HOCHSCHULE MITTWEIDA
University of Applied Sciences

Betriebssysteme

Windows systeminterne Spuren

Autor: Ronny Bodach, Tim Wetterau

Stand: 21.05.2024

Bundeskriminalamt

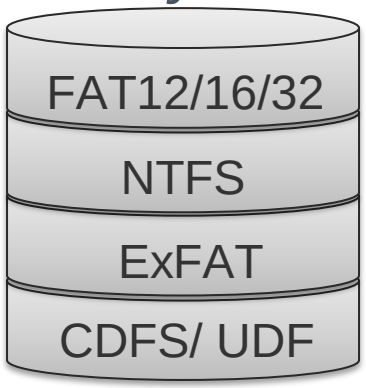
Agenda

1. Überblick
2. Registrierungsdatenbank
3. Betriebssystemartefakte
4. Benutzerkontenzugriffssteuerung
5. Remote Desktop Nutzung

Überblick

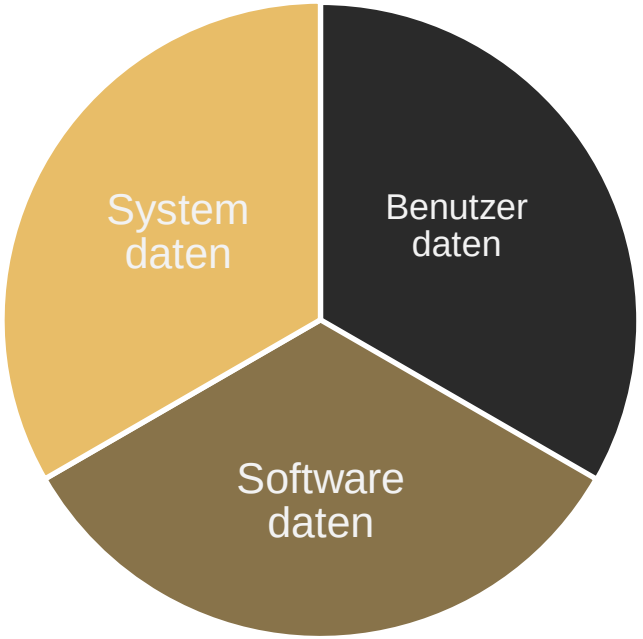
Allgemeine Informationen Windows

Unterstützte Dateisysteme:



Unterstützte Architekturen:

Die interne Datenaufteilung erfolgt in drei unterschiedlichen Kategorien:



Die logische Trennung dieser Daten findet sich dabei an verschiedenen Stellen im Betriebssystemaufbau wieder.

Wichtige Verzeichnispfade

- Systemdaten findet man im Windows Verzeichnis, je nach Betriebssystemversion als „WINDOWS“, „WIN“ oder „WINNT“ benannt.
- Softwaredateien befinden sich im Programm Verzeichnis je nach Betriebssystemversion als „Programme“ oder „Program Files“ benannt.
- Benutzerdaten befinden sich im Benutzerdaten-Verzeichnis. Für die Windows Versionen Windows 95,98 und ME im Verzeichnis „Eigene Dateien“.
- Unter Windows NT, 2000 und XP im Verzeichnis „Dokumente und Einstellungen“ und unter Windows Vista, Windows 7, 8, 10 und 11 im Verzeichnis „Users“ in einem Benutzerverzeichnis benannt nach dem Benutzerkontonamen.

Wichtige Verzeichnispfade

- Einstellungen und Anwenderspezifische Daten zu einzelnen installierten Software-anwendungen werden in Unterverzeichnissen gespeichert.
- Unter Windows NT, 2000 und XP in:
  - „\Anwendungsdaten“ und „\Lokale Einstellungen\Anwendungsdaten“
- Unter Windows Vista, 2003, 2008, 2012, 2013, 7, 8, 10 und 11 in:
  - „\AppData\Local“, „\AppData\LocalLow“ und „\AppData\Roaming

Wichtige Verzeichnispfade

Windows (64 Bit) Besonderheiten

- Seit der Einführung von 64Bit Windows wird 32Bit und 64Bit-Software in unterschiedlichen Verzeichnissen installiert
- alle 32Bit-Programme auf 64Bit-Betriebssystemen in ein Programmverzeichnis mit dem Präfix „(x86)“ installiert
- auch auf Systemebene eine solche Trennung vorhanden
- im Windows Verzeichnis auf 64Bit-Betriebssystemen zusätzliches Verzeichnis:

„SysWOW64“

in dem sich die 32 Bit Systemkomponenten des Betriebssystems befinden

Bei der forensischen Untersuchung sind je nach Sachverhalt daher auch diese Verzeichnisse von Bedeutung.

Windows Benutzerverwaltung SID

- Benutzerverwaltung wird durch den Security Identifier (SID) realisiert
- Eindeutige Identifikation von System, Benutzer und Gruppen
- Access Control Lists an die SID gebunden
  - festgelegten Zugriffsrechte und Eigentümer von Dateien
  - NTFS-Dateisystemen für die Benutzerzugriffsverwaltung
- Werden Benutzernamen geändert oder gelöscht bleiben deren SID unverändert derjenigen Datei oder demjenigen Verzeichnis zugeordnet.

S-1-5-21-347610211-2160907307-1134779817-1001

Revisionsnummer Domäne oder lokales System Benutzernummer

Kurzzeichen für SID Identifier Authority

Spurenarten und Fundstellen

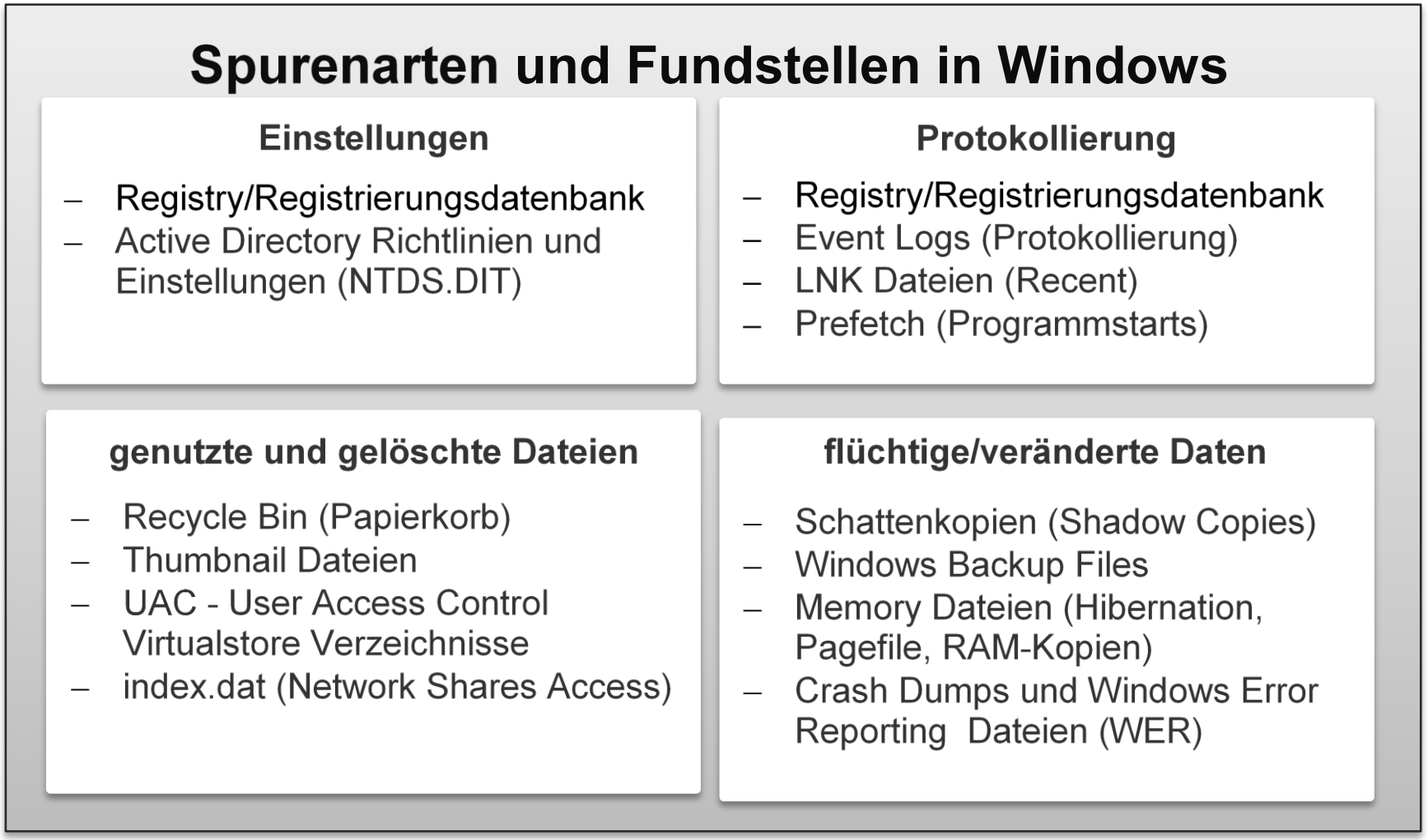


Abbildung Spurenarten und Fundstellen in Windows Quelle: Autor

Registrierungsdatenbank

Registrierungsdatenbank

Speicherung von Einstellungen in der Registrierungsdatenbank:

- Die gespeicherten Daten werden in sogenannte Registrierungshives aufgeteilt und in Schlüsseln (Keys) mit Name Wert Paaren (Values) abgelegt.
- Hive (Bienenstock) = Teilbaum der Registry
- Datenablage in Binärformat
- Bei Windows NT4, Windows 2000 und spätere haben die Dateien das **Windows NT Registry File (REGF) Format**. Für Windows 95, 98 und ME sind die Dateien im **Windows 9x Registry File (CREG)** Format organisiert.
- Ein Hive ist dabei nicht zwangsweise mit einem Haupt- oder Wurzelschlüssel identisch. So gibt es Wurzelschlüssel, die aus mehreren einzelnen Hives bestehen.

Registrierungsdatenbank

Speicherung von Einstellungen in der Registrierungsdatenbank:

- Die Trennung der drei Datenformen ist auch auf Ebene der Registrierung vorhanden.
- Die Datenbanken existieren in Form von Dateien im Verzeichnis:
  „[Root-Laufwerk]/[Windows Verzeichnis]/System32/Config“
- Die Registrierungsdatei für die Benutzereinstellungen befindet sich im jeweiligen Benutzerdaten Verzeichnis unter:
  „[Root-Laufwerk]/[Benutzerdaten Verzeichnis]/[Benutzername]/“
- Die Registrierungsdatei für die Benutzerkontenverwaltung wurde mit Windows NT eingeführt. In ihr werden die Einstellungen zu vorhandenen Benutzern des Betriebssystems gespeichert.
- Seit Windows 7 werden einige der Benutzerinformationen auch in einem weiteren Benutzerspezifischen Schlüssel gespeichert:
  „\AppData\Local\Microsoft\Windows\usrclass.dat“.

Registrierungsdatenbank

Speicherung von Einstellungen in der Registrierungsdatenbank:

Typ	Windows 95,98 und ME	Windows NT, XP und höher	korrespondierende Hives
Systemeinstellungen	SYSTEM.DAT	SYSTEM	HKEY_LOCAL_MACHINE/SYSTEM
Softwareeinstellungen	SOFTWARE.DAT	SOFTWARE	HKEY_LOCAL_MACHINE/SOFTWARE
Benutzereinstellungen	USER.DAT	NTUSER.DAT	HKEY_CURRENT_USER/HKEY_USERS
Benutzerkontenverwaltung	-	SAM	HKEY_LOCAL_MACHINE/SAM
Benutzerrechte und Richtlinien	-	SECURITY	HKEY_LOCAL_MACHINE/SECURITY

Registrierungsdatenbank

Speicherung von Einstellungen in der Registrierungsdatenbank:

Von einigen Schlüssel gibt es auch verlinkte/gespiegelte Hauptschlüssel:

HKEY_CLASSES_ROOT: enthält Informationen über unterstützte Dateitypen des Rechners und die dazugehörigen Dateiendungen. Der Wurzelschlüssel ist bei den neueren Windows-Versionen seit Windows 2000 nicht real, sondern eine Kombination aus: HKEY_LOCAL_MACHINE\Software\Classes und HKEY_CURRENT_USER\Software\ Classes

HKEY_CURRENT_CONFIG: ist eine Spiegelung auf HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Hardware Profiles\ Current.

