

**Student:**

Jose Cruz

Email:

jose.cruz2@udc.edu

## Time on Task:

9 hours, 20 minutes

## Progress:

100%

Report Generated: Tuesday, April 4, 2023 at 11:42 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.

# Conducting Forensic Investigations on Linux Systems (4e)

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

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

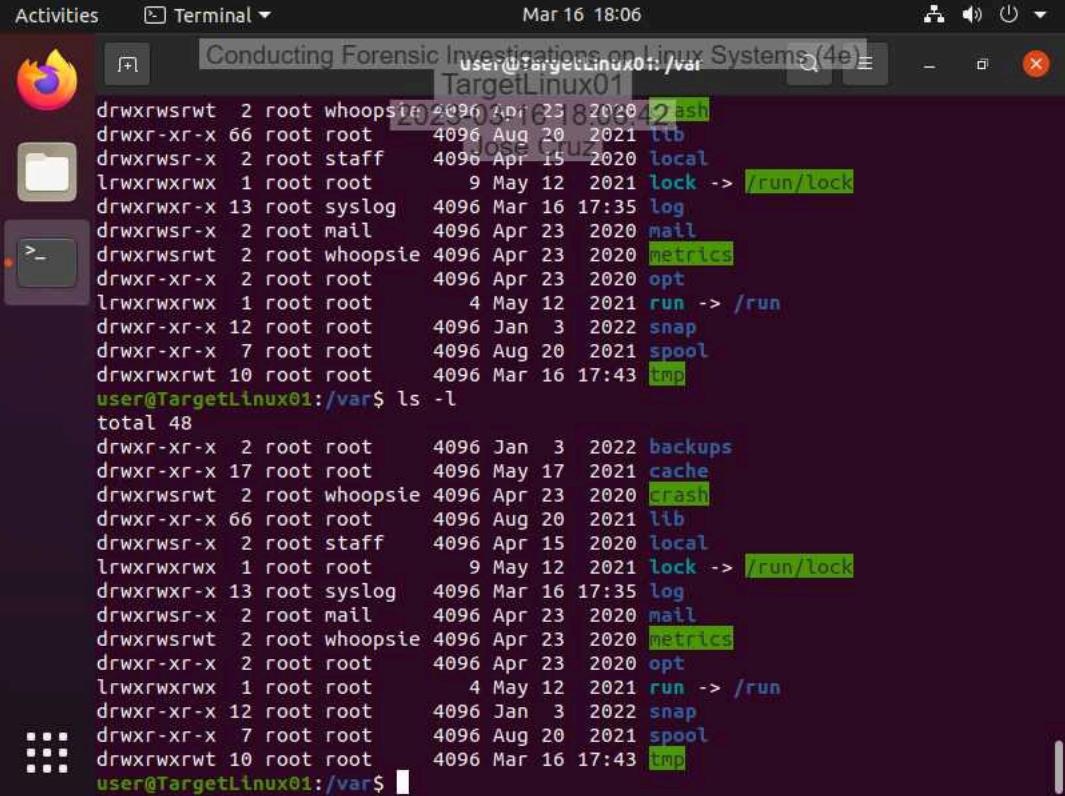
The screenshot shows a terminal window titled "Terminal" with the command "ls -l /etc" running. The output lists numerous files and directories with their permissions, ownership, modification times, and names. Key files visible include /etc/ctl.d, /etc/systemd, /etc/terminfo, /etc/thermald, /etc/timezone, /etc/tmpfiles.d, /etc/ubuntu-advantage, /etc/ucf.conf, /etc/udev, /etc/udisks2, /etc/ufw, /etc/update-manager, /etc/update-motd.d, /etc/update-notifier, /etc/UPower, /etc/usb\_modeswitch.conf, /etc/usb\_modeswitch.d, /etc/vim, /etc/vmware-tools, /etc/vtrgb, /etc/vulkan, /etc/wgetrc, /etc/wpa\_supplicant, /etc/X11, /etc/xattr.conf, /etc/xdg, and /etc/xml. The terminal prompt is "user@TargetLinux01:/etc\$".

```
drwxr-xr-x  2 root root 4096 May 17 2021 ctl.d
drwxr-xr-x  5 root root 4096 May 17 2021 systemd
drwxr-xr-x  2 root root 4096 Apr 23 2020 terminfo
drwxr-xr-x  2 root root 4096 May 17 2021 thermald
-rw-r--r--  1 root root 17 May 17 2021 timezone
drwxr-xr-x  2 root root 4096 Apr 22 2020 tmpfiles.d
drwxr-xr-x  2 root root 4096 May 17 2021 ubuntu-advantage
-rw-r--r--  1 root root 1260 Dec 14 2018 ucf.conf
drwxr-xr-x  4 root root 4096 May 17 2021 udev
drwxr-xr-x  2 root root 4096 Apr 23 2020 udisks2
drwxr-xr-x  3 root root 4096 Apr 23 2020 ufw
drwxr-xr-x  3 root root 4096 May 17 2021 update-manager
drwxr-xr-x  2 root root 4096 May 17 2021 update-motd.d
drwxr-xr-x  2 root root 4096 Apr  2 2020 update-notifier
drwxr-xr-x  2 root root 4096 Apr 23 2020 UPower
-rw-r--r--  1 root root 1523 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
d-----  1 root root 4096 Apr 23 2020 xml
Show Applications at root
user@TargetLinux01:/etc$
```

