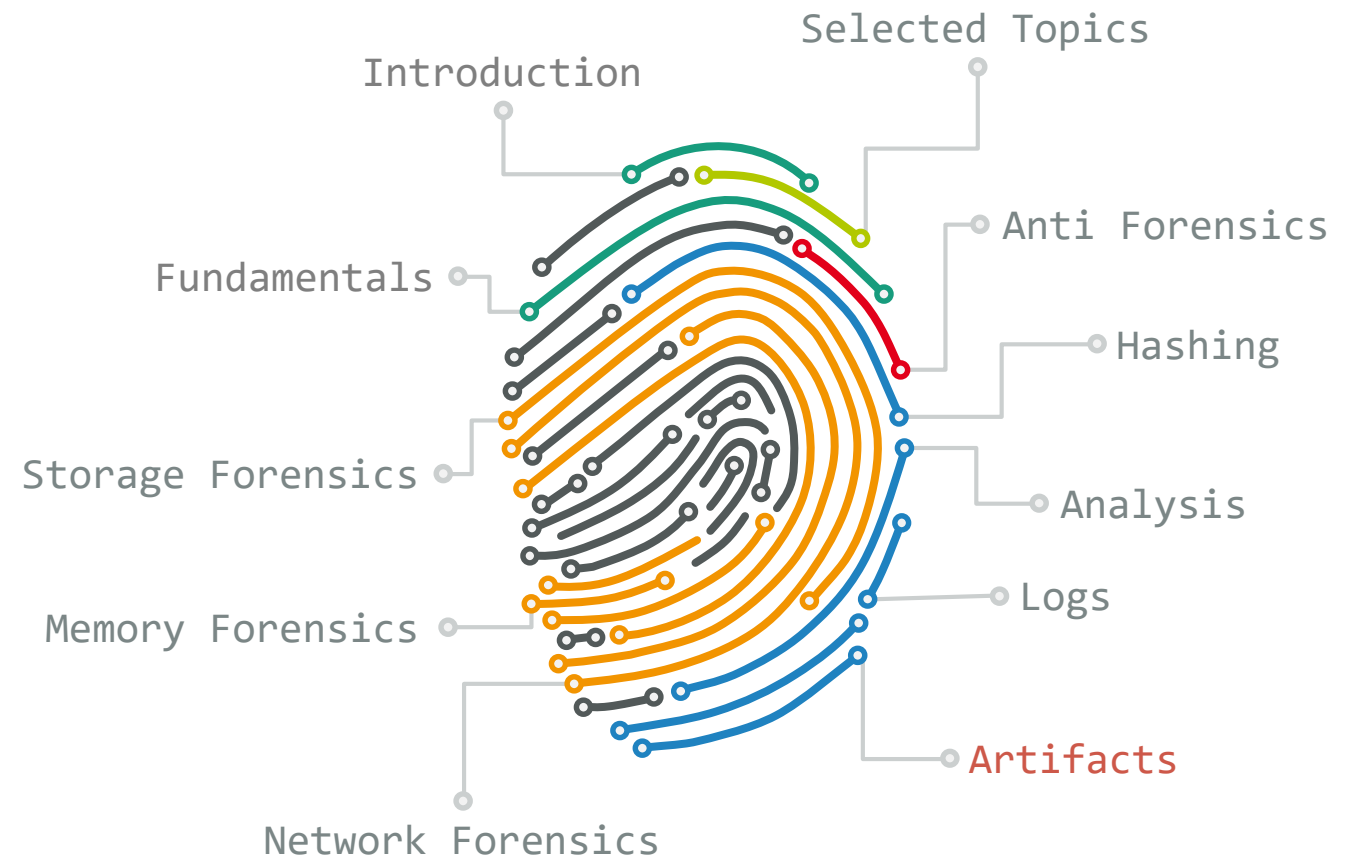


Prof. Dr. Elmar Padilla et al.

Digitale Forensik

06 - Artifacts



Artifacts


~/df/01-fundamentals

Artifacts

Actually, there are lots of different definitions.
In this lecture: **an addressable piece of data.**

A piece of data.

- Files
- Metadata
- Registry keys
- Database entries
- Network connections
- ...



Single pieces of a jigsaw puzzle.

An addressable piece of data.

Single pieces of a jigsaw puzzle.


~/df/01-fundamentals

Digital Evidence

„[...] digital evidence of an incident is any digital data that contain reliable information that supports or refutes a hypothesis about the incident.“
[Carner, Spafford, „An Event-Based Digital Forensic Investigation Framework“, 2004.]

Still, a piece of data.

- Files
- Metadata
- Registry keys
- Database entries
- Network connections
- ...



Singles pieces of the jigsaw puzzle you want to solve.

Still, a piece of data.

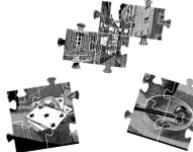
Singles pieces of the jigsaw puzzle you want to solve.

~/df/01-fundamentals

Hypotheses

Questions to be answered.

- Has user A visited website X?
- Was the system compromised?
- Has this USB device been plugged in to this computer?
- Did user B open that document?
- ...



Solving individual parts of the jigsaw puzzle.

Questions to be answered.

Solving individual parts of the jigsaw puzzle.

Artifacts



How do we know which data is worth looking at?



How do we know when an artifact is digital evidence?

How do we get started at all?

Artifacts



Did we mention that **everything but the kitchen sink** generates artifacts?

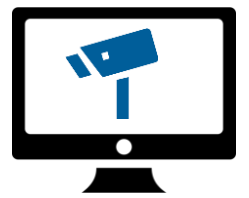
- Of **different types**?
- In **proprietary, undocumented formats** and **locations**?
- With different **reliability** and **trustworthiness**?

Artifacts



Luckily, the artifacts for common questions are already well researched and documented.

Until the next update, that is `~_(\ツ)_/~`

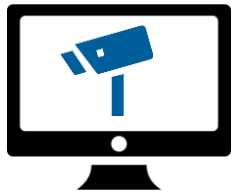


Artifacts



Luckily, the artifacts for **common questions** are already **well researched** and **documented**.

Until the next update, that is `~_(\ツ)_/~`



Artifacts



Luckily, the artifacts for common questions are already well researched and documented.

Until the next update, that is `~_(\ツ)_/~`



Let's start with some operating system artifacts!

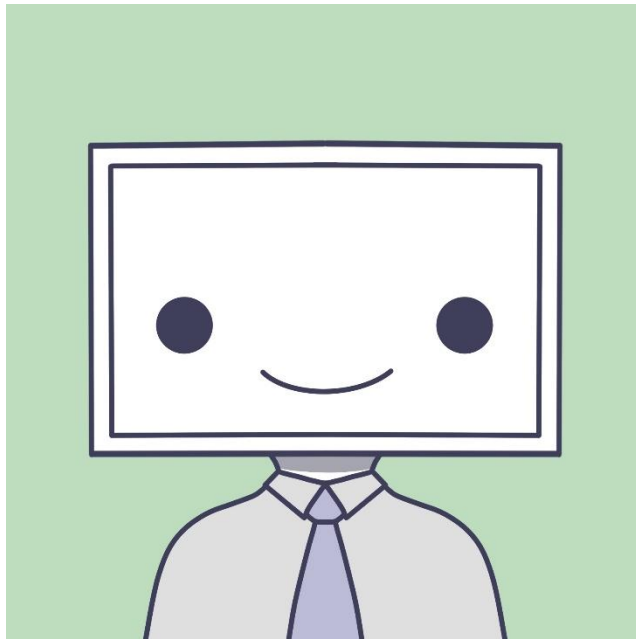
Artifacts: Windows



Windows 10

Artifacts: Windows

user-specific



Location:
`%UserProfile%\...`
E.g. `C:\Users\lynx\...`

VS.

system-specific



Location:
`%SystemRoot%\...`
E.g. `C:\...`

Was the file
ever created or viewed by
the user?

When?

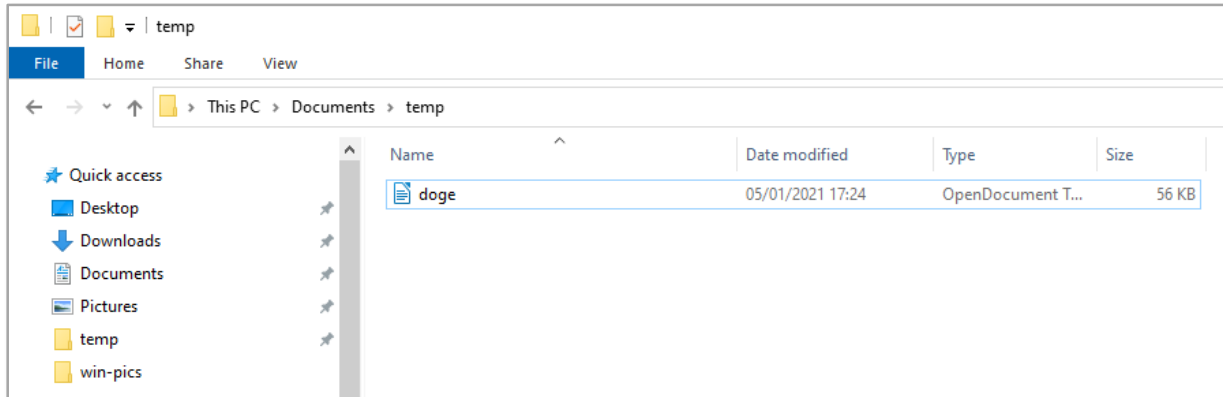
Did the user access it
more than once?



LNK files

Location:

`%UserProfile%\AppData\Roaming\Microsoft\Windows\Recent\`



- Binary
- Proprietary
- Created **automatically** on **first GUI interaction** with a file
- „Recently used files“

```
PS C:\> ls C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\ -File | sort LastWriteTime -Descending
```

```
Directory: C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent
```

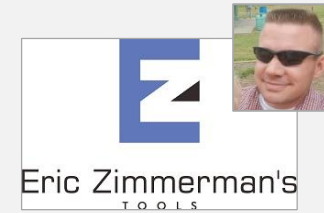
```
Mode                LastWriteTime         Length Name
----                -
...
-a----             1/5/2021   5:53 PM           720 doge1.lnk
-a----             1/5/2021   5:51 PM           715 doge.lnk
...
```

```
PS C:\> LECmd.exe -f C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge.lnk
```

```
LECmd version 1.4.0.0
```

```
Author: Eric Zimmerman (saericzimmerman@gmail.com)  
https://github.com/EricZimmerman/LECmd
```

Remember the name!



```
...  
Processing 'C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge.lnk'
```

```
Source file: C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge.lnk
```

```
Source created: 2021-01-05 16:24:42  
Source modified: 2021-01-05 16:51:46  
Source accessed: 2021-01-05 17:13:33
```

Timestamps of the LNK file, not the original file

```
--- Header ---
```

```
Target created: 2021-01-05 16:24:42  
Target modified: 2021-01-05 16:24:42  
Target accessed: 2021-01-05 16:46:22
```

Timestamps of the original file

```
File size: 56.839
```

Size of the original file

```
...  
--- Link information ---
```

```
Flags: VolumeIdAndLocalBasePath
```

```
>>Volume information
```

```
Drive type: Fixed storage media (Hard drive)  
Serial number: 7AE123F5  
Label: (No label)  
Local path: C:\Users\katz\Documents\temp\doge.odt
```

Volume infos

Path of the original file

```
...  
----- Processed 'C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge.lnk' in 0,10763380 seconds -----
```

```
PS C:\> LECmd.exe -f C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge.lnk
```

```
LECmd version 1.4.0.0
```

```
Author: Eric Zimmerman (saericzimmerman@gmail.com)  
https://github.com/EricZimmerman/LECmd
```

```
...  
Processing 'C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge.lnk'
```

```
Source file: C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge.lnk
```

```
Source created: 2021-01-05 16:24:42  
Source modified: 2021-01-05 16:51:46  
Source accessed: 2021-01-05 17:13:33
```

time **created** -> **first** interaction with the original file
time **modified** -> **last** interaction with the original file

```
--- Header ---
```

```
Target created: 2021-01-05 16:24:42  
Target modified: 2021-01-05 16:24:42  
Target accessed: 2021-01-05 16:46:22
```

time **created** != time **modified**
=> opened **more than once**

```
File size: 56.839
```

```
...  
--- Link information ---
```

```
Flags: VolumeIdAndLocalBasePath
```

```
>>Volume information
```

```
Drive type: Fixed storage media (Hard drive)  
Serial number: 7AE123F5  
Label: (No label)  
Local path: C:\Users\katz\Documents\temp\doge.odt
```

LNK file is modified each time the original is opened.

```
...  
----- Processed 'C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge.lnk' in 0,10763380 seconds -----
```

```
PS C:\> LECmd.exe -f C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge.lnk

LECmd version 1.4.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd
...
Processing 'C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge.lnk'

Source file: C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge.lnk
  Source created: 2021-01-05 16:24:42
  Source modified: 2021-01-05 16:51:46
  Source accessed: 2021-01-05 17:13:33

--- Header ---
  Target created: 2021-01-05 16:24:42
  Target modified: 2021-01-05 16:24:42
  Target accessed: 2021-01-05 16:46:22

  File size: 56.839
  ...
--- Link information ---
Flags: VolumeIdAndLocalBasePath

>>Volume information
  Drive type: Fixed storage media (Hard drive)
  Serial number: 7AE123F5
  Label: (No label)
  Local path: C:\Users\katz\Documents\temp\doge.odt
...
----- Processed 'C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge.lnk' in 0,10763380 seconds -----
```

~/df/06-artifacts/windows/ Hochschule Bonn-Rhein-Sieg Fraunhofer FKIE

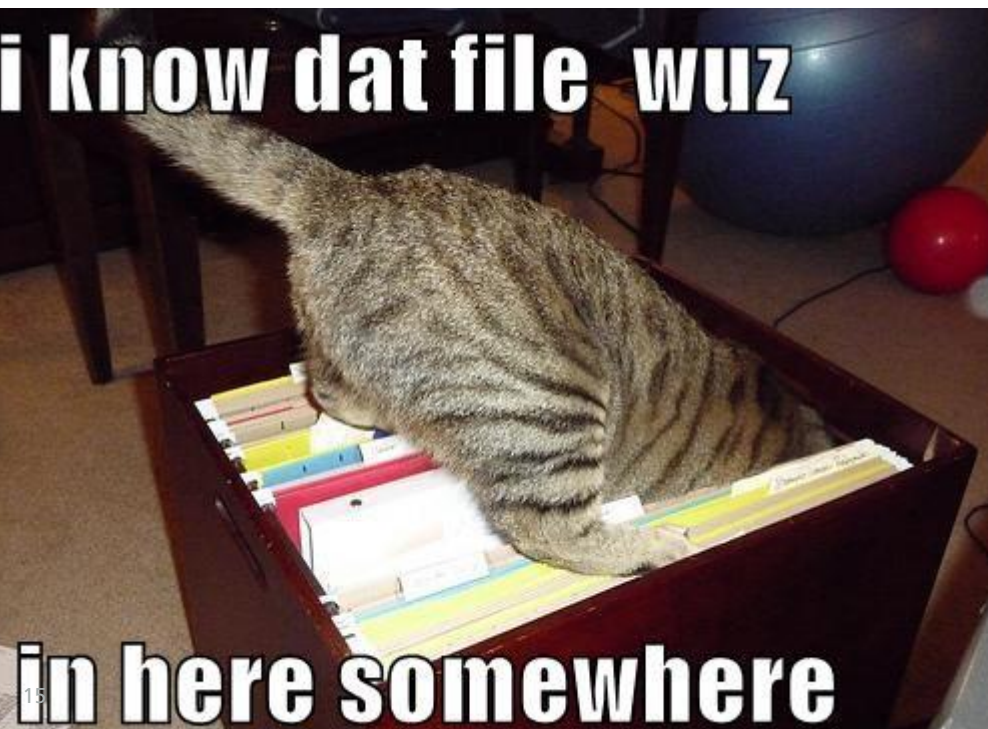
Was the file ever created or viewed by the user?

When?

Did the user access it more than once?



What about files that
do not reside on the user's device anymore?



LNK files

```
PS C:\> lecmd -f C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\house-on-fire.jpg.lnk
```

```
Source file: C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\house-on-fire.jpg.lnk
```

```
Source created: 2021-01-10 12:47:53
```

```
Source modified: 2021-01-10 12:47:53
```

```
Source accessed: 2021-01-10 18:25:54
```

time created == time modified
=> opened once

```
--- Header ---
```

```
Target created: 2021-01-10 12:47:53
```

```
Target modified: 2021-01-10 12:47:54
```

```
Target accessed: 2021-01-09 23:00:00
```

```
File size: 21.061
```

```
>>Volume information
```

```
Drive type: Removable storage media (Floppy, USB)
```

```
Serial number: CC09D6F1
```

```
Label: (No label)
```

```
Local path: F:\house-on-fire.jpg
```


LNK files

```
PS C:\> lecmd -f C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\house-on-fire.jpg.lnk
```

```
Source file: C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\house-on-fire.jpg.lnk
```

```
Source created: 2021-01-10 12:47:53
```

```
Source modified: 2021-01-10 12:47:53
```

```
Source accessed: 2021-01-10 18:25:54
```

time created == time modified
=> opened once

```
--- Header ---
```

```
Target created: 2021-01-10 12:47:53
```

```
Target modified: 2021-01-10 12:47:54
```

```
Target accessed: 2021-01-09 23:00:00
```

```
File size: 21.061
```

```
>>Volume information
```

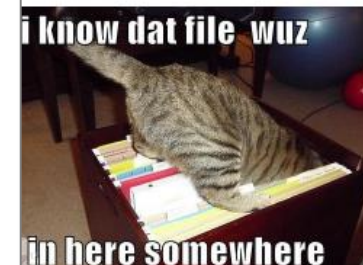
```
Drive type: Removable storage media (Floppy, USB)
```

```
Serial number: CC09D6F1
```

```
Label: (No label)
```

```
Local path: F:\house-on-fire.jpg
```

What about files that
do not reside on the user's device anymore?



Find F:\!
Or: don't trust drive letters.



LNK files

```
PS C:\> lecmd -f  
C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\house-  
on-fire.jpg.lnk
```

```
Source file:  
C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\house-  
on-fire.jpg.lnk  
Source created: 2021-01-10 12:47:53  
Source modified: 2021-01-10 12:47:53  
Source accessed: 2021-01-10 18:25:54
```

```
--- Header ---  
Target created: 2021-01-10 12:47:53  
Target modified: 2021-01-10 12:47:54  
Target accessed: 2021-01-09 23:00:00
```

File size: 21.061

```
>>Volume information  
Drive type: Removable storage media (Floppy, USB)  
Serial number: CC09D6F1  
Label: (No label)  
Local path: F:\house-on-fire.jpg
```

```
PS C:\> lecmd -f  
C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\this_is_  
fine.jpg.lnk
```

```
Source file:  
C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\this_is_  
fine.jpg.lnk  
Source created: 2021-01-10 12:51:08  
Source modified: 2021-01-10 12:51:08  
Source accessed: 2021-01-10 18:26:05
```

```
--- Header ---  
Target created: 2021-01-10 12:51:07  
Target modified: 2021-01-10 12:51:10  
Target accessed: 2021-01-09 23:00:00
```

File size: 53.072

```
>>Volume information  
Drive type: Removable storage media (Floppy, USB)  
Serial number: F8BB153B  
Label: (No label)  
Local path: F:\this_is_fine.jpg
```

different devices!

same parent directory

LNK files

```

PS C:\> lecmd -f
C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\house-on-fire.jpg.lnk

Source file:
C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\house-on-fire.jpg.lnk
  Source created: 2021-01-10 12:47:53
  Source modified: 2021-01-10 12:47:53
  Source accessed: 2021-01-10 18:25:54

--- Header ---
  Target created: 2021-01-10 12:47:53
  Target modified: 2021-01-10 12:47:54
  Target accessed: 2021-01-09 23:00:00

File size: 21.061

>>Volume information
  Drive type: Removable storage media (Floppy, USB)
  Serial number: CC09D6F1
  Label: (No label)
  Local path: F:\house-on-fire.jpg

```

```

PS C:\> lecmd -f
C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\this_is_fine.jpg.lnk

Source file:
C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\this_is_fine.jpg.lnk
  Source created: 2021-01-10 12:47:53
  Source modified: 2021-01-10 12:47:53
  Source accessed: 2021-01-10 18:25:54

--- Header ---
  Target created: 2021-01-10 12:47:53
  Target modified: 2021-01-10 12:47:54
  Target accessed: 2021-01-09 23:00:00

File size: 55.072

>>Volume information
  Drive type: Removable storage media (Floppy, USB)
  Serial number: F8BB153B
  Label: (No label)
  Local path: F:\this_is_fine.jpg

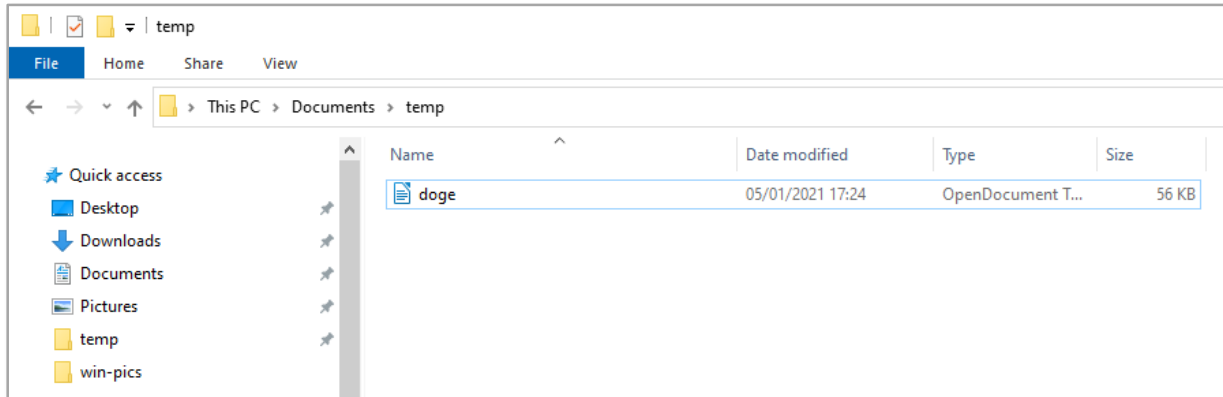
```



What if the file was deleted?



LNK files



```
PS C:\> ls C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\ -File | sort LastWriteTime -Descending
```

Mode	LastWriteTime	Length	Name
-a----	1/5/2021 5:53 PM	720	doge1.lnk
-a----	1/5/2021 5:51 PM	715	doge.lnk

LNK files

```
PS C:\> LECmd.exe -f C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge1.lnk
```

Source file: C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge1.lnk

Source created: 2021-01-05 16:53:57
Source modified: 2021-01-05 16:53:57
Source accessed: 2021-01-05 17:14:08

--- Header ---

Target created: 2021-01-05 16:53:40
Target modified: 2018-02-23 07:36:40
Target accessed: 2021-01-05 16:53:57

File size: 279.818

--- Link information ---

Flags: VolumeIdAndLocalBasePath

>>Volume information

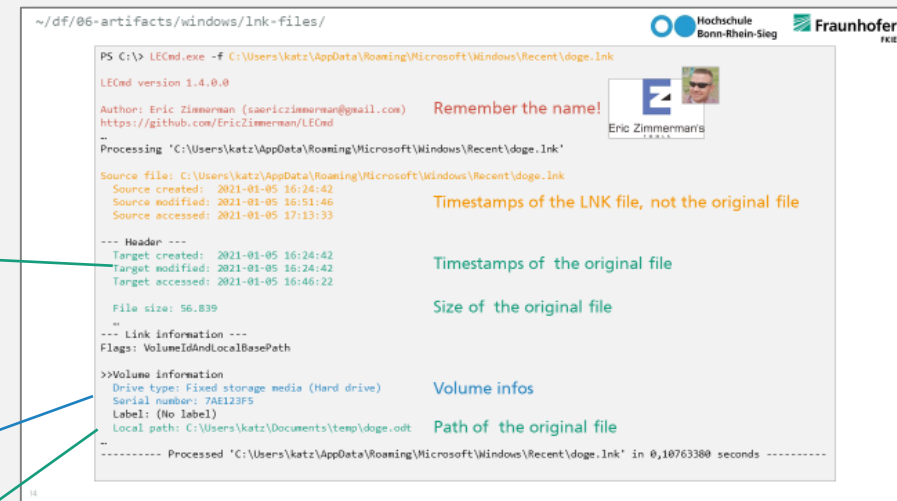
Drive type: Fixed storage media (Hard drive)
Serial number: 7AE123F5
Label: (No label)
Local path: C:\Users\katz\Documents\temp\doge1.png

--- Target ID information (Format: Type ==> Value) ---

Absolute path: My Computer\Documents\temp\doge1.png

----- Processed 'C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge1.lnk' in 0,10400910 seconds -----

Recap



Remember the name! Eric Zimmerman

Timestamps of the LNK file, not the original file

Timestamps of the original file

Size of the original file

Volume infos

Path of the original file

LNK files

```
PS C:\> LECmd.exe -f C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge1.lnk
```

```
Source file: C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge1.lnk
```

```
Source created: 2021-01-05 16:53:57
```

```
Source modified: 2021-01-05 16:53:57
```

```
Source accessed: 2021-01-05 17:14:08
```

```
--- Header ---
```

```
Target created: 2021-01-05 16:53:40
```

```
Target modified: 2018-02-23 07:36:40
```

```
Target accessed: 2021-01-05 16:53:57
```

```
File size: 279.818
```

```
--- Link information ---
```

```
Flags: VolumeIdAndLocalBasePath
```

```
>>Volume information
```

```
Drive type: Fixed storage media (Hard drive)
```

```
Serial number: 7AE123F5
```

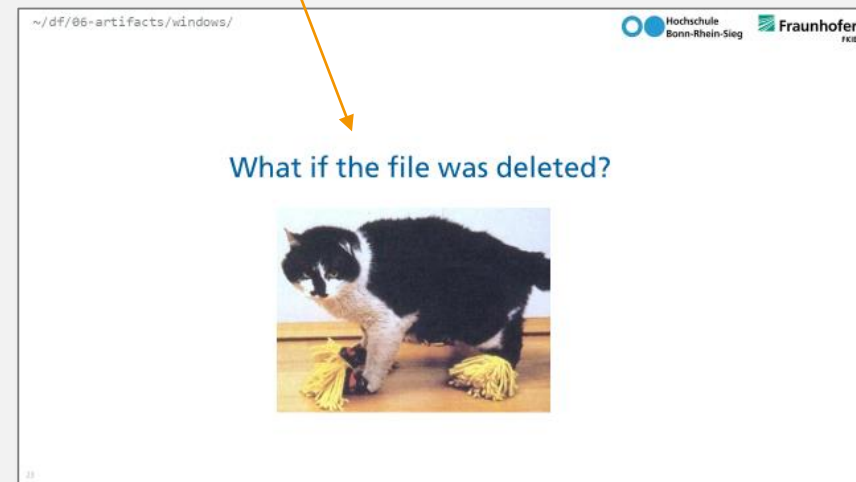
```
Label: (No label)
```

```
Local path: C:\Users\katz\Documents\temp\doge1.png
```

```
--- Target ID information (Format: Type ==> Value) ---
```

```
Absolute path: My Computer\Documents\temp\doge1.png
```

```
----- Processed 'C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge1.lnk' in 0,10400910 seconds -----
```



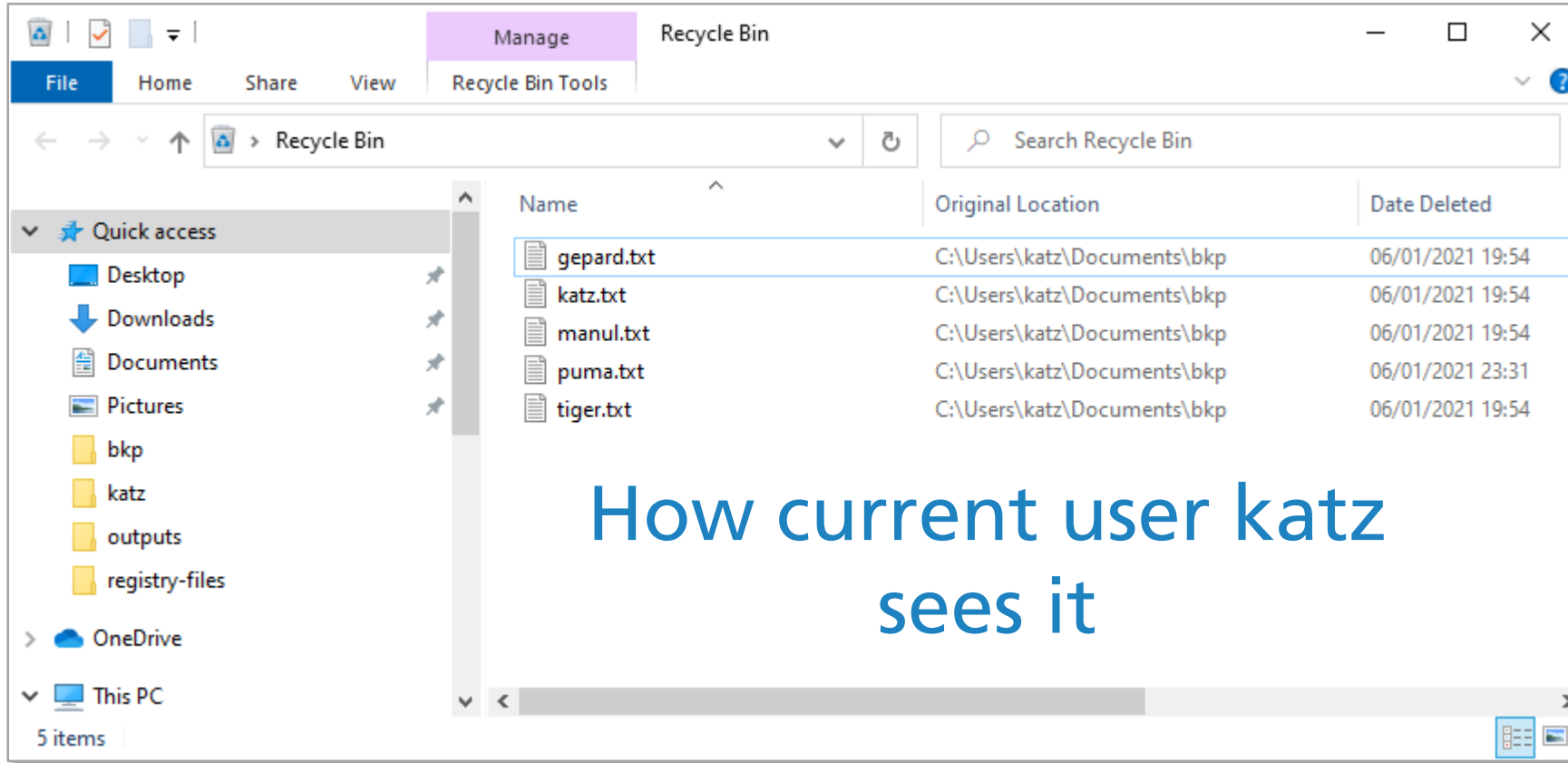
Recycle Bin

Speaking about deleted files.

Diggin' in the trash, or:
What happens in the recycle bin?

