



Betriebssysteme Windows Logs und Accounts

Autor: Ronny Bodach, Tim Wetterau Stand: 23.05.2024



Bundeskriminalamt



Agenda

- 1. Ereignisanzeige
- 2. EVT- und EVTX-Dateiformat
- 3. Zeit- und Zugriffsanalyse
- 4. Logging von Anwendungsausführungen
- 5. Laufwerkszugriffe



Windows Logging Ereignisanzeige

Ereignisanzeige

🛃 Ereignisanzeige		- 🗆 ×
Datei Aktion Ansicht ?		
🔶 🧼 🙍 📰 🚺 🖬		
 Ereignisanzeige (Lokal) Benutzerdefinierte Ansichten Administrative Ereignisse Windows-Protokolle Anwendung 	Sicherheit Anzahl von Ereignissen: 14.608 Schlüsselwörter Datum und Uhrzeit Quelle Überwachung erfolgreich 14.03.2022 09:15:50 Microsoft Windows Überwachung erfolgreich 14.03.2022 09:15:50 Microsoft Windows Überwachung erfolgreich 14.03.2022 09:15:50 Microsoft Windows	Aktionen Sicherheit Sicherheit
 Sicherheit Installation System Weitergeleitete Ereignisse Anwendungs- und Dienstprotokolle AESMService Hardware-Ereignisse IntelAudioServiceLog Internet Explorer Enovo Microsoft Microsoft Microsoft Office Alerts OneApp_IGCC OpenSSH Admin Operational Schlüsselverwaltungsdienst Windows PowerShell Abonnements 	Uberwachung erfolgreich 14.03.2022 09:15:50 Microsoft Windows Überwachung erfolgreich 14.03.2022 09:15:50 Microsoft Windows Überwachung erfolgreich 14.03.2022 09:15:49 Microsoft Windows Serie in 5270 Microsoft Windows Serie in 5270 Microsoft Windows Serie in 5270 Microsoft Windows	Benutzerdefinierte Ansicht importieren Protokoll löschen Aktuelles Protokoll filtern
	Allgemein Details Die Anmeldeinformationen in der Anmeldeinformationsverwaltung wurden gelesen.	 Eigenschaften Suchen Alle Ereignisse speichern unter Aufgabe an dieses Protokoll anfügen
	Antragsteller: Sicherheits-ID: DESKTOP-5MHG39V\fische11 Kontoname: fische11 Kontoname: DESKTOP_5MHG20V	Ansicht Aktualisieren Hilfe
	Protokollname: Sicherheit Quelle: Microsoft Windows security i Protokolliert: 14.03.2022 09:15:50 Ereignis-ID: 5379 Aufgabenkategorie: User Account Manage Ebene: Informationen Schlüsselwörter: Überwachung erfolger Benutzer: Nicht zutreffend Computer: DESKTOP-5MHG39V Vorgangscode: Info Veitere Informationen: Onlinehilfe	 Finite Ereignis 5379, Microsoft Windows security aud Ereigniseigenschaften Aufgabe an dieses Ereignis anfügen Kopieren Ausgewählte Ereignisse speichern Aktualisieren Hilfe



Ereignisanzeige

- Protokollierung von Ereignissen und Fehlern
- Zielgruppe: Admins
- geeignet um Anwendernutzungsprofil zu erstellen
 - Computernutzungszeiten (alle logs)
 - WLAN-Verbindungen (DHCP-Client)
 - Dateienlöschung (NTFS-Log)
 - Netzwerkshare (SMB-Client, SMB-Server)
 - angeschlossene Geräte



Windows Logging EVT und EVTX

Windows Logging

- Das Logging bei Windows unterscheidet sich fundamental vom Logging unter anderen Betriebssystemen wie etwa UNIX
 - Keine Textdateien mit beschreibenden Einträgen
 - Führen von binäre Log Dateien mit einzelnen Eventcodes
- Verschiedene Formate:
 - Bei Windows 2000, XP und 2003 wird das Event Log in EVT-Dateien abgelegt.
 - Seit Windows Vista wurde das Format auf das Windows XML Event Log im EVTX-Format geändert.





EVT-Dateien

- Die Log Dateien sind in: %System%\system32\config abgelegt. Bei Windows 2000,XP und 2003 gibt es drei Log Dateien:
 - Application.evt
 - System.evt
 - Security.evt
- Bei den Server Betriebssystemen kommen folgende wichtige Log Dateien hinzu :
 - DNS Server.evt
 - Directory Service.evt
 - File Replication Service.evt



EVT-Dateien - Aufbau der Log Dateien

- Zwei Teile: Header und Body
- Body besteht aus:
 - Event Records
 - Cursor Record
 - freiem Speicher
 - \rightarrow Body = Ringspeicher
 - → ist dieser voll, wird der älteste Eintrag vom neuesten überschrieben
 - → Sollte noch freier Speicher existieren, so kann dieser ausgenullt sein, Slack enthalten oder mit Padding gefüllt sein.



Bundeskriminalamt



EVTX-Dateien

- Ab Windows Vista wurde das EVT-Log durch das Windows XML Event Log, kurz EVTX-Format, ersetzt.
- Bei Windows Vista, Windows 7, Windows 8 und Windows 10 liegen die Log Dateien in:

%SystemRoot%\system32\winevt\logs

- Es gibt wesentlich mehr Log Dateien (Win 7 > 60; Win 10 > 250)
 - Application.evtx
 - System.evtx
 - Security.evtx

• • • • • •



EVTX-Dateien

- Log-Dateien, welche im forensischen Kontext von Interesse sein können
 - HardwareEvents.evtx

.

- InternetExplorer.evtx
- Microsoft-Windows-TerminalServices-LocalSessionManager%40perational.evtx
- Microsoft-Windows-PowerShell%40perational,evtx
- Microsoft-Windows-TerminalServices-RemoteConnectionManager%40perational.evtx

11 Betriebssysteme / Windows Logs und Accounts | Tim Wetterau, B.Sc. (C) 23.05.2024 Hochschule Mittweida



- EVTX-Dateien bestehen aus File Header und mehreren folgenden Chunks
- Jeder Chunk enthält einen Chunk Header und mehrere Records
- nach den Records kann ein Slack folgen.





- Der EVTX File Header ist immer 4096 Bytes lang
 - es werden aber nur die ersten 128 Byte verwendet
 - Header hat folgenden Aufbau:

Offset	Größe	Beschreibung		
0x0000	8	Signatur 'ElfFile'		
0x0008	8	Ältester Chunk		
0x0010	8	Aktueller Chunk		
0x0018	8	Nummer des nächsten Records		
0x0020	4	Länge des verwendeten Headers in Bytes (immer 0x80)		
0x0024	2	Minor Version (immer 1)		
0x0026	2	Major Version (immer 3)		
0x0028	2	Länge des Headers in Bytes (immer 0x1000)		
0x002A	2	Anzahl der Chunks		
0x002C	76	Unbekannt (ausgenullt)		
0x0078	4	Flags		
0x007C	4	Prüfsumme		



- Ein Chunk ist immer 64 KiB groß
- Jeder Chunk hat eine Signatur '**ElfChnk**'
- Der Chunk Header ist wie folgt aufgebaut:

Offset	Größe	Beschreibung
0x0000	8	Signatur 'ElfChnk'
0x0008	8	Nummer des ersten Log Records
0x0010	8	Nummer des letzten Log Records
0x0018	8	Nummer des ersten File Records
0x0020	8	Nummer des letzten File Records
0x0028	4	Offset Tabelle (immer 0x80)
0x002C	4	Offset des letzten Records
0x0030	4	Offset des nächsten Records
0x0034	4	Prüfsumme über die Daten
0x0038	68	Unbekannt
0x007C	4	Prüfsumme über den Header
0x0080	64x4	String Table
0x0180	32x4	Template Table



• Jeder Event Record hat wieder einen Header. Der ist wie folgt aufgebaut:

Offset	Größe	Beschreibung
0x0000	4	Signatur 0x2a, 0x2a, 0x00, 0x00
0x0004	4	Record Länge in Byte
0x0008	8	Nummer des Records
0x0010	8	Time Created Zeitstempel
var.	var.	Binär XML Stream
var.	4	Record Länge in Byte



- Die EVTX-Logs können, wie die EVT-Logs mit bestimmten Viewern Menschenlesbar dargestellt werden. Bei EVTX-Logs ist dabei auch eine Darstellung in XML möglich:
- XML-Schema nach der Dekodierung:

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider Name="EventLog" /> <EventID Qualifiers="32768">6013</EventID> <Level>4</Level> <Task>0</Task> <Keywords>0x8000000000000/Keywords> <TimeCreated SystemTime="2019-12-21T14:38:40.938225200Z" /> <EventRecordID>17189</EventRecordID> <Channel>System</Channel> <Security /> </System> <EventData> <Data>720306</Data> <Data>60</Data> <Data>-60 W. Europe Standard Time</Data> </EventData> </Event>



- Die Binäre XML-Kodierung erfolgt in 3 Schritten:
 - Tokenisierung und Binarisierung
 - Schritt Substitution
 - Schritt Templates



1. Tokenisierung und Binarisierung

• aus

- <EventID>1234</EventID>
- wird
 - *#OpenStartElementTag#*
 - EventID
 - *#CloseStartElementTag#*
 - 1234
 - *#EndElementTag#*

Value	Meaning	Example
0x00	EndOfBXmlStream	
0x01	OpenStartElementTag	< name >
0x02	CloseStartElementTag	< name >
0x03	CloseEmptyElementTag	< name />
0x04	EndElementTag	
0x05	Value	attribute = "value"
0x06	Attribute	attribute = "value"
0x0c	TemplateInstance	
0x0d	NormalSubstitution	
0x0e	OptionalSubstitution	
0x0f	StartOfBXmlStream	



2. Schritt Substitution

- Strings die komprimiert dargestellt werden können, werden durch entsprechende Formate substituiert.
- Beispiel:
 - <EventID>1234</EventID>
 - 1234 (integer)
- Aus 4 Byte String 1234 wird ein 2 Byte unsigned Int.



3. Schritt Templates

- Oft ähneln sich aufeinanderfolgende Events, dann werden nur die Unterschiede zum vorherigen Event gespeichert
 - Bspw. nur der Zeitstempel, wenn dieser das einzige Attribut ist, was sich geändert hat

Hinweis: Eine manuelle Dekodierung ist sehr mühsam, aber bei gecarvten Fragmenten teils unumgänglich.



- Die EVT- und EVTX-Log Einträge enthalten nur sehr wenig menschenlesbaren Kontext
 - werden erst durch Viewer verständlich
 - variable Daten werden aus den Event Records mit vordefinierten Log Templates extrahiert
 - Nutzen System-DLLs und EXEs als Ressourcen zur EventID-Auflösung
 - Bspw. Mittels Microsoft Event Viewer

→ DLLs, die das Message Template enthalten, müssen gefunden werden
 → Sonst kann Zuordnung von EventID zu Ereignis nicht stattfinden
 → Zuordnung von Event nach DLL geschieht über die Registry



• Windows (mindestens ab NT4) verwaltet eine Liste der Ereignisprotokollanbieter in der Registry unter dem Schlüssel:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\

 Dieser Schlüssel enthält einen Unterschlüssel pro Protokolltyp (z. B. System) und Protokollquelle (z. B. Workstation):

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\System\



- Dieser Unterschlüssel enthält einen Wert mit dem Namen EventMessageFile
- Dieser Wert enthält einen oder mehrere Dateinamen, z.B.
 %SystemRoot%\System32\netmsg.dll





- Vorlagen f
 ür Ereignisnachrichten werden in "Message-Table Ressource" Dateien gespeichert
 - = ausführbare PE/COFF-Dateien mit Ressourcenabschnitt (".rsrc")
 - Eine Ressource im Ressourcenabschnitt der Dateien sollte eine Message-Table Ressource sein, wie im Folgenden unter Nutzung des Ressource Hackers gezeigt.







25 Betriebssysteme / Windows Logs und Accounts | Tim Wetterau, B.Sc. (C) 23.05.2024 Hochschule Mittweida



Beispiel Windows XP

- Unter Windows XP lautet die entsprechende Ereignismeldungszeichenfolge, wenn die Nachrichtenressource die Datei C:\Windows\System32\netmsg.dll ist und die Ereigniskennung 3260 (0x00000cbc) lautet:
 - Dieser Computer wurde erfolgreich mit %1 '%2' verbunden.
- Hier sind **%1** und **%2** Platzhalter, die auf die erste und zweite Zeichenfolge im entsprechenden Ereignisprotokoll verweisen. Die tatsächliche Reihenfolge der Zeichenfolgen in der formatierten Zeichenfolge hängt von der Grammatik der Sprache ab, in der die Nachrichtenzeichenfolge generiert wird.



Beispiel Windows XP

- Wenn eine Ressourcendatei gelöscht wird, geht die Bedeutung aus dem Log Eintrag verloren
- wenn die entsprechende Komponente nicht installiert ist, kann eine Nachricht nicht korrekt angezeigt werden.
- Dies wird durch folgende Ausgabe des Event Viewers dann deutlich:
 - "The description for Event ID 10016 from source Microsoft-Windows-DistributedCOM cannot be found."
- → In diesem Fall kann eine korrekte Darstellung nur mit der korrekten Ressource Datei erfolgen.



- Dazu kann man verschiedene Möglichkeiten nutzen:
 - Untersuchung der Event Logs im Live System
 - Virtualisierung des Asservates und Untersuchung des Event Log im virtualisierten System
 - Extraktion der Ressourcendateien und Registry Informationen auf das Untersuchungssystem

 - Recherche der EventID im Internet für die entsprechende Anwendung



Hinweis

Die EventID der Standard Microsoft Installationen können auf einem Windows Untersuchungssystem in der Regel korrekt dargestellt werden. Hier sollte es keine Probleme mit fehlenden Ressourcen Dateien geben. Sollten Server Betriebssysteme ausgewertet werden, kann dies jedoch bei einzelnen Server Diensten bereits zu fehlenden Log Darstellungen führen!