HKEY_CURRENT_USER: ist eine Spiegelung von: HKEY_USERS\<Benutzer-SID> wobei <Benutzer-SID> die SID des aktuell am System angemeldeten Benutzer ist.

Registrierungsdatenbank

Speicherung von Einstellungen in der Registrierungsdatenbank:

Weiterhin gibt es folgende Hives für Systemdienste:

– **%systemroot%\System32\config\.DEFAULT:**
HKU\.DEFAULT und HKU\HKU\S-1-5-18 für User Local System

–**%systemroot%\ServiceProfiles\LocalService\Ntuser.dat:**
HKU\HKU\S-1-5-19 für User Local Service

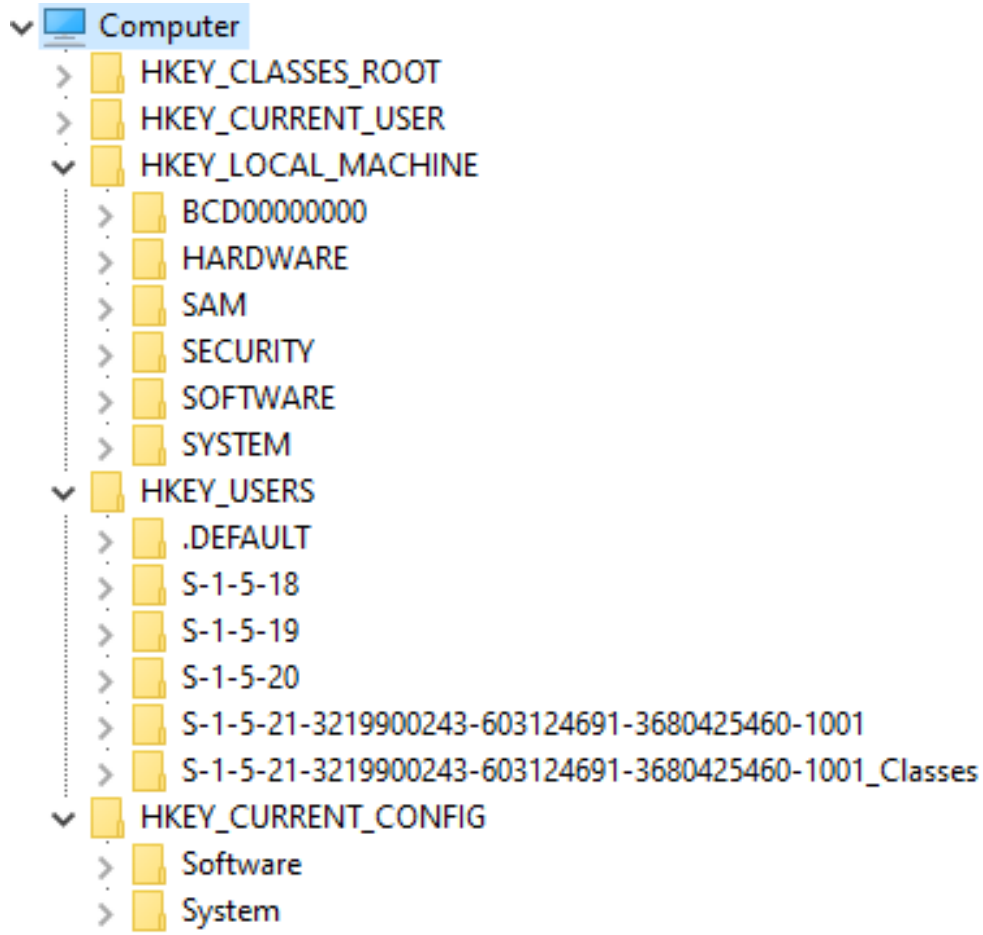
–**%systemroot%\ServiceProfiles\NetworkService\Ntuser.dat:**
HKU\HKU\S-1-5-20 für User Network Service

Sonstige Hives wären dann noch:

–**\Device\HarddiskVolume1\Boot\BCD:**
HKLM\BCD00000000 Konfiguration für den Bootloader

Registrierungsdatenbank

Speicherung von Einstellungen in der Registrierungsdatenbank:



Registrierungsdatenbank

Speicherung von Einstellungen in der Registrierungsdatenbank:

Es existieren oft Kopien von Hives, welche sich an anderer Stelle befinden

Beispiele dieser sog. Supporting Files sind:

- **system.alt** Kopie des system Hives
- **.log** Logs zu den einzelnen Hives
- **.sav** Kopien der Hives während des Bootvorgangs

Referenz: https://learn.microsoft.com/de-de/troubleshoot/windows-server/performance/windows-registry-advanced-users

Registrierungsdatenbank

Speicherung von Einstellungen in der Registrierungsdatenbank:

- Jeder Wert kann eine theoretische Größe von 1024 kB haben.
- Folgende Datentypen sind bei aktuellen Versionen möglich:

Datentyp	Beschreibung
REG_BINARY	Roher Binärcode
REG_DWORD	binärer 32-bit Integer-Wert
REG_QWORD	binärer 64-bit Integer-Wert
REG_SZ	Unicode-String
REG_EXPAND_SZ	Zeichenkette variabler Länge (enthält Umgebungsvariablen wie %systemroot%) Werden bei Lesezugriff expandiert
REG_MULTI_SZ	Multi-Parameter-String (einzelne Elemente durch Standard-Trennzeichen abgetrennt)
REG_FULL_RESOURCE_DESCRIPTOR	Ein Wert der eine kodierte Beschreibung der Hardware-Ressource enthält, z.B. eines Laufwerkes, Chipsatzes usw.

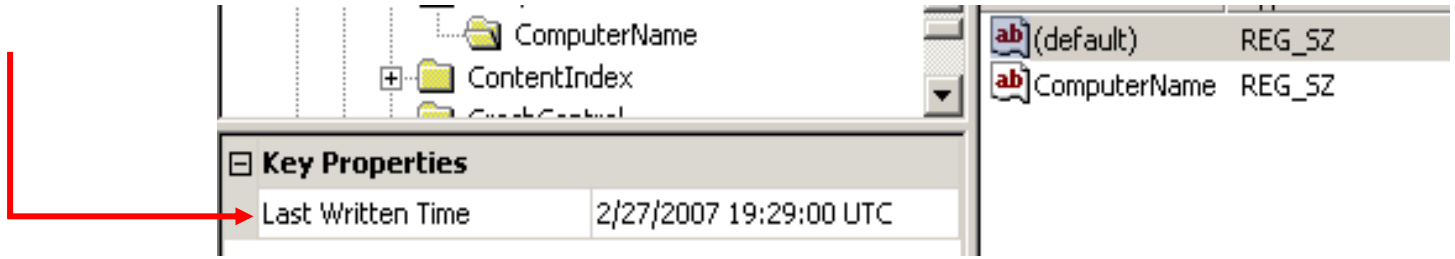
Registrierungsdatenbank Speicherorte

Klasse	Eintragungen
Timezone Informationen	Zeitzonen Informationen
Netzwerk Historie	WLAN / LAN Informationen (Adapter/Settings – IP)
	Firewall Settings
	SSID's und MAC Adressen
	Zeitstempel von Verbindungen
USB Storage / Geräte	Volume Serials
	Volume Namen
	Laufwerksbuchstaben
	Zeitstempel von Verbindungen
	USB User ID's
	Geräteidentifikationen
Most Recent Used	Last Visited MRU (Executables)
	Open Save MRU (Dokumente)
	Run MRU (Start Commands)
User Assist Keys	Programm und Datei Starts vom Desktop
Shell Bags	Informationen zu geöffneten Verzeichnissen
Cached User Credentials	Gespeicherte Domainpasswörter (SYSTEM/SECURITY)
Dienste und Treiber	Systemdienste und Systemtreiber Einstellungen

Forensisch bedeutsame Registry Informationen

LastWrite Registrierungsschlüssel

- Jeder Registrierungsschlüssel enthält einen Wert Namens Last Written
- Enthält Zeitstempel der letzten Änderung des Keys
- Zeitstempel zählt die Nanosekunden seit dem 01.01.1601.



WICHTIG:

- Der Zeitstempel bezieht sich immer auf die letzte Änderung des Keys
- bezieht sich nicht auf Änderung der einzelnen Values
- wird eine Value geändert, ändert sich aber die Last Written Time des Keys

Forensisch bedeutsame Registry Informationen

Zeitstempel und Zeitzoneninformationen

- Analyse von Zeitstempeln nur mit Informationen zu systeminterner Zeit/Zeitzone möglich

  → ***HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation***

- Relevante Zeitzonen Informationen sind:
  - **UTC** – wird als Weltzeit überall dort für Zeitangaben benutzt, wo eine weltweit einheitliche Zeitskala benötigt wird
  - **Local Time** – gibt die lokale Zeit an.
  - **Standard Time** – gesetzlich definierte Zeitzählung; heutzutage meist die dem Längengrad entsprechende Zeitzone, die sich von UTC um eine ganze Zahl von Stunden unterscheidet.
  - **Daylight Time** – Entspricht der Sommerzeit.

Forensisch bedeutsame Registry Informationen

Zeitstempel und Zeitzoneninformationen

Berechnung der Zeitzoneninformationen mit folgenden Formeln:

$$\boldsymbol{UTC} = Local\ Time + ActiveTimeBias$$

$$\boldsymbol{Local\ Time} = UTC - ActiveTimeBias$$

$$\boldsymbol{Standard\ Time} = Bias + StandardBias$$

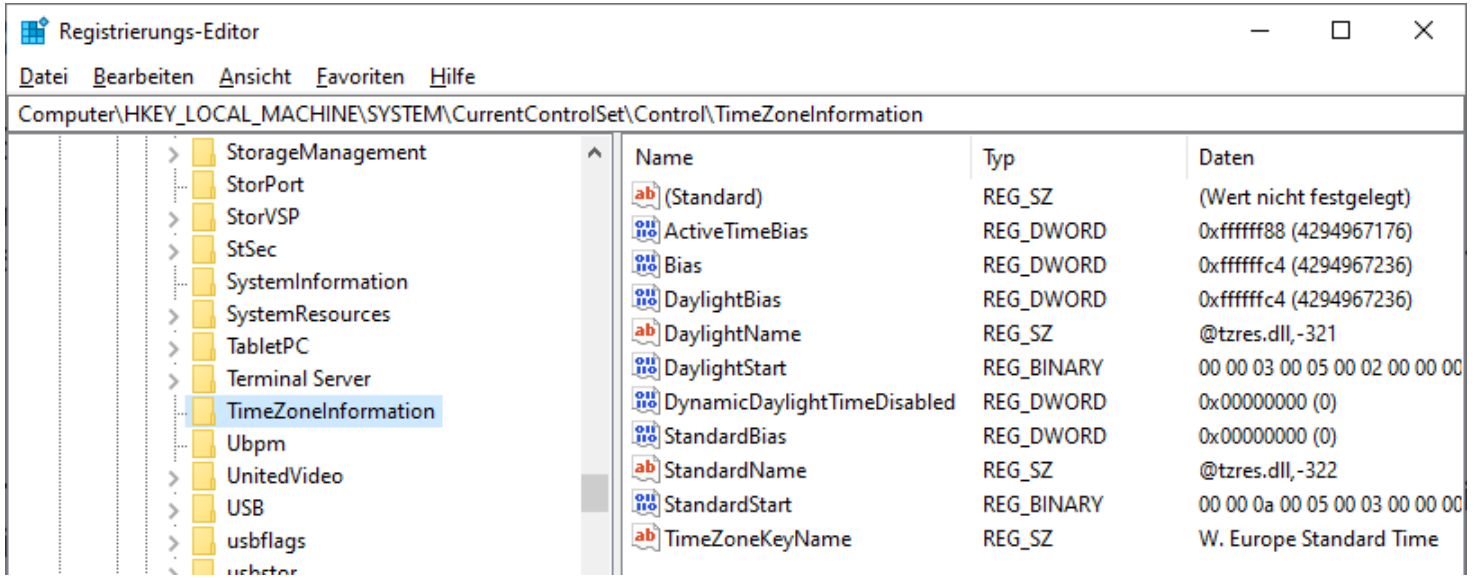
$$\boldsymbol{Daylight\ Time} = Bias + DaylightBias$$

