**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.



1. Auflage 2012


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

# Kapitel 6
# Verschlüsselung ..... 341

# Kapitel 7
# Online-Aktivitäten .....381

# 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 wegzudenkendeTatwerkzeuge 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 Benutzerkennung 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 sein[1], 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 Netzwerkkabel 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, abstrahlschützende 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 Papierausdrucken hinterlegen manche Drucker an einer bestimmten Stelle ein mit dem bloßen Auge unsichtbares Wasserzeichen, in dem Drukker- und Dateiinformationen 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 WERKZEUGKOFFER[1]

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 externen 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 ausfällt[1],

[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

## B



## C

## D

## E



## F

## G



## H

## M



## N

## T



## U



## V

## W



## X



## Y



## Z