KAPITEL VIER

Digitale Spuren in Windows

Hacks #46-55

Als das am häufigsten eingesetzte Betriebssystem im Heim- und auch Unternehmensbereich ist Windows heute aus der Welt der Computer kaum wegzudenken. In der digitalen Forensik spiegelt sich das natürlich wider. Das Problem bei der Auswertung vieler Spuren besteht darin, dass viele systemeigene Fragmente proprietäre Formate nutzen, die teilweise gar nicht oder nur dürftig dokumentiert sind. Glücklicherweise existiert im Internet eine große Community von Forensikern, die sich in kleinen Blogposts, aber auch in umfangreicheren Artikeln über die Analyse bestimmter Fragmente von Microsofts Betriebssystem austauschen. Viele dieser Leute haben sich daran gemacht, undokumentierte Formate für die Analyse auseinanderzubauen und eigene kleine, spezifische Tools zur Untersuchung dieser Formate zu entwickeln. Ein paar dieser Tools empfehlen wir Ihnen in diesem Kapitel, wobei wir Ihnen auch direkt die Links zum einfachen Download bereitstellen.

Freuen Sie sich auf Hacks, die viele derjenigen Spuren analysieren, die Sie vielleicht aus Ihrem Alltag an einem Windows-PC kennen, z.B. der Papierkorb, die zuletzt verwendeten Dateien und die Vorschaubilder aus dem Explorer. Wie andere Betriebssysteme auch, hinterlässt Windows an vielen Stellen im System Fragmente, die Rückschlüsse auf Benutzerverhalten, Systemeinstellungen, gelöschte Dateien und Vieles mehr geben. Viel Spaß beim Stöbern!

- Sehen Sie, was gedruckt wurde [Hack #53]
- Stöbern Sie im Müll [Hack #54]
- Passwort vergessen? Kein Problem! [Hack #55]

HACK #46 Wichtige Verzeichnisse in Windows XP / Vista / 7

»VID – Very Important Directories«

Heutzutage existieren auf jedem Datenträger, auf dem ein Windows-Betriebssystem installiert ist, Abertausende von Dateien und Ordnern. Da fällt es einem manchmal schwer, die Übersicht zu behalten. Das ist der Grund dafür, dass Sie in diesem Kapitel eine Schnellübersicht über die wichtigsten Verzeichnisse in den Betriebssystemen Windows XP, Vista und 7 finden. So können Sie sich schnell auch auf einem fremden System zurechtfinden und wissen, in welchen Verzeichnissen Sie Ihre Spurensuche beginnen können.

Windows XP

Tabelle 4-1: Wichtige Verzeichnisse in Windows XP

Verzeichnis	Nutzen
C:\Dokumente und Einstellungen\BENUTZER\	Persönliches Verzeichnis eines Benutzers mit eigenen Daten und Ordnern *
C:\Dokumente und Einstellungen\BENUTZER\ Eigene Dateien\, Eigene Bilder\, Eigene Musik\ usw.	Dateien, die der Nutzer selbst dort abgelegt hat *
C:\Dokumente und Einstellungen\BENUTZER\Desktop\	Die Arbeitsoberfläche des Nutzers *
C:\Dokumente und Einstellungen\BENUTZER\Anwendungsdaten\ C:\Dokumente und Einstellungen\BENUTZER\Lokale Einstellungen\Anwendungsdaten\	Benutzerspezifische Konfigurationen und temporäre Dateien von Programmen *
C:\Dokumente und Einstellungen\BENUTZER\Cookies\	Cookies von besuchten Webseiten und Drittanbietern des Internet Explorer *
C:\Dokumente und Einstellungen\BENUTZER\Favoriten\	Von Benutzer oder Programmen angelegte Lesezeichen *
C:\Dokumente und Einstellungen\BENUTZER\Recent\	Zuletzt geöffnete Dateien des Benutzers *
C:\Dokumente und Einstellungen\BENUTZER\Temp\	Zwischengespeicherte Dateien, z. B. direkt geöffnete, ungespeicherte Dateien aus Browsern und anderen Programmen *
C:\Dokumente und Einstellungen\BENUTZER\Temporary Internet Files\	Zwischengespeicherte Webseiten des Internet Explorer *
C:\Dokumente und Einstellungen\BENUTZER\Verlauf\	Verlauf von Internet und Windows Explorer *
C:\Programme\	Standardordner für installierte Programme
C:\Windows\System32\config\	Speicherort für Registry-Dateien und Ereignisprotokolle

Tabelle 4-1: Wichtige Verzeichnisse in Windows XP (Fortsetzung)

Verzeichnis	Nutzen
C:\Windows\Prefetch	Eine Liste ausgeführter Programme mit Zusatzinformationen
C:\RECYCLER\	Die »entfernten« Dateien jedes Benutzers
C:\System Volume Information\	Restore Points

Windows Vista und Windows 7

Tabelle 4-2: Wichtige Verzeichnisse in Windows Vista und Windows 7

Verzeichnis	Nutzen
C:\Users\BENUTZER\	Persönliches Verzeichnis eines Benutzers mit eigenen Daten und Ordnern *
C:\Users\BENUTZER\ Documents\, Pictures\, Music\ usw.	Dateien, die der Nutzer selbst dort abgelegt hat *
C:\Users\BENUTZER\Desktop\	Die Arbeitsoberfläche des Nutzers *
C:\Users\BENUTZER\AppData\Roaming\ C:\Users\BENUTZER\AppData\Local\	Benutzerspezifische Konfigurationen und temporäre Dateien von Programmen *
C:\Users\BENUTZER\AppData\Roaming\Microsoft\Windows\Cookies\	Cookies von besuchten Webseiten und Drittanbietern des Internet Explorer *
C:\Users\BENUTZER\Favorites\	Vom Benutzer oder Programmen angelegte Lesezeichen *
C:\Users\BENUTZER\AppData\Roaming\Microsoft\Windows\Recent	Zuletzt geöffnete Dateien des Benutzers *
C:\Users\BENUTZER\ AppData\Local\Temp\	Zwischengespeicherte Dateien, z. B. direkt geöffnete, ungespeicherte Dateien aus Browsern und anderen Programmen *
C:\Users\BENUTZER\AppData\Local\Microsoft\Windows\Temporary Internet Files	Zwischengespeicherte Webseiten des Internet Explorer *
C:\Users\BENUTZER\AppData\Local\Microsoft\Windows\History	Speicherort für den Verlauf des Internet und Windows Explorer *
C:\Users\BENUTZER\AppData\Local\Microsoft\Windows\Explorer\	Thumbcache-Dateien mit Vorschaugrafiken
C:\Program Files\	Standardordner für installierte Programme
C:\Windows\System32\config\	Speicherort für Registry-Dateien
C:\Windows\Prefetch	Eine Liste ausgeführter Programme mit Zusatzinformationen
C:\$Recycle.bin\	Die »entfernten« Dateien jedes Benutzers
C:\System Volume Information\	Volumenschattenkopien
C:\Windows\System32\winevt\Logs	Speicherpfad für Ereignisprotokolle (Logdateien)

Natürlich handelt es sich bei diesen Tabellen nicht um abschließende Aufzählungen. Sie sollten die anderen Verzeichnisse eines Systems daher keinesfalls vernachlässigen.

Wenn Sie sich für weitere interessante Orte im Windows-Betriebssystem und in Webbrowsern interessieren, sollten Sie sich unbedingt die Hacks in diesem Kapitel und in Kapitel 6 ansehen.

*Zwar hat standardmäßig nur der Nutzer selbst Zugriff auf diese Verzeichnisse, aber durch Nutzung eines Administrator-Accounts oder Umgehung der NTFS-Berechtigungen können auch Dritte in diese Verzeichnisse schreiben.

HACK #47 Die Registry-Top-10

»Zentral gespeichert«

Mindestens genauso interessant wie die Dateien und Ordner im Dateisystem ist auf Windows-Systemen die Registry. Die Registry ist die zentrale Datenbank, in der das Windows-Betriebssystem und auch die meisten gängigen Anwendungen ihre Einstellungen speichern. Jedes Programm, das einmal auf dem Rechner installiert war, hinterlässt hier seine Spuren, denn nur die wenigsten Anwendungen löschen bei der Deinstallation ihre hinterlegten Informationen aus der Registry.

Die Registry ist hierarchisch strukturiert und besteht aus fünf Hauptschlüsseln (auch Wurzelschlüssel genannt):

- HKEY_CLASSES_ROOT (HKCR)
- HKEY_LOCAL_MACHINE (HKLM)
- HKEY_USERS (HKU)
- [HKEY_CURRENT_USER (HKCU)]
- [HKEY_CURRENT_CONFIG (HKCC)]

Die letzten beiden CURRENT-Schlüssel sind streng genommen keine eigenständigen Schlüssel, sondern lediglich Verweise, die während der Laufzeit des Systems gebildet werden. So verweist HKCU auf den entsprechenden Unterschlüssel von HKU, und HKCC verweist auf den entsprechenden Unterschlüssel von HKLM.

Alle Registry-Informationen werden beim Systemstart in den Arbeitsspeicher geladen, während des laufenden Betriebs dort gehalten und beim Herunterfahren in folgende Dateien auf die Windows-Partition geschrieben:

- C:\Windows\System32\config\SOFTWARE (= HKLM\Software)

- C:\Windows\System32\config\SYSTEM (= HKLM\System)
- C:\Windows\System32\config\SECURITY (= HKLM\Security)
- C:\Windows\System32\config\SAM (= HKLM\SAM)
- Windows XP:
  C:\Dokumente und Einstellungen\BENUTZER\NTUSER.DAT
  (= HKU\BENUTZER)

  Vista / 7:
  C:\Users\BENUTZER\NTUSER.DAT

  und

  C:\Users\BENUTZER\AppData\Local\Microsoft\Windows\USRCLASS.dat
  (= HKU\BENUTZER)

Diese Dateien treten in unterschiedlichen Formen auf. Ohne Dateiendung sind es die ursprünglichen, vollständigen Registry-Dateien. Mit der Endung *.log* sind es Dateien, die lediglich Änderungen von Registry-Werten enthalten. Mit der Endung *.sav* handelt es sich um Sicherungskopien der Ursprungs-Registry. Die Endung *.alt* taucht lediglich bei der Sicherungskopie der Datei *SYSTEM* auf.

Zum Betrachten dieser Registry-Dateien benötigt man spezielle Programme. In den einschlägigen Forensikprogrammen sind diese meist eingebaut oder als Zusatzkomponenten erhältlich. Als freie Produkte empfehlen wir für Windows den *RegistryViewer* (*http://www.forensikhacks.de/regview*) und für Linux *RegRipper* (*http://www.forensikhacks.de/regrip*).