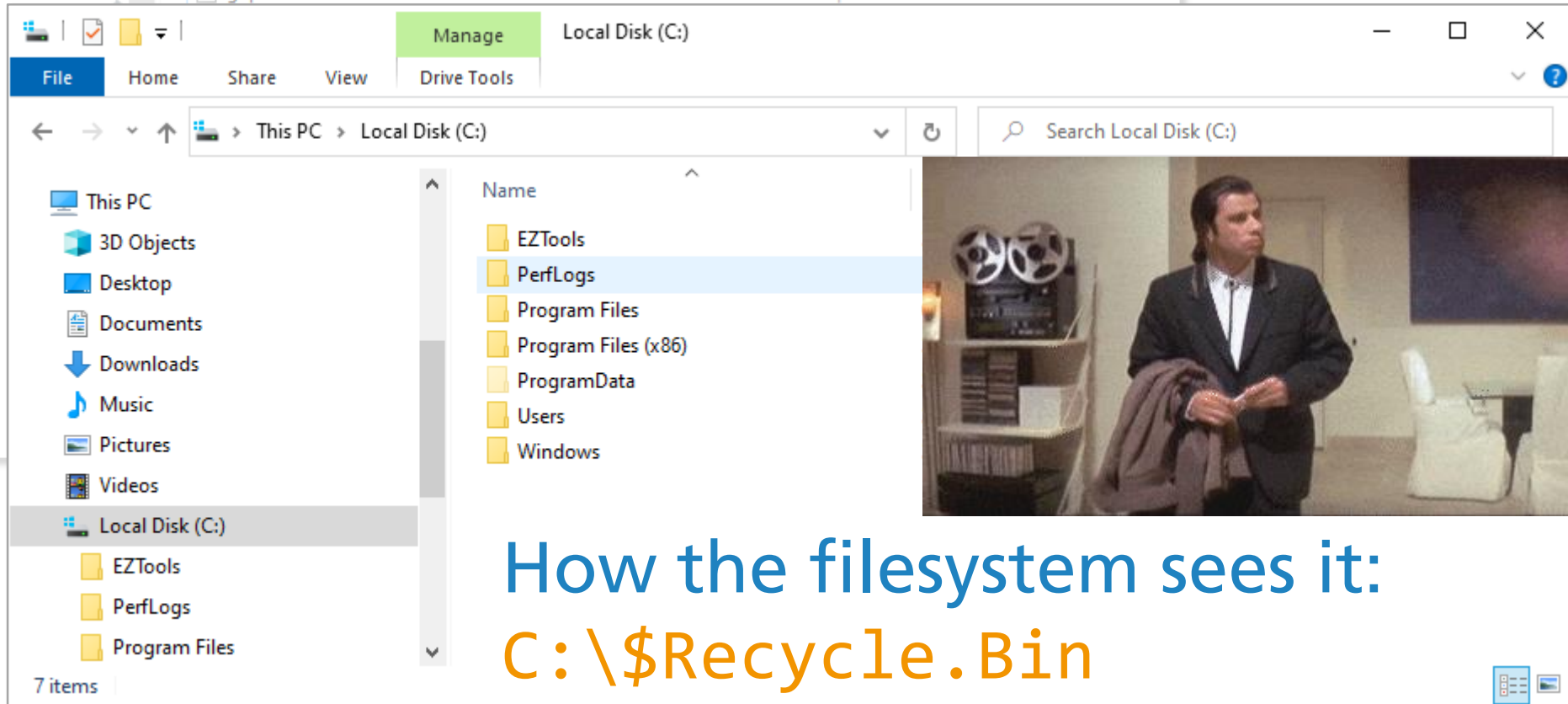
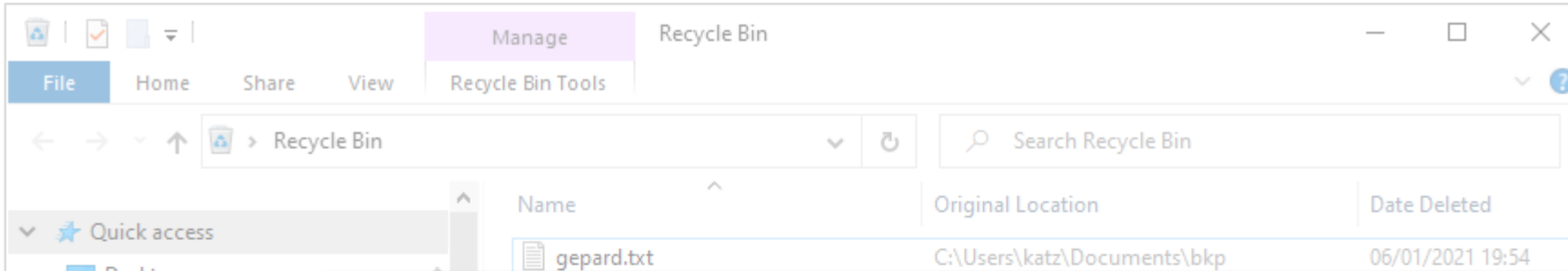


Recycle Bin



How the filesystem sees it:
C:\\$Recycle.Bin

Recycle Bin



Recycle Bin

```
PS C:\> ls -Hidden
```

```
Directory: C:\
```

Mode	LastWriteTime		Length	Name
----	-----	-----	-----	----
d--hs-	12/30/2020	12:34 PM		\$Recycle.Bin
d--hsl	8/14/2020	6:38 PM		Documents and Settings
d--h--	12/30/2020	1:40 PM		ProgramData
d--hs-	8/14/2020	6:38 PM		Recovery
d--hs-	8/14/2020	9:40 AM		System Volume Information
-a-hs-	1/6/2021	5:46 PM	1342177280	pagefile.sys
-a-hs-	1/6/2021	5:46 PM	268435456	swapfile.sys

Recycle Bin

```
PS C:\> cd '.\$Recycle.Bin\'
PS C:\$Recycle.Bin> ls -Hidden
```

Directory: C:\\$Recycle.Bin

Mode	LastWriteTime	Length	Name
----	-----	-----	----
d--hs-	8/26/2020 7:00 PM		S-1-5-18
d--hs-	8/14/2020 9:38 AM		S-1-5-21-1752181755-1580187878-119375555-1000
d--hs-	8/14/2020 11:05 AM		S-1-5-21-1752181755-1580187878-119375555-1001
d--hs-	12/30/2020 12:25 PM		S-1-5-21-1752181755-1580187878-119375555-1002
d--hs-	1/6/2021 11:31 PM		S-1-5-21-1752181755-1580187878-119375555-1003

S-1-5-21-1752181755-1580187878-119375555-1003

security identifier
revision level
identifier authority (5: NT Authority)
domain or local system
relative ID - RID (normal users: >=1000)

or a user → *“A security identifier (SID) is a **unique value of variable length** that is used to **identify a security principal** (such as a security group) in Windows operating systems. SIDs that identify generic users or generic groups is [sic!] well known.”*

<https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/security-identifiers-in-windows>

User name from SID

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (1/0) View Help

Registry hives (1) Available bookmarks (1/0)

Enter text to search... Find

Key name # values # subkeys Last write timestamp

C:\Users\katz\Docu...
 Associated deleted re...
 ROOT
 SAM
 Domains
 Account
 Aliases
 Users
 000001F4
 000001F5
 000001F7
 000001F8
 000003E9
 000003EA
 000003EB
 Names
 Admi...
 Defa...
 Guest
 katz
 manul
 mari
 WDA...
 Built-in
 LastSkuUpgrade
 RXACT

User Id	Invali...	Total ...	Created On	Last Login Time	Last Password Chan...	Last Incorrect Passw...	Expires ...	User Name	Full Name	Password Hi...	Groups	Comment
500	0	0	2020-08-14 07:38:42					Administrator			Administrators	Built-in account for administering the computer/domain
501	0	0	2020-08-14 07:38:42					Guest			Guests	Built-in account for guest access to the computer/domain
503	0	0	2020-08-14 07:38:42					DefaultAccount			System Managed Accounts Group	A user account managed by the system.
504	0	0	2020-08-14 07:38:42		2020-08-14 16:36:20			WDAGUtilityAccount				A user account managed and used by the system for Windows Defender Application Guard scenarios.
1001	0	17	2020-08-14 09:03:21	2020-12-30 11:16:52	2020-08-14 09:03:22	2020-12-30 10:49:41		mari			Administrators	
1002	0	2	2020-12-30 11:23:08	2021-01-06 14:03:41	2020-12-30 11:23:08	2020-12-30 11:24:50		manul			Administrators, Users	
1003	0	15	2020-12-30 11:32:54	2021-01-06 15:09:54	2020-12-30 11:32:54	2021-01-05 16:12:17		katz			Administrators, Users	

user ID (RID)

username

registry key

Key: ROOT\SAM\Domains\Account\Users

Value: (default) Collapse all hives

Names

Name	Created On	Last Write
Admi...	2020-08-14 07:38:42	
Defa...	2020-08-14 07:38:42	
Guest	2020-08-14 07:38:42	
katz	2020-12-30 11:32:54	
manul	2020-12-30 11:23:08	
mari	2020-08-14 09:03:21	
WDA...	2020-08-14 07:38:42	

Type viewer Binary viewer

Value name (default)

Value type RegUnknown (0x3EB, 1003 decimal)

Value 00-00-00-00

Raw value



Recycle Bin

```
PS C:\$Recycle.Bin\S-1-5-21-1752181755-1580187878-119375555-1003> ls | sort Name
```

Mode	LastWriteTime	Length	Name	
-a----	1/6/2021 11:31 PM	102	\$I3WV62F.txt	} \$I files – metadata (binary)
-a----	1/6/2021 7:54 PM	102	\$I7GMYA2.txt	
-a----	1/6/2021 7:54 PM	102	\$IBFKMAS.txt	
-a----	1/6/2021 7:54 PM	106	\$IOFZFVF.txt	
-a----	1/6/2021 7:54 PM	104	\$IPJFTR4.txt	
-a----	1/6/2021 7:54 PM	104	\$IV52TY8.txt	} \$R files – recovery data
-a----	1/6/2021 11:29 PM	15	\$R3WV62F.txt	
-a----	1/6/2021 1:48 PM	5	\$RBFKMAS.txt	
-a----	1/6/2021 2:56 PM	18	\$ROFZFVF.txt	
-a----	1/6/2021 1:48 PM	13	\$RPJFTR4.txt	
-a----	1/6/2021 1:47 PM	6	\$RV52TY8.txt	

```
PS C:\$Recycle.Bin\S-1-5-21-1752181755-1580187878-119375555-1003> RBCmd.exe -f '.\$IV52TY8.txt'
```

```
RBCmd version 0.5.0.0
```

```
Source file: .\$IV52TY8.txt
```

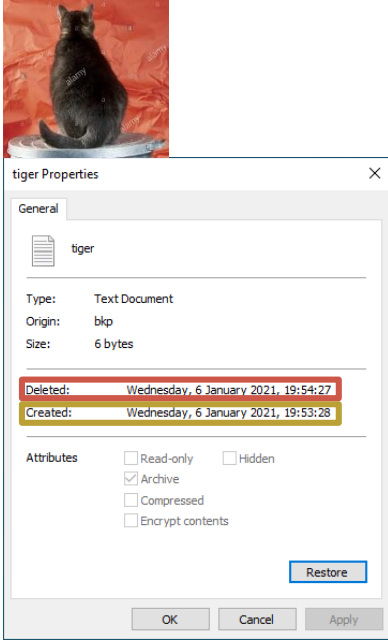
```
Version: 2 (Windows 10)
```

```
File size: 6 (6B)
```

```
File name: C:\Users\katz\Documents\bkp\tiger.txt
```

```
Deleted on: 2021-01-06 18:54:27.1510000
```

Recycle Bin: timestamps



\$R file is **created** after it is **modified** if we trust timestamps :D

- 06-01-2021 ??? – tiger.txt created and modified
- 06-01-2021 19:53:28 – tiger.txt in Recycle Bin created
- 06-01-2021 19:53:28 – \$R-file created
- 06-01-2021 19:54:27 – tiger.txt deleted
- 06-01-2021 19:54:27 – \$I-file created and modified
- 06-01-2021 13:47:58 – \$R-file modified
- 06-01-2021 ??? – tiger.txt recovered
- 06-01-2021 19:54:27 – tiger.txt created
- 06-01-2021 13:47:58 – tiger.txt modified

```
PS C:\$Recycle.Bin\S-1-5-21-1752181755-1580187878-119375555-1003> ls | select Name, LastAccessTime, CreationTime, LastWriteTime
```

Name	LastAccessTime	CreationTime	LastWriteTime	
\$IV52TY8.txt	1/8/2021 12:36:48 PM	1/6/2021 7:54:27 PM	1/6/2021 7:54:27 PM	tiger.txt deleted
\$RV52TY8.txt	1/7/2021 9:34:13 PM	1/6/2021 7:53:28 PM	1/6/2021 1:47:58 PM	

```
PS C:\Users\katz\Documents\bkp> ls | select Name, LastAccessTime, LastWriteTime, CreationTime
```

Name	LastAccessTime	LastWriteTime	CreationTime	
tiger.txt	1/8/2021 10:11:11 PM	1/6/2021 1:47:58 PM	1/6/2021 7:53:28 PM	tiger.txt recovered

Name	LastAccessTime	CreationTime	LastWriteTime	
\$IV52TY8.txt	1/8/2021 10:11:10 PM	1/6/2021 7:54:27 PM	1/6/2021 7:54:27 PM	\$I file is still in the recycle bin

Same with tiger.txt :D

Did a user open a folder on an external media?



When?

What if it was deleted afterwards

Shellbags: the registry part



I'm back, baby.

User-specific registry hive:

```
%UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat
```

Keys:

```
Local Settings\Microsoft\Windows\Shell\Bags
```

```
Local Settings\Microsoft\Windows\Shell\BagsMRU
```

- Binary (registry)
- Proprietary (registry)
- Updated **automatically** on **GUI interaction** with a folder
- Viewed folder details

Shellbags



I'm back, baby.

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (1/0) View Help

Registry hives (1) Available bookmarks (1/0)

Enter text to search... Find

Key name

- com.microsoft.3dviewer
- com.microsoft.print3d
- Extensions
- feedback-hub
- http
- https
- insiderhub
- Local Settings
 - ImmutableMuiCache
 - MrtCache
 - MuiCache
 - Software
 - Microsoft
 - Windows
 - CurrentVersion
 - Shell
 - BagMRU
 - 0
 - 1
 - 2
 - 0
 - 0
 - 1
 - Bags
 - 1
 - 2
 - 3
 - 4

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
NodeSlot	RegDword	4		<input type="checkbox"/>	<input type="checkbox"/>
MRUListEx	RegBinary	00-00-00-00-...	D0-F7-17-00	<input type="checkbox"/>	<input type="checkbox"/>
0	RegBinary	6C-00-31-00-...	69-00-6E-00-...	<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Slack viewer

Type viewer	Slack viewer
00000000	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D
0000000E	6C 00 31 00 00 00 00 00 29 52 79 5A 10 00
0000001C	43 4F 4D 50 41 4E 7E 31 00 00 54 00 09 00
0000002A	04 00 EF BE 29 52 79 5A 28 52 00 B8 2E 00
00000038	00 00 A0 42 EA 00 00 00 00 00 00 00 00 00
00000046	00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000004E	63 00 6F 00 6D 00 70 00 61 00 6E 00 79 00
00000054	2D 00 69 00 6E 00 74 00 65 00 72 00 6E 00
00000062	61 00 6C 00 73 00 00 00 18 00 00 00

1.) RyZ.
 COMPAN~1. . . T.
 . . i ¼ RyZ(R.
 . . Bè.
 .
 c. o. m p. a. n. y.
 - . i . n . t . e . r . n
 a . l . s

Current offset: 0 (0x0) Bytes selected: 0 (0x0) Data interpreter ?

Key: S-1-5-21-1752181755-1580187878-119375555-1004_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0 Value: 0 Collapse all hives

Selected hive: UsrClass.dat Last write: 2021-01-09 11:31:49 3 of 3 values shown (100,00 %) Load complete Hidden keys: 0 2

shellbags

Shellbags

folders
timestamps

shellbag
timestamps

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Has Explored	Miscellaneous
memes	Folder icon	Directory	2	2021-01-08 22:42:04	2021-01-08 22:42:04	2021-01-07 23:00:00	2021-01-09 11:32:09		<input type="checkbox"/>	FAT file system
photos	Folder icon	Directory	1	2021-01-08 22:42:22	2021-01-08 22:42:04	2021-01-07 23:00:00	2021-01-09 11:32:16		<input type="checkbox"/>	FAT file system
screenshots	Folder icon	Directory	0	2021-01-08 22:46:46	2021-01-08 22:46:46	2021-01-07 23:00:00	2021-01-09 11:32:31	2021-01-09 11:32:31	<input type="checkbox"/>	FAT file system

Name: important-pics
Absolute path: Desktop\F:\important-pics
Key-Value name path: BagMRU2-1
Registry last write time: 2021-01-09 11:38:30.051

Target timestamps
Created on: 2021-01-08 22:40:12.000
Modified on: 2021-01-08 22:40:12.000
Last accessed on: 2021-01-07 23:00:00.000

Miscellaneous
Shell type: Directory
Node slot: 6
MRU position: 1
of child bags: 3

user actively opened these folders

```
PS F:\> tree
Folder PATH listing
Volume serial number is CC09-D6F1
F:.
├── important-docs
├── important-pics
│   ├── memes
│   ├── photos
│   └── screenshots
└── important-sans-cheatsheets
```



Shellbags

ShellBags Explorer v1.4.0.0

File Tools Help

Value

Desktop

F:\

- important-docs
- company-internals
- important-pics**
- screenshots
- photos
- memes

Home Folder

My Computer

Drag a column header here to group by that column

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Has Explored	Miscellaneous
?	#c	No im...	#c	=	=	=	=	=	<input checked="" type="checkbox"/>	#c
memes	📁	Directory	2	2021-01-08 22:42:04	2021-01-08 22:42:04	2021-01-07 23:00:00	2021-01-09 11:32:09		<input type="checkbox"/>	FAT file system
photos	📁	Directory	1	2021-01-08 22:42:22	2021-01-08 22:42:04	2021-01-07 23:00:00	2021-01-09 11:32:16		<input type="checkbox"/>	FAT file system
screenshots	📁	Directory	0	2021-01-08 22:46:46	2021-01-08 22:46:46	2021-01-07 23:00:00	2021-01-09 11:32:31	2021-01-09 11:32:31	<input type="checkbox"/>	FAT file system

ShellBags Explorer v1.4.0.0

File Tools Help

Value

Desktop

F:\

- important-docs**
- company-internals
- important-pics
- screenshots
- photos
- memes

Home Folder

My Computer

deleted folder which was also opened by the user

at this time (more or less)

Summary Details Hex

Name: important-docs
 Absolute path: Desktop\F:\important-docs
 Key-Value name path: BagMRU2-0
 Registry last write time: 2021-01-09 11:38:30.051

Target timestamps
 Created on: 2021-01-06 12:48:00.000
 Modified on: 2021-01-06 12:47:58.000
 Last accessed on: 2021-01-05 23:00:00.000

```

PS F:\> tree
Folder PATH listing
Volume serial number is CC09-D6F1
F:.
├── important-docs
├── important-pics
│   ├── memes
│   ├── photos
│   └── screenshots
└── important-sans-cheatsheets
  
```

Shellbags

ShellBags Explorer v1.4.0.0

File Tools Help

Value

Desktop

F:\

- important-docs
- company-internals
- important-pics**
- screenshots
- photos
- memes

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Has Explored	Miscellaneous
memes	[Folder Icon]	Directory	2	2021-01-08 22:42:04	2021-01-08 22:42:04	2021-01-07 23:00:00	2021-01-09 11:32:09		<input type="checkbox"/>	FAT file system
photos	[Folder Icon]	Directory	1	2021-01-08 22:42:22	2021-01-08 22:42:04	2021-01-07 23:00:00	2021-01-09 11:32:16		<input type="checkbox"/>	FAT file system
screenshots	[Folder Icon]	Directory	0	2021-01-08 22:46:46	2021-01-08 22:46:46	2021-01-07 23:00:00	2021-01-09 11:32:31	2021-01-09 11:32:31	<input type="checkbox"/>	FAT file system

ShellBags Explorer v1.4.0.0

File Tools Help

Value

Desktop

F:\


- important-docs**
- company-internals
- important-pics
- screenshots
- photos
- memes

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Has Explored	Miscellaneous
company-internals	[Folder Icon]	Directory	0	2021-01-09 11:19:50	2021-01-09 11:19:50	2021-01-08 23:00:00	2021-01-09 11:31:49	2021-01-09 11:31:49	<input type="checkbox"/>	FAT file system

~/df/06-artifacts/windows/

Hochschule Bonn-Rhein-Sieg Fraunhofer FKIE

Did a user open a folder on an external media?



When?

What if it was deleted afterwards

```
PS F:\> tree
Folder PATH listing
Volume serial number is CC09-D6F1
F:.
├── important-docs
├── important-pics
│   ├── memes
│   ├── photos
│   └── screenshots
└── important-sans-cheatsheets
```

name: important-docs
 absolute path: Desktop\F:\important-docs
 registry-Value name path: BagMRU2-0
 registry last write time: 2021-01-09 11:38:30.051

target timestamps
 created on: 2021-01-06 12:48:00.000
 modified on: 2021-01-06 12:47:58.000
 last accessed on: 2021-01-05 23:00:00.000

Speaking of external
media...

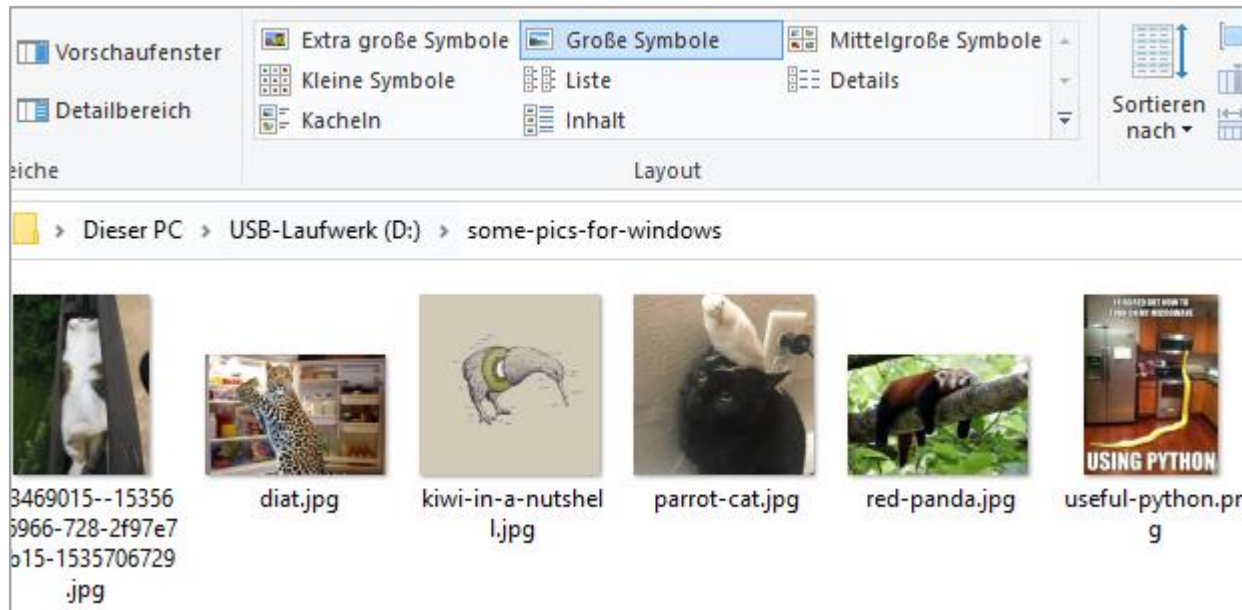
Can we link an image to a
computer?



Thumbcache

Location:

```
%UserProfile%\AppData\Local\Microsoft\Windows\Explorer\
```



- Binary
- Proprietary
- Created on **preview setting change** for a folder

Thumbcache

```
PS C:\> ls C:\Users\manul\AppData\Local\Microsoft\Windows\Explorer\ | sort LastWriteTime -Descending
```

Mode	LastWriteTime	Length	Name
----	-----	-----	----
...			
-a----	1/6/2021 3:12 PM	29232	iconcache_idx.db
-a----	1/6/2021 3:04 PM	3145728	iconcache_256.db
...			
-a----	12/30/2020 12:24 PM	24	iconcache_wide_alternate.db
-a----	12/30/2020 12:24 PM	24	iconcache_wide.db
-a----	12/30/2020 12:24 PM	24	iconcache_sr.db
-a----	12/30/2020 12:24 PM	24	iconcache_96.db
-a----	12/30/2020 12:24 PM	24	iconcache_1920.db
-a----	12/30/2020 12:24 PM	1048576	iconcache_16.db
...			
-a----	12/30/2020 12:24 PM	24	thumbcache_wide.db
-a----	12/30/2020 12:24 PM	24	thumbcache_wide_alternate.db
-a----	12/30/2020 12:24 PM	24	thumbcache_sr.db
-a----	12/30/2020 12:24 PM	24	thumbcache_1920.db
-a----	12/30/2020 12:24 PM	24	thumbcache_2560.db
-a----	12/30/2020 12:24 PM	24	thumbcache_1280.db
-a----	12/30/2020 12:24 PM	1048576	thumbcache_256.db
-a----	12/30/2020 12:24 PM	24	thumbcache_768.db
-a----	12/30/2020 12:24 PM	1048576	thumbcache_48.db
-a----	12/30/2020 12:24 PM	3145728	thumbcache_96.db
-a----	12/30/2020 12:24 PM	1048576	thumbcache_32.db
-a----	12/30/2020 12:24 PM	1048576	thumbcache_16.db

Icon thumbnails database
(desktop, etc.)
small, medium, large, etc.

Very small file size, most
probably empty

Image thumbnails database
small, medium, large, etc.

Thumbcache

```
PS C:\> ls C:\Users\manul\AppData\Local\Microsoft\Windows\Explorer\ | sort LastWriteTime -Descending
```

```
Mode                LastWriteTime         Length Name
----                -
...
-a----             1/6/2021   3:12 PM         29232 iconcache_idx.db
-a----             1/6/2021   3:04 PM       3145728 iconcache_256.db
...
-a----            12/30/2020  12:24 PM          24 iconcache_wide_alternate.db
-a----            12/30/2020  12:24 PM          24 iconcache_wide.db
-a----            12/30/2020  12:24 PM          24 iconcache_sr.db
-a----            12/30/2020  12:24 PM          24 iconcache_96.db
-a----            12/30/2020  12:24 PM          24 iconcache_1920.db
```

Icon thumbnails database
(desktop, etc.)
small, medium, large, etc.

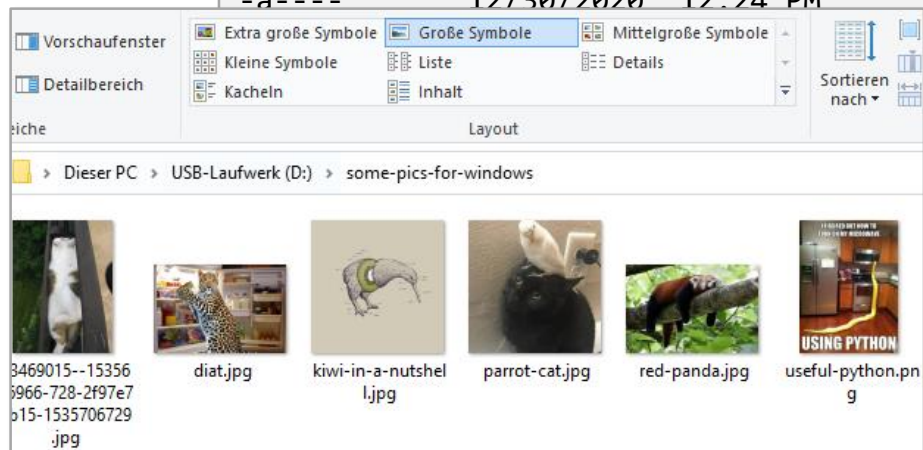
```
1048576 iconcache_16.db

24 thumbcache_wide.db
24 thumbcache_wide_alternate.db
24 thumbcache_sr.db
24 thumbcache_1920.db
24 thumbcache_2560.db
24 thumbcache_1280.db
```

Very small file size, most
probably empty

```
1048576 thumbcache_256.db
24 thumbcache_768.db
1048576 thumbcache_48.db
3145728 thumbcache_96.db
1048576 thumbcache_32.db
1048576 thumbcache_16.db
```

Image thumbnails database
small, medium, large, etc.



```
-a----            12/30/2020  12:24 PM
-a----            12/30/2020  12:24 PM
-a----            12/30/2020  12:24 PM
-a----            12/30/2020  12:24 PM
-a----            12/30/2020  12:24 PM
```

Thumbcache

#	Filename	Cache Entry Offset	Cache Entry S...	Data Offset	Data Size	Data Checksum	Header Checksum	Cache Entry Hash	System	Location
1	af2749a243de8f76.png	295188 B	105 KB	295276 B	105 KB	a857c77f599a4b6a	026adb5f2f4bbe8f	af2749a243de8f76	Windows 10	D:\thumbnails\thumbcache_256.db
2	bae9726a3cbeb40e.jpg	143962 B	29 KB	144050 B	29 KB	09a5ead4ada6e1cd	409636f916656b3f	bae9726a3cbeb40e	Windows 10	D:\thumbnails\thumbcache_256.db
3	a312ef7712191b21.jpg	189302 B	27 KB	189390 B	27 KB	862f09e52a0d94fa	bd142fc84dc5c557	a312ef7712191b21	Windows 10	D:\thumbnails\thumbcache_256.db
4	a1884ff52fc35e2.jpg	125192 B	18 KB	125280 B	18 KB	7e4d72ed62c951c7	8e7bed440c6e67bd	a1884ff52fc35e2	Windows 10	D:\thumbnails\thumbcache_256.db
5	13f13b2031f27a0.jpg	239446 B	17 KB	239532 B	17 KB	a6f2057122d4dab7	8433c7ac8508cd4	013f13b2031f27a0	Windows 10	D:\thumbnails\thumbcache_256.db
6	73a6249be74b1d09.jpg	108858 B	15 KB	108946 B	15 KB	f6920f1364dd5229	70035158e67673b4	73a6249be74b1d09	Windows 10	D:\thumbnails\thumbcache_256.db
7	5b86ed2b29e20693.jpg	279206 B	15 KB	279294 B	15 KB	9f9ae8d860aa248c	85bb14b4fa1822e4	5b86ed2b29e20693	Windows 10	D:\thumbnails\thumbcache_256.db
8	6aa2877bf2e36cc4.jpg	173890 B	15 KB	173978 B	14 KB	9b250ea38f81f77b	9bac56eea8c06d99	6aa2877bf2e36cc4	Windows 10	D:\thumbnails\thumbcache_256.db
9	e02406d3cd188682.jpg	94200 B	14 KB	94288 B	14 KB	f2e0daa57d68b53d	50659cd09193e0a9	e02406d3cd188682	Windows 10	D:\thumbnails\thumbcache_256.db
10	2ce41946904dc8a6.jpg	265568 B	13 KB	265656 B	13 KB	ac25fcb7805eb812	2a801d99b6762e8d	2ce41946904dc8a6	Windows 10	D:\thumbnails\thumbcache_256.db
11	84119a4b6e896999.jpg	61974 B	12 KB	62062 B	12 KB	46688205e9972aa0	768bbfc6a5722642	84119a4b6e896999	Windows 10	D:\thumbnails\thumbcache_256.db
12	1371b674f83a87b6.jpg	49452 B	12 KB	49540 B	12 KB	539ba4cab836a6a3	0374c60d611fcd0e	1371b674f83a87b6	Windows 10	D:\thumbnails\thumbcache_256.db
13	28c4a97e4402de30.jpg	25182 B	11 KB	25270 B	11 KB	18f1c9d49082bc3f	21a4fdf87df05f14	28c4a97e4402de30	Windows 10	D:\thumbnails\thumbcache_256.db
14	7e3033d80448b451.jpg	37376 B	11 KB	37464 B	11 KB	fb7b9ff3c4d6c960	be02936e15e213e6	7e3033d80448b451	Windows 10	D:\thumbnails\thumbcache_256.db
15	f3e24a84aef2e77.jpg	227624 B	11 KB	227712 B	11 KB	8ed8242c2e39ac8f	50ce8b475a8a2129	f3e24a84aef2e77	Windows 10	D:\thumbnails\thumbcache_256.db
16	77ae123f5?1000000030...	4872 B	11 KB	4974 B	11 KB	16cd191964a84dd9	56b1fa0b6d69339c	f307d27990c46405	Windows 10	D:\thumbnails\thumbcache_256.db
17	e5ca113442da1538.jpg	75094 B	10 KB	75182 B	10 KB	cc5248452aa944e8	c45721e4fde9ace9	e5ca113442da1538	Windows 10	D:\thumbnails\thumbcache_256.db
18	e2ef665d4b160876.jpg	217822 B	8 KB	217910 B	8 KB	1f2a9ff3d0be3d69	8251ebdaddc0f109	e2ef665d4b160876	Windows 10	D:\thumbnails\thumbcache_256.db
19	5db7bc80eb23aa1.jpg	16276 B	8 KB	16364 B	8 KB	c752cbb78a094284	60a41dd50474b95b	5db7bc80eb23aa1	Windows 10	D:\thumbnails\thumbcache_256.db
20	bbb29e413383080c.jpg	85544 B	8 KB	85632 B	8 KB	f3b8cbe09093e4a3	50292376b18caf84	bbb29e413383080c	Windows 10	D:\thumbnails\thumbcache_256.db
21	e4a114740478e788.jpg	257702 B	7 KB	257790 B	7 KB	adf173f20cf3e6ec	ab1be653009182b3	e4a114740478e788	Windows 10	D:\thumbnails\thumbcache_256.db
22	4a518aaaca14ff5d.jpg	424 B	3 KB	512 B	3 KB	37582905ad9db91e	13107c7c4f17bf57	4a518aaaca14ff5d	Windows 10	D:\thumbnails\thumbcache_256.db
23	::{645FF040-5081-101...	24 B	0 KB	160 B	0 KB	0000000000000000	10ea598cd60aba95	0924bc51f9b84ee8	Windows 10	D:\thumbnails\thumbcache_256.db
24	1d2ac44d98910ed2	160 B	0 KB	248 B	0 KB	0000000000000000	f3088b96fff2a7ef	1d2ac44d98910ed2	Windows 10	D:\thumbnails\thumbcache_256.db
25	72283bca6bedccab	248 B	0 KB	336 B	0 KB	0000000000000000	1de4b8dfa5265999	72283bca6bedccab	Windows 10	D:\thumbnails\thumbcache_256.db



```
-a---- 12/30/2020 12:24 PM 1048576 thumbcache_256.db
-a---- 12/30/2020 12:24 PM 24 thumbcache_768.db
-a---- 12/30/2020 12:24 PM 1048576 thumbcache_48.db
-a---- 12/30/2020 12:24 PM 3145728 thumbcache_96.db
-a---- 12/30/2020 12:24 PM 1048576 thumbcache_32.db
-a---- 12/30/2020 12:24 PM 1048576 thumbcache_16.db
```

