Conducting Forensic Investigations on Linux Systems (4e)

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

Student:	Email:
Jake Simpson	jaksimps@iu.edu

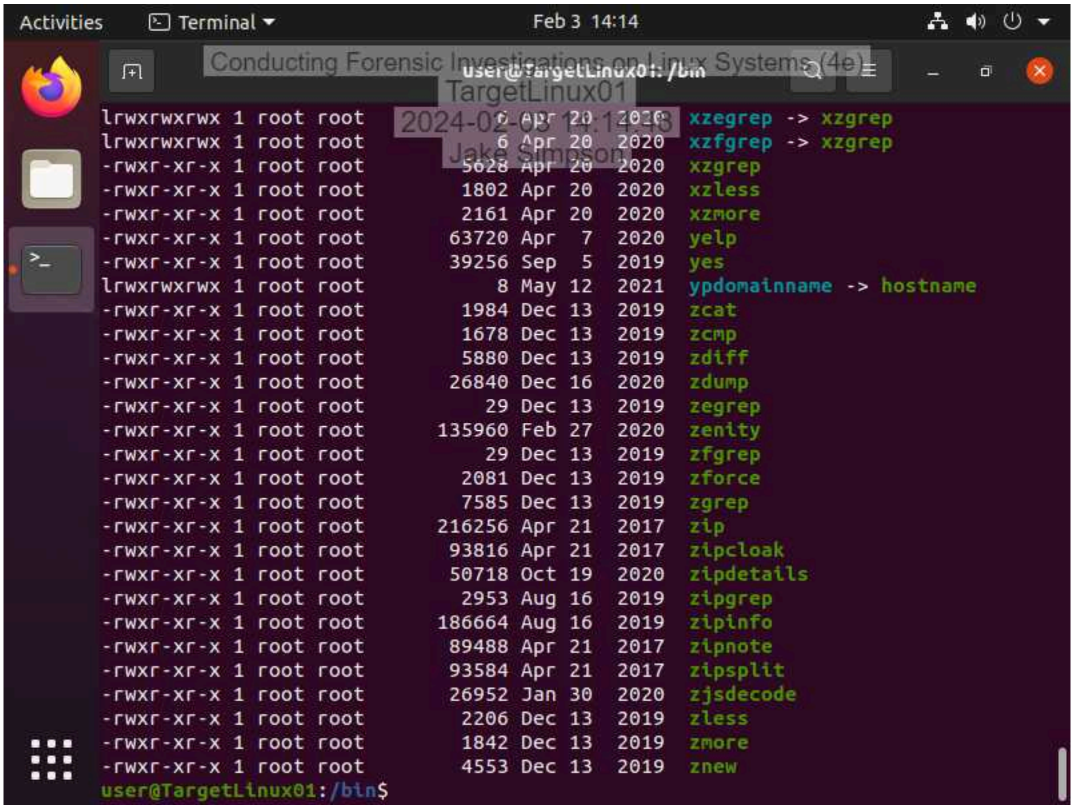
Time on Task:	Progress:
1 hour, 12 minutes	100%

