Conducting Forensic Investigations on Linux Systems (4e)

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

Student: Alexis Cherpes	Email: cherpea@ferris.edu

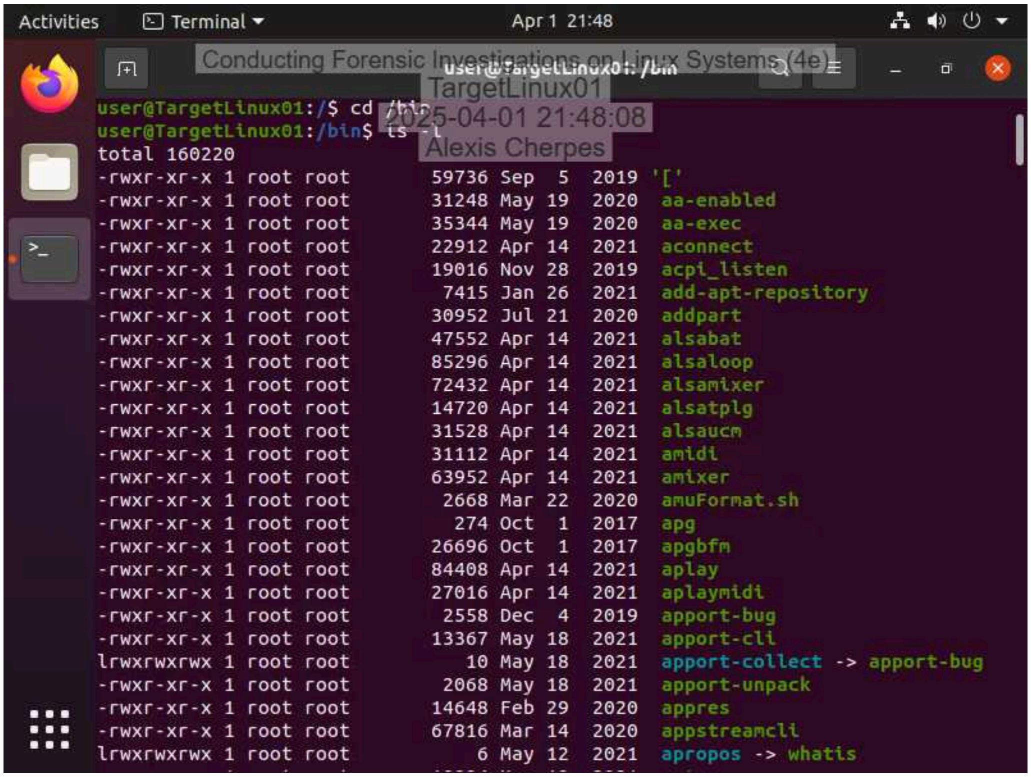
Time on Task: 1 hour, 10 minutes	Progress: 100%

