Universidad Carlos III de Madrid

Report for Linux Analysis

Juan Diego Llano Miraval

Fecha: 19/05/2024

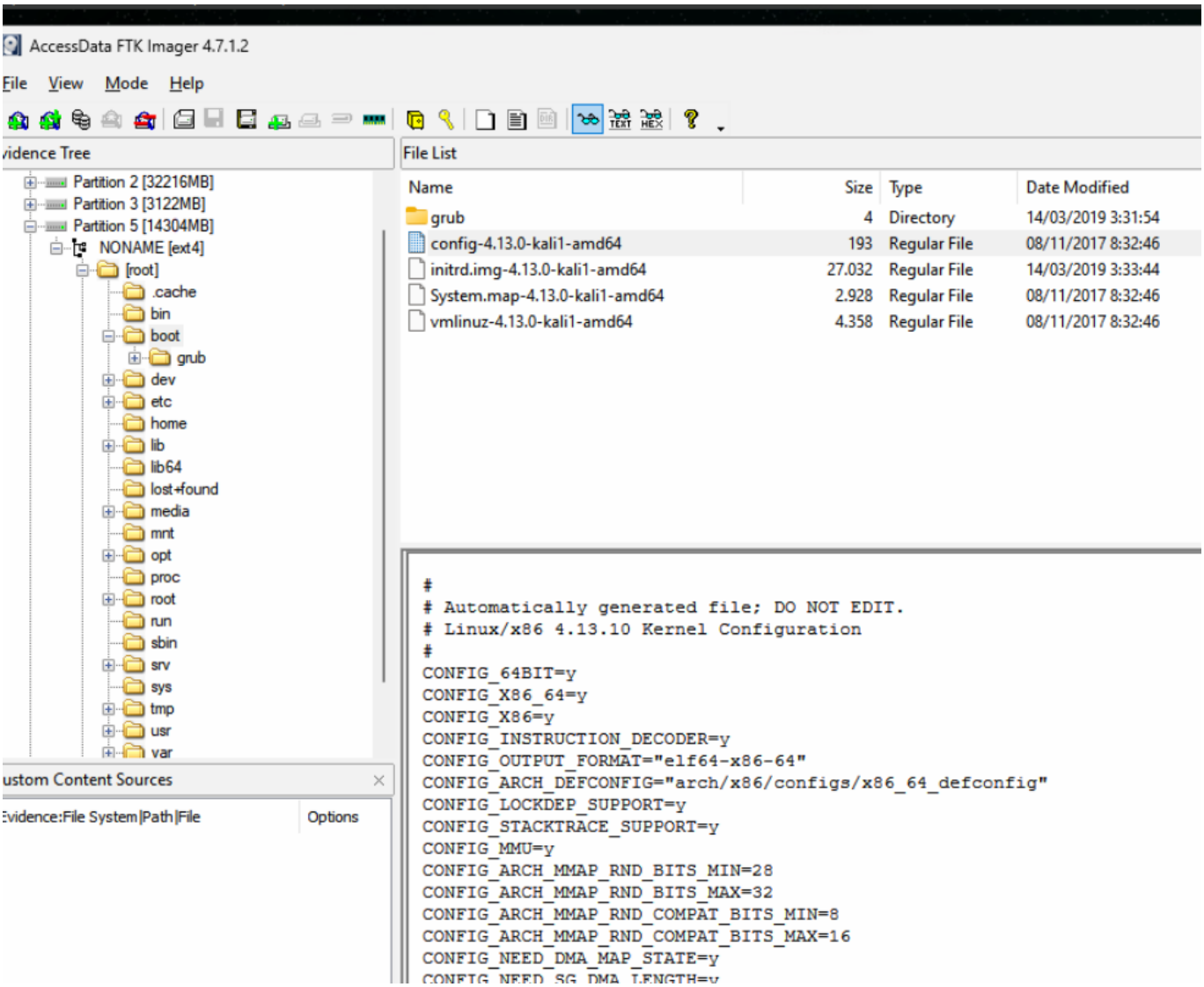
procedure

We validate the sha256:

```
a82c89650253f6b68fa26329d7f7c046bdb64183f2b5b4810e2a287b0718dde1  Horcrux.E01
7219e0e9a2e25b5b4dfce372cc1031f576aa3bb9b9c25b39c6d5ec5b1d6d1660  Horcrux.E01.txt
2a718bed8fa943f203eae28df38bdf65cfb3441b1280240789c218c7c690965a  Horcrux.E02
6530df91d9a395962661a11e0a1b833742a839f39cd4de5b006f681524c83c2b  Horcrux.E03
007426232694f9a93312e25d608e4f199814717ccce29674dab5f38ce2044663  Horcrux.E04
2e2f5bcf5155bc765129a0747151b05440de817ef4d469c56d752bf50f870188  Horcrux.E05
431b4e1769a0d0e797330cfb359519375d415346aef10c40085d7ff2264f2ffd  Horcrux.E06
91c96ea50b53ec122085e71ed9f1eb507073b95db8c2b2610fc9d3cc8b8a6a10  Horcrux.E07
3a93aec6c549f035f69c3eae86b3b66ebee566ccec3b295477af12fa51c2f9e4  Horcrux.E08
b99a4715e7c38e251b1e42db680cf8f5769874803965835c1c9cdeaa2acda610  Horcrux.E09
361b92f03c2cc18dc7b5e793b2c657f4b98e191e8a036df77fcfdbffea91c863  Horcrux.E10
2a2ef6dbb3583da9f77733db02979dc4412f2316d8e1cffccbd86024ce34c331  Horcrux.E11
16a1f3daa4561f9c19d88e45ff5a69ed455b07f039079ca1061479eae8a93e79  Horcrux.E12
ed5135b941d24e2b45ab451a96c27b348e0b8676811458f76e1b1b00237620a4  Horcrux.E13
a4bbd61a1a816aa0d665e53eb49f5d892b2edc7f9697516075c2f2a786bef256  Horcrux.E14
```

