# Conducting Forensic Investigations on Linux Systems (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 06

| | |
|---|---|
| Student: | Email: |
| Samman Chouhan | schouhan1@hawk.iit.edu |

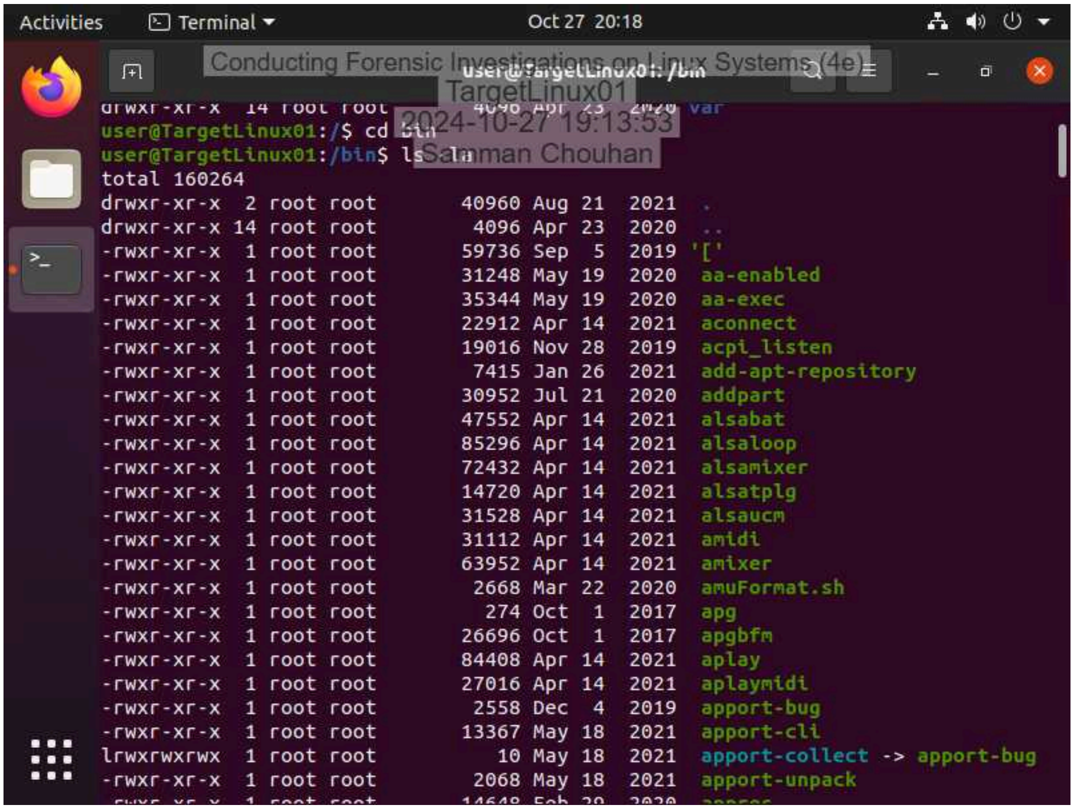
| | |
|---|---|
| Time on Task: | Progress: |
| 1 hour, 23 minutes | 100% |

Report Generated: Sunday, October 27, 2024 at 9:36 PM

## Section 1: Hands-On Demonstration

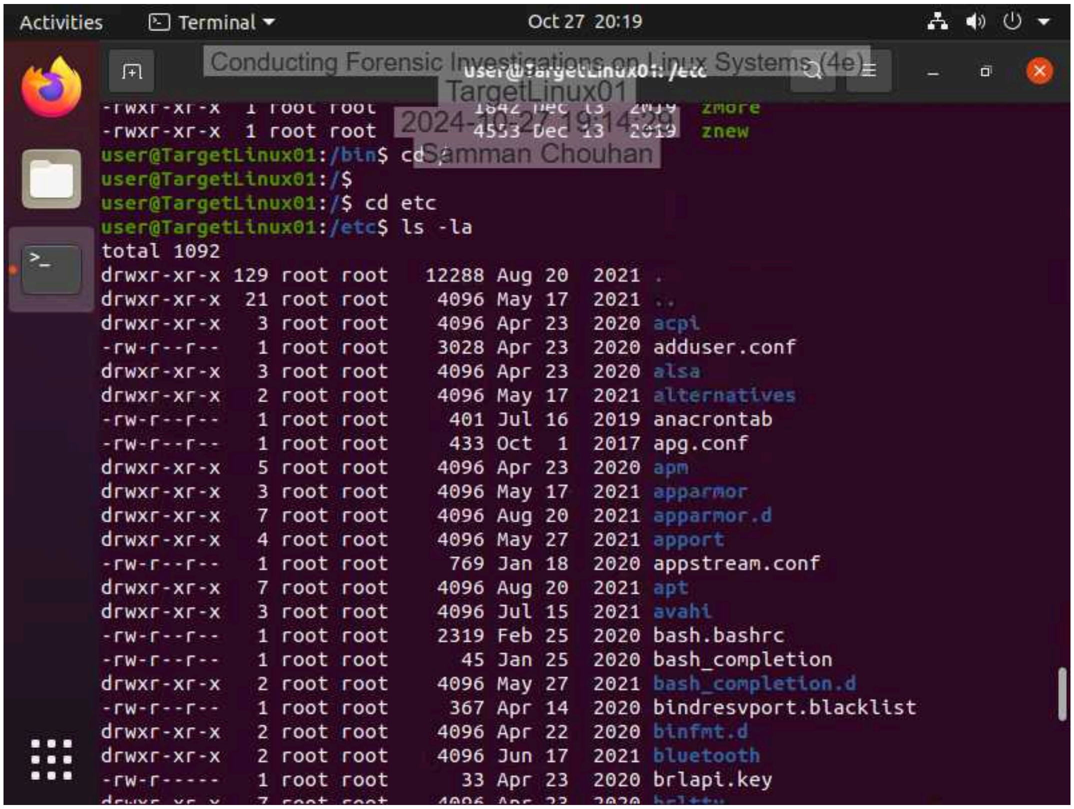
### Part 1: Explore a Live Linux System

17. **Make a screen capture** showing the **contents of the /bin directory**.



