



cutting through complexity™

Windows 7 Forensik

- ein Überblick über Artefakte -

Alexander Geschonneck

Partner, KPMG Forensic Technology





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 Anforderungen. 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.



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

The screenshot shows the X-Ways Forensics interface. The main window displays the file system structure of a partition, with the \Boot directory selected. The file memtest.exe is highlighted in blue. The bottom pane shows the hex data of the selected file, with the ASCII column displaying the text "MZ" and "is program cannot".

Name	Type	Path	Size	Attr.	Metadata
Fonts		\Boot	0,7 KB		
fr-FR		\Boot	272 B		
hu-HU		\Boot	272 B		
it-IT		\Boot	272 B		
ja-JP		\Boot	272 B		
ko-KR		\Boot	272 B		
nb-NO		\Boot	272 B		
nl-NL		\Boot	272 B		
pl-PL		\Boot	272 B		
pt-BR		\Boot	272 B		
pt-PT		\Boot	272 B		
ru-RU		\Boot	272 B		
sv-SE		\Boot	272 B		
tr-TR		\Boot	272 B		
zh-CN		\Boot	272 B		
zh-HK		\Boot	272 B		
zh-TW		\Boot	272 B		
BCD		\Boot	36,0 KB	SHA	
BCD.LOG	registry	\Boot	256 KB	SHA (...)	
BCD.LOG1	log1	\Boot	0 B	SHA	
BCD.LOG2	log2	\Boot	0 B	SHA	
bootmgr		\Boot	375 KB	X	
BOOTSTAT.DAT	dat	\Boot	64,0 KB	SHA	
memtest.exe	exe	\Boot	474 KB	A	

Data Interpreter

8 Bit (±): 77
16 Bit (±): 23117
32 Bit (±): 9460301
FILETIME: 01.01.1601
00:21:29

Selected: 1 file, 0 dir. (474 KB)

memtest.exe
\Boot

File size: 476 KB
487.424 bytes
W/o slack: 485.440 bytes
Valid data length: 485.440 bytes

Page 1 of 5078 Offset: 0 = 77 Block: n/a Size: n/a



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



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

The screenshot shows a Windows Explorer window for 'Hard disk 0, P2' containing two files: 'BitLocker' (39.0 GB) and '\$Boot' (8.0 KB). Below the Explorer window, a hex editor displays the partition's signature. The hex data shows the signature starting with 'EB 58' at offset 0, which is highlighted in blue. The ASCII view shows 'ëX -FVE-FS-' at the same position. A tooltip on the right identifies the partition as 'Hard disk 0, Partition 2' with a 'File system: BitLocker' and '[Read-only mode]'.

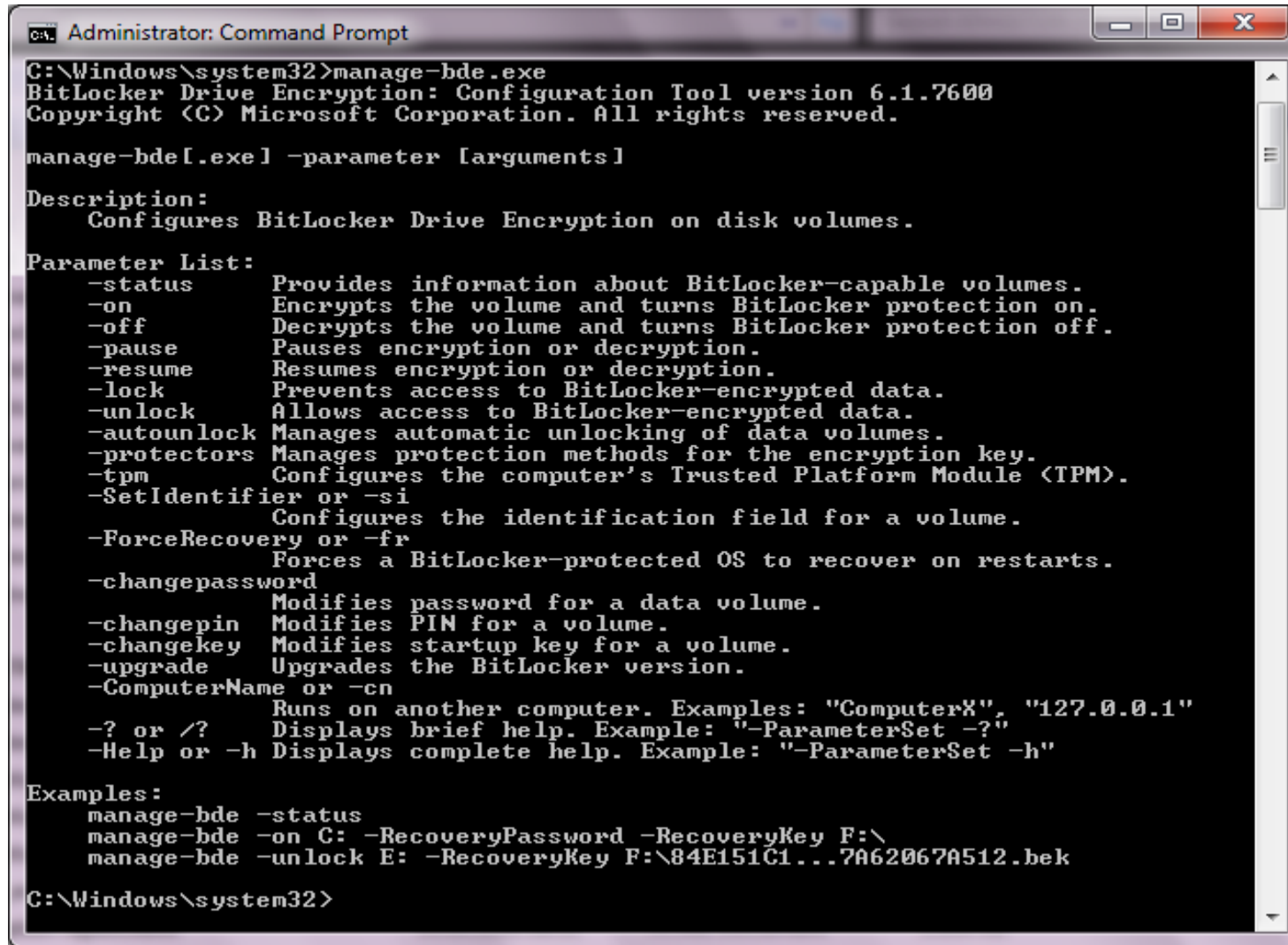
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
000000000000	EB	58	90	2D	46	56	45	2D	46	53	2D	00	02	08	00	00
000000000016	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	28	03	00
000000000032	00	00	00	00	E0	1F	00	00	00	00	00	00	00	00	00	00

