Insider Challenge

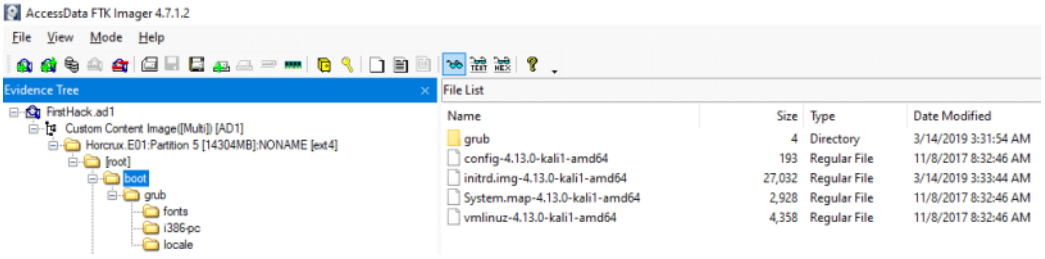
Scenario:

After Karen started working for 'TAAUSAI,' she began to do some illegal activities inside the company. 'TAAUSAI' hired you as a soc analyst to kick off an investigation on this case.

You acquired a disk image and found that Karen uses Linux OS on her machine. Analyze the disk image of Karen's computer and answer the provided questions.

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

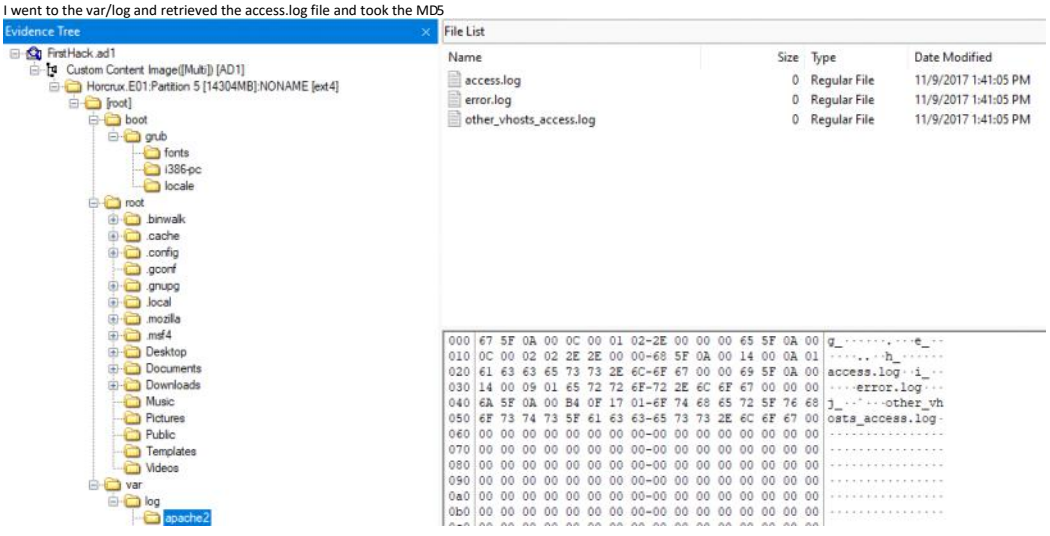
I opened the image file with FTK Imager and at the boot folder I saw the Kali version