Report Generated: Thursday, May 22, 2025 at 4:49 PM

Section 1: Hands-On Demonstration

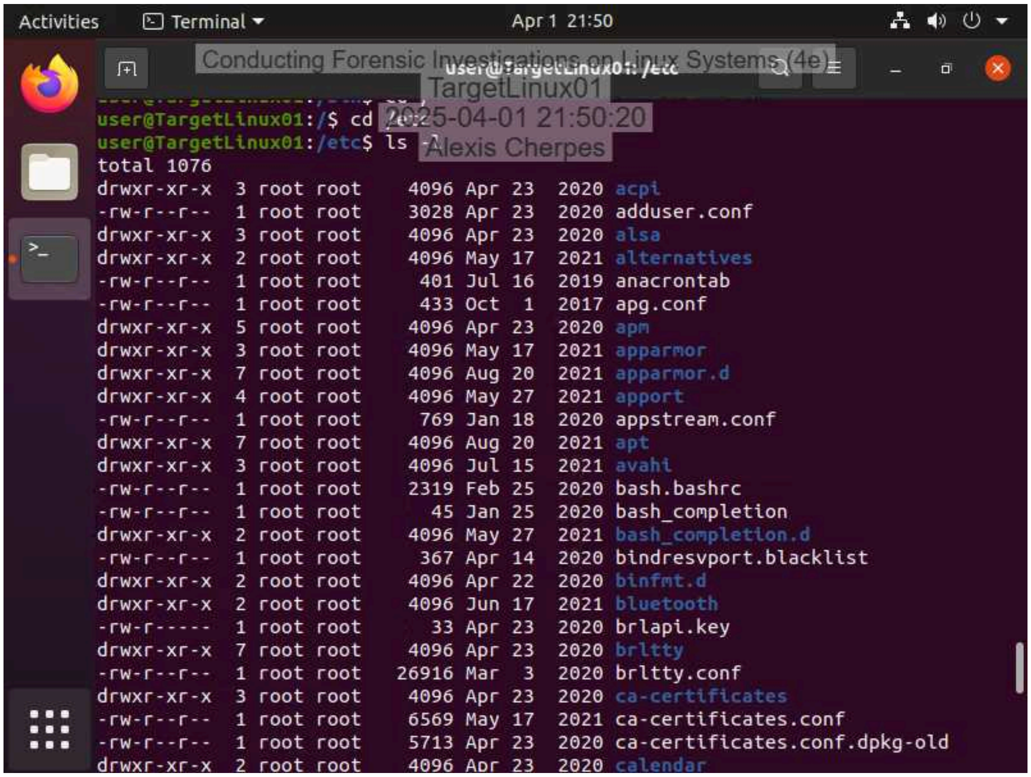
Part 1: Explore a Live Linux System

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



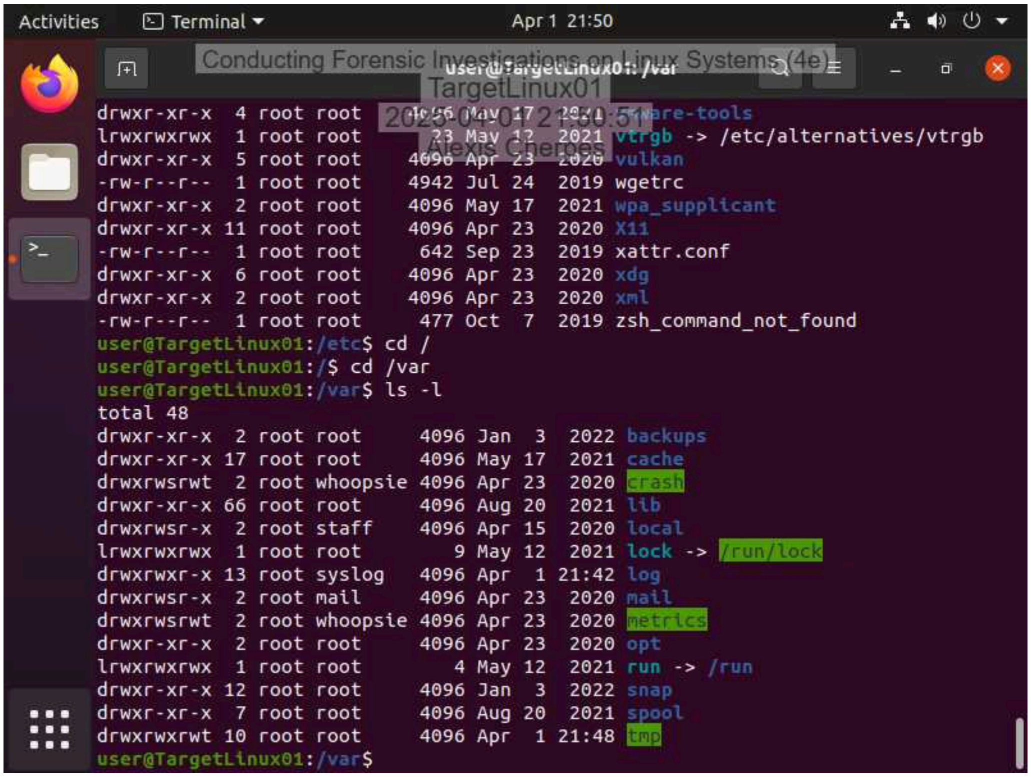
```
user@TargetLinux01:/$ cd /bin
user@TargetLinux01:/bin$ ls -l
total 160220
-rwxr-xr-x 1 root root       59736 Sep  5  2019 '['
-rwxr-xr-x 1 root root       31248 May 19  2020  aa-enabled
-rwxr-xr-x 1 root root       35344 May 19  2020  aa-exec
-rwxr-xr-x 1 root root       22912 Apr 14  2021  aconnect
-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  appres
-rwxr-xr-x 1 root root       67816 Mar 14  2020  appstreamcli
lrwxrwxrwx 1 root root           6 May 12  2021  apropos -> whatis
```

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



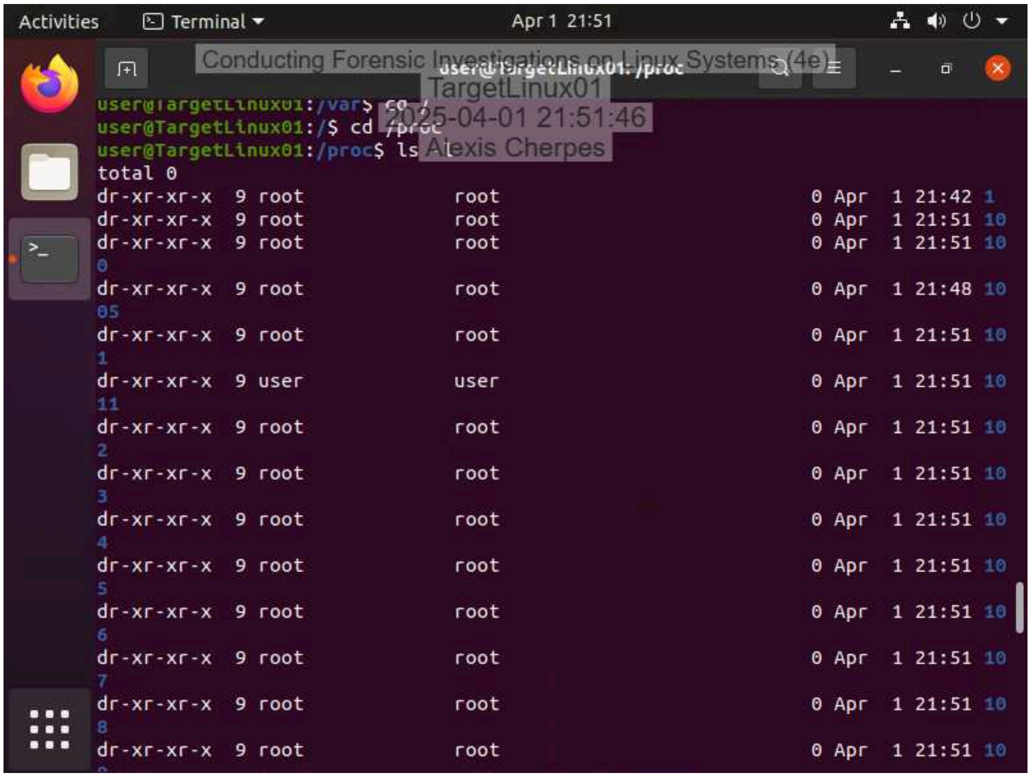
```
user@TargetLinux01:/$ cd /etc
user@TargetLinux01:/etc$ ls -l
total 1076
drwxr-xr-x  3 root root    4096 Apr 23  2020 acpi
-rw-r--r--  1 root root    3028 Apr 23  2020 adduser.conf
drwxr-xr-x  3 root root    4096 Apr 23  2020 alsa
drwxr-xr-x  2 root root    4096 May 17  2021 alternatives
-rw-r--r--  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
-rw-r--r--  1 root root   26916 Mar  3  2020 brltty.conf
drwxr-xr-x  3 root root    4096 Apr 23  2020 ca-certificates
-rw-r--r--  1 root root    6569 May 17  2021 ca-certificates.conf
-rw-r--r--  1 root root    5713 Apr 23  2020 ca-certificates.conf.dpkg-old
drwxr-xr-x  2 root root    4096 Apr 23  2020 calendar
```

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



```
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 Apr  1 21:42 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
drwxr-xr-x  7 root root     4096 Aug 20  2021 spool
drwxrwxrwt 10 root root     4096 Apr  1 21:48 tmp
user@TargetLinux01:/var$
```