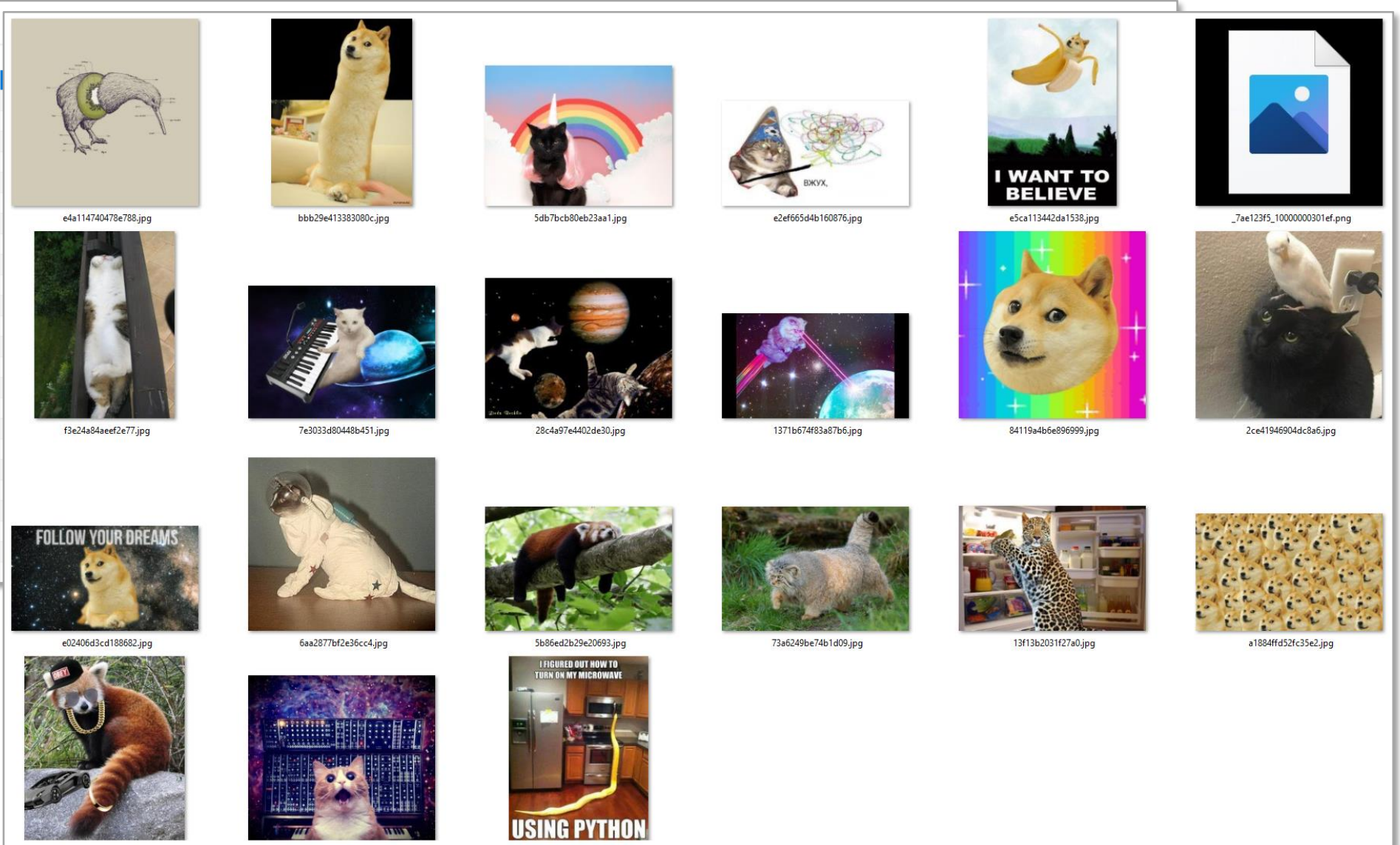
Tryin' database with largest thumbnails

Thumbcache

Thumbcache Viewer

File Edit View Tools Help

#	Filename	Cache Entry Offset	Cache Entry S...
1	af2749a243de8f76.png	295188 B	105 KB
2	bae9726a3cbeb40e.jpg	143962 B	29 KB
3	a312ef7712191b21.jpg	189302 B	27 KB
4	a1884ffd52fc35e2.jpg	125192 B	18 KB
5	13f13b2031f27a0.jpg	239446 B	17 KB
6	73a6249be74b1d09.jpg	108858 B	15 KB
7	5b86ed2b29e20693.jpg	279206 B	15 KB
8	6aa2877bf2e36cc4.jpg	173890 B	15 KB
9	e02406d3cd188682.jpg	94200 B	14 KB
10	2ce41946904dc8a6.jpg	265568 B	13 KB
11	84119a4b6e896999.jpg	61974 B	12 KB
12	1371b674f83a87b6.jpg	49452 B	12 KB
13	28c4a97e4402de30.jpg	25182 B	11 KB
14	7e3033d80448b451.jpg	37376 B	11 KB
15	f3e24a84aef2e77.jpg	227624 B	11 KB
16	?7ae123f5?1000000030...	4872 B	11 KB
17	e5ca113442da1538.jpg	75094 B	10 KB
18	e2ef665d4b160876.jpg	217822 B	8 KB
19	5db7bcb80eb23aa1.jpg	16276 B	8 KB
20	bbb29e413383080c.jpg	85544 B	8 KB
21	e4a114740478e788.jpg	257702 B	7 KB
22	4a518aaaca14ff5d.jpg	424 B	3 KB
23	::{645FF040-5081-101...	24 B	0 KB
24	1d2ac44d98910ed2	160 B	0 KB
25	72283bca6bedccab	248 B	0 KB



Thumbcache

Thumbcache Viewer

#	Filename	Cache Entry Offset	Cache Entry S...
1	af2749a243de8f76.png	295188 B	105 KB
2	bae9726a3cbeb40e.jpg	143962 B	29 KB
3	a312ef7712191b21.jpg	189302 B	27 KB
4	a1884ffd52fc35e2.jpg	125192 B	18 KB
5	13f13b2031f27a0.jpg	239446 B	17 KB
6	73a6249be74b1d09.jpg	108858 B	15 KB
7	5b86ed2b29e20693.jpg	279206 B	15 KB
8	6aa2877bf2e36cc4.jpg	173890 B	15 KB
9	e02406d3cd188682.jpg	94200 B	14 KB
10	2ce41946904dc8a6.jpg	265568 B	13 KB
11	84119a4b6e896999.jpg	61974 B	12 KB
12	1371b674f83a87b6.jpg	49452 B	12 KB
13	28c4a97e4402de30.jpg	25182 B	11 KB
14	7e3033d80448b451.jpg	37376 B	11 KB
15	f3e24a84aef2e77.jpg	227624 B	11 KB
16	?7ae123f5?1000000030...	4872 B	11 KB
17	e5ca113442da1538.jpg	75094 B	10 KB
18	e2ef665d4b160876.jpg	217822 B	8 KB

~/df/06-artifacts/windows/

Speaking of external media...

Can we link an image to a computer?

WINDOWS REGISTRY

Recent files?

Autostart?

Malware persistence?



I'm back, baby.

Connected devices?

More user to
program
mappings?

Registry

*“A **central hierarchical database** used in Windows 98, Windows CE, Windows NT, and Windows 2000 used to **store information that is necessary to configure the system for one or more users, applications, and hardware devices.**”*

<https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users>

“Central nervous system of the computer.”

– Kevin Ripa

Registry

system hives

%SystemRoot%\Windows\system32\config\

registry



user hives

%UserProfile%\NTUSER.DAT

%UserProfile%\Local Settings\Software\Microsoft\Windows\UsrClass.dat

```
PS C:\Windows\System32\config> tree /F
Volume serial number is 7AE1-23F5
```

```
C:..
| BBI
| BCD-Template
| COMPONENTS
| DEFAULT
| DRIVERS
| ELAM
| SAM
| SECURITY
| SOFTWARE
| SYSTEM
|
|---Journal
|---RegBack
|---systemprofile
|---TxR
```

- ⇒ *connected devices*
- ⇒ *network & WIFI connections*
- ⇒ *global system settings*
- ⇒ *user accounts infos*
- ⇒ *startup progs/services*
- ⇒ *moar*

```
PS C:\Users\katz> ls -Hidden
```

Mode	LastWriteTime	Length	Name
----	-----	-----	----
...			
-a-h--	1/9/2021 12:06 AM	1572864	NTUSER.DAT

- ⇒ *mounted devices*
- ⇒ *user specific settings*
- ⇒ *user activity infos*
- ⇒ *most recently used lists*
- ⇒ *applications launched*
- ⇒ *moar*

no file system access to UsrClass.dat on the running system

~_(\ツ)_/~

Registry

system hives

registry



user hives

%UserProfile%\NTUSER.DAT

%UserProfile%\Local

oft

Analysis issues:

- ⇒ complex, undocumented, proprietary
- ⇒ behavior changes between Windows versions

```
PS C:\Windows\
Volume serial
C:..
  BBI
  BCD-Templa
  COMPONENTS
  DEFAULT
  DRIVERS
  ELAM
  SAM
  SECURITY
  SOFTWARE
  SYSTEM
  Journal
  RegBack
  systemprofile
  TxR
```

⇒ moar

- ⇒ user specific settings
- ⇒ user activity infos
- ⇒ most recently used lists
- ⇒ applications launched
- ⇒ moar

Length	Name
572864	

no file system access to
UsrClass.dat
on the running system

~_(\ツ)_/~

Registry

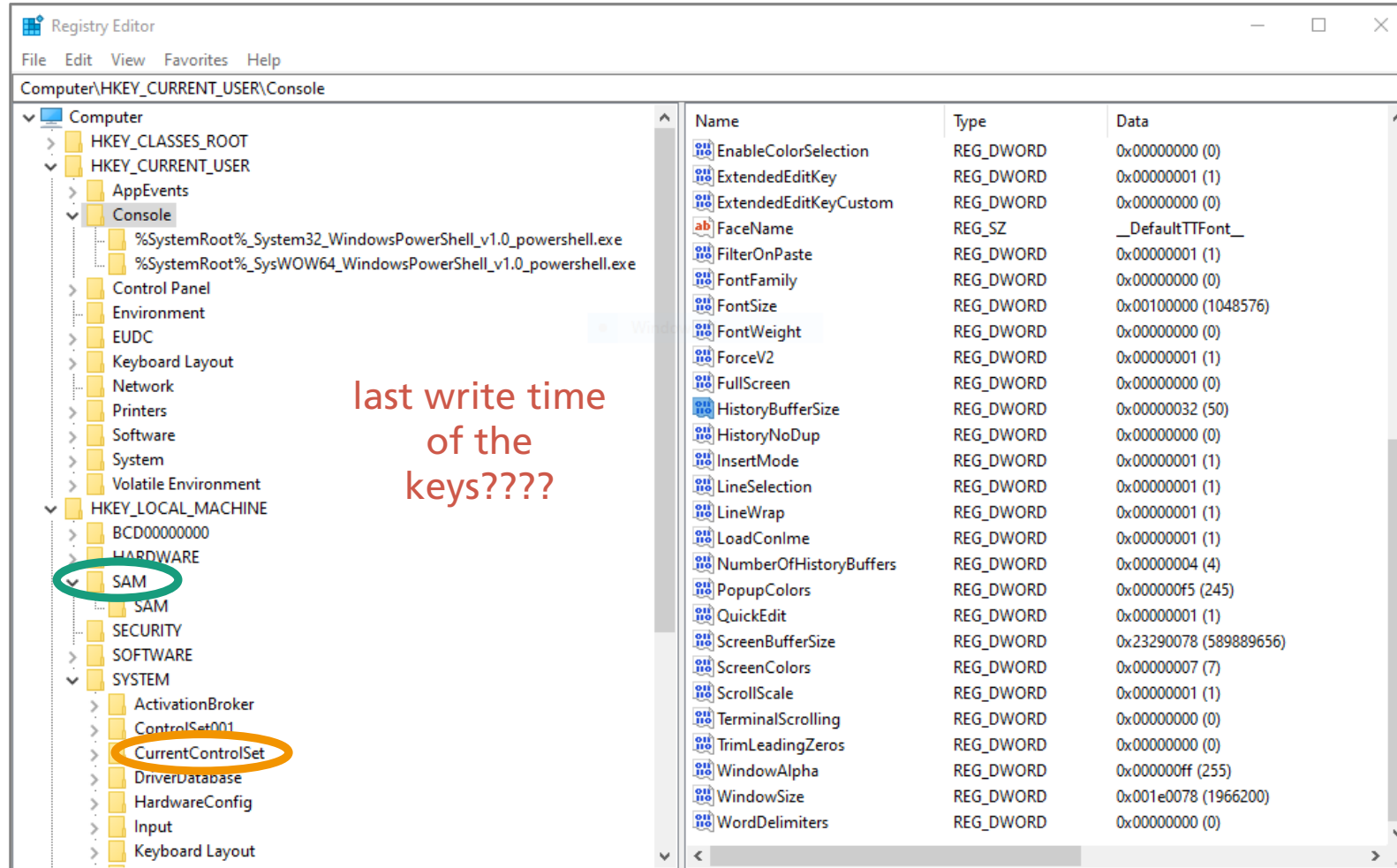
The screenshot shows the Windows Registry Editor window. The left pane displays the tree structure of the registry. The right pane shows a list of registry values for the selected key.

Annotations:

- key:** Points to the **Console** key in the left pane.
- subkey:** Points to the subkey **%SystemRoot%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe** in the left pane.
- value:** Points to the **EnableColorSelection** value in the right pane.
- value type:** Points to the **REG_DWORD** type in the right pane.
- value data:** Points to the **0x00000000 (0)** data in the right pane.

Name	Type	Data
EnableColorSelection	REG_DWORD	0x00000000 (0)
ExtendedEditKey	REG_DWORD	0x00000001 (1)
ExtendedEditKeyCustom	REG_DWORD	0x00000000 (0)
FaceName	REG_SZ	__DefaultTTFont__
FilterOnPaste	REG_DWORD	0x00000001 (1)
FontFamily	REG_DWORD	0x00000000 (0)
FontSize	REG_DWORD	0x00100000 (1048576)
FontWeight	REG_DWORD	0x00000000 (0)
ForceV2	REG_DWORD	0x00000001 (1)
FullScreen	REG_DWORD	0x00000000 (0)
HistoryBufferSize	REG_DWORD	0x00000032 (50)
HistoryNoDup	REG_DWORD	0x00000000 (0)
InsertMode	REG_DWORD	0x00000001 (1)
LineSelection	REG_DWORD	0x00000001 (1)
LineWrap	REG_DWORD	0x00000001 (1)
LoadConlme	REG_DWORD	0x00000001 (1)
NumberOfHistoryBuffers	REG_DWORD	0x00000004 (4)
PopupColors	REG_DWORD	0x000000f5 (245)
QuickEdit	REG_DWORD	0x00000001 (1)
ScreenBufferSize	REG_DWORD	0x23290078 (589889656)
ScreenColors	REG_DWORD	0x00000007 (7)
ScrollScale	REG_DWORD	0x00000001 (1)
TerminalScrolling	REG_DWORD	0x00000000 (0)
TrimLeadingZeros	REG_DWORD	0x00000000 (0)
WindowAlpha	REG_DWORD	0x000000ff (255)
WindowSize	REG_DWORD	0x001e0078 (1966200)
WordDelimiters	REG_DWORD	0x00000000 (0)

Registry



last write time
of the
keys????

unavailable
for the user

exists only on the
running system

Registry

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (1/0) View Help

Registry hives (1) Available bookmarks (1/0)

Enter text to search for: Find

now available

C:\Windows\system32\config\SAM

Associated deleted records

Key name	values	# subkeys	Last write timestamp
ROOT	0	1	2020-08-14 16:36:20
SAM	2	3	2020-08-14 23:06:53
Domains	1	2	2020-08-14 16:36:20
Account	2	3	2021-01-09 11:18:47
Aliases	1	2	2020-08-14 16:36:20
Groups	1	2	2020-08-14 16:36:20
Users	1	9	2021-01-09 11:18:47
000001F4	3	0	2020-08-14 16:37:41
000001F5	3	0	2020-08-14 16:37:41
000001F7	4	0	2020-08-14 16:37:41
000001F8	5	0	2020-08-14 16:37:41
000003E9	5	0	2020-12-30 11:16:38
000003EA	5	0	2021-01-09 11:39:42
000003EB	6	0	2021-01-11 08:03:59
000003EC	5	0	2021-01-10 17:50:53
Names	1	8	2021-01-09 11:18:47
Administrator	1	0	2020-08-14 07:38:42
DefaultAccount	1	0	2020-08-14 07:38:42
Guest	1	0	2020-08-14 07:38:42
katz	1	0	2020-12-30 11:32:54
manul	1	0	2020-12-30 11:23:08
mari	1	0	2020-08-14 09:03:21
tiger	1	0	2021-01-09 11:18:47
WDAGUtilityAccount	1	0	2020-08-14 07:38:42
Builtin	3	3	2021-01-09 12:01:46

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
F	RegB...	03-00-01-00-00-00-00-00-...	76-68-00-00	<input type="checkbox"/>	<input type="checkbox"/>
V	RegB...	00-00-00-00-F4-00-00-00-...	02-00-02-00-00-00-00-00-...	<input type="checkbox"/>	<input type="checkbox"/>
ForcePassw...	RegB...	00-00-00-00		<input type="checkbox"/>	<input type="checkbox"/>
Supplement...	RegB...	00-00-00-00-9C-05-00-00-...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
ResetData	RegB...	7B-00-22-00-76-00-65-00-...		<input type="checkbox"/>	<input type="checkbox"/>
UserTile	RegB...	01-00-00-00-03-00-00-00-...	00-00-00-00-00-00-00-00-...	<input type="checkbox"/>	<input type="checkbox"/>

data

timestamps

Type viewer

Offset	Hex	ASCII
00000000	7B 00 22 00 76 00 65 00 72 00 73 00 69 00 6F 00 6E 00 22 00 3A	{ ". v.e.r.s.i.o.n." : :
00000015	00 31 00 2C 00 22 00 71 00 75 00 65 00 73 00 74 00 69 00 6F 00	.1, ". q.u.e.s.t.i.o.
0000002A	6E 00 73 00 22 00 3A 00 58 00 78 00 22 00 71 00 75 00 65 00 73	n.s." : : [{ ". q.u.e.s
0000003F	00 74 00 69 00 6F 00 6E 00 22 00 3A 00 22 00 57 00 68 00 61 00	.t.i.o.n." : : ". W.h.a
00000054	74 00 20 00 77 00 61 00 73 00 20 00 79 00 6F 00 75 00 72 00 20	t. . w.a.s . y.o.u.r.
00000069	00 66 00 69 00 72 00 73 00 74 00 20 00 70 00 65 00 74 00 19 20	.f.i.r.s.t. . p.e.t.
0000007E	73 00 20 00 6E 00 61 00 6D 00 65 00 3F 00 22 00 2C 00 22 00 61	s . n.a.m.e.? ". , . a
00000093	00 6E 00 73 00 77 00 65 00 72 00 22 00 3A 00 22 00 6D 00 6F 00	.n.s.w.e.r." : : ". m.o
000000A8	75 00 73 00 65 00 22 00 7D 00 2C 00 78 00 22 00 71 00 75 00 65	u.s.e." } , , { ". q.u.e
000000BD	00 73 00 74 00 69 00 6F 00 6E 00 22 00 3A 00 22 00 57 00 68 00	.s.t.i.o.n." : : ". W.h.
000000D2	61 00 74 00 19 20 73 00 20 00 74 00 68 00 65 00 20 00 6E 00 61	a.t. . s . t.h.e . n.a
000000E7	00 6D 00 65 00 20 00 6F 00 66 00 20 00 74 00 68 00 65 00 20 00	.m.e . o.f . t.h.e .

Current offset: 0 (0x0) Bytes selected: 0 (0x0) Data interpreter ?

Key: ROOT\SAM\Domains\Account\Users\000003EB

Value: ResetData Collapse all hives

Selected hive: SAM Last write: 2021-01-11 08:03:59 6 of 6 values shown (100,00 %) Hive 'C:\tiger-registry\SAM' unloaded Hidden keys: 0 2

How often did a user
run an application?

When was the last run?



Registry

NTUSER.DAT: UserAssist

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (23/0) View Help

Registry hives (2) Available bookmarks (24/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
StreamMRU	2	0	2020-12-30 13:26
Streams	0	2	2020-12-30 13:26
StuckRects3	1	0	2021-01-06 13:44
Taskband	5	1	2020-12-30 17:36
TWinUI	0	1	2020-12-30 11:44
TypedPaths	6	0	2021-01-09 12:33
User Shell Folders	20	0	2020-12-30 11:33
UserAssist	0	9	2020-12-30 11:33
{9E04CAB2-CC14-11DF-BB...	1	1	2020-12-30 11:33
{A3D53349-6E61-4557-8F...	1	1	2020-12-30 11:33
{B267E3AD-A825-4A09-82...	1	1	2020-12-30 11:33
{BCB48336-4DD4-48FF-BB...	1	1	2020-12-30 11:33
{CAA59E3C-4792-41A5-99...	1	1	2020-12-30 11:33
CEBFF5CD-ACE2-4F4F-91...	1	1	2020-12-30 11:33
Count	49	0	2021-01-11 10:11
{F2A1CB5A-E3CC-4A2E-AF...	1	1	2020-12-30 11:33
{F4E57C4B-2036-45F0-A9...	1	1	2020-12-30 11:33
{FA99DFC7-6AC2-453A-A5...	1	1	2020-12-30 11:33
VirtualDesktops	0	0	2020-12-30 11:33
VisualEffects	0	19	2020-12-30 11:33
Wallpapers	7	0	2021-01-09 11:27
WordWheelQuery	4	0	2021-01-05 16:11
Ext	0	0	2020-12-30 11:33
FileAssociations	1	1	2020-12-30 11:33

Values UserAssist

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
HRZR_PGYPHNPbhag:pgbe	RegBinary	FF-FF-FF-FF-00-00-00-00...	36-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Zvpebfsg.Trfgnegrq_8jrxlo3q8oojr!Ncc	RegBinary	00-00-00-00-0E-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
HRZR_PGYFRFFVBA	RegBinary	00-00-00-00-1F-01-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Zvpebfsg.JvaqbjfSrrqonpxUho_8jrxlo3q8oojr!Ncc	RegBinary	00-00-00-00-00-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Zvpebfsg.JvaqbjfZncf_8jrxlo3q8oojr!Ncc	RegBinary	00-00-00-00-0C-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Zvpebfsg.Crbcyr_8jrxlo3q8oojr!k4p7n3o7ql2188l46q4ln362l19np5n5805r5k	RegBinary	00-00-00-00-08-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Zvpebfsg.ZvpebfsgFgvpxlAbgrf_8jrxlo3q8oojr!Ncc	RegBinary	00-00-00-00-0A-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
{INP14R77-02R7-4R5Q-O744-2RO1NR519807}FavccvatGbbj.rkr	RegBinary	00-00-00-00-0F-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
{INP14R77-02R7-4R5Q-O744-2RO1NR519807}zfcvrag.rkr	RegBinary	00-00-00-00-08-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
{INP14R77-02R7-4R5Q-O744-2RO1NR519807}labgrcnq.rkr	RegBinary	00-00-00-00-19-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
ZFRqtr.HfreQngn.Qrsnhyg	RegBinary	00-00-00-00-03-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Zvpebfsg.Jvaqbjf.PybhqRkrevrprUbfj_pj5a1u2gklrj!Ncc	RegBinary	00-00-00-00-00-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Zvpebfsg.Jvaqbjf.Pbegan_pj5a1u2gklrj!PbeganHV	RegBinary	00-00-00-00-00-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
ZFRqtr	RegBinary	00-00-00-00-07-00-00-00...	E0-A0-0A-00	<input type="checkbox"/>	<input type="checkbox"/>
P:\Hfref\Xngm\NccQngn\Ybpy\Grzc\7mF01241QR6\frghc-fgho.rkr	RegBinary	00-00-00-00-00-00-00-00...	00-00-28-00	<input type="checkbox"/>	<input type="checkbox"/>
Zvpebfsg.Jvaqbjf.Rkcybere	RegBinary	00-00-00-00-36-00-00-00...	14CD-07F9	<input type="checkbox"/>	<input type="checkbox"/>
Zvpebfsg.Jvaqbjf.Cubgbf_8jrxlo3q8oojr!Ncc	RegBinary	00-00-00-00-09-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Zvpebfsg.Jvaqbjf.FnegZrahRkrevrprUbfj_pj5a1u2gklrj!Ncc	RegBinary	00-00-00-00-00-00-00-00...	C3-7F-42-C3	<input type="checkbox"/>	<input type="checkbox"/>
jvaqbjf.vzzrefvirpbagebycnary_pj5a1u2gklrj!zvpebfsg.jvaqbjf.vzzrefvirpbagebycnary	RegBinary	00-00-00-00-03-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
30804600NS4N39PO	RegBinary	00-00-00-00-0C-00-00-00...	2D-00-34-00	<input type="checkbox"/>	<input type="checkbox"/>
Zvpebfsg.Jvaqbjf.FurryRkrevrprUbfj_pj5a1u2gklrj!Ncc	RegBinary	00-00-00-00-01-00-00-00...	43-00-6C-00	<input type="checkbox"/>	<input type="checkbox"/>
{INP14R77-02R7-4R5Q-O744-2RO1NR519807}JvaqbjfCbjeFurry\1.0\cbjefurry.rkr	RegBinary	00-00-00-00-00-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
{INP14R77-02R7-4R5Q-O744-2RO1NR519807}lpzq.rkr	RegBinary	00-00-00-00-01-00-00-00...	78-E9-08-00	<input type="checkbox"/>	<input type="checkbox"/>
{INP14R77-02R7-4R5Q-O744-2RO1NR519807}FifgrzCebcegrvrfNqnaprq.rkr	RegBinary	00-00-00-00-01-00-00-00...	35-00-32-00	<input type="checkbox"/>	<input type="checkbox"/>
P:\RMGbbj\ErvtfgelRkcybere\ErvtfgelRkcybere.rkr	RegBinary	00-00-00-00-01-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
P:\Hfref\Xngm\Qbjaybnqf\Trg-MvzreznaGbbj\ErvtfgelRkcybere\ErvtfgelRkcybere.rkr	RegBinary	00-00-00-00-22-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
P:\Hfref\Xngm\Qbjaybnqf\ernqeqp_qr_kn_peq_vafngnyy.rkr	RegBinary	00-00-00-00-00-00-00-00...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>

rot13
~_(\ツ)_/~

CEBFF5CD corresponds to GUI programs (Win 10)

Type viewer Slack viewer

```

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25
00000000 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00
00000026 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00
yyyy.....z.....z.....z.....z.....
.....z.....z.....z.....zyyyy.....

