KPMG

cutting through complexity™

Windows 7 Forensik

- ein Überblick über Artefakte –

Alexander Geschonneck

Partner, KPMG Forensic Technology

Forensic Technology von KPMG

Digital Evidence Recovery / Evidence and Disclosure Management

Erfassung, Speicherung, Abfrage, Analyse, Sichtung
und Verteilung großer Volumen von sichergestellten Informationen und der hieraus erzeugten Aufbereitungs-ergebnisse (E-Discovery) in einem dedizierten und sicherheitszertifizierten Forensic Data Center.

Records Risk Management

Unterstützung der Mandanten bei der Klärung aller Fragen
im Zusammenhang mit Risiken und der Verantwortung für

Daten und Dokumente (Records) und der Einhaltung der damit verbundenen rechtlichen Anforderun-gen.
Schaffung von Transparenz für die Unternehmensleitung über den Informationsbestand durch Kategorisierung und Klassifizierung der Datenbestände

Forensic Data Analytics

Fraud-Detection-Routinen und die von KPMG entwickelte Analyseplattform KTrace helfen bei der Untersuchung von großen strukturierten Datenbeständen nach Auffälligkeiten oder schon näher identifizierten Sachverhalten.

KPMG

cutting through complexity™

Neues Partitionsschema unter Windows 7

Neues Partitionsschema bei der Installation von Windows 7

Bei der Installation werden standardmäßig immer mindestens zwei Partitionen angelegt

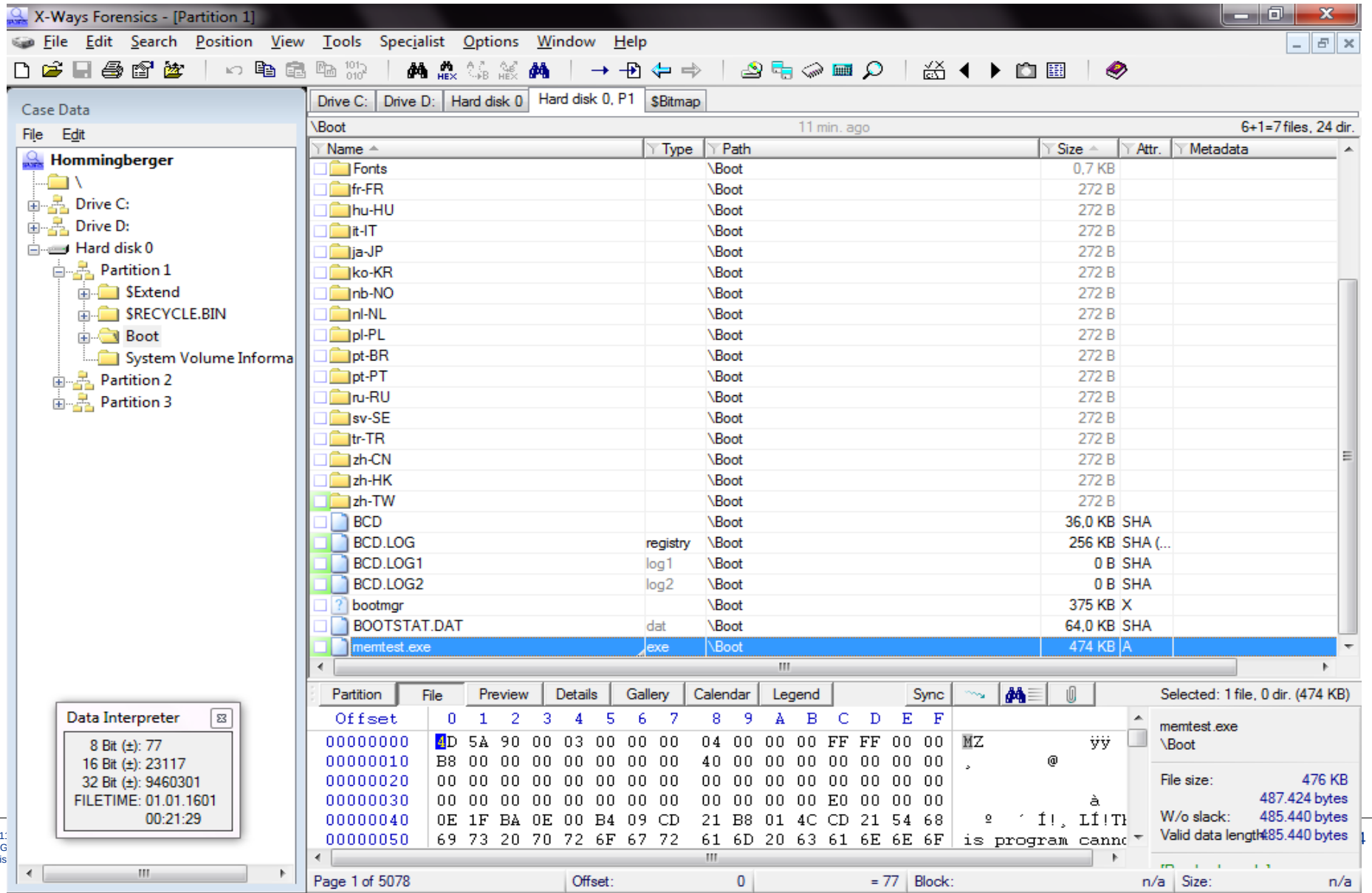
- „BitLocker Ready“

Eine „Bootpartition“ mit einer Größe von rund 100 MB

- Enthält den Bootsektor, Bootmanager, verschiedene Sprachkonfigurationen, Fonts, Tools (memtest)
- Immer unverschlüsselt
- NTFS-Dateisystem
- Standardmäßig ist dieser Partition kein Laufwerks-Buchstabe zugewiesen

Die „Systempartition“, der standardmäßig der restliche Platz zugewiesen wird - ggfs. BitLocker-verschlüsselt

Neues Partitionsschema bei der Installation von Windows 7: Ansicht in X-Ways



KPMG

cutting through complexity™

Überblick Windows BitLocker

Funktionen von BitLocker

BitLocker...

- Ist ein in Windows integriertes Verschlüsselungstool
- Ermöglicht eine Festplattenvollverschlüsselung
- Ermöglicht die Nutzung eingebauter TPM-Chips
- Ist gut in übliche Windows-Unternehmensinfrastrukturen integriert

BitLocker setzt für die Verschlüsselung der Systempartition entweder einen TPM-Chip (ab Version 1.2) oder ein BIOS mit der Fähigkeit von Pre-Boot-USB-Erkennung voraus

- Standardmäßig funktioniert die Verschlüsselung nur mit TPM-Chip
- Durch eine Änderung der Gruppenrichtlinien wird auch USB-Stick Authentifikation gestattet

KPMG

cutting through complexity™

Änderungen bei BitLocker gegenüber Windows Vista

Änderungen bei BitLocker im Überblick

Neues BitLocker-Format

- BitLocker Partitionen in Windows 7 haben eine leicht geänderte Signatur
- Alte Windows-Versionen können Windows 7-BitLocker-Partitionen nicht öffnen
- Windows 7 öffnet jedoch Vista-Partitionen

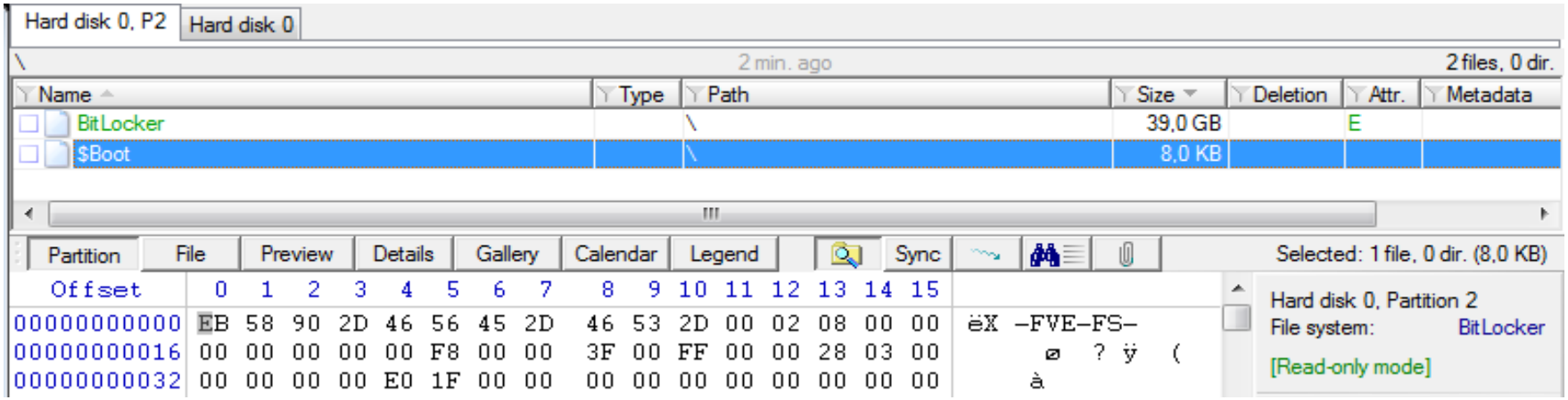
Unter Vista können seit Service Pack 1 auch andere Partitionen als die Systempartition verschlüsselt werden