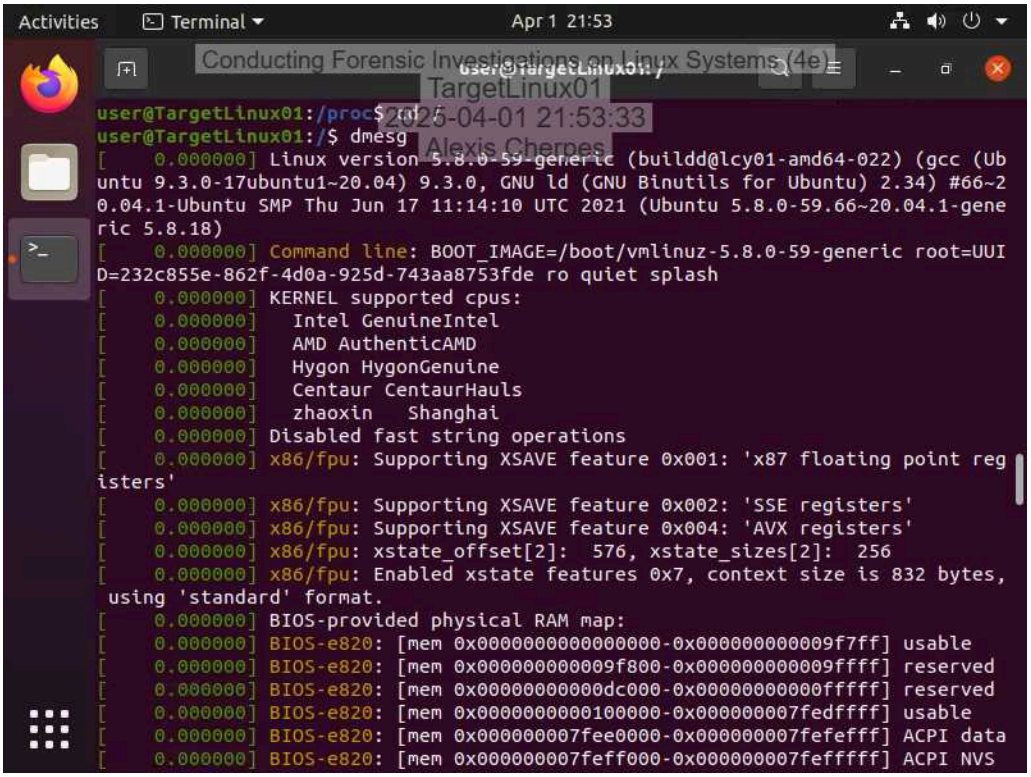
22. **Make a screen capture** showing the **contents of the /proc directory**.


Activities
Terminal
Apr 1 21:51
user@TargetLinux01: /proc
Conducting Forensic Investigations on Linux Systems (4e)
TargetLinux01
2025-04-01 21:51:46
Alexis Cherpes

```
user@TargetLinux01:/var$ cd /
user@TargetLinux01:/$ cd /proc
user@TargetLinux01:/proc$ ls -l
total 0
dr-xr-xr-x  9 root           root                         0 Apr  1 21:42 1
dr-xr-xr-x  9 root           root                         0 Apr  1 21:51 10
dr-xr-xr-x  9 root           root                         0 Apr  1 21:51 10
0
dr-xr-xr-x  9 root           root                         0 Apr  1 21:48 10
05
dr-xr-xr-x  9 root           root                         0 Apr  1 21:51 10
1
dr-xr-xr-x  9 user           user                         0 Apr  1 21:51 10
11
dr-xr-xr-x  9 root           root                         0 Apr  1 21:51 10
2
dr-xr-xr-x  9 root           root                         0 Apr  1 21:51 10
3
dr-xr-xr-x  9 root           root                         0 Apr  1 21:51 10
4
dr-xr-xr-x  9 root           root                         0 Apr  1 21:51 10
5
dr-xr-xr-x  9 root           root                         0 Apr  1 21:51 10
6
dr-xr-xr-x  9 root           root                         0 Apr  1 21:51 10
7
dr-xr-xr-x  9 root           root                         0 Apr  1 21:51 10
8
dr-xr-xr-x  9 root           root                         0 Apr  1 21:51 10
```

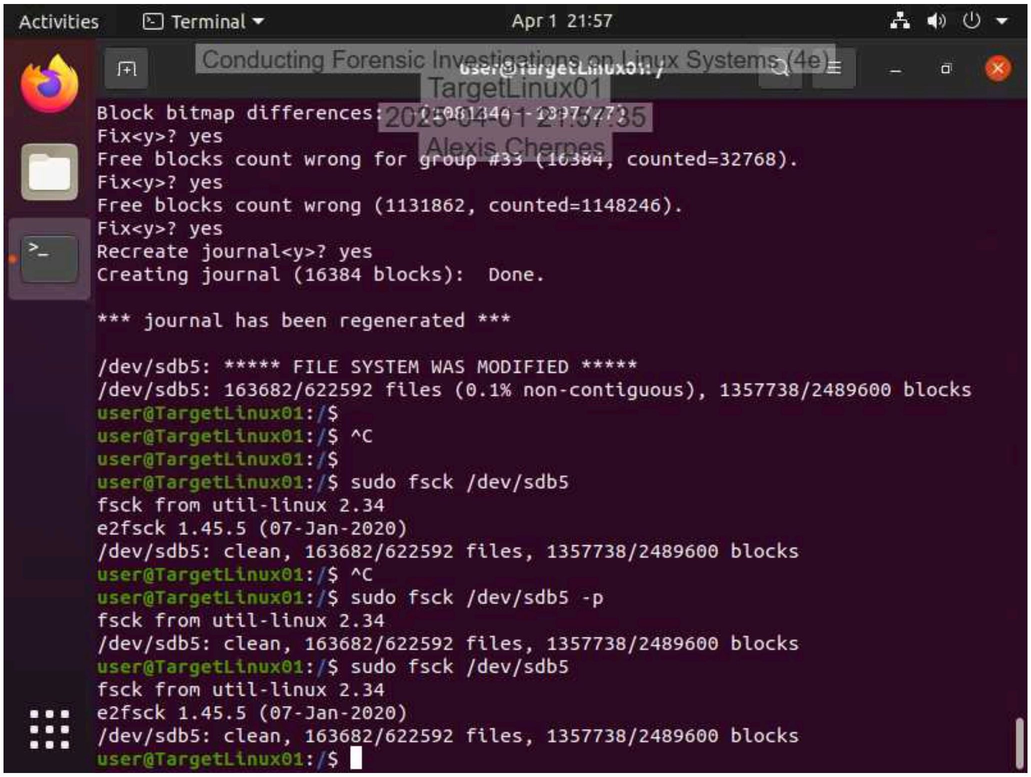
Part 2: Use Linux Shell Commands for Forensic Investigations