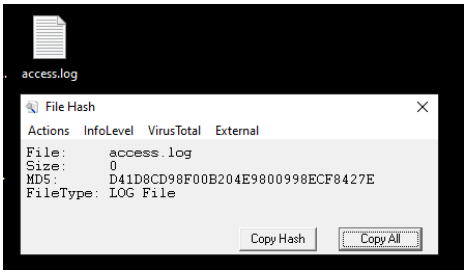


Answer: kali

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

I went to the var/log and retrieved the access.log file and took the MD5

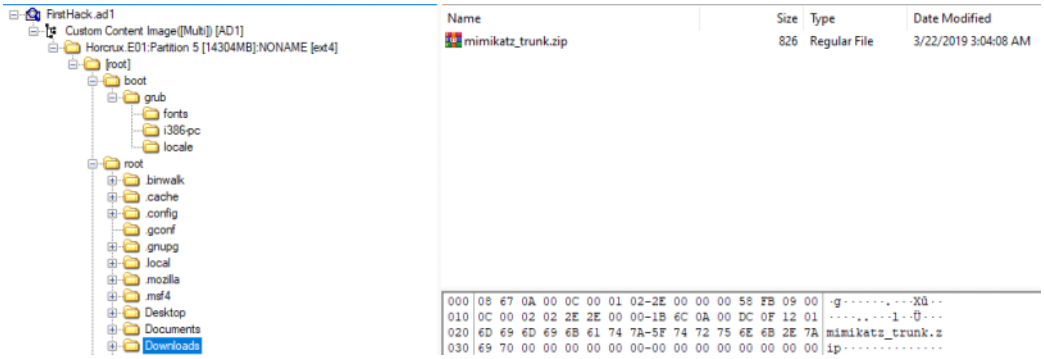




Answer: d41d8cd98f00b204e9800998ecf8427e

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

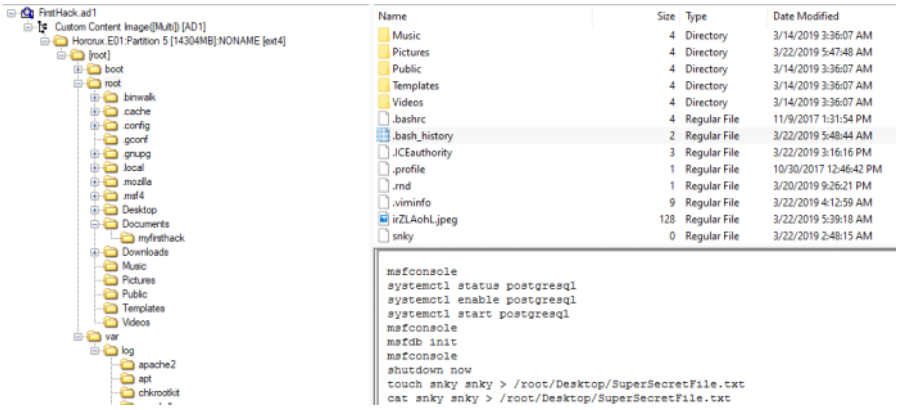
I went to the Downloads folder



Answer: mimikatz_trunk.zip

Task 4:
There was a super-secret file created. What is the absolute path?

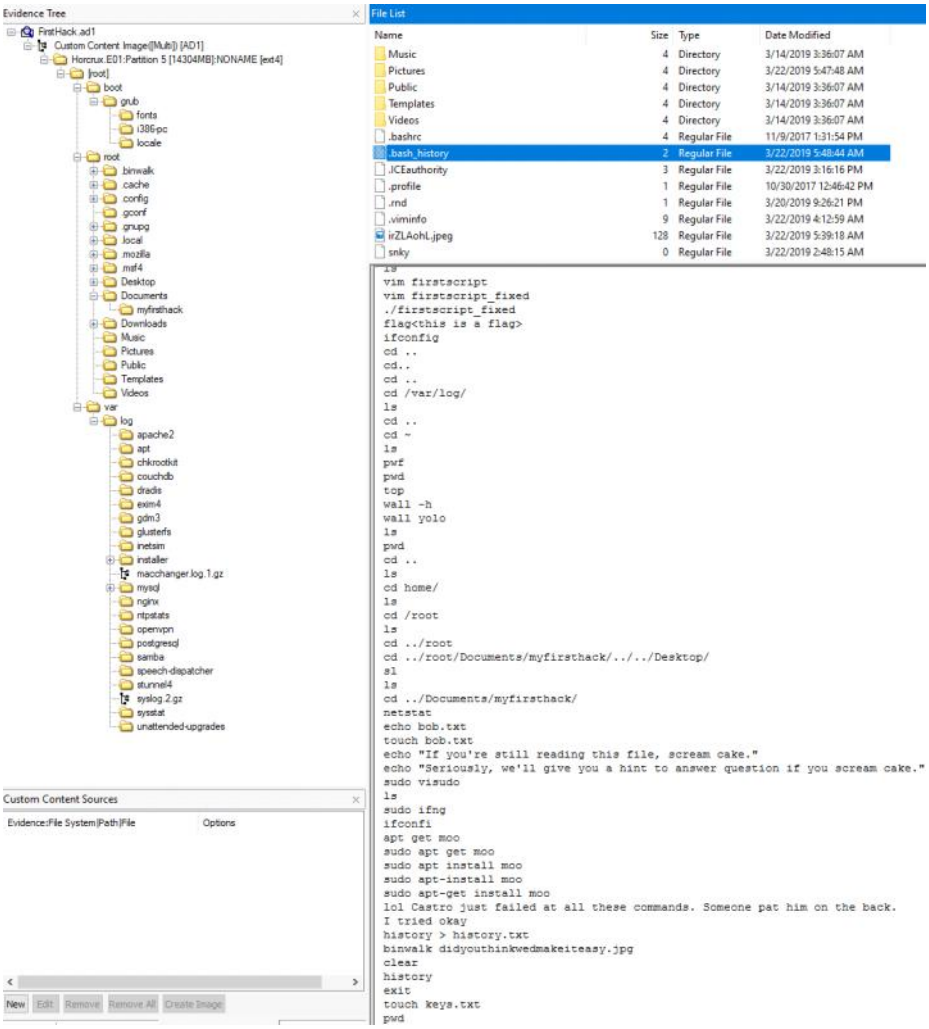
I checked the .bash_history and found the secret file



