SOC Masters

ENDPOINT FORENSICS REPORT

CyberDefenders : Insider

Scenario

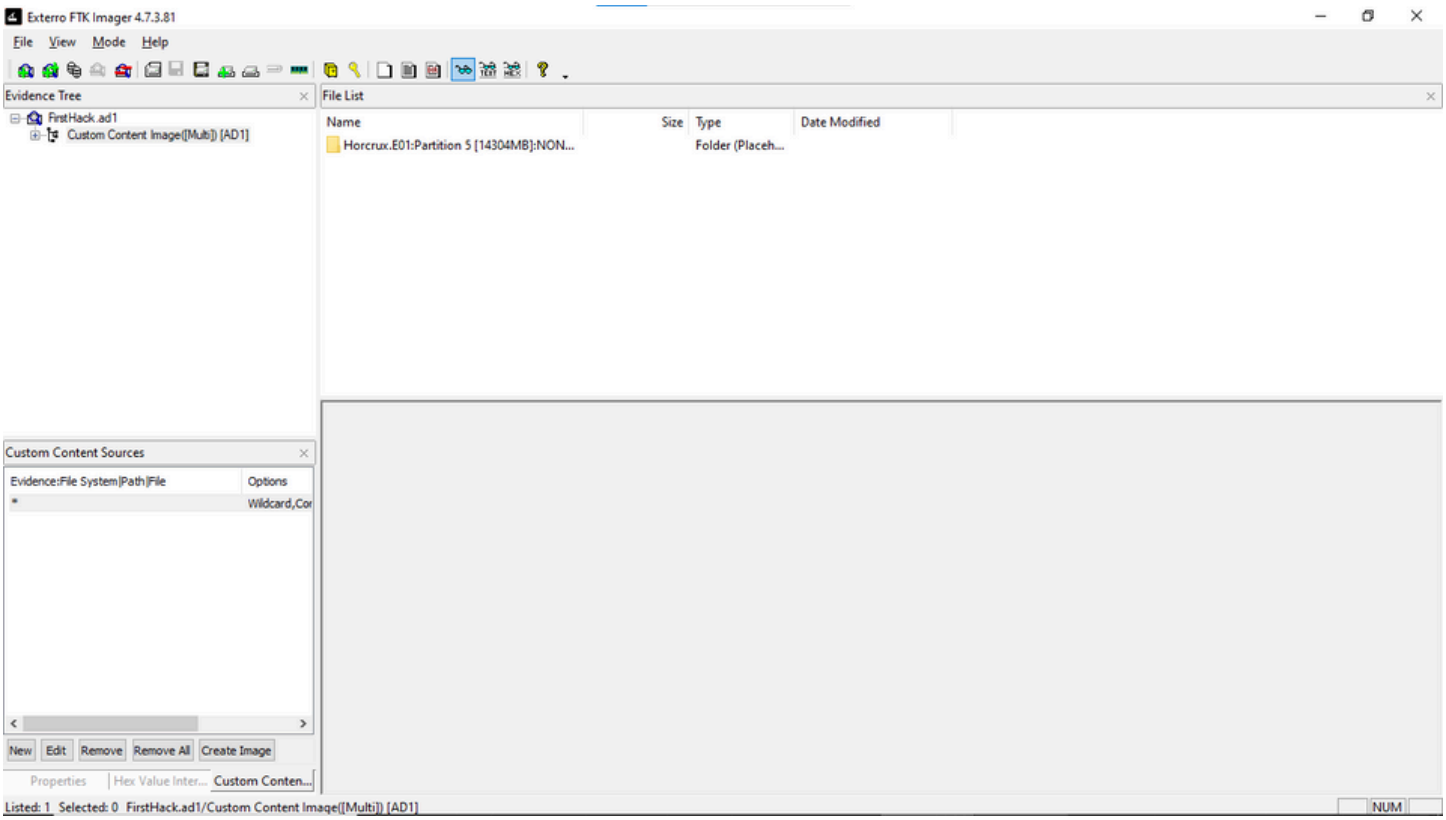
After Karen started working for 'TAAUSAI,' she began doing illegal activities inside the company. 'TAAUSAI' hired you as a soc analyst to kick off an investigation on this case.

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.

Tools Used

1. FTK Imager

- **Purpose:** Forensic image mounting, previewing, and file extraction.
- **Use Case:** Used to mount and examine the segmented evidence image (FristHack.d1) in a forensically sound manner. Allowed quick navigation through the file system to identify user activity, extract suspicious files, and recover deleted data for deeper analysis.



