



FORENSIC

Windows 7 Forensik

Alexander Geschonneck
Partner Forensic Technology
CEBIT 2010, 5. März 2010

ADVISORY

AUDIT • TAX • ADVISORY

Windows 7 Forensik: Themenüberblick

- Übersicht Microsoft Windows 7 Editionen
- Neues Partitionsschema
- Neuerungen bei BitLocker
- Neues bei Dateisystemen
- Änderungen in der Registry
- Betriebssystem-Artefakte
- RAM-Analyse unter Windows 7

KPMG Forensic: Unsere Dienstleistungen

Fraud Risk Management

Konzeptionierung, Implementierung, Optimierung von ganzheitlichen Fraud Risk Management-Systemen und Systemelementen/Maßnahmen

Intellectual Property & Contract Governance

IP-Management inkl. Überprüfung der Einhaltung von Lizenzverträgen und Implementierung von IP-Sicherheitskonzepten

Corporate Intelligence

Fachspezifische Recherche und Analyse sowie zielgerichtete Aufbereitung von Hintergrundinformationen zu Unternehmen, Geschäftspersonen und Vermögenswerten

Forensic unterstützt Sie bei ...

Sachverhaltsaufklärung
Präventionsfragen und -konzepten
Sicherstellung von Vermögenswerten



Investigations

Aufdeckung und Untersuchung von wirtschaftskriminellen Straftaten und Handlungen in und gegen Institutionen unserer Mandanten

Forensic Technology

Sicherung und Wiederherstellung digitaler Beweismittel sowie systematische Analyse/Auswertung von (un)strukturierten Datenbeständen

Dispute Advisory Services

Untersuchung von Vertragsverletzungen, gerichtsverwertbare Schadens- und Wertermittlung, Schlichterfunktion

Übersicht Microsoft Windows 7 Editionen

Überblick Windows 7 und Vista Editionen

	Windows 7					Windows Vista				
	Starter	Home Basic	Premium	Professional	Ultimate&Enterprise	Starter	Home Basic	Home Premium	Business	Ultimate&Enterprise
max. CPU-Chips	1	1	1	2	2	1	1	1	2	2
max. GB RAM 32 / 64bit	4 ¹ / -	4 ¹ / 8	4 ¹ / 16	4 ¹ / 192	4 ¹ / 192	4 ¹ / -	4 ¹ / 8	4 ¹ / 16	4 ¹ / 128	4 ¹ / 128
32-bit Version	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
64-bit Version	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓
EFS	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓
Bitlocker	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓ ²
Bitlocker To Go	RO	RO	RO	RO	✓	RO	RO	RO	RO	RO

¹ = max. 3 GB (→ 32-Bit!), Rest ggf. über RAM-Disk nutzbar

² = nur ab Vista ≥ SP1

✓ / ✗ = funktioniert oder existent / funktioniert nicht oder nicht existent

Überblick Windows 7 und Vista Editionen

	Windows 7					Windows Vista				
	Starter	Home Basic	Premium	Professional	Ultimate&Enterprise	Starter	Home Basic	Home Premium	Business	Ultimate&Enterprise
VSS	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓
VSS Prev. Vers	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓
Windows Virtual PC	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗
XP-Mode	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
VHD Support	✗	✓	✓	✓	✓	✗	✗ ³	✗ ³	✗ ³	✗ ³
VHD-Mount/Boot	✗/✗	✓/✗	✓/✗	✓/✓	✓/✓	✗/✗	✓ ³ /✗	✓ ³ /✗	✓ ³ /✗	✓ ³ /✗

³ = nur ab/ mit Virtual PC 2007 SP 1 nutzbar

✓/ ✗ = funktioniert oder existent / funktioniert nicht oder nicht existent

Neues Partitionsschema

Neues Partitionsschema bei der Installation von Windows 7 (1/2)

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

Neues Partitionsschema bei der Installation von Windows 7 (2/2)

X-Ways Forensics - [Partition 1]

File Edit Search Position View Tools Specialist Options Window Help

Case Data

Hommingberger

- Drive C:
- Drive D:
- Hard disk 0
 - Partition 1
 - \$Extend
 - \$RECYCLE.BIN
 - Boot
 - System Volume Information
 - Partition 2
 - Partition 3

Drive C: Drive D: Hard disk 0 Hard disk 0, P1 \$Bitmap

\Boot 11 min. ago 6+1=7 files, 24 dir.

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

memtest.exe
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

Änderungen bei BitLocker

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
- **Seit Vista SP1 können auch andere Partitionen als die Systempartition verschlüsselt werden**
- **Neuer Dateiname für Recovery Key Files**
- **BitLocker To Go für mobile Geräte**
- **Überarbeitetes Tool zur BitLocker-Verwaltung**

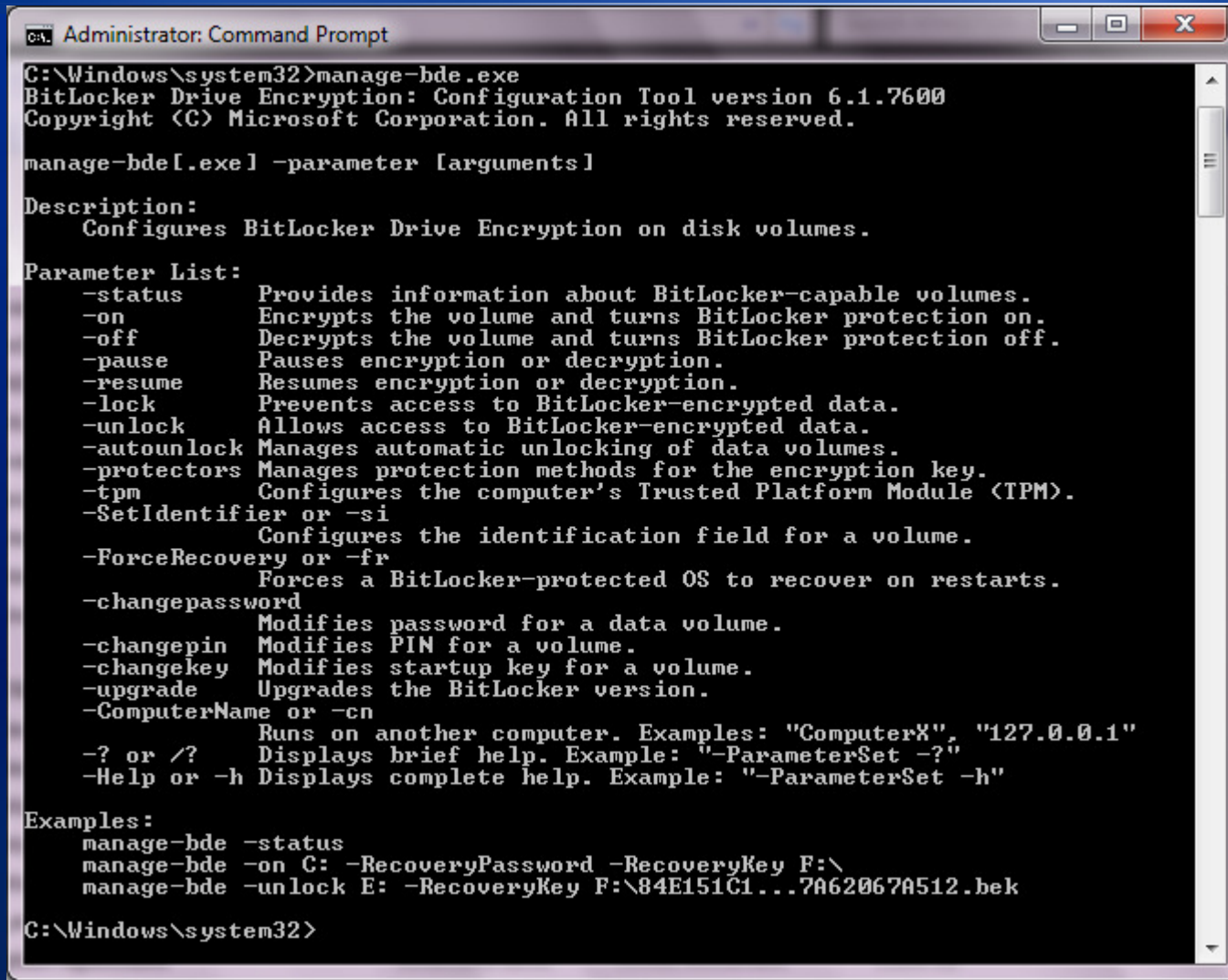
Änderungen bei BitLocker: Neue Signatur in Windows 7