Überarbeitetes Tool zur BitLocker-Verwaltung

BitLocker To Go für mobile Geräte ist neu bei Windows 7

Neuer Dateiname für Recovery Key Files

Änderungen bei BitLocker: Neue Signatur in Windows 7

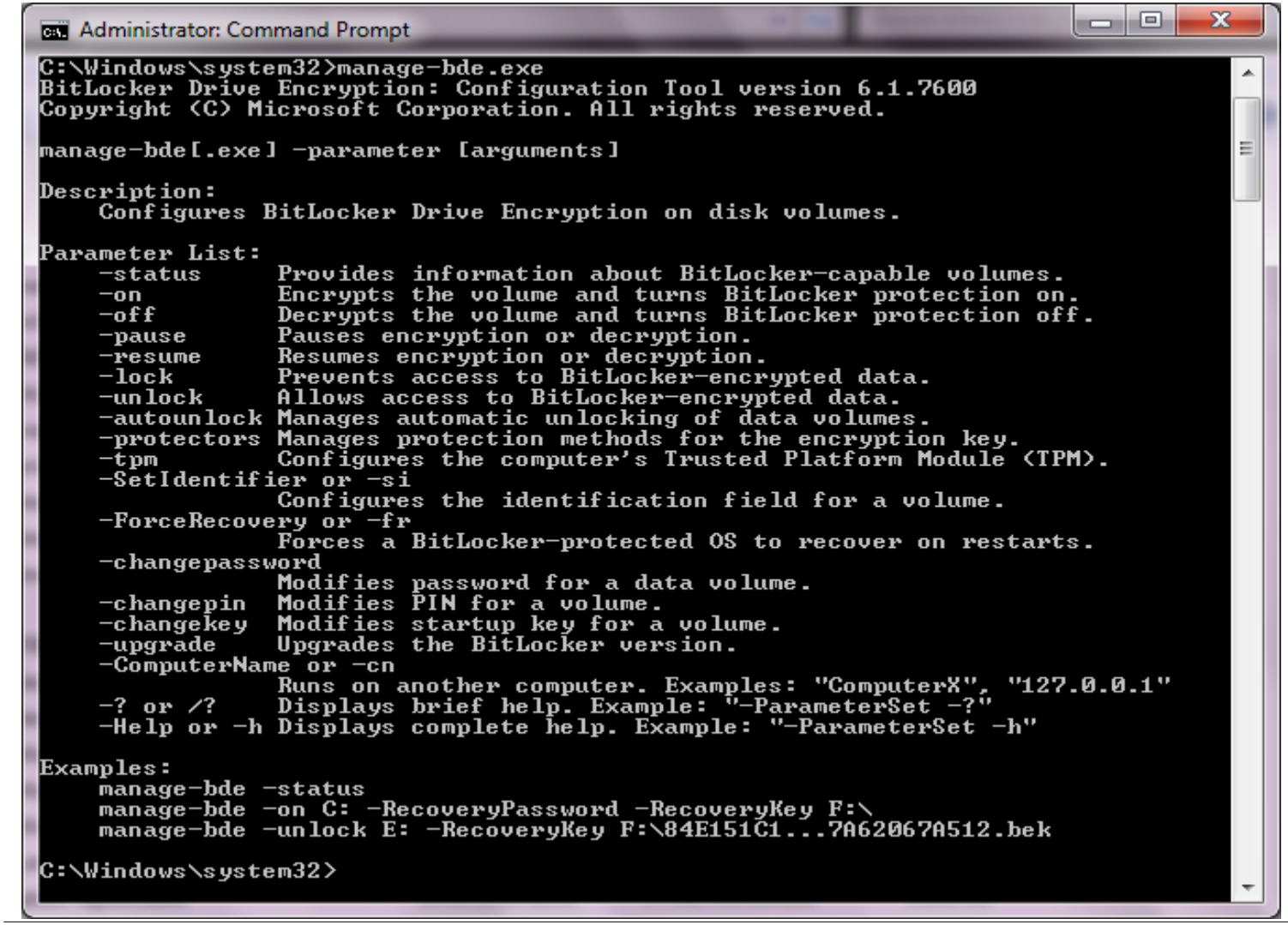


Signatur beginnt nun mit Hex EB 58 statt EB 52 wie bei Vista

Typischer Header „-FVE-FS-“ ist jedoch noch vorhanden

X-Ways Forensics kennzeichnet die Partition bereits als BitLocker

Änderungen bei BitLocker:
Neues Management-Tool „manage-bde.exe“

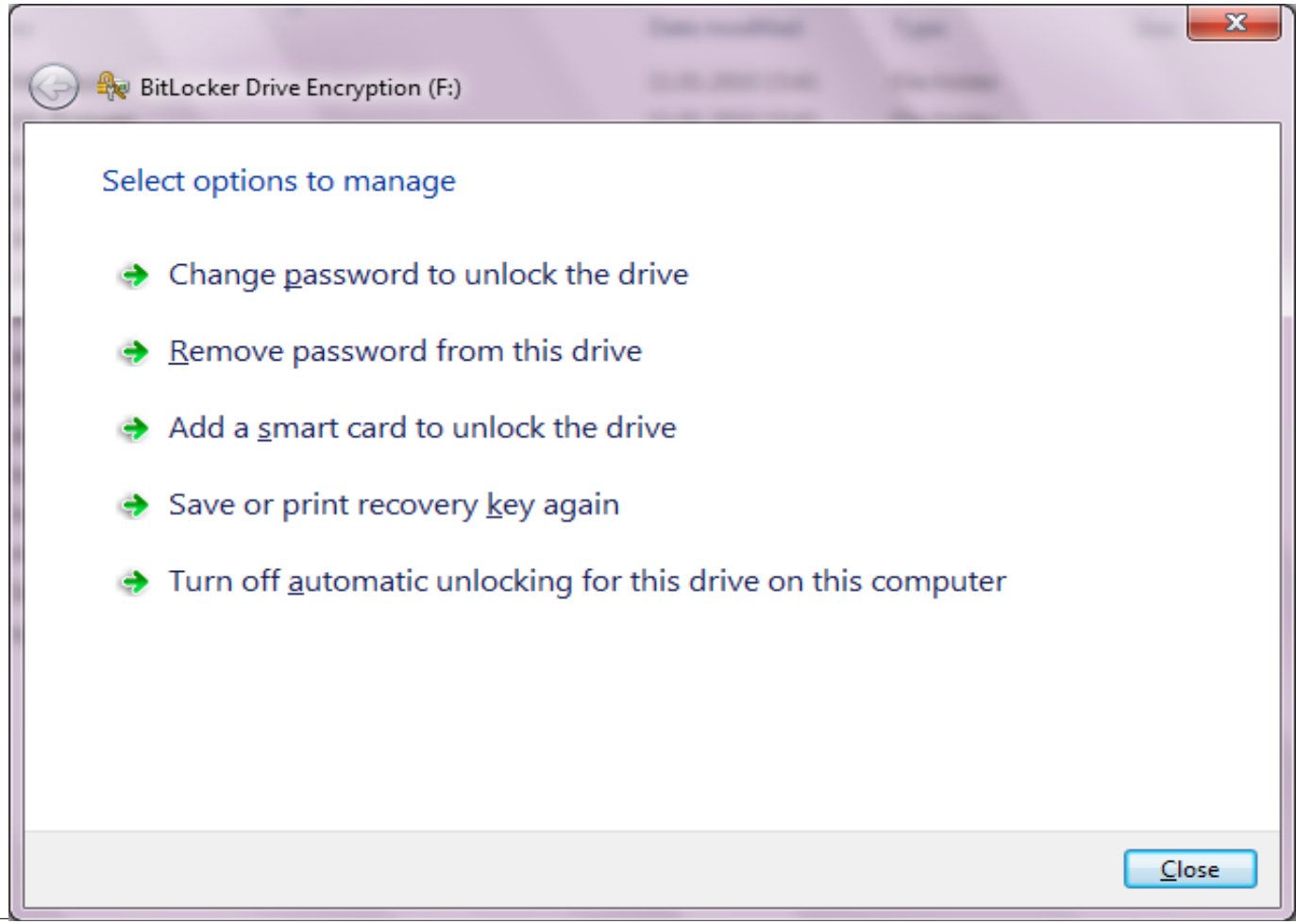


Änderungen bei BitLocker: BitLocker To Go

BitLocker für mobile Datenträger

Verschlüsselungsoptionen „To Go“:

- Passwort,
- Smart Card und
- Automatic Unlocking
- Kombinationen davon sind möglich



Änderungen bei BitLocker: BitLocker To Go

Hohe Integration in das Betriebssystem:

- Automatische Passwortabfrage und anschließendes Mounten
- Über „Hardware sicher entfernen“ wird auch automatisch die Verschlüsselung berücksichtigt
- BitLocker To Go kann auch ohne Nutzung von BitLocker für die internen Platten eingesetzt werden
- Unterstützung von FAT, FAT32, exFAT und NTFS
- Read-only Zugriff auch für ältere Betriebssysteme über „BitLocker To Go Lesetool“
- Verschlüsselung mobiler Datenträger kann durch Group Policy erzwungen werden
  (sonst wird nur Lesezugriff gestattet)

KPMG

cutting through complexity™

Ordner Virtualisierung

Ordner Virtualisierung

Seit Windows Vista sind bestimmte Systemordner für normale Benutzer (= Nicht-Admins) nur eingeschränkt im Zugriff.

Microsofts Ziel hierbei war eine höhere Systemstabilität – normaler Benutzer sollen die Stabilität des Systems nicht einfach durch Überschreiben zentraler Dateien beeinträchtigen können.

Dies betrifft die folgenden Ordner des Systemlaufwerks. In diese können normale Benutzer nicht schreiben. Statt dessen werden Schreibzugriffe „virtualisiert“:

Geschützter Ordner	Umgeleiteter Zielordner
\Program Files	\Users\[username]\AppData\Local\VirtualStore\Program Files
\ProgramData	\Users\[username]\AppData\Local\VirtualStore\ProgramData
\Windows	\Users\[username]\AppData\Local\VirtualStore\Windows