Forensisch bedeutsame Registry Informationen

Zeitstempel und Zeitzoneninformationen

Entscheidend für Berechnung sind die Werte:

- **ActiveTimeBias**
- **Bias**
- **DaylightBias**
- **StandardBias**

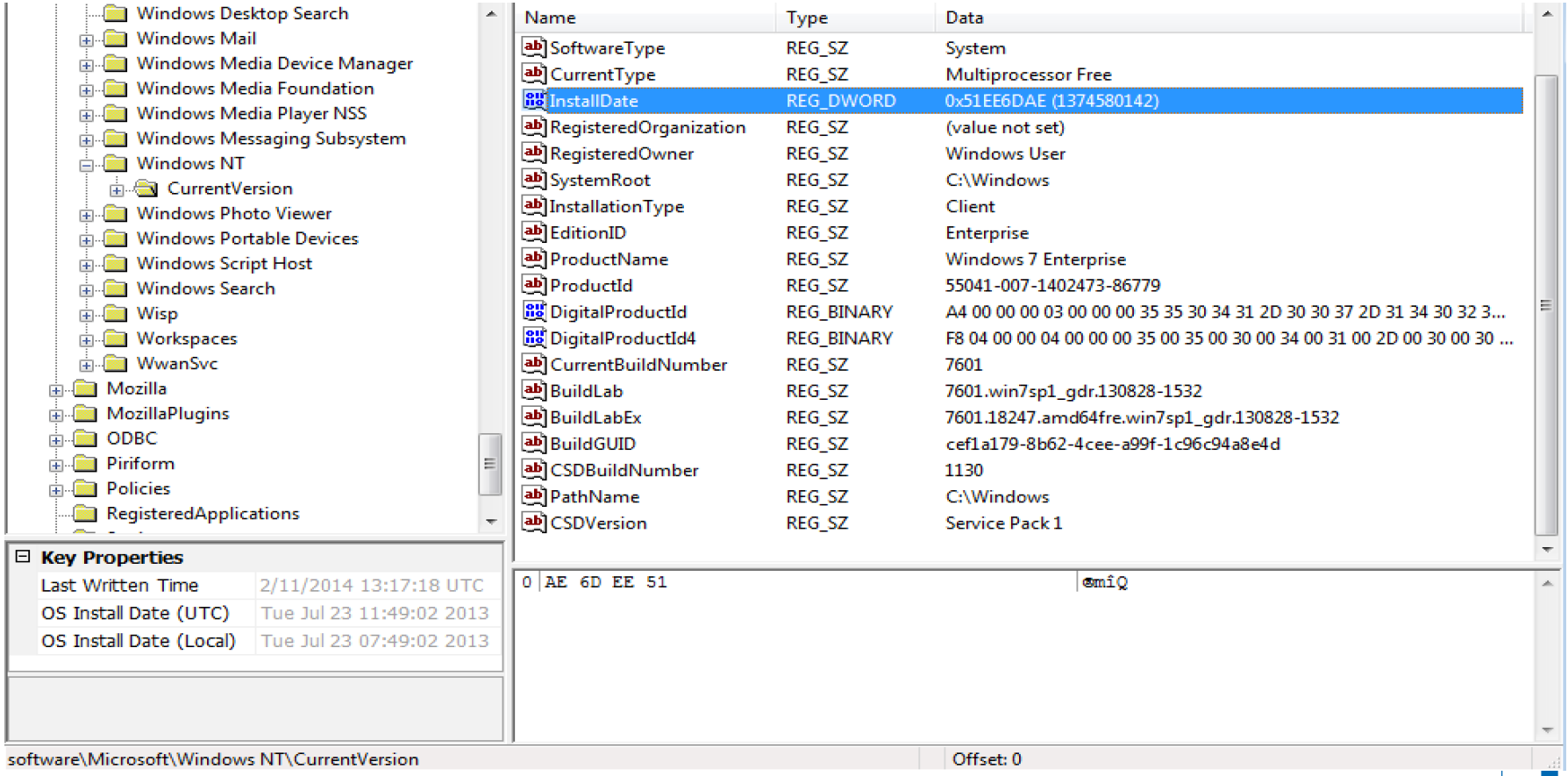


Die Informationen befinden sich alle im angegebenen Hive der TimeZoneInformation.

Forensisch bedeutsame Registry Informationen

Operating System Version und Computerinformationen

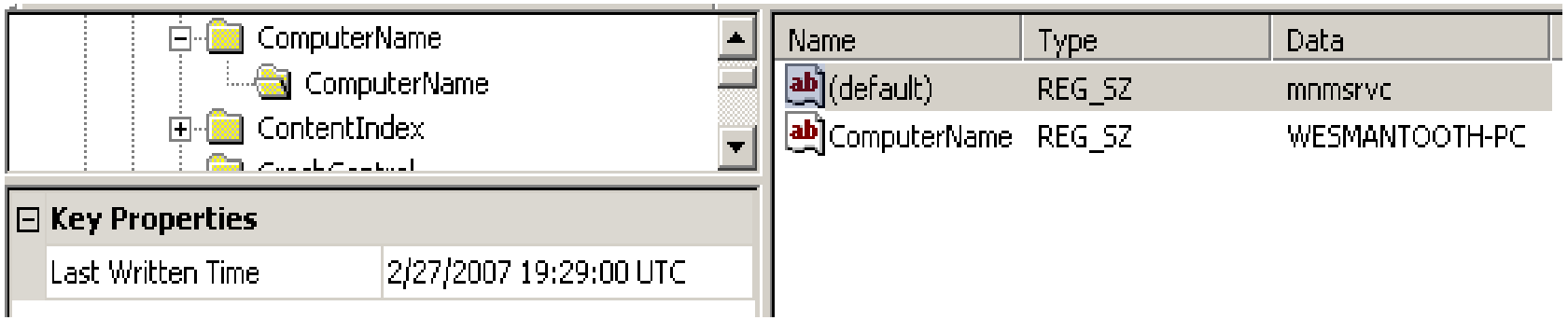
→ *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion*



Forensisch bedeutsame Registry Informationen

Operating System Version und Computerinformationen

SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName



Forensisch bedeutsame Registry Informationen

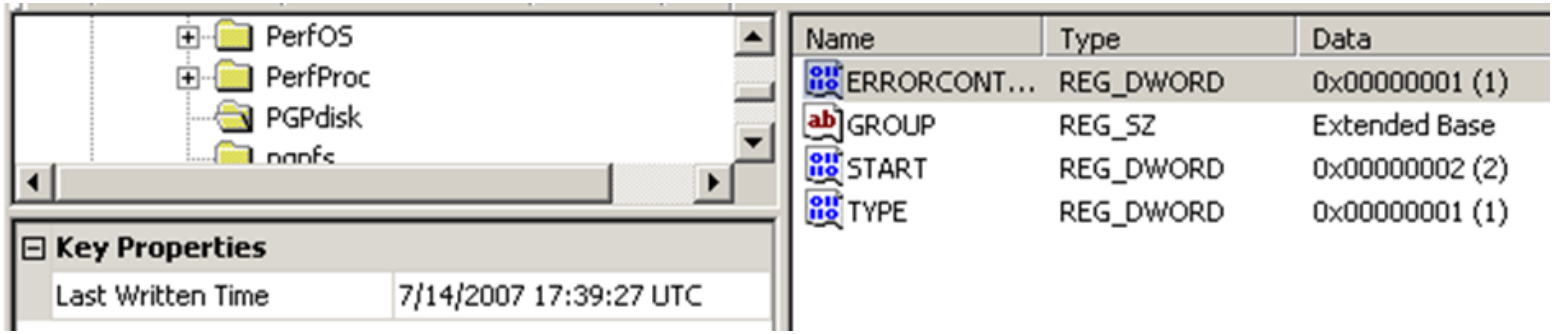
Autorun Locations

- Windows verfügt über Reihe von **Autorun Locations**.
- Aufgeführte Programme, werden beim Systemstart automatisch ausgeführt:
  - ***HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce***
  - ***HKLM\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run***
  - ***HKLM\Software\Microsoft\Windows\CurrentVersion\Run***
  - ***HKLM\SYSTEM\CurrentControlSet\Services (Typ 0x02 = Start)***

Forensisch bedeutsame Registry Informationen

Autorun Locations

- Möglichkeit auch Programme bei der Benutzeranmeldung am Computer automatisch auszuführen:
  - ***HKCU\Software\Microsoft\Windows\CurrentVersion\Windows\Run***
  - ***HKCU\Software\Microsoft\Windows\CurrentVersion\Run***
  - ***HKCU\Software\Microsoft\Windows\CurrentVersion\Runonce***

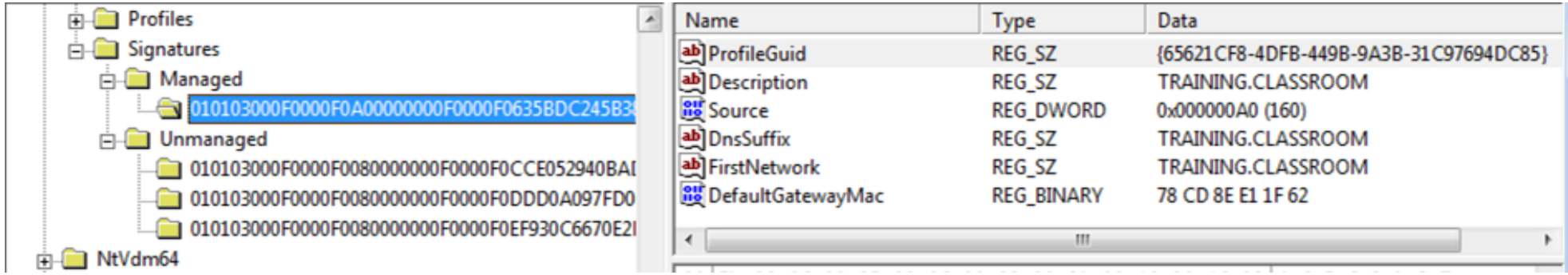


Forensisch bedeutsame Registry Informationen

Netzwerkverbindungen - Managed by a Domain (Vista/7/8/10)

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed

- DnsSuffix = Domain
- FirstNetwork = SSID
- DefaultGatewayMac = Media Access Control (MAC) Adresse des Gateway
- Last Written Time = Letzte Verbindung mit dem Netzwerk