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“



```
Administrator: Command Prompt
C:\Windows\system32>manage-bde.exe
BitLocker Drive Encryption: Configuration Tool version 6.1.7600
Copyright (C) Microsoft Corporation. All rights reserved.

manage-bde[.exe] -parameter [arguments]

Description:
  Configures BitLocker Drive Encryption on disk volumes.

Parameter List:
  -status          Provides information about BitLocker-capable volumes.
  -on              Encrypts the volume and turns BitLocker protection on.
  -off             Decrypts the volume and turns BitLocker protection off.
  -pause          Pauses encryption or decryption.
  -resume         Resumes encryption or decryption.
  -lock           Prevents access to BitLocker-encrypted data.
  -unlock         Allows access to BitLocker-encrypted data.
  -autounlock     Manages automatic unlocking of data volumes.
  -protectors     Manages protection methods for the encryption key.
  -tpm            Configures the computer's Trusted Platform Module (TPM).
  -SetIdentifier or -si
                  Configures the identification field for a volume.
  -ForceRecovery or -fr
                  Forces a BitLocker-protected OS to recover on restarts.
  -changepassword
                  Modifies password for a data volume.
  -changePIN      Modifies PIN for a volume.
  -changekey      Modifies startup key for a volume.
  -upgrade        Upgrades the BitLocker version.
  -ComputerName or -cn
                  Runs on another computer. Examples: "ComputerX", "127.0.0.1"
  -? or /?       Displays brief help. Example: "-ParameterSet -?"
  -Help or -h    Displays complete help. Example: "-ParameterSet -h"

Examples:
  manage-bde -status
  manage-bde -on C: -RecoveryPassword -RecoveryKey F:\
  manage-bde -unlock E: -RecoveryKey F:\84E151C1...7A62067A512.bek

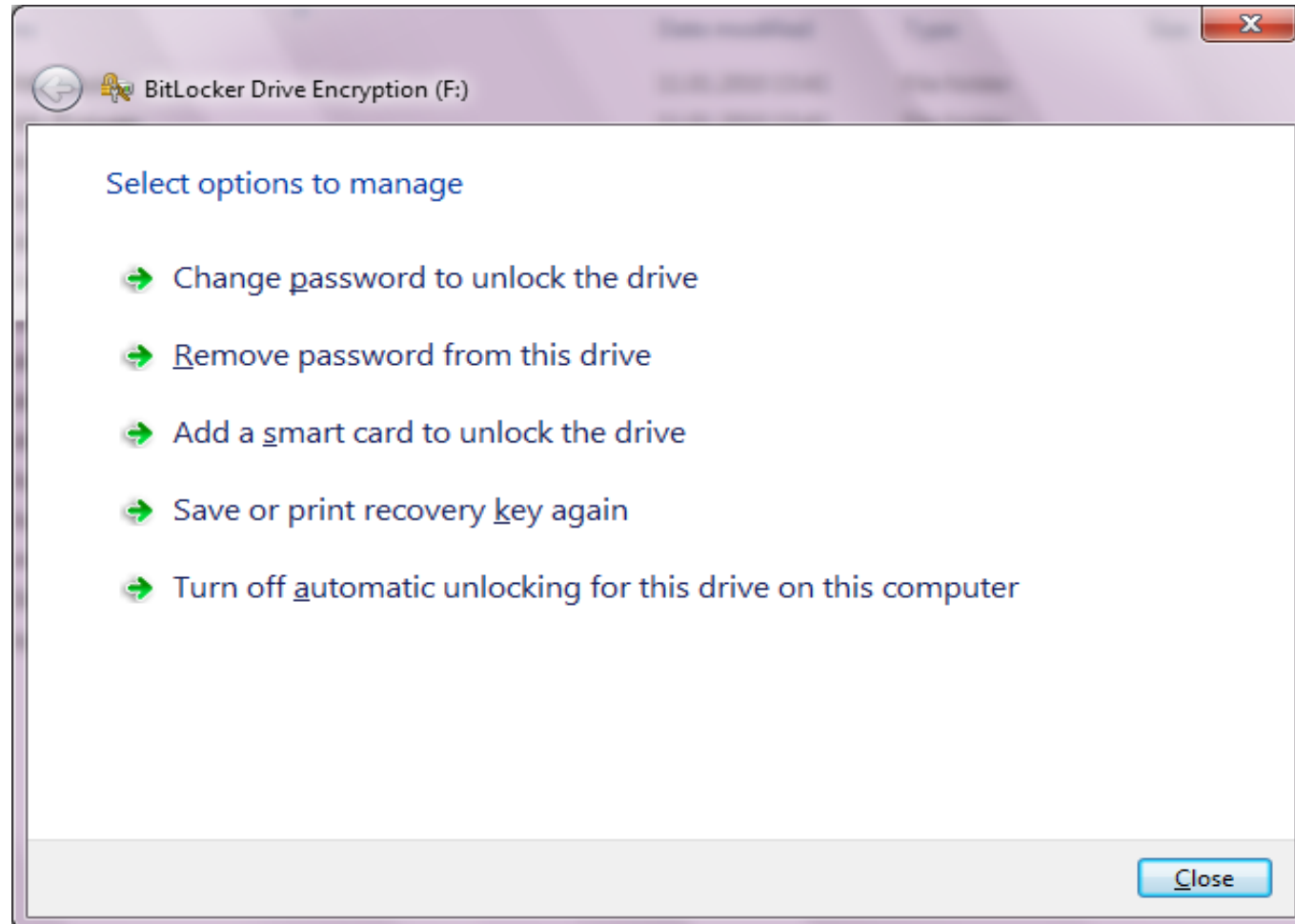
C:\Windows\system32>
```

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)