# Conducting Forensic Investigations on Linux Systems (4e)

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

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



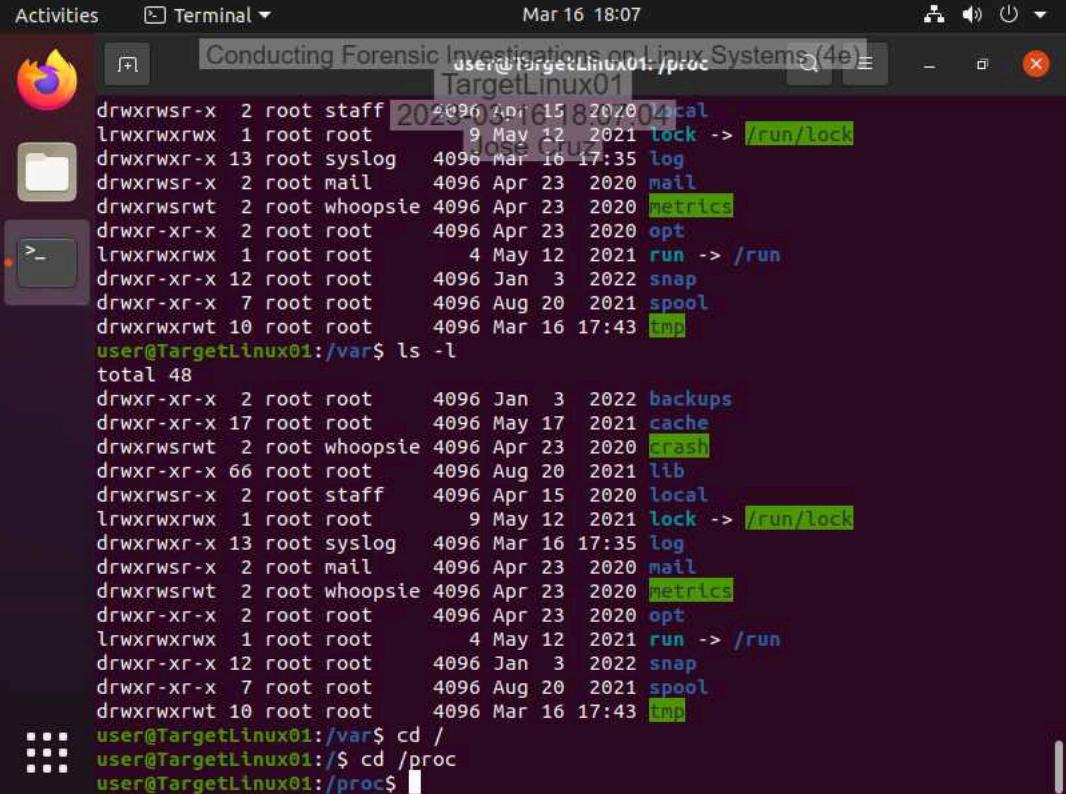
The screenshot shows a terminal window titled "user@TargetLinux01: /var\$". The command "ls -l" is run to list the contents of the /var directory. The output shows various files and directories with their permissions, last modified date, and names. Some files like "ash", "log", "metrics", "tmp", and "run" are highlighted in green, while others like "cache", "crash", "lib", "mail", and "spool" are highlighted in blue. The terminal window is part of a desktop environment with icons for a browser, file manager, and terminal visible in the dock.

```
drwxrwsrwt 2 root whoopsie 4096 Apr 23 2020 ash
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 Mar 16 17:35 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 Mar 16 17:43 tmp
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 Mar 16 17:35 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 Mar 16 17:43 tmp
user@TargetLinux01:/var$
```

# Conducting Forensic Investigations on Linux Systems (4e)

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

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



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "user@TargetLinux01:/proc". The terminal content displays the output of the "ls -l" command in the /proc directory, listing various files and directories with their permissions, modification times, and names. The "lock" file is shown as a symbolic link to "/run/lock". The "log" file is also present. Other files listed include "local", "cache", "metrics", "opt", "snap", "spool", and "tmp". The terminal prompt at the bottom is "user@TargetLinux01:/proc\$".