Report Generated: Saturday, February 3, 2024 at 3:30 PM

Section 1: Hands-On Demonstration

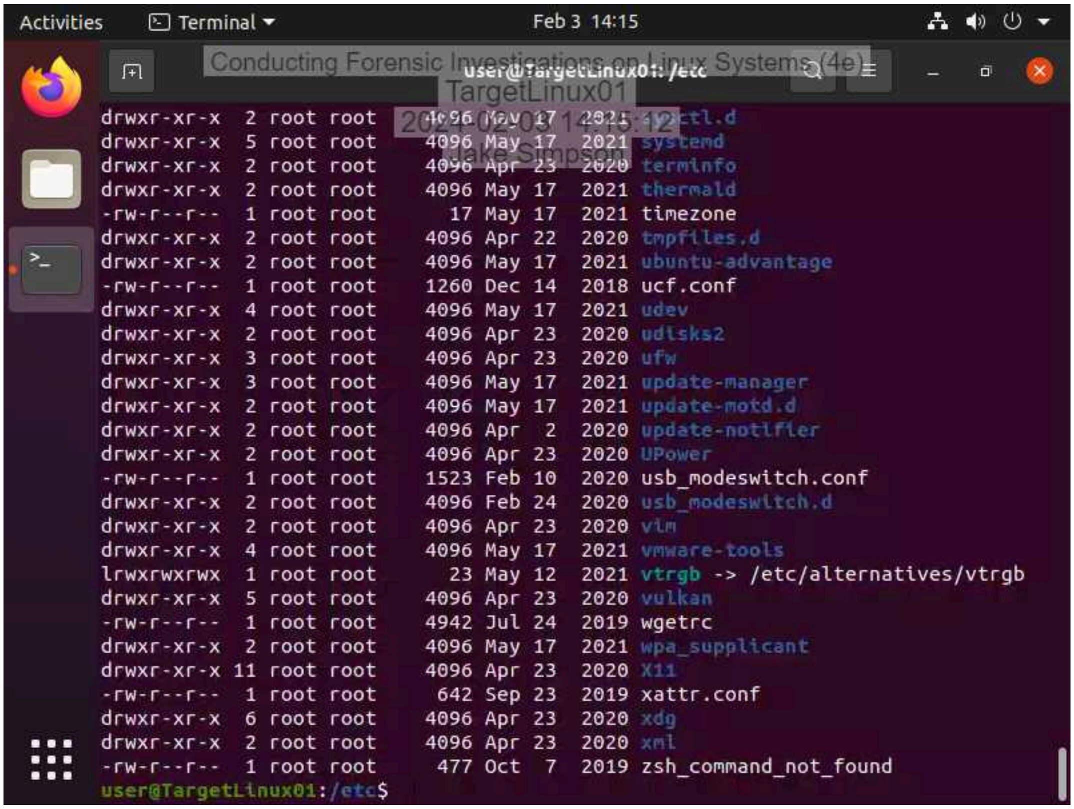
Part 1: Explore a Live Linux System

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



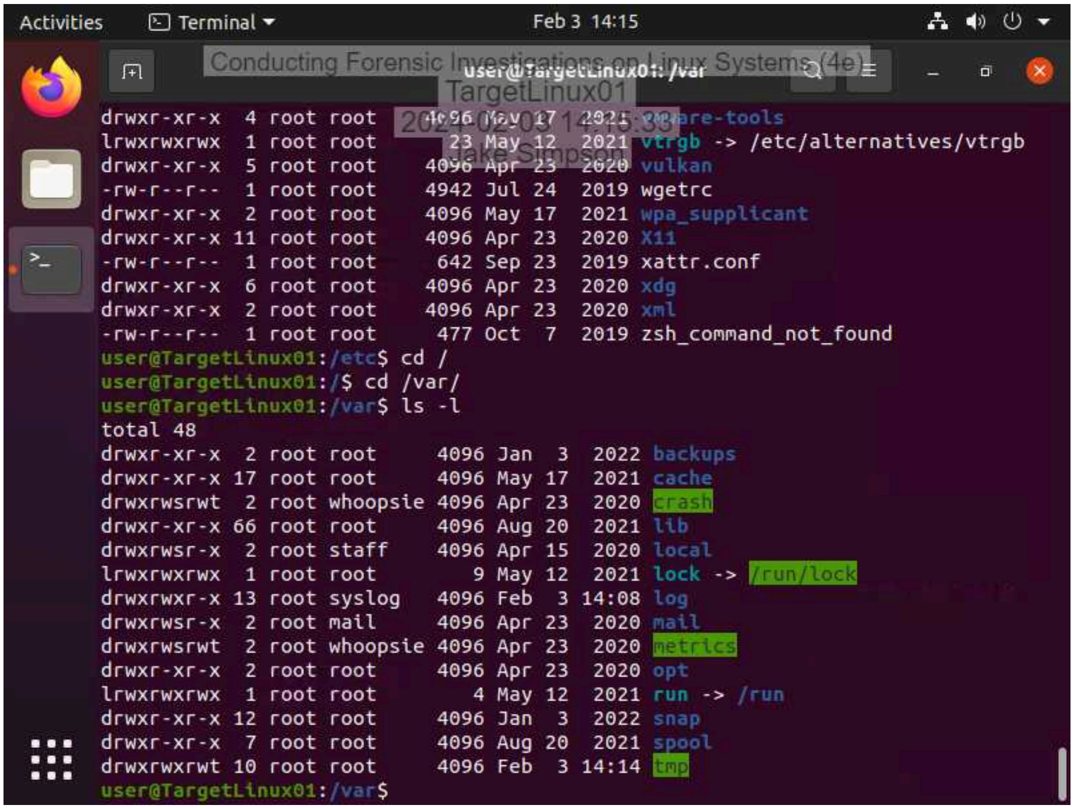
```
lrwxrwxrwx 1 root root         6 Apr 20  2020  xzegrep -> xzgrep
lrwxrwxrwx 1 root root         6 Apr 20  2020  xzfgrep -> xzgrep
-rwxr-xr-x 1 root root      5628 Apr 20  2020  xzgrep
-rwxr-xr-x 1 root root      1802 Apr 20  2020  xzless
-rwxr-xr-x 1 root root      2161 Apr 20  2020  xzmore
-rwxr-xr-x 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
user@TargetLinux01:/bin$
```

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



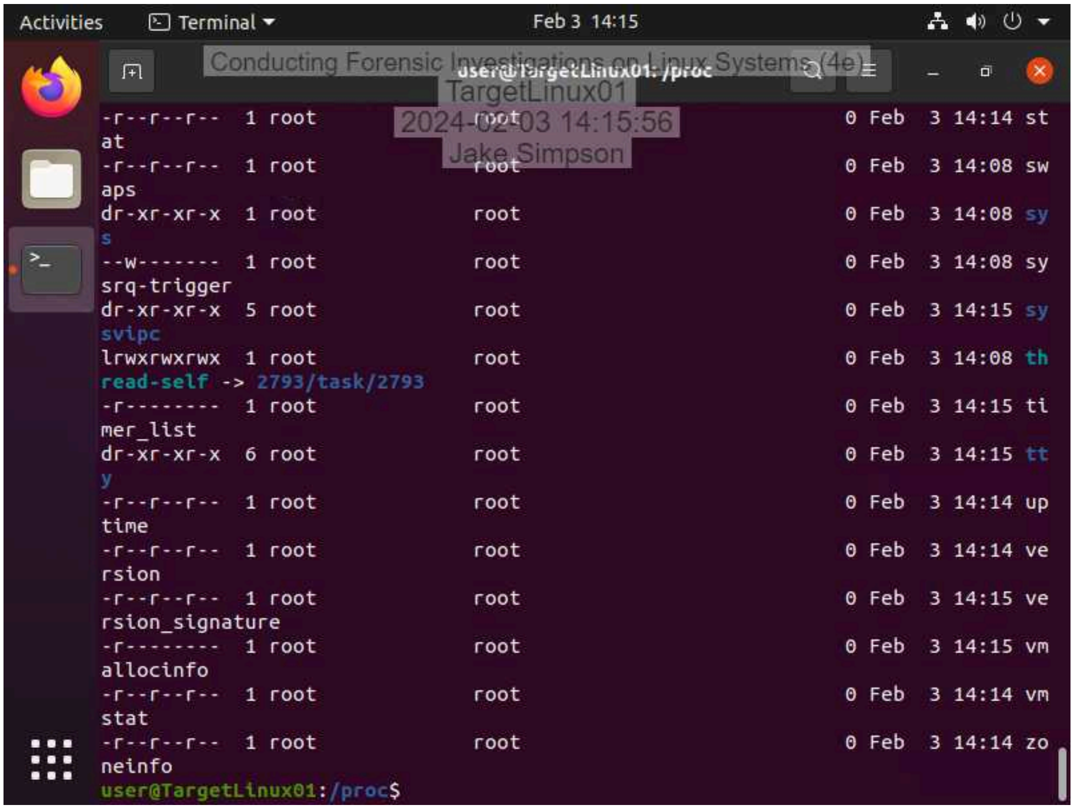
```
drwxr-xr-x  2 root root    4096 May 17  2021 sysctl.d
drwxr-xr-x  5 root root    4096 May 17  2021 systemd
drwxr-xr-x  2 root root    4096 Apr 23  2020 terminfo
drwxr-xr-x  2 root root    4096 May 17  2021 thermald
-rw-r--r--  1 root root      17 May 17  2021 timezone
drwxr-xr-x  2 root root    4096 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
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**.