• Software zur Einsicht von Log Dateien im Live System findet sich unter:

Systemsteuerung \rightarrow System \rightarrow Verwaltung \rightarrow Ereignisanzeige

- → kann auch genutzt werden, um Event Logs vom untersuchten Asservat darzustellen
- Mögliches Tool: Log2Timeline/Plaso
 - Erstellung von Timelines mit den Standard Events von Microsoft Produkten
 - Plaso nutzt dazu eine eigene Ressource Table Datenbank.
 - https://github.com/log2timeline/plaso
- Es gibt noch einige **weitere Tools** zum Einsehen der Event Logs:
 - LogParser
 - Event Log Explorer
 - LOGAlyze

Windows Logging Zeit- und Zugriffsanalyse

Zeit- und Zugriffsanalysen - Eventlogs

- Uber die Eintragungen in die Event Log Dateien können Feststellungen unter anderem darüber getroffen werden, ob ein **Computer** zu einer **bestimmten Zeit aktiv** war oder nicht.
- Es können fundamentale Aussagen über das Starten und Herunterfahren von Computern festgestellt werden.
- Es können Eintragungen ermittelt werden, die beweisen, dass die Uhrzeit auf dem aktuellen Stand war, zu einem fraglichen Zeitpunkt, mit Hilfe der **Event Eintragungen** zu NTP Diensten.



Zeit- und Zugriffsanalysen - Eventlogs

- Die Event Log Eintragungen enthalten zudem Hinweise auf Dienst Start und Beendigungen. Dies kann hilfreich sein, bei der Feststellung ob bestimmte Malware bestimmte Dienste deaktiviert hat.
- Das Event Log beinhaltet unter anderem auch Events zu dessen Löschung, sofern das Event Log manuell zu einem bestimmten Zeitpunkt gelöscht wurde.





Last Login und Last Password Change

- Listet die lokalen Konten des Systems mit den folgenden Eigenschaften auf:
 - zugehörige SID
 - Zeitpunkt der Passwortänderung
- Speicherort
 - C:\windows\system32\config\SAM
 - SAM\Domains\Account\Users

→ nur die letzte Anmeldezeit und der letzte Zeitpunkt des Passwortwechsel werden gespeichert



Last Login und Last Password Change



SAM im WRR Registry Viewer angezeigt



Success/Fail Logons

- Ermitteln der Konten, welche für Anmeldeversuche verwendet wurden. Verfolgung der Kontonutzung für bekannte oder kompromittierte Konten.
- Speicherort
 - Win7/8/10:%system root%\System32\winevt\logs\Security.evtx
- Interpretation
 - 4624 Successful Logon
 - 4625 Failed Logon
 - 4634 | 4647 Successful Logoff
 - 4648 Logon using explicit credentials (Runas)
 - 4672 Account logon with superuser rights (Administrator)
 - 4720 An account was created


Logon Typen

- Anmeldeereignisse können sehr genaue Informationen über folgende Daten geben
 - Datum
 - Uhrzeit
 - Benutzername
 - Hostname
 - Erfolgs- / Fehlerstatus
 - Art/Weise des Anmeldversuchs

→ Interpretation der EventID 4624 Eintragungen (nächste Folie)



Logon Typen - Interpretation

- 2 Logon via console
- 3 Network Logon
- 4 Batch Logon
- 5 Windows Service Logon
- 7 Credentials used to unlock screen

- 8 Network logon sending credentials (cleartext)
- 9 Different credentials used than logged on user
- 10 Remote interactive logon (RDP)
- 11 Cached credentials used to logon
- 12 Cached remote interactive (similar



Remote Desktop Protocol Usage

- Speichert Remote Desktop Protocol Logons im Event Log des Ziel Computers.
- Speicherort
 - Win7/8/10: %system root%\System32\winevt\logs\Security.evtx
- Interpretation
 - Win7/8/10
 - Event ID 4778 Session Connected/Reconnected
 - Event ID 4779 Session Disconnected
 - Event log enthält Hostname und IP-Adresse des Remote Computers, der die Verbindung aufbaut





Services / Dienste im Event Log

- Durch Analysieren der Protokolle auf verdächtige Dienste, die zum Startzeitpunkt ausgeführt werden, können Hinweise auf Malware festgestellt werden
- Überprüfungs- und Schutzdienste werden dabei eventuell um die Zeit eines vermuteten Angriffes gestartet oder gestoppt.
- Speicherort
 - Win7/8/10: %system root%\System32\winevt\logs\System.evtx
- Interpretation
 - Nächste Folie



Services / Dienste im Event Log

- Eine große Menge von Malware und Würmern in freier Wildbahn nutzt Dienste.
- Beim Booten gestartete Dienste deuten auf Advanced Persistent Threads hin.
- Dienste können aufgrund von Angriffen wie Prozess Injection abstürzen.

- 7034 Service crashed unexpectedly
- 7035 Service sent a Start/Stop control
- 7036 Service started or stopped
- 7040 Start type changed (Boot | On Request | Disabled)
- 7045 A service was installed on the system (Win2008R2+)
- 4697 A service was installed on the system (from Security log)



Logging von Anwendungsausführungen

UserAssist

- Vom Desktop aus gestartete GUI-basierte Programme werden im Launcher auf einem Windows-System nachverfolgt.
- Speicherort
 - NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\U serAssist\{GUID}\Count
- Interpretation
 - Alle Eintragungen sind ROT-13 Encoded
 - 75048700 Active Desktop (Windows XP)
 - CEBFF5CD Executable File Execution (Windows 7/8/10)
 - F4E57C4B Shortcut File Execution (Windows 7/8/10)





UserAssist

🔁 NTUSER 44.DAT		
☆ Common tasks	🕒 🔯 🖗 🕹 🔎 🗭 💥	
Export to REGEDIT4 format	Value	Тире
🔚 Save Report	Turged Patho	REG_BINARY
Explorer tasks	User Shell Folders	REG_BINARY
Section File Information	Berlassist 👪 (0139Q44R-6NSR-49S2-8690-3QNSPNR6SS08)\Nppffbevtf\qvfcynlfjvgpu.yax	REG_BINARY
> County Docords	🖮 🧰 (CEBFF5CD-ACE2-4F4F-: 🚟 (0139Q44R-6NSR-49S2-8690-3QNSPNR6SS08)\Npprffbevrf\Pnyphyngbe.yax	REG_BINARY
es security Records	Count 🔐 (0139Q44R-6NSR-4952-8690-3QNSPNR6SS08)\Npprffbevrf\Fgvpxl Abgrf.yax	REG_BINARY
😻 SAM	🖶 🧰 (F4E57C4B-2036-45F0-A 🗱 (01390.44F-6NSF-4852-8690-30NSPNR6S508NNppr/fbevr/NFavccvat Gbby.yax	REG_BINARY
👔 Windows Installation	Count	REG_BINARY
💓 Hardware	General VisualEffects General VisualEffect General VisualEffects General Visual	REG_BINART
Billeer Data	Wallpapers Wellpapers W	REG BINARY
Cser Data	Group Policy Group Policy Group Policy (0.775677.2920.44P2.04D154M0156M0154M0154M0164M0142) (0.775677.2920.44P2.04D154M0154M0154M0154M0142)	BEG BINARY
Startup Applications	HomeGroup Haze FGYPENPEharnohe Haze FGYPENPEharnohe	BEG BINABY
🛞 Services and Drivers		REG BINARY
Network Configuration	Internet Settings	REG BINARY
	WL MUL	REG BINARY
Windows Firewall Settings		-
🔮 Environment	- BADAR Original	
🛅 Shell Folders	- Run [N 7755077-2820-44P3-N6N2-N0N601054N51]\Nppcffbey	rf
🗐 Outlook Express	- RunOnce	
Barri Data	Screensavers	
💥 haw Data	🖶 🧰 Shell Extensions	
	🕀 🧰 Sidebar	
	🕀 🧰 Telephony	
	- 🗀 ThemeManager	
	🕀 🧰 Themes	
	😥 🧰 WinTrust	
	- 🖻 DWM	
	🕀 🧰 Shell 🗸 🗸	
	Result Panel	
	Key	
	Verschiebung / Rotation	
	13	
	Kodiert	
		0.5
	Search Log	25
	Key Path CMI-CreateHive(6A1C4018-979D-4291-A7DC-7AED1C	
/indows NT Registry 1553 keys lo	oaded C:\temp\xwf\temp\NTUSER 44.DAT	