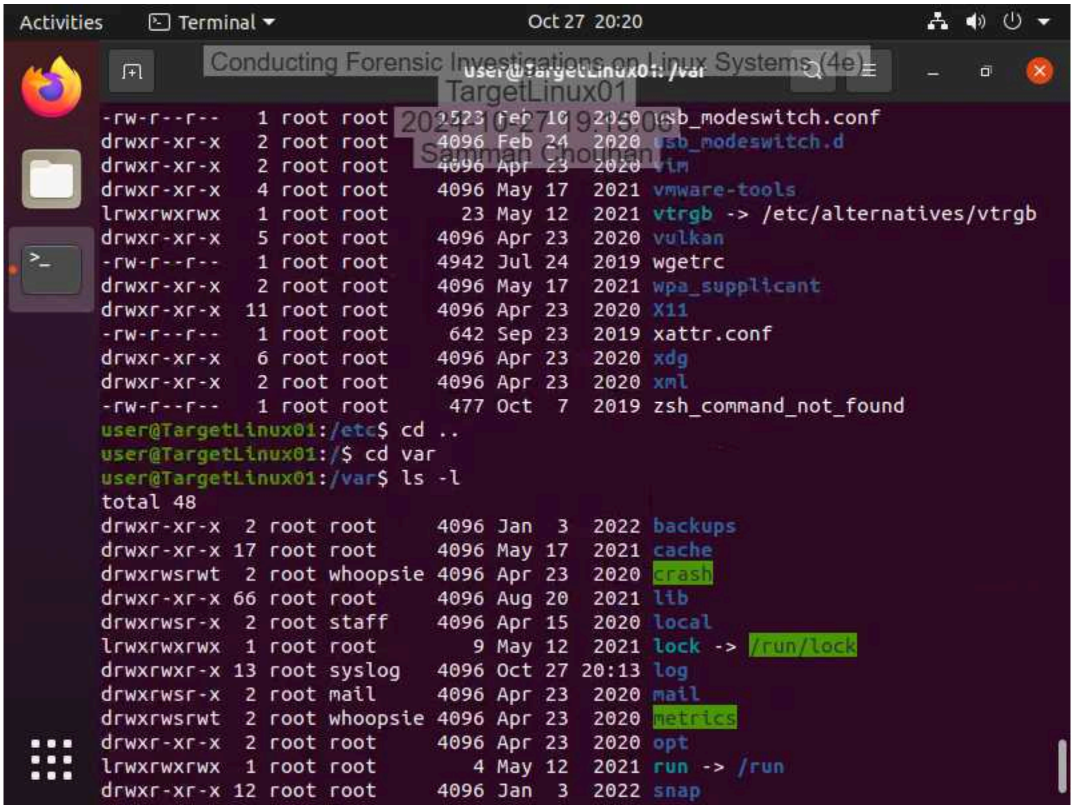
```
drwxr-xr-x 14 root root      4096 Apr 23  2020 var
user@TargetLinux01:/$ cd bin
user@TargetLinux01:/bin$ ls -la
total 160264
drwxr-xr-x  2 root root     40960 Aug 21  2021 .
drwxr-xr-x 14 root root      4096 Apr 23  2020 ..
-rwxr-xr-x  1 root root     59736 Sep  5  2019 '['
-rwxr-xr-x  1 root root     31248 May 19  2020  aa-enabled
-rwxr-xr-x  1 root root     35344 May 19  2020  aa-exec
-rwxr-xr-x  1 root root     22912 Apr 14  2021  aconnect
-rwxr-xr-x  1 root root     19016 Nov 28  2019  acpi_listen
-rwxr-xr-x  1 root root      7415 Jan 26  2021  add-apt-repository
-rwxr-xr-x  1 root root     30952 Jul 21  2020  addpart
-rwxr-xr-x  1 root root     47552 Apr 14  2021  alsabat
-rwxr-xr-x  1 root root     85296 Apr 14  2021  alsaloop
-rwxr-xr-x  1 root root     72432 Apr 14  2021  alsamixer
-rwxr-xr-x  1 root root     14720 Apr 14  2021  alsatplg
-rwxr-xr-x  1 root root     31528 Apr 14  2021  alsaucm
-rwxr-xr-x  1 root root     31112 Apr 14  2021  amidi
-rwxr-xr-x  1 root root     63952 Apr 14  2021  amixer
-rwxr-xr-x  1 root root      2668 Mar 22  2020  amuFormat.sh
-rwxr-xr-x  1 root root       274 Oct  1  2017  apg
-rwxr-xr-x  1 root root     26696 Oct  1  2017  apgbfm
-rwxr-xr-x  1 root root     84408 Apr 14  2021  aplay
-rwxr-xr-x  1 root root     27016 Apr 14  2021  aplaymidi
-rwxr-xr-x  1 root root      2558 Dec  4  2019  apport-bug
-rwxr-xr-x  1 root root     13367 May 18  2021  apport-cli
lrwxrwxrwx  1 root root        10 May 18  2021  apport-collect -> apport-bug
-rwxr-xr-x  1 root root      2068 May 18  2021  apport-unpack
-rwxr-xr-x  1 root root     14648 Feb 29  2020
```

20. **Make a screen capture** showing the **contents of the /etc directory**.



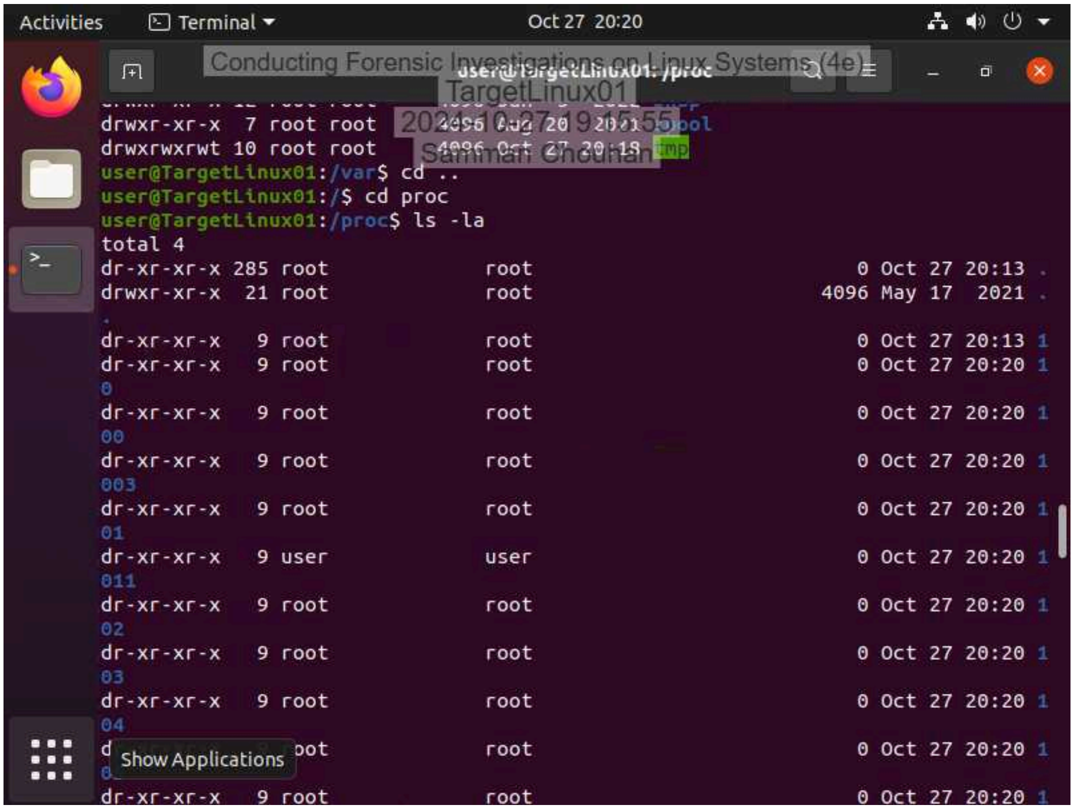
```
-rwxr-xr-x  1 root root   1842 Dec 13  2019 zmore
-rwxr-xr-x  1 root root   4553 Dec 13  2019 znew
user@TargetLinux01:/bin$ cd ..
user@TargetLinux01:/$
user@TargetLinux01:/$ cd etc
user@TargetLinux01:/etc$ ls -la
total 1092
drwxr-xr-x 129 root root   12288 Aug 20  2021 .
drwxr-xr-x  21 root root    4096 May 17  2021 ..
drwxr-xr-x   3 root root    4096 Apr 23  2020 acpi
-rw-r--r--   1 root root    3028 Apr 23  2020 adduser.conf
drwxr-xr-x   3 root root    4096 Apr 23  2020 alsa
drwxr-xr-x   2 root root    4096 May 17  2021 alternatives
-rw-r--r--   1 root root     401 Jul 16  2019 anacrontab
-rw-r--r--   1 root root     433 Oct  1  2017 apg.conf
drwxr-xr-x   5 root root    4096 Apr 23  2020 apm
drwxr-xr-x   3 root root    4096 May 17  2021 apparmor
drwxr-xr-x   7 root root    4096 Aug 20  2021 apparmor.d
drwxr-xr-x   4 root root    4096 May 27  2021 apport
-rw-r--r--   1 root root     769 Jan 18  2020 appstream.conf
drwxr-xr-x   7 root root    4096 Aug 20  2021 apt
drwxr-xr-x   3 root root    4096 Jul 15  2021 avahi
-rw-r--r--   1 root root    2319 Feb 25  2020 bash.bashrc
-rw-r--r--   1 root root      45 Jan 25  2020 bash_completion
drwxr-xr-x   2 root root    4096 May 27  2021 bash_completion.d
-rw-r--r--   1 root root     367 Apr 14  2020 bindresvport.blacklist
drwxr-xr-x   2 root root    4096 Apr 22  2020 binfmt.d
drwxr-xr-x   2 root root    4096 Jun 17  2021 bluetooth
-rw-r-----   1 root root      33 Apr 23  2020 brlapi.key
drwxr-xr-x   7 root root    4096 Apr 23  2020 brltty
```