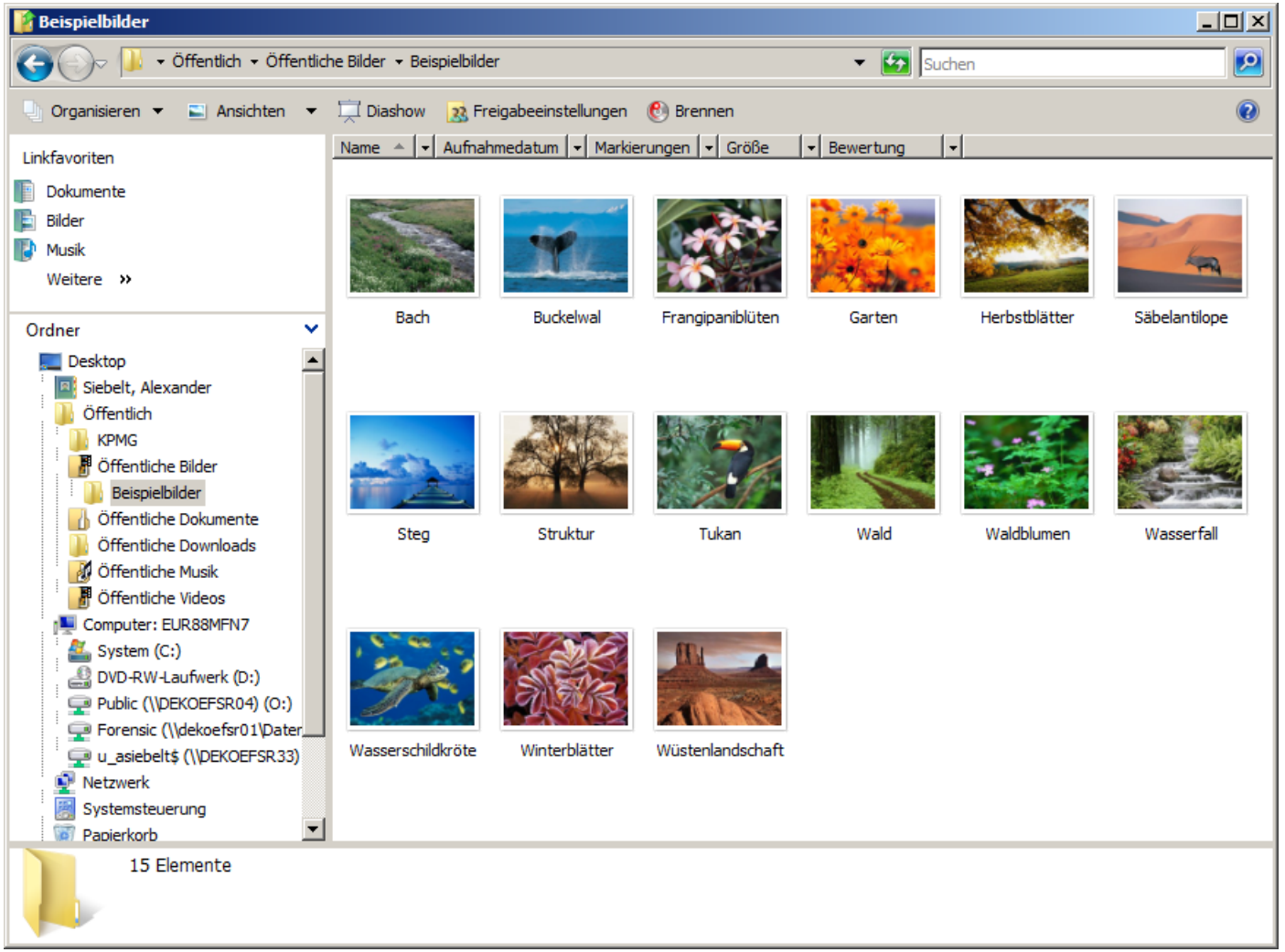
Für den normalen Benutzer ist der geänderte Zielordner nicht erkennbar – er muss jedoch bei der forensischen Analyse berücksichtigt werden!

KPMG

cutting through complexity™

Thumbcache Dateien

Thumbcache-Dateien



- Thumbcaches speichern die Vorschaubilder der Explorer-Symbolansichten zwischen
- Es gibt mehrere Thumbcache-Dateien für Vorschaubilder in unterschiedlichen Größen

Änderungen am Format der Thumbcache-Dateien

Früher existierten Thumbnail-Dateien `thumbs.db` pro Ordner, in dem Windows einmal Bilder in der Vorschaufunktion angezeigt hat

- Diese sind seit Windows Vista abgelöst

Es gibt nun zentrale Thumbcache-Dateien pro User im Ordner `\Users\[username]\AppData\Local\Microsoft\Windows\Explorer`

Die Dateien heißen thumbcache_NNN.db

- Die „NNN“ sind abhängig von der Auflösung der darin hinterlegten Bilder

Leicht geänderter Dateiheader:

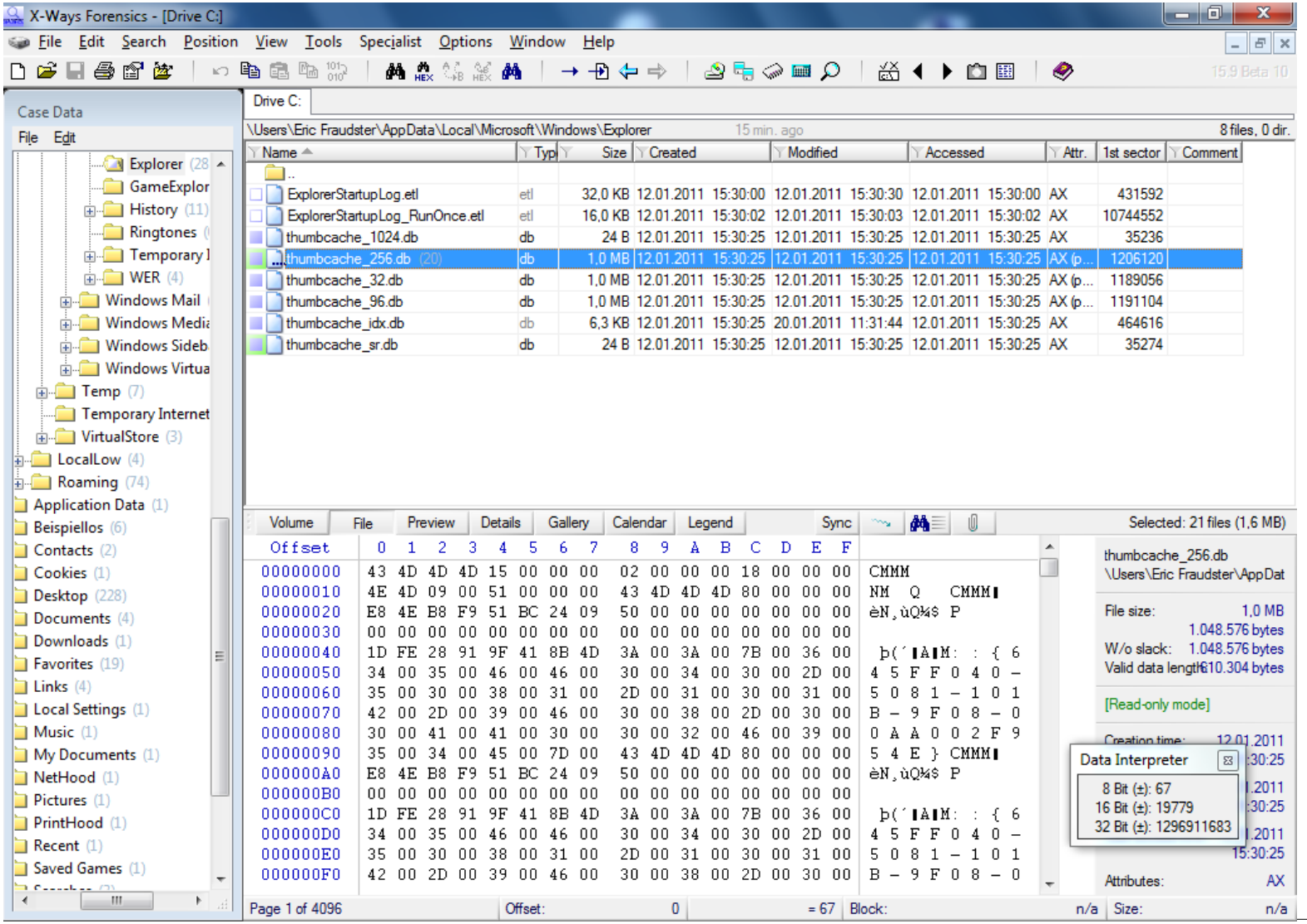
- Vista: 43 4D 4D 4D 14
- Win7: 43 4D 4D 4D 15

Das Windows 7 Format wird mit EnCase 6.16 momentan noch nicht unterstützt; X-Ways Forensics ab 15.6 funktioniert jedoch

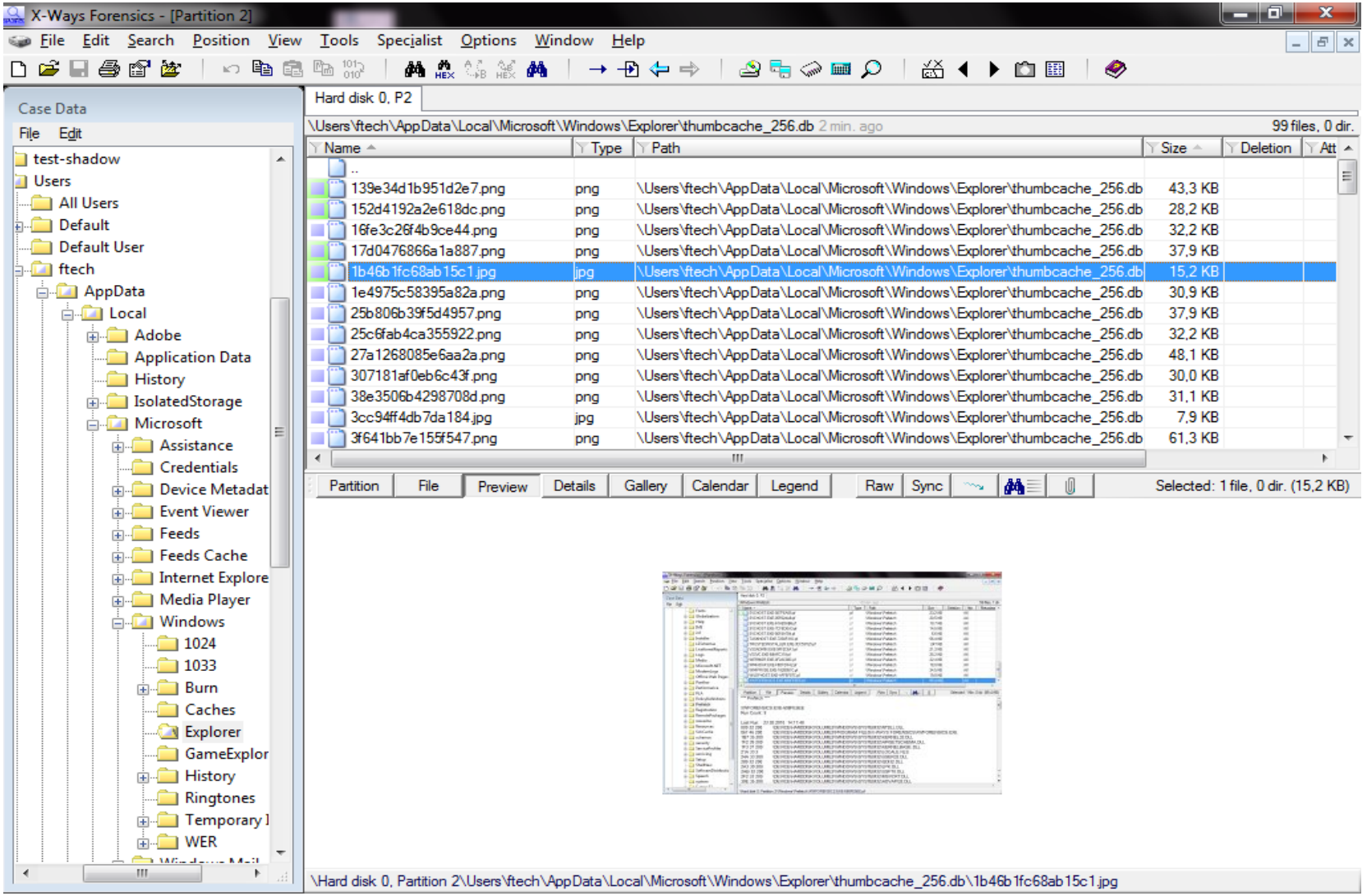
Mit X-Ways Forensics können die in den Thumbcaches hinterlegten Bilder extrahiert und im Dateibrowser angezeigt werden

- (siehe Screenshot)

Liste Thumbcache-Dateien in X-Ways Forensics



Anzeigen der extrahierten Bilder aus einer Thumbcache-Datei



KPMG

cutting through complexity™

Prefetch-Dateien

Prefetch-Dateien

Microsoft Betriebssysteme nutzen seit Windows XP Prefetch-Dateien, um die Performance beim Start von Applikationen zu erhöhen.