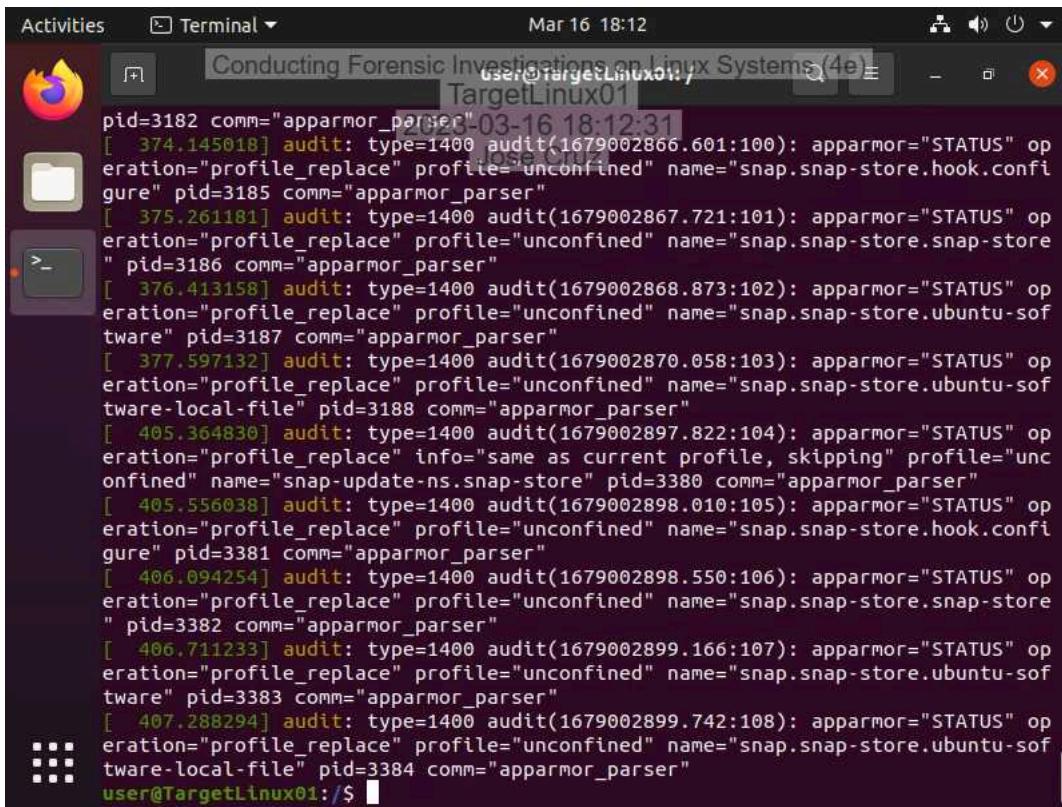
```
drwxrwsr-x 2 root staff 4096 Apr 15 2020 local
lrwxrwxrwx 1 root root 9 May 12 2021 lock -> /run/lock
drwxrwxr-x 13 root syslog 4096 Mar 16 17:35 log
drwxrwsr-x 2 root mail 4096 Apr 23 2020 mail
drwxrwsrwt 2 root whoopsie 4096 Apr 23 2020 metrics
drwxr-xr-x 2 root root 4096 Apr 23 2020 opt
lrwxrwxrwx 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
drwxrwsrwt 10 root root 4096 Mar 16 17:43 tmp
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 Mar 16 17:35 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
drwxrwsrwt 10 root root 4096 Mar 16 17:43 tmp
user@TargetLinux01:/var$ cd /
user@TargetLinux01:$ cd /proc
user@TargetLinux01:/proc$
```

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

# Conducting Forensic Investigations on Linux Systems (4e)

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

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



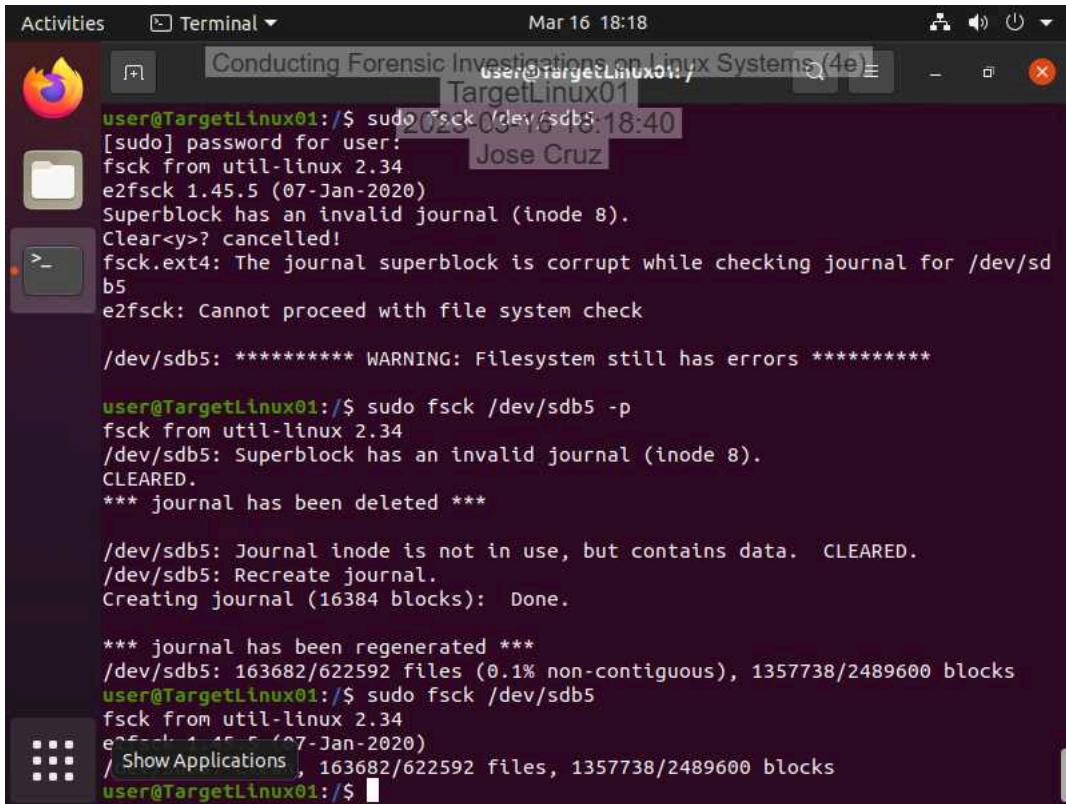
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Conducting Forensic Investigations on Linux Systems (4e)" and the command being run is "dmesg". The output of the command is displayed in the terminal window, showing multiple audit log entries from March 16, 2018, at 18:12:31. The logs detail various audit events related to apparmor\_parser processes and profile\_replace operations on snap.snap-store and snap.snap-store.ubuntu-software-local-file profiles. The terminal window is part of a desktop interface with icons for a browser, file manager, and terminal visible on the left.

```
pid=3182 comm="apparmor_parser" Mar 16 18:12:31 [ 374.145018] audit: type=1400 audit(1679002866.601:100): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.hook.configure" pid=3185 comm="apparmor_parser"
[ 375.261181] audit: type=1400 audit(1679002867.721:101): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.snap-store" pid=3186 comm="apparmor_parser"
[ 376.413158] audit: type=1400 audit(1679002868.873:102): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software" pid=3187 comm="apparmor_parser"
[ 377.597132] audit: type=1400 audit(1679002870.058:103): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software-local-file" pid=3188 comm="apparmor_parser"
[ 405.364830] audit: type=1400 audit(1679002897.822:104): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="snap-update-ns.snap-store" pid=3380 comm="apparmor_parser"
[ 405.556038] audit: type=1400 audit(1679002898.010:105): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.hook.configure" pid=3381 comm="apparmor_parser"
[ 406.094254] audit: type=1400 audit(1679002898.550:106): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.snap-store" pid=3382 comm="apparmor_parser"
[ 406.711233] audit: type=1400 audit(1679002899.166:107): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software" pid=3383 comm="apparmor_parser"
[ 407.288294] audit: type=1400 audit(1679002899.742:108): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software-local-file" pid=3384 comm="apparmor_parser"
```