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



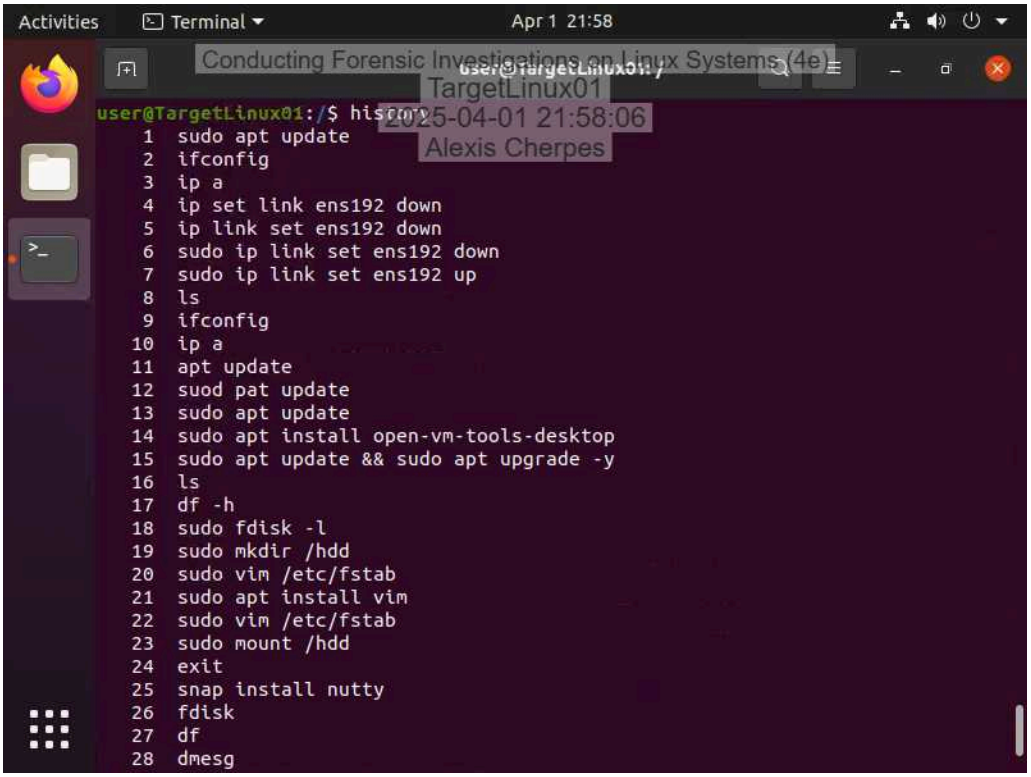
```
user@TargetLinux01:/proc$ cd /
user@TargetLinux01:/$ dmesg
[    0.000000] Linux version 5.8.0-59-generic (buildd@lcy01-amd64-022) (gcc (Ub
untu 9.3.0-17ubuntu1~20.04) 9.3.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #66~2
0.04.1-Ubuntu SMP Thu Jun 17 11:14:10 UTC 2021 (Ubuntu 5.8.0-59.66~20.04.1-gene
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
[    0.000000] BIOS-e820: [mem 0x000000007fee0000-0x000000007fefefff] ACPI data
[    0.000000] BIOS-e820: [mem 0x000000007feff000-0x000000007fefffff] ACPI NVS
```

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



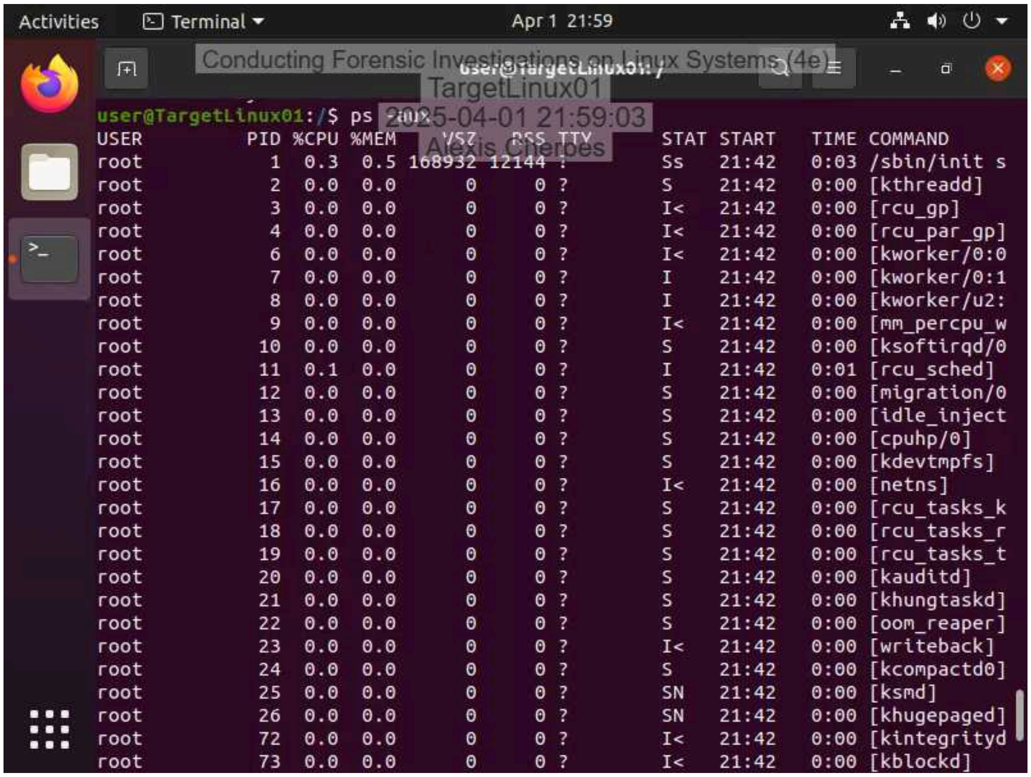
```
Block bitmap differences: -(1081344--1097727)
Fix<y>? yes
Free blocks count wrong for group #33 (16384, counted=32768).
Fix<y>? yes
Free blocks count wrong (1131862, counted=1148246).
Fix<y>? yes
Recreate journal<y>? yes
Creating journal (16384 blocks):  Done.

*** journal has been regenerated ***

/dev/sdb5: ***** FILE SYSTEM WAS MODIFIED *****
/dev/sdb5: 163682/622592 files (0.1% non-contiguous), 1357738/2489600 blocks
user@TargetLinux01:/$
user@TargetLinux01:/$ ^C
user@TargetLinux01:/$
user@TargetLinux01:/$ sudo fsck /dev/sdb5
fsck from util-linux 2.34
e2fsck 1.45.5 (07-Jan-2020)
/dev/sdb5: clean, 163682/622592 files, 1357738/2489600 blocks
user@TargetLinux01:/$ ^C
user@TargetLinux01:/$ sudo fsck /dev/sdb5 -p
fsck from util-linux 2.34
/dev/sdb5: clean, 163682/622592 files, 1357738/2489600 blocks
user@TargetLinux01:/$ sudo fsck /dev/sdb5
fsck from util-linux 2.34
e2fsck 1.45.5 (07-Jan-2020)
/dev/sdb5: clean, 163682/622592 files, 1357738/2489600 blocks
user@TargetLinux01:/$
```