Die Prefetch-Dateien enthalten Informationen über die Dateien, die beim Start einer Applikation nachgeladen werden müssen.

Einige weitere Informationen machen die Analyse von Prefetch-Files für die forensische Untersuchung interessant:

- Sie enthalten Informationen über die gestarteten Programme
- Sie enthalten Informationen über die Häufigkeit der Programmstarts
- Sie enthalten Informationen über den Zeitpunkt des letzten Programmstarts
- Sie enthalten Informationen über die durch das Programm geöffneten Dateien

Neben der Optimierung von Programmstarts besteht auch die Möglichkeit den Windows-Systemstart zu optimieren („Boot Prefetching“).

Die Prefetch-Dateien werden im Ordner \Windows\Prefetch abgelegt.

Die Inhalte der Prefetch-Dateien werden von Zeit zu Zeit in die Datei \Windows\Prefetch\layout.ini übertragen. Diese Informationen werden durch das Defragmentierungstool genutzt, um Dateien optimaler auf der Festplatte anzuordnen.

Bei Solid State Drives (SSDs) ist die Erstellung von Prefetch-Dateien standardmäßig deaktiviert.

Prefetch-Dateien

Beide Optimierungen können getrennt voneinander über den folgenden Registry-Schlüssel aktiviert oder deaktiviert werden:

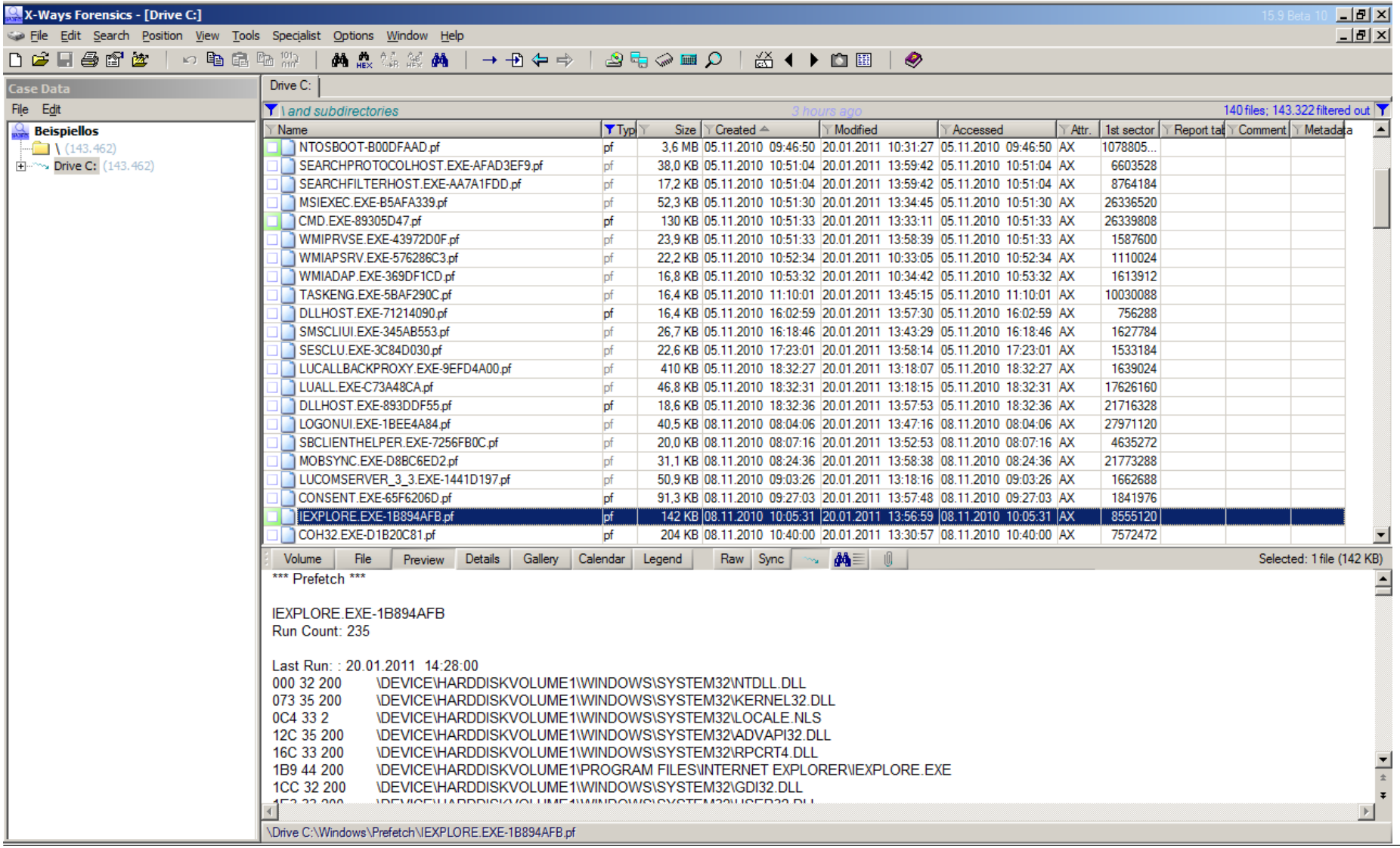
- `HKLM\System\ControlSet00X\Control\Session Manager\Memory Management\Prefetch Parameters`

Schlüsselwert	Funktion	Anmerkung
0	Beide Prefetching-Arten deaktiviert	
1	Nur Application Prefetching aktiviert	
2	Nur Boot Prefetching aktiviert	Standard bei Windows 2003
3	Application und Boot Prefetching aktiviert	Standard bei Windows XP, Vista und 7

Analyse von Prefetch-Dateien

- Die Prefetch-Dateien befinden sich im Ordner \Windows\Prefetch des Systemlaufwerkes
- Dort werden die Dateien mit der Endung .pf hinterlegt
- Der Dateiname besteht aus dem Dateinamen der ausgeführten Datei (bspw. OUTLOOK.EXE), gefolgt von einem hexadezimalen Hashwert, der aus dem Ordner, in dem die ausführbare Datei liegt, berechnet wird
- Wird also eine gleichbenannte Datei aus unterschiedlichen Ordnern heraus ausgeführt, führt dies zu mehreren Prefetch-Dateien
- Im Dateiinhalt der Prefetch-Dateien befinden sich u.a. die Anzahl der Programmstarts und der Zeitpunkt des letzten Programmstarts
- Diese Informationen können komfortable mit Hilfe von X-Ways Forensics über die „Preview-Funktion“ angezeigt werden
- Auch der Pfad der ausführbaren Daten lässt sich aus den Inhalten der .pf-Datei entnehmen
- Die Boot Prefetching-Datei heißt immer „NTOSBOOT-B00DFAAD.pf“ und wird im selben Ordner abgelegt

Screenshot: Analyse Prefetch-Dateien in X-Ways Forensics



Forensischer Nutzen von Prefetch-Dateien

Anhand der Prefetch-Dateien kann im Rahmen von Untersuchungen festgestellt werden, wann welche Anwendungen gestartet wurden

Durch die Existenz von Prefetch-Dateien kann nachgewiesen werden, dass Programme auf dem Rechner vorhanden waren und ausgeführt wurden, auch wenn diese zwischenzeitlich schon wieder vom Rechner entfernt wurden

Durch die Zeitstempel der Prefetch-Dateien können weitere Informationen gewonnen werden:

- Der Erstellungszeitstempel definiert den erstmaligen Start der Anwendung
- Der Modifikationszeitstempel definiert den letztmaligen Start der Anwendung

Im Zusammenhang mit anderen Datenquellen, wie etwa den Event Logs, kann der Programmstart einzelnen Benutzern zugeordnet werden

KPMG

cutting through complexity™

Verknüpfungen (LNK-Dateien)

Verknüpfungen (LNK-Dateien)

Verknüpfungen werden an vielen Stellen des Windows-Betriebssystems verwendet, u.a. auch im Startmenü

Eine für forensische Untersuchungen interessante Stelle, an der Verknüpfungen genutzt werden, sind die sog. „Recent“-Ordner

