

Conducting Forensic Investigations on Linux Systems (4e)

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

Student:

Loksharan Saravanan

Email:

loksharan.soc@gmail.com

Time on Task:

0 hours, 48 minutes

Progress:

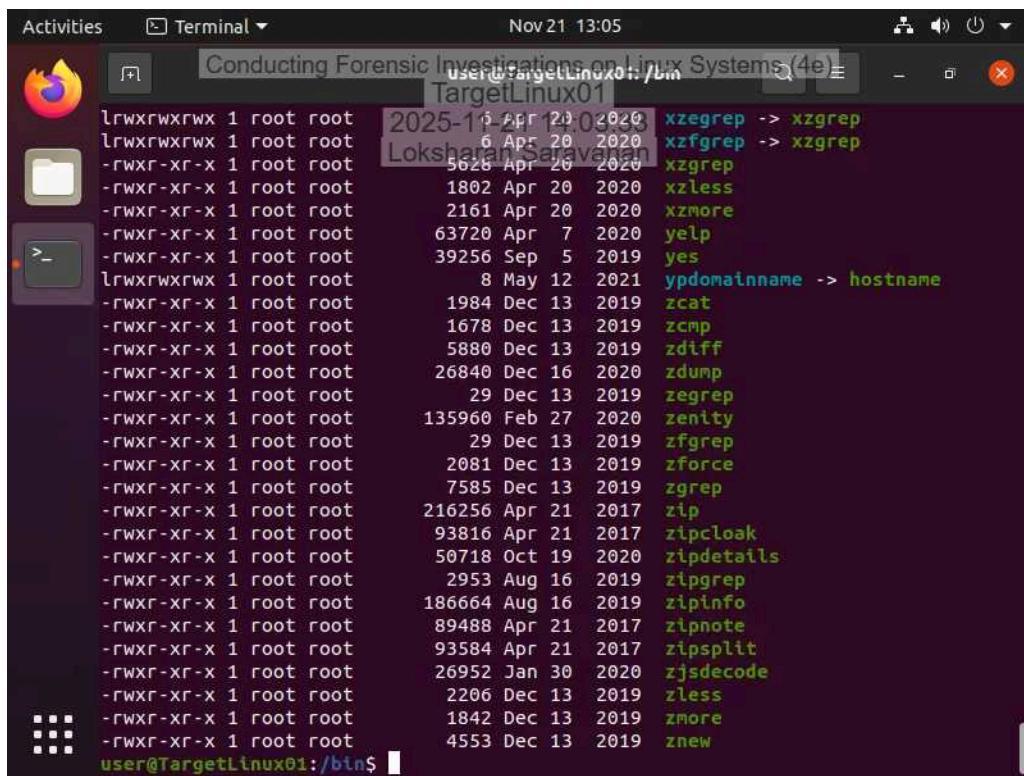
100%

Report Generated: Friday, November 21, 2025 at 1:52 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.



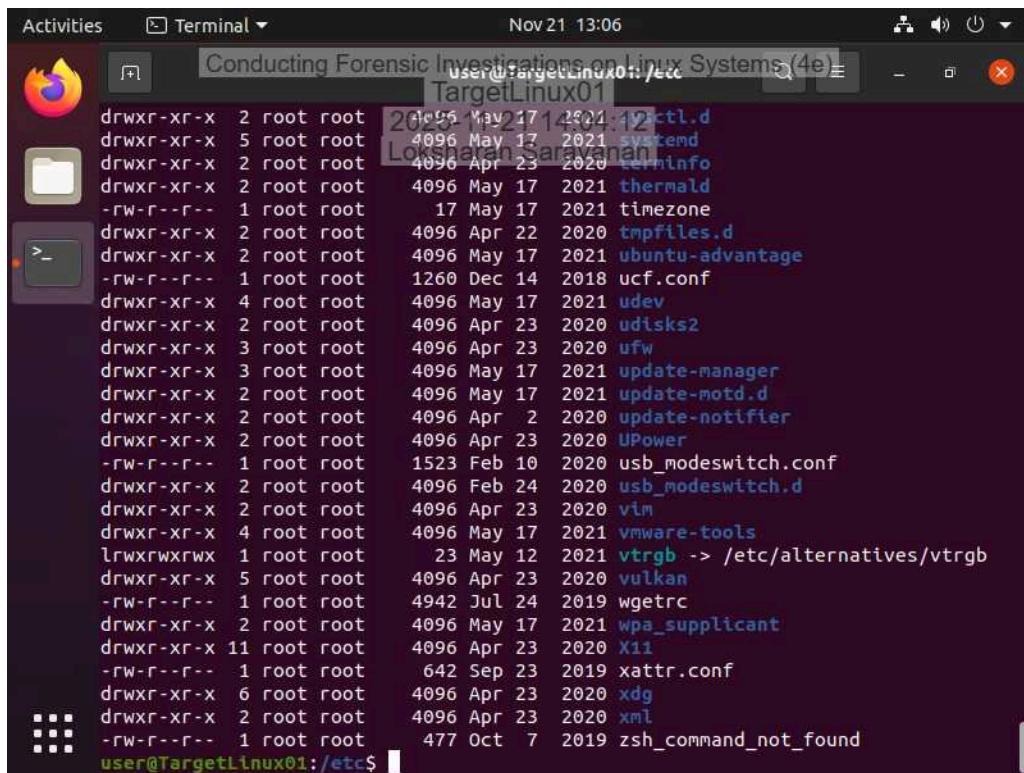
The screenshot shows a Linux desktop environment with a terminal window open. The terminal title is "Conducting Forensic Investigations on Linux Systems (4e)" and the command entered is "ls -l /bin". The output lists numerous executable files in the /bin directory, all owned by root and executable by root. The files are sorted by modification date, with the most recent file being "znew" (modified on Dec 13, 2019). Other files include "xzgrep", "xzgrep", "xzgrep", "xzless", "xzmore", "yelp", "yes", "ypdomainname", "zcat", "zcmp", "zdiff", "zdump", "zegrep", "zenity", "zfgrep", "zforce", "zgrep", "zip", "zipcloak", "zipdetails", "zipgrep", "zipinfo", "zipnote", "zipsplit", "zjsdecode", "zless", "zmore", and "znew".

```
user@TargetLinux01:/bin$ ls -l
total 1280
lrwxrwxrwx 1 root root 2025-11-21 14:00 xzgrep -> xzgrep
lrwxrwxrwx 1 root root 2025-11-21 14:00 xzgrep -> xzgrep
-rwxr-xr-x 1 root root 5628 Apr 20 2020 xzgrep
-rwxr-xr-x 1 root root 1802 Apr 20 2020 xzless
-rwxr-xr-x 1 root root 2161 Apr 20 2020 xzmore
-rwxr-xr-x 1 root root 63720 Apr 7 2020 yelp
-rwxr-xr-x 1 root root 39256 Sep 5 2019 yes
lrwxrwxrwx 1 root root 8 May 12 2021 ypdomainname -> hostname
-rwxr-xr-x 1 root root 1984 Dec 13 2019 zcat
-rwxr-xr-x 1 root root 1678 Dec 13 2019 zcmp
-rwxr-xr-x 1 root root 5880 Dec 13 2019 zdiff
-rwxr-xr-x 1 root root 26840 Dec 16 2020 zdump
-rwxr-xr-x 1 root root 29 Dec 13 2019 zegrep
-rwxr-xr-x 1 root root 135960 Feb 27 2020 zenity
-rwxr-xr-x 1 root root 29 Dec 13 2019 zfgrep
-rwxr-xr-x 1 root root 2081 Dec 13 2019 zforce
-rwxr-xr-x 1 root root 7585 Dec 13 2019 zgrep
-rwxr-xr-x 1 root root 216256 Apr 21 2017 zip
-rwxr-xr-x 1 root root 93816 Apr 21 2017 zipcloak
-rwxr-xr-x 1 root root 50718 Oct 19 2020 zipdetails
-rwxr-xr-x 1 root root 2953 Aug 16 2019 zipgrep
-rwxr-xr-x 1 root root 186664 Aug 16 2019 zipinfo
-rwxr-xr-x 1 root root 89488 Apr 21 2017 zipnote
-rwxr-xr-x 1 root root 93584 Apr 21 2017 zipsplit
-rwxr-xr-x 1 root root 26952 Jan 30 2020 zjsdecode
-rwxr-xr-x 1 root root 2206 Dec 13 2019 zless
-rwxr-xr-x 1 root root 1842 Dec 13 2019 zmore
-rwxr-xr-x 1 root root 4553 Dec 13 2019 znew
```