21. **Make a screen capture** showing the **contents of the /var directory**.



```
-rw-r--r--   1 root root     2523 Feb 10  2020 usb_modeswitch.conf
drwxr-xr-x   2 root root     4096 Feb 24  2020 usb_modeswitch.d
drwxr-xr-x   2 root root     4096 Apr 23  2020 vim
drwxr-xr-x   4 root root     4096 May 17  2021 vmware-tools
lrwxrwxrwx   1 root root       23 May 12  2021 vtrgb -> /etc/alternatives/vtrgb
drwxr-xr-x   5 root root     4096 Apr 23  2020 vulkan
-rw-r--r--   1 root root     4942 Jul 24  2019 wgetrc
drwxr-xr-x   2 root root     4096 May 17  2021 wpa_supplicant
drwxr-xr-x  11 root root     4096 Apr 23  2020 X11
-rw-r--r--   1 root root      642 Sep 23  2019 xattr.conf
drwxr-xr-x   6 root root     4096 Apr 23  2020 xdg
drwxr-xr-x   2 root root     4096 Apr 23  2020 xml
-rw-r--r--   1 root root      477 Oct  7  2019 zsh_command_not_found
user@TargetLinux01:/etc$ cd ..
user@TargetLinux01:/$ cd var
user@TargetLinux01:/var$ ls -l
total 48
drwxr-xr-x  2 root root     4096 Jan  3  2022 backups
drwxr-xr-x 17 root root     4096 May 17  2021 cache
drwxrwsrwt  2 root whoopsie 4096 Apr 23  2020 crash
drwxr-xr-x 66 root root     4096 Aug 20  2021 lib
drwxrwsr-x  2 root staff    4096 Apr 15  2020 local
lrwxrwxrwx  1 root root        9 May 12  2021 lock -> /run/lock
drwxrwxr-x 13 root syslog   4096 Oct 27 20:13 log
drwxrwsr-x  2 root mail     4096 Apr 23  2020 mail
drwxrwsrwt  2 root whoopsie 4096 Apr 23  2020 metrics
drwxr-xr-x  2 root root     4096 Apr 23  2020 opt
lrwxrwxrwx  1 root root        4 May 12  2021 run -> /run
drwxr-xr-x 12 root root     4096 Jan  3  2022 snap
```

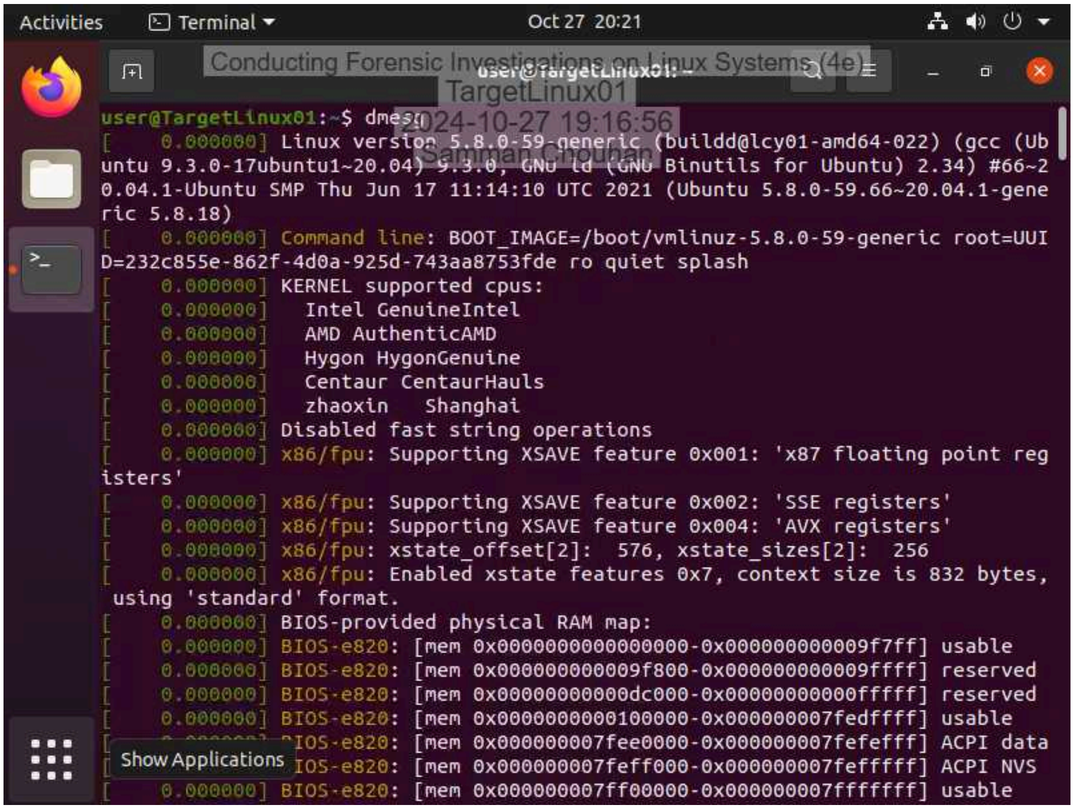
22. **Make a screen capture** showing the **contents of the /proc directory**.



```
drwxr-xr-x  7 root root  4096 Aug 20  2021 spool
drwxrwxrwt 10 root root  4096 Oct 27 20:18 tmp
user@TargetLinux01:/var$ cd ..
user@TargetLinux01:/$ cd proc
user@TargetLinux01:/proc$ ls -la
total 4
dr-xr-xr-x 285 root             root                    0 Oct 27 20:13 .
drwxr-xr-x  21 root             root                 4096 May 17  2021 .
.
dr-xr-xr-x   9 root             root                    0 Oct 27 20:13 1
dr-xr-xr-x   9 root             root                    0 Oct 27 20:20 1
0
dr-xr-xr-x   9 root             root                    0 Oct 27 20:20 1
00
dr-xr-xr-x   9 root             root                    0 Oct 27 20:20 1
003
dr-xr-xr-x   9 root             root                    0 Oct 27 20:20 1
01
dr-xr-xr-x   9 user             user                    0 Oct 27 20:20 1
011
dr-xr-xr-x   9 root             root                    0 Oct 27 20:20 1
02
dr-xr-xr-x   9 root             root                    0 Oct 27 20:20 1
03
dr-xr-xr-x   9 root             root                    0 Oct 27 20:20 1
04
d             oot             root                    0 Oct 27 20:20 1
0
dr-xr-xr-x   9 root             root                    0 Oct 27 20:20 1
```

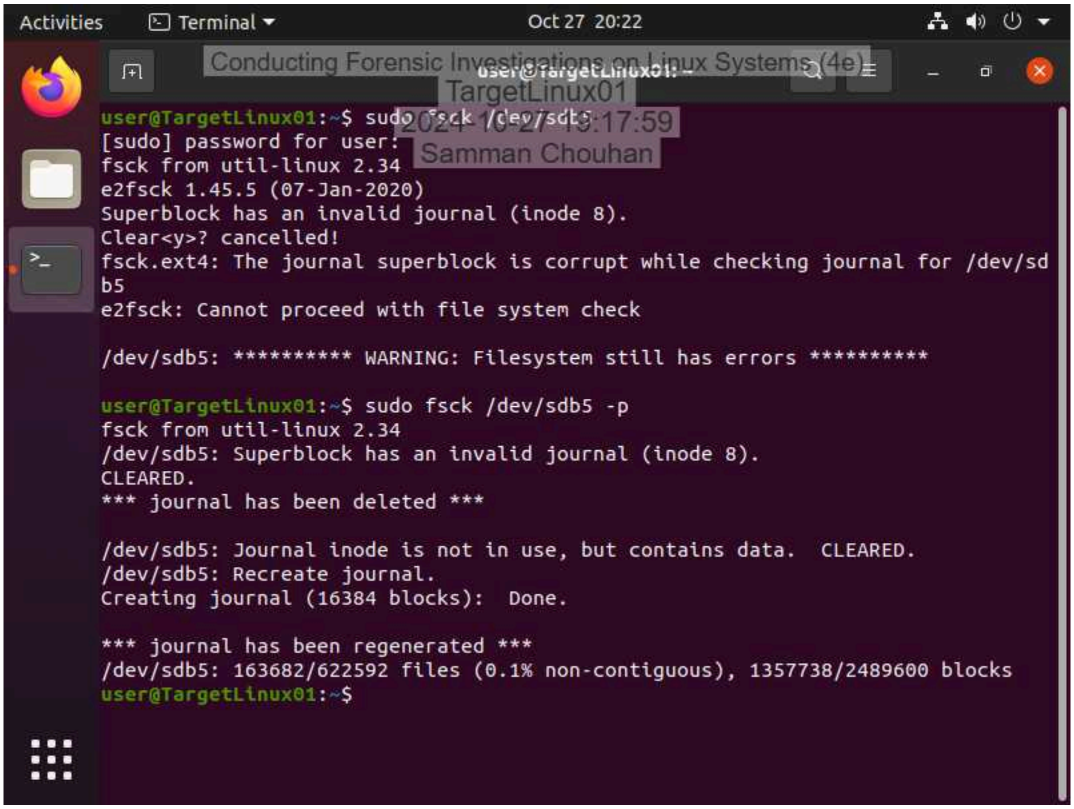
## Part 2: Use Linux Shell Commands for Forensic Investigations