The screenshot shows a Windows Explorer window for 'Hard disk 0, P2' (Hard disk 0). The file list shows two files: 'BitLocker' (39,0 GB) and '\$Boot' (8,0 KB). Below the file list, a hex editor view is displayed, showing the partition's header. The hex data starts with 'EB 58 90 2D 46 56 45 2D 46 53 2D 00 02 08 00 00', which corresponds to the ASCII string '-FVE-FS-'. The right pane shows 'Hard disk 0, Partition 2' with '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	00	F8	00	00	3F	00	FF	00	00	28	03
000000000032	00	00	00	00	00	00	1F	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.

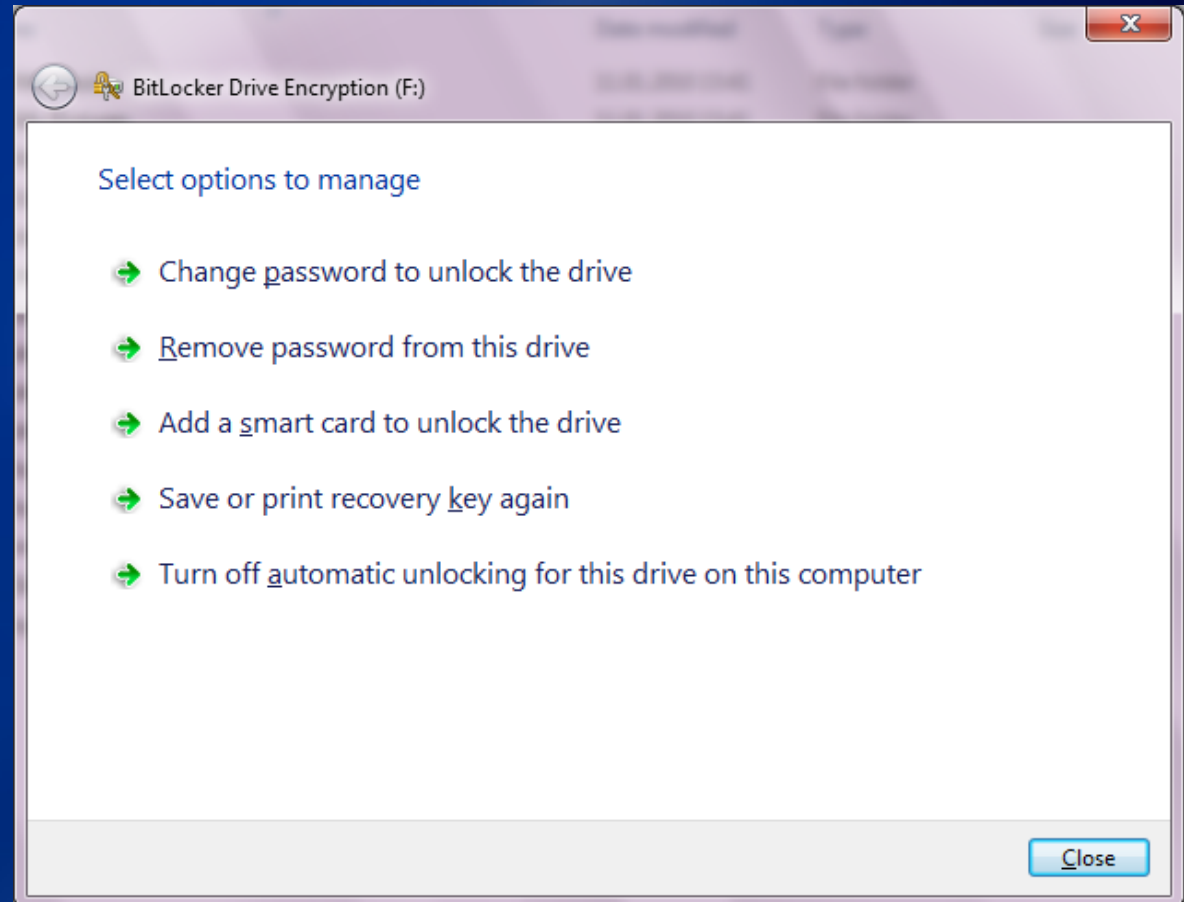
Parameter List:
  -status          Provides information about BitLocker-capable volumes.
  -on              Encrypts the volume and turns BitLocker protection on.
  -off             Decrypts the volume and turns BitLocker protection off.
  -pause          Pauses encryption or decryption.
  -resume          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

