sind.

Die bei MH-Service One- und Trecorder genannten Geräte genügen auch mobilen Ansprüchen, weil gleich ein Trolley mitgeliefert wird, wenngleich diese mobilen Geräte trotzdem ziemlich schwer sind, so dass ein Einsatz in einem Altbau im fünften Stockwerk ohne Aufzug durchaus dem Embonpoint des Forensikers guttun wird.

Diese Computer haben mehrere Prozessoren, alle denkbaren Anschlüsse, viel Arbeitsspeicher und meist ein integriertes RAID-System zur sicheren Speicherung der »Kundendaten«. Außerdem sind ein oder mehrere Hardware-Schreibschutzmodule bereits eingebaut und vorkonfiguriert. Sie verrichten sowohl unter Windows- als auch unter Linux-Betriebssystemen zuverlässige Arbeit. Extra-Wünsche werden erfüllt. Die Preise der Auswertecomputer variieren stark je nach Ausstattung zwischen zirka 4000 und 20000 Euro.

Das Equipment sollte beim Kauf unbedingt auf dem neuesten technischen Stand sein, denn die Computer, die man damit auswerten wird, sind es schließlich erfahrungsgemäß auch, insbesondere im Privatbereich. Allerdings sind die modernsten und schicksten Grafik- und Soundkarten oder Bildschirme in der Computerforensik irrelevant, diebezüglich genügt die Mindestausstattung.

Wert legen sollte man auf so viele Anschlüsse wie möglich. Neben mehreren USB-3.0-Anschlüssen, die auch an unterschiedlichen Bussen im PC hängen, sind Firewire, eSata, Kartenlesegeräte und möglichst mehrere Gigabit-Netzwerkkarten unbedingt erforderlich. Nur so ist es möglich, ein Image auf ein angeschlossenes NAS-Festplattensystem zu übertragen und gleichzeitig das Netzwerk zu analysieren beziehungsweise in einem getrennten Netzwerk im Internet zu recherchieren.

Ein DVD-/Blueray-Brenner schadet ebenfalls nicht, denn oft ist es vor Ort nötig, einem Beteiligten ein paar Dateien zu übergeben oder man erhält eine Blueray-CD als Asservat.

Es mag zwar altmodisch anmuten, aber auch ein Diskettenlaufwerk (eingebaut oder per USB anzuschließen) gehört zur Pflichtausstattung. Viele Betriebe sichern ihre Daten noch auf Disketten und auch diese Datenträger müssen eingelesen werden können.



Bild 1.2: Der TreCorder kann drei Festplatten gleichzeitig über Schreibschutzmodule auf separate Platten sichern. Er ist auch in kleineren Ausführungen verfügbar

Für die mobile Ausstattung ist ein kleiner Gigabit-Switch (vier bis acht Ports) nützlich, über den man sich mit einem auszuwertenden Netzwerk verbinden kann.

Für den Vor-Ort-Einsatz sind Transportkoffer für die Geräte unabdingbar, zudem sachgerechte Transportkapazitäten für die beschlagnahmten Datenträger oder Computer.

Empfehlenswert für die Laborausstattung ist eine CD-Poliermaschine. Sie kann stark verschmutzte CDs und DVDs reinigen und leicht verkratzte CDs/DVDs polieren und dabei gute Resultate erzielen.

Ein weiterer wichtiger Punkt ist die Redundanz. Man sollte immer die Möglichkeit haben, auf ein Ausweichsystem zurückgreifen zu können. Arbeitet man beispielsweise an zwei Fällen gleichzeitig, kann jeder auf einem anderen Computer abgewickelt werden. Oder wenn in einem dringenden Fall ein Gerät plötzlich einen Defekt hat und nicht mehr einsatzfähig ist, muss man trotzdem in der Lage sein, die Fallbearbeitung zeitnah fortsetzen zu können. Dabei braucht man nicht unbedingt zweimal die gleiche Hardware zu kau-

fen, man kann auch in Betracht ziehen, eine Austausch-Serviceleistung mit einzukaufen. Im professionellen Fachhandel können derartige Verträge beim Kauf abgeschlossen werden.

Vom fertig konfigurierten Auswerte-PC fertigt man sich dann regelmäßig Images an. Bei Geräteausfall oder Diebstahl kann man dann am nächsten Werktag eine gleichwertige Hardware in Betrieb nehmen, seine Images einspielen und weiterarbeiten.

Neben dieser allgemeinen Hardwareausstattung werden aber noch eine ganze Reihe weiterer Komponenten benötigt.



Bild 1.3: Verschiedene externe Schreibschutzmodule mit unterschiedlichen Anschlussmöglichkeiten

Schreibschutzmodule

Eine für das gerichtsverwertbare Auswerten von Computern zwingende Voraussetzung sind Schreibschutzmodule, auch Write Blocker genannt, wo immer dies möglich ist. Dieser Nachsatz besagt auch, dass es Situationen gibt, in denen man nicht mit einem Schreibschutz arbeiten kann, beispielsweise wenn Festplatten eines laufenden Servers gesichert werden müssen.



Bild 1.4: Eine Asservatplatte wird über ein externes Schreibschutzmodul an einen Laptop angeschlossen

Schreibschutzmodule sorgen dafür, dass nicht versehentlich auf die Beweismittel, also auf die auszuwertenden Festplatten oder USB-Sticks geschrieben werden kann. Sie puffern die Daten zwischen, die sonst auf dem Datenträger gespeichert würden. Schreibschutzmodule gibt es in Hard- und in Softwareform, wobei immer Hardwareschreibschutzmodule vorzuziehen sind. Bei Softwareschreibschutzmodulen besteht trotz sorgfältiger Programmierung der Software immer ein Restrisiko, wenn die Software oder der Computer abstürzt. Eventuell könnte dann der Schutz außer Kraft gesetzt werden.