Ihre eigene Registry können Sie übrigens mit dem Windows-eigenen Registry-Editor anschauen. Klicken Sie einfach auf START → AUSFÜHREN oder drücken Sie die Windows-Taste zusammen mit der Taste R und tippen Sie `Regedit` ein.

Obwohl die Registry eine echte Fundgrube für nützliche Informationen ist, sollten Sie bei Ihren Untersuchungen insbesondere die folgende Top 10 der Registy-Schlüssel im Auge haben.

Tabelle 4-3: Die Registry-Top-10

TOP	Registry-Schlüssel	Nutzen
1	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU HKCU\Software\Microsoft\Office\10.0\Word\Data HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU HKCU\Software\Microsoft\MediaPlayer\Player\RecentFileList	Zuletzt geöffnete Dateien, Ordner und Programme

Tabelle 4-3: Die Registry-Top-10 (Fortsetzung)

TOP	Registry-Schlüssel	Nutzen
2	HKLM\SOFTWARE\	Einstellungen für alle installierten Programme
3	HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation	Zeitzoneninformationen; wichtig, um Zeitstempel auf dem System richtig deuten zu können.
4	HKLM\SYSTEM\ControlSet00X\ Services\Tcpip\Parameters\Interfaces\	Netzwerk-einstellungen
5	HKLM\SYSTEM\MountedDevices	Gemountete Geräte, z. B. USB-Sticks oder verschlüsselte Container
6	HKLM\SYSTEM\ControlSet00x\Enum\USB HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR	Angeschlossene USB-Geräte
7	HKCU\Software\Microsoft\ Internet Explorer\TypedURLs	Eingegebene URLs im Internet Explorer
8	HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce HKLM\Software\Microsoft\Windows\CurrentVersion\policies\ Explorer\Run HKLM\Software\Microsoft\Windows\CurrentVersion\Run HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run HKCU\Software\Microsoft\Windows\CurrentVersion\Run HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce	Diese Programme werden beim Start des Betriebssystems automatisch gestartet. Insbesondere Schadsoftware nistet sich hier gern ein.
9	HKCU\Software\Microsoft\Internet Explorer\IntelliForms\SPW HKCU\Software\Microsoft\Protected Storage System Provider	Verschlüsselte Passwörter, die sich jedoch durch Secure Storage Viewer entschlüsseln lassen
10	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	Informationen über das Betriebssystem

HACK
#48

Ihre Goldgrube – MRU-Listen für alle Zwecke

»Ich weiß, was Du letzten Sommer getan hast.«

Nachdem Sie im vorigen Hack die Windows-Registry etwas besser kennengelernt haben, möchten wir Ihnen in diesem Hack eine Kurzübersicht über die wichtigsten Orte für »Most Recently Used«- (MRU-)Listen zur Verfügung stellen. Diese Listen können für Sie deshalb von großer Bedeutung sein, weil Sie mit ihrer Hilfe feststellen können, welche Dateien und Programme der Nutzer zuletzt verwendet hat, und welche Orte für ihn und somit potenziell auch für Sie interessant sein könnten. Die Listen können sogar Verweise zu längst gelöschten und überschrieben Ordnern beinhalten und erfassen geöffnete Dateien auch dann, wenn sie von externen und/oder verschlüsselten Medien aus aufgerufen wurden.

Tabelle 4-4: MRU-Listen

Ort	Nutzen
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	Zuletzt geöffnete Dokumente (Startmenü)
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	Im »Ausführen«-Dialog ausgeführte Programme
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU (XP) HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU (Vista/7)	Zuletzt gespeicherte und geöffnete Dokumente (über Common Dialog)
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU (XP) HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU (Vista/7) HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRULegacy (Vista/7)	Zuletzt besuchte Dokumente (über Common Dialog)
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\CIDSizeMRU HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\FirstFolder	Informationen über angepasste Fensterlayouts
HKCU\Software\Microsoft\MediaPlayer\Player\RecentFileList HKCU\Software\Microsoft\MediaPlayer\Player\RecentURLList	Vom MediaPlayer geöffnete Dokumente und URLs
HKCU\Software\Microsoft\Office\10.0\Word\Data HKCU\Software\Microsoft\Office\10.0\Excel\Recent Files HKCU\Software\Microsoft\Office\10.0\PowerPoint\Recent File List HKCU\Software\Microsoft\Office\10.0\Common\Open Find\Microsoft Access\Settings\File New Database\File Name MRU	Zuletzt in Office XP geöffnete Dateien
C:\Dokumente und Einstellungen\BENUTZER\Recent (XP) C:\Users\BENUTZER\AppData\Roaming\Microsoft\Windows\Recent (Vista/7)	Zuletzt geöffnete Dokumente des Benutzers
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths (Vista/7)	Im Explorer eingetippte Pfade
HKCU\Software\Microsoft\Internet Explorer\TypedURLs	Aufgerufene URLs des Internet Explorer
HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit	Zuletzt in Regedit geöffnete Dateien
HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List	Zuletzt in Paint geöffnete Dateien
HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\WordPad\Recent File List	Zuletzt in Wordpad geöffnete Dateien
HKCU\Software\Adobe\Acrobat Reader\VERSION\AVGeneral\cRecentFiles	Zuletzt im Acrobat Reader geöffnete Dateien
NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags	Informationen über die Darstellung von Verzeichnissen; können Aufschluss selbst über längst gelöschte und überschriebene Verzeichnisstrukturen geben.

HACK #49 Welche Programme wurden gestartet?

»Fahrtenbuch der Applikationen«

Wenn Sie wissen möchten, wie oft welches Programm auf einem Computer gestartet wurde, wann es zuerst und wann zuletzt aufgerufen wurde und welche Dateien zusammen mit der Anwendung geladen werden, sind Sie in diesem Hack genau richtig.

Das Windows-Betriebssystem speichert seit Windows XP Informationen über häufig ausgeführte Anwendungen in sogenannten *Prefetch*-Dateien: Die Idee dahinter ist, dass das Betriebssystem beliebte Programme schneller laden kann, wenn es schon im Vorfeld weiß, welche Bibliotheken und Hilfsdateien für dieses Programm mitgeladen werden müssen.

Diese *Prefetch*-Dateien, von denen maximal 128 gespeichert werden, finden sich standardmäßig im Verzeichnis *C:\Windows\Prefetch*.

Sie sind leicht an der Dateiendung *.pf* zu erkennen. Natürlich können sich auch in gelöschten Bereichen *Prefetch*-Dateien befinden. In den **Hacks [#29]**, **[#30]**, **[#34]** und **[#35]** erfahren Sie, wie Sie Daten aus solchen Bereichen wiederherstellen.

Für die Suche nach gelöschten Prefetch-Dateien empfehlen wir, nach folgenden Signaturen zu suchen:

`\x11\x00\x00\x00\x53\x43\x43\x41` für Windows XP

`\x17\x00\x00\x00\x53\x43\x43\x41` für Windows Vista / Windows 7

Wenn Sie sich schon einmal die *Prefetch*-Dateien auf einem System angesehen haben, ist Ihnen vielleicht aufgefallen, dass es für ein Programm mehrere Dateien mit der Endung *.pf* geben kann. Der Schein trügt hier jedoch, denn für ein und dasselbe Programm gibt es tatsächlich nur eine einzige Datei. Alle *.pf*-Dateien tragen neben dem Programmnamen auch noch vier Bytes an Hexwerten im Dateinamen. Wenn diese Hexwerte unterschiedlich sind, handelt es sich um eine andere Version der ausgeführten Datei, z. B. aus einem anderen Verzeichnis heraus oder nach einem Update.

Wie eingangs erwähnt, finden Sie wertvolle Informationen in *Prefetch*-Dateien. Hier einige Beispiele:

- Offset 0x10:
  Name der ausgeführten Datei
- Offset 0x78 (XP), 0x80 (Vista/7):
  Zeitstempel des letzten Aufrufs

- Offset 0x90 (XP), 0x98 (Vista/7):
  Anzahl der Aufrufe der Datei (Run Count)

Einen Indikator für die erste Ausführung des Programms gibt die Erstellungszeit der *Prefetch*-Datei.

Eine gute und effiziente Möglichkeit, um *Prefetch*-Dateien auszuwerten, stellt unter Windows das Programm *Windows File Analyzer (WFA)* dar. Es ist kostenlos unter *http://www.forensikhacks.de/wfa* erhältlich. Neben der Analyse von *Prefetch*-Dateien beherrscht *WFA* übrigens auch noch andere nützliche Funktionen, auf die wir in anderen Hacks zurückgreifen. Nach dem Entpacken von *WFA.exe* sollten Sie zunächst einmal alle *Prefetch*-Dateien, die Sie analysieren möchten, in einen Ordner auf Ihre Festplatte extrahieren. Danach starten Sie *WFA.exe* und klicken einfach auf FILE → ANALYZE PREFETCH. In der erscheinenden Dialogbox brauchen Sie nun nur noch das Verzeichnis auszuwählen, das die *Prefetch*-Dateien enthält. Mit der Tastenkombination *Strg+P* können Sie das Ergebnis ausdrucken oder an einen PDF-Drucker senden.

