COMPUTER FORENSIK HACKS™

O'REILLY®

HACKS SERIES™

Lorenz Kuhlee & Victor Völzow

COMPUTER-FORENSIK HACKS™

Lorenz Kuhlee
Victor Völzow

O'REILLY®
Beijing · Cambridge · Farnham · Köln · Sebastopol · Tokyo

Kommentare und Fragen können Sie gerne an uns richten:
O'Reilly Verlag
Balthasarstr. 81
50670 Köln
E-Mail: kommentar@oreilly.de

Bibliografische Information Der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über *http://dnb.d-nb.de* abrufbar.

Lektorat: Volker Bombien, Köln
Fachliche Begutachtung: Prof. Dr. Felix Freiling
Korrektorat: Eike Nitz, Köln
Satz: III-satz, Husby, www.drei-satz.de
Umschlaggestaltung: Michael Oreal, Köln
Produktion: Andrea Miß, Köln
Belichtung, Druck und buchbinderische Verarbeitung:
Druckerei Kösel, Krugzell; www.koeselbuch.de

ISBN 978-3-86899-121-5

Dieses Buch ist auf 100% chlorfrei gebleichtem Papier gedruckt.

Inhalt

Vorwort und Danksagungen

Wir möchten uns ganz herzlich bei allen Personen bedanken, die bei der Entstehung dieses Buches mitgewirkt haben, uns unterstützt haben und uns durch Ihre Fragestellungen und Vorschläge inspiriert haben.

Lorenz Kuhlee

Wenn mir vor gar nicht langer Zeit jemand gesagt hätte, dass ich ein Buch schreibe, hätte ich ihn belächelt. Doch nun habe ich genau das getan. Dies hat vor allem Volker Bombien vom O'Reilly Verlag möglich gemacht und dafür und das damit in mich gesetzte Vertrauen möchte ich ihm danken. Außerdem auch Herrn Prof. Dr. Freiling für die Fachaufsicht.

Besonders hervorheben möchte ich, dass dieses Buch nur durch die überaus gute und kreative Zusammenarbeit zwischen Victor Völzow und mir zustande gekommen ist. Der Bereich Computer-Forensik ist mir im Laufe der Jahre vor allem auch wegen der guten Zusammenarbeit und dem Austausch innerhalb der Computer-Forensik-Gemeinschaft sehr ans Herz gewachsen. Daher danke ich allen Forensikern, die ich während meiner Tätigkeit als Fachlehrer kennen und schätzen lernen durfte. Gerne würde ich jeden einzelnen hier erwähnen, die Liste wäre jedoch zu lang. Dennoch möchte ich einem besonders danken, da er mich immer wieder inspiriert hat. Danke Jörn!

Ich hoffe, dass dieses Buch bei seinen Lesern Anklang findet und eine hilfreiche Stütze für die Forensik-Community wird.

Zuletzt möchte ich meiner Lebensgefährtin Anja danken, die mich immer wieder ermutigt hat, das Projekt zu Ende zu führen und obwohl wir viel gemeinsame Zeit entbehren mussten, immer Verständnis hatte. Das ist nicht selbstverständlich. Danke, mein Stern.

Victor Völzow

Vielen Dank, dass Sie unser Buch zur Hand genommen haben. Es gibt mittlerweile eine ganze Menge guter Forensik-Bücher auf dem Markt, daher ehrt uns die Tatsache, dass Sie sich für unseres entschieden haben, ungemein. Als Lorenz mir letztes Jahr von seiner Idee für dieses Buch erzählte, war ich schnell begeistert, weil mir die Idee gefiel, ein Forensik-Buch zu schreiben, das einen völlig anderen Ansatz verfolgt. 100 Hacks mit 100 konkreten Aufgabenstellungen und zielgerichteten Lösungen – das war neu in der digitalen Forensik.

Unzählige arbeitsintensive Abende und Wochenenden sind seit dem ersten Kontakt zum O'Reilly Verlag vergangen, in denen wir Stück für Stück die 100 Hacks mit Leben füllen konnten. Diese Zeit der Zusammenarbeit mit Lorenz empfand ich als außerordentlich angenehm und persönlich wie auch fachlich bereichernd. Zu dem positiven Entstehungsprozess beigetragen hat auch Volker Bombien, der uns hervorragend betreute und ein feines Gefühl dafür bewies, wie viel Freiraum einerseits und wie viel Druck andererseits er uns zumuten konnte. Vielen Dank dafür!

Ohne die unzähligen Forensiker-Kollegen, mit denen ich in meiner Tätigkeit als Computer-Forensiker und Fachlehrer zusammenarbeiten durfte, wäre dieses Buch nie zustande gekommen. Ihre Problemstellungen, Erklärungen, Ideen, Tipps und Tricks, ihre Fragen und ihr Feedback sind die Triebfeder von *Computer-Forensik Hacks*. Es sind schlichtweg zu viele Kollegen, Freunde und Kommilitonen, denen ich viel zu verdanken habe. Sie hier alle aufzuzählen, würde den Rahmen des Buches sprengen. Ihnen allen gilt mein Dank! Stellvertretend für sie möchte ich gern speziell Andreas Schoppe und dem ZK 50 danken.

Ein Projekt wie dieses Buch ist nicht möglich, wenn nicht auch das soziale Umfeld viel Verständnis und die nötige Begeisterungsfähigkeit dafür aufbringen. Ein großer Dank geht daher an meine Familie und meine Freunde. Ganz besonders möchte ich meiner Frau Anna danken für Ihr Verständnis und Ihr Einfühlungsvermögen, wenn das ersehnte Abendprogramm einer Vielzahl von Tastaturanschlägen weichen musste. Vielen Dank für Deine unerschöpfliche Geduld und unendliche Liebe!

Zu guter Letzt möchte ich Felix Freiling für die zwar leider zu seltenen, aber dafür umso interessanteren Gedankenaustausche danken. Vielen herzlichen Dank auch dafür, dass Du Dich bereit erklärt hast, die Fachaufsicht für dieses Buch zu übernehmen.

Grußwort von Prof. Dr. Felix Freiling

Computer-Forensik Hacks: Erscheint der Titel nicht als Widerspruch in sich? Schließlich ist Hacking ein eher negativ besetzter Begriff, der häufig mit den Straftätern, also den »Bösen«, assoziiert wird. Und mit Computer-Forensik wird doch eher mit der Polizei, also den »Guten«, verbunden. Vermittelt dieses Buch also »den Guten böse Dinge«? Wie passt das zusammen?

