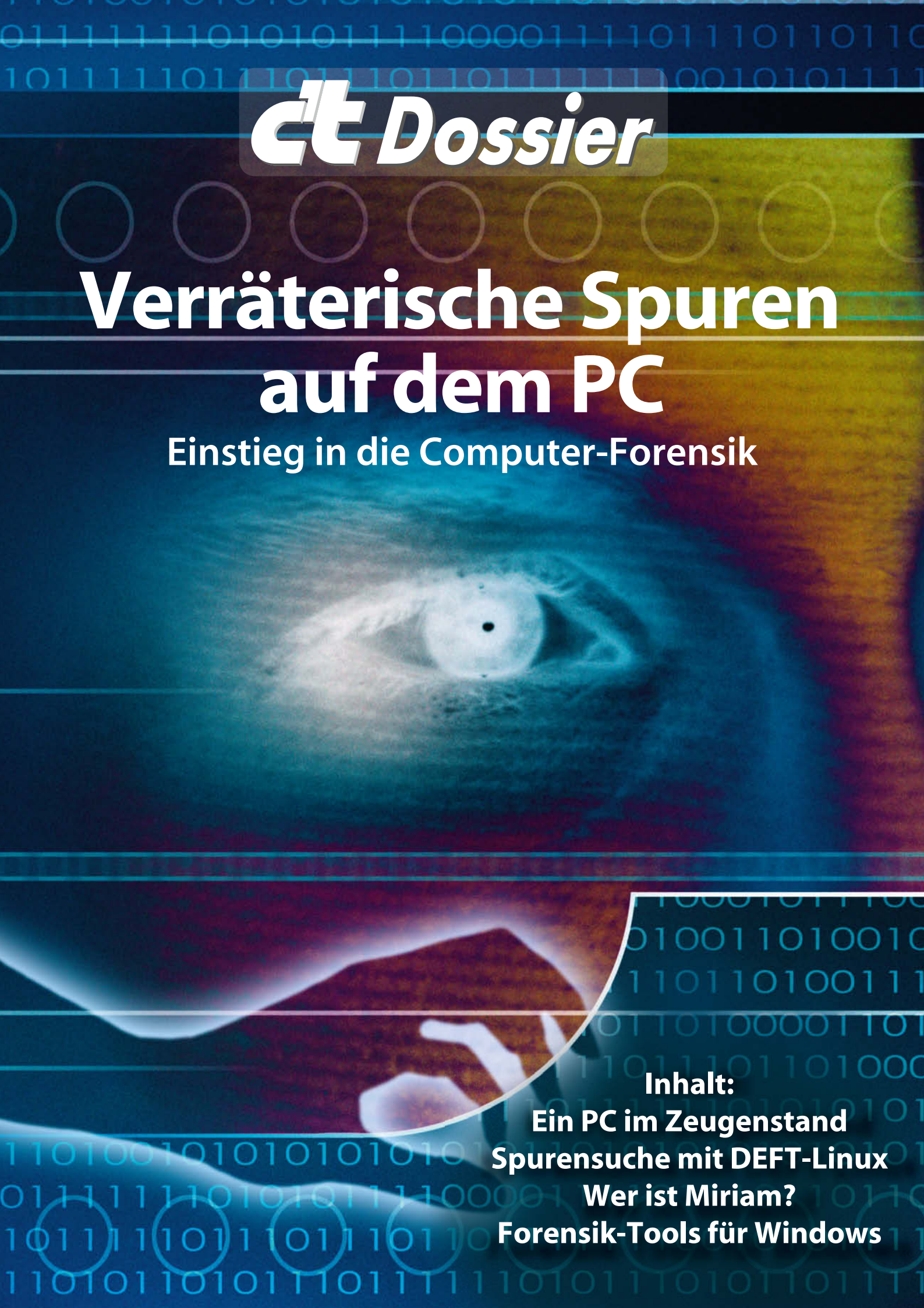
c't Dossier

Verräterische Spuren auf dem PC

Einstieg in die Computer-Forensik



Inhalt:

c't Dossier

Verräterische Spuren auf dem PC

Einstieg in die Computer-Forensik

Ein Computer beherbergt mehr Daten, als man gemeinhin annimmt. Klar, da sind Browser-Verlauf, längst vergessene Bilder und Steuererklärungen. Aber professionelle Forensiker fördern auch gelöschte Dateien und Informationen zur Nutzung des Computers zu Tage. Die verraten oft mehr, als einem lieb sein kann. Testen Sie selbst, was Ihr PC über Sie weiß.

Die Artikel stammen aus c't Magazin für Computertechnik 20/2014.

Impressum

c't Dossier: Verräterische Spuren auf dem PC
Chefredakteur: Detlef Grell
Konzeption: Dr. Oliver Diedrich
Redaktion: Jürgen Schmidt (ju)
Mitarbeiter dieser Ausgabe: Tanja Lautenschläger, Heiko Rittelmeier
Umschlaggestaltung: Martin Kreft

ISBN 978-3-95788-017-8 (v1)

Heise Zeitschriften Verlag GmbH & Co. KG
Karl-Wiechert-Allee 10
30625 Hannover

Tanja Lautenschläger

Zeuge der Anklage

Ein PC im Zeugenstand

Im Prozess gegen Tom K. kommt es heute zu einer vielleicht entscheidenden Aussage: Das Gericht befragt den PC des Angeklagten, um dem Sachverhalt auf den Grund zu gehen. Wird dieser den Vorwurf des Filesharings bestätigen?

Gericht: Ich rufe in den Zeugenstand: Den Personalcomputer des Beschuldigten Tom K.! Bitte stellen Sie sich erst einmal vor.
Zeuge: Mein Name ist E1-731, Acer Aspire E1-731. In mir schlägt das Herz eines Pentium Dual Core und mit meinem 4 GByte großen Kurzzeitgedächtnis kann ich noch ganz gut mithalten, auch wenn die Entwicklung inzwischen weiter ist und ich vielleicht nicht mehr ganz dem neuesten Stand der Technik entspreche. Ich bin also sozusagen „im besten Alter"!

Meine Daten speichere ich auf einer 500 GByte großen Festplatte. Ich kann aber auch optische Datenträger lesen und beschreiben. Weiterhin verfüge ich über diverse Anschlüsse, von USB über HDMI bis hin zu VGA und anderen.
Gericht: Unter welcher Adresse sind Sie für gewöhnlich zu erreichen?
Zeuge: Ich bin über WLAN in das Funknetz des Angeklagten eingebunden und dort via TCP/IP zu erreichen. Ich habe zwar keine wirklich feste IP-Adresse, bekomme aber vom WLAN-Router aus Gewohnheit immer die gleiche zugeteilt: 192.168.0.101. Die wird dann mit der MAC-Adresse meines WLAN-Adapters assoziiert, die auch als physikalische oder Hardware-Adresse bekannt ist. Diese weltweit eindeutige Zeichenfolge 00:50:8b:ae:7e:f6 steckt in allen Datenpaketen, die ich ins Netz schicke oder die für mich gedacht sind. Sie wird mich wohl mein Leben lang begleiten – sofern mein Besitzer sie nicht explizit ändert. Die ersten drei Bytes „00:50:8b" habe ich übrigens dem Hersteller des WLAN-Moduls zu verdanken – der Firma Compaq.

An diesen Adressen bin ich aber nur aus meiner unmittelbaren Umgebung zu erreichen. Meine Kommunikation mit anderen PCs im Internet erfolgt über den Router, der in alle Netzwerk-Pakete statt meiner seine eigene IP-Adresse einträgt. Diese erhält er bei jedem Einwählvorgang – also alle 24 Stunden neu von der Gegenstelle der Telekom. Damit hab ich nichts zu tun; für Genaueres dazu befragen Sie besser den Router beziehungsweise die Telekom.

Die Befragung beginnt

Anklage: Gut. Ich möchte gerne im Laufe dieser Verhandlung Speicherorte identifizieren, an denen wir möglicherweise Spuren finden, um die hier verhandelte Anklage wegen illegalem Download von Musikdateien aufzuklären. Fangen wir ganz vorne an: Entschuldigen Sie bitte die Formulierung, aber Sie sind in erster Linie eine Kombination aus von Menschen gefertigten Bauteilen. Wie kommt es, dass Sie so genau über sich selbst Bescheid wissen?
Zeuge: Hier kommt das BIOS (Basic Input/Output System) ins Spiel. Diese Software ist fest in der Hauptplatine eingebettet: auf einem nichtflüchtigen Speicher, in meinem Fall einem Flash-EEPROM. Nur durch dieses BIOS bin ich in der Lage, meine verschiedenen Komponenten anzusprechen und funktionsfähig zu machen, sowie mein Betriebssystem zu starten.

Die Übereinstimmung mit dem altgriechischen Wort bios – zu Deutsch Leben – ist übrigens eine Anspielung darauf, dass diese Software meinen Einzelteilen quasi Leben einhaucht.
Anklage: Ich verstehe. Sie sprachen jetzt von einem Speichermodul auf dem Mainboard. Können da auch die für uns relevanten Daten untergebracht sein? Ganz konkret suchen wir hier ja nach größeren Mengen illegal heruntergeladener Musikdateien. Die benötigen ja auch eine gewisse Menge Speicherplatz!
Zeuge: Nein. Dafür ist so ein EEPROM zu klein. Das Betriebssystem – ein auch nicht mehr ganz taufrisches Windows 7 – und auch alle anderen Daten, die ich verwalte, liegen auf meiner eben schon erwähnten Festplatte.

Ordnung ist das halbe Leben

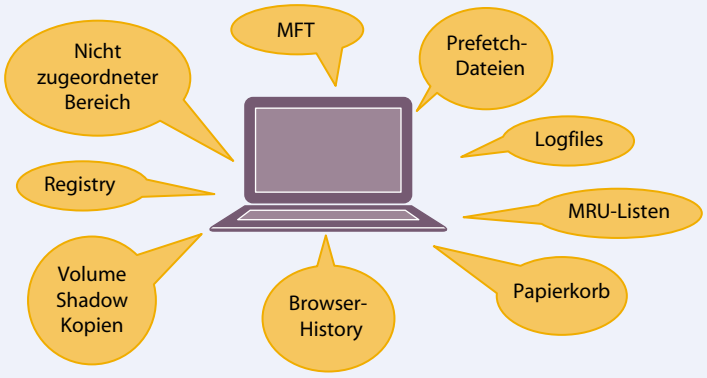
Gericht: Und wie ist das alles organisiert? Also wie wissen Sie, wo dort was zu finden ist?
Zeuge: Dazu muss ich ein bisschen weiter ausholen. Meine Festplatte ist in rund eine Million 512 Byte kleine Blöcke unterteilt. Diese werden zu mehreren großen und zusammenhängenden Bereichen, den Partitionen zusammengefasst. Die Partitionstabelle am Anfang der Festplatte sagt mir, welche Blöcke zu welcher Partition gehören.

Innerhalb dieser Partitionen habe ich beim Formatieren ein Dateisystem angelegt, das mir verrät, wo ich welche Daten abgelegt habe. Es verbindet nämlich den Dateinamen mit der Speicheradresse – also den von der Datei belegten Blöcken.
Anklage: Aha! Auf dieses „Dateisystem" würde ich gerne einmal näher eingehen. Gibt es da verschiedene? Verwenden Sie ein bestimmtes?
Zeuge: Ich arbeite mit NTFS, da dies das Standard-Dateisystem von Windows ist.
Anklage: Und wie zuverlässig ist dieses System? Ich meine, gehen dabei auch mal Daten verloren? Was ist, wenn der Angeklagte die Festplatte neu formatiert hat?
Zeuge: Um solche Ausfälle zu vermeiden, habe ich beim ersten Formatieren jeden einzelnen Sektor getestet, eventuell fehlerhafte Blöcke markiert und von der weiteren Verwendung ausgeschlossen. Erst danach habe ich das Dateisystem eingerichtet. Dann ist die Festplatte wie leergefegt.

Wenn die Festplatte später noch einmal formatiert wird, – etwa beim Neu-Einrichten des Systems – findet meist nur noch eine Schnell-Formatierung statt; Menschen haben anscheinend wenig Zeit und lassen dann sowohl die Fehlerüberprüfung als auch eine gründliche Löschung der Festplatte einfach weg.

Der Computer als Zeuge

Der PC speichert Informationen an vielen verschiedenen Orten. Forensiker kennen sie alle und werten sie systematisch aus.



Nicht vergessen, nur verlegt

Anklage: Das heißt, es werden gar nicht alle Daten vernichtet, wenn die Festplatte neu formatiert wird?
Zeuge: Genau. Tatsächlich erzeuge ich bei einer Schnellformatierung einfach nur ein frisches Inhaltsverzeichnis des Dateisystems, die sogenannte Master File Table, kurz MFT. Das bedeutet, die eigentlichen Daten sind alle noch da, aber ich kann sie nicht mehr lokalisieren, weil sie in der frischen MFT nicht mehr aufgeführt sind.