Answer: /root/Desktop/SuperSecretFile.txt

Task 5:
What program used didyouthinkwedmakeiteasy.jpg during execution?

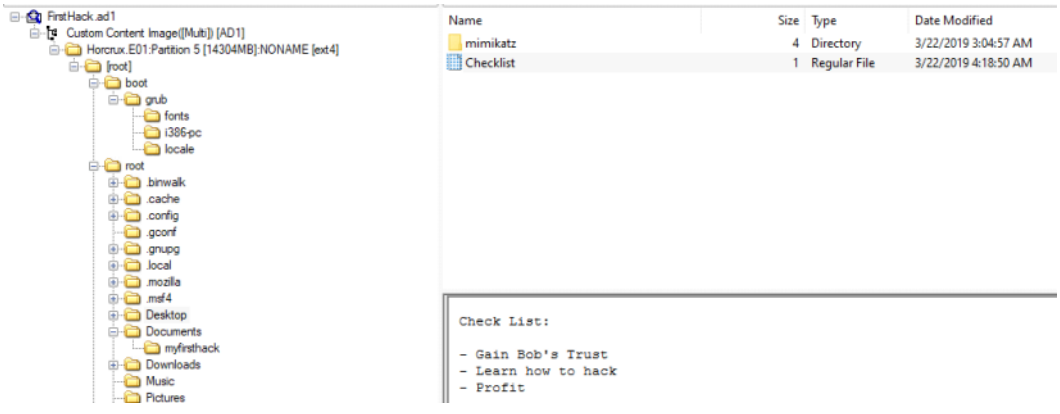
I checked the .bash_history inside the root folder and saw binwalk with the jpg filename



Answer: binwalk

Task 6:
What is the third goal from the checklist Karen created?

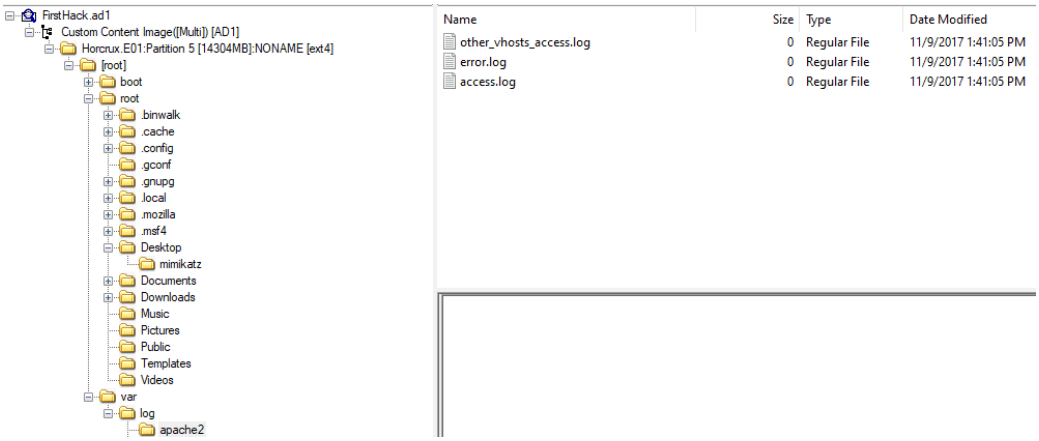
I found the Checklist file on the Desktop



Answer: profit

Task 7:
How many times was apache run?

