

Conducting Forensic Investigations on Linux Systems (4e)

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

Student:

Vishal Singh Bhardvaj

Email:

Time on Task:

2 hours, 2 minutes

Progress:

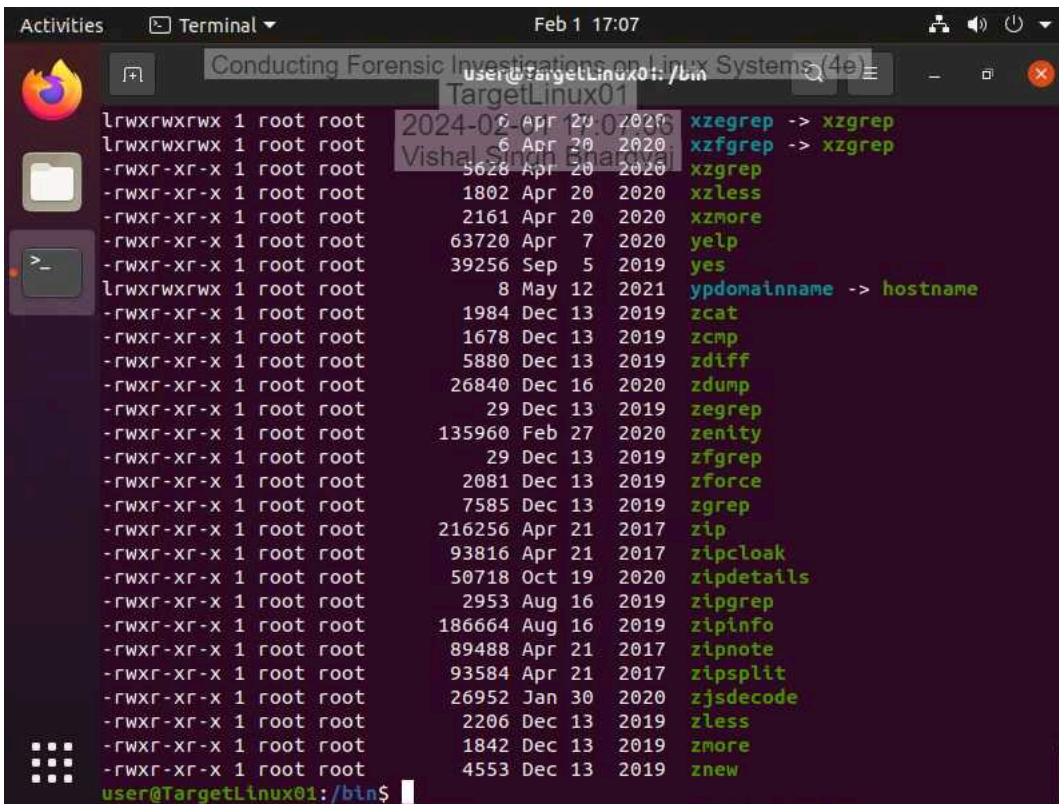
100%

Report Generated: Thursday, February 1, 2024 at 6:57 PM

Section 1: Hands-On Demonstration

Part 1: Explore a Live Linux System

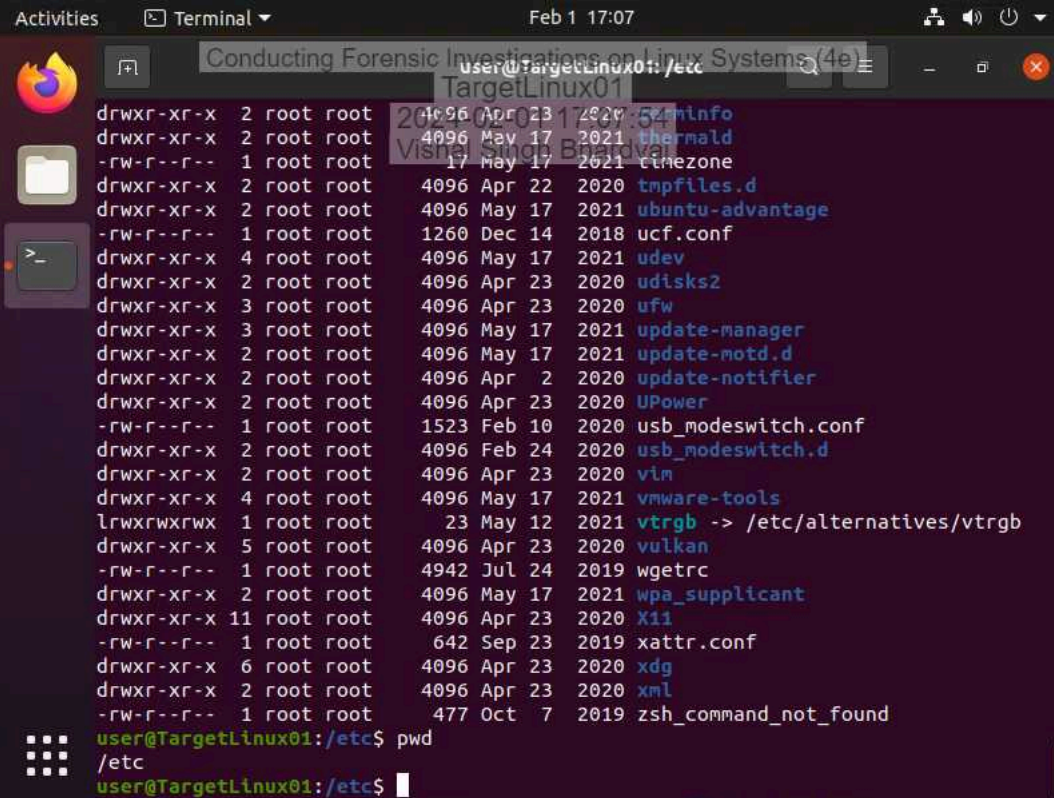
17. Make a screen capture showing the contents of the `/bin` directory.



A terminal window titled "Terminal" showing the command `ls -l /bin` and its output. The output lists various system binaries with their permissions, sizes, dates, and names. The terminal window has a dark background and a light-colored text. The title bar shows "Activities", "Terminal", and the date "Feb 1 17:07". The terminal content is as follows:

```
user@TargetLinux01: /bin$ ls -l /bin
lrwxrwxrwx 1 root root 10 Apr 27 2020 xzegrep -> xzgrep
lrwxrwxrwx 1 root root 10 Apr 27 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$
