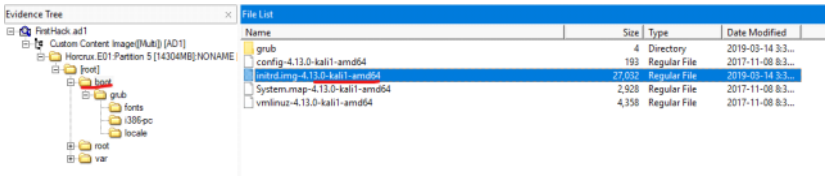
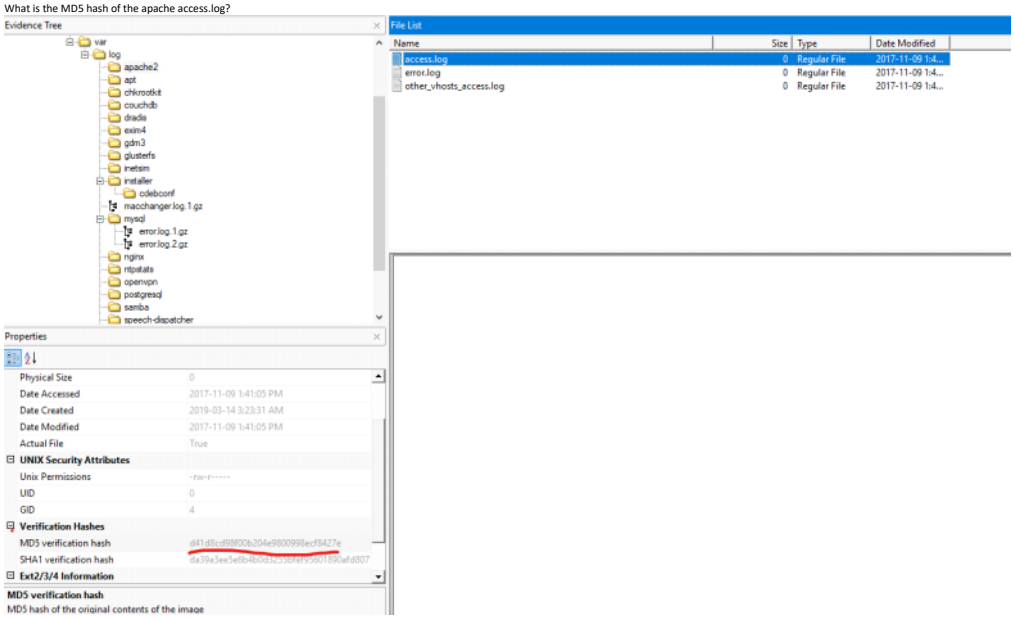
Insider

Saturday, 23 April, 2022 6:17 AM

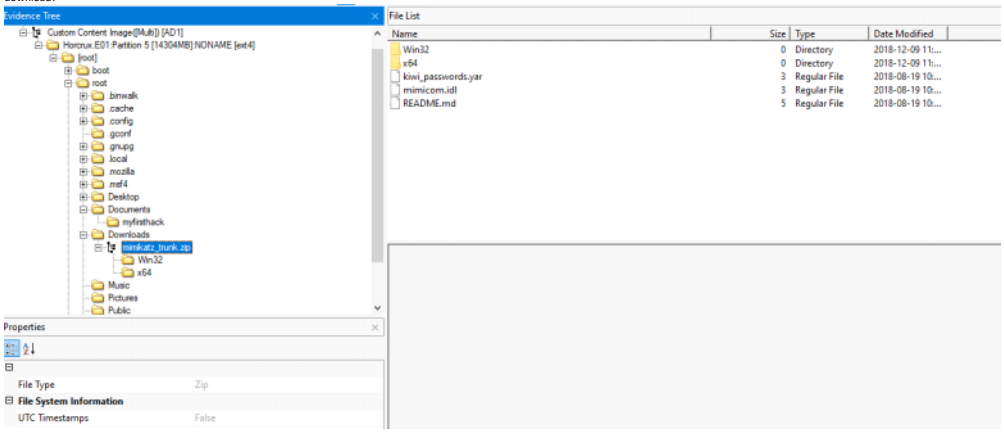
What distribution of Linux is being used on this machine?