Schreibschutzmodule unabdingbar.

Für den Übertragungsweg zwischen dem Auswertecomputer und dem Schreibschutzmodul gibt es unterschiedliche Möglichkeiten wie Firewire, USB oder einen direkten Anschluss an einen IDE/SATA-Bus.

Das ausgebaute Asservat wird über ein IDE-, SATA- oder USB-Kabel an das externe Schreibschutzmodul angeschlossen, dann werden die Asservatplatte und das Schreibschutzmodul gemeinsam ebenfalls mit einem entsprechenden Kabel an den Auswertecomputer des IT-Forensikers angeschlossen. Die Schreibschutzmodule der Hersteller Tableau, Wiebetech, Voom und ICS können in Deutschland beispielsweise von MH-Service in Karlsruhe bezogen werden.

Zum anderen gibt es interne Schreibschutzmodule, die direkt in den forensischen Auswertecomputer eingebaut sind.



Bild 1.5: Internes Schreibschutzmodul, hier integriert in einen Forensik-Auswertecomputer

1.2.2 Externer Speicher

Die Festplattenkapazitäten nehmen rasant zu, 4-TByte-Festplatten (1 TByte = 1024 GByte) sind auf dem Markt erhältlich und auch in den auszuwertenden Computern zu erwarten. Oft sind auch mehrere Festplatten und weitere Datenträger in einem Computer eingebaut, beispielsweise externe Festplatten, die ebenfalls gesichert werden müssen. Es wird also bereits bei der Sicherung vor Ort eine gewisse Speicherkapazität benötigt.

Dafür bieten sich sogenannte Network-Attached-Storage-Systeme an (NAS). Das sind portable Geräte mit eigener Intelligenz und mehreren eingebauten Festplatten, die zu einem RAID-System zusammengefasst sind und gegebenenfalls auch erweitert werden können. Das RAID-System (RAID 5, 6 oder 10) gibt zusätzliche Sicherheit; falls eine Festplatte dieses Systems ausfällt¹,

¹ Dabei ist aber zu beachten, dass zum gleichen Zeitpunkt erworbene und in Betrieb genommene Festplatten zum ungefähr gleichen Zeitpunkt den Geist aufgeben! Die Marketingaussagen bezüglich der absoluten Sicherheit eines Festplattenverbunds

STICHWORTVERZEICHNIS

\$	
\$AttrDef.....	187
\$BadClus.....	187
\$Bitmap.....	187, 193
\$Boot.....	187
\$Index_Root.....	191
\$LogFile.....	187
\$MFT.....	187, 189
\$MFT suchen.....	195
\$MFT, Dateiheder.....	190
\$MFT, Dateinamen.....	191
\$MFT, Datenbereich.....	191
\$MFT, Inhalt der.....	192
\$MFT-Startadresse.....	195
\$Recycle.bin.....	116, 235
\$Volume.....	187
.....	490
>.....	487
>>.....	488
24-Bit-BMP-Format.....	127
7Z-Archiv, Header.....	121

A	
Abschlussbericht.....	490
Abspiellisten.....	257
Abstreitbarer Container.....	374
Acronis Disk Director GPT.....	178
Active-Flag.....	175
Adaptec-Controller.....	46
Adapter.....	21
AdapterWatch.....	459
Adobe Reader.....	147
Adressauflösung.....	462
Advanced Disk Imager Tool.....	60
Advanced Instant Messengers Password Recovery.....	433
AdvancedMailboxPasswordRecovery.....	411
AFF-Image.....	59

Aid4Mail.....	385
AIR.....	72
AllDup.....	300
Alternative Data Stream.....	120
Analysevorbereitung.....	49
Animationsdateien, Header.....	130
Anmeldedaten f. E-Mail.....	258
Anmeldung am PC, letzte.....	268
Anschlüsse.....	22
AntiTwin.....	301
antiword.....	136
Anzahl d. a. d. Standardeingabe eingegebenen Wörter/Zeichen/Zeilen.....	489
Apple Partition Map, Kennzeichen.....	212
Apple-Partitionseintrag, Aufbau e.....	212
Arbeitsspeicher (RAM).....	224
Arbeitsspeicher, Daten sichern.....	36
Archive.....	140
Archiv-Passwörter knacken.....	351
ARJ-Archiv, Header.....	121
arping.....	463
ARP-Tabelle.....	462
arpwatch.....	463
ASCII-Dateien.....	304
AsteriskLogger.....	357
ATA Disk Password Utility.....	378
ATA-Befehle.....	228
ATA-Passwörter.....	377
Attribut-Header, Aufbau d.....	192
Audiodatei, modifizierte.....	314
Audiodateien, Metadaten.....	318
Ausgabeumleitung.....	487
Ausgeschaltetes System antreffen.....	31
Auslagerungsdatei auswerten.....	312
Auslagerungsdatei, Name der.....	40
Auslagerungspartition.....	225
Auslagerungsspeicher.....	39
Auswertecomputer, Eigenschaften.....	22

Autologon 257
 Autopsy Forensic Browser 107
 Autostartprogramme 257, 260
 Auto-Vervollständigung 257
 awk 415