# Conducting Forensic Investigations on Linux Systems (4e)

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

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



The screenshot shows a terminal window titled "Conducting Forensic Investigations on Linux Systems (4e)" running on a "TargetLinux01" host. The terminal displays the output of the fsck command being run on /dev/sdb and /dev/sdb5. The user, Jose Cruz, enters their password. The fsck process finds an invalid journal on the superblock and attempts to clear it, but fails due to a corrupted journal. It then creates a new journal on /dev/sdb5. The final output shows a regenerated journal with 163,682 files and 135,7738 blocks.

```
user@TargetLinux01:/$ sudo fsck /dev/sdb
[sudo] password for user: Jose Cruz
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 ***

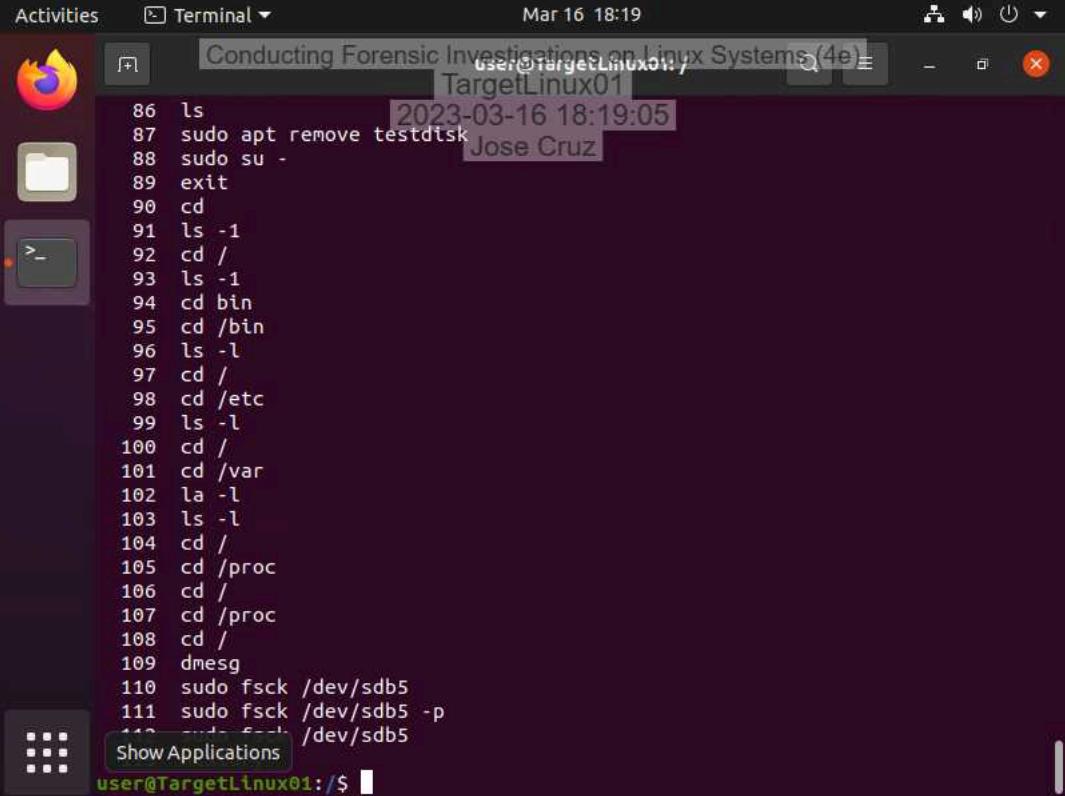
/dev/sdb5: Journal inode is not in use, but contains data. CLEARED.
/dev/sdb5: Recreate journal.
Creating journal (16384 blocks): Done.

*** journal has been regenerated ***
/dev/sdb5: 163682/622592 files (0.1% non-contiguous), 1357738/2489600 blocks
user@TargetLinux01:/$ sudo fsck /dev/sdb5
fsck from util-linux 2.34
e2fsck 1.45.5 (07-Jan-2020)
/ Show Applications, 163682/622592 files, 1357738/2489600 blocks
user@TargetLinux01:/$
```

