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

KPMG Forensic: **Unsere Dienstleistungen**

Forensic unterstützt Sie bei …

Sachverhaltsaufklärung
Präventionsfragen und -konzepten
Sicherstellung von Vermögenswerten

Fraud Risk Management

Konzeptionierung, Implementierung, Optimierung von ganzheitlichen Fraud Risk Management-Systemen und System-elementen/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 Hintergrund-informationen zu Unternehmen, Geschäfts-personen und Vermögenswerten

Investigations

Aufdeckung und Untersuchung von wirtschafts-kriminellen 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	Pre-mium	Profes-sional	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

RO = Read Only über Bitlocker To Go – Lesetool

KPMG

Überblick Windows 7 und Vista Editionen

	Windows 7					Windows Vista				
	Starter	Home Basic	Pre-mium	Profes-sional	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

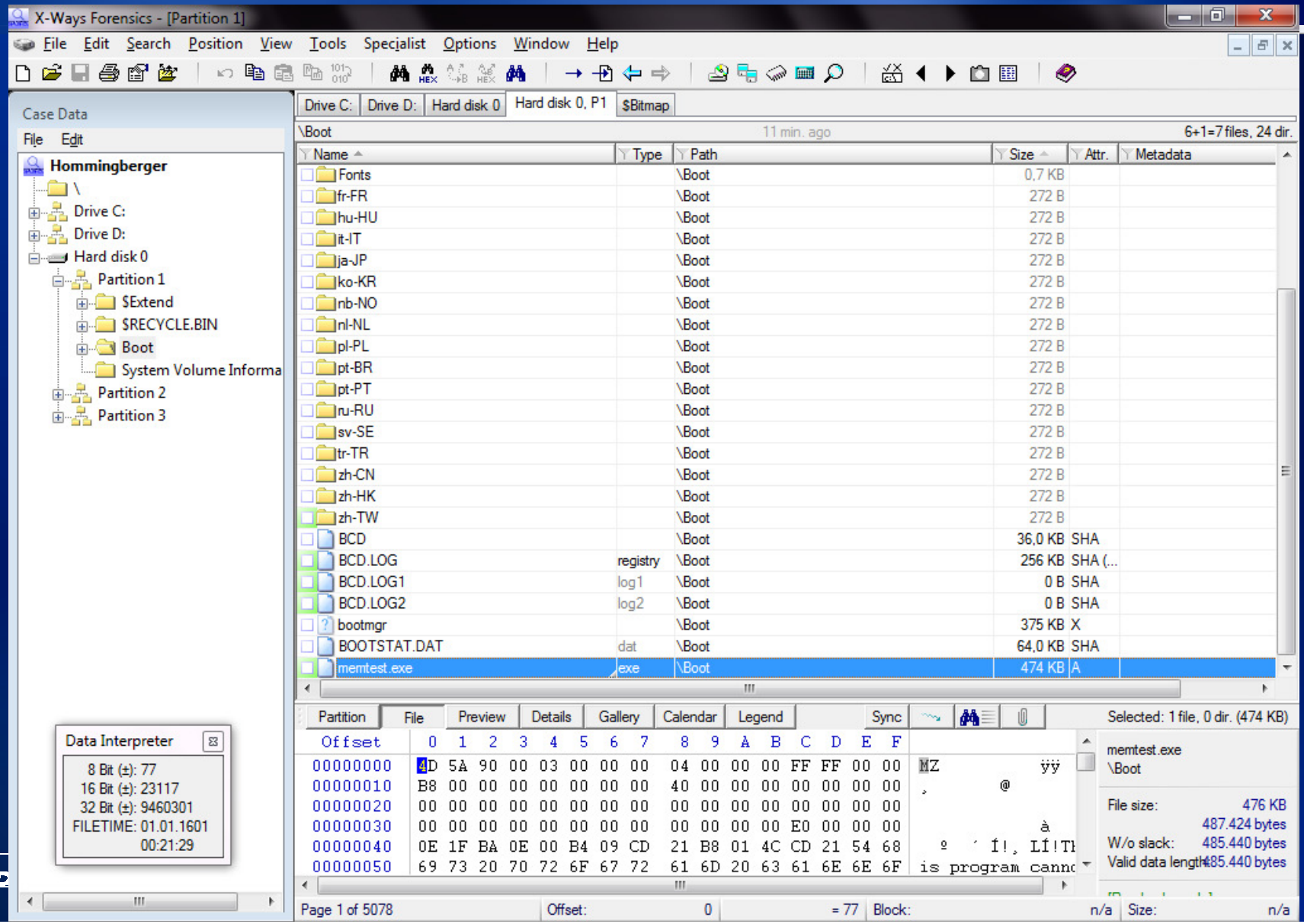
KPMG

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)