```

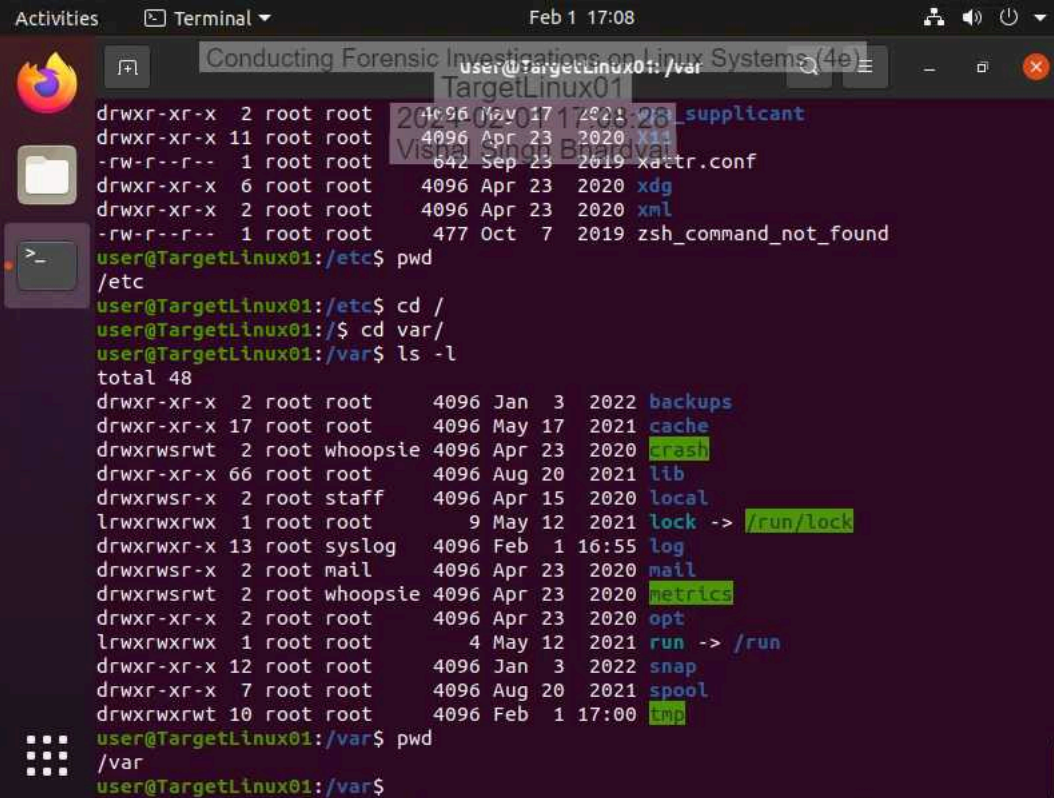
20. Make a screen capture showing the contents of the `/etc` directory.



```
user@TargetLinux01: /etc
TargetLinux01
4096 Apr 23 2020 5zinfo
4096 May 17 2021 thermald
17 May 17 2021 timezone
4096 Apr 22 2020 tmpfiles.d
4096 May 17 2021 ubuntu-advantage
1260 Dec 14 2018 ucf.conf
4096 May 17 2021 udev
4096 Apr 23 2020 udisks2
4096 Apr 23 2020 ufw
4096 May 17 2021 update-manager
4096 May 17 2021 update-motd.d
4096 Apr 2 2020 update-notifier
4096 Apr 23 2020 UPower
1523 Feb 10 2020 usb_modeswitch.conf
4096 Feb 24 2020 usb_modeswitch.d
4096 Apr 23 2020 vim
4096 May 17 2021 vmware-tools
23 May 12 2021 vtrgb -> /etc/alternatives/vtrgb
4096 Apr 23 2020 vulkan
4942 Jul 24 2019 wgetrc
4096 May 17 2021 wpa_supplicant
4096 Apr 23 2020 X11
642 Sep 23 2019 xattr.conf
4096 Apr 23 2020 xdg
4096 Apr 23 2020 xml
477 Oct 7 2019 zsh_command_not_found

user@TargetLinux01:/etc$ pwd
/etc
user@TargetLinux01:/etc$
```