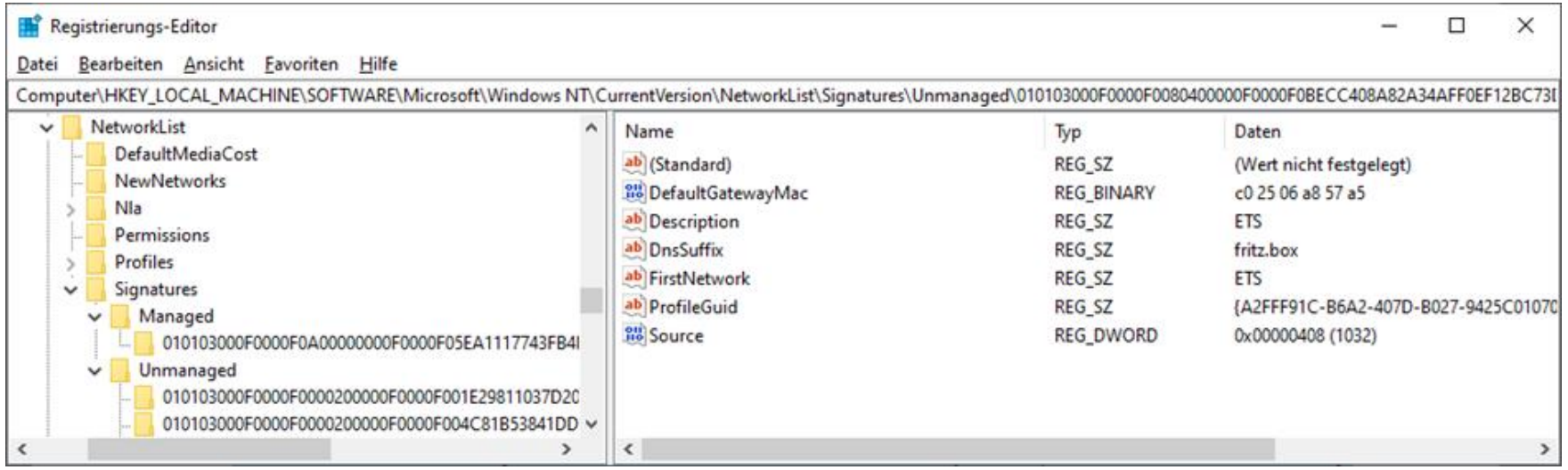


Forensisch bedeutsame Registry Informationen

Netzwerkverbindungen - NotManaged by a Domain (Vista/7/8/10)

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

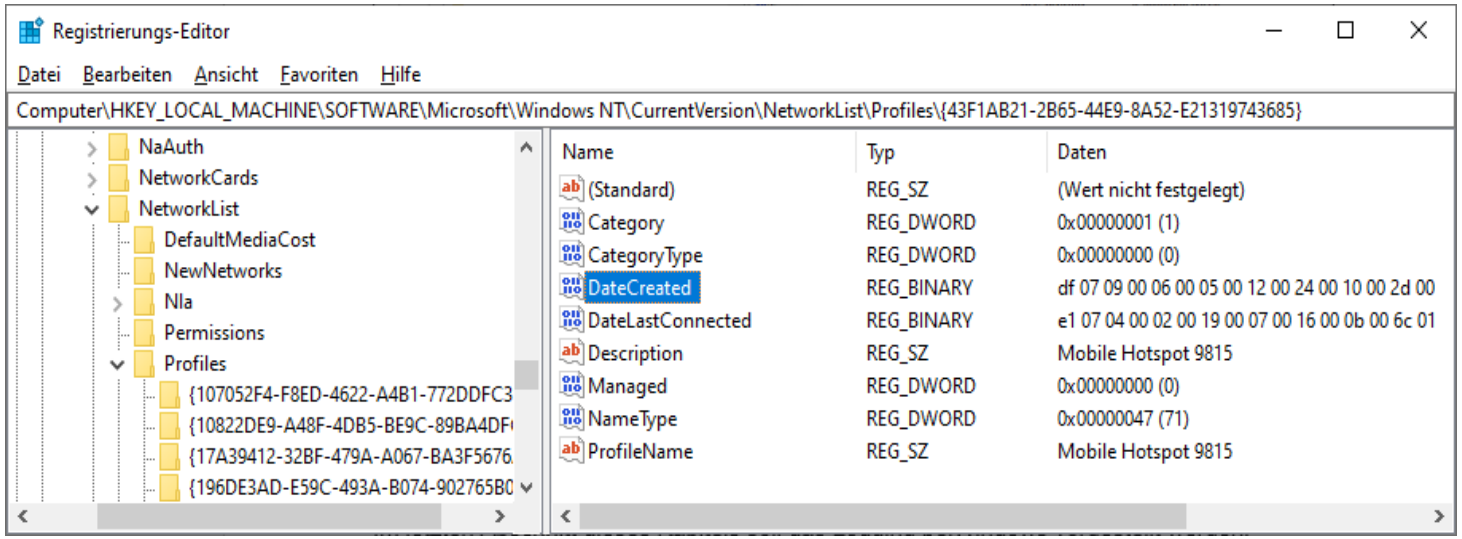
- DnsSuffix = Domain
- FirstNetwork = SSID
- DefaultGatewayMac = Media Access Control (MAC) Adresse des Gateway
- Last Written Time = Letzte Verbindung mit dem Netzwerk



Forensisch bedeutsame Registry Informationen

Netzwerkadapter

- *HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\{GUID} (XP)*
- *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles (Vista/7/8)*



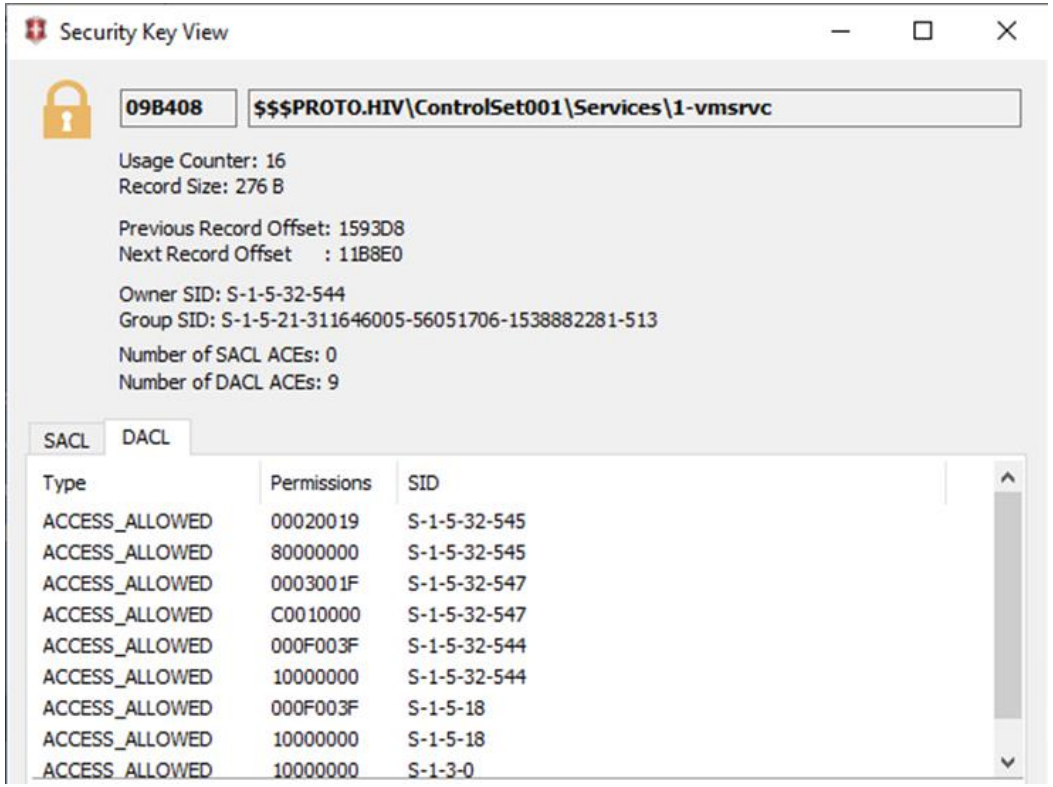
- **NameType**
  - 0x47 = Wireless
  - 0x06 = Wired
  - 0x17 = Broadband
- **Date** = 128-bit Systemdatum

Zugriffsberechtigungen auf Registry Daten

Zugriffe auf Registryschlüssel per SID geregelt:

- **SID gespeichert von:**
  - Besitzers
  - Erzeuger
  - Änderungsberechtigte

→ unterschiedliche Zugriffsberechtigungen zu gewährleisten.



Registrierungsdatenbank 64 Bit Support

- für Support von 32 Bit Softwareanwendungen auf 64 Bit Umgebungen extra Schlüssel eingeführt
- Zu finden in der SOFTWARE Registrierungsdatei ein.

HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node

- für 32 Bit Anwendungen relevanten Informationen notwendigerweise als 64 Bit Formate abgelegt

Betriebssystemartefakte

Papierkorb, Thumbs

Der Papierkorb

$Recycle.Bin oder $RECYCLE.BIN?

→ Sicherlich kennen die meisten den Papierkorb als $Recycle.Bin. Dieser wird jedoch auch oft als $RECYCLE.BIN angezeigt, aber warum?

- '$' bedeutet, dass der Papierkorb zum System gehört
- $Recycle.Bin befindet sich auf dem Windows-Laufwerk (C:\)
- $RECYCLE.BIN wird auf ein Laufwerk geschrieben, das an ein Windows-System angeschlossen (z. B. ein sekundäres Laufwerk)

Untersuchung der Papierkorbdaten

- Im $Recycle.Bin befinden sich Unterverzeichnisse der SID (Security Identifier) der am System eingerichteten Benutzer
  - jeder Benutzer hat einen eigenen Papierkorb hat

- Unterscheidung der Dateien in $I oder $R-Dateien
  - Haben beide unkonventionelle Namen

- Lokation des Papierkorbs: C:\$Recycle.Bin\<SID>
  - ACHTUNG: versteckte Datei

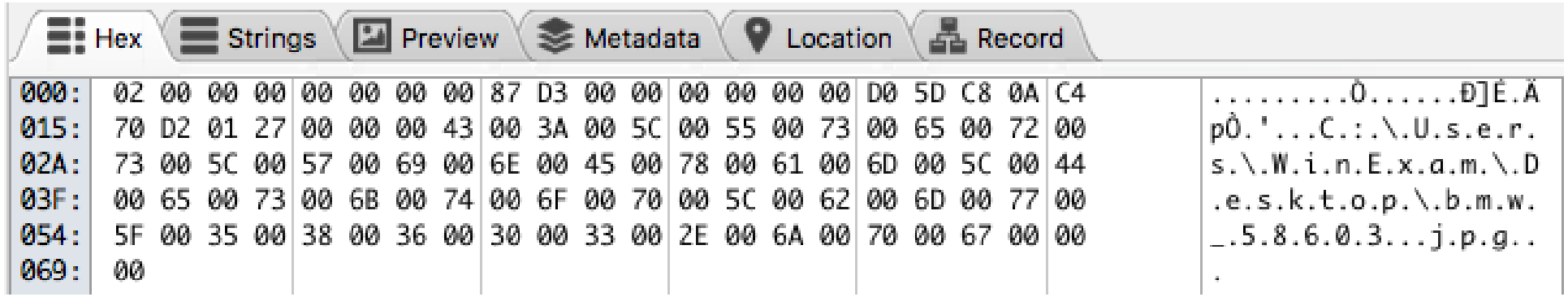
Dateiennamen mit $I-Anfang

Dateien, die mit $I beginnen, sind im Wesentlichen die Metadaten für die bestimmte gelöschte Datei. Im Gegensatz zu früheren Windows-Versionen hat die $I-Datei keine feste Größe von 544 Byte und ist nur so groß, wie sie sein muss.