B

Base64-Kodierung 383
 Basis-Betriebssystem 29
 BearShare, heruntergeladenen Dateien suchen 452
 Benutzer, Standardeinstellungen 262
 Benutzer, zuletzt angemeldete 260
 Benutzer-/Benutzergruppennamen 268
 Benutzerkennungen 116
 Benutzerkonten suchen 270
 Benutzerkontendatenbank 259
 Benutzerkonto ermitteln 268
 Benutzername (Registry) 270
 Benutzername, SID auflösen in 268
 Benutzerpasswort, Registry 344
 Benutzerpasswörter, Speicherort 268
 Benutzerprofile, Speicherort 267
 benutzerspezifische Einstellungen 116
 Bereich, als leer markierter 189
 Betriebssystemkennungen 181
 Betriebssystemstatus wiederherstellen 116
 Betriebssystemversion abfragen 34
 Beweismaterial, Unveränderlichkeit 17
 Beweismittel verbieten 49
 BIFF-Format, Header 138
 Bild, transparente Elemente 126
 Bild-/Grafikformate 123
 Bilddatei, modifizierte 314
 Bilddateien anzeigen, Programme 123
 Bilddateien, Metadaten 318
 Bilder, leicht geänderte 299
 Bildersuche über Klartextsuche 248
 Bildschirmfotos 484
 Bildschirmfotos in virtuellen Maschinen 486
 Bildschirmfotos unter Linux 486
 Binärdateien vergleichen 294, 295
 BIOS, wechseln in 43
 BIOS-Passwort 377
 BIOS-Uhr 90
 BitLocker 375
 BitLocker Encryption Key 376
 BitLocker To Go 376
 Bitlocker-Passwort 376
 Bitmapformat 123
 BitTorrent, heruntergeladenen Dateien suchen 450
 Blogeinträge auslesen 428
 Boot-CD 55
 Bootdatenträger 43

Booten nicht von Platte 43
 Booten von CD 51
 Bootmanager 100
 Bootsektor 173
 Bootvorgang abbrechen 55
 Bootvorgang auf CD umstellen 55
 Broadcast 459
 Browser 411
 Browser, Passwörter in 358
 Browsercache 420
 Browser-Favoriten 413
 Browser-Lesezeichen 413
 Brute-Force-Attacke 362
 Bürogeräte, Dateispeicher in 21
 Bus-Systeme 42
 Byteblock ändern 314

C

Cacheback 410
 Cain&Abel 347
 cat 119, 488
 CCleaner 172
 CD/DVD einlesen (defekte) 82
 CD/DVD, Kratzer 83
 CD/DVD-Dateisystemtyp 99
 CD/DVD-Format 80
 CD/DVD-Image 80
 CD-Brennprogramme 82
 CD-Image einbinden (Lin.) 98
 CD-Image einbinden (Win.) 102
 CDRTools 84
 CD-Sessions 81
 Chat 428
 Chat Examiner 437
 Chat, Cache 434
 Chat, Logging 429
 Chat, Übertragungsprotokoll 429
 Chat-Channel 428
 Chat-Dateien suchen 429
 Chat-Kontaktdaten 429, 438
 Chatlogs, Fundstellen 434
 Chat-Mitschnitt suchen, gelöschten 433
 Chat-Passwörter suchen 431
 Chat-Programme suchen 430
 Chatrooms 429
 Chat-Server 428
 Cisco-Router, Standardpasswörter 379
 Client/Server-Datenbanken 161
 Clonespy 302
 Cloud-Computing 413
 Cluster 182
 Cluster, Zahl d. Sektoren 195
 cmp 295

STICHWORTVERZEICHNIS

cmp, Parameter.....	297	Dateiverkettungen.....	193
Computer meldet sich im Netz an.....	463	Dateizeit auslesen.....	201
Computername.....	267	Dateizuordnungstabelle.....	182
Container.....	113	Dateizuordnungstabelle, virtuelle.....	182
Container, verschlüsselte.....	142	Daten restaurieren.....	189
content.xml.....	151	Datenanteil-Attribute.....	197
Controller.....	41	Datenbereich-Adressierung.....	193
Cookie, Passwort.....	421	Datenrettung.....	16
D			
Datarun.....	193	Datenspeicherplatz f. Image.....	51
Datarun analysieren.....	204	Datenstrom duplizieren.....	488
Datei einlesen.....	489	Datenträger formatieren.....	171
Datei konvertieren.....	122	Datenträger, logischer.....	80
Datei löschen.....	234	Datenträgerbezeichnungen (Lin.).....	210
Datei löschen auf Netzwerkservers.....	235	Datenträger-Image.....	57
Datei löschen auf Wechseldatenträger.....	235	Datenträger-Image einbinden (Lin.).....	99
Datei, anhängen an.....	488	Datenträgerrettung.....	107
Datei, Bearbeiter einer.....	322	Datenübertragungsgeschwindigkeiten f. Image.....	51
Datei, enorm große.....	367	Datum konvertieren.....	338
Dateiattribute.....	192	Datums-/Zeiteinstellungen abgleichen.....	43
Dateicontainer.....	139	Datums-/Zeitstempel.....	88
Datei-Duplikate löschen.....	301	Datums-/Zeitstempel d. Dateisystems.....	94
Datei-Duplikate suchen.....	300	Datums-/Zeitstempel in Metadaten.....	322
Datei-Eigenschaften a. Betriebssystemebene.....	321	dbf-Format, Header.....	162
Dateien auflisten.....	489	db-Format, Header.....	163
Dateien byteweise vergleichen.....	295	dbx-Datei.....	399f.
Dateien durchsuchen.....	303	dbx-Dateien konvertieren.....	401
Dateien in Dateien.....	312	dcfldd.....	59
Dateien vergleichen.....	293	dcfldd, Parameter.....	64
Dateien verstecken.....	47, 113	dcode.....	95, 338
Dateien zeilenweise vergleichen.....	294	dd.....	59
Dateien, eingebettete.....	113	dd, Parameter.....	60
Dateien, gelöschte/nicht zugeordnete.....	113, 234	dd_rescue/ddrescue.....	70
Dateien, Speicherorte.....	113	Default-Gateway ermitteln.....	459
Dateienamen suchen.....	241	Defaultroute.....	457
Dateiende-Zeichen.....	159	defekten Datenträger sichern.....	69
Dateiformate.....	117	Desktop-Festplattensicherung.....	44
Dateifragmente suchen.....	198	Device Configuration Overlay erkennen.....	231
Dateigrößenbeschränkung.....	63	DHCP-Server ermitteln.....	459
Dateiheader anzeigen.....	118	Dialupass.....	356
Dateiheader suchen.....	236	Dictionary-Attack.....	362
Dateiindex erzeugen.....	114	diff.....	294
Dateikennung/File-Identifizier.....	122, 189	dig.....	470
Dateinamensendung.....	117, 119	Digitalkamera.....	279
Dateinhalt anzeigen.....	119	Disk Monitor.....	54
Dateislack.....	226	disk_stat.....	233
Dateisuche, allg. Vorgehensweise.....	114	Diskettenaufteilung.....	172
Dateisystem, ladbares.....	107	Diskexplorer.....	205
Dateisysteme.....	182	Distributed Network Attack.....	354
Dateisystemtreiber (Linux).....	99	DLLs.....	167
Dateityp über Klartexteinträge finden.....	247	dmesg.....	54, 233
Dateityp-Informationen ermitteln.....	247	DNS-Server ermitteln.....	459
		DOC-Datei konvertieren.....	135
		docfileviewer.....	322