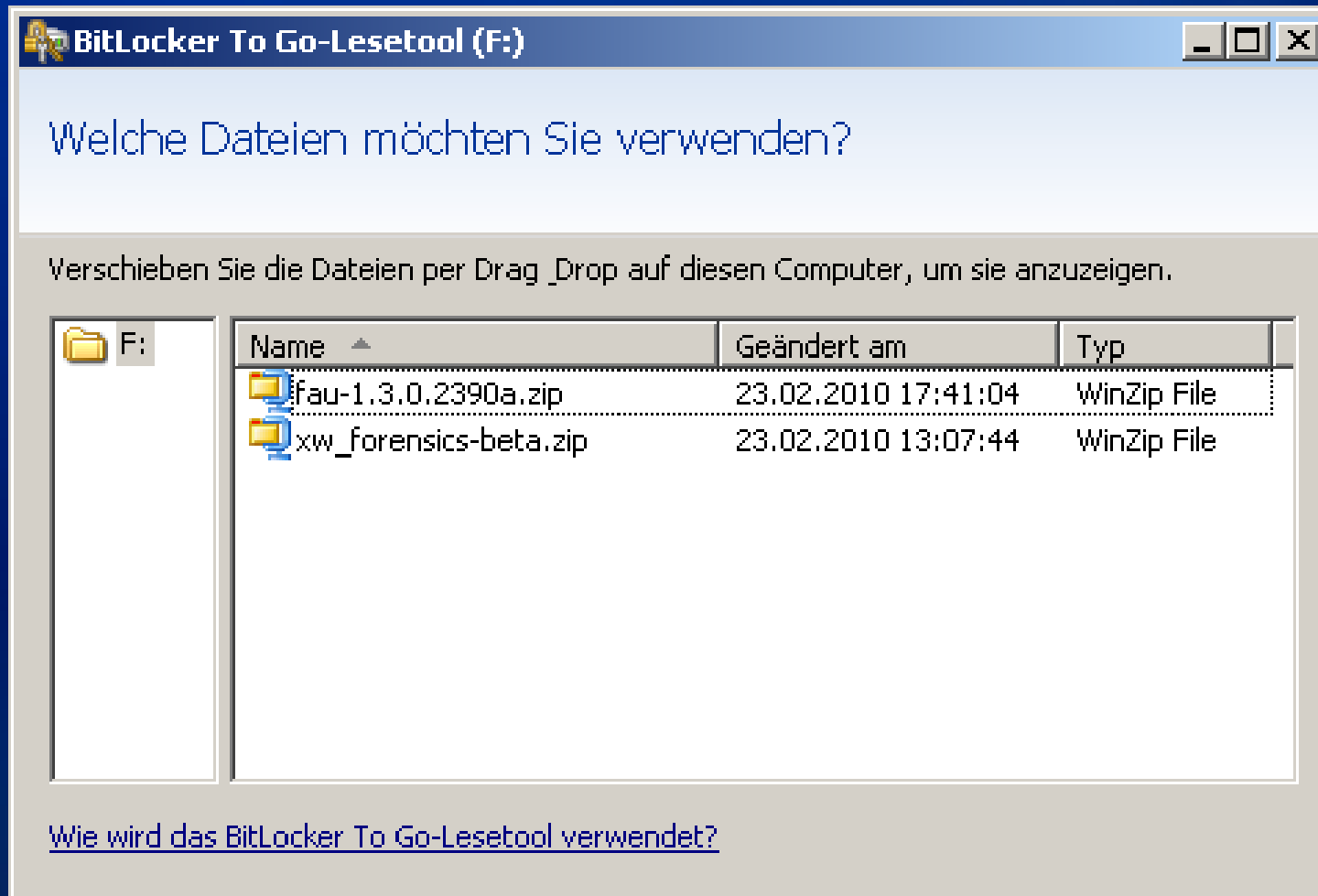
- BitLocker für mobile Datenträger
- Verschlüsselungsoptionen „To Go“:
 - Passwort,
 - Smart Card und
 - Automatic Unlocking
 - Kombinationen davon sind möglich



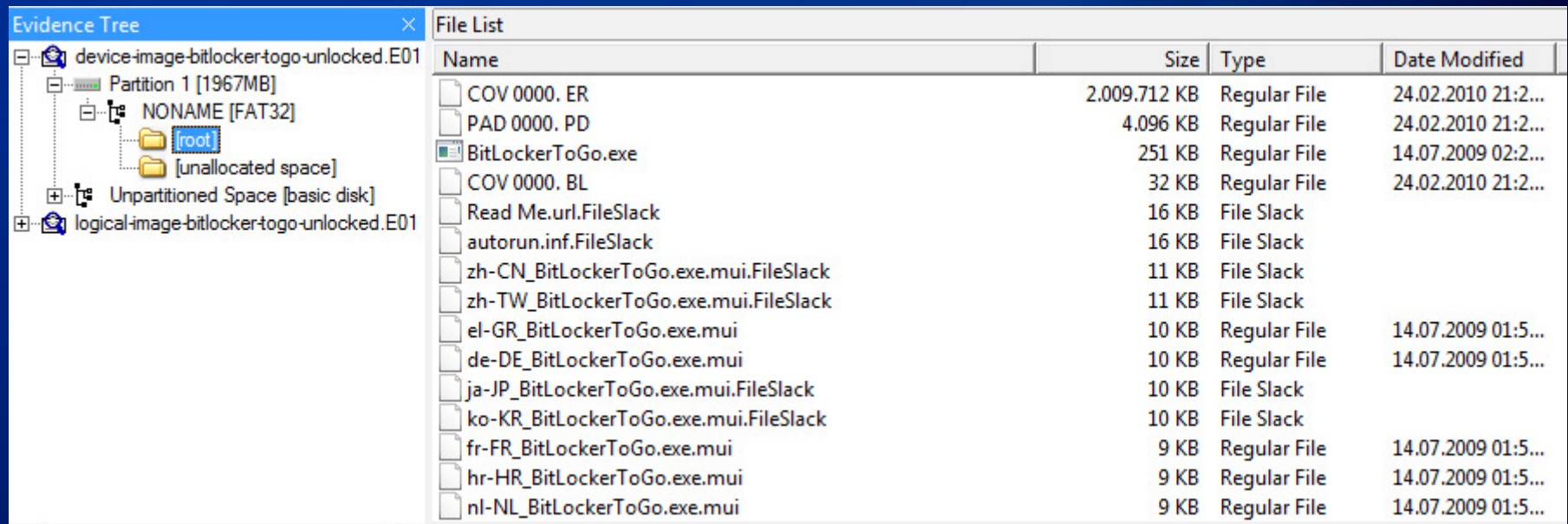
Änderungen bei BitLocker: BitLocker To Go

- **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“

Änderungen bei BitLocker: BitLocker To Go - Lesetool



Änderungen bei BitLocker: BitLocker To Go – Verschlüsselte Ansicht



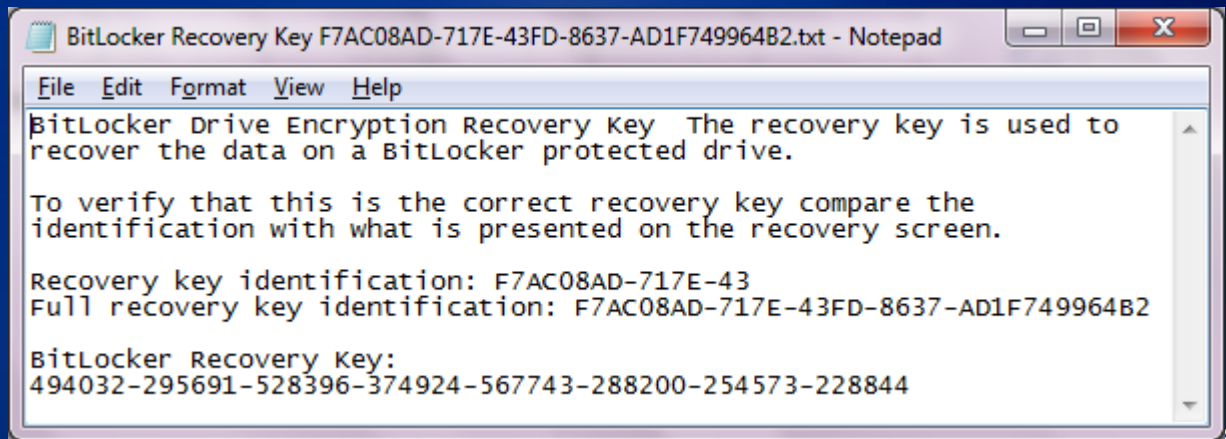
The screenshot displays a forensic analysis interface. On the left, the 'Evidence Tree' shows a hierarchy: 'device-image-bitlocker-togo-unlocked.E01' contains 'Partition 1 [1967MB]', which contains 'NONAME [FAT32]', which contains 'root' and '[unallocated space]'. Below this is 'Unpartitioned Space [basic disk]' and 'logical-image-bitlocker-togo-unlocked.E01'. On the right, the 'File List' table shows the contents of the 'root' directory.