```

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Key: ROOT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count Value: HRZR_PGYPHNPbhag:pgbe Collapse all hives

Registry

executable full path

run count

last run time

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (23/0) View Help

Registry hives (2) Available bookmarks (24/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
StreamMRU	2	0	2020-12-30 13:26
Streams	0	2	2020-12-30 13:26
StuckRects3	1	0	2021-01-06 13:4
Taskband	5	1	2020-12-30 17:38
TWinUI	0	1	2020-12-30 11:4
TypedPaths	6	0	2021-01-09 12:3
User Shell Folders	20	0	2020-12-30 11:3
UserAssist	0	9	2020-12-30 11:3
{9E04CAB2-CC14-11DF-BB...	1	1	2020-12-30 11:3
{A3D53349-6E61-4557-8F...	1	1	2020-12-30 11:3
{B267E3AD-A825-4A09-82...	1	1	2020-12-30 11:3
{BCB48336-4DDD-48FF-BB...	1	1	2020-12-30 11:3
{CAA59E3C-4792-41A5-99...	1	1	2020-12-30 11:3
{CEBFF5CD-ACE2-4F4F-91...	1	1	2020-12-30 11:3
Count	49	0	2021-01-11 10:1
{F2A1CB5A-E3CC-4A2E-AF...	1	1	2020-12-30 11:3
{F4E57C4B-2036-45F0-A9...	1	1	2020-12-30 11:3
{FA99DFC7-6AC2-453A-A5...	1	1	2020-12-30 11:3
VirtualDesktops	0	0	2020-12-30 11:3
VisualEffects	0	19	2020-12-30 11:3
Wallpapers	7	0	2021-01-09 11:2
WordWheelQuery	4	0	2021-01-05 16:1
Ext	0	0	2020-12-30 11:3
FileAssociations	1	1	2020-12-30 11:3
FileHistory	0	1	2020-12-30 11:3
GameDVR	2	1	2021-01-08 05:5
Group Policy	0	2	2021-01-10 17:5
Holographic	1	2	2020-12-30 11:3
ime	0	1	2020-12-30 11:3
ImmersiveShell	1	1	2020-12-30 11:3
InstallService	0	1	2020-12-30 18:2
Internet Settings	12	10	2021-01-09 10:3
Lock Screen	3	0	2021-01-10 23:4
Mobility	0	5	2020-12-30 12:0
Notifications	0	1	2020-12-30 11:4
OOBE	0	1	2021-01-09 11:1
PenWorkspace	0	1	2020-12-30 11:3
Policies	0	0	2020-12-30 11:3
PrecisionTouchPad	11	1	2020-12-30 11:3

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UIEME_CTLSESSION	=	287	1493 0d, 20h, 53m, 04s	
Microsoft.Windows.Explorer		54	279 0d, 2h, 31m, 15s	2021-01-10 21:57:04
C:\Users\katz\Downloads\Get-ZimmermanTools\RegistryExplorer\RegistryExplorer.exe	34	141	0d, 4h, 34m, 42s	2021-01-11 09:36:35
{System32}\notepad.exe	25	102	0d, 0h, 47m, 52s	2021-01-10 23:27:39
{Program Files x86}\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	16	42	0d, 0h, 30m, 52s	2021-01-10 17:39:04
{System32}\SnippingTool.exe	15	68	0d, 0h, 31m, 11s	2021-01-09 14:17:09
Microsoft.Getstarted_8wekyb3d8bbwe!App	14	21	0d, 0h, 07m, 00s	2020-12-30 11:31:56
{System32}\WindowsPowerShell\v1.0\powershell.exe	13	241	0d, 4h, 59m, 55s	2021-01-10 16:15:38
Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App	13	19	0d, 0h, 06m, 08s	2020-12-30 11:31:56
{Windows}\regedit.exe	12	22	0d, 0h, 45m, 28s	2021-01-11 08:37:09
30B046B0AF4A39CB	12	111	0d, 2h, 13m, 38s	2021-01-10 17:38:23
Microsoft.WindowsMaps_8wekyb3d8bbwe!App	12	17	0d, 0h, 05m, 17s	2020-12-30 11:31:56
Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x	11	15	0d, 0h, 04m, 25s	2020-12-30 11:31:56
{Program Files X64}\AccessData\FTK Imager\FTK Imager.exe	10	57	0d, 0h, 51m, 38s	2021-01-09 11:58:03
C:\Users\katz\Downloads\Get-ZimmermanTools\ShellBagsExplorer\ShellBagsExplorer.exe	10	44	0d, 0h, 44m, 14s	2021-01-09 16:26:04
Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App	10	13	0d, 0h, 03m, 34s	2020-12-30 11:31:56
Microsoft.Windows.Photos_8wekyb3d8bbwe!App	9	13	0d, 0h, 02m, 09s	2021-01-09 14:20:53
{System32}\mspaint.exe	8	9	0d, 0h, 01m, 51s	2020-12-30 11:31:56
MSEdge	7	0	0d, 0h, 00m, 00s	2021-01-09 11:13:14
Microsoft.XboxGamingOverlay_8wekyb3d8bbwe!App	6	0	0d, 0h, 00m, 00s	2021-01-08 05:53:00
TheDocumentFoundation.LibreOffice.Calc	6	9	0d, 0h, 05m, 23s	2021-01-10 13:48:41
Microsoft.ScreenSketch_8wekyb3d8bbwe!App	4	5	0d, 0h, 02m, 02s	2021-01-10 13:45:22

Total rows: 49

Type viewer Slack viewer

```

00000000  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25
00000026  80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00

```

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Key: ROOT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count Value: HRZR_PGYPHPNbhag:pgbe Collapse all hives

What about recent
files?

Registry

file name corresponding last open time of a file with .pdf
Ink file extension

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (23/0) View Help

Registry hives (2) Available bookmarks (24/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
HKEY_CURRENT_USER\RecentDocs	126	22	2021-01-11 10:14
.cfg	2	0	2021-01-05 22:16
.pdf	20	0	2021-01-10 17:45
.png	21	0	2021-01-11 10:14
.ps1	2	0	2020-12-30 11:46
.tsv	2	0	2020-12-30 17:46
.txt	14	0	2021-01-10 19:51
.xlsx	3	0	2020-12-30 18:46
.zip	4	0	2020-12-30 17:25
Folder	31	0	2021-01-11 10:14
Ribbon	2	0	2020-12-30 11:44
RunMRU	0	0	2020-12-30 11:44
SearchPlatform	0	1	2020-12-30 11:33
Shell Folders	31	0	2020-12-30 11:33
Shutdown	1	0	2021-01-09 10:36
StartPage	2	0	2020-12-30 11:33
StartupApproved	0	1	2021-01-05 16:20
StreamMRU	2	0	2020-12-30 13:26
Streams	0	2	2020-12-30 13:26

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
.pdf	18	windows-intusion-discovery.pdf	windows-intusion-discovery.pdf.lnk	=	2021-01-10 17:45:52	
.pdf	17	00-trethn+G-kickoff-2019-10-10-10.pdf	00-trethn+G-kickoff-2019-10-10-10.pdf.lnk			
.pdf	16	linux-intrusion-discovery.pdf	linux-intrusion-discovery.pdf.lnk			
.pdf	15	ShellBagsExplorerManual.pdf	ShellBagsExplorerManual.pdf.lnk			
.pdf	2	RegistryExplorerManual.pdf	RegistryExplorerManual.lnk			
.pdf	14	sheet-03-enc-files.pdf	sheet-03-enc-files.lnk			
.pdf	13	windows-forensics.pdf	windows-forensics.lnk			
.pdf	8	WindowsCommandLineSheetV1.pdf	WindowsCommandLineSheetV1.lnk			
.pdf	3	windows_to_unix_cheatsheet.pdf	windows_to_unix_cheatsheet.lnk			
.pdf	5	225.pdf	225.lnk			
.pdf	6	230.pdf	230.lnk			
.pdf	7	235.pdf	235.lnk			
.pdf	12	170.pdf	170.lnk			
.pdf	11	PowerShell.pdf	PowerShell.lnk			
.pdf	10	LinuxCLI.pdf	LinuxCLI.lnk			
.pdf	9	LinuxCLI101.pdf	LinuxCLI101.lnk			
.pdf	4	hex_file_and_regex_cheat_sheet.pdf	hex_file_and_regex_cheat_sheet.lnk			
.pdf	1	EricZimmermanCommandLineToolsCheatSheet-v1.0(1).pdf	EricZimmermanCommandLineToolsCheatSheet-v1.0(1).lnk			
.pdf	0	EricZimmermanCommandLineToolsCheatSheet-v1.0.pdf	EricZimmermanCommandLineToolsCheatSheet-v1.0.lnk			

Total rows: 19

Type viewer Slack viewer

```

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25
00000000 45 00 72 00 69 00 63 00 5A 00 69 00 6D 00 6D 00 65 00 72 00 6D 00 61 00 6E 00 43 00 6F 00 6D 00 6D 00 61 00 6E 00
00000026 64 00 4C 00 69 00 6E 00 65 00 54 00 6F 00 6F 00 6C 00 73 00 43 00 68 00 65 00 61 00 74 00 53 00 68 00 65 00 65 00
0000004C 74 00 2D 00 76 00 31 00 2E 00 30 00 2E 00 70 00 64 00 66 00 00 00 00 00 32 00 00 00 00 00 00 00 00 00 00 45 72
00000072 69 63 5A 69 6D 6D 65 72 6D 61 6E 43 6F 6D 6D 61 6E 64 4C 69 6E 65 54 6F 6F 6C 73 43 68 65 61 74 53 68 65 65 74 2D
00000098 76 31 2E 30 2E 6C 6E 6B 00 00 92 00 09 00 04 00 EF BE 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000BE 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 72 00 69 00 63 00 5A 00 69 00 6D 00 6D 00 65 00 72 00
000000E4 6D 00 61 00 6E 00 43 00 6F 00 6D 00 6D 00 61 00 6E 00 64 00 4C 00 69 00 6E 00 65 00 54 00 6F 00 6F 00 6C 00 73 00
0000010A 43 00 68 00 65 00 61 00 74 00 53 00 68 00 65 00 65 00 65 00 74 00 2D 00 76 00 31 00 2E 00 30 00 2E 00 6C 00 6E 00 68 00
00000130 00 00 40 00 00 00

```

Key: ROOT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\pdf

Data interpreter ?

NTUSER.DAT:
RecentDocs

Which USB devices
were connected?



Registry

SYSTEM: USBSTOR


Registry Explorer v1.6.0.0

File Tools Options Bookmarks (27/0) View Help

Registry hives (2) Available bookmarks (50/1)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
ACPI	0	10	2020-08-14 16:36:15
ACPI_HAL	1	1	2020-08-14 16:36:15
DISPLAY	1	1	2020-08-14 16:36:20
HDAUDIO	1	1	2020-08-14 16:36:16
HID	1	1	2020-08-14 16:36:16
HTRREE	1	1	2020-08-14 16:36:15
PCI	10	10	2020-12-30 17:57:46
ROOT	15	15	2020-08-14 16:36:16
SCSI	2	2	2020-08-14 16:36:16
STORAGE	1	1	2020-08-14 16:36:16
SWD	4	4	2020-12-30 18:11:22
USB	7	7	2021-01-06 13:50:53
USBSTOR	0	3	2021-01-06 13:50:53
Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00	0	3	2021-01-06 16:48:02
4C5300001090511402480	12	2	2021-01-06 13:50:53
4C530000240824122435&0	12	2	2021-01-10 12:50:02
4C530000280818104555&0	12	2	2021-01-06 16:48:02
Disk&Ven_SanDisk&Prod_Ultra&Rev_1.00	0	2	2021-01-05 22:15:13
Disk&Ven_USB2.0&Prod_Flash_Disk&Rev_2.50	0	1	2020-12-30 18:11:22
Hardware Profiles	0	2	2021-01-09 10:38:09
Policies	0	0	2019-03-19 04:53:37
Services	0	701	2021-01-10 18:04:31
Software	0	1	2019-03-19 04:53:37
DriverDatabase	6	4	2020-12-30 18:11:22
HardwareConfig	2	1	2021-01-09 10:38:09
Input	0	2	2019-03-19 04:53:37
Keyboard Layout	0	2	2019-03-19 06:21:06
Maps	0	1	2019-03-19 04:53:37
MountedDevices	11	0	2021-01-10 12:50:54
ResourceManager	0	1	2019-03-19 04:53:37
ResourcePolicyStore	0	2	2019-03-19 04:53:37
RNG	2	0	2021-01-09 10:38:09
Select	4	0	2019-03-19 04:53:37
Setup	9	9	2021-01-06 16:48:02
Software	0	1	2019-03-19 04:53:37
State	0	1	2019-03-19 04:53:37
WaaS	0	2	2020-08-14 07:40:32
WPA	0	14	2020-12-30 18:00:22
Unassociated deleted values	20	0	



Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
DeviceDesc	RegSz	@disk.inf,%disk_devdesc%;Disk drive	74-00-2E-00	<input type="checkbox"/>	<input type="checkbox"/>
Capabilities	RegDword	16		<input type="checkbox"/>	<input type="checkbox"/>
Address	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
ContainerID	RegSz	{f15670cc-6215-5bad-8bbe-6f272bd882d1}	6E-00-64-00-6F-00	<input type="checkbox"/>	<input type="checkbox"/>
HardwareID	RegMultiSz	USBSTOR\DiskSanDisk_Cruzer_Blade____1.00 US...	35-00-2D-00	<input type="checkbox"/>	<input type="checkbox"/>
CompatibleI...	RegMultiSz	USBSTOR\Disk USBSTOR\RAW GenDisk		<input type="checkbox"/>	<input type="checkbox"/>
ClassGUID	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}	63-00-72-00-6F-00	<input type="checkbox"/>	<input type="checkbox"/>
Service	RegSz	disk	00-00	<input type="checkbox"/>	<input type="checkbox"/>
Driver	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}\0005	69-00-72-00	<input type="checkbox"/>	<input type="checkbox"/>
Mfg	RegSz	@disk.inf,%genmanufacturer%;(Standard disk d...	65-00-3F-00-6D-00	<input type="checkbox"/>	<input type="checkbox"/>
FriendlyName	RegSz	SanDisk Cruzer Blade USB Device	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
ConfigFlags	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Slack viewer Binary viewer

Value name: FriendlyName

Value type: RegSz

Value: SanDisk Cruzer Blade USB Device

Raw value: 53-00-61-00-6E-00-44-00-69-00-73-00-6B-00-20-00-43-00-72-00-75-00-7A-00-65-00-72-00-20-00-42-00-6C-00-61-00-64-00-65-00-20-00-55-00-53-00-42-00-20-00-44-00-65-00-76-00-69-00-63-00-65-00-00-00

Slack: 00-00-00-00

Key: ROOT\ControlSet001\Enum\USBSTOR\DiskVen_SanDiskProd_Cruzer_BladeRev_1.00\4C5300002408241224350

Value: FriendlyName Collapse all hives



Program execution evidence:

- *did the program run on the computer?*
- *how often?*
- *when was the last run?*

Prefetch files

```
~$ ls -Filter *.pf C:\Windows\Prefetch
```

Directory: C:\Windows\Prefetch

Mode	LastWriteTime	Length	Name	hash
-a----	11/26/2021 10:54 AM	2078	AM_DELTA_PATCH_1.353.1553.0.E-956CC28D.pf	
-a----	11/26/2021 12:32 PM	14181	APPLICATIONFRAMEHOST.EXE-CCEEF759.pf	
-a----	11/26/2021 11:15 AM	10901	ATBROKER.EXE-2E15A492.pf	
-a----	11/26/2021 12:31 PM	5715	AUDIODG.EXE-BDFD3029.pf	
-a----	11/25/2021 11:19 AM	36450	AUTORUNS.EXE-FEE2E5E8.pf	
-a----	11/26/2021 12:18 PM	11903	BACKGROUNDTASKHOST.EXE-A89D33B8.pf	
-a----	11/26/2021 10:21 AM	13483	BACKGROUNDTRANSFERHOST.EXE-4FEEC2B3.pf	
-a----	11/25/2021 11:05 AM	8174	BYTECODEGENERATOR.EXE-C1E9BCE6.pf	
-a----	11/26/2021 11:01 AM	2841	CMD.EXE-4A81B364.pf	
-a----	11/25/2021 11:32 AM	2230	CMD.EXE-AC113AA8.pf	
-a----	11/25/2021 3:25 PM	2510	COMPATTELRUNNER.EXE-DB97728F.pf	
-a----	11/26/2021 12:40 PM	10288	CONHOST.EXE-1F3E9D7E.pf	
-a----	11/26/2021 12:31 PM	27798	CONSENT.EXE-531BD9EA.pf	
-a----	11/26/2021 10:37 AM	12488	CONTROL.EXE-817F8F1D.pf	
-a----	11/26/2021 12:31 PM	5429	CSRSS.EXE-3FE41F7E.pf	
-a----	11/26/2021 10:33 AM	7763	CTFMON.EXE-9450846B.pf	
-a----	11/25/2021 11:28 AM	46191	DEVENV.EXE-B844FD26.pf	
-a----	11/26/2021 12:40 PM	10022	DLLHOST.EXE-28A8211F.pf	
-a----	11/26/2021 12:31 PM	4813	DLLHOST.EXE-504C779A.pf	
-a----	11/26/2021 4:27 AM	4869	DLLHOST.EXE-570206E5.pf	
-a----	11/26/2021 12:46 PM	3641	DLLHOST.EXE-5E46FA0D.pf	
-a----	11/26/2021 10:49 AM	10255	DLLHOST.EXE-6FCDC72B.pf	
-a----	11/26/2021 9:40 AM	6360	DLLHOST.EXE-CA6900A0.pf	
-a----	11/26/2021 9:37 AM	11397	DLLHOST.EXE-D22EEB48.pf	
-a----	11/26/2021 10:24 AM	12019	DLLHOST.EXE-D46AA2AE.pf	
-a----	11/26/2021 11:16 AM	4462	DLLHOST.EXE-D8E67ED6.pf	
-a----	11/3/2021 3:36 PM	6940	DLLHOST.EXE-E86779C7.pf	
-a----	11/26/2021 10:37 AM	5158	DLLHOST.EXE-ECB71776.pf	
-a----	11/26/2021 12:40 PM	3752	DLLHOST.EXE-FC981FFE.pf	

application name

hash

Location:

C:\Windows\Prefetch\

- Binary
- Proprietary
- Created automatically on (first) execution of a program
- Used to pre-load - „pre-fetch“- resources needed by a program

```
~$ pecmd -f C:\Windows\Prefetch\SUSPICIOUS-BINARY.EXE-5F20DE50.pf
```

```
[...]
Processing 'C:\Windows\Prefetch\SUSPICIOUS-BINARY.EXE-5F20DE50.pf'
```

```
Created on: 2021-11-26 11:16:09
Modified on: 2021-11-26 11:49:01
Last accessed on: 2021-11-26 11:50:19
```

```
Executable name: SUSPICIOUS-BINARY.EXE
Hash: 5F20DE50
File size (bytes): 6.046
Version: Windows 10 size of what??? 0_0
```

```
Run count: 3
Last run: 2021-11-26 11:48:51
Other run times: 2021-11-26 11:40:31, 2021-11-26 11:15:59
```

Volume information:

```
#0: Name: \VOLUME{01d7d109adab1526-86adbfce} Serial: 86ADBFCE Created: 2021-11-03 23:22:32 Directories: 5 File references: 14
```

Directories referenced: 5

- 0: \VOLUME{01d7d109adab1526-86adbfce}\USERS
- 1: \VOLUME{01d7d109adab1526-86adbfce}\USERS\LYNX
- 2: \VOLUME{01d7d109adab1526-86adbfce}\USERS\LYNX\DOWNLOADS
- 3: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS
- 4: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32

Files referenced: 11

- 00: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\NTDLL.DLL
- 01: \VOLUME{01d7d109adab1526-86adbfce}\USERS\LYNX\DOWNLOADS\SUSPICIOUS-BINARY.EXE
- 02: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\KERNEL32.DLL
- 03: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\KERNELBASE.DLL
- 04: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\LOCALE.NLS
- 05: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\UCRTBASE.DLL
- 06: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\MSVCP140.DLL

the same executable is run from a different locations => multiple prefetch files with different hashes

executable name

eight-character hash of the executable full path

Run count. Obviously.

Timestamps of last eight runs

directory where the executable lies

Serial number of the volume

executable full path

```
~$ pecmd -f C:\Windows\Prefetch\SUSPICIOUS-BINARY.EXE-5F20DE50.pf
```

```
[...]
Processing 'C:\Windows\Prefetch\SUSPICIOUS-BINARY.EXE-5F20DE50.pf'
```

```
Created on: 2021-11-26 11:16:09
Modified on: 2021-11-26 11:49:01
Last accessed on: 2021-11-26 11:50:19
```

Possibly first execution time (unreliable)

the same executable is run from a different locations => multiple prefetch files with different hashes

```
Executable name: SUSPICIOUS-BINARY.EXE
Hash: 5F20DE50
File size (bytes): 6.046
Version: Windows 10
```

Last run time (more or less)

size of what??? 🤖_🤖

```
Run count: 3
Last run: 2021-11-26 11:48:51
Other run times: 2021-11-26 11:40:31, 2021-11-26 11:15:59
```

Run count. Obviously.

Timestamps of last eight runs

Volume information:

```
#0: Name: \VOLUME{01d7d109adab1526-86adbfce} Serial: 86ADBFCE Created: 2021-11-03 23:22:32 Directories: 5 File references: 14
```

Directories referenced: 5

directory where the executable lies

Serial number of the volume

- 0: \VOLUME{01d7d109adab1526-86adbfce}\USERS
- 1: \VOLUME{01d7d109adab1526-86adbfce}\USERS\LYNX
- 2: \VOLUME{01d7d109adab1526-86adbfce}\USERS\LYNX\DOWNLOADS
- 3: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS
- 4: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32

executable full path

Files referenced: 11

- 00: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\NTDLL.DLL
- 01: \VOLUME{01d7d109adab1526-86adbfce}\USERS\LYNX\DOWNLOADS\SUSPICIOUS-BINARY.EXE
- 02: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\KERNEL32.DLL
- 03: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\KERNELBASE.DLL
- 04: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\LOCALE.NLS
- 05: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\UCRTBASE.DLL
- 06: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\MSVCP140.DLL

```
~$ pecmd -f C:\Windows\Prefetch\SUSPICIOUS-BINARY.EXE-5F20DE50.pf
```

```
[...]  
Processing 'C:\Windows\Prefetch\SUSPICIOUS-BINARY.EXE-5F20DE50.pf'
```

```
Created on: 2021-11-26 11:16:09  
Modified on: 2021-11-26 11:49:01  
Last accessed on: 2021-11-26 11:50:19
```

```
Executable name: SUSPICIOUS-BINARY.EXE  
Hash: 5F20DE50  
File size (bytes): 6.046  
Version: Windows 10
```

```
Run count: 3  
Last run: 2021-11-26 11:48:51  
Other run times: 2021-11-26 11:40:31, 2021-11-26 11:15:59
```

Volume information:

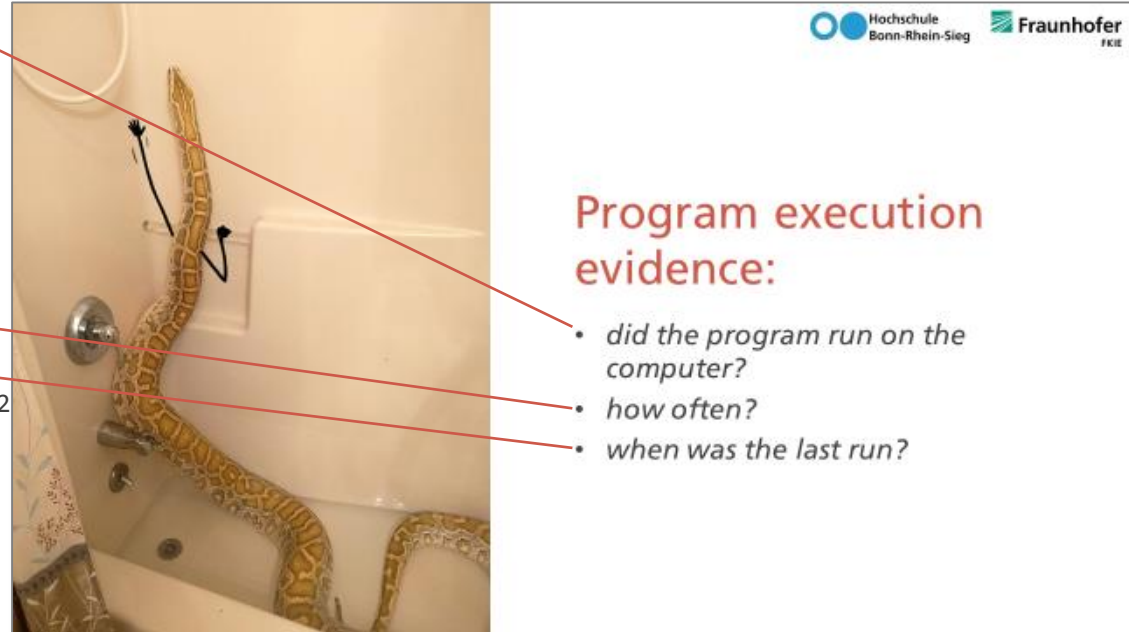
```
#0: Name: \VOLUME{01d7d109adab1526-86adbfce} Serial: 86ADBFCE Created: 202
```

Directories referenced: 5

```
0: \VOLUME{01d7d109adab1526-86adbfce}\USERS  
1: \VOLUME{01d7d109adab1526-86adbfce}\USERS\LYNX  
2: \VOLUME{01d7d109adab1526-86adbfce}\USERS\LYNX\DOWNLOADS  
3: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS  
4: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32
```

Files referenced: 11

```
00: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\NTDLL.DLL  
01: \VOLUME{01d7d109adab1526-86adbfce}\USERS\LYNX\DOWNLOADS\SUSPICIOUS-BINARY.EXE  
02: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\KERNEL32.DLL  
03: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\KERNELBASE.DLL  
04: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\LOCALE.NLS  
05: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\UCRTBASE.DLL  
06: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\MSVCP140.DLL
```



Program execution evidence:

- did the program run on the computer?
- how often?
- when was the last run?

Know normal

```
~$ ls -Filter *.pf C:\Windows\Prefetch | select Name
```

```
[...]
BACKGROUNDTASKHOST.EXE-A89D33B8.pf
BACKGROUNDTRANSFERHOST.EXE-4FEEC2B3.pf
BYTECODEGENERATOR.EXE-C1E9BCE6.pf
CMD.EXE-4A81B364.pf
CMD.EXE-AC113AA8.pf
COMPATTELRUNNER.EXE-DB97728F.pf
CONHOST.EXE-1F3E9D7E.pf
CONSENT.EXE-531BD9EA.pf
CONTROL.EXE-817F8F1D.pf
CSRSS.EXE-3FE41F7E.pf
CTFMON.EXE-9450846B.pf
DEVENV.EXE-B844FD26.pf
DLLHOST.EXE-28A8211F.pf
DLLHOST.EXE-504C779A.pf
DLLHOST.EXE-570206E5.pf
DLLHOST.EXE-5E46FA0D.pf
[...]
EXPLORER.EXE-A80E4F97.pf
FIREFOX_INSTALLER.EXE-3706D5A8.pf
FIREFOX.EXE-A606B53C.pf
FIRSTLOGONANIM.EXE-674CDAB9.pf
FONTDRVHOST.EXE-31E45F6D.pf
GETHELP.EXE-CC7E4E5F.pf
HELPPANE.EXE-FEDC965B.pf
IDENTITY_HELPER.EXE-DC893A1C.pf
IPCONFIG.EXE-912F3D5B.pf
LOCKAPP.EXE-59620D5A.pf
MMC.EXE-53159585.pf
MMC.EXE-EF66D102.pf
LOGONUI.EXE-09140401.pf
MICROSOFT_PHOTOS.EXE-250E9CBF.pf
MICROSOFT_SERVICEHUB.CONTROLL-0D86E532.pf
MICROSOFTEDGEUPDATE.EXE-C4317749.pf
MICROSOFTEDGEUPDATECOMPREGISTE_3E0DDFD1.pf
NOTEPAD.EXE-D8414F97.pf
ONEDRIVE.EXE-0C970464.pf
ONEDRIVESETUP.EXE-3197492C.pf
POWERSHELL.EXE-920BBA2A.pf
REG.EXE-E7E8BD26.pf
REGEDIT.EXE-90FEEA06.pf
RUNDLL32.EXE-23EA2E5B.pf
RUNDLL32.EXE-3A5F5976.pf
RUNDLL32.EXE-5A6C2401.pf
[...]
RUNTIMEBROKER.EXE-06226CEB.pf
RUNTIMEBROKER.EXE-06A7E291.pf
RUNTIMEBROKER.EXE-3977076E.pf
[...]
SC.EXE-945D79AE.pf
SCHTASKS.EXE-5CA45734.pf
SEARCHAPP.EXE-0651CA85.pf
SHELLEXPERIENCEHOST.EXE-066223DB.pf
SHELLEXPERIENCEHOST.EXE-A3608B1E.pf
SMSS.EXE-E9C28FC6.pf
SPPSVC.EXE-B0F8131B.pf
STARTMENUEXPERIENCEHOST.EXE-76B447E1.pf
SUSPICIOUS-BINARY.EXE-5F20DE50.pf
SVCHOST.EXE-033BBABB.pf
SVCHOST.EXE-090AEBE5.pf
SVCHOST.EXE-0B3A9016.pf
SVCHOST.EXE-0B80E7F6.pf
SVCHOST.EXE-1190E58E.pf
[...]
TASKHOSTW.EXE-3E0B74C8.pf
TEXTINPUTHOST.EXE-18B298A2.pf
TEXTINPUTHOST.EXE-4AE33179.pf
TIWORKER.EXE-A68903B5.pf
TRACKER.EXE-AF1EC648.pf
TRUSTEDINSTALLER.EXE-3CC53155.pf
```

Know normal

```
~$ ls -Filter *.pf C:\Windows\Prefetch | select Name
```

```
[...]
BACKGROUNDTASKHOST.EXE-A89D33B8.pf
BACKGROUNDTRANSFERHOST.EXE-4FEEC2B3.pf
BYTECODEGENERATOR.EXE-C1E9BCE6.pf
CMD.EXE-4A81B364.pf
CMD.EXE-AC113AA8.pf
COMPATTELRUNNER.EXE-DB97728F.pf
CONHOST.EXE-1F3E9D7E.pf
CONSENT.EXE-531BD9EA.pf
CONTROL.EXE-817F8F1D.pf
CSRSS.EXE-3FE41F7E.pf
CTFMON.EXE-9450846B.pf
DEVENV.EXE-B844FD26.pf
DLLHOST.EXE-28A8211F.pf
DLLHOST.EXE-504C779A.pf
DLLHOST.EXE-570206E5.pf
DLLHOST.EXE-5E46FA0D.pf
[...]
EXPLORER.EXE-A80E4F97.pf
FIREFOX_INSTALLER.EXE-3706D5A8.pf
FIREFOX.EXE-A606B53C.pf
FIRSTLOGONANIM.EXE-674CDAB9.pf
FONTDRVHOST.EXE-31E45F6D.pf
GETHELP.EXE-CC7E4E5F.pf
HELPPANE.EXE-FEDC965B.pf
IDENTITY_HELPER.EXE-DC893A1C.pf
IPCONFIG.EXE-912F3D5B.pf
LOCKAPP.EXE-59620D5A.pf
MMC.EXE-53159585.pf
MMC.EXE-EF66D102.pf
LOGONUI.EXE-09140401.pf
MICROSOFT_PHOTOS.EXE-250E9CBF.pf
MICROSOFT_SERVICEHUB.CONTROLL-0D86E532.pf
MICROSOFTEDGEUPDATE.EXE-C4317749.pf
MICROSOFTEDGEUPDATECOMPREGISTE_3E0DDFD1.pf
```

manages processes and threads

hosts COM processes

file explorer

logon guys

```
NOTEPAD.EXE-D8414F97.pf
ONEDRIVE.EXE-0C970464.pf
ONEDRIVESETUP.EXE-3197492C.pf
POWERSHELL.EXE-920BBA2A.pf
REG.EXE-E7E8BD26.pf
REGEDIT.EXE-90FEEA06.pf
RUNDLL32.EXE-23EA2E5B.pf
RUNDLL32.EXE-3A5F5976.pf
RUNDLL32.EXE-5A6C2401.pf
[...]
RUNTIMEBROKER.EXE-06226CEB.pf
RUNTIMEBROKER.EXE-06A7E291.pf
RUNTIMEBROKER.EXE-3977076E.pf
[...]
SC.EXE-945D79AE.pf
SCHTASKS.EXE-5CA45734.pf
SEARCHAPP.EXE-0651CA85.pf
SHELLEXPERIENCEHOST.EXE-066223DB.pf
SHELLEXPERIENCEHOST.EXE-A3608B1E.pf
SMSS.EXE-E9C28FC6.pf
SPPSVC.EXE-B0F8131B.pf
STARTMENUEXPERIENCEHOST.EXE-76B447E1.pf
SUSPICIOUS-BINARY.EXE-5F20DE50.pf
SVCHOST.EXE-033BBABB.pf
SVCHOST.EXE-090AEBE5.pf
SVCHOST.EXE-0B3A9016.pf
SVCHOST.EXE-0B80E7F6.pf
SVCHOST.EXE-1190E58E.pf
[...]
TASKHOSTW.EXE-3E0B74C8.pf
TEXTINPUTHOST.EXE-18B298A2.pf
TEXTINPUTHOST.EXE-4AE33179.pf
TIWORKER.EXE-A68903B5.pf
TRACKER.EXE-AF1EC648.pf
TRUSTEDINSTALLER.EXE-3C6531E5.pf
```

runs dlls as executables

it's complicated....