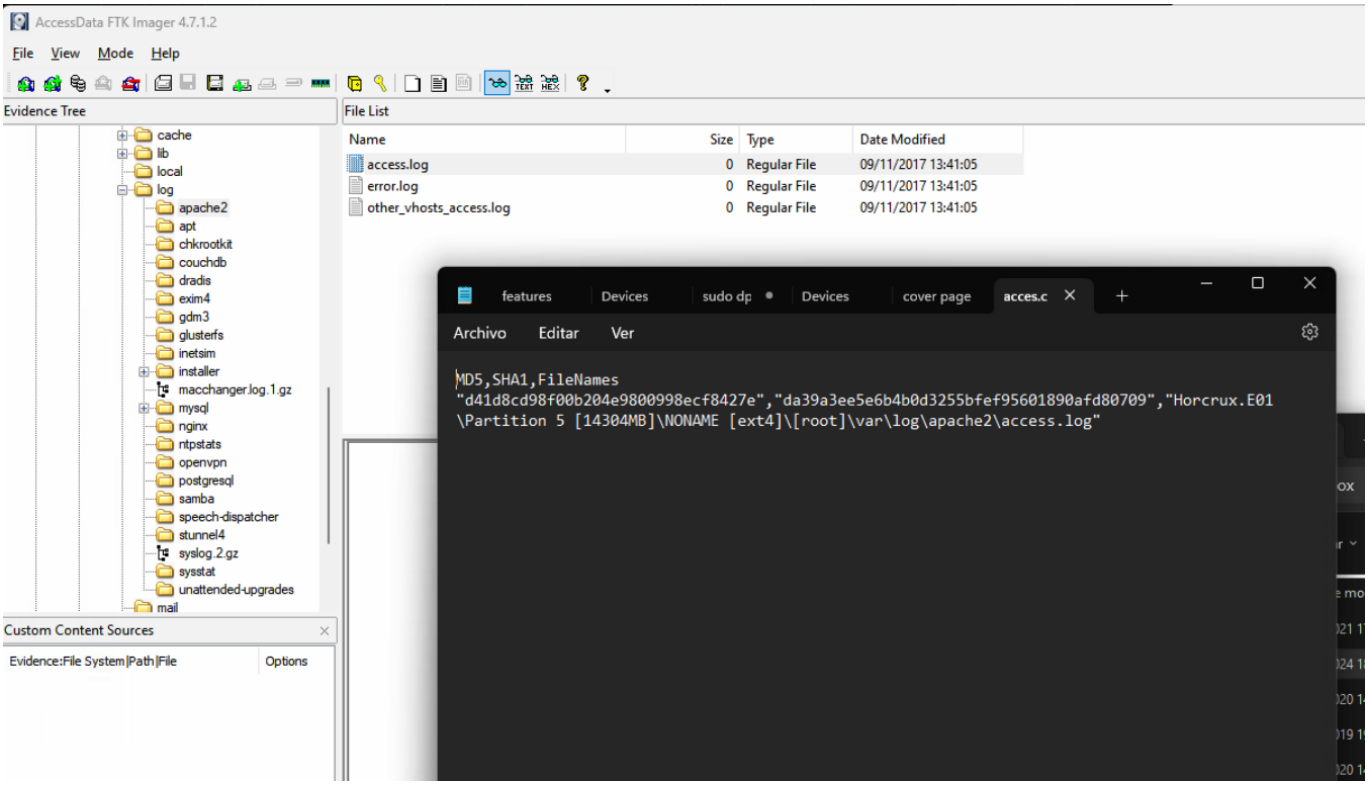
1. What distribution of Linux is being used on this machine?

On the partition 5, on the boot folder we can see some kali files, so we can confirm this is a Kali Linux.