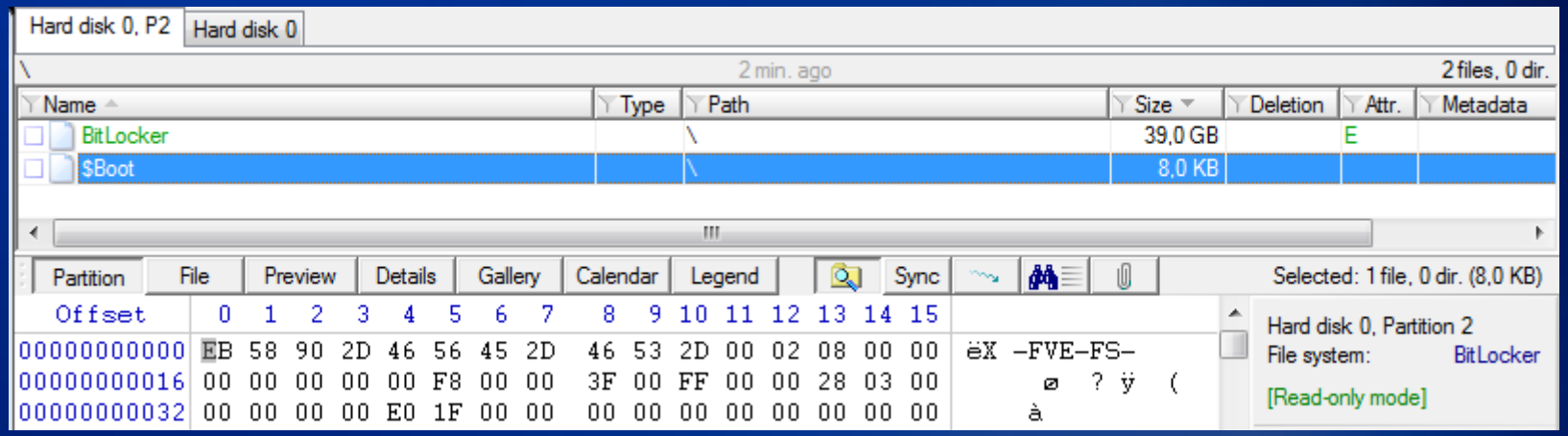


Änderungen bei BitLocker

Änderungen bei BitLocker im Überblick

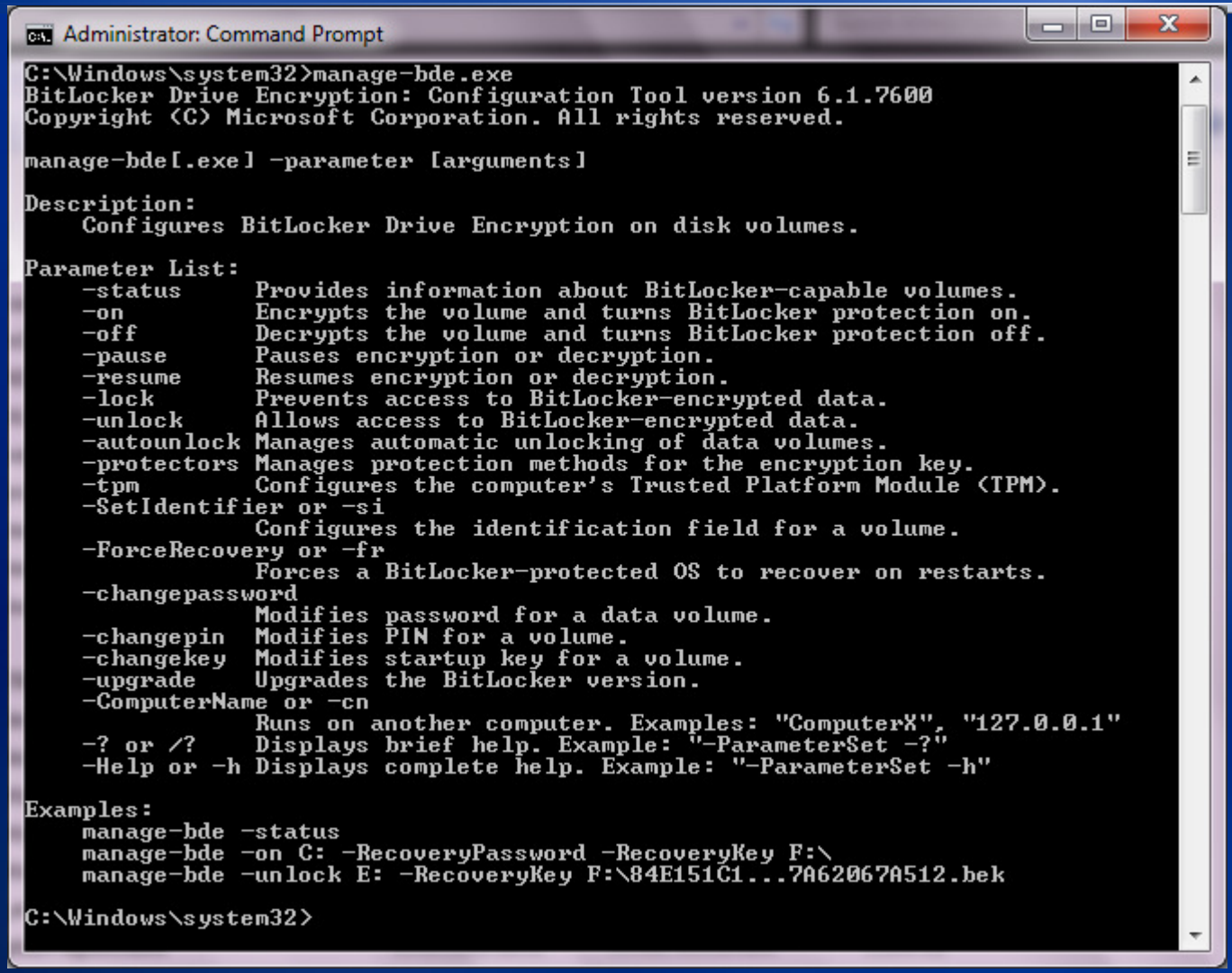
- **Neues BitLocker-Format**
  - BitLocker Partitionen in Windows 7 haben eine leicht geänderte Signatur
  - Alte Windows-Versionen können Windows 7-BitLocker-Partitionen nicht öffnen
    - Windows 7 öffnet jedoch Vista-Partitionen
- **Seit Vista SP1 können auch andere Partitionen als die Systempartition 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



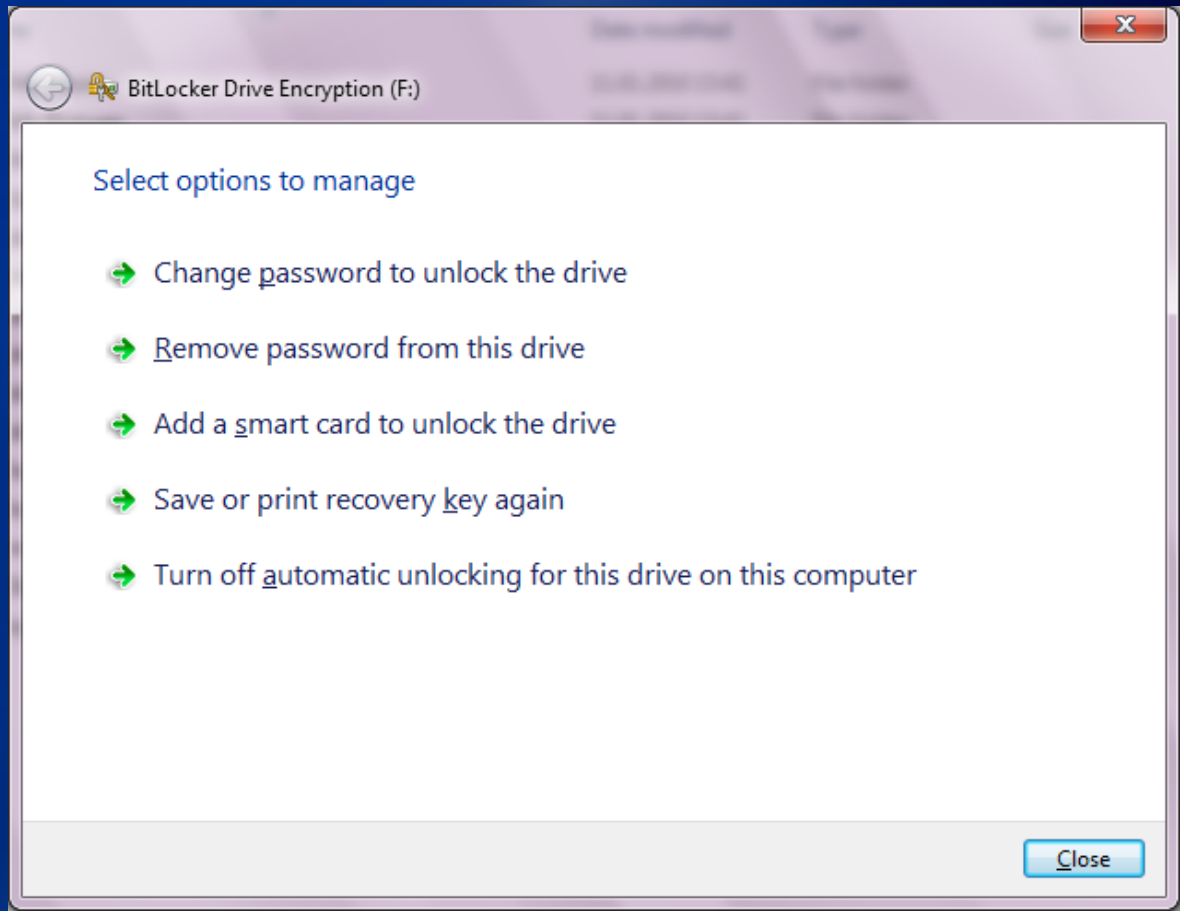
- Signatur beginnt nun mit Hex EB 58 statt EB 52 wie bei Vista
- Typischer Header „-FVE-FS-“ ist jedoch noch vorhanden
- X-Ways Forensics kennzeichnet die Partition bereits als BitLocker