session manager

hosts service dlls

runs Windows tasks

manages Windows Updates

Find evil (or suspicious at least)

```
~$ ls -Filter *.pf C:\Windows\Prefetch | select Name
```

```
[...]
BACKGROUNDTASKHOST.EXE-A89D33B8.pf
BACKGROUNDTRANSFERHOST.EXE-4FEEC2B3.nf
BYTECODEGENERATOR.EXE-C1E9BCE6.pf
CMD.EXE-4A81B364.pf
CMD.EXE-AC113AA8.pf
COMPATTELRUNNER.EXE-DB97728F.pf
CONHOST.EXE-1F3E9D7E.pf
CONSENT.EXE-531BD9EA.pf
CONTROL.EXE-817F8F1D.pf
CSRSS.EXE-3FE41F7E.pf
CTFMON.EXE-9450846B.pf
DEVENV.EXE-B844FD26.pf
DLLHOST.EXE-28A8211F.pf
DLLHOST.EXE-504C779A.pf
DLLHOST.EXE-570206E5.pf
DLLHOST.EXE-5E46FA0D.pf
[...]
EXPLORER.EXE-A80E4F97.pf
FIREFOX_INSTALLER.EXE-3706D5A8.pf
FIREFOX.EXE-A606B53C.pf
FIRSTLOGONANIM.EXE-674CDAB9.pf
FONTDRVHOST.EXE-31E45F6D.pf
GETHELP.EXE-CC7E4E5F.pf
HELPPANE.EXE-FEDC965B.pf
IDENTITY_HELPER.EXE-DC893A1C.pf
IPCONFIG.EXE-912F3D5B.pf
LOCKAPP.EXE-59620D5A.pf
MMC.EXE-53159585.pf
MMC.EXE-EF66D102.pf
LOGONUI.EXE-09140401.pf
MICROSOFT_PHOTOS.EXE-250E9CBF.pf
MICROSOFT_SERVICEHUB.CONTROLL-0D86E532.pf
MICROSOFTEDGEUPDATE.EXE-C4317749.pf
MICROSOFTEDGEUPDATECOMBEGISTE_350DD5D1.pf
```


cmd.exe, powershell.exe:
shells
command-line access & remote execution

sc.exe, schtasks.exe:
services and tasks cmd utilities
persistence & [remote] execution

```
NOTEPAD.EXE-D8414F97.pf
ONEDRIVE.EXE-0C970464.pf
ONEDRIVESETUP.EXE-3197492C.pf
POWERSHELL.EXE-920BBA2A.pf
REG.EXE-E7E8BD26.pf
REGEDIT.EXE-90FEEA06.pf
RUNDLL32.EXE-23EA2E5B.pf
RUNDLL32.EXE-3A5F5976.pf
RUNDLL32.EXE-5A6C2401.pf
[...]
RUNTIMEBROKER.EXE-06226CEB.pf
RUNTIMEBROKER.EXE-06A7E291.pf
RUNTIMEBROKER.EXE-3977076E.pf
[...]
SC.EXE-945D79AE.pf
SCHTASKS.EXE-5CA45734.pf
SEARCHAPP.EXE-0651CA85.pf
SHELLEXPERIENCEHOST.EXE-066223
SHELLEXPERIENCEHOST.EXE-A3608B
SMSS.EXE-E9C28FC6.pf
SPPSVC.EXE-B0F8131B.pf
STARTMENUMEXPERIENCEHOST.EXE-76
SUSPICIOUS-BINARY.EXE-5F20DE50
SVCHOST.EXE-033BBABB.pf
SVCHOST.EXE-090AEBE5.pf
SVCHOST.EXE-0B3A9016.pf
SVCHOST.EXE-0B80E7F6.pf
SVCHOST.EXE-1190E58E.pf
[...]
TASKHOSTW.EXE-3E0B74C8.pf
TEXTINPUTHOST.EXE-18B298A2.pf
TEXTINPUTHOST.EXE-4AE33179.pf
TIWORKER.EXE-A68903B5.pf
TRACKER.EXE-AF1EC648.pf
TRUSTEDINSTALLER.EXE-3CC53155.pf
```

reg.exe:
registry cmd utility
persistence (registry key modification)

- More suspicious stuff:
- at.exe: *privilege escalation*
 - net.exe: *mapping drives for lateral movement, enumerate groups*
 - wmic.exe: *remote execution*
 - rar.exe: *data exfiltration*
 - SysInternals PsTools:
 - PsExec: *remote execution*
 - PSLoggedOn: *logon enumeration*
 - ProcDump: *dumping credentials from memory*



Hochschule
Bonn-Rhein-Sieg

Fraunhofer
FKIE

**Program execution
evidence:**

- *did the program run on the computer?*
- *how often?*
- *when was the last run?*

Moar program execution evidence

Amcache

Location:

C:\Windows\appcompat\Programs\Amcache.hve

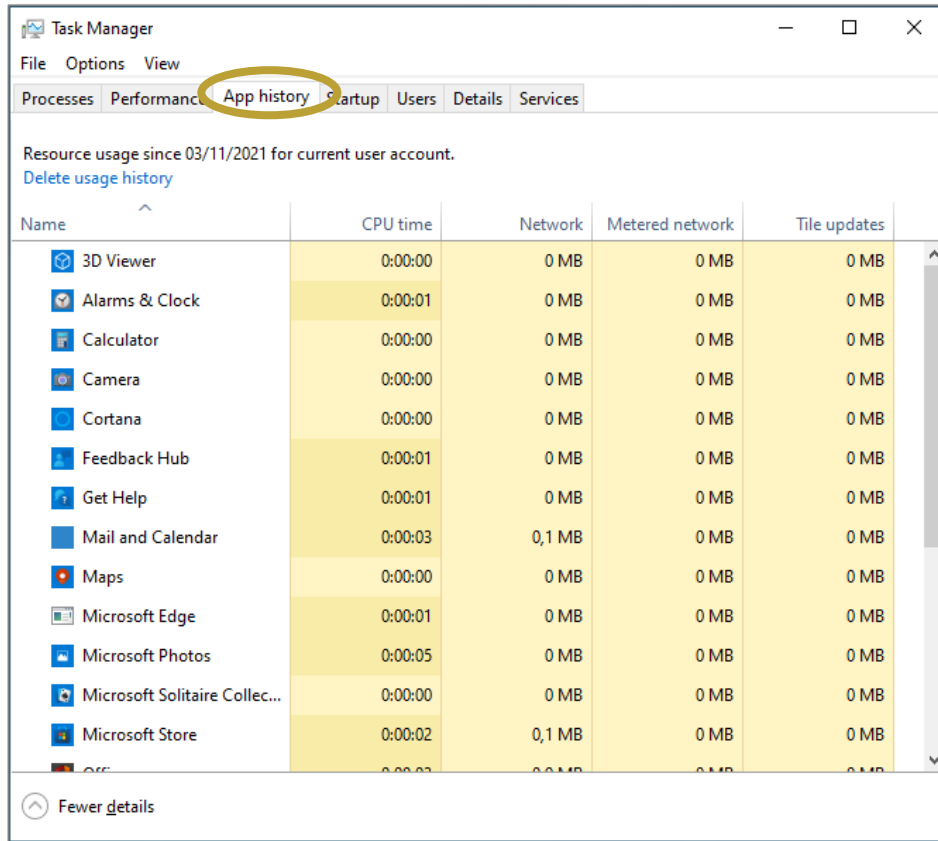
~\$ AmcacheParser.exe -i -f C:\Windows\appcompat\Programs\Amcache.hve --csv Z:\amcache\

#	B	C	D	E	F	G	H	I	J	K	L
Programid	FileKeyLastWriteTimestamp	SHA1	IsOComponent	FullPath	Name	FileExtension	LinkDate	ProductName	Size	Version	
1	00061153ea89f528c5a21853d7763d38c95800000904	25.11.2021 10:24	d1825c3e44b7bce02d41f0c3e93f8762c5b9e9	False	c:\users\lynx\documents\programs\autoruns\autoruns.exe	.exe	26.10.2021 18:41	sysinternals autoruns	2497400		
2	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:09	b4108c1d6832f0d036eedcd3d7f684d43be04996	True	c:\windows\system32\compattelrunner.exe	.exe			160072	10.0.19645.1029 (winbuild.160720)	
3	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:09	11eba7b1e26c7d492a2c161ac48370811d0b01e	True	c:\windows\system32\csrss.exe	.exe			17600	10.0.19041.546 (winbuild.160720)	
4	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:09	9914f5914c02add1d3590844a628b3c5a5fa2c48	True	c:\windows\system32\devicecensus.exe	.exe			57672	10.0.19645.1029 (winbuild.160720)	
5	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:09	70f820592c0f63d39181c77284a426fef17ad6a	True	c:\windows\system32\drvinst.exe	.exe			350208	10.0.19041.928 (winbuild.160720)	
6	00069ee783c59a352b570ff3481793a68510000ffff	25.11.2021 10:30	c3bc5b7df388924a8b655c0ca69db1e20481e441	False	c:\users\lynx\source\repos\levitask\x64\release\levitask.exe	.exe	25.11.2021 10:30		11776		
7	0006781b32ae4b40eaa20eb9ba3a4f5adb00000904	25.11.2021 09:09	1d7a8052eebfba8c395cfd543c5a4efb57a0a	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgecomregistershellarm	.exe	19.02.2021 05:54	microsoft edge	163752	1.3.141.63	
8	0006f9368d1ce8356b0711cefb486c9e3d00000904	25.11.2021 09:09	1a6d250bb90113e323a7081f86cc733525ab400a	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgeupdateondemand.exe	.exe	19.02.2021 05:54	microsoft edge update	101288	1.3.141.63	
9	0006f9368d1ce8356b0711cefb486c9e3d00000904	25.11.2021 09:09	2454bc252496eae5e859e2c016b01707178	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgeupdatesetup.exe	.exe	19.02.2021 05:55	microsoft edge update	1783720	1.3.141.63	
10	0006f9368d1ce8356b0711cefb486c9e3d00000904	25.11.2021 09:09	9f76ef75fb7b0e7cbf90b96be9490600f4b34ad6	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgeupdate.exe	.exe	19.02.2021 05:54	microsoft edge update	214952	1.3.141.63	
11	0006f9368d1ce8356b0711cefb486c9e3d00000904	25.11.2021 09:09	9204f1571532a61dc0f795c350db6591340076c	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgeupdatecore.exe	.exe	19.02.2021 05:54	microsoft edge update	242088	1.3.141.63	
12	0006f9368d1ce8356b0711cefb486c9e3d00000904	25.11.2021 09:09	50a14bbf37ad85a3c53b487df1a7024a633e80e	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgeupdatebroker.exe	.exe	19.02.2021 05:54	microsoft edge update	101288	1.3.141.63	
13	0006f9368d1ce8356b0711cefb486c9e3d00000904	25.11.2021 09:09	9f76ef75fb7b0e7cbf90b96be9490600f4b34ad6	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgeupdate.exe	.exe	19.02.2021 05:54	microsoft edge update	214952	1.3.141.63	
14	0006f9368d1ce8356b0711cefb486c9e3d00000904	25.11.2021 09:09	9b2dee8860b22d27b8f81b3d371955cfd13be17b8	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgeupdatecomregistershellarm	.exe	19.02.2021 05:54	microsoft edge update	208296	1.3.141.63	
15	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:09	7750ce7170633339d10aed3aaefbc03b589064a	True	c:\windows\system32\mosucoreworker.exe	.exe			1538048	10.0.19041.906 (winbuild.160720)	
16	0006a3875f747b7ab583589050f11aeb59d00000904	25.11.2021 09:09	27f72f7c554e7a4385116649920ce11f766473b4	False	c:\programdata\microsoft\windows defender\platform\4.18.2110.6.0\mpcmdrun.exe	.exe	08.10.2011 19:17	microsoft windows operating system	901056	4.18.2110.6 (winbuild.160101)	
17	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:09	5d6102f5a170e982c7b2c9c1a0a0d435f1d	True	c:\windows\system32\msiexec.exe	.exe			69632	5.0.19041.1 (winbuild.160101)	
18	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:09	85536ad6faee43b728ed12ee8ffca41f74f6446	True	c:\program files\windows defender\msmpeng.exe	.exe	18.01.1993 16:54	microsoft windows operating system	103384	4.18.1909.6 (winbuild.160101)	
19	0006a3875f747b7ab583589050f11aeb59d00000904	25.11.2021 09:09	ce74a47c0959491bab221156774cb276e4e43	True	c:\programdata\microsoft\windows defender\platform\4.18.2110.6.0\msmpeng.exe	.exe	05.11.2062 16:43	microsoft windows operating system	128376	4.18.2110.6 (winbuild.160101)	
20	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:09	9aae97e24c54838786df253403ccc405594d2	True	c:\windows\system32\musnotificat.exe	.exe			689664	10.0.19041.906 (winbuild.160720)	
21	0006a3875f747b7ab583589050f11aeb59d00000904	25.11.2021 09:09	ea94143582d2c2dcd6f4d0b4b7f08db03fab069c	False	c:\programdata\microsoft\windows defender\platform\4.18.2110.6.0\nissrv.exe	.exe	24.05.1975 10:53	microsoft windows operating system	2872024	4.18.2110.6 (winbuild.160101)	
22	0006df8f19f0e05c89330971e8f66e2c3500000904	25.11.2021 09:09	93be70fa9485709880238d32a4a00ff1547e26	False	c:\users\lynx\appdata\local\microsoft\onedrive\onedrive.exe	.exe	15.02.1976 08:12	microsoft onedrive	252440		
23	000651ddd855a3a37f94406e2f75418870400000904	25.11.2021 09:09	aeb72a0fa95e53305054edc9f1d09a8a17d3bb1	False	c:\users\lynx\appdata\local\microsoft\onedrive\onedrivesetup.exe	.exe	25.06.2021 12:12	microsoft onedrive	4870312		
24	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:09	ce8669d8826c8795115d58c6e2726ae53943dce9	True	c:\windows\system32\onedrivesetup.exe	.exe			3087020	1.904	
25	000651ddd855a3a37f94406e2f75418870400000904	25.11.2021 09:09	afb1026d608a0d8d7351ab2dcb2e62ef9f988f7	False	c:\users\lynx\appdata\local\microsoft\onedrive\onedrivesetup.exe	.exe	23.03.1970 14:01	microsoft onedrive	4072312		
26	000638a1b9b57566585011ed5b422fcb00000904	25.11.2021 09:50	efeeec83af5715e3e19935c855225274d0e52	False	c:\users\lynx\documents\programs\processexplorer\procp.exe	.exe	17.08.2021 02:07	process explorer	2839416	16.43	
27	0006e51efa8a67107b2dceef4f3f8e4f40c00000000	25.11.2021 10:57	as606c758769487c384d11cb7850ff73704aa	False	c:\users\lynx\documents\programs\registryexplorer\registryexplorer.exe	.exe	08.10.2021 17:25	registry explorer	62116088	1.6.0.0	
28	000680120503c9b46f9f03d88cc9b03d00000904	25.11.2021 09:15	c52fcb2bc203d73cf54c55936149c3a6c9ef3	False	c:\users\lynx\appdata\local\temp\72502cd58f3\setup-stub.exe	.exe	24.07.2021 22:21	firefox	477616	94.0.2	
29	000656c1dcd3135db5c1699d5a0ed954fae00000904	25.11.2021 09:16	b4d0496b3de4bcecd1dd0f3df87501ccc36c7cb	False	c:\program files (x86)\microsoft\edgeupdate\install\dec39d2f-dcb8-474a-bdae-ab876e208	.exe	12.01.2021 23:56	microsoft edge installer	2873744	96.0.1054.34	
30	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:05	0897b4076ec223a6f3c27d78197a615f0d50ad52	True	c:\windows\system32\sihclient.exe	.exe			394144	10.0.19041.1288 (winbuild.160720)	
31	00064d72d8fa466a9e19ee593394048d46f0000ffff	26.11.2021 17:28	e5f22d92cb8e2cd0d0616c4a5ea66d97c0d4b096	False	c:\users\lynx\downloads\suspicious-binary.exe	.exe	25.11.2021 10:32		11776		
32	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:09	01d0b7461e45b41c886192df6d425ba8d42d82	True	c:\windows\system32\svchost.exe	.exe			57360	10.0.19041.546 (winbuild.160720)	
33	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:11	fed4b4a753a9541389a870c69e624be07569ccd	True	c:\windows\system32\taskhost.exe	.exe	21.06.2081 11:10	microsoft windows operating system	97096	10.0.19041.906 (winbuild.160720)	
34	00009322624d44355f8a5e015d309d08bd20000904	03.11.2021 15:13	8ce2b2054a5f303a413a4efc212277851834c1	False	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856d364e35_10.0.19041.1310_x-ww	.exe	20.11.2018 17:35	microsoft windows operating system	281936	10.0.19041.1310 (winbuild.160720)	
35	00061cefb8bbaab60f7f0a7f325e278c1c00000904	25.11.2021 09:09	d912efb63512665f16762e34d54f5a684a70fdbca	False	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856d364e35_10.0.19041.1310_x-ww	.exe			239416	10.0.19041.925 (winbuild.160720)	
36	00067856a2d414db7579050fa23e79f9e90000904	03.11.2021 14:51	3e0f810ef3e0a36c13c97ee8246784fb7cbbc	False	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856d364e35_10.0.19041.1310_x-ww	.exe	13.07.2099 10:15	microsoft windows operating system	281928	10.0.19041.1220 (winbuild.160720)	
37	00069457203cf8d4798b6e2443aee7e9090000ffff	26.11.2021 11:12	95fe5ae2f89d9c5d73963955d8ba684a70fdbca	False	c:\users\lynx\downloads\very-suspicious-binary.exe	.exe	22.11.2021 13:36		63488		
38	00062a25971c1e41e8f9ccac8e8d32cfa000000000	25.11.2021 09:54	ff7b88904ed09c159f5faebf81e9f6af264	False	c:\users\lynx\appdata\local\temp\b6bc20481404a7b2c1208594744\vs_bootstrapper_d15\vs_setup_bootstrapper.exe	.exe	19.05.2087 07:44	visual studio	301952	21.152.58712	
39	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:13	dd5f35048912997ed108f80c9d12ce47e3b684a	True	c:\windows\system32\werfault.exe	.exe	26.07.2039 22:39	microsoft windows operating system	586632	10.0.19041.1081 (winbuild.160720)	
40	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:09	7b2e3990de386df08a049ecb611b9ab17c1497c	True	c:\windows\system32\winlogon.exe	.exe	02.11.1995 04:19	microsoft windows operating system	946460	10.0.19041.1266 (winbuild.160720)	
41	0000f519fee486de87e73cb92d3ca802400000000	25.11.2021 09:09	3f5c88006e75e1fbbd8de658d1d66aeac432de75	True	c:\windows\system32\wuauclt.exe	.exe			64008	10.0.19041.906 (winbuild.160720)	

Program name
Full path
SHA1 base 16

suspicious-binary.exe
c:\users\lynx\downloads\suspicious-binary.exe
e5f22d92cb8e2cd0d0616c4a5ea66d97c0d4b096

SRUM: system resource usage monitor



SRUM is a feature in modern Windows systems which collect statistics on execution of binaries. The information is stored in an Extensible Storage Engine (ESE) database. ESE is Microsoft's proprietary single file database format, acting similarly to SQLite, as a default storage engine for many applications — including the SRUM database.

[<https://velociraptor.velocidex.com/digging-into-the-system-resource-usage-monitor-srum-afbadb1a375>]

SRUM: system resource usage monitor

Task Manager window showing resource usage since 03/11/2021 for the current user account. The 'App history' tab is selected. The table lists various applications and their resource usage.

Name	CPU time	Network	Metered network	Tile updates
3D Viewer	0:00:00	0 MB	0 MB	0 MB
Alarms & Clock	0:00:01	0 MB	0 MB	0 MB
Calculator	0:00:00	0 MB	0 MB	0 MB
Camera	0:00:00	0 MB	0 MB	0 MB
Cortana	0:00:00	0 MB	0 MB	0 MB
Feedback Hub	0:00:01	0 MB	0 MB	0 MB
Get Help	0:00:01	0 MB	0 MB	0 MB
Mail and Calendar	0:00:03	0,1 MB	0 MB	0 MB
Maps	0:00:00	0 MB	0 MB	0 MB
Microsoft Edge	0:00:01	0 MB	0 MB	0 MB
Microsoft Photos	0:00:05	0 MB	0 MB	0 MB
Microsoft Solitaire Collec...	0:00:00	0 MB	0 MB	0 MB
Microsoft Store	0:00:02	0,1 MB	0 MB	0 MB

View -> Show history for all Processes

Task Manager window showing resource usage since 03/11/2021 for the current user and system accounts. The 'App history' tab is selected. The table lists various system processes and their resource usage. The process 'suspicious-binary.exe' is circled in red.

Name	CPU time	Network	Metered network	Tile updates
suspicious.exe	0:00:01	0 MB	0 MB	0 MB
suspicious-binary.exe	0:00:01	0 MB	0 MB	0 MB
Sysinternals Process Expl...	0:00:01	0 MB	0 MB	0 MB
System	0:17:05	9,9 MB	0 MB	0 MB
System Guard Runtime ...	0:00:08	0 MB	0 MB	0 MB
System interrupts	0:44:32	0 MB	0 MB	0 MB
Task Manager	0:00:10	0 MB	0 MB	0 MB
TimeZone Sync Task	0:00:01	0 MB	0 MB	0 MB
Tips	0:00:00	0 MB	0 MB	0 MB
Uninstalled processes	0:11:55	98,4 MB	0 MB	0 MB
Updateability From SCM	0:00:01	0 MB	0 MB	0 MB
User OOBE Broker	0:00:01	0 MB	0 MB	0 MB
Userinit Logon Application	0:00:01	0 MB	0 MB	0 MB

SRUM: system resource usage monitor

Location:

C:\Windows\System32\sru\SRUDB.dat - ESE DB

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SRUM\Extensions

While running, Windows temporarily stores this data in the `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SRUM\Extensions` and writes to `SRUDB.dat` at shutdown. SRUM contains a wealth of information about user activity including the full path to executables, CPU time in the foreground and background, and the SID responsible for execution.

You can expect to find the last 30 days of application data in SRUM.

[<https://frsecure.com/blog/windows-forensics-execution/>]

Name	CPU time	Network	Metered network	Tile updates
suspicious.exe	0:00:01	0 MB	0 MB	0 MB
User OOBE Broker	0:00:01	0 MB	0 MB	0 MB
Userinit Logon Application	0:00:01	0 MB	0 MB	0 MB

SRUM: system resource usage monitor

```
~$ SrumECmd.exe -f Z:\srum\SRUDB.dat -r Z:\srum\software.hve --csv Z:\srum\
```

A	B	C	D	E	F	G	H	I	J	K	L	
1	Id	Timestamp	ExeInfo	ExeInfoDescription	ExeTimestamp	SidType	Sid	UserName	Userld	Appld	EndTime	DurationMs
2762	3850	25.11.2021 20:53	sqlwriter.exe		04/30/2016 06:30:29 +00:00	LocalSystem	S-1-5-18	systemprofile	6	906	2021-11-25 20:52:59.6107282	102063
2763	3970	25.11.2021 20:55	sqlwriter.exe		04/30/2016 06:30:29 +00:00	LocalSystem	S-1-5-18	systemprofile	6	906	2021-11-25 20:55:02.0411014	110593
2764	4080	25.11.2021 20:57	sqlwriter.exe		04/30/2016 06:30:29 +00:00	LocalSystem	S-1-5-18	systemprofile	6	906	2021-11-25 20:57:00.0101628	60000
2765	4179	25.11.2021 21:52	sqlwriter.exe		04/30/2016 06:30:29 +00:00	LocalSystem	S-1-5-18	systemprofile	6	906	2021-11-25 21:12:00.0103852	456000
2766	5377	26.11.2021 08:42	sqlwriter.exe		04/30/2016 06:30:29 +00:00	LocalSystem	S-1-5-18	systemprofile	6	906	2021-11-26 08:41:01.2959388	397395
2767	5608	26.11.2021 09:08	sqlwriter.exe		04/30/2016 06:30:29 +00:00	LocalSystem	S-1-5-18	systemprofile	6	906	2021-11-26 09:02:00.0055549	792934
2768	6070	26.11.2021 09:42	sqlwriter.exe		04/30/2016 06:30:29 +00:00	LocalSystem	S-1-5-18	systemprofile	6	906	2021-11-26 09:40:00.0023445	479987
2769	6267	26.11.2021 10:01	sqlwriter.exe		04/30/2016 06:30:29 +00:00	LocalSystem	S-1-5-18	systemprofile	6	906	2021-11-26 10:01:51.1390596	670520
2770	6514	26.11.2021 10:15	sqlwriter.exe		04/30/2016 06:30:29 +00:00	LocalSystem	S-1-5-18	systemprofile	6	906	2021-11-26 10:04:00.0137168	59999
2771	6868	26.11.2021 11:44	sqlwriter.exe		04/30/2016 06:30:29 +00:00	LocalSystem	S-1-5-18	systemprofile	6	906	2021-11-26 11:44:00.0272873	359996
2772	2342	25.11.2021 11:53	SrTasks.exe		08/06/2024 08:17:24 +00:00	LocalSystem	S-1-5-18	systemprofile	6	1271	2021-11-25 11:50:00.0047388	59998
2773	1913	25.11.2021 11:07	StandardCollector.Service.exe		05/01/2019 06:11:54 +00:00	LocalSystem	S-1-5-18	systemprofile	6	1163	2021-11-25 10:36:00.0038076	360000
2774	6518	26.11.2021 10:15	suspicious.exe		11/25/2021 10:32:16 +00:00	UnknownOrUserSid	S-1-5-21-1469023789-276253711-1706919858-1001	lynx	304	1657	2021-11-26 10:15:00.0141615	120000
2775	6598	26.11.2021 10:44	suspicious.exe		11/25/2021 10:32:16 +00:00	UnknownOrUserSid	S-1-5-21-1469023789-276253711-1706919858-1001	lynx	304	1657	2021-11-26 10:15:41.1233338	41110
2776	6853	26.11.2021 11:44	suspicious-binary.exe		11/25/2021 10:32:16 +00:00	UnknownOrUserSid	S-1-5-21-1469023789-276253711-1706919858-1001	lynx	304	1663	2021-11-26 11:42:00.0118646	239997
2777	6992	26.11.2021 12:02	suspicious-binary.exe		11/25/2021 10:32:16 +00:00	UnknownOrUserSid	S-1-5-21-1469023789-276253711-1706919858-1001	lynx	304	1663	2021-11-26 11:50:00.0119067	120000
2778	8293	26.11.2021 17:42	suspicious-binary.exe		11/25/2021 10:32:16 +00:00	UnknownOrUserSid	S-1-5-21-1469023789-276253711-1706919858-1001	lynx	304	1663	2021-11-26 17:29:00.0276735	180015
2779	1077	25.11.2021 09:10	svchost.exe	[netsvcs] [UserManager]	12/14/1972 16:22:50 +00:00	LocalSystem	S-1-5-18	systemprofile	6	58	2021-11-25 09:10:00.0163861	491252
2780	1079	25.11.2021 09:10	svchost.exe	[LocalService] [SstpSvc]	12/14/1972 16:22:50 +00:00	LocalService	S-1-5-19	LocalService	4	303	2021-11-25 09:10:00.0163861	491252
2781	1080	25.11.2021 09:10	svchost.exe	[NetworkService] [CryptSvc]	12/14/1972 16:22:50 +00:00	NetworkService	S-1-5-20	NetworkService	30	61	2021-11-25 09:10:00.0163861	491252
2782	1081	25.11.2021 09:10	svchost.exe	[RPCSS]	12/14/1972 16:22:50 +00:00	NetworkService	S-1-5-20	NetworkService	30	29	2021-11-25 09:10:00.0163861	491252
2783	1082	25.11.2021 09:10	svchost.exe	[NetworkService] [LanmanWorkstation]	12/14/1972 16:22:50 +00:00	NetworkService	S-1-5-20	NetworkService	30	52	2021-11-25 09:10:00.0163861	491252
2784	1087	25.11.2021 09:10	svchost.exe	[LocalServiceNetworkRestricted] [WinHttpAutoProxySvc]	12/14/1972 16:22:50 +00:00	LocalService	S-1-5-19	LocalService	4	59	2021-11-25 09:10:00.0163861	491252
2785	1088	25.11.2021 09:10	svchost.exe	[netsvcs] [g								
2786	1089	25.11.2021 09:10	svchost.exe	[UnistackSv								
2787	1090	25.11.2021 09:10	svchost.exe	[LocalServi								
2788	1091	25.11.2021 09:10	svchost.exe	[netsvcs] [S								
2789	1093	25.11.2021 09:10	svchost.exe	[LocalServi								
2790	1094	25.11.2021 09:10	svchost.exe	[LocalServi								
2791	1095	25.11.2021 09:10	svchost.exe	[NetworkS								
2792	1096	25.11.2021 09:10	svchost.exe	[netsvcs] [V								
2793	1097	25.11.2021 09:10	svchost.exe	[LocalServi								
2794	1098	25.11.2021 09:10	svchost.exe	[LocalServi								
2795	1099	25.11.2021 09:10	svchost.exe	[LocalSyste								
2796	1102	25.11.2021 09:10	svchost.exe	[LocalSyste								
2797	1103	25.11.2021 09:10	svchost.exe	[DcomLaun								

Program name

suspicious-binary.exe

User

lynx

SID


S-1-5-21-1469023789-276253711-1706919858-1001

Some execution end-times

2021-11-26 11:42:00.0118646

2021-11-26 11:50:00.0119067

2021-11-26 17:29:00.0276735



Hochschule
Bonn-Rhein-Sieg


Fraunhofer
FKIE

Program execution evidence:

- *did the program run on the computer?*
- *how often?*
- *when was the last run?*

~/df/06-artifacts/

Artifacts



Luckily, the artifacts for common questions are already well researched and documented. Until the next update, that is "_(:)_"

Let's start with some operating system artifacts!

Speaking about Windows updates...

Shimcache

Location:

```
SYSTEM\ControlSet001\Control\Session Manager\AppCompatCache
```

Before Windows 10:
evidence of **program execution**.

After Windows 10:
Not anymore!
Generated for all executables (almost).

Used to check if certain **executables are present on the system**.

System compatibility database
Helps identify Windows compatibility issues with software.