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

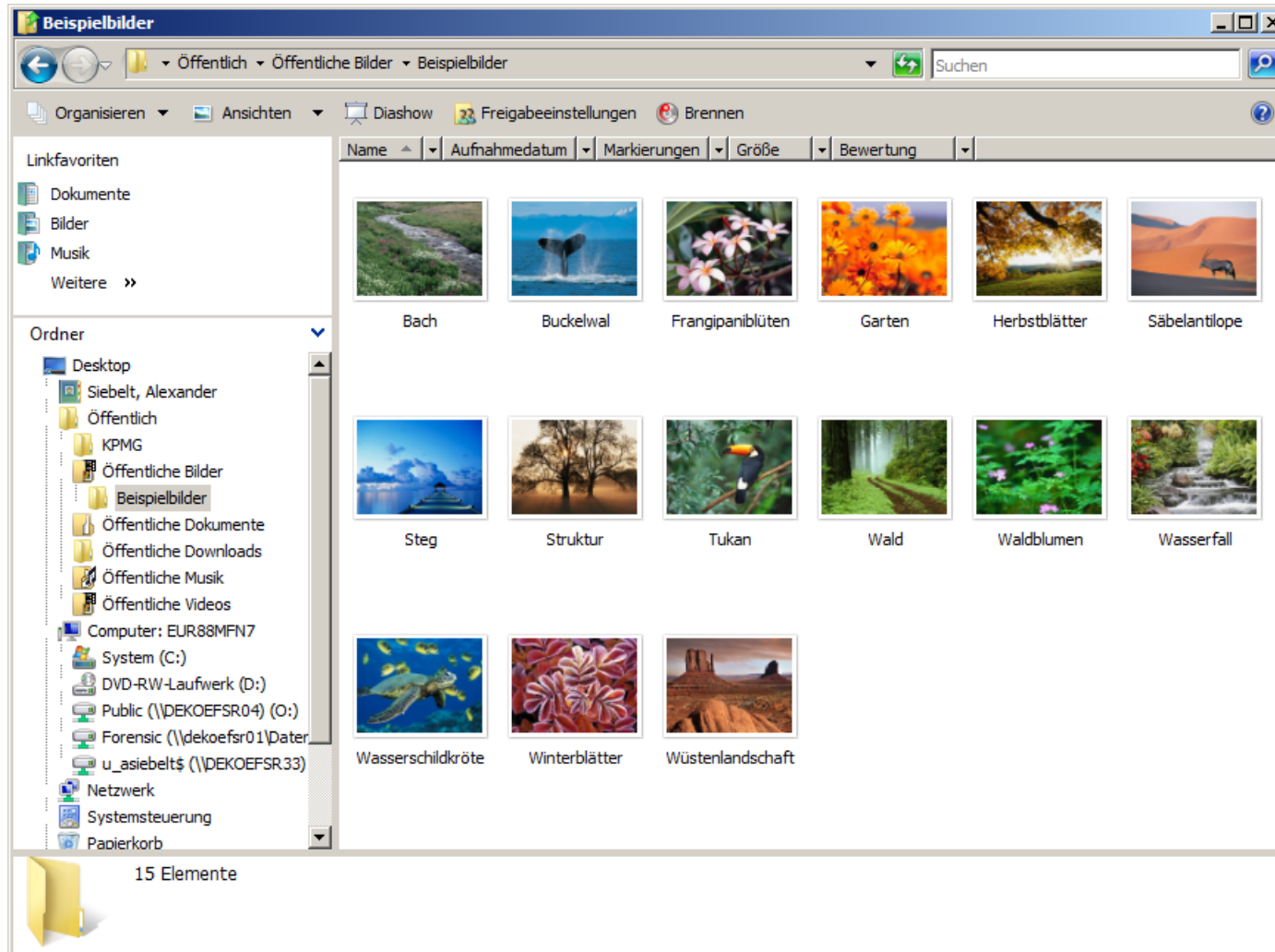
Für den normalen Benutzer ist der geänderte Zielordner nicht erkennbar – er muss jedoch bei der forensischen Analyse berücksichtigt werden!



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

Case Data

File Edit

Explorer (28)

- GameExplor
- History (11)
- Ringtones (0)
- Temporary I
- WER (4)
- Windows Mail
- Windows Media
- Windows Sideb
- Windows Virtua
- Temp (7)
- Temporary Internet
- VirtualStore (3)
- LocalLow (4)
- Roaming (74)
- Application Data (1)
- Beispiellos (6)
- Contacts (2)
- Cookies (1)
- Desktop (228)
- Documents (4)
- Downloads (1)
- Favorites (19)
- Links (4)
- Local Settings (1)
- Music (1)
- My Documents (1)
- NetHood (1)
- Pictures (1)
- PrintHood (1)
- Recent (1)
- Saved Games (1)

Drive C:

\Users\Eric Fraudster\AppData\Local\Microsoft\Windows\Explorer 15 min. ago 8 files, 0 dir.

Name	Type	Size	Created	Modified	Accessed	Attr.	1st sector	Comment
ExplorerStartupLog.etl	etl	32,0 KB	12.01.2011 15:30:00	12.01.2011 15:30:30	12.01.2011 15:30:00	AX	431592	
ExplorerStartupLog_RunOnce.etl	etl	16,0 KB	12.01.2011 15:30:02	12.01.2011 15:30:03	12.01.2011 15:30:02	AX	10744552	
thumbcache_1024.db	db	24 B	12.01.2011 15:30:25	12.01.2011 15:30:25	12.01.2011 15:30:25	AX	35236	
thumbcache_256.db (20)	db	1,0 MB	12.01.2011 15:30:25	12.01.2011 15:30:25	12.01.2011 15:30:25	AX (p...	1206120	
thumbcache_32.db	db	1,0 MB	12.01.2011 15:30:25	12.01.2011 15:30:25	12.01.2011 15:30:25	AX (p...	1189056	
thumbcache_96.db	db	1,0 MB	12.01.2011 15:30:25	12.01.2011 15:30:25	12.01.2011 15:30:25	AX (p...	1191104	
thumbcache_idx.db	db	6,3 KB	12.01.2011 15:30:25	20.01.2011 11:31:44	12.01.2011 15:30:25	AX	464616	
thumbcache_sr.db	db	24 B	12.01.2011 15:30:25	12.01.2011 15:30:25	12.01.2011 15:30:25	AX	35274	

Selected: 21 files (1,6 MB)

Volume	File	Preview	Details	Gallery	Calendar	Legend	Sync											
	Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
	00000000	43	4D	4D	4D	15	00	00	00	02	00	00	00	18	00	00	00	CMMM
	00000010	4E	4D	09	00	51	00	00	00	43	4D	4D	4D	80	00	00	00	NM Q CMMM
	00000020	E8	4E	B8	F9	51	BC	24	09	50	00	00	00	00	00	00	00	èN,ùQ%\$ P
	00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00000040	1D	FE	28	91	9F	41	8B	4D	3A	00	3A	00	7B	00	36	00	p('IAM: : { 6
	00000050	34	00	35	00	46	00	46	00	30	00	34	00	30	00	2D	00	4 5 F F 0 4 0 -
	00000060	35	00	30	00	38	00	31	00	2D	00	31	00	30	00	31	00	5 0 8 1 - 1 0 1
	00000070	42	00	2D	00	39	00	46	00	30	00	38	00	2D	00	30	00	B - 9 F 0 8 - 0
	00000080	30	00	41	00	41	00	30	00	30	00	32	00	46	00	39	00	0 A A 0 0 2 F 9
	00000090	35	00	34	00	45	00	7D	00	43	4D	4D	4D	80	00	00	00	5 4 E } CMMM
	000000A0	E8	4E	B8	F9	51	BC	24	09	50	00	00	00	00	00	00	00	èN,ùQ%\$ P
	000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	000000C0	1D	FE	28	91	9F	41	8B	4D	3A	00	3A	00	7B	00	36	00	p('IAM: : { 6
	000000D0	34	00	35	00	46	00	46	00	30	00	34	00	30	00	2D	00	4 5 F F 0 4 0 -
	000000E0	35	00	30	00	38	00	31	00	2D	00	31	00	30	00	31	00	5 0 8 1 - 1 0 1
	000000F0	42	00	2D	00	39	00	46	00	30	00	38	00	2D	00	30	00	B - 9 F 0 8 - 0

thumbcache_256.db
 \Users\Eric Fraudster\AppData

File size: 1,0 MB
 1.048.576 bytes
 W/o slack: 1.048.576 bytes
 Valid data length: 10.304 bytes

[Read-only mode]

Creation time: 12.01.2011 15:30:25

Data Interpreter

8 Bit (±): 67
 16 Bit (±): 19779
 32 Bit (±): 1296911683

Attributes: AX

Page 1 of 4096 Offset: 0 = 67 Block: n/a Size: n/a

Anzeigen der extrahierten Bilder aus einer Thumbcache-Datei

The screenshot displays the X-Ways Forensics interface. On the left, the 'Case Data' tree shows the file system structure, with 'AppData' > 'Local' > 'Microsoft' > 'Windows' > 'Explorer' > 'thumbcache_256.db' selected. The main pane shows a list of 99 files extracted from this cache. The file '1b46b1fc68ab15c1.jpg' is highlighted in blue. Below the list, a preview window shows the selected image file's metadata, including its path and size.