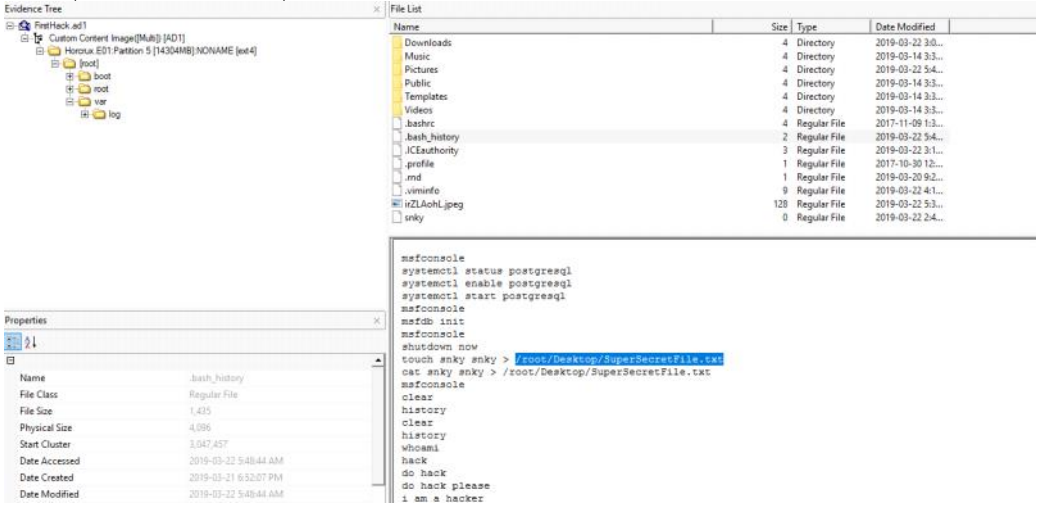
What is the MD5 hash of the apache access.log?



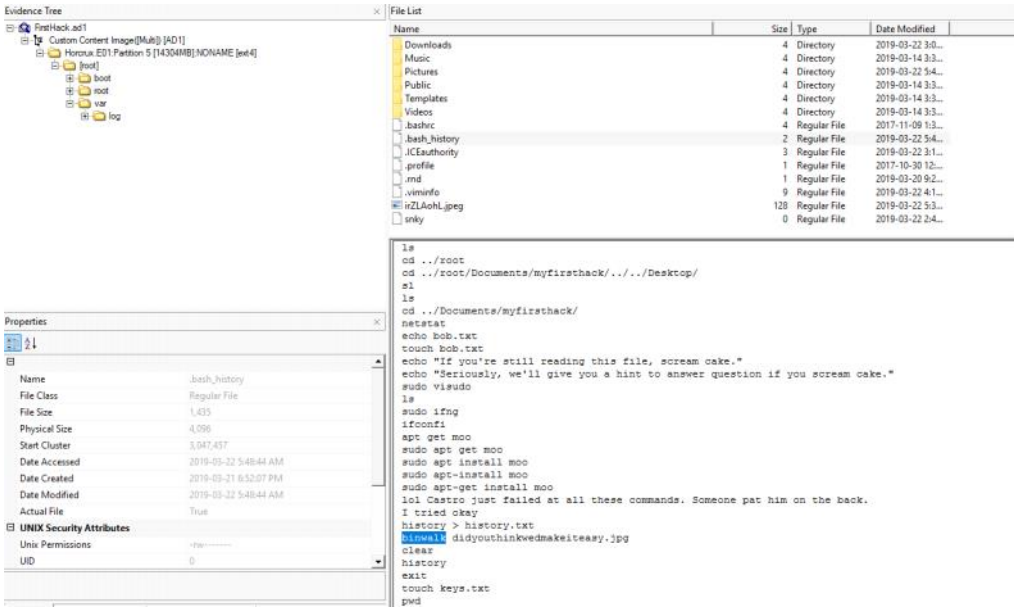
It is believed that a credential dumping tool was downloaded? What is the file name of the download?