Aufbau der Metadaten Datei:

Offset	Size	Data Description
0	8	Header
8	8	Deleted File Size
16	8	Date/Time File Deleted
24	4	File Name Length
28	Variable Length	File Name And Path

Beispiel gelöschte Dateien

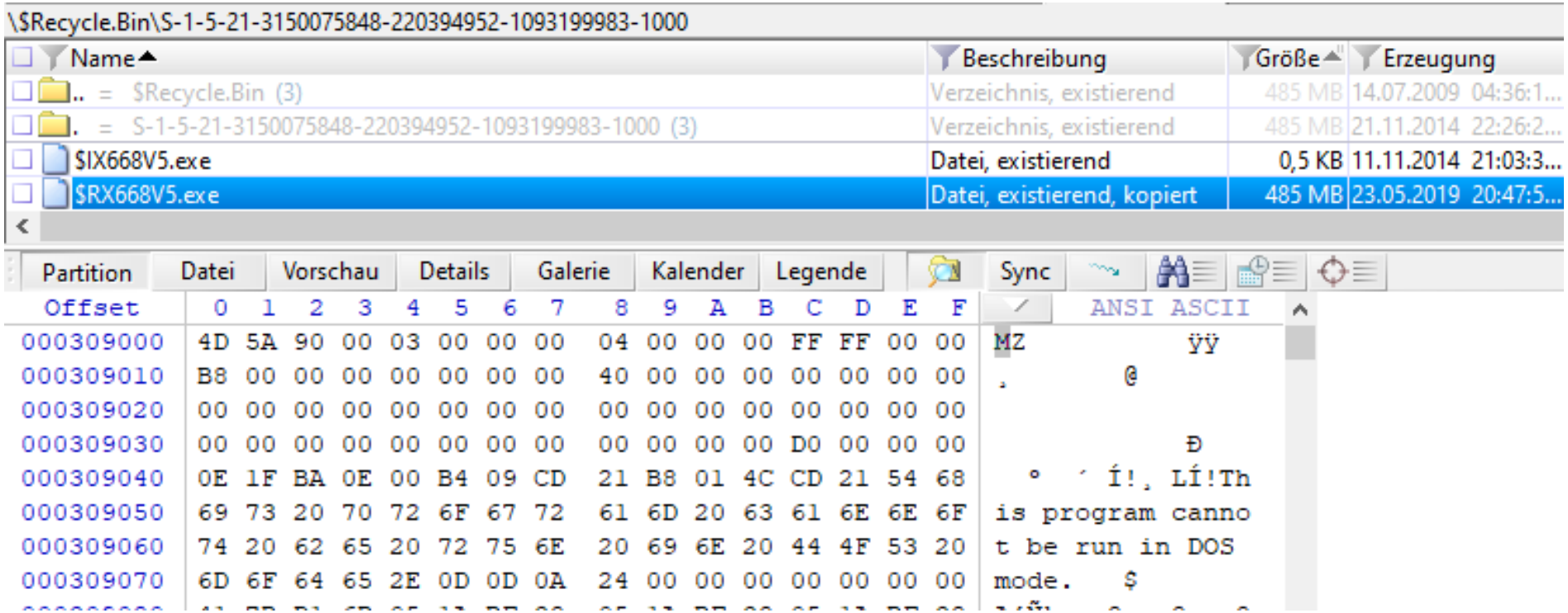


Description	Hex Value	Interpreted Data
Header	0200000000000000	2
Deleted File Size	87D3000000000000	54151
Date/TIme Deleted	D05DC80AC470D201	2017-01-17 13:17:24 (UTC)
File Name Length	27000000	39
File Name And Path	43003A005C0055007300 6500720073005C005700 69006E00450078006100 6D005C00440065007300 6B0074006F0070005C00 62006D0077005F003500 3800360030003300 2E006A00700067	C.:.\.U.s.e.r.s.\.W.i.n.E.x.a.m. \.D.e.s.k.t.o.p.\.b.m.w._. 5.8.6.0.3...j.p.g

Dateiennamen mit $R-Anfang

Die Dateien, die mit $R beginnen, sind der Inhalt der tatsächlichen in den Papierkorb verschobenen Dateien.

→ Tatsächlicher Dateiinhalt

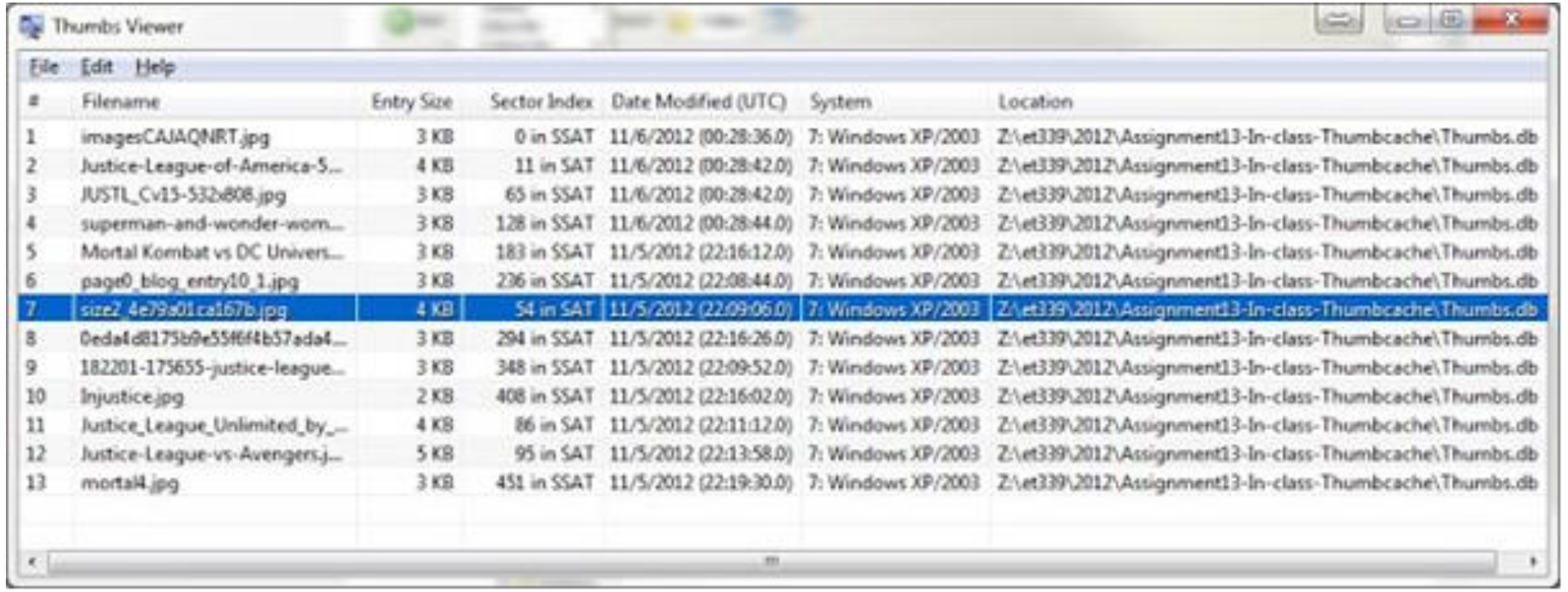


Thumbs und Thumbcache

- Der Windows-Thumbcache und die Thumbs.db-Datei sind eine hervorragende Quelle für grafische Beweise für Untersuchungen zu Dateikenntnis und Dateinutzung.
- Thumbcache-Bilder sind versteckte Systemdateien, die kleinere Bilder von Multimediadateien darstellen und dazu dienen, dem Benutzer eine grafische Ansicht der Dateien in einem bestimmten Verzeichnis zu ermöglichen.
- Thumbcache-Dateien werden zentral für jedes Benutzerkonto gespeichert. Diese Beweise können als stummer Zeuge für einen Benutzer dienen, der Bilder ansieht, oder als Aufzeichnung von Bildern, die einmal auf einem System vorhanden waren.

Thumbs und Thumbcache

- Thumbs Dateien sind die bis Window XP genutzten Datendateien mit Vorschaubildern, die zugleich auch den Dateinamen enthielten. Die thumb.db Dateien waren nicht zentral abgelegt sondern in den jeweiligen Verzeichnissen mit den Daten.



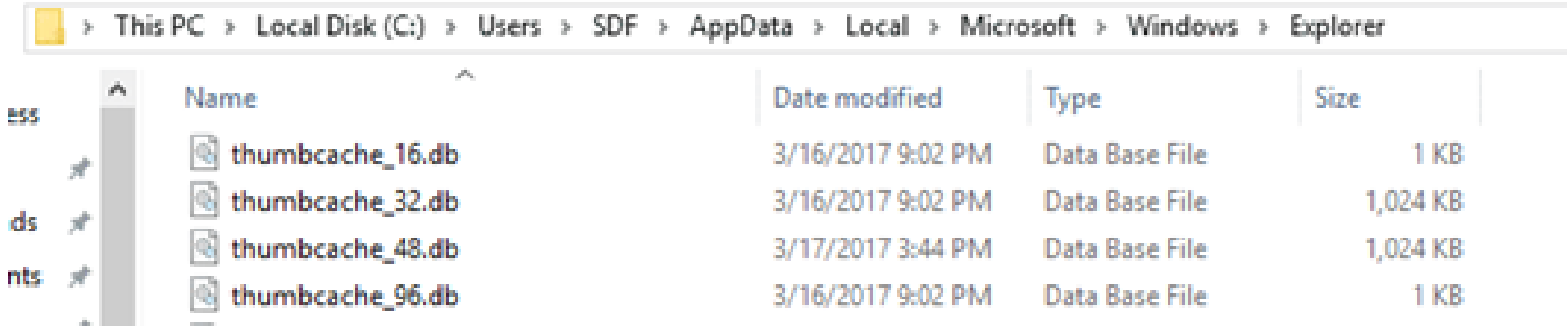
#	Filename	Entry Size	Sector Index	Date Modified (UTC)	System	Location
1	imagesCAJAQNRT.jpg	3 KB	0 in SSAT	11/6/2012 (00:28:36.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
2	Justice-League-of-America-5...	4 KB	11 in SAT	11/6/2012 (00:28:42.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
3	JUSTL_Cv15-532x808.jpg	3 KB	65 in SSAT	11/6/2012 (00:28:42.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
4	superman-and-wonder-wom...	3 KB	128 in SSAT	11/6/2012 (00:28:44.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
5	Mortal Kombat vs DC Univers...	3 KB	183 in SSAT	11/5/2012 (22:16:12.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
6	page0_blog_entry10_1.jpg	3 KB	236 in SSAT	11/5/2012 (22:08:44.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
7	size2_4e79a01ca167b.jpg	4 KB	54 in SAT	11/5/2012 (22:09:06.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
8	0eda4d8175b9e55f6f4b57ada4...	3 KB	294 in SSAT	11/5/2012 (22:16:26.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
9	182201-175655-justice-league...	3 KB	348 in SSAT	11/5/2012 (22:09:52.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
10	Injustice.jpg	2 KB	408 in SSAT	11/5/2012 (22:16:02.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
11	Justice_League_Unlimited_by_...	4 KB	86 in SAT	11/5/2012 (22:11:12.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
12	Justice-League-vs-Avengers.j...	5 KB	95 in SAT	11/5/2012 (22:13:58.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
13	mortal4.jpg	3 KB	451 in SSAT	11/5/2012 (22:19:30.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db

Thumbs und Thumbcache

- Ab Windows Vista hat Microsoft die Verwendung von Thumbs.db-Datenbankdateien auf Verzeichnisebene auf das Speichern von Miniaturbildern in einer einzelnen Ordnerstruktur umgestellt
- einzelne Dateien gespeichert, die alle angezeigten Elemente basierend auf der ausgewählten Symbolgröße enthalten
- Thumbcache-Dateien sind direkt an jeden Benutzer gebunden
  - → in separaten Benutzerverzeichnis gespeichert.
  - Lokation ab Windows Vista:

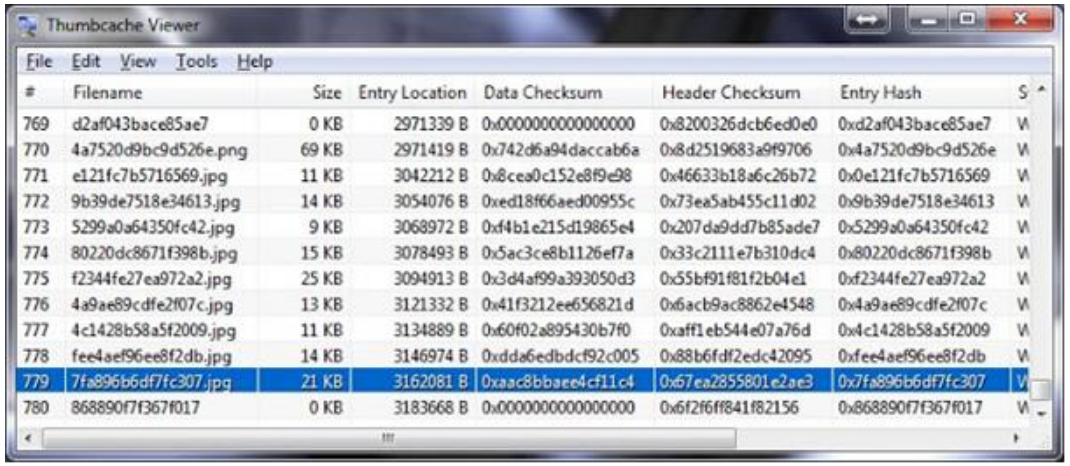
```
C:\Users\<Username>\AppData\Local\Microsoft\Windows\Explorer
```

Thumbs und Thumbcache



Thumbs und Thumbcache

- Speicherung in Thumcache.db je nach Datenformat
  - original.jpg → als JPG-Datei gespeichert
  - Original.png → als PNG-Datei gespeichert
- Behalten nicht ursprünglichen Namen bei
  - werden in Unicode Zeichenfolge umbenannt
  - ThumbnailCacheID genannt wird.