Name	Size	Type	Date Modified
COV 0000. ER	2.009.712 KB	Regular File	24.02.2010 21:2...
PAD 0000. PD	4.096 KB	Regular File	24.02.2010 21:2...
BitLockerToGo.exe	251 KB	Regular File	14.07.2009 02:2...
COV 0000. BL	32 KB	Regular File	24.02.2010 21:2...
Read Me.url.FileSlack	16 KB	File Slack	
autorun.inf.FileSlack	16 KB	File Slack	
zh-CN_BitLockerToGo.exe.mui.FileSlack	11 KB	File Slack	
zh-TW_BitLockerToGo.exe.mui.FileSlack	11 KB	File Slack	
el-GR_BitLockerToGo.exe.mui	10 KB	Regular File	14.07.2009 01:5...
de-DE_BitLockerToGo.exe.mui	10 KB	Regular File	14.07.2009 01:5...
ja-JP_BitLockerToGo.exe.mui.FileSlack	10 KB	File Slack	
ko-KR_BitLockerToGo.exe.mui.FileSlack	10 KB	File Slack	
fr-FR_BitLockerToGo.exe.mui	9 KB	Regular File	14.07.2009 01:5...
hr-HR_BitLockerToGo.exe.mui	9 KB	Regular File	14.07.2009 01:5...
nl-NL_BitLockerToGo.exe.mui	9 KB	Regular File	14.07.2009 01:5...

- Typische Dateien bei verschlüsselter Ansicht
- Bei Betrachtung im HexEditor finden sich zusätzlich die typischen BitLocker-Signaturen im Datenträger (2D 46 56 45 2D 46 53 2D – „-FVE-FS-“)

Änderungen bei BitLocker: Forensische Analyse

- **Nutzung von Recovery Keys zum Entschlüsseln**
 - Können genutzt werden, um BitLocker- und BitLocker To Go-Volumes zu öffnen
 - Der ausführliche Text in der Datei kann für die Signatursuche in Forensik Tools genutzt werden
 - Bei Live-Analyse von gemounteten BitLocker-Volumes kann der Recovery Key extrahiert werden
 - Neuer Dateiname der Recovery Files



The screenshot shows a Notepad window titled "BitLocker Recovery Key F7AC08AD-717E-43FD-8637-AD1F749964B2.txt - Notepad". The text inside the window is as follows:

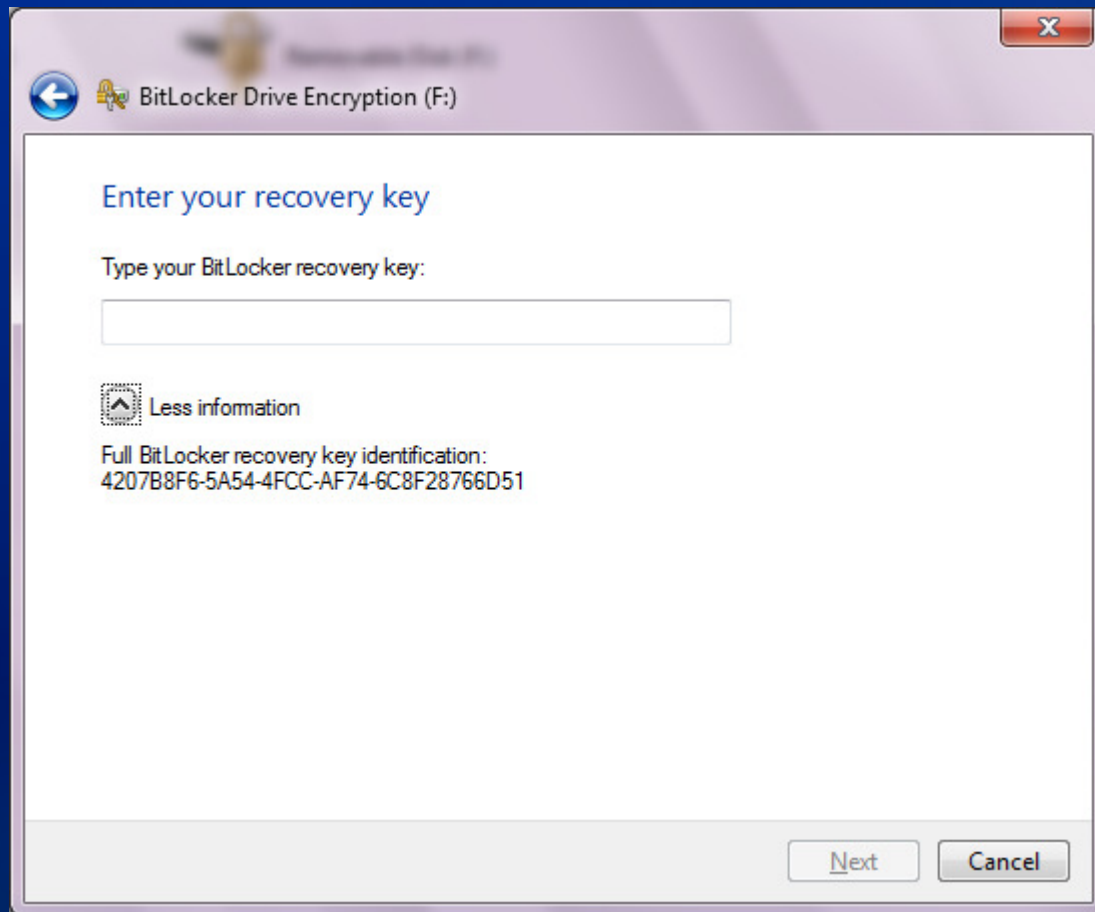
```
File Edit Format View Help
BitLocker Drive Encryption Recovery Key The recovery key is used to
recover the data on a BitLocker protected drive.

To verify that this is the correct recovery key compare the
identification with what is presented on the recovery screen.

Recovery key identification: F7AC08AD-717E-43
Full recovery key identification: F7AC08AD-717E-43FD-8637-AD1F749964B2

BitLocker Recovery Key:
494032-295691-528396-374924-567743-288200-254573-228844
```

Änderungen bei BitLocker: Forensische Analyse



Änderungen bei BitLocker: Forensische Analyse

- **Unverschlüsseltes Imaging nur möglich, wenn eine einzelne Partition eingebunden und anschließend kopiert wird – das ganze Laufwerk kann so nicht kopiert werden**
 - Der BitLocker Treiber hängt sich zwischen Dateisystem und Volume Manager ein
 - Direkter Zugriff auf den Volume Manager liefert stets verschlüsselte Inhalte, auch wenn ein Zugriff auf die Partition bereits freigeschaltet ist