Überschrieben werden die Dateien erst, wenn ich ihren Speicherplatz für neue Dateien brauche. In der Master File Table stehen übrigens sehr detaillierte Informationen zu jeder einzelnen Datei: Welche Blöcke auf der Festplatte dazugehören, wer welche Zugriffsberechtigungen hat, aber auch solche Sachen wie Größe, Erstellungsdatum, letztes Änderungsdatum, etc.
Anklage: So, so. Das könnte unter Umständen noch interessant werden! Ist es denn möglich, ein solches altes Inhaltsverzeichnis wiederzufinden?
Zeuge: Ist die MFT eines Dateisystems einmal überschrieben, gibt es kein Zurück mehr. Allerdings gibt es auch ohne MFT eine Möglichkeit, an die Daten aus dem System noch einmal heran zu kommen.

Die ganzen Blöcke einer Festplatte, die entweder noch völlig leer sind oder nicht zu einer Datei aus dem aktuellen Dateisystem gehören, nennt man den „Nicht zugeordneten" Speicherbereich. Dieser „Unallocated Space" ist für forensische Untersuchungen äußerst interessant, da man hier noch viele Informationen finden kann, auch wenn sie in keiner MFT mehr stehen.

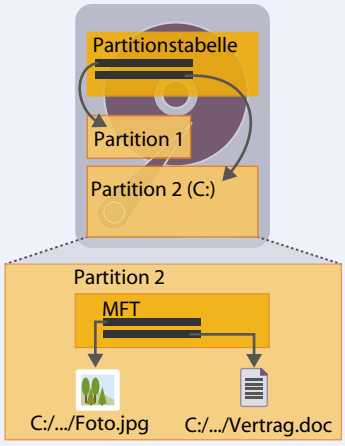
Im Wesentlichen arbeitet man dabei den gesamten Bereich systematisch Byte für Byte ab und sucht nach typischen Anfängen einer Datei. Dabei hofft man, dass deren Daten dann direkt dahinter folgen und nicht über verschiedene Bereiche der Festplatte verteilt sind. Es kann aber natürlich auch passieren, dass Dateien schon teilweise überschrieben sind.
Anklage: Gehe ich dann recht in der Annahme, dass wir also manche Musikdateien, nach denen hier gesucht wird, zumindest teilweise noch im Unallocated Space finden können?
Zeuge: Ja, das ist korrekt.
Gericht: Dann fordere ich Sie hiermit auf, die erforderliche Datenwiederherstellung vorzunehmen. Das Gericht wird sich so lange vertagen.

Drei Stunden später

Zeuge: Im fraglichen Bereich der Festplatte konnten 2 493 Dateien im MP3-Format gefunden werden. 453 davon sind schon teilweise überschrieben. Es liegen keine Metadaten dazu mehr vor, es ist also zum Beispiel nicht bekannt, in welchem Verzeichnis sich diese Dateien zuletzt befanden und es sind auch keine MAC-Times mehr bekannt.

Festplatten

Die Festplatte wird durch Partitionstabelle und MFT verwaltet. Schnelles Formatieren löscht nur die MFT, nicht aber die Daten.



Gericht: Die MAC-Adresse haben wir schon kennengelernt, aber was sind denn jetzt bitte „MAC-Times"?
Zeuge: Das ist ein Begriff, der sich eingebürgert hat. Jede Datei in einem Dateisystem bekommt drei Zeitstempel: Datum der letzten Änderung (Modified), Datum des letzten Zugriffs (Accessed) und Erstellungsdatum (Created). Die drei Anfangsbuchstaben ergeben „MAC".
Verteidigung: Da keine Metadaten mehr vorhanden sind, bleibt also immer noch zu klären, wie diese Dateien auf die Festplatte des Zeugen gelangt sind.
Gericht: Das ist richtig. Den nicht zugeordneten Bereich der Festplatte haben wir aber nun ausgewertet. Fakt ist bisher, es sind Musikdateien vorhanden. Kommen wir zum bestehenden Dateisystem und den Hinweisen, die wir darauf finden können. Wenn ich Sie richtig verstanden habe, ist hier auch das aktuell installierte Betriebssystem zu finden.
Zeuge: Ja. Im zugeordneten Bereich der Systempartition ist das Betriebssystem Windows 7 installiert.
Gericht: Können Sie uns etwas mehr zu diesem System sagen?
Zeuge: Windows 7 hat die Angewohnheit, die Festplatte, auf der es installiert wird, in mindestens zwei Partitionen aufzuteilen: Zum einen die sogenannte Bootpartition, die den Bootsektor enthält. Diese Partition ist immer unverschlüsselt und bekommt keinen Laufwerksbuchstaben zugewiesen. Das ist auch der Grund, warum sie auf den ersten Blick nicht zu sehen ist.
Anklage: Sie ist also von Hause aus nicht sichtbar? Das wäre ja grundsätzlich ein gutes Versteck! Gibt es eine Möglichkeit, diesen Bereich sichtbar zu machen?
Zeuge: Ja, die gibt es, ich kann sie prinzipiell sogar anzeigen. Es ist allerdings nicht so einfach, hier etwas zu verstecken, denn zum einen ist diese Partition von Anfang an so gut wie vollständig belegt und zum anderen rate ich dringend davon ab, hier womöglich etwas zu löschen, um Platz zu schaffen, sonst komme ich eventuell durcheinander und kann Windows nicht mehr richtig starten!

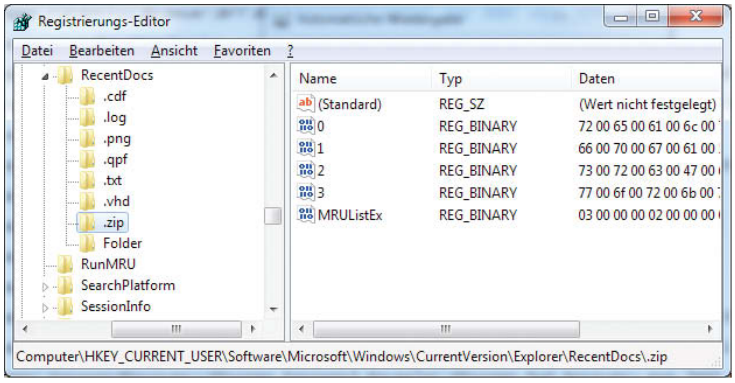
Die zweite Partition

Anklage: Verstehe. Dann bleibt ja nur noch die zweite Partition, um nach weiteren Spuren zu suchen. Können Sie uns darüber etwas mehr erzählen?
Zeuge: Diese zweite Partition ist die normale „Systempartition", die üblicherweise mit C: benannt wird, und der der restliche Platz zugewiesen wird – sofern nicht ein Hersteller noch etwas für seine Wiederherstellungspartition abzweigt. Seit Windows Vista ist die Verschlüsselungssoftware Bitlocker in den Enterprise und Ultimate-Editionen enthalten. Damit könnte ich Festplatten, Partitionen komplett verschlüsseln! Ich habe allerdings nur „Home Premium" und kenne dieses Bordmittel daher nur vom Hörensagen.

Als mein Besitzer mich zum ersten Mal aus der Verpackung nahm und gestartet hat, legte er schon während des Hochfahrens einen „Benutzer" in Windows an. Dieser erste Benutzer ist immer ein „Administrator", was ihm so ziemlich alle Rechte in Bezug auf Installationen und Systemeingriffe einräumt. Anscheinend heißt er Tom, denn so hat er das Konto genannt.
Anklage: Ja, das passt. Wir verhandeln hier heute ja den Vorwurf gegen Tom Krämer. Wurden denn noch weitere Benutzerkonten eingerichtet? Und ist das Konto „Tom" per Passwort geschützt?
Zeuge: Es wurden weiterhin nur die systemeigenen Konten, die durch Windows selbst erzeugt werden, angelegt. Das Konto Tom ist mit einem Passwort gesichert, so wie ich es auch empfohlen habe.
Gericht: Sie benötigen dieses Passwort aber nicht, um etwa jetzt auf diese Daten zuzugreifen, ist das korrekt?
Zeuge: Nein. Das Passwort sperrt nur den Zugang zu Windows und einigen wenigen speziell gesicherten Dateien. Dazu gehört etwa ein verschlüsselter Tresor, der Windows Vault, in dem Windows unter anderem von Tom gespeicherte Passwörter abgelegt hat. Alle anderen Daten kann ich – und im Übrigen auch ein anderer Computer, an den man meine Festplatte anschließt – jederzeit und völlig ungehindert lesen.
Anklage: Gut. Wie ist der Benutzer Tom weiter vorgegangen?
Zeuge: Tom hat angefangen, Programme zu installieren.
Anklage: Gibt es von diesen Programmen eine Liste? Das heißt, kann man irgendwo erfahren, welche Programme alle auf ihrer Festplatte installiert sind?

Datenschatz Registry

Zeuge: Ja, eine solche Liste gibt es. Sie ist in der Registrierungsdatenbank von Windows



Die Most-Recently-Used-Einträge (MRUs) in der Registry sind ein wichtiger Datenschatz für Forensiker. Doch erst die richtigen Tools machen sie lesbar.

gespeichert, die auch als „Registry“ bekannt ist. Dort sind noch sehr viel mehr Informationen zu dem aktuellen System und zu den installierten Programmen abgelegt.

Gericht: Welche Informationen lassen sich denn aus der Registry gewinnen?

Zeuge: Alles hier aufzuzählen würde wahrscheinlich den Rahmen sprengen, aber ich sehe dort, welche USB-Geräte jemals mit mir verbunden waren, welche Programme der Anwender zuletzt über den Befehl „Ausführen“ gestartet hat und die letzten 25 Internetadressen, die er von Hand im Internet Explorer eingetippt hat. Viele Programme merken sich hier auch, welche Dokumente sie zuletzt geöffnet hatten. Darüber hinaus gibt es Informationen zu installierten Treibern, benutzten Dateifreigaben und vieles mehr.

Anklage: In unserem Fall soll der Angeklagte mit dem Filesharing-Programm „Bearshare“ illegal urheberrechtlich geschützte Musikdateien aus dem Internet heruntergeladen und auch wieder zum Download durch andere Nutzer freigegeben haben.

Verteidigung: Wie das Gericht der Web-Seite des Herstellers entnehmen kann, bietet das Programm Bearshare schon mindestens seit 2007 keine solchen Funktionen mehr. Es dient vielmehr ausschließlich der Nutzung der legalen Download-Plattform.

Anklage: Das ist korrekt. Doch die alten Versionen sind noch funktionsfähig und können mit dem nach wie vor existenten Peer-to-Peer-Netz Gnutella in Kontakt treten. Zeuge: Ist oder war dieses Programm auf Ihrer Festplatte installiert?

Zeuge: Ja. Meine Registry-Einträge belegen, dass Bearshare am 23. 03. 2012 auf meiner Festplatte installiert wurde.

Anklage: Sie können doch bestimmt auch feststellen, welche Version installiert wurde. War es die aktuelle des Herstellers?

Zeuge: Nein. Der Dateiname der Installationsdatei deckt sich nicht mit der aktuell auf der Seite des Herstellers angebotenen Datei sondern weist auf eine deutlich ältere Version hin. Außerdem erfolgte die Installation nicht aus einem Download-Ordner, sondern vom Laufwerk F: aus – also vermutlich von einem USB-Stick.

Verteidigung: Das widerspricht aber Ihrer zu Protokoll gegebenen Aussage, dass das Programm Bearshare nicht auf Ihrer Festplatte vorhanden ist.

Zeuge: Das liegt daran, dass es zwischen dem 18. und 25. 12. 2013 wieder deinstalliert wurde. Das sehe ich unter anderem an meinen Schattenkopien.

Ein Schatten meiner selbst

Gericht: Schattenkopien? Zu diesem Begriff brauchen wir nähere Erläuterungen.

Zeuge: Der Volume Shadow Service (VSS) ist ein System-Dienst, der bei Windows 7 standardmäßig aktiviert ist. Ich erzeuge dabei sogenannte Schattenkopien im Ordner C:\System Volume Information\, die verschiedene Versionen von Dateien und viele weitere Informationen über ein System zu einem ganz bestimmten Zeitpunkt enthalten. Damit kann man auch ganz leicht als Benutzer einen bestimmten Zustand wiederherstellen, zum Beispiel, wenn bei einer Installation etwas schiefgegangen ist. Bekannt ist diese Funktion durch die „Wiederherstellungspunkte“.