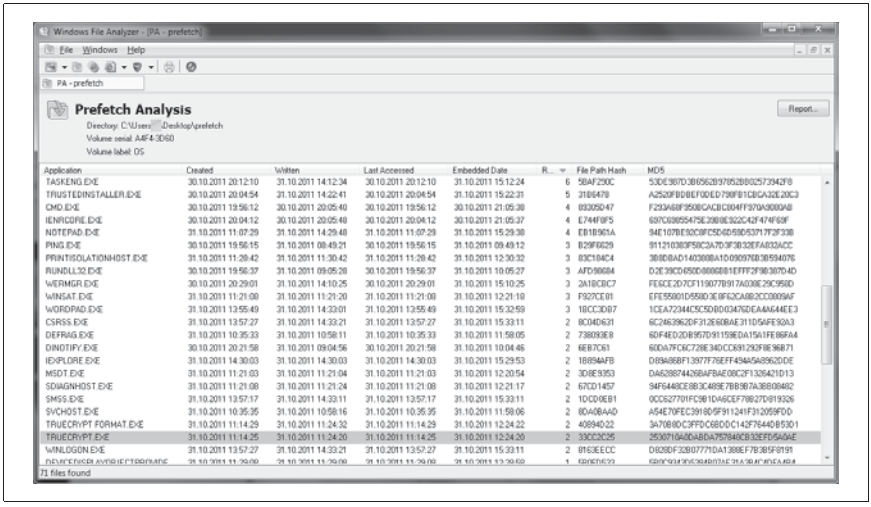

Abbildung 4-1: Prefetch-Auswertung mit Windows File Analyzer

Als weiteres Programm zur Analyse von *Prefetch*-Dateien empfiehlt sich der *Windows Prefetch Parser*, der sowohl unter Windows als auch unter Linux und Mac OS X funktioniert. Das kommandozeilenbasierte Tool kann unter *http://www.forensikhacks.de/prefetch* kostenlos heruntergeladen werden. Sobald Sie es auf Ihrem System entpackt haben, können Sie es einfach auf den Ordner ansetzen, der die extrahierten *Prefetch*-Dateien enthält, und zwar mit folgenden Kommandos:

unter Windows mit

```
dir c:\fall\export\prefetch\*.pf /b /s | pf.exe -v > prefetch.txt
```

und unter Linux mit

```
ls /home/user/fall/export/prefetch/*.pf | ./pf -m > prefetch.txt
```

Durch Abgleich der Run Counts von existierenden mit gelöschten Prefetch-Dateien können Sie sich für besonders interessante Programme eine Zeitleiste aufbauen. Wenn Sie z. B. die existierende Datei *TRUECRYPT.EXE-33CC2C25.pf* mit einem Run Count von 5 und einem letzten Ausführungsdatum am 03.03.2012, 12:00:00 Uhr UTC vorfinden und außerdem drei gelöschte *TRUECRYPT.EXE-33CC2C25.pf* mit unterschiedlichen Run Counts und Ausführungszeiten wiederherstellen können, verfügen Sie über eine komplette Dokumentation jeder einzelnen Ausführung des Programms. Eine mögliche Darstellung könnte aussehen wie in der folgenden Tabelle.

Tabelle 4-5: Zeitleiste für die Ausführung des Programms TrueCrypt

Prefetch-Datei	Ausführungszeit	Run Count
	(Erstellungszeit der Prefetch-Datei) 21.01.2012, 12:14:37 Uhr UTC	1
TRUECRYPT.EXE-33CC2C25.pf (gelöscht)	11.02.2012, 18:35:58 Uhr UTC	2
TRUECRYPT.EXE-33CC2C25.pf (gelöscht)	27.02.2012, 15:29:41 Uhr UTC	3
TRUECRYPT.EXE-33CC2C25.pf (gelöscht)	02.03.2012, 22:57:12 Uhr UTC	4
TRUECRYPT.EXE-33CC2C25.pf (existiert)	03.03.2012, 12:00:00 Uhr UTC	5

HACK
#50

So werten Sie Ereignisprotokolle aus

»Ein Log für alle Fälle«

Wann auch immer Sie wissen möchten, was zu einem bestimmten Zeitpunkt auf einem Computer passiert ist oder in welchem Zustand sich das System zu einem bestimmten Zeitpunkt befunden hat – Logdateien können Ihnen wertvolle Erkenntnisse zu diesen Fragestellungen geben. Unter Windows werden Logdateien als »Ereignisprotokolle« bezeichnet. Je nachdem, welche Version von Microsofts Betriebssystem Sie untersuchen, werden Sie auf unterschiedlich viele dieser Ereignisprotokolle treffen. Ob und wenn ja wann eine Aktion im Hintergrund mitprotokolliert wird, hängt nicht nur von der Betriebssystemversion ab, sondern auch von den eingestellten Gruppenrichtlinien. In diesem Hack gehen wir daher weniger auf bestimmte Logdateien oder Ereignisse ein, sondern geben Ihnen das notwendige Werkzeug an die Hand, um selbstständig die üblichsten Formen von Ereignisprotokollen untersuchen zu können.

Quo vadis, Ereignisprotokoll?

Bevor Sie mit der Auswertung von Ereignisprotokollen anfangen können, müssen Sie wissen, wo diese gespeichert werden. Alle Aktionen, die laut Systemeinstellungen überwacht und mitprotokolliert werden sollen, werden in Dateien auf die Festplatte des Computers geschrieben. Windows XP und Vista / 7 nutzen dabei standardmäßig folgende Pfade:

- Windows XP:
  c:\Windows\System32\config
- Windows Vista / 7:
  c:\Windows\System32\winevt\Logs

Natürlich können diese Standardpfade auch vom Benutzer verändert werden. Ob die Speicherpfade vom Standard abweichen, können Sie in folgendem Schlüssel der Windows Registry nachvollziehen:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog
```

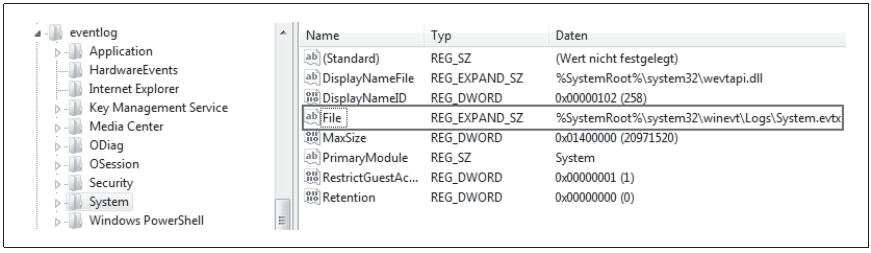

Abbildung 4-2: Für jedes Ereignisprotokoll ist der Speicherpfad in der Registry abgelegt.

Wenn Sie einen Blick in diese Verzeichnisse werfen, erkennen Sie die Ereignisprotokolldateien an den folgenden Dateiendungen:

- .evt Windows NT 3.1 bis Windows XP
- .evtx Windows Vista / 7
- .etl Event Trace Logs des Service *Event Tracing für Windows*

Die Protokolldateien von Windows XP und Vista / 7 unterscheiden sich nicht nur in ihren Dateiendungen, sondern auch in ihrem Aufbau. Daher benötigen Sie auch verschiedene Tools zur Auswertung beider Protokollarten, aber dazu gleich mehr.

Nun, da Sie wissen, wie Sie Protokolldateien unter Windows anhand ihrer Dateiendung und ihres Speicherpfades erkennen können, werden Sie schnell feststellen, dass unter Windows Vista / 7 standardmäßig die Protokollierung von erheblich mehr Ereignissen aktiviert ist als unter Windows XP. Das

schlägt sich natürlich in der Anzahl der gespeicherten Logdateien nieder. Hier nur einige Beispiele:

- Systemlog — *Sysevent.evt*
  System.evtx
- Sicherheitslog — *Secevent.evt*
  Security.evtx
- Anwendungslog — *Appevent.evt*
  Application.evtx
- Hardwareereignislog — *HardwareEvents.evtx*
  Setuplog — *Setup.evtx*
- verschiedenste Anwendungslogs — z. B. *Internet Explorer.evtx*
- verbundene WLAN-Netzwerke — Microsoft-Windows-WLAN-Auto Config*.evtx
- weitergeleitetete Eventlogs — auf entfernten PCs gesammelt

Auf zur Auswertung

Die eigentliche Herausforderung bei der Untersuchung von Ereignisprotokollen besteht darin, die Masse der Daten herunterzufiltern auf die Informationen, die Sie tatsächlich interessieren. Sie könnten sich beispielsweise nur diejenigen Logeinträge anzeigen lassen, die in einem bestimmten Zeitraum mitprotokolliert wurden. Oder Sie filtern lediglich fehlgeschlagene oder erfolgreiche Loginversuche heraus. Für diese Filteraufgaben gibt es für beide Sorten von Logdateien (*.evt* und *.evtx*) gute kostenlose Programme.

Für Windows XP empfehlen wir Ihnen den *Event Log Explorer* von FSPro Labs (*http://www.forensikhacks.de/eventxp*). Seine Nutzung ist allerdings nur für private Verwendung kostenlos. Kommerzielle Benutzer müssen eine kommerzielle Lizenz erwerben. Nach Installation des Programms können Sie *.evt*- und *.evtx*-Dateien mit dem *Event Log Explorer* öffnen, indem Sie auf *File* → *Open Log File* klicken oder das zugehörige Symbol in der Schnellzugriffsleiste anwählen. Ist die Datei erst einmal geladen, sehen Sie auf der rechten Bildschirmseite alle Ereignisse. Die wahre Stärke von *Event Log Explorer* ist die Filterfunktion. Um Filter zu setzen, klicken Sie einfach auf das entsprechende Symbol in der Schnellzugriffsleiste oder rufen Sie *View* → *Filter (bzw. Strg+L)* auf. Dann können Sie ganz gezielt nach einzelnen Ereignistypen von bestimmten Benutzern zu genau definierten Zeiträumen suchen (siehe Abbildung 4-3).

Wenn Sie sehr große Logs auszuwerten haben, sollten Sie die Einstellungen unter *View* → *Log Loading Options* anpassen. Sie können dort schon im Vorfeld filtern. Sollten Sie bei der Untersuchung eines Systems festgestellt haben, dass die ein-

gestellte Zeitzone von Ihrer Zeitzone abweicht, passen Sie die Einstellungen unter *View* → *Time Correction* an. Sie können dort Werte von +23 bis –23 eintragen.

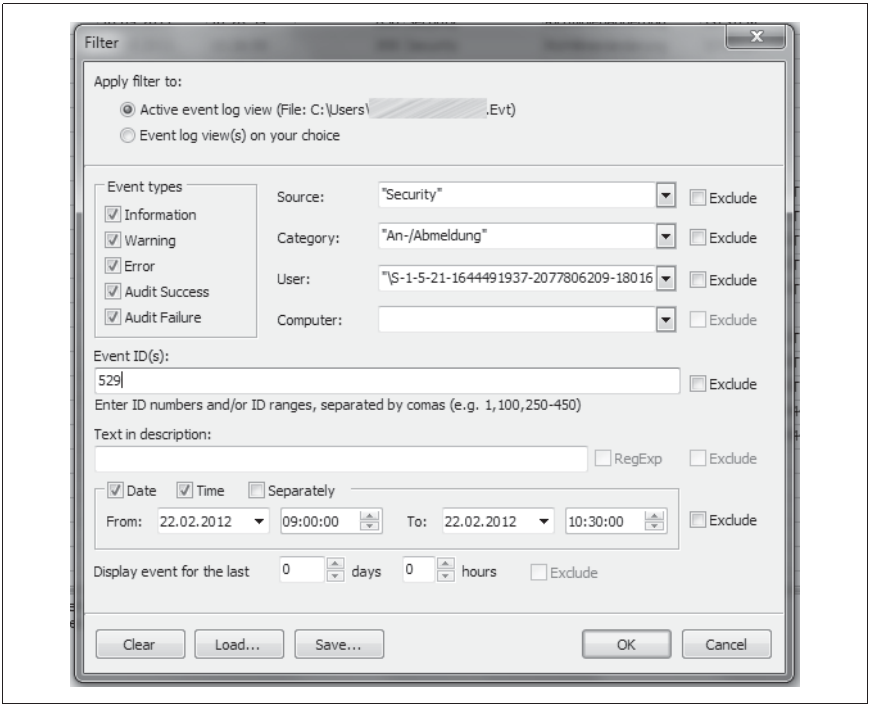

Abbildung 4-3: Die mächtige Filterfunktion von Event Log Explorer

Für Ereignisprotokolle unter Windows Vista bzw. 7 können Sie problemlos und kostenlos den eingebauten *Event Viewer* nutzen, den Microsoft seinem Betriebssystem beigelegt hat. *eventvwr.exe* verfügt im Vergleich zum Vorgänger unter Windows XP über eine ausführlichere Darstellung und erweiterte Filterfunktionen. Diese sind zwar nicht ganz so mächtig mit beim *Event Log Explorer*, reichen aber aus, um die zu untersuchenden Datenmengen wirksam zu reduzieren.

Den Event Viewer starten Sie, indem Sie im Windows-7-Startmenü einfach `eventvwr.exe` eintippen. Auch hier können Sie externe Ereignisprotokolldateien laden lassen. Klicken Sie dazu einfach auf *Aktion* → *Gespeicherte Protokolldatei öffnen*. Die Inhalte der geöffneten Datei finden Sie auf der linken Bildschirmseite unter *Ereignisanzeige* → *Gespeicherte Protokolle*. Nun können Sie einen Filter auf die Daten setzen, indem Sie rechts auf *Aktuelles Protokoll filtern…* klicken.

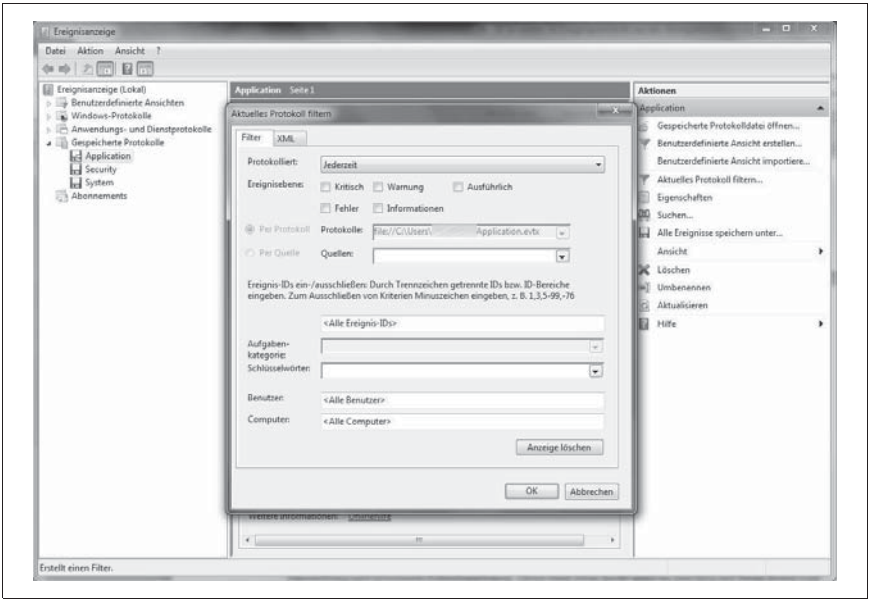

Abbildung 4-4: Anwendung von Filterfunktionen des eingebauten Event Viewer auf gespeicherte Protokolle

Ein weiteres, sehr mächtiges Tool, das von Microsoft kostenlos zur Verfügung gestellt und insbesondere zur Bewältigung von wirklich umfangreichen Ereignisprotokollen geeignet ist, ist der *LogParser* (*http://www.forensikhacks.de/logpars*). Er ist so universell einsetzbar und mächtig an Funktionsvielfalt, dass man ihm problemlos ein eigenes Buch widmen könnte. Daher wollen wir uns nur einige wenige Praxisbeispiele anschauen:

```
LogParser.exe -i:evt -o:datagrid "SELECT * FROM Security.evtx WHERE Message
LIKE '%logon%'"
```

oder

```
LogParser.exe -i:evt -o:datagrid "SELECT * FROM Security.evtx WHERE EventID
= 4720"
```

Wie Sie an diesem Beispiel sehen können, haben wir das Programm mit Optionen für das Inputformat (`-i`) und das Outputformat (`-o`) gestartet. Die Ausgabe erfolgt in unserem Fall im Logparser-eigenen Format Datagrid. Die Anweisung in den Anführungszeichen beschreibt, welche Daten woher anhand welcher Kriterien gefiltert werden sollen. In unserem Beispiel werden aus der Datei *Security.evtx* alle Datensätze herausgefiltert, die in der Spalte *Message* das Wort *logon* enthalten. Wenn Sie schon über Erfahrungen mit SQL-Abfragen verfügen, dürfte Ihnen das Abfrageschema bekannt vorkommen.

```
LogParser.exe -i:evt -o:CSV "SELECT TimeGenerated AS Zeit, EXTRACT_
TOKEN(Strings, 0, '|') AS Konto FROM Security.evtx WHERE EventID NOT IN
(541;542;543) AND EventType = 8 AND EventCategory = 13824"
```

Zeigt Ihnen Loginzeiten und Namen der zuletzt eingeloggten Benutzerkonten. Als Ausgabe haben wir dieses Mal `-o:CSV` (kommaseparierte Werte) gewählt. Der Vorteil bei diesem Format liegt in der Möglichkeit der Weiterarbeitung durch andere Tools und auch dem einfachen Import in Tabellenkalkulationsprogramme.

