Forensik Guide

Digitale Ermittlungen

„Finden von kopierten, gesendeten und gelöschten Daten“

erstellt von

Marko Rogge
am 17.07.2019

Inhaltsverzeichnis

1 Einleitung, Allgemeine Hinweise zur Vorgehensweise

Dieses Dokument dient der Hilfestellung zum Auffinden von Spuren in Windows Systemen, wenn Daten kopiert, verschoben, versendet (z.B. E-Mail) und/oder gelöscht wurden. Zudem wird darauf eingegangen, wo Spuren zu finden sind, wenn USB-Devices verbunden waren. Weiterhin werden entsprechende Browser- und Internet-Artefakte aufgezeigt, die Hinweise auf die Nutzung von Web-Mails beinhalten können. Da so genannte Cloud-Dienste zum einen zunehmen und Anwender diese auch zunehmend nutzen, wird in diesem Dokument ebenfalls darauf eingegangen, wo sich Spuren von Cloud-Diensten befinden. Es wird festgehalten, wo in Windows Systemen Spuren zu finden sind und welche Tools zu Hilfe genommen werden können.

BITTE BEACHTEN: Eine rechtliche Würdigung aller beschriebener Methoden ist nicht gegeben!

Grundsätzlich sollte hierbei zwischen Live Forensik und Post-mortem unterschieden werden, da einige Methoden an den Registry-Hives-Files durchgeführt werden und einige im laufenden Betrieb eines Systems.

Post-mortem: Untersuchung eines Speicherabbildes / Daten daraus

Live Forensik, **Live-Response**: laufendes System, flüchtige Daten (z.B. RAM)

Anmerkungen zur Tool Sammlung **DART2**: Es sind in DART2 sehr viele kostenfreie Tools der Firma Nirsoft enthalten. Diese Tools bieten für die Forensik durchaus Hilfestellungen. Ich möchte sie jedoch anhalten, sich nicht zu sehr auf die Ergebnisse dieser Tools zu verlassen. Verifizieren sie immer die Ergebnisse die sie erzielt haben mit anderen Tools oder manuellen Methoden.

Es empfiehlt sich, individuell nach der Fragestellung aus einem Vorgang die Vorgehensweise zu bestimmen.

2 Zeitstempel und deren Bedeutung

Modification-Time

- Zeitstempel wird aktualisiert, wenn sich der Inhalt der Datei verändert
- Beim Kopieren oder Verschieben nicht verändert
- Bei Veränderung des Dateinamens oder der Dateiattribute nicht verändert

Access-Time

- Zeitstempel wird aktualisiert, wenn Metadaten oder Dateiinhalte angezeigt werden
- Anzeige von Dateieigenschaften
- Öffnen von Dateien

Creation-Time

- Zeitstempel wird bei neuer Erstellung oder Kopie einer Datei aktualisiert
- Beim Verschieben wird dieser Zeitstempel nicht aktualisiert

Unter Windows Vista, 7 und 8 ist der Last Access Time Zeitstempel in der Standardinstallation deaktiviert!

Registry-Pfad:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLa
stAccess
Update
```

3 Relevante Registry Hives zur Auswertung

Windows 7, 8 und Windows 10:

```
C:\Users\user_name\NTUSER.DAT
C:\Windows\System32\config\DEFAULT
C:\Windows\System32\config\SAM
C:\Windows\System32\config\SECURITY
C:\Windows\System32\config\SOFTWARE
C:\Windows\System32\config\SYSTEM
```

4 Vorgehensweise mit EnCase um Hives zu betrachten

EnCase hat einen integrierten Registry-Viewer, der die entsprechenden Hives darstellt und auswertbar macht. Eine Möglichkeit ist hierbei, direkt in EnCase zu arbeiten und die entsprechenden Hives dafür zu öffnen, um die Registry-Keys zu betrachten.

Methode: Post-mortem

Dazu empfiehlt sich folgende Vorgehensweise:

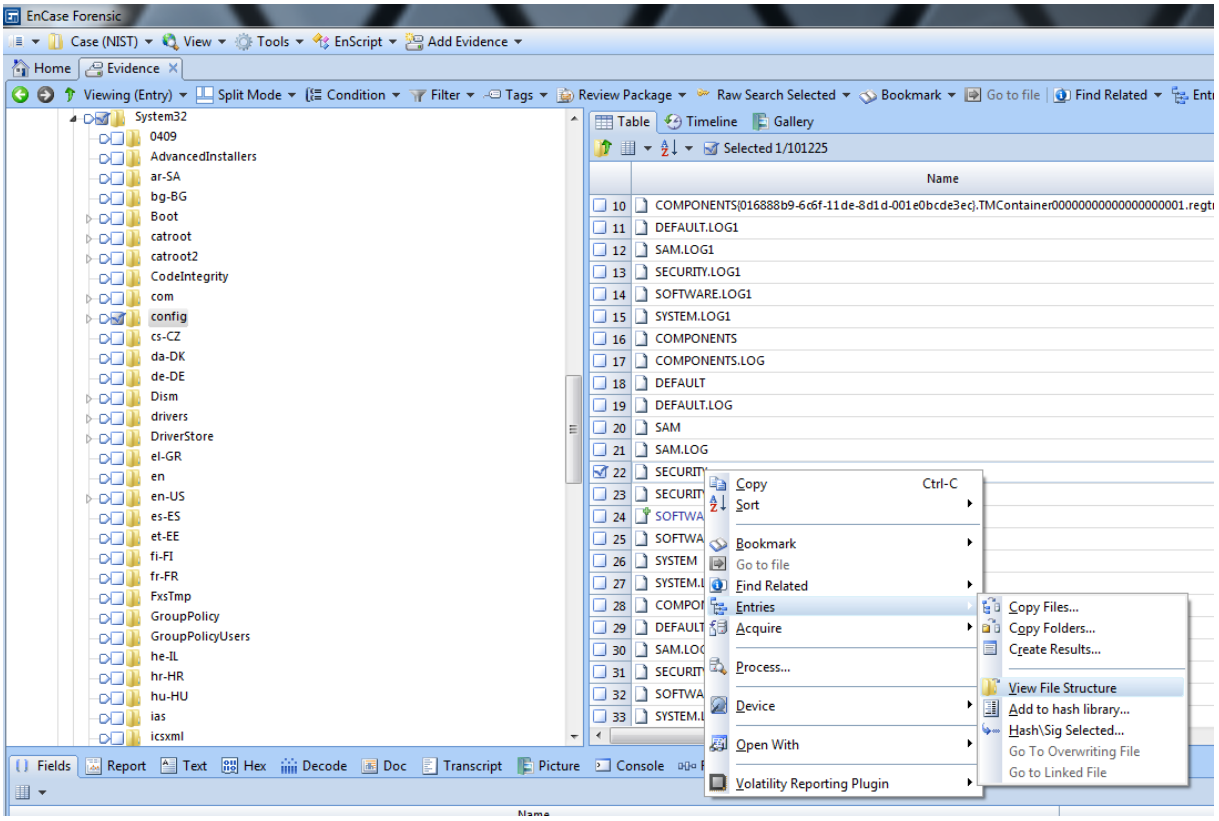


Abbildung 1: eingebundener Case in \Windows\System32\config\

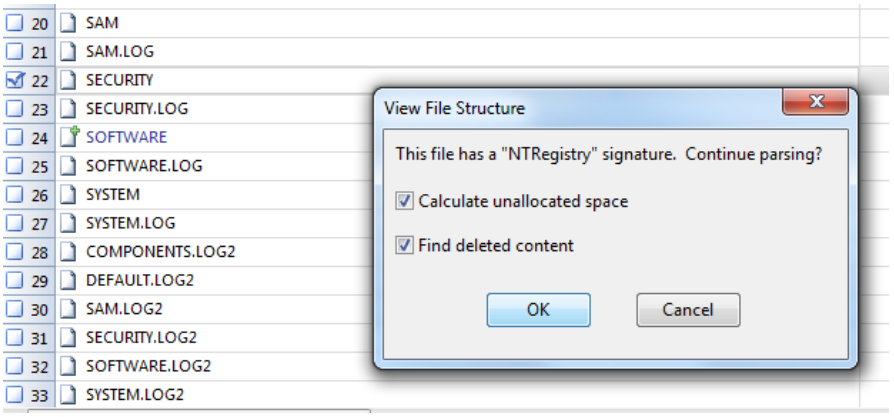


Abbildung 2: Parsing Options

Nachdem man den Case erfolgreich eingebunden hat, sucht man den entsprechenden Hive, den man auswerten möchte. Anschließend öffnet man mit einem rechts-Klick das Untermenü und öffnet den Hive über „Entries – View File Strcture“. Anschliessend bekommt der Hive ein grünes Kreuz und kann geöffnet werden.

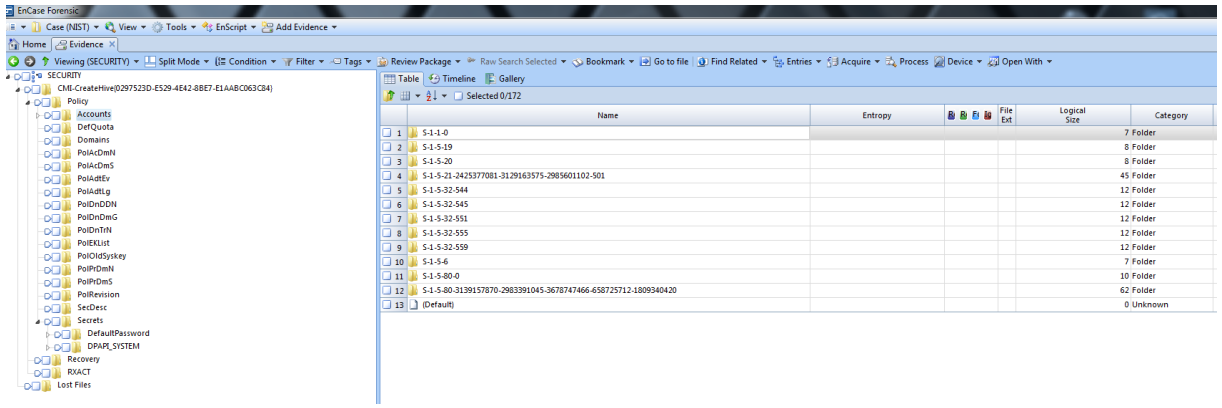


Abbildung 3: Account Hives in EnCase – SECURITY Hive

Eine weitere Vorgehensweise, wenn man gezielt nach Informationen in den Hives suchen möchte, ist das Processing des Cases. Dabei sollten aber nicht alle Module aktiviert werden. Es empfiehlt sich, nachstehende Einstellungen vorzunehmen:

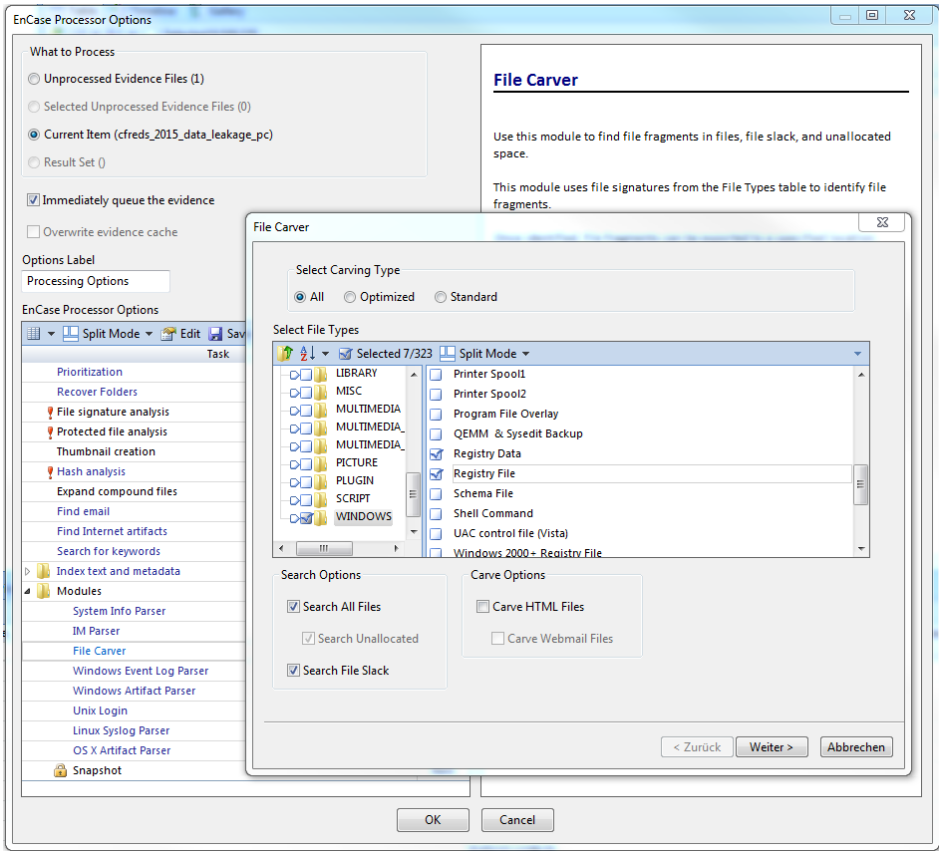


Abbildung 4: Processing Einstellungen für das Carving

Folgende Optionen sollten aktiviert werden:

1- Expand Compound Files: Enable
2- File Carver: Enable Windows – Registry Data und Registry File
3- System Info Parser: Enable

Ergänzend möchte ich anführen, dass insbesondere das extrahieren von gepackten Daten nicht sehr zuverlässig von EnCase in der Version 7.x durchgeführt wird. Insbesondere bei PST-Dateien traten massive Abweichungen auf.

4.1 Export der Registry Hives

Eine weitere Möglichkeit die Hives auszuwerten und zu untersuchen ist der Export aus EnCase, um die Registry Files mit einem externen Viewer auswerten zu können.

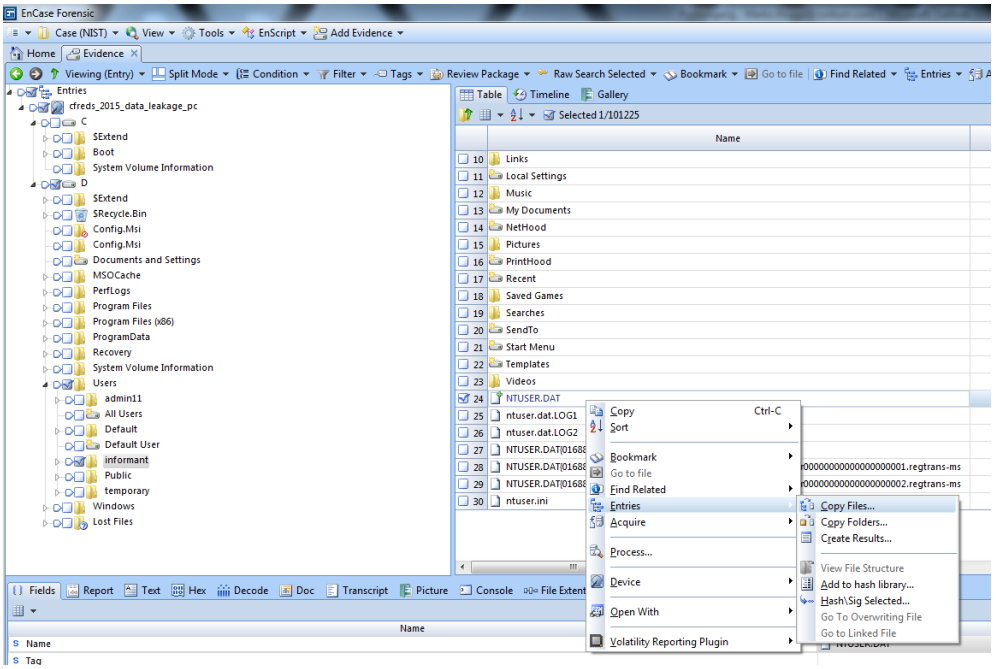
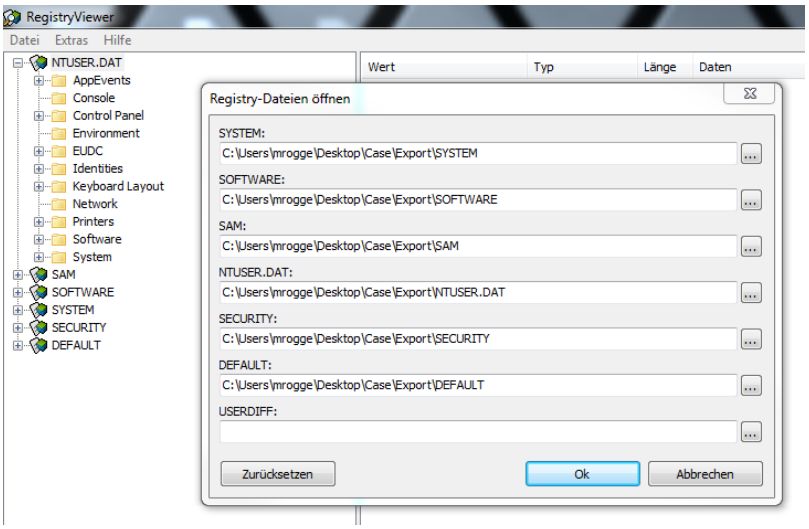


Abbildung 5: Exporte relevanter Hives aus EnCase

Anschließend kann man die Hives in die Software RegistryViewer laden und nach den Registry Keys durchsuchen:



Methode: Post-mortem

5 Angeschlossene USB-Devices und Storages

5.1 Identifizieren von USB Devices

Registry Keys zur Anzeige von Devices, die über die USB-Schnittstelle mit dem vorliegenden EDV-Gerät verbunden wurden:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB

Innerhalb des Devices befindet sich ein weiterer Ordner, der die Device ID darstellt:

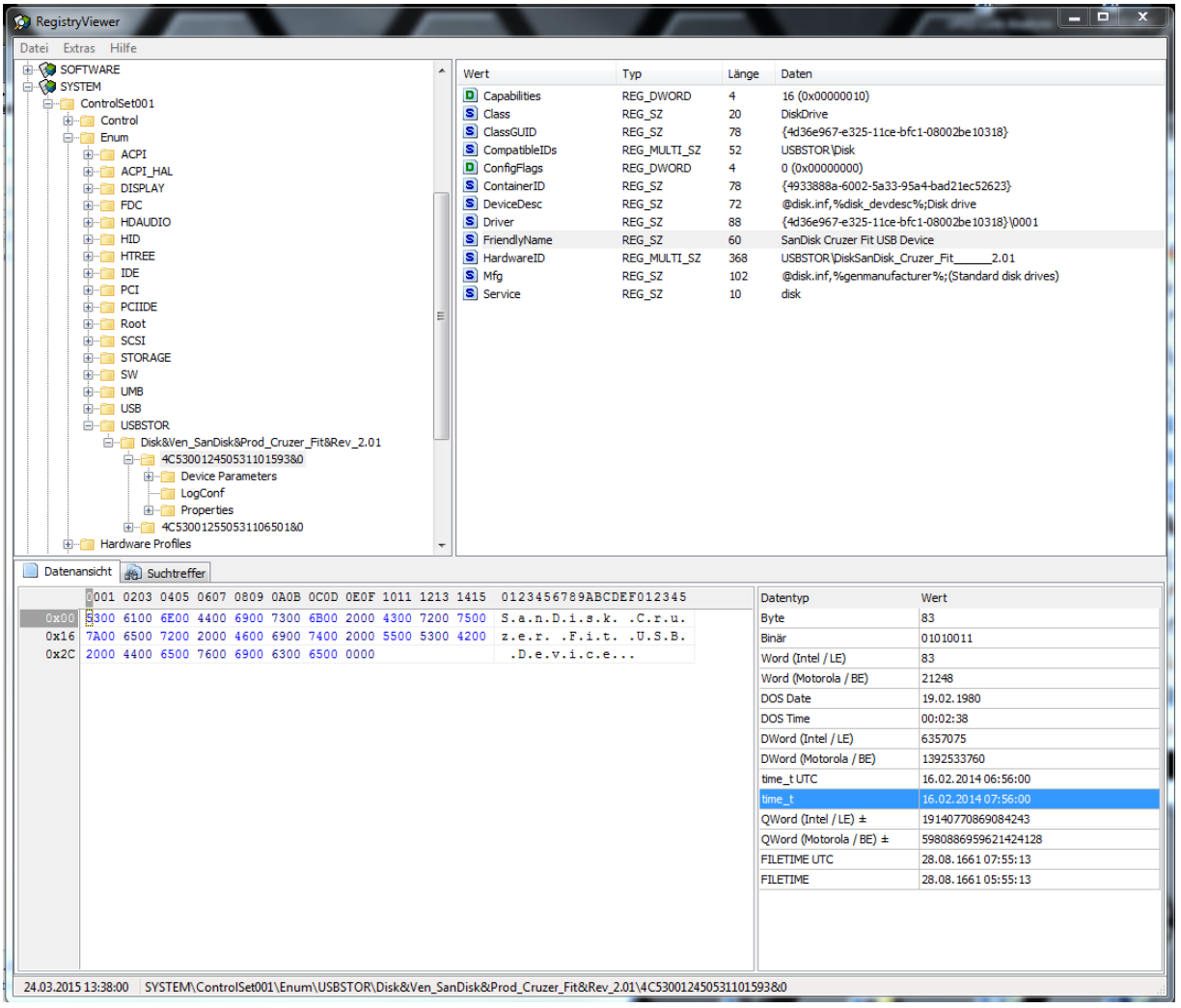


Abbildung 6: Device ID im RegistryViewer

Methode: Post-mortem

Innerhalb des Windows Systems werden ebenfalls Informationen zu USB-Devices gespeichert:

C:\Windows\inf\setupapi.dev.log

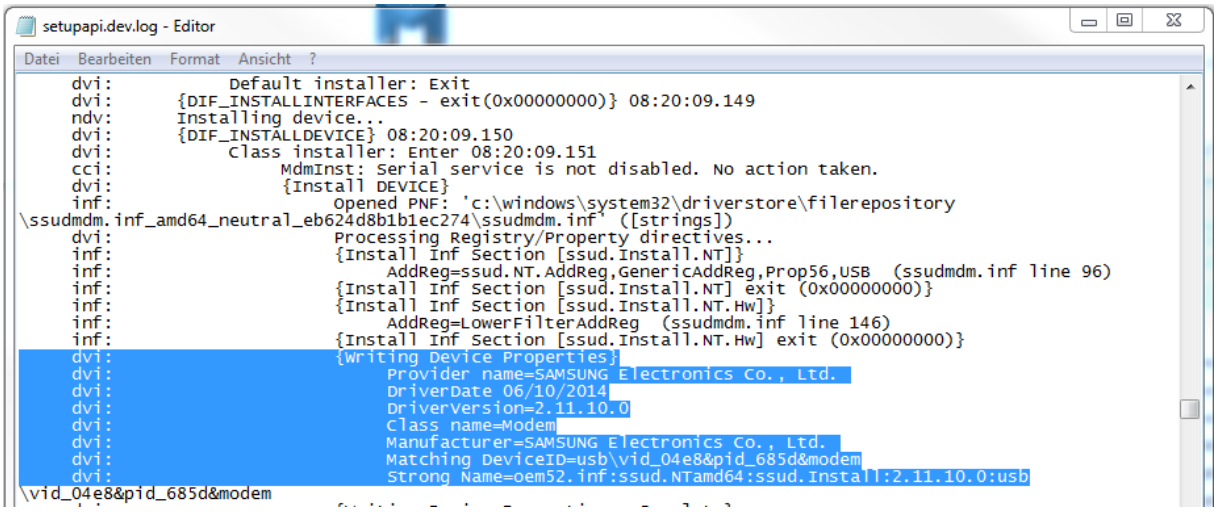


Abbildung 7: setupapi.dev.log Einsicht

Sofern es sich um ein laufendes System handelt, welches nicht forensisch untersucht werden muss, kann hier auch USBDeview von NirSoft zum Einsatz kommen, welches alle angeschlossenen USB Devices auflistet. USBDeview steht in der Forensic Tool Sammlung DART2 zur Verfügung:

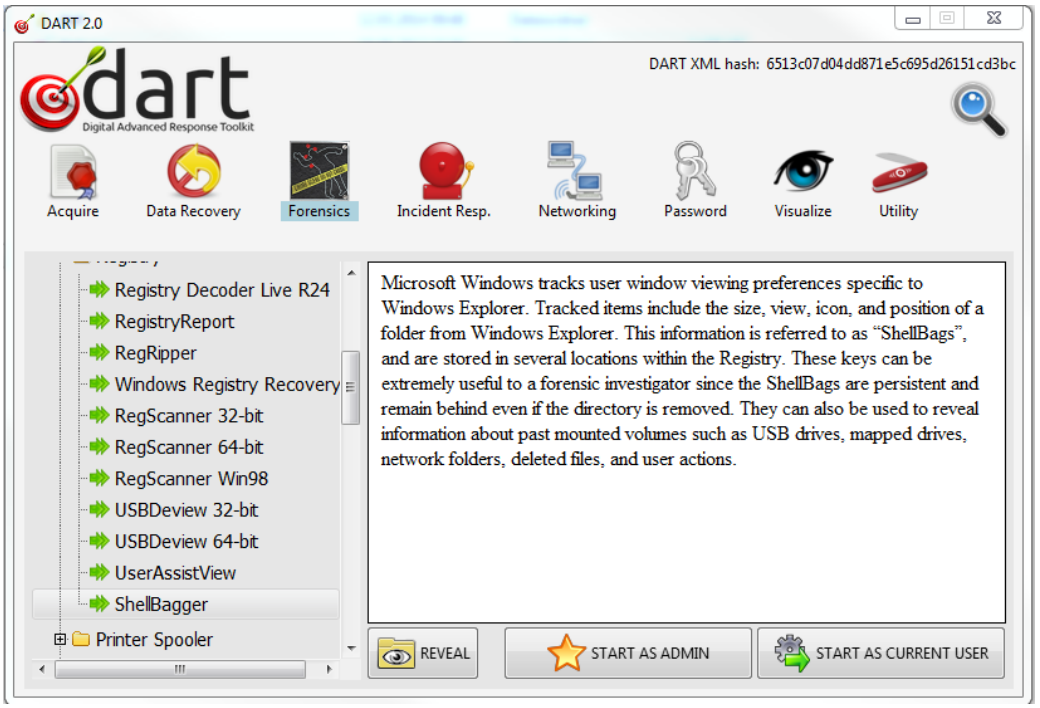
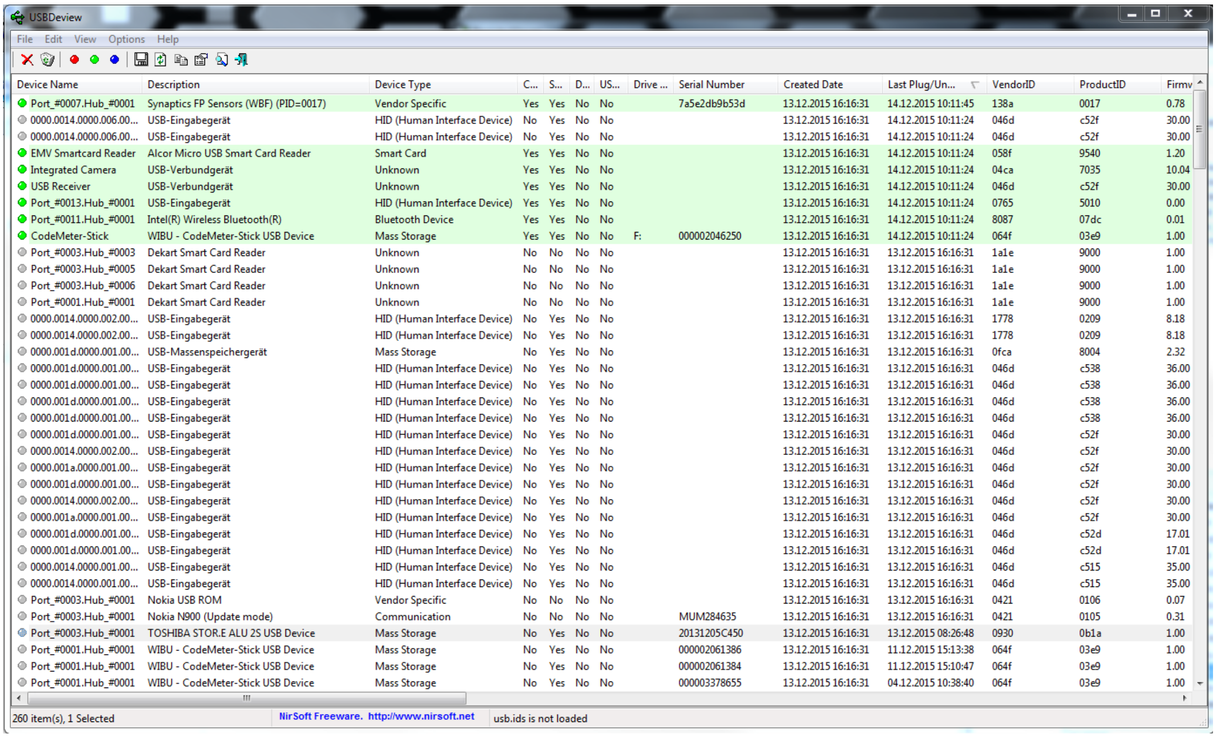


Abbildung 8: DART 2.0 mit USBDeview



Device Name	Description	Device Type	C...	S...	D...	US...	Drive ...	Serial Number	Created Date	Last Plug/Un...	VendorID	ProductID	Firmv
Port_#0007.Hub_#0001	Synaptics FP Sensors (WBF) (PID=0017)	Vendor Specific	Yes	Yes	No	No		7a5e2db9b53d	13.12.2015 16:16:31	14.12.2015 10:11:45	138a	0017	0.78
0000.0014.0000.006.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	14.12.2015 10:11:24	046d	c52f	30.00
0000.0014.0000.006.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	14.12.2015 10:11:24	046d	c52f	30.00
EMV Smartcard Reader	Alcor Micro USB Smart Card Reader	Smart Card	Yes	Yes	No	No			13.12.2015 16:16:31	14.12.2015 10:11:24	058f	9540	1.20
Integrated Camera	USB-Verbundgerät	Unknown	Yes	Yes	No	No			13.12.2015 16:16:31	14.12.2015 10:11:24	04ca	7035	10.04
USB Receiver	USB-Verbundgerät	Unknown	Yes	Yes	No	No			13.12.2015 16:16:31	14.12.2015 10:11:24	046d	c52f	30.00
Port_#0013.Hub_#0001	USB-Eingabegerät	HID (Human Interface Device)	Yes	Yes	No	No			13.12.2015 16:16:31	14.12.2015 10:11:24	0765	5010	0.00
Port_#0011.Hub_#0001	Intel(R) Wireless Bluetooth(R)	Bluetooth Device	Yes	Yes	No	No			13.12.2015 16:16:31	14.12.2015 10:11:24	8087	07dc	0.01
CodeMeter-Stick	WIBU - CodeMeter-Stick USB Device	Mass Storage	Yes	Yes	No	No	F:	000002046250	13.12.2015 16:16:31	14.12.2015 10:11:24	064f	03e9	1.00
Port_#0003.Hub_#0003	Dekart Smart Card Reader	Unknown	No	No	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	1a1e	9000	1.00
Port_#0003.Hub_#0005	Dekart Smart Card Reader	Unknown	No	No	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	1a1e	9000	1.00
Port_#0003.Hub_#0006	Dekart Smart Card Reader	Unknown	No	No	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	1a1e	9000	1.00
Port_#0001.Hub_#0001	Dekart Smart Card Reader	Unknown	No	No	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	1a1e	9000	1.00
0000.0014.0000.002.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	1778	0209	8.18
0000.0014.0000.002.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	1778	0209	8.18
0000.001d.0000.001.00...	USB-Massenspeichergerät	Mass Storage	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	0fca	8004	2.32
0000.001d.0000.001.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c538	36.00
0000.001d.0000.001.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c538	36.00
0000.001d.0000.001.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c538	36.00
0000.001d.0000.001.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c538	36.00
0000.001d.0000.001.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c52f	30.00
0000.0014.0000.002.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c52f	30.00
0000.001a.0000.001.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c52f	30.00
0000.001d.0000.001.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c52f	30.00
0000.0014.0000.002.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c52f	30.00
0000.001a.0000.001.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c52f	30.00
0000.001d.0000.001.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c52d	17.01
0000.001d.0000.001.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c52d	17.01
0000.0014.0000.001.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c515	35.00
0000.0014.0000.001.00...	USB-Eingabegerät	HID (Human Interface Device)	No	Yes	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	046d	c515	35.00
Port_#0003.Hub_#0001	Nokia USB ROM	Vendor Specific	No	No	No	No			13.12.2015 16:16:31	13.12.2015 16:16:31	0421	0106	0.07
Port_#0003.Hub_#0001	Nokia N900 (Update mode)	Communication	No	No	No	No		MUM284635	13.12.2015 16:16:31	13.12.2015 16:16:31	0421	0105	0.31
Port_#0003.Hub_#0001	TOSHIBA STOR.E ALU 2S USB Device	Mass Storage	No	Yes	No	No		20131205C450	13.12.2015 16:16:31	13.12.2015 08:26:48	0930	0b1a	1.00
Port_#0001.Hub_#0001	WIBU - CodeMeter-Stick USB Device	Mass Storage	No	Yes	No	No		000002061386	13.12.2015 16:16:31	11.12.2015 15:13:38	064f	03e9	1.00
Port_#0001.Hub_#0001	WIBU - CodeMeter-Stick USB Device	Mass Storage	No	Yes	No	No		000002061384	13.12.2015 16:16:31	11.12.2015 15:10:47	064f	03e9	1.00
Port_#0001.Hub_#0001	WIBU - CodeMeter-Stick USB Device	Mass Storage	No	Yes	No	No		000003378655	13.12.2015 16:16:31	04.12.2015 10:38:40	064f	03e9	1.00

Abbildung 9: Einblick in USBDeview

Methode: Live-Response

5.2 Identifizieren von eingebundenen Storage

Bei manchen Computern/Laptops kann man über Wechselschächte oder Wechsellaufwerke Devices einbinden, Daten dorthin kopieren und das Devices anschließend wieder entfernen.

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\STORAGE\Volume

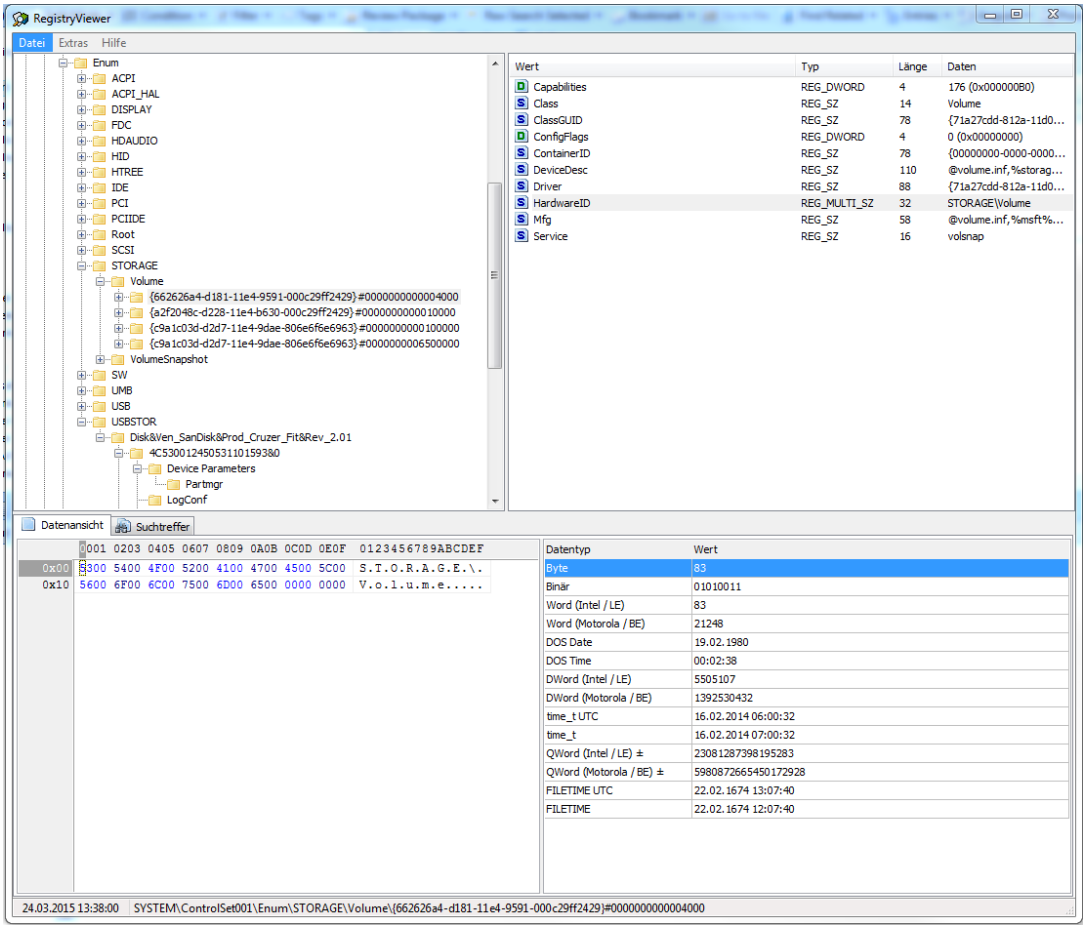


Abbildung 10: Der RegistryViewer stellt die Storages im Verzeichnisbaum dar. Die Informationen werden aus der Registry geladen.

Methode: Post-mortem

5.3 Welche Devices wurden gemountet

Zur Anzeige der tatsächlich gemounteten Devices kann man sich den nachstehenden Ordner in der Registry öffnen. Innerhalb des Ordners werden dann in der rechten Spalte die Devices angezeigt. Mit einem Doppel-Klick auf das Device, bekommt man die Details angezeigt:

HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

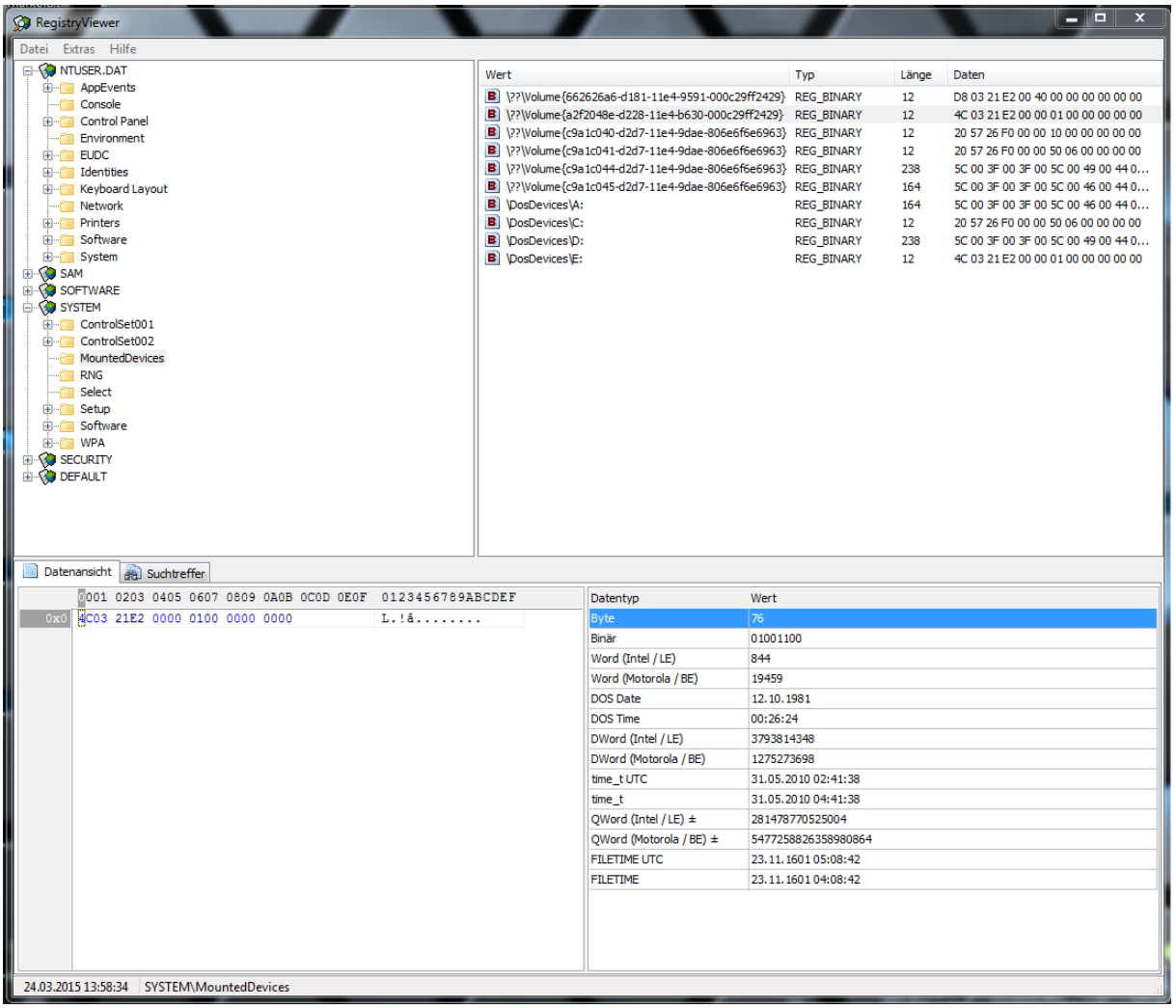


Abbildung 11: Mounted Devices aus der Registry

Methode: Post-mortem

5.4 Eingebundene Laufwerke und Devices

In der Registry lassen sich alle eingebundene und gemountete Devices und Laufwerke anzeigen:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
```

