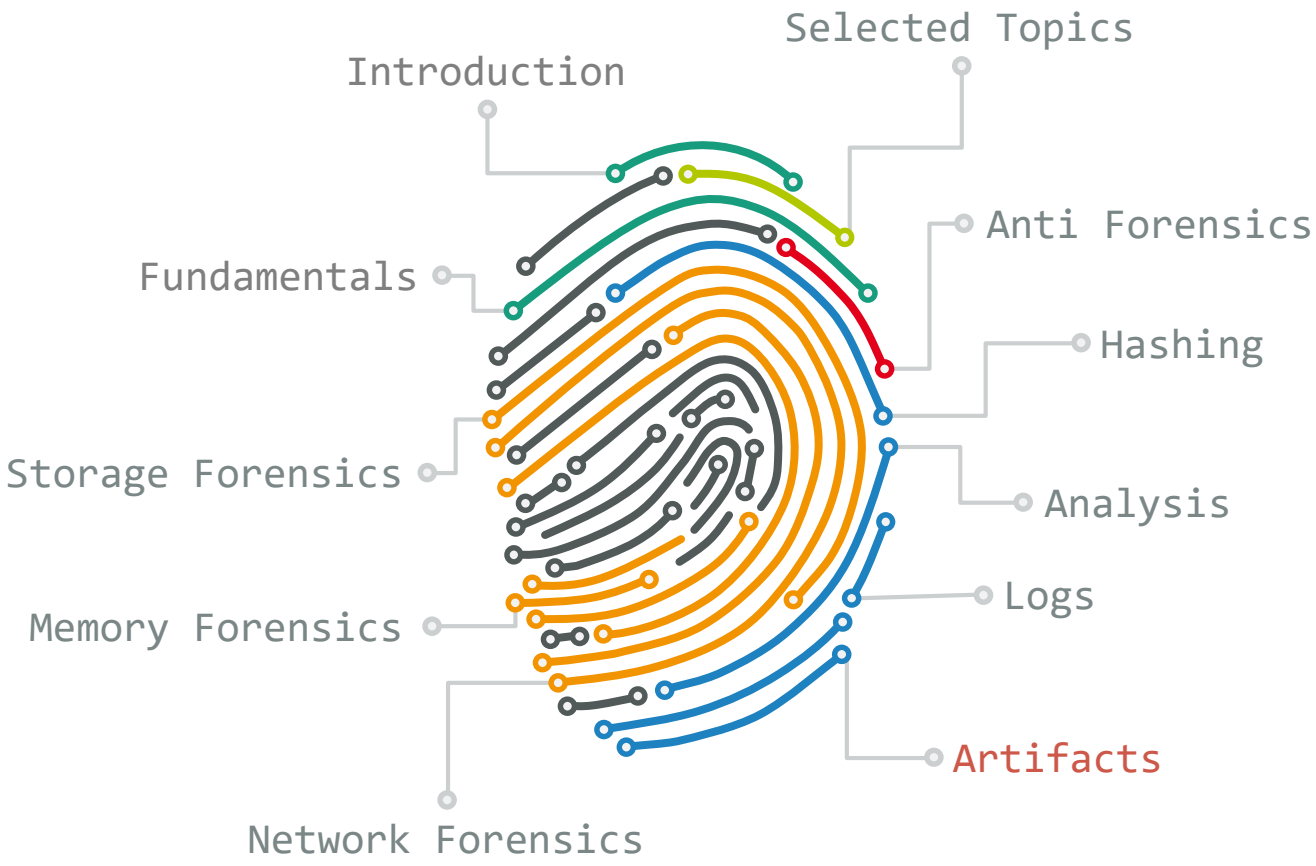
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Prof. Dr. Elmar Padilla et al.

Digitale Forensik

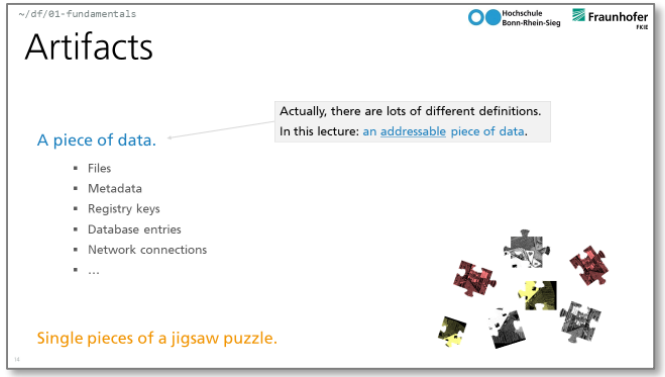
06 - Artifacts

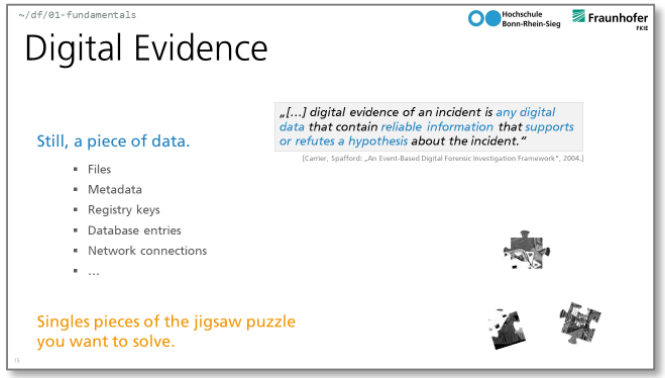


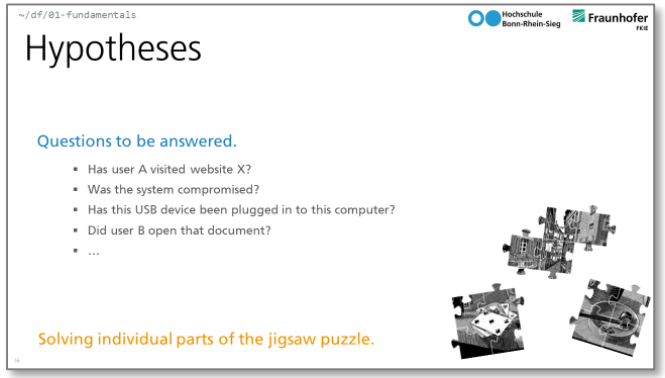
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts







An addressable piece of data.

Single pieces of a jigsaw puzzle.

Still, a piece of data.

Singles pieces of the jigsaw puzzle you want to solve.

Questions to be answered.

Solving individual parts of the jigsaw puzzle.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts

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

Until the next update, that is ¯_(ツ)_/¯

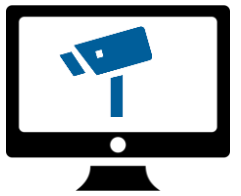
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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!

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

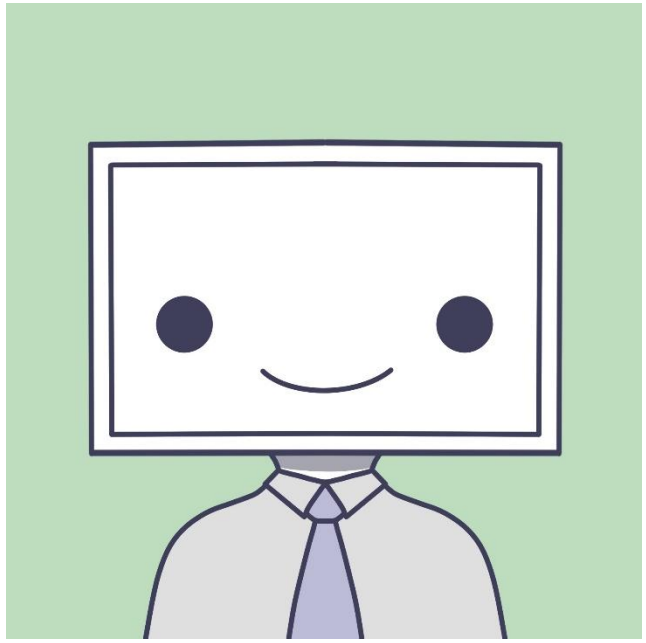
Artifacts: Windows

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts: Windows

user-specific



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

vs.

system-specific

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

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?

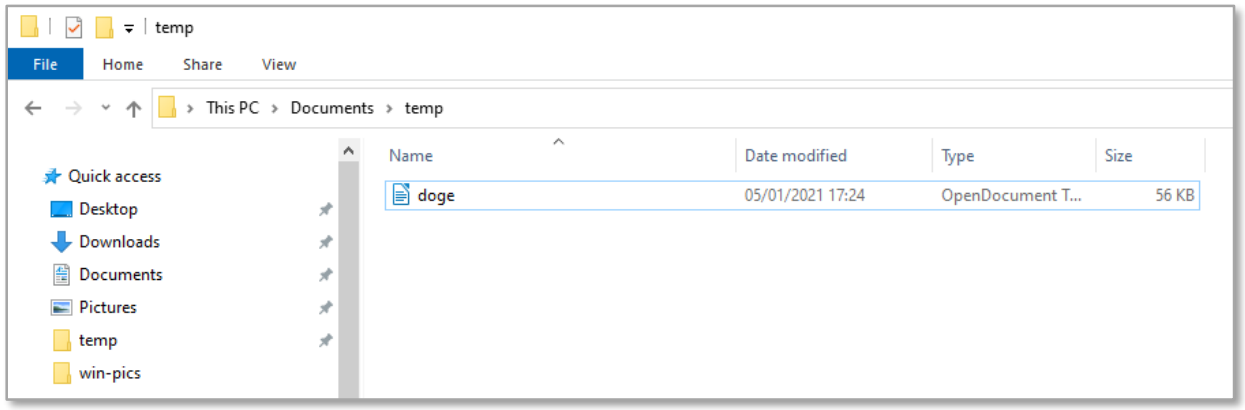
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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
…
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 ----------
```

Remember the name!

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

```
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 ----------
```

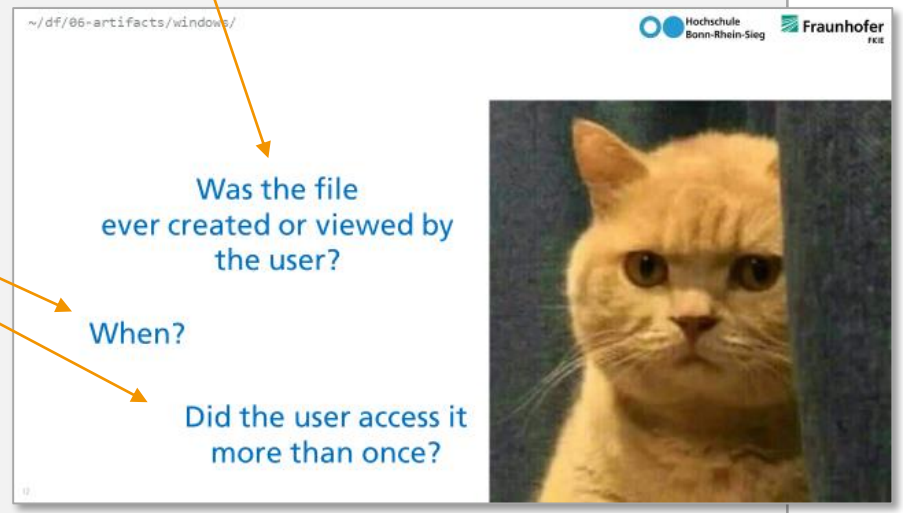
time created -> first interaction with the original file
time modified -> last interaction with the original file

time created != time modified

=> opened more than once

LNK file is modified each time the original is opened.

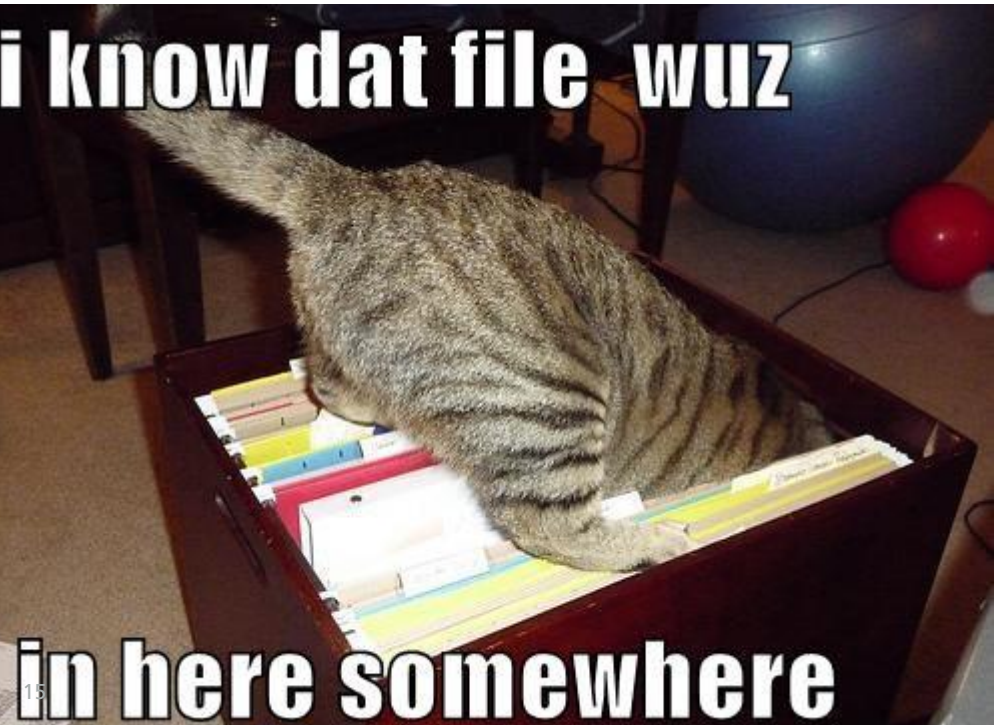
```
PS C:\> LECmd.exe -f C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge.lnk

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 ----------
```



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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
```

time created == time modified

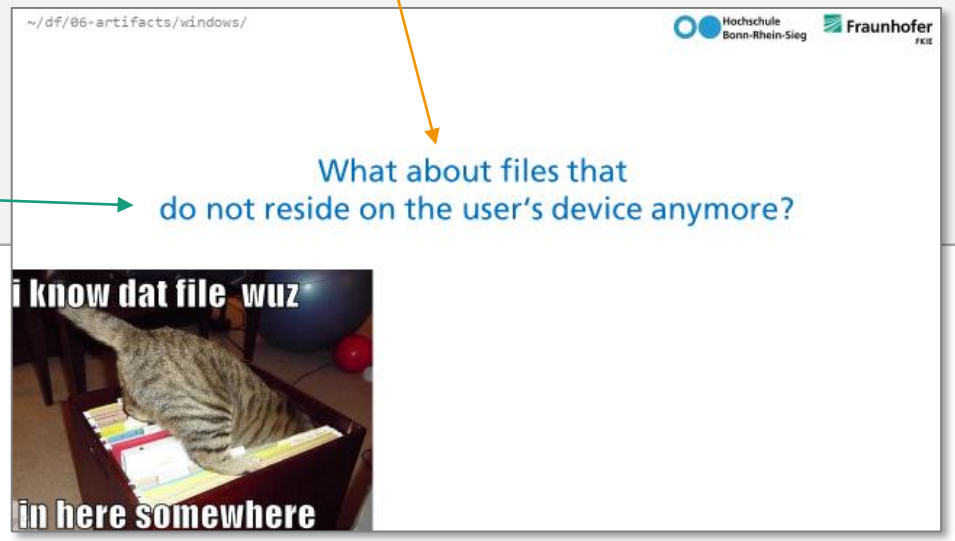
=> opened once

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
```

time created == time modified

=> opened once



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Find F:\!

Or: don‘t trust drive letters.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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
```

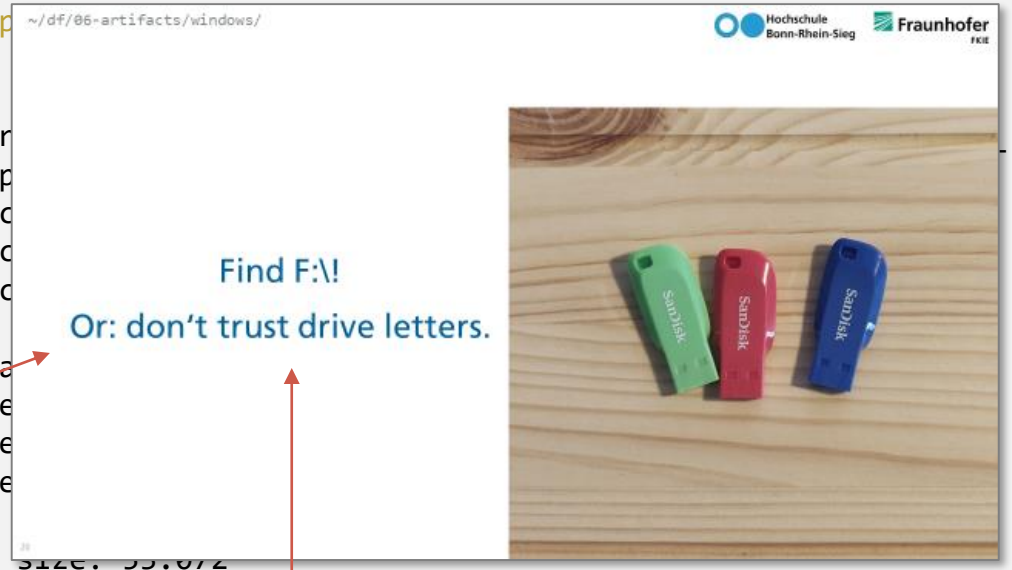
different devices!

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.jp

Source
C:\User
fine.jp
  Sourc
  Sourc
  Sourc

--- Hea
  Targe
  Targe
  Targe

  File

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

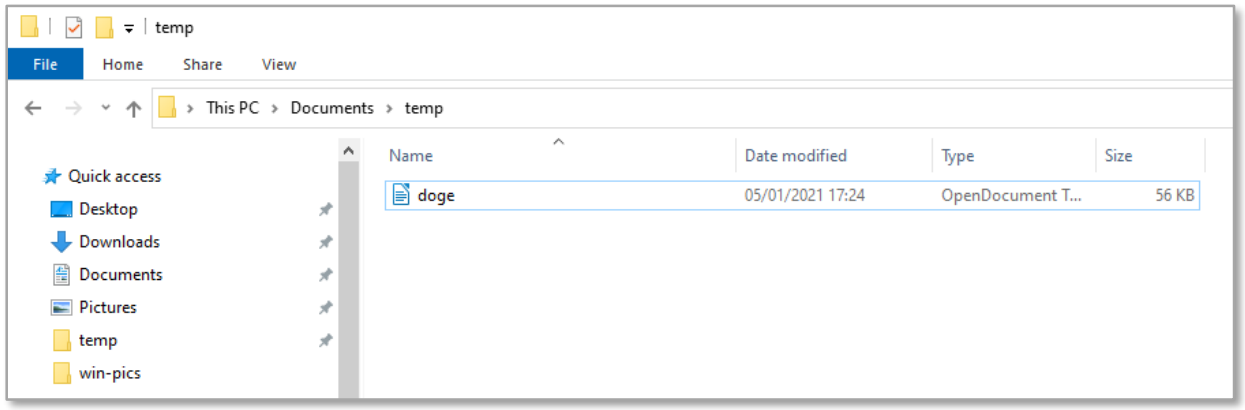


What if the file was deleted?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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
```

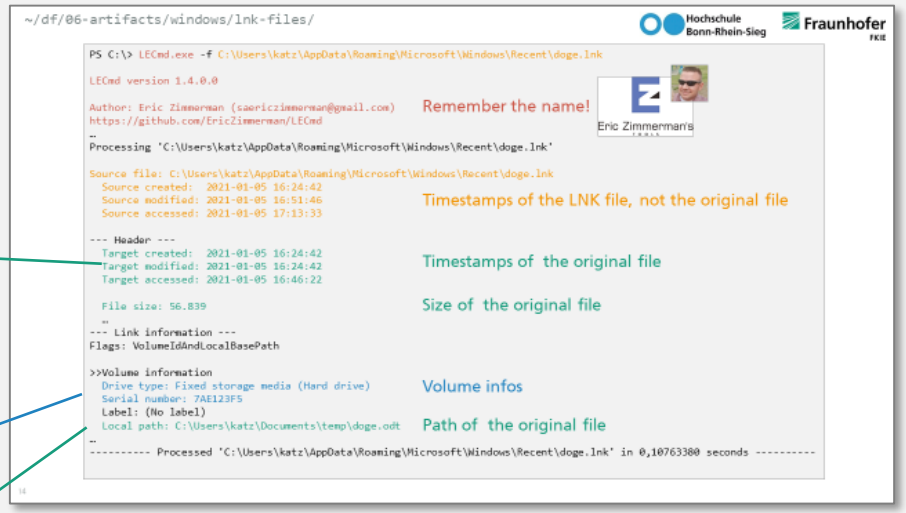
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

LNK files

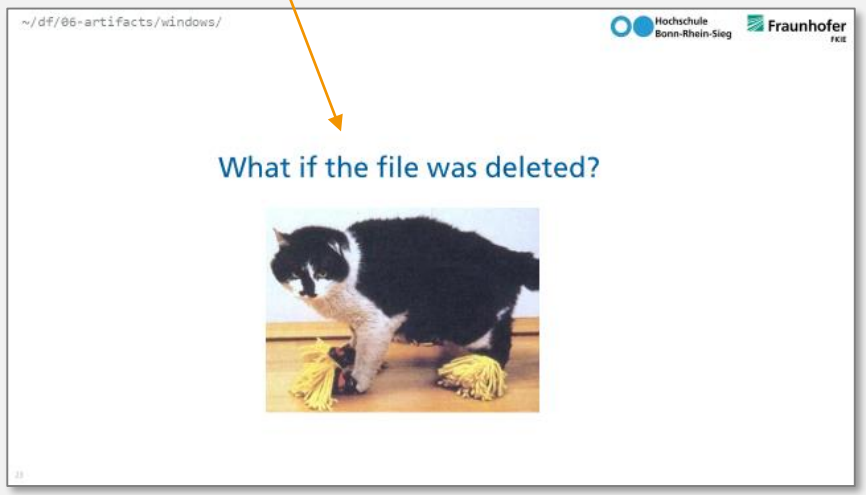
```
PS C:\> LECmd.exe -f C:\Users\katz\AppData\Roaming\Microsoft\Windows\Recent\doge1.lnk