Für mich stellt sich diese Frage nicht: Hacking, also der innovative und häufig auch offensive Umgang mit Computertechnik, bildet die Grundlage jeder vernünftigen IT-Sicherheitskompetenz. Wer Hacking versteht, kann reale Gefahren besser einschätzen und Angreiferverhalten besser antizipieren. Diese Einsicht, die durch wissenschaftliche Studien gestützt wird, setzt sich auch in der Praxis immer mehr durch.

Wir brauchen also eher mehr Hacking als weniger. Vor allem brauchen wir mehr Hacking für die »Guten«, um mit der Gegenseite Schritt zu halten. Nicht nur deshalb ist das vorliegende Buch von Victor Völzow und Lorenz Kuhlee so wertvoll. Die Autoren haben es geschafft, aktuelle Techniken der digitalen Forensik präzise und unterhaltsam darzustellen. Ein lesenswertes Buch, das Spaß macht und die Praxis positiv beeinflussen wird. Möge die Lektüre dieses Buches mehr »Völzows« und »Kuhlees« hervorbringen, sodass der Titel *Computer-Forensik Hacks* in Kürze keinen Widerspruch mehr hervorruft.

Prof. Dr. Felix Freiling ist Inhaber des Lehrstuhls für IT-Sicherheitsinfrastrukturen an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Sein Forschungsschwerpunkt liegt im Bereich der offensiven IT-Sicherheit und der digitalen Forensik.

Einleitung

Gerade mal ein Jahrzehnt ist es her, dass sich in einzelnen Büros von Systemadministratoren und Strafverfolgungsbehörden intensiver mit der Auswertbarkeit digitaler Daten für Verfahrenszwecke beschäftigt wurde. Das bis dato wenig erforschte Feld der Computer-Forensik erregte zunehmendes Interesse, wurden schließlich immer mehr Daten auf Computersystemen vorgehalten. Zwar beschäftigten sich bereits in den 80er Jahren schon die ersten Pioniere mit der Frage, wohin welche Software welche Daten schreibt und wie gelöschte Daten wiederhergestellt werden können, doch wurde ihren ersten Erkenntnissen noch wenig Beachtung geschenkt. Erst mit der nahezu flächendeckenden Verbreitung von IT-Systemen in Privathaushalten, Unternehmen, Behörden und bei Betreibern kritischer Infrastrukturen wurde der hohe Stellenwert von qualifizierten, digitalforensischen Untersuchungen erkannt. Schließlich wurden beispielsweise Verstöße gegen Unternehmensrichtlinien und Vorfälle gegen den Schutz geistigen Eigentums mehr und mehr mit Hilfe von Computern begangen. Auch Straftäter begannen, sich die digitalen Medien zunutze zu machen. Sie verlagerten herkömmliche Straftaten wie beispielsweise Betrug und Erpressung zunehmend in das Internet und kreierten sogar völlig neue Deliktsfelder, die IT-Systeme nicht nur als Tatmittel, sondern auch als Angriffsziel nutzten.

Seit dieser Zeit hat sich eine täglich wachsende Gemeinde von Computer-Forensikern gebildet, die sich auf Webseiten und Foren im Internet, aber auch »offline« auf Konferenzen, Trainings und Messen weltweit miteinander austauscht. Immer mehr Fachbücher nehmen sich mittlerweile der Computer-Forensik und auch der ihr entwachsenen Digitalen Forensik an. Und auch die Wissenschaft hat sich dieses Themas inzwischen angenommen und hilft einem komplexen Fachgebiet, das mit vereinzelten Bastlern seinen Ursprung nahm, durch Anwendung wissenschaftlicher Methoden zu dem Fortschritt und der Anerkennung, die es verdient. Die wenigen Vorlesungen zur Computer-Forensik, die einst optional im Rahmen des ein oder anderen Informatik-

studiums belegt werden konnten, sind heute in Umfang und Qualität zu vollwertigen Master Studiengängen gereift – in Deutschland wie auch international.

Auch die Industrie weiß inzwischen um die Wichtigkeit forensischer Untersuchungen. Zwar genießen die Verfügbarkeit von Systemen und die Vermeidung von Imageschäden höchste Priorität, dennoch nutzt man die Kenntnisse aus der Computer-Forensik, um Vorfälle zu analysieren. So lassen sich nicht nur Hinweise auf den Täter und dessen Vorgehen finden, sondern auch Sicherheitslücken schließen und Ablaufpläne für künftige Sicherheitsvorfälle standardisieren und optimieren.

Dieses Buch ist eine Sammlung von Ideen, Methoden, Tipps und Tricks (kurz: Hacks) aus allen möglichen Arbeitsschritten in der Computer-Forensik. Wir haben Ihnen praktische Lösungen für echte Problemstellungen in kleine, bekömmliche Portionen gepackt, die Sie nicht nur lesen, sondern auch direkt anwenden können. Zu jeder praktischen Lösung geben wir Ihnen aber auch das notwendige Hintergrundwissen mit auf dem Weg, das Sie benötigen, um sowohl das Problem wie auch den Lösungsansatz nachvollziehen zu können. Das Konzept dieses Buches lässt es nicht zu, Ihnen zu jedem Thema eine voll umfassende Erklärung mitzuliefern. Da Sie aber bei dem Griff zu diesem Buch sicherlich kein hoch-wissenschaftliches, mehrbändiges Standardwerk zur Computer-Forensik gesucht haben, versorgen wir Sie stattdessen mit dem, was Sie auch wirklich wollten: 100 spannende und interessante Hacks rund um das Thema Computer-Forensik.

Wie dieses Buch verwendet werden soll

Sie können, wenn Sie möchten, dieses Buch von Anfang bis Ende durchlesen. Da aber jeder Hack eine selbständige Einheit bildet, können Sie sich auch einfach anhand des Inhaltsverzeichnisses ein Thema Ihrer Wahl heraussuchen und direkt dort einsteigen. Oder nutzen Sie dieses Buch doch als Nachschlagewerk. So machen wir es übrigens auch! Viele Ideen und Problemlösungen aus unserer Praxis haben ihren Weg in dieses Buch gefunden – da auch unser Gedächtnis Grenzen hat, nutzen wir die einzelnen Hacks als Gedächtnisstütze.

Wann auch immer Sie beim Durchstöbern der Hacks Vorkenntnisse aus einem anderen Hack benötigen, weisen wir Sie in dem Text darauf hin. Bei manchen Tipps werden Sie auch Verweise zu Anleitungen oder Hintergrundinformationen im Internet finden.