Änderungen bei BitLocker: Zugriff auf verschlüsselte Partitionen

- **Es gibt unterschiedliche Methoden, um im Rahmen einer forensischen Analyse auf eine BitLocker-Partition zuzugreifen**
- **Live Analyse**
 - Ausgabe des Recovery-Keys mit Hilfe des manage-bde Tools, wenn Partition freigeschaltet
 - Entschlüsseln der Partition mit Hilfe des manage-bde Tools, wenn Partition freigeschaltet
 - Direkte Sicherung der freigeschalteten BitLocker-Partition
 - USB-Stick zum Freischalten der BitLocker-Partition liegt vor (bei verschlüsselter Systempartition)

Änderungen bei BitLocker: Zugriff auf verschlüsselte Partitionen

- **Post-mortem:**

- Nutzung vorhandener BitLocker Recovery Keys
- Nutzung bekannter Passwörter (BitLocker To Go)
- Data Recovery Agent ist für BitLocker konfiguriert
 - Zusätzliches Schlüsselpaar, das per Group-Policy verteilt wird und ein Entschlüsseln erlaubt
 - Nutzung i.d.R. bei Unternehmenskunden
- Recovery-Daten sind in Active Directory hinterlegt
 - Group Policy hierfür muss aktiviert sein

Neues bei Dateisystemen

Neues bei Dateisystemen (1/6): NTFS-Features

- **Windows 7 nutzt weiterhin die NTFS-Version 3.1**
- **Es werden weiterhin die transaktions-basierten NTFS-Ergänzungen genutzt**
 - Abgelegt im Ordner `\$Extend\$RmMetadata` und dessen Unterordnern
 - Mehrere Dateioperationen können zu einer Transaktion zusammengefasst werden
 - Anschließend kann die Transaktion als Ganzes wie bei einer Datenbank committed (also geschrieben) oder zurückgerollt werden

Neues bei Dateisystemen (2/6): NTFS-Features

- **Transaktions-basierte NTFS-Ergänzungen (ctd.)**
 - Anwendungen müssen angepasst werden, um dieses Feature nutzen zu können
 - Wird vom Windows-Betriebssystem selbst nicht für alle Dateien genutzt
 - Wenige Anwendungen nutzen das Feature nach unseren Recherchen bislang – selbst die meisten Microsoft-Applikationen nicht

Neues bei Dateisystemen (3/6): Formatieren von Partitionen / ADS

- **Formatieren einer Partition ohne QuickFormat überschreibt vorher vorhandene Inhalte komplett**
 - Vor Windows Vista waren alte Inhalte rekonstruierbar
 - Gilt für NTFS, FAT und exFAT
 - format.exe: Neuer Parameter „/P:<n>“ – definiert die Anzahl der Nullfill-Läufe
- **Alternate Data Streams**
 - Lassen sich mit Hilfe des dir-Befehls anzeigen
 - Option „/r“

Neues bei Dateisystemen (4/6): exFAT

- **Nachfolger für FAT-Dateisysteme bei mobilen Devices**
- **Auch verfügbar für Windows Vista ab SP1 und andere MS-Betriebssysteme via Updates**
- **Ursprünglich eingeführt für Windows CE 6.0 in 2006**
- **Wird ohne Update bspw. nicht von Windows XP als gültiges Laufwerk erkannt**
- **Features:**
 - Maximale Dateigröße jetzt 2^{64} Bytes
 - Unterstützt Laufwerke >32 GB
 - Keine Journal-Funktionen, weniger Overhead
 - Bis zu 32MB Cluster-Größe

Neues bei Dateisystemen (5/6): Forensische Analyse exFAT

- Unterstützung für exFAT in EnCase 6.15 vorhanden
- X-Ways Forensics unterstützt die Analyse von exFAT in Version 15.6 noch nicht
 - Filecarving funktioniert natürlich dennoch

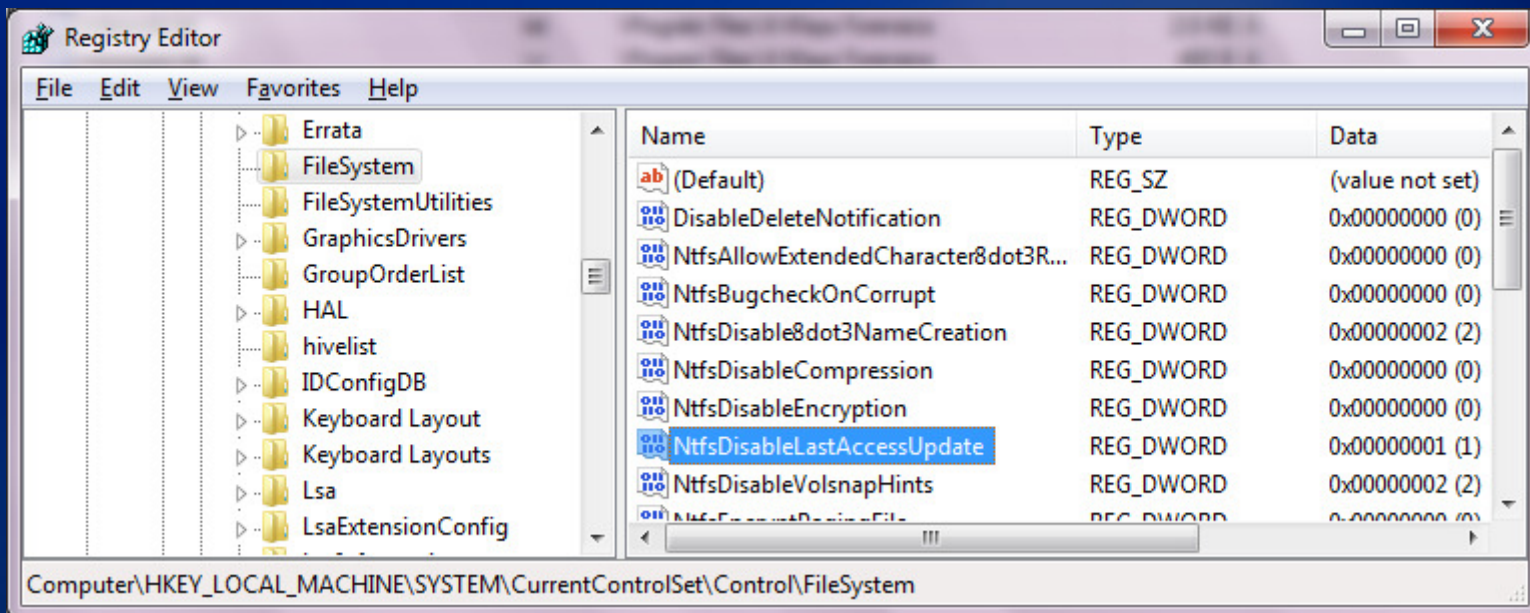
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
000000000	EB	76	90	45	58	46	41	54	20	20	20	00	00	00	00	00
000000016	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000064	3F	00	00	00	00	00	00	00	C1	AF	07	00	00	00	00	00
000000080	80	00	00	00	F0	01	00	00	80	02	00	00	A8	F5	00	00
000000096	06	00	00	00	CB	BD	6B	56	00	01	00	00	09	03	01	80
000000112	03	00	00	00	00	00	00	00	33	C9	8E	D1	BC	F0	7B	8E
000000128	D9	A0	FB	7D	B4	7D	8B	F0	AC	98	40	74	0C	48	74	0E
000000144	B4	0E	BB	07	00	CD	10	EB	EF	A0	FD	7D	EB	E6	CD	16
000000160	CD	19	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Removable medium ...
File system: exFAT
[Read-only mode]
Physical sector No.: 63
Logical sector No.: 0
Total capacity: 246 MB
257.917.440 bytes
Bytes per sector: 512
Sector count: 503.745
Physical disk: 1
Display time zone: UTC +01:00
Mode: hexadecimal
Character set: ANSI ASCII
Offsets: decimal
Bytes per page: 17x16=272