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



Änderungen bei BitLocker: BitLocker To Go

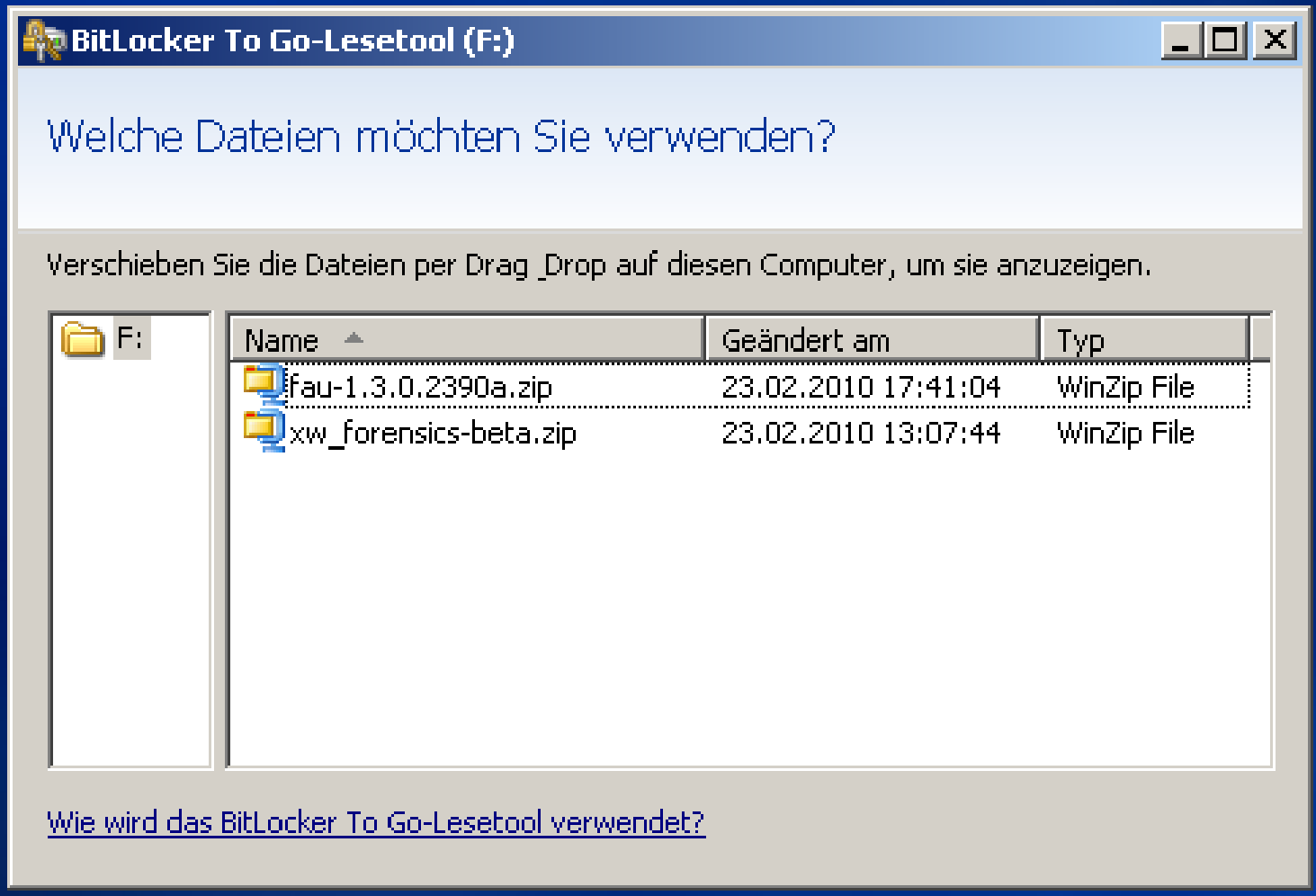
- **BitLocker für mobile Datenträger**
- **Verschlüsselungsoptionen „To Go“:**
  - Passwort,
  - Smart Card und
  - Automatic Unlocking
  - Kombinationen davon sind möglich