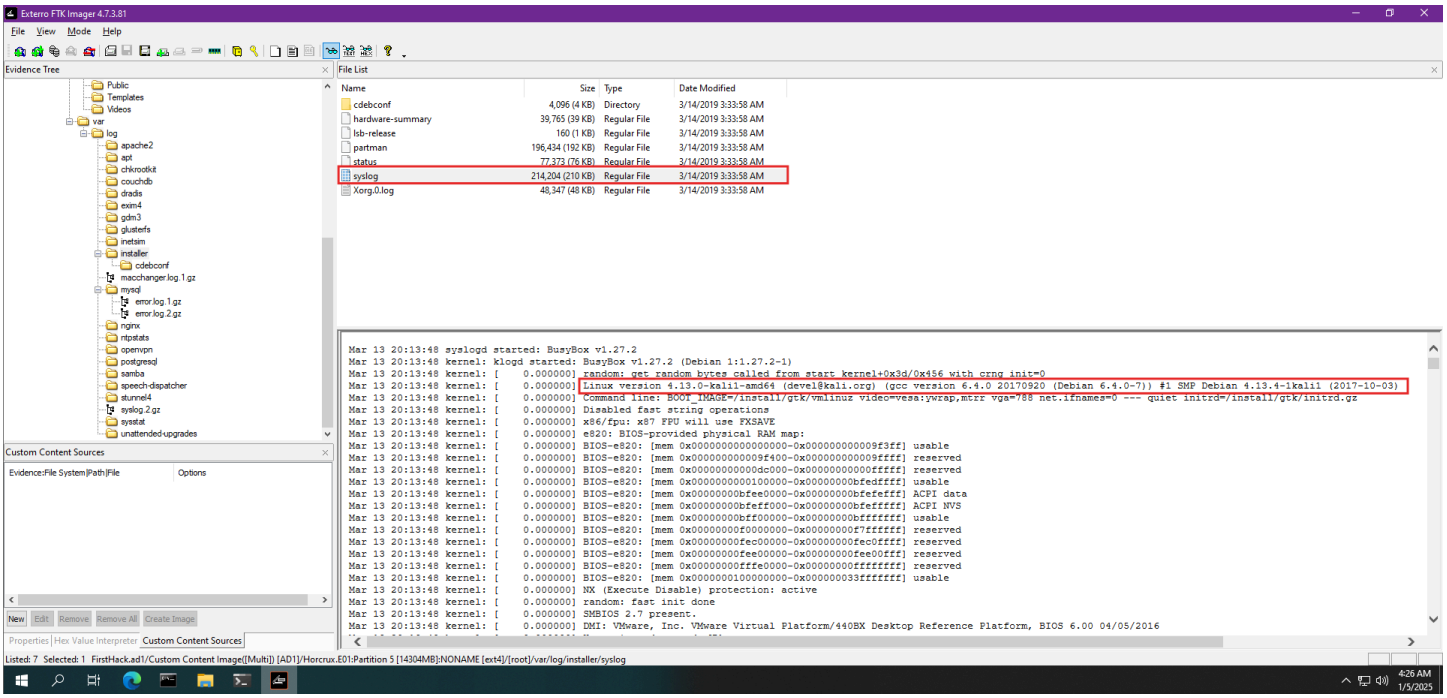
Investigation Overview

✅ Q1 – What distribution of Linux is being used on this machine?

Approach:

1. Loaded the disk image into **FTK Imager**.
2. Navigated to: /var/log/installer/syslog.
3. Located kernel boot message:

Linux version 4.13.0-kali1-amd64 (devel@kali.org)

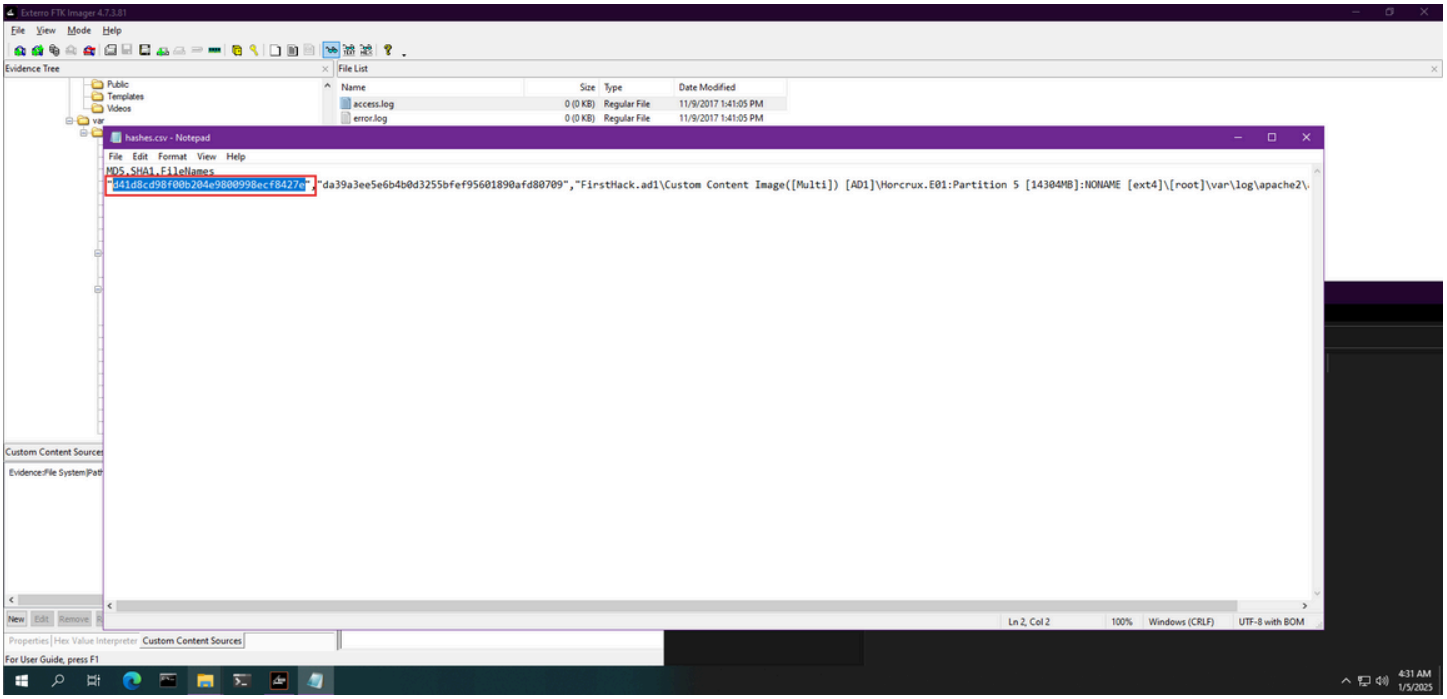


Answer: Kali

✅ Q2 – What is the MD5 hash of the apache access.log?

