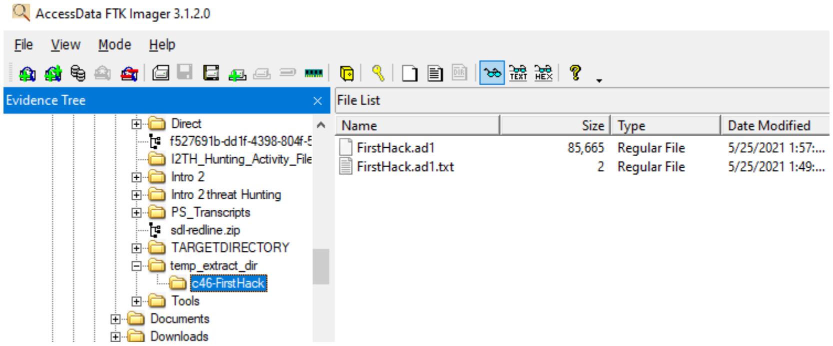
Insider Lab - Walk through

Created	@August 1, 2025 2:55 AM

Introduction

In this lab, you will take on the role of a Security Operations Center (SOC) analyst tasked with investigating suspicious activities conducted by an employee named Karen. Karen is suspected of engaging in unauthorized and potentially illegal actions within her organization, TAAUSAI. The investigation is based on a forensic disk image of Karen's Linux-based workstation, which is analyzed to uncover evidence of malicious activity.

The walkthrough demonstrates how to investigate insider threats by examining system logs, Bash history, downloaded files, and artifacts using FTK Imager. It highlights practical techniques for analyzing file integrity, identifying privilege escalation, and uncovering potential attacks. By the end of this lab, you will gain insights into endpoint forensics, log analysis, and the importance of monitoring insider threats to secure organizational systems.

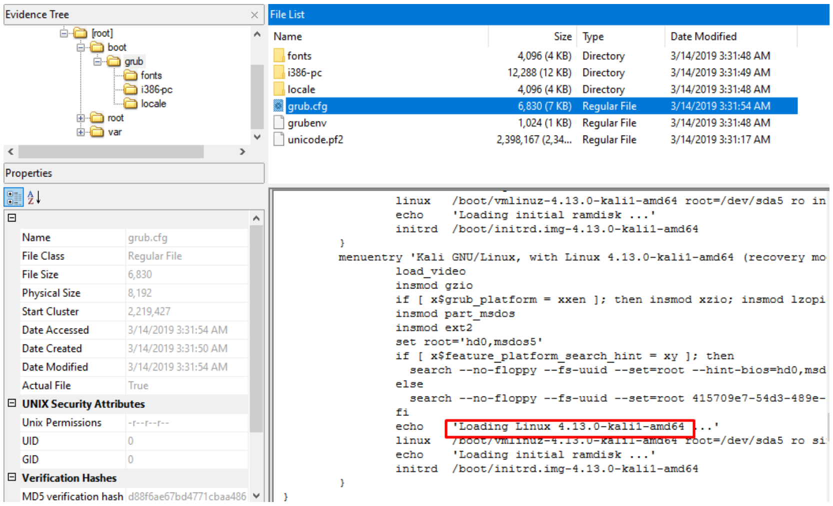


Name	Size	Type	Date Modified
FirstHack.ad1	85,665	Regular File	5/25/2021 1:57:...
FirstHack.ad1.txt	2	Regular File	5/25/2021 1:49:...

Analysis

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

To determine the Linux distribution being used on this machine, we begin by examining the file system captured in the disk image using FTK Imager. After loading the disk image, we navigate through the directory structure to locate logs or configuration files that can reveal system information. A good starting point is the /var/log/ directory, which often contains logs related to system activities and installation details.