Die Hacks in diesem Buch benutzen grundsätzlich kostenlose Software, also Open-Source- oder Freeware Software. Bei wenigen Lösungen verweisen wir aber auch auf Software, die für die Privatnutzung kostenlos, für gewerbliche oder behördliche Nutzung jedoch kostenpflichtig ist. Die von uns beschriebe-

nen Programme laufen durchgängig auf den Betriebssystemen Microsoft Windows oder Linux. Sie sollten daher über Systeme beider Art verfügen (z.B: auch als virtuelle Maschine). Sollten Sie noch nicht firm in einem der beiden Betriebssysteme sein, bitten wir Sie, sich vorher entsprechend zu informieren. Das Internet hält eine Menge toller Anleitungen und nachvollziehbarer Tutorials mit Tipps zur Installation und Ersteinstieg z.B. in Linux (wir empfehlen für den Einstieg Ubuntu oder Fedora) für Sie bereit.

In den Fällen, in denen eine Software einmal nicht oder nur unter bestimmten Umständen kostenlos ist, müssen Sie selbst prüfen, unter welchen Einsatzzweck Ihre Verwendung des Programmes fällt. Wir weisen Sie auf etwaige Kosten eines Produkts oder auf Lizenzeinschränkungen hin, können jedoch nicht dafür garantieren, dass zu dem Zeitpunkt, zu dem Sie unser Buch lesen, die Software immer noch kostenlos, frei nutzbar oder zu einem bestimmten Preis zu erhalten ist. In jedem Fall müssen Sie die Lizenzbestimmungen des Herstellers beachten.

Wie dieses Buch aufgebaut ist

Sehen Sie dieses Buch wie ein Kochbuch. Es enthält 100 köstliche Gerichte, die Sie unabhängig voneinander kochen können. Wie in einem Kochbuch finden Sie auch in diesem Buch unterschiedliche Gänge, also mehrere Vorspeisen, eine ganze Palette an Hauptgerichten und auch einige süße Nachspeisen. Erkennen Sie die Chronologie in der Speisefolge? Genauso chronologisch gehen wir in diesem Buch auch die einzelnen Arbeitsschritte der Computer-Forensik durch. Es beginnt mit Tipps & Tricks zur Vorbereitung und Datensicherung, gefolgt von einigen Hacks zu Dateisystemen. Der Hauptteil dreht sich um Datenwiederherstellung und das Analysieren der unterschiedlichsten digitalen Spuren, bevor einige Schmankerl zu den Themen Hacking und Virtualisierung als Nachtisch auf Sie warten. Insgesamt warten acht Kapitel darauf, von Ihnen entdeckt zu werden:

Kapitel 1, *Datensicherung*
: Am Anfang jeder forensischen Auswertung steht im Normalfall die Sicherung von Daten. In diesem Kapitel finden Sie Tipps und Tricks, wie Sie sich am besten auf Datensicherungen vorbereiten können und wie Sie sie auf unterschiedliche Arten unter verschiedenen Umständen sichern können. Da in der Forensik der Aspekt der Gerichtsverwertbarkeit eine große Rolle spielt, gehen wir auch auf Cross-Kontaminierung, unterschiedliche Abbildformate und deren Verifizierung ein.

Kapitel 2, *Dateisysteme*
: Bevor Sie Spuren auf einem Datenträger suchen, sollten Sie wissen, auf welcher Grundlage all die beweisrelevanten Daten entstanden sind. Als Forensiker ist es daher unumgänglich, sich mit Dateisystemen und deren

Aufbau zu beschäftigen. Zwar ist dieses Kapitel das wohl abstrakteste, doch ist es bei weitem keine theoretische Abhandlung aller möglichen Bytes in einem Dateisystem. Stattdessen liegen für Sie einige wesentliche Elemente der gängigsten Dateisysteme in kurzen Hacks zum Ausprobieren bereit.

Kapitel 3, *Analyse und Wiederherstellung von Daten*

Nachdem Sie Daten gesichert und deren Ablage auf dem Dateisystem einer Partition verstanden haben, beschreiten Sie den Hauptteil dieses Buches – die Analyse und Wiederherstellung von Daten. Von Techniken zum Hash-Abgleich, Signaturanalysen über Carving, Mounten und Block-Hashing bis hin zu Schlüsselwortsuchen mit Regulären Ausdrücken und intensiver Logdatei-Auswertung: Hier finden Sie alles, was das Forensiker-Herz begehrt.

Kapitel 4, *Digitale Spuren in Windows*

Etwas intensiviert wird die Spurensuche und –auswertung in den Kapiteln vier bis sechs. Hier gehen wir auf betriebssystem- und applikationsspezifische Artefakt ein. Entdecken Sie in Kapitel vier beispielsweise, welche Dokumente und Programme ein Benutzer zuletzt oder am häufigsten ausgeführt hat, sehen Sie, was gedruckt wurde, welche Bilder betrachtet wurden und welche Dateien gelöscht wurden.

Kapitel 5, *Digitale Spuren in Linux*

Durch die zunehmende Verbreitung von Linux, insbesondere im Server-Bereich, werden Sie sich früher oder später auch mit diesem Betriebssystem auseinander setzen müssen. Vielleicht haben Sie ja ohnehin schon ein Faible für das OS mit dem Pinguin? Umso besser, denn in diesem Kapitel werden Sie Linux aus forensischer Sicht betrachten. Das fängt an bei einem ersten, schnellen Überblick, welches Linux-Derivat Ihnen überhaupt vorliegt, welche Partitionen und welche Software auf dem System eingerichtet sind und geht weiter mit einer Analyse von Netzwerkdiensten und deren Konfiguration. Schließlich werden Sie sich auf die Spuren der User machen, indem Sie deren Konfiguration und Historie analysieren.

Kapitel 6, *Internetartefakte*

Das sechste Kapitel nimmt Sie mit in die spannende Welt der Internetartefakte. Da sich heutzutage fast jeder Bürger im Netz bewegt und wie eingangs dargestellt das Internet auch immer häufiger zur Begehung von Verstößen und Straftaten missbraucht wird, sind Internetartefakte oft von hoher Bedeutung für Verfahren. In diesem Kapitel zeigen wir Ihnen nicht nur, wie Sie einzelne Applikationen auswerten können, Sie lernen beiläufig auch noch eine Methodik, mit der Sie nahezu jede beliebige Anwendung untersuchen können, die auf SQLite-Datenbanken basiert.