Windows speichert in den Ordnern die zuletzt geöffneten Dateien

- \Users\[username]\AppData\Roaming\Microsoft\Windows\Recent

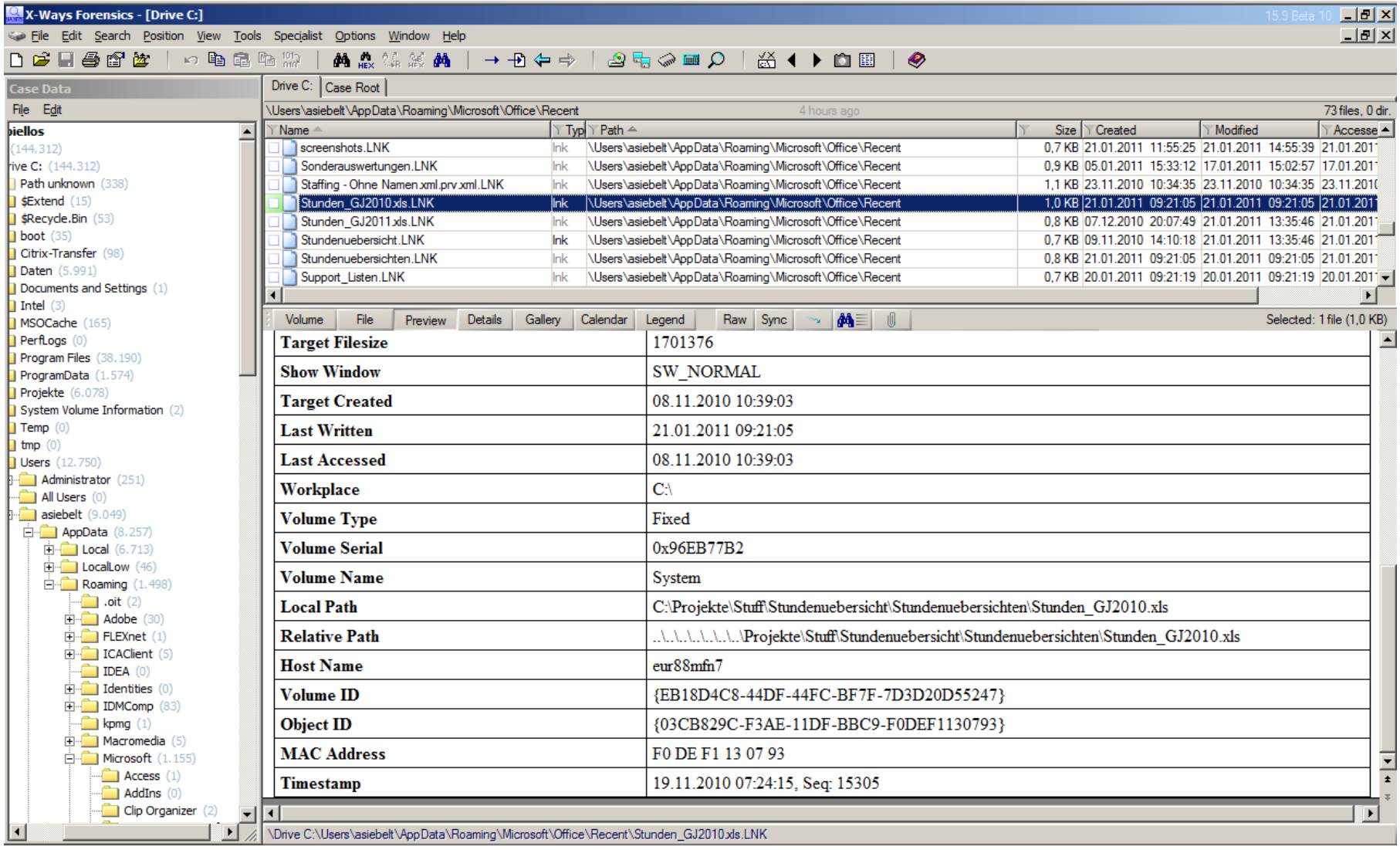
Für jede geöffnete Datei wird dort eine Verknüpfung hinterlegt.

Diese Daten werden u.a. genutzt, um im Startmenü die Liste der zuletzt geöffneten Dateien anzuzeigen.

Falls Microsoft Office im Einsatz ist, werden mit Office geöffnete Dateien zusätzlich hier als Verknüpfung hinterlegt:

- \Users\[username]\AppData\Roaming\Microsoft\Office\Recent

Detailansicht einer Verknüpfung im “Recent”-Ordner



Verknüpfungen (LNK-Dateien)

Die MAC-Zeitstempel der Verknüpfung können analysiert werden:

- Der Zeitpunkt der Erstellung der Verknüpfung fällt auf das erste Öffnen des Dokuments
- Die letzte Änderungszeit der Verknüpfung definiert den Zeitpunkt der letzten Öffnung des Dokuments

In den Verknüpfungen selbst sind einige weitere Artefakte gespeichert:

- MAC-Zeitstempel der Quelldatei
- Informationen über das Volume (Name, Art, Laufwerksbuchstabe), auf dem die Quelldatei liegt
- Ursprünglicher Ordner, in dem die Quelldatei liegt
- Größe der Quelldatei

Forensischer Nutzen der Analyse der Verknüpfungen

Es werden auch Dokumente angezeigt, die sich niemals auf der analysierten Festplatte befunden haben

Möglicherweise können relevante Netzwerk-Shares identifiziert werden

Sehr ergiebige Datenquelle, um die tatsächliche Nutzung des PCs nachzuvollziehen

KPMG

cutting through complexity™

Volume Shadow Copies

Volume Shadow Copies: Grundlagen

Seit Windows 2003 gibt es den sog. „Volume Shadow Copy Service“ (VSS), der im Hintergrund mehrere Versionen von Dateien vorhält

Seit Windows Vista und auch in Windows 7 ist dieser Dienst standardmäßig aktiviert

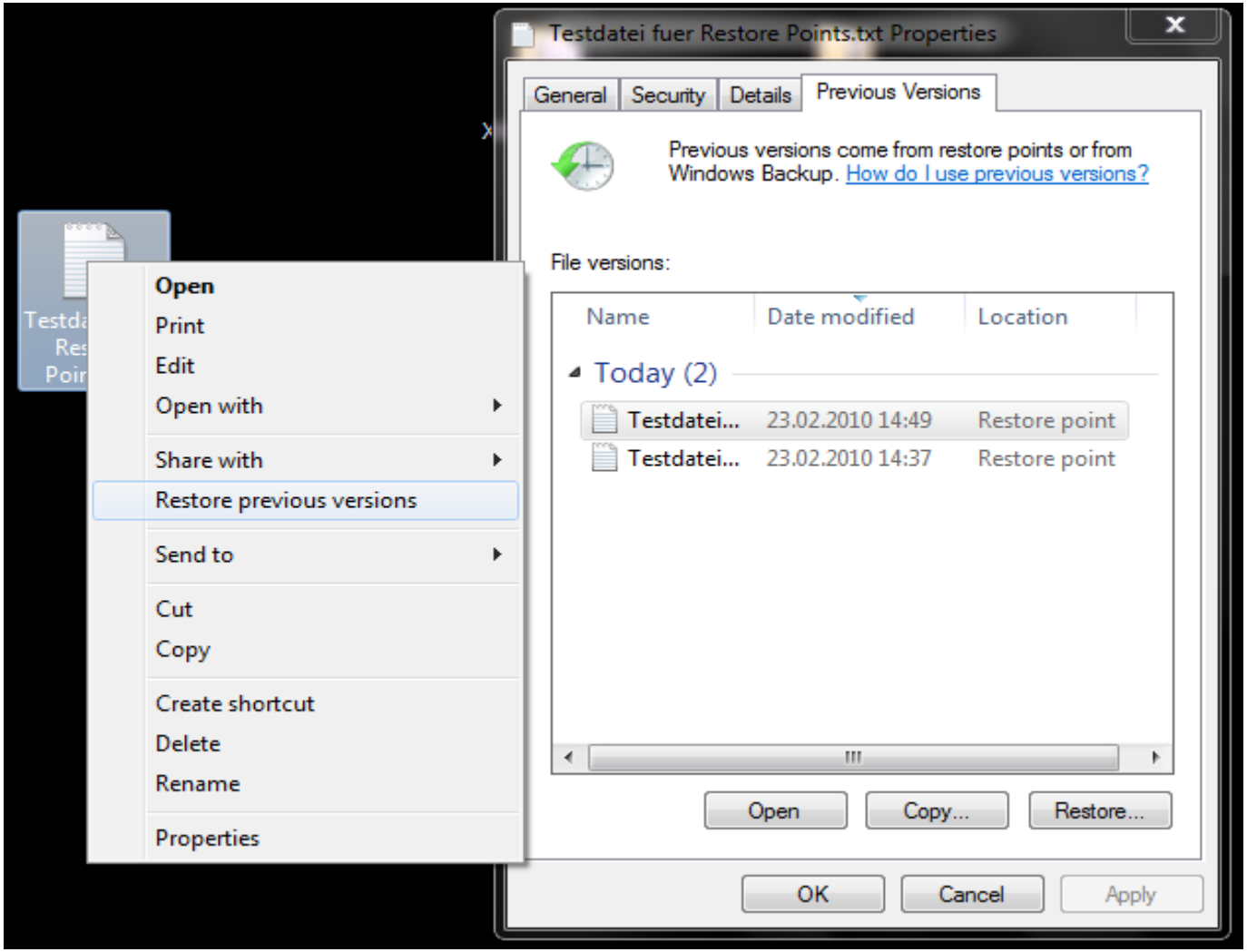
Die gesicherten Daten werden im Verzeichnis „System Volume Information“ abgelegt

Schattenkopien dienen als einheitliche Datenquelle für zwei Funktionen:

- Restore Points
- Previous Versions

Schattenkopien ersetzen die „Restore Points“-Funktionalität aus den Windows-Versionen vor Vista

Volume Shadow Copies: Wiederherstellen einzelner Dateien / Previous Versions

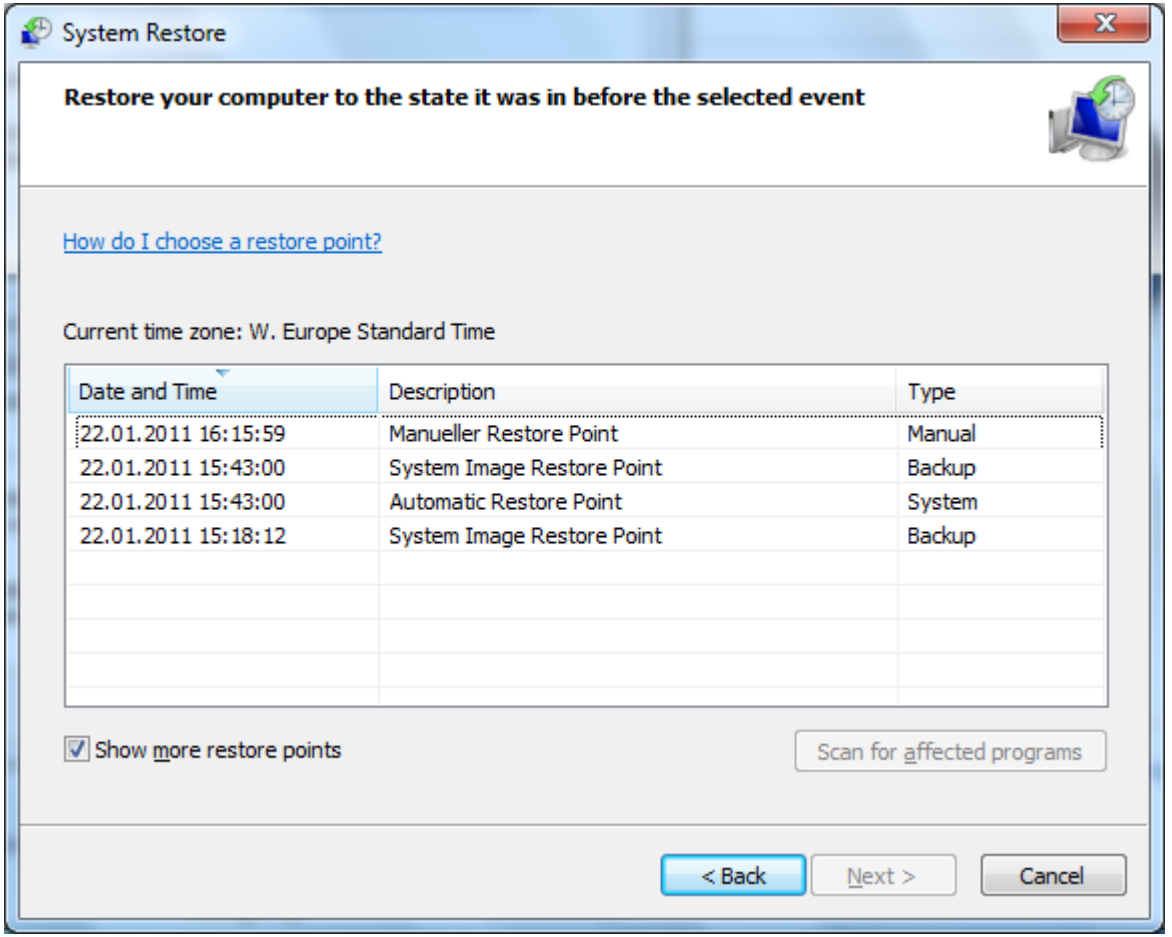


Gespeicherte vorherige Versionen von Dateien können:

- An eine beliebige Stelle kopiert werden („Copy“)
- Wiederhergestellt werden und damit die aktuelle Fassung ersetzen („Restore“)

Im 2. Fall geht die aktuelle Version der Datei verloren.