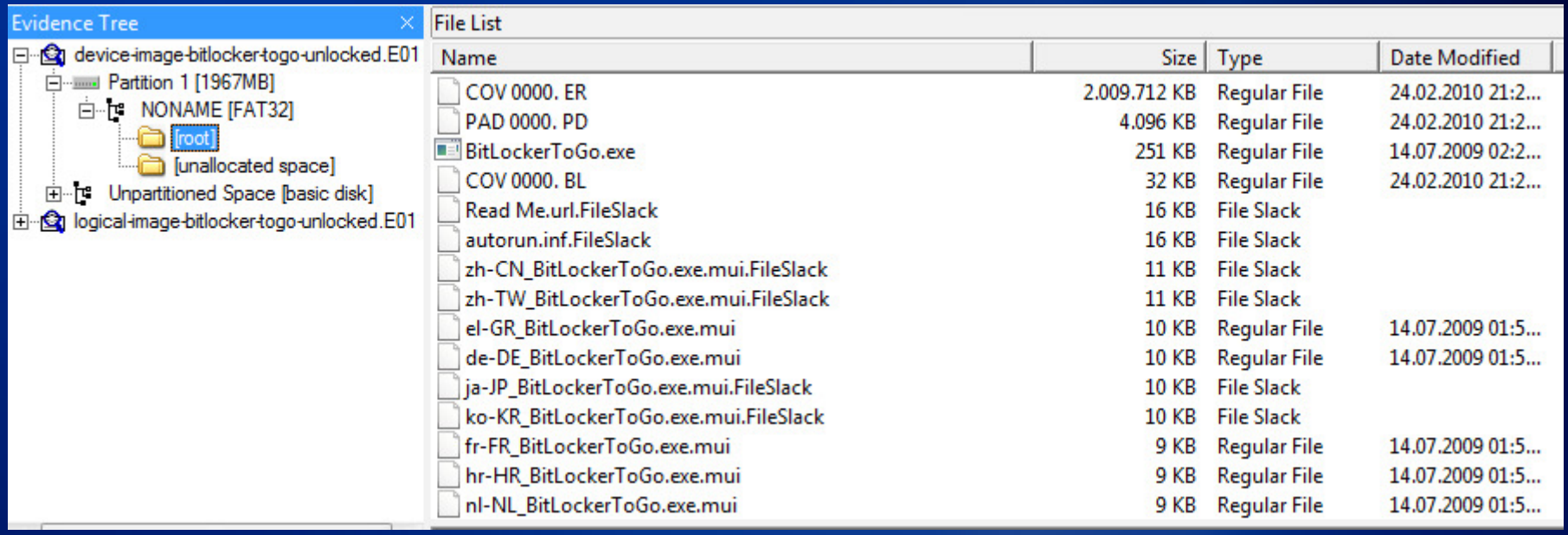
Änderungen bei BitLocker: BitLocker To Go

- **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“

Änderungen bei BitLocker: BitLocker To Go - Lesetool



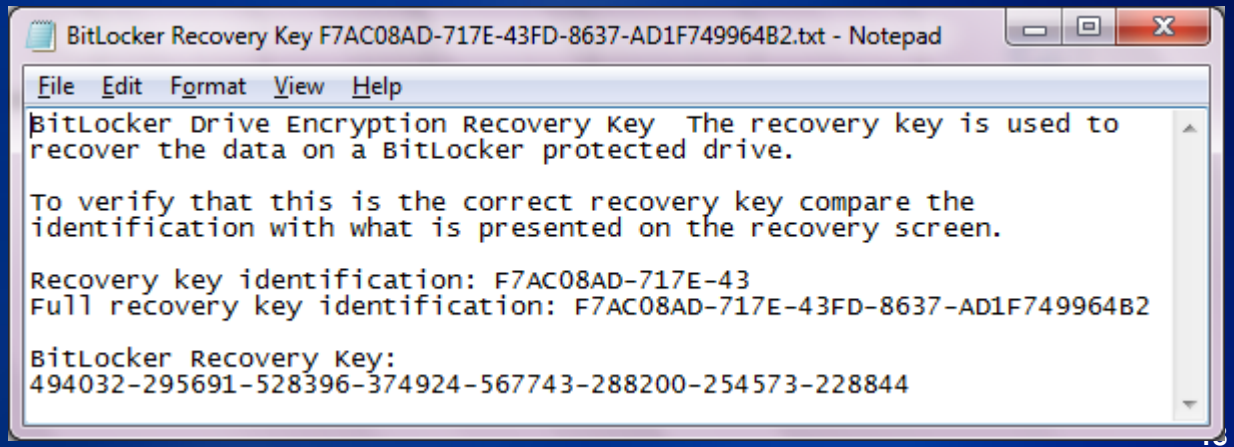
Änderungen bei BitLocker: BitLocker To Go – Verschlüsselte Ansicht



- 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-“)

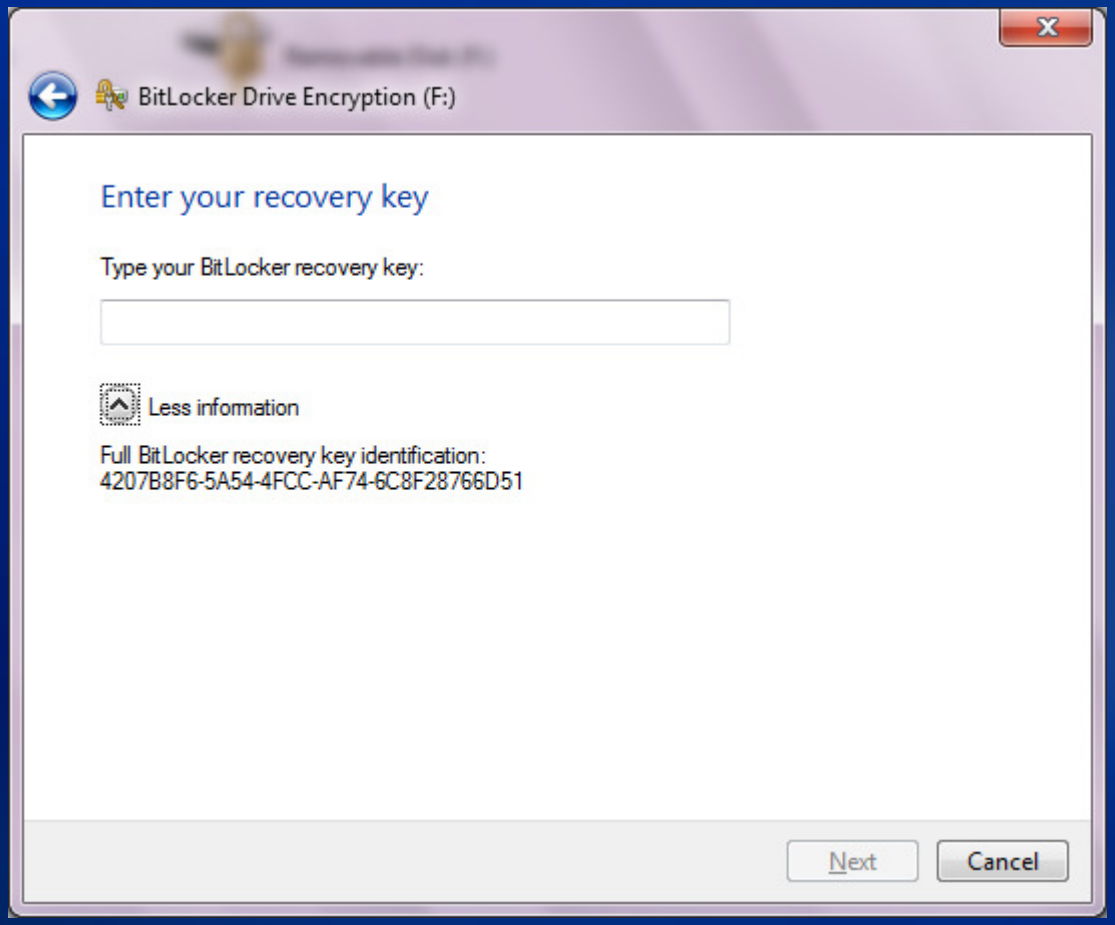
Änderungen bei BitLocker: Forensische Analyse