DOC-Format, Header 135, 137
docX entpacken..... 152
docX-Dateien..... 138, 151
Dokumentation 481
Dokumentinhalte vergleichen 298
Domain..... 458
Domain Name System..... 465
Dongle..... 343
DOS-Stub 166
DoublePics 299
Download-Clients suchen 448
Downloadverzeichnis..... 266
Druckereinstellungen..... 116
Druckjob-Dateien..... 142
Drucksysteme 142
dumphive 261
dumphive kompilieren 272
Duplikate in Text entfernen..... 415
DVD, Kapazität..... 60

E

E01-Images 59
EFI-Firmware..... 175
EFS-Verschlüsselung 371
EFS-Verschlüsselung knacken 352
EFS-Verschlüsselung, Benutzerpasswort 344
Eigenen Rechner ansprechen 456
Eingeschaltetes System antreffen..... 31
Elcomsoft Advanced EFS Data Recovery 352
Elcomsoft Password Recovery Bundle..... 350
E-Mail, Absendedatum umrechnen 393
E-Mail, Dateiheder 395, 396
E-Mail, Uhrzeit..... 393
E-Mail-Account-Passwörter knacken..... 411
E-Mailadresse durchsuchen..... 308
E-Mail-Anhang..... 383
E-Mail-Anhang in gelöschten Bereichen suchen 383
E-Mail-Aufbau..... 382
E-Mail-Auswerteprogramme 385
E-Mail-Datei, einzelne 383
E-Mail-Dateien, Formate..... 382, 394
Email-Examiner 385, 408
E-Mail-Header 382
E-Mail-Header herunterladen 381
E-Mail-Konten, Passwort knacken 355
E-Mails 381
E-Mails in einer Datei gespeichert 382
E-Mails suchen..... 385
E-Mails, fremde einlesen 388
E-Mails, verschlüsselte..... 368, 384
E-Mail-Verwaltungsprogramm 381
eml..... 383
EnCase-Image 59, 66

Ereigniseinträge/Ereignislogs 335
Ereignisprotokolleintrag, Aufbau..... 336
Erweiterte Partition 174
Etherape 480
Ethernetadresse..... 455
Event-ID 335
Eventlog/Ereignisprotokoll 276
Eventlogs 116
Eventlogs auswerten 335
evt(x)-Datei 276, 339
ewf_acquire kompilieren..... 66
EWF-Images 59
Excel-Dateiformat 138
exec 242
ExFAT 187
EXIF-Daten 281
ext, Blockgröße 208
ext, Partitionsgröße auslesen..... 210
ext, Superblock 207
ext2/3/4..... 206
ext-Datenträger einbinden (Win.)..... 106
Externe Datenträger..... 47
ext-Partition, Aufteilung 207
ext-Partition, gelöschte 210
Extrahierte Dateien 257

F

Facebook 423
Facebook, Benutzerdaten 425
Facebook, Chat-Protokoll 429
Facebook, Personenbeziehungen 427
Facebook, Registry-Einträge 424
Facebook-Passwort 425
Facebook-Visualizer 427
Fachvokabular, Wörterbuch mit 364
Farbinformationen..... 118
FAT (File Allocation Table) 182
FAT 32 Volume Boot Sector, Inhalt d..... 186
FAT, Größenbeschränkung d. Images 59
FAT-Partition, Elemente 185
FAT-Partition, Rootverzeichnis 183
FAT-Verzeichniseinträge 186
FavoritesView..... 414
Fax, TIFF-Unterformat Klasse F 124
Festplatte an Auswerte-PC anschließen..... 52
Festplatte nicht ausbauen 55
Festplatte, Datenfehler auf 57
Festplatten-Anschlussarten 41, 44
Festplattenaufteilung..... 172
Festplattengrößen 41
Festplatten-Image einbinden (Win.) 103
Festplattenkapazität auslesen 54
Festplattenpartition 172