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



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 ----------
```



Hochschule Bonn-Rhein-Sieg

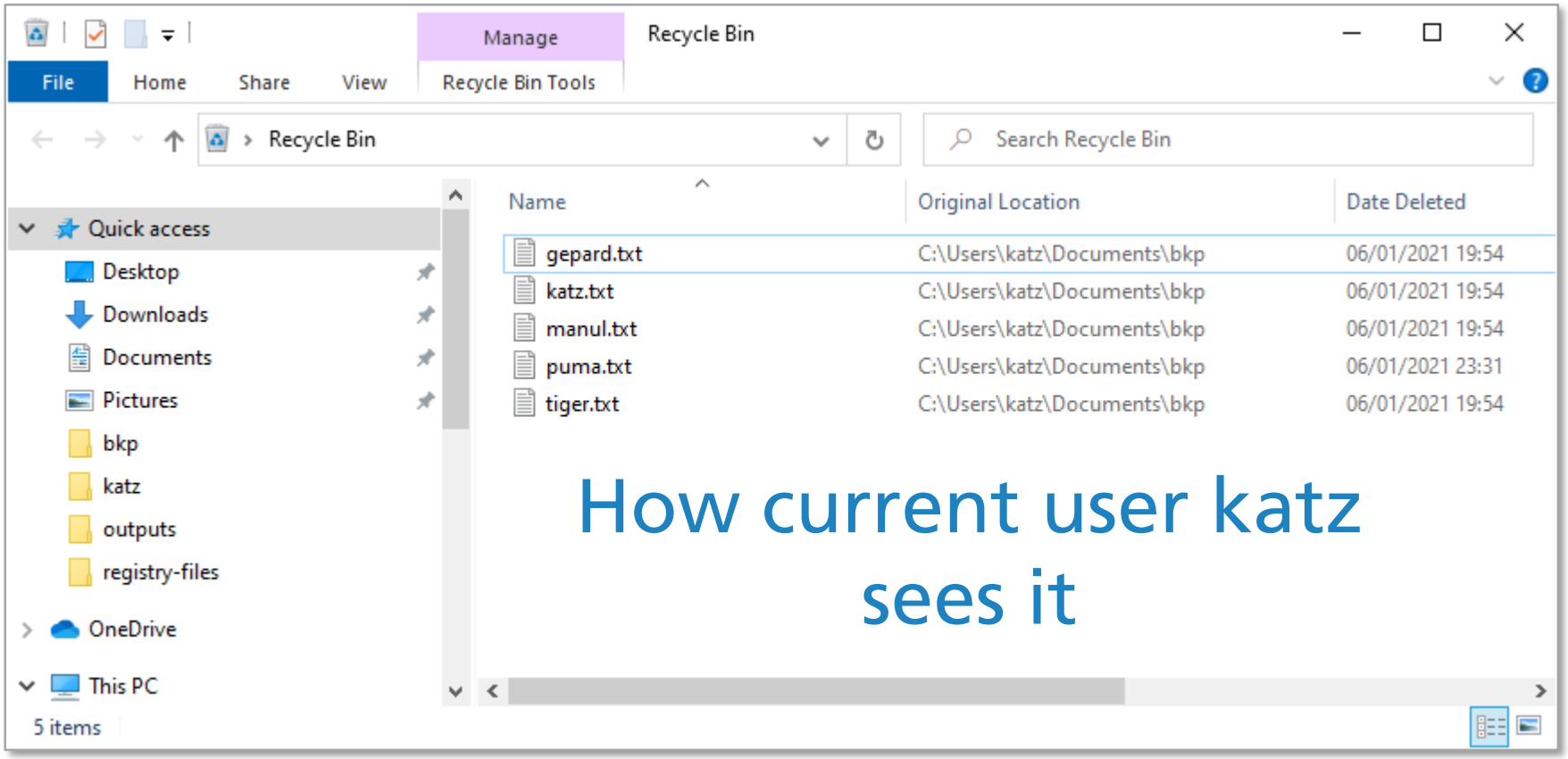
Fraunhofer FKIE

Recycle Bin

Speaking about deleted files.

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

Recycle Bin



How current user katz sees it

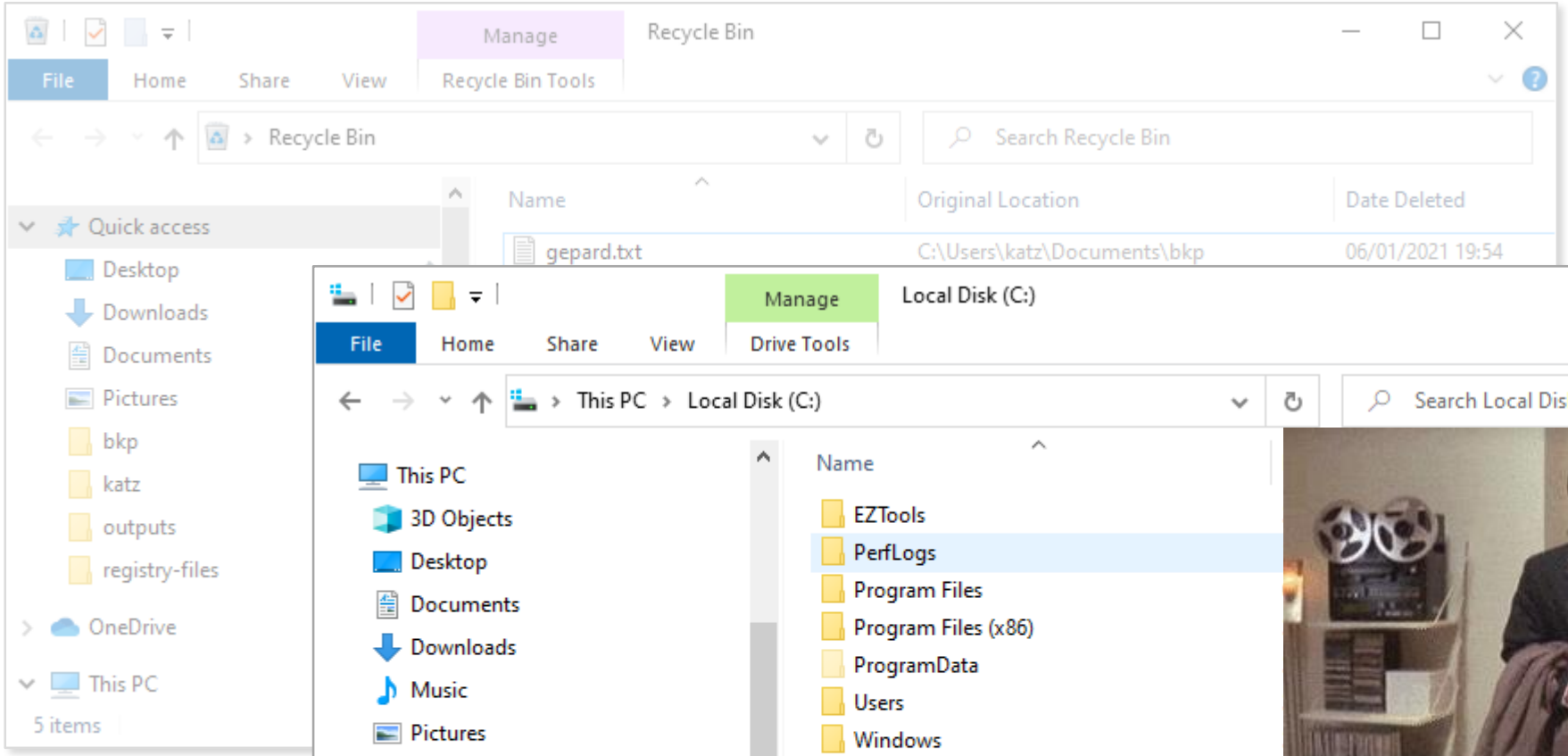
How the filesystem sees it:

`C:\$Recycle.Bin`

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Recycle Bin



How the filesystem sees it:

`C:\$Recycle.Bin`

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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

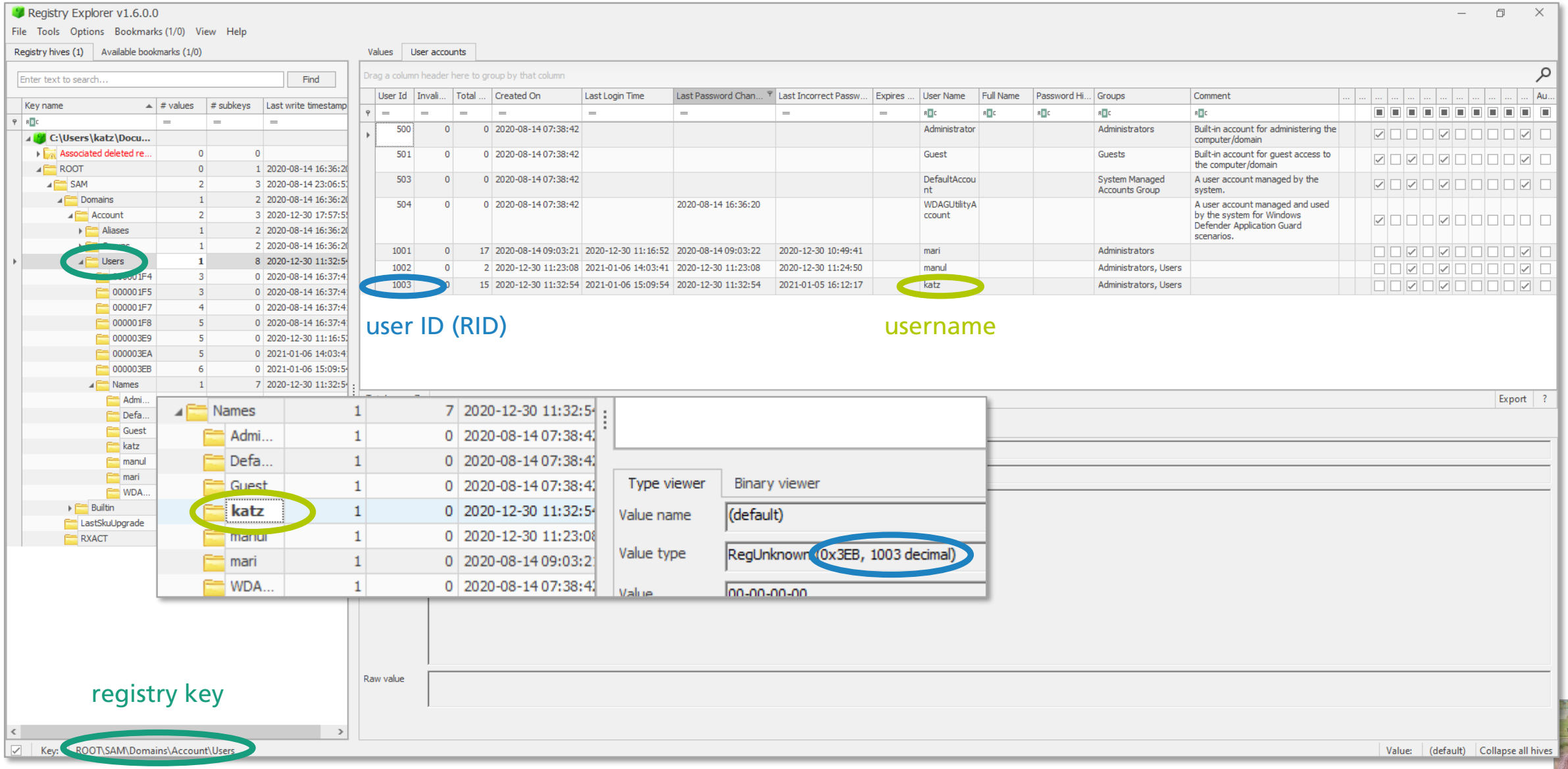
"A security identifier (SID) is a unique value of variable length that is used to identify a security principal (such as a security group) in Windows operating systems. SIDs that identify generic users or generic groups is [sic!] *well known."*

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

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

User name from SID



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Recycle Bin

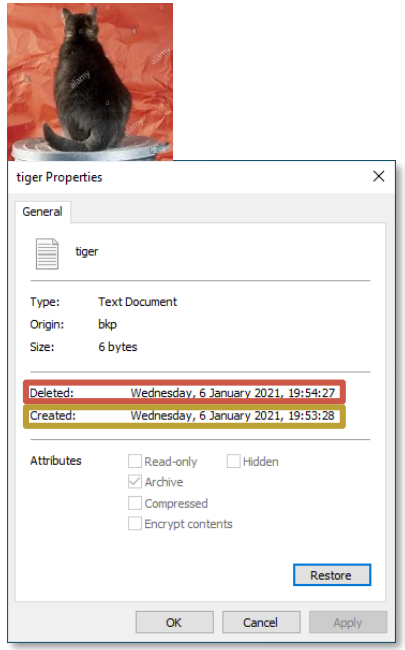
```
PS C:\$Recycle.Bin\S-1-5-21-1752181755-1580187878-119375555-1003> ls | sort Name

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/6/2021  11:31 PM            102 $I3WV62F.txt
-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
-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
```

$I files – metadata (binary)

$R files – recovery data

```
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
$RV52TY8.txt 1/7/2021 9:34:13 PM  1/6/2021 7:53:28 PM  1/6/2021 1:47:58 PM
```

tiger.txt deleted

```
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

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Did a user open a folder on an external media?

When?

What if it was deleted afterwards

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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`

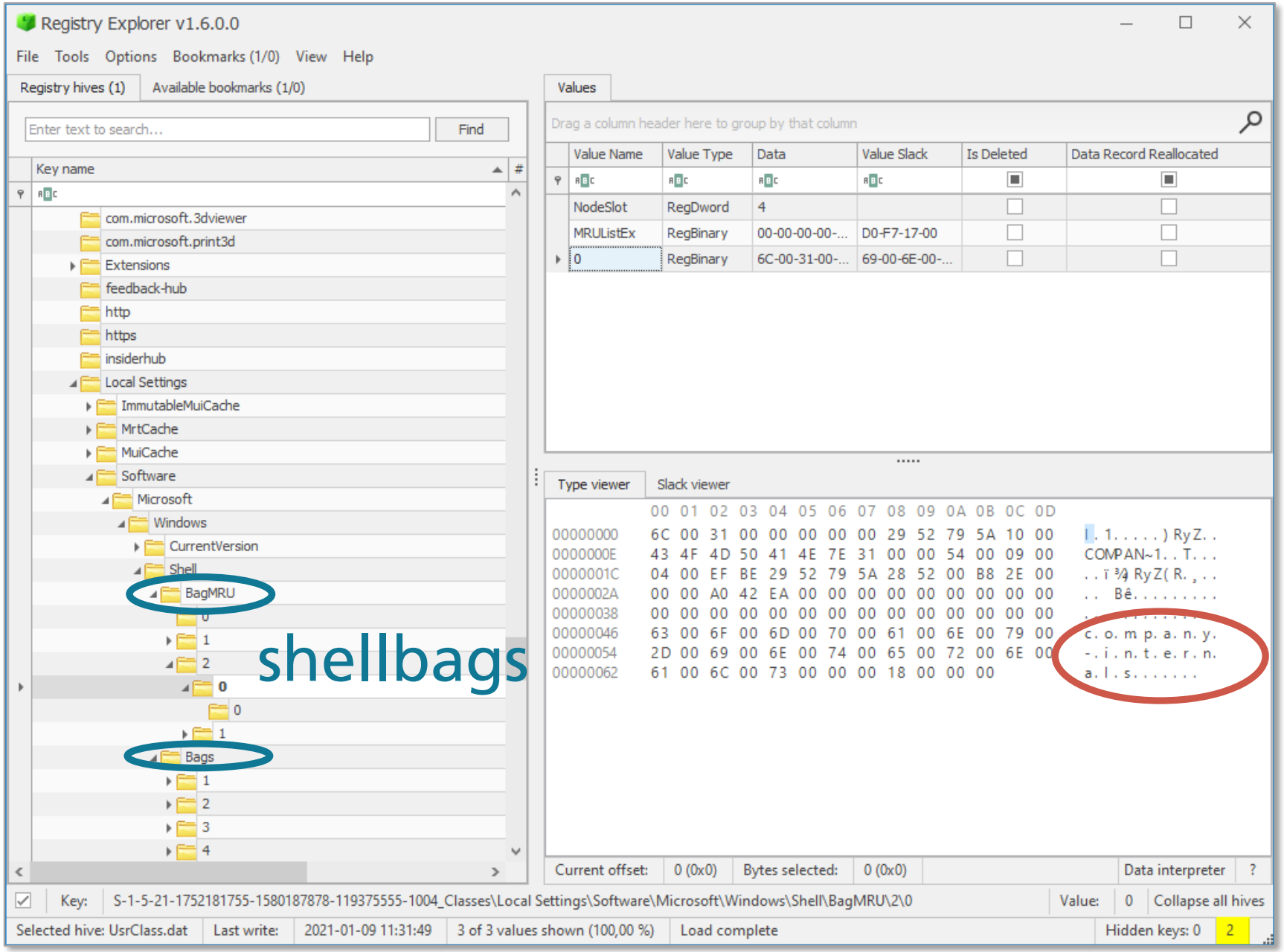
- Binary (registry)
- Proprietary (registry)
- Updated automatically on GUI interaction with a folder
- Viewed folder details

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Shellbags

I'm back, baby.



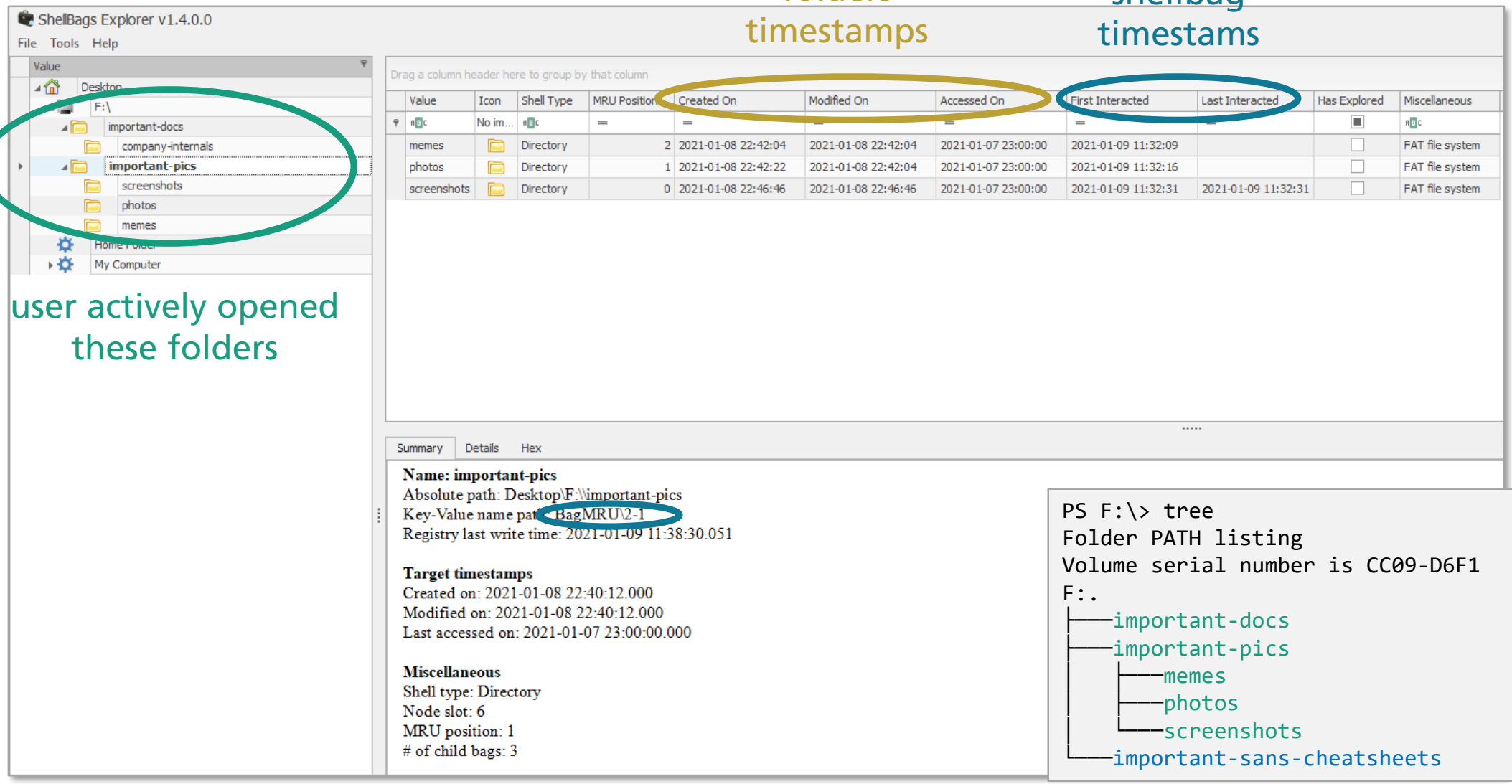
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Shellbags