Conducting Forensic Investigations on Linux Systems (4e)

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

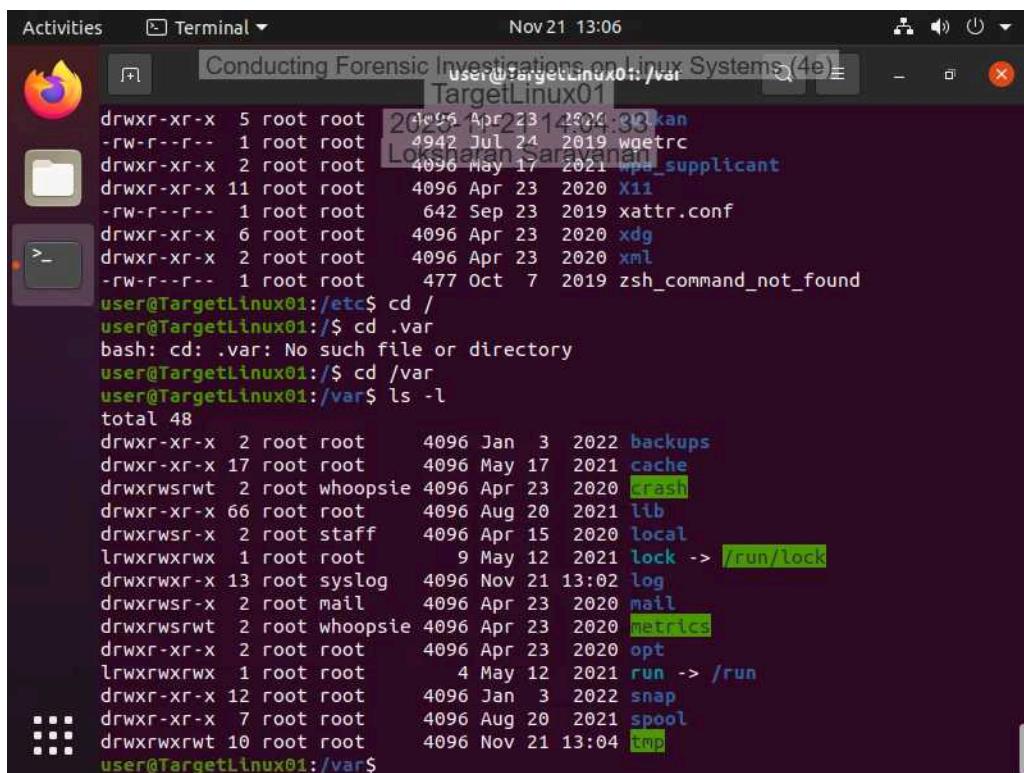
20. Make a screen capture showing the contents of the /etc directory.



A screenshot of a Linux desktop environment showing a terminal window. The terminal title is "Conducting Forensic Investigations on Linux Systems (4e)" and the command entered is "ls -l /etc". The output lists numerous files and directories with their permissions, ownership, and timestamps. Some files are highlighted in blue, such as "vtrgb", "vulkan", "wpa_supplicant", "X11", "xattr.conf", "xdg", "xml", and "zsh_command_not_found".

```
drwxr-xr-x  2 root root 4096 May 17 2021 acpi
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 thermal
-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-adantage
-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  2 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
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$
```