STICHWORTVERZEICHNIS

Festplatten-Speziallabor	58	GPT-Datenträger konvertieren	178
Festplattenverschlüsselung, Bindung an Hardware...	43	GPT-Festplatte, 1. Sektor	176
Festplattenverwaltungsdaten auslesen	54	GPT-Festplatte, Bereiche	176
file	247	GPT-Header	176f.
File Records	191	GPT-Partitionsgröße	176
Filesharing-Netz	443	Greenwich Mean Time (GMT)	91
Filesharing-Protokolle	444	grep, Binärdateien untersuchen	306
find	236, 241	grep, Metazeichen maskieren	307
find, Befehlsübergabe	243	grep, Optionen	305
find, Escape-Sequenzen	247	grep, Suchmuster	306
find, Parameter	243	grep, Zeichenklassen	308
find, printf	246	grep/egrep/fgrep	304
Firefox, Profil-Manager aufrufen	389	Größer-Zeichen	487
Firefox, Registry	420	Grundregeln beim Auffinden e. PC	31
Firefox-Cookies	421	gTableauParm	230
Flachbandkabel	44	gthumb	289
Flat File	161	GUID Partition Table	172, 175, 212
flc/fli-Format, Header	130	guymager	74
flv-Format, Header	131		
foremost	236	H	
Forensik-Software	29	Hackerangriff	454
Fork	117	Hardwareinformationen	260
Foto, GPS-Daten d. Aufnahmeorts	283	Hardwarekonfiguration	263
Fotoapparat	28	Hardwareschreibschutzmodule	25
Fotoapparat, Datum	487	Hardware-Uhr	90
Fotoapparat-Fingerabdruck	282	Hardwareverschlüsselung	342
Fotoapparat-Speicher anzeigen	281	Hauptspeicher, Daten im	36
Foto-Format	125	Hauptspeicherinhalt ansehen	310
FreeOTFE-Container	372	Hauptspeicherinhalt indizieren	311
FTK-Imager	76	hdparm	232
Funkuhr	43, 90	hdunlock	378
		Helix	55
G		Hex Workshop	196
galleta	422	Hexadezimalzahl in Dezimal konvertieren	268
GELI-Verschlüsselung	342	HFS+	211, 214
Gelöschte Dateien	116	HFS-Partition suchen	213
Gelöschte Dateien suchen	236	hiberfil.sys	39, 116, 225, 309
Geotagging	283	Hibernation-Modus	39, 116
Geräte, angeschlossene	116, 276	High-Level-Formatierung	171
Geräteeintrag (Linux)	97	Hiren's BootCD	107
Gerichtsverwertbares Arbeiten	16, 49	History analysieren	414
Gesichtserkennung	284, 300, 428	HKEY_CLASSES_ROOT	262
GetDataBack	199	HKEY_CURRENT_CONFIG	263
GIF-Animationen	128	HKEY_CURRENT_USER	262
GIF-Format, Header	127	HKEY_CURRENT_USER\Software\Classes	262
Gigabit-Switch	23	HKEY_LOCAL_MACHINE	263
Gimp	123	HKEY_LOCAL_MACHINE\Software	262
GnuPG-Format, Header	368	HKEY_LOCAL_MACHINE\Software\Classes	262
Google Talk, Chat-Protokoll	429	HKEY_PERFORMANCE_DATA	263
gphoto2	279	HKEY_USERS	263
gphoto2, Optionen	280	Hops	463
GPS-Koordinaten auf Landkarte eintragen	283	host	473
GPT	175	Host Protected Area (HPA) erkennen	227

Hostname, Aufbau	458
hosts-Datei	456
html-Format, Header	147
HTML-Wrapper um Thumbnails schreiben	288

I

ICQ-Kontakte	266, 440
IDE-Bus	42
IECacheView	418
ifconfig	19, 34, 459
Image aufspalten	61
Image einhängen	97
Image in virtuelle Maschine umwandeln	59
Image mit VMware einbinden	104
Image schreiben (Linux)	60
Image v. defektem Datenträger	69
Image verifizieren	86
Image zurückschreiben	66
Image, Datenübertragungsgeschwindigkeiten	51
Image, Logical Drive	80
Image, MD5-Prüfsumme	59
Image, Metadaten in	59
Image, Startsektor	68
Image, verschlüsseltes laden	98
Image, virtuelle Maschine	103
Image-Aufspaltung	58
Image-Datenbereich, Beginn	100
Image-Formate	58
Image-Gerätetreiber (Win.)	102
Image-Prüfsumme	65, 86
Images unter Windows	76
ImportExportTools	392
Index, alphabetischen schreiben	311
index.dat	116, 256, 416
Indexdateien	197
Infektion verbergen	47
info2	116, 251
Inkscape	123, 129
innerer Container	374
Inode, Inhalt d.	210
Node-Tabelle	209
insmod	97
Interlaced	126
Internet Evidence Finder	312, 428, 435
Internet Explorer, Adressen	266
Internet Explorer, Browsercache	416
Internet Explorer, History	416
Internet Explorer-Autologon	266
Internet Explorer-Cache	395
Internet Explorer-Cookies	421
Internet Explorer-Suchbegriffe	266, 267
Internet History anzeigen	116, 414
Internet History, Firefox	420

Internet History, Zeitstempel	416
Internetadressen, eingetippte	413, 419
Internetverhalten, Profil	32
IP in Ethernetadresse wandeln	462
IP-/Gateway-Informationen	267
IP-Adresse bekanntgeben	463
IP-Adresse suchen	308, 459
IP-Adresse, Ablauffrist der	459
IP-Adresse, Aufbau	455
IP-Adresse, statische/dynamische vergeben	459
IP-Adressen in Domainnamen übersetzen	459
IP-Adressen umwandeln	465
ipconfig	34, 459
IP-Paket, Aufbau	457
IP-Paket, Versand	457
IP-Paket, Weg verfolgen	463
IP-Protokoll	455
IrfanView	284
ISO-9660-Format	80
IsoBuster	83
ISO-Image mit Laufwerkstreiber verbinden	102

J

Jabber Protocol	429
JPG-Artefakte	125
JPG-Format, Header	125

K

Kabel	21
Kabelverlauf prüfen	33
Kameradaten	281
Kamera-Speicherbereich	279
Kartenleser	42
Kompressionsprogramme	140
Konsole restaurieren	119
Kontenbezogene Daten	257

