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.