6 JumpLists überprüfen – Windows 7 und Windows 8

In den Jumplists können die letzten Zugriffe eines Users auf einem Windows 7 oder 8 System überprüft werden. Mittels EnCase kann man zu den entsprechenden Speicherbereichen gehen und sich die entsprechenden Listen in EnCase direkt betrachten.

Speicherort:

```
C:\Users\[User Profile]\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
C:\Users\[User Profile]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations
```

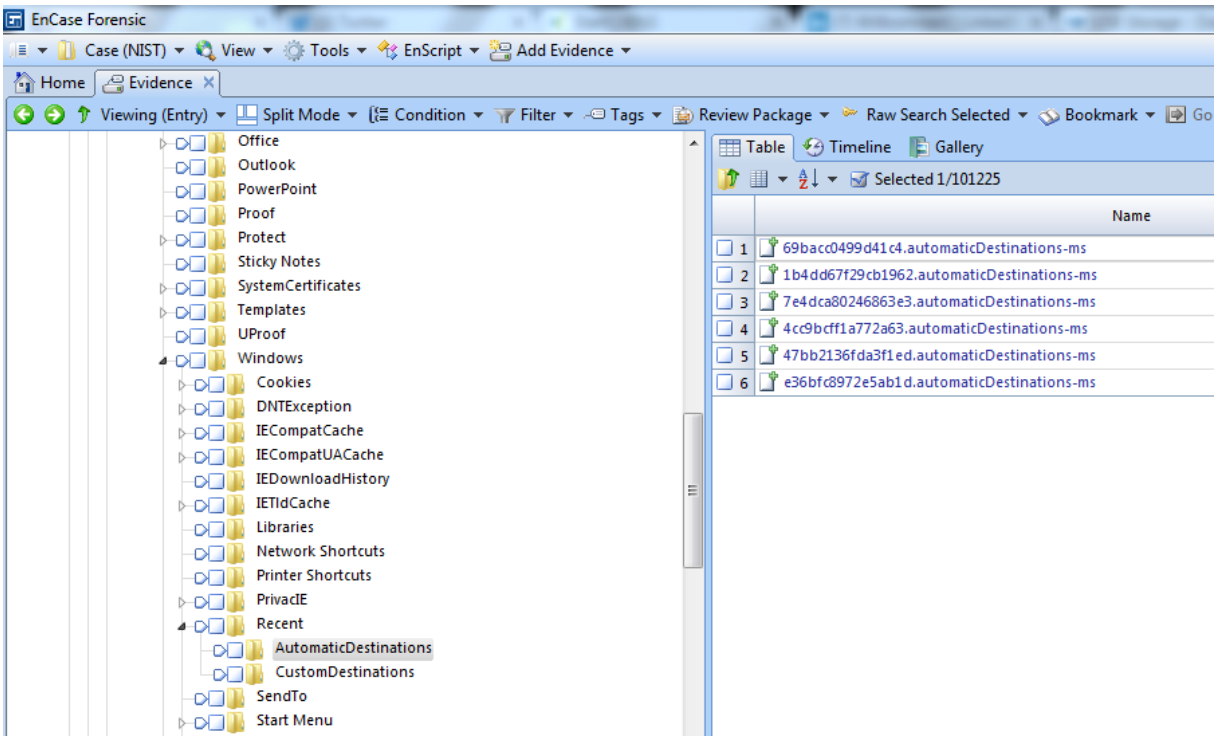


Abbildung 12: Speicherort der Jumplists

Methode: Post-mortem

Auf einem Live-System kann man mittels DART2 auf JumpListsView zugreifen und sich die JumpLists automatisiert anzeigen lassen.