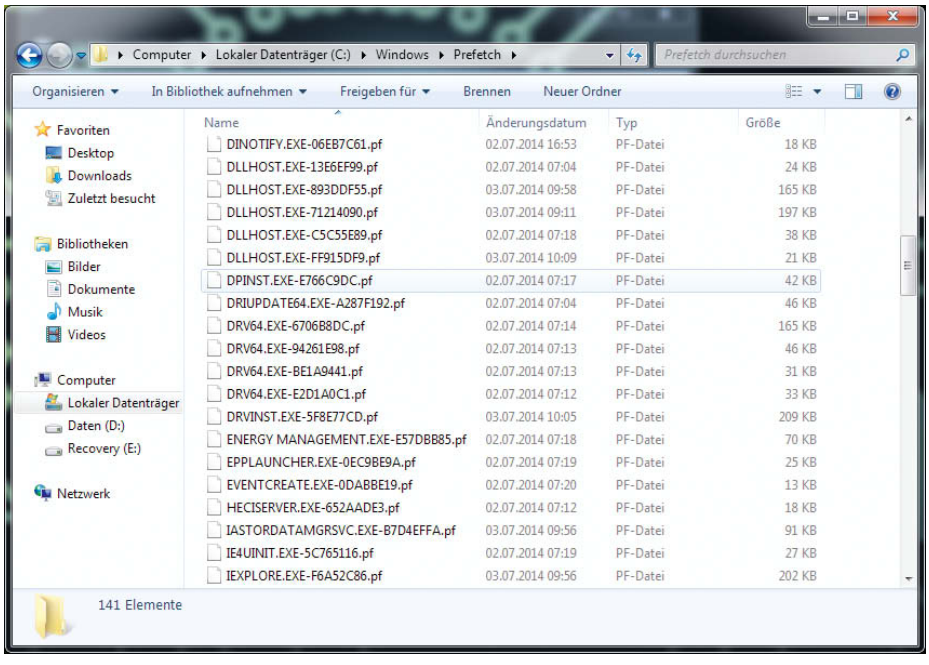
Hinter den Kulissen erstelle ich dabei regelmäßig Änderungsdateien, die es mir ermöglichen, einen früheren Zustand wiederherzustellen. Das mache ich routinemäßig alle sieben Tage – oder bei Bedarf, wenn größere Änderungen etwa durch die Installation von neuer Software anfallen. Selbst wenn Dateien zwischenzeitlich gelöscht, überschrieben oder verschlüsselt wurden, können über die Schattenkopien frühere Versionen wiederhergestellt werden.

Mit speziellen forensischen Tools kann aus diesen gesammelten Daten das Image eines Datenträgers zum Zeitpunkt der jeweiligen Erstellung der Schattenkopie wieder hergestellt werden. Allerdings wird standardmäßig nur die Systempartition C: derart gesichert. Auch beschränkt sich die Wiederherstellung auf Dateien der wichtigsten Dateitypen; Anwenderdateien – also insbesondere dessen Dokumente und Musikdateien – sind explizit ausgeschlossen. Schließlich will man nicht, dass nach einer Wiederherstellung plötzlich alle zwischenzeitlich erstellten Dokumente verschwunden sind.

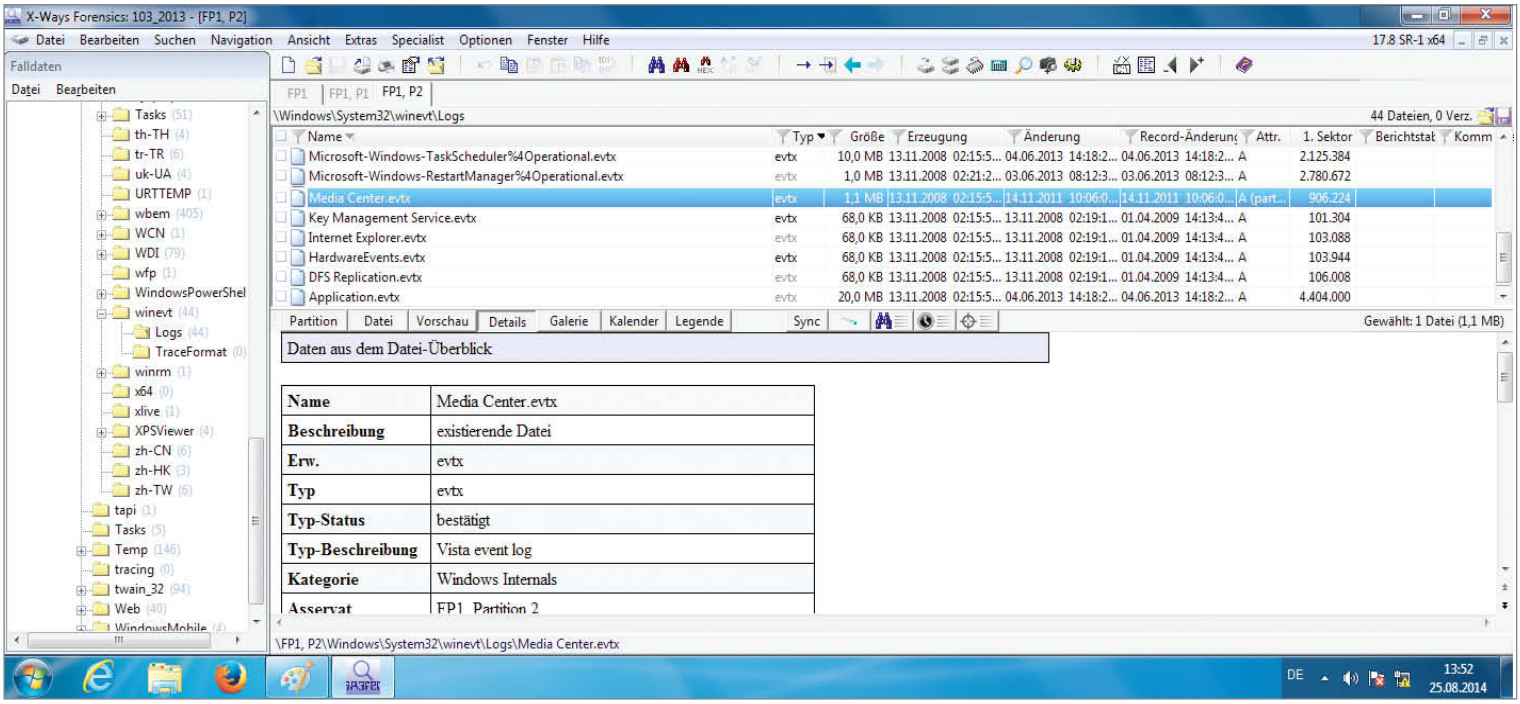
Außerdem werden regelmäßig die ältesten Wiederherstellungspunkte gelöscht, wenn drei beziehungsweise fünf Prozent des Speichers durch Schattenkopien belegt sind. Wie weit diese Wiederherstellungsmöglichkeit in die Vergangenheit reicht, hängt also von der Größe der Festplatte und den Aktivitäten des Benutzers ab.

In dem System zum Zeitpunkt des Wiederherstellungspunkts vom 18. 12. 2013, den ich angelegt hatte, weil hier mehrere Programme deinstalliert wurden, war das Programm Bearshare noch auf meiner Festplatte. Stelle ich hingegen den Zustand der nächsten Routinespeicherung vom 25. 12. wieder her, kann ich es nicht mehr finden.

Anklage: Es kann also eindeutig nachgewiesen werden, dass dieses Programm zum frag-



Der versteckte Prefetch-Ordner verrät, welche Programme auf dem PC gestartet wurden.



Kommerzielle Software wie X-Ways Forensics liefert viele Informationen wie spezielle Log-Dateien bereits gut aufbereitet auf dem Silber-Tablett. Aber auch kostenlose Tools wie die in den folgenden Artikeln bringen solche Informationen zum Vorschein.

lichen Zeitpunkt auf Ihrer Festplatte installiert war.

Zeuge: Ja, das ist korrekt. Ich konnte auch noch eine weitere Datei zu diesem Programm finden, die ebenfalls belegt, dass das Programm vorhanden war. Für jedes ausgeführte Programm lege ich mir nämlich im Ordner C:\Windows\Prefetch eine sogenannte Prefetch-Datei mit der Endung .pf an, in der ich mir merke, welche Komponenten und Dienste alle zu dem Programm dazu gehören und geladen werden müssen, wenn das Programm gestartet wird. So funktioniert der Programmstart wesentlich schneller, und ich habe auch einen Überblick darüber, welche Anwendung welche Bibliothek nutzt und muss diese dann eventuell nur einmal laden. Sogar Programme, die von einem externen Speichermedium gestartet werden (zum Beispiel ein USB-Stick oder eine Festplatte), merke ich mir so, um beim nächsten Mal vorbereitet zu sein.

Verteidigung: Nur weil dieses Programm einmal installiert war, heißt das ja noch nicht, dass die fraglichen Musikdateien auch darüber illegal heruntergeladen wurden. Der Zeuge sagte doch explizit, dass Musikdateien durch die Schattenkopien nicht erfasst werden.

Anklage: Das ist richtig. Aber vielleicht lässt sich dies ja indirekt nachweisen. Zeuge E1, wäre es denn möglich, durch die entsprechende Schattenkopie den Zustand der Festplatte und damit auch die Konfiguration von Bearshare wieder herzustellen?

Viele Wege zum Ziel

Zeuge: Ja, sicher. Die Schattenkopie kann extrahiert werden und spezielle Programme können daraus eine virtuelle Maschine, also einen nur logisch existierenden Computer generieren. Dieser lässt sich dann genauso bedienen, wie ich auch. Ich könnte dann zum Beispiel das zu diesem Zeitpunkt noch installierte Programm öffnen und nachsehen, welcher Ordner für Downloads vorgesehen war, beziehungsweise welche Verbindungen eingerichtet waren.

Genauso gut könnte ich auch versuchen, die speziellen Logfiles des Programms entweder durch spezielle Datenwiederherstellungs-Programme oder über die Schattenkopie wiederzufinden und in denen Hinweise auf die fragliche MP3-Datei zu entdecken.

Gericht: Was müssen wir uns denn unter einem Logfile vorstellen?

Zeuge: Ein Logfile ist eine Protokoll-Datei. Hier werden bestimmte, vorher genau definierte Aktionen eines Programms festgehalten, meistens sogar mit Zeitstempeln. Prinzipiell kann jedes Programm ein Logfile anlegen. Für Informationen, die das System betreffen, sind natürlich die Logfiles von Windows besonders interessant.

Hier kann man zum Beispiel erfolgreiche oder fehlgeschlagene Anmeldeversuche, Konfigurationsänderungen, Fehlermeldungen, den Anschluss externer Geräte, aber auch Virenvorkommnisse oder Firewall-Verstöße sehen. Jedes dieser Vorkommnisse wird als „Event" bezeichnet, weswegen die Logfiles von Windows auch „Eventlog" heißen. Diese Dateien befinden sich im Ordner C:\Windows\system32\winevt und enden meistens mit .evt oder .evtx.

Anklage: Gibt es denn durch das Programm Bearshare erzeugte Logfiles?

Zeuge: Ich werde mal nachsehen … Ja, ich denke, ich habe einige Protokolldateien gefunden, die zu dem Programm gehören, und die noch nicht überschrieben wurden. Bearshare hat offenbar für jeden Benutzer eine Datei namens shistory.im angelegt und darin abgespeichert, welche Suchbegriffe er eingegeben hat.

Außerdem habe ich noch weitere Protokolle gefunden, die auflisten, welche Dateien angeboten wurden und welche heruntergeladen wurden.

Gericht: Das klingt doch außerordentlich aufschlussreich! Die genaue Auswertung dieser Protokolle werden wir dann später noch vornehmen.

Gibt es denn noch weitere Informationsquellen, die berücksichtigt werden könnten?

Zeuge: Naja, ich könnte nun noch aus den Most-Recently-Used-Listen auslesen, welche Dateien zuletzt genutzt beziehungsweise geöffnet wurden. Ich könnte im Papierkorb nachsehen, welche Dateien erst kürzlich gelöscht wurden. Ich könnte in den Netzwerkkonfigurationen nachsehen, mit welchen Netzwerken ich in letzter Zeit verbunden war. Ich könnte in den Aufzeichnungen der installierten Internet-Browser nachsehen, welche Suchbegriffe eingegeben wurden, welche Dateien über einen Browser herunter geladen wurden, …

Gericht: Ähm, Ja, danke! Ich denke das reicht uns fürs Erste. Wir werden nun die detaillierten Analysen abwarten und uns dann zurückziehen um diese neuen Informationen zu bewerten. Wir danken dem Zeugen an dieser Stelle schon einmal für die interessanten Ausführungen! (ju) c't

NEU

c't Security

2014

Doppel-
Live-DVD

c't Bankix
Forensik:
DEFT-Linux + DART

Themenauswahl:

Router-Angriffen vorbeugen

Kontrolle über die eignen Daten

Sicher im **Netz**

Passwörter knacken

Das neue Security-Sonderheft der c't

Ab dem 3. 11. im Handel

www.ctspecial.de

Heiko Rittelmeier

Auf Spurensuche

Forensische Analyse eines PC mit DEFT

DEFT-Linux ist eine Linux-Distribution, die sich speziell an Forensiker richtet. Mit ihren Tools kann man alle möglichen auf einer Festplatte gespeicherten Informationen über deren Besitzer zum Vorschein bringen: von detaillierten Listen seiner Aktivitäten bis hin zu längst gelöschten Dateien. Machen Sie doch mal den Selbstversuch mit Ihrem Windows-PC.