2. What is the MD5 hash of the apache access.log?

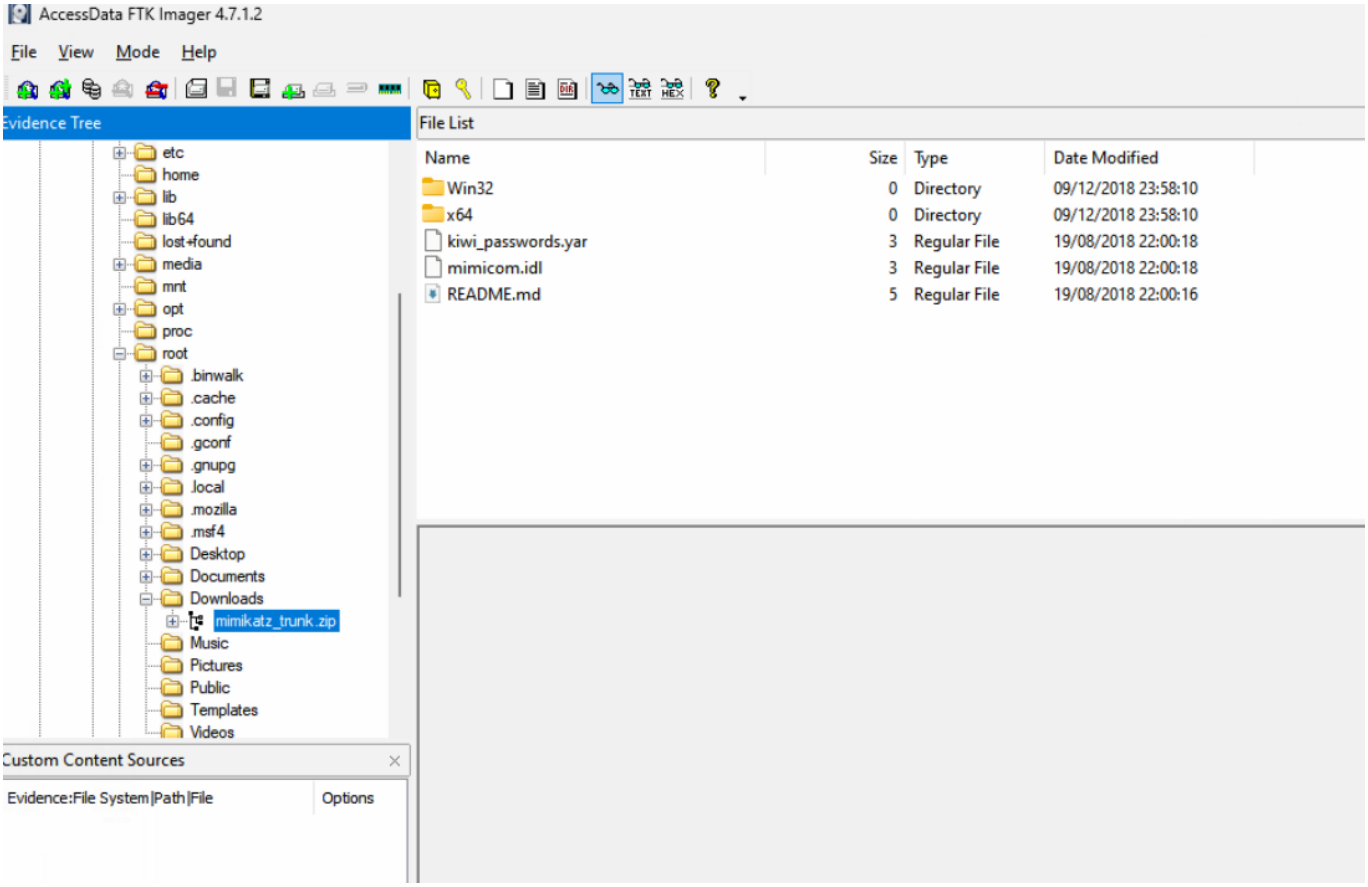
By looking at `/var/log/apache2/access.log` we cans see the file, we right click and export hash list. The output is:



d41d8cd98f00b204e9800998ecf8427e

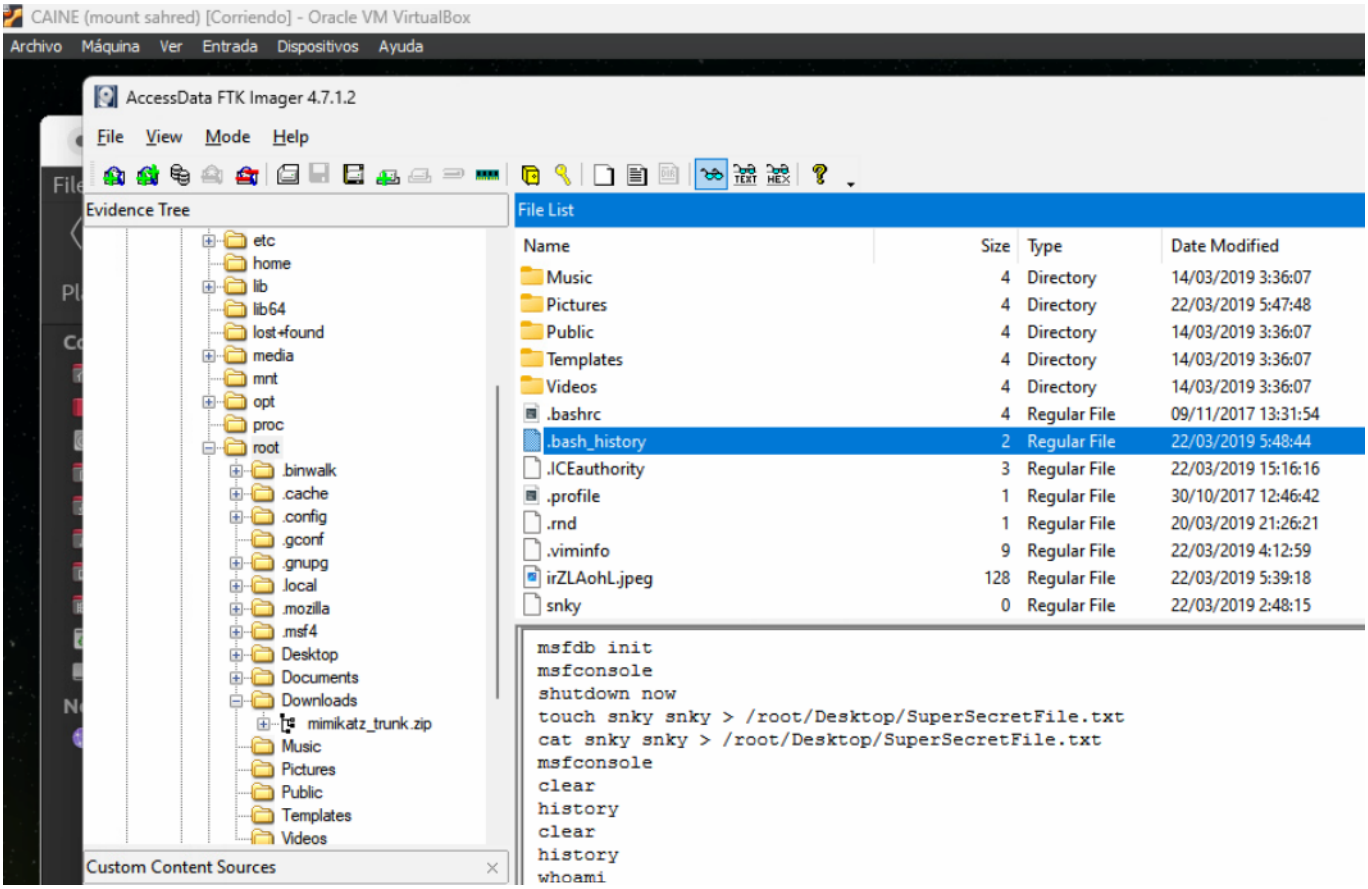
3. It is believed that a credential dumping tool was downloaded. What is the file name of the download?