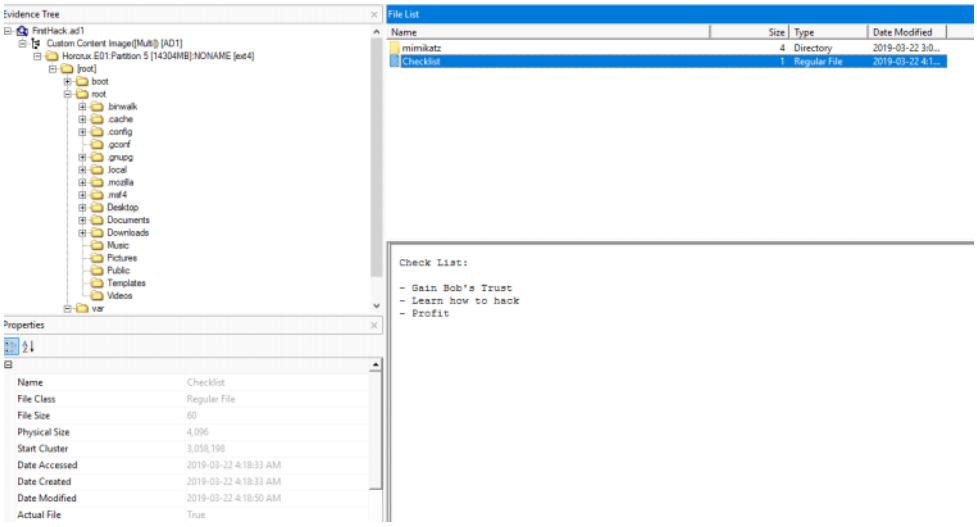
There was a super-secret file created. What is the absolute path?



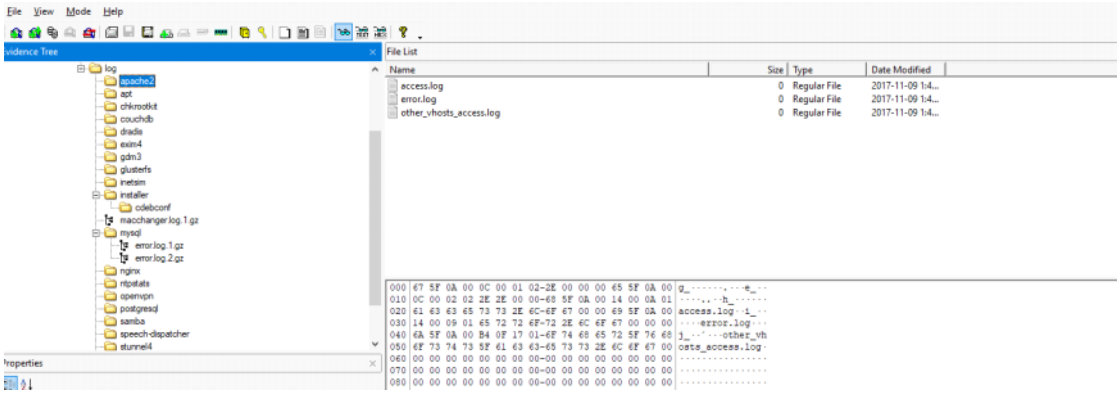
What program used didyouthinkwedmakeiteasy.jpg during execution?