- **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 Signatur-suche in Forensik Tools genutzt werden
  - Bei Live-Analyse von gemounteten BitLocker-Volumes kann der Recovery Key extrahiert werden
  - Neuer Datei-name der Re-covery Files



KPMG

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-Ergäzungen 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-Ergäzungen (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“

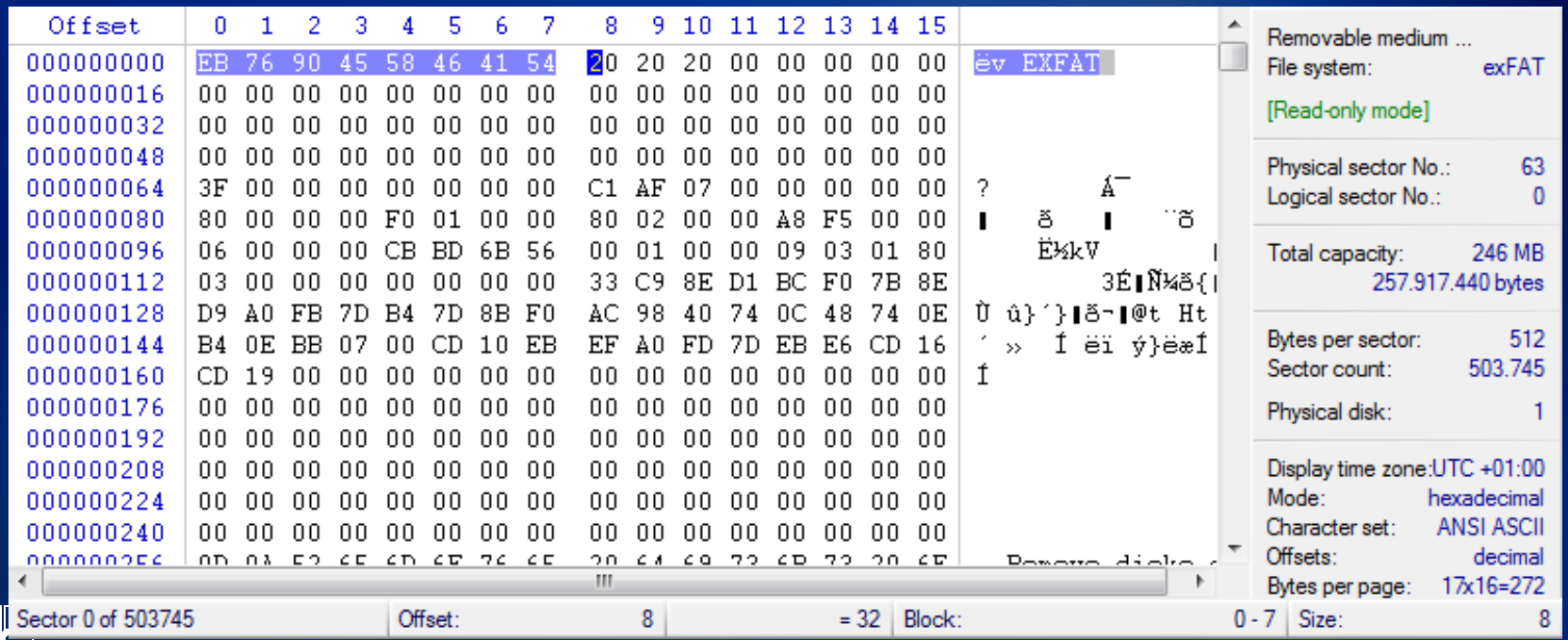
Neues bei Dateisystemen (4/6): exFAT

- **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

KPMG

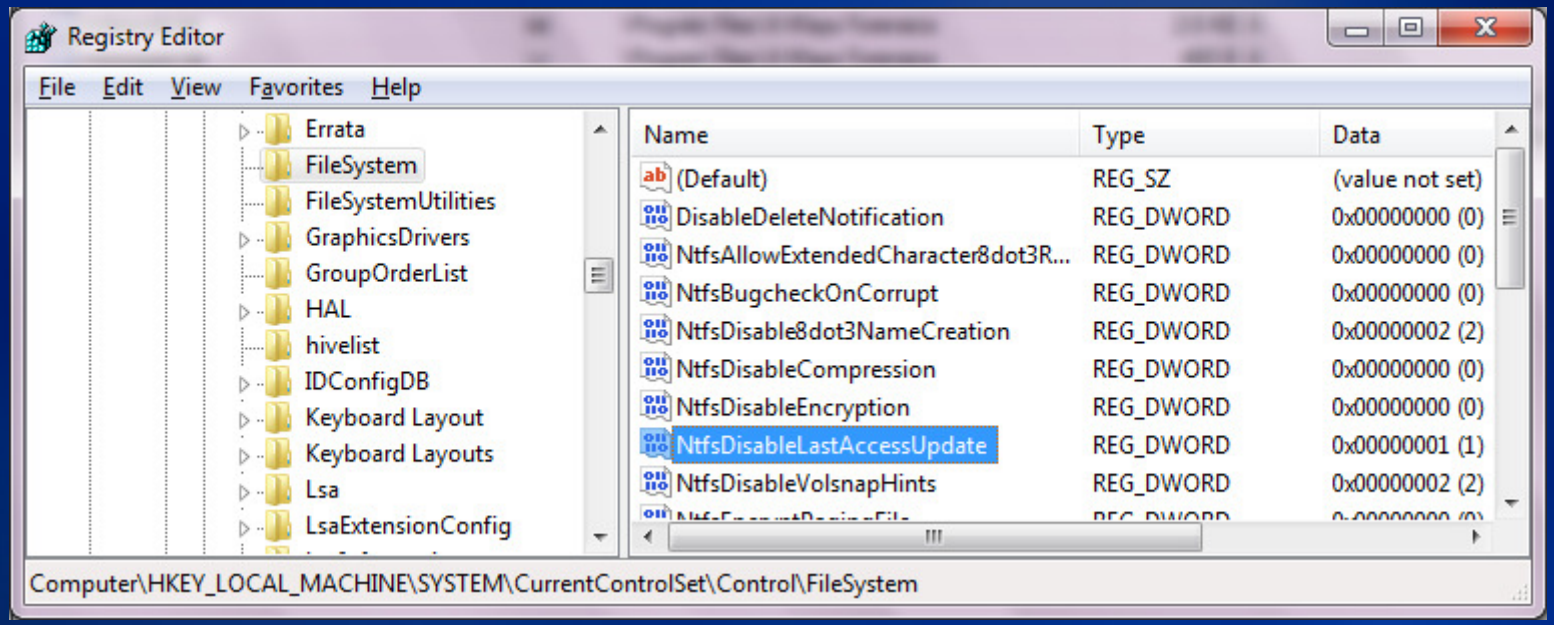
Neues bei Dateisystemen (5/6): Forensische Analyse exFAT