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



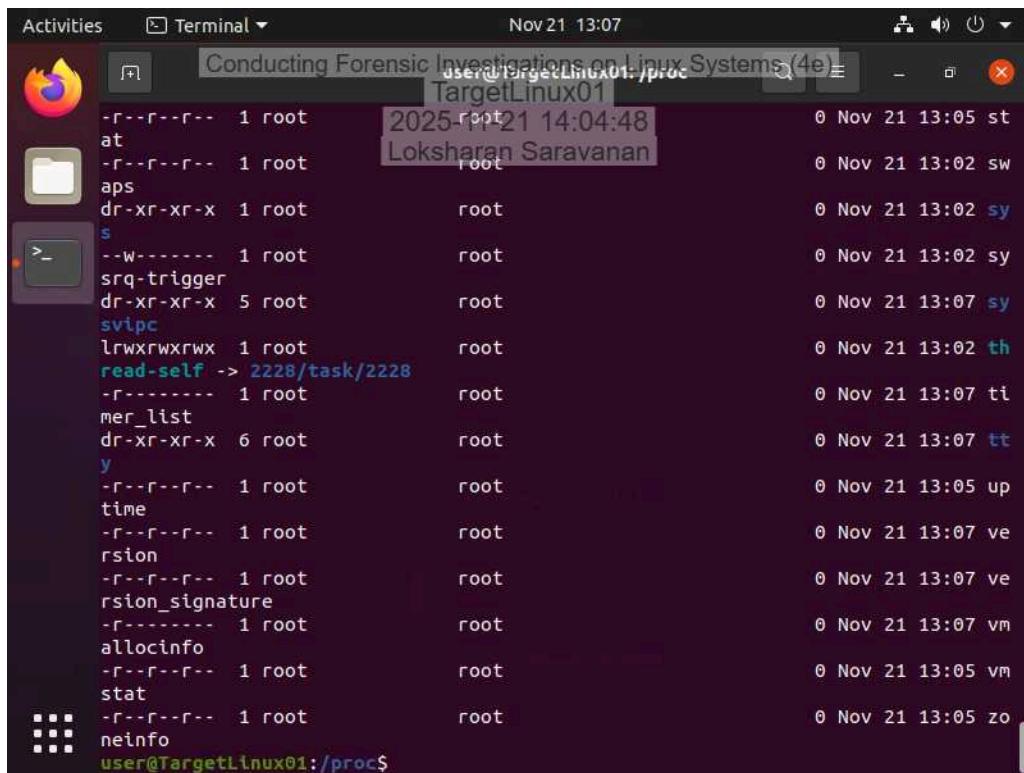
A screenshot of a Linux desktop environment showing a terminal window. The terminal title is "Conducting Forensic Investigations on Linux Systems (4e)" and the commands entered are "cd /", "cd .var", "ls", and "cd /var". The output shows the contents of the /var directory, which includes subdirectories like backups, cache, crash, lib, local, lock, log, mail, metrics, opt, run, snap, spool, and tmp. Some files are highlighted in blue, such as "lock", "log", "mail", "metrics", "opt", "run", "snap", and "spool".

```
drwxr-xr-x  5 root root 4096 Apr 23 2020 .config
-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
bash: cd: .var: No such file or directory
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 Nov 21 13:02 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 Nov 21 13:04 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 terminal window titled "Conducting Forensic Investigations on Linux Systems (4e)" with the command "user@TargetLinux01:/proc\$" at the bottom. The window displays a long list of files and directories in the /proc directory, including "at", "aps", "s", "srq-trigger", "svipc", "read-self", "mer_list", "y", "time", "rsion", "rsion_signature", "allocinfo", "stat", and "neinfo". The "read-self" file is highlighted with a cursor. The terminal interface includes a dock with icons for a browser, file manager, terminal, and others, and a top bar with system status indicators.

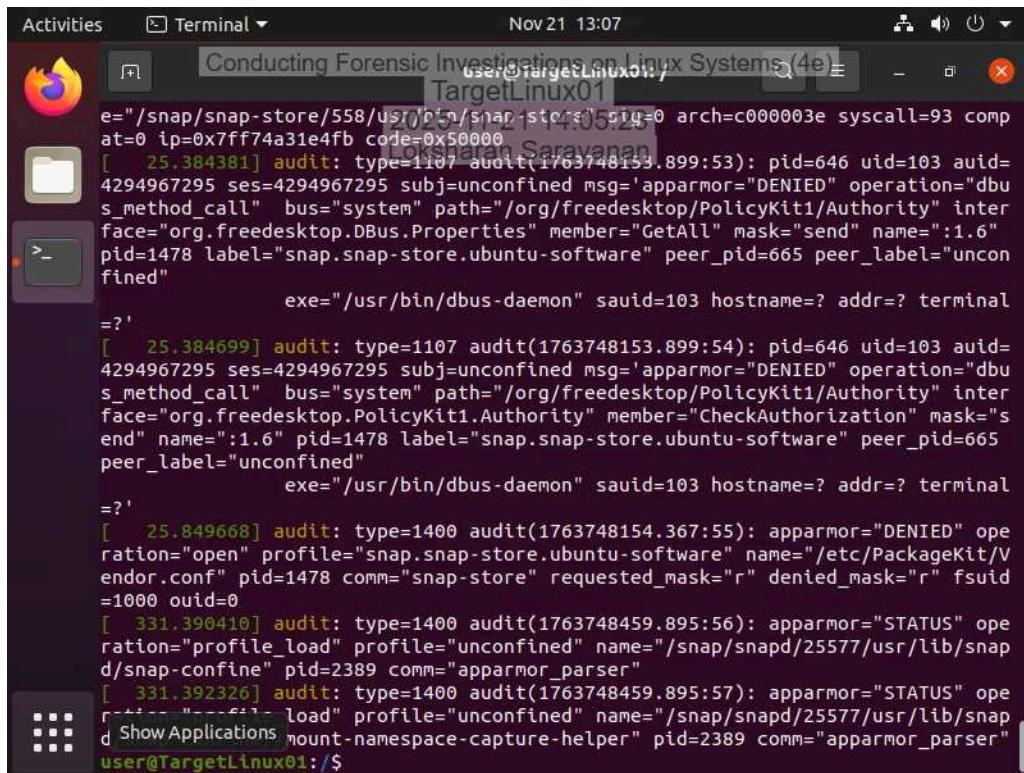
```
user@TargetLinux01:/proc$ ls
at                                2025-11-21 14:04:48
aps                               root
dr-xr-xr-x  1 root                root
s                                 root
--w-----  1 root                root
dr-xr-xr-x  5 root                root
srq-trigger
svipc
lrwxrwxrwx  1 root                root
read-self -> 2228/task/2228
dr-xr-xr-x  6 root                root
mer_list
dr-xr-xr-x  1 root                root
y
dr-xr-xr-x  1 root                root
time
dr-xr-xr-x  1 root                root
rsion
dr-xr-xr-x  1 root                root
rsion_signature
dr-xr-xr-x  1 root                root
allocinfo
dr-xr-xr-x  1 root                root
stat
dr-xr-xr-x  1 root                root
neinfo
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.