Approach:

1. Opened the disk image using **FTK Imager**.
2. Located the Apache access.log file in:
   /var/log/apache2/access.log
3. Right-clicked the file > **Export File Hash** > Selected **MD5**.
4. Retrieved the hash from the generated hash report.

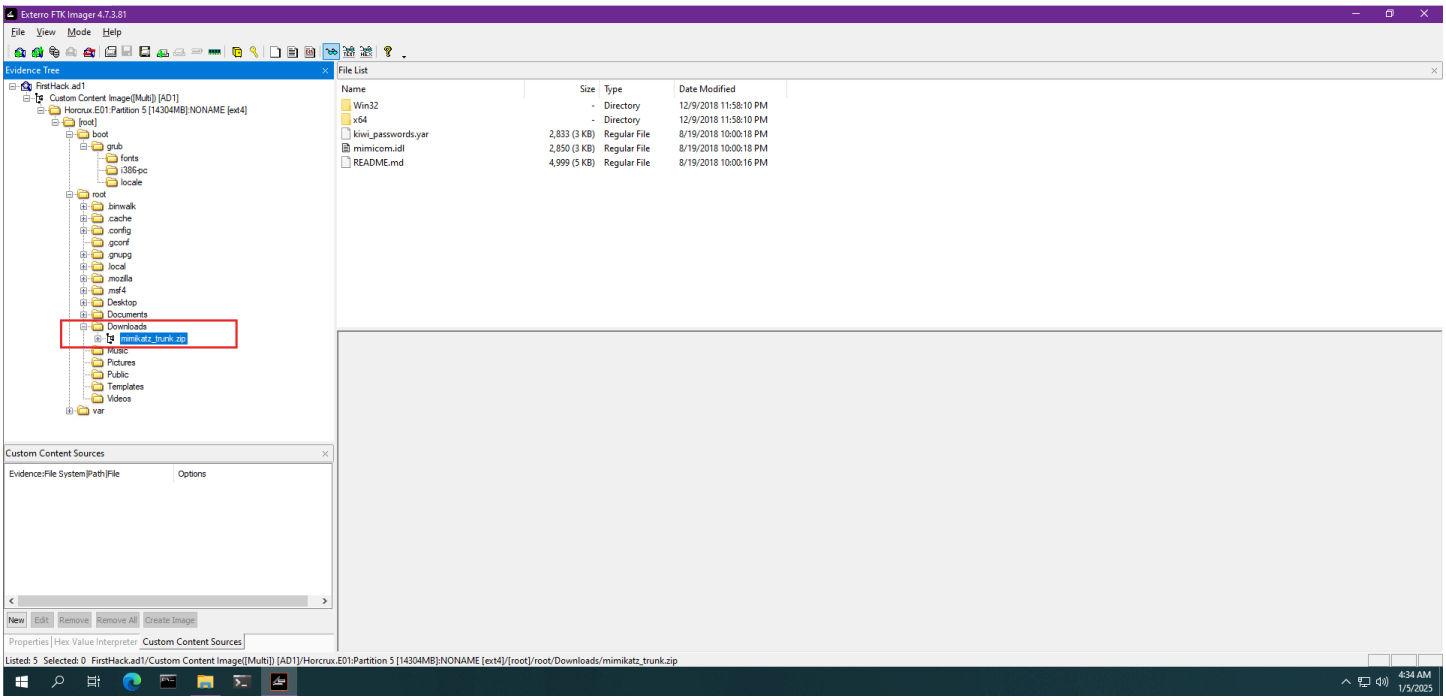


Answer: d41d8cd98f00b204e9800998ecf8427e

✅ Q3 – It is believed that a credential dumping tool was downloaded. What is the file name of the download?

Approach:

1. Loaded the disk image in **FTK Imager**.
2. Navigated to:
   /root/Downloads/



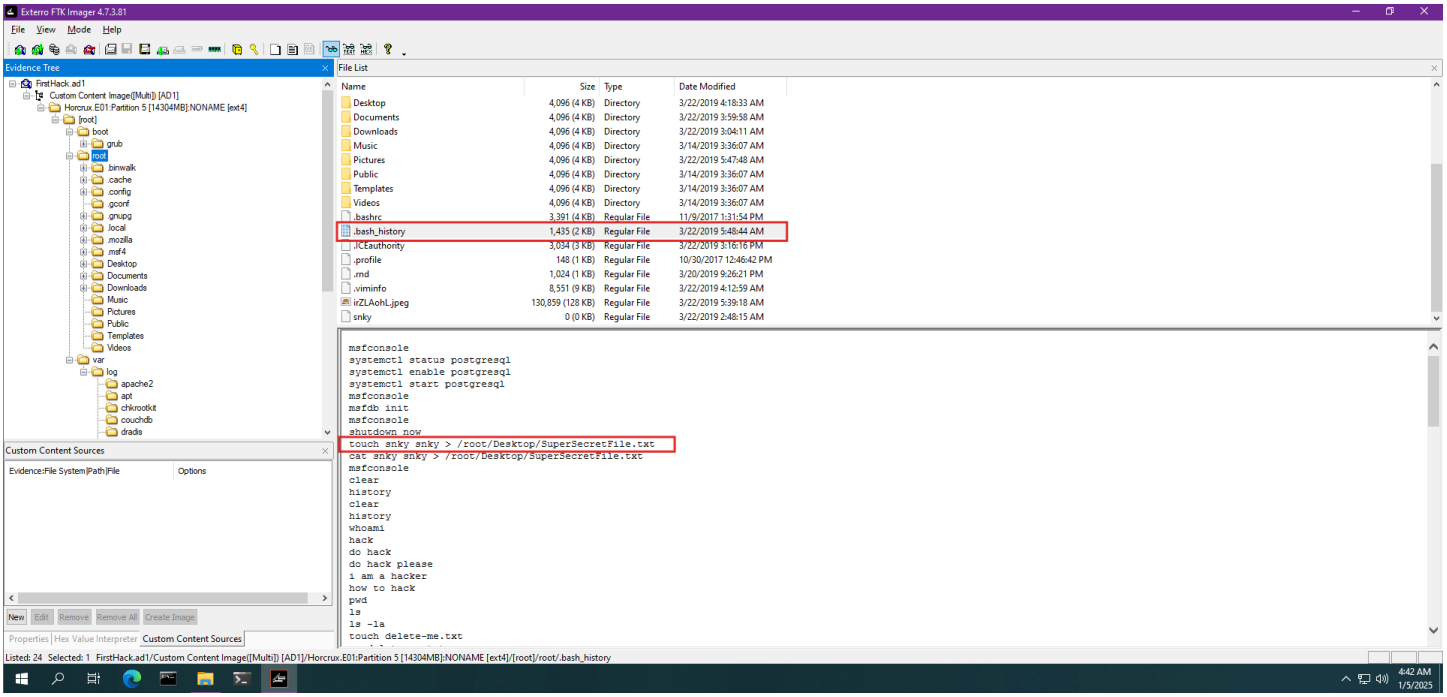
3.Reviewed file names and identified a suspicious archive:
mimikatz_trunk.zip

Answer: mimikatz_trunk.zip

✅ Q4 – There was a super-secret file created. What is the absolute path?

Approach:

1. Loaded the disk image in **FTK Imager**.
2. Navigated to: /root/.bash_history



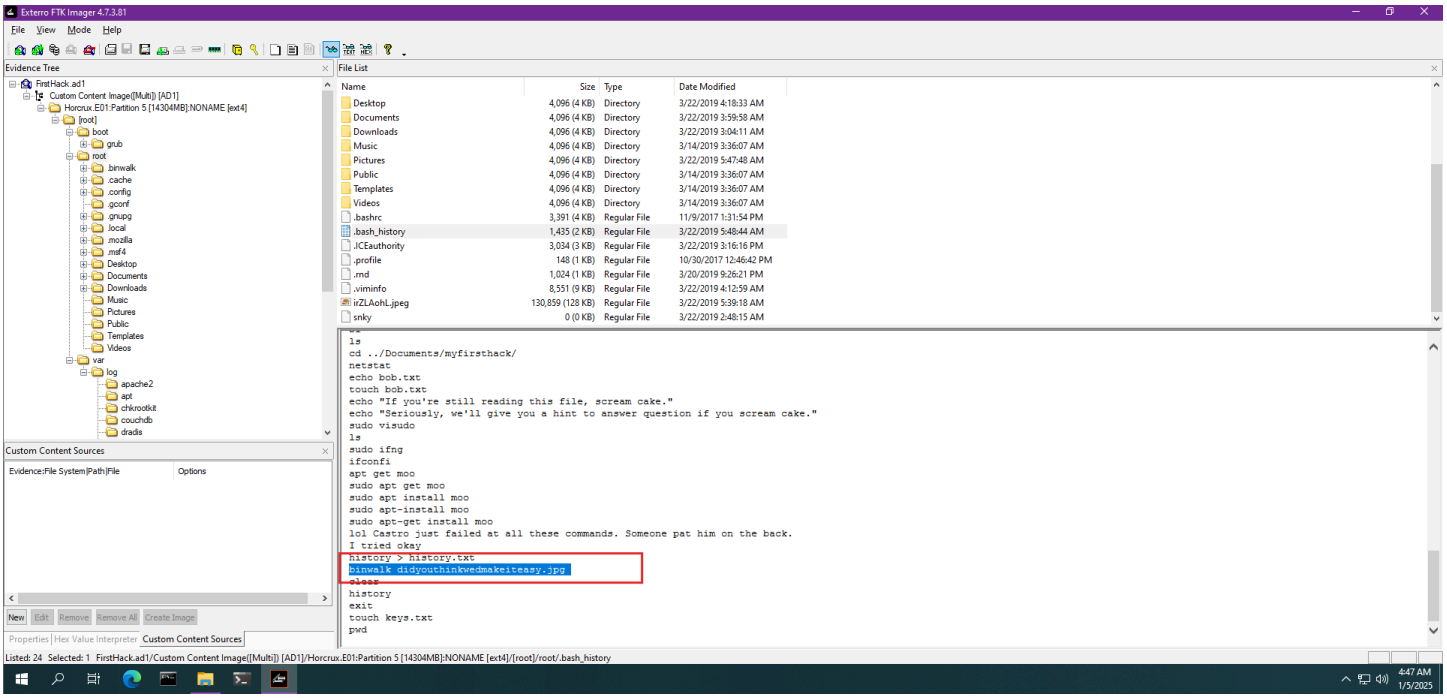
3.Found the command:
snky > /root/Desktop/SuperSecretFile.txt

Answer: /root/Desktop/SuperSecretFile.txt

✅ Q5 – What program used didyouthinkwedmakeiteasy.jpg during execution?