Looking trhough the files leads me to the Download folder where I see `mimikatz_trunk.zip`



4. There was a super secret file created, what is the absolute path?

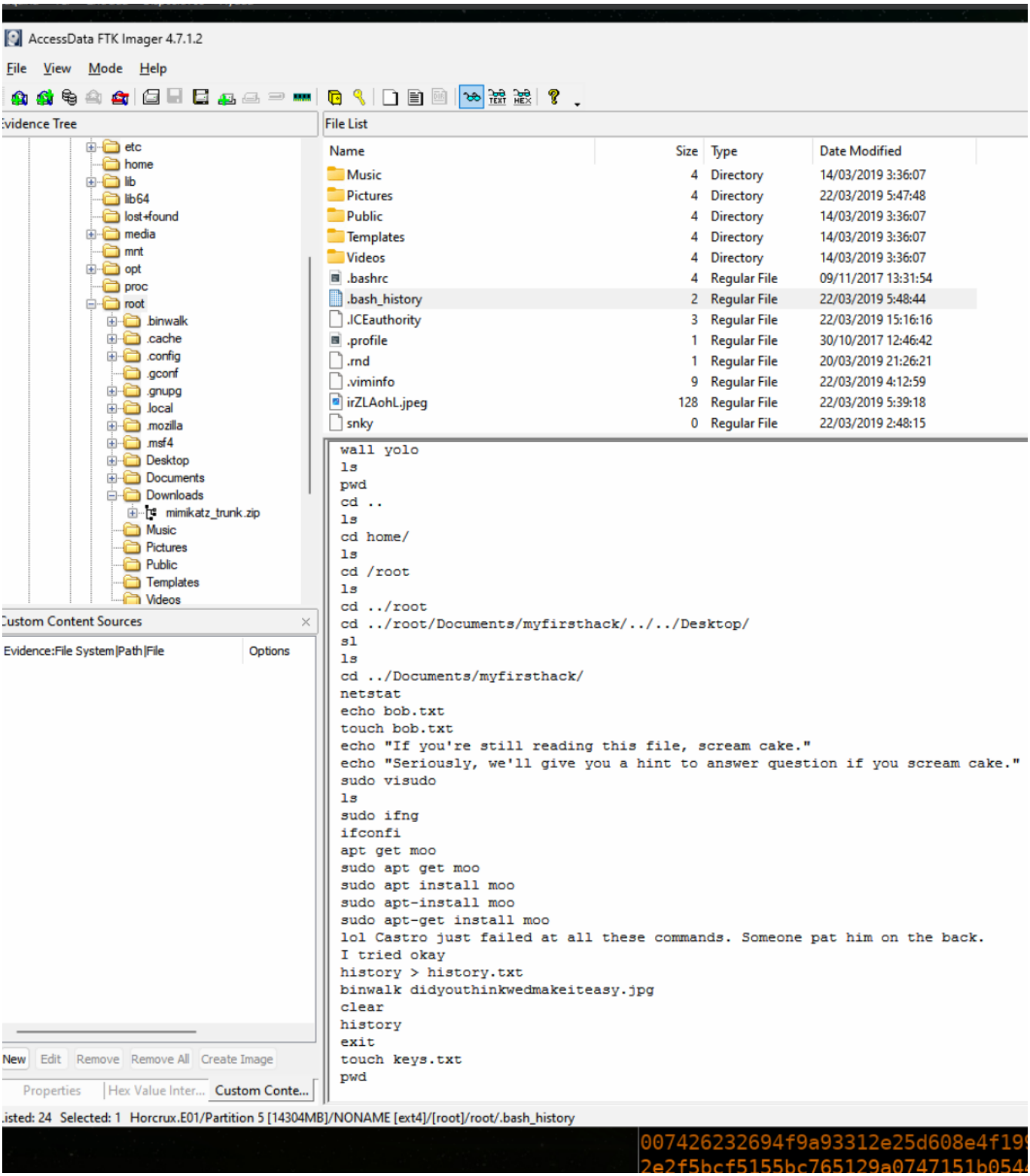
On the .bash_history we can trace down the commands and found:



`/root/Desktop/SuperSecretFile.txt`

5. What program used “didyouthinkwedmakeiteasy.jpg” during execution?

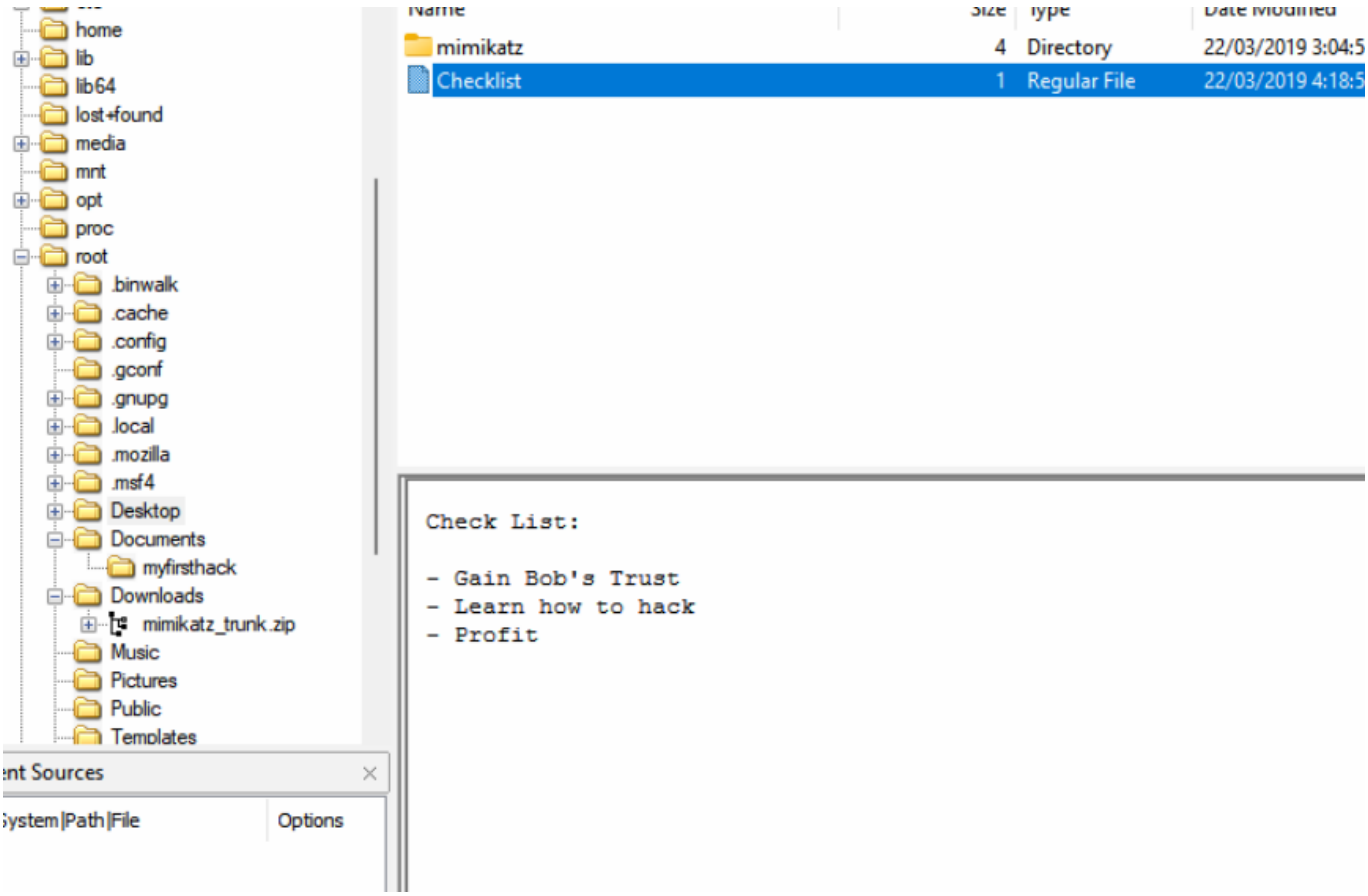
On the same .bash_history we look for any command using “didyouthinkwedmakeiteasy.jpg” and we found:



binwalk

6. What is the third goal from the checklist Karen created?

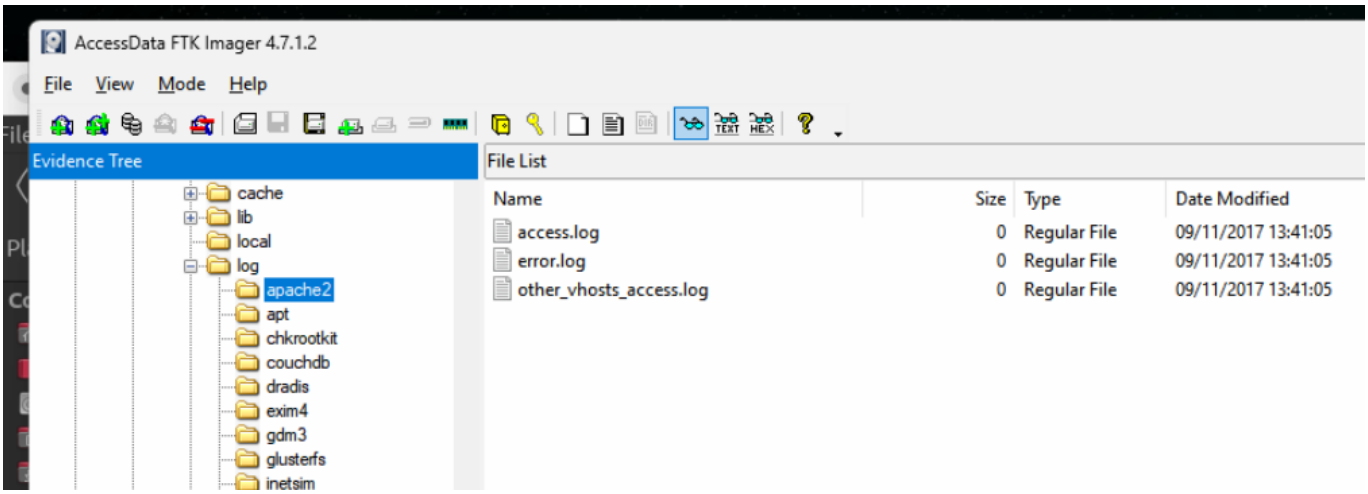
As we saw previously, there was a secret file created on Desktop, so we take a look and found the check list:



the third goal is profit.