```
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 Feb  3 14:08 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 Feb  3 14:14 tmp
user@TargetLinux01:/var$
```

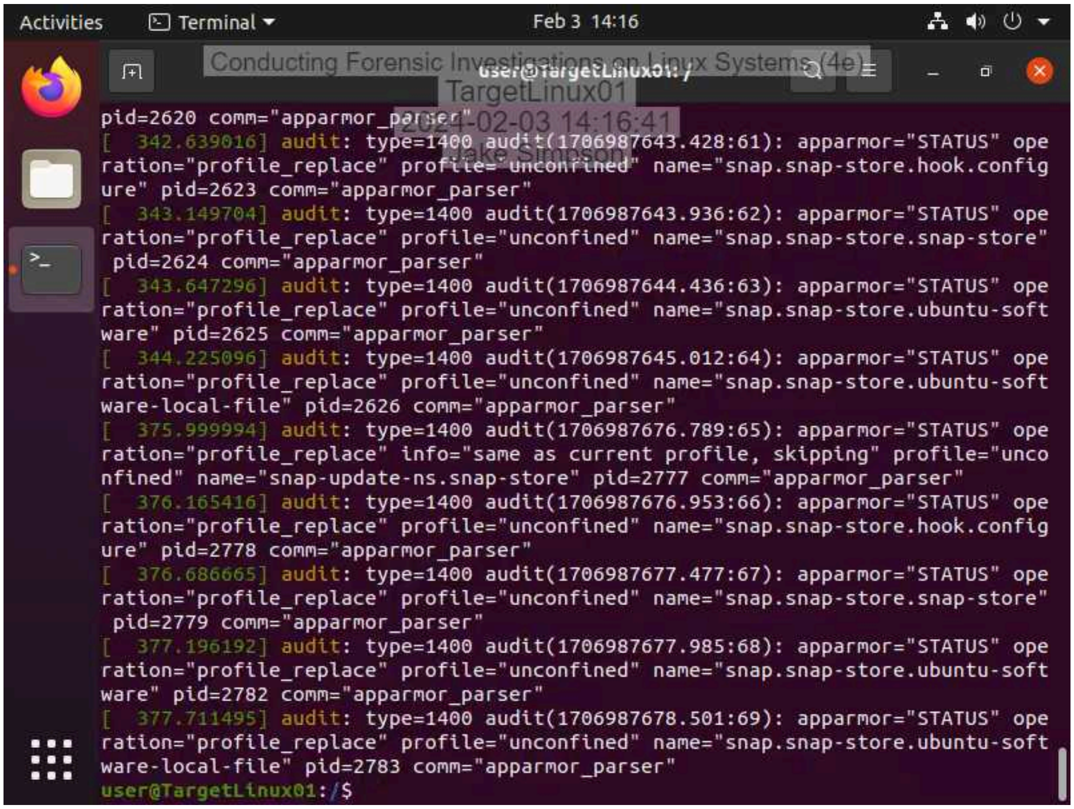
22. **Make a screen capture** showing the **contents of the /proc directory**.


Activities
Terminal
Feb 3 14:15
user@TargetLinux01: /proc
Conducting Forensic Investigations on Linux Systems (4e)
TargetLinux01
2024-02-03 14:15:56
Jake Simpson

```
-r--r--r--  1 root          root                  0 Feb  3 14:14 st
at
-r--r--r--  1 root          root                  0 Feb  3 14:08 sw
aps
dr-xr-xr-x  1 root          root                  0 Feb  3 14:08 sy
s
--w-------  1 root          root                  0 Feb  3 14:08 sy
srq-trigger
dr-xr-xr-x  5 root          root                  0 Feb  3 14:15 sy
svipc
lrwxrwxrwx  1 root          root                  0 Feb  3 14:08 th
read-self -> 2793/task/2793
-r--------  1 root          root                  0 Feb  3 14:15 ti
mer_list
dr-xr-xr-x  6 root          root                  0 Feb  3 14:15 tt
y
-r--r--r--  1 root          root                  0 Feb  3 14:14 up
time
-r--r--r--  1 root          root                  0 Feb  3 14:14 ve
rsion
-r--r--r--  1 root          root                  0 Feb  3 14:15 ve
rsion_signature
-r--------  1 root          root                  0 Feb  3 14:15 vm
allocinfo
-r--r--r--  1 root          root                  0 Feb  3 14:14 vm
stat
-r--r--r--  1 root          root                  0 Feb  3 14:14 zo
neinfo
user@TargetLinux01:/proc$
```

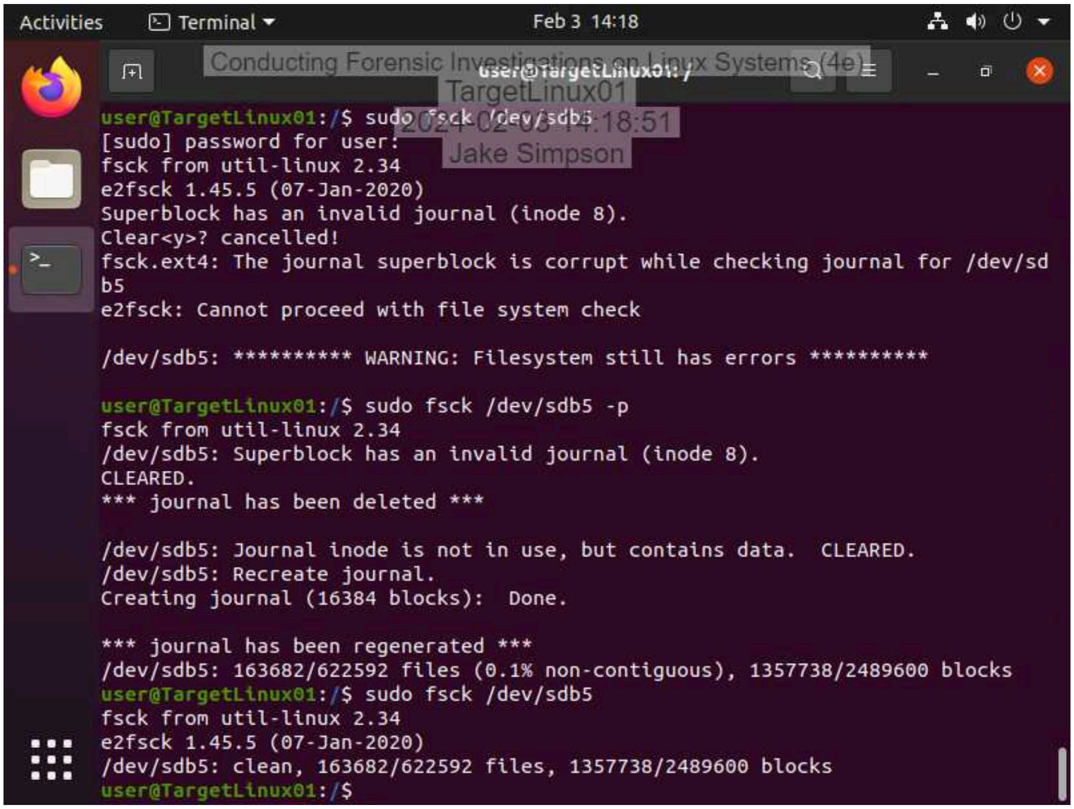
Part 2: Use Linux Shell Commands for Forensic Investigations

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



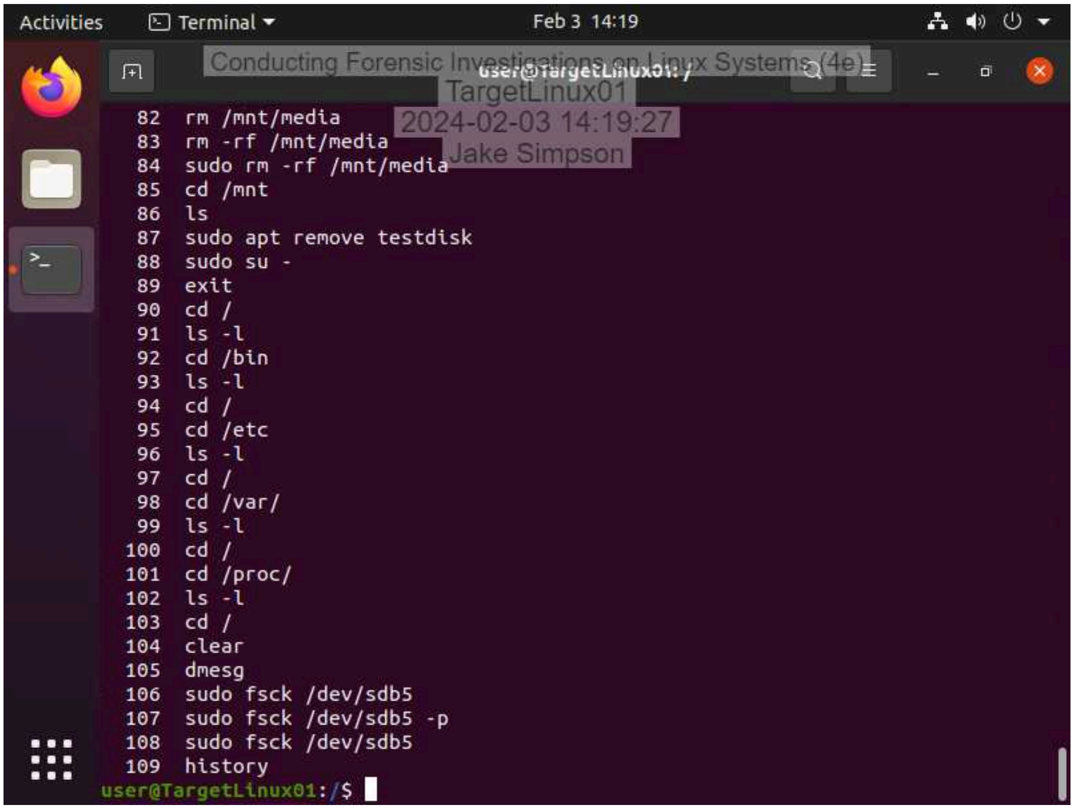
```
pid=2620 comm="apparmor_parser"
[  342.639016] audit: type=1400 audit(1706987643.428:61): apparmor="STATUS" ope
ration="profile_replace" profile="unconfined" name="snap.snap-store.hook.config
ure" pid=2623 comm="apparmor_parser"
[  343.149704] audit: type=1400 audit(1706987643.936:62): apparmor="STATUS" ope
ration="profile_replace" profile="unconfined" name="snap.snap-store.snap-store"
 pid=2624 comm="apparmor_parser"
[  343.647296] audit: type=1400 audit(1706987644.436:63): apparmor="STATUS" ope
ration="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-soft
ware" pid=2625 comm="apparmor_parser"
[  344.225096] audit: type=1400 audit(1706987645.012:64): apparmor="STATUS" ope
ration="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-soft
ware-local-file" pid=2626 comm="apparmor_parser"
[  375.999994] audit: type=1400 audit(1706987676.789:65): apparmor="STATUS" ope
ration="profile_replace" info="same as current profile, skipping" profile="unco
nfined" name="snap-update-ns.snap-store" pid=2777 comm="apparmor_parser"
[  376.165416] audit: type=1400 audit(1706987676.953:66): apparmor="STATUS" ope
ration="profile_replace" profile="unconfined" name="snap.snap-store.hook.config
ure" pid=2778 comm="apparmor_parser"
[  376.686665] audit: type=1400 audit(1706987677.477:67): apparmor="STATUS" ope
ration="profile_replace" profile="unconfined" name="snap.snap-store.snap-store"
 pid=2779 comm="apparmor_parser"
[  377.196192] audit: type=1400 audit(1706987677.985:68): apparmor="STATUS" ope
ration="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-soft
ware" pid=2782 comm="apparmor_parser"
[  377.711495] audit: type=1400 audit(1706987678.501:69): apparmor="STATUS" ope
ration="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-soft
ware-local-file" pid=2783 comm="apparmor_parser"
user@TargetLinux01:/$
```

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