Kapitel 7, *Hacking & Co.*

Die Überschrift dieses Kapitels täuscht vielleicht ein wenig: Sie werden hier keine Tipps und Tricks zum Cracken von Systemen erhalten. Schon gar nicht werden Sie »zum Hacker ausgebildet«. Sie werden jedoch bestimmte Angriffsvektoren kennenlernen und Beispiele dafür, wie Sie Hinweise auf Sicherheitsvorfälle ausmachen und vielleicht sogar noch Spuren des Angreifers auffinden können.

Kapitel 8, *Virtualisierung*

Eine Technik, die seit wenigen Jahren immer häufiger in der Forensik verwendet wird, ist das Virtualisieren. Streng genommen sollten Sie in der Lage sein, alle Spuren, die Sie in einer virtualisierten Umgebung finden, auch in dem toten Datenträgerimage aufzuspüren. Doch kann das simulierte Inbetriebnehmen eines Rechners viele Artefakte schneller und von der Darstellung her anschaulicher darstellen als dies beispielsweise bei einem Einstellungswert in der Windows Registry oder einem Wert in einer Konfigurationsdatenbank der Fall ist. In Kapitel acht erfahren Sie, wie Sie Datenträgerimages zum Virtualisieren mounten, sie mit Hilfe von qemu schnell und performant in Betrieb nehmen können und Treiberprobleme lösen können. Weiterhin bekommen Sie Tricks an die Hand, wie Sie im Fall, dass Sie das Passwort für Ihre virtuelle Maschine vergessen haben, dieses unkompliziert wiederherstellen können und so auch die Stärke Ihrer eigenen Passworte überprüfen können.

Besuchen Sie uns auf der Webseite zum Buch

Wir haben alle Lösungen mehrfach selbst getestet, bevor wir sie für Sie niedergeschrieben haben. Daher sind wir sehr zuversichtlich, dass Sie Ihren Spaß und auch Erfolg mit den Hacks haben werden. Sollten Sie dennoch einmal nicht weiterkommen nehmen Sie doch einfach Kontakt zu uns auf. Am besten geht das über die Webseite zu diesem Buch:

http://www.forensikhacks.de

Über diese Seite erreichen Sie auch sämtliche Links aus diesem Buch, damit Sie nicht mühsam ellenlange URLs abtippen müssen.

Nutzen Sie doch einen Besuch auf unserer Seite auch, um uns Ihre Anregungen, Ideen und Verbesserungsvorschläge mitzuteilen, damit wir die Computer-Forensik Hacks erweitern und optimieren können. Vielleicht haben Sie auch die ein oder andere Idee für weitere Hacks oder aber Ihnen hat ein Hack aus dem Buch geholfen, eine Untersuchung erfolgreich abzuschließen? Wir freuen uns auf Ihr Feedback und Ihre Ideen!

Typografische Konventionen

In diesem Buch werden die folgenden typografischen Konventionen verwendet:

Kursivschrift
: Kennzeichnet URLs, Dateinamen, Dateinamen-Erweiterungen und Verzeichnis-/Ordnernamen. Ein Pfad im Dateisystem wird zum Beispiel als */Entwicklung/Anwendungen* erscheinen.

`Nichtproportionalschrift`
: Wird verwendet, um Code-Beispiele, den Inhalt von Dateien, Konsolenausgaben sowie Namen von Variablen, Befehlen und andere Code-Ausschnitte anzuzeigen. In Code-Beispielen verwenden wir manchmal das Symbol »\« am Ende einer Zeile. Dies soll symbolisieren, dass die Zeile eigentlich fortlaufend ist. Sie können beim Abtippen des Codes also das »\« ignorieren.

`Nichtproportionalschrift fett`
: Wird zur Hervorhebung von Code-Abschnitten verwendet, bei denen es sich normalerweise um neue Ergänzungen zu altem Code handelt.

Sie sollten besonders auf Anmerkungen achten, die mit den folgenden Symbolen vom Text abgehoben werden:

Das ist ein Tipp, ein Hinweis oder eine allgemeine Anmerkung. Er enthält nützliche ergänzende Informationen zum nebenstehenden Thema.

Das ist eine Warnung oder Ermahnung zur Vorsicht, die oftmals anzeigt, dass Ihr Geld oder Ihre Privatsphäre in Gefahr ist.

Die Thermometer-Symbole, die neben jedem Hack stehen, geben die jeweilige Komplexität des Hacks an

 leicht  mittel  schwer

Verwendung von Code-Beispielen

Dieses Buch soll Ihnen dabei helfen, Ihren Job zu erledigen. Im Allgemeinen können Sie den Code aus diesem Buch in Ihren Programmen oder in Ihrer Dokumentation einsetzen. Sie müssen uns nicht kontaktieren und um Erlaubnis fragen, es sei denn, Sie kopieren einen erheblichen Teil des Codes. Das Schreiben eines Programms zum Beispiel, das mehrere Codeteile aus diesem Buch verwendet, bedarf keiner Genehmigung. Der Vertrieb oder das Verteilen

einer CD-ROM mit Beispielen aus O'Reilly-Büchern bedarf *allerdings* einer Genehmigung. Wenn in einer Antwort auf eine Frage dieses Buch zitiert und Beispielcode daraus angeführt wird, bedarf dies keiner Genehmigung. Das Einbinden einer erheblichen Menge an Beispielcode aus diesem Buch in die Dokumentation Ihres Produkts bedarf *allerdings* der Genehmigung.

Wir freuen uns über einen Nachweis, verlangen aber keinen. Ein Nachweis enthält normalerweise Titel, Autor, Verlag und ISBN. Zum Beispiel: »*Computer-Forensik Hacks* von Lorenz Kuhlee und Victor Völzow. O'Reilly Verlag 2012, ISBN 978-3-86899-121-5.«

Wenn Sie vermuten, dass Ihr Gebrauch von Code-Beispielen außerhalb des fairen Gebrauchs oder der hier erteilten Genehmigungen liegt, wenden Sie sich bitte unter *permissions@oreilly.com* an uns.

Datensicherung

Hacks #1-14

Die Sicherung von digitalen Spuren ist der erste und gleichzeitig kritischste Schritt bei der Durchführung einer digitalforensischen Untersuchung. Erfahrungsgemäß ist die Datensicherung derjenige Prozess, bei dem die meisten unumkehrbaren Fehler begangen werden können. So könnten zum Beispiel unbeabsichtigte Schreibzugriffe auf dem zu analysierenden Datenträger erfolgen. Dadurch wäre am Ende erheblicher Schaden auf dem Speichermedium verursacht, da eventuell zu rettende Daten im schlechtesten Fall unwiederbringlich gelöscht wären. Abgesehen davon ist im Hinblick auf den klassischen forensischen Prozess jegliche Integrität der Daten zu bewahren, um Vorwürfen der Manipulation von Beweismitteln vorzubeugen.