L

LAN-Passwort	345
Laptop ausschalten	32
Laptop, Akku entfernen	42
Laufende Prozesse	309
Laufwerk f. Virtualisierung vorbereiten	104
Laufwerksdateien einbinden (Win.)	102
libewf	66
Limewire, heruntergeladenen Dateien suchen	451
Linux-/Unix-Zeit, Beginn	91
Linux-Boot-CDs	108
Linux-Dateisysteme	206
Linux-Live-CD	51, 55
Linux-RAM auslesen	41
Linux-Shutdown	31
Linux-Wiederherstellungssystem	107

STICHWORTVERZEICHNIS

Live ContactsView	433
LiveView	104
Localhost	456
Log-Dateien	339
Logfunktion	487
Logical-Block-Adressierung	176
Logon-Zeit	116, 268
Lokale SIDs	267
Loopback-Adresse	456
Loop-Device (Def.)	97
Loop-Device aushängen	98f.
Loop-Device, Name des	97f.
Loop-Devices, Kerneltreiber laden	97
Löschen, sicheres	172
losetup, Parameter	98
Lowlevel-Formatierung	46, 172
ls	114, 489

M

MAC-Adresse	455
MAC-Adresse ermitteln	18
MAC-Adresse fälschen	19
MAC-Adresse, anpingen über	463
Macintosh booten	212
Macintosh herunterfahren	32
Macintosh, Metadaten im Fork	117
MAC-Zeitstempel	90, 190
Mail PassView	355
Mail-Account auf POP-Server	382
Mailbox-Format	382
MailPassView	371
Mailserversuchen	411
Master Boot Record	172
Master Boot Record reparieren	216
Master Boot Record, Ende des	174
Master File Table (MFT)	187
Master File Table, Eintragsbeginn/-ende	193
Master File Table, Startadresse d.	189
mbox	382
MD5-Hashwert	86
md5sum	59, 86, 87
MessenPass	431
Metadaten	113, 192
Metadaten auswerten	318
MetadatenSpeicherung in Image	59
MFT, 1. Eintrag	196
MFT-Attribute, ausgelagerte	197
MFT-Eintrag analysieren	199
MFT-Fragmentierung	197
MFT-Header-Kennung	200
Microsoft-Mails importieren	392
Mittäterkreis	32
Mobiltelefone, Empfang unterbrechen	20

more	119
Mount, schreibgesichertes	52
Mountpunkt	98
MozillaCacheView	421
mp3-Dateien, leicht geänderte	302
mp3/4-Format, Header	131f.
msgmgmt.fdb	408
MSN Messenger	266
Mülleimer	116
Mülleimer e. E-Mail-Clients	384
Musikstücke, leicht geänderte	299

N

Namensauflösung	464
NAS	20, 26
Navigationssystem	21
Navision-Datenbankdatei	408
NetAnalysis	312
Network Password Recovery	359, 380
Netzstecker ziehen	32
Netzwerk, aktuelle Zeit festhalten	488
Netzwerk-Aufbau	458
Netzwerkeinstellungen	116
Netzwerkfreigaben, Passwörter für	359, 380
Netzwerkkarte ermitteln	459
Netzwerkkarte, Adresse	18
Netzwerkkarten im Netz, welche?	462
Netzwerkkarten-Nummer	455
Netzwerk-Passwörter	379
Netzwerk-Teilnehmer	460
Netzwerktools	47
Netzwerkumgebung grafisch darstellen	480
Netzwerkverbindungen, aktive anzeigen	34
Netzwerkverkehr mitschneiden	453, 473
NFS, Zeitstempel	89
nmap	460
nmap, grafische Oberfläche	461
nmapfe	461
Notauswurf d. PC	42
Notebook-Festplattensicherung	44
nslookup	469
NSRL-Hashset	298
NTFS	187
NTFS, Aufbau d. Volume Boot Record	179
NTFS, Volume Boot Record	189
NTFS-Bootloader	187
NTFS-Partition, Datei löschen auf	198
NTFS-Systemdateien	187
NTFS-Treiber	188
ntfsundelete	204
NTFS-Versionen	188
NT-Kernel, Header	310
NT-Passwort	345

ntuser.dat 116, 257
 ntuser.dat, Daten 266

O

Oder-Suche in Text 415
 ODT-Format entpacken 156
 OE-Addressbook 399
 Office-Dateien, Metadaten 319
 ogg-Format, Header 132
 OLE-Container 136
 OLE-Container, Adressen im Headerblock 327
 OLE-Container, Aufbau 323
 OLE-Container, Blocknummern 326
 OLE-Container, Dateiheader 325
 OLE-Container, Header 323
 OLE-Container, Root-Eintrag 331
 OLE-Container, Wurzeleintrag 323
 OLE-Dokument, Bestandteile 329
 One-/Recorder 22
 Online-Speicherplatz 28, 413
 ooxml-Format 151
 OpenOffice.org Draw 123
 Opera Cache View 421
 Opera, Internet-History, 421
 Ophcrack 344
 Outlook 404
 Outlook Express 399
 Outlook Express Freebie Backup 400
 Outlook Express, Adressen 399
 Outlook-Mails importieren 392
 Outlook-Passwörter 266

P

Packprogramme (Linux) 62
 pagefile.sys 39, 116, 225, 309
 Papierkorb 250
 Papierkorb auslesen 251
 Papierkorb leeren 198, 235
 Paradox-Betrachter 163
 Partition, Dateien und Verzeichnisse 189
 Partition, erweiterte 172
 Partitionen einbinden 99
 Partitionen verschlüsseln 375
 Partitionen, eingerichtete anzeigen 233
 Partitionen, gelöschte suchen 216
 Partitionsanfang suchen 178, 180
 Partitionsgröße 180
 Partitionskennungen im MBR 175
 Partitionstabelle löschen 171
 Partitionstabelle, Aufbau 173
 Partitionstabelle, Größe 172
 pasco 414
 Password 354