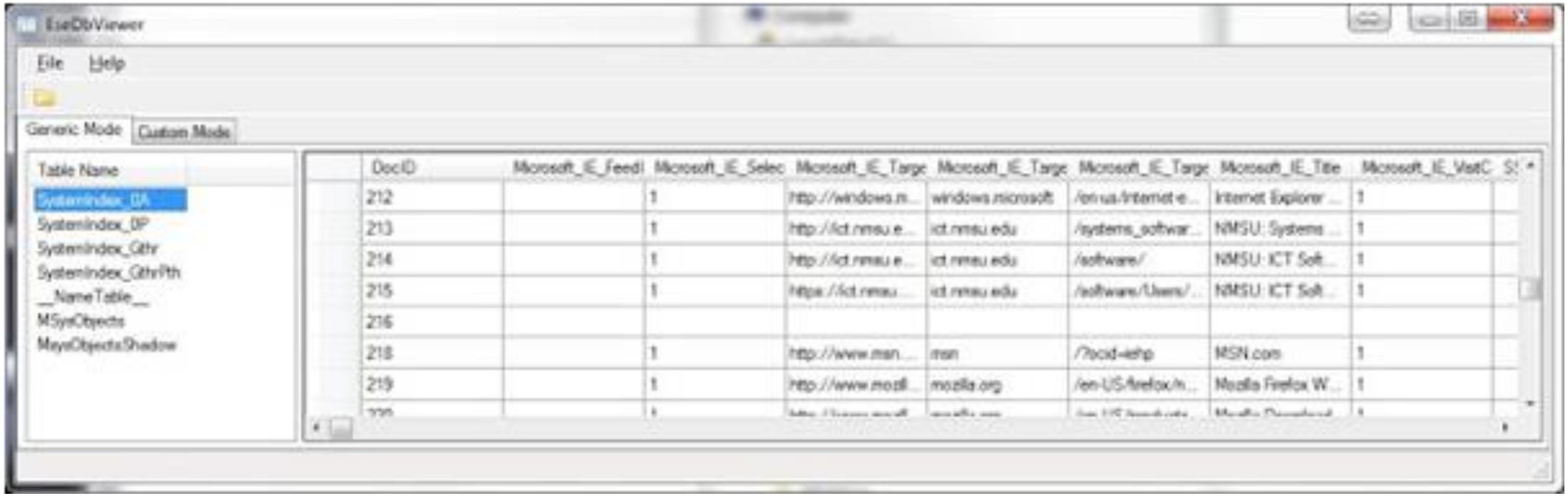


#	Filename	Size	Entry Location	Data Checksum	Header Checksum	Entry Hash	S
769	d2af043bace85ae7	0 KB	2971339 B	0x0000000000000000	0x8200326dcb6ed0e0	0xd2af043bace85ae7	W
770	4a7520d9bc9d526e.png	69 KB	2971419 B	0x742d6a94daccab6a	0x8d2519683a9f9706	0x4a7520d9bc9d526e	W
771	e121fc7b5716569.jpg	11 KB	3042212 B	0x8cea0c152e8f9e98	0x46633b18a6c26b72	0x0e121fc7b5716569	W
772	9b39de7518e34613.jpg	14 KB	3054076 B	0xed18f66aed00955c	0x73ea5ab455c11d02	0x9b39de7518e34613	W
773	5299a0a64350fc42.jpg	9 KB	3068972 B	0xf4b1e215d19865e4	0x207da9dd7b85ade7	0x5299a0a64350fc42	W
774	80220dc8671f398b.jpg	15 KB	3078493 B	0x5ac3ce8b1126ef7a	0x33c2111e7b310dc4	0x80220dc8671f398b	W
775	f2344fe27ea972a2.jpg	25 KB	3094913 B	0x3d4af99a393050d3	0x55bf91f81f2b04e1	0xf2344fe27ea972a2	W
776	4a9ae89cdfe2f07c.jpg	13 KB	3121332 B	0x41f3212ee656821d	0x6acb9ac8862e4548	0x4a9ae89cdfe2f07c	W
777	4c1428b58a5f2009.jpg	11 KB	3134889 B	0x60f02a895430b7f0	0xaff1eb544e07a76d	0x4c1428b58a5f2009	W
778	fee4aef96ee8f2db.jpg	14 KB	3146974 B	0xdda6edbdcf92c005	0x88b6fdf2edc42095	0xfee4aef96ee8f2db	W
779	7fa896b6df7fc307.jpg	21 KB	3162081 B	0xaac8bbaee4cf11c4	0x67ea2855801e2ae3	0x7fa896b6df7fc307	W
780	868890f7f367f017	0 KB	3183668 B	0x0000000000000000	0x6f2f6ff841f82156	0x868890f7f367f017	W

Thumbs und Thumbcache

- Thumbcache-Datenbank keine Informationen, mit denen Thumbnails mit ursprünglichen Dateinamen oder Speicherorten verknüpft werden können
- Evtl. möglich über die Verwendung der Windows-Suchdatenbank (Windows.edb).
  - speichert die ThumbnailCacheID als Teil seiner Metadaten für indizierte Dateien
  - Tabelle SystemIndex_0A enthält:
    - Pfad
    - Dateinamenangabe
    - verknüpftes Programm
    - ThumbnailCacheID.

Thumbs und Thumbcache



Thumbs und Thumbcache

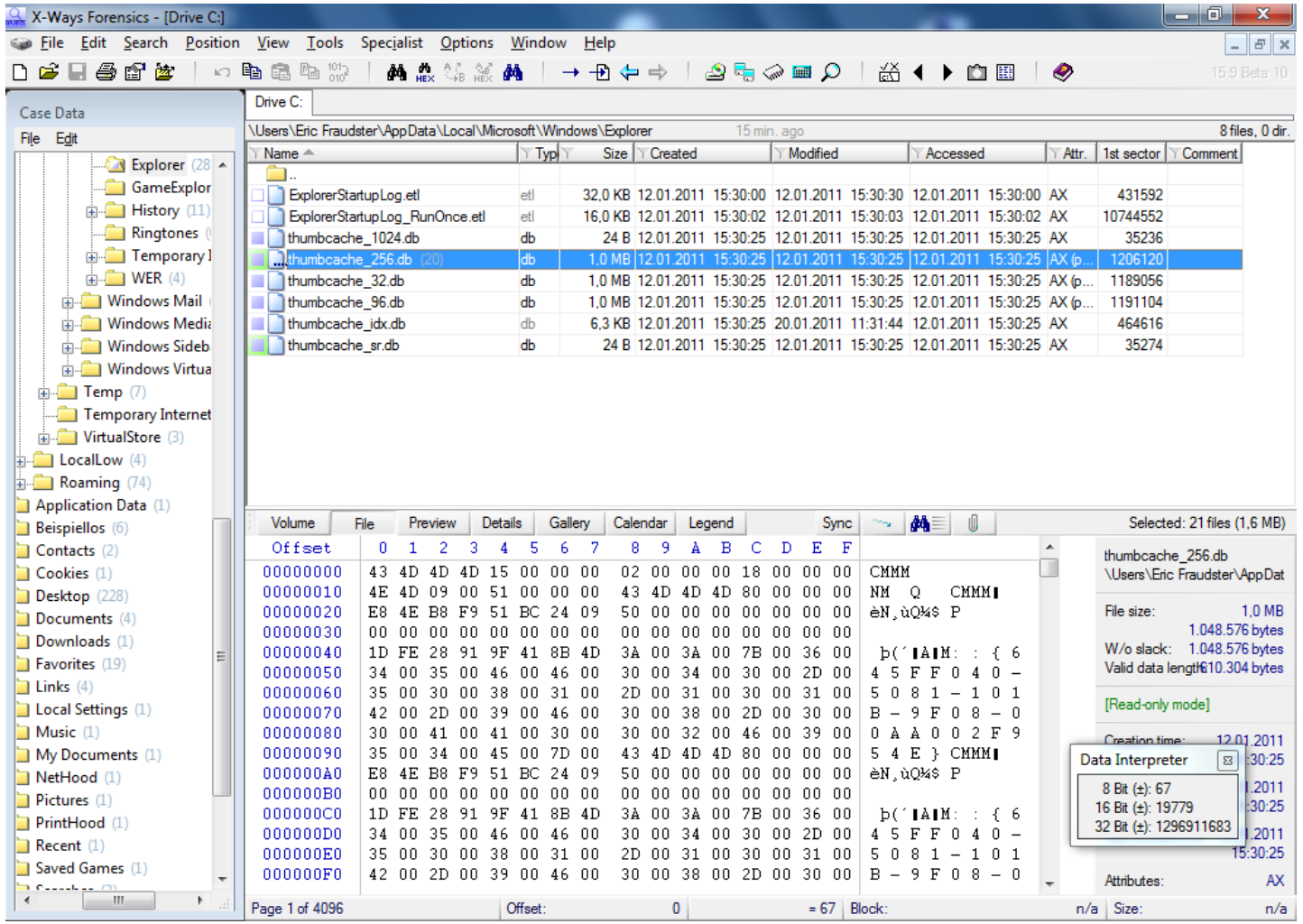
- Speicherort der EDB-Datei:

  `C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb`

- **Tools:**
  - Thumbcache Viewer //thumbcacheviewer.github.io/
  - ESEDB Viewer //www.woanware.co.uk/forensics/esedbviewer.html
- **Hinweis:**
  - Sofern ein Verzeichnis mit Bildern im Netzwerk aufgerufen wird, werden reguläre Thumbs.db Dateien geschrieben. Dies Verhalten ist unter Windows 7, 8 und 10 feststellbar!
  - Die Thumbcache Erzeugung kann per Registry deaktiviert werden!