2. **Make a screen capture** showing the **results of the dmesg command**.



```
user@TargetLinux01:~$ dmesg
[    0.000000] Linux version 5.8.0-59-generic (buildd@lcy01-amd64-022) (gcc (Ub
untu 9.3.0-17ubuntu1~20.04) 9.3.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #66~2
0.04.1-Ubuntu SMP Thu Jun 17 11:14:10 UTC 2021 (Ubuntu 5.8.0-59.66~20.04.1-gene
ric 5.8.18)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.8.0-59-generic root=UUI
D=232c855e-862f-4d0a-925d-743aa8753fde ro quiet splash
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
[    0.000000]   Hygon HygonGenuine
[    0.000000]   Centaur CentaurHauls
[    0.000000]   zhaoxin   Shanghai
[    0.000000] Disabled fast string operations
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point reg
isters'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
[    0.000000] x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
[    0.000000] x86/fpu: Enabled xstate features 0x7, context size is 832 bytes,
 using 'standard' format.
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009f7ff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009f800-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000dc000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x000000007fedffff] usable
[              IOS-e820: [mem 0x000000007fee0000-0x000000007fefefff] ACPI data
[              IOS-e820: [mem 0x000000007feff000-0x000000007fefffff] ACPI NVS
[    0.000000] BIOS-e820: [mem 0x000000007ff00000-0x000000007fffffff] usable
```

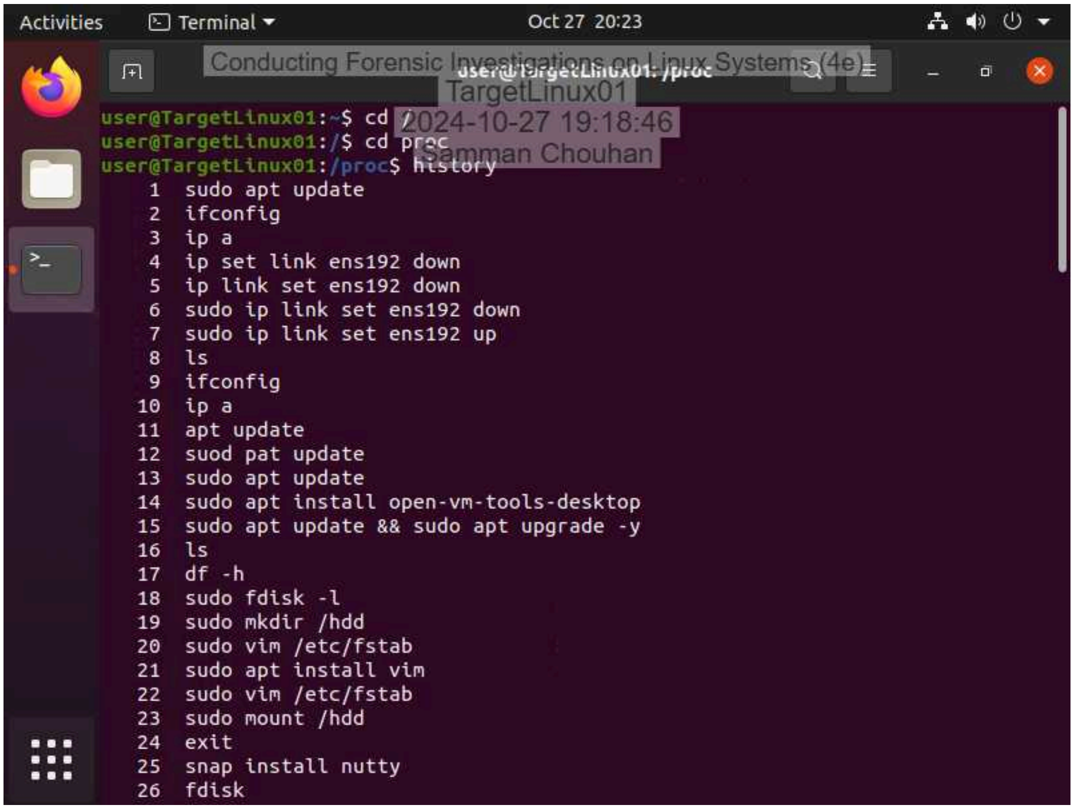
7. **Make a screen capture** showing the **results of the fsck command.**



Conducting Forensic Investigations on Linux Systems (4e)
TargetLinux01
2024-10-27 19:17:59
Samman Chouhan

```
user@TargetLinux01:~$ sudo fsck /dev/sdb5
[sudo] password for user:
fsck from util-linux 2.34
e2fsck 1.45.5 (07-Jan-2020)
Superblock has an invalid journal (inode 8).
Clear<y>? cancelled!
fsck.ext4: The journal superblock is corrupt while checking journal for /dev/sd
b5
e2fsck: Cannot proceed with file system check

/dev/sdb5: ********** WARNING: Filesystem still has errors **********

user@TargetLinux01:~$ sudo fsck /dev/sdb5 -p
fsck from util-linux 2.34
/dev/sdb5: Superblock has an invalid journal (inode 8).
CLEARED.
*** journal has been deleted ***

/dev/sdb5: Journal inode is not in use, but contains data.  CLEARED.
/dev/sdb5: Recreate journal.
Creating journal (16384 blocks):  Done.

*** journal has been regenerated ***
/dev/sdb5: 163682/622592 files (0.1% non-contiguous), 1357738/2489600 blocks
user@TargetLinux01:~$
```

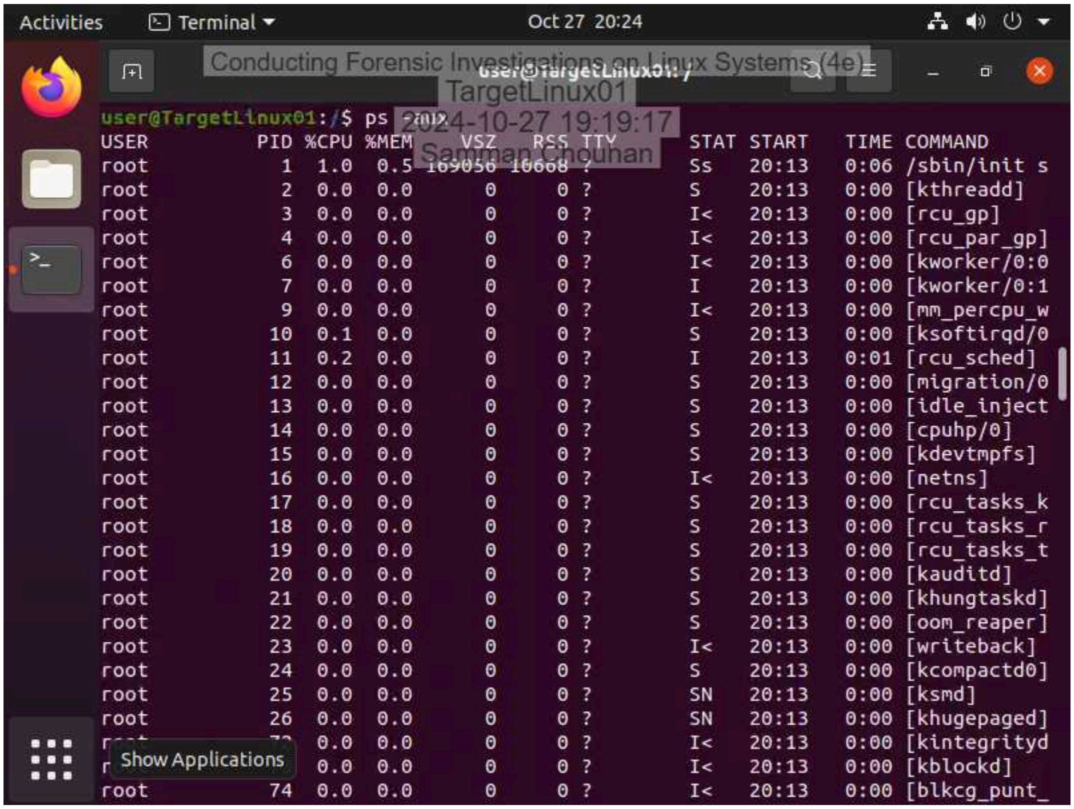
9. **Make a screen capture** showing the **results of the history command**.