Sector 0 of 503745
Offset: 8
= 32
Block: 0 - 7
Size: 8

Neues bei Dateisystemen (6/6): MAC-Zeitstempel

- Standardmäßig wird bei NTFS-Dateisystemen weiterhin der Access-Zeitstempel bei einem Lesezugriff nicht aktualisiert
- Dies erschwert die Analyse von Zeitreihen



Neues in der Registry

Änderungen in der Registry: Überblick

- **Folgende ausgewählte inhaltliche Änderungen sollen näher analysiert werden:**
 - UserAssist Keys
 - Verbundene Netzwerke

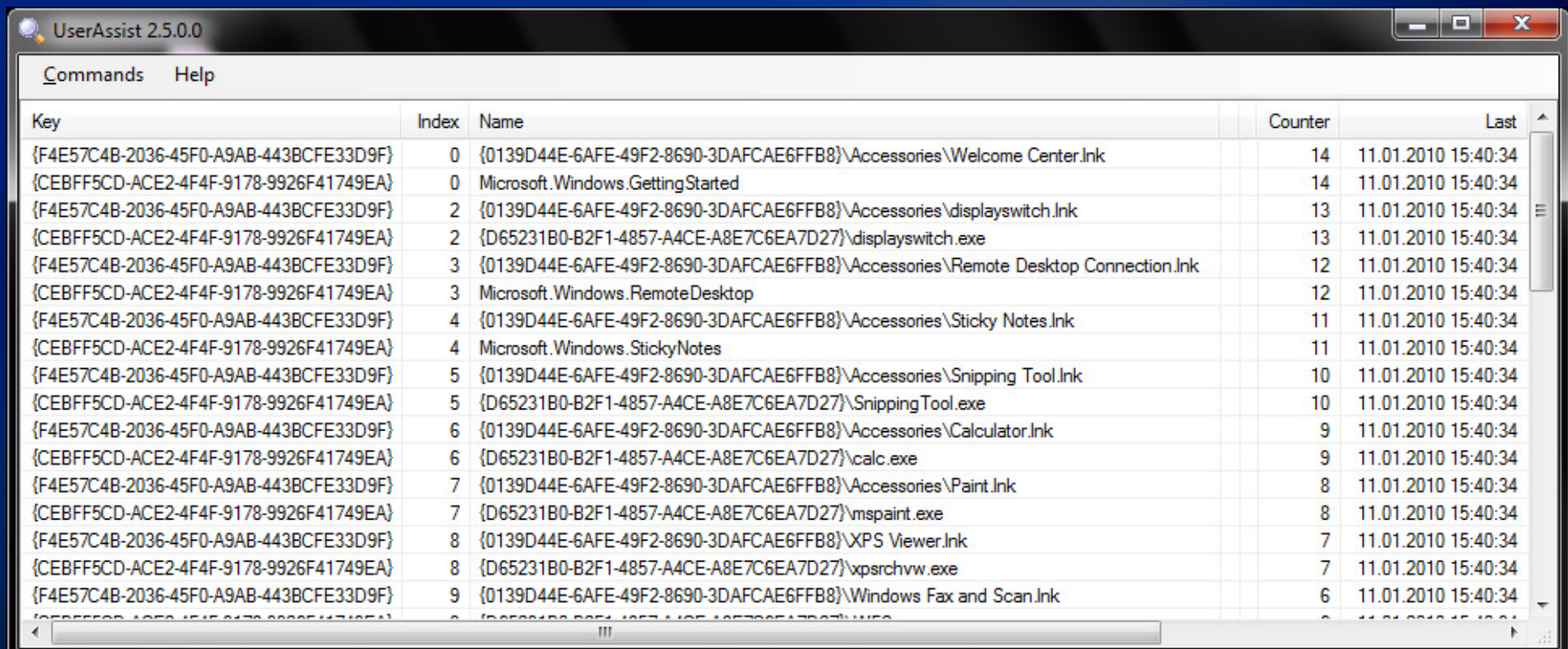
Registry Änderungen:

UserAssist Registry Keys (1/3)

- **Geändertes Format für die UserAssist Registry Keys mit Windows 7**
- **UserAssist Keys enthalten Nutzungsstatistiken zu den gestarteten Programmen**
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\ [...]\Count`
- **Die dort enthaltenen Keys enthalten im Wesentlichen die ROT13-verschleierte Programmnamen**
- **Zum Teil sind die Pfade durch GUIDs ersetzt**
- **Die Values zu den Keys enthalten die weiteren Nutzdaten**

Registry Änderungen: UserAssist Registry Keys (3/3)

- UserAssist Tool + Recherche von Didier Stevens
- <http://blog.didierstevens.com>
- Work in Progress – Bedeutung einiger Keys sind noch nicht bekannt



The screenshot shows the UserAssist 2.5.0.0 application window. It has a menu bar with 'Commands' and 'Help'. Below the menu bar is a table with the following columns: 'Key', 'Index', 'Name', 'Counter', and 'Last'. The table lists various registry keys and their corresponding names, counters, and last modification dates. The keys are listed in descending order of counter value.

Key	Index	Name	Counter	Last
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	0	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Welcome Center.lnk	14	11.01.2010 15:40:34
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	0	Microsoft.Windows.GettingStarted	14	11.01.2010 15:40:34
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	2	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\displayswitch.lnk	13	11.01.2010 15:40:34
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	2	{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\displayswitch.exe	13	11.01.2010 15:40:34
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	3	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Remote Desktop Connection.lnk	12	11.01.2010 15:40:34
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	3	Microsoft.Windows.RemoteDesktop	12	11.01.2010 15:40:34
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	4	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Sticky Notes.lnk	11	11.01.2010 15:40:34
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	4	Microsoft.Windows.StickyNotes	11	11.01.2010 15:40:34
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	5	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk	10	11.01.2010 15:40:34
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	5	{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\SnippingTool.exe	10	11.01.2010 15:40:34
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	6	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Calculator.lnk	9	11.01.2010 15:40:34
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	6	{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\calc.exe	9	11.01.2010 15:40:34
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	7	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk	8	11.01.2010 15:40:34
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	7	{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\mspaint.exe	8	11.01.2010 15:40:34
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	8	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\XPS Viewer.lnk	7	11.01.2010 15:40:34
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	8	{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\xpsrchvw.exe	7	11.01.2010 15:40:34
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	9	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Windows Fax and Scan.lnk	6	11.01.2010 15:40:34