```
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:/$ 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:/$
```

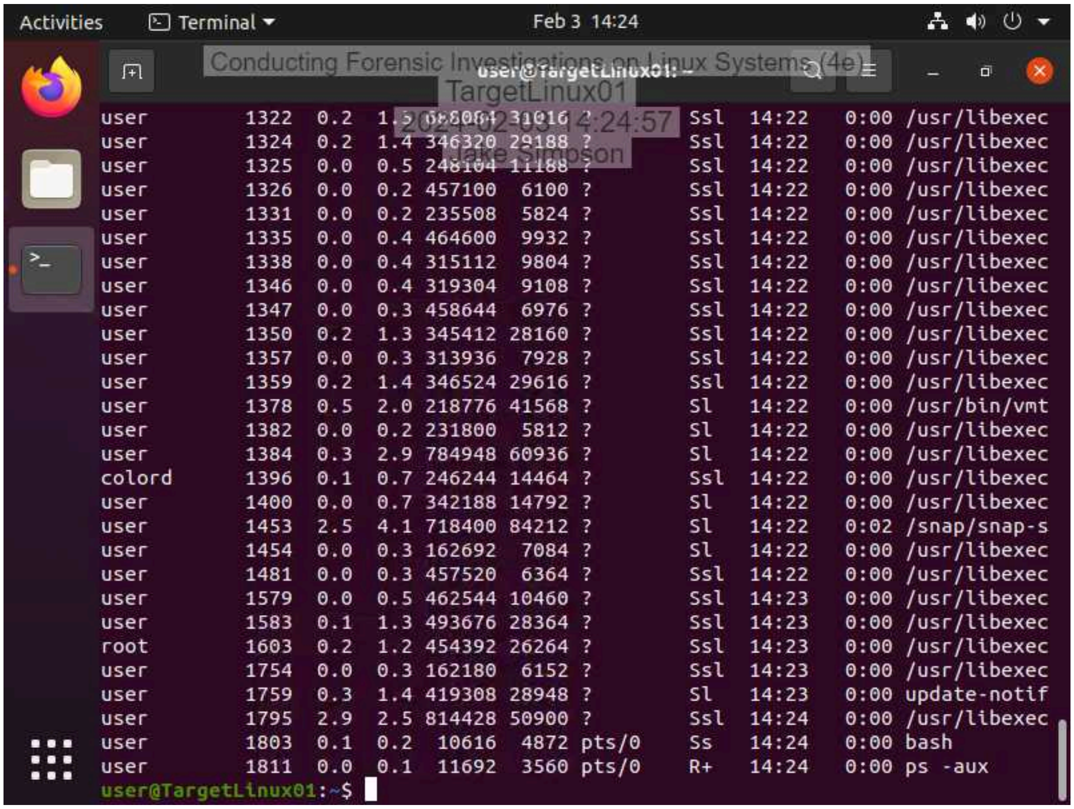
9. **Make a screen capture** showing the **results of the history command**.



Conducting Forensic Investigations on Linux Systems (4e)
TargetLinux01
2024-02-03 14:19:27
Jake Simpson

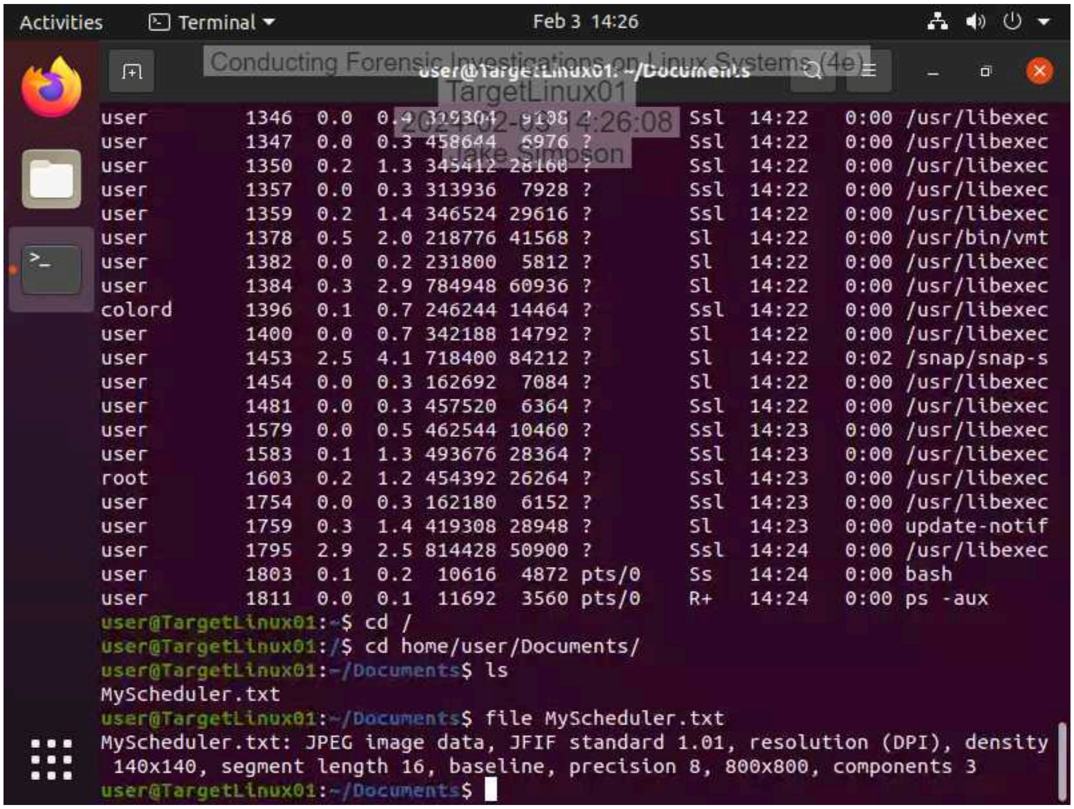
```
   82  rm /mnt/media
   83  rm -rf /mnt/media
   84  sudo rm -rf /mnt/media
   85  cd /mnt
   86  ls
   87  sudo apt remove testdisk
   88  sudo su -
   89  exit
   90  cd /
   91  ls -l
   92  cd /bin
   93  ls -l
   94  cd /
   95  cd /etc
   96  ls -l
   97  cd /
   98  cd /var/
   99  ls -l
  100  cd /
  101  cd /proc/
  102  ls -l
  103  cd /
  104  clear
  105  dmesg
  106  sudo fsck /dev/sdb5
  107  sudo fsck /dev/sdb5 -p
  108  sudo fsck /dev/sdb5
  109  history
user@TargetLinux01:/$ 
```

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