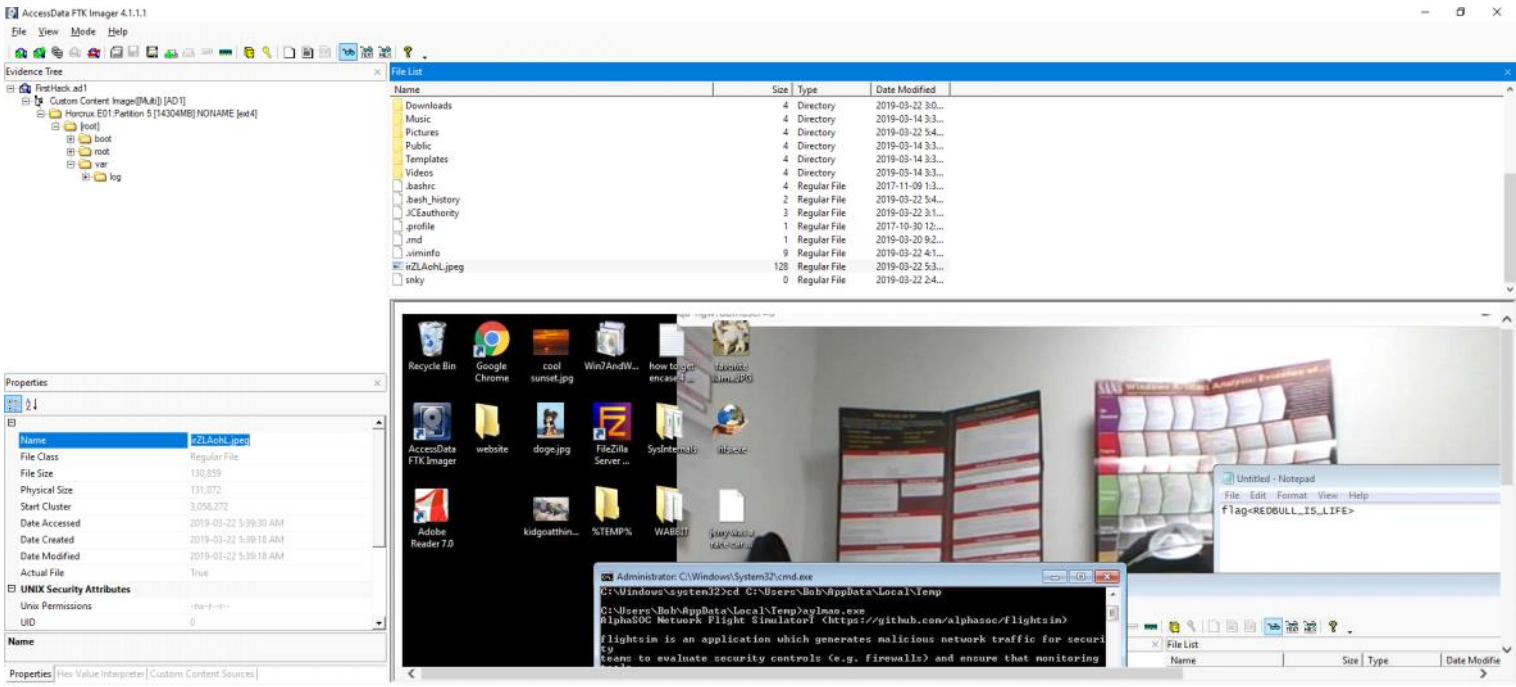
What is the third goal from the checklist Karen created?



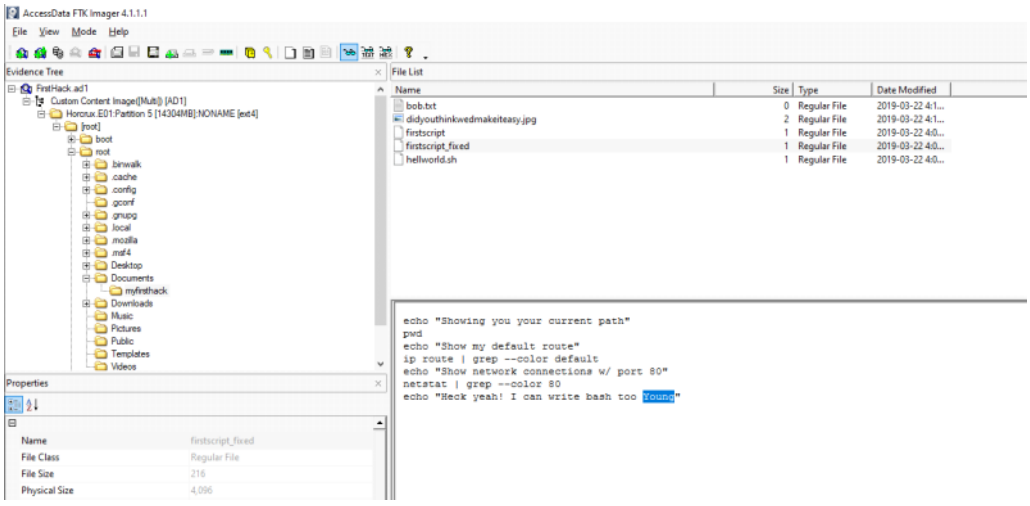
How many times was apache run? Apache did not run