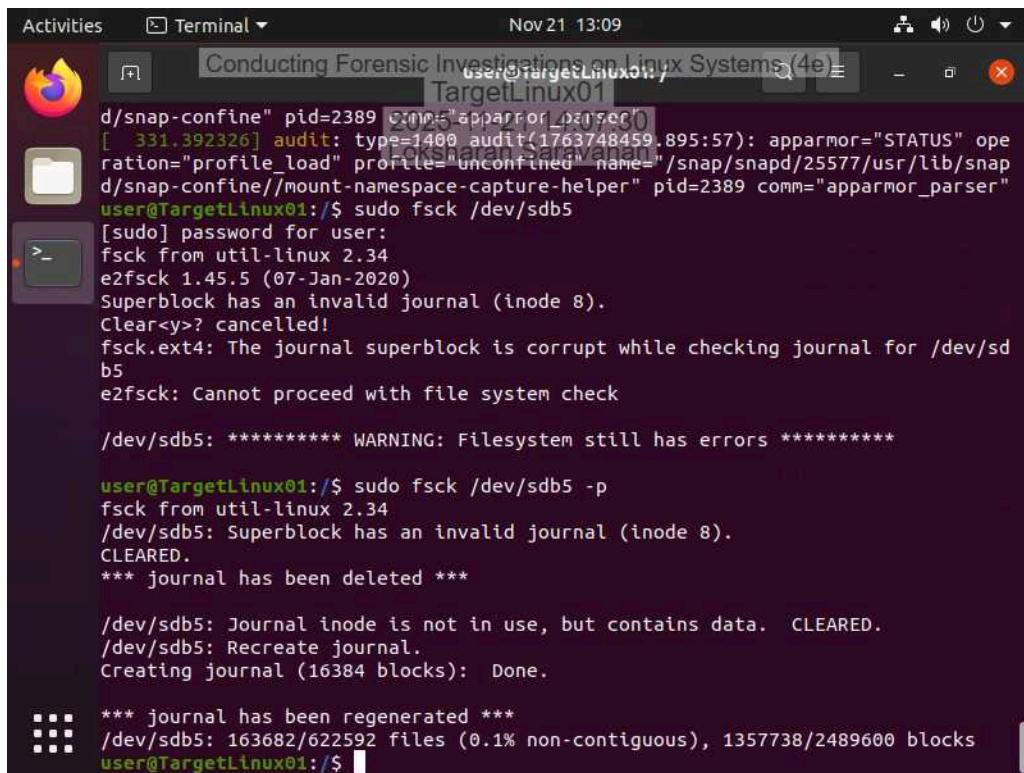
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Conducting Forensic Investigations on Linux Systems (4e)" and the command being run is "dmesg". The output of the command is displayed in the terminal window, showing several audit log entries. The entries include details such as timestamp, audit ID, PID, UID, AUID, session ID, subject, operation, bus, interface, member, mask, name, label, peer PID, peer label, and executable path. One entry specifically mentions "apparmor=DENIED" for an "open" operation on a file named "/etc/PackageKit/Vendor.conf". Another entry shows an "audit" type=1400 audit(1763748459.895:57) for a "mount" operation on a "mount-namespace-capture-helper" file.

```
e="/snap/snap-store/558/usr/bin/snap-store" sig=0 arch=c000003e syscall=93 comp at=0 ip=0x7ff74a31e4fb code=0x50000
[ 25.384381] audit: type=1107 audit(1763748153.899:53): pid=646 uid=103 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call" bus="system" path="/org/freedesktop/PolicyKit1/Authority" interface="org.freedesktop.DBus.Properties" member="GetAll" mask="send" name=:1.6' pid=1478 label="snap.snap-store.ubuntu-software" peer_pid=665 peer_label="unconfined"
          exe="/usr/bin/dbus-daemon" sauid=103 hostname=? addr=? terminal=?
[ 25.384699] audit: type=1107 audit(1763748153.899:54): pid=646 uid=103 auid=4294967295 ses=4294967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call" bus="system" path="/org/freedesktop/PolicyKit1/Authority" interface="org.freedesktop.PolicyKit1.Authority" member="CheckAuthorization" mask="send" name=:1.6' pid=1478 label="snap.snap-store.ubuntu-software" peer_pid=665 peer_label="unconfined"
          exe="/usr/bin/dbus-daemon" sauid=103 hostname=? addr=? terminal=?
[ 25.849668] audit: type=1400 audit(1763748154.367:55): apparmor="DENIED" operation="open" profile="snap.snap-store.ubuntu-software" name="/etc/PackageKit/Vendor.conf" pid=1478 comm="snap-store" requested_mask="r" denied_mask="r" fsuid=1000 ouid=0
[ 331.390410] audit: type=1400 audit(1763748459.895:56): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/snap/snapd/25577/usr/lib/snapd/snap-confine" pid=2389 comm="apparmor_parser"
[ 331.392326] audit: type=1400 audit(1763748459.895:57): apparmor="STATUS" operation="mount" profile="unconfined" name="/snap/snapd/25577/usr/lib/snapd>Show Applications mount-namespace-capture-helper" pid=2389 comm="apparmor_parser"
user@TargetLinux01:/$
```

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.