Registry Änderungen: Registry Keys zu verbundenen Netzwerken

- **Seit Windows Vista werden in der Registry Informationen zu den Netzwerken abgelegt, mit denen ein Rechner verbunden war**
- `HKLM\Software\Microsoft\Windows NT\Current Version\NetworkList\Profiles\[GUID]`
- **Für jedes Netzwerkprofil wird ein separater Unterordner mit einer GUID angelegt**
- **Dort finden sich u.a. Informationen zum Zeitpunkt der ersten und letzten Verbindung zu diesem Netzwerk**

Registry Änderungen: Registry Keys zu verbundenen Netzwerken

The screenshot shows the Windows Registry Editor with the following structure:

- NetworkList
 - NewNetworks
 - Nla
 - Permissions
 - Profiles
 - {CB4B3179-583A-4040-B94E-2B5C15E4BC84}
 - Signatures
 - Managed
 - Unmanaged
 - 010103000F0000F0080000000F0000F0594E
 - NvCache
 - OpenGLDrivers
 - PeerDist
 - PeerNet
 - Perflib
 - PerHwIdStorage
 - Ports
 - Prefetcher

The right pane shows the values for the selected key:

Name	Type	Value
(Default)	REG_SZ	(value not set)
ProfileName	REG_SZ	Network
Description	REG_SZ	Network
Managed	REG_DWORD	0x00000000 (0)
Category	REG_DWORD	0x00000001 (1)
DateCreated	REG_BINARY	DA 07 02 00 02 00 17 00 09 00 2B 00 0C 00 33 00
NameType	REG_DWORD	0x00000006 (6)
DateLastConnected	REG_BINARY	DA 07 02 00 00 00 1C 00 14 00 33 00 34 00 F1 02
CategoryType	REG_DWORD	0x00000000 (0)
IconType	REG_DWORD	0x00000000 (0)

An X-Ways Forensics dialog box is open, displaying the hex value: DA 07 02 00 02 00 17 00 09 00 2B 00 0C 00 33 00.

Taskbar: 28.02.2010 20:51:52 SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{CB4B3179-583A-4040-B94E-2B5C15E4BC84} Drive C:\Wir

Registry Änderungen: Registry Keys zu verbundenen Netzwerken

- **Seit Windows Vista werden in der Registry Informationen zu den Netzwerken abgelegt, mit denen ein Rechner verbunden war**
- `HKLM\Software\Microsoft\Windows NT\Current Version\NetworkList\Profiles\[GUID]`
- **Für jedes Netzwerkprofil wird ein separater Unterordner mit einer GUID angelegt**
- **Dort finden sich u.a. Informationen zum Zeitpunkt der ersten und letzten Verbindung zu diesem Netzwerk**

Registry Änderungen: Registry Keys zu verbundenen Netzwerken

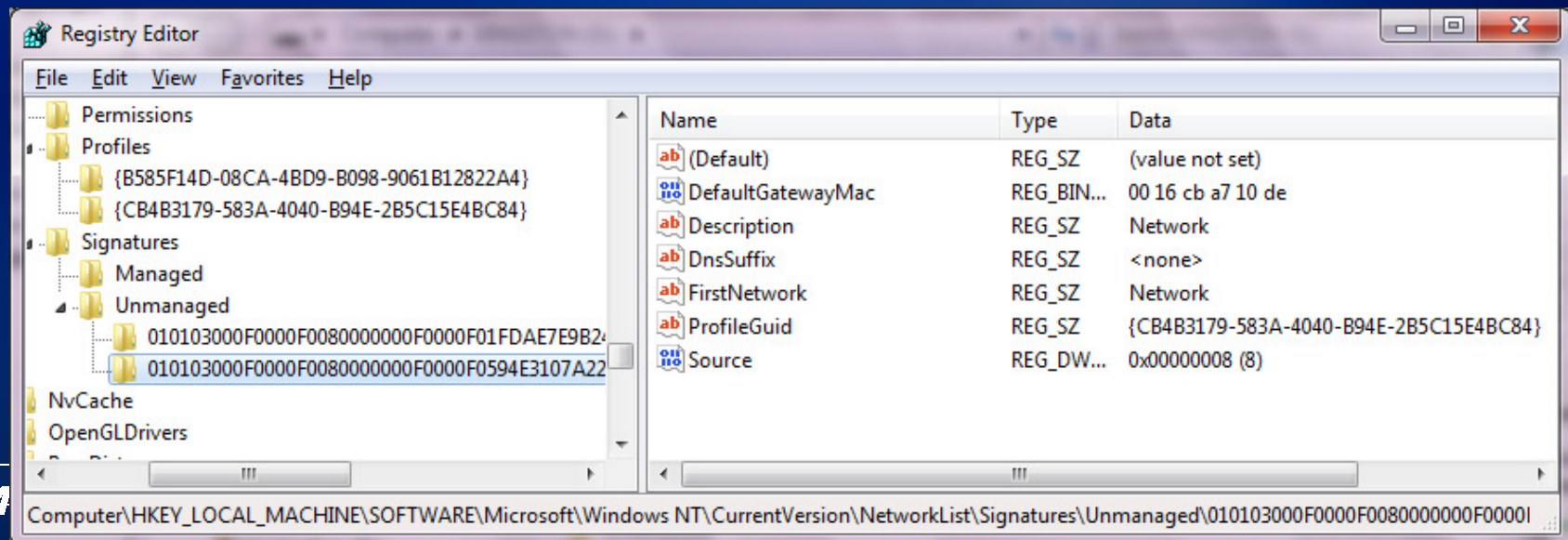
- DA 07 02 00 02 00 17 00 09 00 2B 00 0C 00 33 00

- **Umrechnung der Kodierung:**

- Jahr: DA 07 => 2010
- Monat: 02 00 => Februar
- Wochentag: 02 00 => Dienstag
- Tag: 17 00 => 23
- Stunde: 09 00 => 9
- Minute: 2B 00 => 43
- Sekunde: 0C 00 => 12
- Millisekunde: 33 00 => 51

Registry Änderungen: Registry Keys zu verbundenen Netzwerken

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures
- **Speichert die MAC-Adresse des Default-Gateways und bei Wireless-Verbindungen die SSID des Netzwerks**
- **Zuordnung zum Netzwerkprofil über den Key „ProfileGuid“**



Betriebssystem-Artefakte

Betriebssystem Artefakte: Überblick

- **Thumbcache-Dateien**
- **Windows Papierkorb**
- **Volume Shadow Copies**
- **Windows Event Log**
- **Prefetching**
- **Ordner Virtualisierung**
- **Libraries**
- **JumpLists**
- **Sticky Notes**
- **XP-Mode**

Speicherforensik

RAM-Sicherung unter Windows 7

- **Windd ab Version 1.30 von Matthieu Suiche unterstützt die RAM-Sicherung unter Windows 7**
 - Support für 32- und 64-Bit-Architekturen
 - Administrator-Rechte notwendig
 - Weitere Tools zur Memory-Sicherung verfügbar:
 - winen aus der EnCase-Software
 - FTK Imager von AccessData

RAM-Analyse unter Windows 7

- **Analyse mit X-Ways Forensics zeigt teilweise schon die Speicherstrukturen von Windows 7 an**
 - Erlaubt die weitere Analyse im Hinblick auf Prozesse und sonstige Artefakte im Hauptspeicher
 - Analyse funktioniert bereits mit 32-Bit-Versionen von Windows 7
 - Nach unseren Experimenten wird 64-Bit Speicher noch nicht direkt unterstützt
 - Eine Analyse durch File Carving funktioniert natürlich dennoch

RAM-Analyse unter Windows 7

The screenshot displays the X-Ways Forensics application window titled "X-Ways Forensics - [memdump-win7-32bit]". The interface is divided into several panes:

- Case Data:** A tree view on the left showing the file structure. The selected path is "Festplatte 0 > memdump-win7-32bit > Objects > BaseNamedObjects".
- File List:** A table in the center showing a list of files. The file "win32dd.exe" is selected, with a size of 33.2 MB.
- Hex/ASCII View:** The bottom pane shows a detailed view of the selected file's contents, including offset, hex, and ASCII representations.
- Data Interpreter:** A window on the right showing file metadata for "win32dd.exe".