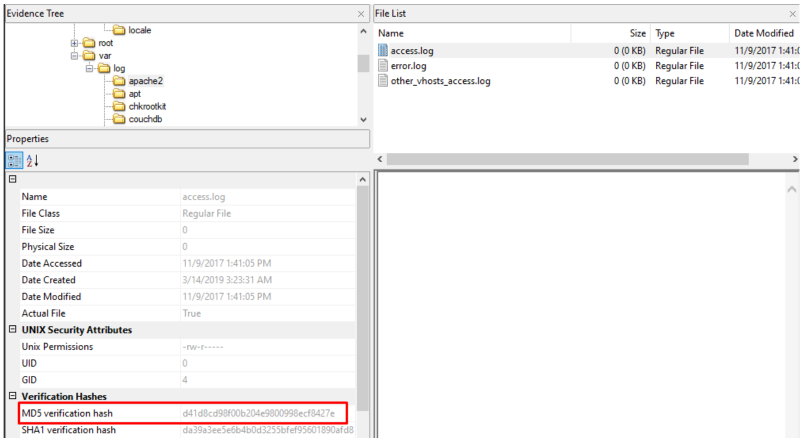
Name	Size	Type	Date Modified
fonts	4,096 (4 KB)	Directory	3/14/2019 3:31:48 AM
i386-pc	12,288 (12 KB)	Directory	3/14/2019 3:31:49 AM
locale	4,096 (4 KB)	Directory	3/14/2019 3:31:48 AM
grub.cfg	6,830 (7 KB)	Regular File	3/14/2019 3:31:54 AM
grubenv	1,024 (1 KB)	Regular File	3/14/2019 3:31:48 AM
unicode.pf2	2,398,167 (2,34...	Regular File	3/14/2019 3:31:17 AM

Name	grub.cfg
File Class	Regular File
File Size	6,830
Physical Size	8,192
Start Cluster	2,219,427
Date Accessed	3/14/2019 3:31:54 AM
Date Created	3/14/2019 3:31:50 AM
Date Modified	3/14/2019 3:31:54 AM
Actual File	True
UNIX Security Attributes	
Unix Permissions	-r--r--r--
UID	0
GID	0
Verification Hashes	
MD5 verification hash	d88f6ae67bd4771cbaa486

```
                linux   /boot/vmlinuz-4.13.0-kali1-amd64 root=/dev/sda5 ro in
                echo    'Loading initial ramdisk ...'
                initrd  /boot/initrd.img-4.13.0-kali1-amd64
        }
        menuentry 'Kali GNU/Linux, with Linux 4.13.0-kali1-amd64 (recovery mo
                load_video
                insmod gzio
                if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopi
                insmod part_msdos
                insmod ext2
                set root='hd0,msdos5'
                if [ x$feature_platform_search_hint = xy ]; then
                  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msd
                else
                  search --no-floppy --fs-uuid --set=root 415709e7-54d3-489e-
                fi
                echo    'Loading Linux 4.13.0-kali1-amd64 ...'
                linux   /boot/vmlinuz-4.13.0-kali1-amd64 root=/dev/sda5 ro si
                echo    'Loading initial ramdisk ...'
                initrd  /boot/initrd.img-4.13.0-kali1-amd64
        }
}
```

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

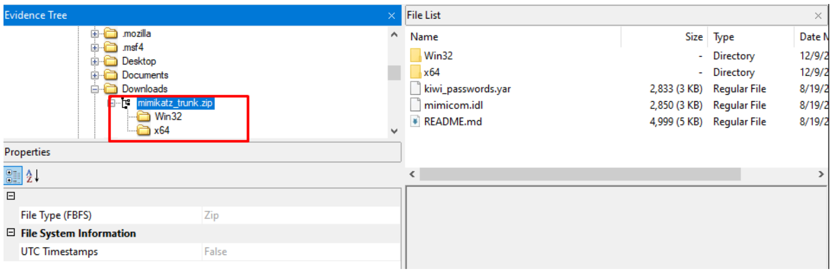
To find the MD5 hash of apache access.log we go to **"/var/log/apache2/access.log"** & see the properties tab.