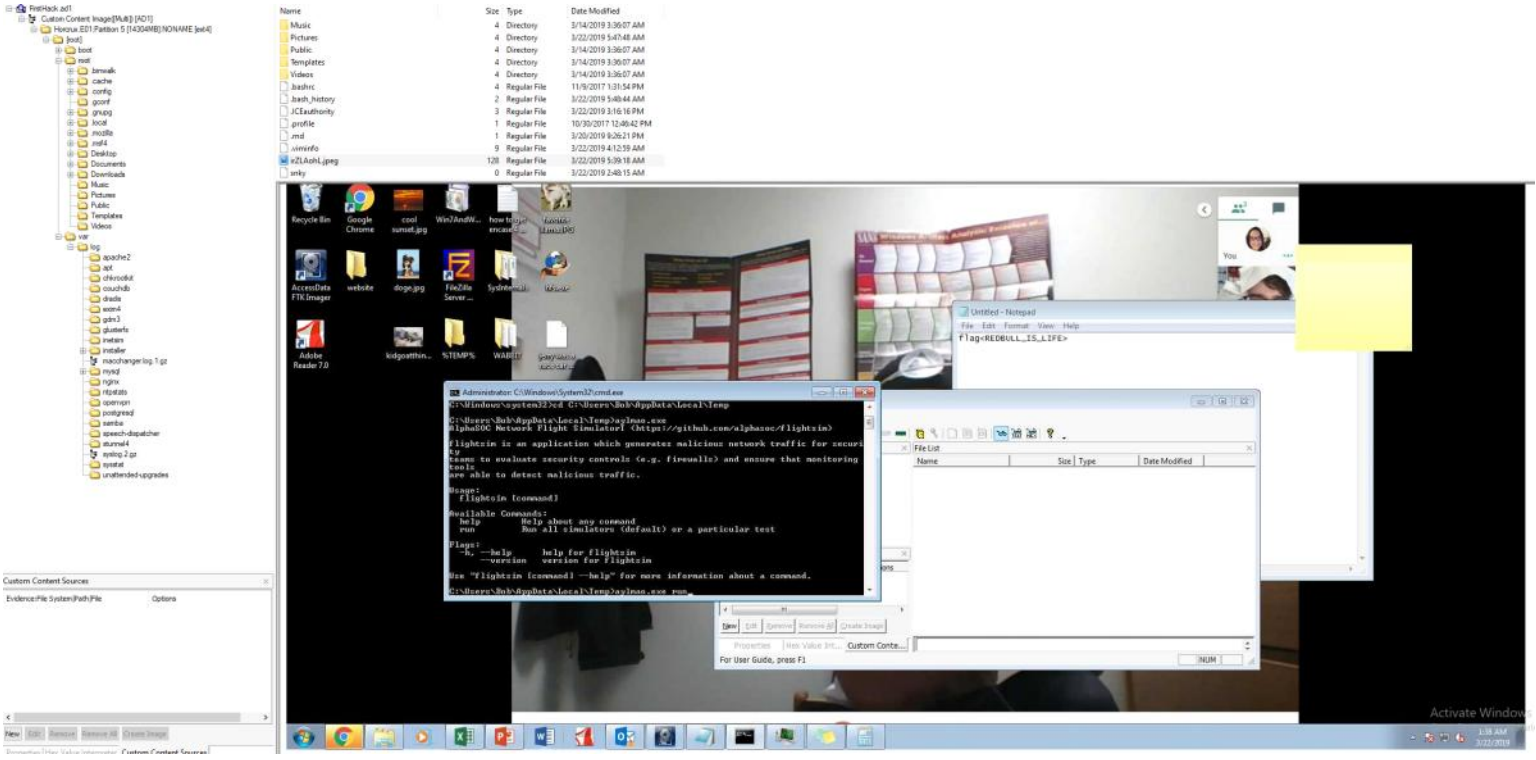
I checked the apache2 folder and all the logs was empty that means the Apache was never run



Answer: 0

Task 8:
It is believed this machine was used to attack another. What file proves this?