```
LogParser -i:FS -o:NAT "SELECT Path, Size, CreationTime FROM C:\*.* ORDER BY
Size"
```

In diesem Beispiel können Sie sehen, dass Sie *LogParser.exe* nicht nur für die Auswertung von Ereignisprotokollen verwenden können. Dieser Aufruf stellt Ihnen im NAT-Format auf der Konsole die Dateien auf *C:* mit Größe und Erstellungszeit dar – und zwar sortiert nach der Dateigröße. Sie können mit *Logparser.exe* sogar grafische Statistiken zeichnen lassen und auch andere Logformate auswerten. Im Internet finden Sie eine Vielzahl an tollen Anwendungsmöglichkeiten. Stöbern Sie doch ruhig einmal nach »Logparser.exe Examples«.

Ereignisse werden mit sogenannten Event-IDs gekennzeichnet. Über Filterung nach diesen IDs lassen sich also gezielt Ereignistypen wie zum Beispiel alle erfolgreichen Useranmeldungen herausfiltern. Eine gute Möglichkeit, nach Event-IDs zu recherchieren, bietet die Website EventID (*http://www.forensikhacks.de/eventid*).

Event-IDs in Windows XP, Vista und 7 unterscheiden sich. Versichern Sie sich, dass Sie nach der korrekten Event-ID suchen, bevor Sie mit dem Filtern beginnen.

HACK #51 Reisen Sie in die Vergangenheit

»Warum auch Schatten Kopien haben können«

Ein tolles Feature an Windows ist Möglichkeit der Erstellung von sogenannten Systemwiederherstellungspunkten. Diese ermöglichen es, den Zustand von wichtigen Systemdateien und seit Windows Vista / 7 auch anderer Dateien zu einem Zeitpunkt X festzuhalten. Sollte der Benutzer durch Softwareinstallationen oder Änderungen an Konfigurationen sein System in einen instabilen Zustand gebracht haben, kann er dann immer wieder zu Zustand X zurückkehren – und alles funktioniert wieder wie geschmiert.

Für Sie bietet diese Funktion natürlich auch ihre Vorteile, denn Sie können sich den Zustand von Systemdateien, Windows-Registry und auch normalen Dateien und Ordnern in der Vergangenheit anschauen. Selbst wenn also ein ehemaliger Mitarbeiter die wichtigen Projektdaten nicht nur gelöscht, sondern gleich noch überschrieben hat oder der Beschuldigte den Erpresserbrief nur kurzfristig auf seinem System gespeichert und anschließend entfernt hat, haben Sie dank Systemwiederherstellungspunkten die Chance, auf eine alte Kopie dieser Daten zurückzugreifen. Klingt spannend? Ist es auch! Los geht's.

Sowohl für Windows XP als auch für Vista / 7 werden die Systemwiederherstellungspunkte im Ordner *C:\System Volume Information* gespeichert. Selbst mit Administratorrechten kommen Benutzer im laufenden Betrieb nicht an die Dateien und Ordner in diesem Verzeichnis heran. Man müsste sich zuvor Systemrechte verschaffen oder externe Tools einsetzen, um diese Zugriffskontrolle zu umgehen. Das heißt, dass eine Manipulation zwar nicht unmöglich, aber sehr schwierig ist – und mithin bei Otto Normaluser eher unwahrscheinlich.

Systemwiederherstellungspunkte unter Windows XP

Systemwiederherstellungspunkte unter Windows XP werden durch unterschiedliche Ereignisse angelegt, zum Beispiel beim ersten Booten des Systems, alle 24 Stunden, bei der Installation von Programmen, bei Windows-Updates, vor der Installation eines unsignierten Treibers oder wenn sie durch den Benutzer manuell angestoßen werden. Die Wiederherstellungspunkte rotieren nach dem Prinzip *First In, First Out* und dürfen standardmäßig maximal 12 % des Festplattenspeichers belegen. Ihre Auswertung ist relativ einfach, da alle Daten vollständig innerhalb der Unterverzeichnisse von *System Volume Information* vorliegen.

Schauen wir uns den Verzeichnisaufbau der Systemwiederherstellungspunkte unter Windows XP einmal genauer an.

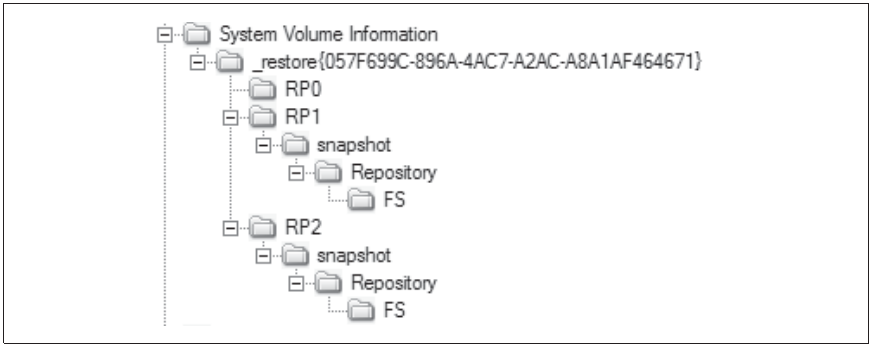

Abbildung 4-5: Verzeichnisaufbau der Systemwiederherstellungspunkte unter Windows XP

Am wichtigsten sind für Sie die einzelnen *RP*-Verzeichnisse sowie deren Unterordner *snapshot*. In den *RP*-Verzeichnissen finden Sie die Verwaltungsdatei *rp.log*, die Ihnen durch einen Zeitstempel in den letzten 8 Bytes verrät, wann der Wiederherstellungspunkt erstellt wurde. Des Weiteren finden Sie in den *RP*-Verzeichnissen alle gesicherten Systemdateien. Je nach Konfiguration des Systemwiederherstellungsdienstes werden zusätzlich zu den Systemdateien auch noch weitere Dateien basierend auf ihrer Dateiendung mitgesichert, standardmäßig geschieht das aber nicht. In der Datei *C:\Windows\system32\Restore\filelist.xml* können Sie einsehen, welche Dateien und Dateiendungen für die Sicherung vorgesehen sind.

Alle gesicherten Dateien liegen in umbenannter Form im Format *A########.ini* (Originalendung wird übernommen), das heißt, Sie können diese Dateien im Original betrachten und auswerten. Woher die Dateien stammen und wie ihr Originalname war, können Sie den *change.log**-Dateien entnehmen.

Im Unterverzeichnis *snapshot* finden Sie Zustände der Windows-Registry zum Zeitpunkt des Wiederherstellungspunkts. In Hacks [#47] und [#48] zeigen wir Ihnen, welche wertvollen Informationen die Registry enthalten kann.

Wenn Sie nun sorgfältig die *A########.**-Dateien zusammen mit den zugehörigen *change.log*-Dateien und auch die Registry-Abbilder analysieren, können Sie alte Versionen von mittlerweile gelöschten Dateien oder auch ehemals installierten Programmen (z. B. Schadsoftware, Keylogger etc.) feststellen.

Systemwiederherstellungspunkte unter Vista / 7

Ganz so einfach wie unter Windows XP funktioniert die Auswertung der Systemwiederherstellungspunkte unter Windows Vista / 7 leider nicht. Grund dafür ist die effizientere Speichermethode durch einen neuen Dienst namens *Volume Shadow Copy Service* (daher auch der Name Volumenschattenkopien für Systemwiederherstellungspunkte unter Vista / 7). Statt wie zuvor komplette Kopien der zu sichernden Dateien abzulegen, werden unter Windows Vista / 7 nur noch Änderungen an den Dateien in 16 Kilobyte großen Blöcken mitprotokolliert. Hat also der Erpresser nur einen kleinen Teil des Erpresserschreibens geändert, fänden Sie unter Windows XP unter Umständen noch das komplette frühere Schreiben, während Sie unter Vista / 7 nur die 16 Kilobyte großen Blöcke mit geändertem Inhalt zu Gesicht bekämen. Doch keine Angst, es gibt eine Lösung für diese Herausforderung.

Um auf Volumenschattenkopien zugreifen zu können, muss sich die Festplatte, auf der diese gespeichert sind, als lokale Festplatte im System befinden. Nur so ist die Rekonstruktion aus den einzelnen kleinen Blöcken möglich. Das bedeutet, dass Sie an einem toten Datenträgerimage die Aus-

wertung nicht so ohne Weiteres durchführen können. Selbst das Mounten des Image in das lokale System reicht meist nicht aus, um auf die Volumenschattenkopien zuzugreifen. Wir brauchen also einen Trick.

Im Folgenden zeigen wir Ihnen das Vorgehen bei einem toten Image. Sollten Sie es mit einem Live-System zu tun haben, benötigen Sie lediglich die folgenden Schritte.

1. Erstellen Sie aus Ihrem toten Image eine virtuelle Festplatte, zum Beispiel im *.vmdk*-Format. Wenn Sie sich unsicher sind, empfehlen wir Ihnen einen Blick in Kapitel 8.
2. Erstellen Sie eine virtuelle Maschine, zum Beispiel im *.vmx*-Format für VMWare Player. Booten Sie entweder direkt von der neu erstellten virtuellen Festplatte (bei Problemen siehe Kapitel 8) oder binden Sie die neue virtuelle Platte einfach als Zweitfestplatte in eine schon bestehende virtuelle Maschine auf Basis von Windows Vista / 7 ein.
3. Finden Sie heraus, welchen Laufwerksbuchstaben Ihre neu erstellte virtuelle Festplatte in der gebooteten virtuellen Maschine erhalten hat.
4. Starten Sie eine Kommandozeile *cmd.exe* mit Administratorberechtigung. Führen Sie den Befehl `vssadmin List Shadows /for=E:` aus (wobei `E:` der von Ihnen zuvor lokalisierte Laufwerksbuchstabe ist). Sie erhalten eine Auflistung aller verfügbaren Schattenkopien inklusive ihrer Erstellungszeit. Suchen Sie sich die Kopie heraus, die für Ihren Fall zeitlich am relevantesten scheint, und kopieren Sie die Pfadangabe, die unmittelbar nach *Schattenkopievolume*: steht, in die Zwischenablage. Sie sollte in etwa so aussehen:

   ```
   \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy5
   ```

5. Diese kopierte Pfadangabe brauchen Sie jetzt, denn Sie müssen mit folgendem Befehl einen Link auf die Volumenschattenkopie setzen:

   ```
   mklink /d c:\schatten5
   \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy5\
   ```

   

   Beachten Sie unbedingt den letzten Backslash hinter der Pfadangabe. Vergessen Sie ihn, werden Sie später beim Zugriff auf das Verzeichnis eine Fehlermeldung erhalten.

   Dadurch wird die Volumenschattenkopie mit der Nummer 5 in das Verzeichnis *schatten5* im Dateisystem Ihrer virtuellen Maschine eingehängt und Sie können darauf zugreifen.
6. Geben Sie das Verzeichnis *schatten5* für Ihre lokale Maschine frei. Sie können das tun, indem Sie beispielsweise eine Netzwerkfreigabe in Ihrer vir-

tuellen Maschine einrichten oder einen »gemeinsamen Ordner« nutzen, den Ihnen die meisten Virtualisierungslösungen zur Verfügung stellen.

7. Von nun an arbeiten Sie wieder auf Ihrer lokalen Maschine. Erstellen Sie ein Image vom freigegebenen Verzeichnis (siehe Kapitel 1).
8. Sie können nun entweder die komplette Volumenschattenkopie untersuchen oder die Auswertung etwas effektiver gestalten, indem Sie von allen Dateien der ursprünglich zu untersuchenden Festplatte eine Hash-Datenbank erstellen und diese bekannten Dateien über einen Hash-Abgleich auf der Volumenschattenkopie ausblenden lassen. So reduzieren Sie die Masse der auszuwertenden Daten auf diejenigen Dateien, deren Inhalte sich in der Volumenschattenkopie von den Originaldaten unterscheiden.

Wenn Sie einfach nur einen Blick auf die Inhalte einer Volumenschattenkopie werfen möchten, können Sie sich die Schritte 5, 6, 7 und 8 sparen. Sie können entweder auf der virtuellen Maschine das kostenlose Programm *ShadowExplorer* (*http://www.forensikhacks.de/shadow*) benutzen, mit dem Sie über eine grafische Oberfläche auf die verschiedenen Schattenkopien der verbundenen virtuellen Platten zugreifen können, oder Sie klicken im *Windows Explorer* mit der rechten Maustaste auf die zu untersuchende Partition, wählen VORGÄNGERVERSIONEN WIEDERHERSTELLEN, klicken nach kurzer Wartezeit auf die Schattenkopie Ihrer Wahl und bestätigen mit ÖFFNEN. Die Schattenkopie wird dann als simulierte Netzwerkfreigabe Ihres Local Host angezeigt und Sie können alle Verzeichnisse untersuchen.

HACK #52 Finden Sie Spuren in Vorschaudatenbanken

»Miniaturbilder im Fokus«

Wenn Sie schon einmal im *Windows Explorer* die Ordner mit Ihren Urlaubsbildern aufgerufen haben, haben Sie sicherlich auch schon einmal Bekanntschaft gemacht mit den Vorschaugrafiken, die Ihnen den Überblick über Ihre geschossenen Fotos erleichtern. Vielleicht ist Ihnen auch schon einmal aufgefallen, dass der erste Aufruf eines Verzeichnisses mit vielen großen Bilddateien länger dauert als der zweite und dritte Aufruf. Das liegt daran, dass Windows die kleinen Vorschaubilder, die Ihnen auf dem Bildschirm angezeigt werden, beim ersten Aufruf des Verzeichnisses zunächst berechnet und dann fest in einer Datenbank abspeichert. Beim nochmaligen Aufruf des Verzeichnisses wird dann nur noch die Datenbank abgefragt. Die Vorschaubilder sind also als Beschleunigung für den Benutzer gedacht. Ihre Generierung ist standardmäßig aktiviert und die Ablage erfolgt in einer versteckten Vorschaudatenbank.

In der Forensik können diese Vorschaubilder deshalb eine große Rolle spielen, weil sie selbst dann gespeichert bleiben, wenn die eigentlichen Original-

bilder gelöscht oder in ein anderes Verzeichnis auf einem anderen Datenträger kopiert werden. Das heißt, Sie können bei Ihrer Untersuchung auf Vorschauansichten der entwendeten Konstruktionszeichnungen stoßen, auch wenn der Täter diese Zeichnungen schon lange von seinem Computer entfernt hat. Grund genug, sich diese Vorschaudatenbanken einmal näher anzuschauen, meinen Sie nicht?

Vorschaubilder in Windows XP

In Windows XP speichert der *Windows Explorer* die Vorschaugrafiken standardmäßig in dem Verzeichnis ab, von dem aus die Vorschauansicht aufgerufen wurde. Die Datenbankdatei namens *Thumbs.db* findet sich also genau in diesem Verzeichnis wieder. Sie liegt im OLE2-Format vor und beinhaltet nicht nur alle Vorschaubilder, sondern in dem Eintrag CATALOG auch alle Dateinamen der dazugehörigen Originalbilder.

Für die Untersuchung von *Thumbs.db* gibt es einige sehr gute kostenlose Tools. Mit dem *Windows File Analyzer* von MiTec (*http://www.forensikhacks.de/wfa*) können Sie einfach über das Menü unter *File → Analyze Thumbnail Database → Windows XP…* die von Ihnen zu untersuchende Datei *Thumbs.db* öffnen. Ihnen werden dann alle enthaltenen Bilder mit Originalnamen angezeigt. Wenn Sie beweisrelevante Daten gefunden haben, können Sie einfach auf REPORT klicken, um diese Daten für Ihren Bericht zu exportieren.

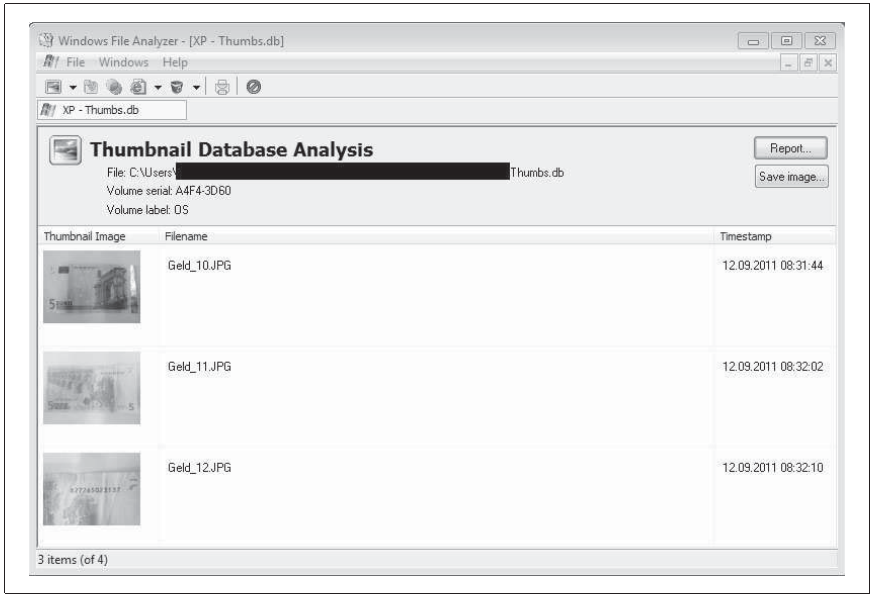

Abbildung 4-6: Thumbs.db-Darstellung mit Windows File Analyzer

Mit *vinetto* von Michel Roukine (*http://www.forensikhacks.de/vinetto*) steht Ihnen unter Linux und Mac OS X ebenfalls ein gutes kostenloses Tool zum Auswerten von *Thumbs.db*-Datenbanken zur Verfügung. Nach dem Herunterladen und Installieren können Sie es über die Kommandozeile mit folgendem Befehls nutzen:

```
$ vinetto –H -o /fall/12345/thumbs /mnt/fall/12345/bilder/Thumbs.db
```

Das extrahiert nicht nur die Vorschaubilder, sondern erstellt Ihnen gleichzeitig noch einen brauchbaren Report im HTML-Format.

Vorschaubilder in Windows Vista / 7

Anders als unter Windows XP werden unter Windows Vista / 7 die Thumbnail-Datenbanken nicht mehr dezentral pro Ordner angelegt, sondern stattdessen an einem zentralen Ort für das gesamte System. Dieses Verzeichnis findet sich unter *C:\Users\<Benutzername>\AppData\Local\Microsoft\Windows\Explorer*.

Die Datenbanken erkennen Sie am Dateinamen, der sich aus dem Präfix *thumbcache_* gefolgt von der maximalen Seitenlänge der enthaltenen Vorschaugrafiken in Pixeln, also 32, 96, 256 oder 1024 zusammensetzt.

Auch Vorschaugrafiken von externen Datenträgern werden in den zentralen Thumbcache-Datenbanken gespeichert. Das bedeutet, dass Sie beweisrelevante Bilddateien sogar dann auffinden können, wenn sie nie auf der lokalen Festplatte des Systems gespeichert waren.

Unter Umständen speichern auch Windows Vista / 7 noch *Thumbs.db*-Dateien. Das ist zum Beispiel bei Netzwerklaufwerken der Fall.

Sie können die Thumcache-Datenbanken manuell auswerten, indem Sie über diese Datenbanken nach *.bmp*- und *.jpg*-Signaturen carven lassen (siehe **Hacks [#29]** und **[#34]**). Sie erhalten dann zwar nicht die Originalnamen der Dateien, aber diese Zuordnung ist bei Thumbcache-Datenbanken unter Windows Vista / 7 ohnehin schwierig. Die Datenbanken enthalten nämlich lediglich Hashwerte, die sogenannten *Thumbnail Cache IDs*, die zum Beispiel über einen Abgleich mit der *windows.edb*-Datenbank des *Windows Suchindexers* möglich ist.

Für die halbautomatische Auswertung von Thumbcache-Dateien in Windows Vista / 7 empfehlen wir Ihnen das kostenlose Programm *Thumbcache Viewer* (*http://www.forensikhacks.de/thumb*). Zwar bietet es keine Galeriean-

sicht, aber dieses Manko können Sie umgehen, indem Sie alle Thumbnails in einen Ordner auf Ihrem lokalen System extrahieren lassen und dann mit dem Windows Explorer oder mit einem Bildbetrachter Ihrer Wahl anschauen.

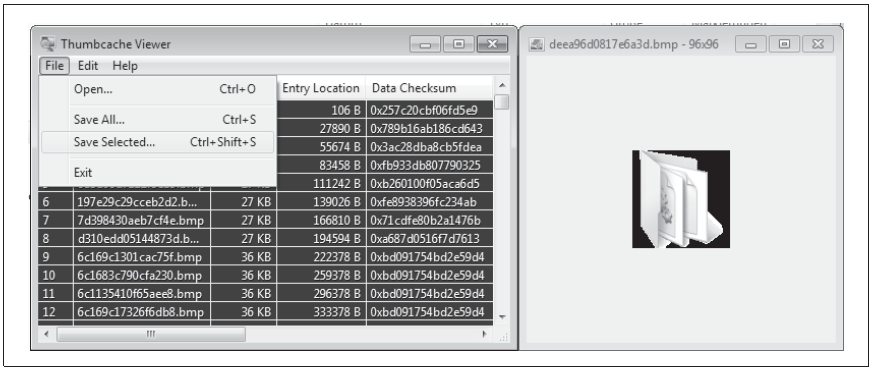

Abbildung 4-7: Thumbcache-Darstellung mit dem Thumbcache Viewer

Die beweisrechtliche Würdigung von Spuren in Thumbcache-Datenbanken ist als schwierig anzusehen, da Vorschaugrafiken durch unterschiedliche Aktionen generiert werden können. Das Vorhandensein einer Vorschaugrafik weist nicht zwangsläufig darauf hin, dass das Bild in der Vorschauansicht des Explorers auf diesem System angeschaut worden sein muss. Thumbs.db-Datenbanken könnten beispielsweise von einem anderen System kopiert worden sein.

Es sind weiterhin Fälle bekannt, in denen Windows-7-Thumbcaches Vorschaubilder von Dateien auf einer externen Festplatte enthielten, obwohl lediglich der Datenträger mit dem System verbunden wurde, die Dateien aber nie in der Vorschauansicht betrachtet wurden.

HACK #53 Sehen Sie, was gedruckt wurde

»Der Tinte auf der Spur«

Bei der Untersuchung von Datenträgern können insbesondere im Unternehmensumfeld die gedruckten Dokumente eine große Rolle spielen. Hat der Mitarbeiter vertrauliche Firmendaten ausgedruckt, bevor er das Unternehmen verließ? Wurde das anonyme Bedrohungsschreiben vom Computer eines Mitarbeiters aus geschrieben und ausgedruckt? Kann dem Erpresser nachgewiesen werden, dass er den Erpresserbrief von seinem PC aus drucken ließ? Das sind Fragestellungen, deren Beantwortung wir Ihnen mit diesem Hack erleichtern wollen.

Die schlechte Nachricht zuerst: Die erste, unverbindliche Antwort auf diese Fragen lautet Jein. Die Herausforderung beim Nachweis von Druckaufträgen liegt darin, dass standardmäßig zwar jeder Druckauftrag durch die Druckerwarteschleife (Spooler) von Windows geht, sobald das Dokument jedoch erfolgreich gedruckt wurde, auch wieder sofort vom System gelöscht wird. Das bedeutet, dass die Wahrscheinlichkeit, einen alten Druckauftrag zu finden, relativ gering ist. Sie müssen also Datenwiederherstellungstechniken bemühen, um aus gelöschten Bereichen alte, bereits entfernte Druckaufträge wiederherstellen zu können. In den **Hacks [#29]**, **[#30]**, **[#34]** und **[#35]** können Sie die entsprechenden Verfahren nachlesen.

Für die Suche nach gelöschten Druckaufträgen empfehlen wir, nach folgenden Signaturen zu suchen. Erhalten Sie keine oder zu wenig Treffer, sollten Sie versuchen, die Signaturen etwas breiter zu fassen:

\x01\x00\x00\x00..\x00.{34,34}EMF	für EMF-Dateien
\x00\x00\x01\x00.\x00\x00	für SPL-Dateien
\x68\x49\x00\x00\x88	für SHD-Dateien (wenig einheitlich)

Die Druckaufträge werden von Windows standardmäßig in folgendem Verzeichnis gespeichert:

C:\Windows\System32\spool\PRINTERS.

Der Pfad kann jedoch auch abweichen. Sie können das überprüfen, indem Sie sich den folgenden Registry-Eintrag näher ansehen:

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\
DefaultSpoolDirectory
```

Zu einem Druckauftrag gehören immer zwei Dateien. Die eine hat die Endung *.shd* und enthält Metainformationen zum Auftrag, kann Ihnen also Fragen beantworten wie: Wie hieß das gedruckte Dokument? Wann wurde es mit welchen Druckertreibern gedruckt? Welcher Benutzer hat es aus welchem Programm heraus gedruckt? Sie sehen: *.shd*-Dateien können Ihnen wertvolle Informationen geben.

Die andere Datei, die zu einem Druckauftrag gehört, enthält das eigentliche Dokument, das gedruckt werden soll. Sie hat denselben Namen wie die zugehörige *.shd*-Datei, allerdings weist sie die Endung *.spl* auf. Die Dokumenteninhalte sind in dieser Datei im *Windows Enhanced Metafile Format* (EMF) gespeichert.