- **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



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

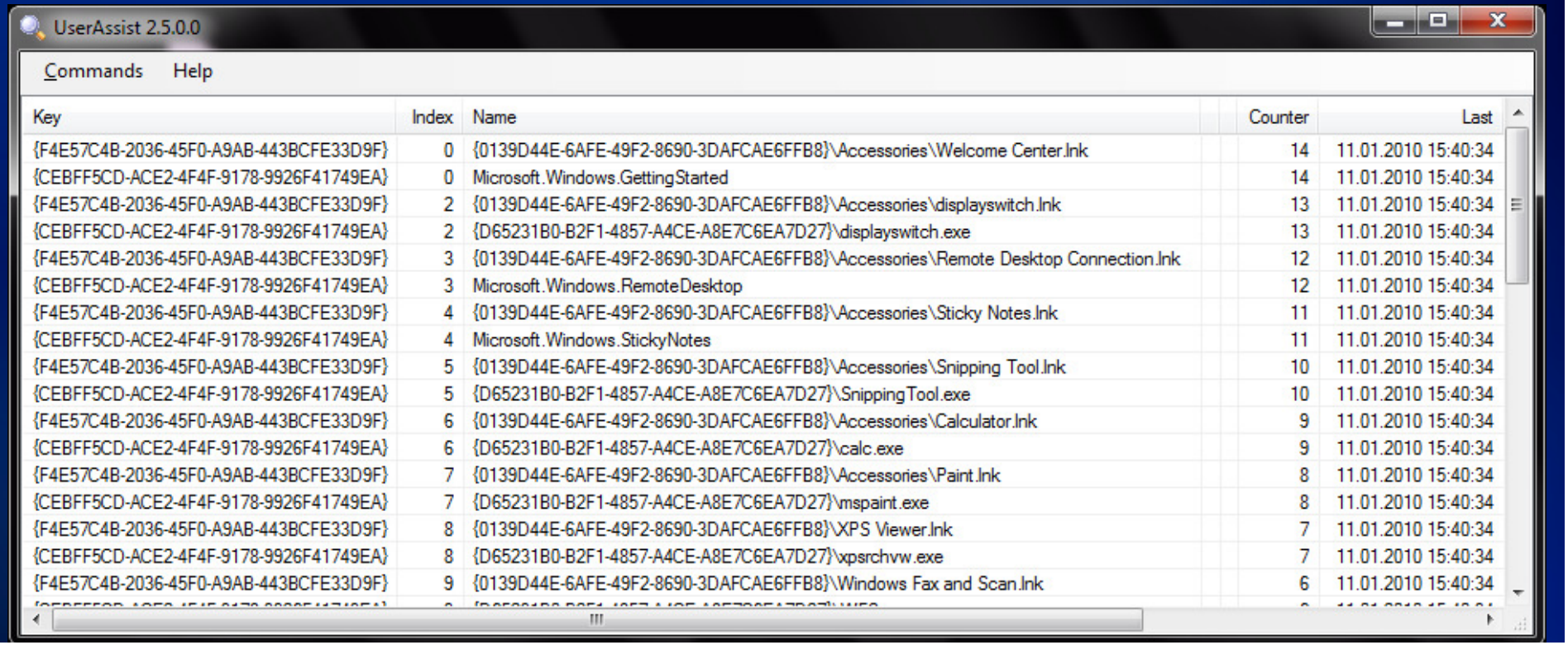
- **Folgende ausgewählte inhaltliche Änderungen sollen näher analysiert werden:**
  - UserAssist Keys
  - Verbundene Netzwerke

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-verschleierten 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