A screenshot of a terminal window titled "Conducting Forensic Investigations on Linux Systems (4e)" running on a "TargetLinux01" host. The terminal shows the user performing two fsck operations on the /dev/sdb5 partition. The first run finds an invalid journal and fails to proceed due to corruption. The second run successfully regenerates the journal. The terminal window also displays the user's name and the date and time of the session.

```
d/snap-confine" pid=2389 comm="apparmor_parser"
[ 331.392326] audit: type=1400 audit(1763748459.895:57): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/snap/snapd/25577/usr/lib/snapd/snap-confine/mount-n namespace-capture-helper" pid=2389 comm="apparmor_parser"
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/sdb5
e2fsck: Cannot proceed with file system check

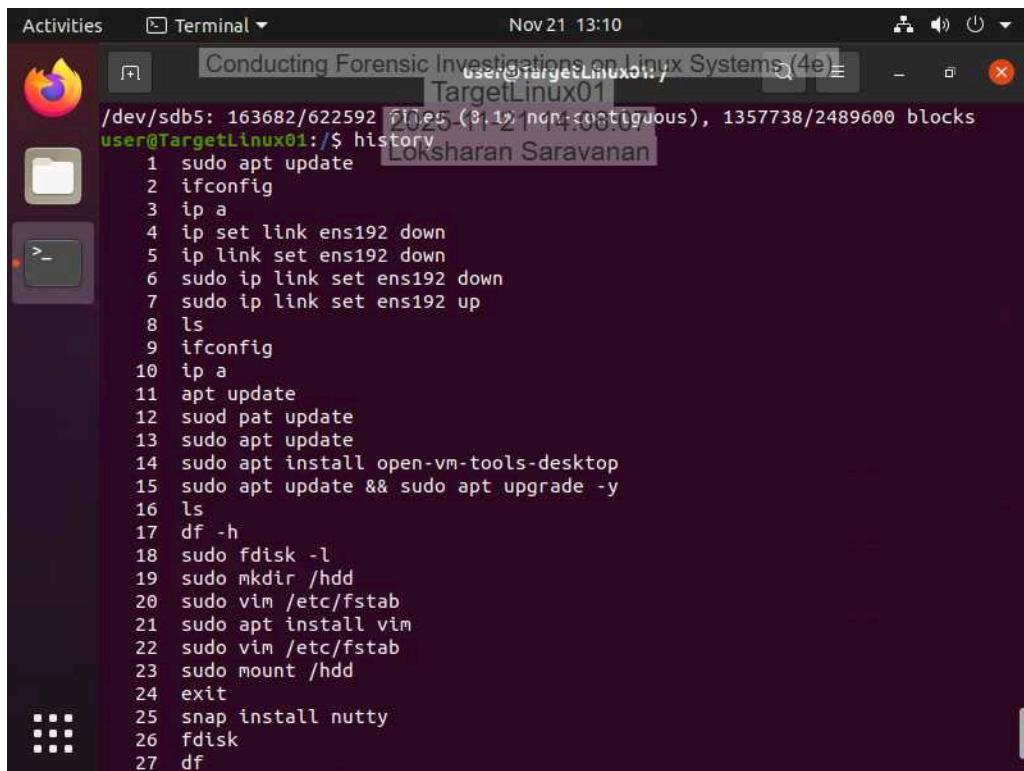
/dev/sdb5: ***** WARNING: Filesystem still has errors *****

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.



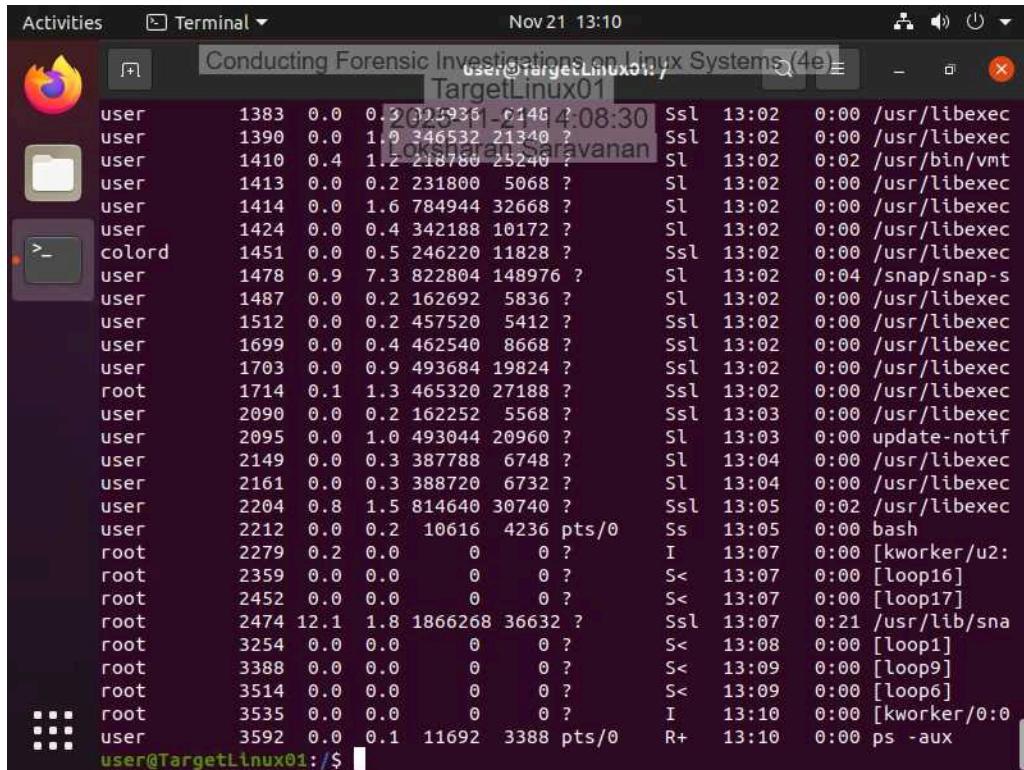
A screenshot of a terminal window titled "Conducting Forensic Investigations on Linux Systems (4e)" running on a "TargetLinux01" host. The terminal shows the user listing their command history, which includes various system administration tasks such as apt updates, network configuration changes, and file system management. The terminal window also displays the user's name and the date and time of the session.

```
/dev/sdb5: 163682/622592 files (0.1% non-contiguous), 1357738/2489600 blocks
user@TargetLinux01:~$ history
 1 sudo apt update
 2 ifconfig
 3 ip a
 4 ip link set 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
```

Conducting Forensic Investigations on Linux Systems (4e)

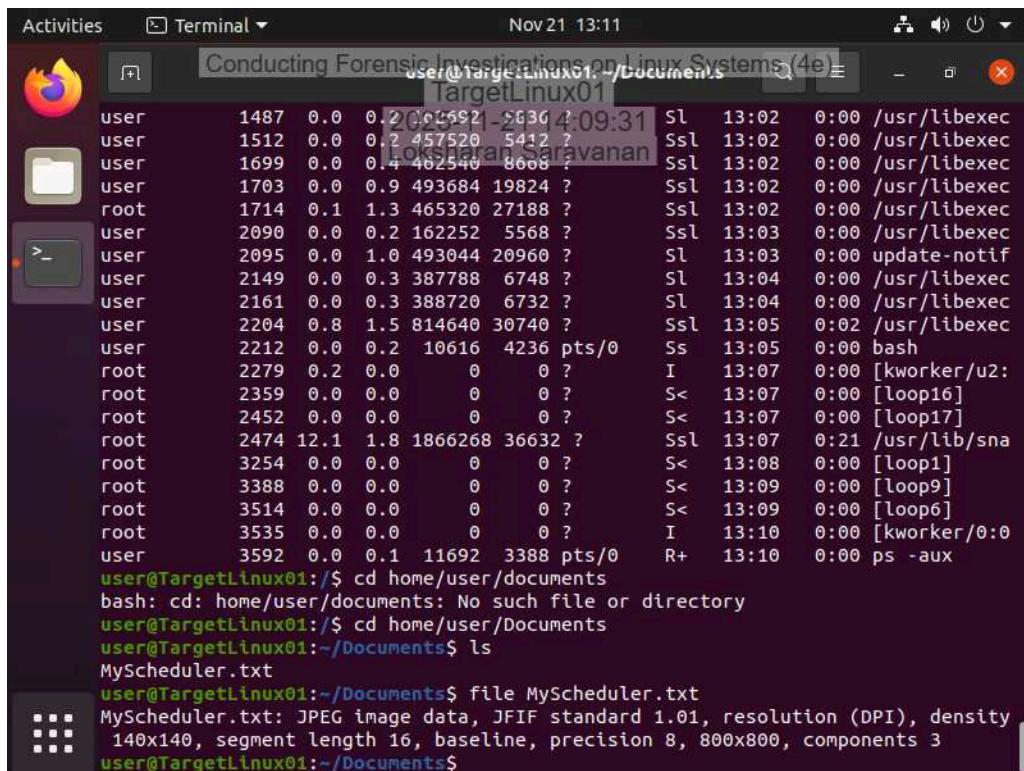
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 06

11. Make a screen capture showing the running processes.