© Registry Explorer

Shimcache

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (27/0) View Help

Registry hives (1) Available bookmarks (27/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
C:\Windows\system32\config...	=	=	1601-01-01 00:00:00
{4d36e972-e325-11ce-bfc1-080...	5	13	2021-11-26 08:33:00
{53f56307-b6bf-11d0-94f2-00a...	0	1	2021-11-03 14:24:36
{6bdd1fc6-810f-11d0-bec7-080...	6	2	2019-12-07 09:13:43
AppCompatCache	3	0	2021-11-26 17:42:48
bam	7	1	2021-11-03 14:24:37
Devices	0	0	2021-11-03 15:11:32
ComputerName	2	0	2021-11-03 14:26:13
CrashControl	10	1	2019-12-07 09:51:08
DeviceClasses	0	65	2021-11-26 08:49:03
Environment	15	0	2021-11-25 09:59:13
EventLog	16	9	2021-11-03 14:24:46
FilesNotToSnapshot	8	0	2019-12-07 09:51:08
FileSystem	26	0	2021-11-03 14:24:37
FirewallPolicy	4	7	2019-12-07 09:16:23
Memory Management	16	2	2021-11-26 17:42:57

Bookmark information

Hive: C:\Windows\system32\config\SYSTEM

Category: Program execution

Name: AppCompatCache

Key path: ControlSet001\Control\Session Manager\AppCompatCache

Short description: System compatibility database

Long description: Helps identify Windows compatibility issues with software. Be sure to check ControlSet002 for additional entries as well

Values

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
AppCompatCache	RegBinary	34-00-00-00-11-34-00-00-00-00-00-00-B6-01...	00-00-00-00-00-00-00-00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>
CacheMainSdb	RegBinary	31-30-74-73-73-9E-8F-AE-1C-00-00-00-16-0...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
SdbTime	RegBinary	66-BC-69-21-C3-D0-D7-01-00-00-00-00-00-0...	92-7B-89-2F	<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Slack viewer AppCompatCache

Cache Entry Position	Program Name	Modified Time
0	C:\Users\ynx\AppData\Local\Temp\CB183F78-4E71-4280-B2ED-5020-FED5482A\dismhost.exe	2021-04-09 13:49:56
1	C:\Users\ynx\Downloads\suspicious-binary.exe	2021-11-25 10:32:16
2	C:\Users\ynx\Downloads\more-evil - Copy.exe	2021-11-25 10:32:16
3	C:\Users\ynx\Downloads\very-suspicious-binary.exe	2021-11-22 13:36:59
4	C:\Users\ynx\Downloads\evil - Copy.exe	2021-11-22 13:36:59
5	C:\Windows\system32\reg.exe	2019-12-07 09:09:13
6	C:\Windows\suspicious.exe	2021-11-25 19:39:03
7	indows\SoftwareDistribution\Download\Install\AM_Delta_Patch_3.1553.0.exe	2021-11-26 09:54:03
8	indows\PSEXESVC.exe	2021-11-26 10:12:35
9	C:\Windows\system32\perfmom.exe	2019-12-07 09:09:26
10	C:\Windows\system32\WerFault.exe	2021-11-03 14:57:55
11	C:\Users\ynx\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\Microsoft.SharePoint.exe	2021-11-25 09:05:08
12	0000000b 00600000041e0022 000a00004a610000 8664 Microsoft.MicrosoftEdge.Stable 8wekyb3d8bbwe	1601-01-01 00:00:00
13	C:\Program Files (x86)\Microsoft\Edge\Application\96.0.1054.34\identity_helper.exe	2021-11-23 03:41:45

executed

never executed

Total rows: 522

Export ?

Key: ControlSet001\Control\Session Manager\AppCompatCache

Value: AppCompatCache Collapse all hives

Selected hive: SYSTEM Last write: 26/11/2021 17:42:48 +00:00 3 of 3 values shown (100,00 %)

Hidden keys: 0 11



Are there any traces of
malware persistence?

Persistence

*Persistence consists of techniques that adversaries use to **keep access to systems across restarts, changed credentials, and other interruptions** that could cut off their access.*

[<https://attack.mitre.org/tactics/TA0003/>]

*Once **malware gains access to a system**, it often looks **to be there for a long time**. This behavior is known as **persistence**. If the persistence mechanism is unique enough, it can even serve as a great way to fingerprint a given piece of malware.*

[<https://www.oreilly.com/library/view/practical-malware-analysis/9781593272906/ch12s04.html>]



Registry autostart keys

The following run keys are created by default on Windows systems:

- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce`

Run keys may exist under multiple hives.^{[2][3]} The `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx` is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency.^[4] For example, it is possible to load a DLL at logon using a "Depend" key with `RunOnceEx: reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.dll]"`^[5]

The following Registry keys can be used to set startup folder items for persistence:

- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`

The following Registry keys can control automatic startup of services during boot:

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices`

Using policy settings to specify startup programs creates corresponding values in either of two Registry keys:

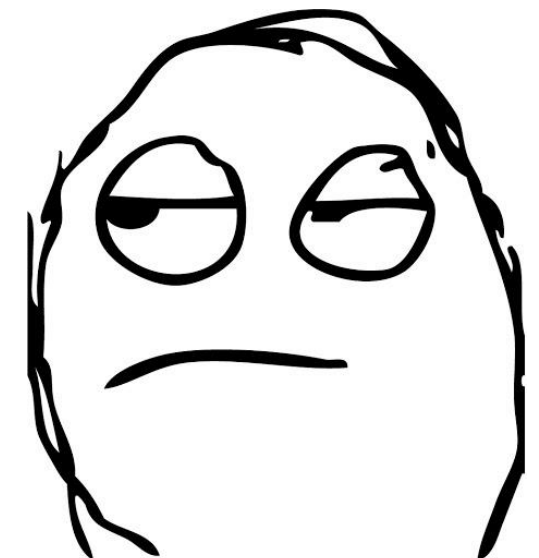
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run`

The Winlogon key controls actions that occur when a user logs on to a computer running Windows 7. Most of these actions are under the control of the operating system, but you can also add custom actions here. The `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit` and `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell` subkeys can automatically launch programs.

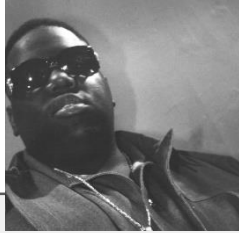
Programs listed in the load value of the registry key `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows` run when any user logs on.

By default, the multistring `BootExecute` value of the registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager` is set to `autocheck autochk *`. This value causes Windows, at startup, to check the file-system integrity of the hard disks if the system has been shut down abnormally. Adversaries can add other programs or processes to this registry value which will automatically launch at boot.

Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](#) to make the Registry entries look as if they are associated with legitimate programs.



Registry



the most notorious persistence mechanism ever

NTUSER, SYSTEM: Run-key

Microsoft\Windows\CurrentVersion\Run

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (23/1) View Help

Registry hives (1) Available bookmarks (23/1)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
Ext	0	0	2020-12-30 11:33:37
FileAssociations	1	1	2020-12-30 11:33:34
FileHistory	0	1	2020-12-30 11:33:31
GameDVR	2	1	2021-01-08 05:55:07
Group Policy	0	2	2021-01-11 13:55:46
Holographic	1	2	2020-12-30 11:33:53
ime	0	1	2020-12-30 11:33:31
ImmersiveShell	1	1	2020-12-30 11:33:55
InstallService	0	1	2020-12-30 18:26:19
Internet Settings	12	10	2021-01-11 13:50:10
Lock Screen	3	0	2021-01-11 13:55:57
Mobility	0	5	2020-12-30 12:07:43
Notifications	0	1	2020-12-30 11:43:33
OOBE	0	1	2021-01-09 11:18:47
PenWorkspace	0	1	2020-12-30 11:33:31
Policies	0	0	2020-12-30 11:33:31
PrecisionTouchPad	11	1	2020-12-30 11:33:31
Privacy	3	0	2020-12-30 11:34:40
PushNotifications	1	4	2020-12-30 11:34:43
RADAR	2	0	2020-12-30 11:33:31
Run	2	0	2021-01-11 13:55:50
RunOnce	0	0	2021-01-06 13:43:56
Screensavers	0	4	2020-12-30 11:33:31
Search	16	5	2021-01-11 13:57:44
Security and Maintenance	0	2	2020-12-30 11:36:41
SettingSync	4	1	2020-12-30 11:34:41
Shell Extensions	1	1	2020-12-30 11:33:36
SignalManager	0	1	2020-12-30 11:33:55
SmartGlass	1	0	2020-12-30 11:33:31
StartLayout	0	1	2020-12-30 11:33:40
StartupNotify	1	0	2021-01-09 22:38:25
StorageSense	0	2	2020-12-30 11:44:44
Store	0	1	2021-01-10 16:15:17
TaskFlow	1	0	2020-12-30 11:33:40
Telephony	0	1	2020-12-30 11:33:31
ThemeManager	11	0	2020-12-30 16:53:22
Themes	9	3	2020-12-30 11:33:38
UFH	0	1	2020-12-30 11:33:35
Uninstall	0	1	2020-12-30 11:44:55
WindowsSettings	0	0	2020-12-30 11:33:31

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
OneDrive	RegSz	"C:\Users\katz\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background		<input type="checkbox"/>	<input type="checkbox"/>
REExplorer	RegSz	"C:\Users\katz\Downloads\Get-ZimmermanTools\RegistryExplorer\RegistryExplorer.exe"		<input type="checkbox"/>	<input type="checkbox"/>

suspicious executable from Downloads folder...

Type viewer Binary viewer

Value name REExplorer

Value type RegSz

Value C:\Users\katz\Downloads\Get-ZimmermanTools\RegistryExplorer\RegistryExplorer.exe"

Raw value 43-00-3A-00-5C-00-55-00-73-00-65-00-72-00-73-00-5C-00-68-00-61-00-74-00-7A-00-5C-00-44-00-6F-00-77-00-6E-00-6C-00-6F-00-61-00-64-00-73-00-5C-00-47-00-65-00-74-00-2D-00-5A-00-69-00-6D-00-6D-00-65-00-72-00-6D-00-61-00-6E-00-54-00-6F-00-6F-00-6C-00-73-00-5C-00-52-00-65-00-67-00-69-00-73-00-74-00-72-00-79-00-45-00-78-00-70-00-6C-00-6F-00-72-00-65-00-72-00-5C-00-52-00-65-00-67-00-69-00-73-00-74-00-72-00-79-00-45-00-78-00-70-00-6C-00-6F-00-72-00-65-00-72-00-2E-00-65-00-78-00-65-00-22-00-00-00

Key: ROOT\Software\Microsoft\Windows\CurrentVersion\Run Value: REExplorer Collapse all hives

Registry



the most notorious persistence mechanism ever

NTUSER, SYSTEM: Run-key

Microsoft\Windows\CurrentVersion\Run

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (23/1) View Help

Registry hives (1) Available bookmarks (23/1)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
Ext	0	0	2020-12-30 11:33:37
FileAssociations	1	1	2020-12-30 11:33:34
FileHistory	0	1	2020-12-30 11:33:31
GameDVR	2	1	2021-01-08 05:55:07
Group Policy	0	2	2021-01-11 13:55:46
Holographic	1	2	2020-12-30 11:33:53
ime	0	1	2020-12-30 11:33:31
ImmersiveShell	1	1	2020-12-30 11:33:55
InstallService	0	1	2020-12-30 18:26:19
Internet Settings	12	10	2021-01-11 13:50:10
Lock Screen	3	0	2021-01-11 13:55:57
Mobility	0	5	2020-12-30 12:07:43
Notifications	0	1	2020-12-30 11:43:33
OOBE	0	1	2021-01-09 11:18:47
PenWorkspace	0	1	2020-12-30 11:33:31
Policies	0	0	2020-12-30 11:33:31
PrecisionTouchPad	11	1	2020-12-30 11:33:31
Privacy	3	0	2020-12-30 11:34:40
PushNotifications	1	4	2020-12-30 11:34:43
RADAR	2	0	2020-12-30 11:33:31
Run	2	0	2021-01-11 13:55:50
RunOnce	0	0	2021-01-06 13:43:56
Screensavers	0	4	2020-12-30 11:33:31
Search	16	5	2021-01-11 13:57:44
Security and Maintenance	0	2	2020-12-30 11:36:41
SettingSync	4	1	2020-12-30 11:34:41
Shell Extensions	1	1	2020-12-30 11:33:36
SignalManager	0	1	2020-12-30 11:33:55
SmartGlass	1	0	2020-12-30 11:33:31
StartLayout	0	1	2020-12-30 11:33:40
StartupNotify	1	0	2021-01-09 22:38:25
StorageSense	0	2	2020-12-30 11:44:44
Store	0	1	2021-01-10 16:15:17
TaskFlow	1	0	2020-12-30 11:33:40
Telephony	0	1	2020-12-30 11:33:31
ThemeManager	11	0	2020-12-30 16:53:22
Themes	9	3	2020-12-30 11:33:38
UFH	0	1	2020-12-30 11:33:35
Uninstall	0	1	2020-12-30 11:44:55
WindowsSettings	0	0	2020-12-30 11:23:21

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
OneDrive	RegSz	"C:\Users\katz\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background		<input type="checkbox"/>	<input type="checkbox"/>
REExplorer	RegSz	"C:\Users\katz\Downloads\Get-ZimmermanTools\RegistryExplorer\RegistryExplorer.exe"		<input type="checkbox"/>	<input type="checkbox"/>

suspicious executable from Downloads folder...

~/df/06-artifacts/windows/registry/ Hochschule Bonn-Rhein-Sieg Fraunhofer FKIE

Are there any traces of malware persistence?

Key: ROOT\Software\Microsoft\Windows\CurrentVersion\Run Value: REExplorer Collapse all hives

...looking for
rogue services on
the system...



Services

*In Windows NT operating systems, a **Windows service** is a computer program that operates in the background. It is similar in concept to a Unix daemon[...]*

Windows services can be configured to start when the operating system is started and run in the background as long as Windows is running[...]

Services

Name	Description	Status	Startup Type	Log On As
Touch Keyboard and Handwriting Panel Service	Enables Touch Keyboard and Han...	Running	Manual (Trig...	Local System
Udk User Service_2fe84	Shell components service		Manual	Local System
Update Orchestrator Service	Manages Windows Updates. If sto...	Running	Automatic (...)	Local System
UPnP Device Host	Allows UPnP devices to be hosted ...		Manual	Local Service
User Data Access_2fe84	Provides apps access to structured...	Running	Manual	Local System
User Data Storage_2fe84	Handles storage of structured user...	Running	Manual	Local System
User Experience Virtualization Service	Provides support for application a...		Disabled	Local System
User Manager	User Manager provides the runtim...	Running	Automatic (T...	Local System
User Profile Service	This service is responsible for loadi...	Running	Automatic	Local System
Virtual Disk	Provides management services for...		Manual	Local System
VirtualBox Guest Additions Service	Manages VM runtime information...	Running	Automatic	Local System
Visual Studio Standard Collector Service 150	Visual Studio Data Collection Servi...		Manual	Local System
Volume Shadow Copy	Manages and implements Volume...		Manual	Local System
Volumetric Audio Compositor Service	Hosts spatial analysis for Mixed Re...		Manual	Local Service
WalletService	Hosts objects used by clients of th...		Manual	Local System
WarpJITSvc	Provides a JIT out of process servic...		Manual (Trig...	Local Service
Web Account Manager	This service is used by Web Accou...	Running	Manual	Local System
WebClient	Enables Windows-based programs...		Manual (Trig...	Local Service
Wi-Fi Direct Services Connection Manager Service	Manages connections to wireless s...		Manual (Trig...	Local Service
Windows Audio	Manages audio for Windows-base...	Running	Automatic	Local Service
Windows Audio Endpoint Builder	Manages audio devices for the Wi...	Running	Automatic	Local System
Windows Backup	Provides Windows Backup and Re...		Manual	Local System
Windows Biometric Service	The Windows biometric service gi...		Manual (Trig...	Local System
Windows Camera Frame Server	Enables multiple clients to access ...		Manual (Trig...	Local System
Windows Connect Now - Config Registrar	WCNCSVC hosts the Windows Co...		Manual	Local Service
Windows Connection Manager	Makes automatic connect/discon...	Running	Automatic (T...	Local Service
Windows Defender Advanced Threat Protection Service	Windows Defender Advanced Thre...		Manual	Local System
Windows Defender Firewall	Windows Defender Firewall helps ...	Running	Automatic	Local Service
Windows Encryption Provider Host Service	Windows Encryption Provider Hos...		Manual (Trig...	Local Service
Windows Error Reporting Service	Allows errors to be reported when ...		Manual (Trig...	Local System
Windows Event Collector	This service manages persistent su...		Manual	Network Service
Windows Event Log	This service manages events and e...	Running	Automatic	Local Service
Windows Font Cache Service	Optimizes performance of applica...	Running	Automatic	Local Service
Windows Image Acquisition (WIA)	Provides image acquisition service...		Manual	Local Service
Windows Insider Service	Provides infrastructure support for...		Manual (Trig...	Local System
Windows Installer	Adds, modifies, and removes appli...		Manual	Local System
Windows License Manager Service	Provides infrastructure support for...		Manual (Trig...	Local Service
Windows Management Instrumentation	Provides a common interface and ...	Running	Automatic	Local System
Windows Management Service	Performs management including ...		Manual	Local System
Windows Mobile Hotspot Service	Provides the ability to share cellu...		Manual (Trig...	Local Service
Windows Modules Installer	Enables installation, modification, ...		Manual	Local System
Windows Perception Service	Enables spatial perception, spatial ...		Manual (Trig...	Local Service
Windows Perception Simulation Service	Enables spatial perception simulati...		Manual	Local System
Windows Push Notifications System Service	This service runs in session 0 and h...	Running	Automatic	Local System
Windows Push Notifications User Service_2fe84	This service hosts Windows notific...	Running	Automatic	Local System
Windows PushToInstall Service	Provides infrastructure support for...		Manual (Trig...	Local System
Windows Remote Management (WS-Management)	Windows Remote Management (...)		Manual	Network Service
Windows Search	Provides content indexing, proper...	Running	Automatic (...)	Local System
Windows Security Service	Windows Security Service handles ...	Running	Manual	Local System
Windows Threat Protection	Protects your computer from mali...	Running	Automatic	Local System
Windows Time	Maintains date and time synchron...		Manual (Trig...	Local Service
Windows Update	Enables the detection, download, ...	Running	Manual (Trig...	Local System
Windows Update Medic Service	Enables remediation and protectio...		Manual	Local System
WinHTTP Web Proxy Auto-Discovery Service	WinHTTP implements the client H...	Running	Manual	Local Service
Wired AutoConfig	The Wired AutoConfig (DOT3SVC) ...		Manual	Local System
WLAN AutoConfig	The WLANSVC service provides th...		Manual	Local System
WMI Performance Adapter	Provides performance library infor...		Manual	Local System
Work Folders	This service syncs files with the W...		Manual	Local Service
Workstation	Creates and maintains client netw...	Running	Automatic	Network Service

In V computer

Windows s system is sta

ows service is a kind. It is similar to unix daemon[...] the operating system as Windows is running[...]

Services

User-friendly name and description

Name	Description	Status	Startup Type	Log On As
Touch Keyboard and Handwriting Panel Service	Enables Touch Keyboard and Han...	Running	Manual (Trig...	Local System
Udk User Service_2fe84	Shell components service		Manual	Local System
Update Orchestrator Service	Manages Windows Updates. If sto...	Running	Automatic (...)	Local System
UPnP Device Host	Allows UPnP devices to be hosted ...		Manual	Local System
User Data Access_2fe84	Provides apps access to structured...	Running	Manual	Local System
User Data Storage_2fe84	Handles storage of structured user...	Running	Manual	Local System
User Experience Virtualization Service	Provides support for application a...		Disabled	Local System
User Manager	User Manager provides the runtime...	Running	Automatic (T...	Local System
User Profile Service	This service is responsible for loadi...	Running	Automatic	Local System
Virtual Disk	Provides management services for...		Manual	Local System
VirtualBox Guest Additions Service	Manages VM runtime information...	Running	Automatic	Local System
Visual Studio Standard Collector Service 150	Visual Studio Data Collection Servi...		Manual	Local System
Volume Shadow Copy	Manages and implements Volume...		Manual	Local System
Volumetric Audio Compositor Service	Hosts spatial analysis for Mixed Re...		Manual	Local Service
WalletService	Hosts objects used by clients of th...		Manual	Local System
WarpJITSvc	Provides a JIT out of process servic...		Manual (Trig...	Local Service
Web Account Manager	This service is used by Web Accou...	Running	Manual	Local System
WebClient	Enables Windows-based programs...		Manual (Trig...	Local Service
Wi-Fi Direct Services Connection Manager Service	Manages connections to wireless s...		Manual (Trig...	Local Service
Windows Audio	Manages audio for Windows-base...	Running	Automatic	Local Service
Windows Audio Endpoint Builder	Manages audio devices for the Wi...	Running	Automatic	Local System
Windows Backup	Provides Windows Backup and Re...		Manual	Local System
Windows Biometric Service	The Windows biometric service gi...		Manual (Trig...	Local System
Windows Camera Frame Server	Enables multiple clients to access ...		Manual (Trig...	Local System
Windows Connect Now - Config Registrar	WCNCSVC hosts the Windows Co...		Manual	Local Service
Windows Connection Manager	Makes automatic connect/discon...	Running	Automatic (T...	Local Service
Windows Defender Advanced Threat Protection Service	Windows Defender Advanced Thre...		Manual	Local System
Windows Defender Firewall	Windows Defender Firewall helps ...	Running	Automatic	Local Service
Windows Encryption Provider Host Service	Windows Encryption Provider Hos...		Manual (Trig...	Local Service
Windows Error Reporting Service	Allows errors to be reported when ...		Manual (Trig...	Local System
Windows Event Collector	This service manages persistent su...		Manual	Network Service
Windows Event Log	This service manages events and e...	Running	Automatic	Local Service
Windows Font Cache Service	Optimizes performance of applica...	Running	Automatic	Local Service
Windows Image Acquisition (WIA)	Provides image acquisition service...		Manual	Local Service
Windows Insider Service	Provides infrastructure support for...		Manual (Trig...	Local System
Windows Installer	Adds, modifies, and removes appli...		Manual	Local System
Windows License Manager Service	Provides infrastructure support for...		Manual (Trig...	Local Service
Windows Management Instrumentation	Provides a common interface and ...	Running	Automatic	Local System
Windows Management Service	Performs management including ...		Manual	Local System
Windows Mobile Hotspot Service	Provides the ability to share cellu...		Manual (Trig...	Local Service
Windows Modules Installer	Enables installation, modification, ...		Manual	Local System
Windows Perception Service	Enables spatial perception, spatial ...		Manual (Trig...	Local Service
Windows Perception Simulation Service	Enables spatial perception simulati...		Manual	Local System
Windows Push Notifications System Service	This service runs in session 0 and h...	Running	Automatic	Local System
Windows Push Notifications User Service_2fe84	This service hosts Windows notific...	Running	Automatic	Local System
Windows PushToInstall Service	Provides infrastructure support for...		Manual (Trig...	Local System
Windows Remote Management (WS-Management)	Windows Remote Management (...)		Manual	Network Service
Windows Search	Provides content indexing, proper...	Running	Automatic (...)	Local System
Windows Security Service	Windows Security Service handles ...	Running	Manual	Local System
Windows Threat Protection	Protects your computer from mali...	Running	Automatic	Local System
Windows Time	Maintains date and time synchron...		Manual (Trig...	Local Service
Windows Update	Enables the detection, download, ...	Running	Manual (Trig...	Local System
Windows Update Medic Service	Enables remediation and protectio...		Manual	Local System
WinHTTP Web Proxy Auto-Discovery Service	WinHTTP implements the client H...	Running	Manual	Local Service
Wired AutoConfig	The Wired AutoConfig (DOT3SVC) ...		Manual	Local System
WLAN AutoConfig	The WLANSVC service provides th...		Manual	Local System
WMI Performance Adapter	Provides performance library infor...		Manual	Local System
Work Folders	This service syncs files with the W...		Manual	Local Service
Workstation	Creates and maintains client netw...	Running	Automatic	Network Service

Services

User-friendly name and description

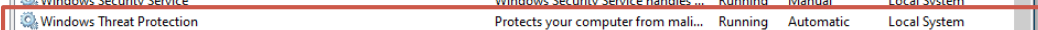
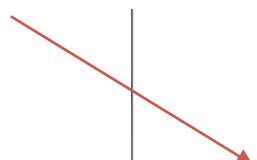
Defined by service author

Name	Description	Status	Startup Type	Log On As
Touch Keyboard and Handwriting Panel Service	Enables Touch Keyboard and Han...	Running	Manual (Trig...	Local System
Udk User Service_2fe84	Shell components service		Manual	Local System
Update Orchestrator Service	Manages Windows Updates. If sto...	Running	Automatic (...)	Local System
UPnP Device Host	Allows UPnP devices to be hosted ...		Manual	Local System
User Data Access_2fe84	Provides apps access to structured...	Running	Manual	Local System
User Data Storage_2fe84	Handles storage of structured user...	Running	Manual	Local System
User Experience Virtualization Service	Provides support for application a...		Disabled	Local System
User Manager	User Manager provides the runtim...	Running	Automatic (T...	Local System
User Profile Service	This service is responsible for loadi...	Running	Automatic	Local System
Virtual Disk	Provides management services for...		Manual	Local System
VirtualBox Guest Additions Service	Manages VM runtime information...	Running	Automatic	Local System
Visual Studio Standard Collector Service 150	Visual Studio Data Collection Servi...		Manual	Local System
Volume Shadow Copy	Manages and implements Volume...		Manual	Local System
Volumetric Audio Compositor Service	Hosts spatial analysis for Mixed Re...		Manual	Local Service
WalletService	Hosts objects used by clients of th...		Manual	Local System
WarpJITSvc	Provides a JIT out of process servic...		Manual (Trig...	Local Service
Web Account Manager	This service is used by Web Accou...	Running	Manual	Local System
WebClient	Enables Windows-based programs...		Manual (Trig...	Local Service
Wi-Fi Direct Services Connection Manager Service	Manages connections to wireless s...		Manual (Trig...	Local Service
Windows Audio	Manages audio for Windows-base...	Running	Automatic	Local Service
Windows Audio Endpoint Builder	Manages audio devices for the Wi...	Running	Automatic	Local System
Windows Backup	Provides Windows Backup and Re...		Manual	Local System
Windows Biometric Service	The Windows biometric service gi...		Manual (Trig...	Local System
Windows Camera Frame Server	Enables multiple clients to access ...		Manual (Trig...	Local System
Windows Connect Now - Config Registrar	WCNCSVC hosts the Windows Co...		Manual	Local Service
Windows Connection Manager	Makes automatic connect/discon...	Running	Automatic (T...	Local Service
Windows Defender Advanced Threat Protection Service	Windows Defender Advanced Thre...		Manual	Local System
Windows Defender Firewall	Windows Defender Firewall helps ...	Running	Automatic	Local Service
Windows Encryption Provider Host Service	Windows Encryption Provider Hos...		Manual (Trig...	Local Service
Windows Error Reporting Service	Allows errors to be reported when ...		Manual (Trig...	Local System
Windows Event Collector	This service manages persistent su...		Manual	Network Service
Windows Event Log	This service manages events and e...	Running	Automatic	Local Service
Windows Font Cache Service	Optimizes performance of applica...	Running	Automatic	Local Service
Windows Image Acquisition (WIA)	Provides image acquisition service...		Manual	Local Service
Windows Insider Service	Provides infrastructure support for...		Manual (Trig...	Local System
Windows Installer	Adds, modifies, and removes appli...		Manual	Local System
Windows License Manager Service	Provides infrastructure support for...		Manual (Trig...	Local Service
Windows Management Instrumentation	Provides a common interface and ...	Running	Automatic	Local System
Windows Management Service	Performs management including ...		Manual	Local System
Windows Mobile Hotspot Service	Provides the ability to share cellu...		Manual (Trig...	Local Service
Windows Modules Installer	Enables installation, modification, ...		Manual	Local System
Windows Perception Service	Enables spatial perception, spatial ...		Manual (Trig...	Local Service
Windows Perception Simulation Service	Enables spatial perception simulati...		Manual	Local System
Windows Push Notifications System Service	This service runs in session 0 and h...	Running	Automatic	Local System
Windows Push Notifications User Service_2fe84	This service hosts Windows notific...	Running	Automatic	Local System
Windows PushToInstall Service	Provides infrastructure support for...		Manual (Trig...	Local System
Windows Remote Management (WS-Management)	Windows Remote Management (...)		Manual	Network Service
Windows Search	Provides content indexing, proper...	Running	Automatic (...)	Local System
Windows Security Service	Windows Security Service handles ...	Running	Manual	Local System
Windows Threat Protection	Protects your computer from mali...	Running	Automatic	Local System
Windows Time	Maintains date and time synchron...		Manual (Trig...	Local Service
Windows Update	Enables the detection, download, ...	Running	Manual (Trig...	Local System
Windows Update Medic Service	Enables remediation and protectio...		Manual	Local System
WinHTTP Web Proxy Auto-Discovery Service	WinHTTP implements the client H...	Running	Manual	Local Service
Wired AutoConfig	The Wired AutoConfig (DOT3SVC) ...		Manual	Local System
WLAN AutoConfig	The WLANSVC service provides th...		Manual	Local System
WMI Performance Adapter	Provides performance library infor...		Manual	Local System
Work Folders	This service syncs files with the W...		Manual	Local Service
Workstation	Creates and maintains client netw...	Running	Automatic	Network Service

Services

Name	Description	Status	Startup Type	Log On As
Touch Keyboard and Handwriting Panel Service	Enables Touch Keyboard and Han...	Running	Manual (Trig...	Local System
Udk User Service_2fe84	Shell components service		Manual	Local System
Update Orchestrator Service	Manages Windows Updates. If sto...	Running	Automatic (...)	Local System
UPnP Device Host	Allows UPnP devices to be hosted ...		Manual	Local System
User Data Access_2fe84	Provides apps access to structured...	Running	Manual	Local System
User Data Storage_2fe84	Handles storage of structured user...	Running	Manual	Local System
User Experience Virtualization Service	Provides support for application a...		Disabled	Local System
User Manager	User Manager provides the runtim...	Running	Automatic (T...	Local System
User Profile Service	This service is responsible for loadi...	Running	Automatic	Local System
Virtual Disk	Provides management services for...		Manual	Local System
VirtualBox Guest Additions Service	Manages VM runtime information...	Running	Automatic	Local System
Visual Studio Standard Collector Service 150	Visual Studio Data Collection Servi...		Manual	Local System
Volume Shadow Copy	Manages and implements Volume...		Manual	Local System
Volumetric Audio Compositor Service	Hosts spatial analysis for Mixed Re...		Manual	Local Service
WalletService	Hosts objects used by clients of th...		Manual	Local System
WarpJITSvc	Provides a JIT out of process servic...		Manual (Trig...	Local Service
Web Account Manager	This service is used by Web Accou...	Running	Manual	Local System
WebClient	Enables Windows-based programs...		Manual (Trig...	Local Service
Wi-Fi Direct Services Connection Manager Service	Manages connections to wireless s...		Manual (Trig...	Local Service
Windows Audio	Manages audio for Windows-base...	Running	Automatic	Local Service
Windows Audio Endpoint Builder	Manages audio devices for the Wi...	Running	Automatic	Local System
Windows Backup	Provides Windows Backup and Re...		Manual	Local System
Windows Biometric Service	The Windows biometric service gi...		Manual (Trig...	Local System
Windows Camera Frame Server	Enables multiple clients to access ...		Manual (Trig...	Local System
Windows Connect Now - Config Registrar	WCNCSCV hosts the Windows Co...		Manual	Local Service
Windows Connection Manager	Makes automatic connect/discon...	Running	Automatic (T...	Local Service
Windows Defender Advanced Threat Protection Service	Windows Defender Advanced Thre...		Manual	Local System
Windows Defender Firewall	Windows Defender Firewall helps ...	Running	Automatic	Local Service
Windows Encryption Provider Host Service	Windows Encryption Provider Hos...		Manual (Trig...	Local Service
Windows Error Reporting Service	Allows errors to be reported when ...		Manual (Trig...	Local System
Windows Event Collector	This service manages persistent su...		Manual	Network Service
Windows Event Log	This service manages events and e...	Running	Automatic	Local Service
Windows Font Cache Service	Optimizes performance of applica...	Running	Automatic	Local Service
Windows Image Acquisition (WIA)	Provides image acquisition service...		Manual	Local Service
Windows Insider Service	Provides infrastructure support for...		Manual (Trig...	Local System
Windows Installer	Adds, modifies, and removes appli...		Manual	Local System
Windows License Manager Service	Provides infrastructure support for...		Manual (Trig...	Local System
Instrumentation Service	Provides a common interface and ...	Running	Automatic	Local System
at Service	Performs management including ...		Manual	Local System
ller	Provides the ability to share cellu...		Manual (Trig...	Local Service
vice	Enables installation, modification, ...		Manual	Local System
vice	Enables spatial perception, spatial ...		Manual (Trig...	Local Service
Windows Perception Simulation Service	Enables spatial perception simulati...		Manual	Local System
Windows Push Notifications System Service	This service runs in session 0 and h...	Running	Automatic	Local System
Windows Push Notifications User Service_2fe84	This service hosts Windows notific...	Running	Automatic	Local System
Windows PushToInstall Service	Provides infrastructure support for...		Manual (Trig...	Local System
Windows Remote Management (WS-Management)	Windows Remote Management (...)		Manual	Network Service
Windows Search	Provides content indexing, proper...	Running	Automatic (...)	Local System
Windows Security Service	Windows Security Service handles ...	Running	Manual	Local System
Windows Threat Protection	Protects your computer from mali...	Running	Automatic	Local System
Windows Time	Maintains date and time synchron...		Manual (Trig...	Local Service
Windows Update	Enables the detection, download, ...	Running	Manual (Trig...	Local System
Windows Update Medic Service	Enables remediation and protectio...		Manual	Local System
WinHTTP Web Proxy Auto-Discovery Service	WinHTTP implements the client H...	Running	Manual	Local Service
Wired AutoConfig	The Wired AutoConfig (DOT3SVC) ...		Manual	Local System
WLAN AutoConfig	The WLANSVC service provides th...		Manual	Local System
WMI Performance Adapter	Provides performance library infor...		Manual	Local System
Work Folders	This service syncs files with the W...		Manual	Local Service
Workstation	Creates and maintains client netw...	Running	Automatic	Network Service