Conducting Forensic Investigations on Linux Systems (4e)
TargetLinux01
2024-10-27 19:18:46
Samman Chouhan

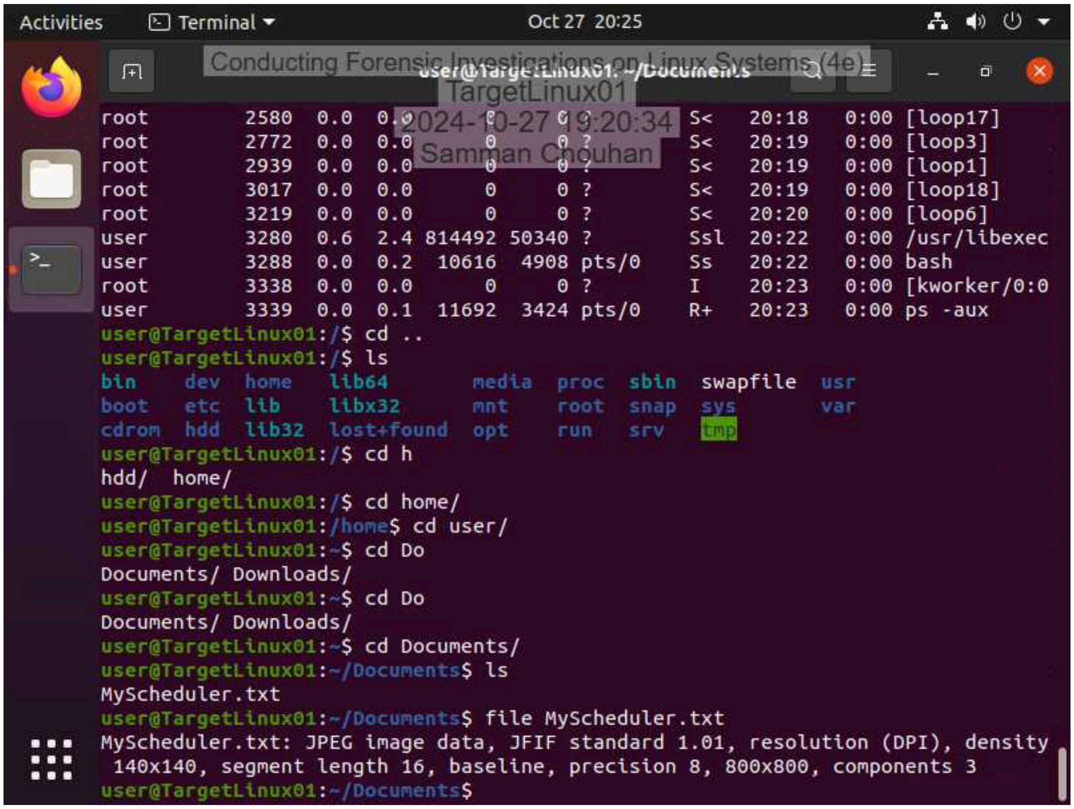
```
user@TargetLinux01:~$ cd /
user@TargetLinux01:/$ cd proc
user@TargetLinux01:/proc$ history
    1  sudo apt update
    2  ifconfig
    3  ip a
    4  ip set link ens192 down
    5  ip link set ens192 down
    6  sudo ip link set ens192 down
    7  sudo ip link set ens192 up
    8  ls
    9  ifconfig
   10  ip a
   11  apt update
   12  suod pat update
   13  sudo apt update
   14  sudo apt install open-vm-tools-desktop
   15  sudo apt update && sudo apt upgrade -y
   16  ls
   17  df -h
   18  sudo fdisk -l
   19  sudo mkdir /hdd
   20  sudo vim /etc/fstab
   21  sudo apt install vim
   22  sudo vim /etc/fstab
   23  sudo mount /hdd
   24  exit
   25  snap install nutty
   26  fdisk
```

11. **Make a screen capture** showing the **running processes**.



```
user@TargetLinux01:/$ ps -aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  1.0  0.5 169056 10668 ?        Ss   20:13   0:06 /sbin/init s
root           2  0.0  0.0      0     0 ?        S    20:13   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   20:13   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   20:13   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   20:13   0:00 [kworker/0:0
root           7  0.0  0.0      0     0 ?        I    20:13   0:00 [kworker/0:1
root           9  0.0  0.0      0     0 ?        I<   20:13   0:00 [mm_percpu_w
root          10  0.1  0.0      0     0 ?        S    20:13   0:00 [ksoftirqd/0
root          11  0.2  0.0      0     0 ?        I    20:13   0:01 [rcu_sched]
root          12  0.0  0.0      0     0 ?        S    20:13   0:00 [migration/0
root          13  0.0  0.0      0     0 ?        S    20:13   0:00 [idle_inject
root          14  0.0  0.0      0     0 ?        S    20:13   0:00 [cpuhp/0]
root          15  0.0  0.0      0     0 ?        S    20:13   0:00 [kdevtmpfs]
root          16  0.0  0.0      0     0 ?        I<   20:13   0:00 [netns]
root          17  0.0  0.0      0     0 ?        S    20:13   0:00 [rcu_tasks_k
root          18  0.0  0.0      0     0 ?        S    20:13   0:00 [rcu_tasks_r
root          19  0.0  0.0      0     0 ?        S    20:13   0:00 [rcu_tasks_t
root          20  0.0  0.0      0     0 ?        S    20:13   0:00 [kauditd]
root          21  0.0  0.0      0     0 ?        S    20:13   0:00 [khungtaskd]
root          22  0.0  0.0      0     0 ?        S    20:13   0:00 [oom_reaper]
root          23  0.0  0.0      0     0 ?        I<   20:13   0:00 [writeback]
root          24  0.0  0.0      0     0 ?        S    20:13   0:00 [kcompactd0]
root          25  0.0  0.0      0     0 ?        SN   20:13   0:00 [ksmd]
root          26  0.0  0.0      0     0 ?        SN   20:13   0:00 [khugepaged]
r                 0.0  0.0      0     0 ?        I<   20:13   0:00 [kintegrityd
r                 0.0  0.0      0     0 ?        I<   20:13   0:00 [kblockd]
root          74  0.0  0.0      0     0 ?        I<   20:13   0:00 [blkcg_punt_
```