Eine professionelle, gerichtsverwertbare Datensicherung kann bei der Frage nach der Zulässigkeit eines Beweismittels vor Gericht von entscheidender Bedeutung sein. Darüber hinaus bestärkt eine fachmännisch durchgeführte Sicherung die Glaubwürdigkeit des sachverständigen Forensikers vor Gericht.

Noch kritischer zu sehen ist die Sicherung von flüchtigen Daten wie dem Inhalt des Arbeitsspeichers (RAM, random access memory). Fehler in diesem Stadium werden erbarmungslos bestraft. Diese Bits und Bytes leisten für die spätere Auswertung einen wertvollen Beitrag; so können sie beispielsweise Passwörter beinhalten, die nirgends sonst auf herkömmlichen Datenträgern gespeichert sind.

Dieses Kapitel zeigt dem Einsteiger in hilfreichen Hacks, wie er forensische Abbilder seiner geliebten und wichtigen Daten erzeugt. Dem professionell orientierten Leser sind die Hacks eine wunderbare Erweiterung seiner Werkzeugkiste.

Die Hacks in diesem Kapitel sind in folgende vier Kategorien unterteilt: Sicherung flüchtiger Daten, Sicherung von Speichermedien, Praxiseinsatz von Boot-DVDs und Sichern über Netzwerke.

Vorbereitung

- Woran Sie denken sollten [Hack #1]
- So säubern Sie Ihre Backup-Datenträger [Hack #2]

Live-Sicherung flüchtiger Daten

- Bevor es zu spät ist – RAM sichern [Hack #3]
- RAM sichern trotz Passwortsicherung [Hack #4]
- Wenn nichts mehr hilft: Cold Boot [Hack #5]
- Weitere flüchtige Daten richtig sichern [Hack #6]
- Automatisieren Sie Live-Sicherungen mit Skripten [Hack #7]

Sicherung von Speichermedien

- So sichern Sie Daten auf der Kommandozeile [Hack #8]
- Wenn Sie doch eine GUI bevorzugen [Hack #9]
- Vertrauen ist gut, Kontrolle ist besser [Hack #10]

Tipps und Tricks zur Datensicherung

- Boot DVDs für die Datensicherung [Hack #11]
- Aus der Ferne sichern [Hack #12]
- Aus der Ferne sicher sichern [Hack #13]
- Wenn Ihnen das Format nicht passt [Hack #14]

HACK #1 Woran Sie denken sollten

»Vorbereitung ist die halbe Miete«

Bei der Sicherung digitaler Daten sind im Vorfeld verschiedene Vorüberlegungen anzustellen. Das fängt bei ganz trivialen Dingen an. Wie wollen Sie zum Beispiel ohne Schraubendreher an die Festplatte eines Computers gelangen?

Dieser Hack beschäftigt sich mit den vorbereitenden Maßnahmen vor dem Datensicherungsprozess und nimmt auch Rücksicht auf die besonderen Herausforderungen bei einer Datensicherung außerhalb Ihrer gewohnten Büro-/Laborumgebung. Naturgemäß können wir nicht alle Eventualitäten abdecken, da jede Untersuchung verschiedenen Gegebenheiten unterliegt. Aus diesem Grund listen wir im Folgenden eine große Anzahl an möglichen Utensilien auf, selbst für ungewöhnliche Situationen. Dem Leser sei überlassen, eine individuelle Auswahl zu treffen.

Folgende Utensilien schlagen wir Ihnen vor

Eine *Kamera,* um die Umgebung und den Zustand des zu untersuchenden Computers zu dokumentieren. Das ist wichtig, um den Ursprungszustand des Geräts und seiner Umgebung festzuhalten. Ein Bild sagt mehr als tausend Worte! Eventuell kann die spätere Auswertung es erfordern, sich an Detailinformationen zu erinnern. Ein Bild oder ein Film von einer Videokamera hilft Ihrem Gedächtnis auf die Sprünge. Auf diese Weise sind selbst noch so verwirrende Kabelverbindungen in der Rekonstruktion ein Kinderspiel.

Verpackungsmaterialien. Üblicherweise sind elektronische Komponenten sehr empfindlich. Um sie vor jeglicher Art von äußeren Einflüssen zu schützen, ist es wichtig, entsprechendes Verpackungsmaterial vorzuhalten. Festplatten, Computer und Peripheriegeräte sind insbesondere vor Hitze durch Sonneneinstrahlung, Nässe durch Regen, Schmutz und Staub sowie transportbedingten Erschütterungen zu schützen. Bei offenliegenden Platinen und Chips ist eine antistatische Verpackung unabdingbar.

Handschuhe. Sie glauben gar nicht, was sich so alles in einem Computergehäuse ansammeln kann. Insbesondere die Kombination von Staub und Zigarettenrauch kann eine schmierige Angelegenheit sein. Davon abgesehen kann es je nach Auftrag notwendig sein, spurenschonend vorzugehen.

Taschenlampe. Ohne das zusätzliche Licht einer Taschenlampe ist es verzwickt, sich in einem dunklen Computergehäuse zurechtzufinden. Besonders kleine Jumper, Steckverbindungen und Seriennummern sind mit einer Taschenlampe viel leichter zu erkennen. Aber vergessen Sie die Ersatzbatterien nicht!

Aufkleber und Umhängeschilder sind nützlich, um Geräte und Kabelverbindungen zu kennzeichnen. Sie können damit Nummern vergeben, um diese Komponenten eindeutig identifizieren und zuordnen zu können.

Messer, Schere und Zange helfen Ihnen dabei, Aufkleber auf die richtige Größe zuzuschneiden und Kabelbinder zu lösen.

Ein *Schraubendreherset* inklusive einer reichhaltigen Auswahl an unterschiedlichen Bits ist ein Muss. Ob zum Öffnen eines PC- oder Notebook-Gehäuses, zur Entnahme einer Festplatte oder zum Öffnen einer externen Festplatte: Schraubendreher werden Sie immer brauchen.

Ihr *Notebook* sollten Sie ebenfalls bei jedem Datensicherungsauftrag bei sich haben. Die Datensicherungssoftware, die Sie in einer ruhigen Stunde auf ihrem Notebook installiert haben, kann in zeitkritischen oder problematischen Momenten Gold wert sein.