UserAssist in WRR und decodiert extern





Open/Save Most Recent Used

- Verfolgung von Dateien, die in einer Windows-Shell-Dialogbox geöffnet oder gespeichert wurden.
 - Generiert demnach eine Menge an Daten
 - Monitored alle Daten die aus Webbrowsern kommen
 - Und die Mehrheit an täglich genutzten Anwendungen

Speicherort

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ ComDlg32\ OpenSaveMRU (Windows XP)
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ ComDlg32\OpenSavePIDIMRU (Windows 7/8/10)



Open/Save Most Recent Used

- Interpretation
 - der "*" key Dieser Subkey enthält die meistgenutzten Dateien einer OpenSaveDialogbox
 - .??? die drei Buchstaben-Extension enthalten die meistgenutzten Dateien einer OpenSaveDialogbox für eine spezifische Dateinamenerweiterungen
 * Reistierung-Edit
 * Reistierung-Edit
 * Die Berbeite Ansich Faurte Hife

tei	Bearbeiten	Ansich	t Favo	riten Hilfe															
mpu	ter\HKEY_C	URRENT_	USER\S	OFTWARE\Microsoft\	Win	dows\Curren	tVersion	Explore	r\ComD	lg32\Op	penSave	PidIMRU	J\docx						
		· • • • • • • • • • • • • • • • • • • •	ComDig CIDS Firstf Last\ Last\ Oper	₁₃₂ izeMRU folder fisitedPidIMRU fisitedPidIMRULegacy sSavePidIMRU	Â	Name (Standar 0 1 MRUList Sinänyett bea	rd) :Ex	Typ REG REG REG REG	_SZ _BINARY _BINARY _BINARY	, ,	Dater (Wert 14 00 3a 00 01 00	n nicht fe 1f 50 e0 1f 41 62 00 00 00	estgelegt 4f d0 20 fd 86 5d 00 00 0	t)) ea 3a 69 d e3 24 5 0 ff ff ff f	9 10 a2 o 0 49 a7 o ff	18 08 0 2 55 b	0 2b 6 c7	30 2a	
			e) is	ocx e g libx]	Vertname: 0 Vert: 00000158	00	00	00	80	96	98	00	54				T	
			m m pr pr pr pr pr pr pr pr pr pr pr pr pr	isi isix ipn iff obt obt t t t sx p		00000160 00000168 00000170 00000178 00000188 00000188 00000190 00000198 00000198	00 00 03 6E 6E 00 BE 93 00	72 63 00 10 65 20 5C 7C 2E 00	00 00 00 00 74 54 00 58 00 90	79 6B 18 00 4A 72 65 09 00 00 00	00 00 00 72 61 73 00 8F 00 8F	48 4D 99 20 74 74 04 99 F1 00	00 00 58 50 65 00 58 19 АА	61 65 31 DD 65 6F 72 EF DD 00 00		r.y c.k J etr Te \ X.	. . / . / . /	Ηα Η 	~
1				-)												OK		Abbrec	:hen





 \sim

Last-Visited Most Recent Used

- Anwendungsdateien (EXE) die zum letzten Öffnen der Dateien in OpenSaveMRU Schlüssel genutzt wurden
- Des Weiteren enthält der Eintrag den letzten Dateipfad, der von dieser Anwendung aufgerufen wurde.
- Beispiel Notepad.exe wurde das letzte Mal gestartet vom Verzeichnis C:\Users\Rob\Desktop

Speicherort

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDl g32\LastVisitedMRU (Windows XP)
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDl g32\LastVisitedPidIMRU (Windows 7/8/10)





Shell Bags

- Enthält Informationen, auf welche Ordner Lokal, im Netzwerk und auf Wechselspeichermedien zugegriffen wurde.
- Gibt Hinweise auf bereits gelöschte oder überschriebene Verzeichnisse, sowie deren Zugriffszeitpunkt + ggf. wann auf diese zugegriffen wurde

Speicherort

- Explorer Zugriff:
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
- Desktop Zugriff:
- NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
- NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags



Recent Dateien

- Registrierungsschlüssel, der die zuletzt geöffneten Dateien und Ordner protokolliert
- Wird zum Erstellen der Liste "Zuletzt verwendet" des Startmenüs verwendet

• Speicherort

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
- Interpretation
 - RecentDocs Mit dem Gesamtschlüssel wird die Gesamtreihenfolge der letzten 150 geöffneten Dateien oder Ordner nachverfolgt..
 - .??? In diesem Unterschlüssel werden die zuletzt geöffneten Dateien mit einer bestimmten Erweiterung gespeichert.
 - Folder In diesem Unterschlüssel werden die zuletzt geöffneten Ordner gespeichert.





Recent Dateien

NTUSER 44.DAT -----**Common tasks** 🕒 🖾 🛛 🖀 🖧 🔎 🛸 Export to REGEDIT4 format. 🖭 🛄 UUUpen Value Data Type 🗟 🧰 Clsid 80 🛤 Report. REG BINARY 64 00 61 00 74 00 65 00 72 00 65 00 73 00 65 00 74 00 2E 00 62 00 61 00 74 00 2E 00 74 00 78 00. E ComDia32 MRUListEx REG. BINARY 05 00 00 04 00 00 03 00 00 02 00 00 00 01 00 00 00 00 00 00 FF FF FF FF Explorer tasks Discardable 22 1 REG_BINARY 44 00 61 00 72 00 73 00 74 00 65 00 6C 00 6C 00 75 00 6E 00 67 00 20 00 75 00 6E 00 64 00 20 0. Section 10 File Information ExtractionWigard 2 2 3 REG_BINARY 53 00 79 00 73 00 74 00 65 00 6D 00 20 00 75 00 6E 00 64 00 20 00 53 00 69 00 63 00 68 00 65 0. 🔄 🧰 FileExts As Security Records REG_BINARY 41 00 6E 00 7A 00 65 00 69 00 67 00 65 00 00 00 5E 00 32 00 00 00 00 00 00 00 00 00 00 00 41 6. LowRegistry 22 4 REG_BINARY 🐑 SAM 4E 00 65 00 74 00 7A 00 77 00 65 00 72 00 68 00 20 00 75 00 6E 00 64 00 20 00 49 00 6E 00 74 0. iii. iiii MenuOider REG RINA 74 00 65 00 61 00 6D 00 63 00 69 00 72 00 63 00 6C 00 65 00 2E 00 61 00 69 00 00 00 70 00 32 1 7. Windows Installation 🖲 🦲 Modules 1 Data View _ \times 😸 🚞 MountPoints2 Hardware NewShortcutHandlers User Data 2 Value name - RecentDocs Startup Applications 5 is. 🚞 ia. 💼 Services and Drivers REG BINARY Summan Folder Network Configuration RunMRU Position 001 0203 0405 0607 0809 0A0B 0C0D 0E0F 0123456789ABCDEF Windows Firewall Settings E SearchPlatform Start Offset 7400 6500 6100 6D00 6300 6900 7200 6300 H.e.a.m.c.i.r.c. Environment Shell Folders Position 0x10 6C00 6500 2E00 6100 6900 0000 7000 3200 1.e...a.i...p.2. StartPage Selection 0 0x20 0000 0000 0000 0000 0000 7465 616D 6369teamci Shell Folders StartPage2 Numbers 0x30 7263 6065 2E61 692E 606E 6B00 5000 0800 rcle.ai.lnk.P... Callook Express 🖲 🧰 Streams Signed 8 116 0x40 🛃 Raw Data Unsigned 8 116 0x50 StuckRects2 116 Signed 16 0x60 0000 0000 0000 7400 6500 6100 6D00 6300t.e.a.m.c. Taskband 116 Unsigned 16 0x70 6900 7200 6300 6000 6500 2200 6100 6900 i.r.c.l.e...a.i. TypedPaths 6619252 Signed 32 0x80 2E00 6C00 6E00 6B00 0000 2000 0000 ..l.n.k... ... User Shell Folders 6619252 Unsigned 32 💩 🧰 UserAssist 30681189079908468 Signed 64 VisuaEffects Float 32 0,00 Walpapers
 Walpaper 0.00 Float 64 Group Policy Datetime 🖶 🦲 HomeGroup WIN 64 24.03.1698 08:44:52 UNDX 32 18.03.1970 14:40:52 🐵 🧰 ime DOS 32 05.03.1980 00:03:40 Result Panel Key Search Log Save data... Swap Endian Unicode Chars Unicode Big Endian OK Key Path CMI-CreateHive(6A1C4018-979D-4291-A7DC-7AED1C75 Windows NT Registry 1553 keys loaded C:\temp\xwf\temp\NTUSER 44.DAT