# Conducting Forensic Investigations on Linux Systems (4e)

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

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



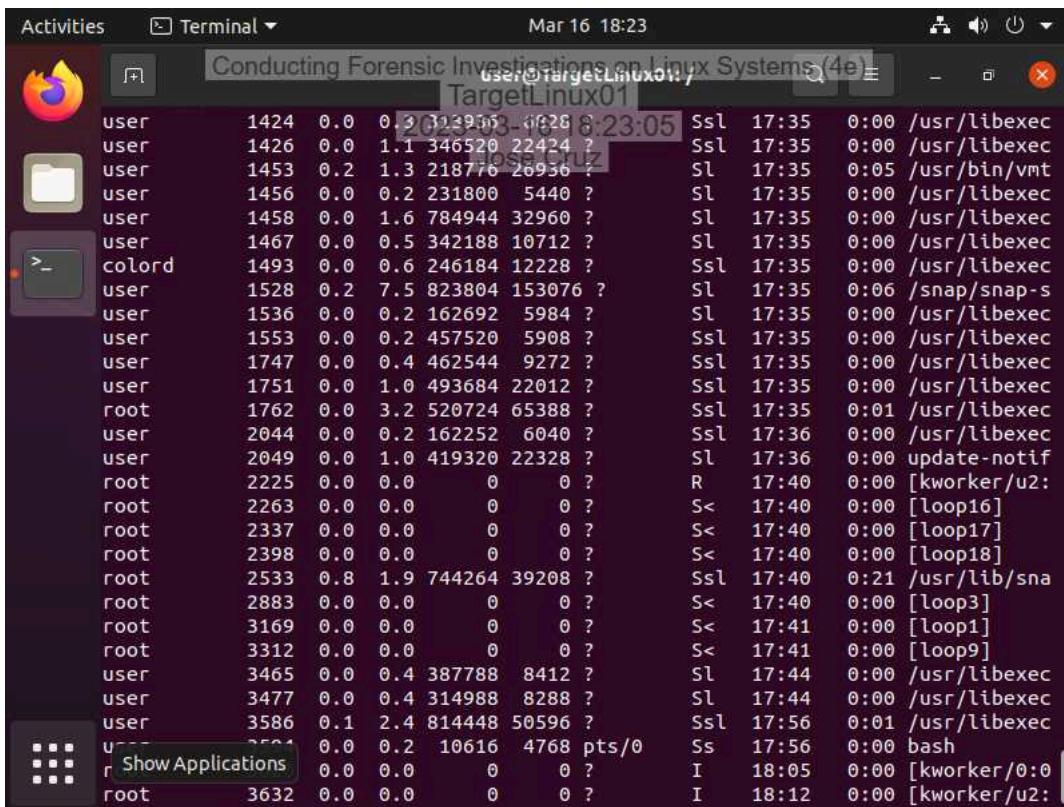
The screenshot shows a terminal window titled "user@TargetLinux01" with the command "history" running. The terminal output lists 112 commands, mostly related to navigating the file system and performing fsck checks on /dev/sdb5. The terminal interface includes a docked application bar on the left and a top panel with system icons.

```
86 ls [2023-03-16 18:19:05]
87 sudo apt remove testdisk
88 sudo su -
89 exit
90 cd
91 ls -l
92 cd /
93 ls -l
94 cd bin
95 cd /bin
96 ls -l
97 cd /
98 cd /etc
99 ls -l
100 cd /
101 cd /var
102 la -l
103 ls -l
104 cd /
105 cd /proc
106 cd /
107 cd /proc
108 cd /
109 dmesg
110 sudo fsck /dev/sdb5
111 sudo fsck /dev/sdb5 -p
112 sudo fsck /dev/sdb5
Show Applications
user@TargetLinux01:/$
```

# Conducting Forensic Investigations on Linux Systems (4e)

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

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



The screenshot shows a terminal window titled "Conducting Forensic Investigations on Linux Systems (4e)" with the command "ps aux" running. The output lists various processes with columns for User, PID, CPU usage, and Command. The terminal is part of a desktop environment with icons for Activities, Terminal, and Applications visible.

User	PID	CPU	Memory	Time	State	Command
user	1424	0.0	0.3 3119 10 0:028	17:35	Ssl	/usr/libexec
user	1426	0.0	1.1 346520 22424 ?	17:35	Ssl	/usr/libexec
user	1453	0.2	1.3 218776 26936 ?	17:35	Sl	/usr/bin/vmt
user	1456	0.0	0.2 231800 5440 ?	17:35	Sl	/usr/libexec
user	1458	0.0	1.6 784944 32960 ?	17:35	Sl	/usr/libexec
user	1467	0.0	0.5 342188 10712 ?	17:35	Sl	/usr/libexec
colord	1493	0.0	0.6 246184 12228 ?	17:35	Ssl	/usr/libexec
user	1528	0.2	7.5 823804 153076 ?	17:35	Sl	/snap/snap-s
user	1536	0.0	0.2 162692 5984 ?	17:35	Sl	/usr/libexec
user	1553	0.0	0.2 457520 5908 ?	17:35	Ssl	/usr/libexec
user	1747	0.0	0.4 462544 9272 ?	17:35	Ssl	/usr/libexec
user	1751	0.0	1.0 493684 22012 ?	17:35	Ssl	/usr/libexec
root	1762	0.0	3.2 520724 65388 ?	17:35	Ssl	/usr/libexec
user	2044	0.0	0.2 162252 6040 ?	17:36	Ssl	/usr/libexec
user	2049	0.0	1.0 419320 22328 ?	17:36	Sl	update-notif
root	2225	0.0	0.0 0 0 ?	17:40	R	[kworker/u2:
root	2263	0.0	0.0 0 0 ?	17:40	S<	[loop16]
root	2337	0.0	0.0 0 0 ?	17:40	S<	[loop17]
root	2398	0.0	0.0 0 0 ?	17:40	S<	[loop18]
root	2533	0.8	1.9 744264 39208 ?	17:40	Ssl	/usr/lib/sna
root	2883	0.0	0.0 0 0 ?	17:40	S<	[loop3]
root	3169	0.0	0.0 0 0 ?	17:41	S<	[loop1]
root	3312	0.0	0.0 0 0 ?	17:41	S<	[loop9]
user	3465	0.0	0.4 387788 8412 ?	17:44	Sl	/usr/libexec
user	3477	0.0	0.4 314988 8288 ?	17:44	Sl	/usr/libexec
user	3586	0.1	2.4 814448 50596 ?	17:56	Ssl	/usr/libexec
user	3591	0.0	0.2 10616 4768 pts/0	17:56	Ss	bash
r	Show Applications	0.0	0.0 0 0 ?	18:05	I	[kworker/0:0]
root	3632	0.0	0.0 0 0 ?	18:12	I	[kworker/u2:]