Password Recovery Tool Kit 354
 PasswordFox 358, 426
 Paßwort dynamisch verschlüsseln 373
 Passwort im RAM suchen 36, 311
 Passwort in Arbeitsspeicher 373
 Passwortdatenbank v. Firefox, 426
 Passworteingabe hinter Sternchen 357
 Passwörter 116
 Passwörter in Office-Dokumenten 369
 Passwort-Ermittlungsverfahren 360
 Passwort-Knackprogramme 344
 Passwörterlängen 341
 PC, verdächtigen ausschalten 32
 PC, verdächtigen nicht ausgeschaltet 34
 PC-Name 116
 PDF lesen 146
 PDF, mehrseitiges Dokument speichern 146
 pdf-Format, Header 146
 PDF-Viewer 147
 PeerLab 449
 Peer-to-Peer-Netze 443
 Perkeo 297
 pfx-Datei 371
 PGP knacken 354
 PGP-Format, Header 368
 PGP-Verschlüsselung 369
 Picasa 284
 ping 456, 460
 Pingscan 461
 Pipeline 489f.
 PNG 126
 png-Format, Header 126
 PoolTools 311
 Primäre Partition 175
 printf, Platzhalter 245
 Proactive System Password Recovery 346
 profiles.ini 388
 Programmdateien-Prüfsummenvergleich 298
 Programme (installierte), Fundort 116
 Programme ohne Installation 248
 Programme suchen 272
 Programmgergebnisse weiterleiten 489
 Programm-Icon, Eigenschaften editieren 389
 Programmverknüpfungen 258, 262
 Protokoll-Analyzer 474
 Protokoll-Anlagen 483
 Protokollaufbau 482
 Protokolldateien 339
 Prozess, Header e. laufenden 311
 Prüfsumme erzeugen 65
 Prüfsummen-Datenbanken 297
 Prüfsummenvergleich, unwirksamer 299
 Prüfsummenvergleiche 297

STICHWORTVERZEICHNIS

psd-Format, header	129
PS-Format, Header	144
pst-Dateien konvertieren.....	404

Q

qemu-img	103
----------------	-----

R

RAID-System	26
Rainbow-Tabellen	348, 365
RAM auswerten	309
RAM-Imaging-Tool.....	36
RAW-Dateien (Image) konvertieren.....	103
RAW-Image	59
RAW-Image anlegen.....	59
RAW-Image konvertieren	59
readpst	405
readpst, Parameter.....	407
Recent-Dokumente.....	267
Recent-Inhalte	116
recycle.bin.....	251
regedit.exe	261
Registrierdatenbank, globale Dateien.....	257
Registrierdatenbankschlüssel, Datentypen.....	264, 265
Registrierdatenbankschl., Unterstützungsdateien.....	263
Registrierungsschlüssel (Def.)	264
Registry, Benutzerpasswort.....	344
Registry, Chat-Benutznamen.....	439
Registry, Zugriffsprogramme	261
Registryeinträge in SYSTEM.....	266, 267
Regscan	261
reset.....	119
Residente Daten	201, 192
Restore Points	248
rifiuti.....	251
Rootkits	47
Root-Nameserver	465
Router	457
Router-Passwörter	379
Routingtabelle.....	457
RTF-Format.....	137
RTF-Format, Header	161
Ruhezustand des PC	116, 225
Ruhezustandsdatei auswerten	312

S

SAM.....	116, 259
SAM/SYSTEM, Dumpdatei erzeugen aus	349
SamInside.....	349
SAN.....	20
SAS	46
SATA-Bus.....	42
scalpel.....	236, 310

scalpel kompilieren.....	236
scalpel konfigurieren	237
scalpel, E-Mail-Dateien suchen.....	394
scalpel, Optionen.....	239
scalpel-Konfigdatei (scalpel.conf) erweitern	237, 394
Schlafmodus	39
Schnellformatierung	171
Schreibschutzmodul anschließen.....	52
Schreibschutzmodul, Asservat anschliessen	25
Schreibschutzmodule	24
script	487
SCSI-Platten.....	42, 45f.
SeaMonkey.....	386
SECURITY.....	116
Sektoren. verfügbare anzeigen	233
Server-Festplattensicherung	46
Serversystem herunterfahren.....	32
Session-Cookies.....	421
SHA-Verfahren	86
Shutdown time.....	260
SID	116
SID auflösen.....	268
SIDs, vordefinierte.....	269
Skype, Chat-Mitschnitt.....	442
Skype, Telefonie-Mitschnitt.....	441
SkypeLogView	442
Slackspace.....	226
Snagit	485
Social Engineering.....	360, 425
SOFTWARE.....	116
Sommerzeit.....	91
sort.....	311
Soziale Netzwerke, veröff. Personeninformationen	423
Speicherauslagerungsdatei	116
Speicherbedarf, Rechenbeispiel	27
Speicherdump.....	117
Speicherdump auswerten	309
split, Parameter.....	61
Spurensicherung	15
Sqlite-Datenbank in csv konvertieren	422
Standardeingabe umleiten	489
Steganographie.....	312
Steganographie-Programme	315
Stegdetect, Optionen.....	316
Steghide.....	315
strings.....	311
Suchbereiche	168
Suchmaschinen-Begriff suchen	411
Suchmuster.....	304
Sumatra PDF.....	147
Superblock suchen.....	210
Superblock-Kennung.....	210
Suspend-to-Disk-Modus	116, 225

svg-Format, Header..... 129
 System Information for Windows 54
 Systemprotokoll (Linux)..... 54
 Systemuhr..... 90