Der *Schreibschutzadapter*, auch gern als »Gummihandschuhe des Forensiker« bezeichnet, muss immer dann zum Einsatz kommen, wenn Sie forensische

Datensicherungen erstellen wollen. Er gewährleistet, dass keine Schreibzugriffe auf das zu sichernde Medium stattfinden.

Verschiedene *Anschlüsse* für SATA-, SAS-, IDE- und auch SCSI-Festplatten sollten Sie deshalb vorrätig halten, da all diese Anschlussarten noch immer zum Einsatz kommen und Sie vorher nie wissen, welche Art von Festplatte in einem Computer verbaut ist.

Boot-DVDs und Software-Tools – siehe **[Hack #11]**.

Speichermedien intern sowie extern mit Schnittstellen wie eSATA, USB, Firewire und auch LAN sind die Arbeitsgrundlage für jede Datensicherung. Irgendwo müssen die zu sichernden Daten ja hingeschrieben werden. Im Zweifel gilt: Lieber zu viel Speicher vorhalten als zu wenig.

Formulare kommen dann ins Spiel, wenn Sie Abläufe und Vorgehensweisen dokumentieren müssen. Im Regelfall spielen solche Dinge immer dann eine Rolle, wenn Sie es mit Verfahren zu tun haben, die eine betriebliche oder gerichtliche Relevanz besitzen.

Kabel, zum Beispiel Netzwerkkabel oder Cross-over-Kabel, brauchen Sie immer dann, wenn Sie selbst in einem Netzwerk tätig werden wollen. Über ein Cross-over-Kabel können Sie beispielsweise die Sicherung eines kompletten Datenträgers über das Netzwerk auf Ihren Computer durchführen.

Ein *Erdungs-/Anti-Statik-Armband* bewahrt Sie davor, Ihr eigenes oder fremdes technisches Gerät beim Ein- und Ausbau durch sich entladende elektrostatische Aufladungen zu beschädigen oder gar zu zerstören. Würden Sie einem Kunden oder etwa einem Richter gern erklären, warum ein zuvor völlig intakter Rechner nach Ihrer »Behandlung« plötzlich keinen Mucks mehr von sich gibt?

Mit einer *Funkuhr* können Sie sekundengenau dokumentieren, wann Sie welche Maßnahmen durchgeführt haben. In dem Fall, dass Sie ein laufendes System sichern möchten (mehr dazu in den **[Hacks #3–#7]**), können Sie anhand einer Funkuhr die Abweichung der Systemzeit zur Echtzeit feststellen.

Stift und Papier – so banal es klingen mag, aber Sie werden Stift und Papier immer brauchen. Sei es, um Seriennummern zu notieren, ihre Maßnahmen zu dokumentieren, eine Netzplanskizze aufzuzeichnen, oder was es sonst noch alles so gibt ...

Umzugskartons sind immer dann vonnöten, wenn Sie eine Datensicherung außerhalb Ihres Büros/Labors durchführen müssen. Sie wissen nie, wie viele Geräte Sie später eventuell zu Ihrem Büro/Labor transportieren müssen.

Ein *WLAN-Sniffer/-Scanner* kann Ihnen dabei helfen, kabellose Netzwerkspeicher aufzuspüren. Das kann in Szenarien von Bedeutung sein, in denen Sie eine Datensicherung außerhalb Ihres Büros durchführen müssen.

Klären Sie vor jedem Einsatz dieser Technik ab, ob er in diesem speziellen Fall rechtlich zulässig und gewünscht ist.

Last, but not least – der universelle *DVD-Fach-Öffner*: eine Büroklammer!

Als kleine Hilfestellung für die Praxis haben wir Ihnen die folgende Checkliste zusammengestellt.

Tabelle 1-1: Checkliste: Vorbereitung

Daran sollten Sie denken	Check
Kamera (inkl. Ersatzbatterien und Speicherkarten)	☐
Verpackungsmaterialien (Plastiktüten, Anti-Statik-Tüten)	☐
Handschuhe	☐
Taschenlampe (inkl. Ersatzbatterien)	☐
Aufkleber und Umhänger	☐
Messer, Schere und Zange	☐
Schraubendreherset (inkl. umfangreicher Bit-Satz)	☐
Laptop	☐
Hardware-Schreibschutz	☐
Adapterstecker (IDE, SATA, SAS, SCSI, ZIF)	☐
Boot-DVDs (inkl. Softwaretools)	☐
Speichermedien (USB, eSATA, LAN)	☐
Formulare	☐
Kabel (insb. Netzwerkkabel, Cross-over-Kabel)	☐
Erdungs-/Anti-Statik-Armband	☐
Funkuhr	☐
Stift & Papier	☐
Umzugskartons	☐
Klebeband	☐
WLAN-Sniffer/-Scanner	☐
Büroklammer (»der universelle DVD-Fach-Öffner«)	☐

HACK #2

So säubern Sie Ihre Backup-Datenträger

»Ein jeder kehre vor seiner eigenen Tür.«

Ganz egal, aus welchem Grund Sie Daten sichern möchten, eines werden Sie immer brauchen: Speicherplatz. Bei stetig steigenden Speicherkapazitäten und fallenden Hardwarepreisen bieten sich heutzutage vornehmlich Festplatten an, egal ob als einzelne externe Geräte oder im geschwindigkeitsoptimier-

ten Raid-Verbund. Sie sollten bei jeder Art der Datensicherung immer darauf achten, auf einen anderen Datenträger als den ursprünglichen zu sichern. Ansonsten wäre die »Sicherung« im Falle eines Hardwaredefekts oder Verlust des Originals gleich mit verloren. Auch das Wiederherstellen von gelöschten Dateien und Verzeichnissen auf ein- und denselben Datenträger wäre fatal. Abgesehen davon, dass diese Verfahrensweise gegen den wichtigsten Grundsatz der digitalen Forensik verstößt – nämlich kein Beweismittel zu verändern –, birgt sie gleichzeitig die Gefahr, Daten unwiederbringlich zu überschreiben, die eigentlich wiederhergestellt werden sollten. Sie sehen: An einem zusätzlichen Datenträger für die zu sichernden Daten führt kein Weg vorbei.