Das "Digital Evidence & Forensics Toolkit", kurz DEFT, können Sie in der aktuellen Version 8.2 als ISO-Datei von www.deftlinux.net/files herunterladen und als Datenträgerabbild auf eine DVD brennen. Starten Sie Ihren Rechner anschließend von dieser DVD. Das zugrunde liegende Ubuntu Linux kommt mit den meisten Systemen mit 64-Bit-CPU problemlos zurecht. Falls Ihres zu den wenigen Ausnahmen gehört, können Sie trotzdem die DART-Windows-Tools nutzen, die im folgenden Artikel vorgestellt werden.

Als System-Sprache bietet das Boot-Menü leider nur Englisch, Spanisch und Italienisch an. Es lohnt sich jedoch trotzdem, vor dem Start von „DEFT Linux 8 live“ via F3 die deutsche Tastatur-Belegung (Keymap German) auszuwählen, damit man später auch alle Zeichen erreichen kann.

DEFT wird beim Start keine Datenträger einbinden oder gar verändern. Es orientiert sich da ganz an der Vorgehensweise eines Forensikers, der das Objekt seiner Untersuchung auf gar keinen Fall verändern darf. Eine Benutzeranmeldung ist nicht erforderlich; nach dem Start ist man sofort als Benutzer „root“ aktiv und kann somit die benötigten Datenträger selbst einbinden. Das geschieht am einfachsten über den speziell dafür vorgesehenen MountManager.

Dieser ist über den grünen Menü-Button links unten unter „DEFT > MountManager“ oder direkt über die Schnellstartleiste erreichbar. Nach dem Start erscheint eine Warnung, dass man im Begriff ist, ein Programm aufzurufen, das möglicherweise Daten auf den Datenträgern ändern könnte. Nach der Bestätigung, dass man weiß, was man tut, startet MountManager und zeigt eine Übersicht über die im System erkannten Laufwerke, die übrigens auch dynamisch aktualisiert wird.

In den meisten Fällen, dürfte das so aussehen, wie in unserem Screenshot: eine eingebaute Festplatte sda, die in die zwei Partitionen sda1 und sda2 unterteilt ist. Beide sind bei den meisten Windows-Installationen NTFS-formatiert. Die erste ist in der Regel zwischen 100 und 400 MByte groß, die zweite belegt den restlichen Platz der Festplatte. Manche Systeme haben zusätzlich noch eine Wiederherstellungspartition von einigen wenigen GByte, die vom Computerhersteller eingerichtet wurde und die für eine Neuinstallation benötigten Dateien enthält. Neben den Windows-Installationsdaten sind hier üblicherweise auch die für das spezielle System erforderlichen Treiber abgelegt.

Die erste Partition und die Wiederherstellungspartition kann man für den momentanen Zweck links liegen lassen. Ziel der Untersuchung ist die Partition zwei, die das Windows-System enthält. Im abgebildeten Beispiel also „sda2“ mit einer Größe von knapp 64 GByte.

Zum Einbinden eines Datenträgers braucht man unter Linux ein Verzeichnis als Mountpoint, das leer sein sollte. DEFT stellt zu diesem Zweck schon ein paar vorbereitete Verzeichnisse für die vereinfachte Arbeit mit Windows-Datenträgern unter /mnt/ bereit: c, d, e, raw1, raw2, raw3 und smb.

Um die Gefahr zu minimieren, dass man hinterher etwas durcheinanderbringt, ist es von Vorteil, dass man sich an die Microsoft-Namenskonvention anlehnt und die Systempartition des Windows-Datenträgers unter

/mnt/c einbindet. Vorher sollte man jedoch darauf achten, dass bei den Optionen unter „What users can do at this partition“ der Wert „only read“ eingestellt ist. Damit wird die Partition schreibgeschützt eingebunden und man vermeidet jede böse Überraschung bei der späteren Arbeit mit verschiedenen Tools.

Über das Menü „Partition“ > „Mount“ kommt man an den Punkt, wo man seine Einstellungen vor dem eigentlichen Mounten der Partition abschließend überprüfen kann, der finale Klick auf „Mount“ bindet dann die gewählte Partition unter Nutzung der unter „Options“ eingetragenen Optionen („ro“) in das gewählte Verzeichnis ein. Wenn man Laufwerke direkt über den File-Manager einbindet („mount in protected mode“), werden diese ebenfalls ohne Schreibmöglichkeit mit einem Verzeichnis unter /media verbunden.

Wem die vom MountManager über die Partitionen angegebenen Daten nicht ausreichen, der kann über die Shell noch mehr erfahren. Die startet man über das Icon „LXTerminal“ und kann dann auf viele zusätzliche, textbasierte Tools zugreifen. Wer vergessen hat, beim Start das Tastatur-Layout umzustellen, macht vorher noch einen Abstecher zu „Startbutton > Preferences > Lxkeymap“.

Dann kann man sich beispielsweise mit dem SMART-Tools wichtige Informationen zum Hardware-Status eines Laufwerks anzeigen lassen.

```
smartctl -a /dev/sda
```

gibt Daten aus, die von der integrierten Selbstüberwachung des Datenträgers gesammelt wurden. Hierzu gehören Einschaltvorgänge, Fehlerraten und andere Daten, die der Bewertung der voraussichtlichen Lebenszeit und der Zuverlässigkeit des Laufwerks dienen können. Mit Hilfe des Parameters „-xa“ wird die Liste sogar noch umfangreicher und enthält dann zum Beispiel noch Informationen über bislang gemessene Maximal- und Minimaltemperaturen.

Umfassende Informationen über die Partitionierung einer Festplatte ermittelt das Tool „mmls“, das Bestandteil der in DEFT enthaltenen Toolsammlung The Sleuthkit ist.

```
mmls /dev/sda
```

liefert eine Tabelle mit den Start- und Endsektoren der von mmls erkannten Partitionen. Hierdurch lassen sich beispielsweise auch Rückschlüsse auf versteckte Partitionen oder bislang unbelegten Speicherplatz ziehen. Einen Teil der dort ausgegebenen Daten braucht man auch für weitergehende Analysen in anderen Programmen.

Bevor man mit der Untersuchung des Systems fortfährt, sollte man einen ausreichend großen externen Datenträger (USB-Stick oder USB-Festplatte) anschließen und diesen per MountManager ohne Schreibschutz (also mit Default-Einstellungen) mounten. Als Mountpoint bietet sich hierzu ein neu erstelltes Verzeichnis /media/stick oder /media/usbdisk an. Eine zweite interne Festplatte zur Datenablage wäre selbstverständlich genauso geeignet.

Wichtig ist nur, dass man einen Speicherort hat, an dem man Auswertungsergebnisse oder wiederhergestellte Daten ablegen kann, der nicht auf der zu untersuchenden Festplatte liegt. Die zu untersuchende Festplatte sollte man hierzu ausdrücklich NICHT verwenden, da dies zu unerwünschten Kollisionen und verfälschten Ergebnissen führen kann. So könnten etwa Log-Dateien oder wiederhergestellte Daten Bereiche überschreiben, in denen vorher noch wiederherstellbare Daten lagen.

Internet-Nutzung

Bevor man sich auf die zeitintensive Suche nach gelöschten Daten macht, bietet sich eine Untersuchung der noch vollständig vorhandenen Informationen an. Gerade bei den neueren Browsern kann man sehr schnell einen Überblick darüber bekommen, wo die Interessen des Benutzers beim Surfen liegen, wenn der keine speziellen Vorkehrungen zur Löschung von Verlaufsdaten getroffen hat. Besonders einfach machen es dem Forensiker die Browser Firefox und Chrome. Beide speichern – neben anderen spannenden Daten wie Bookmarks – den Verlauf der Internet-Aktivitäten in einer SQLite-Datenbank, die mit Hilfe eines SQLite-Browsers ganz einfach ausgelesen werden kann.

Die Datenbank des Firefox-Browsers liegt seit Windows Vista üblicherweise im Pfad c:\Users\%benutzername%\AppData\Roaming\Mozilla\Firefox\Profiles\%profilname%\; Windows XP legte die Anwenderdaten noch unter „c:\Dokumente und Einstellungen\Anwendungsdaten“ ab. Zur Untersuchung kopiert man die Datei places.sqlite am besten auf den Analyse-Stick und öffnet sie dann mit dem SQLite Database Browser (Start > DEFT > Analyse). Achtung: Das Öffnen direkt vor Ort scheitert daran, dass der SQLite-Browser dort dann auch eine temporäre Datei anlegen möchte.

„Browse Data“ im Hauptfenster und Auswahl der Tabelle „moz_places“ gibt dann die Liste der Seiten aus, die sich aktuell in der History des Firefox befinden. Die kann man entweder in der Standardansicht durchstöbern oder mit geschickten SQL-Statements unter „Execute SQL“ gezielt auswerten. Damit hat man bei der Spurensuche viel mehr Möglichkeiten als in der schlichten Verlaufsansicht des Browsers. Die 25 meistbesuchten Seiten zeigt:

```
SELECT * FROM moz_places ORDER BY visit_count DESC
LIMIT 25;
```

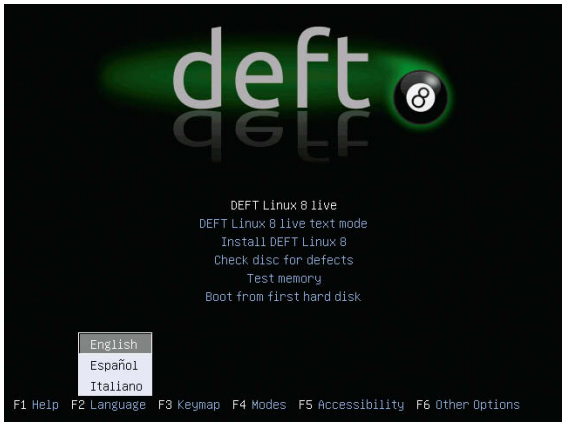
In der SQLite-Datenbank stecken neben den reinen Verlaufsdaten außerdem einige interessante Einträge, die man sonst nicht zu Gesicht bekommt. Ein Beispiel ist die Spalte „typed“ in der Tabelle moz_places: Ein dort gespeicherter Wert „1“ deutet darauf hin, dass der Benutzer die Adresse zumindest teilweise manuell eingegeben hat. Das Argument „Ich hab mich nur versehentlich verklickt“ ist damit schnell entkräftet.

Wer sich etwas mit SQL auskennt, kann die Inhalte mehrerer Tabellen verknüpfen und dabei auch gleich kryptische Datensätze direkt in ein menschenlesbares Format umwandeln. Die folgende SQL-Abfrage gibt die History mit menschenlesbaren Zeitstempeln aus, die nach Anzahl der Besuche absteigend sortiert ist:

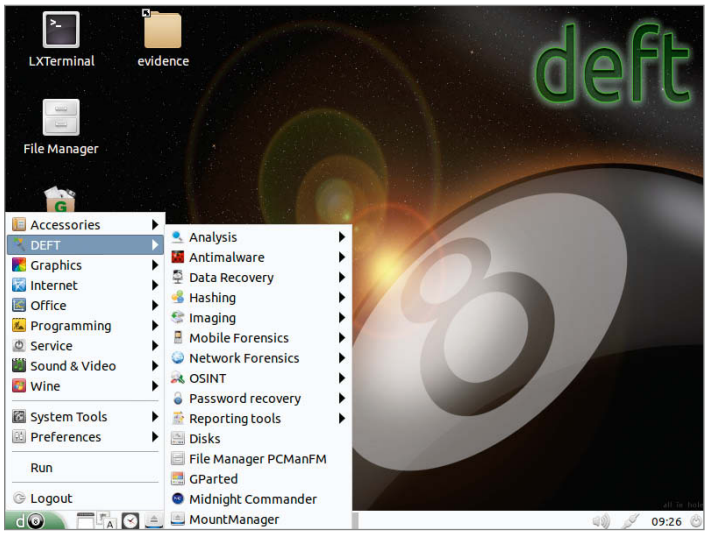
```
SELECT moz_historyvisits.id,
moz_places.url, moz_places.title,
moz_places.visit_count,
moz_places.typed,
datetime((moz_historyvisits.visit_date/1000000),
"unixepoch","localtime"),
moz_historyvisits.visit_type FROM moz_places,
moz_historyvisits WHERE
moz_historyvisits.place_id = moz_places.id
ORDER BY visit_count DESC;
```

Google Chrome speichert seine History ebenfalls in einer allerdings etwas anders aufgebauten SQLite-Datenbank, die ab Windows Vista üblicherweise im Pfad c:\Users\%benutzername%\AppData\Local\Google\Chrome\User Data\Default\ unter dem Namen History (ohne Erweiterung) zu finden ist.

Neben den besuchten Webseiten werden in dieser Datei beispielsweise in der Tabelle „downloads“ die vom User durchgeführten Downloads gespeichert, die Auswertungen mit etwas anderen Zielrichtungen erlauben. Allein mit den Daten, die die SQLite-Datenbanken der Browser speichern, könnte man sich einige Zeit beschäftigen und einige Artikel füllen. Als Einstieg soll das an dieser Stelle aber genügen.