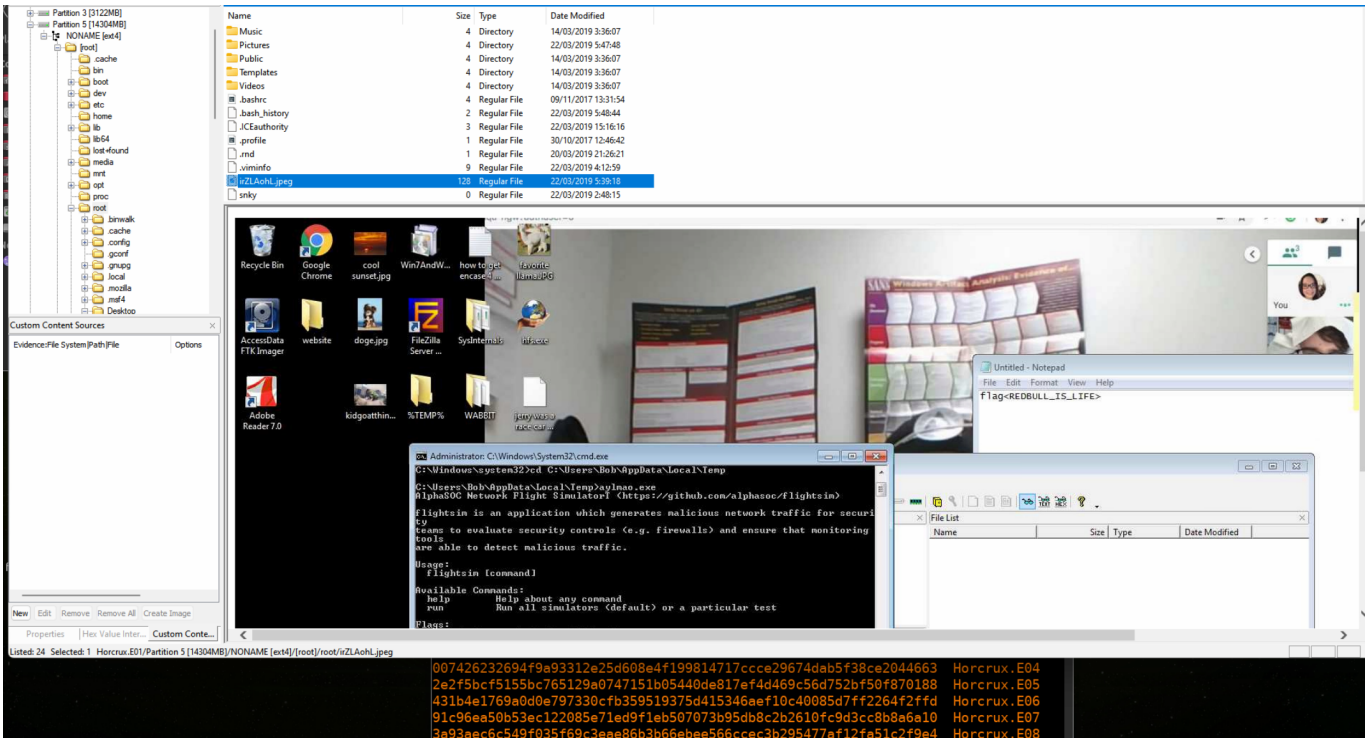
7. How many times was apache run?

When looking at the logs for any time stamp, we realized that the logs have 0 bytes, they were ready to start but the service never started, so the time apache ran was 0.



8. It is believed this machine was used to attack another, what file proves this?"

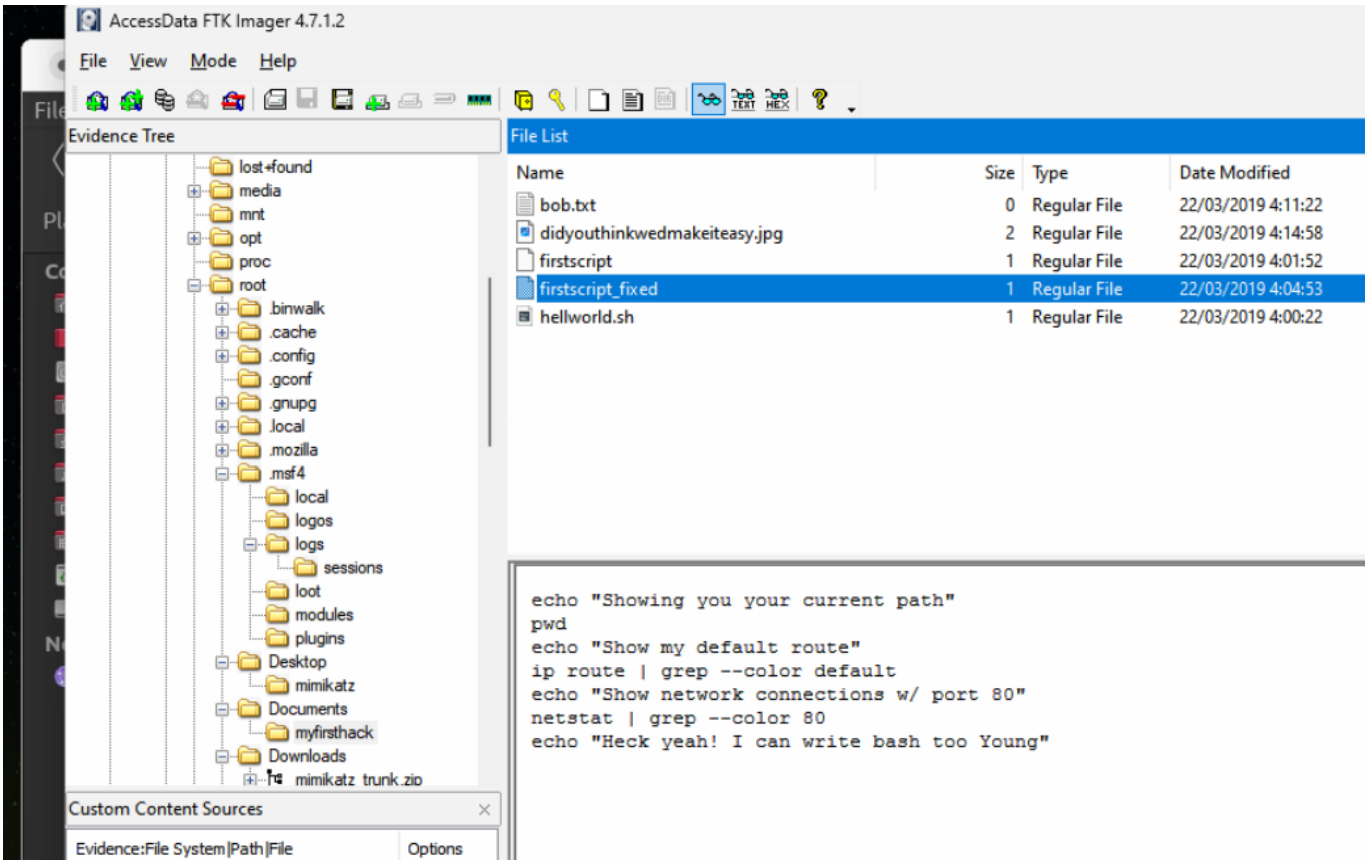
We know there ia a metsploit framework being used, but on the history we cant find evidence of an attack to someone. By expanding the view, we checked the images, and found:



this is a screenshot of a windows machine, but the image is from a Kali Linux, this might be taken from the victim.

9. Within the Documents file path, it is believed that Karen was taunting a fellow computer expert through a bash script. Who was Karen taunting?

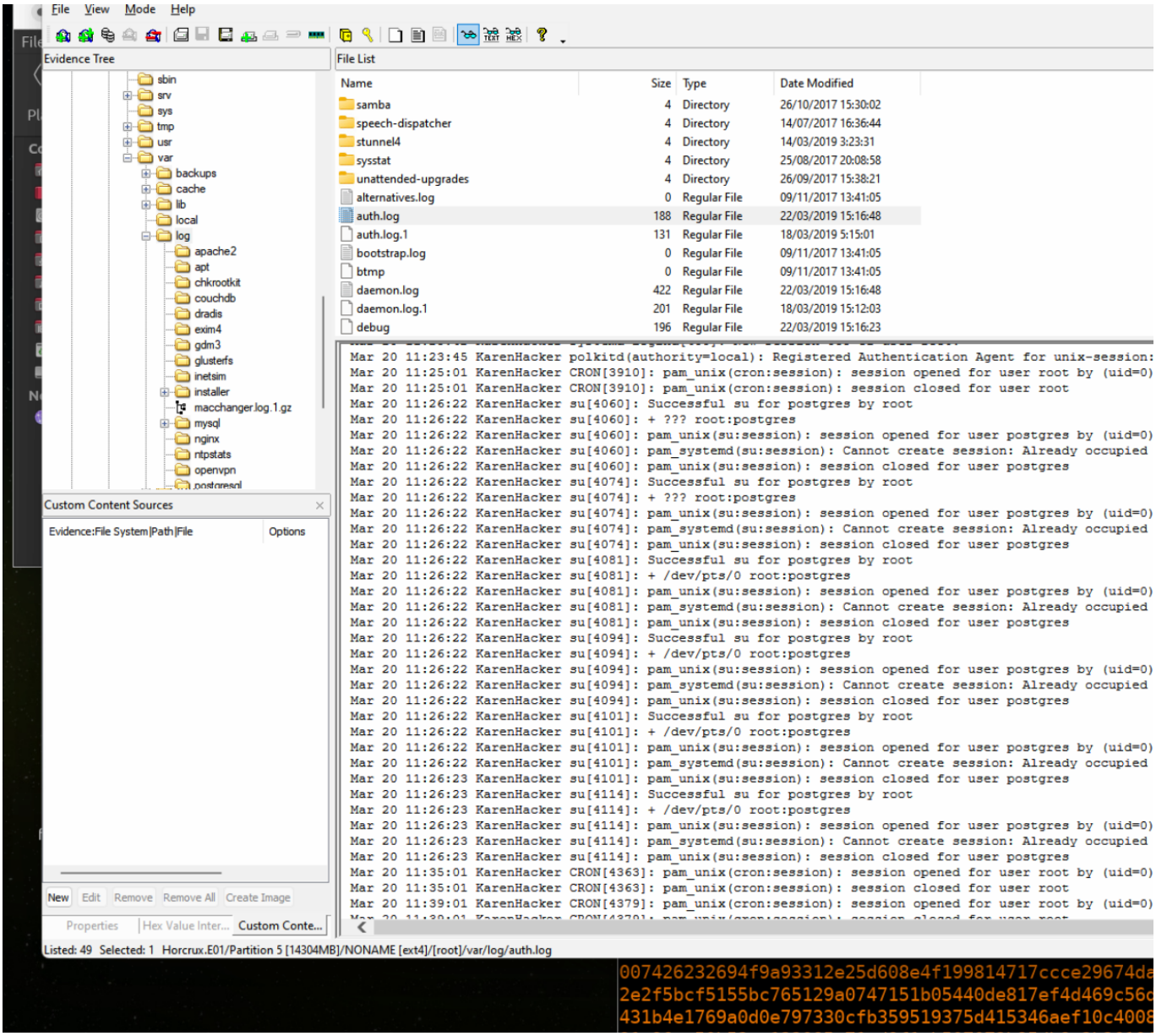
On the firstscript_fixed we can found a message to Young:



she was tauting Young

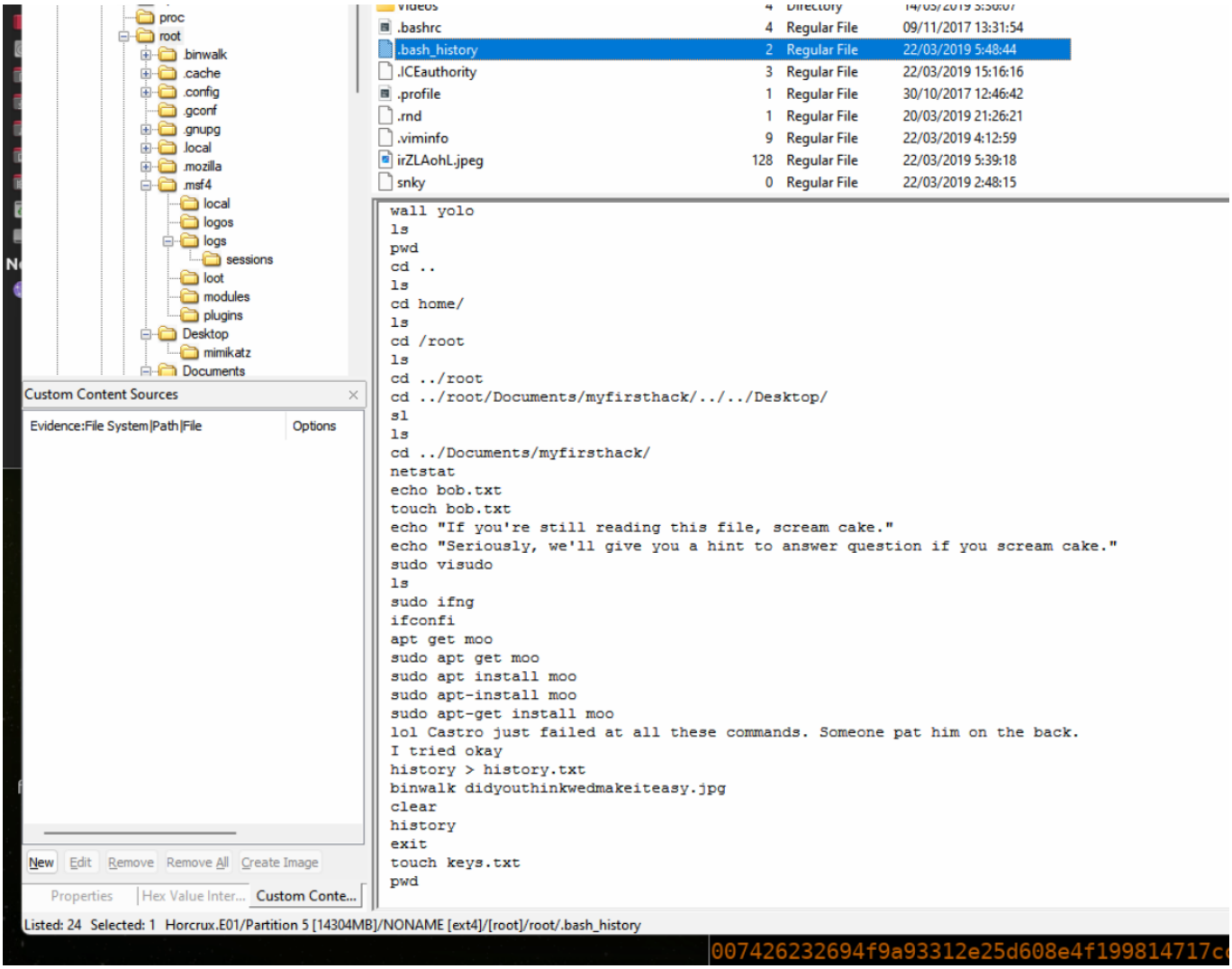
10. A user su'd to root at 11:26 multiple times. Who was it?"

By looking at `/var/log/auth.log` we can look the requested time and found that it was postgres:



11. "Based on the bash history, what is the current working directory?

the last directory change was to: `/root/Documents/myfirsthack`


proc
root
.binwalk
.cache
.config
.gconf
.gnupg
.local
.mozilla
.msf4
local
logos
logs
sessions
loot
modules
plugins
Desktop
mimikatz
Documents
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
.bashrc 4 Regular File 09/11/2017 13:31:54
.bash_history 2 Regular File 22/03/2019 5:48:44
.ICEauthority 3 Regular File 22/03/2019 15:16:16
.profile 1 Regular File 30/10/2017 12:46:42
.rnd 1 Regular File 20/03/2019 21:26:21
.viminfo 9 Regular File 22/03/2019 4:12:59
irZLAohL.jpeg 128 Regular File 22/03/2019 5:39:18
snky 0 Regular File 22/03/2019 2:48:15
wall yolo
ls
pwd
cd ..
ls
cd home/
ls
cd /root
ls
cd ../root
cd ../root/Documents/myfirsthack/../../Desktop/
sl
ls
cd ../Documents/myfirsthack/
netstat
echo bob.txt
touch bob.txt
echo "If you're still reading this file, scream cake."
echo "Seriously, we'll give you a hint to answer question if you scream cake."
sudo visudo
ls
sudo ifng
ifconfi
apt get moo
sudo apt get moo
sudo apt install moo
sudo apt-install moo
sudo apt-get install moo
lol Castro just failed at all these commands. Someone pat him on the back.
I tried okay
history > history.txt
binwalk didyouthinkwedmakeiteasy.jpg
clear
history
exit
touch keys.txt
pwd
Listed: 24 Selected: 1 Horcrux.E01/Partition 5 [14304MB]/NONAME [ext4]/[root]/root/.bash_history
0074262326694f9a93312e25d608e4f199814717c