```
user         1322  0.2  1.5 688084 31016 ?        Ssl  14:22   0:00 /usr/libexec
user         1324  0.2  1.4 346320 29188 ?        Ssl  14:22   0:00 /usr/libexec
user         1325  0.0  0.5 248104 11188 ?        Ssl  14:22   0:00 /usr/libexec
user         1326  0.0  0.2 457100  6100 ?        Ssl  14:22   0:00 /usr/libexec
user         1331  0.0  0.2 235508  5824 ?        Ssl  14:22   0:00 /usr/libexec
user         1335  0.0  0.4 464600  9932 ?        Ssl  14:22   0:00 /usr/libexec
user         1338  0.0  0.4 315112  9804 ?        Ssl  14:22   0:00 /usr/libexec
user         1346  0.0  0.4 319304  9108 ?        Ssl  14:22   0:00 /usr/libexec
user         1347  0.0  0.3 458644  6976 ?        Ssl  14:22   0:00 /usr/libexec
user         1350  0.2  1.3 345412 28160 ?        Ssl  14:22   0:00 /usr/libexec
user         1357  0.0  0.3 313936  7928 ?        Ssl  14:22   0:00 /usr/libexec
user         1359  0.2  1.4 346524 29616 ?        Ssl  14:22   0:00 /usr/libexec
user         1378  0.5  2.0 218776 41568 ?        Sl   14:22   0:00 /usr/bin/vmt
user         1382  0.0  0.2 231800  5812 ?        Sl   14:22   0:00 /usr/libexec
user         1384  0.3  2.9 784948 60936 ?        Sl   14:22   0:00 /usr/libexec
colord       1396  0.1  0.7 246244 14464 ?        Ssl  14:22   0:00 /usr/libexec
user         1400  0.0  0.7 342188 14792 ?        Sl   14:22   0:00 /usr/libexec
user         1453  2.5  4.1 718400 84212 ?        Sl   14:22   0:02 /snap/snap-s
user         1454  0.0  0.3 162692  7084 ?        Sl   14:22   0:00 /usr/libexec
user         1481  0.0  0.3 457520  6364 ?        Ssl  14:22   0:00 /usr/libexec
user         1579  0.0  0.5 462544 10460 ?        Ssl  14:23   0:00 /usr/libexec
user         1583  0.1  1.3 493676 28364 ?        Ssl  14:23   0:00 /usr/libexec
root         1603  0.2  1.2 454392 26264 ?        Ssl  14:23   0:00 /usr/libexec
user         1754  0.0  0.3 162180  6152 ?        Ssl  14:23   0:00 /usr/libexec
user         1759  0.3  1.4 419308 28948 ?        Sl   14:23   0:00 update-notif
user         1795  2.9  2.5 814428 50900 ?        Ssl  14:24   0:00 /usr/libexec
user         1803  0.1  0.2  10616  4872 pts/0    Ss   14:24   0:00 bash
user         1811  0.0  0.1  11692  3560 pts/0    R+   14:24   0:00 ps -aux
user@TargetLinux01:~$ 
```

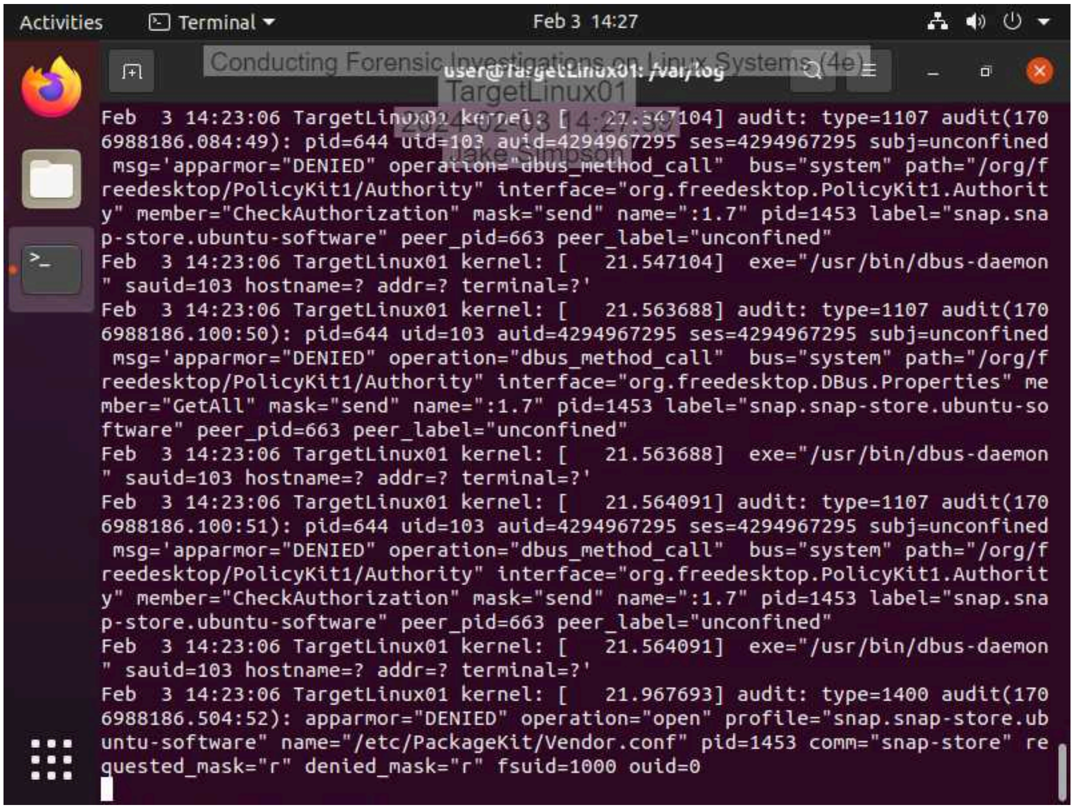
15. **Make a screen capture** showing the **results of the file command**.


Activities
Terminal
Feb 3 14:26
user@TargetLinux01: ~/Documents
Conducting Forensic Investigations on Linux Systems (4e)
TargetLinux01
2022-02-03 14:26:08
Jake Simpson