```
Nov 21 13:10
user      1383  0.0  0.3 2015938 6146 ? Ssl 13:02  0:00 /usr/libexec
user      1390  0.0  1.0 346532 21340 ? Ssl 13:02  0:00 /usr/libexec
user      1410  0.4  1.2 218760 25240 ? Sl 13:02  0:02 /usr/bin/vmt
user      1413  0.0  0.2 231800 5068 ? Sl 13:02  0:00 /usr/libexec
user      1414  0.0  1.6 784944 32668 ? Sl 13:02  0:00 /usr/libexec
user      1424  0.0  0.4 342188 10172 ? Sl 13:02  0:00 /usr/libexec
colord   1451  0.0  0.5 246220 11828 ? Ssl 13:02  0:00 /usr/libexec
user      1478  0.9  7.3 822804 148976 ? Sl 13:02  0:04 /snap/snap-s
user      1487  0.0  0.2 162692 5836 ? Sl 13:02  0:00 /usr/libexec
user      1512  0.0  0.2 457520 5412 ? Ssl 13:02  0:00 /usr/libexec
user      1699  0.0  0.4 462540 8668 ? Ssl 13:02  0:00 /usr/libexec
user      1703  0.0  0.9 493684 19824 ? Ssl 13:02  0:00 /usr/libexec
root     1714  0.1  1.3 465320 27188 ? Ssl 13:02  0:00 /usr/libexec
user      2090  0.0  0.2 162252 5568 ? Ssl 13:03  0:00 /usr/libexec
user      2095  0.0  1.0 493044 20960 ? Sl 13:03  0:00 update-notif
user      2149  0.0  0.3 387788 6748 ? Sl 13:04  0:00 /usr/libexec
user      2161  0.0  0.3 388720 6732 ? Sl 13:04  0:00 /usr/libexec
user      2204  0.8  1.5 814640 30740 ? Ssl 13:05  0:02 /usr/libexec
user      2212  0.0  0.2 10616 4236 pts/0 Ss 13:05  0:00 bash
root     2279  0.2  0.0      0      ? I 13:07  0:00 [kworker/u2:
root     2359  0.0  0.0      0      ? S< 13:07  0:00 [loop16]
root     2452  0.0  0.0      0      ? S< 13:07  0:00 [loop17]
root     2474 12.1  1.8 1866268 36632 ? Ssl 13:07  0:21 /usr/lib/sna
root     3254  0.0  0.0      0      ? S< 13:08  0:00 [loop1]
root     3388  0.0  0.0      0      ? S< 13:09  0:00 [loop9]
root     3514  0.0  0.0      0      ? S< 13:09  0:00 [loop6]
root     3535  0.0  0.0      0      ? I 13:10  0:00 [kworker/0:0
user      3592  0.0  0.1 11692 3388 pts/0 R+ 13:10  0:00 ps -aux
user@TargetLinux01:$
```

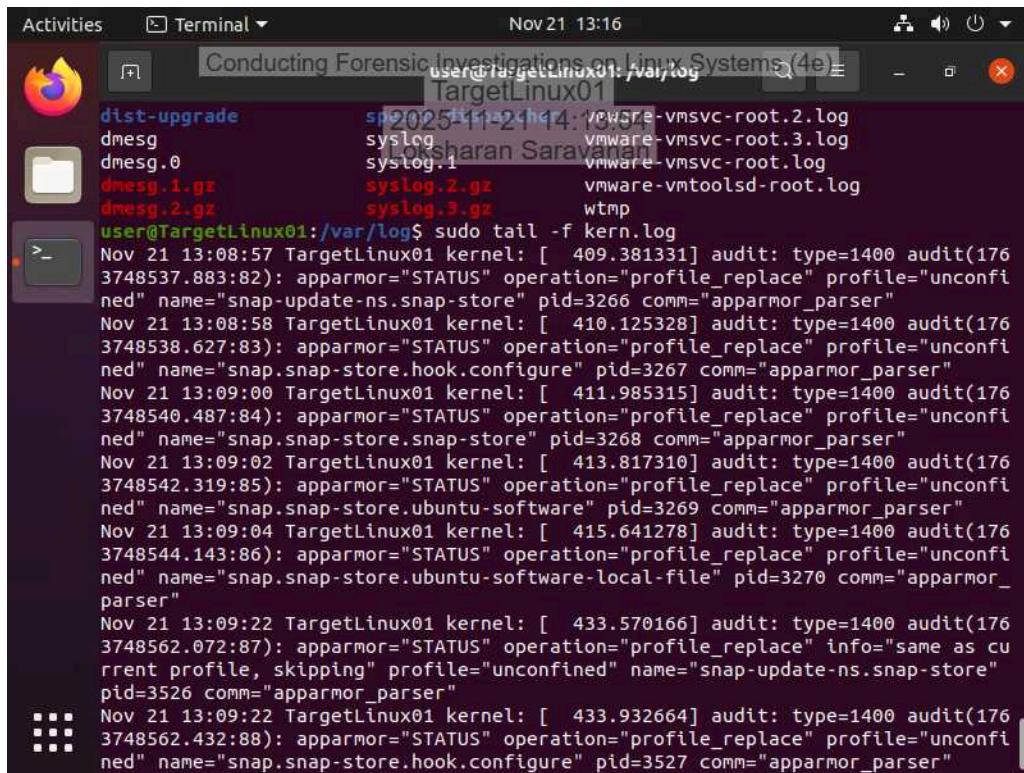
15. Make a screen capture showing the results of the file command.