Thumbs und Thumbcache

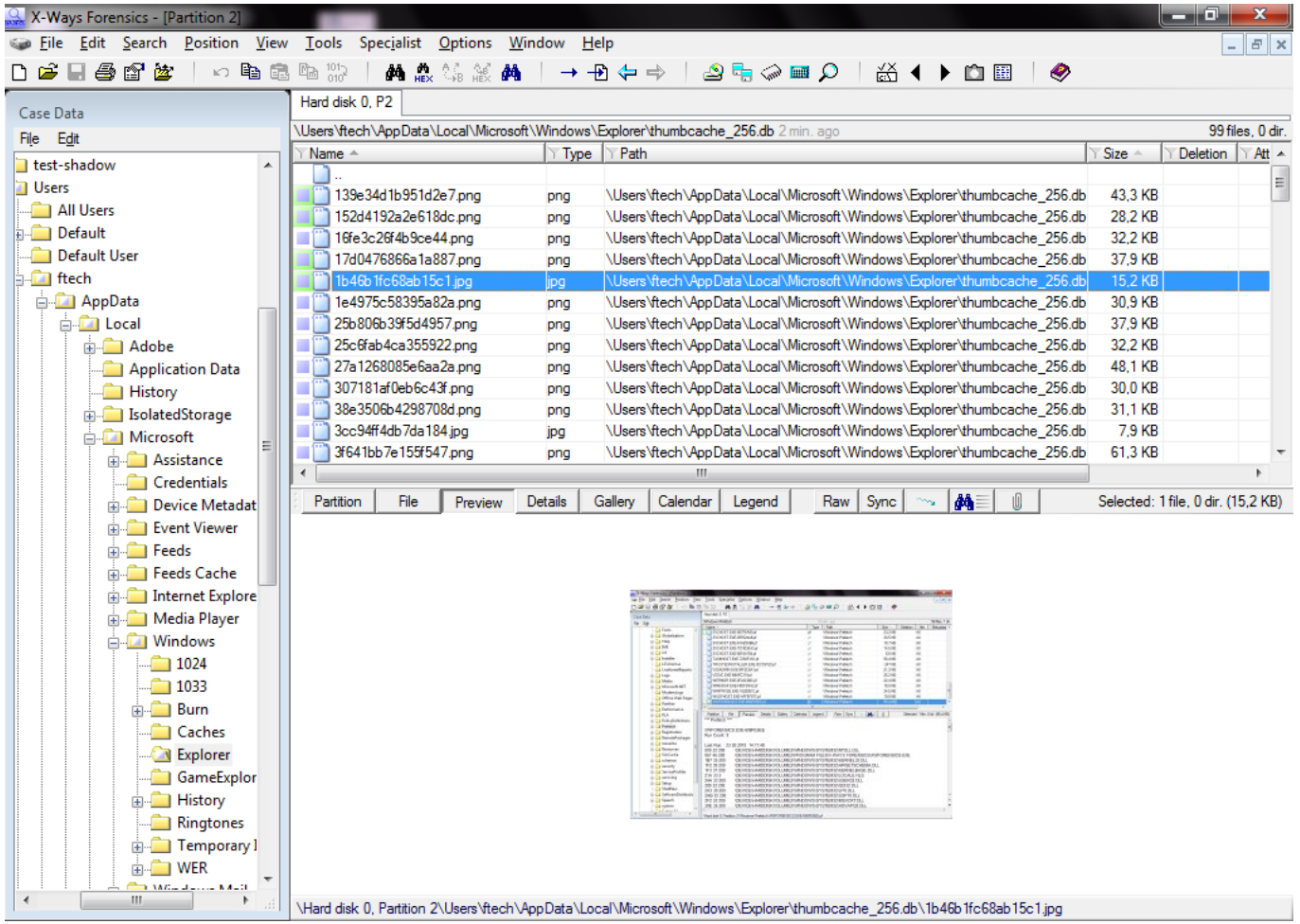
X-Ways analysiert Thumb.db und ThumbCache Dateien beim Dateiüberblick erweitern in eingebetteten Dateien und extrahiert hierbei die Vorschaubilder und ThumbCacheID.



Thumbs und Thumbcache

Zudem kann X-Ways die Windows.edb Datei lesen.

Eine Zuordnung von ThumbCacheID zu Vorschaubildern wird von X-Ways jedoch nicht unterstützt.



Benutzerkontenzugriffs-steuerung

User Access Control (UAC)

- User-Access-Control (UAC) = neues Sicherheitsfeature seit Windows Vista
- Verhindert Zugriff von Anwendungen auf die Programme und Systemverzeichnisse ohne administrative Kennung
- keine Software darf, ob Browser oder Festplattentool Zugriff auf diese durch die UAC geschützten Bereiche nehmen
- außer die jeweilige Software wird mit Administratorrechten ausgeführt (rechte Maustaste – Ausführen als Administrator).

User Access Control (UAC)

- nach wie vor Anwendungen, die durch ihre Implementierung gegen diesen Grundsatz verstoßen
  - Schreiben anwendungsspezifische Nutzerdaten im eigenen Programmverzeichnis
  - Diese Anwendungen werden durch das Betriebssystem ermittelt
  - alle Schreib/Lese Operationen auf virtuelles Programmverzeichnis umgeleitet

→ **C:\Users\<User>\AppData\Local\VirtualStore“**

- Dieses Verzeichnis hat daher eine wichtige Bedeutung für die Untersuchung und sollte immer mit in Augenschein genommen werden.

User Access Control (UAC)

- Auch in der Registry interessant
- User ohne Administrator-Berechtigung können nicht in den Registrierungshive HKEY_LOCAL_MACHINE/SOFTWARE schreiben
  - Schreibzugriffe in diesen Bereich werden umgebogen und werden für den Benutzer transparent zugeordnet.

  → **HKEY_CURENT_USERS\Software\Classes\VirtualStore\Machine\Software**
- Die virtuellen Registrierungsschlüssel werden jedoch nicht in die Datei NTUSER.DAT geschrieben, sondern in das Anwendungsdatenverzeichnis unter

  → **„\AppData\Local\Microsoft\Windows\usrclass.dat“**
- Bei der Auswertung von Registrierungsinformationen sind diese Ablageorte daher ebenfalls zu untersuchen.

Remote Desktop Nutzung

Betriebssystemspezifika Windows

RDP CACHE FORENSIK

- Angriffe auf Windows Netzwerke häufig mittels RDP (respektive Terminal Server)
- RDP Initialangriff für Seitwärtsbewegungen - Lateral Movements
- Verwendung des Windows "mstsc" -Clients erbringt zusätzliche Artefakte:
  - automatische Cache-Dateien
  - enthalten Bereiche des Computerbildschirm (Angreifersicht)
  - Cachedateien sind weiterer Beweisgegenstand für die Forensik

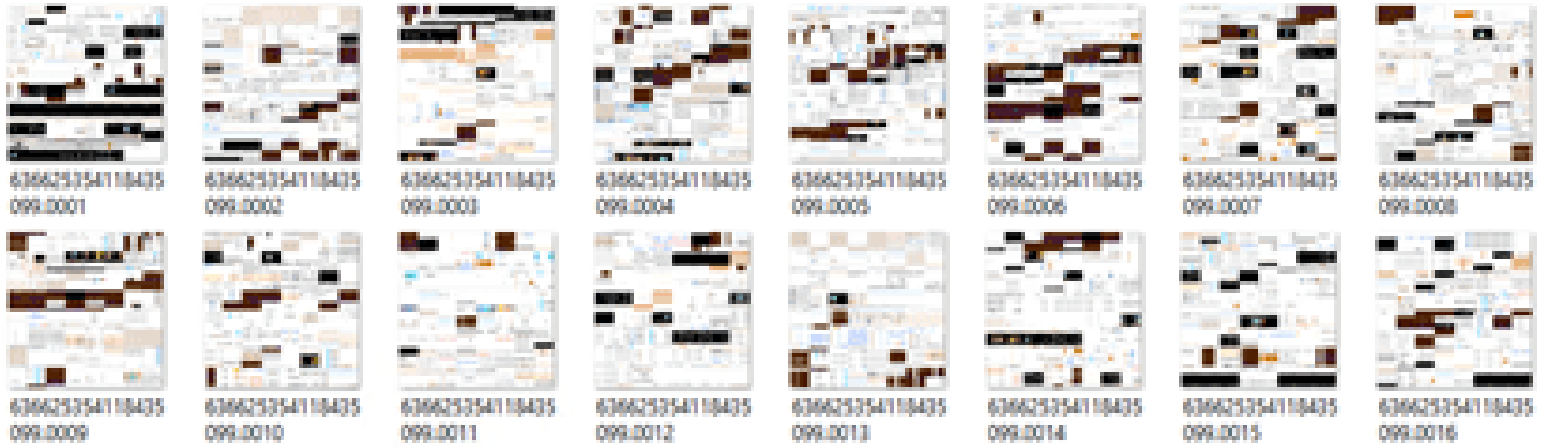
Zu finden auf dem folgenden Pfad:

C:\Users\XXX\AppData\Local\Microsoft\Terminal Server Client\Cache

Betriebssystemspezifika Windows

RDP CACHE FORENSIK

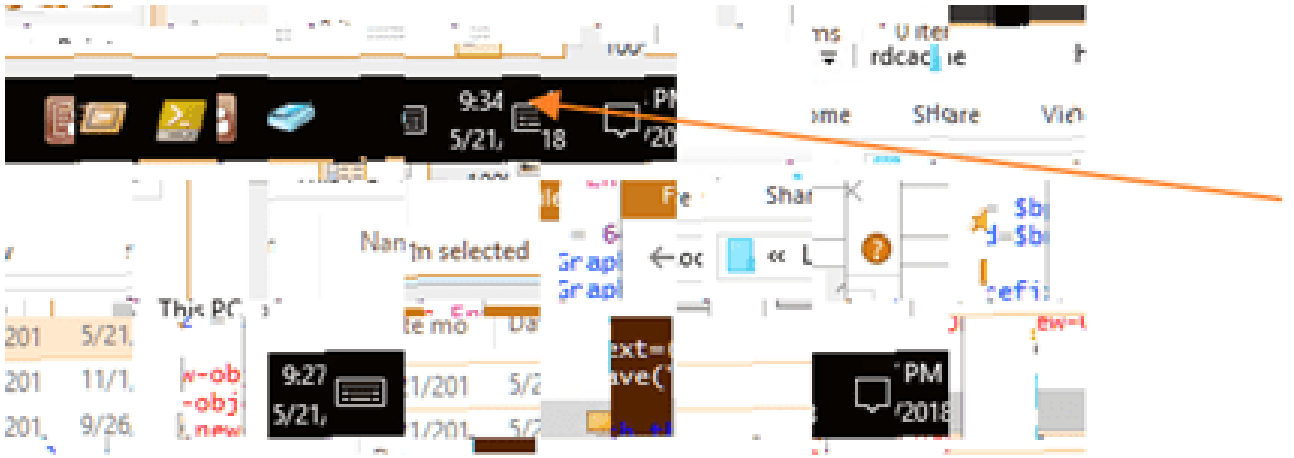
- Notwendigkeit:
  - Werkzeug zur Extraktion der gespeicherten Bilder der Cache Dateien
  - Tool etwa "bmc-tools" von ANSSI-FR
- Extraktion von Bitmaps mit einer Größe von 64x64
- nur als Puzzle Teile verwendbar, können trotzdem wichtige Hinweise enthalten