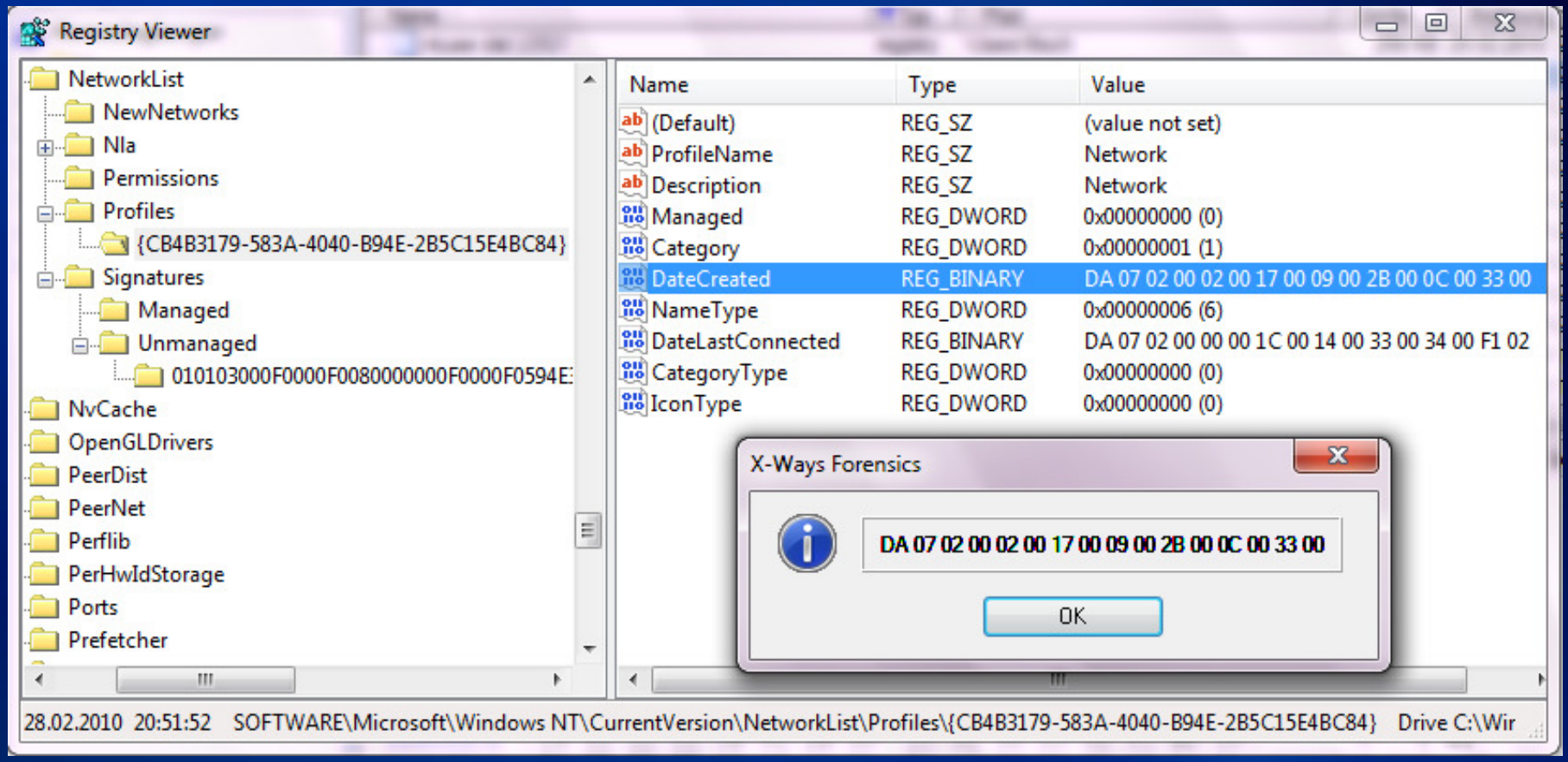


Key	Index	Name	Counter	Last
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	0	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Welcome Center.lnk	14	11.01.2010 15:40:34
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	0	Microsoft.Windows.GettingStarted	14	11.01.2010 15:40:34
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	2	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\displayswitch.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\CurrentVersion\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



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\CurrentVersion\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

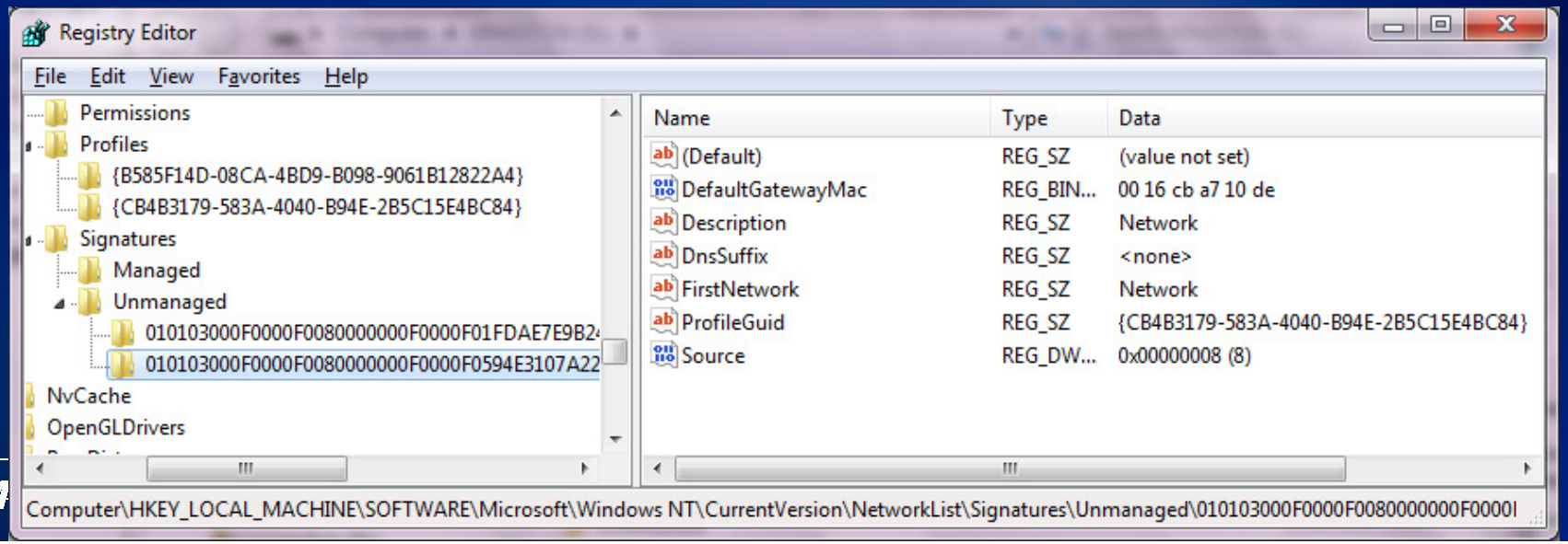
Registry Änderungen: Registry Keys zu verbundenen Netzwerken