Wenn Sie forensisch korrekt arbeiten müssen oder möchten, sollten Sie sicherstellen und belegen können, dass Sie Maßnahmen ergriffen haben, um Cross-Kontamination zu vermeiden. Oder würden Sie sich gern in der Lage sehen, vor Gericht begründen zu müssen, warum sich in Slack-Bereichen von gesicherten oder exportierten Dateien des Vorgangs B noch alte Informationen aus Vorgang A befinden? Mindestens genauso ungünstig wäre es, wenn Sie Daten nur sichern, um sie an eine externe Abteilung oder ein anderes Unternehmen weiterzuleiten, und sich sensible Informationen von Ihnen oder Ihrem Unternehmen in gelöschten Bereichen des übergebenen Datenträgers finden.

Um solche Vorfälle zu vermeiden, ist es wichtig, alle Informationen auf dem Backup-Datenträger vollständig zu löschen, bevor er mit neuen Daten befüllt wird. In der Forensik ist mit »echtem« Löschen das mehrfache Überschreiben der Daten, das sogenannte »Wipen«, gemeint. Nur das Wipen garantiert, dass keine Dateien und Datenfragmente von dem Datenträger wiederhergestellt werden können. Weder Neupartitionieren noch Formatieren o. Ä. stellen einen wirksamen Schutz vor Cross-Kontamination dar.

Unter Windows gibt es viele Programme, die ganze Datenträger wipen können, darunter auch einige kostenlose:

- Disk Wipe: *http://www.forensikhacks.de/diskwipe*
- MiniTool Drive Wipe: *http://www.forensikhacks.de/drivewipe*
- Wipe Disk: *http://www.forensikhacks.de/wipedisk*

Diesen Tools gemein ist, dass sie sehr leicht und intuitiv zu bedienen sind. Sie bieten meist die Option, ganze Laufwerke oder nur einzelne Partitionen zu überschreiben. Zusätzlich bieten die meisten Programme auch noch mehrere unterschiedliche Löschmethoden an. Das reicht vom einfachen Überschreiben ausschließlich mit Nullen bis hin zum mehrfachen Überschreiben mit Zufallswerten.

Aber auch die kommerziellen Forensik-Suiten wie *EnCase*, *FTK* und *X-Ways* sind mit Funktionalitäten zum Wipen ausgestattet. Die Software *EnCase* bei-

spielsweise bietet selbst im Acquisition-Modus, der keinen Lizenz-Dongle benötigt, im Menü unter *Tools* die Funktion *Drive Wipe*.

Wenn Sie lieber mit Linux arbeiten, können Sie mit einfachen Befehlen auf der Kommandozeile einen Datenträger überschreiben:

```
dd if=/dev/zero of=/dev/sdX
```

überschreibt den Datenträger *sdX* einfach mit Nullen, und

```
dd if=/dev/urandom of=/dev/sdX
```

überschreibt den Datenträger *sdX* einfach mit Zufallswerten.

Möchten Sie hingegen nur eine bestimmte Partition überschreiben, können Sie folgende Befehle nutzen:

```
dd if=/dev/zero of=/dev/sdX1
```

oder

```
dd if=/dev/urandom of=/dev/sdX2
```

HACK #3 Bevor es zu spät ist – RAM sichern

»Was man hat, das hat man.«

Sie haben sich schon immer gefragt, wie Sie Daten retten können, die sich gar nicht auf der Festplatte Ihres Computers befinden? Vielleicht möchten Sie auch gern Schadsoftware untersuchen, die sich in Bereichen außerhalb Ihrer Festplatte versteckt? Dann sind Sie hier goldrichtig, denn im Folgenden zeigen wir Ihnen, wie Sie Ihren Random Access Memory (RAM), landläufig auch »Arbeitsspeicher« genannt, sichern können.

Die Bezeichnung Arbeitsspeicher ist übrigens sehr treffend, denn mit den Daten, die sich an diesem Speicherort befinden, wird in der Regel ständig gearbeitet. Sie werden geschrieben, gelesen, bewegt und überschrieben, und sie sind diejenigen Daten, die am empfänglichsten für Veränderungen sind. Egal, welche Daten bei der Nutzung des PCs im Arbeitsspeicher entstanden sind – sobald Sie Ihren Computer ausschalten, vergisst der RAM innerhalb weniger Sekunden bis Minuten seine Inhalte. Doch dazu mehr im [Hack #5], der Ihnen zeigt, wie Sie Inhalte des Arbeitsspeichers selbst nach dem Ausschalten des PCs sichern können.

Daten im Arbeitsspeicher unterliegen also nicht nur einer starken Fluktuation, sondern auch einer hohen Flüchtigkeit – man spricht hier auch von *Volatilität*. Das Besondere an den Daten im Arbeitsspeicher ist, dass sie sogar solche Daten beinhalten, die der Nutzer vielleicht nie auf seinem PC abspeichern wollte und denen er daher nie einen Speicherplatz auf der Festplatte zugewiesen hat. Wenn Sie beispielsweise gerade eine E-Mail, eine Chatnach-

richt oder ein Textdokument verfassen, ist die Wahrscheinlichkeit sehr hoch, Fragmente des Texts im Arbeitsspeicher Ihres Computers zu finden, obwohl Sie sie nie als Datei gespeichert haben.

Die genannten Eigenschaften des Arbeitsspeichers machen ihn für die Forensik natürlich besonders interessant, stellen den Forensiker jedoch vor neue Herausforderungen. So interessant die Daten im Arbeitsspeicher auch sein mögen: Die Gefahr, sie zu verlieren oder unbeabsichtigt zu überschreiben, ist erheblich höher als bei herkömmlichen Datenträgern. Das sollten Sie nicht nur bei Wahl des richtigen Sicherungstools, sondern auch beim Sicherungsvorgang selbst beachten.

Unter Windows haben sich folgende Softwarelösungen zur Sicherung des Arbeitsspeichers etabliert:

- *Win32dd.exe* und *Win64dd.exe*, enthalten im *MoonSols Windows Memory Toolkit*; die Community Edition ist kostenfrei zu haben, siehe *http://www.forensikhacks.de/win32dd*.
- *Winen.exe* und *Winen64.exe*, enthalten in der kommerziellen Forensik-Software *EnCase* ab Version 6.11; kommerziell, siehe *http://www.forensikhacks.de/winen*.
- *Mdd.exe*, auch ManTech Memory DD genannt, von der ManTech International Corporation; Open Source-Software, siehe *http://www.forensikhacks.de/mdd*.
- *FTK Imager*, Freeware, siehe *http://www.forensikhacks.de/ftki*.