50 **Betriebssysteme / Windows Logs und Accounts** Perist Wetterau, B.Sc. Recent Files Eintragungen (C) 23.05.2024 Hochschule Mittweida





- Von Windows automatisch erstellte Verknüpfungsdateien
- Verlaufsdateien zur Verknüpfung
- Beim Öffnen von lokalen und Remote-Datendateien und -dokumenten wird eine Verknüpfungsdatei (.lnk) erstellt.
- Speicherort
 - C:\%USERPROFILE%\Recent (Windows XP)
 - C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\ (Windows 7/8/10)
 - C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\ (Windows 7/8/10)
 - Beachten Sie, dass dies der primäre Speicherort von LNK-Dateien ist. Sie können aber auch an anderen Orten gefunden werden.



Interpretation

- Datum / Uhrzeit-Datei mit diesem Namen wurde zum ersten Mal geöffnet
 - Erstellungsdatum der Shortcut-Datei (LNK)
- Datum / Uhrzeit-Datei mit diesem Namen wurde zuletzt geöffnet
 - Datum der letzten Änderung der LNK-Datei (Shortcut)
- Daten der LNK-Target-Datei (interne LNK-Dateiinformationen)
 - Änderungs-, Zugriffs- und Erstellungszeiten der Zieldatei
 - Volume-Informationen (Name, Typ, Seriennummer)
 - Informationen zur Netzwerkfreigabe
 - Ursprünglicher Speicherort
 - Name des Systems

Hinweis:

- Es werden in den Recent Verzeichnissen auch Dokumente angezeigt, die sich niemals auf der analysierten Festplatte befunden haben!
- Möglicherweise können dadurch relevante Netzwerk-Shares identifiziert werden.
- LNK-Dateien sind eine sehr ergiebige Datenquelle, um die tatsächliche Nutzung des PCs nachzuvollziehen.





Target Attributes	A
Target File Size	10040
Show Window	SW_NORMAL
Target Created	23.02.2015 08:34:26 +1
Last Written	23.02.2015 08:34:26 +1
Last Accessed	23.02.2015 08:35:17 +1
ID List	Desktop\N:\Geheime Projekte\ C=23.02.2015 07:35:04 M=23.02.2015 07:35:36 ULTRA GEHEIMER VERTRAG.docx C=23.02.2015 07:34:26 M=23.02.2015 07:34:28 Size=10040
Network share name	\\BERSERKER2\Archiv
DriveLetter	N:
Target path	+
Working Directory	N:\Geheime Projekte
Known Folder Tracking	false
PROPERTYSTORAGE	{46588AE2-4CBC-4338-BBFC-139326986DCE}
Size	0
Host Name	berserker2
Host Name Volume ID	berserker2 {117F8236-FAB7-70BA-9187-DF8DD40CB2F0}

LNK Datei in X-Ways





Office Files Most Recent Used

- Ähnlich wie bei den Zuletzt geöffneten Dateien (Recent Dateien) werden hiermit die letzten Dateien nachverfolgt, die von jeder MS Office-Anwendung geöffnet wurden. Der letzte Eintrag, der gemäß der MRU hinzugefügt wurde, ist der Zeitpunkt, zu dem die letzte Datei von einer bestimmten MS Office-Anwendung geöffnet wurde.
- Speicherort
 - NTUSER.DAT\Software\Microsoft\Office\VERSION
 - 15.0 = Office 365
 - 14.0 = Office 2010
 - 12.0 = Office 2007
 - 11.0 = Office 2003
 - 10.0 = Office XP
 - NTUSER.DAT\Software\Microsoft\Office\<VERSION>\<APP>\UserMRU\LiveID_####\
 FileMRU

Prefetch Dateien

- Steigert die Leistung eines Systems, durch das Vorladen von Codepages häufig verwendeter Anwendungen
- Der Cache-Manager überwacht alle Dateien und Verzeichnisse, auf die für jede Anwendung oder jeden Prozess verwiesen wird, und ordnet sie einer *.PF-Datei zu.
 - auf 1024 Dateien beschränkt (unter XP und Win7 Begrenzt auf 128 Dateien)
 - Format: <exename>-<hash>.pf
- Speicherort
 - C:\Windows\Prefetch
- Interpretation
 - Jede *.pf-Datei enthält die letzte Ausführungszeit, die Häufigkeit der Ausführung sowie die vom Programm verwendeten Geräte- und Dateihandles
 - Erstmalige Ausführung der Anwendung = Erstellungszeit
 - Letzter Zeitpunkt der Ausführung der Anwendung = Änderungszeit

Bundeskriminalamt

Jump Lists

- Gestaltung der Windows 7-Taskleiste (Jump Lists) zum schnellen und einfachen Zugriff auf häufig oder kürzlich verwendete Elemente
- Kann nicht nur aktuelle Mediendateien umfassen, sondern auch aktuelle Tasks
- Im Ordner AutomaticDestinations gespeicherte Daten wird jeweils eine eindeutige Dateikennung mit AppID der zugeordneten Anwendung vorangestellt.
- Jede Datei ist separate LNK-Datei in numerischer Reihenfolge von (normalerweise) 1 - frühesten bis >=1 jüngsten

Speicherort

 C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\A utomaticDestinations (Windows 7/8/10)



Jump Lists

Interpretation

- Erstmalige Ausführung der Anwendung.
 Erstellungszeit = Erstes Element, das der AppID-Datei hinzugefügt wurde.
- Letzter Zeitpunkt der Ausführung der Anwendung mit geöffneter Datei.
 Änderungszeit = Zuletzt zur AppID-Datei hinzugefügtes Element.
- Liste der JumpList-IDs -> http://web.archive.org/web/20190427230518/http://www.forensicswi ki.org/wiki/List_of_Jump_List_IDs





Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F ANSI ASCII 00001210 80 40 20 C9 D2 29 D6 05 D0 01 FF FF FF FF 3D 00 €@ ÉÒ)Ö Ð ŸŸŸ 00001220 3A 00 3A 00 7B 00 30 00 33 00 31 00 45 00 34 00 :: { 0 3 1 E 4 00001230 38 00 32 00 35 00 2D 00 37 00 42 00 39 00 34 00 8 2 5 - 7 B 9 4 00001240 4C 00 00 01 14 02 00 00 00 00 00 C0 00 00 00 L À 00001250 00 00 00 46 83 00 00 00 20 20 00 00 A2 90 E4 D1 Ff c äÑ 00001260 D1 05 D0 01 A2 90 E4 D1 D1 05 D0 01 A2 90 E4 D1 Ñ Đ ¢ ãÑ Đ ¢ ãÑ 00001270 D1 05 D0 01 C2 0D 00 00 00 00 00 00 01 00 00 00 Ñ Đ Â 00001280 00 00 00 00 00 00 00 00 00 00 00 36 00 14 00 6 "{ÃM±léF'L 00001290 | 1F 42 25 48 1E 03 94 7B C3 4D B1 31 E9 46 B4 4C | B%H 000012A0 8D D5 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 Õ î»b# 000012B0 2F 92 1E 49 43 56 F4 4A A7 EB 4E 7A 13 8D 81 74 // ICVôJSENz t 000012C0 00 00 00 07E 00 00 00 1C 00 00 01 00 00 00 000012D0 1C 00 00 00 2D 00 00 00 00 00 00 00 7D 00 00 00 Î> 000012E0 11 00 00 00 03 00 00 00 1B 0F CE 3E 10 00 00 00 000012F0 00 43 3A 5C 55 73 65 72 73 5C 4A 6F 68 6E 20 44 C:\Users\John D 00001300 6F 65 5C 41 70 70 44 61 74 61 5C 52 6F 61 6D 69 oe\AppData\Roami 00001310 6E 67 5C 4D 69 63 72 6F 73 6F 66 74 5C 57 69 6E ng\Microsoft\Win 00001320 64 6F 77 73 5C 4C 69 62 72 61 72 69 65 73 5C 56 dows\Libraries\V 00001330 69 64 65 6F 73 2E 6C 69 62 72 61 72 79 2D 6D 73 ideos.library-ms 00001340 00 00 39 00 00 00 09 00 00 A0 2D 00 00 31 53 9 - 1S 00001350 50 53 55 28 4C 9F 79 9F 39 4B A8 D0 E1 D4 2D E1 PSU(LŸyŸ9K~ĐÁÔ-Á 00001360 D5 F3 11 00 00 07 00 00 00 00 0B 00 00 FF Õó ÿ 00001380 00 00 A0 58 00 00 00 00 00 00 00 77 69 6E 2D 70 х win-p 00001390 6E 32 32 6F 66 61 34 33 73 36 00 1C 5A 3F B9 BA n22ofa43s6 Z?¹⁰ 000013A0 33 41 4A 83 63 B6 73 4E 24 01 8F 3B F5 B2 D4 C4 3AJfc¶sN\$;õ°ÔÄ 000013B0 71 E4 11 BD E9 E8 2A EA 24 FD 46 1C 5A 3F B9 BA qā **é**\$\$\$F Z? ** 000013C0 33 41 4A 83 63 B6 73 4E 24 01 8F 3B F5 B2 D4 C4 3AJfc¶sN\$;0°ÔÄ 000013D0 71 E4 11 BD E9 E8 2A EA 24 FD 46 00 00 00 00 00 gä ** é* \$ v f 00001400 2D 00 34 00 44 00 43 00 33 00 2D 00 42 00 31 00 - 4 D C 3 - B 1 00001410 33 00 31 00 2D 00 45 00 39 00 34 00 36 00 42 00 3 1 - E 9 4 6 B 00001420 34 00 34 00 43 00 38 00 44 00 44 00 35 00 7D 00 4 4 C 8 D D 5 } 00001430 5C 00 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 \ D o c u m e n 00001440 74 00 73 00 2E 00 6C 00 69 00 62 00 72 00 61 00 ts.libra 00001450 72 00 79 00 2D 00 6D 00 73 00 62 A7 83 89 5F 8F r v - m s b\$ft 00001460 82 E0 1C 5A 3F B9 BA 33 41 4A 83 63 B6 73 4E 24 , à Z?1°3AJfc¶sN\$ 00001470 01 8F 39 F5 B2 D4 C4 71 E4 11 BD E9 E8 2A EA 24 95°ÔÄqä %éè*ê\$ 00001480 FD 46 1C 5A 3F B9 BA 33 41 4A 83 63 B6 73 4E 24 yr Z?¹°3AJfc¶sN\$

 Count
 7

 Rank
 18,40

7	11.11.2014 23:40:01,7 +1	C:\Users\John Doe\Documents\Amped FIVE\samples\frame-averaging- label	win- pn22ofa43s6	1,00
6	11.11.2014 23:39:13,1 +1	C:\Users\John Doe\Desktop\Amped	win- pn22ofa43s6	1,00
5	21.11.2014 23:37:02,7 +1	C:\Users\John Doe\Desktop	win- pn22ofa43s6	1,00
1	21.11.2014 22:57:37,6 +1	:: {031E4825-7B94-4DC3-B131-E946B44C8DD5}\Documents.library- ms	win- pn22ofa43s6	4,00
2	21.11.2014 22:57:37,6 +1	::{031E4825-7B94-4DC3-B131-E946B44C8DD5}\Pictures.library-ms	win- pn22ofa43s6	3,90
3	21.11.2014 22:57:37,6 +1	::{031E4825-7B94-4DC3-B131-E946B44C8DD5}\Music.library-ms	win- pn22ofa43s6	3,80
4	21.11.2014 22:57:37,6 +1	::{031E4825-7B94-4DC3-B131-E946B44C8DD5}\Videos.library-ms	win- pn22ofa43s6	3,70

Jump List

Jump List in X-Ways





Windows Logging Laufwerkszugriffe

Externe Laufwerke / Network Shares

- Eine wenig bekannte Tatsache über den IE-Verlauf ist, dass die in den Verlaufsdateien gespeicherten Informationen nicht nur mit dem Browsen im Internet zusammenhängen.
- Der Verlauf zeichnet auch den lokalen und Remote-Dateizugriff (über Netzwerkfreigaben / UNC Pfade) auf.
- So können Zugriffshistorien auf Dateien über längere Zeiträume ermittelt werden, auf welche Dateien und Anwendungen zugegriffen wurde.



Externe Laufwerke / Network Shares

- Speicherort
 - IE6-7

%USERPROFILE%\LocalSettings\History\History.IE5

– IE8-9

%USERPROFILE%\AppData\Local\Microsoft\WindowsHistory\History.IE5

– IE10-11

%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

- Interpretation
 - In index.dat gespeichert als: file: ///N:/directory/filename.ext
 - Bedeutet nicht, dass die Datei im Browser geöffnet wurde!



Key Identifizierung von USB-Geräten

→ Angeschlossene USB-Geräte werden in der Registry unter einem bestimmten Schlüssel gespeichert.