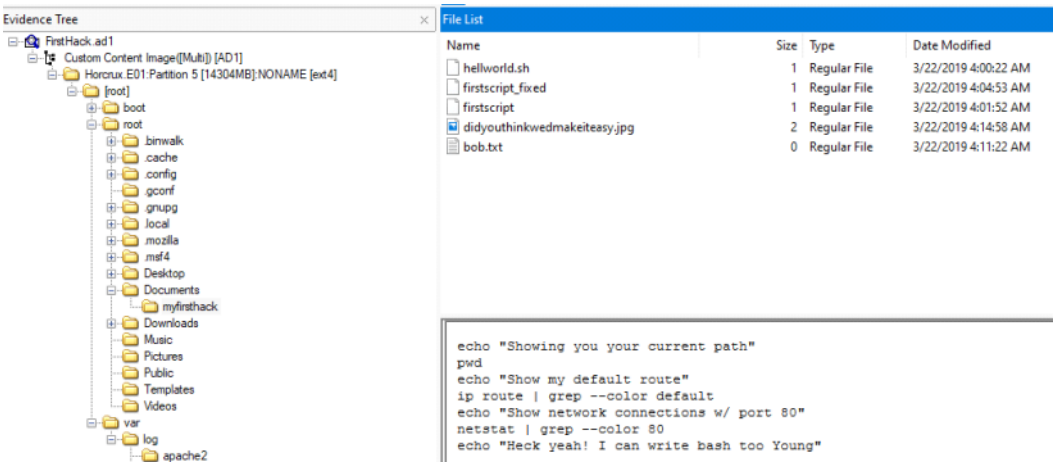
I saw an image inside the root folder and inside the image there was some picture from Windows machine with a cmd



Answer: irZLAohL.jpeg

Task 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?

I checked the firstscript_fixed inside the Documents\myfirsthack folder



Answer: young

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

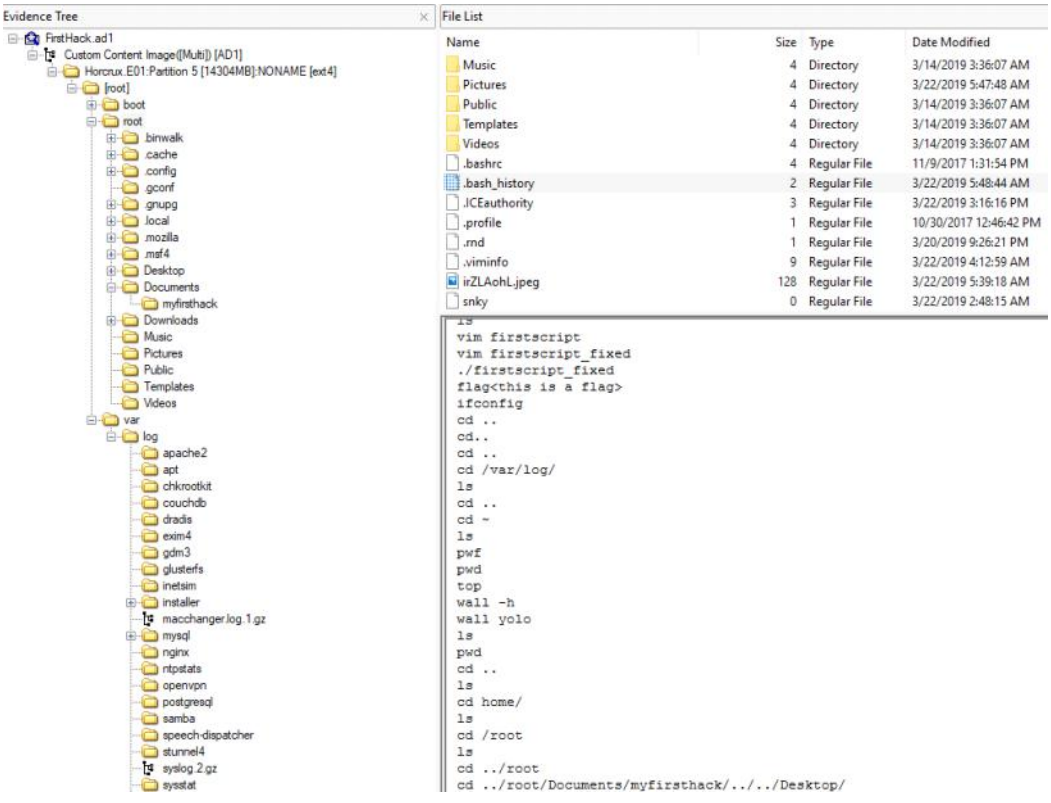
I checked the var\log\auth.log and opened it with Notepad++ and searched for 11:26

```
Mar 20 11:25:01 KarenHacker CRON[3910]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 20 11:25:01 KarenHacker CRON[3910]: pam_unix(cron:session): session closed for user root
Mar 20 11:26:22 KarenHacker su[4060]: Successful su for postgres by root
Mar 20 11:26:22 KarenHacker su[4060]: + ??? root:postgres
```

Answer: postgres

Task 11:
Based on the bash history, what is the current working directory?

I checked the .bash_history and noticed the pwd command and then the path



Answer: root/Documents/myfirsthack/