Name	Size	Type	Date Modified
access.log	0 (0 KB)	Regular File	11/9/2017 1:41:(
error.log	0 (0 KB)	Regular File	11/9/2017 1:41:(
other_vhosts_access.log	0 (0 KB)	Regular File	11/9/2017 1:41:(

Name	access.log
File Class	Regular File
File Size	0
Physical Size	0
Date Accessed	11/9/2017 1:41:05 PM
Date Created	3/14/2019 3:23:31 AM
Date Modified	11/9/2017 1:41:05 PM
Actual File	True
UNIX Security Attributes	
Unix Permissions	-rw-r-----
UID	0
GID	4
Verification Hashes	
MD5 verification hash	d41d8cd98f00b204e9800998ecf8427e
SHA1 verification hash	da39a3ee5e6b4b0d3255bfef95601890afd8

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



Evidence Tree

- .mozilla
- .msf4
- Desktop
- Documents
- Downloads
  - mimikatz_trunk.zip
    - Win32
    - x64

File List

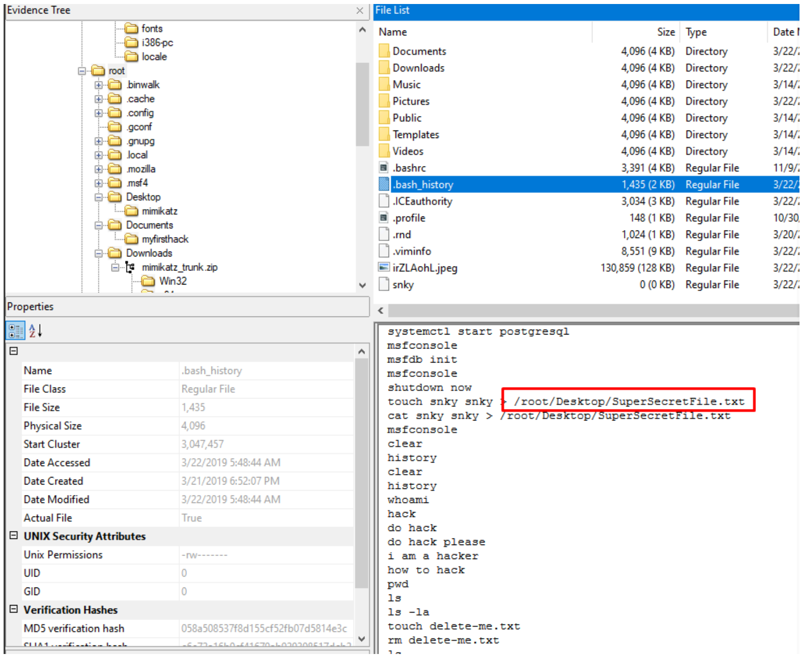
Name	Size	Type	Date M
Win32	-	Directory	12/9/2
x64	-	Directory	12/9/2
kiwi_passwords.yar	2,833 (3 KB)	Regular File	8/19/2
mimicom.idl	2,850 (3 KB)	Regular File	8/19/2
README.md	4,999 (5 KB)	Regular File	8/19/2

Properties

File Type (FBFS)	Zip
File System Information	
UTC Timestamps	False

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

To find this we have to check the bash_history file.



Evidence Tree

- fonts
- i386-pc
- locale
- root
  - .binwalk
  - .cache
  - .config
  - .gconf
  - .gnupg
  - .local
  - .mozilla
  - .msf4
  - Desktop
    - mimikatz
  - Documents
    - myfirsthack
  - Downloads
    - mimikatz_trunk.zip
      - Win32

File List

Name	Size	Type	Date I
Documents	4,096 (4 KB)	Directory	3/22/
Downloads	4,096 (4 KB)	Directory	3/22/
Music	4,096 (4 KB)	Directory	3/14/
Pictures	4,096 (4 KB)	Directory	3/22/
Public	4,096 (4 KB)	Directory	3/14/
Templates	4,096 (4 KB)	Directory	3/14/
Videos	4,096 (4 KB)	Directory	3/14/
.bashrc	3,391 (4 KB)	Regular File	11/9/
.bash_history	1,435 (2 KB)	Regular File	3/22/
.ICEauthority	3,034 (3 KB)	Regular File	3/22/
.profile	148 (1 KB)	Regular File	10/30,
.rnd	1,024 (1 KB)	Regular File	3/20/
.viminfo	8,551 (9 KB)	Regular File	3/22/
irZLAohL.jpeg	130,859 (128 KB)	Regular File	3/22/
snky	0 (0 KB)	Regular File	3/22/