Name	Type	Path	Size	Deletion	Att
..					
139e34d1b951d2e7.png	png	\\Users\ftech\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	43,3 KB		
152d4192a2e618dc.png	png	\\Users\ftech\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	28,2 KB		
16fe3c26f4b9ce44.png	png	\\Users\ftech\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	32,2 KB		
17d0476866a1a887.png	png	\\Users\ftech\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	37,9 KB		
1b46b1fc68ab15c1.jpg	jpg	\\Users\ftech\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	15,2 KB		
1e4975c58395a82a.png	png	\\Users\ftech\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	30,9 KB		
25b806b39f5d4957.png	png	\\Users\ftech\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	37,9 KB		
25c6fab4ca355922.png	png	\\Users\ftech\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	32,2 KB		
27a1268085e6aa2a.png	png	\\Users\ftech\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	48,1 KB		
307181af0eb6c43f.png	png	\\Users\ftech\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	30,0 KB		
38e3506b4298708d.png	png	\\Users\ftech\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	31,1 KB		
3cc94ff4db7da184.jpg	jpg	\\Users\ftech\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	7,9 KB		
3f641bb7e155f547.png	png	\\Users\ftech\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	61,3 KB		



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

X-Ways Forensics - [Drive C:] 15.9 Beta 10

File Edit Search Position View Tools Specialist Options Window Help

Drive C: | and subdirectories | 3 hours ago | 140 files, 143.322 filtered out

Name	Typ	Size	Created	Modified	Accessed	Attr.	1st sector	Report ta	Comment	Metadata
NTOSBOOT-B00DFAAD.pf	pf	3,6 MB	05.11.2010 09:46:50	20.01.2011 10:31:27	05.11.2010 09:46:50	AX	1078805...			
SEARCHPROTOCOLHOST.EXE-AFAD3EF9.pf	pf	38,0 KB	05.11.2010 10:51:04	20.01.2011 13:59:42	05.11.2010 10:51:04	AX	6603528			
SEARCHFILTERHOST.EXE-AA7A1FDD.pf	pf	17,2 KB	05.11.2010 10:51:04	20.01.2011 13:59:42	05.11.2010 10:51:04	AX	8764184			
MSIEXEC.EXE-B5AFA339.pf	pf	52,3 KB	05.11.2010 10:51:30	20.01.2011 13:34:45	05.11.2010 10:51:30	AX	26336520			
CMD.EXE-89305D47.pf	pf	130 KB	05.11.2010 10:51:33	20.01.2011 13:33:11	05.11.2010 10:51:33	AX	26339808			
WMIPRVSE.EXE-43972D0F.pf	pf	23,9 KB	05.11.2010 10:51:33	20.01.2011 13:58:39	05.11.2010 10:51:33	AX	1587600			
WMIAPSRV.EXE-576286C3.pf	pf	22,2 KB	05.11.2010 10:52:34	20.01.2011 10:33:05	05.11.2010 10:52:34	AX	1110024			
WMIADAP.EXE-369DF1CD.pf	pf	16,8 KB	05.11.2010 10:53:32	20.01.2011 10:34:42	05.11.2010 10:53:32	AX	1613912			
TASKENG.EXE-5BAF290C.pf	pf	16,4 KB	05.11.2010 11:10:01	20.01.2011 13:45:15	05.11.2010 11:10:01	AX	10030088			
DLLHOST.EXE-71214090.pf	pf	16,4 KB	05.11.2010 16:02:59	20.01.2011 13:57:30	05.11.2010 16:02:59	AX	7562888			
SMSCLUI.EXE-345AB553.pf	pf	26,7 KB	05.11.2010 16:18:46	20.01.2011 13:43:29	05.11.2010 16:18:46	AX	1627784			
SESCLU.EXE-3C84D030.pf	pf	22,6 KB	05.11.2010 17:23:01	20.01.2011 13:58:14	05.11.2010 17:23:01	AX	1533184			
LUCALLBACKPROXY.EXE-9EFD4A00.pf	pf	410 KB	05.11.2010 18:32:27	20.01.2011 13:18:07	05.11.2010 18:32:27	AX	1639024			
LUALL.EXE-C73A48CA.pf	pf	46,8 KB	05.11.2010 18:32:31	20.01.2011 13:18:15	05.11.2010 18:32:31	AX	17626160			
DLLHOST.EXE-893DDF55.pf	pf	18,6 KB	05.11.2010 18:32:36	20.01.2011 13:57:53	05.11.2010 18:32:36	AX	21716328			
LOGONUI.EXE-1BEE4A84.pf	pf	40,5 KB	08.11.2010 08:04:06	20.01.2011 13:47:16	08.11.2010 08:04:06	AX	27971120			
SBCLIENHELPER.EXE-7256FB0C.pf	pf	20,0 KB	08.11.2010 08:07:16	20.01.2011 13:52:53	08.11.2010 08:07:16	AX	4635272			
MOBSYNC.EXE-D8BC6ED2.pf	pf	31,1 KB	08.11.2010 08:24:36	20.01.2011 13:58:38	08.11.2010 08:24:36	AX	21773288			
LUCOMSERVER_3_3.EXE-1441D197.pf	pf	50,9 KB	08.11.2010 09:03:26	20.01.2011 13:18:16	08.11.2010 09:03:26	AX	1662688			
CONSENT.EXE-65F6206D.pf	pf	91,3 KB	08.11.2010 09:27:03	20.01.2011 13:57:48	08.11.2010 09:27:03	AX	1841976			
IEXPLORE.EXE-1B894AFB.pf	pf	142 KB	08.11.2010 10:05:31	20.01.2011 13:56:59	08.11.2010 10:05:31	AX	8555120			
COH32.EXE-D1B20C81.pf	pf	204 KB	08.11.2010 10:40:00	20.01.2011 13:30:57	08.11.2010 10:40:00	AX	7572472			

Selected: 1 file (142 KB)

*** Prefetch ***

IEXPLORE.EXE-1B894AFB
Run Count: 235

Last Run: : 20.01.2011 14:28:00

```

000 32 200 \DEVICE\HARDDISK\VOLUME1\WINDOWS\SYSTEM32\NTDLL.DLL
073 35 200 \DEVICE\HARDDISK\VOLUME1\WINDOWS\SYSTEM32\KERNEL32.DLL
0C4 33 2 \DEVICE\HARDDISK\VOLUME1\WINDOWS\SYSTEM32\LOCALE.NLS
12C 35 200 \DEVICE\HARDDISK\VOLUME1\WINDOWS\SYSTEM32\ADVAPI32.DLL
16C 33 200 \DEVICE\HARDDISK\VOLUME1\WINDOWS\SYSTEM32\RPCRT4.DLL
1B9 44 200 \DEVICE\HARDDISK\VOLUME1\PROGRAM FILES\INTERNET EXPLORER\IEXPLORE.EXE
1CC 32 200 \DEVICE\HARDDISK\VOLUME1\WINDOWS\SYSTEM32\GDI32.DLL
1F3 33 200 \DEVICE\HARDDISK\VOLUME1\WINDOWS\SYSTEM32\USER32.DLL
    
```

\Drive C:\Windows\Fetch\IEXPLORE.EXE-1B894AFB.pf

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



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

X-Ways Forensics - [Drive C:] 15.9 Beta 10

File Edit Search Position View Tools Specialist Options Window Help

Case Data Drive C: Case Root

\Users\asiebelt\AppData\Roaming\Microsoft\Office\Recent 4 hours ago 73 files, 0 dir.