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



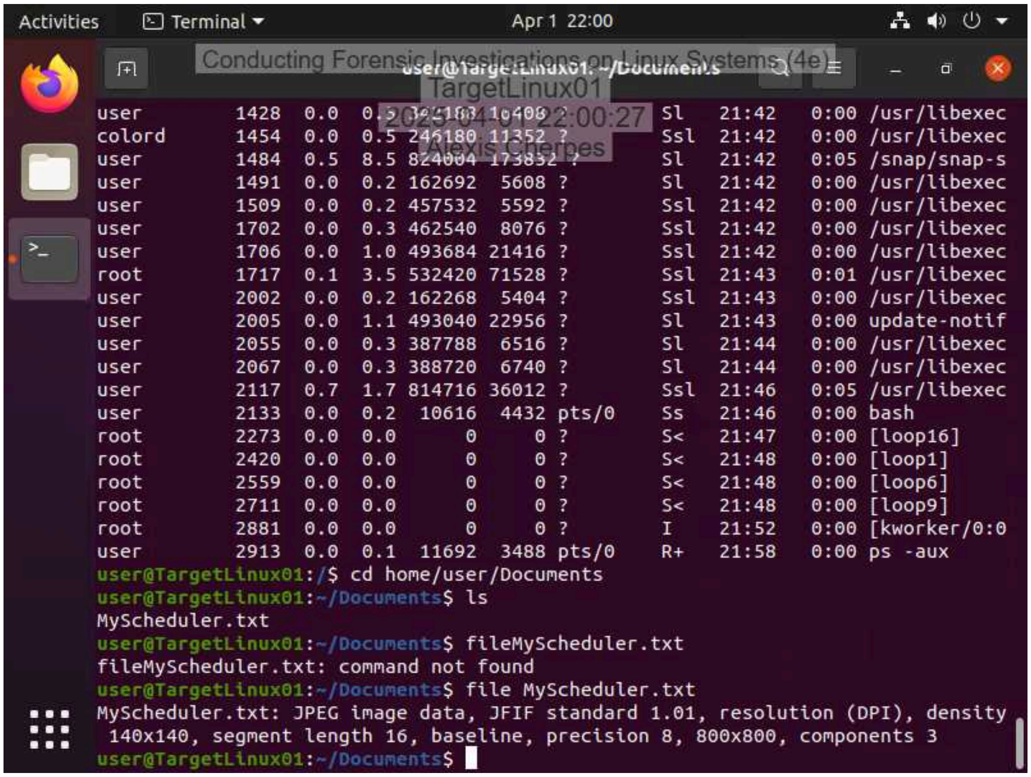
```
user@TargetLinux01:/$ history
    1  sudo apt update
    2  ifconfig
    3  ip a
    4  ip set link ens192 down
    5  ip link set ens192 down
    6  sudo ip link set ens192 down
    7  sudo ip link set ens192 up
    8  ls
    9  ifconfig
   10  ip a
   11  apt update
   12  suod pat update
   13  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
   27  df
   28  dmesg
```

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  0.3  0.5 168932 12144 ?        Ss   21:42   0:03 /sbin/init s
root           2  0.0  0.0      0     0 ?        S    21:42   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   21:42   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   21:42   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   21:42   0:00 [kworker/0:0
root           7  0.0  0.0      0     0 ?        I    21:42   0:00 [kworker/0:1
root           8  0.0  0.0      0     0 ?        I    21:42   0:00 [kworker/u2:
root           9  0.0  0.0      0     0 ?        I<   21:42   0:00 [mm_percpu_w
root          10  0.0  0.0      0     0 ?        S    21:42   0:00 [ksoftirqd/0
root          11  0.1  0.0      0     0 ?        I    21:42   0:01 [rcu_sched]
root          12  0.0  0.0      0     0 ?        S    21:42   0:00 [migration/0
root          13  0.0  0.0      0     0 ?        S    21:42   0:00 [idle_inject
root          14  0.0  0.0      0     0 ?        S    21:42   0:00 [cpuhp/0]
root          15  0.0  0.0      0     0 ?        S    21:42   0:00 [kdevtmpfs]
root          16  0.0  0.0      0     0 ?        I<   21:42   0:00 [netns]
root          17  0.0  0.0      0     0 ?        S    21:42   0:00 [rcu_tasks_k
root          18  0.0  0.0      0     0 ?        S    21:42   0:00 [rcu_tasks_r
root          19  0.0  0.0      0     0 ?        S    21:42   0:00 [rcu_tasks_t
root          20  0.0  0.0      0     0 ?        S    21:42   0:00 [kauditd]
root          21  0.0  0.0      0     0 ?        S    21:42   0:00 [khungtaskd]
root          22  0.0  0.0      0     0 ?        S    21:42   0:00 [oom_reaper]
root          23  0.0  0.0      0     0 ?        I<   21:42   0:00 [writeback]
root          24  0.0  0.0      0     0 ?        S    21:42   0:00 [kcompactd0]
root          25  0.0  0.0      0     0 ?        SN   21:42   0:00 [ksmd]
root          26  0.0  0.0      0     0 ?        SN   21:42   0:00 [khugepaged]
root          72  0.0  0.0      0     0 ?        I<   21:42   0:00 [kintegrityd
root          73  0.0  0.0      0     0 ?        I<   21:42   0:00 [kblockd]
```

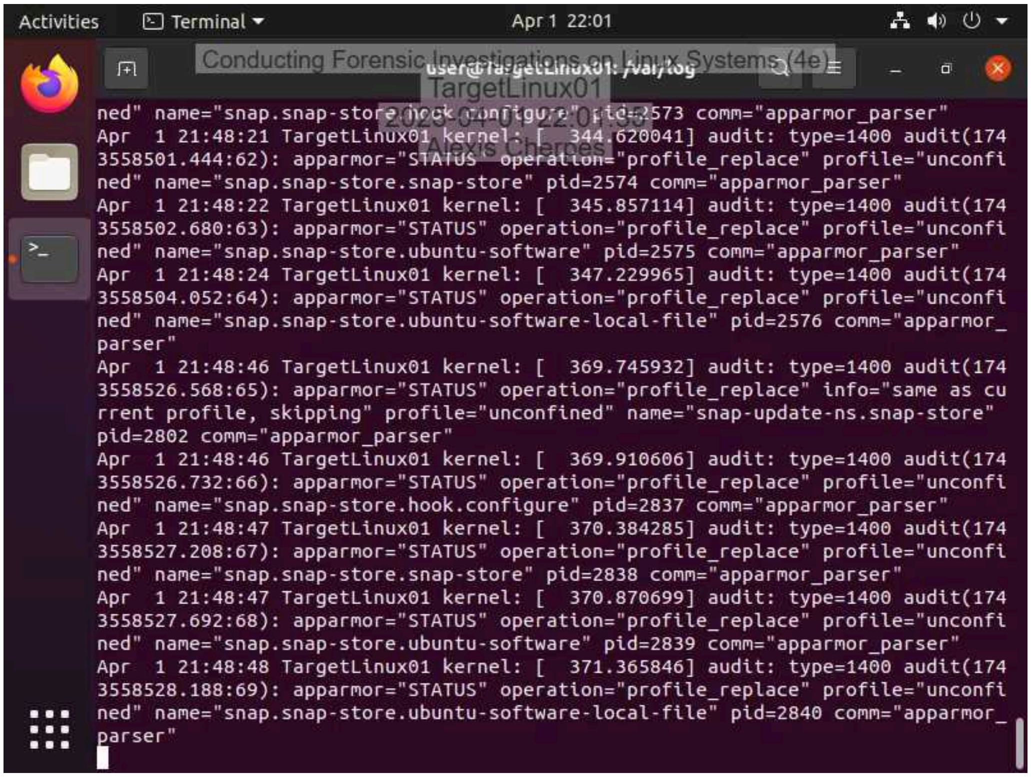
15. **Make a screen capture** showing the **results of the file command**.


Activities
Terminal
Apr 1 22:00
user@TargetLinux01: ~/Documents
Conducting Forensic Investigations on Linux Systems (4e)
TargetLinux01
2025-04-01 22:00:27
Alexis Cherpes