Um DEFT zu benutzen, muss man den PC von der DVD booten; wenn es nicht starten will, helfen manchmal die „Other Options“ unter F6.



Das „d“ in der grünen Ecke links unten öffnet das Startmenü, in dem eine umfangreiche Werkzeug-Sammlung zum Stöbern einlädt.

Mehr Komfort

Im ersten Schritt wurde ganz bewusst ein eher manueller Ansatz zur Untersuchung gewählt, um einen direkten Einblick in die gespeicherten Daten zu ermöglichen und damit ein Gefühl für die vorhandenen Daten zu bekommen. Selbstverständlich gibt es auch Tools, die dem Forensiker die Arbeit erleichtern und die recht schnell übersichtliche Ergebnisse liefern.

Eines der mächtigsten Hilfsprogramme ist „log2timeline“, das aktuell schon sehr viele Datenquellen – also unterschiedliche Logfile-Formate – unterstützt und dank seines modularen Aufbaus im Prinzip jederzeit um weitere Analysemodule ergänzt werden kann.

Ein einfaches Beispiel ist die Analyse der History des Internet Explorer, die Sie mit

```
log2timeline -f iehistory -r ↵
                    /mnt/c/Users/<benutzername>/
```

erstellen können. Allerdings bleibt auch log2timeline noch etwas hinter dem Komfort kommerzieller Forensik-Tools zurück. Um mit den Daten wirklich zu arbeiten, muss man sie zunächst etwa mit „-w /media/stick/iehist.csv“ in eine CSV-Datei auf dem Analyse-Stick schreiben.

Diese Datei können Sie dann mit einer Tabellenverarbeitung wie der des enthaltenen LibreOffice oder später mit Excel genauer analysieren. Neben CSV beherrscht log2timeline auch viele andere Formate (Details verrät „-o list“). Und es analysiert auf Wunsch auch andere Datenquellen, darunter die Protokoll-Dateien von Firefox, Chrome, Opera, Safari, Adobe Reader, Skype und mehr. Es beherrscht sogar einige Mac-OS- und Linux-Datenquellen; „-f list“ gibt die vollständige Liste aus. Kommt es auf genaue Zeitangaben an, sollten Sie mit „-z“ die Zeitzone korrigieren.

E-Mail-Daten

Viele Mail-Programme schreiben E-Mails wie Thunderbird im Klartext in das Dateisystem. Zusätzliche Daten lagert Thunderbird in ebenfalls leicht zu analysierende SQLite-Datenbanken aus. Eine größere Herausforderung ist etwa Outlook, das E-Mails bevorzugt in einer PST-Datei speichert. Mit dem Tool „Startbutton > DEFT > Analysis > Readpst“ kann man den Inhalt einer solchen PST-Datei jedoch sehr schnell konvertieren.

```
readpst -DS /<Anwendungsdaten>/Local/Microsoft/↵
                                Outlook/Outlook.pst
```

bewirkt, dass alle Datensätze der PST-Datei – also E-Mails, Adressen, Termine und Journaleinträge – an der aktuellen Stelle ins Filesystem geschrieben werden. Das Ganze landet dabei in einer Ordnerstruktur, die dem Persönlichen Ordner im Outlook ähnelt. Soweit noch verfügbar, bezieht sich das mit den verwendeten Parametern auch auf die bereits in Outlook gelöschten Inhalte. Die Dateien kann man dann anschließend effizient durchsuchen oder systematisch aufbereiten. Schnelle Ergebnisse liefert ein

```
grep -iR <Suchbegriff> .
```

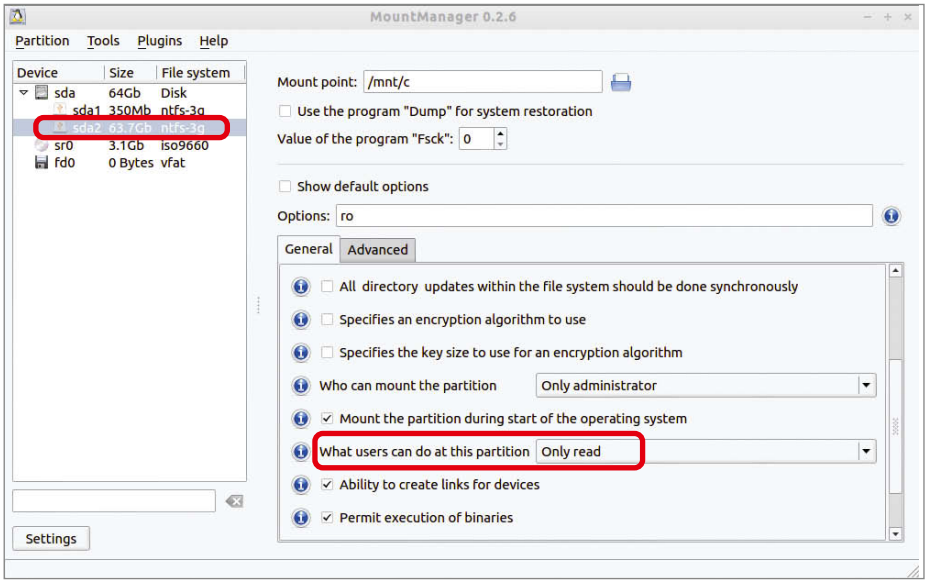
auf der Kommandozeile; für mehr Komfort greift man zu einer leistungsfähigen Volltextsuche wie Recoll (Start > DEFT > Analyse).

Nutzungsanalyse

Ein wichtiger Schritt jeder forensischen Analyse ist die Auswertung der zuletzt genutzten Dokumente („Jumplist“). Seitdem diese Liste im Betriebssystem nicht mehr global, sondern pro Anwendung verwaltet wird, kann man das unter Windows wesentlich genauer analysieren. Wir verzichten deshalb hier auf die Auswertung der Jumplists; die existierende Linux-Software reicht bei Weitem nicht an Windows-Tools heran, wie sie der Artikel zur Spurensuche in Windows auf Seite 96 vorstellt.

Etwas einfacher aus Sicht eines Linux-Systems ist der Umgang mit den Prefetch-Dateien, die beginnend mit Windows XP für jedes gestartete Programm vom Betriebssystem im Prefetch-Ordner erstellt werden. Die Dateien folgen dem Namensschema %Dateiname%-%Prüfsumme%.pf. Zweck dieses Prefetch-Mechanismus ist die Beschleunigung des Starts von Anwendungen. Als Nebeneffekt liefert der Mechanismus unter anderem die Information, wann welches Programm zuletzt gestartet wurde; einen ersten Einblick in das Nutzungsverhalten liefern schon die Zeitstempel der Dateien. Ein kleines Python-Skript, das Sie über den Link am Ende des Artikel erhalten, bereitet die Daten der Prefetch-Dateien gut auf; das Werkzeug log2timeline von DEFT kann diese Informationen ebenfalls auswerten.

Außer der Beschleunigung des Startprozesses hat dieser Ordner übrigens keine weitere Funktion. Das ist auch der Grund, warum Windows 7 diese Funktion abschaltet, wenn es auf einer SSD installiert ist. Der Geschwindigkeitsgewinn wäre nur marginal und die



Wenn man mit dem Forensik-Linux einen PC untersuchen will, muss man das zu untersuchende Laufwerk zuerst einbinden.

eventuell reduzierte Lebensdauer des Datenträgers nicht wert. Anwender können den Ordner also unbesorgt gelegentlich leeren oder sogar den Prefetch über Registry-Änderungen abschalten.

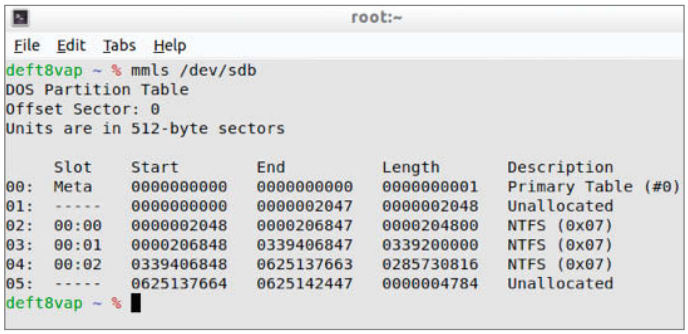
Gelöscht, aber nicht weg

Praktisch alle aktuellen Dateisysteme verzichten schon aus Gründen der Geschwindigkeitsoptimierung darauf, Daten beim Löschen komplett zu vernichten beziehungsweise zu überschreiben. Der ungenutzte Bereich einer Festplatte ist damit ein wahrer Datenschatz für jeden Forensiker.

Generell wird durch einen Löschvorgang nur das Inhaltsverzeichnis des Datenträgers modifiziert und so die Datei als „gelöscht" und der vorher belegte Datenbereich als „wiederverwendbar" gekennzeichnet. Das System benutzt diese Speicherbereiche erst, wenn wieder Daten auf den Datenträger geschrieben werden müssen. Je nach Dateisystem wird bei künftigen Schreibvorgängen auch zunächst der noch nie genutzte Platz bevorzugt, weil die gelöschten Dateien ja von bereits anderweitig genutzten Blöcken umgeben sind und somit eine Fragmentierung der neu anzulegenden Dateien droht. So ist es nur eine logische Folge, dass gerade auf sehr großen Festplatten noch erstaunlich viele eigentlich gelöschte Dateien wiederherstellbar sind, weil sie nicht durch neue oder geänderte Dateien überschrieben wurden.

An dieser Stelle sei auch noch mit einem anderen Gerücht aufgeräumt: Wenn ein Block auf einer herkömmlichen Festplatte dann doch einmal überschrieben wurde, sind die zuvor gespeicherten Daten verloren. Sie lassen sich durch Restmagnetisierung oder ähnliches Voodoo aus Floppy-Disk-Zeiten nicht wiederherstellen. Ob allerdings das Überschreiben einer Datei wirklich alle Blöcke der Festplatte löscht, die deren Daten enthalten hatten, ist ein ganz anderes Thema.

Für die Wiederherstellung von gelöschten Daten gibt es eine Menge Tools mit teilweise sehr speziellen Fähigkeiten. Eines der bekanntesten und am leichtesten bedienbaren ist PhotoRec. Um es zu benutzen, benötigt man in der Regel eine separate USB-Festplatte, da bei einem Komplettdurchlauf sehr schnell viele tausend Dateien gefunden und dann auch geschrieben werden. Sorgen Sie also dafür, dass auf dem Zielmedium reichlich Platz zur Verfügung steht.



Kommandozeilen-Tools wie mmls geben nützliche Hintergrundinformationen etwa zur Aufteilung der Festplatte.

Am einfachsten startet man das Tool via „photorec" von der DEFT-Kommandozeile und spezifiziert in den folgenden Menüs Quelle und Ziel der Operationen. Will man ein Image einer Festplatte als Quelle nutzen, muss man das direkt beim Start angeben:

```
photorec ./sample01.e01
```

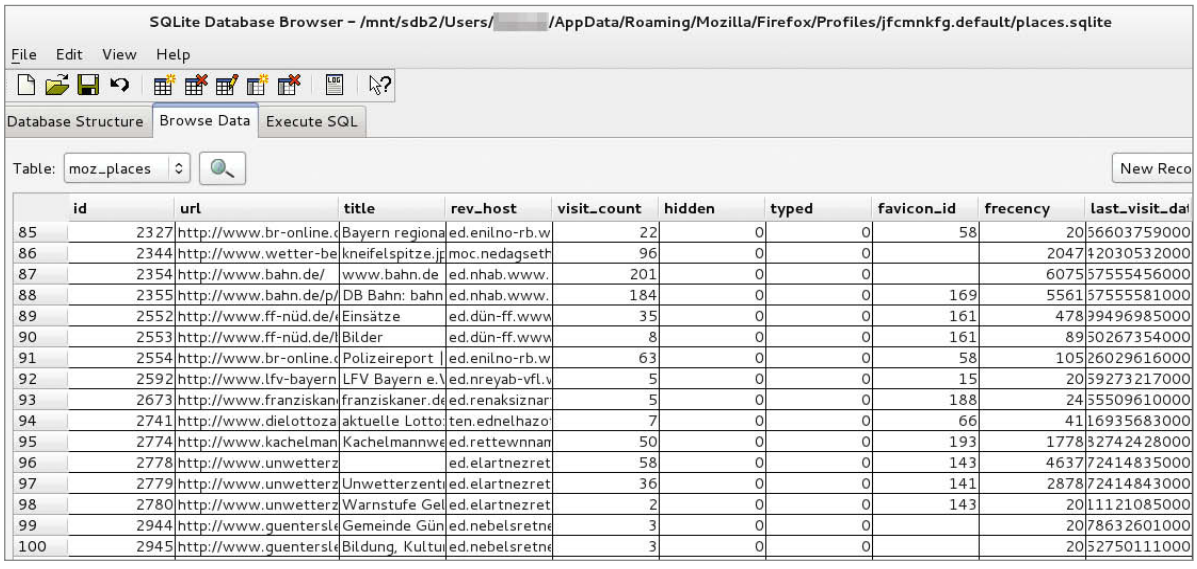
Das Programm wird über ein einfaches, textbasiertes Menü gesteuert, das fast komplett mit den Pfeiltasten Hoch/Runter und Links/Rechts bedient werden kann. Man sollte sich hier übrigens von der etwas altbackenen Optik nicht täuschen lassen: PhotoRec ist eine sehr leistungsfähige Wiederherstellungssoftware auf technisch aktuellem Stand, die mit den meisten modernen Filesystemen umgehen kann.