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

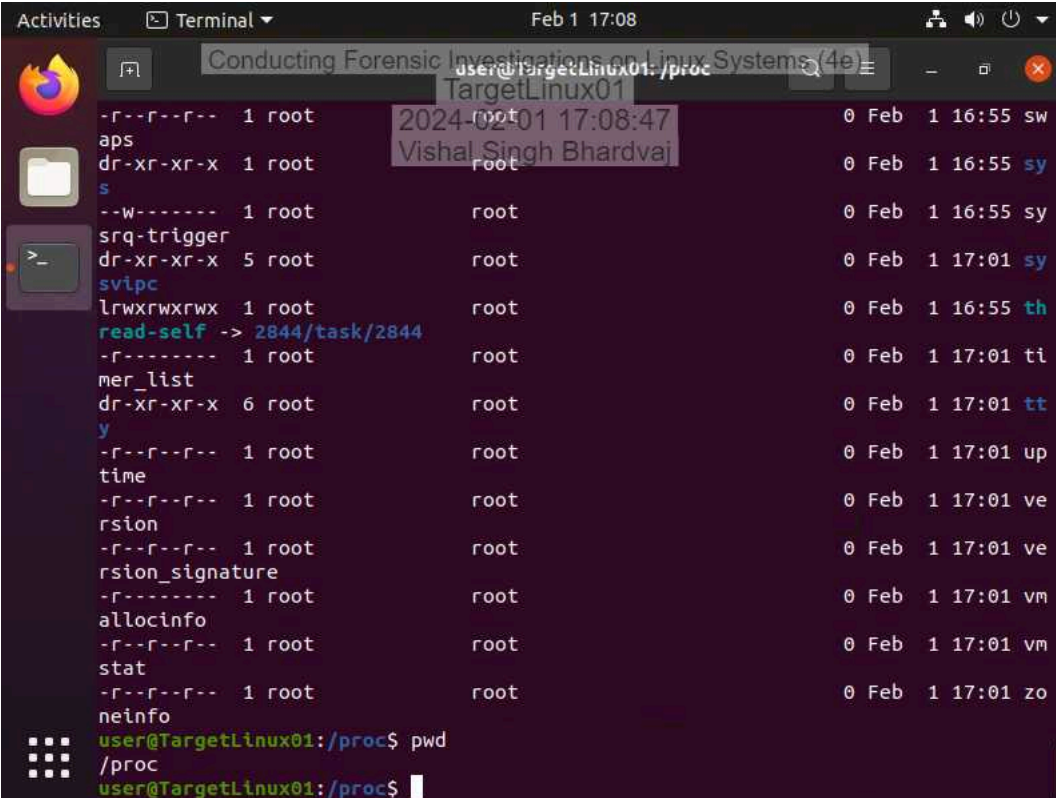


A terminal window titled "Terminal" with a date and time of "Feb 1 17:08". The window shows a user at "TargetLinux01" with a prompt "user@TargetLinux01: /var". The user enters "ls -l" and the output shows a list of files and directories in /var. The output is as follows:

```
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  1 16:55 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  1 17:00 tmp
```