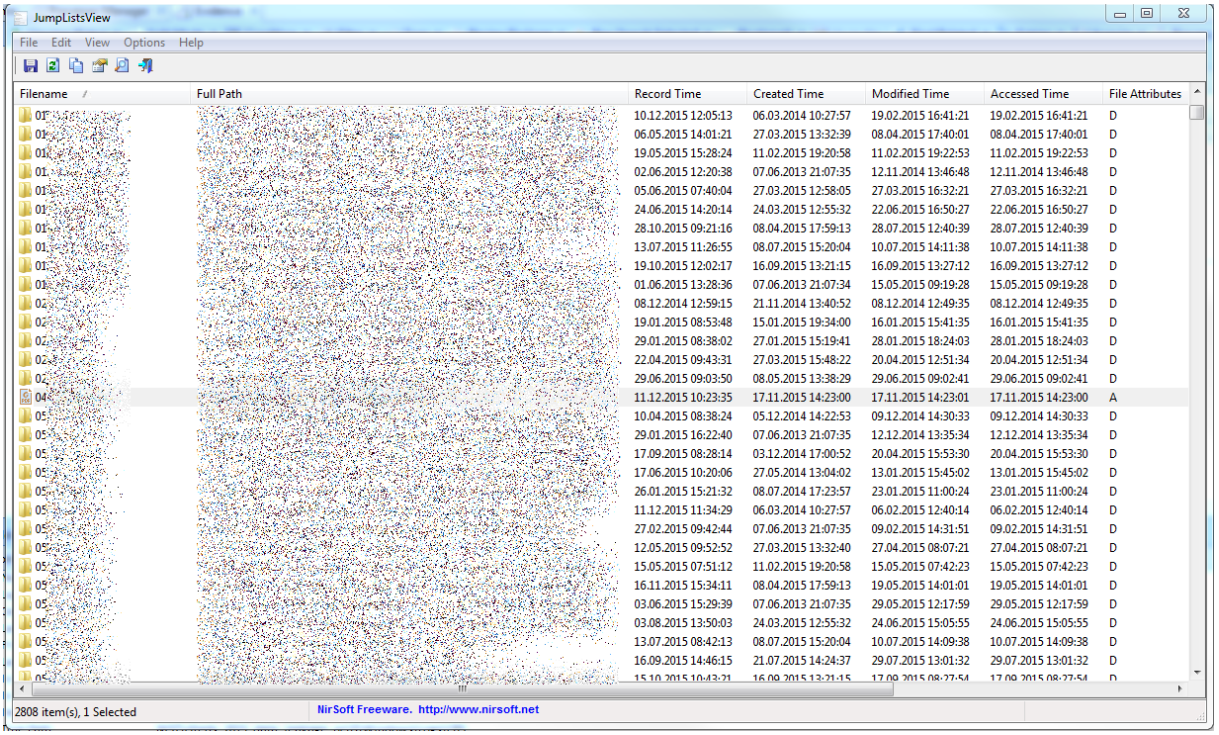


Abbildung 13: JumplistsViewer

Methode: Live-Response

7 E-Mail Anhänge über Outlook versendet

Bei laufenden Systemen ist es möglich Outlook dahin gehend zu untersuchen, welche Anhänge per E-Mail versendet wurden und wer Empfänger und Absender waren. Hierfür bietet DART2 das Tool „OutlookAttachView“, welches eine Übersicht der E-Mails mit Attachement ausgibt:

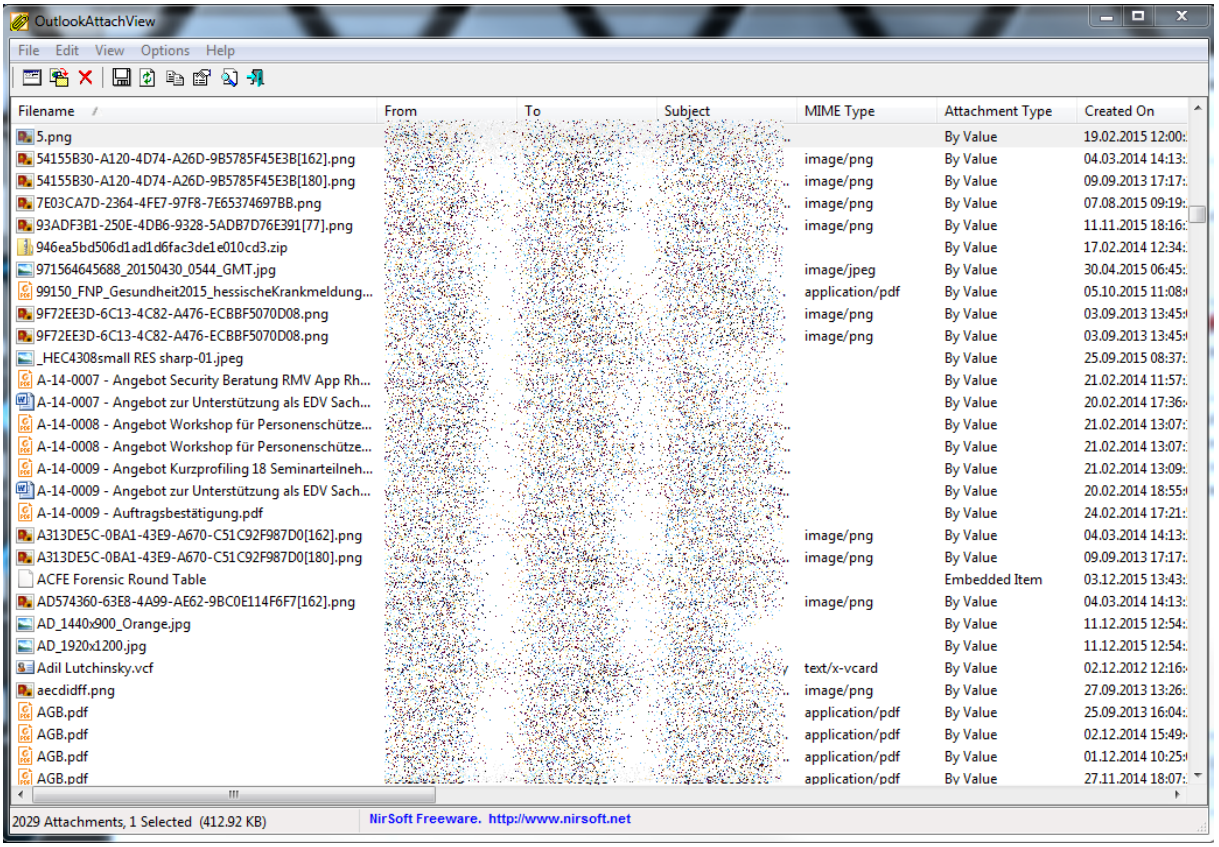


Abbildung 14: Welche Daten wurden als Anhang per E-Mail versendet

Methode: Live-Response

8 CD- oder DVD-Brenner

Um zu überprüfen ob Daten auf eine CD oder DVD gebrannt wurden, kann man sich den folgenden Registry-Key anschauen. Dort sind die Dateien mit Dateinamen ersichtlich, die gebrannt wurden.

Beispiel aus dem NIST Testcase:

```
C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Chrysanthemum.jpg
```

Registry Key:

```
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning
```

Das Verzeichnis für die Daten im Filesystem:

```
C:\Users\Username\AppData\Local\Microsoft\Windows\Burn\Burn
```

Methode: Post-mortem

8.1 Hinweis zu CD´s oder DVD´s:

Wurden Daten auf eine CD oder DVD gebrannt, werden diese häufig anschließend dann gelöscht, da es sich in den meisten Fällen um Kopien handelt. Ein Blick in den „$Recycle.Bin“ Ordner kann unter Umständen die Dateien noch beinhalten, diese wiederum auf den Ordner im Filesystem des Benutzers zeigen:

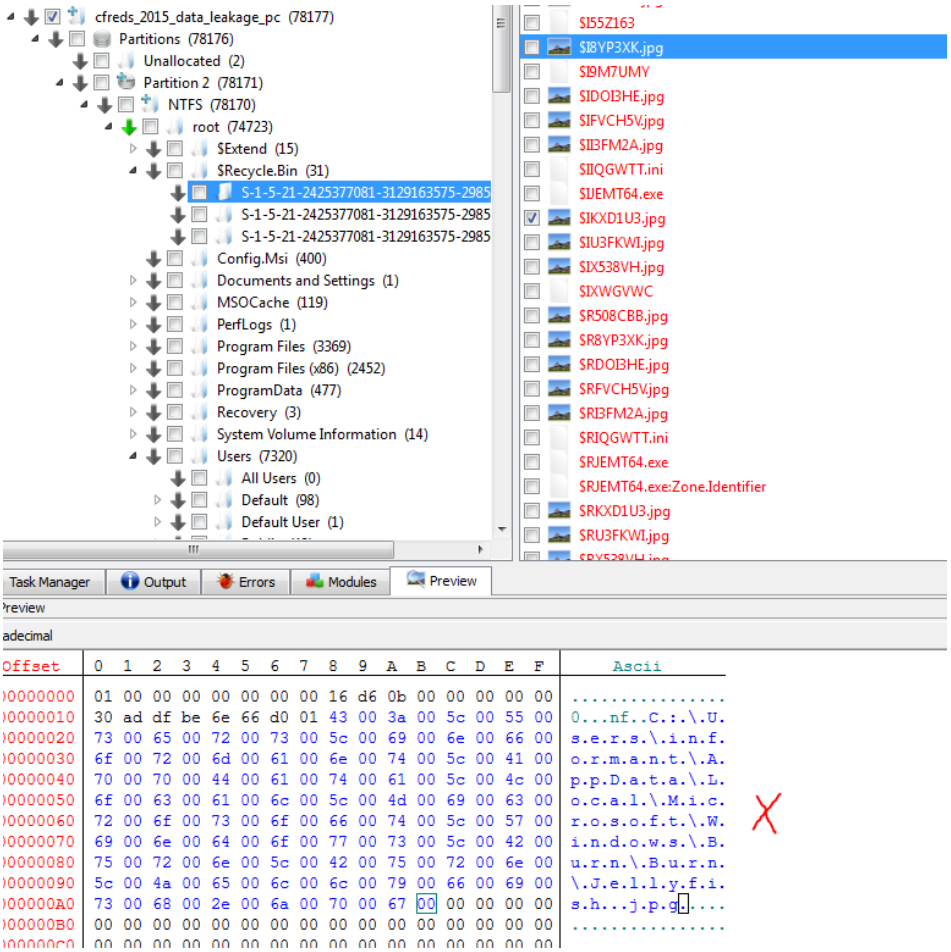


Abbildung 15: Screenshot vom „Digital Forensic Framework“ - gebrannte JPG-Datei die in das Userverzeichnis ~\Burn zeigt

9 Windows Event Logs

Windows Event Logs zeichnen auf, was in einem System von statten geht, wie z.B. Logons, Dienste starten oder beenden usw. Die Windows Logs finden sich zur Auswertung im folgenden Ordner:

\Windows\System32\winevt\Logs\

10 ShellBags

ShellBags zeigen auf, auf welche Verzeichnisse ein Nutzer zugegriffen, gelöscht oder erstellt hat.

Windows 7:

HKEY_USERS\UserID\LocalSettings\Software\Microsoft\Windows\Shell

Beispiel:

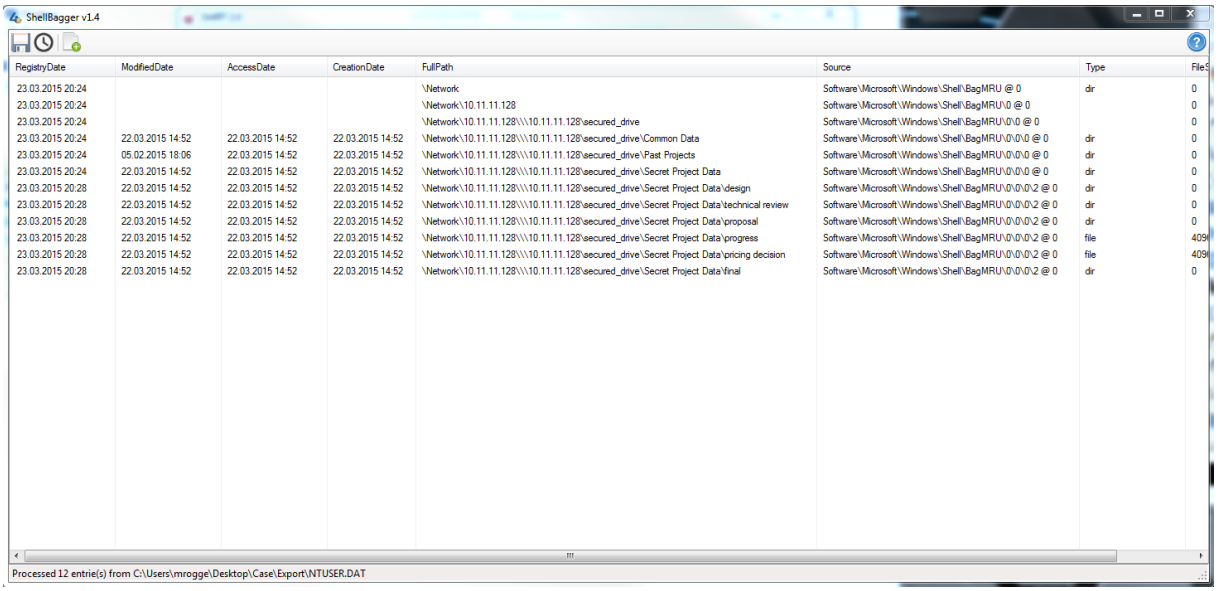


Abbildung 16: ShellBagger aus DART2.