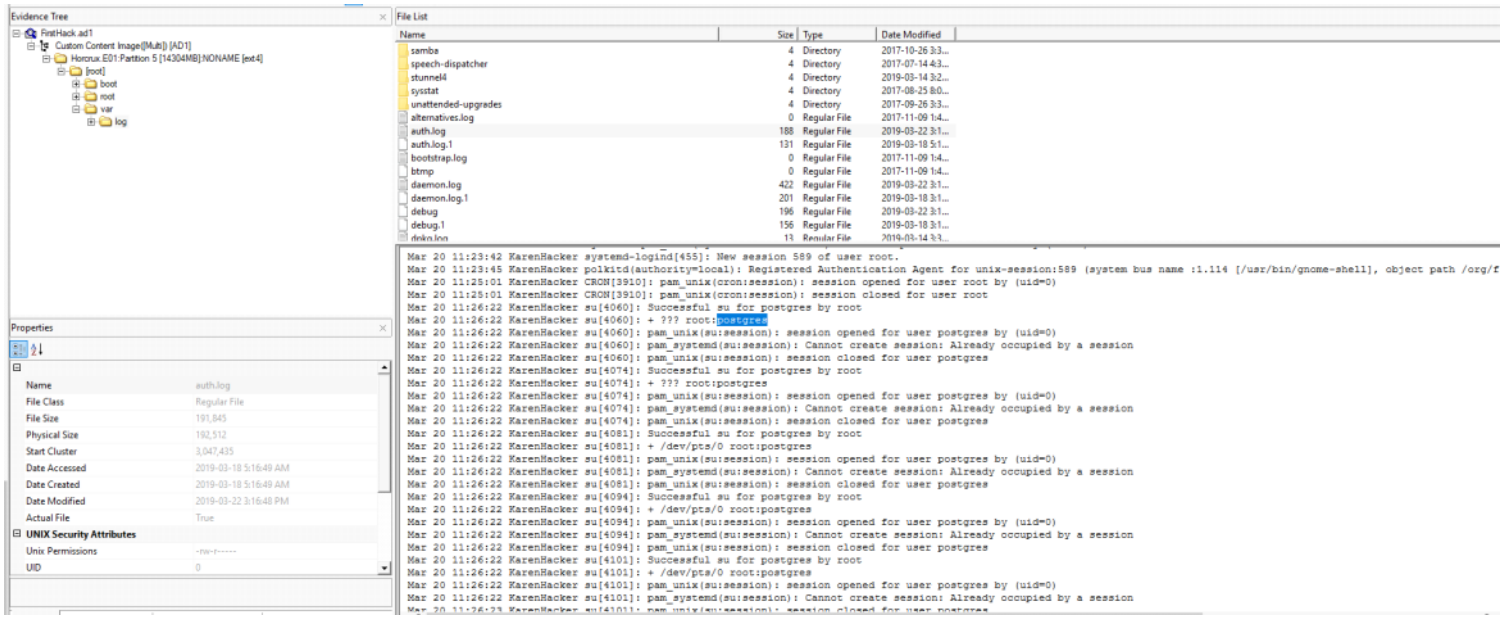
It is believed this machine was used to attack another. What file proves this?