Approach:

1. Reviewed /root/.bash_history.
2. Found this execution command:
   binwalk didyouthinkwedmakeiteasy.jpg

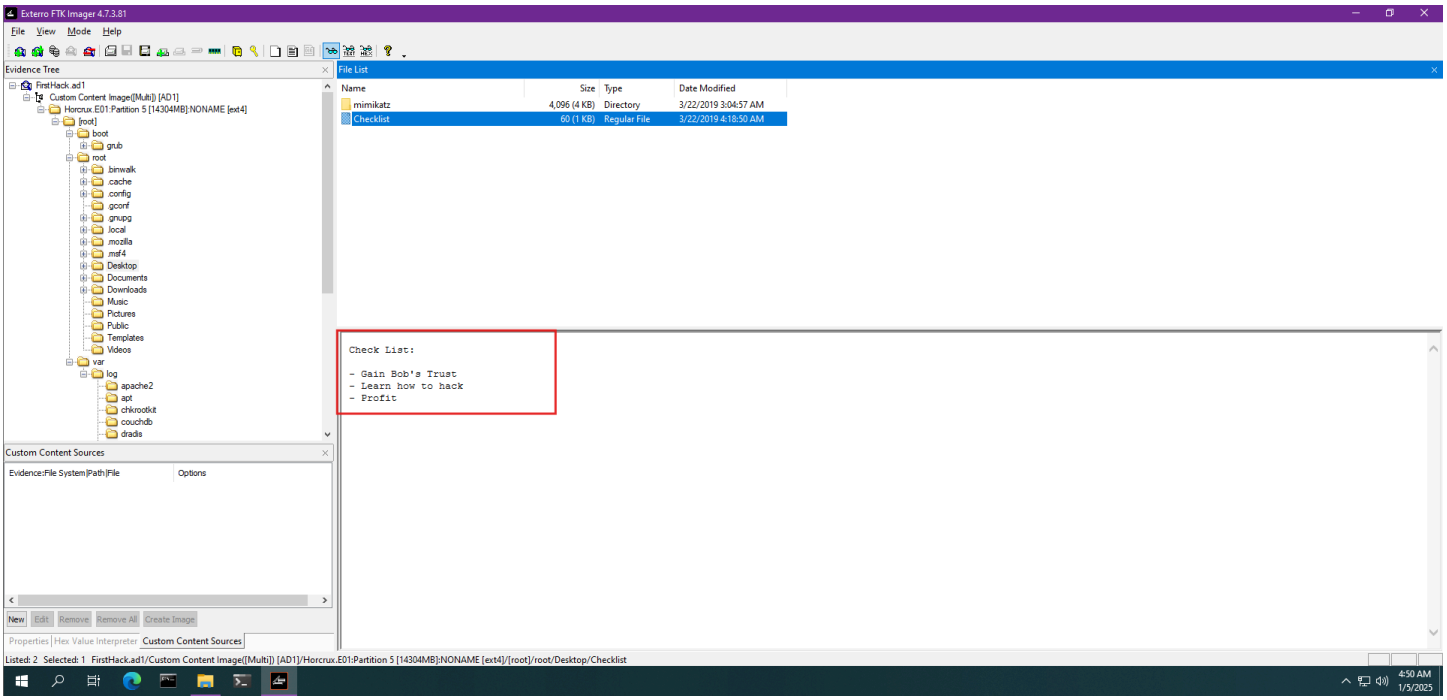


Answer: binwalk

✅ Q6 – What is the third goal from the checklist Karen created?

Approach:

1. Navigated to: /root/Desktop/Checklist
2. Opened the file and found the following list:
   - Gain Bob's Trust
   - Learn how to hack
   - **Profit** ← third item



Answer: Profit

✅ Q7 – How many times was Apache run?

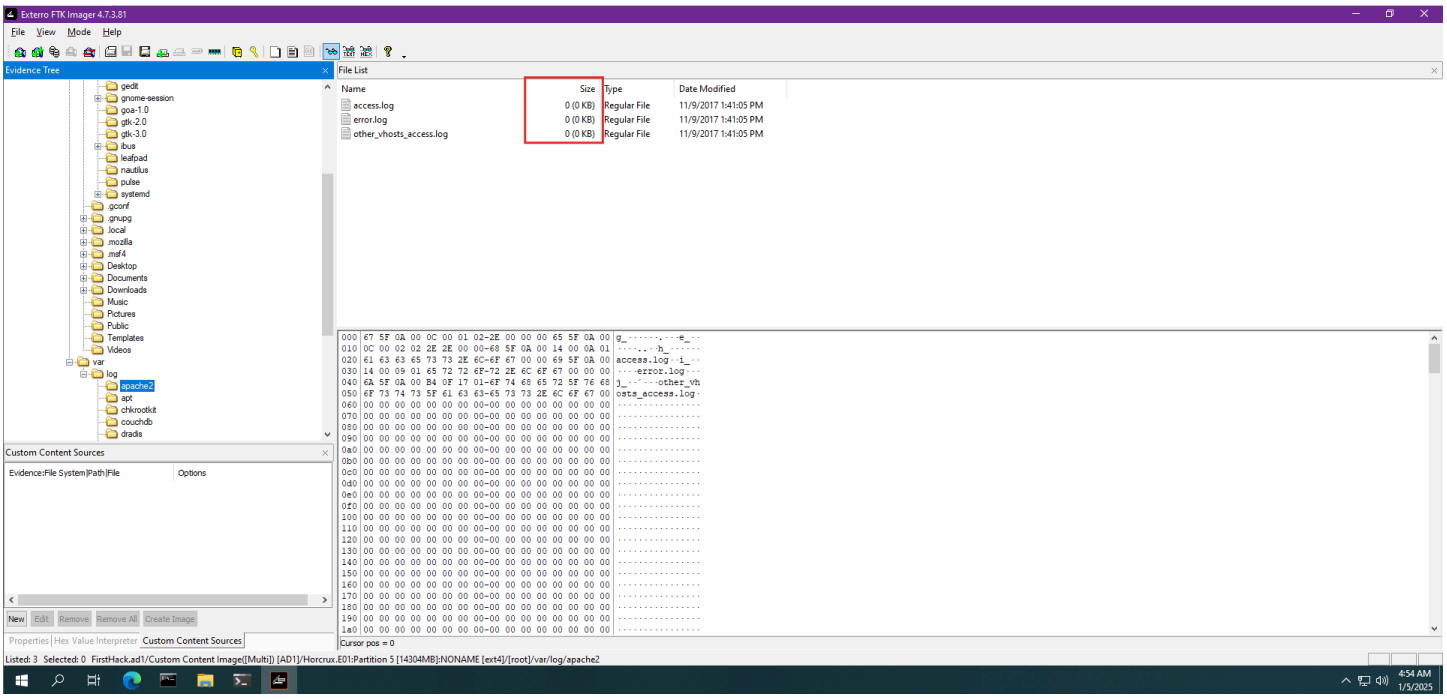
Approach:

Navigated to: /var/log/apache2/

Checked the following log files:

- access.log
- error.log
- other_vhosts_access.log

  All files were empty (0 KB), indicating no recorded activity.



Answer: 0

✅ Q8 – It is believed this machine was used to attack another. What file proves this?

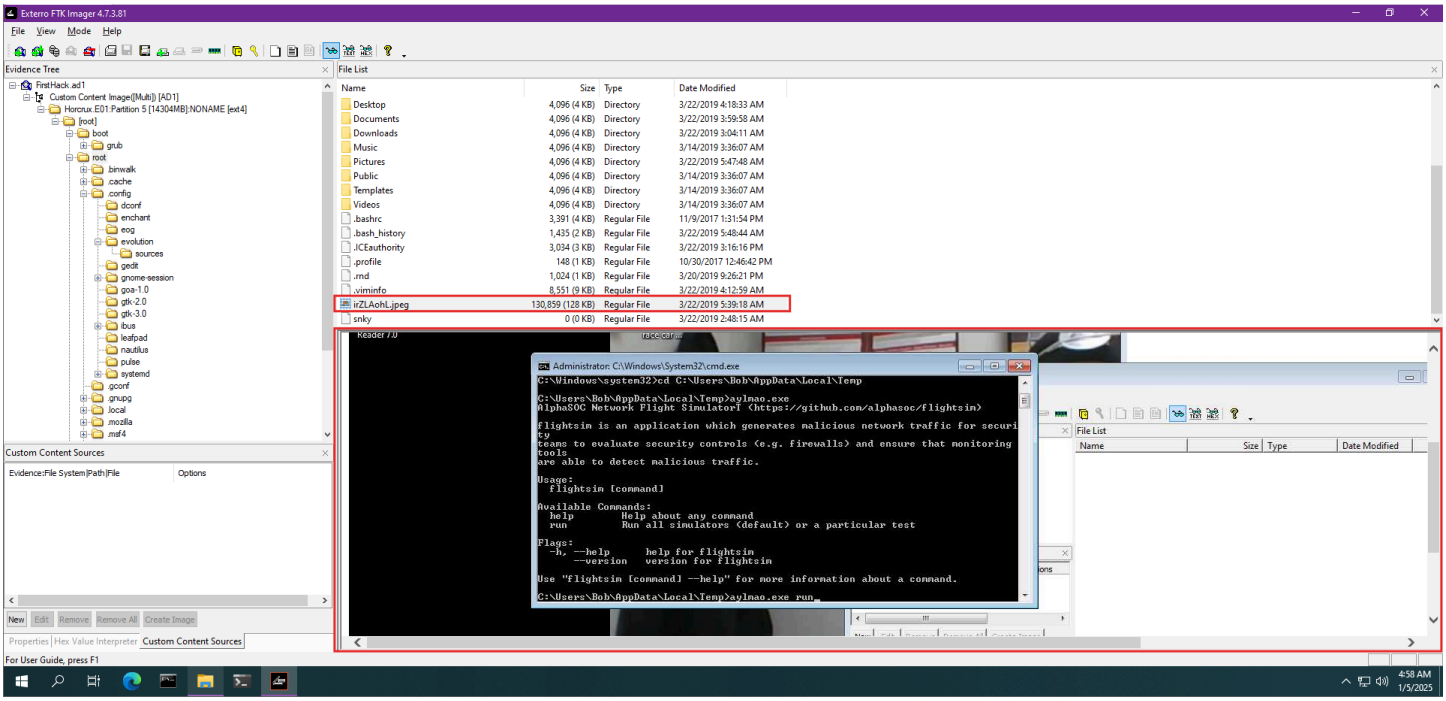
Approach:

Discovered a suspicious file named irZLAohL.jpeg in /root/

Also found evidence of a program flightSim.exe being executed in:

C:\Users\Bob\AppData\Local\Temp

The terminal showed the command: flightSim.exe run, which is used to simulate attacks.