There is no „Windows Threat Protection“ service on Windows



Services

Name	Description	Status	Startup Type	Log On As
Touch Keyboard and Handwriting Panel Service	Enables Touch Keyboard and Han...	Running	Manual (Trig...	Local System
Udk User Service_2fe84	Shell components service		Manual	Local System
Update Orchestrator Service	Manages Windows Updates. If sto...	Running	Automatic (...)	Local System
UPnP Device Host	Allows UPnP devices to be hosted ...		Manual	Local Service
User Data Access_2fe84	Provides apps access to structured...	Running	Manual	Local System
User Data Storage_2fe84	Handles storage of structured user...	Running	Manual	Local System
User Experience Virtualization Service	Provides support for application a...		Disabled	
User Manager	User Manager provides the runtim...	Running	Automatic (T...	
User Profile Service	This service is responsible for loadi...	Running	Automatic	
Virtual Disk	Provides management services for...		Manual	
VirtualBox Guest Additions Service	Manages VM runtime information...	Running	Automatic	
Visual Studio Standard Collector Service 150	Visual Studio Data Collection Servi...		Manual	
Volume Shadow Copy	Manages and implements Volume...		Manual	
Volumetric Audio Compositor Service	Hosts spatial analysis for Mixed Re...		Manual	
WalletService	Hosts objects used by clients of th...		Manual	
WarpJITSvc	Provides a JIT out of process servic...		Manual (Trig...	
Web Account Manager	This service is used by Web Accou...	Running	Manual	
WebClient	Enables Windows-based programs...		Manual (Trig...	
Wi-Fi Direct Services Connection Manager Service	Manages connections to wireless s...		Manual (Trig...	
Windows Audio	Manages audio for Windows-base...	Running	Automatic	
Windows Audio Endpoint Builder	Manages audio devices for the Wi...	Running	Automatic	
Windows Backup	Provides Windows Backup and Re...		Manual	
Windows Biometric Service	The Windows biometric service gi...		Manual (Trig...	
Windows Camera Frame Server	Enables multiple clients to access ...		Manual (Trig...	
Windows Connect Now - Config Registrar	WCNCSVC hosts the Windows Co...		Manual	
Windows Connection Manager	Makes automatic connect/discon...	Running	Automatic (T...	
Windows Defender Advanced Threat Protection Service	Windows Defender Advanced Thre...		Manual	
Windows Defender Firewall	Windows Defender Firewall helps ...	Running	Automatic	
Windows Encryption Provider Host Service	Windows Encryption Provider Hos...		Manual (Trig...	
Windows Error Reporting Service	Allows errors to be reported when ...		Manual (Trig...	
Windows Event Collector	This service manages persistent su...		Manual	
Windows Event Log	This service manages events and e...	Running	Automatic	
Windows Font Cache Service	Optimizes performance of applica...	Running	Automatic	
Windows Image Acquisition (WIA)	Provides image acquisition service...		Manual	
Windows Insider Service	Provides infrastructure support for...		Manual (Trig...	
Windows Installer	Adds, modifies, and removes appli...		Manual	
Windows License Manager Service	Provides infrastructure support for...		Manual (Trig...	
Windows Management Instrumentation	Provides a common interface and ...	Running	Automatic	
Windows Management Service	Performs management including ...		Manual	
Windows Mobile Hotspot Service	Provides the ability to share cellu...		Manual (Trig...	
Windows Modules Installer	Enables installation, modification, ...		Manual	
Windows Perception Service	Enables spatial perception, spatial ...		Manual (Trig...	
Windows Perception Simulation Service	Enables spatial perception simulati...		Manual	
Windows Push Notifications System Service	This service runs in session 0 and h...	Running	Automatic	Local System
Windows Push Notifications User Service_2fe84	This service hosts Windows notific...	Running	Automatic	Local System
Windows PushToInstall Service	Provides infrastructure support for...		Manual (Trig...	Local System
Windows Remote Management (WS-Management)	Windows Remote Management (...)		Manual	Network Service
Windows Search	Provides content indexing, proper...	Running	Automatic (...)	Local System
Windows Security Service	Windows Security Service handles ...	Running	Manual	Local System
Windows Threat Protection	Protects your computer from mali...	Running	Automatic	Local System
Windows Time	Maintains date and time synchron...		Manual (Trig...	Local Service
Windows Update	Enables the detection, download, ...	Running	Manual (Trig...	Local System
Windows Update Medic Service	Enables remediation and protectio...		Manual	Local System
WinHTTP Web Proxy Auto-Discovery Service	WinHTTP implements the client H...	Running	Manual	Local Service
Wired AutoConfig	The Wired AutoConfig (DOT3SVC) ...		Manual	Local System
WLAN AutoConfig	The WLANSVC service provides th...		Manual	Local System
WMI Performance Adapter	Provides performance library infor...		Manual	Local System
Work Folders	This service syncs files with the W...		Manual	Local Service
Workstation	Creates and maintains client netw...	Running	Automatic	Network Service

Windows Threat Protection Properties (Local Computer)

General | Log On | Recovery | De

Service name: **EvilService** „real“ service name, still user-defined

Display name: Windows Threat Protection

Description: Protects your computer from malicious software. Stopping or deleting this service may leave your machine unprotected

Path to executable: **C:\Users\lynx\Downloads\evil.exe** real path to service binary

Startup type: **Automatic** autostart

Service status: Running

Start parameters:

Start Stop Pause Resume

OK Cancel Apply

Services

Location:

SYSTEM\ControlSet001\Services

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (27/0) View Help

Registry hives (1) Available bookmarks (27/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
ControlSet001	=	=	=
Eaphost	11	2	2019-12-07 09:14:30
ebdrv	8	2	2021-11-03 14:24:37
edgeupdate	10	0	2021-11-03 14:25:15
edgeupdatem	10	0	2021-11-03 14:25:16
EFS	9	3	2019-12-07 09:15:07
EhStorClass	7	1	2021-11-22 14:20:21
EhStorTcgDrv	8	2	2021-11-03 14:24:37
embeddedmode	10	3	2019-12-07 09:15:07
EntAppSvc	11	2	2019-12-07 09:14:30
ErrDev	8	0	2019-12-07 09:13:54
ESENT	0	1	2019-12-07 09:14:30
EventLog	16	9	2021-11-03 14:24:46
EventSystem	11	1	2019-12-07 09:14:30
EvilService	7	0	2021-11-22 14:30:08
exfat	6	0	2019-12-07 09:14:30
fastfat	6	0	2019-12-07 09:14:30
Fax	11	1	2019-12-07 09:49:22
fdc	6	0	2019-12-07 09:13:54
fdPHost	11	1	2019-12-07 09:14:30
FDResPub	11	4	2019-12-07 09:15:07
fhsvc	14	3	2019-12-07 09:15:07
FileCrypt	9	1	2019-12-07 09:14:30
FileInfo	9	1	2019-12-07 09:14:30
Filetrace	10	1	2019-12-07 09:14:30
flpydisk	6	0	2019-12-07 09:13:54
FltMgr	9	0	2019-12-07 09:14:30

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Sl...	Is Delet...	Data Rec...
Type	RegDword	16		<input type="checkbox"/>	<input type="checkbox"/>
Start	RegDword	2		<input type="checkbox"/>	<input type="checkbox"/>
ErrorControl	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
ImagePath	RegExpandSz	C:\Users\lynx\Downloads\evil.exe	69-00	<input type="checkbox"/>	<input type="checkbox"/>
DisplayName	RegSz	Windows Threat Protection		<input type="checkbox"/>	<input type="checkbox"/>
ObjectName	RegSz	LocalSystem	73-00-0...	<input type="checkbox"/>	<input type="checkbox"/>
Description	RegSz	Protects your computer from malicious software. Stopping or deleting this service may leave your machine unprotected.		<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Binary viewer

Value name: Type

Value type: RegDword

Value: 16

Raw value: 10-00-00-00

Key: ControlSet001\Services\EvilService

Selected hive: SYSTEM Last write: 2021-11-22 14:30:08 7 of 7 values shown (100,00 %) Load complete

Value: Type Collapse all hives

Hidden keys: 0 6

autostart

path to service executable

Services

Location:

SYSTEM\ControlSet001



Registry Explorer v1.6.0.0

File Tools Options Bookmarks (27)

Registry hives (1) Available bookmarks

Enter text to search...

Key name

Key name	Value	Type	Start	Path	Description	Value Sl...	Is Delet...	Data Rec...
Start	2	RegDword	2019-12-07 09:14:30				<input type="checkbox"/>	<input type="checkbox"/>
ErrorControl	1	RegDword	2021-11-03 14:24:37				<input type="checkbox"/>	<input type="checkbox"/>
ImagePath	C:\Users\Ynx\Downloads\evl.exe	RegExpandSz	2021-11-03 14:25:15		Windows Threat Protection	69-00	<input type="checkbox"/>	<input type="checkbox"/>
DisplayName	Windows Threat Protection	RegSz	2021-11-22 14:20:21				<input type="checkbox"/>	<input type="checkbox"/>
ObjectName	LocalSystem	RegSz	2021-11-03 14:24:37			73-00-0...	<input type="checkbox"/>	<input type="checkbox"/>
Description	Protects your computer from malicious software. Stopping or deleting this service may leave your machine unprotected.	RegSz	2019-12-07 09:15:07				<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Binary viewer

Value name Type

Value type RegDword

Value 16

Raw value 10-00-00-00

Key: ControlSet001\Services\EvilService

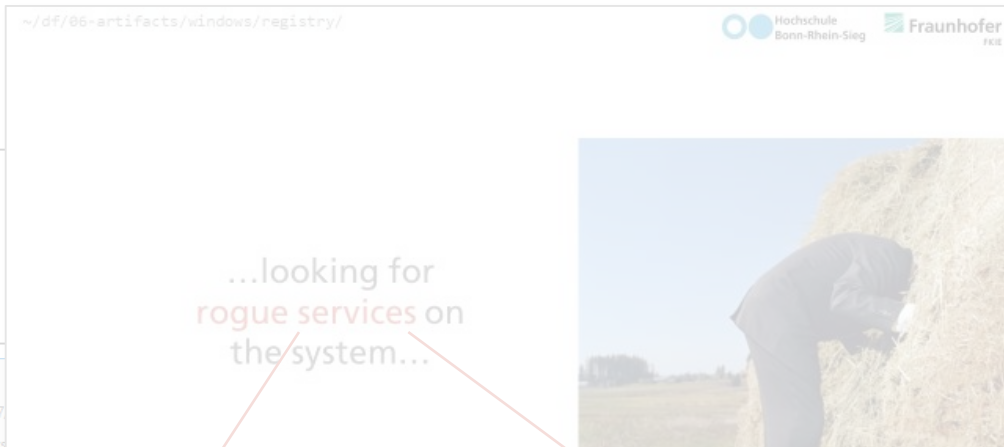
Selected hive: SYSTEM Last write: 2021-11-22 14:30:08 7 of 7 values shown (100,00 %) Load complete

Hidden keys: 0 6

Services

Location:

SYSTEM\ControlSet001



Correlate with program execution evidence!

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (27)

Registry hives (1) Available bookmarks

Enter text to search...

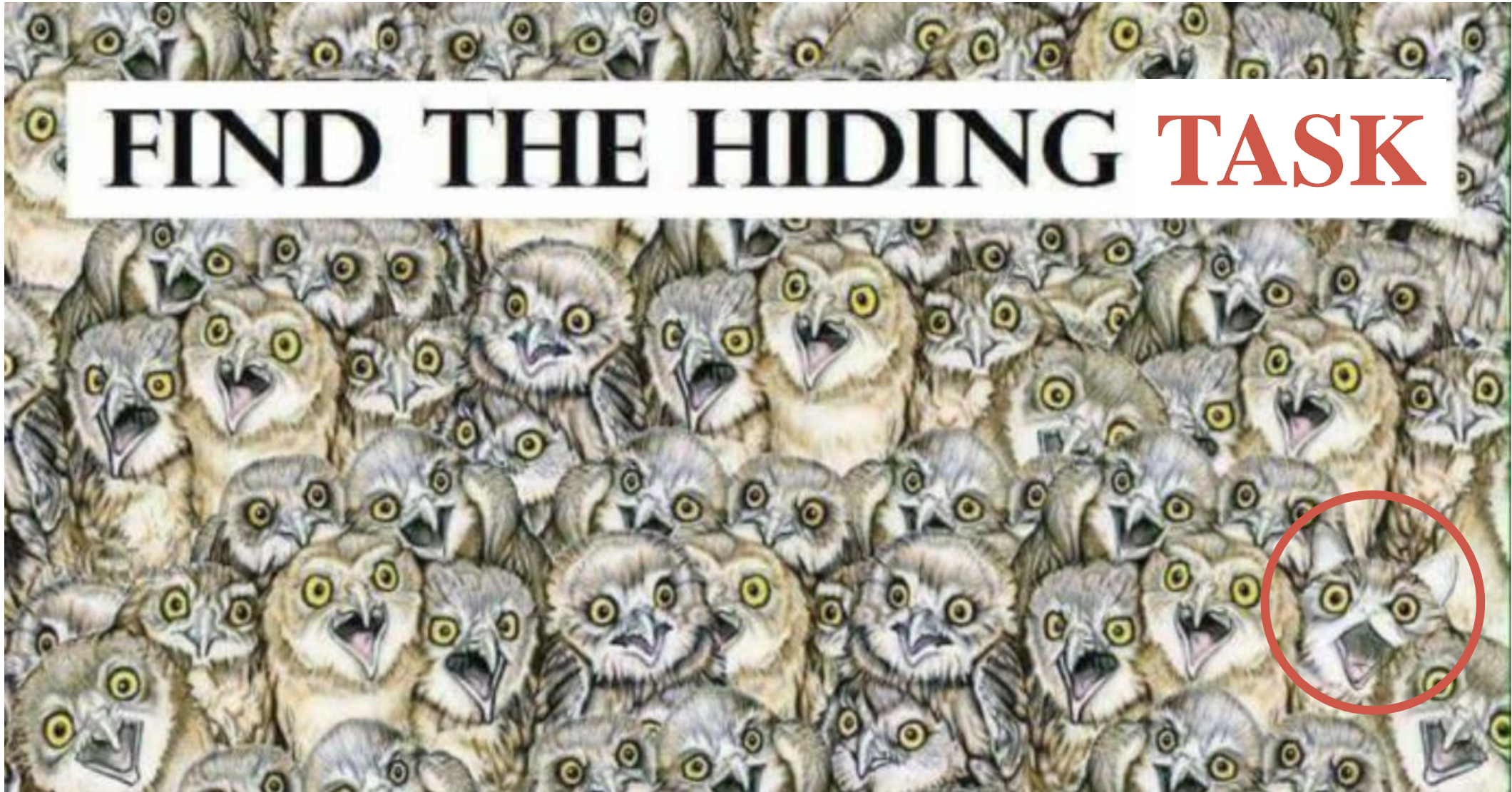
Key name

Key name	Value	Is Delet...	Data Rec...
Eaphost	11		
ebdrv	8		
edgeupdate	10		
edgeupdatem	10		
EPS	9		
EhStorClass	7		
EhStorTcgDrv	8		
embeddedmode	10		
EntAppSvc	11		
ErrDev	8		
ESENT	0		
EventLog	16		
EventSystem	11		
EvilService	7		
exfat	6		
fastfat	6		
Fax	11		
fdc	6		
fdPHost	11		
FDResPub	11		
fhsvc	14		
FileCrypt	9		
FileInfo	9		
Filetrace	10		
flpydisk	6		
FltMgr	9		

Key: ControlSet001\Services\EvilService

Selected hive: SYSTEM Last write: 2021-11-22 14:30:08 7 of 7 values shown (100,00 %) Load complete

Value: Type Collapse all hives Hidden keys: 0 6



FIND THE HIDING TASK



Active tasks are tasks that are currently enabled.

Name	Trigger defines when to do task	Path to the task relative to tasks location
Task Name	Next Run Time	Triggers
OobeDiscovery		Multiple triggers defined
PenSyncDataAvailable		Custom Trigger
ProcessMemoryDiagnosticEvents		Multiple triggers defined
Proxy		At system startup
RecommendedTroubleshootingSc...		Multiple triggers defined
ReconcileFeatures		Multiple triggers defined
ReconcileLanguageResources		At log on of any user - A...
RegisterDeviceAccountChange		Multiple triggers defined
RegisterDevicePolicyChange		Multiple triggers defined
RegisterDeviceProtectionStateCha...		Custom Trigger
RegisterDeviceSettingChange		Multiple triggers defined
RegisterUserDevice		Multiple triggers defined
RemoteAssistanceTask		Multiple triggers defined
Report policies		Custom Trigger
Schedule Scan Static Task		Multiple triggers defined
Scheduled Start		Multiple triggers defined
Secure-Boot-Update		Custom Trigger
SpaceAgentTask		Multiple triggers defined
SpaceManagerTask		Multiple triggers defined
Storage Tiers Management Initializ...		Custom Trigger
StorageCardEncryption Task		Custom Trigger
Synchronize Language Settings		Multiple triggers defined
SyspartRepair		Custom Trigger
SystemSoundsService		At log on of any user
SystemTask		Multiple triggers defined
TouchpadSyncDataAvailable		Custom Trigger
Tpm-HASCertRetr		Custom Trigger
Tpm-Maintenance		Multiple triggers defined
UpdateModelTask		Custom Trigger
UpdateUserPictureTask		Custom Trigger
UsageDataFlushing		Multiple triggers defined
Usb-Notifications		Multiple triggers defined
UserTask		Multiple triggers defined
UserTask-Roam		Multiple triggers defined
VirusScan		At log on of any user
WiFiTask		Custom Trigger
WiFiTask		Custom Trigger
WIM-Hash-Management		Multiple triggers defined
WindowsActionDialog		Custom Trigger
Work Folders Logon Synchronizati...		At log on of any user
Work Folders Maintenance Work		At log on of any user

Task Scheduler (formerly Scheduled Tasks)[1] is a job scheduler in Microsoft Windows that launches computer programs or scripts at pre-defined times or after specified time intervals. [...] The Windows Task Scheduler infrastructure is the basis for the Windows PowerShell scheduled jobs feature introduced with PowerShell v3.[6]

Task Scheduler can be compared to cron or anacron on Unix-like operating systems. [...]

Location:

`C:\Windows\System32\Tasks\path-to-the-task`

Active tasks are tasks that are currently enabled and have not expired.

Summary: 103 total

Task Name	Next Run Time	Triggers	Location
OobeDiscovery		Multiple triggers defined	\Microsoft\Windows\WwanSvc
PenSyncDataAvailable		Custom Trigger	\Microsoft\Windows\Input
ProcessMemoryDiagnosticEvents		Multiple triggers defined	\Microsoft\Windows\MemoryDiagnostic
Proxy		At system startup	\Microsoft\Windows\Autochk
RecommendedTroubleshootingSc...		Multiple triggers defined	\Microsoft\Windows\Diagnosis
ReconcileFeatures		Multiple triggers defined	\Microsoft\Windows\Flighting\FeatureConfig
ReconcileLanguageResources		At log on of any user - A...	\Microsoft\Windows\LanguageComponents\Installer
RegisterDeviceAccountChange		Multiple triggers defined	\Microsoft\Windows\DeviceDirectoryClient
RegisterDevicePolicyChange		Multiple triggers defined	\Microsoft\Windows\DeviceDirectoryClient
RegisterDeviceProtectionStateCha...		Custom Trigger	\Microsoft\Windows\DeviceDirectoryClient
RegisterDeviceSettingChange		Multiple triggers defined	\Microsoft\Windows\DeviceDirectoryClient
RegisterUserDevice		Multiple triggers defined	\Microsoft\Windows\DeviceDirectoryClient
RemoteAssistanceTask		Multiple triggers defined	\Microsoft\Windows\RemoteAssistance
Report policies		Custom Trigger	\Microsoft\Windows\UpdateOrchestrator
Schedule Scan Static Task		Multiple triggers defined	\Microsoft\Windows\UpdateOrchestrator
Scheduled Start		Multiple triggers defined	\Microsoft\Windows\WindowsUpdate
Secure-Boot-Update		Custom Trigger	\Microsoft\Windows\PI
SpaceAgentTask		Multiple triggers defined	\Microsoft\Windows\SpacePort
SpaceManagerTask		Multiple triggers defined	\Microsoft\Windows\SpacePort
Storage Tiers Management Initializ...		Custom Trigger	\Microsoft\Windows\Storage Tiers Management
StorageCardEncryption Task		Custom Trigger	\Microsoft\Windows\EDP
Synchronize Language Settings		Multiple triggers defined	\Microsoft\Windows\International
SyspartRepair		Custom Trigger	\Microsoft\Windows\Chkdsk
SystemSoundsService		At log on of any user	\Microsoft\Windows\Multimedia
SystemTask		Multiple triggers defined	\Microsoft\Windows\CertificateServicesClient
TouchpadSyncDataAvailable		Custom Trigger	\Microsoft\Windows\Input
Tpm-HASCertRetr		Custom Trigger	\Microsoft\Windows\TPM
Tpm-Maintenance		Multiple triggers defined	\Microsoft\Windows\TPM
UpdateModelTask		Custom Trigger	\Microsoft\Windows\UpdateOrchestrat
UpdateUserPictureTask		Custom Trigger	\Microsoft\Windows\Shell
UsageDataFlushing		Multiple triggers defined	\Microsoft\Windows\Flighting\Feature(.....)
Usb-Notifications		Multiple triggers defined	\Microsoft\Windows\USB
UserTask		Multiple triggers defined	\Microsoft\Windows\CertificateServicesClient
UserTask-Roam		Multiple triggers defined	\Microsoft\Windows\CertificateServicesClient
VirusScan		At log on of any user	\Microsoft\Windows\WorkFolders
WiFiTask		Custom Trigger	\Microsoft\Windows\WCM
WiFiTask		Custom Trigger	\Microsoft\Windows\NlaSvc
WIM-Hash-Management		Multiple triggers defined	\Microsoft\Windows\WOF
WindowsActionDialog		Custom Trigger	\Microsoft\Windows\Location
Work Folders Logon Synchronizati...		At log on of any user	\Microsoft\Windows\Work Folders
Work Folders Maintenance Work		At log on of any user	\Microsoft\Windows\Work Folders

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
VirusScan	Ready	At log on of any user		25/11/2021 11:45:16	The operation completed successfully. (0x0)	DESKTOP-I2KNJ8H\lynx	25/11/2021 11:44:37

General Triggers Actions Conditions Settings History (disabled)

Name: name, relative path, source

Location: system and username

Author:

Description:

There is no VirusScan task. Unless you create it >:)



Active tasks are tasks that are currently enabled and have not expired.

Summary: 103 total

Task Name	Next Run Time	Triggers	Location
OobeDiscovery		Multiple triggers defined	\Microsoft\Windows\WwanSvc
PenSyncDataAvailable		Custom Trigger	\Microsoft\Windows\Input
ProcessMemoryDiagnosticEvents		Multiple triggers defined	\Microsoft\Windows\MemoryDiagnostic
Proxy		At system startup	\Microsoft\Windows\Proxy
RecommendedTroubleshootingSc...		Multiple triggers defined	\Microsoft\Windows\Troubleshooting
ReconcileFeatures		Multiple triggers defined	\Microsoft\Windows\ReconcileFeatures
ReconcileLanguageResources		At log on of any user - A...	\Microsoft\Windows\ReconcileLanguageResources
RegisterDeviceAccountChange		Multiple triggers defined	\Microsoft\Windows\DeviceManagement
RegisterDevicePolicyChange		Multiple triggers defined	\Microsoft\Windows\DeviceManagement
RegisterDeviceProtectionStateCha...		Custom Trigger	\Microsoft\Windows\DeviceManagement
RegisterDeviceSettingChange		Multiple triggers defined	\Microsoft\Windows\DeviceManagement
RegisterUserDevice		Multiple triggers defined	\Microsoft\Windows\DeviceDirectoryClient
RemoteAssistanceTask		Multiple triggers defined	\Microsoft\Windows\RemoteAssistance
Report policies		Custom Trigger	\Microsoft\Windows\UpdateOrchestrator
Schedule Scan Static Task		Multiple triggers defined	\Microsoft\Windows\UpdateOrchestrator
Scheduled Start		Multiple triggers defined	\Microsoft\Windows\WindowsUpdate
Secure-Boot-Update		Custom Trigger	\Microsoft\Windows\PI
SpaceAgentTask		Multiple triggers defined	\Microsoft\Windows\SpacePort
SpaceManagerTask		Multiple triggers defined	\Microsoft\Windows\SpacePort
Storage Tiers Management Initializ...		Custom Trigger	\Microsoft\Windows\Storage Tiers Management
StorageCardEncryption Task		Custom Trigger	\Microsoft\Windows\EDP
Synchronize Language Settings		Multiple triggers defined	\Microsoft\Windows\International
SyspartRepair		Custom Trigger	\Microsoft\Windows\Chkdsk
SystemSoundsService		At log on of any user	\Microsoft\Windows\Multimedia
SystemTask		Multiple triggers defined	\Microsoft\Windows\CertificateServicesClient
TouchpadSyncDataAvailable		Custom Trigger	\Microsoft\Windows\Input
Tpm-HASCertRetr		Custom Trigger	\Microsoft\Windows\TPM
Tpm-Maintenance		Multiple triggers defined	\Microsoft\Windows\TPM
UpdateModelTask		Custom Trigger	\Microsoft\Windows\UpdateOrchestrator
UpdateUserPictureTask		Custom Trigger	\Microsoft\Windows\Shell
UsageDataFlushing		Multiple triggers defined	\Microsoft\Windows\Flighting\Feature...
Usb-Notifications		Multiple triggers defined	\Microsoft\Windows\USB
UserTask		Multiple triggers defined	\Microsoft\Windows\CertificateServicesClient
UserTask-Roam		Multiple triggers defined	\Microsoft\Windows\CertificateServicesClient
VirusScan		At log on of any user	\Microsoft\Windows\WorkFolders
WiFiTask		Custom Trigger	\Microsoft\Windows\WCM
WiFiTask		Custom Trigger	\Microsoft\Windows\NlaSvc
WIM-Hash-Management		Multiple triggers defined	\Microsoft\Windows\WOF
WindowsActionDialog		Custom Trigger	\Microsoft\Windows\Location
Work Folders Logon Synchronizati...		At log on of any user	\Microsoft\Windows\Work Folders
Work Folders Maintenance Work		At log on of any user	\Microsoft\Windows\Work Folders

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
VirusScan	Ready	At log on of any user		25/11/2021 11:45:16	The operation completed successfully. (0x0)	DESKTOP-I2KNJ8H\lynx	25/11/2021 11:44:37

General Triggers Actions Conditions Settings History (disabled)

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	C:\Users\lynx\Downloads\more-evil.exe

EXECUTABLE

General Triggers Actions Conditions Settings History (disabled)

Name: VirusScan

Location: \Microsoft\Windows\WorkFolders

Author: DESKTOP-I2KNJ8H\lynx

Description:

name, relative path, source system and username

There is no VirusScan task. Unless you create it >:)



Scheduled tasks

```
~$ cat C:\Windows\System32\Tasks\Microsoft\Windows\WorkFolders\VirusScan
```

```
<?xml version="1.0" encoding="UTF-16"?>  
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">  
  <RegistrationInfo>  
    <Date>2021-11-25T11:44:37</Date>  
    <Author>DESKTOP-I2KNJ8H\lynx</Author>  
    <URI>\Microsoft\Windows\WorkFolders\VirusScan</URI>  
  </RegistrationInfo>  
  <Triggers>  
    <LogonTrigger>  
      <StartBoundary>2021-11-25T11:44:00</StartBoundary>  
      <Enabled>>true</Enabled>  
    </LogonTrigger>  
  </Triggers>  
  <Settings>  
    ...  
  </Settings>  
  <Actions Context="Author">  
    <Exec>  
      <Command>C:\Users\lynx\Downloads\more-evil.exe</Command>  
    </Exec>  
  </Actions>  
  <Principals>  
    <Principal id="Author">  
      <UserId>DESKTOP-I2KNJ8H\lynx</UserId>  
      <LogonType>InteractiveToken</LogonType>  
      <RunLevel>LeastPrivilege</RunLevel>  
    </Principal>  
  </Principals>  
</Task>
```

source host \ creator username

relative path

program or script executed by the task

Scheduled tasks

Registry Explorer v1.6.0.0

Registry Explorer TaskCache\Tasks plugin

Registry hives (1) Available bookmarks (29/0) View Help

TaskCache

Enter text to search... Find

Key name

App Paths
Uninstall
StartMenuInternet
System
System
TaskCache
Boot
Logon
Maintenance
Plain
Tasks
Tree

Bookmark information

Hive
Category
Name
Key path
Short description
Long description

Key: Microsoft
Selected hive: SOFTWARE

Ver...	Key Name	Path	Created On	Last Start	Last Stop	T...	L...	Source	Description	Author
=	#c	#c	=	=	=	=	=	#c	#c	#c
3	{56B93F28-9040-480E-A1C2-B53782D55816}	Microsoft\Windows\WorkFolders\VirusScan	2021-11-25 10:44...	2021-11-25 ...	2021-11-25 10:45:46	0	0			DESKTOP-I2KNJ8H\ynx
3	{7F7622B6-8C09-46ED-A93A-C9FF5CF8B796}	Microsoft\VisualStudio\Updates\BackgroundDownload	2021-11-25 09:56...	2021-11-25 ...		0	-...			Microsoft Visual Studio
3	{0E23F468-4898-4027-830B-9D0D825E4BE1}	Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan	2021-11-25 09:21...	2021-11-25 ...		0	-...		Periodic scan task.	
3	{EAEFF021-8B72-417D-87D2-D67FC4F4CF3F}	Microsoft\Windows\Windows Defender\Windows Defender Cleanup	2021-11-25 09:21...	2021-11-25 ...	2021-11-25 09:36:05	0	0		Periodic cleanup task.	
3	{E87BE476-2C7F-491F-B402-7838477004B2}	Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance	2021-11-25 09:21...	2021-11-25 ...		0	-...		Periodic maintenance task.	
3	{46C8B52A-1686-4978-92C9-61B5A8F13EDB}	Microsoft\Windows\Windows Defender\Windows Defender Verification	2021-11-25 09:21...	2021-11-25 ...	2021-11-25 09:36:05	0	0		Periodic verification task.	
3	{4745B712-96DA-4D13-8FEF-6CFEC625E7E7}	Mozilla\Firefox Background Update 308046B0AF4A39CB	2021-11-25 09:15...			0	0		Die Aufgabe "Hintergrundaktualisierung" sucht nach Updates für Firefox, während Firefox nicht ausgeführt wird. Die Aufgabe wird automatisch von Firefox installiert und erneut installiert, wenn Firefox ausgeführt wird. Um diese Aufgabe zu	Mozilla

SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\
 ...Tree -----> tasks (IDs)
 ...Tasks -----> tasks infos (pro ID)

Scheduled tasks

```
~$ cat C:\Windows\System32\Tasks\Microsoft\Windows\WorkFolders\VirusScan
```

```
<?xml version="1.0" encoding="UTF-16"?>  
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">  
  <RegistrationInfo>  
    <Date>2021-11-25T11:44:37</Date>  
    <Author>DESKTOP-I2KNJ8H\lynx</Author>  
    <URI>\Microsoft\Windows\WorkFolders\VirusScan</URI>  
  </RegistrationInfo>  
  <Triggers>  
    <LogonTrigger>  
      <StartBoundary>2021-11-25T11:44:00</StartBoundary>  
      <Enabled>>true</Enabled>  
    </LogonTrigger>  
  </Triggers>  
  <Settings>  
  ...  
</Settings>  
  <Actions Context="Author">  
    <Exec>  
      <Command>C:\Users\lynx\Downloads\more-evil.exe</Co  
    </Exec>  
  </Actions>  
  <Principals>  
    <Principal id="Author">  
      <UserId>DESKTOP-I2KNJ8H\lynx</UserId>  
      <LogonType>InteractiveToken</LogonType>  
      <RunLevel>LeastPrivilege</RunLevel>  
    </Principal>  
  </Principals>  
</Task>
```

program



Scheduled tasks

```
~$ cat C:\Windows\System32\Tasks\Microsoft\Windows\WorkFolders\VirusScan
```

```

<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2021-11-25T11:44:37</Date>
    <Author>DESKTOP-I2KNJ8H\lynx</Author>
    <URI>\Microsoft\Windows\WorkFolders\TaskScheduler\Task\Task
  </RegistrationInfo>
  <Triggers>
    <LogonTrigger>
      <StartBoundary>Logon</StartBoundary>
      <Enabled>true</Enabled>
    </LogonTrigger>
  </Triggers>
  <Settings>
    ...
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Users\lynx\Downloads\more-evil.exe</Command>
    </Exec>
  </Actions>
  <Principals>
    <Principal id="Author">
      <UserId>DESKTOP-I2KNJ8H\lynx</UserId>
      <LogonType>InteractiveToken</LogonType>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
</Task>

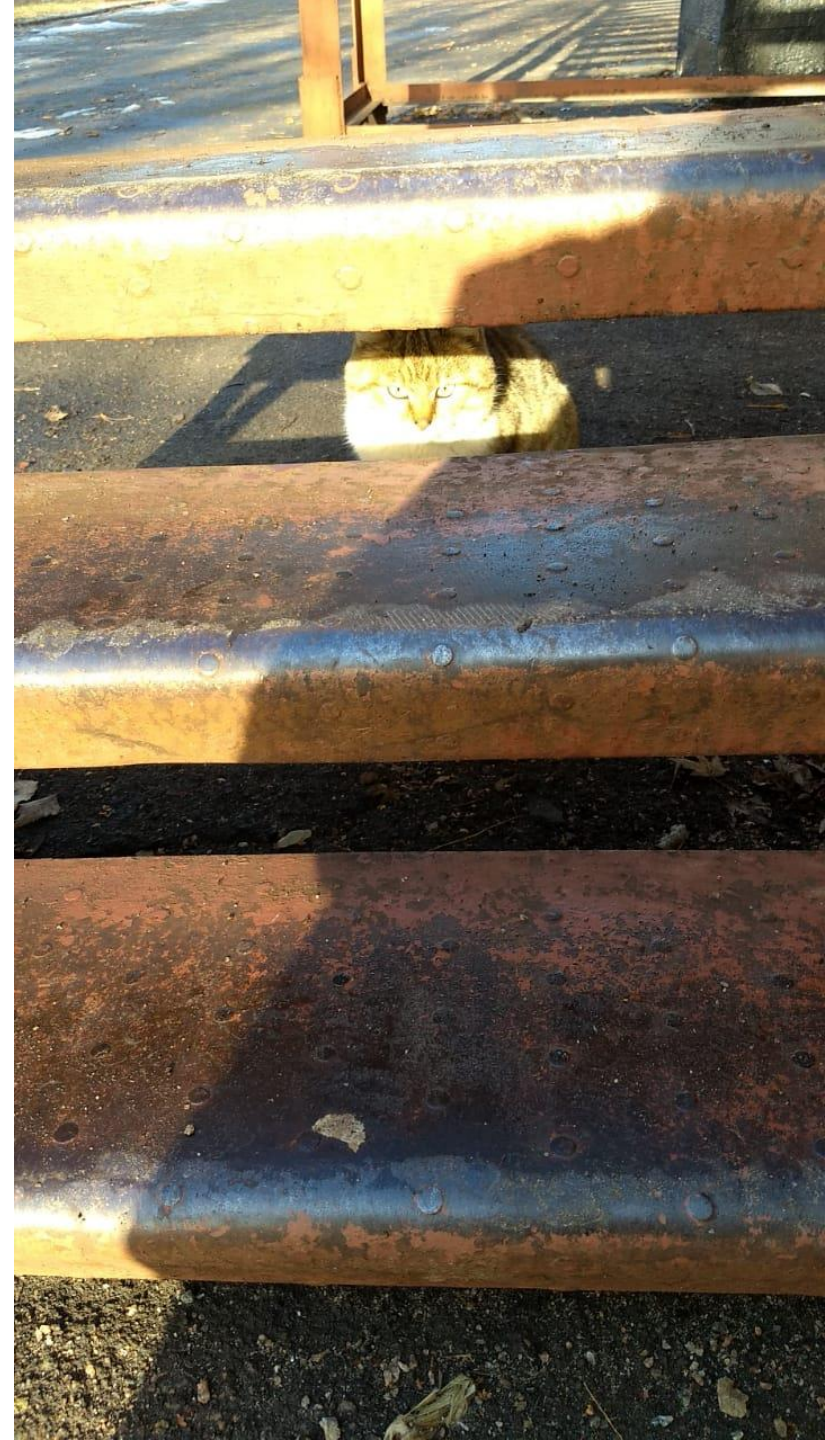
```

Correlate with program execution evidence!

program



Are there any interesting
or suspicious logons?



Event logs to the rescue

```
~$ cat failed-login.xml
```

```
<Event>
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="54849625-5478-4994-a5ba-3e3b0328c30d" />
    <EventID>4625</EventID>
    ...
    <TimeCreated SystemTime="2021-11-26 08:48:35.1597150" />
    <EventRecordID>6895</EventRecordID>
    ...
    <Channel>Security</Channel>
    <Computer>DESKTOP-I2KNJ8H</Computer>
    <Security />
  </System>
  <EventData>
    <Data Name="SubjectUserSid">S-1-0-0</Data>
    <Data Name="SubjectUserName">-</Data>
    <Data Name="SubjectDomainName">-</Data>
    <Data Name="SubjectLogonId">0x0</Data>
    <Data Name="TargetUserSid">S-1-0-0</Data>
    <Data Name="TargetUserName">lanx</Data>
    <Data Name="TargetDomainName">.</Data>
    <Data Name="Status">0xC000006D</Data>
    <Data Name="FailureReason">%2313</Data>
    <Data Name="SubStatus">0xC0000064</Data>
    <Data Name="LogonType">3</Data>
    <Data Name="LogonProcessName">NtLmSsp </Data>
    <Data Name="AuthenticationPackageName">NTLM</Data>
    <Data Name="WorkstationName">DESKTOP-NI9V1EK</Data>
    ...
    <Data Name="IpAddress">10.0.0.1</Data>
    <Data Name="IpPort">0</Data>
  </EventData>
</Event>
```

Event logs

```
~$ cat failed-login.xml
```

```
<Event>
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="54849625-5478-4994-a5ba-3e3b0328c30d" />
    <EventID>4625</EventID>
    ...
    <TimeCreated SystemTime="2021-11-26 08:48:35.1597150" />
    <EventRecordID>6895</EventRecordID>
    ...
    <Channel>Security</Channel>
    <Computer>DESKTOP-I2KNJ8H</Computer>
    <Security />
  </System>
  <EventData>
    <Data Name="SubjectUserSid">S-1-0-0</Data>
    <Data Name="SubjectUserName">-</Data>
    <Data Name="SubjectDomainName">-</Data>
    <Data Name="SubjectLogonId">0x0</Data>
    <Data Name="TargetUserSid">S-1-0-0</Data>
    <Data Name="TargetUserName">lanx</Data>
    <Data Name="TargetDomainName">.</Data>
    <Data Name="Status">0xC000006D</Data>
    <Data Name="FailureReason">%2313</Data>
    <Data Name="SubStatus">0xC0000064</Data>
    <Data Name="LogonType">3</Data>
    <Data Name="LogonProcessName">NtLmSsp </Data>
    <Data Name="AuthenticationPackageName">NTLM</Data>
    <Data Name="WorkstationName">DESKTOP-NI9V1EK</Data>
    ...
    <Data Name="IpAddress">10.0.0.1</Data>
    <Data Name="IpPort">0</Data>
  </EventData>
</Event>
```

Status and Sub Status Code:

status and sub_status_code	description
0XC000005E	There are currently no logon servers available to service the logon request.
0xC0000064	user name does not exist
0xC000006A	user name is correct but the password is wrong
0XC000006D	This is either due to a bad username or authentication information
0XC000006E	Unknown user name or bad password.
0XC000006F	user tried to logon outside his day of week or time of day restrictions
0xC0000070	workstation restriction or Authentication Policy Silo violation (look for event ID 4820 on domain controller)
0xC0000071	expired password
0xC0000072	account is currently disabled
0XC00000DC	Indicates the Sam Server was in the wrong state to perform the desired operation.
0xC0000133	clocks between DC and other computer too far out of sync
0xc000015b	The user has not been granted the requested logon type (aka logon right) at this machine
0XC000018C	The logon request failed because the trust relationship between the primary domain and the trusted domain failed.
0XC0000192	An attempt was made to logon but the netlogon service was not started.
0XC0000193	account expiration
0XC0000224	user is required to change password at next logon
0xC0000225	evidently a bug in Windows and not a risk
0xC0000234	user is currently locked out
0XC0000413	Logon Failure: The machine you are logging onto is protected by an authentication firewall. The specified account is not allowed to authenticate to the machine.

Log Sample:

Event logs

```
~$ cat failed-login.xml
```

```

<Event>
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="54849625-5478-49
    <EventID>4625</EventID>
    ...
    <TimeCreated SystemTime="2021-11-26 08:48:35.1597150" />
    <EventRecordID>6895</EventRecordID>
    ...
    <Channel>Security</Channel>
    <Computer>DESKTOP-I2KNJ8H</Computer>
    <Security />
  </System>
  <EventData>
    <Data Name="SubjectUserSid">S-1-0-0</Data>
    <Data Name="SubjectUserName">-</Data>
    <Data Name="SubjectDomainName">-</Data>
    <Data Name="SubjectLogonId">0x0</Data>
    <Data Name="TargetUserSid">S-1-0-0</Data>
    <Data Name="TargetUserName">lanx</Data>
    <Data Name="TargetDomainName">.</Data>
    <Data Name="Status">0xC000006D</Data>
    <Data Name="FailureReason">%2313</Data>
    <Data Name="SubStatus">0xC0000064</Data>
    <Data Name="LogonType">3</Data>
    <Data Name="LogonProcessName">NtLmSsp </Data>
    <Data Name="AuthenticationPackageName">NTLM</Data>
    <Data Name="WorkstationName">DESKTOP-NI9V1EK</Data>
    ...
    <Data Name="IpAddress">10.0.0.1</Data>
    <Data Name="IpPort">0</Data>
  </EventData>
</Event>

```

Status and Sub Status Code:

status and sub_status_code	description
0XC000005E	There are currently no logon request.
0xC0000064	user name does not exist
0xC000006A	user name is correct but password is incorrect. This is either due to a typo or the user is not in the local security database.
0XC000006D	Unknown user name or password. This indicates that the user tried to logon outside of the local security database.
0XC000006E	Unknown user name or password. This indicates that the user tried to logon outside of the local security database.
0XC000006F	workstation restriction violation (look for event 4625).
0xC0000070	expired password
0xC0000071	account is currently disabled
0xC0000072	Indicates the Sam Server is not available.
0XC00000DC	Indicates the Sam Server is not available.
0xC0000133	account expiration
0xC000015b	user is required to change password at next logon
0XC000018C	evidently a bug in Windows and not a risk
0XC0000192	user is currently locked out
0XC0000193	Logon Failure: The machine you are logging onto is protected by an authentication firewall. The specified account is not allowed to authenticate to the machine.
0XC0000224	
0xC0000225	
0xC0000234	
0XC0000413	

Log Sample:

```
~$ cat failed-login-ez-evt-x-explorer.xml
```

```

{
  "PayloadData1": "Target: .\\lanx",
  "PayloadData2": "LogonType 3",
  "PayloadData3": "FailureReason: user name does not exist",
  "UserName": "-\\-",
  "RemoteHost": "DESKTOP-NI9V1EK (10.0.0.1)",
  "ExecutableInfo": "-",
  "MapDescription": "Failed logon",
  "ChunkNumber": 82,
  "Computer": "DESKTOP-I2KNJ8H",
  "Payload": "{\"EventData\": {\"Data\": ...}}",
  "Channel": "Security",
  "Provider": "Microsoft-Windows-Security-Auditing",
  "EventId": 4625,
  "EventRecordId": "6895",
  "ProcessId": 596,
  "ThreadId": 664,
  "Level": "LogAlways",
  "Keywords": "Audit failure",
  "SourceFile": "Z:\\logs-remote-access\\Security.evtx",
  "ExtraDataOffset": 0,
  "HiddenRecord": false,
  "TimeCreated": "2021-11-26T08:48:35.1597150+00:00",
  "RecordNumber": 6895
}

```

```

~$ evtxcmd --inc 4625 -f Z:\\logs-remote-access\\Security.evtx --json
Z:\\logs-remote-access\\out-json --sd 2021-11-25

```

Network logon.

Substatus as text.

Remote host infos.

Event ID meaning.

Event logs

```
~$ cat failed-login.xml
```

```

<Event>
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="54849625-5478-49
    <EventID>4625</EventID>
    ...
    <TimeCreated SystemTime="2021-11-26 08:48:35.1597150" />
    <EventRecordID>6895</EventRecordID>
    ...
    <Channel>Security</Channel>
    <Computer>DESKTOP-I2KNJ8H</Computer>
    <Security />

```

```
~$ cat failed-login-ez-evt-x-explorer.xml
```

```

{
  "PayloadData1": "Target: .\\lanx",
  "PayloadData2": "LogonType 3",
  "PayloadData3": "FailureReason: user name does not exist",
  "UserName": "-\\-",
  "RemoteHost": "DESKTOP-NI9V1EK (10.0.0.1)",
  "ExecutableInfo": "-",
  "MapDescription": "Failed logon",
  "ChunkNumber": 82,
  "Computer": "DESKTOP-I2KNJ8H",
  "Payload": "{\"EventData\":{\"Data\ ...}]",
  "Channel": "Security",
  "Provider": "Microsoft-Windows-Security-Auditing",
  "EventId": 4625,
  "EventRecordId": "6895",
  "ProcessId": 596,
  "ThreadId": 664,
  "Level": "LogAlways",
  "Keywords": "Audit failure",
  "SourceFile": "Z:\\logs-remote-access\\Security.evtx",
  "ExtraDataOffset": 0,
  "HiddenRecord": false,
  "TimeCreated": "2021-11-26T08:48:35.1597150+00:00",
  "RecordNumber": 6895
}

```

Are there any interesting or suspicious logons?



status and description

are currently no request.

name does not exist. The user name is correct but is either due to a restriction.

known user name or tried to logon outside of restrictions.

station restriction (look for event ID 4625).

ed password.

unt is currently disabled.

ates the Sam Server operation.

ks between DC and other computer too far out of sync.

user has not been granted the requested logon type (logon right) at this machine.

logon request failed because the primary domain attempt was made to logon but not started.

unt expiration.

is required to change password.

ntly a bug in Windows authentication.

is currently locked out.

Well... Maybe... Maybe not...

```

  <Data Name="IpPort">0</Data>
</EventData>
</Event>

```

Logon Failure: The machine is protected by an authentication firewall. The specified account is not allowed to authenticate to the machine.

Log Sample:

Event logs

```
~$ cat failed-login.xml
```

```

<Event>
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="54849625-5478-49
    <EventID>4625</EventID>
    ...
    <TimeCreated SystemTime="2021-11-26 08:4
    <EventRecordID>6895</EventRecordID>
    ...
    <Channel>Security</Channel>
    <Computer>DESKTOP-I2KNJ8H</Computer>
    <Security />
  </System>
  <EventData>
    <Data Name="IpPort">0</Data>
  </EventData>
</Event>

```

Are there any interesting or suspicious logons?

```
~$ cat failed-login-ez-evt-x-explorer.xml
```

```

{
  "PayloadData1": "Target: .\\lanx",
  "PayloadData2": "LogonType 3",
  "PayloadData3": "FailureReason: user name does not exist",
  "UserName": "-\\-",
  "RemoteHost": "DESKTOP-NI9V1EK (10.0.0.1)",
  "ExecutableInfo": "-",
  "MapDescription": "Failed logon",
}

```

- Has a user just made a typo?
- Or someone is trying account info bruteforcing?
- And: is this host allowed to access this account at all?



...ation (look for event
red password
ount is currently dis
icates the Sam Ser
desired operation.
ks between DC and other computer too far out of sync
user has not been granted the requested logon type
logon right) at this machine
logon request failed beca
een the primary domain a
attempt was made to logon
not started.
ount expiration
is required to change pas
ently a bug in Windows ar
is currently locked out

Logon Failure: The machine yi
protected by an authentication firewall. The specified
account is not allowed to authenticate to the machine.

Log Sample:

Well...
Maybe...
Maybe not...

Event logs

Which event Ids are interesting? What are meaning of status codes? How do I find out, if....

Accounts related stuff

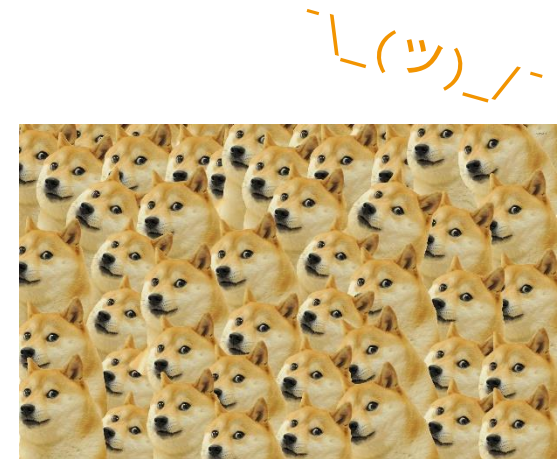
- 4624/4625 - successful/failed logon
- 4672 - login as admin
- 4648 - login with explicit credentials
- 4720 - account created
- ...

„Security events“

- 4950 - firewall settings are changed
- 5025 - firewall is disabled
- 1006 - malware detected
- 5012 - Scanning for viruses is disabled
- ...

Logging manipulation

- 1102 - Audit Log Cleared - Security Logs
- 104 - Audit Log Cleared - System Log
- ...



Event logs

Which event Ids are interesting? What are meaning of status codes? How do I find out, if....

Accounts related stuff

- 4624/4625 - successful/failed logon
- 4672 - login as admin
- 4648 - login with explicit credentials
- 4720 - account created
- ...

„Security events“

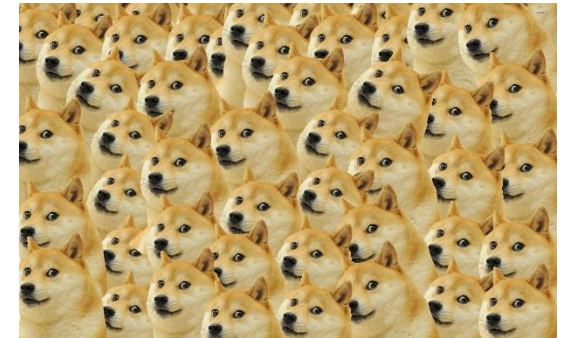
- 4950 - firewall settings are changed
- 5025 - firewall is disabled
- 1006 - malware detected
- 5012 - Scanning for viruses is disabled
- ...

Logging manipulation

- 1102 - Audit Log Cleared - Security Logs
- 104 - Audit Log Cleared - System Log
- ...

Also:

- RDP related
- services related
- tasks related
- powershell
- and many more!



[<https://digitalforensics.wordpress.com/2020/08/10/notable-event-ids-from-windows-event-logs/>]

[<https://wiki.sans.blue/#!Tools/WindowsEventLogsTable.md>]

[<https://github.com/mdecrevoisier/Windows-auditing-mindmap>]



Are there any traces of
remote execution?

Event logs to the rescue vol. II

line	Event R...	Time Created	Event Id	Channel	Computer	Map Description	User Name	Remote Host	Exec...	Process Name	Target	Payload Data2	Payload Data3
485	12053	2021-11-28 15:34:00	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x7F4275
486	12056	2021-11-28 15:34:30	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x7F59FE
487	12060	2021-11-28 15:41:55	4624	Security	DESKTOP-I2KNJ8H	Successful logon	WORKGROUP\DESKTOP-I2KNJ8H\$	- (-)		C:\Windows\System32\services.exe	Target: NT AUTHORITY\SYSTEM	LogonType 5	LogonId: 0x3E7
488	12061	2021-11-28 15:41:55	4672	Security	DESKTOP-I2KNJ8H	Administrative logon	NT AUTHORITY\SYSTEM (S-1-...			C:\Windows\System32\services.exe	PrivilegeList: SeAssignPrimaryTokenP...	LogonId: 0x3E7	
489	12066	2021-11-28 15:45:50	4624	Security	DESKTOP-I2KNJ8H	Successful logon	WORKGROUP\DESKTOP-I2KNJ8H\$	- (-)		C:\Windows\System32\services.exe	Target: NT AUTHORITY\SYSTEM	LogonType 5	LogonId: 0x3E7
490	12067	2021-11-28 15:45:50	4672	Security	DESKTOP-I2KNJ8H	Administrative logon	NT AUTHORITY\SYSTEM (S-1-...			C:\Windows\System32\services.exe	PrivilegeList: SeAssignPrimaryTokenP...	LogonId: 0x3E7	
491	12068	2021-11-28 15:46:11	4672	Security	DESKTOP-I2KNJ8H	Administrative logon	DESKTOP-I2KNJ8H\lynx (S-1-...			C:\Windows\PSEXESVC.exe	PrivilegeList: SeSecurityPrivilege, ...	LogonId: 0x85CF61	
492	12069	2021-11-28 15:46:11	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: DESKTOP-I2KNJ8H\lynx	LogonType 3	LogonId: 0x85CF61
493	12071	2021-11-28 15:46:11	4648	Security	DESKTOP-I2KNJ8H	A logon was attempte...	WORKGROUP\DESKTOP-I2KNJ8H\$	- (-)		C:\Windows\PSEXESVC.exe	Target: DESKTOP-I2KNJ8H\lynx	TargetServerName: localhost	PID: 0x1788
494	12072	2021-11-28 15:46:11	4624	Security	DESKTOP-I2KNJ8H	Successful logon	WORKGROUP\DESKTOP-I2KNJ8H\$	DESKTOP-I2KNJ8H (-)		C:\Windows\PSEXESVC.exe	Target: DESKTOP-I2KNJ8H\lynx	LogonType 2	LogonId: 0x85D04A
495	12073	2021-11-28 15:46:11	4624	Security	DESKTOP-I2KNJ8H	Successful logon	WORKGROUP\DESKTOP-I2KNJ8H\$	DESKTOP-I2KNJ8H (-)		C:\Windows\PSEXESVC.exe	Target: DESKTOP-I2KNJ8H\lynx	LogonType 2	LogonId: 0x85D067
496	12074	2021-11-28 15:46:11	4672	Security	DESKTOP-I2KNJ8H	Administrative logon	DESKTOP-I2KNJ8H\lynx (S-1-...				PrivilegeList: SeSecurityPrivilege, ...	LogonId: 0x85D04A	
497	12076	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D341
498	12078	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D35A
499	12080	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D373
500	12082	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D38E
501	12084	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D3AD
502	12086	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D3AD
503	12088	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D3AD
504	12090	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D3AD
505	12092	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D3AD
506	12094	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D3AD
507	12096	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D3AD
508	12098	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D3AD
509	12100	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D3AD
510	12103	2021-11-28 15:46:42	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-I19V1EK (10.0.0.1)	-		Target: NT AUTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x85D3AD

Successful network logon from remote host 10.0.0.1

C:\Windows\PSEXESVC.exe

LogonType 3

PsExec is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. PsExec's most powerful uses include launching interactive command-prompts on remote systems and remote-enabling tools like IpConfig that otherwise do not have the ability to show information about remote systems.

[https://docs.microsoft.com/en-us/sysinternals/downloads/psexec]

Further artifacts

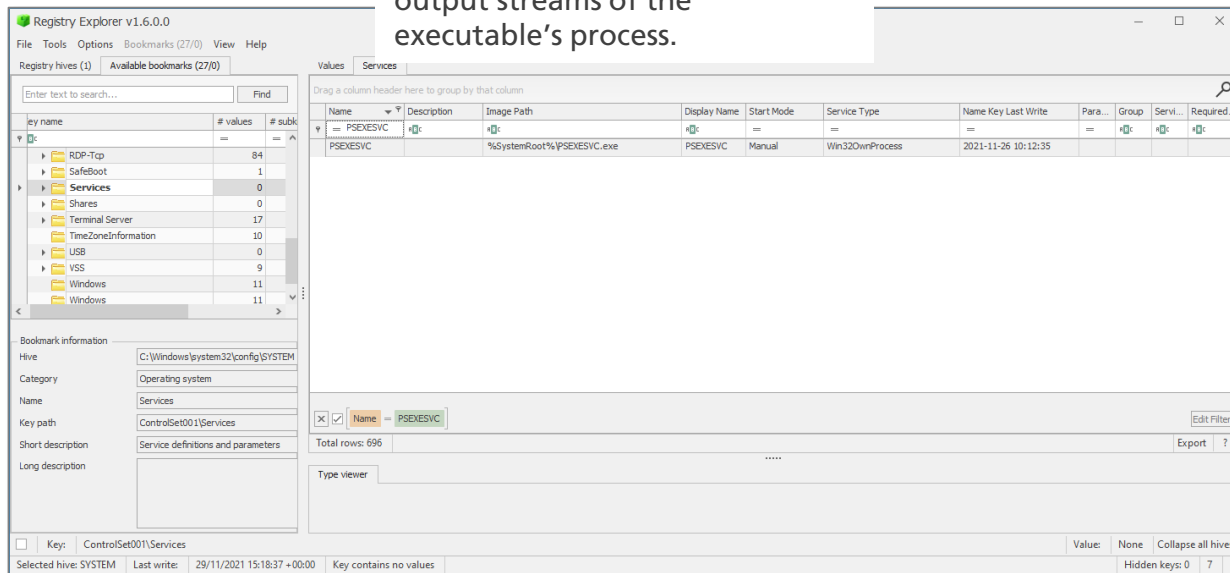
Copies PSEXESVC.exe to C:\Windows\ as well as other executed binaries:

```

~$ ls c:\windows\
...
-a----      11/26/2021  11:30 PM          208384 notepad.exe
-a----      11/28/2021   3:42 PM           6336 PFR0.log
-a----      12/7/2019   10:10 AM          31241 ProfessionalEducationN.xml
-a----      12/7/2019   10:10 AM          31281 ProfessionalN.xml
-a----      12/7/2019   10:10 AM          31241 ProfessionalWorkstationN.xml
-a----      11/28/2021   3:47 PM          496016 PSEXESVC.exe
-a----      4/9/2021     3:50 PM          370176 regedit.exe
-a----      11/3/2021    3:57 PM          136192 splwow64.exe
...

```

Creates and starts PSEXESCV service that controls input and output streams of the executable's process.



Program execution evidence for PSEXESVC service and remotely executed programs:

prefetch

```

...
Command line: -f C:\Windows\Prefetch\PSEXESVC.EXE-7F956DAF.pf
...
Created on: 2021-11-28 14:47:56
Modified on: 2021-11-28 14:47:56
Last accessed on: 2021-11-29 14:59:46

Executable name: PSEXESVC.EXE
Hash: 7F956DAF
File size (bytes): 18.842
Version: Windows 10

Run count: 1
Last run: 2021-11-28 14:47:45
...
5: \VOLUME{01d7d109adab1526-86adbfc}\WINDOWS
...
00: \VOLUME{01d7d109adab1526-86adbfc}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d7d109adab1526-86adbfc}\WINDOWS\PSEXESVC.EXE
...

Files referenced: 10

00: \VOLUME{01d7d109adab1526-86adbfc}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d7d109adab1526-86adbfc}\WINDOWS\SUSPICIOUS.EXE
...

```

The screenshot shows the Timeline Explorer interface with a table of process execution events:

Line	Tag	Id	Exe Info	End Time	Duration Ms	Timestamp
5276		6352	PSEXESVC.exe	2021-11-26 10:01:51	511779	2021-11-26 10:01:53
5376		6452	PSEXESVC.exe	2021-11-26 10:15:00	608876	2021-11-26 10:15:00
5442		6518	suspicious.exe	2021-11-26 10:15:00	120000	2021-11-26 10:15:00
5522		6598	suspicious.exe	2021-11-26 10:15:41	41110	2021-11-26 10:44:00
5500		6576	PSEXESVC.exe	2021-11-26 10:18:00	119986	2021-11-26 10:44:00
5644		6720	PSEXESVC.exe	2021-11-26 11:33:00	120005	2021-11-26 11:44:00
15235		16311	PSEXESVC.exe	2021-11-28 15:13:00	643546	2021-11-28 15:17:00
15547		16623	suspicious.exe	2021-11-28 15:35:00	119992	2021-11-28 15:45:00
15524		16600	PSEXESVC.exe	2021-11-28 15:37:00	719994	2021-11-28 15:45:00
15685		16761	suspicious.exe	2021-11-28 15:47:00	60007	2021-11-28 16:21:00
15689		16765	PSEXESVC.exe	2021-11-28 15:50:00	180015	2021-11-28 16:21:00

Further artifacts

~/df/06-artifacts/ Event logs to the rescue vol. II

Successful network logon from remote host 10.0.0.1

PSEXEC is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. PSEXEC's most powerful uses include launching interactive command prompts on remote systems and remote-enabling tools like IpConfig that otherwise do not have the ability to show information about remote systems.

[https://docs.microsoft.com/en-us/sysinternals/downloads/psexec]

~/df/06-artifacts/ Further artifacts

Program execution evidence for PSEXECV service and remotely executed programs:

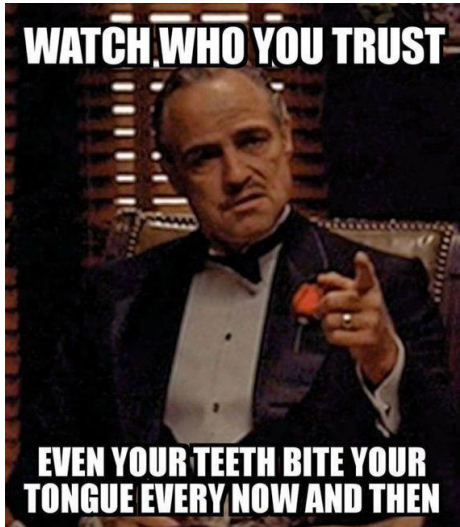
Copies PSEXECV.exe to C:\Windows\ as well as other executed binaries:

Creates and starts PSEXECV service that controls input and output streams of the executable's process.

SRUM

~/df/06-artifacts/ Are there any traces of remote execution?

Key Takeaways



Everything can be forged!
Don't rely on a single artifact!
Check for consistency!



Do your own experiments!
Validate findings of others!

Any Questions?