Volume Shadow Copies: Wiederherstellen des gesamten Systems



Volume Shadow Copies: Erstellung von Schattenkopien

Unter Windows 7 werden zu folgenden Ereignissen Schattenkopien erstellt:

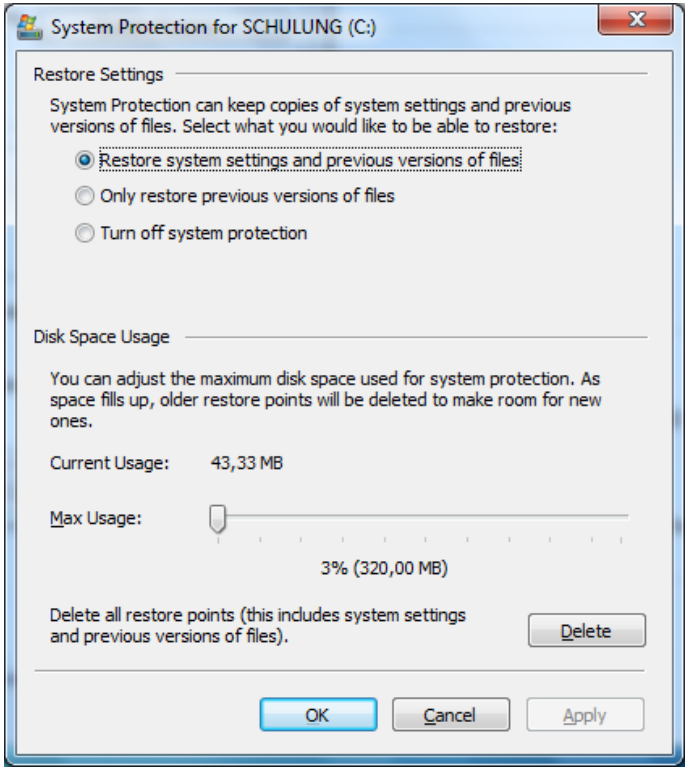
- Manuell erstellt
- Alle 7 Tage automatisch (Vista: alle 24 Stunden)
- Vor einem Windows-Update oder der Installation eines unsignierten Treibers
- Anwendung, die eine Sicherung über die Windows-API anfordert

Daten aus Schattenkopien werden (standardmäßig) entfernt, wenn…

…mehr als 5% des Speichers bei einer Partition >64GB…

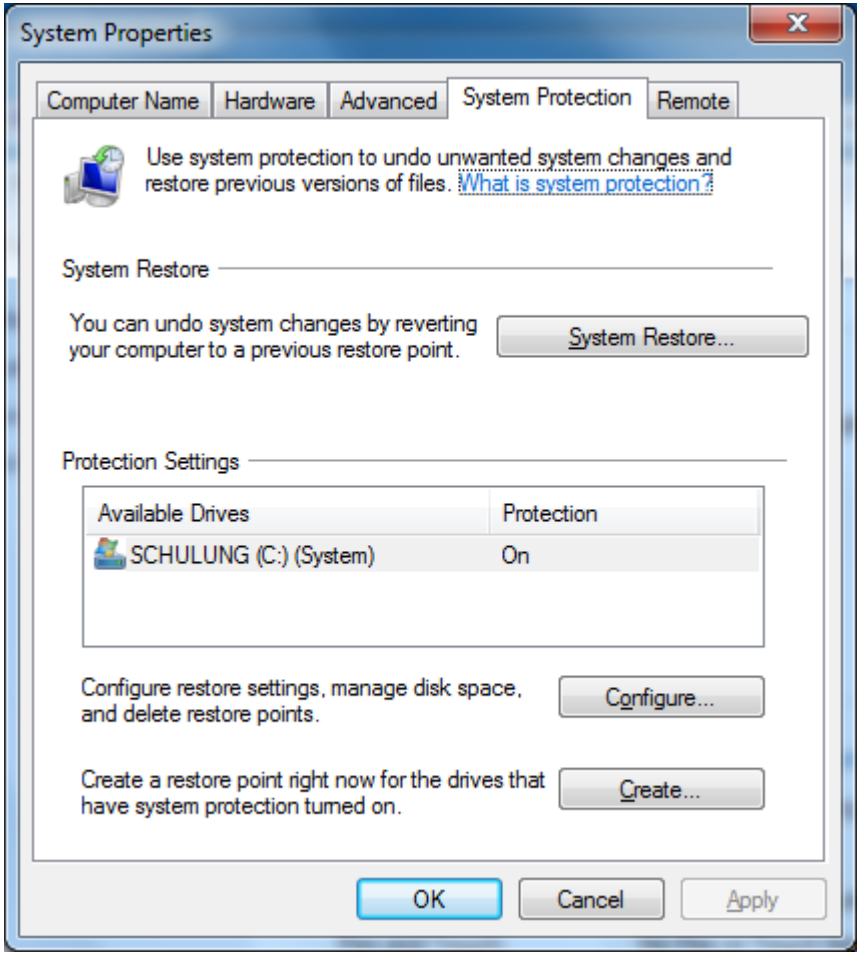
…mehr als 3% des Speichers bei einer Partition <64GB…

belegt sind.



Volume Shadow Copies: Manuelle Erstellung

Control panel -> System -> System protection



Volume Shadow Copies: Forensischer Nutzen

Schattenkopien bleiben erhalten, selbst wenn die zugehörigen Quelldateien gelöscht, gewiped oder verschlüsselt werden

Frühere Versionen von Dateien können aus Schattenkopien wiederhergestellt werden

Daher sind Schattenkopien ein wichtiges Element im Rahmen der Analyse gelöschter Dateien

Volume Shadow Copies: Technische Funktionsweise

Wichtig für das Verständnis der Funktionsweise ist das sog. „Copy-on-Write“-Konzept:

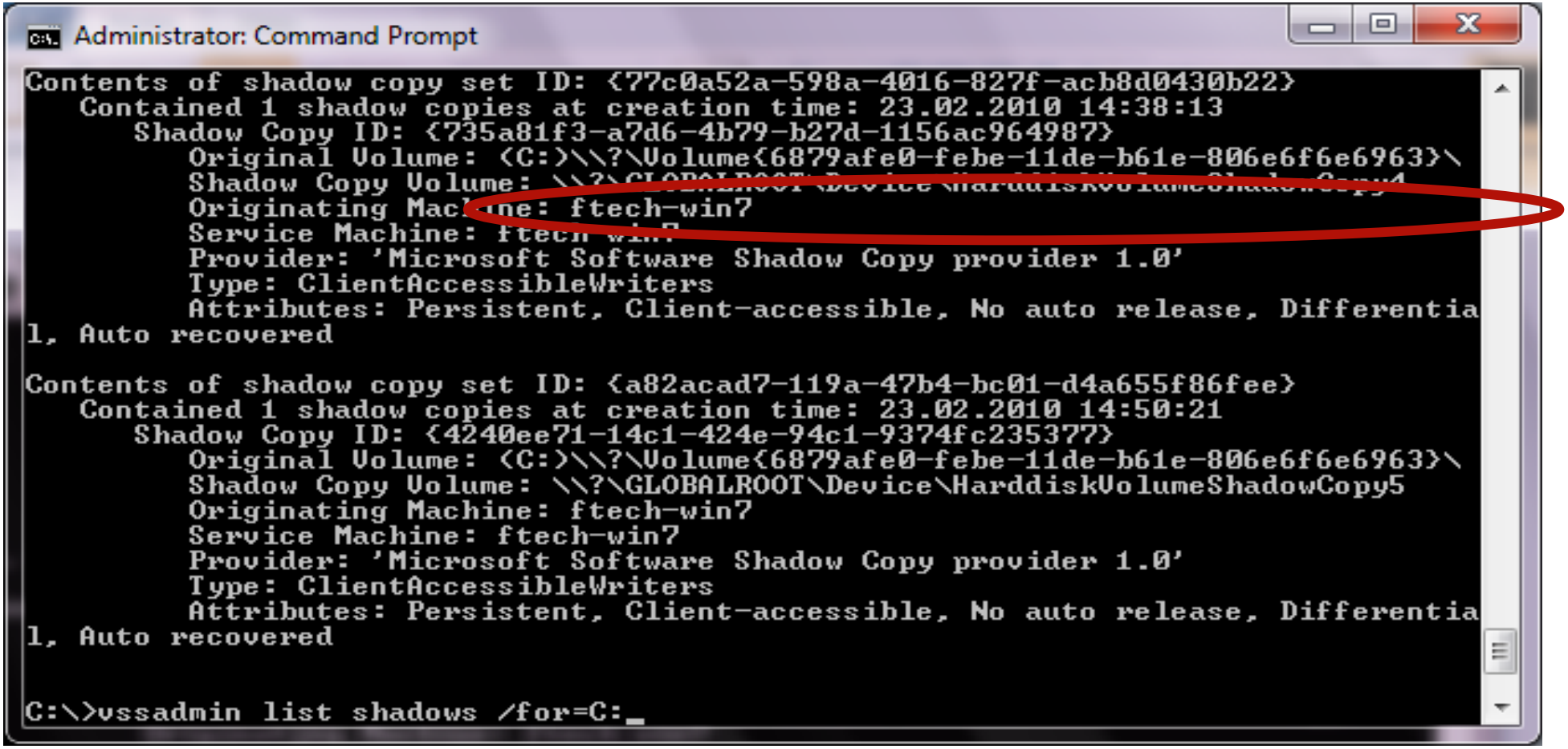
Änderungen in eine Schattenkopie werden nur dann geschrieben, wenn die Originaldatei geändert wurde

- Daher funktioniert die Erstellung eines kompletten Restore Points auch so schnell!