Es gibt einige kommerzielle Werkzeuge, die gerade bei hochgradig fragmentierten Festplatten eine etwas bessere Wiederherstellungs-Quote erzielen. Doch diese kosten dann meist auch gleich richtig Geld. Hinzu kommt, dass auch der Preis der Software keine guten Ergebnisse garantiert. Oft liegen auch hier Werbeversprechen und Realität weit auseinander.

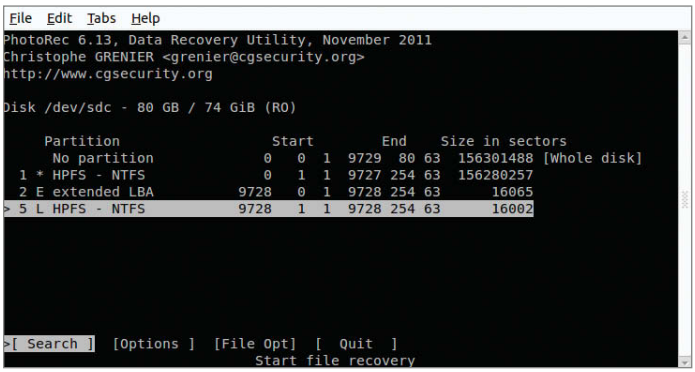
Zusammenfassend ist PhotoRec ein exzellentes Allround-Tool zur Datenrettung, das auch keineswegs – wie der Name nahelegt – auf die Wiederherstellung von Bilddateien beschränkt ist. Welche Dateien es retten soll, kann man unter „File Opt" einstellen. Eine Beschränkung auf Bild-Dateien kann die Suche deutlich beschleunigen und reduziert natürlich auch die produzierte Datenmenge. Um die weiter zu beschränken, empfiehlt es sich auch, die Suche nicht über die gesamte Festplatte, sondern nur über einzelne Partitionen und dort nur den jeweils freien Bereich laufen zu lassen. Sonst findet das Tool nämlich auch alle Dateien erneut, die gar nicht gelöscht wurden.

Nach der abschließenden Auswahl des Ordners, in dem die wiederhergestellten Daten abgelegt werden sollen, beginnt der Suchlauf. Er kann – je nach Größe des Datenträgers, Inhalt der Partition und Umfang der zu suchenden Dateitypen – durchaus einige Stunden dauern.

Die eigentliche Herausforderung ist es, nach einem Wiederherstellungslauf die tatsächlich relevanten Daten zu extrahieren. Auch Forensik-Profis sehen sich regelmäßig mit dem Problem konfrontiert, die Stecknadel im Heuhaufen – oder eben das eine beweiskräftige Bild unter Zehntausenden zu finden.



Die Browser-Historie bietet tiefe Einblicke in die Aktivitäten des Nutzers. Der direkte Zugriff auf die Datenbank erlaubt sehr gezielte Suchen.



Der Name und das antiquierte Aussehen täuschen: PhotoRec ist eines der besten Werkzeuge zur Wiederherstellung von Dateien aller Art.

Eine systematische Auswertung wird dadurch erschwert, dass PhotoRec die Dateien ohne Sortierung über viele Unterverzeichnisse verteilt. Hilfreiche Informationen wie Dateinamen oder Zeitstempel sind bei den ehemals gelöschten Dateien ebenfalls nicht mehr vorhanden. Zudem kommt aufgrund der verwendeten Algorithmen teilweise sehr viel Schrott heraus – also zum Beispiel Dateien, die rein technisch betrachtet wie eine Bilddatei aussehen, tatsächlich aber keine wirklich sinnvollen Bildinformationen enthalten.

Also muss man sich mit anderen Kriterien behelfen. Für eine erste Sortierung liefert DEFT das Tool photorec-sorter mit, das die bunt durcheinander wiederhergestellten Dateien zumindest pro Typ in ein Verzeichnis sortiert. Bei Bilddateien hat es sich darüber hinaus bewährt, dass man anhand von Metadaten wie Bildgröße, bestimmten EXIF-Daten oder auch Dateigröße eine intelligente Vorsortierung vornimmt, um nicht jedes einzelne Bild tatsächlich anschauen zu müssen. Der Befehl

```
find . -iname \*.jpg -size 4k -exec mv {} ../minis \;
```

macht kurzen Prozess und verschiebt alle JPEG-Dateien unter 4 KByte in den Ordner minis, den man zuvor angelegt haben muss.

Dabei kann auch das Fehlen bestimmter Metadaten ein brauchbares Ausschlusskriterium sein, wenn man etwa nach Fotos sucht, die von einem Smartphone stammen. Auf diese Informationen kann man etwa in einem einfachen Shell-Skript mit dem Kommandozeilen-Werkzeug exiftool zugreifen.

Wer die Bilder direkt sichten möchte, kann zum Beispiel die Linux-Bilderverwaltung Shotwell via

```
apt-get update
apt-get install shotwell
```

nachinstallieren und dort den Ordner mit den Bildern importieren. Dabei sollte man die Option „import in place“ auswählen, um keine neuerlichen Kopien zu erstellen. Shotwell erstellt dann unter anderem automatisch eine Timeline, mit der man sich recht schnell einen Überblick über wichtige und durch Fotos dokumentierte Ereignisse im Leben des Computer-Benutzers verschaffen kann.

Profi-Tools bieten darüber hinaus noch weitere Sortierfunktionen wie die Möglichkeit, Dateien anhand eines Abgleichs ihrer Hash-Werte gegen eine Datenbank bekannter Dateien auszusortieren. Damit fallen etwa die ganzen Dateien des Betriebssystems schon mal weg.

Letztendlich bleibt aber trotz aller Automatisierungsbemühungen ein bestimmtes Maß an manueller Arbeit übrig, um die Relevanz der Informationen im Kontext zu bewerten. So haben etwa auch die verfügbaren Programme zur Sortierung, die dann etwa auch automatisiert pornografische Szenen erkennen sollen, noch einiges Potenzial für Verbesserungen.

Alternativen und Auswege

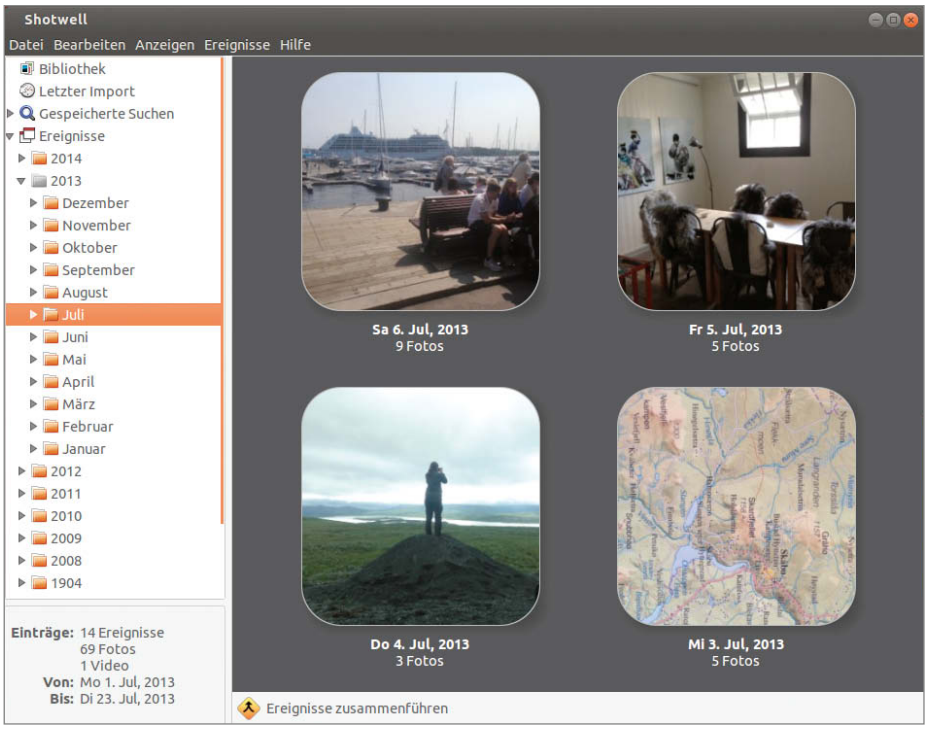
Dieses Tutorial ist nur ein Einstieg in die forensische Analyse einer Festplatte. DEFT hält noch viele weitere Tools bereit, mit denen man zum Teil erstaunliche Dinge zu Tage fördern kann. Gehen Sie doch einfach mal im Start-Menü auf Entdeckungsreise. Und wenn Sie sich unter Linux nicht so richtig wohlfühlen oder DEFT auf Ihrem System nicht starten will, versuchen Sie es mal mit den im folgenden Artikel vorgestellten Tools, die Sie direkt unter Windows nutzen können.

Abschließend stellt sich natürlich noch die Frage, wie man verhindern kann, dass ein Unbefugter die Daten eines Datenträgers so einfach auslesen und interpretieren kann. Prinzipiell hat man natürlich die Möglichkeit, viele der Spuren, die dieses Tutorial analysiert, ganz zu vermeiden. So könnten Sie Ihren Browser nur im privaten Modus benutzen und damit verhindern, dass er eine Verlaufsliste, Cookies und andere verräterische Dinge speichert. Aber das bedeutet dann auch, dass Sie jede URL jedes Mal neu eingeben müssen, weil Sie ja keine Lesezeichen haben und die Autovervollständigung ebenfalls wegfällt.

Ähnliches trifft auf viele der verräterischen Spuren zu: Eigentlich sind die Informationen im Alltag sehr nützlich und man will nicht auf sie verzichten. Ganz davon abgesehen, dass man seine Lebenszeit nicht damit verschwenden will, bei jedem einzelnen Programm herauszufinden, welche Spuren es möglicherweise hinterlässt und wie man ihm das abgewöhnt. Auch die Tools, die einem das angeblich abnehmen, bleiben bestenfalls Stückwerk.

Letztlich ist die einzig wirklich effiziente Methode, sein auf dem PC gespeichertes Privatleben vor dem Zugriff Dritter zu schützen, eine Komplettverschlüsselung der gesamten Festplatte. Unter Mac OS X und Linux gehört das längst zu den Standardfunktionen des Betriebssystems; Microsoft beschränkt das leider immer noch auf die professionellen und somit teureren Windows-Versionen. Da kann dann Truecrypt – oder hoffentlich bald ein Nachfolger – in die Bresche springen. (ju)

c't Zusatz-Tools unter: ct.de/y27h



Mit einer Bildverwaltung wie Shotwell kann man sehr schnell wichtige Ereignisse im Leben des PC-Besitzers finden.

Heiko Rittelmeier

Wer ist Miriam?

Ein ganz normaler PC unter der Lupe

Um ein Gefühl für die Brisanz des Themas zu bekommen, haben wir den Forensiker Heiko R. beauftragt, einen ganz normal genutzten PC forensisch zu untersuchen. Er schildert, wie viele Informationen er über die Besitzerin herausgefunden hat – mit minimalem Aufwand.

Für den Test bekomme ich ein Image von ungefähr 320 GByte. Es enthält zwei interessante Partitionen, vermutlich eine für das Betriebssystem und eine für die Daten. Mein Mittel der Wahl ist in diesem Fall Autopsy unter DEFT Linux: Ich erstelle einen neuen Case und importiere das Image. Ein erster Blick auf die erste Partition lässt mich vermuten, dass es sich bei dem Computer um einen Rechner mit Windows XP handelt. Der nächste Blick gilt dem Ordner „Dokumente und Einstellungen“: Dort gibt es einen Ordner „miriam“ (Name geändert).

Das nächste Ziel ist der Desktop-Ordner; auf den ersten Blick sticht mir eine Datei „adressen_firma.xls“ ins Auge, die anscheinend gelöscht wurde. Die Wiederherstellung kostet einen Klick. Es handelt sich um eine Excel-Tabelle mit Kontaktdaten von Kollegen, teilweise inklusive privater Nummern und Adressen.

Auch Miriam findet sich darin – mit vollem Namen, Geburtsdatum und Privatadresse. Die Dame ist wohl verheiratet, denn es gibt eine zweite Mailadresse von web.de mit anderem Nachnamen. Ihre Aufgabe in der Firma kenne ich jetzt auch – eine ideale Grundlage für gezieltes Phishing.