folders timestamps

shellbag timestams



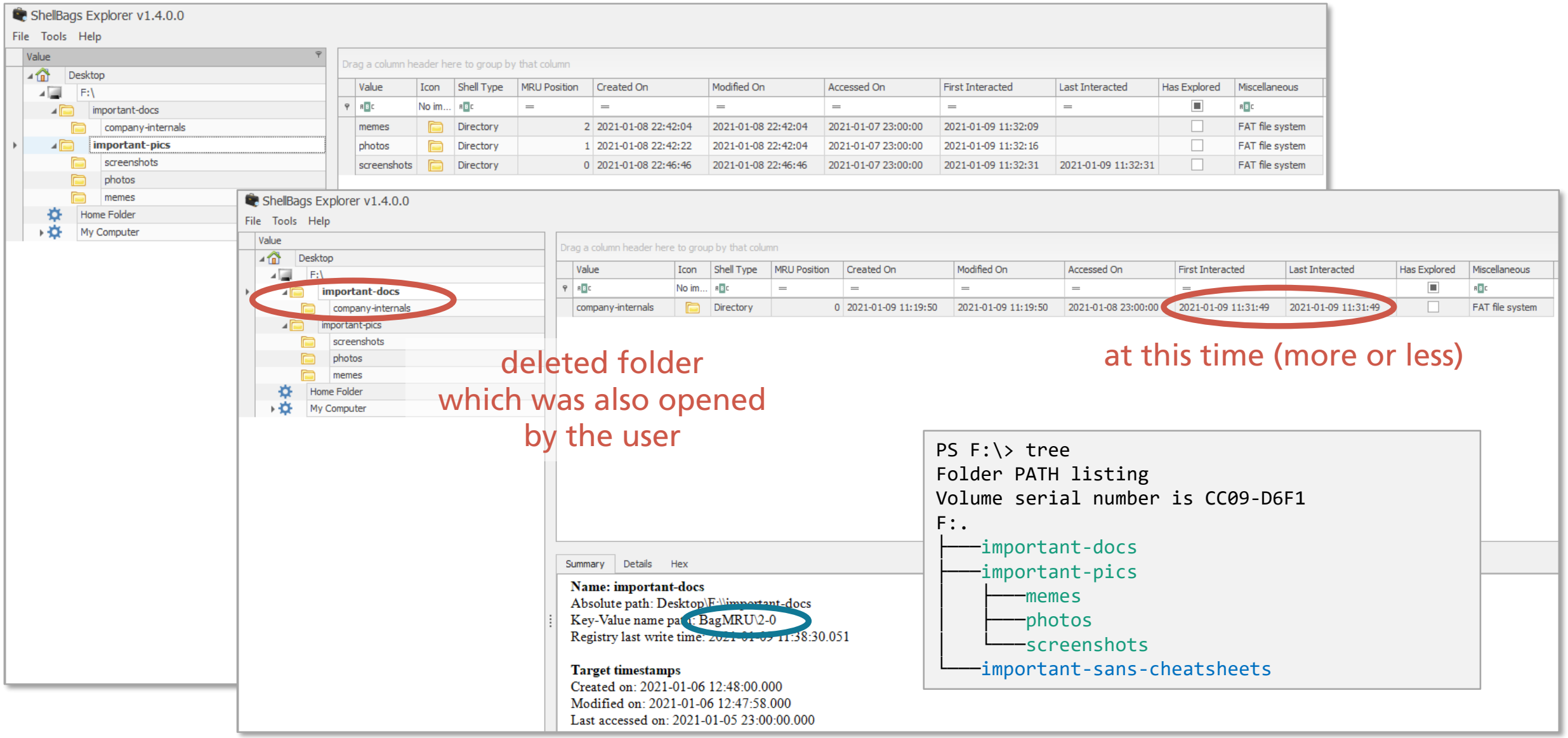
user actively opened these folders

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

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

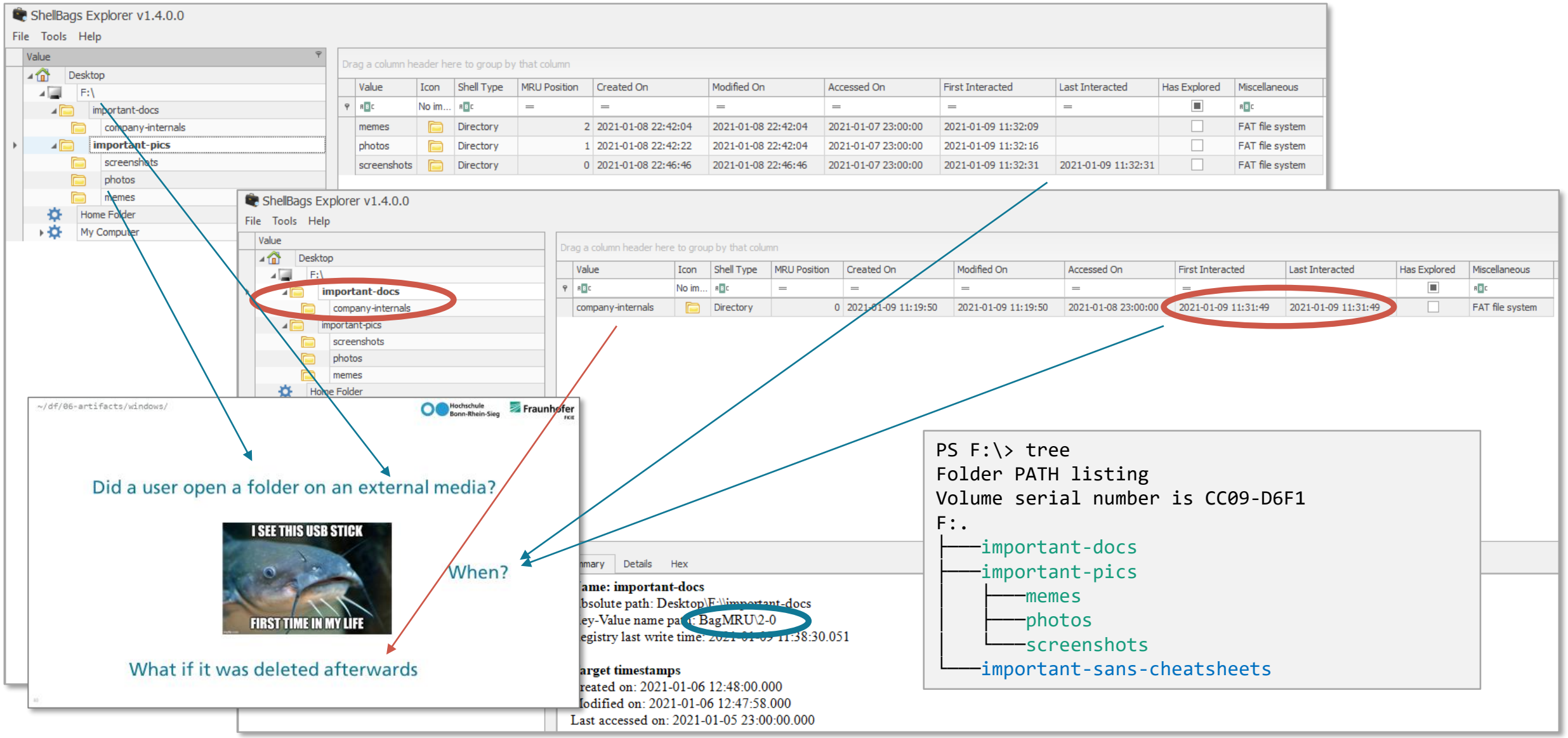
Shellbags



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Shellbags



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

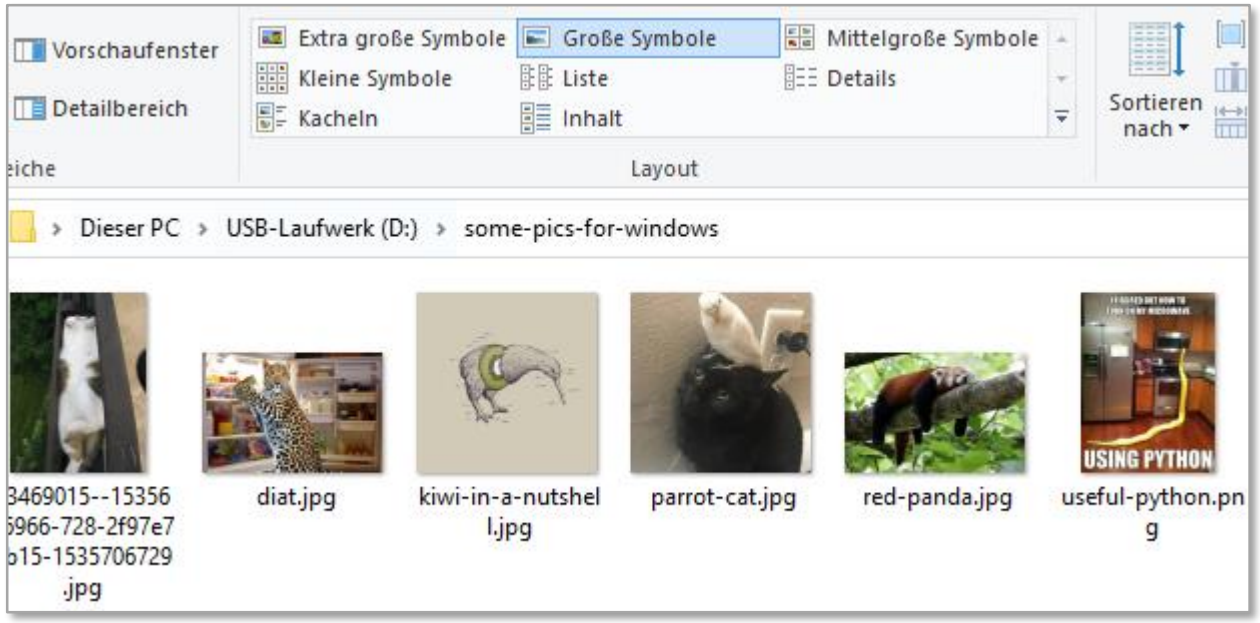
Speaking of external media…

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

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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

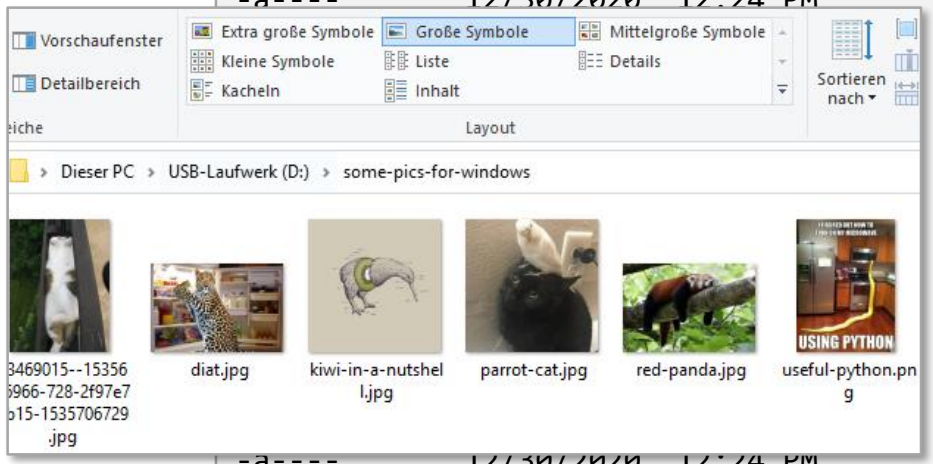
Image thumbnails database
small, medium, large, etc.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Thumbcache

Thumbcache Viewer

File Edit View Tools Help

#	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	a1884ffd52fc35e2.jpg	125192 B	18 KB	125280 B	18 KB	7e4d72ed62c951c7	8e7bed440c6e67bd	a1884ffd52fc35e2	Windows 10	D:\thumbnails\thumbcache_256.db
5	13f13b2031f27a0.jpg	239446 B	17 KB	239532 B	17 KB	a6f2057122d4dab7	8433c7acf8508cd4	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	f3e24a84aeef2e77.jpg	227624 B	11 KB	227712 B	11 KB	8ed8242c2e39ac8f	50ce8b475a8a2129	f3e24a84aeef2e77	Windows 10	D:\thumbnails\thumbcache_256.db
16	?7ae123f5?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	5db7bcb80eb23aa1.jpg	16276 B	8 KB	16364 B	8 KB	c752cbb78a094284	60a41dd50474b95b	5db7bcb80eb23aa1	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

Hochschule Bonn-Rhein-Sieg

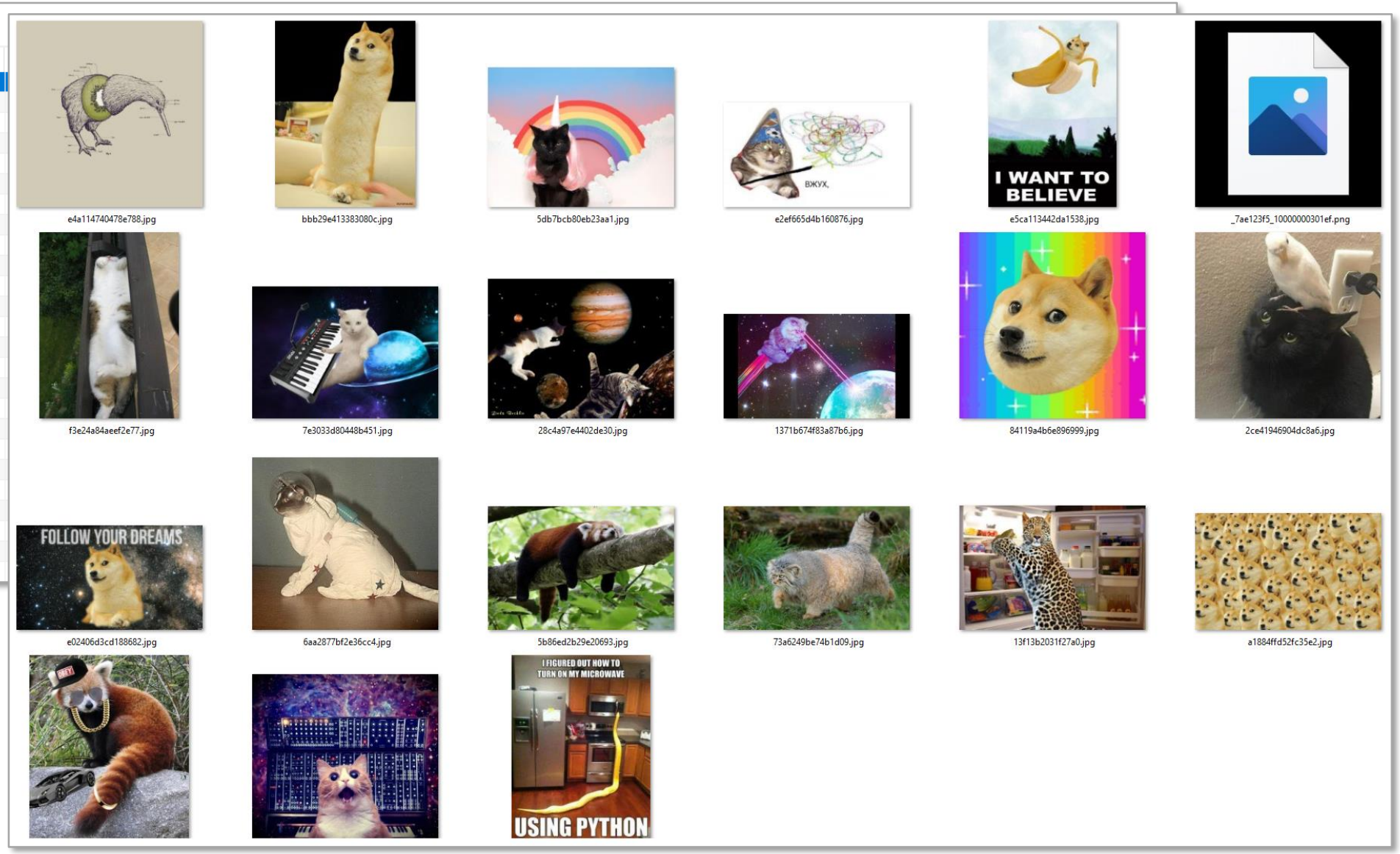
Fraunhofer FKIE

Thumbcache

Thumbcache Viewer

File Edit View Tools Help

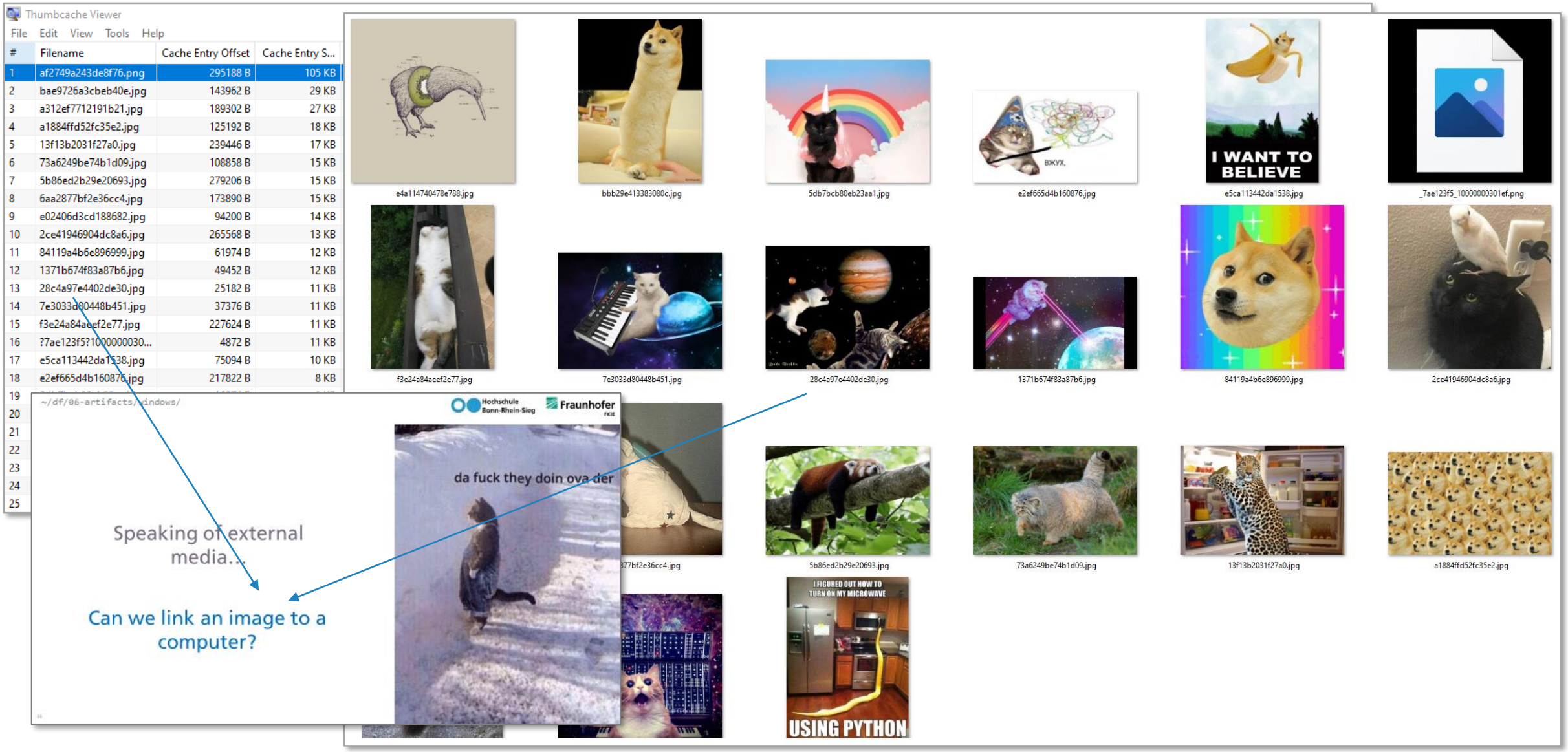
#	Filename	Cache Entry Offset	Cache Entry S...
1	af2749a243de8f76.png	295188 B	105 KB
2	bae9726a3cbeb40e.jpg	143962 B	29 KB
3	a312ef7712191b21.jpg	189302 B	27 KB
4	a1884ffd52fc35e2.jpg	125192 B	18 KB
5	13f13b2031f27a0.jpg	239446 B	17 KB
6	73a6249be74b1d09.jpg	108858 B	15 KB
7	5b86ed2b29e20693.jpg	279206 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	f3e24a84aeef2e77.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



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Thumbcache



WINDOWS REGISTRY

Recent files?

Autostart?

Malware persistence?

I'm back, baby.

Connected devices?

More user to program mappings?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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\`

```
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*

user hives

`%UserProfile%\NTUSER.DAT`

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