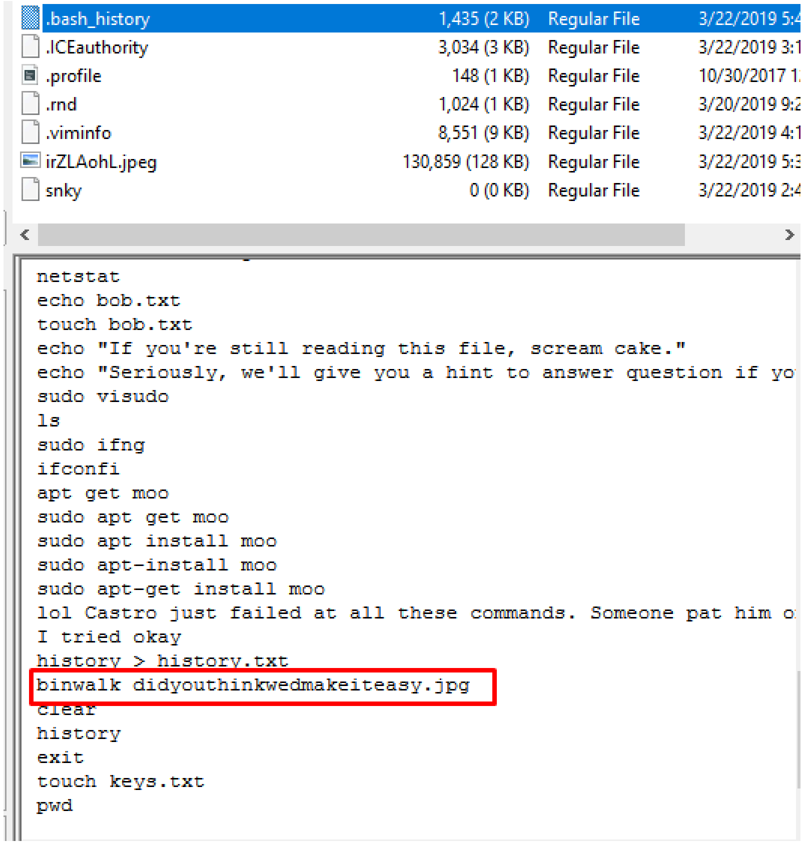
Properties

Name	.bash_history
File Class	Regular File
File Size	1,435
Physical Size	4,096
Start Cluster	3,047,457
Date Accessed	3/22/2019 5:48:44 AM
Date Created	3/21/2019 6:52:07 PM
Date Modified	3/22/2019 5:48:44 AM
Actual File	True
UNIX Security Attributes	
Unix Permissions	-rw-------
UID	0
GID	0
Verification Hashes	
MD5 verification hash	058a508537f8d155cf52fb07d5814e3c

```
systemctl start postgresql
msfconsole
msfdb init
msfconsole
shutdown now
touch snky snky > /root/Desktop/SuperSecretFile.txt
cat snky snky > /root/Desktop/SuperSecretFile.txt
msfconsole
clear
history
clear
history
whoami
hack
do hack
do hack please
i am a hacker
how to hack
pwd
ls
ls -la
touch delete-me.txt
rm delete-me.txt
```

Q.5) What program used didyouthinkwedmakeiteasy.jpg during execution?

To find this again we have to check the bash_history file.