„Miriam ist verheiratet.“

Ein Dokument namens „Anamnesebogen.pdf“ weckt mein Interesse. Es handelt sich um ein leeres Formblatt, das aus dem Internet heruntergeladen wurde. Darauf deutet jedenfalls ein Alternate Data Stream „Zone Identifier“ hin. Der Inhalt „ZoneId=3“ zeigt, dass die Datei aus dem Internet stammt. Zwei gelöschte Dokumente „Eheurkunde.(xxx)“ lassen sich spontan nicht wiederherstellen, das würde mit anderen Werkzeugen möglicherweise trotzdem funktionieren.

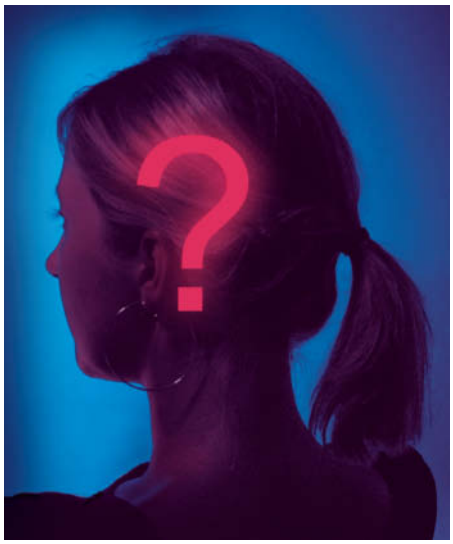
Zumindest zeigt mir die eingescannte Teilnahmebescheinigung einer Fortbildungsveranstaltung, dass ihr Mann „Mark“ heißt (auch hier: Name geändert) und mit Gebäudeplanung zu tun hat. Der Rest der Dateien auf dem Desktop interessiert mich gerade nicht (vorwiegend Kochrezepte).

Ihre privaten Mails liest Miriam anscheinend mit Thunderbird, größere Datendateien sind erkennbar. An der Stelle höre ich auf, ich bin schließlich kein Stalker. Ich finde zumindest keinen Hinweis darauf, dass ich die E-Mails nicht lesen kann. Auch das (vermutlich gespeicherte) Passwort des Mail-Accounts werde ich nicht versuchen auszulesen. Nach diesem ersten Überblick wende ich mich der zweiten Partition zu.

Die Benutzerin scheint Sinn für Ordnung zu haben, alles ist fein säuberlich thematisch in Unterordner eingruppiert.

„… singt im Chor.“

In der nächsten Ebene ist wieder ein Verzeichnis „miriam“ enthalten, darunter eines, das mich besonders interessiert: „BERUF“. Darin finde ich – schön sortiert – Unterlagen zu allen bisherigen und dem aktuellen Arbeitgeber.



Dabei Bewerbungen, Arbeitsverträge, Tabellen mit den gezahlten Gehältern. Der Scan einer Bescheinigung zum Mutterschutz deutet darauf hin, dass die Familie um (mindestens) ein Mitglied gewachsen ist. Ich finde einen Ex-Arbeitgeber aus der Finanzbranche, dazu eine Versicherung und Hinweise auf ein Auslandsstudium.

Der nächste Ordner, dem ich mich zuwende, heißt „SCANS“. Ein Fahrzeugschein verrät mir, wann „Mark“ (der Ehemann) Geburtstag hat. Der Scan der Eheurkunde vervollständigt meinen Überblick über die Familie: geheiratet wurde 2009 in Bremen, Mark kommt aus dem hohen Norden, Miriam eher nicht.

Im Verzeichnis „Outlook“ finde ich mehrere PST-Dateien. Die Größe lässt vermuten, dass da einiges Interessantes drinstecken könnte. Ich lasse auch hier die Finger davon. Eine Datei „Kontakte Verlobung.csv“ liefert mir trotzdem einen Einblick in Miriams Bekanntenkreis.

Außerdem scheint sie in einem Chor zu singen (Stimme „Alt“). Von den restlichen Chormitgliedern kenne ich jetzt auch die Stimmlage, Geburtstage, die privaten Telefonnummern und von vielen auch die Handynummer.

Interessant ist auch das Verzeichnis „WISO Sparbuch“: Es enthält die Steuererklärung eines Jahres (gemeinsame Veranlagung, ein Kind). Ob die Dateien der verschiedenen erkennbaren „WISO“-Versionen passwortgesichert sind, werde ich nicht testen. Zielloses Stöbern in den Dokumenten (teils gelöscht, teilweise nicht) zeigt mir, dass Miriam im Gemeinderat ihrer methodistischen Kirchengemeinde aktiv ist.

Ich beschließe, mich dem Verzeichnis „Bilder“ nur sehr oberflächlich zu widmen. Ich befürchte, dass auch dort viel Privates zu finden sein wird. Ein Bild „Miriam5.jpg“ zeigt eine hübsche Frau mit halblangen blonden Haaren. Auf einem anderen Bild ist sie zwar braunhaarig, auf der Mehrzahl der Bilder aber blond. Ich beschließe, dass mich das gelöschte Bild „Miriam in Badewanne.jpg“ nicht interessiert. Zu Testzwecken lasse ich PhotoRec über die freien Bereiche nach gelöschten Bilddateien suchen. Neben etlichen fehlerhaften Dateien zeigt die Vorschau auch noch deutlich mehr Fotos aus dem privaten Umfeld: Urlaubsfotos, Bewerbungsfotos, Bilder von privaten Feiern und Familienfesten. Portraits von allen möglichen Leuten. Bilder vom bunt bemalten Babybauch, Bilder nach der Geburt, beim Babyschwimmen, beim Stillen. Ein Bild oben ohne am Strand. Nichts, was irgendwie verwerflich wäre. Aber auch nichts, was einen Fremden wie mich irgendetwas angeht.

„… verdient jetzt mehr.“

Ich habe mich jetzt nicht einmal eine Stunde mit dem Image des Datenträgers befasst und fühle mich nicht mehr wohl mit dem, was ich schon jetzt weiß. Ich beschließe deshalb, den Fall an dieser Stelle zu schließen und das Image zu wipen.

Auch für mich als Forensiker war das ein spannendes Experiment, denn üblicherweise interessiere ich mich nicht für die Person, die einen Computer besessen hat. Es war erstaunlich, wie schnell ich mir dabei ein relativ gutes Bild von der Persönlichkeit des Computernutzers verschaffen konnte. Ein Krimineller, der bewusst noch tiefer einsteigt, fände problemlos Anknüpfungspunkte für weitere Aktionen: Phishing bei Arbeitskollegen oder Bekannten, Informationen über Konten und vorhandenes Vermögen, etc. Grund genug, seinen Computer nicht aus der Hand zu geben und dafür zu sorgen, dass auch dann nichts passieren kann, wenn das Gerät doch mal verloren geht. (ju) c't

Heiko Rittelmeier, Jürgen Schmidt

Unter die Haube geschaut

Spurensuche mit speziellen Windows-Tools

Will DEFT nicht booten, ist die Festplatte verschlüsselt oder man hat schlicht keine Lust auf Linux-Frickelei, kommt die Tool-Sammlung DART zur Rettung. Deren Programme laufen ohne Installation direkt unter Windows und fördern viele spannende Informationen zutage.

Das „Digital Advanced Response Toolkit", kurz DART, ist eine Sammlung von hochspezialisierten Tools, die ein laufendes Windows analysieren. Die aktuelle Version v2-2014 können Sie von www.deftlinux.net/files/dart/ herunterladen und beispielsweise mit Winzip entpacken. Dabei wird ein Verzeichnis „dart" angelegt; dort starten Sie einfach das Menü-Programm dart.exe.

Vorab jedoch eine Warnung: Manche Antiviren-Programme schlagen Alarm, wenn sie die DART-Tools sehen. Das hat zumindest eine gewisse Berechtigung. Wenn nämlich ein Programm wie **WirelessKeyView**, das die von Windows gespeicherten WLAN-Passwörter ausliest, ohne Ihr Wissen auf dem PC gelandet ist, dann geht da wahrscheinlich etwas Böses vor sich. Die Tools sind jedoch gut untersucht und es gibt keine Hinweise darauf, dass sie über den dokumentierten Einsatzzweck hinaus heimliche Zusatzfunktionen aufweisen, die einen Trojaner-Vorwurf begründen. Es besteht also kein Grund zur Panik – Sie können diese Warnung ignorieren und die Tools ohne Gefahr benutzen.

Als Erstes warnt DART deutlich, dass die Tools unter Umständen das untersuchte System verändern. Das richtet sich vor allem an Forensiker, die bei einem Einsatz auf einem echten System wichtige Spuren vernichten oder unbrauchbar machen könnten. Aber keines der im Artikel vorgestellten Tools nimmt ungefragt Änderungen an Ihrem System vor; im praktischen Einsatz ergaben sich bei uns keine Probleme. Das heißt zwar nicht, dass man damit keinen Schaden anrichten kann. Aber auch mit einem Schraubenzieher kann man sich ein Auge ausstechen.

Nach der Bestätigung, dass man das akzeptiert, muss man noch einen Ordner festlegen, in dem die gesammelten Erkenntnisse landen sollen – etwa ein neu angelegter namens DART auf dem Desktop ist bequem; besser ist es jedoch, diese Daten extern auf einem USB-Stick zu speichern.

Anschließend lädt eine bunte Oberfläche zum Stöbern ein. In den DART-Menüs findet sich jeweils eine kurze, englische Beschreibung zu jedem Programm. Darunter kann man via „Reveal" den zugehörigen Ordner im Explorer öffnen. Außerdem kann man das Tool über zwei Knöpfe direkt starten – wahlweise als der angemeldete Benutzer oder mit den erweiterten Zugriffsrechten eines Administrators. Letzteres führt zu einer Nachfrage durch Windows, ob man dem Programm gestatten möchte, Änderungen am System vorzunehmen. Manche Tools benötigen diese Rechte zwingend, um auf die zu untersuchenden Ressourcen zugreifen zu können.

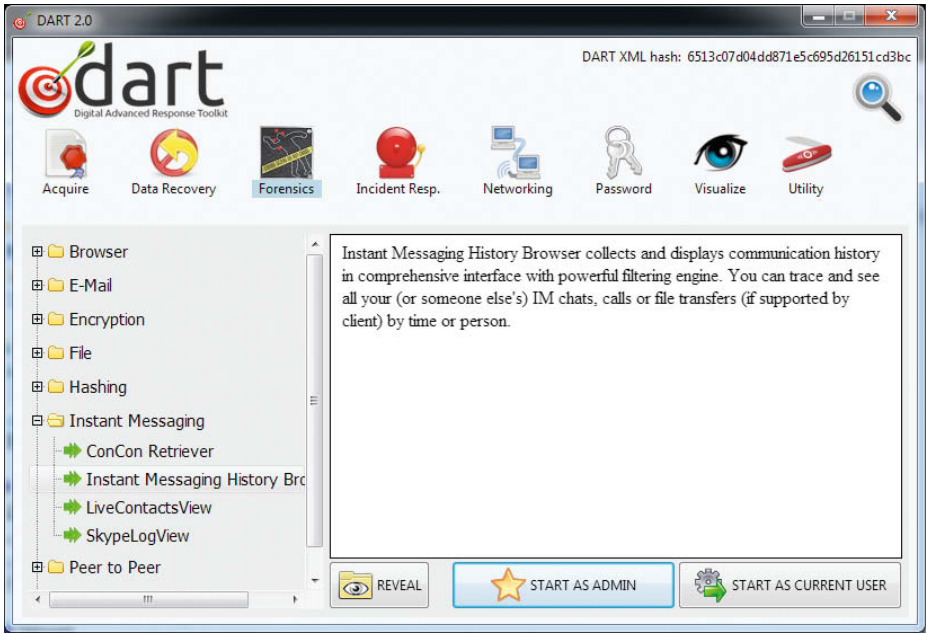
Browser-Geheimnisse

Die interessanteste Rubrik ist „Forensics“. Dort versammeln sich die Tools zur gezielten Spurensuche. Die erste wichtige Anlaufstelle einer Analyse ist oft die Internet-Nutzung, also die vom Browser bereitgestellten Informationen. Dazu finden sich in DART spezielle Tools wie **FirefoxDownloadsView** und **IECacheView**, um Verlauf, Downloads, Lesezeichen und Cookies von Internet Explorer, Firefox, Safari und Chrome zu sichten.

Besonders effizient ist der **Browser History Spy**, der den Verlauf von Firefox, Chrome und IE präsentiert – inklusive der Anzahl der Besuche und der Zeitstempel des letzten. Leider kann man darin nicht gezielt suchen. Das ist die Spezialität des **Browser Forensic Tool**, das den Verlauf aller gängigen Browser parallel nach Schlagwörtern durchsucht. Nur bei Opera erscheinen wohl aufgrund eines Fehlers derzeit keine Ergebnisse (der Entwickler ist benachrichtigt). Man kann auch mehrere Begriffe zu einem Profil zusammenfassen; eine Reihe englischer von „anonymous“ über „junky“ bis „porn“ sind bereits eingerichtet.