```
user        1428  0.0  0.5 344188 10408 ?        Sl   21:42   0:00 /usr/libexec
colord      1454  0.0  0.5 246180 11352 ?        Ssl  21:42   0:00 /usr/libexec
user        1484  0.5  8.5 824004 173832 ?       Sl   21:42   0:05 /snap/snap-s
user        1491  0.0  0.2 162692  5608 ?        Sl   21:42   0:00 /usr/libexec
user        1509  0.0  0.2 457532  5592 ?        Ssl  21:42   0:00 /usr/libexec
user        1702  0.0  0.3 462540  8076 ?        Ssl  21:42   0:00 /usr/libexec
user        1706  0.0  1.0 493684 21416 ?        Ssl  21:42   0:00 /usr/libexec
root        1717  0.1  3.5 532420 71528 ?        Ssl  21:43   0:01 /usr/libexec
user        2002  0.0  0.2 162268  5404 ?        Ssl  21:43   0:00 /usr/libexec
user        2005  0.0  1.1 493040 22956 ?        Sl   21:43   0:00 update-notif
user        2055  0.0  0.3 387788  6516 ?        Sl   21:44   0:00 /usr/libexec
user        2067  0.0  0.3 388720  6740 ?        Sl   21:44   0:00 /usr/libexec
user        2117  0.7  1.7 814716 36012 ?        Ssl  21:46   0:05 /usr/libexec
user        2133  0.0  0.2  10616  4432 pts/0    Ss   21:46   0:00 bash
root        2273  0.0  0.0      0     0 ?        S<   21:47   0:00 [loop16]
root        2420  0.0  0.0      0     0 ?        S<   21:48   0:00 [loop1]
root        2559  0.0  0.0      0     0 ?        S<   21:48   0:00 [loop6]
root        2711  0.0  0.0      0     0 ?        S<   21:48   0:00 [loop9]
root        2881  0.0  0.0      0     0 ?        I    21:52   0:00 [kworker/0:0
user        2913  0.0  0.1  11692  3488 pts/0    R+   21:58   0:00 ps -aux
user@TargetLinux01:/$ cd home/user/Documents
user@TargetLinux01:~/Documents$ ls
MyScheduler.txt
user@TargetLinux01:~/Documents$ fileMyScheduler.txt
fileMyScheduler.txt: command not found
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$ 
```

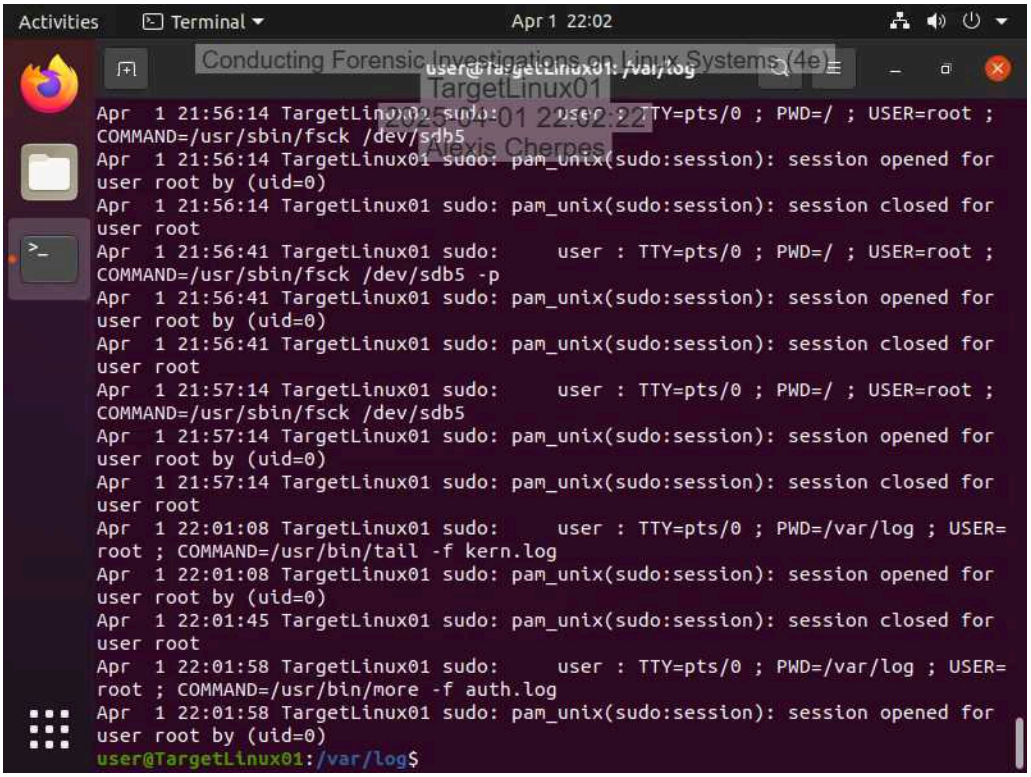
Part 3: Retrieve Logs Files on a Live Linux System

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


Activities
Terminal
Apr 1 22:01
user@TargetLinux01: /var/log
Conducting Forensic Investigations on Linux Systems (4e)
TargetLinux01
2025-04-01 22:01:55
Alexis Chernes