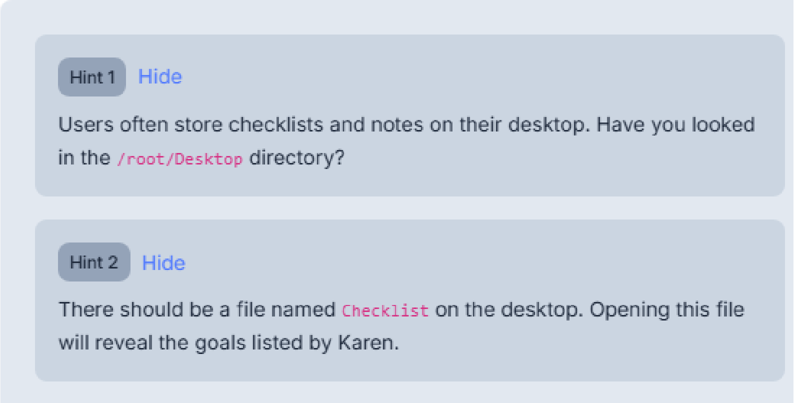


.bash_history	1,435 (2 KB)	Regular File	3/22/2019 5:4
.ICEauthority	3,034 (3 KB)	Regular File	3/22/2019 3:1
.profile	148 (1 KB)	Regular File	10/30/2017 1.
.rnd	1,024 (1 KB)	Regular File	3/20/2019 9:2
.viminfo	8,551 (9 KB)	Regular File	3/22/2019 4:1
irZLAohL.jpeg	130,859 (128 KB)	Regular File	3/22/2019 5:3
snky	0 (0 KB)	Regular File	3/22/2019 2:4

```
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 yo
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 o
I tried okay
history > history.txt
binwalk didyouthinkwedmakeiteasy.jpg
clear
history
exit
touch keys.txt
pwd
```

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

To find this we have to check the Desktop folder. After searching we find the location of the file as “**/root/Desktop/Checklist**”.

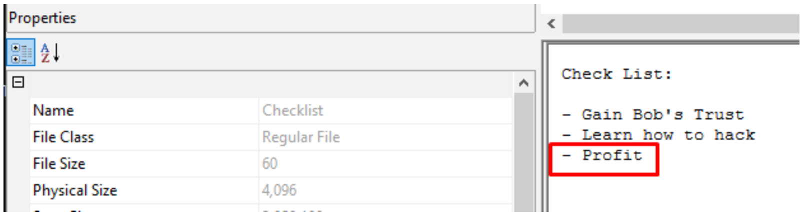


Hint 1 Hide

Users often store checklists and notes on their desktop. Have you looked in the `/root/Desktop` directory?

Hint 2 Hide

There should be a file named `Checklist` on the desktop. Opening this file will reveal the goals listed by Karen.

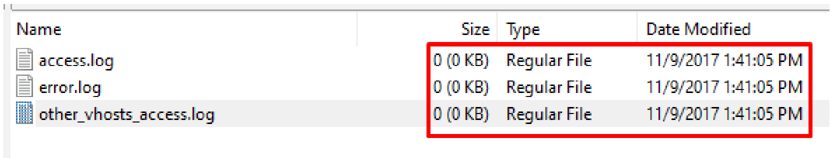


Name	Checklist
File Class	Regular File
File Size	60
Physical Size	4,096

```
Check List:

- Gain Bob's Trust
- Learn how to hack
- Profit
```

Q.7) How many times was apache run?

To find this we have to check the “**/var/log/apache2**” folder.

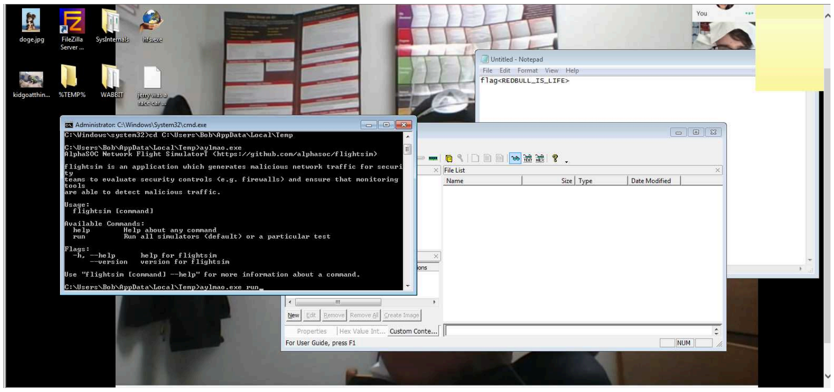


Name	Size	Type	Date Modified
access.log	0 (0 KB)	Regular File	11/9/2017 1:41:05 PM
error.log	0 (0 KB)	Regular File	11/9/2017 1:41:05 PM
other_vhosts_access.log	0 (0 KB)	Regular File	11/9/2017 1:41:05 PM

I believe apache was never run

Question 8: This machine was used to launch an attack on another. Which file contains the evidence for this?