Bevor Sie eines dieser Tools anwenden, denken Sie daran, dass Sie durch Ihre Aktionen einen Teil des Arbeitsspeichers überschreiben werden. Deshalb wollen Sie den »Schaden« vermutlich so gering wie möglich halten. Die Tools *Win32/64dd.exe* und *Winen/64.exe* haben in unseren Tests die geringsten Auswirkungen auf RAM-Inhalte aufgewiesen, daher werden wir Ihnen das Vorgehen mit diesen Programmen näher beschreiben.

Mit *Win32dd.exe* oder *Win64dd.exe* (für 64-Bit Systeme) sichern Sie den Arbeitsspeicher durch Aufruf von

```
win32dd.exe /r /f ram.dd
```

Möchten Sie statt eines Raw-Image eine Sicherung des RAM im Crashdump-Format auf eine Netzwerkressource, dann führt Sie der folgende Befehl zum Ziel:

```
win32dd.de /d /f \\server\ram.dmp
```

Wenn Sie nicht genau wissen, ob Sie auf einem 32- oder 64-Bit-Betriebssystem den RAM sichern, sollten Sie einen Blick auf das freie Zusatzprogramm *DumpIt* werfen. Es vereint *win32dd.exe* und *win64dd.exe* in einer einzigen Datei und

> findet selbstständig heraus, ob es auf einer 32- oder 64-Bit-Plattform läuft. Sie erhalten *DumpIt* unter *http://www.forensikhacks.de/dumpit*.

Die Benutzung von *winen.exe* und *winen64.exe* ist ähnlich simpel. Starten Sie auf der Kommandozeile das Programm ohne Parameter, erscheinen einige Abfragen, in denen Sie Informationen zum Image eingeben können. Wenn Sie allerdings öfter RAM sichern, möchten Sie sich die ständige Neueingabe aller Informationen vielleicht ersparen. Dafür bietet Winen die Möglichkeit, auf zuvor angelegte Konfigurationsdateien zurückzugreifen:

```
winen.exe –f meine.config
```

Zu guter Letzt ist auch mit *mdd.exe* ein Abbild Ihres Arbeitsspeichers schnell und einfach erstellt. Führen Sie den folgenden Befehl aus:

```
mdd_1.3.exe –o ram.dd
```

Natürlich können Sie auch unter Linux und MAC den RAM sichern. Unter Linux war es bei älteren Kernels möglich, direkt auf das RAM-Device zuzugreifen und mit folgendem Befehl eine Sicherung zu erstellen:

```
dd if=/dev/mem of=ram.dd
```

Die neueren Kernels verbieten aus Sicherheitsgründen diesen direkten Zugriff. Eine Umgehung dieses Problems ist mit *fmem* (*http://www.forensikhacks.de/fmem*) möglich.

Für MAC gibt es den *Mac Memory Reader* (*http://www.forensikhacks.de/macmem*) als Lösung. Diesen können Sie wie folgt aufrufen:

```
sudo ./MacMemoryReader /Volumes/STORAGE/ram.mach-o
```

HACK #4

RAM sichern trotz Passwortsicherung

»Dich kriegen wir schon noch.«

Spätestens seit dem vorherigen Hack wissen Sie um die Wichtigkeit der Sicherung flüchtiger Daten, insbesondere des Arbeitsspeichers eines Computers. Sie wissen ebenso, welche Schritte zu unternehmen sind, um den RAM zu sichern. Doch was, wenn Sie den Arbeitsspeicher eines PCs sichern möchten, dessen Bildschirm gesperrt und mit einem Passwort geschützt ist?

Sicher, die einfachste Methode in einem solchen Fall ist, den Besitzer des Rechners nach dem Passwort zu fragen. Doch vielleicht ist dieser nicht verfügbar oder es handelt sich um einen entlassenen Mitarbeiter, dessen Kooperationswille stark zu wünschen übrig lässt. In diesem Fall geben wir Ihnen in diesem Hack das Werkzeug an die Hand, um in vielen Fällen den Arbeitsspeicher auch ohne Kenntnis des Passworts sichern zu können.

Das Zauberwort heißt »Firewire-Attacke«, und so eine Attacke ist gar nicht mal so kompliziert. Diese Technik macht sich ein Feature des Bussystems Firewire (auch i-Link oder IEEE 1394) zunutze. Um die Geschwindigkeit bei der Datenübertragung zu erhöhen, bedient sich Firewire der Technologie *Direct Memory Access (DMA)*. Daten werden über den DMA-Controller direkt in den Arbeitsspeicher geladen, ohne den Umweg über das Betriebssystem und die dort installierten Zugriffskontrollen zu gehen.

Voraussetzungen

Voraussetzung für diese Art der RAM-Sicherung ist, dass der betroffene Computer eine Firewire-Schnittstelle besitzt. Natürlich sollte auch Ihr PC über eine ebensolche verfügen. Sollten diese Schnittstellen nicht vorhanden sein, lassen sie sich optional z. B. über eine PCMCIA-Karte nachrüsten. Die Treiber für die nachgerüstete Firewire-Karte installieren sich auch dann im Hintergrund, wenn der PC mit einem Passwort gesperrt ist.

An die Arbeit

Zum Auslesen des Arbeitsspeichers via Firewire existieren zwei erwähnenswerte Softwaretools: das Paket *PythonRaw1394* von Adam Boileau (*http://www.forensikhacks.de/1394*) für Linux, Windows und Mac OS X und das Paket *Goldfish* vom University College Dublin (*http://www.forensikhacks.de/goldfish*) für Mac OS X. Letzteres ist ausschließlich für Strafverfolgungsbehörden zugänglich und kann nur über das University College Dublin bezogen werden. Daher können wir Ihnen ausschließlich die erste Variante zeigen.

Um mit dem Sichern des gesperrten Rechners zu beginnen, sollten Sie auf Ihrem eigenen PC ein Linux mit den Paketen *libdc1394-22*, *libraw1394-dev*, *swig* und Python in der Version 2.3 bereithalten. Sollten Sie diese Pakete noch nicht installiert haben, empfehlen wir Ihnen, die folgenden Kommandos auszuführen:

```
sudo apt-get install libdc1394-22 libraw1394-dev swig
wget http://www.python.org/ftp/python/2.3.6/Python-2.3.6.tgz
tar -zxvf Python-2.3.6.tgz
cd Python-2.3.6
./configure
// Nun müssen Sie das Makefile editieren und die Zeile
// BASECFLAGS=      -fno-strict-aliasing
// durch
// BASECFLAGS=      -fno-strict-aliasing -fno-stack-protector -U_FORTIFY_
SOURCE
// ersetzen.
make
sudo make install
```