Es wird pro Schattenkopie nur die jeweils letzte Änderung an einer Datei gespeichert

- Als Konsequenz daraus wird also nicht jede Änderung gesichert, sondern nur falls zwischenzeitlich eine neue Schattenkopie angelegt wurde

Volume Shadow Copies: Anzeigen vorhandener Schattenkopien



Volume Shadow Copies: Forensische Analyse

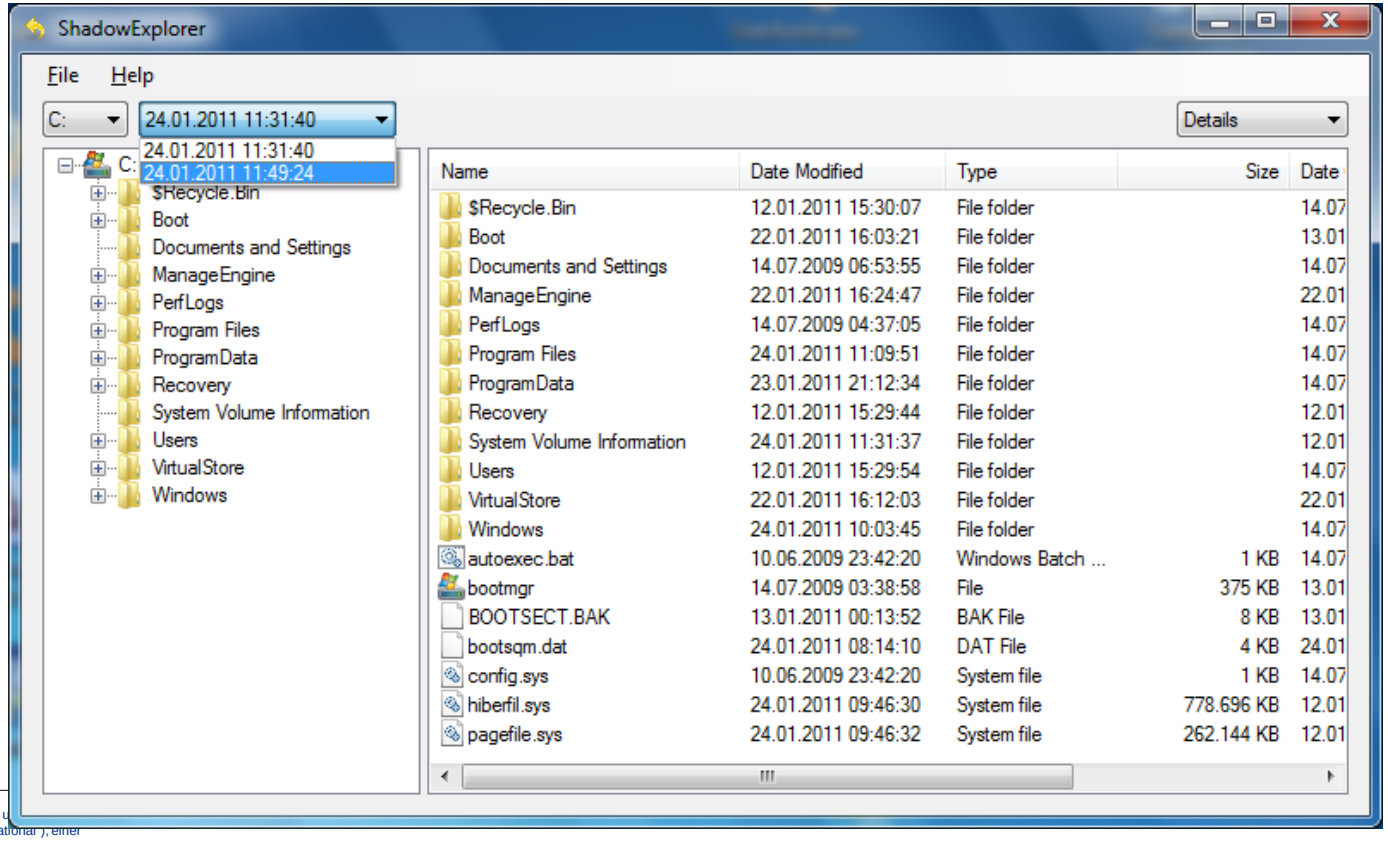
Anhand des Shadow Copy Volume Identifiers kann auf eine Schattenkopie live zugegriffen werden:

```
mklink /d c:\vss-test \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4\
```

Der Befehl erstellt einen Link auf die Schattenkopie

- In „c:\vss-test“ befindet sich dann die Ordneransicht zum Zeitpunkt der Erstellung der Schattenkopie

Alternativ kann hierzu auch das kostenfreie Tool „ShadowExplorer“ genutzt werden:



Volume Shadow Copies: Forensische Analyse

Der Shadow Copy Volume Identifier kann auch als Quelle für eine Image-Erstellung genutzt werden:

```
dd if=\\.\HarddiskVolumeShadowCopy4 of=192.168.0.1 --iport 3000
```

- Erstellt ein Image über das Netzwerk, das etwa mit Hilfe von Netcat auf dem Zielrechner geschrieben werden kann
- Das Image stellt die Sicht auf den Datenträger zum Zeitpunkt der Erstellung der Schattenkopie dar
- Das Image kann dann als logischer Datenträger in übliche Forensik-Tools importiert und näher analysiert werden

Volume Shadow Copies: Forensische Analyse

Das Image einer Shadow Copy hat die selbe Größe wie die Quellpartition

Durch die potentiell hohe Anzahl von Shadow Copies ergeben sich auch sehr große Datenmengen, die auszuwerten sind

- Ggfs. Einschränkung möglich auf Basis des vermuteten Tatzeitraumes
- Durch Bildung von Hashsets und einen entsprechenden Abgleich können die bereits aus anderen Schattenkopien bekannten Dateiversionen ausgeblendet werden

KPMG

cutting through complexity™

Windows Event Logs

Windows Event Log
.evtx Format

Mit Windows Vista wurde das Format für die Eventlogs geändert – es handelt sich jetzt um ein binär kodiertes XML-Format

- Im Zuge des Wechsels des Datenformates haben sich auch die Event IDs geändert

Die Dateien sind im folgenden Ordner abgelegt:
`\windows\system32\winevt\Logs`

Es werden verschiedenartige Ereignisse in separate Dateien gespeichert sogenannte „Channels“:

- Die aus Windows XP noch bekannten Channels Application, Security und System sind noch vorhanden
- Zusätzlich zu den o.g. drei sind die beiden Channel Setup und Forwarded zur Windows-Logs-Gruppe zu zählen

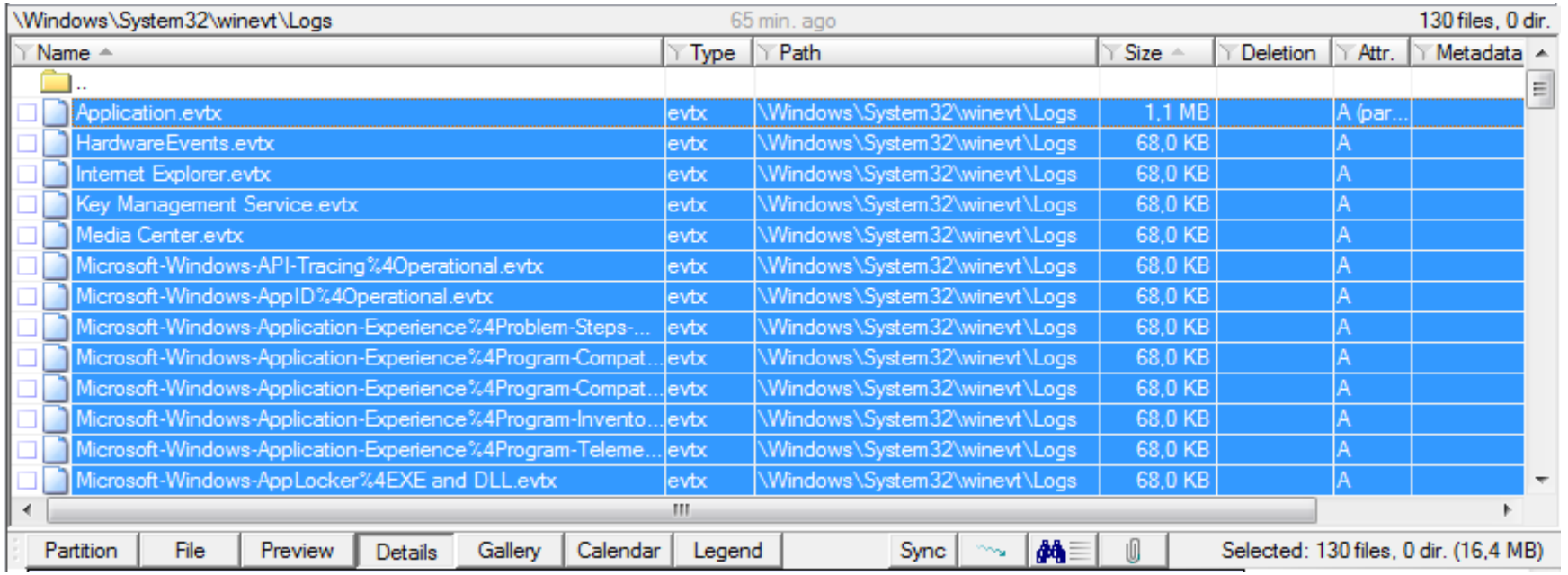
Des Weiteren lassen sich durch Anwendungen oder Servicedienste weitere Channel definieren

- Dies wird in Windows 7 noch umfangreicher als bereits bei Vista genutzt: In einer Standardinstallation sind neben den fünf Windows-Channels bereits 125 .evtx-Dateien vorhanden