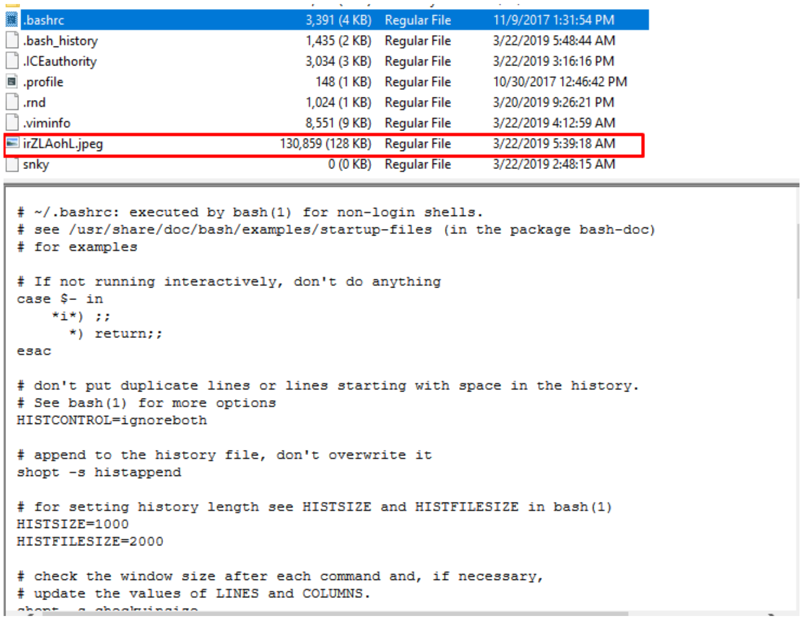
For **Question 8**, we need to determine which other machine Karen’s device attacked. As a starting point, let’s return to the `/root/.bash_history` file to search for any additional clues.



```
flag<REDBULL_IS_LIFE>
```

Administrator: C:\Windows\System32\cmd.exe

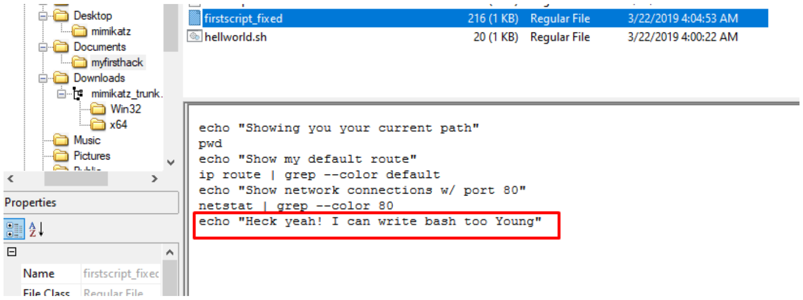
```
C:\Windows\system32>cd C:\Users\Bob\AppData\Local\Temp

C:\Users\Bob\AppData\Local\Temp>aylmao.exe
AlphaSOC Network Flight SimulatorT (https://github.com/alphasoc/flightsim)

flightsim is an application which generates malicious network traffic for securi
ty
teams to evaluate security controls (e.g. firewalls) and ensure that monitoring
tools
are able to detect malicious traffic.

Usage:
  flightsim [command]

Available Commands:
  help        Help about any command
  run         Run all simulators (default) or a particular test

Flags:
  -h, --help      help for flightsim
      --version   version for flightsim

Use "flightsim [command] --help" for more information about a command.

C:\Users\Bob\AppData\Local\Temp>aylmao.exe run_
```



```
.bashrc           3,391 (4 KB)     Regular File   11/9/2017 1:31:54 PM
.bash_history     1,435 (2 KB)     Regular File   3/22/2019 5:48:44 AM
.ICEauthority     3,034 (3 KB)     Regular File   3/22/2019 3:16:16 PM
.profile          148 (1 KB)       Regular File   10/30/2017 12:46:42 PM
.rnd              1,024 (1 KB)     Regular File   3/20/2019 9:26:21 PM
.viminfo          8,551 (9 KB)     Regular File   3/22/2019 4:12:59 AM
irZLAohL.jpeg     130,859 (128 KB) Regular File   3/22/2019 5:39:18 AM
snky              0 (0 KB)         Regular File   3/22/2019 2:48:15 AM
```

```
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
case $- in
    *i*) ;;
      *) return;;
esac

# don't put duplicate lines or lines starting with space in the history.
# See bash(1) for more options
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
```