Name	Typ	Path	Size	Created	Modified	Accessed
screenshots.LNK	Ink	\Users\asiebelt\AppData\Roaming\Microsoft\Office\Recent	0,7 KB	21.01.2011 11:55:25	21.01.2011 14:55:39	21.01.2011
Sonderauswertungen.LNK	Ink	\Users\asiebelt\AppData\Roaming\Microsoft\Office\Recent	0,9 KB	05.01.2011 15:33:12	17.01.2011 15:02:57	17.01.2011
Staffing - Ohne Namen.xml.prv.xml.LNK	Ink	\Users\asiebelt\AppData\Roaming\Microsoft\Office\Recent	1,1 KB	23.11.2010 10:34:35	23.11.2010 10:34:35	23.11.2010
Stunden_GJ2010.xls.LNK	Ink	\Users\asiebelt\AppData\Roaming\Microsoft\Office\Recent	1,0 KB	21.01.2011 09:21:05	21.01.2011 09:21:05	21.01.2011
Stunden_GJ2011.xls.LNK	Ink	\Users\asiebelt\AppData\Roaming\Microsoft\Office\Recent	0,8 KB	07.12.2010 20:07:49	21.01.2011 13:35:46	21.01.2011
Stundeneübersicht.LNK	Ink	\Users\asiebelt\AppData\Roaming\Microsoft\Office\Recent	0,7 KB	09.11.2010 14:10:18	21.01.2011 13:35:46	21.01.2011
Stundeneübersichten.LNK	Ink	\Users\asiebelt\AppData\Roaming\Microsoft\Office\Recent	0,8 KB	21.01.2011 09:21:05	21.01.2011 09:21:05	21.01.2011
Support_Listen.LNK	Ink	\Users\asiebelt\AppData\Roaming\Microsoft\Office\Recent	0,7 KB	20.01.2011 09:21:19	20.01.2011 09:21:19	20.01.2011

Selected: 1 file (1,0 KB)

Target Filesize	1701376
Show Window	SW_NORMAL
Target Created	08.11.2010 10:39:03
Last Written	21.01.2011 09:21:05
Last Accessed	08.11.2010 10:39:03
Workplace	C:\
Volume Type	Fixed
Volume Serial	0x96EB77B2
Volume Name	System
Local Path	C:\Projekte\Stuff\Stundeneübersicht\Stundeneübersichten\Stunden_GJ2010.xls
Relative Path	..\..\..\..\..\Projekte\Stuff\Stundeneübersicht\Stundeneübersichten\Stunden_GJ2010.xls
Host Name	eur88mf7
Volume ID	{EB18D4C8-44DF-44FC-BF7F-7D3D20D55247}
Object ID	{03CB829C-F3AE-11DF-BBC9-F0DEF1130793}
MAC Address	F0 DE F1 13 07 93
Timestamp	19.11.2010 07:24:15, Seq: 15305

Drive C:\Users\asiebelt\AppData\Roaming\Microsoft\Office\Recent\Stunden_GJ2010.xls.LNK

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



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

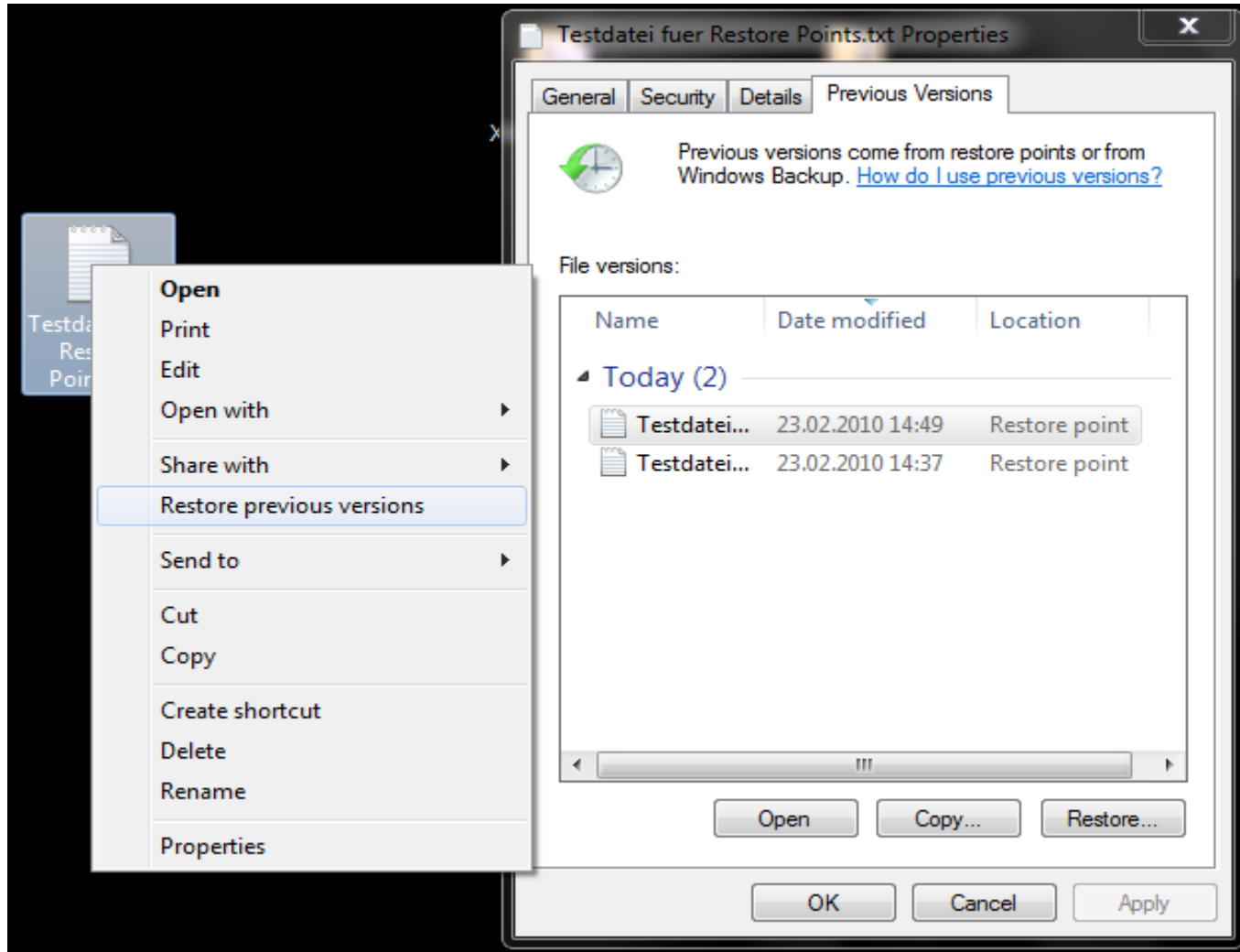
Die gesicherten Daten werden im Verzeichnis „System Volume Information“ abgelegt