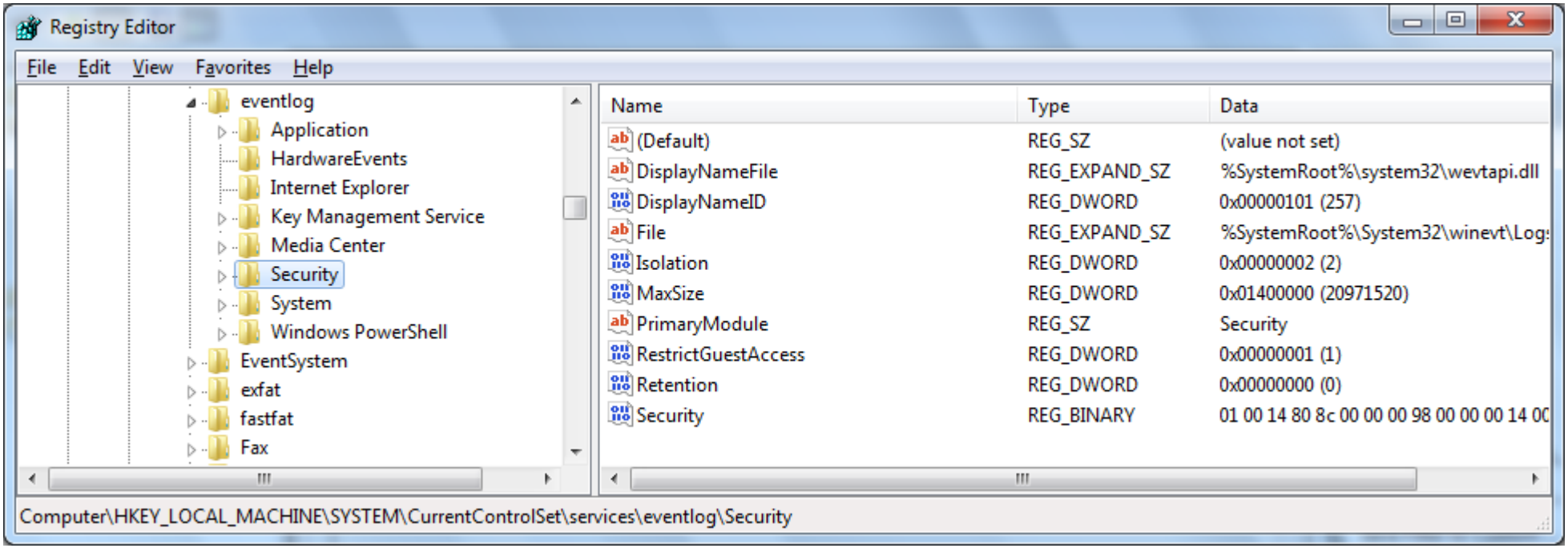
Mit Windows wird ein Event Viewer mitgeliefert, der das .evtx-Format lesen und exportieren kann

- eventvwr.msc
- Exporte sind möglich als .evtx, .xml, .txt und .csv
- Auch das alte .evt-Format lässt sich öffnen

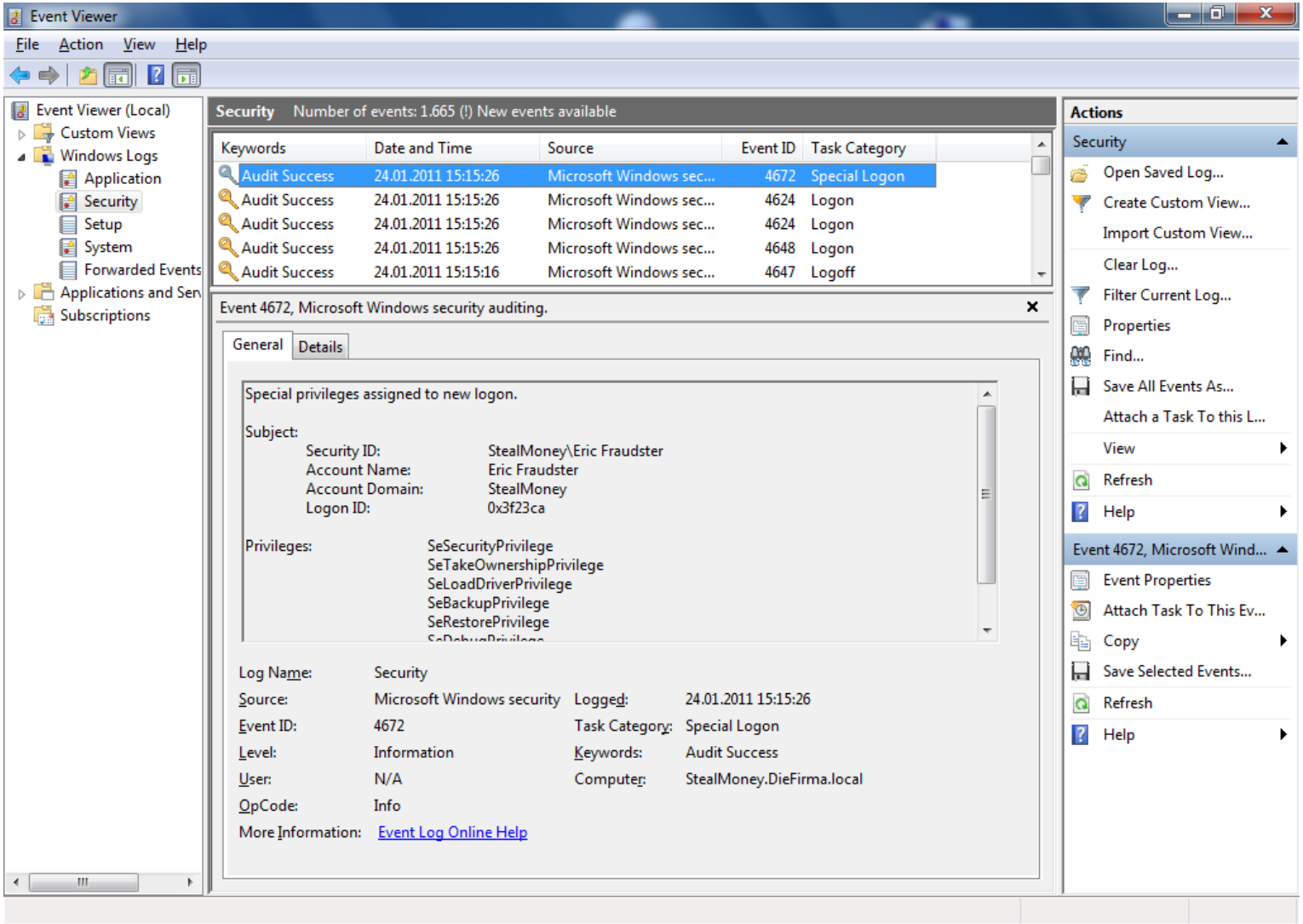
Windows Event Log: Ablageort der Dateien



Windows Event Log: Einstellungen in der Registry



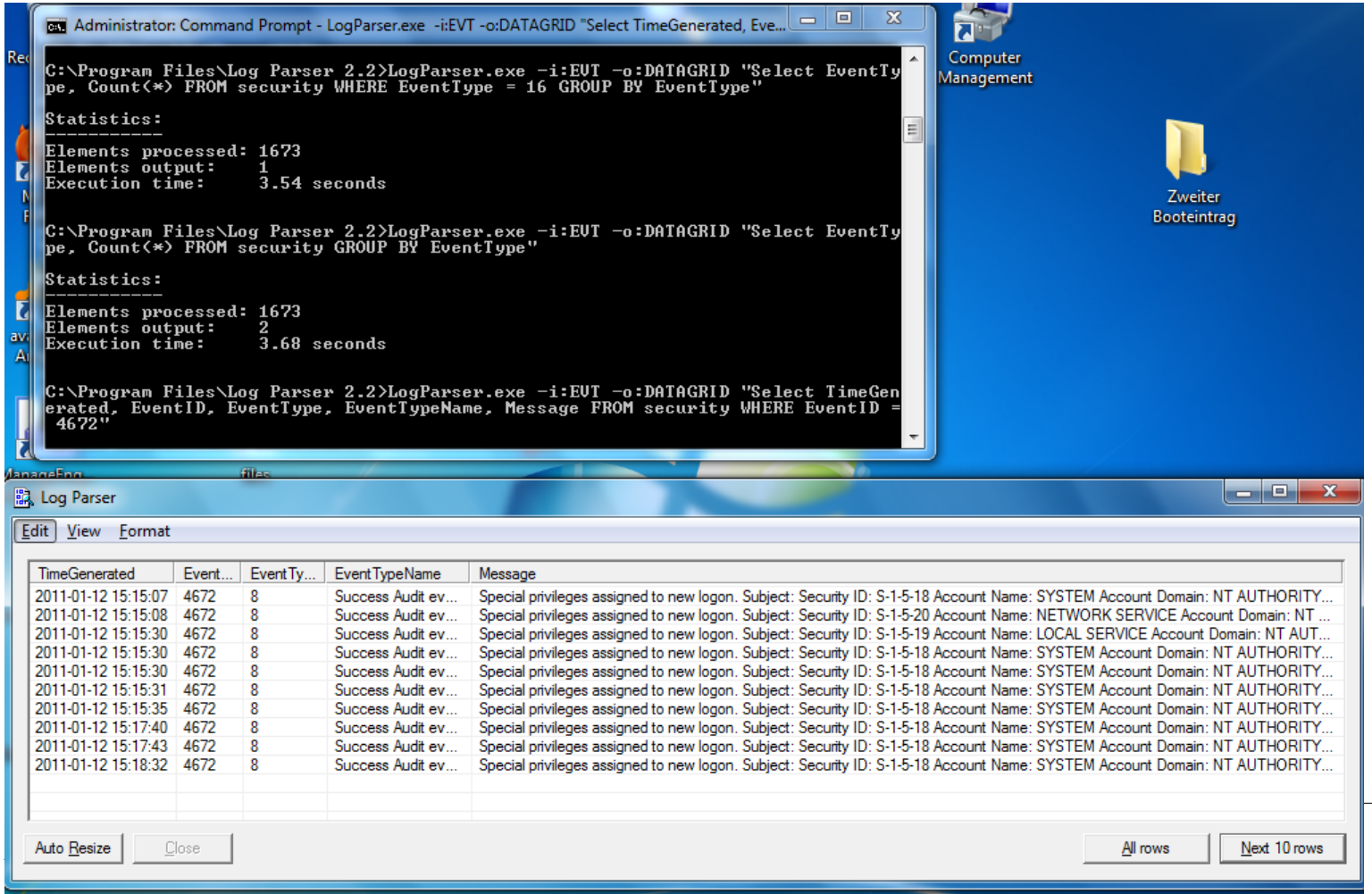
Windows Event Viewer



Evtx Parser / logparser

Mit dem Evtx Parser von Andreas Schuster lassen sich zudem Daten aus beschädigten oder gecarvten Dateien extrahieren

Zusätzlich ist eine Analyse von Event Logs mit dem Microsoft-Tool logparser möglich



Vielen Dank für die Aufmerksamkeit!

Alexander Geschonneck
Partner
Risk & Compliance

Tel. +49 30 20681520

ageschonneck@kpmg.com

KPMG AG Wirtschaftsprüfungsgesellschaft,
a subsidiary of KPMG Europe LLP