Speicherort:

- SYSTEM\CurrentControlSet\Enum\USBSTOR
- SYSTEM\CurrentControlSet\Enum\USB

Interpretation

- Identifiziert den Hersteller, das Produkt und die Version eines an einen Computer angeschlossenen USB-Geräts •
- Identifiziert ein eindeutiges USB-Gerät, das angeschlossen war ٠
- Speichert die Uhrzeit, zu der ein Gerät angeschlossen wurde ۲
- Geräte ohne eindeutige Seriennummer haben ein "&" im zweiten Zeichen der Seriennummer.

Bundeskriminalamt



First/Last Times von USB-Geräten

- First Time Plug und Play Log Files:
 - XP: C:\Windows\setupapi.log
 - Win7/8/10/..: C:\Windows\inf\setupapi.dev.log
- First, Last, und Removal Times: \CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####
 - 0064 = First Install (Win7-)
 - 0066 = Last Connected (Win8-)
 - 0067 = Last Removal (Win8-)

Interpretation

- Device Serial Number
- Log File Zeit ist Lokalzeit



Volume Serial Number

- > Ermitteln der Volume-Seriennummer der Dateisystempartition auf dem USB-Stick.
- > ACHTUNG: nicht die eindeutige USB-Seriennummer der Gerätefirmware!
- > Speicherort
 - HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ENDMgmt

Interpretation

- Berechnung aus dem Volume Name und der USB Unique Seriennummer:
- Auffinden der letzten Ganzzahl in der Zeile
- Konvertieren der dezimalen Seriennummern in hexadezimale Seriennummern
- Die Shortcut-Datei (LNK) enthält die Seriennummer und den Namen des Volumes.
- Der Registrierungsschlüssel RecentDocs enthält in den meisten Fällen den Namen des Volumes, wenn das USB-Gerät über den Explorer geöffnet wird.
- Wird in Systemen mit SSDs kaum verwendet, da Ready Boost dort stdm. Deaktiviert ist





Drive Letter und Volume Name

- Feststellung des Laufwerksbuchstaben beim letzten Anschluss an den Computer.
- > Speicherort:
 - SOFTWARE\Microsoft\Windows Portable Devices\Devices
 - SYSTEM\MountedDevices

> Interpretation:

- Identifizierung des USB-Gerätes, das zuletzt einem bestimmten Laufwerksbuchstaben zugeordnet wurde.
- > funktioniert nur für das zuletzt zugeordnete Laufwerk
- enthält nicht die historischen Aufzeichnungen aller Laufwerksbuchstaben, die Wechseldatenträger zugeordnet waren



LNK-Dateien im Zusammenhang mit externen Geräten

Von allen geöffneten lokalen und remote Datendateien werden Shortcuts Link sogenannte LNK-Dateien automatisch im Recent Verzeichnis des Benutzers angelegt

> Speicherort:

- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent
- %USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent

Interpretation:

- Änderungs-, Zugriffs- und Erstellungszeiten der Zieldatei
- Volume-Informationen (Name, Typ, Seriennummer)
- Informationen zur Netzwerkfreigabe
- Ursprünglicher Speicherort
- Name des Systems



LNK-Dateien im Zusammenhang mit externen Geräten

Für die Interpretation der LNK-Dateien im Zusammenhang mit externen USB-Geräten sind die Volume Informationen von größter Bedeutung.

Durch Kenntnis der Volume-Seriennummer und dem Volume-Namen können die Daten über die LNK-Datei-Analyse und den RECENTDOC-Schlüssel verknüpft und USB-Geräten eindeutig zugeordnet werden!



LNK-Dateien im Zusammenhang mit externen Geräten

Beispiel X-Ways – Kopieren von Dateien aus dem Netzlaufwerk auf den USB-Stick:

Name 🛋	T Beschreibung	т Тур	Hash ¹ (MD5)
🔲 🛄 💶 (Stammverzeichnis)	Stammverzeichnis, existier.		
Generic USB SD Reader, P1 (6)	Verzeichnis, existierend		
🗆 📄 Geheime_zeichnung.drw	Datei, existierend, kopiert	drw	299857EE22D03A3A34BA3EF13BBA62B3
🗆 📄 ULTRA GEHEIMER VERTRAG.docx	Datei, existierend, kopiert	docx	92BF9B5D91DEF99F655C1976B073749F
Boot-Sektor	Datei, virtuell (für Untersu		A7B09B900C4764D2D7645C40C7B55A7C
🗆 📄 FAT 1	Datei, virtuell (für Untersu		FA392474D8EBFD439A390575F7B757CA
🗆 📄 FAT 2	Datei, virtuell (für Untersu		FA392474D8EBFD439A390575F7B757CA
Stammverzeichnis [GB]	Ausschnitt, virtuell (für Un.		1987FC26246FCF1FAB3970A8D9403CC7

Inhalt USB Stick sichergestellt beim Beschuldigten

□ ▼Name▲	Beschreibung	🝸 Тур	Hash ¹ (MD5)	
Image: A start and the star	Verzeichnis, existierend, b			
🗆 🧰 . = Geheime Projekte (2)	Verzeichnis, existierend			
Geheime_zeichnung.drw	Datei, existierend	ascii	299857EE22D03A3A3	4BA3EF13BBA62B3
ULTRA GEHEIMER VERTRAG.docx	Datei, existierend	docx	92BF9B5D91DEF99F6	55C1976B073749F

Inhalt Netzlaufwerk N:\ auf Windows Server (Opfer)



LNK-Dateien im Zusammenhang mit externen Geräten

Beispiel X-Ways – Kopieren von Dateien aus dem Netzlaufwerk auf den USB-Stick:

□ ▼Name▲	Typ Beschreibung	Hash ¹ (MD5)
🗐 🧰 = Windows (4)	Verzeichnis, existierend, b	1
🗐 🦲 . = Recent (4)	Verzeichnis, existierend, b	1
📃 📄 Geheime Projekte.Ink	Datei, existierend, bereits Ink	015CFD50F62CCFB31B00124ABEFB8755
🔝 📄 Geheime_zeichnung.drw.lnk	Datei, existierend, bereits Ink	DE4D26F48DF3439141BB2DA771FF911E
📃 📄 SDCARD (I).lnk	Datei, existierend, bereits Ink	DE9859845BAA83296CC5633A979128F7
📃 📄 ULTRA GEHEIMER VERTRAG.docx.lnk	Datei, existierend, bereits Ink	6FD42A2AE3236A552F4AA45749202987

Inhalt Recent Verzeichnis Windows Client Maschine (Arbeitsplatz Beschuldigter)





LNK-Dateien im Zusammenhang mit externen Geräten

Beispiel X-Ways – Kopieren von Dateien aus dem Netzlaufwerk auf den USB-Stick:

A
10040
SW_NORMAL
23.02.2015 08:34:26 +1
23.02.2015 08:34:26 +1
23.02.2015 08:35:17 +1
Desktop\N:\Geheime Projekte\ C=23.02.2015 07:35:04 M=23.02.2015 07:35:36 ULTRA GEHEIMER VERTRAG.docx C=23.02.2015 07:34:26 M=23.02.2015 07:34:28 Size=10040
\\BERSERKER2\Archiv
N:
+
N:\Geheime Projekte
false
{46588AE2-4CBC-4338-BBFC-139326986DCE}
0
berserker2
{117F8236-FAB7-70BA-9187-DF8DD40CB2F0}
{00000902-0000-0000-0400-E81A00000000}