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

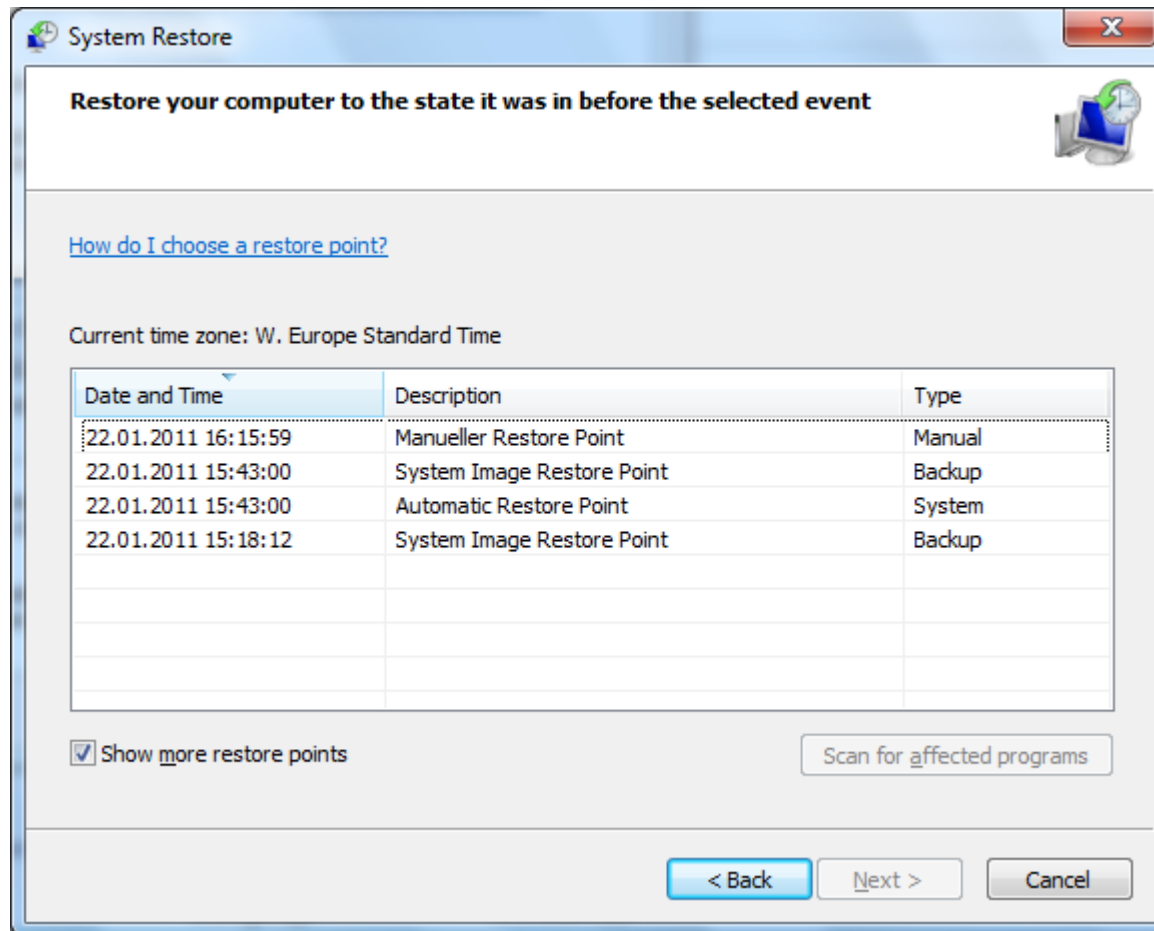


Gespeicherte vorherige Versionen von Dateien können:

- 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:

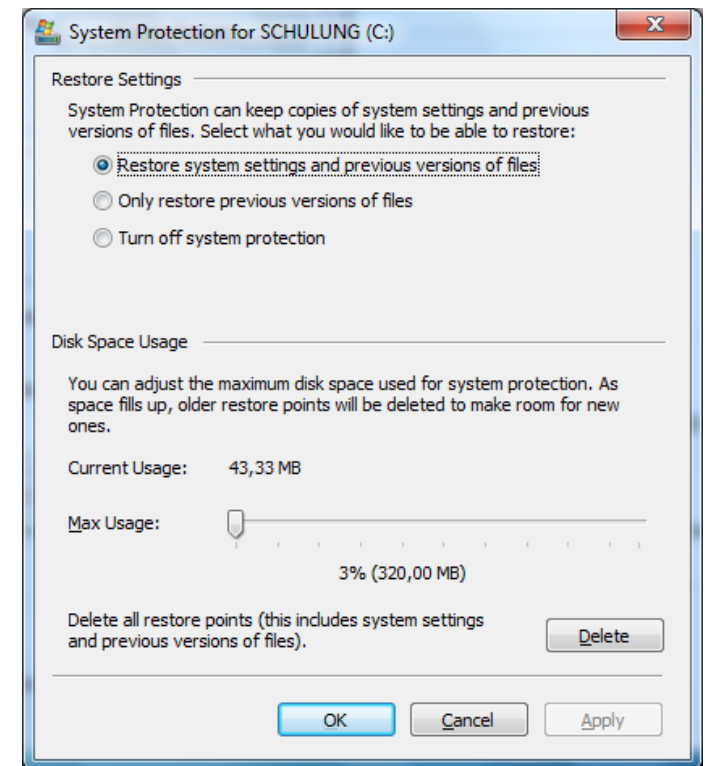
- Manuell erstellt
- Alle 7 Tage automatisch (Vista: alle 24 Stunden)
- Vor einem Windows-Update oder der Installation eines unsigned Treibers
- Anwendung, die eine Sicherung über die Windows-API anfordert

Daten aus Schattenkopien werden (standardmäßig) entfernt, wenn...