Methode: Post-mortem

Beispiel 2 ShellBagsView:

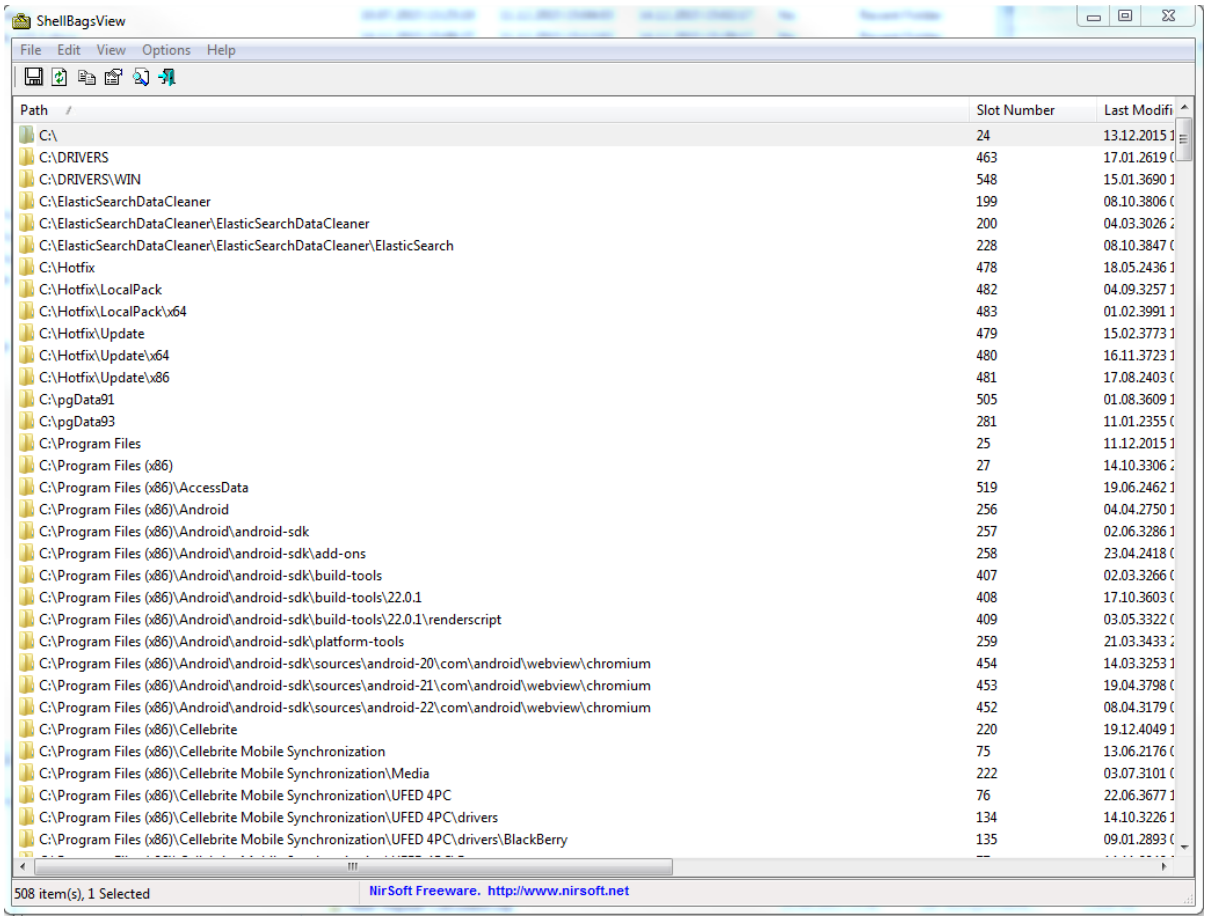


Abbildung 17: ShellBagsView

Methode: Live-Response

Beispiel 3 ShellBag AnalyZer:

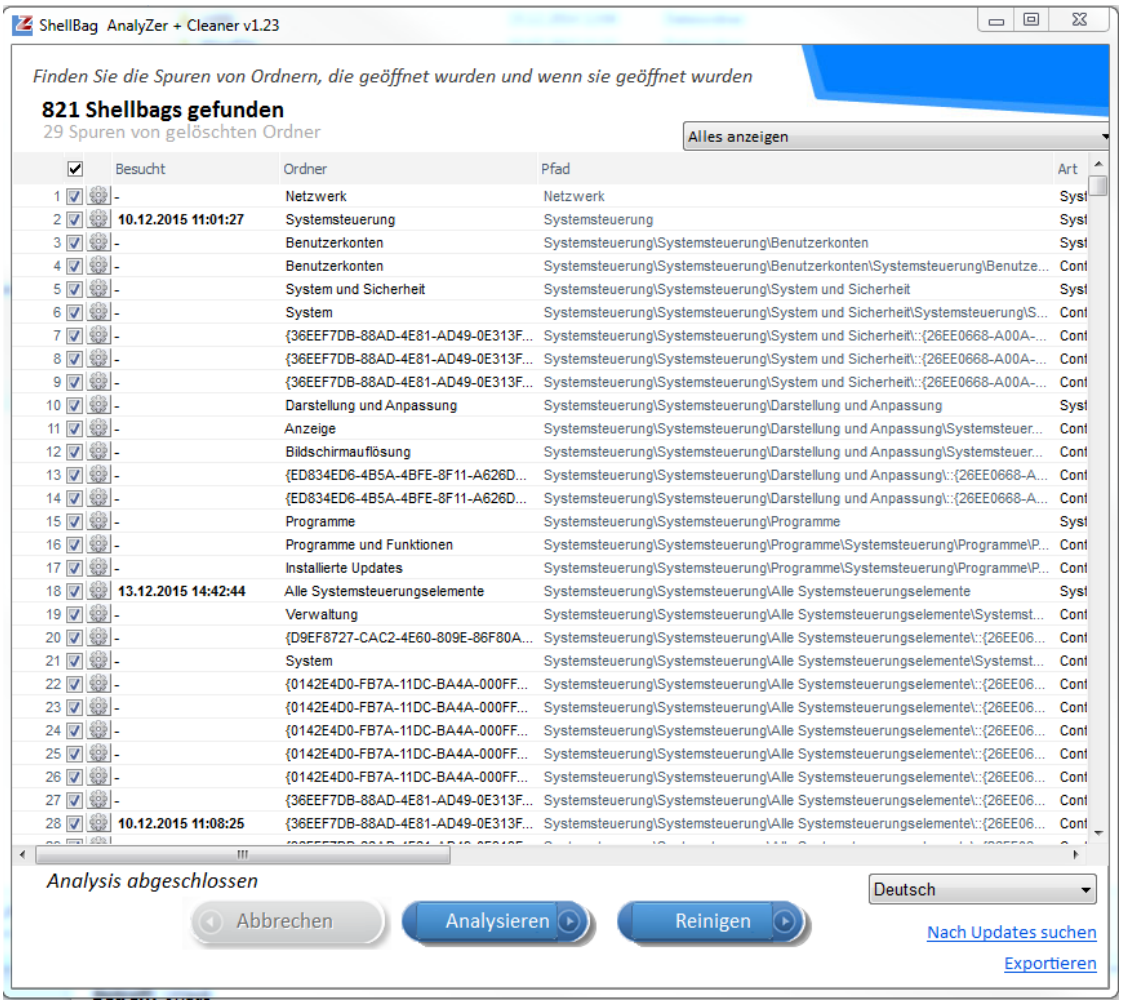


Abbildung 18: ShellBag AnaylZer

Methode: Live-Response

Hierbei sollte darauf geachtet werden, dass bei der Methode Live-Response keine Bereinigung durchgeführt wird, sondern ausschließlich eine Analyse.

11 Eingegebene URL´s und Downloads

Welche URL´s ein Benutzer im Internet Explorer eingegeben hat dient u.a. der Identifizierung von Cloud-Diensten, die über einen Internet-Browser benutzt wurden.

HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main

Downloads Windows 7:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Download

URL Eingabe Windows 7:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

Windows 8:

Zeitstempel an dem die URL´s eingegeben wurden, dargestellt in Filetime	HKEY_LOCAL_MACHINE\Microsoft\Internet Explorer\TypedURLsTime

Internet Cache und Cookies Windows 10:

Cache: \Users\user_name\AppData\Local\Microsoft\Windows\INetCache\ Cookies: \Users\user_name\AppData\Local\Microsoft\Windows\INetCookies\

Für die Untersuchung der Browser bietet DART2 eine umfangreiche Tool Sammlung an, die für den Internet Explorer, Chrome und Firefox angewendet werden kann.

12 Browser Artefakte

Die Browser Artefakte können ebenfalls dazu dienen, Cloud-Dienste über die Daten abgeflossen sind zu identifizieren, oder Web-Mails rekonstruieren zu können. Die Browser Artefakte können bei einem Processierten Case direkt in EnCase betrachtet und ausgewertet werden.

Methode: Post-mortem

12.1 Browser Forensic Tool

Mit dem Browser Forensic Tool kann man sich die History der unterschiedlichen Browser anzeigen lassen, um so einsehen zu können, welche Internet-Seiten der Benutzer angesurft hat. Unterstützt werden folgende Browser:

- Opera
- Apple Safari
- Mozilla Firefox
- Google Chrome
- Internet Explorer
-

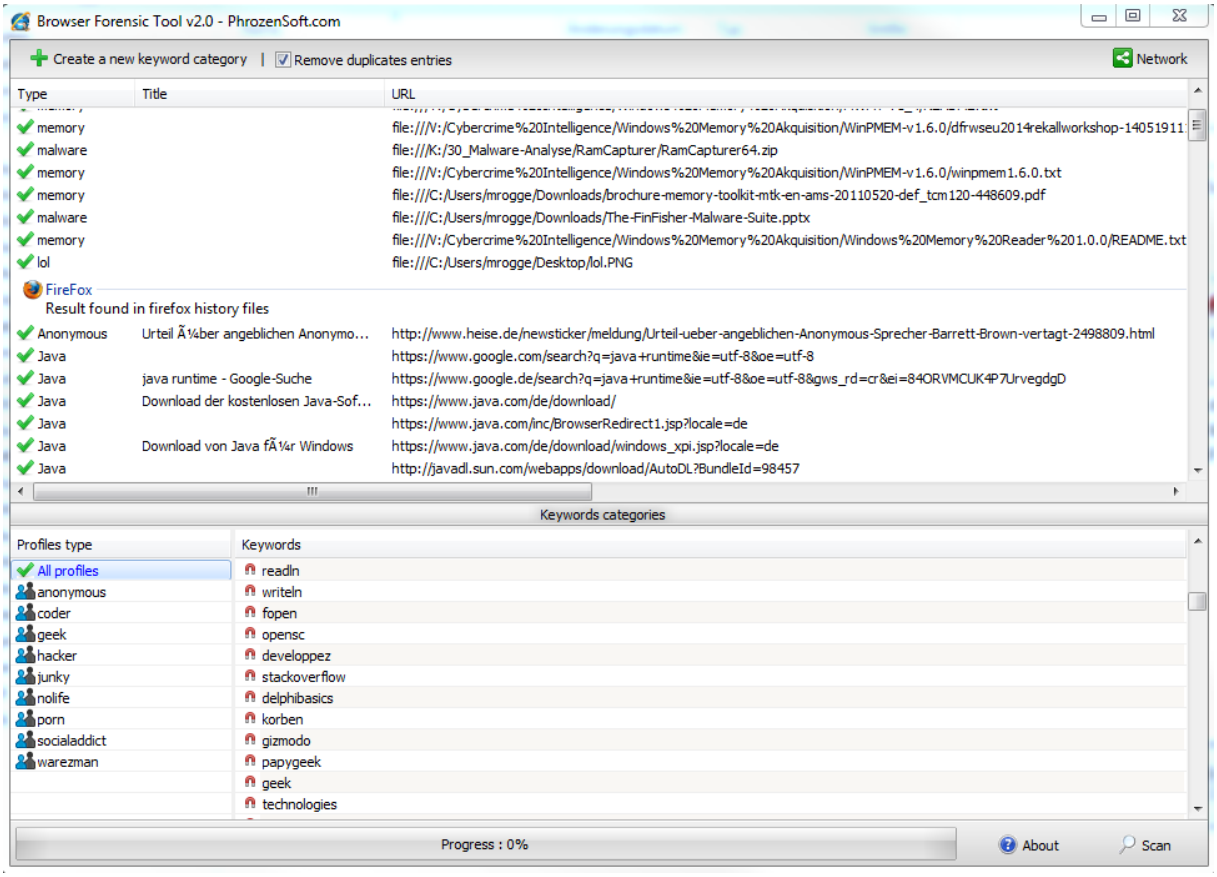


Abbildung 19: Browser Forensic Tool

Methode: Live-Response

12.2 Internet Explorer

- WinXP: %root%/Documents and Settings/%userprofile%/Local Settings/Temporary Internet Files/Content.IE5
- Win Vista/7: %root%/Users/%userprofile%/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5
- Win Vista/7: %root%/Users/%userprofile%/AppData/Local/Microsoft/Windows/Temporary Internet
- Files/Low/Content.IE5
- Win8/IE10: %root%/Users/%userprofile%/AppData/Local/Microsoft/Windows/History
- Win10: \Users\user_name\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

12.3 Mozilla Firefox

- WinXP: %root%/Documents and Settings/%userprofile%/Local Settings/Application Data/Mozilla/Firefox/Profiles/*.default/Cache
- Win7/8: %root%/Users/%userprofile%/AppData/Local/Mozilla/Firefox/Profiles/*.default/Cache
- Linux: /home/%userprofile%/.mozilla/firefox/$PROFILE.default/Cache
- MacOS-X: /Users/%userprofile%/Library/Caches/Firefox/Profiles/$PROFILE.default/Cache/

12.4 Google Chrome

- WinXP: %root%/Documents and Settings/%userprofile%/Local Settings/Application Data/Google/Chrome/User Data/Default/Cache
- Win7/8: %root%/Users/%userprofile%/AppData/Local/Google/Chrome/User Data/Default/Cache
- Linux: /home/%userprofile%/.config/google-chrome/Default/Application Cache/Cache/
- MacOS-X: /Users/%userprofile%/Caches/Google/Chrome/Default/Cache/

13 Letzte Zugriffe

Die letzten Zugriffe eines Benutzers auf Dokumente und Verzeichnisse können Aufschluß darübre geben, was für Dokumente zuletzt angesehen wurden und in welchen Verzeichnissen der Benutzer sich bewegte.