Betriebssystemspezifika Windows

RDP CACHE FORENSIK

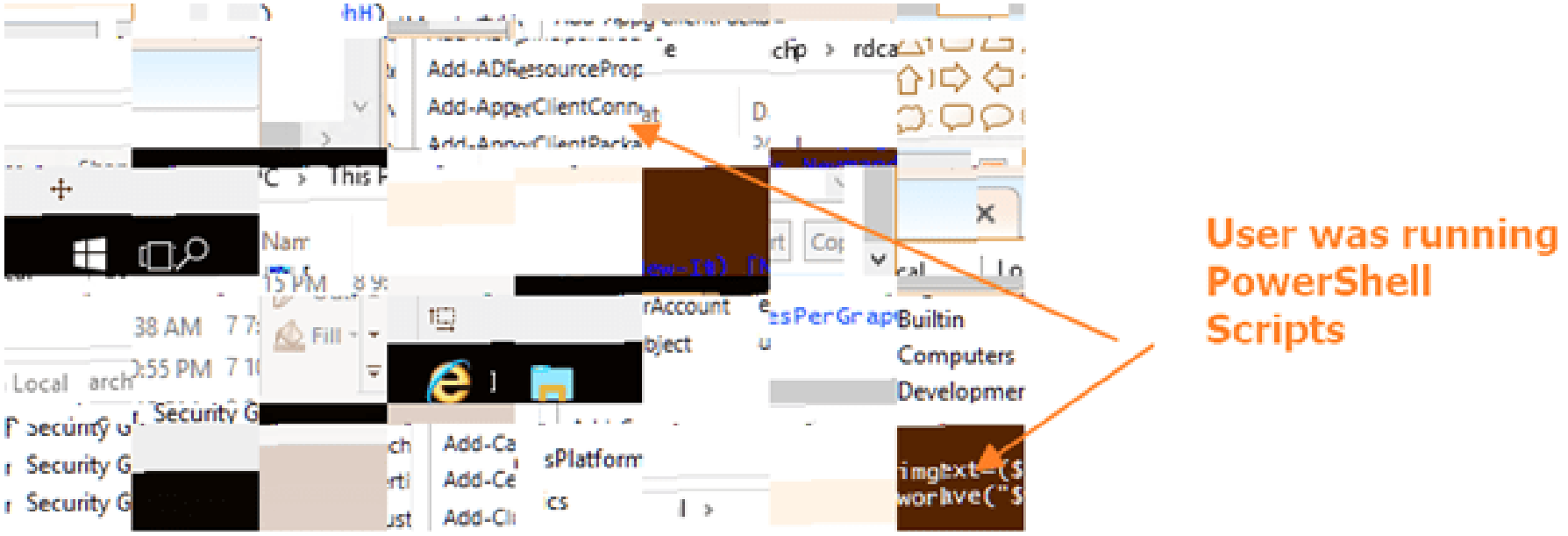
- Extraktion von Bitmaps mit einer Größe von 64x64
- nur als Puzzle Teile verwendbar, können trotzdem wichtige Hinweise enthalten



Betriebssystemspezifika Windows

RDP CACHE FORENSIK

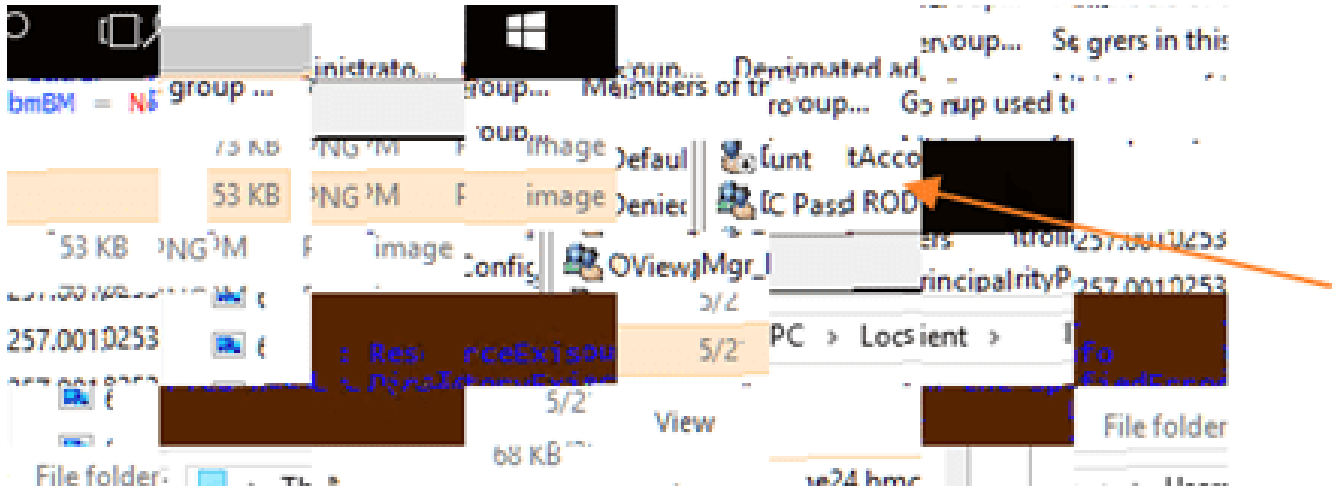
- Extraktion von Bitmaps mit einer Größe von 64x64
- nur als Puzzle Teile verwendbar, können trotzdem wichtige Hinweise enthalten



Betriebssystemspezifika Windows

RDP CACHE FORENSIK

- Extraktion von Bitmaps mit einer Größe von 64x64
- nur als Puzzle Teile verwendbar, können trotzdem wichtige Hinweise enthalten

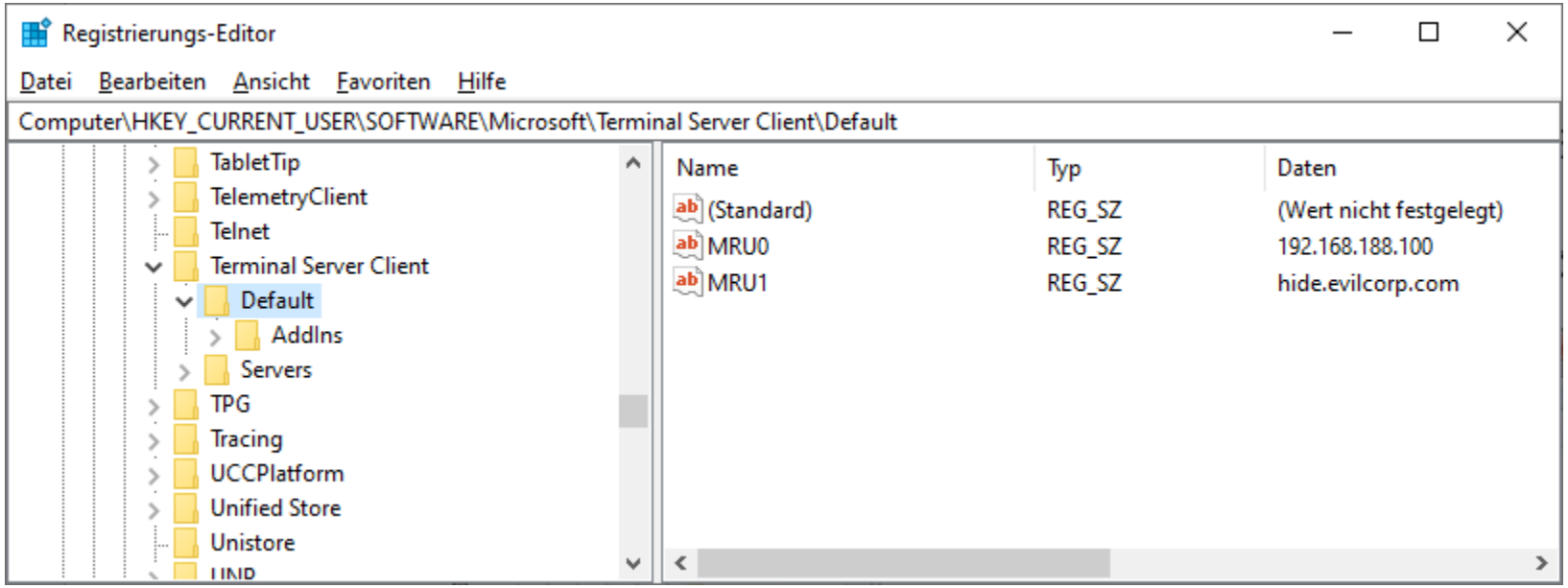


Betriebssystemspezifika Windows

RDP CACHE FORENSIK

Zusätzlich zu den Cache Dateien befinden sich in der Registry die MRU Eintragungen der RDP Server die genutzt wurden:

HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default

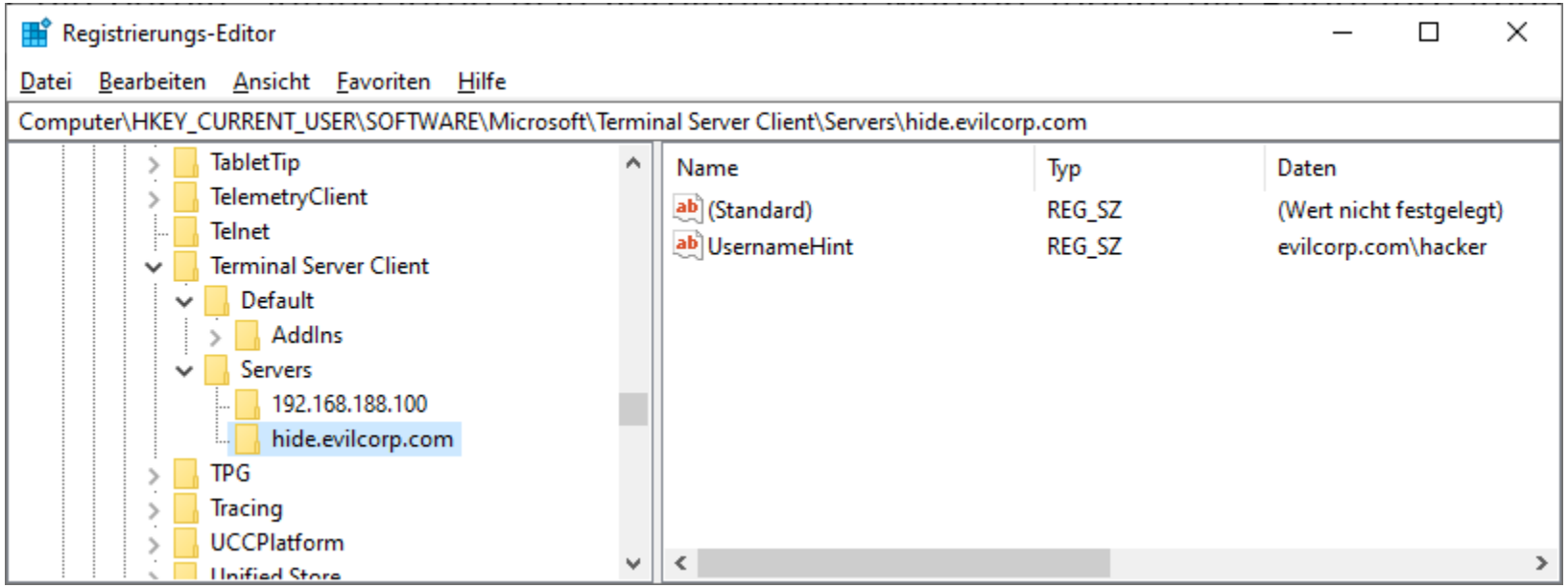


Betriebssystemspezifika Windows

RDP CACHE FORENSIK

Für die bereits aufgebauten RDP Verbindungen werden zudem die Benutzernamen der Anmeldung (***UsernameHint***) gespeichert im Schlüssel:

HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers.



Zusammenfassung

Zusammenfassung

Der Teil 1 der Windows spezifischen Daten ist damit erarbeitet. Die so zu ermittelnden Informationen der einzelnen Bereiche geben jeweils Hinweise auf Dateizugriffe und Dateinutzung am Windows System. Das Zusammenspiel der hier einzeln vorgestellten Windows Artefakte ergibt am Ende ein Gesamtbild der Nutzung von Computersystemen, welche eine wesentliche Rolle in einer forensischen Computeruntersuchung spielen kann.

Im Teil 2 werden wir auf den Punkt externe Datenträgernutzung eingehen, schauen uns Zeit- und Zugriffsanalysen näher an.

Vielen Dank

Tim Wetterau B.Sc.

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Angewandte Computer- und Biowissenschaften

T +49 (0) 3727 58-1752
@ wetterau@hs-mittweida.de
www.cb.hs-mittweida.de

Haus 8 | Richard-Stücklen Bau| Raum 8-303
Am Schwanenteich 6b| 09648 Mittweida

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de