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

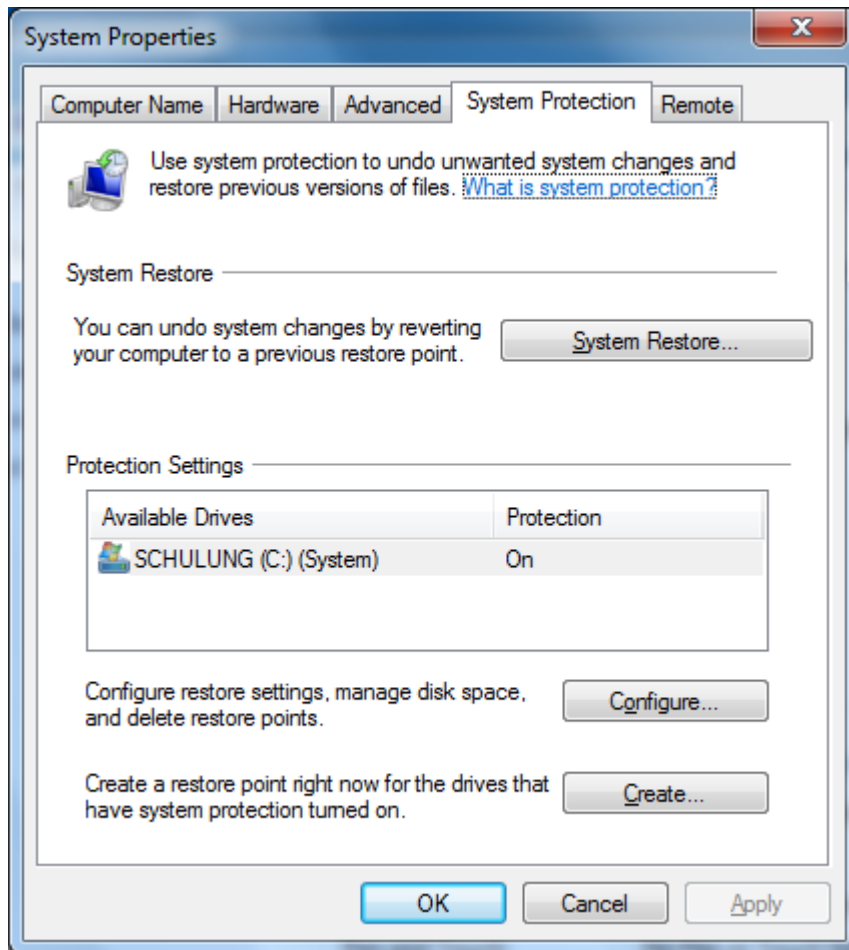
...mehr als 3% des Speichers bei einer Partition <64GB...

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

```
Administrator: Command Prompt
Contents of shadow copy set ID: {77c0a52a-598a-4016-827f-acb8d0430b22}
  Contained 1 shadow copies at creation time: 23.02.2010 14:38:13
    Shadow Copy ID: {735a81f3-a7d6-4b79-b27d-1156ac964987}
      Original Volume: (C:)\?\Volume{6879afe0-febe-11de-b61e-806e6f6e6963}\
      Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4
      Originating Machine: ftech-win7
      Service Machine: ftech-win7
      Provider: 'Microsoft Software Shadow Copy provider 1.0'
      Type: ClientAccessibleWriters
      Attributes: Persistent, Client-accessible, No auto release, Differential
1, Auto recovered

Contents of shadow copy set ID: {a82acad7-119a-47b4-bc01-d4a655f86fee}
  Contained 1 shadow copies at creation time: 23.02.2010 14:50:21
    Shadow Copy ID: {4240ee71-14c1-424e-94c1-9374fc235377}
      Original Volume: (C:)\?\Volume{6879afe0-febe-11de-b61e-806e6f6e6963}\
      Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy5
      Originating Machine: ftech-win7
      Service Machine: ftech-win7
      Provider: 'Microsoft Software Shadow Copy provider 1.0'
      Type: ClientAccessibleWriters
      Attributes: Persistent, Client-accessible, No auto release, Differential
1, Auto recovered

C:\>vssadmin list shadows /for=C:._
```