Windows 7:

Gespeicherte Daten	Key Speicherort in der Registry
Kürzlich aufgerufene Dokumente	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
Kürzlich geöffnete / gespeicherte Dokumente nach Filetypes	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU
Kürzlich geöffnete / gespeicherte Ordner	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU
Zuletzt besuchter Ordner	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRULegacy

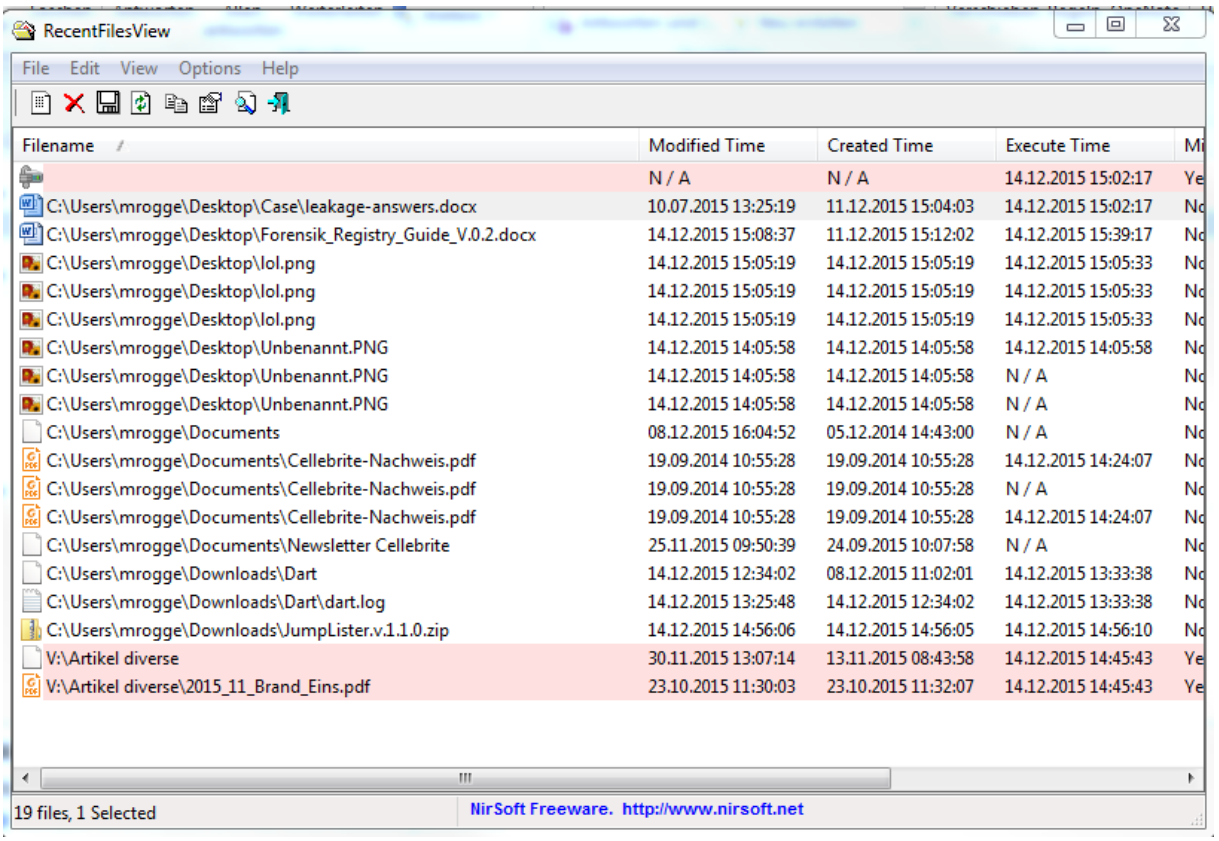


Abbildung 20: RecentFilesView

Methode: Live-Response

14 E-Mail Applikation Windows 10

Kontaktinformationen, E-Mail Header und Anhänge werden getrennt vom E-Mail Body und den Meta Daten gespeichert. Diese findet man in nachstehenden Verzeichnissen:

Body als TXT oder HTML: \Users\user_name\AppData\Local\Comms\Unistore\data\
Metadaten: \Users\user_name\AppData\Local\Comms\UnistoreDB\store.vol

15 Cloud-Dienste

Cloud-Dienste können dazu dienen, Daten aus einem Unternehmen zu kopieren. In diesem Abschnitt wird darauf eingegangen, wo Hinweise auf die Nutzung von Cloud-Diensten zu finden sind. Allgemein gilt bei Cloud-Diensten, dass auch in der History des verwendeten Browsers ebenfalls Hinweise auf die Nutzung zu finden sind.

15.1 Dropbox

Dropbox legt während der Installation aktuell 173 Registry Keys an. Sinnvoller wäre es daher, sich den Usercontent genauer anzuschauen, ob dieser vorhanden oder gelöscht ist:

%appdata%

config.db, filecache.db, sigstore.db, host.db, unlink.db

Hierbei handelt es sich um SQLite Datenbanken, die beispielsweise mit „DB Browser for SQLite“ betrachtet werden können.

Windows 7:

C:\Users\%username%\Dropbox C:\Users\%USERNAME%\AppData\Local\Dropbox\ C:\Users\%USERNAME%\AppData\Roaming\Dropbox\

Mac OS X:

/Users/$USER/.dropbox/

Linux

/home/$USER/.dropbox/

15.2 Google Drive

Google Drive ist ein Dienst der Daten auf entfernten Servern speichern und synchronisieren kann.

Ordner für synchronisierte Daten:

```
C:\Users\<username>\Google Drive
```

In der SQLite Datenbank Snapshot.db befindet sich der Usercontent, mit modified Timestamp, Checksum MD5, Größe und Filename.

Der Anmeldename/Username befindet sich in folgender SQLite Datenbank:

```
C:\Users\<username>\AppData\Local\Google\Drive\user_default\sync_config.db
```

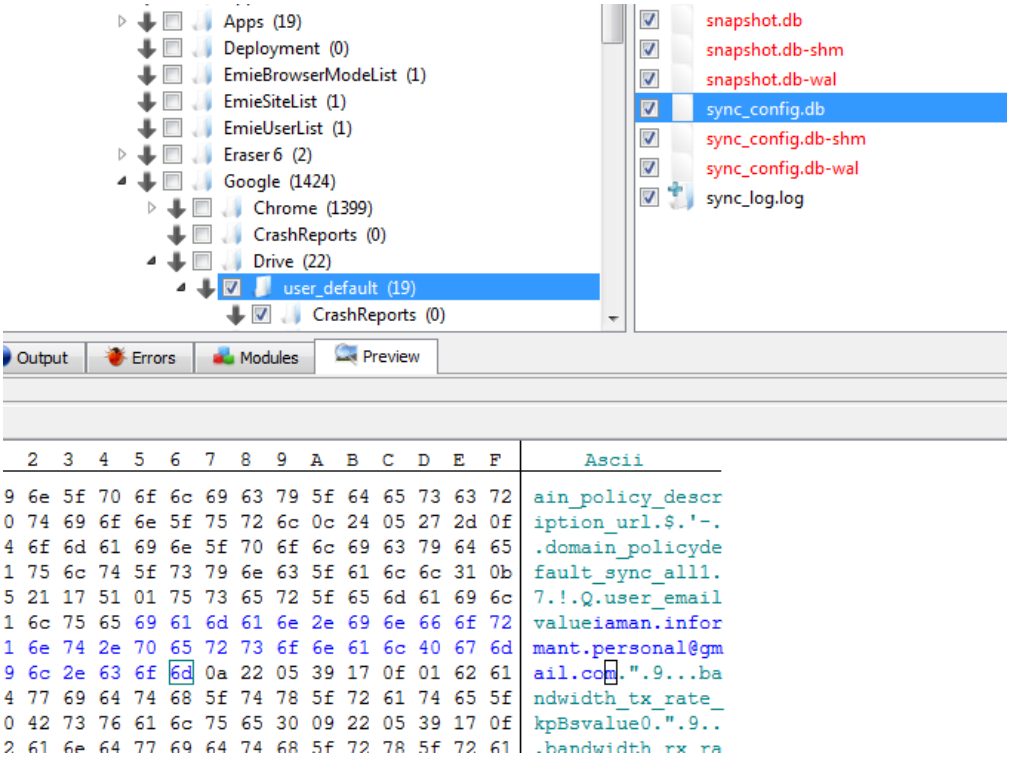


Abbildung 21: Einblick in die sync_config.db

15.3 Microsoft SkyDrive

Für Microsoft SkyDrive werden entsprechend dem jeweiligen User folgende Ordner angelegt.

```
C:\Users\<username>\AppData\Local\Microsoft\SkyDrive
C:\Users\<username>\SkyDrive\
```

Auch der Cloud-Dienst SkyDrive von Microsoft konnte im RAM nachgewiesen werden. Ebenfalls werden dort Login-E-Mail sowie das Password im Klartext gefunden.

16 Zuletzt geöffnete Programme

Die zuletzt geöffneten Programme geben darüber Aufschluss, ob Cloud-Dienste benutzt wurden oder auch, ob Programme zum unwiderruflichen Löschen von Daten benutzt wurden:

Windows 7:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

Beispiel:

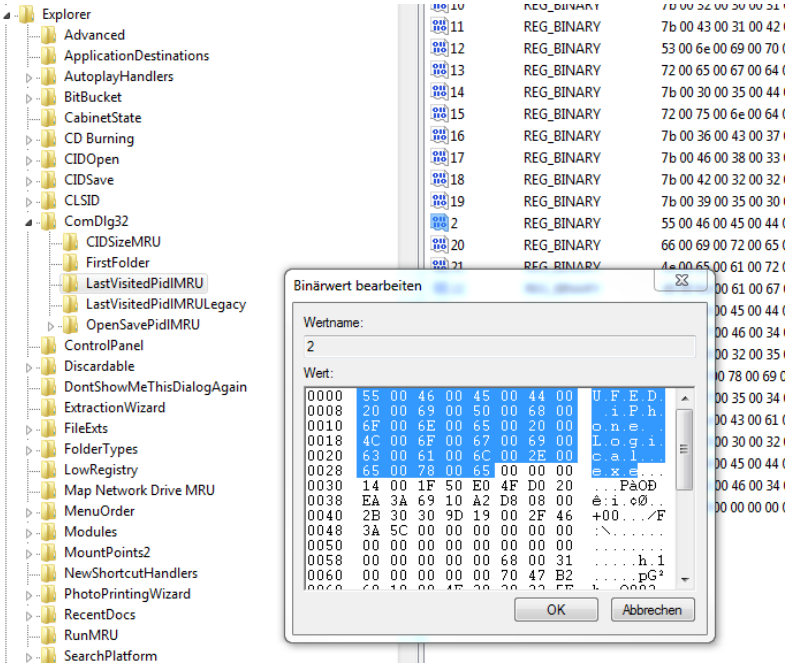


Abbildung 22: zuletzt geöffnete Programme

Gelöschte/Deinstallierte Programme, Windows 7:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

Methode: Post-mortem

17 Mobile Devices

Bei mobilen Devices befinden sich Dokumente oder andere Daten die kopiert und/oder versendet wurden in entsprechenden Ordner, die nach dem dekodieren in Datendateien aufzufinden sind (Physical Analyzer der Firma Cellebrite). Der Umstand, dass auf den meisten modernen mobilen Devices SQLite Datenbanken benutzt werden, um Daten zu speichern, begünstigt, dass Daten weniger zeitnah überschrieben werden. Bei einer genauen Betrachtung ist dann sehr häufig auch der Pfad angegeben der anzeigt, woher eine Dokument stammt:

☑	1				ctrl_boxChecked_norm.pdf	/SUNorthstarTwo7E18.N88OS/System/Library/PrivateFrameworks/iWorkImport.framework/ctrl_boxChecked_norm.pdf
☑	2				ctrl_boxUnchecked_norm.pdf	/SUNorthstarTwo7E18.N88OS/System/Library/PrivateFrameworks/iWorkImport.framework/ctrl_boxUnchecked_norm.pdf
☑	3				Getting Started.pdf	/Data/mobile/Applications/9D45BB3E-5980-4FE8-88C6-0D1C592A4F37/Documents/Getting Started.pdf
☑	4				hour.pdf	/SUNorthstarTwo7E18.N88OS/Applications/MobileTimer.app/hour.pdf
☑	5				Ignition_iPad_GS.pdf	/Data/mobile/Applications/9D45BB3E-5980-4FE8-88C6-0D1C592A4F37/LogMeIn.app/Ignition_iPad_GS.pdf
☑	6				Ignition_iPhone_GS.pdf	/Data/mobile/Applications/9D45BB3E-5980-4FE8-88C6-0D1C592A4F37/LogMeIn.app/Ignition_iPhone_GS.pdf
☑	7				mins.pdf	/SUNorthstarTwo7E18.N88OS/Applications/MobileTimer.app/mins.pdf
☑	8				pmhour.pdf	/SUNorthstarTwo7E18.N88OS/Applications/MobileTimer.app/pmhour.pdf
☑	9				pmmins.pdf	/SUNorthstarTwo7E18.N88OS/Applications/MobileTimer.app/pmmins.pdf
☑	10				secs.pdf	/SUNorthstarTwo7E18.N88OS/Applications/MobileTimer.app/secs.pdf

Abbildung 23: Dokumente in einem Smartphone

Im oben angezeigten Beispiel wurde ein PDF über eine APP geladen, die einen Fernzugriff auf einen Desktopcomputer durchführen kann und von und nach dort Daten laden, kopieren oder löschen kann. Sofern man eine Ermittlung durchführt kann nun geprüft werden, ob und mit welchem Computer das mobile Device synchronisiert war und ob sich diese Daten dort befinden und/oder gelöscht wurden. E-Mails, SMS, MMS und Messenger sollten ebenfalls durchsucht werden, ob darüber Dokumente verteilt wurden. Da mobile Devices in der Forensik keine Standard-Vorgehensweise bieten, was der Schwierigkeit des Dekodierens geschuldet ist, muss jedes mobile Device gesondert betrachtet und ausgewertet werden. Sind Daten unzureichend dekodiert empfiehlt es sich, eine manuelle Suche im Dump nach Dateitypen durchzuführen.