Wenn Sie etwas Glück haben, können Sie Druckaufträge aus gelöschten Bereichen wiederherstellen oder finden sogar noch unbeendete Druckauf-

träge im Spooler-Verzeichnis. Für Besitzer einer kommerziellen Forensiksoftware wie EnCase, FTK oder X-Ways ist das Betrachten dieser Dateien nun ein Kinderspiel, da die SPL-Dateien meist von den internen Dateibetrachtern angezeigt werden können.

Sollten Sie nicht im Besitz einer kommerziellen Forensiksoftware sein, empfehlen wir Ihnen das Programm *SPL Viewer*, das Sie unter *http://www.forensikhacks.de/spl* herunterladen können. Mit ihm öffnen Sie ganz einfach die gewünschten *.spl*-Dateien.

HACK #54 Stöbern Sie im Müll

»Papierkörbe im Vergleich«

Sicherlich haben Sie den Papierkorb unter Windows bereits kennenlernen dürfen. Spätestens wenn Sie versuchen, eine Datei durch Betätigen der Taste *Entf* oder durch Anwählen von LÖSCHEN im Kontextmenü zu entfernen, werden Sie gefragt, ob Sie diese Datei wirklich in den Papierkorb verschieben möchten. Interessanterweise verwendet Microsoft hier die korrekte Bezeichnung, nämlich »verschieben«. Dieses Verb lässt schon erahnen, dass die Datei nicht wirklich gelöscht, sondern einfach nur in einen anderen Ordner verschoben wird, nämlich Ihren Papierkorb. Das wiederum bedeutet für Sie, dass Sie in Ihren Untersuchungen ruhig einmal im Papierkorb stöbern dürfen. Oft genug lassen sich dort interessante Spuren finden.

Die Papierkörbe von Windows XP und Windows Vista / 7 unterscheiden sich grundlegend voneinander. Während der Papierkorb unter XP im Ordner *RECYCLER* zusammen mit einer Verwaltungsdatenbank pro Benutzer abgelegt ist, suchen Sie unter Windows Vista / 7 diesen Ordner vergeblich. Dort nennt er sich nämlich *$Recycle.Bin* und lässt eine zentrale Datenbankdatei missen. Da beide Papierkorbarten unterschiedlich zu untersuchen sind, lassen Sie uns im Folgenden einen Blick auf die Papierkörbe von Windows XP und Windows Vista / 7 werfen.

Der Recycler von Windows XP

Der Papierkorb von Windows XP findet sich im Ordner *<LAUFWERK>:\RECYCLER* wieder. Er beinhaltet standardmäßig ein Unterverzeichnis für jeden Benutzer des Systems, der schon einmal eine Datei gelöscht hat. Diese Unterordner entsprechen dem *Security Identifier* (SID) des jeweiligen Benutzers auf dem jeweiligen System. Die letzten Ziffern dieses SID geben Aufschluss darüber, welchem Benutzer ein Papierkorb zuzuordnen ist. Ein SID sieht so aus:

```
S-1-5-21-1644491937-2077806209-1801674531-1004
```

Der Papierkorb ist in obigem Fall dem Benutzer mit der relativen ID (RID) 1004 zuzuordnen. Über die Windows-Registrierungsdatenbank SAM können Sie herausfinden, welcher Benutzername zu welcher RID gehört.

Jeder dieser Unterordner enthält die gelöschten Dateien des jeweiligen Benutzers. Vielleicht ist Ihnen schon aufgefallen, dass beim Löschen bzw. Verschieben in den Papierkorb die eigentlichen Dateinamen abgeändert werden. Wenn beispielsweise eine Bilddatei gelöscht wurde, könnte ihr neuer Name im Papierkorb *Dc5.jpg* lauten. Sie können bei der Untersuchung eines Papierkorbs bereits aus dieser Bezeichnung erste Rückschlüsse auf die Datei ziehen, wie folgende Abbildung zeigt.

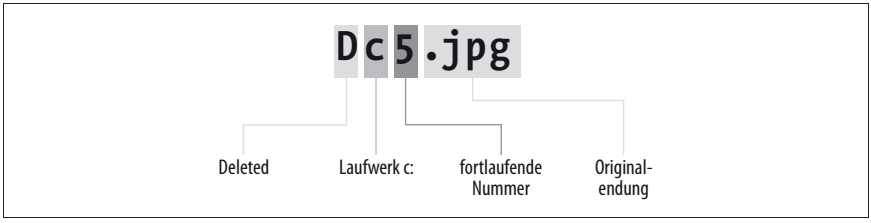

Abbildung 4-8: Aufschlüsselung von Dateinamen im Papierkorb unter Windows XP

Viel interessanter und für Sie aufschlussreicher ist die Untersuchung der Datenbankdatei *INFO2*. In dieser Datei ist jede Datei erfasst, die sich aktuell im Papierkorb befindet bzw. früher einmal dort befunden hat. Windows XP braucht diese Datei, um zu wissen, wann eine Datei gelöscht wurde, wo sie im Original herstammte und wie ihr Originalname war. Ansonsten wäre für den Benutzer ein Widerherstellen aus dem Papierkorb heraus nicht möglich.

Die Datei *INFO2* besteht aus einem Header mit 20 Bytes und Einträgen von jeweils 800 Bytes pro gelöschter Datei. Diese Einträge setzen sich so zusammen:

- Offset 0: Original-Laufwerksbuchstabe, Pfad und Dateiname
- Offset 260: Fortlaufende Nummer korrespondierend zu der im Dateinamen
- Offset 264: Nummer des Laufwerks (0=A, 1=B, 2=C, 3=D etc.)
- Offset 268: Zeitstempel der Löschung im 32-Bit-FILETIME-Format (UTC)
- Offset 276: Logische Originalgröße der Datei in Bytes
- Offset 280: Original-Laufwerksbuchstabe, Pfad und Dateiname in Unicode

Neben diesen wertvollen Informationen über die gelöschten Dateien gibt es weitere Szenarien, die eine Auswertung der Datei *INFO2* unverzichtbar machen. Stellen Sie sich vor, ein Administrator Ihres Unternehmens möchte einen unliebsamen Mitarbeiter loswerden und kopiert belastende Materialien in dessen Papierkorb, oder ein Mitarbeiter versteckt gezielt Daten in seinem eigenen Papierkorb. In diesen Fällen sollten Sie – neben einer Analyse der

Besitzerverhältnisse und Berechtigungen dieser Dateien – unbedingt untersuchen, ob für Dateien Einträge in der *INFO2*-Datei vorliegen.

Die Analyse der *INFO2*-Datei lässt sich übrigens mit den gängigen Forensiktools und auch mit kostenloser Software erleichtern. Wir empfehlen Ihnen dazu den *Windows File Analyzer* von MiTeC (*http://www.forensikhacks.de/wfa*) und *Rifiuti* von McAfee (*http://www.forensikhacks.de/rifiuti*).

Der $Recycle.Bin unter Windows Vista / 7

Ähnlich wie der Papierkorb unter Windows XP enthält auch der Abfalleimer von Windows Vista / 7, der unter *<LAUFWERK>:\$Recycle.Bin* zu finden ist, jeweils einen Unterordner für jeden Benutzer, der schon einmal eine Datei auf dem System gelöscht hat. Die Vergabe des Ordnernamens basierend auf der SID läuft hierbei exakt so ab wie unter Windows XP.

Wenn Sie jedoch einen Blick in eines dieser Unterverzeichnisse werfen, fällt Ihnen sofort auf, dass die gelöschten Dateien dort anders benannt sind und auch von einer *INFO2*-Datei weit und breit keine Spur zu sehen ist.

Statt einer *INFO2*-Datei wird im Papierkorb von Windows Vista / 7 immer ein Set von zwei Dateien pro gelöschter Datei angelegt: eine *$I*-Datei, die Metainformationen enthält, und eine *$R*-Datei, die die eigentlichen Dateiinhalte enthält. In der folgenden Abbildung ist der Aufbau der Dateinamen schematisch dargestellt.

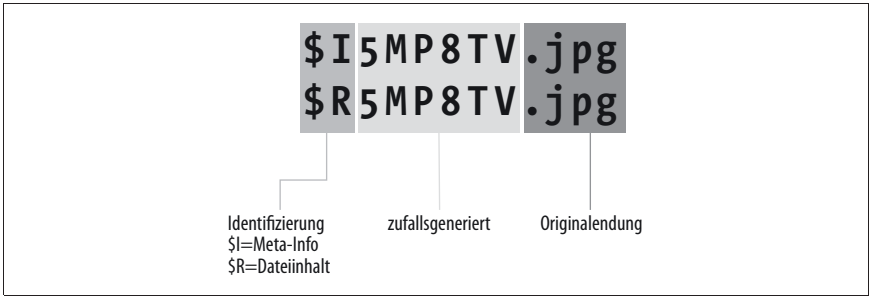

Abbildung 4-9: Aufschlüsselung von Dateinamen im Papierkorb von Windows Vista / 7

Sie sehen, die Metainformationen aus den Einträgen der *INFO2*-Datei sind im *$Recycle.Bin* quasi in einzelne kleine *$I*-Dateien ausgelagert worden. Diese 544 Bytes großen Dateien beinhalten Informationen über Löschzeitpunkt, Originaldateinamen und Originalgröße der gelöschten Datei und sind wie folgt aufgebaut.

- Offset 0:
  Dateiheader 01 gefolgt von 7 Null-Bytes

- Offset 8:
  Logische Originalgröße der Datei in Bytes
- Offset 16:
  Zeitstempel der Löschung im 32-Bit-FILETIME-Format (UTC)
- Offset 24:
  Original-Laufwerksbuchstabe, Pfad und Dateiname in Unicode

Während die meisten kommerziellen Forensikprogramme die Informationen aus den *$I*-Dateien meist automatisch oder skriptgestützt auslesen können, sind uns kaum brauchbare kostenlose Alternativen bekannt. Eine Möglichkeit zur Auswertung des Papierkorbs von Windows Vista / 7 auf einem Live-System stellt der *Recycle Reader* von Live-Forensics dar (*http://www.forensikhacks.de/recyc*).

HACK #55 Passwort vergessen? Kein Problem!

»Ersatzschlüssel gefällig?«

Sie wollten Ihren Rechner gegen Fremdzugriffe schützen und haben daher einen passwortgeschützten Benutzeraccount unter Windows angelegt, erinnern sich jetzt nach längerer Abwesenheit aber nicht mehr an das Passwort? Oder ein ehemaliger Mitarbeiter Ihrer Firma hat ohne Ihre Genehmigung auf dem Firmenlaptop die Passwörter für die Standard-Nutzerzugänge geändert? Kein Problem. Wir beschreiben Ihnen hier eine Methode, wie Sie Ihr Windows-Passwort zurücksetzen können.