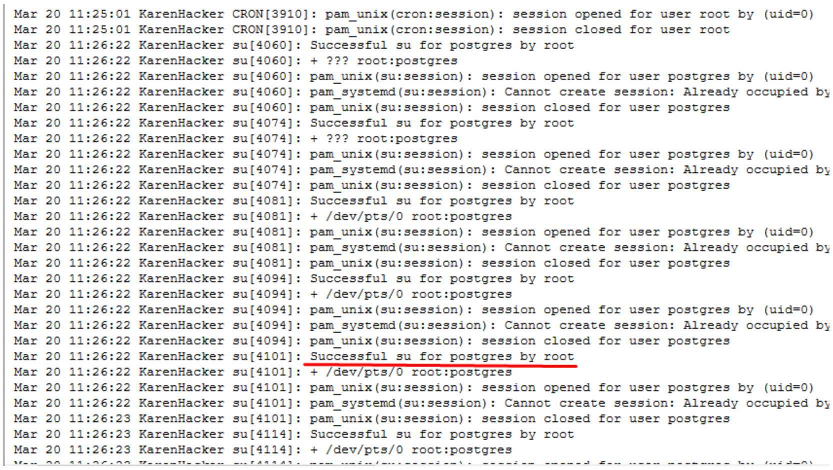
Q9 It is believed that Karen was taunting a fellow computer expert through a bash script within the Documents directory. Who was the expert that Karen was taunting?



```
firstscript_fixed   216 (1 KB)   Regular File   3/22/2019 4:04:53 AM
hellworld.sh        20 (1 KB)    Regular File   3/22/2019 4:00:22 AM
```

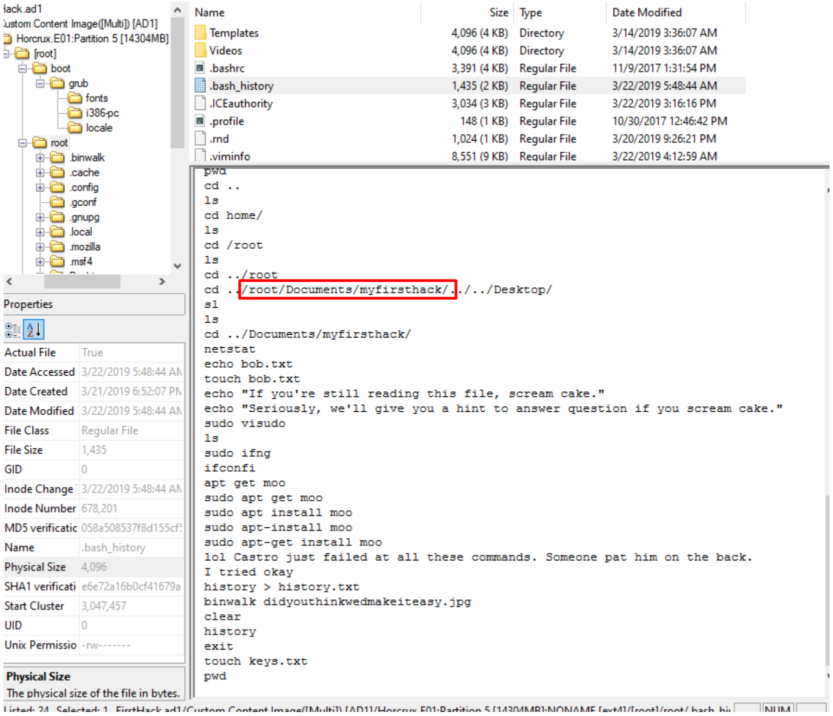
```
echo "Showing you your current path"
pwd
echo "Show my default route"
ip route | grep --color default
echo "Show network connections w/ port 80"
netstat | grep --color 80
echo "Heck yeah! I can write bash too Young"
```