Beispiel: Gesucht werden Dokumente des Dateityps PDF, da keine dekodiert werden konnten. Also öffnet man unter „Speicherabbild“ den Dump des mobilen Devices und sucht darin entsprechende Hexadezimal-Werte unter Bytes mittels der Header Informationen „25504446“:

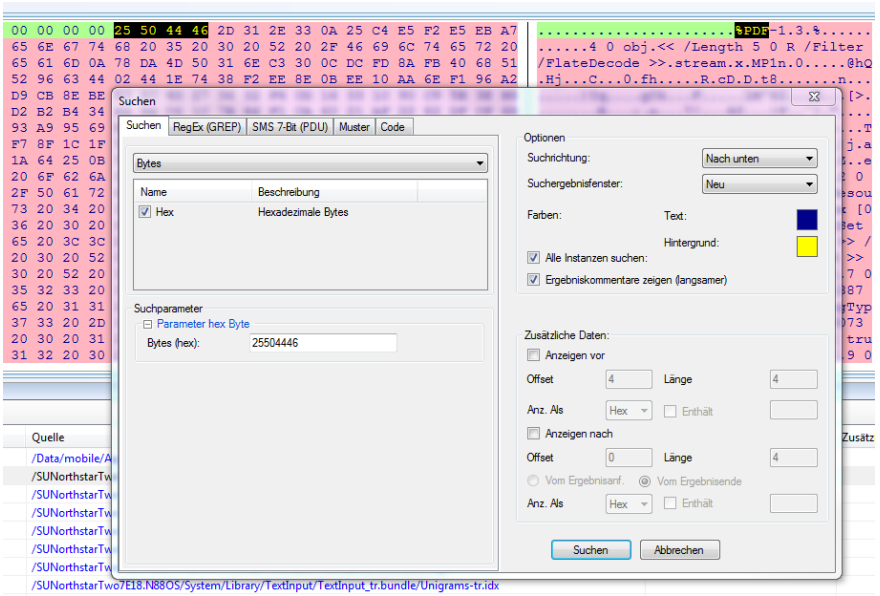


Abbildung 24: Dateitypen im HexEditor

18 Ergänzungen

18.1 Hinweise im RAM

Im RAM ließ sich mehrfach nachweisen, welche letzte intakte „Dropbox“, „Microsoft SkyDrive“ und „Google Drive“ Sitzung geöffnet war. Daraus lassen sich folgende Informationen extrahieren:

Beispiel Strings:

- String: login_email
- String: login_password
- Zusammengefügt: login_email=emailadresse@mail.me&login_password=geheimespasswort

18.2 Live-Response: Undelete360

Zusätzlich kann man nach gelöschten und bereits überschriebenen Daten schauen. Dazu eignet sich Undelete360:

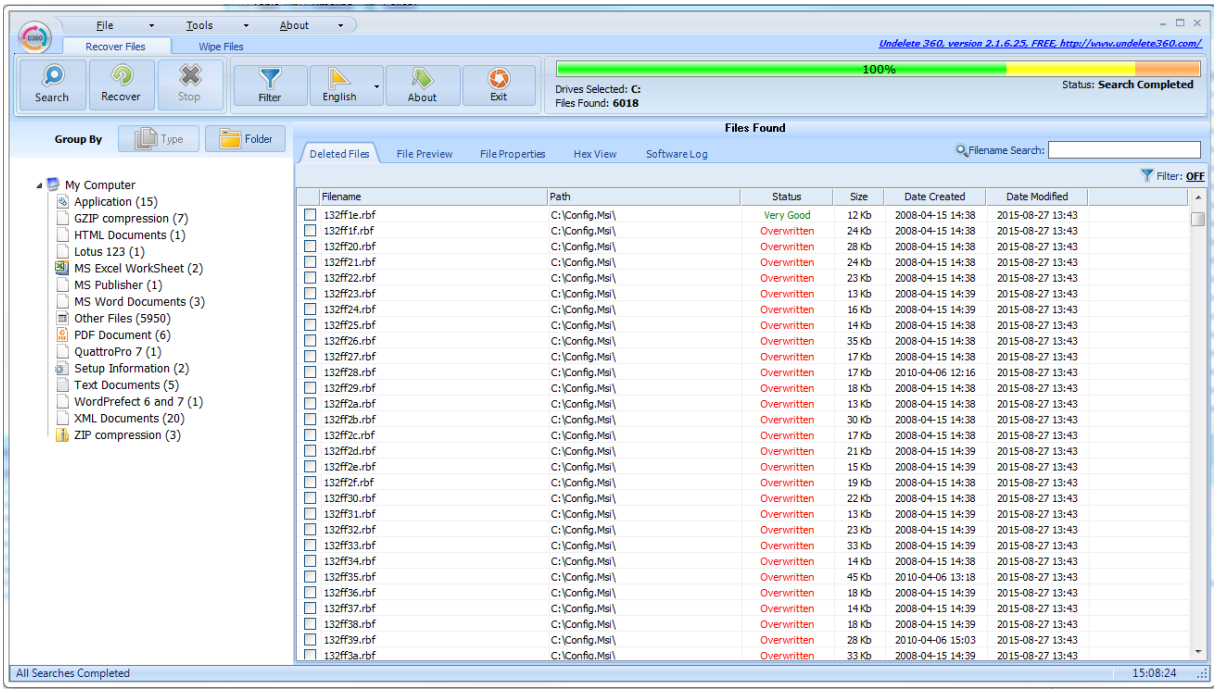


Abbildung 25: Undelete360

18.3 Filesignaturen

Übersicht über Filesignaturen für die manuelle Suche nach Dokumenten oder Artefakten. Damit lassen sich leicht eigene Dateitypen erstellen.

http://www.garykessler.net/library/file_sigs.html

19 Ermittlungsansatz Timeline

Unter Umständen kann es durchaus sein, dass ein direkter Beweis für eine Handlung nicht erbracht werden kann. Hier ist zu prüfen, ob Anti-Forensik angewendet wurde. Beispiel kann sein, dass eine Eraser Software zuletzt installiert wurde, anschließend wurde diese mit einem Zeitversatz später wieder deinstalliert.

Bei einem Anfangsverdacht auf eine nicht legitime Handlung, kann man unter zu Hilfenahme einiger technischer Indizien eine Timeline erstellen. Ich empfehle dabei, so genau wie möglich vorzugehen, um Fehler zu vermeiden. Wichtig hierbei ist, so viele Indizien wie möglich mit aufnehmen, um eine große Indizien-Kette erstellen zu können.

Beispiel zur Vorgehensweise: Soll dargestellt werden, dass eine unerlaubte Handlung durchgeführt wurde, sollten aus den Auswertungen der vollständigen Ereignisse die Timestamps aufgenommen werden.

Wird der Enumeratordienst für tragbare Geräte (WPDBusEnum) gestartet ist dies ein Indiz dafür, dass ein Wechselspeichermedien via USB eingesteckt wurde. Dies wird in der Ereignisanzeige System unter der ID 7036 (Quelle ist Service Control Manager) protokolliert. Beim Start dies Dienstes wird der Status "Ausgeführt" protokolliert. Wird der Dienst beendet, wird der Status "Beendet" protokolliert. Um diese Zeit herum kann dann nachgesehen werden, ob Dateien geöffnet, erstellt oder gespeichert wurden. Zudem muss nachgesehen werden, ob Ordner erstellt, gelöscht oder angelegt wurden, bzw. ob ein Zugriff darauf stattfand. Zudem, ob in dem Zeitraum Cloud-Dienste bedient wurden oder E-Mails versendet. Um dieses Event mit der ID 7036 herum sollten die aus den zusammen getragenen Ereignissen deren Timestamps eine Timeline ergeben. Von Interesse dürfte hierbei auch die Timestamps zwischen beiden Status-Meldungen dies Dienstes sein.

20 Besonderheiten beim Schreiben von Daten auf USB Devices

20.1 Einleitung

Da ich für diese Aufgabe unterschiedliche Tools zu Hilfe genommen habe konnte ich feststellen, dass die Ergebnisse durchaus unterschiedlich sind. Somit müssen zwingend die Ergebnisse die von den Tools ausgeworfen werden gründlich hinterfragt werden. Beispiel: ShellBagsView von NirSoft, der also Last Modified schon mal ein Datum aus der Zukunft darstellt:

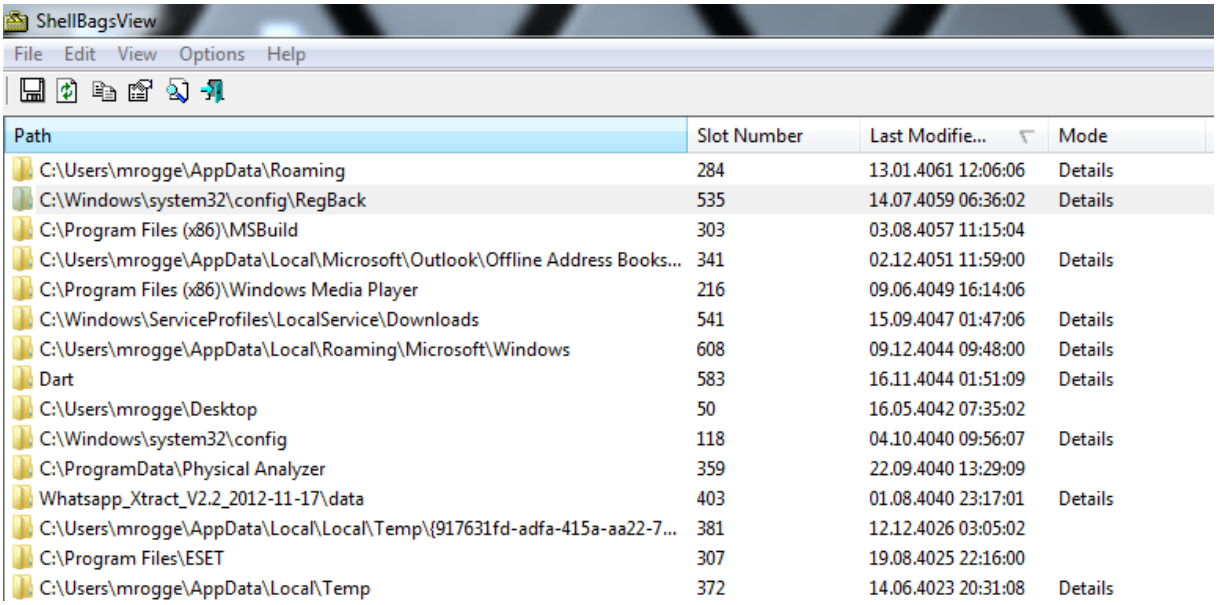


Abbildung 26: ShellBags Untersuchung

20.2 Beispielszenario

Folgendes Szenario habe ich dazu nachgestellt, um zu versuchen, den Beweis erbringen zu können:

Ich habe einen USB-Stick genommen, auf dem ich einen Unterordner „Geheim“ erstellt habe. Darin habe ich eine Datei „Softwaretest_Forensik“ via Copy & Paste hineinkopiert und eine weitere Datei „Forensik_Registry_Guide“ dorthin mittels „Speichern unter“ abgelegt habe.

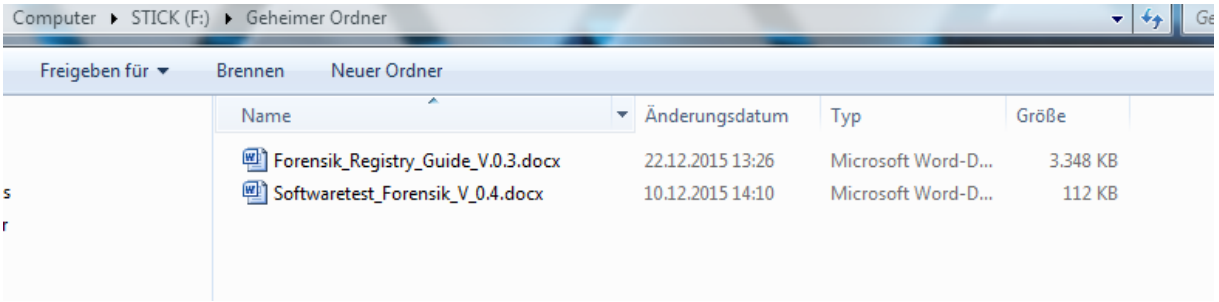


Abbildung 27: Inhalt des Test-USB-Devices

Im Anschluss habe ich nun alle verfügbaren Möglichkeiten ausgeschöpft, um den Nachweis dieser beiden Dateien auf dem USB-Stick erbringen zu können.

20.3 Ergebnisse

Ein erster Hinweis auf den Ordner ist in der Registry zu finden:

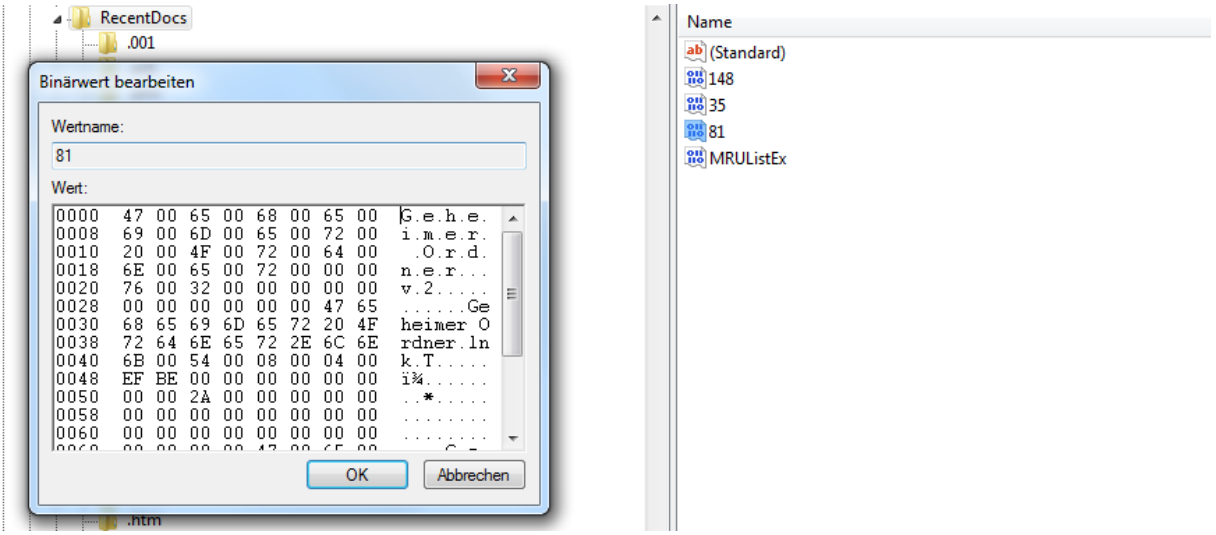


Abbildung 28: Hinweise auf den angelegten Ordner auf dem USB-Device

Daraus lässt sich durchaus schließen, dass ein Ordner namens „Geheimer Ordner“ aus dem Wert „81“ als sym-link (lnk) oder auch Verknüpfung aufgerufen wurde und die Datei aus dem Wert „35“ dort abgespeichert wurde:

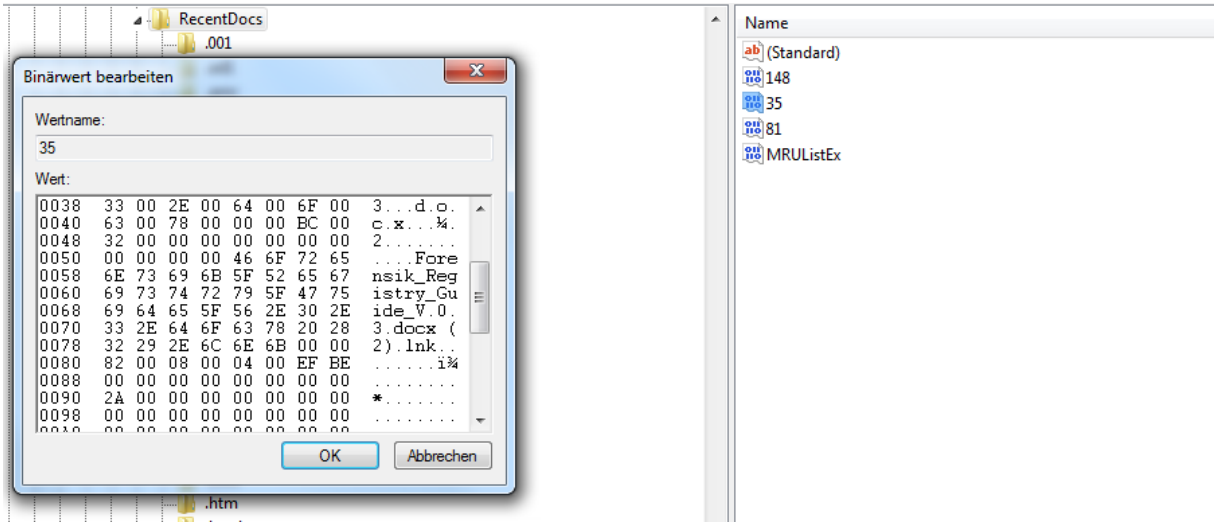


Abbildung 29: Weiterer Hinweis in der Registry

Dies belegt alleinig den Umstand, dass eine Datei auf einem Device abgespeichert wurde. Diese Datei wurde auf dem lokalen Computer erstellt und anschließend dahin gespeichert, aber nicht kopiert. Der Ordner „Geheimer Ordner“ ist allerdings nicht eindeutig als ein USB-Devices zu identifizieren.