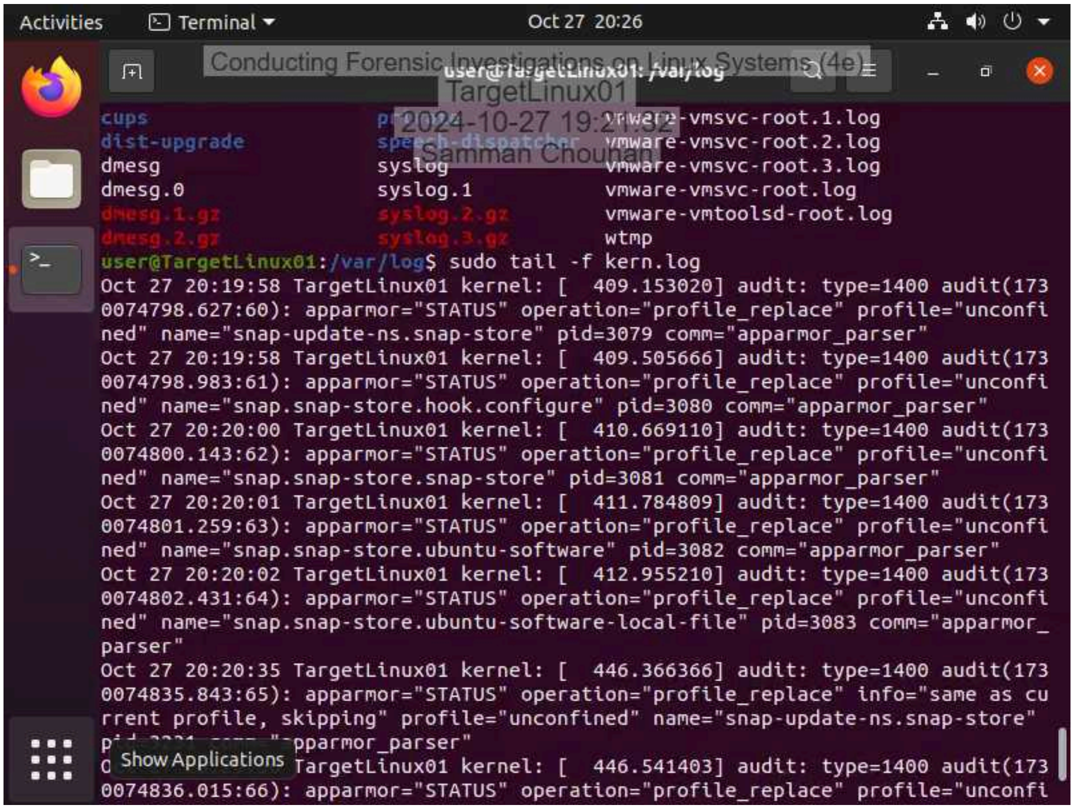
15. **Make a screen capture** showing the **results of the file command**.


Activities
Terminal
Oct 27 20:25
user@TargetLinux01: ~/Documents
Conducting Forensic Investigations on Linux Systems (4e)
TargetLinux01
2024-10-27 19:20:34
Samman Chouhan

```
root          2580  0.0  0.0      0     0 ?        S<   20:18   0:00 [loop17]
root          2772  0.0  0.0      0     0 ?        S<   20:19   0:00 [loop3]
root          2939  0.0  0.0      0     0 ?        S<   20:19   0:00 [loop1]
root          3017  0.0  0.0      0     0 ?        S<   20:19   0:00 [loop18]
root          3219  0.0  0.0      0     0 ?        S<   20:20   0:00 [loop6]
user          3280  0.6  2.4 814492 50340 ?        Ssl  20:22   0:00 /usr/libexec
user          3288  0.0  0.2  10616  4908 pts/0    Ss   20:22   0:00 bash
root          3338  0.0  0.0      0     0 ?        I    20:23   0:00 [kworker/0:0
user          3339  0.0  0.1  11692  3424 pts/0    R+   20:23   0:00 ps -aux
user@TargetLinux01:/$ cd ..
user@TargetLinux01:/$ ls
bin    dev  home   lib64       media  proc  sbin  swapfile  usr
boot   etc  lib    libx32      mnt    root  snap  sys       var
cdrom  hdd  lib32  lost+found  opt    run   srv   tmp
user@TargetLinux01:/$ cd h
hdd/  home/
user@TargetLinux01:/$ cd home/
user@TargetLinux01:/home$ cd user/
user@TargetLinux01:~$ cd Do
Documents/ Downloads/
user@TargetLinux01:~$ cd Do
Documents/ Downloads/
user@TargetLinux01:~$ cd Documents/
user@TargetLinux01:~/Documents$ ls
MyScheduler.txt
user@TargetLinux01:~/Documents$ file MyScheduler.txt
MyScheduler.txt: JPEG image data, JFIF standard 1.01, resolution (DPI), density
 140x140, segment length 16, baseline, precision 8, 800x800, components 3
user@TargetLinux01:~/Documents$
```

## Part 3: Retrieve Logs Files on a Live Linux System

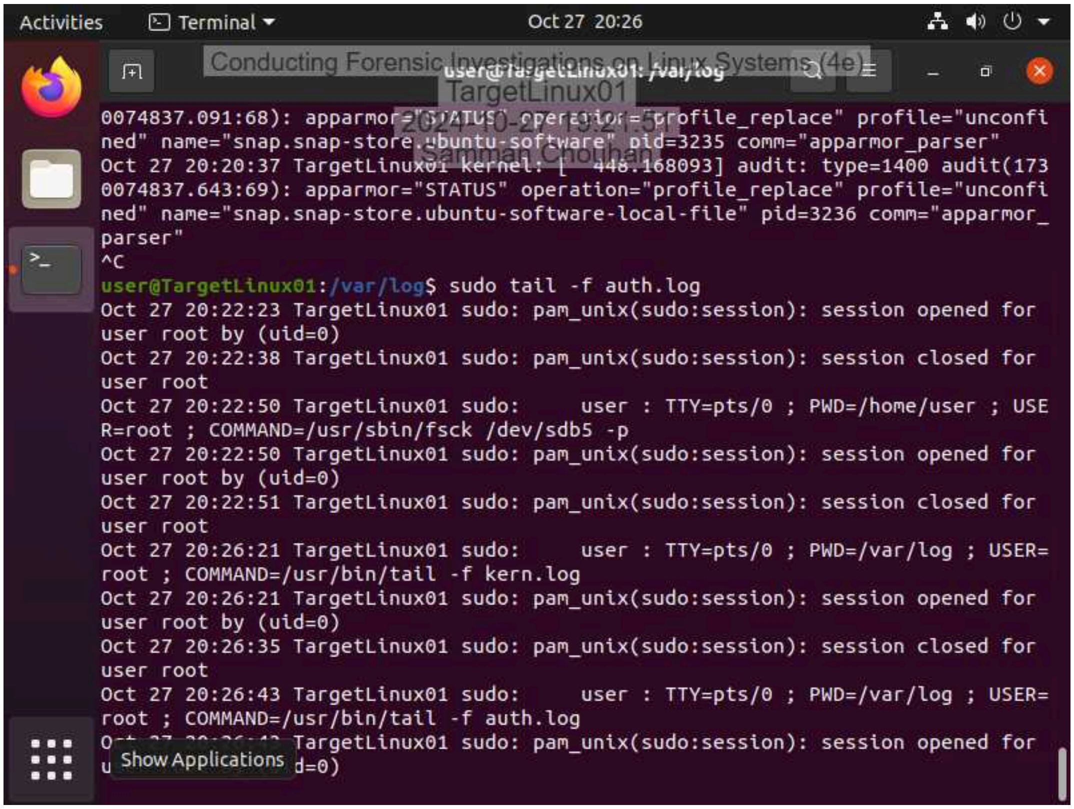
4. **Make a screen capture** showing the **records in the kern.log file.**