```
user        1346  0.0  0.4 329304  9108 ?      Ssl  14:22   0:00 /usr/libexec
user        1347  0.0  0.3 458644  6976 ?      Ssl  14:22   0:00 /usr/libexec
user        1350  0.2  1.3 345412 28160 ?      Ssl  14:22   0:00 /usr/libexec
user        1357  0.0  0.3 313936  7928 ?      Ssl  14:22   0:00 /usr/libexec
user        1359  0.2  1.4 346524 29616 ?      Ssl  14:22   0:00 /usr/libexec
user        1378  0.5  2.0 218776 41568 ?      Sl   14:22   0:00 /usr/bin/vmt
user        1382  0.0  0.2 231800  5812 ?      Sl   14:22   0:00 /usr/libexec
user        1384  0.3  2.9 784948 60936 ?      Sl   14:22   0:00 /usr/libexec
colord      1396  0.1  0.7 246244 14464 ?      Ssl  14:22   0:00 /usr/libexec
user        1400  0.0  0.7 342188 14792 ?      Sl   14:22   0:00 /usr/libexec
user        1453  2.5  4.1 718400 84212 ?      Sl   14:22   0:02 /snap/snap-s
user        1454  0.0  0.3 162692  7084 ?      Sl   14:22   0:00 /usr/libexec
user        1481  0.0  0.3 457520  6364 ?      Ssl  14:22   0:00 /usr/libexec
user        1579  0.0  0.5 462544 10460 ?      Ssl  14:23   0:00 /usr/libexec
user        1583  0.1  1.3 493676 28364 ?      Ssl  14:23   0:00 /usr/libexec
root        1603  0.2  1.2 454392 26264 ?      Ssl  14:23   0:00 /usr/libexec
user        1754  0.0  0.3 162180  6152 ?      Ssl  14:23   0:00 /usr/libexec
user        1759  0.3  1.4 419308 28948 ?      Sl   14:23   0:00 update-notif
user        1795  2.9  2.5 814428 50900 ?      Ssl  14:24   0:00 /usr/libexec
user        1803  0.1  0.2  10616  4872 pts/0  Ss   14:24   0:00 bash
user        1811  0.0  0.1  11692  3560 pts/0  R+   14:24   0:00 ps -aux
user@TargetLinux01:~$ cd /
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$ 
```

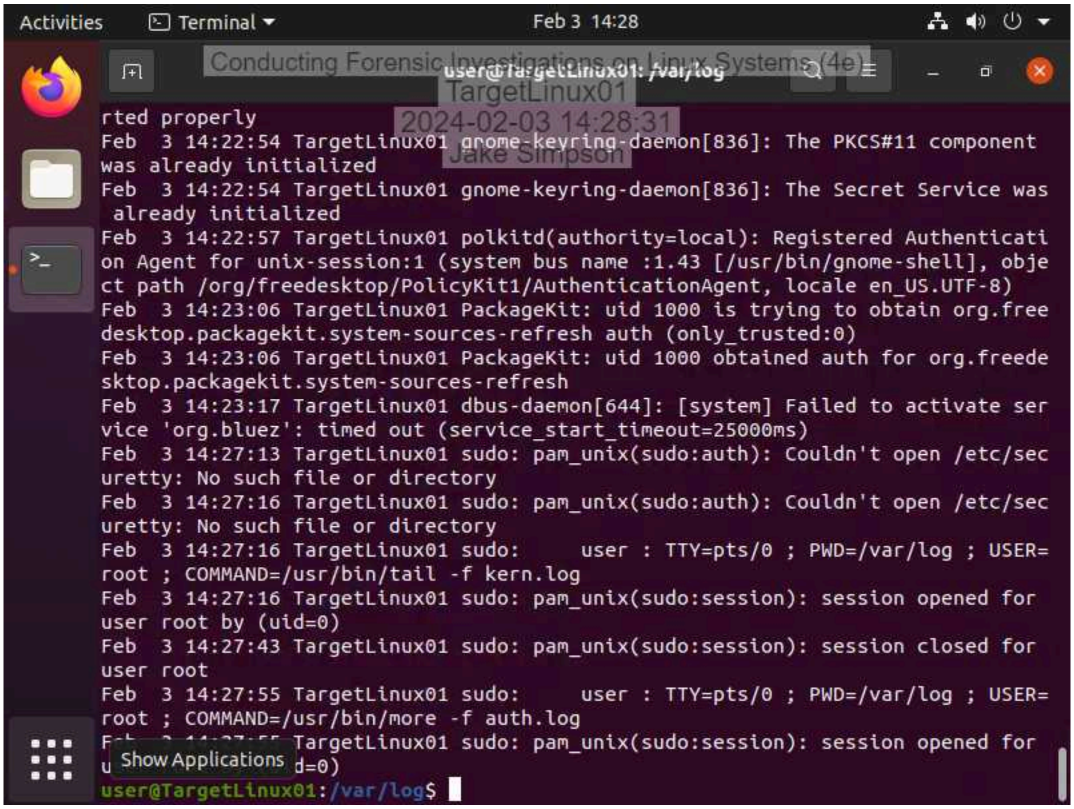
Part 3: Retrieve Logs Files on a Live Linux System

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


Activities
Terminal
Feb 3 14:27
user@TargetLinux01: /var/log
Conducting Forensic Investigations on Linux Systems (4e)
TargetLinux01
2024-02-03 14:27:39
Jake Simpson