# Conducting Forensic Investigations on Linux Systems (4e)

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

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

The screenshot shows a Linux desktop environment with a terminal window open. The terminal title is "Conducting Forensic Investigations on Linux Systems (4e)". The terminal content displays the following:

```
user@TargetLinux01:~/.Documents$ ps aux
user      1553  0.0  0.2 4197540 5408 ? Ssl 17:35 0:00 /usr/libexec
user      1747  0.0  0.4 462544 9272 ? Ssl 17:35 0:00 /usr/libexec
user      1751  0.0  1.0 493684 22012 ? Ssl 17:35 0:00 /usr/libexec
root     1762  0.0  3.2 520724 65388 ? Ssl 17:35 0:01 /usr/libexec
user     2044  0.0  0.2 162252 6040 ? Ssl 17:36 0:00 /usr/libexec
user     2049  0.0  1.0 419320 22328 ? Sl 17:36 0:00 update-notif
root    2225  0.0  0.0      0 0 ? R 17:40 0:00 [kworker/u2:0]
root    2263  0.0  0.0      0 0 ? S< 17:40 0:00 [loop16]
root    2337  0.0  0.0      0 0 ? S< 17:40 0:00 [loop17]
root    2398  0.0  0.0      0 0 ? S< 17:40 0:00 [loop18]
root    2533  0.8  1.9 744264 39208 ? Ssl 17:40 0:21 /usr/lib/sna
root    2883  0.0  0.0      0 0 ? S< 17:40 0:00 [loop3]
root    3169  0.0  0.0      0 0 ? S< 17:41 0:00 [loop1]
root    3312  0.0  0.0      0 0 ? S< 17:41 0:00 [loop9]
user    3465  0.0  0.4 387788 8412 ? Sl 17:44 0:00 /usr/libexec
user    3477  0.0  0.4 314988 8288 ? Sl 17:44 0:00 /usr/libexec
user    3586  0.1  2.4 814448 50596 ? Ssl 17:56 0:01 /usr/libexec
user    3594  0.0  0.2 10616 4768 pts/0 Ss 17:56 0:00 bash
root    3620  0.0  0.0      0 0 ? I 18:05 0:00 [kworker/0:0]
root    3632  0.0  0.0      0 0 ? I 18:12 0:00 [kworker/u2:0]
root    3641  0.0  0.0      0 0 ? I 18:15 0:00 [kworker/0:2]
user    3660  0.0  0.1 11692 3632 pts/0 R+ 18:22 0:00 ps -aux

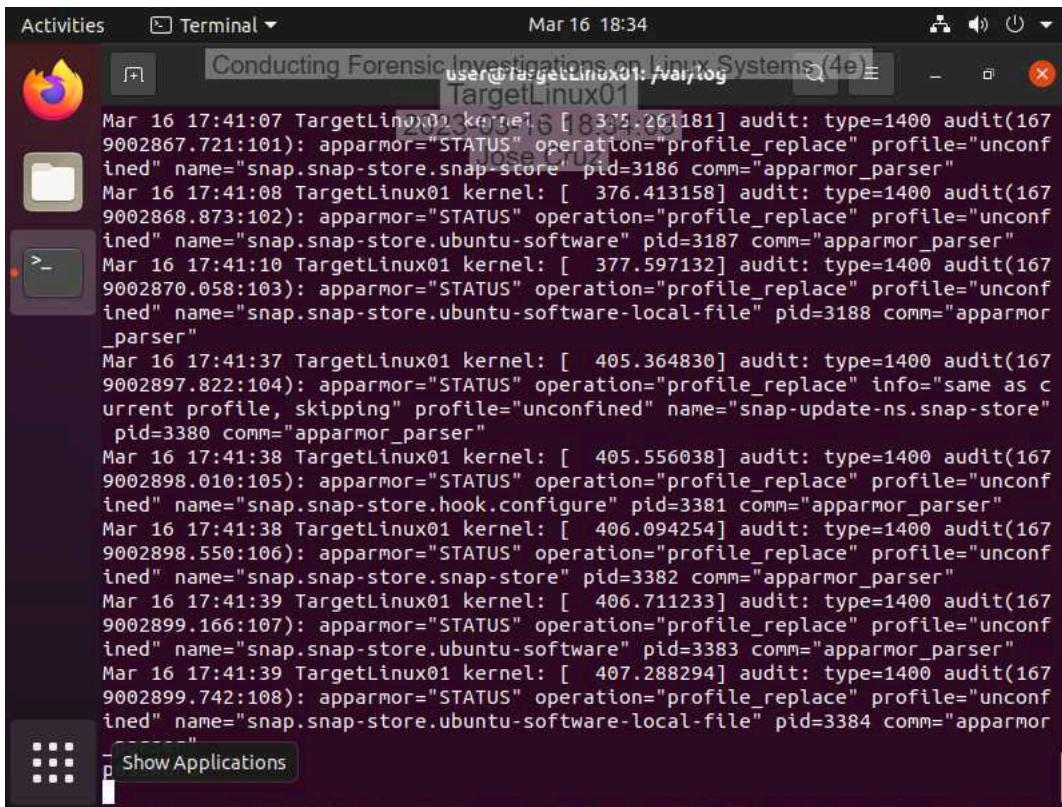
user@TargetLinux01:~/.Documents$ cd home/user/Documents
user@TargetLinux01:~/Documents$ ls
MyScheduler.txt
user@TargetLinux01:~/Documents$ file MyScheduler.txt
MyScheduler.txt: JPEG image data, JFIF standard 1.01, resolution (DPI), density
140x140, segment length 16, baseline, precision 8, 800x800, components 3
user@TargetLinux01:~/Documents$
```