Das passende Device dazu identifizieren in der Registry des Benutzers ist daher schwierig, weil dort eine komplette Liste ohne Timestamps hinterlegt ist.

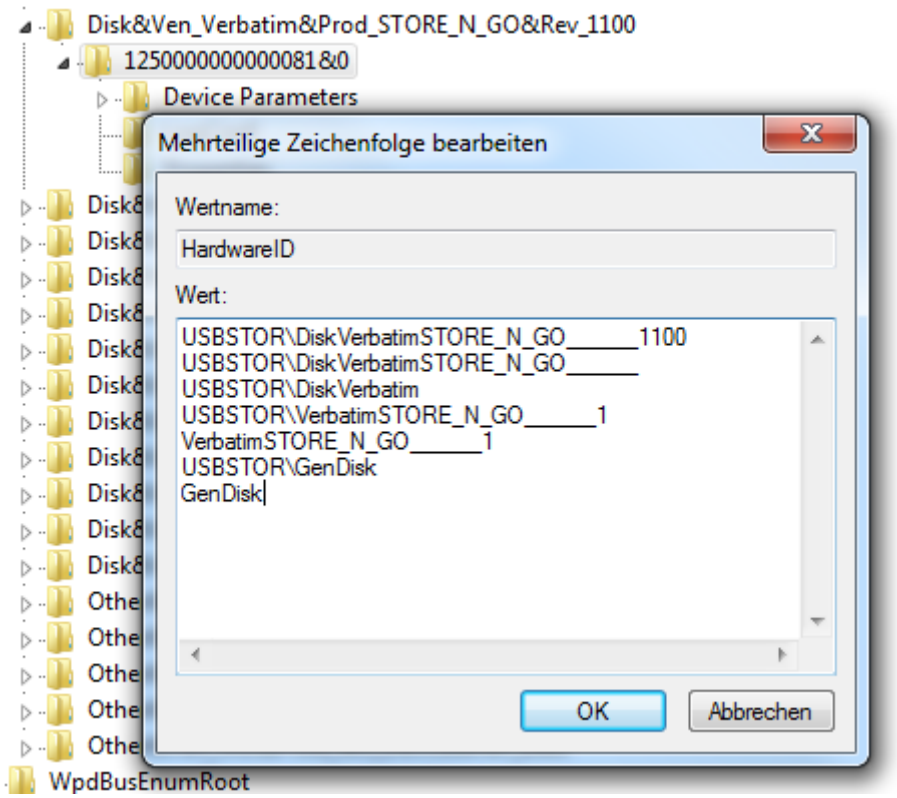


Abbildung 30: Einblick in USBSTOR

Hilfreich wäre hier sich die Shellbags genauer anzuschauen. In den ShellBags des betroffenen Systems können nun folgende Feststellungen getroffen werden:

- Es wurde 2x das gleiche Device eingebunden, welches dann unter E: und F: zu finden waren. Darauf auch sichtbar der Ordner „Geheimer Ordner“.

1	22.12.2015 13:48:16	-	F:\	-	Folders on Network / External Device
2	22.12.2015 13:48:16	Geheimer Ordner	F:\Geheimer Ordner	22.12.2015 13:26:38	Folders on Network / External Device
3	22.12.2015 13:26:46	Geheimer Ordner	E:\Geheimer Ordner	22.12.2015 13:26:38	Folders on Network / External Device
4	22.12.2015 13:26:46	-	E:\	-	Folders on Network / External Device

Abbildung 31: ShellBag Untersuchung externer Devices mit neuem Ordner

ShellBag AnalyZer stellt nun dar, dass das Laufwerke F: zu einer Zeit eingebunden waren, in der auch der Dienst für externe Devices im Betriebssystem gestartet wurde:

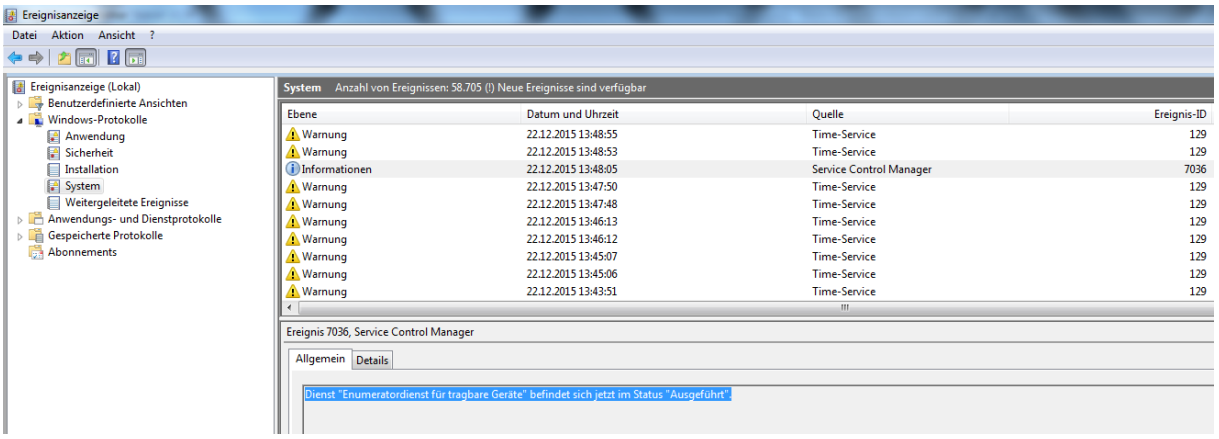


Abbildung 32: Dienst für tragbare Geräte gestartet

Es ist naheliegend und annehmbar, dass es sich bei F: um ein USB-Device handelt.

Zu diesem Zeitpunkt taucht die Datei „Softwaretest_Forensik“, die via Copy & Paste direkt dorthin kopiert wurde, **nicht** auf!

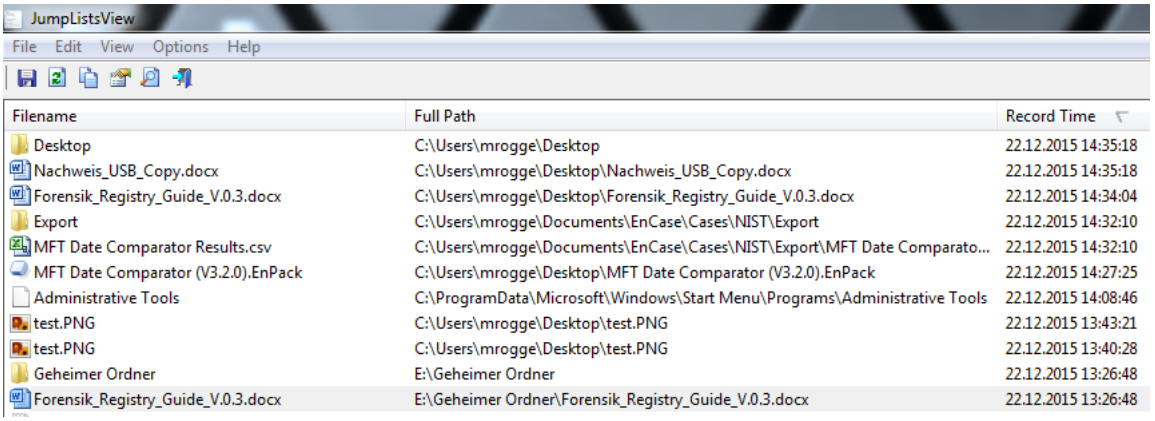


Abbildung 33: JumpListsView liefert keine weiteren Fakten

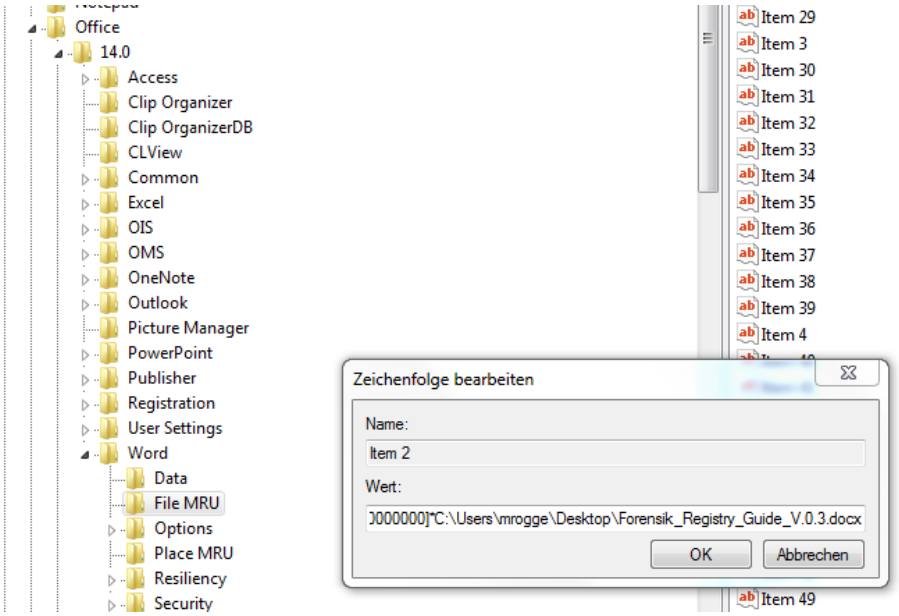
Weitere Registry Keys die helfen können:

HKEY_CURRENT_USER\Software\Microsoft\Office\1x.0\Word\File MRU\

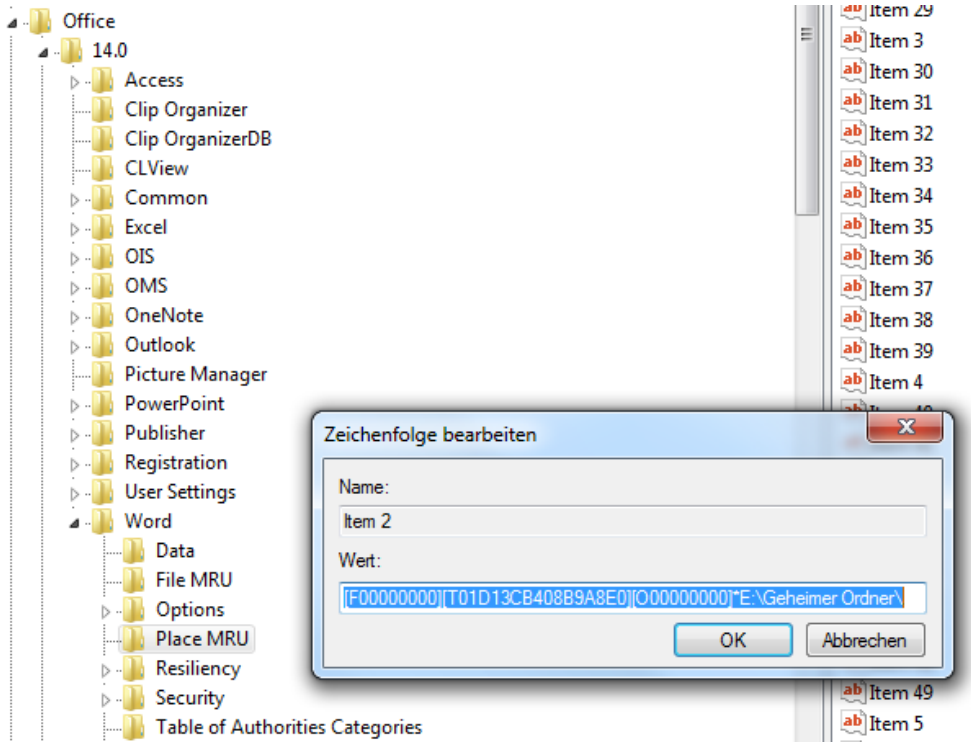
HKEY_CURRENT_USER\Software\Microsoft\Office\1x.0\Excel\File MRU\

HKEY_CURRENT_USER\Software\Microsoft\Office\1x.0\PowerPoint\File MRU\

Item 2:



Entsprechend dem Item kann man dann schauen, wohin das File geschrieben wurde:



Dies verdeutlicht lediglich, dass es direkt auf dem als E: eingehängten USB-Device gespeichert wurde aus Word heraus.

Das Anlegen von Ordnern auf einem USB-Device kann mittels ShellBag Analyse herausgefunden werden, ebenso, wenn Files nach dem kopieren auf einem USB Device dort erneut geöffnet wurden.

Fazit: Es ist nachweisbar, dass Daten auf einem externen USB-Device geschrieben wurden durch direktes speichern auf dem Device. Dies muss mittels „speichern unter“ oder direktes anlagen eines Dokumentes auf dem USB-Device erfolgen. Ebenso kann der Nachweis erbracht werden, wenn neue Ordner auf einem USB-Device angelegt wurden.

Zeitnahe Abläufe können durchaus hinzugezogen werden, wie z.B. weitere Indizien aus geöffneten Dokumenten und zeitliche Abfolge von geöffneten Dokumenten in Verbindung mit dem mounten von USB-Devices.