Conducting Forensic Investigations on Linux Systems (4e)
TargetLinux01
2024-10-27 19:21:32
Samman Chouhan

```
cups                   pr[illegible]           vmware-vmsvc-root.1.log
dist-upgrade           speech-dispatcher       vmware-vmsvc-root.2.log
dmesg                  syslog                  vmware-vmsvc-root.3.log
dmesg.0                syslog.1                vmware-vmsvc-root.log
dmesg.1.gz             syslog.2.gz             vmware-vmtoolsd-root.log
dmesg.2.gz             syslog.3.gz             wtmp
user@TargetLinux01:/var/log$ sudo tail -f kern.log
Oct 27 20:19:58 TargetLinux01 kernel: [  409.153020] audit: type=1400 audit(173
0074798.627:60): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap-update-ns.snap-store" pid=3079 comm="apparmor_parser"
Oct 27 20:19:58 TargetLinux01 kernel: [  409.505666] audit: type=1400 audit(173
0074798.983:61): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.hook.configure" pid=3080 comm="apparmor_parser"
Oct 27 20:20:00 TargetLinux01 kernel: [  410.669110] audit: type=1400 audit(173
0074800.143:62): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.snap-store" pid=3081 comm="apparmor_parser"
Oct 27 20:20:01 TargetLinux01 kernel: [  411.784809] audit: type=1400 audit(173
0074801.259:63): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.ubuntu-software" pid=3082 comm="apparmor_parser"
Oct 27 20:20:02 TargetLinux01 kernel: [  412.955210] audit: type=1400 audit(173
0074802.431:64): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.ubuntu-software-local-file" pid=3083 comm="apparmor_
parser"
Oct 27 20:20:35 TargetLinux01 kernel: [  446.366366] audit: type=1400 audit(173
0074835.843:65): apparmor="STATUS" operation="profile_replace" info="same as cu
rrent profile, skipping" profile="unconfined" name="snap-update-ns.snap-store"
pid=3331 comm="apparmor_parser"
O[illegible] TargetLinux01 kernel: [  446.541403] audit: type=1400 audit(173
0074836.015:66): apparmor="STATUS" operation="profile_replace" profile="unconfi
```

7. **Make a screen capture** showing the **records in the auth.log file**.



```
0074837.091:68): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.ubuntu-software" pid=3235 comm="apparmor_parser"
Oct 27 20:20:37 TargetLinux01 kernel: [  448.168093] audit: type=1400 audit(173
0074837.643:69): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.ubuntu-software-local-file" pid=3236 comm="apparmor_
parser"
^C
user@TargetLinux01:/var/log$ sudo tail -f auth.log
Oct 27 20:22:23 TargetLinux01 sudo: pam_unix(sudo:session): session opened for
user root by (uid=0)
Oct 27 20:22:38 TargetLinux01 sudo: pam_unix(sudo:session): session closed for
user root
Oct 27 20:22:50 TargetLinux01 sudo:     user : TTY=pts/0 ; PWD=/home/user ; USE
R=root ; COMMAND=/usr/sbin/fsck /dev/sdb5 -p
Oct 27 20:22:50 TargetLinux01 sudo: pam_unix(sudo:session): session opened for
user root by (uid=0)
Oct 27 20:22:51 TargetLinux01 sudo: pam_unix(sudo:session): session closed for
user root
Oct 27 20:26:21 TargetLinux01 sudo:     user : TTY=pts/0 ; PWD=/var/log ; USER=
root ; COMMAND=/usr/bin/tail -f kern.log
Oct 27 20:26:21 TargetLinux01 sudo: pam_unix(sudo:session): session opened for
user root by (uid=0)
Oct 27 20:26:35 TargetLinux01 sudo: pam_unix(sudo:session): session closed for
user root
Oct 27 20:26:43 TargetLinux01 sudo:     user : TTY=pts/0 ; PWD=/var/log ; USER=
root ; COMMAND=/usr/bin/tail -f auth.log
Oct 27 20:26:43 TargetLinux01 sudo: pam_unix(sudo:session): session opened for
u                d=0)
```

# Section 2: Applied Learning

## Part 1: Identify Login Attempts on a Linux Drive Image

15. **Document** the names of the two non-root users that attempted to log in, the number of attempts detected, the date/time range of the attempts, the source IP address for the login attempts, and the port.

Two non-root users are 1. Noel 2. Dominic 22 Failed Attempts were found For Noel Date and Time Range , According to the Logs , Noel first tried to login on Jun 11 00:57:11 with last attempt on the same day at 05:06:51 For Dominic Date and Time Range , According to the Logs , Dominic first tried to login on Jun 11 05:07:57 with last attempt on the same day at 05:39:01 ip address and port for 1. Noel 192.168.78.1 , Ports Used - 14444 , 3521 . Service - SSH2 2. Dominic 192.168.78.1 , Ports Used - 4663 , 3417 . Service - SSH2

17. **Document** the date and time the most recent successful login for the user(s) that you previously identified in step 15.

according to the log files when search for the user noel , i do not see any successful attempts for Noel where as while looking for the user dominic , his most recent successful attempt was at Jun 11 05:23:03

## Part 2: Identify Software Installations on a Linux Drive Image

3. **Document** the applications that were installed using apt-get, then use the Internet to identify the ones that might be considered suspicious.

applications installed using apt-get 1.logkeys 2.autotools-dev 3.build-essential 4.autoconf 5.kbd 6.cacti 7.openssh-server after researching i found out that logkeys is an advanced keylogger used on linux machine which is malicious and suspicious

## Part 3: Identify External Drive Attachments on a Linux Drive Image

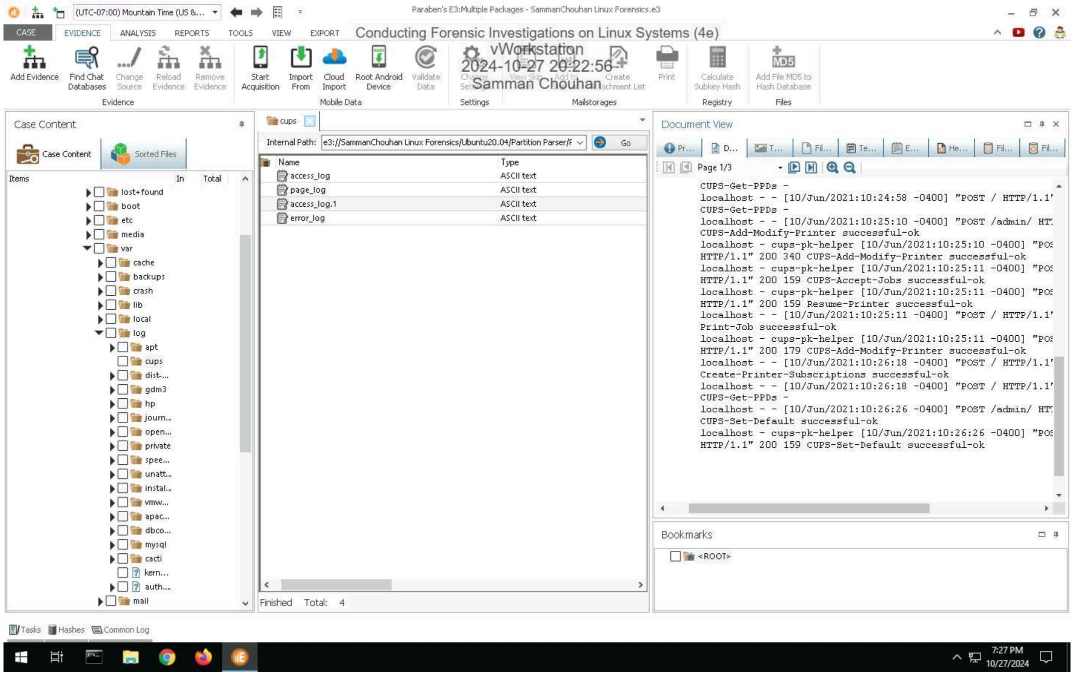
4. **Document** when the USB storage device was connected and its serial number.

according to the kern log file , a USB mass storage device was detected at Jun 10 10:24:12 and its serial number is SerialNumber: 504B4E4B3234303641