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

# Conducting Forensic Investigations on Linux Systems (4e)

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

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



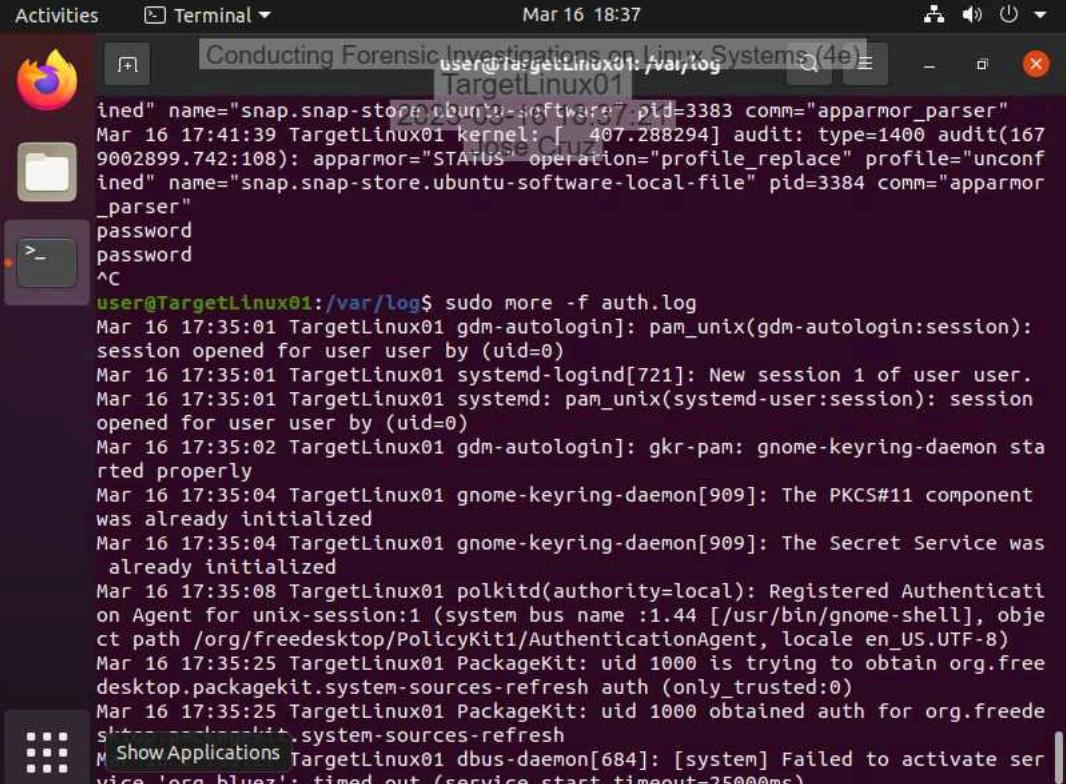
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Conducting Forensic Investigations on Linux Systems (4e)" and the path is "User@TargetLinux01: /var/log". The terminal displays a series of audit log entries from the kernel, specifically from the "kern" file. The log entries are timestamped and show various audit events related to apparmor\_parser operations on snap-related processes. The terminal window is part of a desktop interface with icons for a browser, file manager, and terminal visible in the dock.

```
Mar 16 17:41:07 TargetLinux01 kernel: [ 375.261181] audit: type=1400 audit(1679002867.721:101): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.snap-store" pid=3186 comm="apparmor_parser"
Mar 16 17:41:08 TargetLinux01 kernel: [ 376.413158] audit: type=1400 audit(1679002868.873:102): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software" pid=3187 comm="apparmor_parser"
Mar 16 17:41:10 TargetLinux01 kernel: [ 377.597132] audit: type=1400 audit(1679002870.058:103): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software-local-file" pid=3188 comm="apparmor_parser"
Mar 16 17:41:37 TargetLinux01 kernel: [ 405.364830] audit: type=1400 audit(1679002897.822:104): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="snap-update-ns.snap-store" pid=3380 comm="apparmor_parser"
Mar 16 17:41:38 TargetLinux01 kernel: [ 405.556038] audit: type=1400 audit(1679002898.010:105): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.hook.configure" pid=3381 comm="apparmor_parser"
Mar 16 17:41:38 TargetLinux01 kernel: [ 406.094254] audit: type=1400 audit(1679002898.550:106): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.snap-store" pid=3382 comm="apparmor_parser"
Mar 16 17:41:39 TargetLinux01 kernel: [ 406.711233] audit: type=1400 audit(1679002899.166:107): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software" pid=3383 comm="apparmor_parser"
Mar 16 17:41:39 TargetLinux01 kernel: [ 407.288294] audit: type=1400 audit(1679002899.742:108): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software-local-file" pid=3384 comm="apparmor_parser"
```