```
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)_/¯

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Registry

registry

system hives

%SystemRoot%\Windows\system32\config\

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
```

```
Length Name
------ ----

572864
```

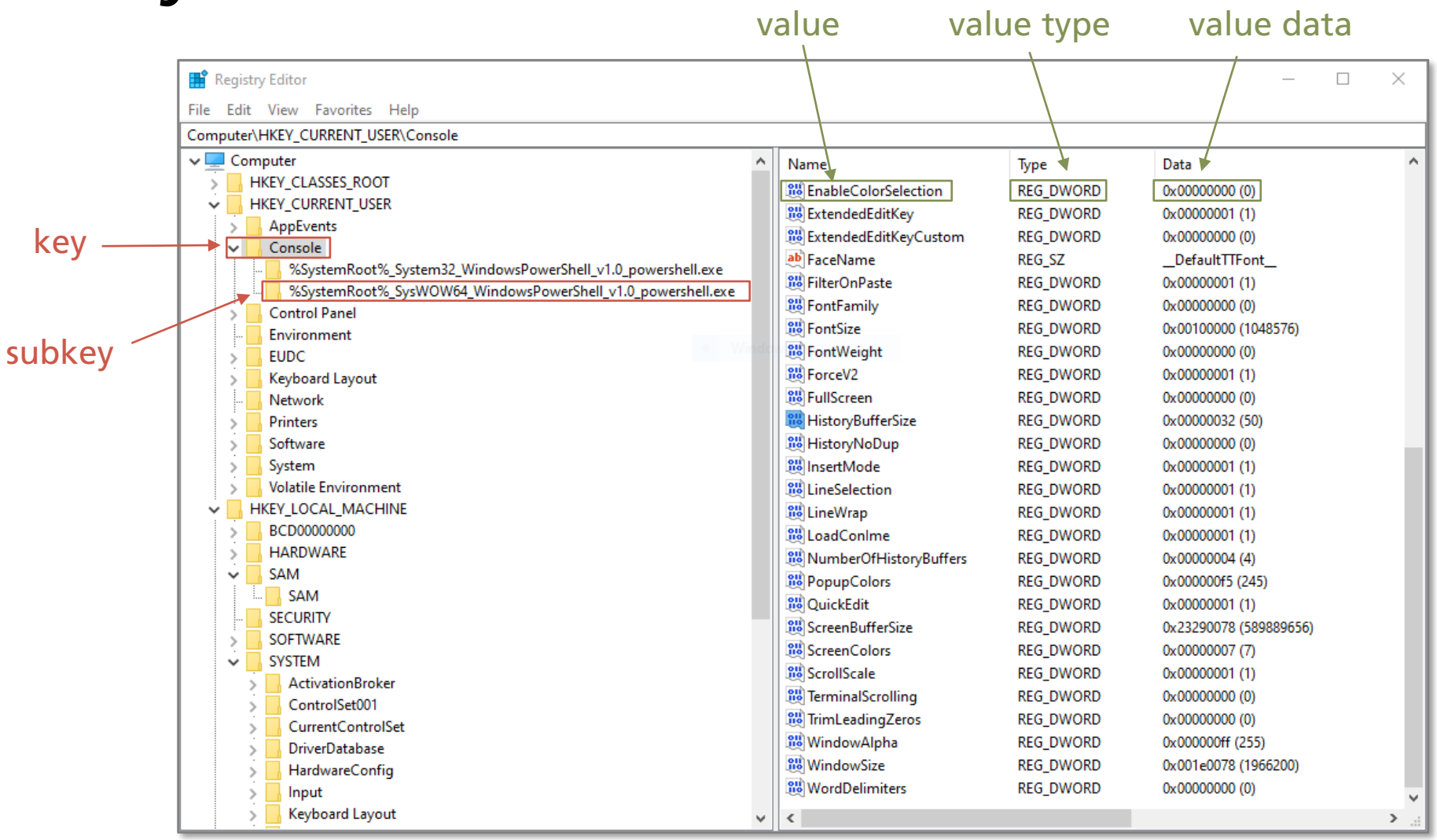
⇒ *moar*

⇒ *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)_/¯

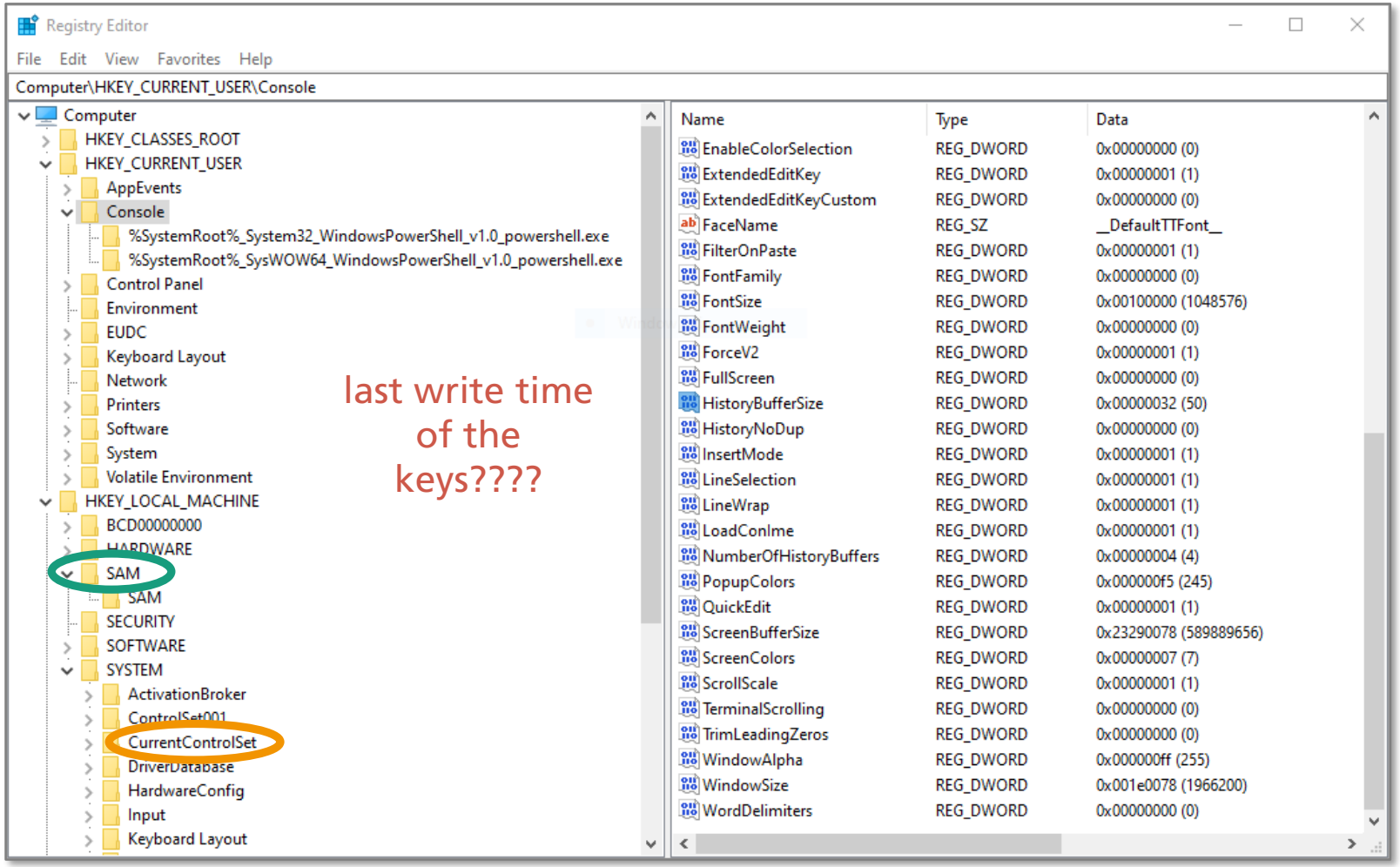
Registry


value
value type
value data
key
subkey
Registry Editor
File Edit View Favorites Help
Computer\HKEY_CURRENT_USER\Console
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
AppEvents
Console
%SystemRoot%_System32_WindowsPowerShell_v1.0_powershell.exe
%SystemRoot%_SysWOW64_WindowsPowerShell_v1.0_powershell.exe
Control Panel
Environment
EUDC
Keyboard Layout
Network
Printers
Software
System
Volatile Environment
HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
SAM
SAM
SECURITY
SOFTWARE
SYSTEM
ActivationBroker
ControlSet001
CurrentControlSet
DriverDatabase
HardwareConfig
Input
Keyboard Layout
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)
LoadConIme 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)

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Registry



last write time of the keys????

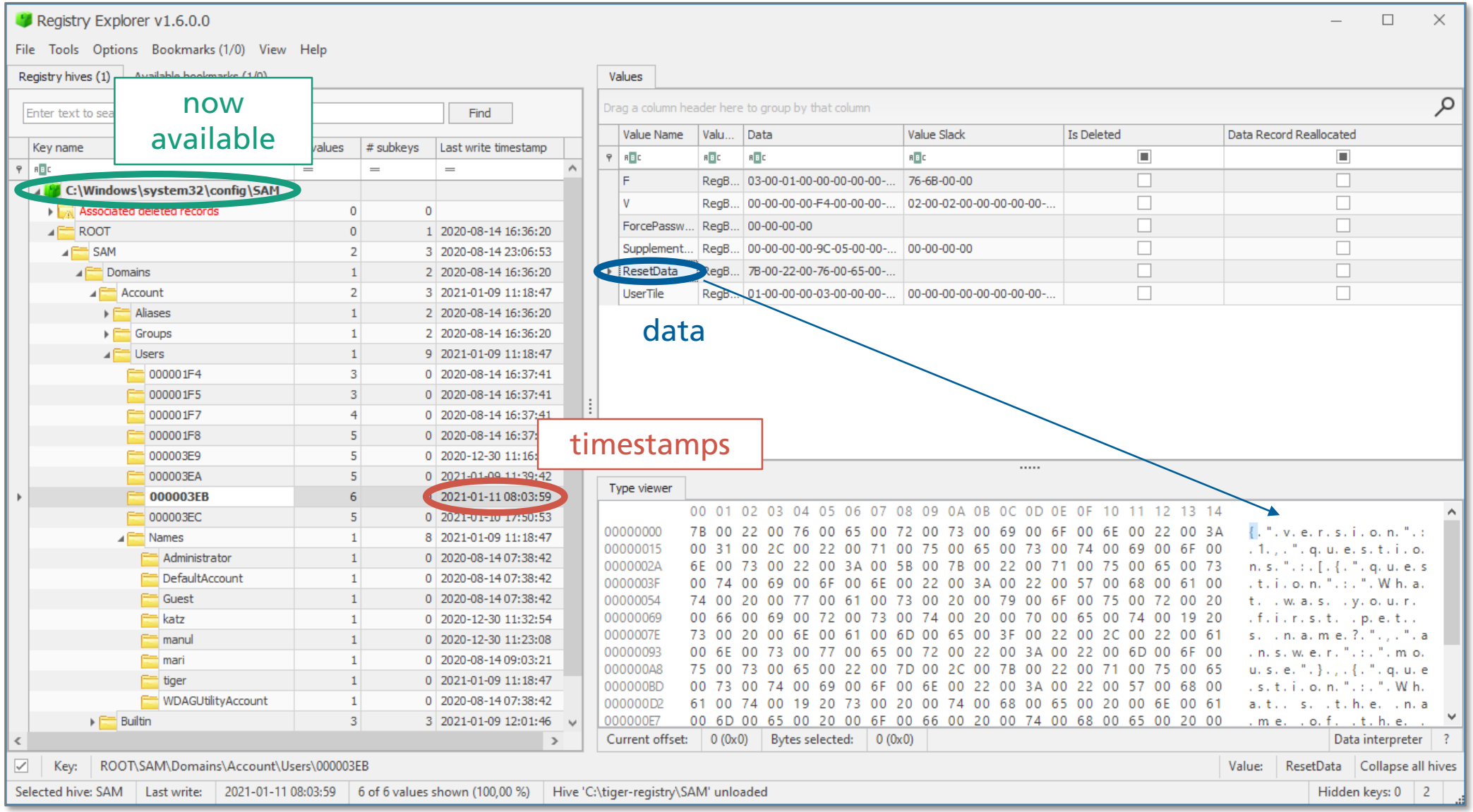
unavailable for the user

exists only on the running system

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Registry



How often did a user run an application?

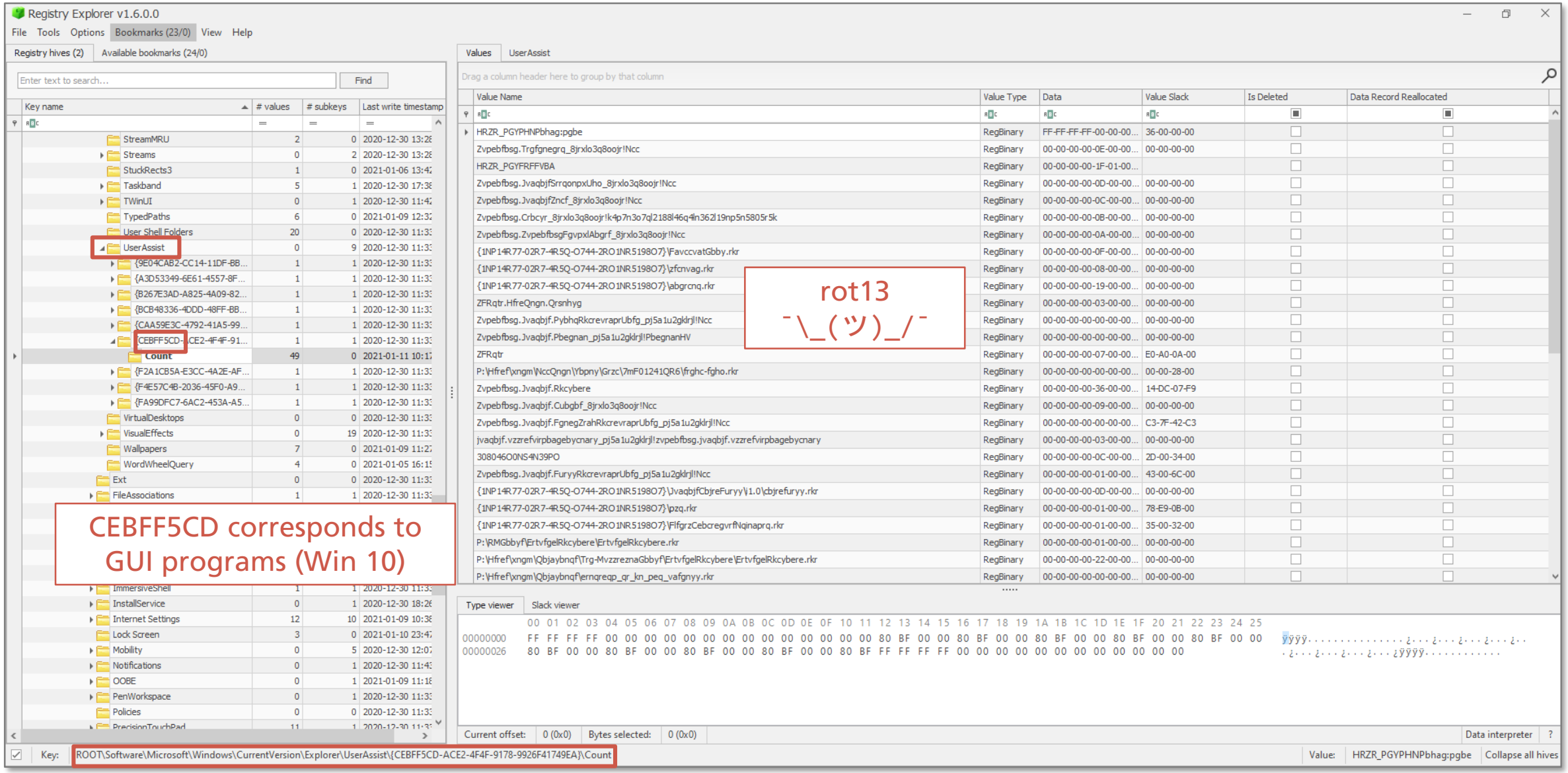
When was the last run?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Registry

NTUSER.DAT: UserAssist



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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 13:47
Taskband	5	1	2020-12-30 17:36
TWinUI	0	1	2020-12-30 11:42
TypedPaths	6	0	2021-01-09 12:32
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
{BCB48336-4DDD-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 10:17
{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 16:15
Ext	0	0	2020-12-30 11:33
FileAssociations	1	1	2020-12-30 11:33
FileHistory	0	1	2020-12-30 11:33
GameDVR	2	1	2021-01-08 05:55
Group Policy	0	2	2021-01-10 17:50
Holographic	1	2	2020-12-30 11:33
ime	0	1	2020-12-30 11:33
ImmersiveShell	1	1	2020-12-30 11:33
InstallService	0	1	2020-12-30 18:26
Internet Settings	12	10	2021-01-09 10:38
Lock Screen	3	0	2021-01-10 23:47
Mobility	0	5	2020-12-30 12:07
Notifications	0	1	2020-12-30 11:43
OOBE	0	1	2021-01-09 11:18
PenWorkspace	0	1	2020-12-30 11:33
Policies	0	0	2020-12-30 11:33
PrecisionTouchPad	11	1	2020-12-30 11:33

Values UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UEME_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
308046B0AF4A39CB	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 Export ?

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 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
```

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

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

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

What about recent files?

Hochschule Bonn-Rhein-Sieg

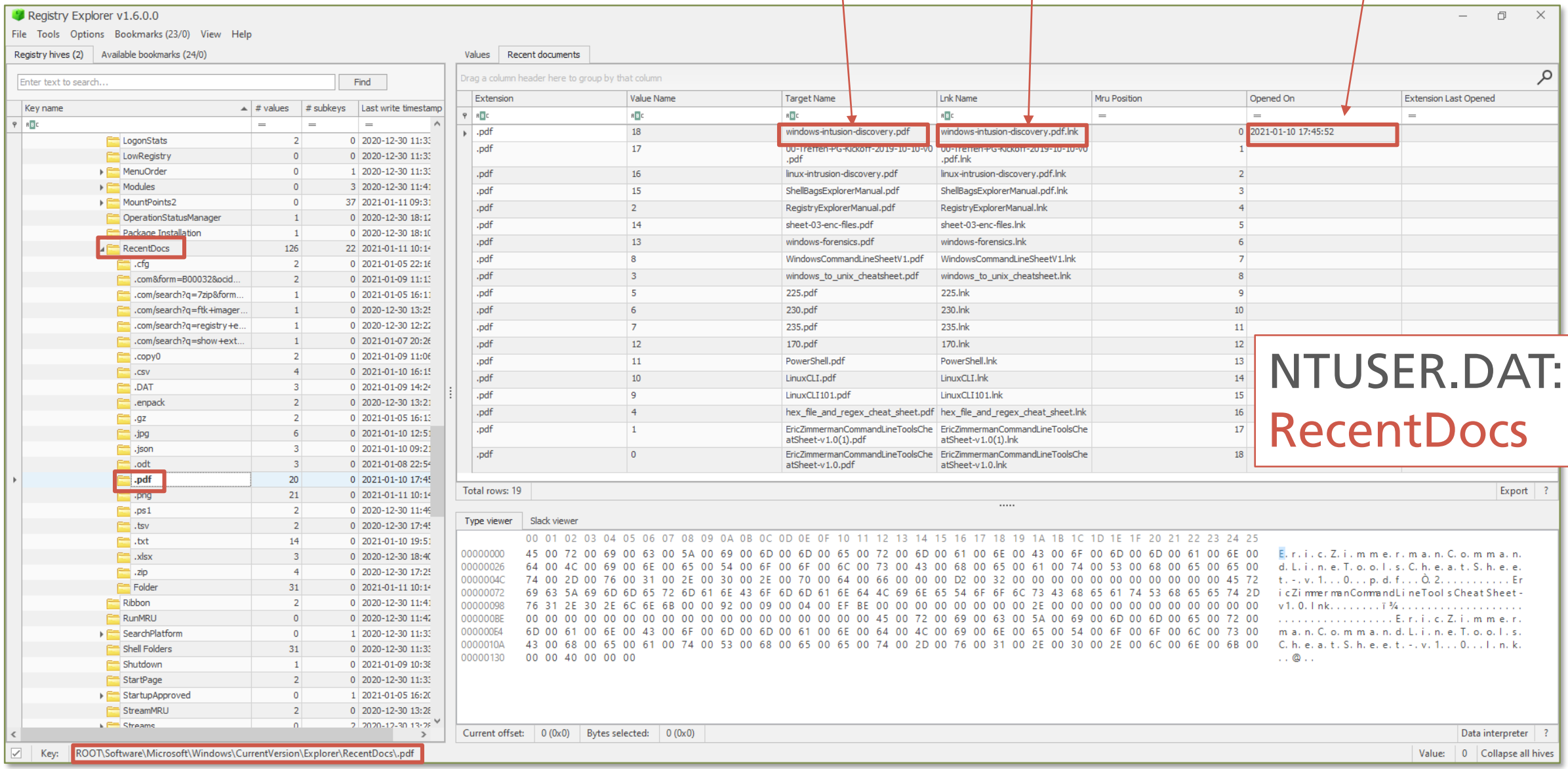
Fraunhofer FKIE

Registry

file name

corresponding lnk file

last open time of a file with .pdf extension



NTUSER.DAT:
RecentDocs

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Which USB devices were connected?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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	0	1	2020-08-14 16:36:15
DISPLAY	0	1	2020-08-14 16:36:20
HDAUDIO	0	1	2020-08-14 16:36:16
HID	0	1	2020-08-14 16:36:16
HTREE	0	1	2020-08-14 16:36:15
PCI	0	10	2020-12-30 17:57:46
ROOT	0	15	2020-08-14 16:36:16
SCSI	0	2	2020-08-14 16:36:16
STORAGE	0	1	2020-08-14 16:36:16
SWD	0	4	2020-12-30 18:11:22
USB	0	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
4C530000010905114024&0	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	13	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	

Values

Drag a column header here to group by that column

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

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\4C530000240824122435O Value: FriendlyName Collapse all hives

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Program execution evidence:

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

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Prefetch files

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

Directory: C:\Windows\Prefetch

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-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

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

size of what??? ʘ_ʘ

Run count. Obviously.

Timestamps of last eight runs

Serial number of the volume

directory where the executable lies

executable full path

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

```
~$ 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: 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
```

Possibly first exectution time (unreliable)

Last run time (more or less)

size of what??? ʘ_ʘ

Run count. Obviously.

Timestamps of last eight runs

Serial number of the volume

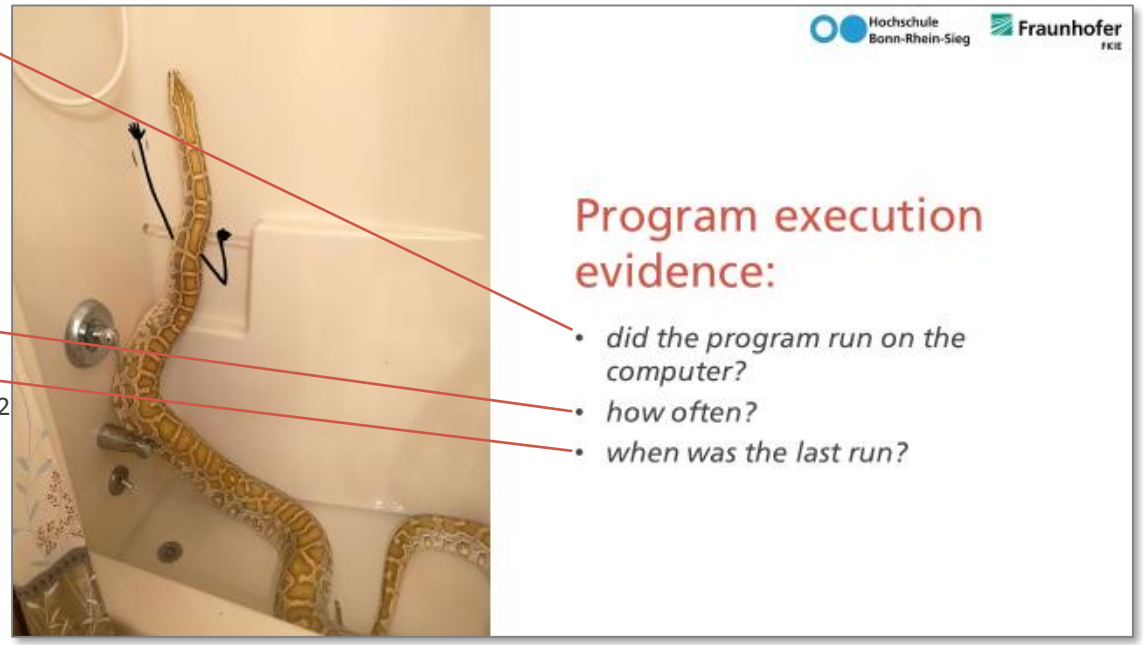
directory where the executable lies

executable full path

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

```
~$ 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
```



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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
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
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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
```

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
```

runs dlls as executables

it's complicated….

session manager

hosts service dlls

runs Windows tasks

manages Windows Updates

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Find evil (or suspicious at least)

```
~$ 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
MICROSOFTEDGEUPDATECOMREGISTE-3F0DDED1.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-066223
SHELLEXPERIENCEHOST.EXE-A3608B
SMSS.EXE-E9C28FC6.pf
SPPSVC.EXE-B0F8131B.pf
STARTMENUEXPERIENCEHOST.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-3CCF31E5.pf
```

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

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

`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*

Moar program execution evidence

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Amcache

Location:

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

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

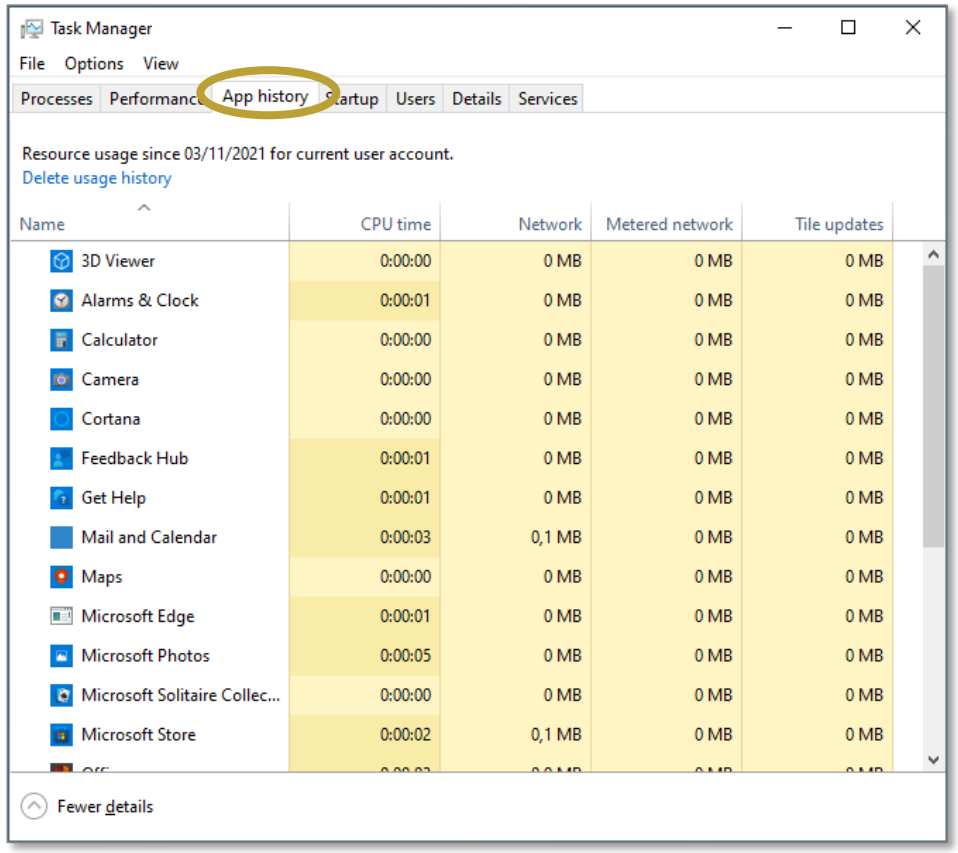
	B	C	D	E	F	G	H	I	J	K	L
1	ProgramId	FileKeyLastWriteTimestamp	SHA1	IsOsComponent	FullPath	Name	FileExtension	LinkDate	ProductName	Size	Version
2	00061153ea89f528c5a21853d7763d38c95800000904	25.11.2021 10:24	d1825c3e44b7bce02d41fc0e3e93fd87b2c5b9e9	False	c:\users\lynx\documents\programms\autoruns\autoruns.exe	Autoruns.exe	.exe	26.10.2021 18:41	sysinternals autoruns	2497400	
3	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:09	b4108c1d6832f0d036eedcd3d2f684d43be04996	True	c:\windows\system32\compattelrunner.exe	CompatTelRunner.exe	.exe			160072	10.0.19645.1029 (winbuild.16
4	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:09	11eba7b1e26cc7d492a2c161ac48370811d0b01e	True	c:\windows\system32\csrss.exe	csrss.exe	.exe			17600	10.0.19041.546 (winbuild.160
5	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:09	9914f5914c02add1d3590844a628b3c5a5fa2c48	True	c:\windows\system32\devicecensus.exe	DeviceCensus.exe	.exe			57672	10.0.19645.1029 (winbuild.16
6	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:09	70f820592c0f63d3f918c177284a426fef17ad6a	True	c:\windows\system32\drvinst.exe	drvinst.exe	.exe			350208	10.0.19041.928 (winbuild.160
7	00069ee783c5c9a352b570ff3481793a68510000ffff	25.11.2021 10:30	c3bc5b7df388924a8b655c0ca69db1e20481e441	False	c:\users\lynx\source\repos\eviltask\x64\release\eviltask.exe	EvilTask.exe	.exe	25.11.2021 10:30		11776	
8	0006781b32ae4b40eaac20eb9b0a3a4f5adb00000904	25.11.2021 09:09	1d7a8052eebfba8c395cf1d543c5a4e6fb57aca0	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgecomregistershellarm	MicrosoftEdgeComRegisterShellARM64.exe	.exe	19.02.2021 05:54	microsoft edge	163752	1.3.141.63
9	0006f9368d1ce8356b0711cefb486cce9e3d00000904	25.11.2021 09:09	1a6d250bb90113e323a7081f86cc7335b5ab400a	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgeupdateondemand.e	MicrosoftEdgeUpdateOnDemand.exe	.exe	19.02.2021 05:54	microsoft edge update	101288	1.3.141.63
10	0006f9368d1ce8356b0711cefb486cce9e3d00000904	25.11.2021 09:09	2454bbc252496eaee5de8594e2c016bf01707178	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgeupdatesetup.exe	MicrosoftEdgeUpdateSetup.exe	.exe	19.02.2021 05:55	microsoft edge update	1783720	1.3.141.63
11	0006f9368d1ce8356b0711cefb486cce9e3d00000904	25.11.2021 09:09	9f76ef75fb7b0e7cbf90b96be9490600f4b34ad6	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgeupdate.exe	MicrosoftEdgeUpdate.exe	.exe	19.02.2021 05:54	microsoft edge update	214952	1.3.141.63
12	0006f9368d1ce8356b0711cefb486cce9e3d00000904	25.11.2021 09:09	9204f1571532a61dc0f795c350dbb6591340076c	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgeupdatecore.exe	MicrosoftEdgeUpdateCore.exe	.exe	19.02.2021 05:54	microsoft edge update	242088	1.3.141.63
13	0006f9368d1ce8356b0711cefb486cce9e3d00000904	25.11.2021 09:09	50a14bbf37ad85a3c53b487dff1a7024a633e8e0	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgeupdatebroker.exe	MicrosoftEdgeUpdateBroker.exe	.exe	19.02.2021 05:54	microsoft edge update	101288	1.3.141.63
14	0006f9368d1ce8356b0711cefb486cce9e3d00000904	25.11.2021 09:09	9f76ef75fb7b0e7cbf90b96be9490600f4b34ad6	False	c:\program files (x86)\microsoft\edgeupdate\microsoftedgeupdate.exe	MicrosoftEdgeUpdate.exe	.exe	19.02.2021 05:54	microsoft edge update	214952	1.3.141.63
15	0006f9368d1ce8356b0711cefb486cce9e3d00000904	25.11.2021 09:09	9b2dee8860b22d27b8f81b33d71955cd13be17b8	False	c:\program files (x86)\microsoft\edgeupdate\1.3.141.63\microsoftedgeupdatecomregisters	MicrosoftEdgeUpdateComRegisterShell64.exe	.exe	19.02.2021 05:54	microsoft edge update	208296	1.3.141.63
16	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:09	7750ce7170635339d10aecd3aaefb0c3b589064a	True	c:\windows\system32\mousocoreworker.exe	MoUsoCoreWorker.exe	.exe			1538048	10.0.19041.906 (winbuild.160
17	0006aa3875f747b7ab583589050f11aeb59d00000904	25.11.2021 09:09	27f727fc554e7a4385116649920ce11f766473b4	False	c:\programdata\microsoft\windows defender\platform\4.18.2110.6-0\mpcmdrun.exe	MpCmdRun.exe	.exe	08.10.2011 19:17	microsoftÂ® windowsÂ® operating system	901056	4.18.2110.6 (winbuild.160101
18	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:09	5d6102f5a170e982c7735bfc2b9c1a0a0d435fd1	True	c:\windows\system32\msiexec.exe	msiexec.exe	.exe			69632	5.0.19041.1 (winbuild.160101
19	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:09	85536ad6afee43b728ed12ee8cffca41f74f6446	True	c:\program files\windows defender\msmpeng.exe	MsMpEng.exe	.exe	18.01.1993 16:54	microsoftÂ® windowsÂ® operating system	103384	4.18.1909.6 (winbuild.160101
20	0006aa3875f747b7ab583589050f11aeb59d00000904	25.11.2021 09:09	ce74a47c0959491bab22115677f4c8b27e6ce4e3	False	c:\programdata\microsoft\windows defender\platform\4.18.2110.6-0\msmpeng.exe	MsMpEng.exe	.exe	05.11.2062 16:43	microsoftÂ® windowsÂ® operating system	128376	4.18.2110.6 (winbuild.160101
21	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:09	9aae97e24c5c483e876ddf2534036cec405594d2	True	c:\windows\system32\musnotification.exe	MusNotification.exe	.exe			689664	10.0.19041.906 (winbuild.160
22	0006aa3875f747b7ab583589050f11aeb59d00000904	25.11.2021 09:09	ea9414358c2a2cdcd6f4d0bdb7fb08db3fab069c	False	c:\programdata\microsoft\windows defender\platform\4.18.2110.6-0\nissrv.exe	NisSrv.exe	.exe	24.05.1975 10:53	microsoftÂ® windowsÂ® operating system	2872024	4.18.2110.6 (winbuild.160101
23	0006df8f19fbe059c89330971e8f66fe2c3500000904	25.11.2021 09:09	93bef70fea94857b9880238d32a4a80ff1547e26	False	c:\users\lynx\appdata\local\microsoft\onedrive\onedrive.exe	OneDrive.exe	.exe	15.02.1976 08:12	microsoft onedrive	2542440	2.122.
24	000651ddd855a3a377594406e2f75418870400000904	25.11.2021 09:09	aeb72a0af9e5533505c4edc9c91d09a8a17d3bb1	False	c:\users\lynx\appdata\local\microsoft\onedrive\update\onedrivesetup.exe	OneDriveSetup.exe	.exe	25.06.2021 12:12	microsoft onedrive	48701312	2.122.
25	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:09	ce8669d8826c8795115d58c62e726ae53943dce9	True	c:\windows\syswow64\onedrivesetup.exe	OneDriveSetup.exe	.exe			30870320	1.904.
26	000651ddd855a3a377594406e2f75418870400000904	25.11.2021 09:09	afb1026d608ad08d7351abd2cb62efc9dfb988f7	False	c:\users\lynx\appdata\local\microsoft\onedrive\onedrivestandaloneupdater.exe	OneDriveStandaloneUpdater.exe	.exe	23.03.1970 14:01	microsoft onedrive	4072312	2.122.
27	00063b8a1b9bb575663585011ecd5b422fcb00000904	25.11.2021 09:50	efeee983af571f5e3e519935ec385225274d05e2	False	c:\users\lynx\documents\programms\processexplorer\procexp.exe	procexp.exe	.exe	17.08.2021 02:07	process explorer	2839416	16.43
28	0006e51efa8a67107b82dceef4f3f8e4f40c00000000	25.11.2021 10:57	a5606c758769487c4384d11ccb785dfff73704aa	False	c:\users\lynx\documents\programms\registryexplorer\registryexplorer.exe	RegistryExplorer.exe	.exe	08.10.2021 17:25	registry explorer	62116088	1.6.0.0
29	0006801205036c9b4f690f3cdd88cc9b030d00000904	25.11.2021 09:15	c52fcb2bcc2030d73cf54c559361496c3a6c9ef3	False	c:\users\lynx\appdata\local\temp\7zs02cd58f3\setup-stub.exe	setup-stub.exe	.exe	24.07.2021 22:21	firefox	477616	94.0.2
30	0006d56c1dcd3153db5c1699d5a0ed954fae00000904	25.11.2021 09:26	b4d0496b3de4bcced1dd0f3df87501cccb36c7cb	False	c:\program files (x86)\microsoft\edgeupdate\install\{dec39d2f-dcb8-474a-bdae-ab876e208	setup.exe	.exe	22.11.2021 23:56	microsoft edge installer	2873744	96.0.1054.34
31	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:05	0897b4076ec223a6f3c27d78197a615f05d0ad52	True	c:\windows\system32\sihclient.exe	sihclient.exe	.exe	12.01.2101 10:52	microsoftÂ® windowsÂ® operating system	394144	10.0.19041.1288 (winbuild.16
32	0006d4f2d8fa5466a9e19ee5933940484d6f0000ffff	26.11.2021 17:28	e5f22d92cb8e2cd0d0616c4a5ea66d97c0d4b096	False	c:\users\lynx\downloads\suspicious-binary.exe	suspicious-binary.exe	.exe	25.11.2021 10:32		11776	
33	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:09	010db07461e45b41c886192df6fd425ba8d42d82	True	c:\windows\system32\svchost.exe	svchost.exe	.exe			57360	10.0.19041.546 (winbuild.160
34	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:11	fed4b4a753a9541389aa670c69e624be07569ccd	False	c:\windows\system32\taskhostw.exe	taskhostw.exe	.exe	21.06.2081 11:10	microsoftÂ® windowsÂ® operating system	97096	10.0.19041.906 (winbuild.160
35	00069332262a4d4355f8a5e015d3090d8bd200000904	03.11.2021 15:13	8ce2b2054af5303c413a4ecfa21227f9851834c1	False	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.190	TiWorker.exe	.exe	20.11.2018 17:35	microsoftÂ® windowsÂ® operating system	281936	10.0.19041.1310 (winbuild.16
36	00061cebfb8bbaab60f7f0a7f3253e278cc100000904	25.11.2021 09:09	d912efb63512d656f167b2e34d5f4c2654293647	False	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.190	TiWorker.exe	.exe			239416	10.0.19041.925 (winbuild.160
37	00067856a2d414db677597d05fa23e79f7e900000904	03.11.2021 14:51	e3e0f810ef3e0a36c13c97eee8246784fb7cbfca	False	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.190	TiWorker.exe	.exe	13.07.2099 10:15	microsoftÂ® windowsÂ® operating system	281928	10.0.19041.1220 (winbuild.16
38	00069d457203cf8d4798b6ee2443aee7e9080000ffff	26.11.2021 11:12	95fe5ae298fd9c5df796e3955d6ba84a70fdabdc	False	c:\users\lynx\downloads\very-suspicious-binary.exe	very-suspicious-binary.exe	.exe	22.11.2021 13:36		63488	
39	00062a25971c1e41ee8f9ccacb8e83d2ecfa00000000	25.11.2021 09:54	ff73b88904ed09c1bcf59cfaeabf81e96fafe264	False	c:\users\lynx\appdata\local\temp\b6bc2d481404a27bc128cf20954744\vs_bootstrapper_d15	vs_setup_bootstrapper.exe	.exe	19.05.2087 07:44	visual studio	301952	2.11.52.58712
40	0000f519feec486de87ed73cb92d3cac802400000000	26.11.2021 09:13	dd5f35048d912997edb108f80c9d2ce47e3b684a	True	c:\windows\system32\werfault.exe	WerFault.exe	.exe	26.07.2039 22:39	microsoftÂ® windowsÂ® operating system	568632	10.0.19041.1081 (winbuild.16
41	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:09	7b2e3990de386df08a049ecb611bc9ab17c1497c	True	c:\windows\system32\winlogon.exe	winlogon.exe	.exe	02.11.1995 04:19	microsoftÂ® windowsÂ® operating system	944640	10.0.19041.1266 (winbuild.16
42	0000f519feec486de87ed73cb92d3cac802400000000	25.11.2021 09:09	3f5c88006e75e1fbbd8de658d1d66aeac432de75	True	c:\windows\system32\wuauclt.exe	wuauclt.exe	.exe			64008	10.0.19041.906 (winbuild.160

```
Program name        suspicious-binary.exe
Full path           c:\users\lynx\downloads\suspicious-binary.exe
SHA1 base 16        e5f22d92cb8e2cd0d0616c4a5ea66d97c0d4b096
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SRUM: system resource usage monitor



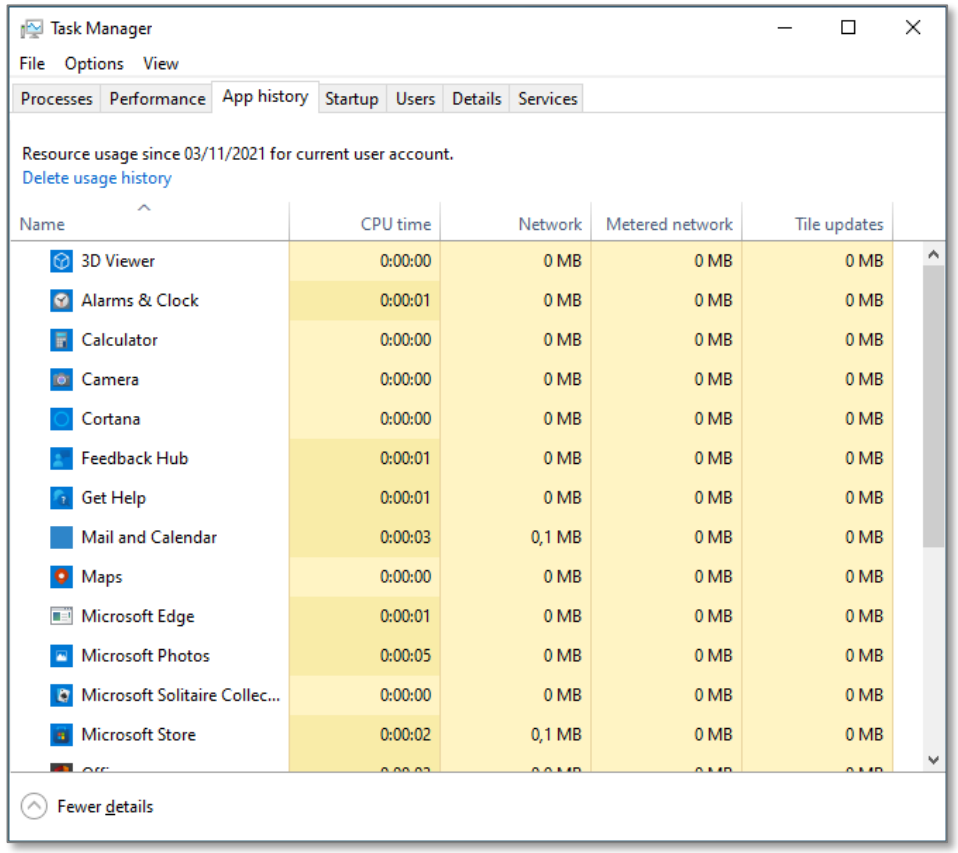
SRUM is a feature in modern Windows systems which collect statistics on execution of binaries. The information is stored in an Extensible Storage Engine (ESE) database. ESE is Microsoft's proprietary single file database format, acting similarly to SQLite, as a default storage engine for many applications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

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

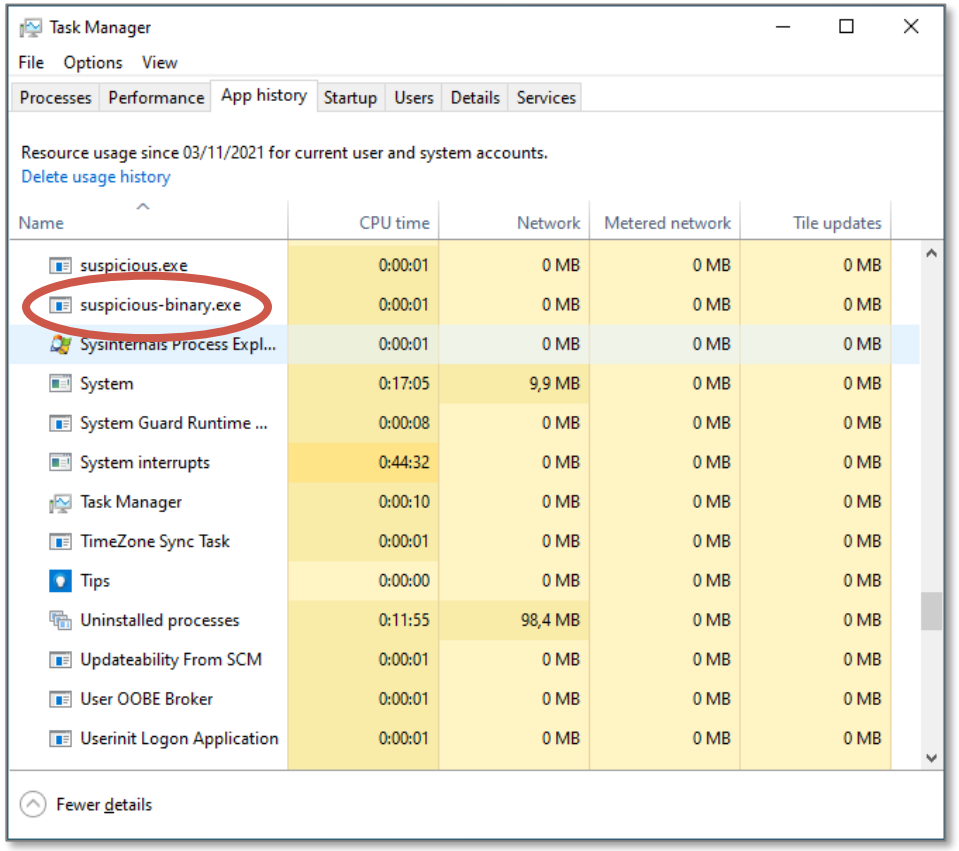
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SRUM: system resource usage monitor



View -> Show history for all Processes



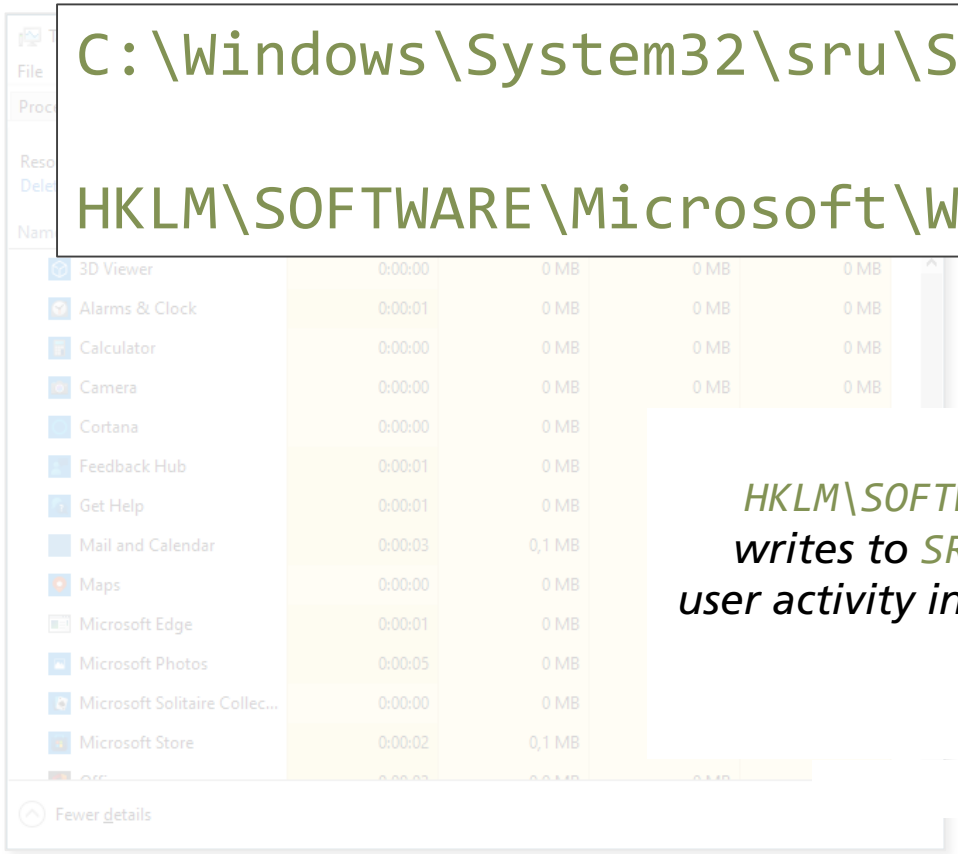
Hochschule Bonn-Rhein-Sieg

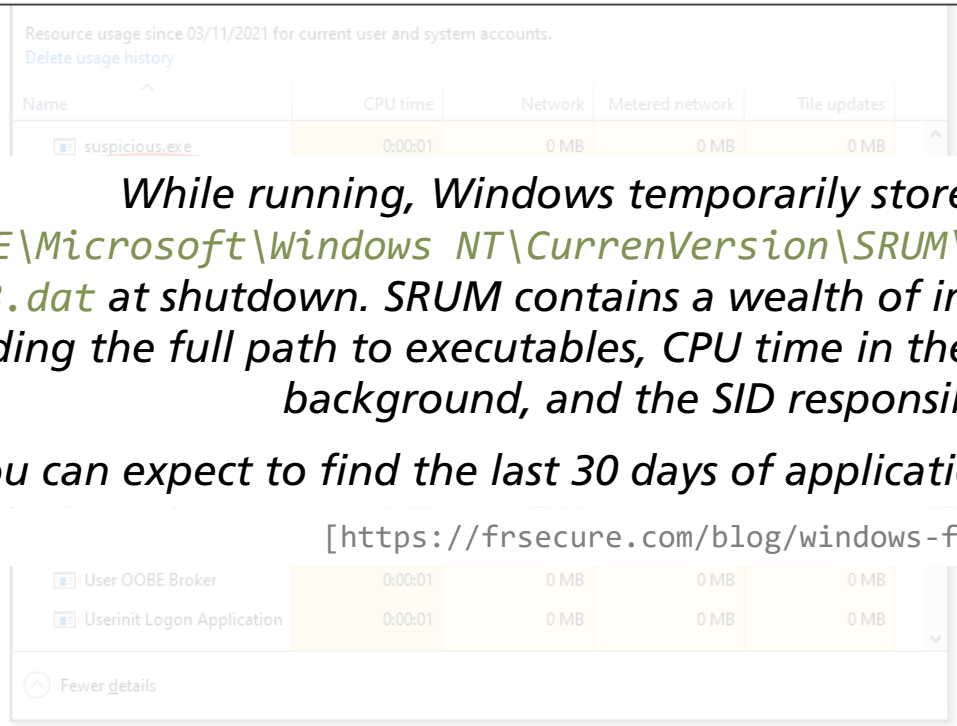
Fraunhofer FKIE

SRUM: system resource usage monitor

Location:

```
C:\Windows\System32\sru\SRUDB.dat – ESE DB

HKLM\SOFTWARE\Microsoft\Windows NT\CurrenVersion\SRUM\Extensions
```





While running, Windows temporarily stores this data in the `HKLM\SOFTWARE\Microsoft\Windows NT\CurrenVersion\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/]

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SRUM: system resource usage monitor

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

	Id	Timestamp	ExeInfo	ExeInfoDescription	ExeTimestamp	SidType	Sid	UserName	UserId	AppId	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

Prefetch files

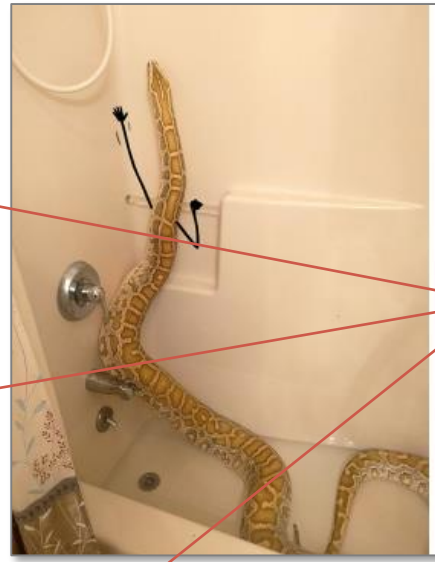
```
~$ ls -Filter *.pf C:\Windows\Prefetch
Directory: C:\Windows\Prefetch

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/26/2021  10:54 AM           2078 AM_DELTA_PATCH_1.353.1553.0.E-056CC28D.pf
-a----        11/26/2021  12:52 PM          14181 APPLICATIONFRAMEHOST.EXE-CCEEF759.pf
-a----        11/26/2021  11:15 AM          10901 ATBROKER.EXE-2E15A492.pf
-a----        11/26/2021  12:51 PM           5715 AUDIODG.EXE-BDFD3029.pf
-a----        11/25/2021  11:19 AM          56450 AUTORUNS.EXE-FEE25E8A.pf
-a----        11/26/2021  12:18 PM          11903 BACKGROUNDTASKHOST.EXE-AB9D538B.pf
-a----        11/26/2021  10:21 AM          13483 BACKGROUNDTRANSFERHOST.EXE-4FEEC2B3.pf
-a----        11/25/2021  11:05 AM           8174 BYTECODEGENERATOR.EXE-C1E98CE6.pf
-a----        11/26/2021  11:01 AM           2841 CMD.EXE-4A815364.pf
-a----        11/25/2021  11:52 AM           2250 CMD.EXE-AC115AAB.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  12:51 PM          27798 CONSENT.EXE-531BD9EA.pf
-a----        11/26/2021  10:57 AM          12488 CONTROL.EXE-817F8F1D.pf
-a----        11/26/2021  12:51 PM           5429 CSRSS.EXE-3FE41F7E.pf
-a----        11/26/2021  10:53 AM           7763 CTFMON.EXE-9450B46B.pf
-a----        11/25/2021  11:28 AM          46191 DEVENV.EXE-B644FD26.pf
-a----        11/26/2021  12:40 PM          10022 DLLHOST.EXE-28AB211F.pf
-a----        11/26/2021  12:51 PM           4813 DLLHOST.EXE-504C779A.pf
-a----        11/26/2021   4:27 AM           4869 DLLHOST.EXE-57020BE5.pf
-a----        11/26/2021  12:46 PM           3641 DLLHOST.EXE-5E46FABD.pf
-a----        11/26/2021  10:49 AM          10255 DLLHOST.EXE-6FCDC72B.pf
-a----        11/26/2021   9:40 AM           6360 DLLHOST.EXE-CA6980A0.pf
-a----        11/26/2021   9:57 AM          11397 DLLHOST.EXE-D22EE8A8.pf
-a----        11/26/2021  10:24 AM          12819 DLLHOST.EXE-D46AA2AE.pf
```

application name

hash

Location:

`C:\Windows\Prefetch\`



Program execution evidence:

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

Amcache

Location:

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

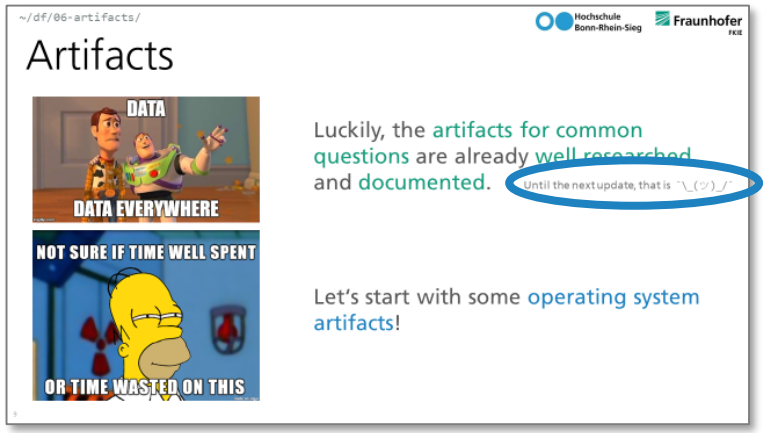
```
~$ AmcacheParser.exe -i -f C:\Windows\appcompat\Programs\Amcache.hve --csv Z:\amcache\amcahce.csv
```

Program name	suspicious-binary.exe
Full path	c:\users\lynx\downloads\suspicious-binary.exe
SHA1 base 16	e5f22d92cb8e2cd0d0616c4a5ea66d97c0d4b096

SRUM: system resource usage monitor

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

Program name	suspicious-binary.exe
User	lynx
SSID	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



Speaking about Windows updates…

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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.

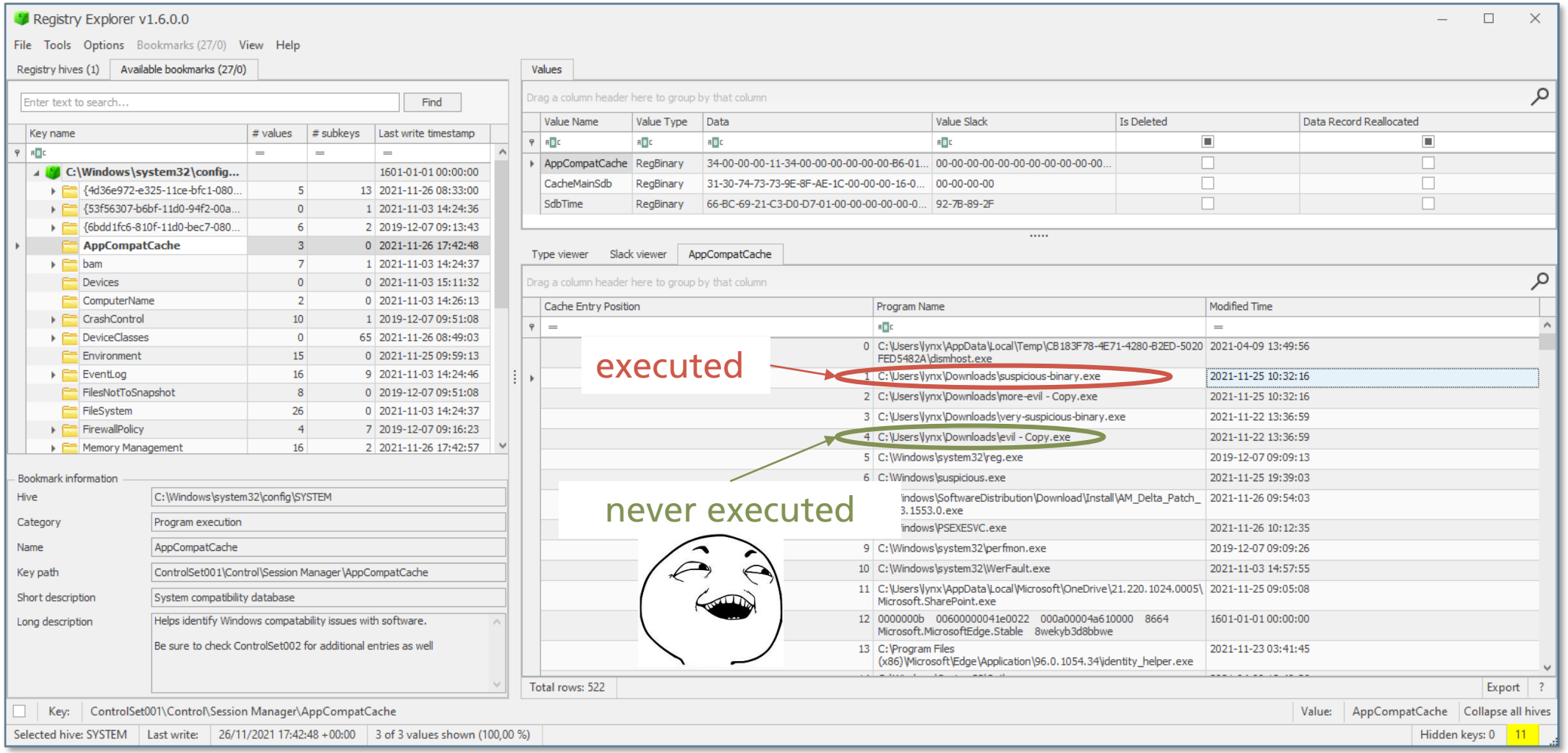
System compatibility database
Helps identify Windows compatibility issues with software.

© Registry Explorer

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Shimcache



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.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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

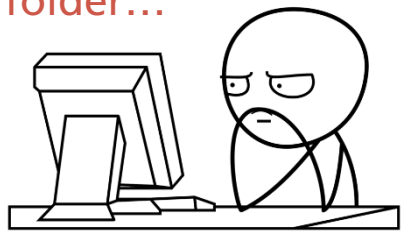
Key name	# values	# subkeys	Last write timestamp
Ext	0	0	2020-12-30 11:33:37
FileAssociations	1	1	2020-12-30 11:33:34
FileHistory	0	1	2020-12-30 11:33:31
GameDVR	2	1	2021-01-08 05:55:07
Group Policy	0	2	2021-01-11 13:55:46
Holographic	1	2	2020-12-30 11:33:53
ime	0	1	2020-12-30 11:33:31
ImmersiveShell	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

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

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-00-6B-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

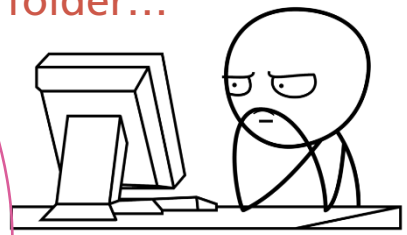
Key name	# values	# subkeys	Last write timestamp
Ext	0	0	2020-12-30 11:33:37
FileAssociations	1	1	2020-12-30 11:33:34
FileHistory	0	1	2020-12-30 11:33:31
GameDVR	2	1	2021-01-08 05:55:07
Group Policy	0	2	2021-01-11 13:55:46
Holographic	1	2	2020-12-30 11:33:53
ime	0	1	2020-12-30 11:33:31
ImmersiveShell	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

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

suspicious executable from `Downloads` folder...



~/df/06-artifacts/windows/registry/

Are there any traces of *malware persistence*?

Raw value: 43-00-3A-00-5C-00-55-00-73-00-65-00-72-00-73-00-5C-00-6B-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

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

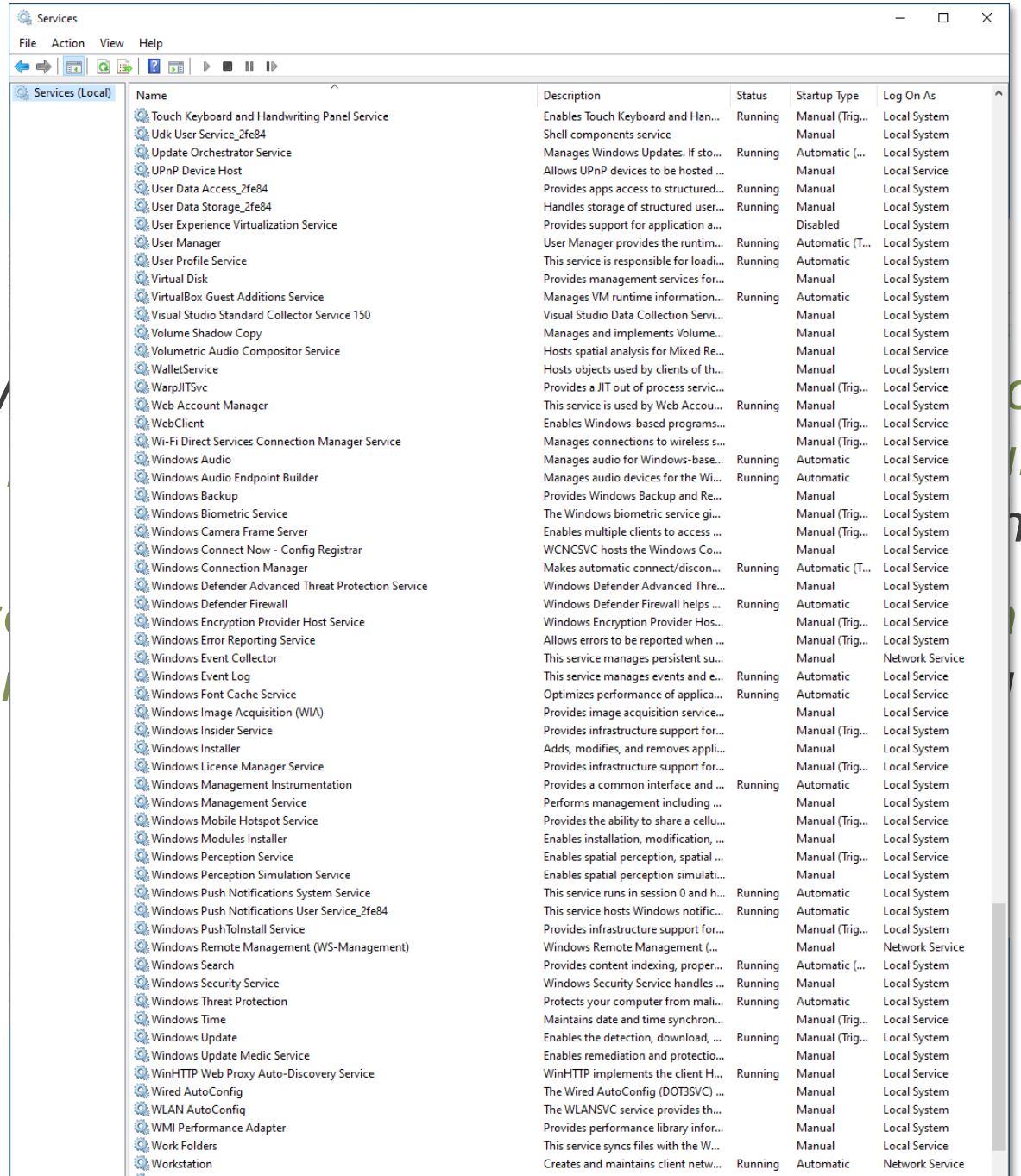
…looking for rogue services on the system…

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



In W
computer

Windows s
system is sta

ows service is a
nd. It is similar
ix daemon[…]

the operating
as Windows is
running[…]

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

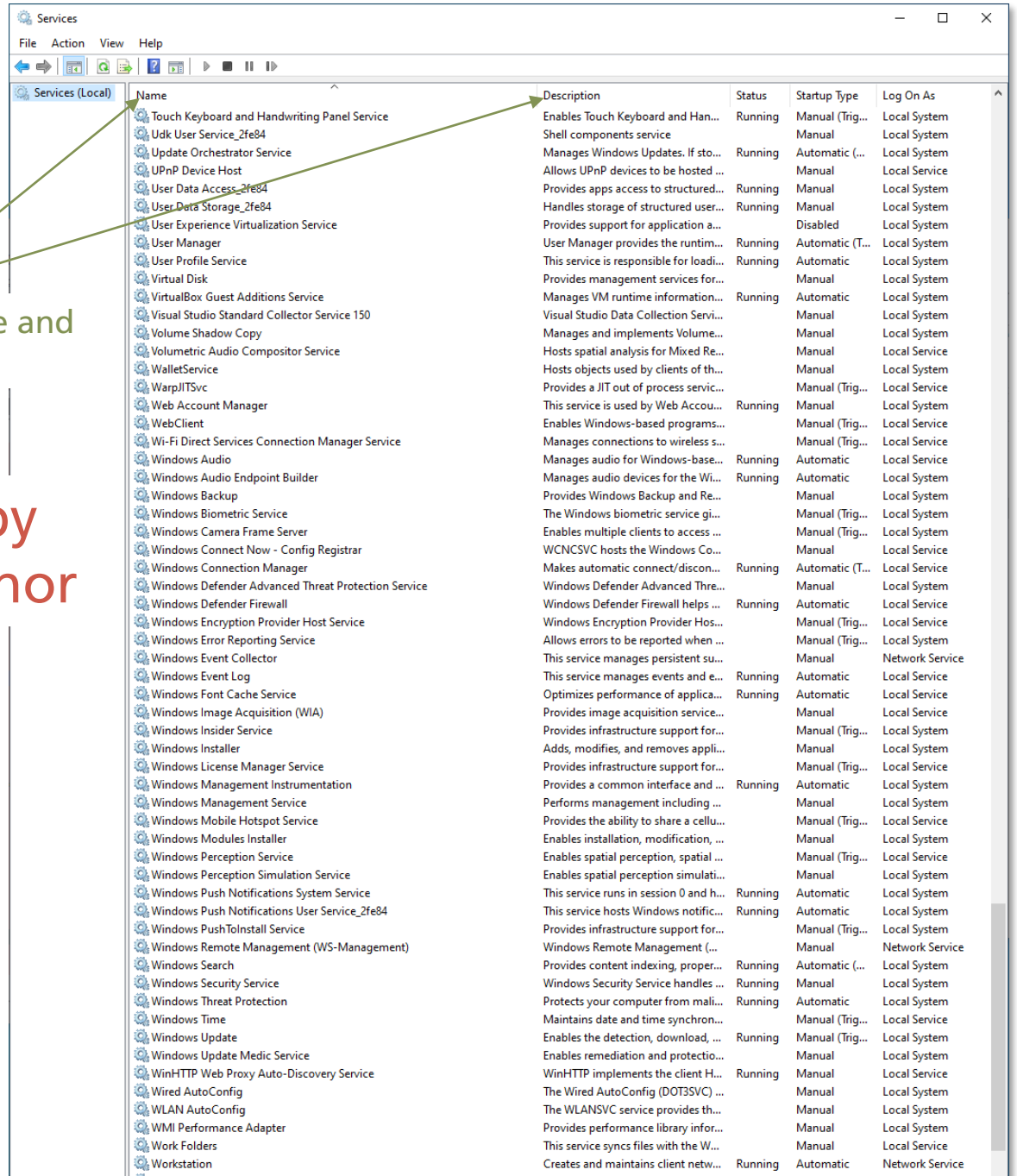
Services

User-friendly name and description

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Services



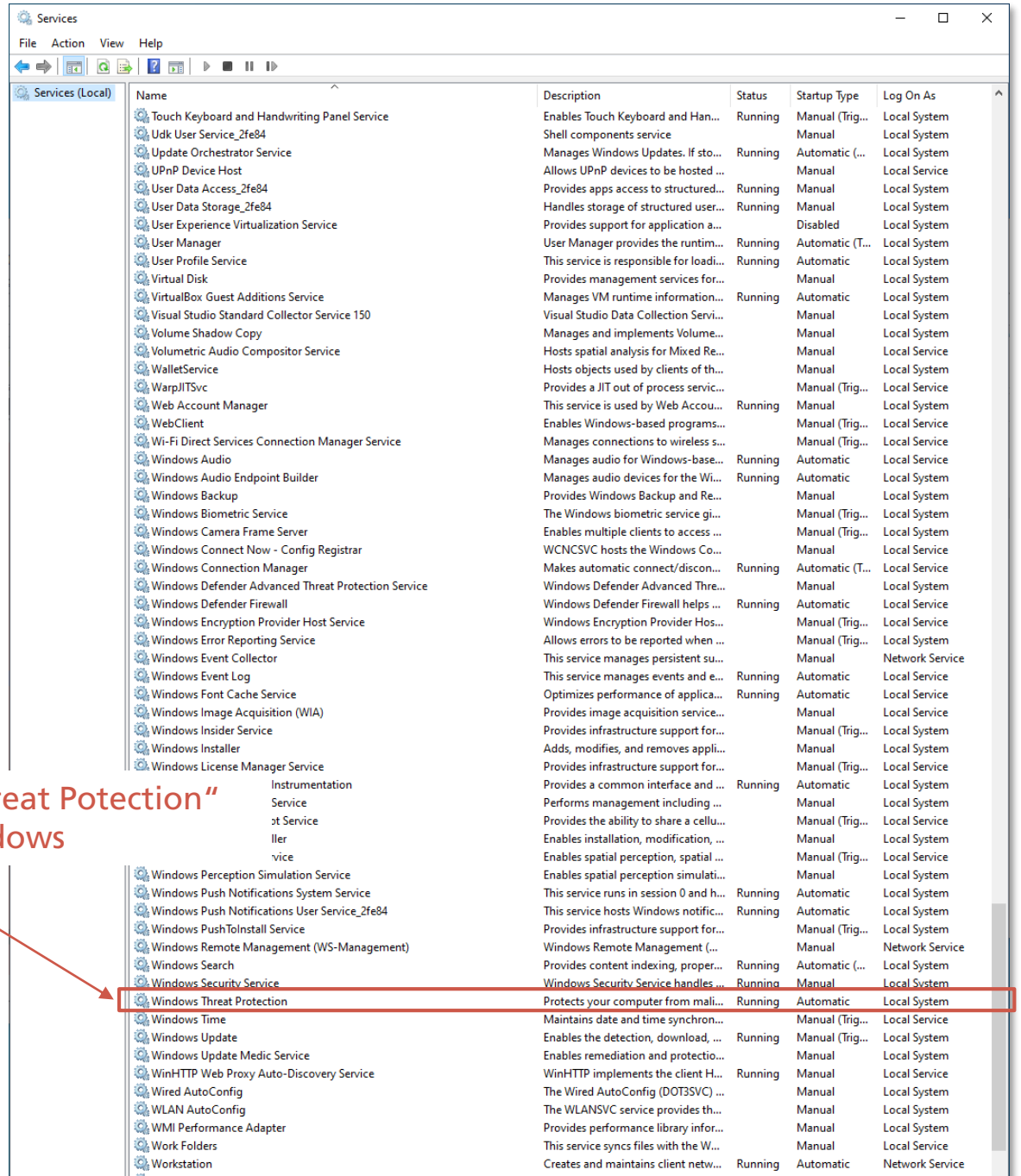
User-friendly name and description

Defined by service author

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Services

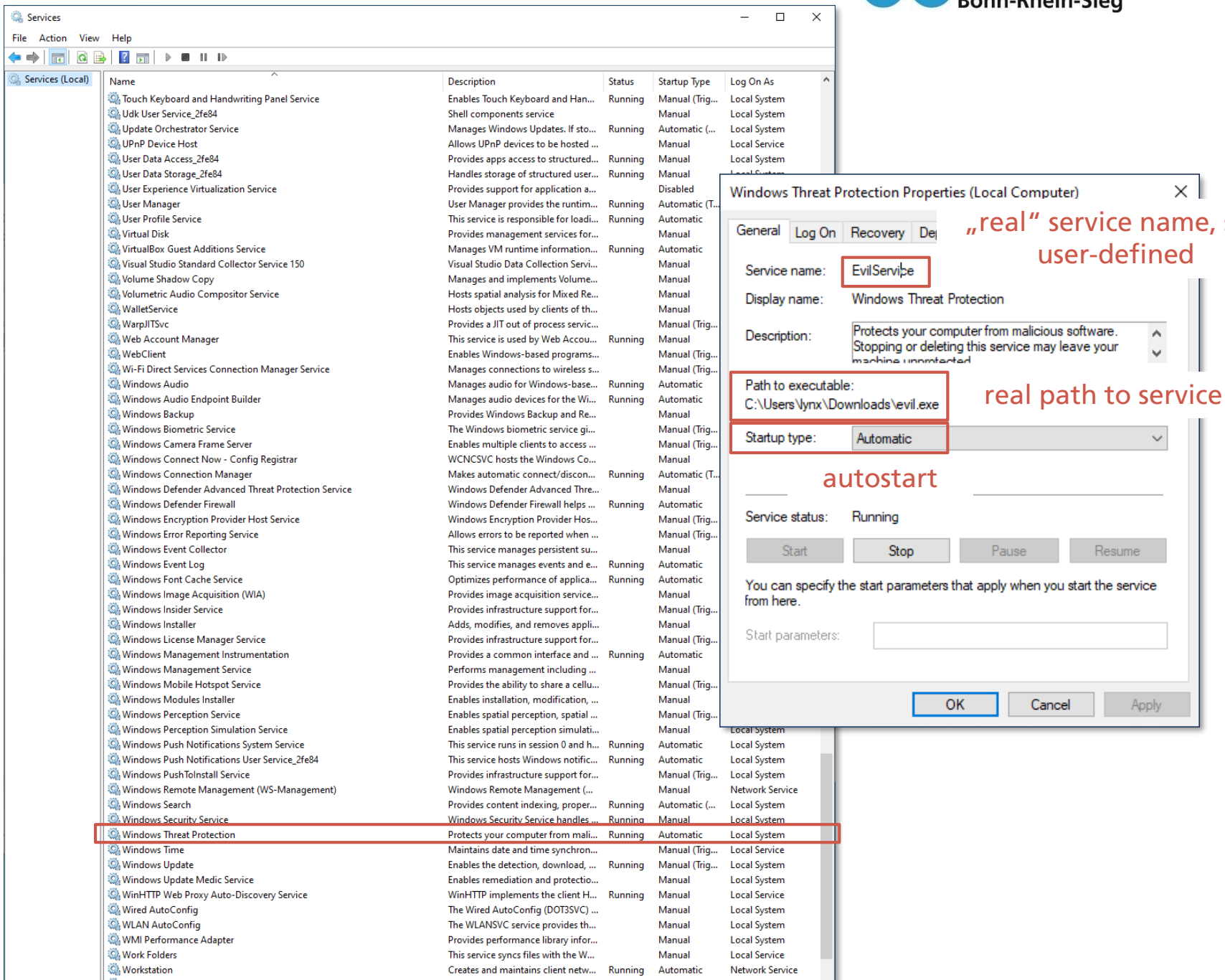


There is no „Windows Threat Potection“ service on Windows

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Services



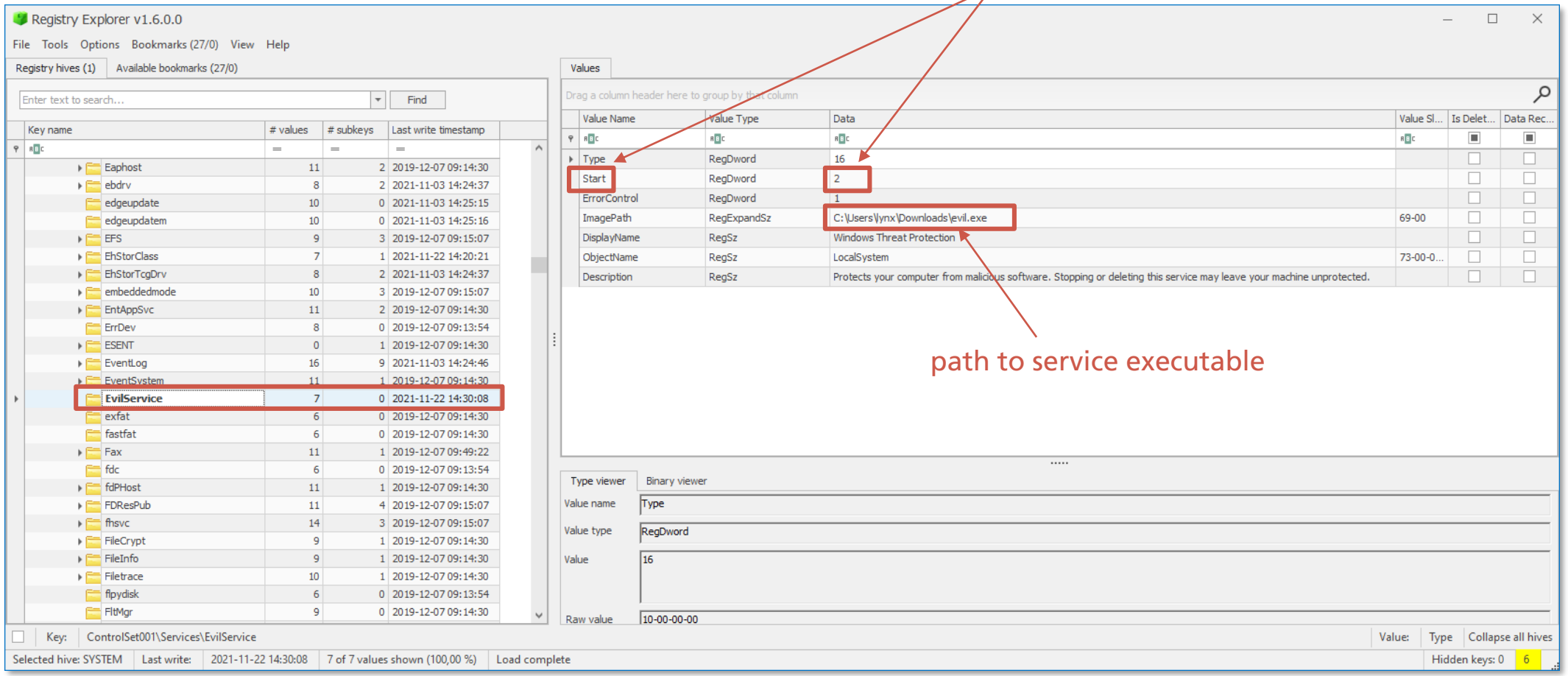
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Services

Location:

`SYSTEM\ControlSet001\Services`



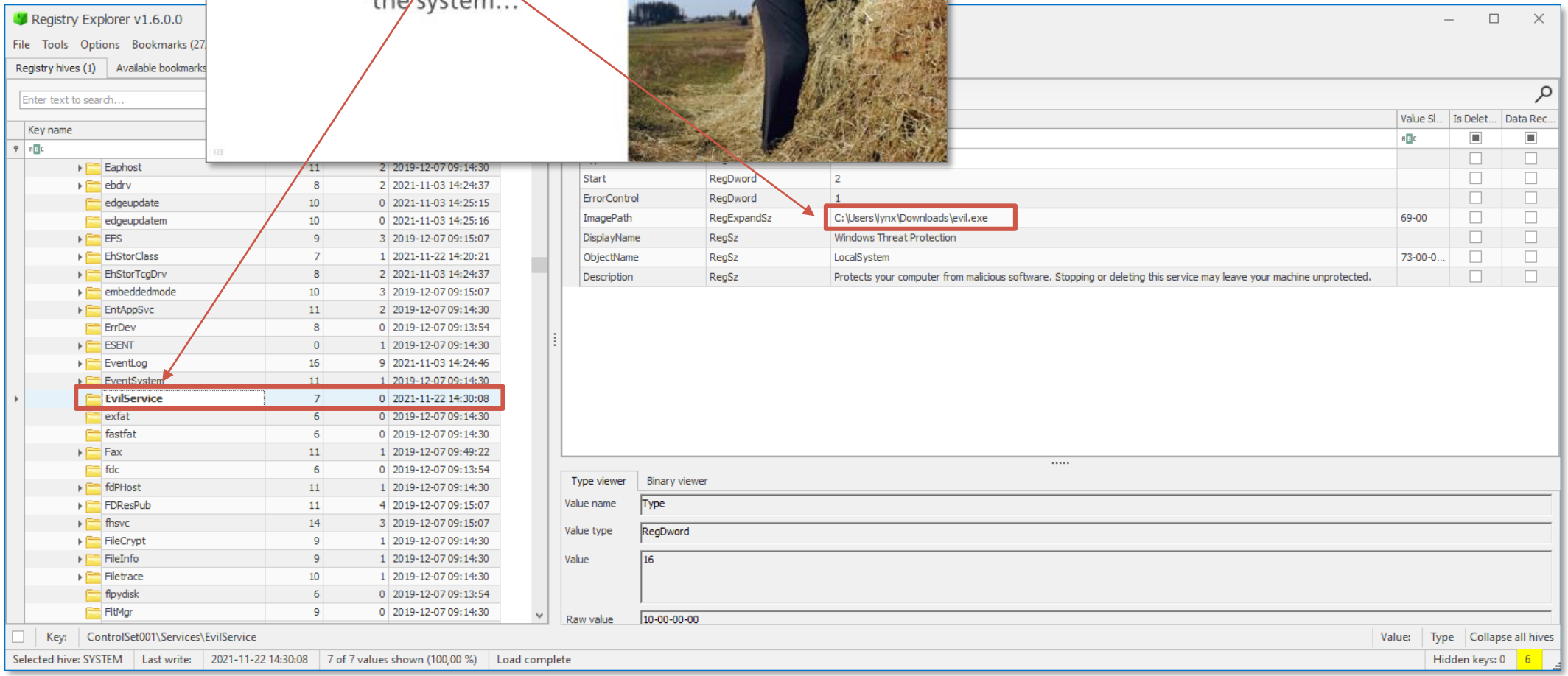
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Services

Location:

`SYSTEM\ControlSet001`

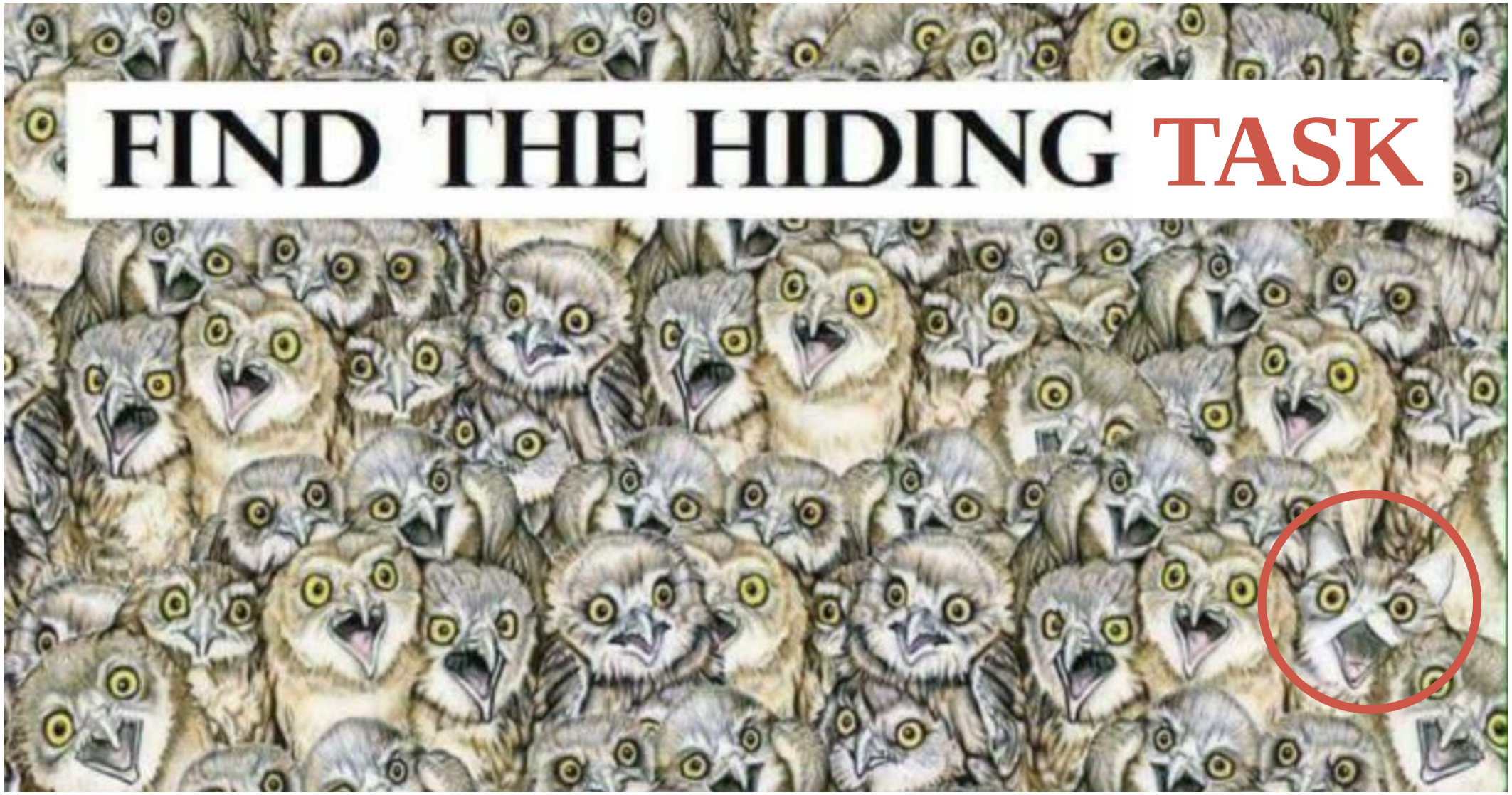


Services

Location:

`SYSTEM\ControlSet001`

Correlate with program execution evidence!


FIND THE HIDING TASK

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Active tasks are tasks that are currently enab

Name

Trigger defines when to do task

Path to the task relative to tasks location

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\LanguageComponentsInstaller
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\UpdateOrchestrator
UpdateUserPictureTask		Custom Trigger	\Microsoft\Windows\Shell
UsageDataFlushing		Multiple triggers defined	\Microsoft\Windows\Flighting\FeatureConfig
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

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\LanguageComponentsInstaller
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: 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 >:)

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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
RecommendedTroubleshootingSc...		Multiple triggers defined	\Microsoft\Windows
ReconcileFeatures		Multiple triggers defined	\Microsoft\Windows
ReconcileLanguageResources		At log on of any user - A...	\Microsoft\Windows
RegisterDeviceAccountChange		Multiple triggers defined	\Microsoft\Windows
RegisterDevicePolicyChange		Multiple triggers defined	\Microsoft\Windows
RegisterDeviceProtectionStateCha...		Custom Trigger	\Microsoft\Windows
RegisterDeviceSettingChange		Multiple triggers defined	\Microsoft\Windows
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)

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 >:)

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Scheduled tasks

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

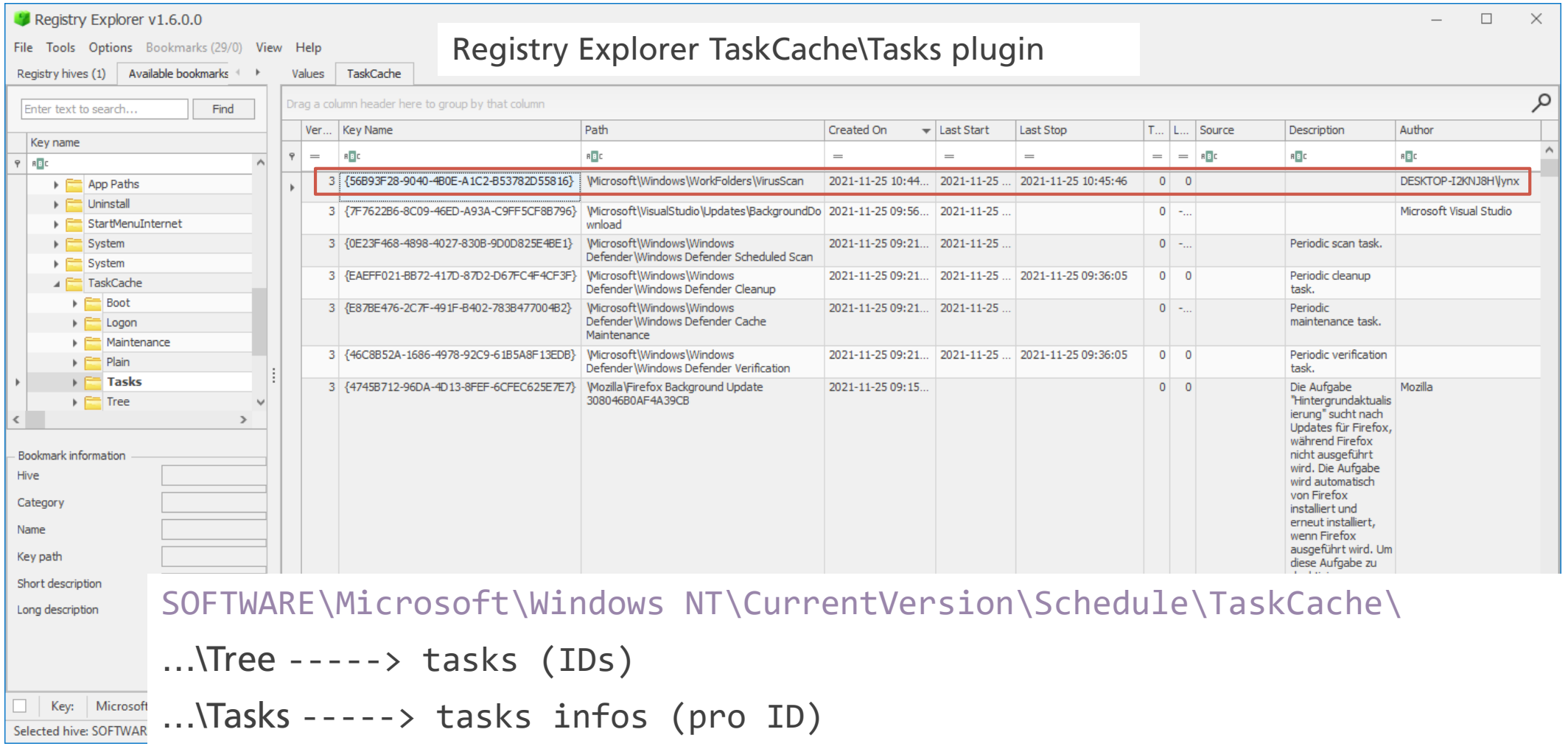
```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2021-11-25T11:44:37</Date>
    <Author>DESKTOP-I2KNJ8H\lynx</Author>
    <URI>\Microsoft\Windows\WorkFolders\VirusScan</URI>
  </RegistrationInfo>
  <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



`SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\`

`...\Tree -----> tasks (IDs)`

`...\Tasks -----> tasks infos (pro ID)`

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

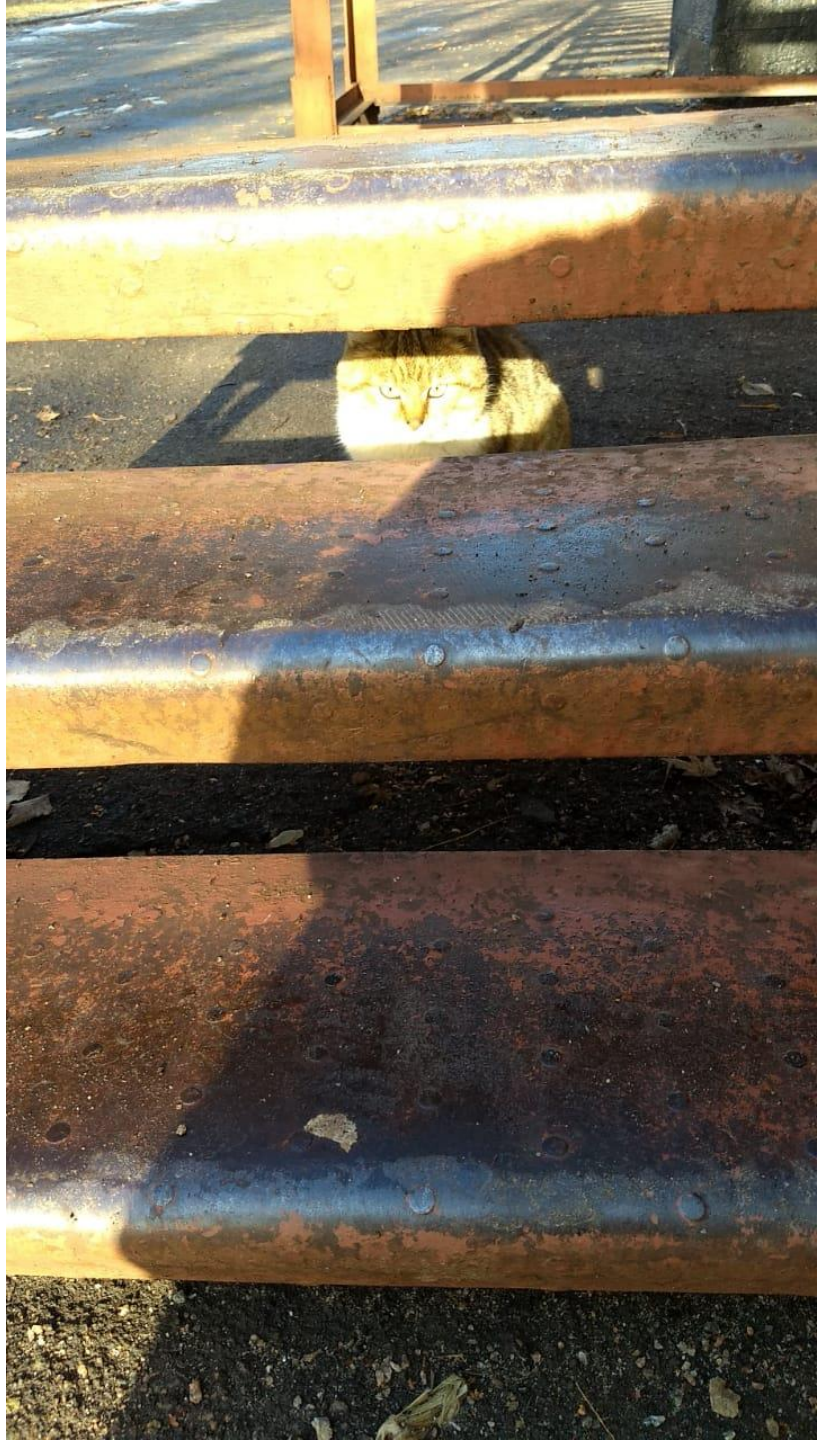
Scheduled tasks

```
~$ 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>2021-11-25T11:44:37</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?



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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>
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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:

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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 ex
0xC000006A	user name is correct b
0XC000006D	This is either due to a
0XC000006E	Information Unknown user name o
0xC000006F	user tried to logon outs restrictions
0xC0000070	workstation restriction violation (look for event
0xC0000071	expired password
0xC0000072	account is currently dis
0XC00000DC	Indicates the Sam Ser the desired operation.
0xC0000133	
0xc000015b	
0XC000018C	
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:

~$ cat failed-login-ez-evtx-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
}
```


Network logon.