Q10 A user executed the su command to gain root access multiple times at 11:26. Who was the user?



```
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
Mar 20 11:26:22 KarenHacker su[4060]: pam_unix(su:session): session opened for user postgres by (uid=0)
Mar 20 11:26:22 KarenHacker su[4060]: pam_systemd(su:session): Cannot create session: Already occupied by
Mar 20 11:26:22 KarenHacker su[4060]: pam_unix(su:session): session closed for user postgres
Mar 20 11:26:22 KarenHacker su[4074]: Successful su for postgres by root
Mar 20 11:26:22 KarenHacker su[4074]: + ??? root:postgres
Mar 20 11:26:22 KarenHacker su[4074]: pam_unix(su:session): session opened for user postgres by (uid=0)
Mar 20 11:26:22 KarenHacker su[4074]: pam_systemd(su:session): Cannot create session: Already occupied by
Mar 20 11:26:22 KarenHacker su[4074]: pam_unix(su:session): session closed for user postgres
Mar 20 11:26:22 KarenHacker su[4081]: Successful su for postgres by root
Mar 20 11:26:22 KarenHacker su[4081]: + /dev/pts/0 root:postgres
Mar 20 11:26:22 KarenHacker su[4081]: pam_unix(su:session): session opened for user postgres by (uid=0)
Mar 20 11:26:22 KarenHacker su[4081]: pam_systemd(su:session): Cannot create session: Already occupied by
Mar 20 11:26:22 KarenHacker su[4081]: pam_unix(su:session): session closed for user postgres
Mar 20 11:26:22 KarenHacker su[4094]: Successful su for postgres by root
Mar 20 11:26:22 KarenHacker su[4094]: + /dev/pts/0 root:postgres
Mar 20 11:26:22 KarenHacker su[4094]: pam_unix(su:session): session opened for user postgres by (uid=0)
Mar 20 11:26:22 KarenHacker su[4094]: pam_systemd(su:session): Cannot create session: Already occupied by
Mar 20 11:26:22 KarenHacker su[4094]: pam_unix(su:session): session closed for user postgres
Mar 20 11:26:22 KarenHacker su[4101]: Successful su for postgres by root
Mar 20 11:26:22 KarenHacker su[4101]: + /dev/pts/0 root:postgres
Mar 20 11:26:22 KarenHacker su[4101]: pam_unix(su:session): session opened for user postgres by (uid=0)
Mar 20 11:26:22 KarenHacker su[4101]: pam_systemd(su:session): Cannot create session: Already occupied by
Mar 20 11:26:23 KarenHacker su[4101]: pam_unix(su:session): session closed for user postgres
Mar 20 11:26:23 KarenHacker su[4114]: Successful su for postgres by root
Mar 20 11:26:23 KarenHacker su[4114]: + /dev/pts/0 root:postgres
```

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



Name	Size	Type	Date Modified
Templates	4,096 (4 KB)	Directory	3/14/2019 3:36:07 AM
Videos	4,096 (4 KB)	Directory	3/14/2019 3:36:07 AM
.bashrc	3,391 (4 KB)	Regular File	11/9/2017 1:31:54 PM
.bash_history	1,435 (2 KB)	Regular File	3/22/2019 5:48:44 AM
.ICEauthority	3,034 (3 KB)	Regular File	3/22/2019 3:16:16 PM
.profile	148 (1 KB)	Regular File	10/30/2017 12:46:42 PM
.rnd	1,024 (1 KB)	Regular File	3/20/2019 9:26:21 PM
.viminfo	8,551 (9 KB)	Regular File	3/22/2019 4:12:59 AM

Actual File	True
Date Accessed	3/22/2019 5:48:44 AN
Date Created	3/21/2019 6:52:07 PN
Date Modified	3/22/2019 5:48:44 AN
File Class	Regular File
File Size	1,435
GID	0
Inode Change	3/22/2019 5:48:44 AN
Inode Number	678,201
MD5 verificatic	058a508537f8d155cf!
Name	.bash_history
Physical Size	4,096
SHA1 verificati	e6e72a16b0cf41679a
Start Cluster	3,047,457
UID	0
Unix Permissio	-rw-------

Physical Size
The physical size of the file in bytes.

```
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 FirstHack.ad1/Custom Content Image([Multi]) [AD1]/Horcrux.E01:Partition 5 [14304MB]:NONAME [ext4]/[root]/root/.bash_hi NUM