# Conducting Forensic Investigations on Linux Systems (4e)

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

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



The screenshot shows a terminal window titled "user@TargetLinux01: /var/log" with the command "sudo more -f auth.log" running. The terminal displays log entries from March 16, 2017, at 17:35:01. The log entries include system boot logs, user authentication attempts, and various system service interactions. The terminal interface includes a title bar, a menu bar with "Activities" and "Terminal", and a status bar showing the date and time.

```
user@TargetLinux01:/var/Log$ sudo more -f auth.log
Mar 16 17:35:01 TargetLinux01 gdm-autologin]: pam_unix(gdm-autologin:session): session opened for user user by (uid=0)
Mar 16 17:35:01 TargetLinux01 systemd-logind[721]: New session 1 of user user.
Mar 16 17:35:01 TargetLinux01 systemd: pam_unix(systemd-user:session): session opened for user user by (uid=0)
Mar 16 17:35:02 TargetLinux01 gdm-autologin]: gkr-pam: gnome-keyring-daemon started properly
Mar 16 17:35:04 TargetLinux01 gnome-keyring-daemon[909]: The PKCS#11 component was already initialized
Mar 16 17:35:04 TargetLinux01 gnome-keyring-daemon[909]: The Secret Service was already initialized
Mar 16 17:35:08 TargetLinux01 polkitd(authority=local): Registered Authentication Agent for unix-session:1 (system bus name :1.44 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Mar 16 17:35:25 TargetLinux01 PackageKit: uid 1000 is trying to obtain org.freedesktop.packagekit.system-sources-refresh auth (only_trusted:0)
Mar 16 17:35:25 TargetLinux01 PackageKit: uid 1000 obtained auth for org.freedesktop.packagekit.system-sources-refresh
M Show Applications TargetLinux01 dbus-daemon[684]: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms)
```

## 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.

The first unauthorized username was "gdm" and "pam\_unix". The number of attempts for gdm was 6 max entries and for pam\_unix was 5 attempts. The date and time for gdm was Jun 11 at 4:47:50. For user pam\_unix date and time was Jun 11 at 5:05:01. Seems the Ip address for both users are 192.168.78.1. The ports being used are 22, 4663, and 3521.

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

User gdm date and time of opened session was in June 11 at 06:08:53. For user pam\_unix the date and time is June 11 at 06:09:01.

### 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.

Seems in the advance search the software "logkeys" was installed on June 10 at 10:44:57.

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

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

The current USB was connected on June 10 at 10:10:24:42, in addition the serial number for the usb is = 3.

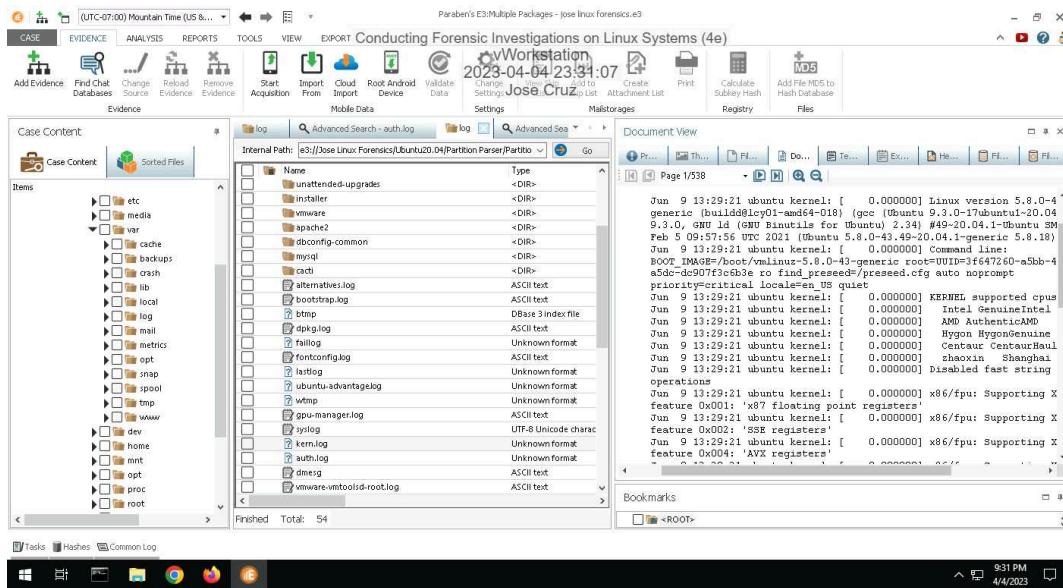
# Conducting Forensic Investigations on Linux Systems (4e)

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

## 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.



### 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.