Die hier beschriebenen Methoden dürfen ausschließlich zu legalen Zwecken, also beispielsweise zu forensischen Untersuchungen innerhalb des rechtlich abgedeckten Umfangs und für Versuchszwecke, beispielsweise das Umgehen des von Ihnen selbst gesetzten Passwortschutzes, eingesetzt werden. Der Paragraph 202c StGB stellt Vorbereitungshandlungen für das Ausspähen von Daten (§202a StGB) und das Abfangen von Daten (§202b StGB) unter Strafe. Darunter fällt unter anderem auch das Verschaffen eines Computerprogramms, dessen Zweck die Begehung einer solchen Tat ist. Gemäß den Beschlüssen 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1524/08 des Bundesverfassungsgerichts sowie einer juristischen Stellungnahme der European Expert Group for IT Security (EICAR), *http://eicar.org/files/jlussi_leitfaden_web.pdf*, fallen Programme mit Dual-Use-Charakter bei legaler Anwendung nicht unter den Paragraphen 202c StGB. Dieser Hinweis stellt keine Rechtsberatung da. Wenn Sie im Zweifel darüber sind, ob bestimmte Techniken unter bestimmten Umständen zu einem Rechtsverstoß führen könnten, ersuchen Sie bitte einen Rechtsbeistand um Rat.

Um in etwa zu verstehen, wie es möglich ist, Windows-Passwörter einfach so zu ersetzen, möchten wir Ihnen einen kurzen Überblick darüber geben, wie das Betriebssystem Windows Ihr Passwort speichert.

Zentraler Dreh- und Angelpunkt in Sachen Passwörter ist die Registry, die Sie in diesem Kapitel schon kennenlernen durften. In der Datenbank des *Security Account Managers* (SAM) sind alle Benutzernamen und Passwörter verschlüsselt abgelegt. In früheren Windows-Versionen wurden die Passwörter als sicherheitsanfällige 128-Bit-LAN-Manager-Hashes (LM Hashes) gespeichert, was aus Gründen der Abwärtskompatibilität auch noch bis in aktuelle Windows-Versionen (bis XP) beibehalten wurde. Windows Vista und 7 speichern ihre Passwörter ebenfalls in der SAM-Datenbank als NT-LAN-Manager-Hashes (NTLM). In beiden Fällen ist möglich, den gespeicherten Passwort-Hash durch einen neu berechneten zu ersetzen, zum Beispiel durch den eines leeren Passworts. Und genau so geht auch die Boot-CD vor, die wir Ihnen nun vorstellen.

Übrigens ist das Abspeichern von Passwörtern als Hashwerte in einer Datenbank keinesfalls eine Eigenheit des Windows-Betriebssystems. Sie können auch Linux-Passwörter in */etc/shadow* auf dieselbe Art ersetzen. Mehr zum Thema Penetrationstests für Windows- und Linux-Passwörter finden Sie in den **Hacks [#96]** bis **[#98]**.

Wenn Sie also Ihr vergessenes Passwort zurücksetzen möchten, laden Sie sich die Boot-CD *Offline NT Password & Registry Editor* von Petter Nordahl-Hagen (*http://pogostick.net/~pnh/ntpasswd/*) herunter. Das auf der Homepage erhältliche ZIP-Archiv beinhaltet eine ISO-Datei, die Sie einfach in gängigen Brennprogrammen auf eine CD brennen können. Alternativ können Sie natürlich auch einen bootfähigen USB-Stick erstellen. Auf der Homepage gibt es entsprechende Anleitungen.

Sobald Sie Ihre Boot-CD fertig haben, legen Sie sie in das optische Laufwerk Ihres PCs ein und starten ihn. Stellen Sie sicher, dass Ihr BIOS ein Booten von CD/DVD erlaubt und dass dieses Gerät Priorität vor der Systemfestplatte erhält. Oft reicht es aus, durch Betätigen von F8 während des Bootvorgangs das Bootmenü vom BIOS aus aufzurufen.

Wenn der PC von der CD bootet, wird zunächst das kleine Linux-Betriebssystem zusammen mit den notwendigen Treibern geladen. Im nächsten Schritt müssen Sie auswählen, auf welchem Laufwerk sich die Windows-Installation befindet, deren Passwörter zurückgesetzt werden sollen.

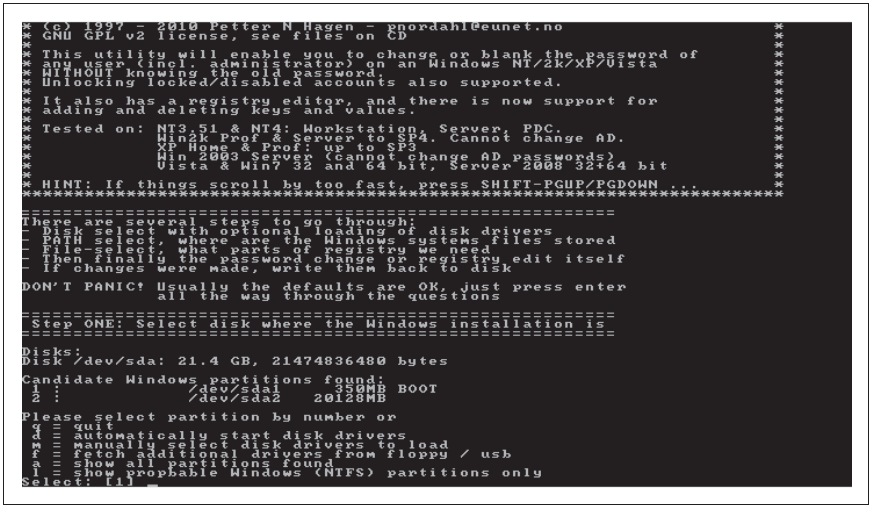

Abbildung 4-10: Gebootete Windows-7-Installation. Partition 2 ist die interessante.

Haben Sie das entsprechende Laufwerk ausgewählt, sollten Sie dem Programm mitteilen, unter welchem Pfad sich die SAM-Datei auf diesem Laufwerk befindet.

Abbildung 4-11: Drücken Sie Enter, um den Standardwert zu akzeptieren.

Die Standardeinstellung *Windows\System32\config* ist meist die richtige. Wählen Sie nun *Password reset [sam system security]* als auszuführende Aktion aus, um dann im vorletzten Schritt den Benutzer auszuwählen, dessen Passwort Sie zurücksetzen möchten.

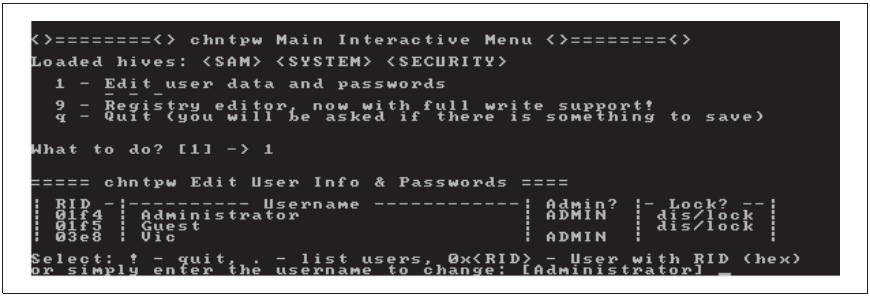

Abbildung 4-12: Sie können den Usernamen einfach im Klartext schreiben.

Nachdem Sie einen User ausgewählt und im Folgeschritt *Clear (blank) user password* gewählt haben, wird Ihnen der Erfolg dieser Aktion durch die Meldung *Password cleared* bestätigt.

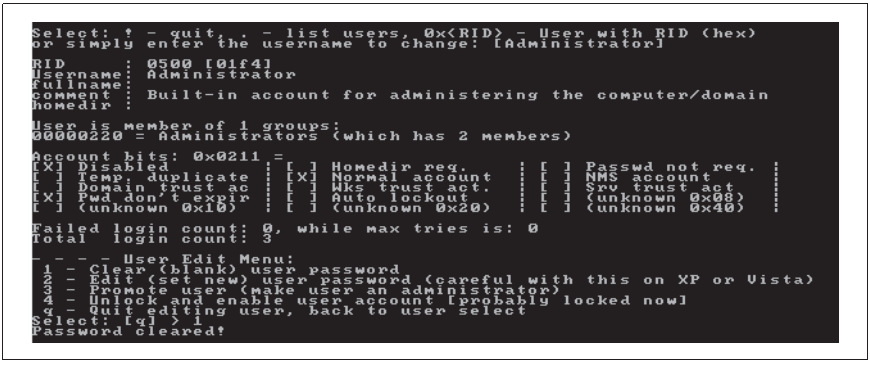

Abbildung 4-13: Wir haben unser vergessenes Passwort erfolgreich zurückgesetzt.

Durch Eingeben eines Ausrufezeichens, gefolgt von einem *q* für *quit*, beenden Sie Ihren Eingriff in die SAM-Datenbank. Nun müssen Sie lediglich Ihre Änderungen speichern. Beachten Sie, dass im letzten Schritt als Standardaktion *[n]* vorgegeben ist, also bei einem Betätigen der Enter-Taste nichts geändert würde.

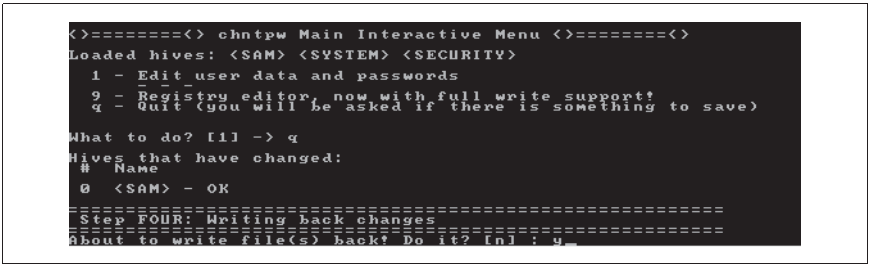

Abbildung 4-14: Ohne Speicherung am Ende gehen alle Änderungen verloren.

Glückwunsch, Sie haben nun beim Neustart des Rechners wieder Zugriff auf Ihr Benutzerkonto!

Sie sollten diese Methode nicht anwenden, wenn Sie Ihre Daten mit der Windows-eigenen EFS-Verschlüsselung geschützt haben. Da diese zwingend den Login mit dem korrekten Passwort benötigt, bedeutet das Zurücksetzen des Passworts, dass Sie trotz erfolgreichen Logins nicht mehr auf die so verschlüsselten Daten zugreifen können.