Substatus as text.

Remote host infos.

Event ID meaning.

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

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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

~$ cat failed-login-ez-evtx-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
}
```


Well…
Maybe…
Maybe not…

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

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>
```

```
~$ cat failed-login-ez-evtx-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",
   "RecordNumber":6895
}
```

- 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?

Are there any interesting or suspicious logons?

Well…
Maybe…
Maybe not…

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Event logs

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

Accounts related stuff

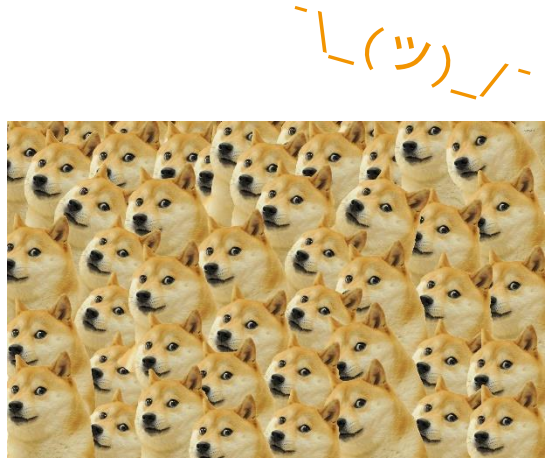
- 4624/4625 – successful/failed logon
- 4672 – login as admin
- 4648 – login with explicit credentials
- 4720 – account created
- …

„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“

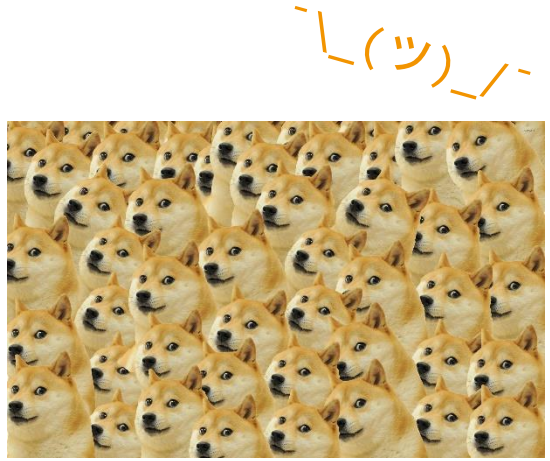
- 4950 – firewall settings are changed
- 5025 – firewall is disabled
- 1006 - malware detected
- 5012 - Scanning for viruses is disabled
- …

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://digitalf0rensics.wordpress.com/2020/08/10/notable-event-ids-from-windows-event-logs/]

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

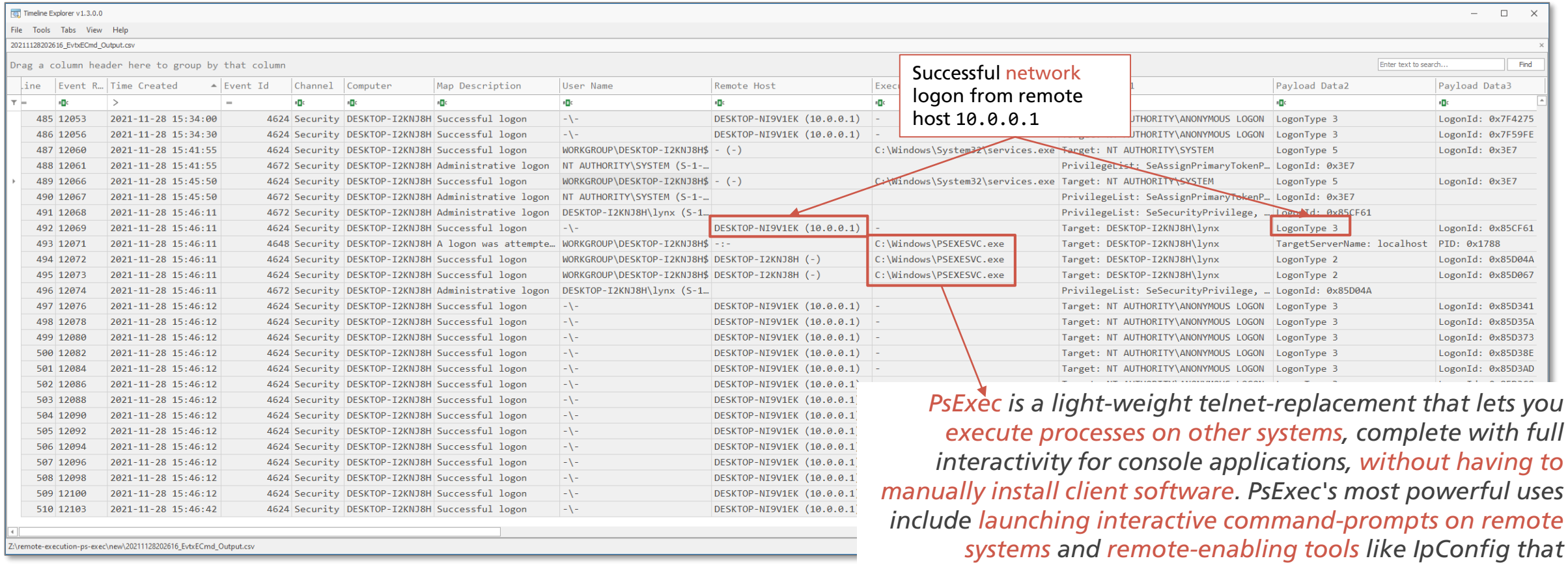
[https://github.com/mdecrevoisier/Windows-auditing-mindmap]

Are there any traces of remote execution?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Event logs to the rescue vol. II



Line	Event R…	Time Created	Event Id	Channel	Computer	Map Description	User Name	Remote Host	Exec…	…	Payload Data2	Payload Data3
485	12053	2021-11-28 15:34:00	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-NI9V1EK (10.0.0.1)	-	…UTHORITY\ANONYMOUS LOGON	LogonType 3	LogonId: 0x7F4275
486	12056	2021-11-28 15:34:30	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-NI9V1EK (10.0.0.1)	-	…UTHORITY\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-…			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-…			PrivilegeList: SeAssignPrimaryTokenP…	LogonId: 0x3E7	
491	12068	2021-11-28 15:46:11	4672	Security	DESKTOP-I2KNJ8H	Administrative logon	DESKTOP-I2KNJ8H\lynx (S-1…			PrivilegeList: SeSecurityPrivilege, …	LogonId: 0x85CF61	
492	12069	2021-11-28 15:46:11	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-NI9V1EK (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-NI9V1EK (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-NI9V1EK (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-NI9V1EK (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-NI9V1EK (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-NI9V1EK (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-NI9V1EK (10.0.0.1)				
503	12088	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-NI9V1EK (10.0.0.1				
504	12090	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-NI9V1EK (10.0.0.1				
505	12092	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-NI9V1EK (10.0.0.1				
506	12094	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-NI9V1EK (10.0.0.1				
507	12096	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-NI9V1EK (10.0.0.1				
508	12098	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-NI9V1EK (10.0.0.1				
509	12100	2021-11-28 15:46:12	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-NI9V1EK (10.0.0.1				
510	12103	2021-11-28 15:46:42	4624	Security	DESKTOP-I2KNJ8H	Successful logon	-\-	DESKTOP-NI9V1EK (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]

Hochschule Bonn-Rhein-Sieg

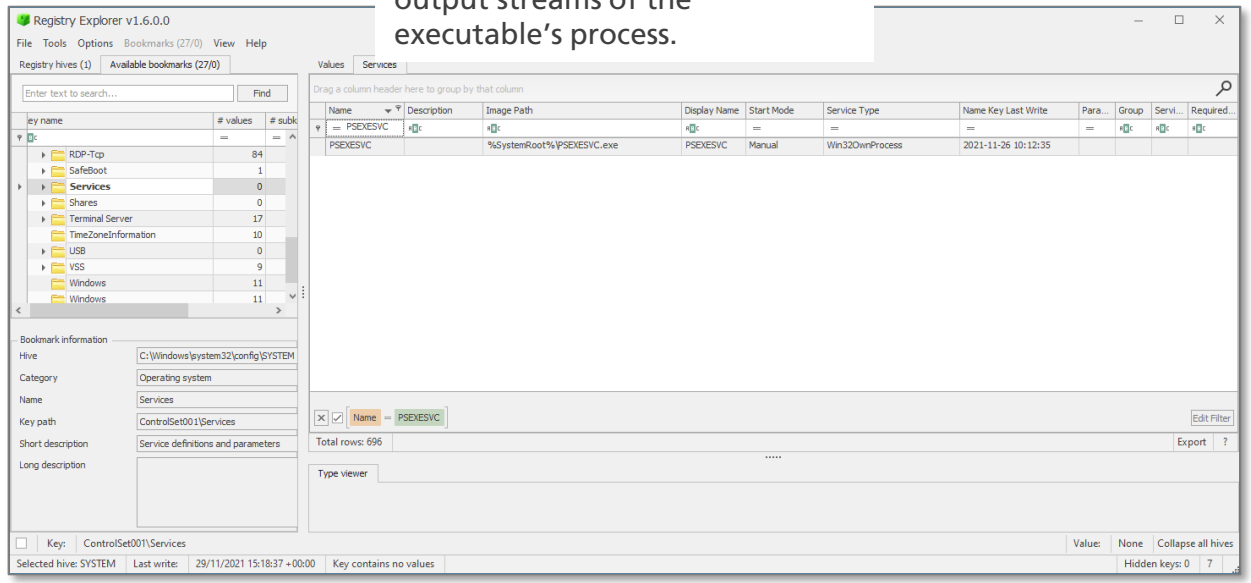
Fraunhofer FKIE

Further artifacts

Copies PSEXESCV.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 PFRO.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.



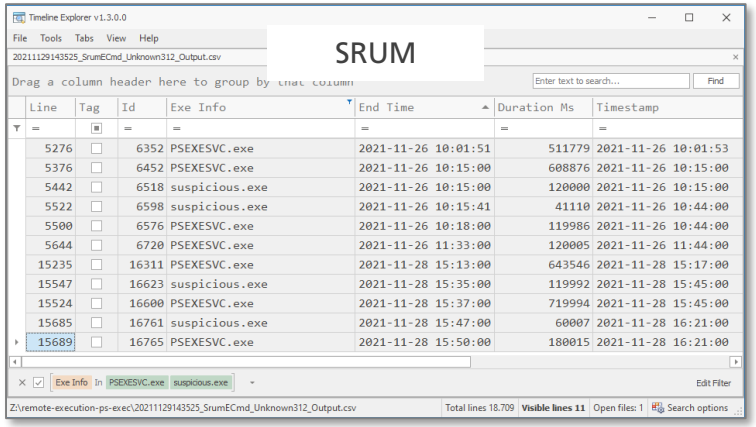
Program execution evidence for PSEXESVC service and remotely executed programs:

```
…
Command line: -f C:\Windows\Prefetch\SUSPICIOUS.
…
Created on: 2021-11-28 15:34:09
Modified on: 2021-11-28 15:46:21
Last accessed on: 2021-11-29 14:59:16

Executable name: SUSPICIOUS.EXE
Hash: 64002D45
File size (bytes): 4.642
Version: Windows 10

Run count: 2
Last run: 2021-11-28 15:46:11
Other run times: 2021-11-28 15:33:59
…
0: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS
…
Files referenced: 10

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

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{01d7d109adab1526-86adbfce}\WINDOWS
…
00: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d7d109adab1526-86adbfce}\WINDOWS\PSEXESVC.EXE
```

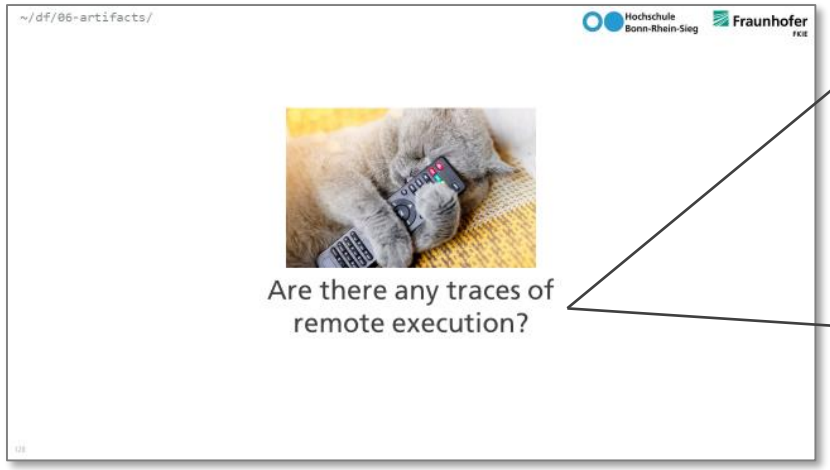
SRUM

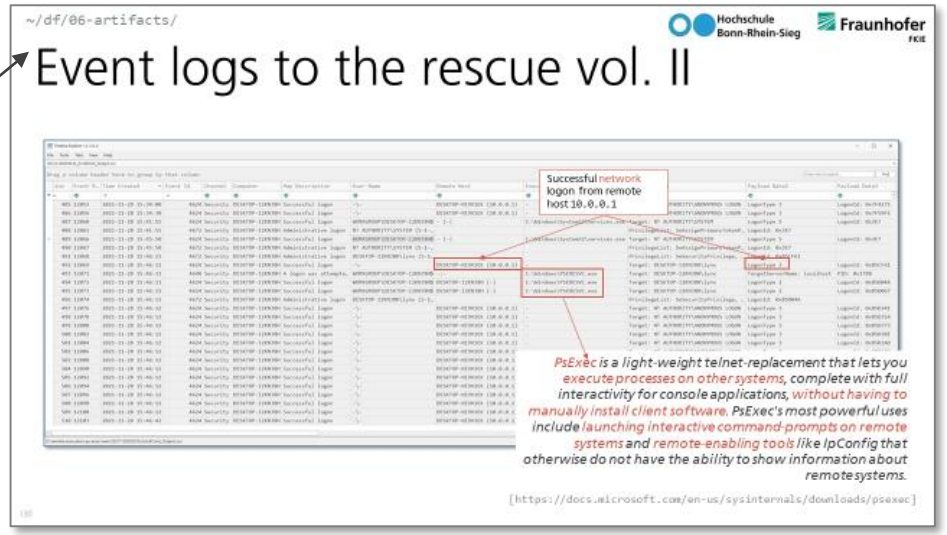


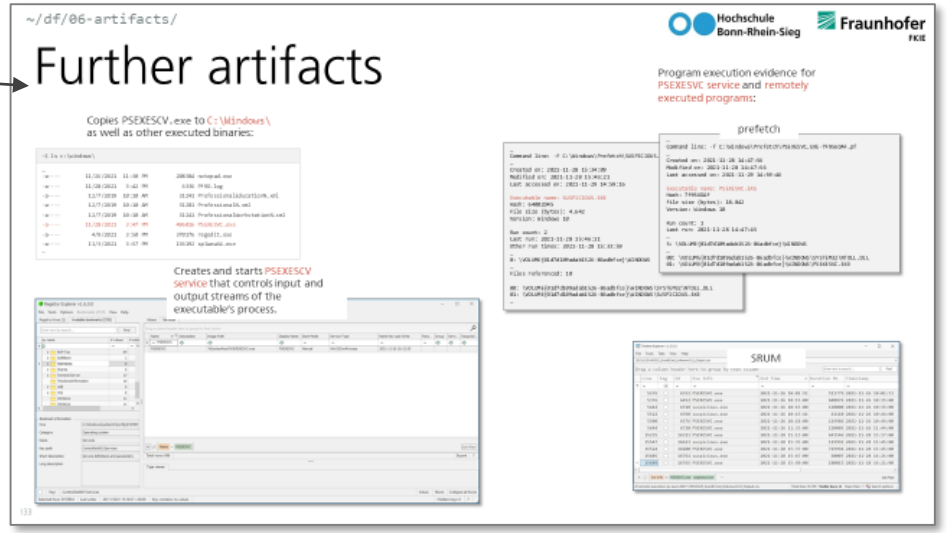
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

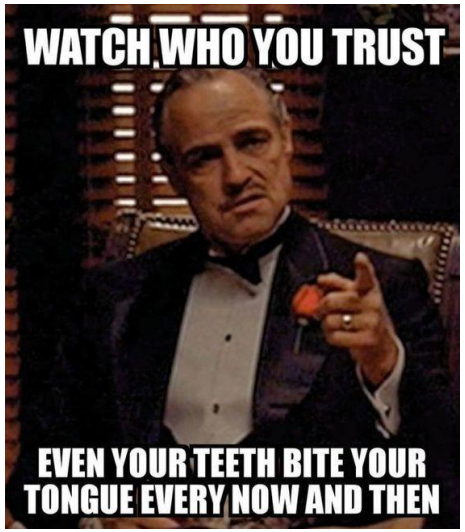
Further artifacts







Key Takeaways



Everything can be forged!

Don‘t rely on a single artifact!

Check for consistency!

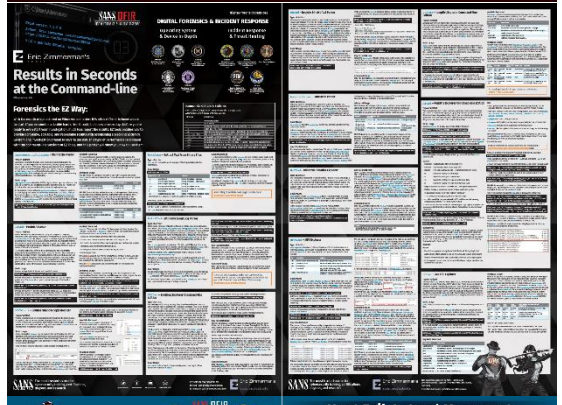
Do your own experiments!

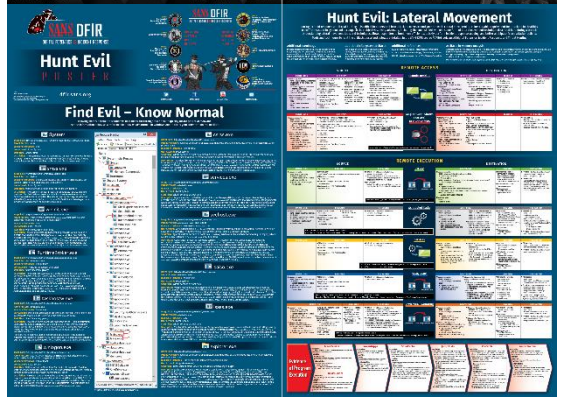
Validate findings of others!

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts





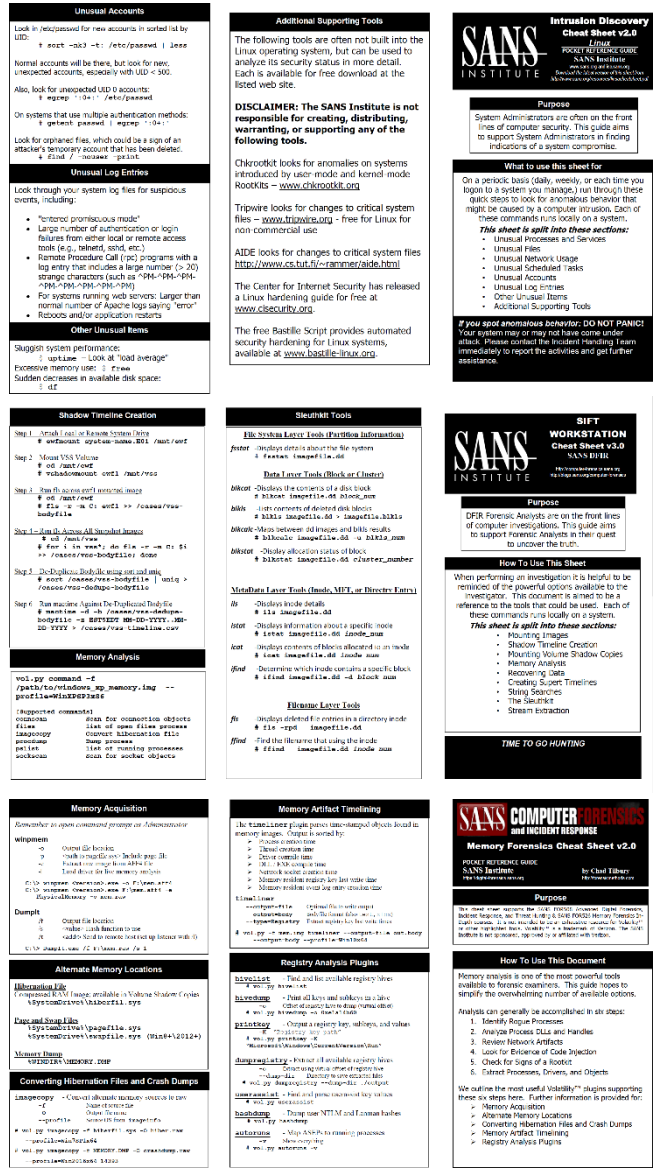
SANS provides a good starting point for

Posters

https://www.sans.org/security-resources/posters/

Cheat Sheets

https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/
https://digital-forensics.sans.org/community/cheat-sheets/



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Any Questions?