Volume Shadow Copies: Forensische Analyse

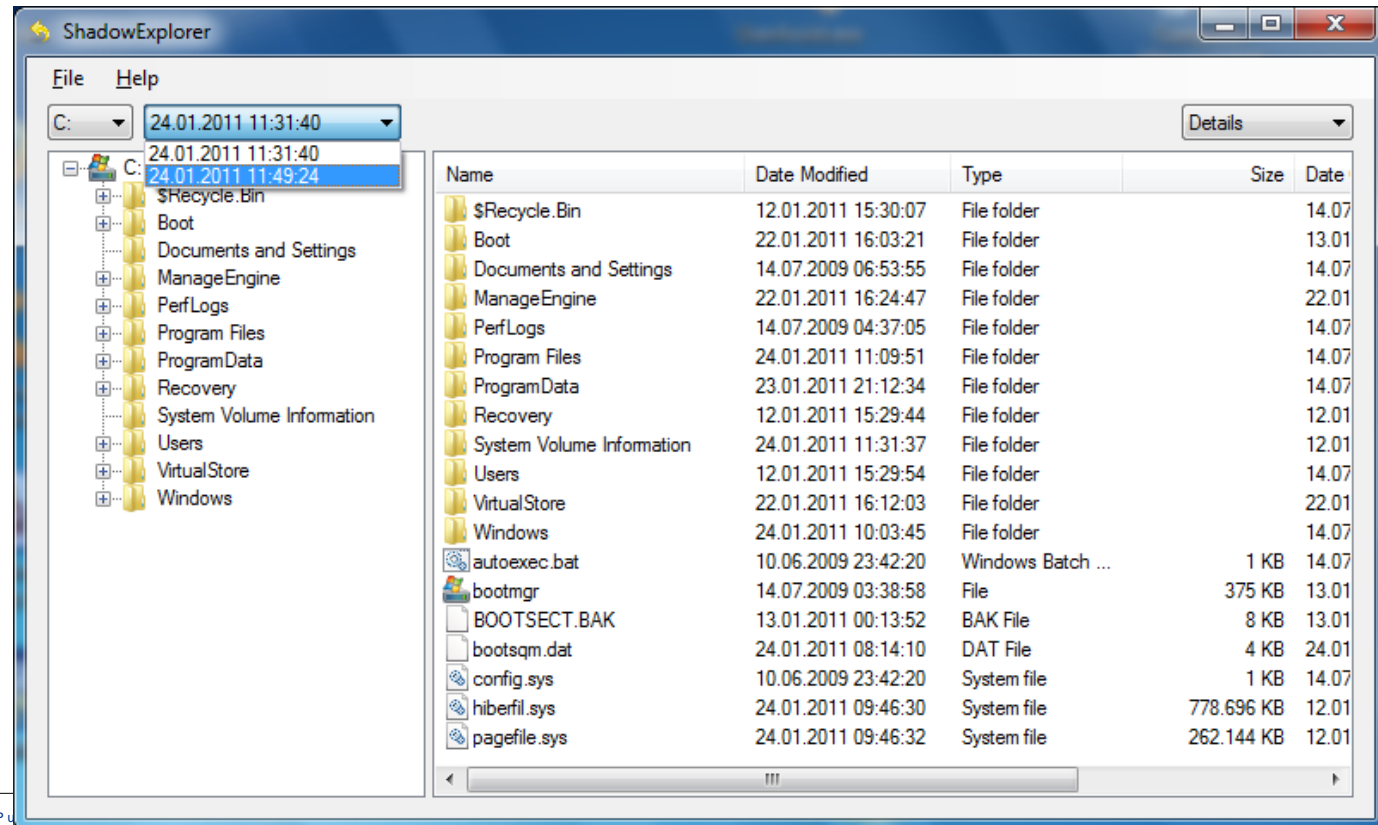
Anhand des Shadow Copy Volume Identifiers kann auf eine Schattenkopie live zugegriffen werden:

```
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



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

The screenshot shows a Windows Explorer window titled "\Windows\System32\winevt\Logs" with a timestamp of "65 min. ago" and "130 files, 0 dir.". The window displays a list of event log files in a table format. The table has columns for Name, Type, Path, Size, Deletion, Attr., and Metadata. All files are of type "evtx" and are located in the path "\Windows\System32\winevt\Logs". The files listed include Application.evtx (1.1 MB), HardwareEvents.evtx (68.0 KB), Internet Explorer.evtx (68.0 KB), Key Management Service.evtx (68.0 KB), Media Center.evtx (68.0 KB), and several Microsoft Windows Application Experience logs (68.0 KB each). The bottom of the window shows a taskbar with tabs for Partition, File, Preview, Details, Gallery, Calendar, Legend, and Sync, along with a status bar indicating "Selected: 130 files, 0 dir. (16.4 MB)".

Name	Type	Path	Size	Deletion	Attr.	Metadata
..						
Application.evtx	evtx	\Windows\System32\winevt\Logs	1,1 MB		A (par...	
HardwareEvents.evtx	evtx	\Windows\System32\winevt\Logs	68,0 KB		A	
Internet Explorer.evtx	evtx	\Windows\System32\winevt\Logs	68,0 KB		A	
Key Management Service.evtx	evtx	\Windows\System32\winevt\Logs	68,0 KB		A	
Media Center.evtx	evtx	\Windows\System32\winevt\Logs	68,0 KB		A	
Microsoft-Windows-API-Tracing%4Operational.evtx	evtx	\Windows\System32\winevt\Logs	68,0 KB		A	
Microsoft-Windows-AppID%4Operational.evtx	evtx	\Windows\System32\winevt\Logs	68,0 KB		A	
Microsoft-Windows-Application-Experience%4Problem-Steps-...	evtx	\Windows\System32\winevt\Logs	68,0 KB		A	
Microsoft-Windows-Application-Experience%4Program-Compat...	evtx	\Windows\System32\winevt\Logs	68,0 KB		A	
Microsoft-Windows-Application-Experience%4Program-Compat...	evtx	\Windows\System32\winevt\Logs	68,0 KB		A	
Microsoft-Windows-Application-Experience%4Program-Invento...	evtx	\Windows\System32\winevt\Logs	68,0 KB		A	
Microsoft-Windows-Application-Experience%4Program-Teleme...	evtx	\Windows\System32\winevt\Logs	68,0 KB		A	
Microsoft-Windows-AppLocker%4EXE and DLL.evtx	evtx	\Windows\System32\winevt\Logs	68,0 KB		A	

Windows Event Log: Einstellungen in der Registry

The screenshot shows the Windows Registry Editor window. The left pane displays a tree view of the registry, with the path `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\eventlog\Security` selected. The right pane shows a list of registry values for this path.

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayNameFile	REG_EXPAND_SZ	%SystemRoot%\system32\wevtapi.dll
DisplayNameID	REG_DWORD	0x00000101 (257)
File	REG_EXPAND_SZ	%SystemRoot%\System32\winevt\Log
Isolation	REG_DWORD	0x00000002 (2)
MaxSize	REG_DWORD	0x01400000 (20971520)
PrimaryModule	REG_SZ	Security
RestrictGuestAccess	REG_DWORD	0x00000001 (1)
Retention	REG_DWORD	0x00000000 (0)
Security	REG_BINARY	01 00 14 80 8c 00 00 00 98 00 00 00 14 00

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\eventlog\Security

Windows Event Viewer

The screenshot shows the Windows Event Viewer application. The left pane displays the tree view with 'Security' selected under 'Windows Logs'. The main pane shows a list of events with the following data:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	24.01.2011 15:15:26	Microsoft Windows sec...	4672	Special Logon
Audit Success	24.01.2011 15:15:26	Microsoft Windows sec...	4624	Logon
Audit Success	24.01.2011 15:15:26	Microsoft Windows sec...	4624	Logon
Audit Success	24.01.2011 15:15:26	Microsoft Windows sec...	4648	Logon
Audit Success	24.01.2011 15:15:16	Microsoft Windows sec...	4647	Logoff

The details pane for event 4672, 'Special privileges assigned to new logon', is open. It shows the following information:

Subject:
Security ID: StealMoney\Eric Fraudster
Account Name: Eric Fraudster
Account Domain: StealMoney
Logon ID: 0x3f23ca

Privileges:
SeSecurityPrivilege
SeTakeOwnershipPrivilege
SeLoadDriverPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeDebugPrivilege

Log Name: Security
Source: Microsoft Windows security
Event ID: 4672
Level: Information
User: N/A
Op Code: Info

Logged: 24.01.2011 15:15:26
Task Category: Special Logon
Keywords: Audit Success
Computer: StealMoney.DieFirma.local

More Information: [Event Log Online Help](#)

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

The screenshot shows a Windows desktop environment. In the foreground, there is a 'Log Parser' application window displaying a table of event log entries. Above it, a 'Command Prompt' window shows the execution of the LogParser.exe tool with various SQL-like queries to filter and analyze event logs.

Command Prompt Output:

```
C:\Program Files\Log Parser 2.2>LogParser.exe -i:EVT -o:DATAGRID "Select EventType, Count(*) FROM security WHERE EventType = 16 GROUP BY EventType"

Statistics:
-----
Elements processed: 1673
Elements output: 1
Execution time: 3.54 seconds

C:\Program Files\Log Parser 2.2>LogParser.exe -i:EVT -o:DATAGRID "Select EventType, Count(*) FROM security GROUP BY EventType"

Statistics:
-----
Elements processed: 1673
Elements output: 2
Execution time: 3.68 seconds

C:\Program Files\Log Parser 2.2>LogParser.exe -i:EVT -o:DATAGRID "Select TimeGenerated, EventID, EventType, EventTypeName, Message FROM security WHERE EventID = 4672"
```

Log Parser Table:

TimeGenerated	Event...	EventTy...	EventTypeName	Message
2011-01-12 15:15:07	4672	8	Success Audit ev...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY...
2011-01-12 15:15:08	4672	8	Success Audit ev...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT ...
2011-01-12 15:15:30	4672	8	Success Audit ev...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUT...
2011-01-12 15:15:30	4672	8	Success Audit ev...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY...
2011-01-12 15:15:30	4672	8	Success Audit ev...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY...
2011-01-12 15:15:31	4672	8	Success Audit ev...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY...
2011-01-12 15:15:35	4672	8	Success Audit ev...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY...
2011-01-12 15:17:40	4672	8	Success Audit ev...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY...
2011-01-12 15:17:43	4672	8	Success Audit ev...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY...
2011-01-12 15:18:32	4672	8	Success Audit ev...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY...

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

© 2011 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Konzerngesellschaft der KPMG Europe LLP und Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative ("KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten.

Der Name KPMG, das Logo und "cutting through complexity" sind eingetragene Markenzeichen von KPMG International.