The user then enters "pwd" and the output is "/var". The user then enters "cd /" and the prompt changes to "user@TargetLinux01:/\$". The user then enters "cd var/" and the prompt changes to "user@TargetLinux01:/var\$". The user then enters "ls -l" and the output is the same as above.

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

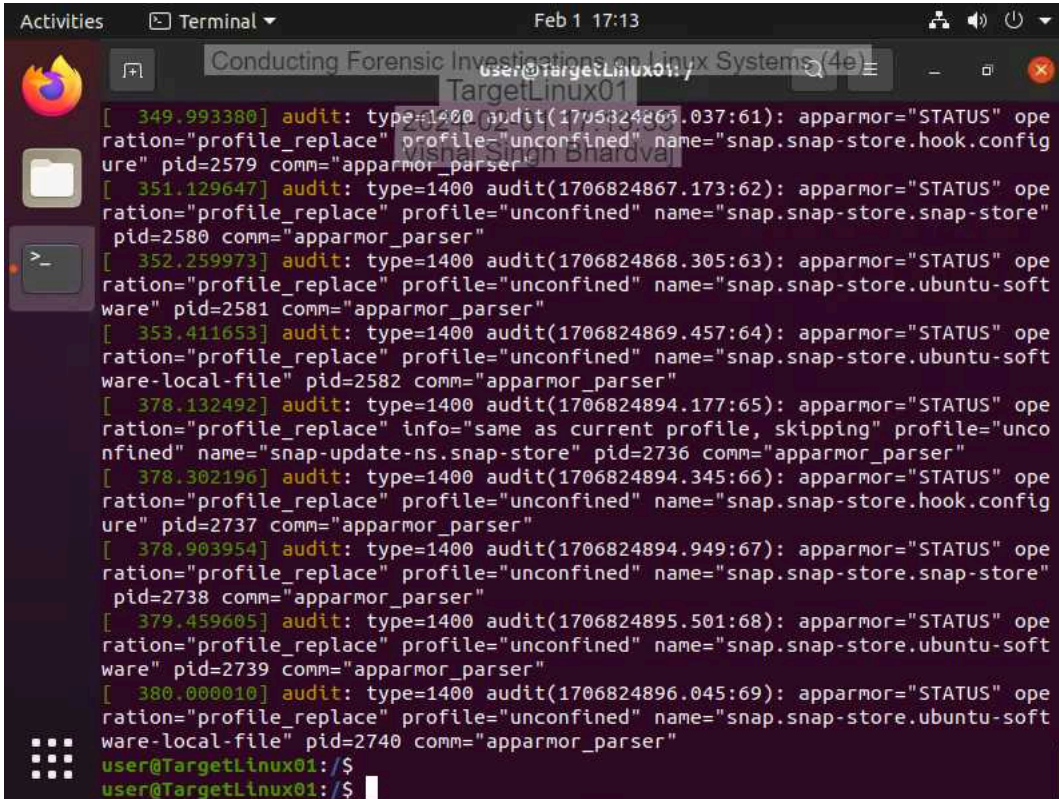


A terminal window titled "Terminal" showing the contents of the /proc directory. The window has a dark background with light-colored text. The terminal output lists various system files and their permissions, owner, and size. The files listed include: aps, dr-xr-xr-x, s, srq-trigger, dr-xr-xr-x, svipc, lrwxrwxrwx, read-self -> 2844/task/2844, mer_list, dr-xr-xr-x, y, time, rsion, rsion_signature, allocinfo, stat, and neinfo. The terminal prompt is user@TargetLinux01:/proc\$. The window title bar shows "Activities", "Terminal", and "Feb 1 17:08".

```
user@TargetLinux01:/proc$ ls -la
-r--r--r-- 1 root root 0 Feb 1 16:55 sw
aps
dr-xr-xr-x 1 root root 0 Feb 1 16:55 sy
s
--w----- 1 root root 0 Feb 1 16:55 sy
srq-trigger
dr-xr-xr-x 5 root root 0 Feb 1 17:01 sy
svipc
lrwxrwxrwx 1 root root 0 Feb 1 16:55 th
read-self -> 2844/task/2844
-r----- 1 root root 0 Feb 1 17:01 ti
mer_list
dr-xr-xr-x 6 root root 0 Feb 1 17:01 tt
y
-r--r--r-- 1 root root 0 Feb 1 17:01 up
time
-r--r--r-- 1 root root 0 Feb 1 17:01 ve
rsion
-r--r--r-- 1 root root 0 Feb 1 17:01 ve
rsion_signature
-r----- 1 root root 0 Feb 1 17:01 vm
allocinfo
-r--r--r-- 1 root root 0 Feb 1 17:01 vm
stat
-r--r--r-- 1 root root 0 Feb 1 17:01 zo
neinfo
user@TargetLinux01:/proc$ pwd
/proc
user@TargetLinux01:/proc$
```