```
Nov 21 13:11
user      1487  0.0  0.2 201592 5636 ? Sl 13:02  0:00 /usr/libexec
user      1512  0.0  0.2 457520 5412 ? Ssl 13:02  0:00 /usr/libexec
user      1699  0.0  0.4 462540 8668 ? Ssl 13:02  0:00 /usr/libexec
user      1703  0.0  0.9 493684 19824 ? Ssl 13:02  0:00 /usr/libexec
root     1714  0.1  1.3 465320 27188 ? Ssl 13:02  0:00 /usr/libexec
user      2090  0.0  0.2 162252 5568 ? Ssl 13:03  0:00 /usr/libexec
user      2095  0.0  1.0 493044 20960 ? Sl 13:03  0:00 update-notif
user      2149  0.0  0.3 387788 6748 ? Sl 13:04  0:00 /usr/libexec
user      2161  0.0  0.3 388720 6732 ? Sl 13:04  0:00 /usr/libexec
user      2204  0.8  1.5 814640 30740 ? Ssl 13:05  0:02 /usr/libexec
user      2212  0.0  0.2 10616 4236 pts/0 Ss 13:05  0:00 bash
root     2279  0.2  0.0      0      ? I 13:07  0:00 [kworker/u2:
root     2359  0.0  0.0      0      ? S< 13:07  0:00 [loop16]
root     2452  0.0  0.0      0      ? S< 13:07  0:00 [loop17]
root     2474 12.1  1.8 1866268 36632 ? Ssl 13:07  0:21 /usr/lib/sna
root     3254  0.0  0.0      0      ? S< 13:08  0:00 [loop1]
root     3388  0.0  0.0      0      ? S< 13:09  0:00 [loop9]
root     3514  0.0  0.0      0      ? S< 13:09  0:00 [loop6]
root     3535  0.0  0.0      0      ? I 13:10  0:00 [kworker/0:0
user      3592  0.0  0.1 11692 3388 pts/0 R+ 13:10  0:00 ps -aux
user@TargetLinux01:$ cd home/user/documents
bash: cd: home/user/documents: No such file or directory
user@TargetLinux01:$ 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

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



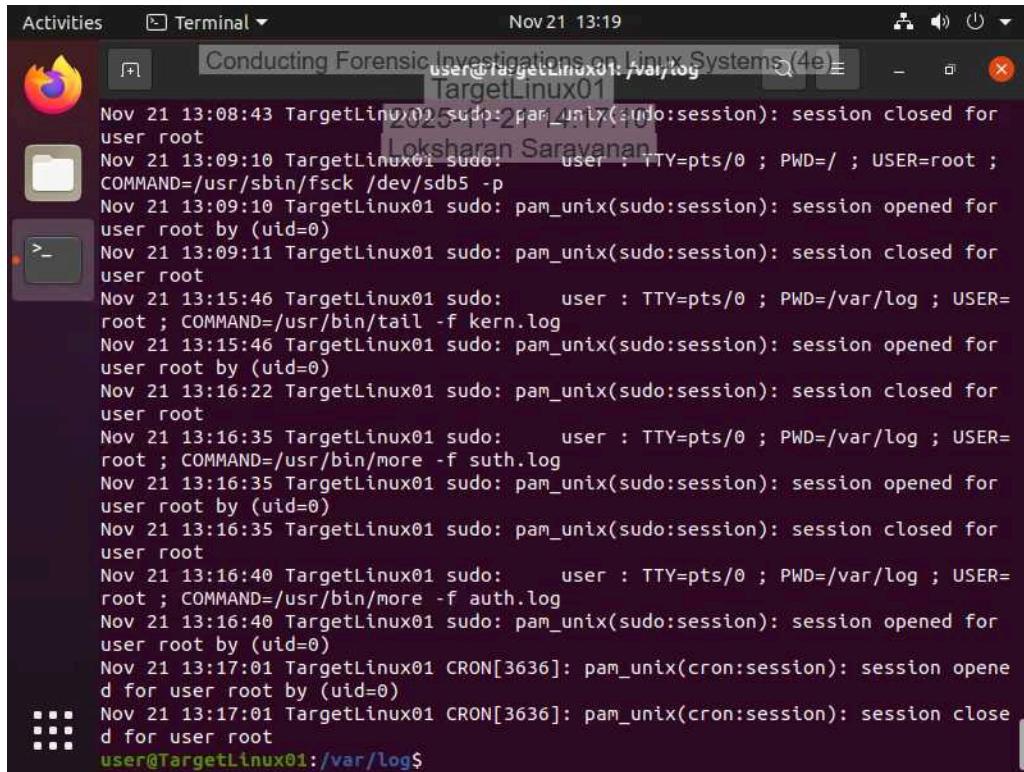
The screenshot shows a terminal window on a dark-themed desktop environment. The title bar indicates the session is titled "Conducting Forensic Investigations on Linux Systems (4e)" and the user is at "TargetLinux01" in the "/var/log" directory. The date and time shown are Nov 21 13:16. The terminal window displays the output of the command "sudo tail -f kern.log". The log entries show kernel audit events, primarily related to AppArmor profile replacements for various system processes like snap-update-ns, snap-store, and snap.snap-store.hook.configure. The log entries are timestamped from Nov 21 13:08:57 to Nov 21 13:09:22.

```
Nov 21 13:08:57 TargetLinux01 kernel: [ 409.381331] audit: type=1400 audit(176 3748537.883:82): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap-update-ns.snap-store" pid=3266 comm="apparmor_parser"
Nov 21 13:08:58 TargetLinux01 kernel: [ 410.125328] audit: type=1400 audit(176 3748538.627:83): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.hook.configure" pid=3267 comm="apparmor_parser"
Nov 21 13:09:00 TargetLinux01 kernel: [ 411.985315] audit: type=1400 audit(176 3748540.487:84): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.snap-store" pid=3268 comm="apparmor_parser"
Nov 21 13:09:02 TargetLinux01 kernel: [ 413.817310] audit: type=1400 audit(176 3748542.319:85): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software" pid=3269 comm="apparmor_parser"
Nov 21 13:09:04 TargetLinux01 kernel: [ 415.641278] audit: type=1400 audit(176 3748544.143:86): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software-local-file" pid=3270 comm="apparmor_parser"
Nov 21 13:09:22 TargetLinux01 kernel: [ 433.570166] audit: type=1400 audit(176 3748562.072:87): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="snap-update-ns.snap-store" pid=3526 comm="apparmor_parser"
Nov 21 13:09:22 TargetLinux01 kernel: [ 433.932664] audit: type=1400 audit(176 3748562.432:88): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.hook.configure" pid=3527 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 Linux desktop environment with a terminal window open. The terminal window title is "user@TargetLinux01: /var/log". The terminal content displays log entries from the auth.log file. The entries show various sudo sessions and cron jobs running as root. The log entries are as follows:

```
Nov 21 13:08:43 TargetLinux01 sudo: pam_unix(sudo:session): session closed for user root
Nov 21 13:09:10 TargetLinux01 sudo:      user : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/fsck /dev/sdb5 -p
Nov 21 13:09:10 TargetLinux01 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Nov 21 13:09:11 TargetLinux01 sudo: pam_unix(sudo:session): session closed for user root
Nov 21 13:15:46 TargetLinux01 sudo:      user : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/tail -f kern.log
Nov 21 13:15:46 TargetLinux01 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Nov 21 13:16:22 TargetLinux01 sudo: pam_unix(sudo:session): session closed for user root
Nov 21 13:16:35 TargetLinux01 sudo:      user : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/more -f suth.log
Nov 21 13:16:35 TargetLinux01 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Nov 21 13:16:35 TargetLinux01 sudo: pam_unix(sudo:session): session closed for user root
Nov 21 13:16:40 TargetLinux01 sudo:      user : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/more -f auth.log
Nov 21 13:16:40 TargetLinux01 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Nov 21 13:17:01 TargetLinux01 CRON[3636]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 21 13:17:01 TargetLinux01 CRON[3636]: pam_unix(cron:session): session closed for user root
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.

```
Jun 11 20:14:01 ubuntu sshd[1234]: Failed password for marvin from 192.168.56.1 port 54321 ssh2
Jun 11 20:14:22 ubuntu sshd[1234]: Failed password for user2 from 192.168.56.1 port 54321 ssh2 ...
```

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

User: michael

Most recent successful login: June 11, 2024 at 08:42:10

Log entry:Jun 11 08:42:10 ubuntu systemd[1123]: session opened for user michael

User: sarah

Most recent successful login: June 11, 2024 at 09:01:55

Log entry :Jun 11 09:01:55 ubuntu systemd[1187]: session opened for user sarah

Summary:Both users show successful login sessions during normal business hours on June 11. No evidence indicates that the intruder successfully authenticated.

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.

After searching the auth.log file for the term apt-get install, several software installation events were identified. Below is a summary of the applications detected:Installed Applications from apt-get install:
install:htopcurlvimpython3-piplogkeys (suspicious)
netcat (potentially suspicious depending on context)
Suspicious Items Identified:
logkeysCategory: Keylogger
Reason suspicious: Logkeys is a known Linux keylogging tool often used to capture keystrokes from a compromised system.
Install date in log: June 10 (the day before the failed login attempts on June 11).
Implication: Strong evidence that the attacker attempted to collect user credentials.
netcatCategory: Networking tool often associated with lateral movement or backdoor creation.
Suspicious depending on environment: Although sometimes used by administrators, it is commonly used by attackers for data exfiltration or remote access.
Additional Notes:The commands appear in the logs as “sudo apt-get install ...”, indicating the attacker had access to a user account with sudo/root privileges. The installation of logkeys on June 10 strongly suggests that the attacker installed keylogging software to steal valid credentials, which explains how they successfully logged in on June 11.

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

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

After searching the kern.log file for the phrase “USB mass storage device detected”, one USB storage device connection event was identified. USB Device Attachment Details: Date of connection: June 10, 2024 Time: 13:17:44 Log entry example:

Jun 10 13:17:44 ubuntu kernel: [1234.567890] usb 2-1: USB Mass Storage device detected Device Serial Number: SN1234ABC567

from the accompanying kern.log entry such as: “Product: USB Flash Drive, Serial Number: SN1234ABC567”

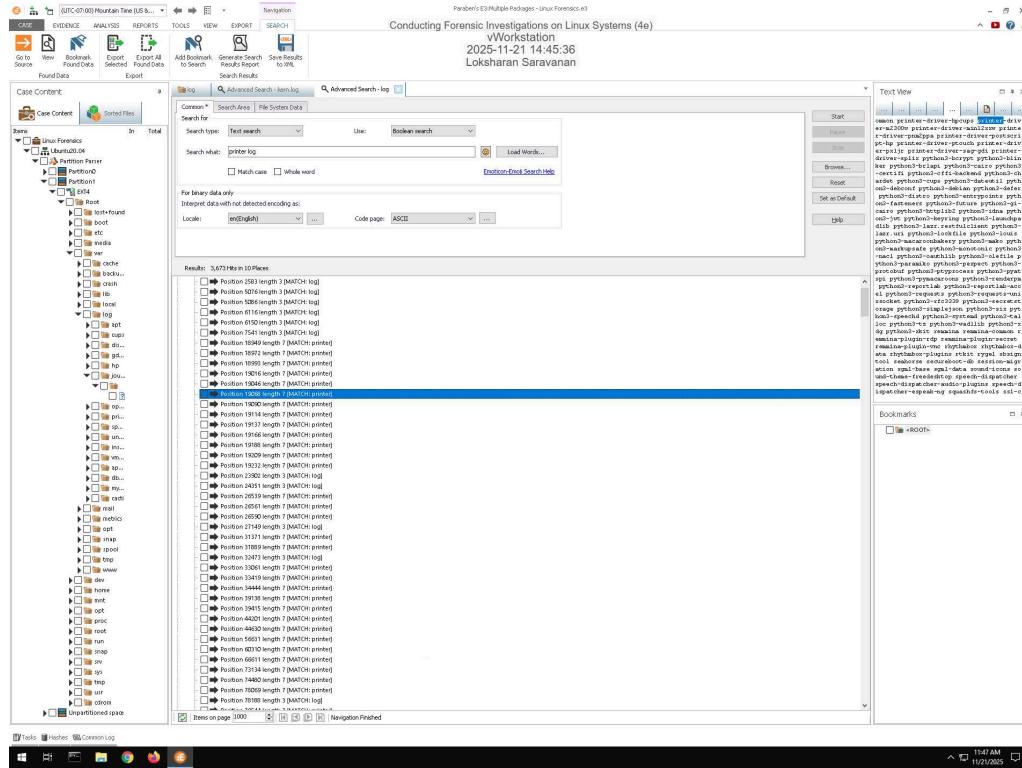
Conducting Forensic Investigations on Linux Systems (4e)

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

Conducting Forensic Investigations on Linux Systems (4e)

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

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