```
ned" name="snap.snap-store.hook.configure" pid=2573 comm="apparmor_parser"
Apr  1 21:48:21 TargetLinux01 kernel: [  344.620041] audit: type=1400 audit(174
3558501.444:62): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.snap-store" pid=2574 comm="apparmor_parser"
Apr  1 21:48:22 TargetLinux01 kernel: [  345.857114] audit: type=1400 audit(174
3558502.680:63): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.ubuntu-software" pid=2575 comm="apparmor_parser"
Apr  1 21:48:24 TargetLinux01 kernel: [  347.229965] audit: type=1400 audit(174
3558504.052:64): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.ubuntu-software-local-file" pid=2576 comm="apparmor_
parser"
Apr  1 21:48:46 TargetLinux01 kernel: [  369.745932] audit: type=1400 audit(174
3558526.568:65): apparmor="STATUS" operation="profile_replace" info="same as cu
rrent profile, skipping" profile="unconfined" name="snap-update-ns.snap-store"
pid=2802 comm="apparmor_parser"
Apr  1 21:48:46 TargetLinux01 kernel: [  369.910606] audit: type=1400 audit(174
3558526.732:66): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.hook.configure" pid=2837 comm="apparmor_parser"
Apr  1 21:48:47 TargetLinux01 kernel: [  370.384285] audit: type=1400 audit(174
3558527.208:67): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.snap-store" pid=2838 comm="apparmor_parser"
Apr  1 21:48:47 TargetLinux01 kernel: [  370.870699] audit: type=1400 audit(174
3558527.692:68): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.ubuntu-software" pid=2839 comm="apparmor_parser"
Apr  1 21:48:48 TargetLinux01 kernel: [  371.365846] audit: type=1400 audit(174
3558528.188:69): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.ubuntu-software-local-file" pid=2840 comm="apparmor_
parser"
```

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