VideoCacheView liefert Einblicke in den Medien-Konsum der Computer-Nutzer. Da tauchen die gestreamten Youtube-Videos genauso auf wie die im Browser angehörten Podcasts. Ob eine Datei nach der Übertragung beziehungsweise Anzeige im Browser im Cache zwischengespeichert wird, ist von der verwendeten Übertragungstechnik und diversen Systemeinstellungen abhängig; bei einem nicht speziell konfigurierten System ist dort erstaunlich viel zu finden. **WebCacheImageInfo** spezialisiert sich auf zwischengespeicherte Bilder; **FBCacheView** sogar auf solche aus Facebook.

Natürlich enthält DART auch Programme wie **MailView**, um Outlook Express, Windows (Live) Mail und Thunderbird ihre gespeicherten Daten zu entreißen. Fast noch spannender sind jedoch die Instant-Messaging-Tools. So bereitet **SkypeLogView** die Skype-Aktivitäten in einer übersichtlichen Tabelle auf.



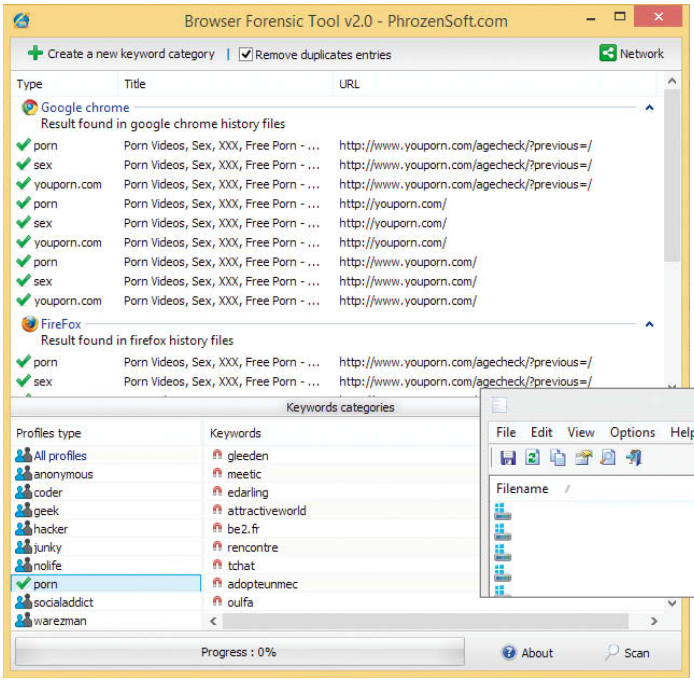
DART präsentiert zu jedem Programm eine kurze Beschreibung und die Möglichkeit, es direkt zu starten.

Nutzungsverhalten

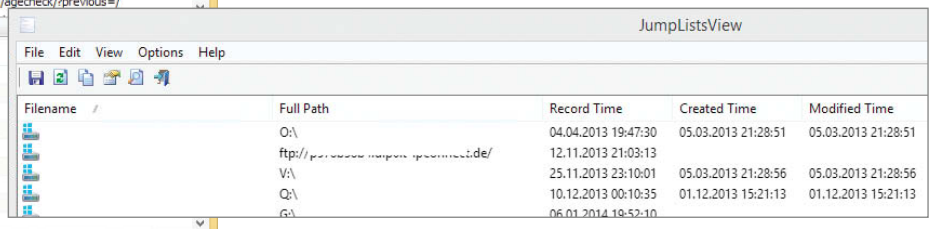
Vor allem Laien erstaunt es oft, wie genau Profis nachträglich die Nutzung eines Computers dokumentieren können. Basis dieser Analysen sind die sogenannten Jumplists, die Microsoft mit Windows 7 eingeführt hat. Sie enthalten für jede Anwendung die zuletzt damit geöffneten Dateien. Das ermöglicht Komfort-Funktionen für den Anwender – und dem Forensiker tiefe Einblicke.

Das Tool **JumpListsView** unter „Windows Forensics“ liest diese Sprunglisten aus und präsentiert sie in einer übersichtlichen Tabelle, die es auf Wunsch in eine HTML-Datei exportiert. Die Menge der damit verfügbaren Daten ist enorm; auf einem normalen Arbeitsplatz-PC fanden sich etwa 3500 Einträge, die fast eineinhalb Jahre zurückreichten. Darunter befanden sich nicht nur die geöffneten Dokumente, sondern auch Links zu FTP-Servern, in denen teilweise sogar Zugangsdaten enthalten waren.

Übrigens speichert Windows auch, wann der Benutzer welche Ordner im Explorer geöffnet hat. Es sichert nämlich jedes Mal die gewählten Optionen für die Explorer-Ansicht in der Registry unter HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags. Besonders interessant: Diese Einträge verschwinden nicht etwa, wenn ein Verzeichnis gelöscht wurde, sondern sie dokumentieren deren Existenz manchmal noch Jahre später. Die Auswertung der Registry-Einträge selbst ist hässlich und kompliziert, aber das Tool **ShellBags-**



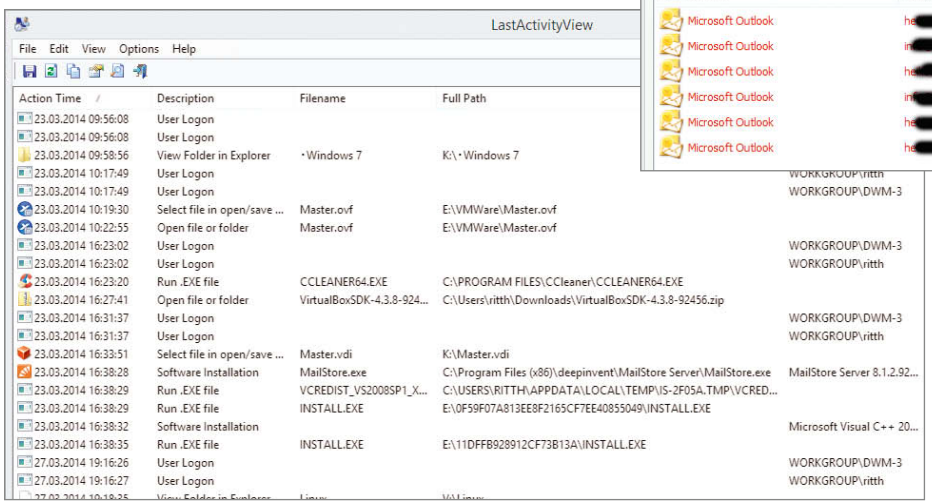
„The Internet is for Porn“ singt eine zynische Puppe im Musical Avenue Q – das Browser Forensic Tool kann das belegen.



In der sogenannten JumpList der zuletzt geöffneten Dokumente finden sich häufig auch Links zu FTP-Servern.

Gespeicherte Passwörter für Mail-Zugänge sind bequem – aber auch ein Sicherheitsproblem. Jedes Programm kann sie auslesen.

LastActivityView erstellt ein Nutzungsprofil, das beängstigend detailliert ausfällt.



View bringt die interessanten Informationen mit wenigen Mausklicks zum Vorschein.

Interessieren speziell die An- und Abmeldevorgänge – eventuell auch aus dem Netz –, sei ein Blick auf **WinLogonView** empfohlen, das diese Informationen aus dem Windows EventLog extrahiert und übersichtlich aufbereitet.

Und richtig unheimlich wird es, wenn **LastActivityView** die Sprunglisten damit kombiniert, wann welches Verzeichnis im Explorer geöffnet wurde, Installationsvorgänge anzeigt und zusammen mit allen An- und Abmeldevorgänge am System in einer Tabelle aufbereitet. Bei einer realen Untersuchung stellte das Tool über 3600 Einträge aus einem Dreivierteljahr zusammen – damit war der gläserne Computer-Nutzer perfekt.

Wer übrigens glaubt, er habe seinen verschlüsselten Truecrypt-Safe quasi unsichtbar als mp4-Datei in seiner Videosammlung vor dem Zugriff durch Fremde versteckt, der starte doch mal **TCHunt** unter „Encryption“. Das analysiert Dateien schnell und gezielt und liefert mit sehr hoher Trefferquote alle möglichen Truecrypt-Container-Dateien zurück. Dann fehlt allerdings immer noch das Passwort.

Passwörter

Apropos: Wer Passwörter auf dem PC speichert, riskiert zwangsläufig, dass sich Schädlinge oder Fremde, die sich Zugang verschaffen, diese Geheimnisse unter den Nagel reißen. So ist es durchaus lehrreich, mit den Tools in der Kategorie „Password“ mal zu stöbern, was auf dem eigenen PC so zu finden ist. Und wer hat sich noch nie gewünscht, durch die dummen Knödel bei der Passwort-Eingabe hindurchsehen zu können, um das gespeicherte, aber gerade deshalb vergessene WLAN-Passwort ablesen zu können? **WirelessKeyView** ftw („for the win“ – Internet-Slang für „Ziel erreicht“).

Die Firma Nirsoft hat eine umfangreiche Sammlung von kleinen Tools veröffentlicht, die neben Windows selbst auch alle möglichen Programme abdeckt, die Passwörter zumindest optional speichern. Da finden sich dann Spezialisten wie **Access PassView**, **PasswordFox**, **PCAnyWhere PasswordView**, **VNCPassView** und **PSTPasswordView** für Outlook-Dateien. Andere Programme beherrschen ganze Kategorien wie **RouterPassView**, **MailPassView** oder **MessenPass**. Manche Tools unterstützen jedoch nur bestimmte Versionen; ob das jeweilige Programm bei Ihnen funktioniert, wird von der genauen Version der jeweils eingesetzten Software abhängen.

Gemein ist den Nirsoft-Tools, dass sie keine Passwörter knacken, sondern nur ungesicherte Passwörter zum Vorschein bringen. Das ist bei denen unter „SecurityXploded“ zumindest teilweise anders. Die decken zwar einen ähnlichen Bereich ab. So liest der **Mail Password Decryptor** die Konfigurationsdaten der gängigen Mail-Clients aus und stellt die dort gefundenen Zugangsdaten zu den Postfächern in einer übersichtlichen Tabelle zusammen. Doch Tools wie **WindowsPasswordKracker** & Co versuchen sich auch daran, diese mit Gewalt beziehungsweise anhand von Wörterbüchern zu erraten.

Gelingt dies bei einem vergessenen Windows-Anmelde-Passwort nicht, kann man das übrigens – mit einem Administrator-Zugang ausgestattet – via **Advanced Password Recovery** ganz einfach neu setzen.

Auch in den übrigen Kategorien finden sich teilweise noch spannende Tools, die einen zweiten Blick lohnen. In der Rubrik „Incident Response“ versammelt sich eine Reihe von Spezialwerkzeugen, die dabei helfen, einen Schädlingsbefall oder einen möglichen Einbruch ins System zu diagnostizieren. Einige von ihnen erfordern allerdings sehr gutes Expertenwissen. Dazu gehört auch ein kompletter Satz von Anti-Rootkit-Tools wie **Gmer** und **IceSword**.

Die Tools unter „Networking“ zeigen deutlich mehr über die Netzwerk-Aktivitäten von Programmen als Windows-Bordmittel. Interessant ist etwa **CrowdInspect**. Das holt zu allen Prozessen automatisiert Bewertungen von VirusTotal, dem Web of Trust und der Malware Hash Registry ein und sucht zusätzlich nach Anzeichen für nachträglich in einen Prozess eingeschleusten Code.

In der Rubrik „Aquire“ finden sich vor allem Werkzeuge zum Brennen von DVDs und dem Erstellen von Speicherabzügen – sowohl der Festplatte (**ForensicCopy**, **FastCopy**) als auch des Arbeitsspeichers (**RamCapture**, **PZenDump**). „Data Recovery“ versammelt eine Reihe von Datenrettungs-Tools, darunter Windows-Versionen des bereits bei DEFT vorgestellten **PhotoRec**. Auch der dort erwähnte **SQLite Database Browser** ist in einer Windows-Version unter „Visualize/Office“ mit an Bord.

Diese Präsentation von DART ist keineswegs vollständig, sondern konzentrierte sich bewusst auf ein paar subjektiv ausgewählte Highlights. Machen Sie sich doch mal selber auf die Suche nach interessanten Tools und berichten Sie uns von spannenden Entdeckungen. Dabei werden Sie unter Umständen auch auf den ein oder anderen leeren Eintrag im DART-Menü stoßen. Das liegt daran, dass manche Programme aus Lizenzgründen nicht direkt mit aufgenommen werden konnten. Die Datei TO-DO.txt gibt zusätzliche Hinweise, wie man manche Programme nachinstallieren kann.

Übrigens – apropos Spuren: DART hat Ihre Entdeckungsreise genau protokolliert. In dem Ordner, den Sie zu Beginn angegeben haben, liegt eine Datei, in der genau vermerkt ist, wie lange Ihre DART-Sitzung dauerte und wann Sie welches DART-Programm gestartet haben. (ju) c't