# Section 3: Challenge and Analysis

## Part 1: Identify Recently Printed Files on a Linux Drive Image

**Make a screen capture** showing the **contents of the printer log file**.



Conducting Forensic Investigations on Linux Systems (4e)
vWorkstation
2024-10-27 20:22:56
Samman Chouhan

cups

Internal Path: e3://SammanChouhan Linux Forensics/Ubuntu20.04/Partition Parser/F

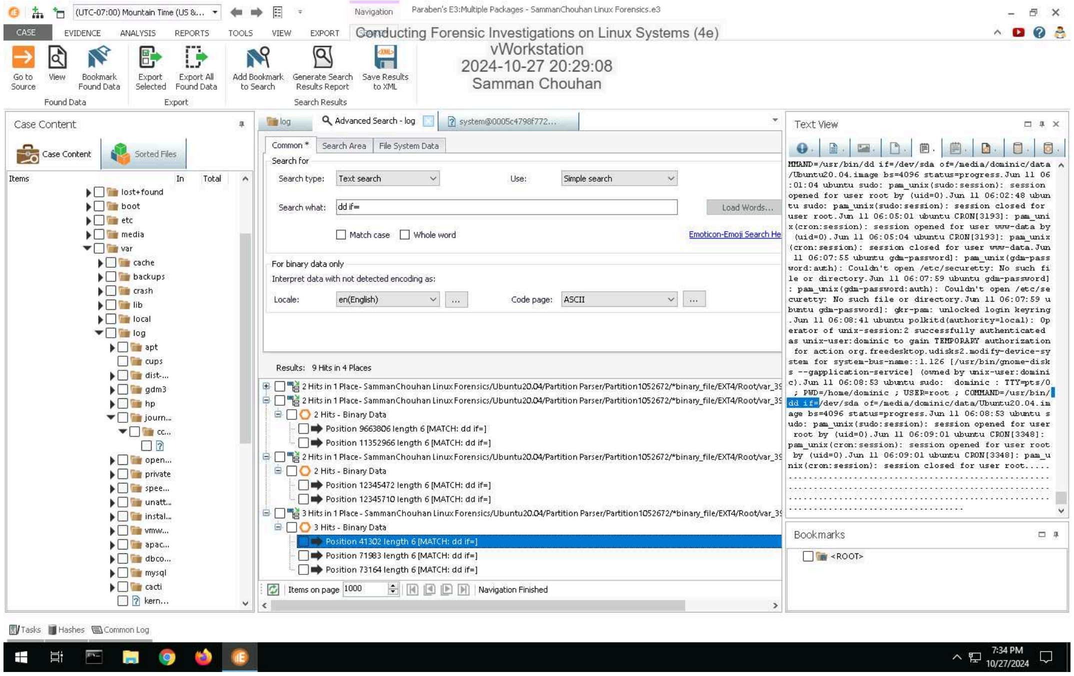
| Name | Type |
|---|---|
| access_log | ASCII text |
| page_log | ASCII text |
| access_log.1 | ASCII text |
| error_log | ASCII text |

Finished Total: 4

```
CUPS-Get-PPDs -
localhost - - [10/Jun/2021:10:24:58 -0400] "POST / HTTP/1.1'
CUPS-Get-PPDs -
localhost - - [10/Jun/2021:10:25:10 -0400] "POST /admin/ HT
CUPS-Add-Modify-Printer successful-ok
localhost - cups-pk-helper [10/Jun/2021:10:25:10 -0400] "PO
HTTP/1.1" 200 340 CUPS-Add-Modify-Printer successful-ok
localhost - cups-pk-helper [10/Jun/2021:10:25:11 -0400] "PO
HTTP/1.1" 200 159 CUPS-Accept-Jobs successful-ok
localhost - cups-pk-helper [10/Jun/2021:10:25:11 -0400] "PO
HTTP/1.1" 200 159 Resume-Printer successful-ok
localhost - - [10/Jun/2021:10:25:11 -0400] "POST / HTTP/1.1'
Print-Job successful-ok
localhost - cups-pk-helper [10/Jun/2021:10:25:11 -0400] "PO
HTTP/1.1" 200 179 CUPS-Add-Modify-Printer successful-ok
localhost - - [10/Jun/2021:10:26:18 -0400] "POST / HTTP/1.1'
Create-Printer-Subscriptions successful-ok
localhost - - [10/Jun/2021:10:26:18 -0400] "POST / HTTP/1.1'
CUPS-Get-PPDs -
localhost - - [10/Jun/2021:10:26:26 -0400] "POST /admin/ HT
CUPS-Set-Default successful-ok
localhost - cups-pk-helper [10/Jun/2021:10:26:26 -0400] "PO
HTTP/1.1" 200 159 CUPS-Set-Default successful-ok
```

## Part 2: Identify Disk Imaging on a Linux Drive Image

**Make a screen capture** showing the **record of the dd command in the Text View**.



Search for

Search type: Text search

Use: Simple search

Search what: dd if=

Load Words...

☐ Match case ☐ Whole word

Emoticon-Emoji Search He

For binary data only

Interpret data with not detected encoding as:

Locale: en(English) ...

Code page: ASCII ...

Results: 9 Hits in 4 Places

```
⊞ ☐ 2 Hits in 1 Place- SammanChouhan Linux Forensics/Ubuntu20.04/Partition Parser/Partition1052672/*binary_file/EXT4/Root/var_39
⊟ ☐ 2 Hits in 1 Place- SammanChouhan Linux Forensics/Ubuntu20.04/Partition Parser/Partition1052672/*binary_file/EXT4/Root/var_39
   ⊟ ☐ 2 Hits - Binary Data
      ☐ Position 9663806 length 6 [MATCH: dd if=]
      ☐ Position 11352966 length 6 [MATCH: dd if=]
⊟ ☐ 2 Hits in 1 Place- SammanChouhan Linux Forensics/Ubuntu20.04/Partition Parser/Partition1052672/*binary_file/EXT4/Root/var_39
   ⊟ ☐ 2 Hits - Binary Data
      ☐ Position 12345472 length 6 [MATCH: dd if=]
      ☐ Position 12345710 length 6 [MATCH: dd if=]
⊟ ☐ 3 Hits in 1 Place - SammanChouhan Linux Forensics/Ubuntu20.04/Partition Parser/Partition1052672/*binary_file/EXT4/Root/var_39
   ⊟ ☐ 3 Hits - Binary Data
      ☐ Position 41302 length 6 [MATCH: dd if=]
      ☐ Position 71983 length 6 [MATCH: dd if=]
      ☐ Position 73164 length 6 [MATCH: dd if=]
```

Items on page 1000 Navigation Finished

```
MMAND=/usr/bin/dd if=/dev/sda of=/media/dominic/data
/Ubuntu20.04.image bs=4096 status=progress.Jun 11 06
:01:04 ubuntu sudo: pam_unix(sudo:session): session
opened for user root by (uid=0).Jun 11 06:02:48 ubun
tu sudo: pam_unix(sudo:session): session closed for
user root.Jun 11 06:05:01 ubuntu CRON[3193]: pam_uni
x(cron:session): session opened for user www-data by
 (uid=0).Jun 11 06:05:04 ubuntu CRON[3193]: pam_unix
(cron:session): session closed for user www-data.Jun
 11 06:07:55 ubuntu gdm-password]: pam_unix(gdm-pass
word:auth): Couldn't open /etc/securetty: No such fi
le or directory.Jun 11 06:07:59 ubuntu gdm-password]
: pam_unix(gdm-password:auth): Couldn't open /etc/se
curetty: No such file or directory.Jun 11 06:07:59 u
buntu gdm-password]: gkr-pam: unlocked login keyring
.Jun 11 06:08:41 ubuntu polkitd(authority=local): Op
erator of unix-session:2 successfully authenticated
as unix-user:dominic to gain TEMPORARY authorization
 for action org.freedesktop.udisks2.modify-device-sy
stem for system-bus-name::1.126 [/usr/bin/gnome-disk
s --gapplication-service] (owned by unix-user:domini
c).Jun 11 06:08:53 ubuntu sudo:  dominic : TTY=pts/0
 ; PWD=/home/dominic ; USER=root ; COMMAND=/usr/bin/
dd if=/dev/sda of=/media/dominic/data/Ubuntu20.04.im
age bs=4096 status=progress.Jun 11 06:08:53 ubuntu s
udo: pam_unix(sudo:session): session opened for user
 root by (uid=0).Jun 11 06:09:01 ubuntu CRON[3348]:
pam_unix(cron:session): session opened for user root
 by (uid=0).Jun 11 06:09:01 ubuntu CRON[3348]: pam_u
nix(cron:session): session closed for user root.....
....................................................
....................................................
....................................................
...................................
```

the syntax "dd if = / of =/" is used to clone disk which was done in this case and can be found done by dominic as also seen in the logs