```
Apr  1 21:56:14 TargetLinux01 sudo:     user : TTY=pts/0 ; PWD=/ ; USER=root ;
COMMAND=/usr/sbin/fsck /dev/sdb5
Apr  1 21:56:14 TargetLinux01 sudo: pam_unix(sudo:session): session opened for
user root by (uid=0)
Apr  1 21:56:14 TargetLinux01 sudo: pam_unix(sudo:session): session closed for
user root
Apr  1 21:56:41 TargetLinux01 sudo:     user : TTY=pts/0 ; PWD=/ ; USER=root ;
COMMAND=/usr/sbin/fsck /dev/sdb5 -p
Apr  1 21:56:41 TargetLinux01 sudo: pam_unix(sudo:session): session opened for
user root by (uid=0)
Apr  1 21:56:41 TargetLinux01 sudo: pam_unix(sudo:session): session closed for
user root
Apr  1 21:57:14 TargetLinux01 sudo:     user : TTY=pts/0 ; PWD=/ ; USER=root ;
COMMAND=/usr/sbin/fsck /dev/sdb5
Apr  1 21:57:14 TargetLinux01 sudo: pam_unix(sudo:session): session opened for
user root by (uid=0)
Apr  1 21:57:14 TargetLinux01 sudo: pam_unix(sudo:session): session closed for
user root
Apr  1 22:01:08 TargetLinux01 sudo:     user : TTY=pts/0 ; PWD=/var/log ; USER=
root ; COMMAND=/usr/bin/tail -f kern.log
Apr  1 22:01:08 TargetLinux01 sudo: pam_unix(sudo:session): session opened for
user root by (uid=0)
Apr  1 22:01:45 TargetLinux01 sudo: pam_unix(sudo:session): session closed for
user root
Apr  1 22:01:58 TargetLinux01 sudo:     user : TTY=pts/0 ; PWD=/var/log ; USER=
root ; COMMAND=/usr/bin/more -f auth.log
Apr  1 22:01:58 TargetLinux01 sudo: pam_unix(sudo:session): session opened for
user root by (uid=0)
user@TargetLinux01:/var/log$
```

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.

Names of the two non-root users that attempted to log in: Dominic, GDMNumber of attempts: 22Date/time range of the attempts: June 1,1 00:57:11 - June 11, 05:39:01Source IP address for the login attempts: 192.168.78.1Port: 14441,3521,4663,3417

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

User: DominicDate and Time of most recent successful login: June 9, 13:31:59 - June 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.

Installed application: logkeys, kbd, autoconf, autotools.dev, build-essentialSuspicious application: logkeys, a key logger that could have been used in spying passwords.

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

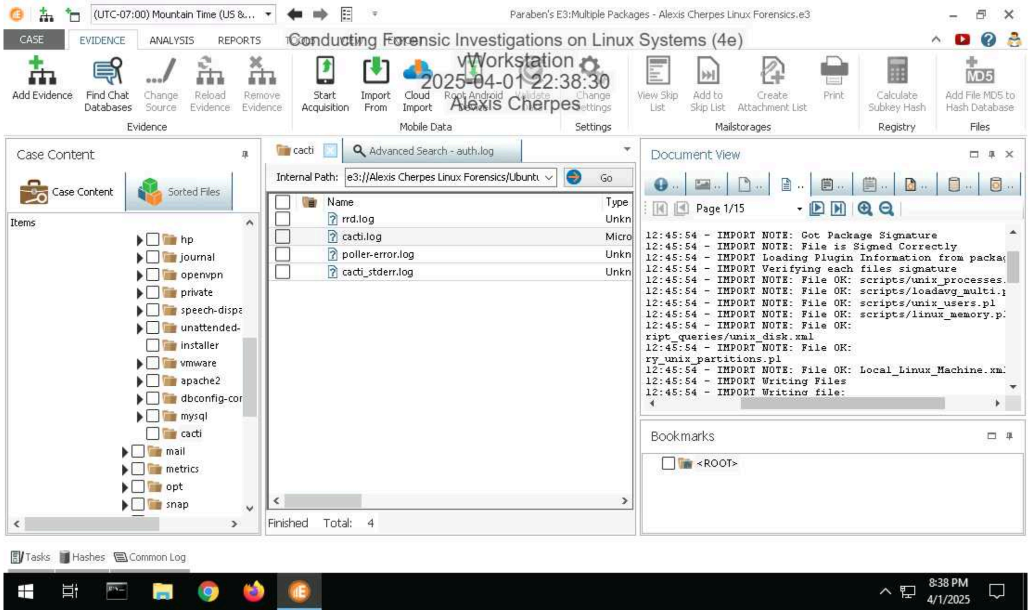
4. **Document** when the USB storage device was connected and its serial number.

USB storage device connected - June 10, 10:24:12Serial Number - FBI1405291710344

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**.



Paraben's E3:Multiple Packages - Alexis Cherpes Linux Forensics.e3

Conducting Forensic Investigations on Linux Systems (4e)
vWorkstation
2025-04-01 22:38:30
Alexis Cherpes

Internal Path: e3://Alexis Cherpes Linux Forensics/Ubuntu

Name	Type
rrd.log	Unkn
cacti.log	Micro
poller-error.log	Unkn
cacti_stderr.log	Unkn

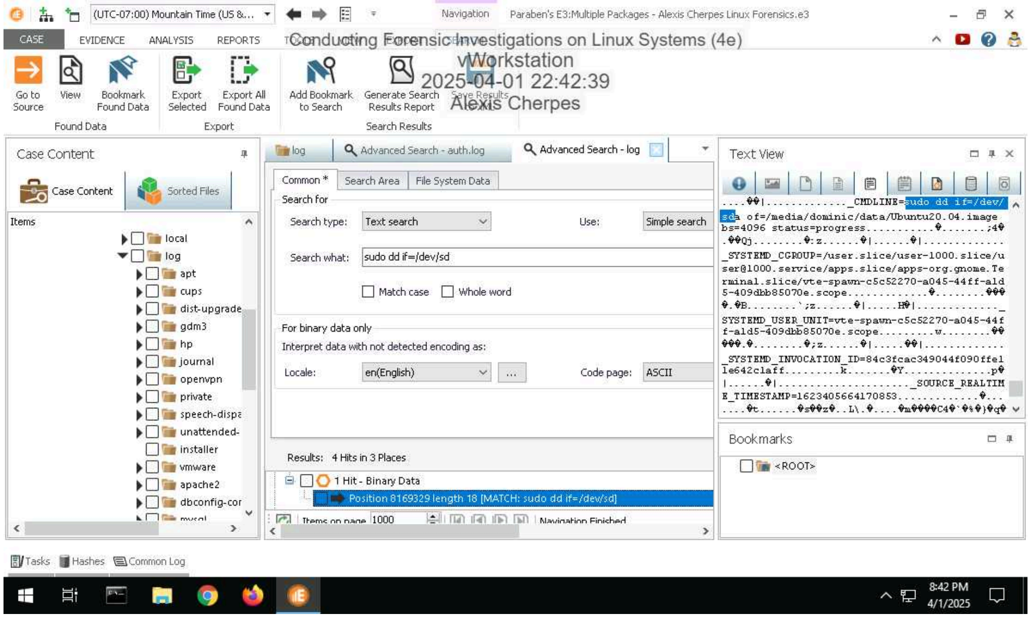
Finished Total: 4

Document View — Page 1/15

```
12:45:54 - IMPORT NOTE: Got Package Signature
12:45:54 - IMPORT NOTE: File is Signed Correctly
12:45:54 - IMPORT Loading Plugin Information from packag
12:45:54 - IMPORT Verifying each files signature
12:45:54 - IMPORT NOTE: File OK: scripts/unix_processes.
12:45:54 - IMPORT NOTE: File OK: scripts/loadavg_multi.p
12:45:54 - IMPORT NOTE: File OK: scripts/unix_users.pl
12:45:54 - IMPORT NOTE: File OK: scripts/linux_memory.pl
12:45:54 - IMPORT NOTE: File OK:
ript_queries/unix_disk.xml
12:45:54 - IMPORT NOTE: File OK:
ry_unix_partitions.pl
12:45:54 - IMPORT NOTE: File OK: Local_Linux_Machine.xml
12:45:54 - IMPORT Writing Files
12:45:54 - IMPORT Writing file:
```

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**.



Paraben's E3:Multiple Packages - Alexis Cherpes Linux Forensics.e3

Conducting Forensic Investigations on Linux Systems (4e)
vWorkstation
2025-04-01 22:42:39
Alexis Cherpes

Search type: Text search
Search what: sudo dd if=/dev/sd
□ Match case □ Whole word
Use: Simple search
For binary data only
Interpret data with not detected encoding as:
Locale: en(English)
Code page: ASCII

Results: 4 Hits in 3 Places
1 Hit - Binary Data
Position 8169329 length 18 [MATCH: sudo dd if=/dev/sd]

Text View

```
....��|............._CMDLINE=sudo dd if=/dev/
sda of=/media/dominic/data/Ubuntu20.04.image
bs=4096 status=progress...........�.......;4�
.��Qj........�:z......�|......�|.............
_SYSTEMD_CGROUP=/user.slice/user-1000.slice/u
ser@1000.service/apps.slice/apps-org.gnome.Te
rminal.slice/vte-spawn-c5c52270-a045-44ff-ald
5-409dbb85070e.scope.............�........���
�.�B........`;z......�|.....H�|.............._
SYSTEMD_USER_UNIT=vte-spawn-c5c52270-a045-44f
f-ald5-409dbb85070e.scope.........w........��
���.�........�;z......�|.....��|............
_SYSTEMD_INVOCATION_ID=84c3fcac349044f090ffel
le642claff.........k.......�Y..............p�
|......�|......................_SOURCE_REALTIM
E_TIMESTAMP=1623405664170853.............�...
.....�t......�s��z�..L\.�....�m����C4�`�%�)�q�
```