The "Data Interpreter" window displays the following information:

- File size: 4,0 GB
- 4.294.967.296 bytes
- W/o slack: 294.967.296 bytes
- [Read-only mode]
- Creation time: 03.03.2010 17:44:38
- Attributes: none
- Case association: Yes

The hex/ASCII view shows the following data:

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000065536	A8	A1	D6	F1	97	AB	00	01	EE	FF	EE	FF	01	00	00	00
0000065552	A8	00	01	00	A8	00	01	00	00	00	01	00	00	00	01	00
0000065568	10	00	00	00	88	05	01	00	00	00	02	00	0F	00	00	00
0000065584	01	00	00	00	00	00	00	00	F0	0F	01	00	F0	0F	01	00
0000065600	00	80	00	00	00	00	00	00	00	00	00	00	00	00	10	00
0000065616	19	A1	D7	41	97	AB	00	00	AD	A2	97	7D	00	00	00	00
0000065632	00	FE	00	00	FF	EE	FF	EE	00	00	10	00	00	20	00	00
0000065648	00	02	00	00	00	20	00	00	4B	01	00	00	FF	EF	FD	7F
0000065664	02	00	38	01	00	00	00	00	00	00	00	00	00	00	00	00
0000065680	E8	0F	01	00	E8	0F	01	00	0F	00	00	00	F8	FF	FF	FF
0000065696	A0	00	01	00	A0	00	01	00	10	00	01	00	10	00	01	00
0000065712	00	00	00	00	00	00	00	00	50	01	01	00	00	00	00	00
0000065728	00	00	00	00	90	05	01	00	90	05	01	00	38	01	01	00
0000065744	AF	6B	0D	0A	00	00	00	00	00	00	00	00	00	00	01	00
0000065760	00	10	00	00	00	00	00	00	00	00	00	00	00	01	00	00
0000065776	01	00	00	00	00	00	00	00	00	00	00	00	04	00	00	00
0000065792	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000065808	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000065824	00	00	00	00	00	00	00	00	00	10	00	00	00	10	00	00

RAM-Carving unter Windows 7

X-Ways Forensics - [MEMORY_c_1] 15.5 SR-2

Datei Bearbeiten Suchen Position Ansicht Extras Specialist Optionen Fenster Hilfe

Falldaten

Datei Bearbeiten

Hommingberger_Memory

MEMORY_c_1

MEMORY_c_1

Partitionierungstyp: ? 1+381=382 Dateien, 0 Partitionen

Name	Typ	Größe	Erzeugung	Änderung	Zugriff	Attr.	1. Sektor	Kommentar
bcd		24,0 KB					5046976	
carved_00001.dll	dll	100 KB					5984	
carved_00002.exe	exe	3,4 MB					6240	
carved_00003.dll64	dll64	184 KB					6528	
carved_00004.xml	xml	3,4 KB					6728	
carved_00005.xml	xml	3,7 KB					6736	
carved_00006.xml	xml	2,9 KB					6752	
carved_00007.xml	xml	3,9 KB					6776	
carved_00008.dll	dll	0,8 MB					6960	

Disk Datei Vorschau Details Galerie Legende Sync

Gewählt: 1 Datei, 0 Verz. (35,7 MB)

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
20DFEB000	2	65	67	66	95	01	00	00	95	01	00	00	55	82	E8	63
20DFEB010	51	B9	CA	01	01	00	00	00	05	00	00	00	00	00	00	00
20DFEB020	01	00	00	00	20	00	00	00	00	E0	3B	02	01	00	00	00
20DFEB030	65	00	6D	00	52	00	6F	00	6F	00	74	00	5C	00	53	00
20DFEB040	79	00	73	00	74	00	65	00	6D	00	33	00	32	00	5C	00
20DFEB050	43	00	6F	00	6E	00	66	00	69	00	67	00	5C	00	53	00
20DFEB060	4F	00	46	00	54	00	57	00	41	00	52	00	45	00	00	00
20DFEB070	C8	88	68	01	6F	6C	DE	11	8D	1D	00	1E	0B	CD	E3	EC
20DFEB080	C8	88	68	01	6F	6C	DE	11	8D	1D	00	1E	0B	CD	E3	EC
20DFEB090	01	00	00	00	C9	88	68	01	6F	6C	DE	11	8D	1D	00	1E
20DFEB0A0	0B	CD	E3	EC	72	6D	74	6D	00	00	00	00	00	00	00	00
20DFEB0B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
20DFEB0C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
20DFEB0D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
20DFEB0E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
20DFEB0F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
20DFEB100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
20DFEB110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
20DFEB120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
20DFEB130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
20DFEB140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
20DFEB150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
20DFEB160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

[C:\WINDD\MEMORY_c_1.d
[Schreibschutz-Modus]

Gesamtkapazität: 16,5 GB
17.716.736.000 Bytes

Bytes pro Sektor: 512

Modus: Text
Zeichensatz: ANSI ASCII
Offsetdarstellung: hexadezimal
Bytes pro Seite: 23x16=368

Fenster-Nr.: 1
Geöffnete Fenster: 1
Fall-Verknüpfung: Ja

Zwischenablage: verfügbar
TEMP-Ordner: 37,6 GB frei
s:\tech\AppData\Local\Temp

Daten-Dolmetscher

8 Bit (±): 114

Sektor 17235800 von 34603000 Offset: 20DFEB000 = 114 Block: 1033B0AA3 - 1033B0AA9

Fazit

Fazit

- **BitLocker To-Go könnte die Analyse von USB-Sticks erschweren**
- **Hersteller von Forensik-Software müssen bei der Unterstützung neuer Features von Windows 7 teilweise noch nachziehen**
- **Viele neue Windows-Artefakte wie bspw. JumpLists oder Libraries**
- **Analyse von VHD-Containern sollte berücksichtigt werden**



Kontakt:

KPMG AG Wirtschaftsprüfungsgesellschaft

Alexander Geschonneck

Partner Forensic Technology

T +49 30 2068-1520

ageschonneck@kpmg.com

www.kpmg.de/forensic

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2009 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Konzerngesellschaft der KPMG Europe LLP und Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International, einer Genossenschaft schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. KPMG und das KPMG-Logo sind eingetragene Markenzeichen von KPMG International.