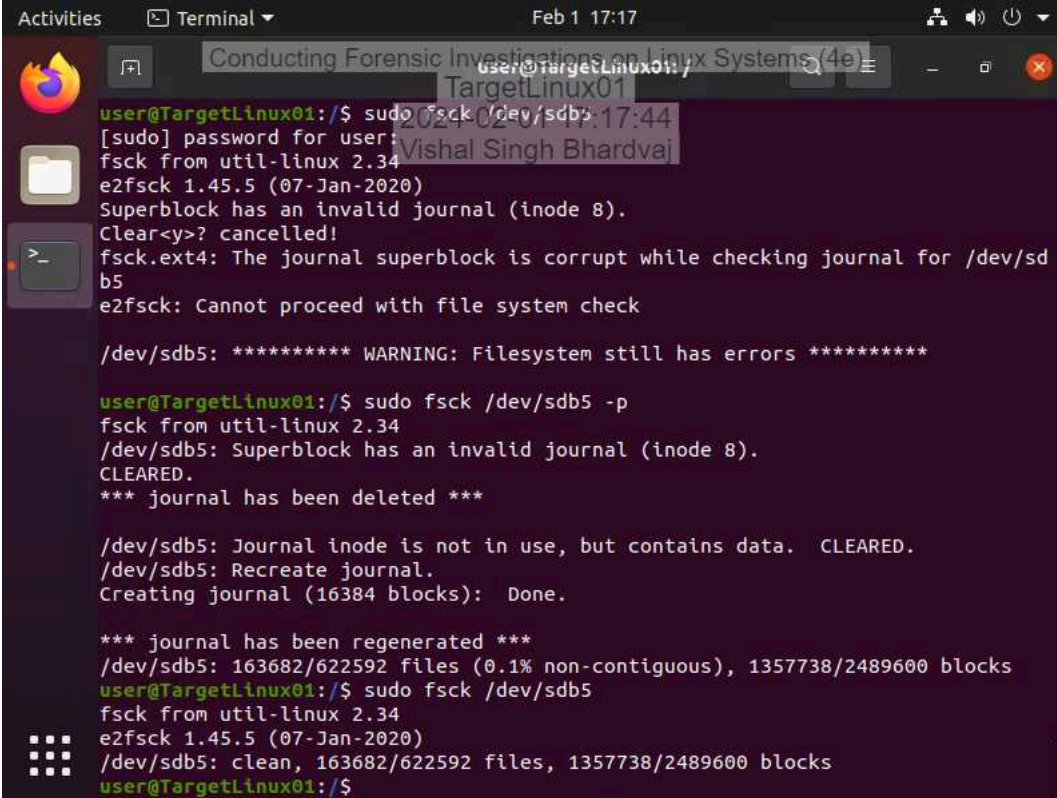
Part 2: Use Linux Shell Commands for Forensic Investigations