```
Feb  3 14:23:06 TargetLinux01 kernel: [   21.547104] audit: type=1107 audit(170
6988186.084:49): pid=644 uid=103 auid=4294967295 ses=4294967295 subj=unconfined
 msg='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/f
reedesktop/PolicyKit1/Authority" interface="org.freedesktop.PolicyKit1.Authorit
y" member="CheckAuthorization" mask="send" name=":1.7" pid=1453 label="snap.sna
p-store.ubuntu-software" peer_pid=663 peer_label="unconfined"
Feb  3 14:23:06 TargetLinux01 kernel: [   21.547104]  exe="/usr/bin/dbus-daemon
" sauid=103 hostname=? addr=? terminal=?'
Feb  3 14:23:06 TargetLinux01 kernel: [   21.563688] audit: type=1107 audit(170
6988186.100:50): pid=644 uid=103 auid=4294967295 ses=4294967295 subj=unconfined
 msg='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/f
reedesktop/PolicyKit1/Authority" interface="org.freedesktop.DBus.Properties" me
mber="GetAll" mask="send" name=":1.7" pid=1453 label="snap.snap-store.ubuntu-so
ftware" peer_pid=663 peer_label="unconfined"
Feb  3 14:23:06 TargetLinux01 kernel: [   21.563688]  exe="/usr/bin/dbus-daemon
" sauid=103 hostname=? addr=? terminal=?'
Feb  3 14:23:06 TargetLinux01 kernel: [   21.564091] audit: type=1107 audit(170
6988186.100:51): pid=644 uid=103 auid=4294967295 ses=4294967295 subj=unconfined
 msg='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/f
reedesktop/PolicyKit1/Authority" interface="org.freedesktop.PolicyKit1.Authorit
y" member="CheckAuthorization" mask="send" name=":1.7" pid=1453 label="snap.sna
p-store.ubuntu-software" peer_pid=663 peer_label="unconfined"
Feb  3 14:23:06 TargetLinux01 kernel: [   21.564091]  exe="/usr/bin/dbus-daemon
" sauid=103 hostname=? addr=? terminal=?'
Feb  3 14:23:06 TargetLinux01 kernel: [   21.967693] audit: type=1400 audit(170
6988186.504:52): apparmor="DENIED" operation="open" profile="snap.snap-store.ub
untu-software" name="/etc/PackageKit/Vendor.conf" pid=1453 comm="snap-store" re
quested_mask="r" denied_mask="r" fsuid=1000 ouid=0
```

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



```
rted properly
Feb  3 14:22:54 TargetLinux01 gnome-keyring-daemon[836]: The PKCS#11 component
was already initialized
Feb  3 14:22:54 TargetLinux01 gnome-keyring-daemon[836]: The Secret Service was
 already initialized
Feb  3 14:22:57 TargetLinux01 polkitd(authority=local): Registered Authenticati
on Agent for unix-session:1 (system bus name :1.43 [/usr/bin/gnome-shell], obje
ct path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Feb  3 14:23:06 TargetLinux01 PackageKit: uid 1000 is trying to obtain org.free
desktop.packagekit.system-sources-refresh auth (only_trusted:0)
Feb  3 14:23:06 TargetLinux01 PackageKit: uid 1000 obtained auth for org.freede
sktop.packagekit.system-sources-refresh
Feb  3 14:23:17 TargetLinux01 dbus-daemon[644]: [system] Failed to activate ser
vice 'org.bluez': timed out (service_start_timeout=25000ms)
Feb  3 14:27:13 TargetLinux01 sudo: pam_unix(sudo:auth): Couldn't open /etc/sec
uretty: No such file or directory
Feb  3 14:27:16 TargetLinux01 sudo: pam_unix(sudo:auth): Couldn't open /etc/sec
uretty: No such file or directory
Feb  3 14:27:16 TargetLinux01 sudo:     user : TTY=pts/0 ; PWD=/var/log ; USER=
root ; COMMAND=/usr/bin/tail -f kern.log
Feb  3 14:27:16 TargetLinux01 sudo: pam_unix(sudo:session): session opened for
user root by (uid=0)
Feb  3 14:27:43 TargetLinux01 sudo: pam_unix(sudo:session): session closed for
user root
Feb  3 14:27:55 TargetLinux01 sudo:     user : TTY=pts/0 ; PWD=/var/log ; USER=
root ; COMMAND=/usr/bin/more -f auth.log
Feb  3 14:27:55 TargetLinux01 sudo: pam_unix(sudo:session): session opened for
u                 d=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.

12 Attempts from user: noel, date: Jun 11 00:57:14 -00:57:35 & 05:06:34-05:06:51, Source IP: 192.168.78.1, Port: 14444 & 3521

5 attempts from user: dominic, date: Jun 11 05:07:57-05:39:01 , Source IP: 192.168.78.1, Port: 4663 & 3417

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

I got 0 results for Noel and 18 for Dominic, his most recent was: 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.