Answer: irZLAohL.jpeg

✅ Q9 – Within the Documents file path, it is believed that Karen was taunting a fellow computer expert through a bash script. Who was Karen taunting?

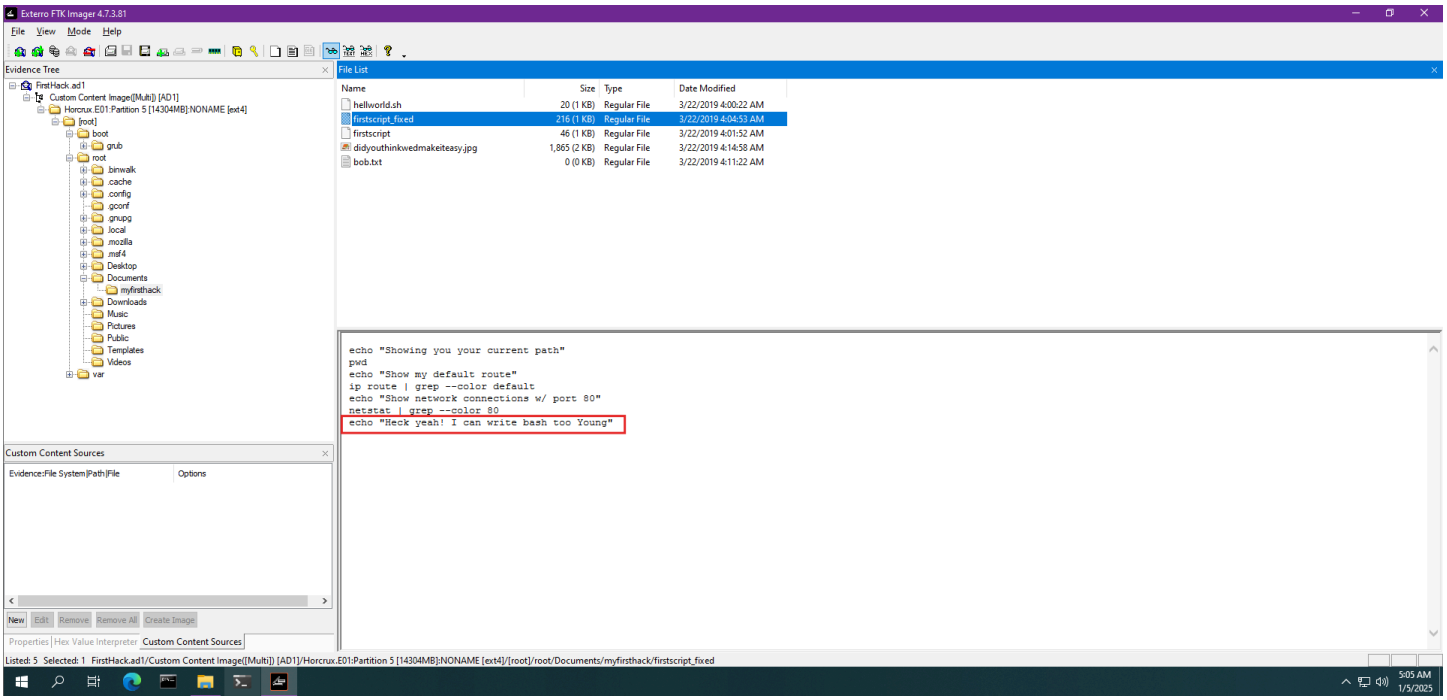
Approach:

Navigated to: /root/Documents/myfirsthack/

Opened the file: firstscript_fixed

At the end of the script, found the line:

echo "Heck yeah! I can write bash too Young"



Answer: Young

✅ Q10 – A user su'd to root at 11:26 multiple times. Who was it?

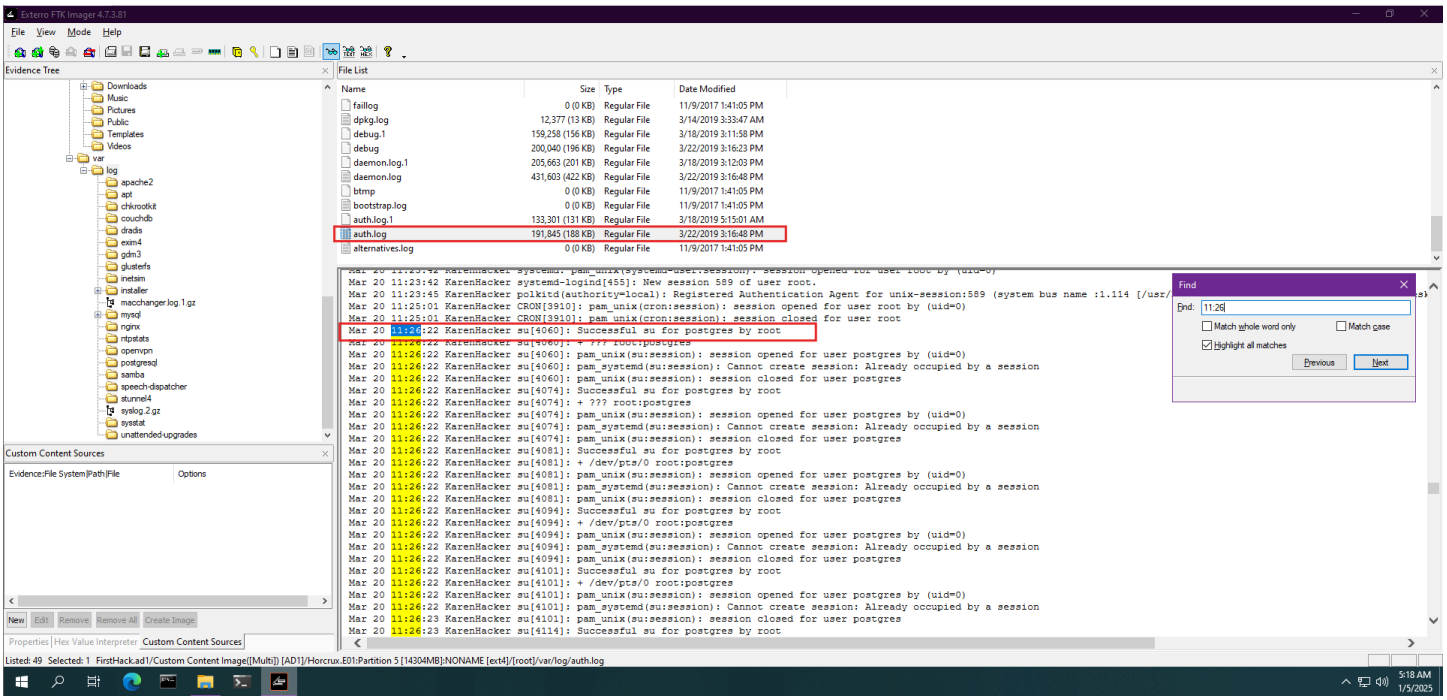
Approach:

Opened /var/log/auth.log

Found the following log entry:

Mar 20 11:26:22 KarenHacker su[4060]: Successful su for postgres by root

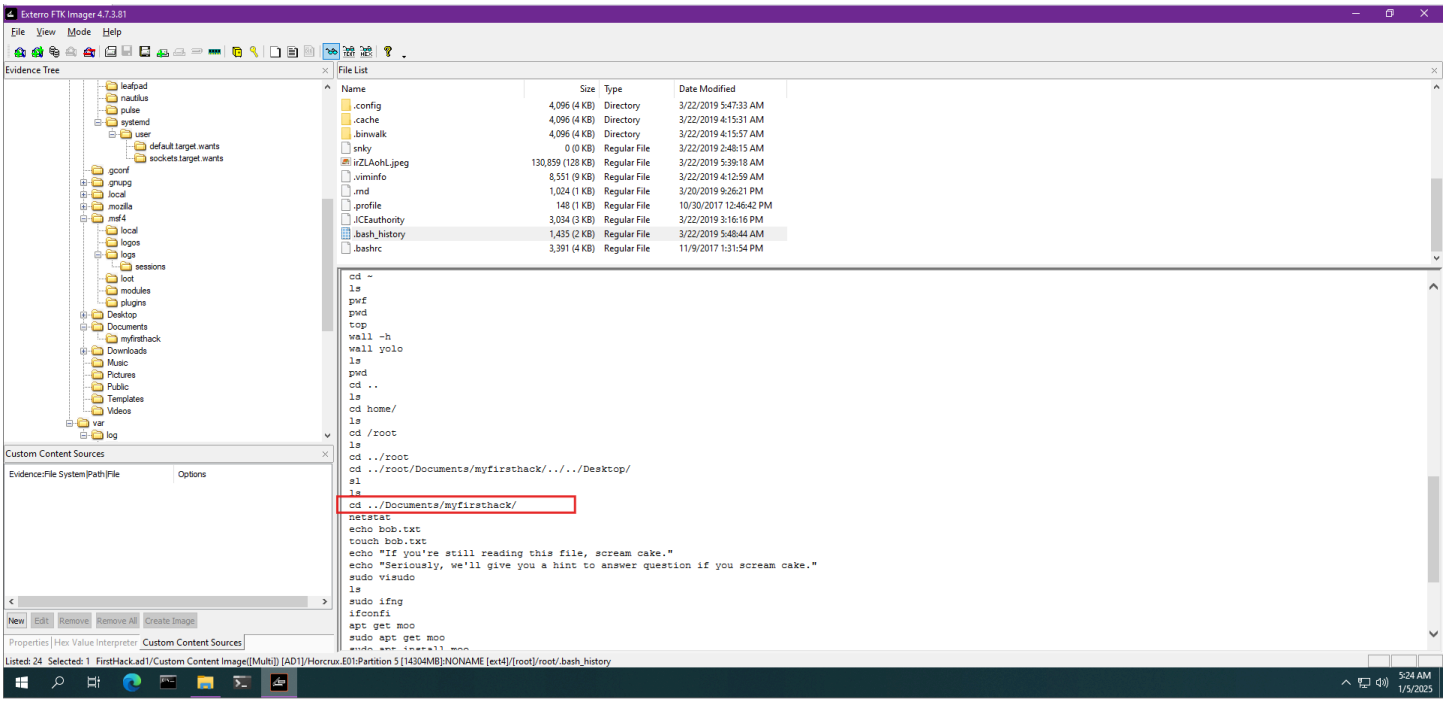
This indicates that user KarenHacker successfully used su to switch to postgres.



Answer: postgres.

✅ Q11 – Based on the bash history, what is the current working directory?

Approach:
Opened .bash_history
Found the command:
cd ../Documents/myfirsthack/
This indicates navigation into /root/Documents/myfirsthack/



Answer: /root/Documents/myfirsthack/

Conclusion

The challenge was approached using a systematic forensic process relying solely on **FTK Imager** for evidence acquisition, image browsing, and file hash validation. The tool provided sufficient access to directories, user activity logs, and configuration files to answer all challenge questions accurately.