Recent Eintrag Datei: ULTRA GEHEIMER VERTRAG.docx

Target Attributes	A
Target File Size	35
Show Window	SW_NORMAL
Target Created	23.02.2015 08:33:32 +1
Last Written	23.02.2015 08:34:52 +1
Last Accessed	23.02.2015 08:35:29 +1
ID List	Desktop\N:\Geheime Projekte\ C=23.02.2015 07:35:04 M=23.02.2015 07:35:36 Geheime_zeichnung.drw C=23.02.2015 07:33:32 M=23.02.2015 07:34:54 Size=35
Network share name	\\BERSERKER2\Archiv
DriveLetter	N:
Target path	+
Working Directory	N:\Geheime Projekte
Known Folder Tracking	false
PROPERTYSTORAGE	{46588AE2-4CBC-4338-BBFC-139326986DCE}
Size	0
Host Name	berserker2
Volume ID	{117F8236-FAB7-70BA-9187-DF8DD40CB2F0}
Object ID	{00000902-0000-0000-0300-E81A00000000}

Recent Eintrag Datei: Geheime_zeichnung.drw



LNK-Dateien im Zusammenhang mit externen Geräten

Beispiel X-Ways – Kopieren von Dateien aus dem Netzlaufwerk auf den USB-Stick:

Target Attributes	(Directory)	Stammverzeichnis [GB]								Aus	schn	itt, v	irtue	ll (fü	ir Un.			1987FC				
Target File Size	0		Container	Date	i	Vorse	chau	D	etail	s	Gale	rie	Kale	ende	r L	.ege	nde			Sync	~ 🛔	4≡ 🖻
Show Window	SW_NORMAL		Offset 00000000	0 53	1 44	2 43	3 41	4 52	5 44	6 20	7 20	8 20	9 20	A 20	B 08	C 00	D 00	E 00	F 09	SDCARD	ANSI .	ASCII
Target Created	01.01.1980 00:00:00 +1		00000010	00	00	00	00	00	00	49	71	ЗA	46	00	00	90	00	00	00	_	Iq:F	
Last Written	01.01.1980 00:00:00 +1		00000020	43 FF	78 FF	00 FF	00 FF	00 FF.	FF FF	FF	FF FF	FF FF	FF FF	FF 00	0F 00	00 FF	A3 FF	FF FF	FF FF	Cx ÿ	799999 799999	£ÿÿ 0000
Last Accessed	01.01.1980 00:00:00 +1		00000040	02	52	00	20	00	56	00	45	00	52	00	OF	00	AЗ	54	00	R V	TE R	£T
ID List	Desktop\I:\		00000050	52 01	00 55	41	00 4C	47	00 54	2E	00 52	64 00	00 41	00	00 0F	6F 00	00 23	63 20	00	RAG	.d 'RA	ос •
Volume Type	Removable		00000070	47	00	45	00	48	00	45	00	49	00	00	00	4D	00	45	00	GEH	EI	ME
Volume Serial	0xDE6D7B78		00000080	55	4C	54	52 46	41	47	7E 4 F	31	44	4F	43	20	00	21	76	44	ULTRAG	-1DOC	!vD
Volume Name	SDCARD		000000A0	42	6E	00	75	00	6E	00	67	00	2E	00	OF	00	51	64	00	Bnun	ng.	Qd
Local Path	1:\		000000B0	72	00	77	00	00	00	FF	FF	FF	FF	00	00	FF	FF	FF	FF	rw	ŸŸŸŸ	ŸŸŸŸ
Known Folder Tracking	false		0000000D0	65	4/	5F	00	7A	00	65	00	69	00	00	00	63	00	68	00	e z	ei ei	Qm ch
PROPERTYSTORAGE	{46588AE2-4CBC-4338-BBFC-139326986DCE}		000000E0	47	45	48	45	49	4D	7E	31	44	52	57	20	00	24	76	44	GEHEIM	I~1DRW	\$vD
Size	0		000000F0 00000100	57	46 00	57 00	46 00	00 00	00	5B 00	44 00	57 00	46 00	03 00	00	23 00	00 00	00 00	00	WFWF	[DWF	#
Recent Fint	rag Verzeichnis/Gerät: SDCARD			 \			 chr				 	 		 C+i	 Iclu					tony		1

Recent cintrag verzeichnis/Gerat: SDCARD

Verzeichniseintrag FAT USB Stick: Root Directory


Laufwerkszugriffe auf USB Geräte

LNK Dateien im Zusammenhang mit externen Geräten

Beispiel X-Ways – Kopieren von Dateien aus dem Netzlaufwerk auf den USB Stick:

larget Attributes	(Directory)		
Target File Size	0		
Show Window	SW_NORMAL		
Target Created	01.01.1980 00:00:00 +1		
Last Written	01.01.1980 00:00:00 +1		
Last Accessed	01.01.1980 00:00:00 +1		
ID List	Desktop\I:\		
Volumo Typo	Removable		
volume rype	Removable		
Volume Serial	0xDE6D7B78		
Volume Serial Volume Name	0xDE6D7B78 SDCARD		
Volume Serial Volume Name Local Path	0xDE6D7B78 SDCARD		
Volume Type Volume Serial Volume Name Local Path Known Folder Tracking	OxDE6D7B78 SDCARD I:\ false		
Volume Serial Volume Name Local Path Known Folder Tracking PROPERTYSTORAGE	OxDE6D7B78 SDCARD I:\ false {46588AE2-4CBC-4338-BBFC-139326986DCE}		

Recent Eintrag Gerät: SDCARD

Offset	Bezeichnung	Wert
0	JMP instruction	EB 3C 90
3	OEM	MSDOS5.0
BIOS Parame	eter Block	
11	Bytes per sector	512
13	Sectors per cluster	64
14	Reserved sectors	4
16	Number of FATs	2
17	Root entries	512
19	Sectors (under 32 MB)	0
21	Media descriptor (hex)	F8
22	Sectors per FAT	242
24	Sectors per track	63
26	Heads	255
28	Hidden sectors	63
32	Sectors (over 32 MB)	3.962.817
36	BIOS drive (hex, HD=8x)	80
37	(Unused)	0
38	Ext. boot signature (29h)	29
39	Volume serial number (decimal)	3.731.716.984
39	Volume serial number (hex)	78 7B 6D DE
43	Volume label	NO NAME
54	File system	FAT16
510	Signature (55 AA)	55 AA

BootSector FAT USB Stick



Zusammenfassung

Zusammenfassung

Sie haben das EVT- bzw. das EVTX-Log vorgestellt bekommen und wie dieses aufgebaut ist.

Log Dateien bieten grundsätzlich wertvolle Informationen über Aktivitäten auf dem System. Es ist jedoch wichtig den Aufbau der Event Logs zu verstehen, da bei fehlenden Ressourcen Dateien, die Event Eintragungen möglicherweise nicht korrekt angezeigt werden.

Die Account Nutzung und die Recent Dateien geben neben den Event Logs einen Hinweis auf Aktivitäten im Betriebssystem wieder. Hierbei können Eintragungen von Programmstarts ebenso wie genutzte Dateien festgestellt werden. Die dazu notwendigen Informationen befinden sich verteilt zum großen Teil in der Registry aber auch in separaten Dateien mit spezifischem Aufbau.

Vielen Dank

Tim Wetterau B.Sc.

Hochschule Mittweida | University of Applied SciencesTechnikumplatz 17 | 09648 MittweidaFakultät Angewandte Computer- und Biowissenschaften

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

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



hs-mittweida.de