logkeys, utotools-dev, build essential, kbd, cacti, openssh-server

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

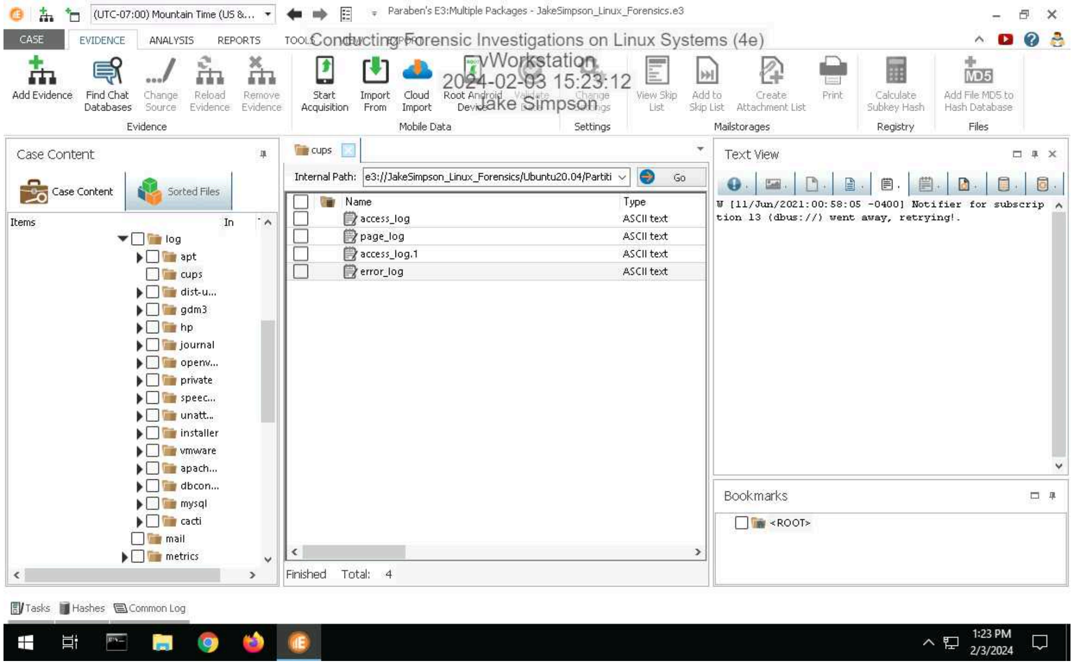
4. **Document** when the USB storage device was connected and its serial number.

Jun 10 10:24:12 and 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
2024-02-03 15:23:12
Jake Simpson

cups

Internal Path: e3://JakeSimpson_Linux_Forensics/Ubuntu20.04/Partiti

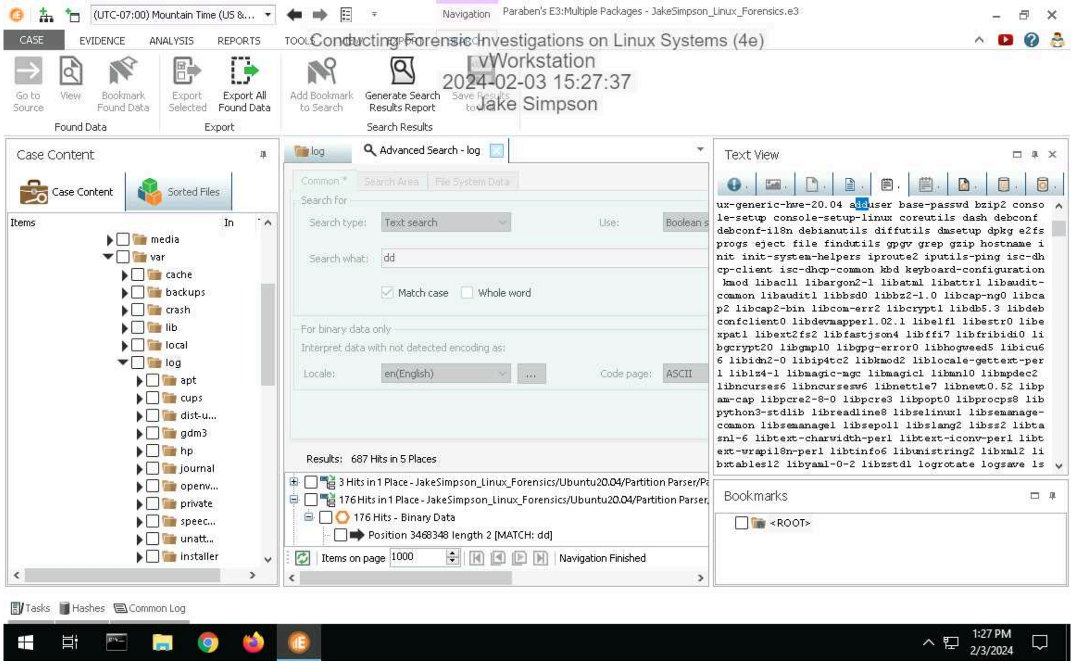
Name	Type
access_log	ASCII text
page_log	ASCII text
access_log.1	ASCII text
error_log	ASCII text

Finished Total: 4

```
W [11/Jun/2021:00:58:05 -0400] Notifier for subscrip
tion 13 (dbus://) went away, retrying!.
```

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 - JakeSimpson_Linux_Forensics.e3

Conducting Forensic Investigations on Linux Systems (4e)
vWorkstation
2024-02-03 15:27:37
Jake Simpson

Search for
Search type: Text search
Use: Boolean s
Search what: dd
☑ Match case ☐ Whole word

For binary data only
Interpret data with not detected encoding as:
Locale: en(English) ...
Code page: ASCII

Results: 687 Hits in 5 Places

```
⊞ ☐ 3 Hits in 1 Place - JakeSimpson_Linux_Forensics/Ubuntu20.04/Partition Parser/Pa
⊟ ☐ 176 Hits in 1 Place - JakeSimpson_Linux_Forensics/Ubuntu20.04/Partition Parser,
   ⊟ ☐ 176 Hits - Binary Data
      ☐ Position 3468348 length 2 [MATCH: dd]
```

Items on page 1000 Navigation Finished

```
ux-generic-hwe-20.04 adduser base-passwd bzip2 conso
le-setup console-setup-linux coreutils dash debconf
debconf-i18n debianutils diffutils dmsetup dpkg e2fs
progs eject file findutils gpgv grep gzip hostname i
nit init-system-helpers iproute2 iputils-ping isc-dh
cp-client isc-dhcp-common kbd keyboard-configuration
 kmod libacl1 libargon2-1 libatm1 libattr1 libaudit-
common libaudit1 libbsd0 libbz2-1.0 libcap-ng0 libca
p2 libcap2-bin libcom-err2 libcrypt1 libdb5.3 libdeb
confclient0 libdevmapper1.02.1 libelf1 libestr0 libe
xpat1 libext2fs2 libfastjson4 libffi7 libfribidi0 li
bgcrypt20 libgmp10 libgpg-error0 libhogweed5 libicu6
6 libidn2-0 libip4tc2 libkmod2 liblocale-gettext-per
l liblz4-1 libmagic-mgc libmagic1 libmnl0 libmpdec2
libncurses6 libncursesw6 libnettle7 libnewt0.52 libp
am-cap libpcre2-8-0 libpcre3 libpopt0 libprocps8 lib
python3-stdlib libreadline8 libselinux1 libsemanage-
common libsemanage1 libsepol1 libslang2 libss2 libta
snl-6 libtext-charwidth-perl libtext-iconv-perl libt
ext-wrapi18n-perl libtinfo6 libunistring2 libxml2 li
bxtables12 libyaml-0-2 libzstd1 logrotate logsave ls
```