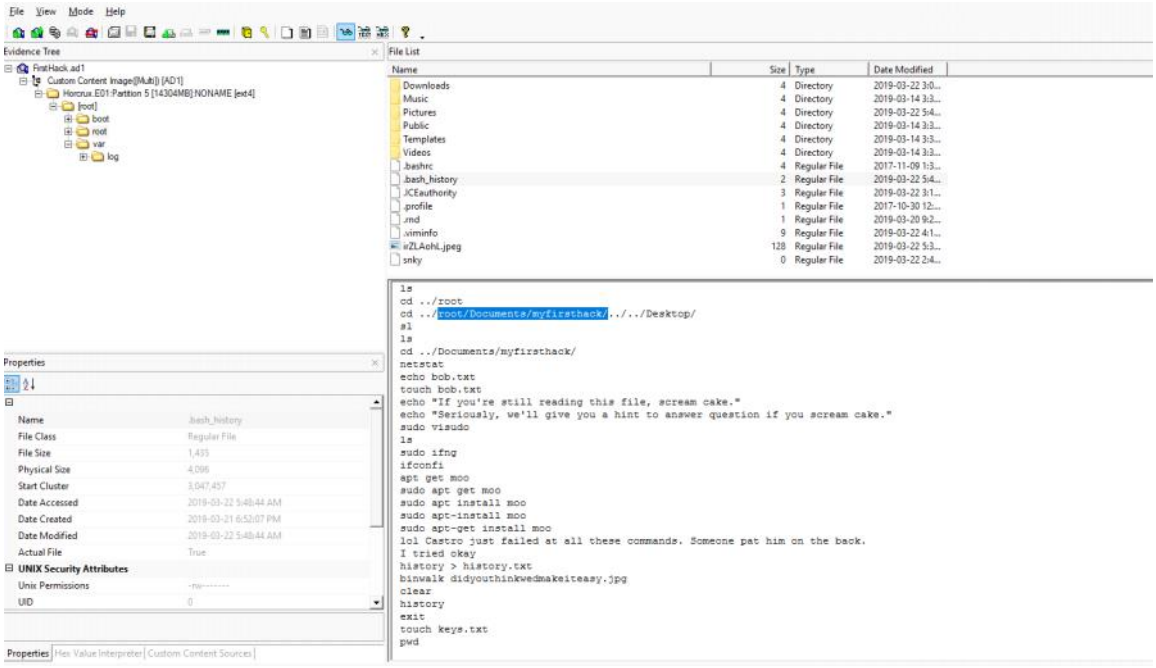
Within the Documents file path, it is believed that Karen was taunting a fellow computer expert through a bash script. Who was Karen taunting?



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



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


File View Mode Help
Evidence Tree
FirstHack.ad1
Custom Content Image([Multi]) [AD1]
Horcrux.E01:Partition 5 [14304MB]:NONAME [ext4]
[root]
boot
root
var
log
File List
Name Size Type Date Modified
Downloads 4 Directory 2019-03-22 3:0...
Music 4 Directory 2019-03-14 3:3...
Pictures 4 Directory 2019-03-22 5:4...
Public 4 Directory 2019-03-14 3:3...
Templates 4 Directory 2019-03-14 3:3...
Videos 4 Directory 2019-03-14 3:3...
.bashrc 4 Regular File 2017-11-09 1:3...
.bash_history 2 Regular File 2019-03-22 5:4...
.ICEauthority 3 Regular File 2019-03-22 3:1...
.profile 1 Regular File 2017-10-30 12:...
.rnd 1 Regular File 2019-03-20 9:2...
.viminfo 9 Regular File 2019-03-22 4:1...
#ZLAohL.jpeg 128 Regular File 2019-03-22 5:3...
snky 0 Regular File 2019-03-22 2:4...
ls
cd ../root
cd .../root/Documents/myfirsthack/../../Desktop/
#1
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
Properties
Name .bash_history
File Class Regular File
File Size 1,433
Physical Size 4,096
Start Cluster 3,047,457
Date Accessed 2019-03-22 5:48:44 AM
Date Created 2019-03-21 6:52:07 PM
Date Modified 2019-03-22 5:48:44 AM
Actual File True
UNIX Security Attributes
Unix Permissions -rw-------
UID 0
Properties Hex Value Interpreter Custom Content Sources