- **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

KPMG

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“**



KPMG

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

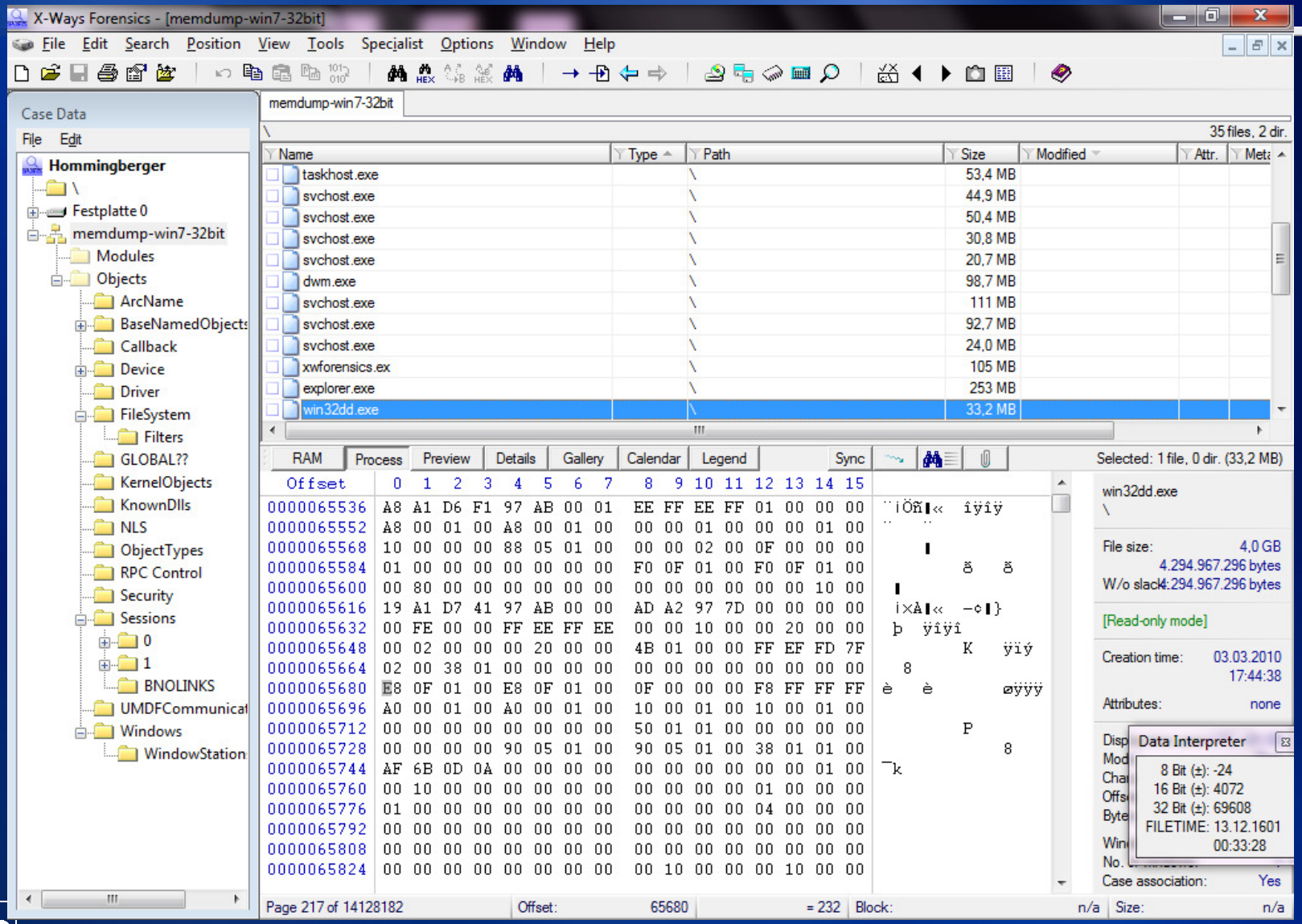
RAM-Sicherung unter Windows 7

- **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

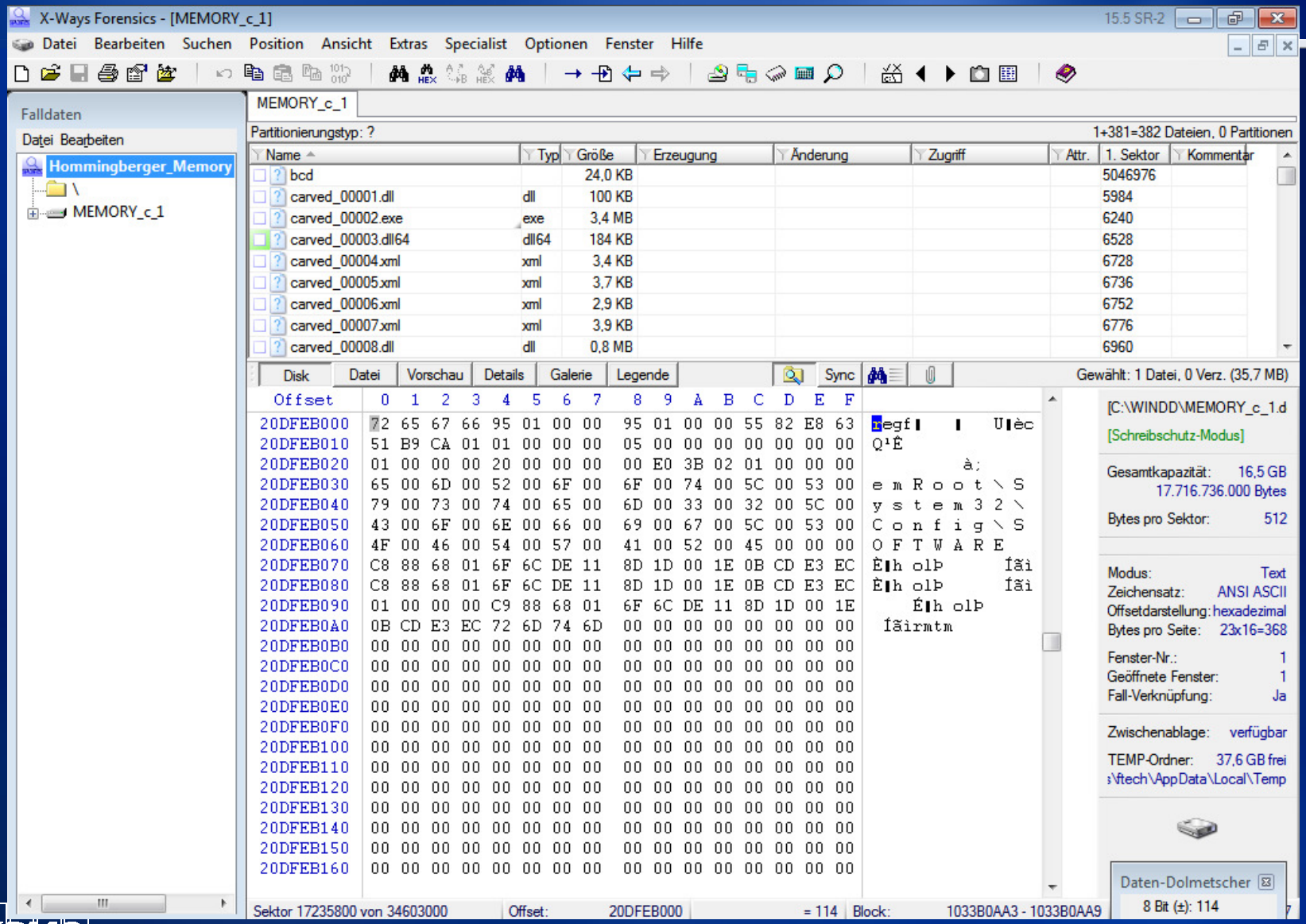
RAM-Analyse unter Windows 7

- **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 wird noch nicht direkt unterstützt
  - Eine Analyse durch File Carving funktioniert natürlich dennoch

RAM-Analyse unter Windows 7



RAM-Carving unter Windows 7



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