T

Tableau Disk Monitor..... 54, 230
 Tableau Hardware Accelerator 343
 Tagesprotokolle 481
 tar.bz2-Datei..... 140
 tar.gz-Datei..... 140
 tar-Archiv 140
 Tastaturfehler auslösen 43
 Tauschbörsen..... 443
 tcdump, Darstellung des Paketinhalts 476
 TCHunt 373
 tcpdump..... 474
 tcpdump, grafische Auswerteprogramme 478
 tcpdump, Oktetts übergeben 476
 tcpdump, Optionen 476
 tcpflow, Optionen 478
 TestDisk 216
 Text, Duplikate entfernen in 415
 Textdateien durchsuchen 304
 Textdateien vergleichen 293
 Textformate, Zeichensatz 158
 The Sleuth Kit..... 107
 thumbcache_xxx.db..... 286
 Thumbnail Database Viewer 290
 Thumbnail, Dateigröße 287
 Thumbnail-Dateien suchen 286
 Thumbnails in HTML-Datei einbetten 281
 thumbs.db 286
 ThumbsDisplay..... 291
 Thunderbird 386, 397
 Thunderbird, Adressbuch..... 398
 Thunderbird, Benutzerprofil..... 388
 Thunderbird, Default-Profil 391
 Thunderbird, Maildateien..... 398
 Thunderbird, Passwörter 399
 Thunderbird, persönl. Wörterbuch 399
 Thunderbird, Profil-Manager 389
 Thunderbird, Profil-Ordner..... 397
 TIF-Datei, Header 124
 TIFF, Macintosh..... 124
 Time Organisation 92
 Token, externer 343
 tonl2eml 409
 T-Online konvertieren 408
 Toshiba-Laptop, BIOS-Passwort 377
 Total Commander 298
 tracert 463
 trash.* 384

Truecrypt-/FreeOTFE-Container, Header..... 373
 TrueCrypt-Bootpasswort..... 375
 TrueCrypt-Container..... 372
 Trusted Platform Module..... 376
 TShark 478
 TTL (Time-to-Live)..... 470
 type..... 118
 TypedURL 258, 266, 419

U

udevinfo..... 276
 UDF-Format 81
 Uhrzeit dokumentieren 32
 Ultimate BootCD 359
 Umleitungszeichen 488
 Unallocated Clusters 189
 uniq... 415
 Urladeprogramm..... 172
 USB-Controller 42
 USB-Geräte suchen..... 276
 UTC... 91
 UUE... 140

V

Vektorformat..... 123
 Vektorgrafik-Standardformat 129
 Verknüpfungen zu anderen Dokumenten..... 146
 Verpolungssicherheit 45
 Verschlüsselte Archivdateien 370
 Verschlüsselte Container..... 370
 Verschlüsselte Datei, Anzeichen für 367
 Verschlüsselte Einzeldateien 368
 Verschlüsselung..... 31
 Verschlüsselung, asymmetrische..... 369
 Verschlüsselung, laufende..... 35
 Verzeichnisse vergleichen..... 295
 VFAT 182
 Videomitschnitt..... 485
 vinetto 288
 Virtuelle Maschine 29
 Virtuelle Maschine konvertieren..... 140
 Virtuelle Maschine, Dateiformat 140
 Virtuelles CD/DVD-Laufwerk (Win.)..... 103
 VMware, Image importieren 69
 vmx-/vmdk-Dateien erzeugen 105
 Vollverschlüsselung 374
 Volume Boot Record 173, 178
 Volume Boot Record, Beginn des 178
 Volume Boot Record, Ende des 179
 Volume Boot Sector 183
 Vorschaubilder 286
 VPN/Dial-Up-Einträge 356

STICHWORTVERZEICHNIS

W	
wab-Datei	399
wav-Format, Header	132
wc	489
Webbrowser, E-Mail über	382, 409
Webmail	382, 409
Webmail-Provider	411
Wechselmedien	20
whois	466
whois, Optionen	468
Wiederherstellungspunkte in VM laden	250
Wiederherstellungspunkte zurücksetzen in VM	250
Windows 7/Vista herunterfahren	32
Windows Mail, Adressbuch	408
Windows Mail, Benutzerdaten	408
Windows Mail, Format	407
Windows Messenger, Kontakte	440
Windows, portables	107
Windows-Adressbuch	399
Windows-BMP, Header	127
Windows-Daten wiederherstellen (Lin.)	107
Windows-Einwahlpasswort	344
Windows-History	257
Windows-Papierkorb	169
Windows-Programmbeginn	166
Windows-RAM auslesen	37
Windows-Startpasswort entfernen	359
Windows-Systemdateien betrachten	256
Windows-Systemzugangs-Passwort	341
Windows-Taschenrechner	268
Windows-Verschlüsselung	258
Windows-Version	260
Winterzeit	91
Wireshark	478
Word Binary File Format	134
Word Password Unlocker	370
Word/Excel Password Recovery Wizard	370
Word-Dokument, Metadaten	320
Word-Dokument, Metadaten wiederherstellen	323
WORM	82
Wörterbuch, Platteninhalt als	365
Wörterbuchhatacke	362
Wörterbücher zusammenstellen	363
WPA2-Verschlüsselung knacken	350
Write Blocker	24
X	
XML-Format (Word), Header	155
XML-Formate	150
xsteg	317
X-Ways Forensic Browser	79
xxd	119
Y	
Yahoo	257
Yahoo Instant Messenger, Dateiheadersuche	440
Yahoo Messenger, dat-Dateien	439
Yahoo Messenger, Kontakte	439
Z	
Zeichensatz	158
Zeilensprung	126
Zeit unter Windows	90
Zeit, Ereignisprotokoll	92
Zeit, lokale errechnen	92
Zeit, Registrierdatenbank	93
Zeitbestimmung	88
Zeiteinstellungen abgleichen	32
Zeitserver	90
Zeitstempel	89
Zeitzone ohne Wechsel	91
Zeitzone, Speicherort	261
Zeitzone	90
zenmap	461
Zeugen	482
ZIP-Archiv (verschlüss.), Header	370
ZIP-Archiv, Header	122