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

A screenshot of a Linux terminal window. The window title is "Conducting Forensic Investigations on Linux Systems (4e)" and the terminal prompt is "user@TargetLinux01:". The terminal displays the output of the `dmesg` command, showing several audit messages from the `apparmor_parser` process. The messages are timestamped and include details about the type of operation, the profile being used, and the name of the process being audited. The output is as follows:

```
[ 349.993380] audit: type=1400 audit(1706824865.037:61): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.hook.config" pid=2579 comm="apparmor_parser"
[ 351.129647] audit: type=1400 audit(1706824867.173:62): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.snap-store" pid=2580 comm="apparmor_parser"
[ 352.259973] audit: type=1400 audit(1706824868.305:63): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software" pid=2581 comm="apparmor_parser"
[ 353.411653] audit: type=1400 audit(1706824869.457:64): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software-local-file" pid=2582 comm="apparmor_parser"
[ 378.132492] audit: type=1400 audit(1706824894.177:65): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="snap-update-ns.snap-store" pid=2736 comm="apparmor_parser"
[ 378.302196] audit: type=1400 audit(1706824894.345:66): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.hook.config" pid=2737 comm="apparmor_parser"
[ 378.903954] audit: type=1400 audit(1706824894.949:67): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.snap-store" pid=2738 comm="apparmor_parser"
[ 379.459605] audit: type=1400 audit(1706824895.501:68): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software" pid=2739 comm="apparmor_parser"
[ 380.000010] audit: type=1400 audit(1706824896.045:69): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-software-local-file" pid=2740 comm="apparmor_parser"
user@TargetLinux01:/$
user@TargetLinux01:/$
```

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

A terminal window titled 'Terminal' with a date and time of 'Feb 1 17:17'. The window shows the execution of the 'fsck' command on '/dev/sdb5'. The output indicates a corrupted journal superblock and provides options to clear or delete it. The user chooses to clear it, and the journal is successfully regenerated. The final output shows the file system is clean.

```
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

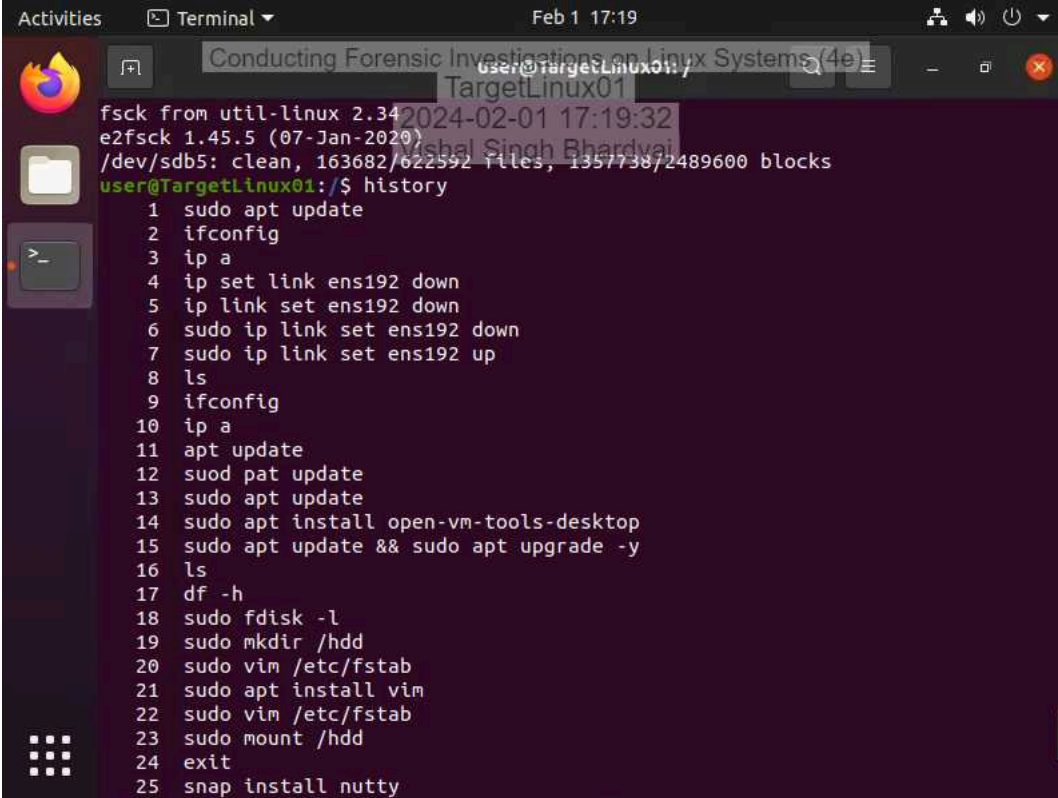
/dev/sdb5: ***** WARNING: Filesystem still has errors *****

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.



The screenshot shows a terminal window titled 'Terminal' with a date and time of 'Feb 1 17:19'. The terminal output displays the results of the 'history' command, listing 25 commands executed in the session. The commands include system checks, network configuration, package updates, and file management. The terminal window has a dark background with light-colored text. The left sidebar shows icons for Activities, Terminal, and a file manager. The top bar includes system status icons like network, volume, and power.

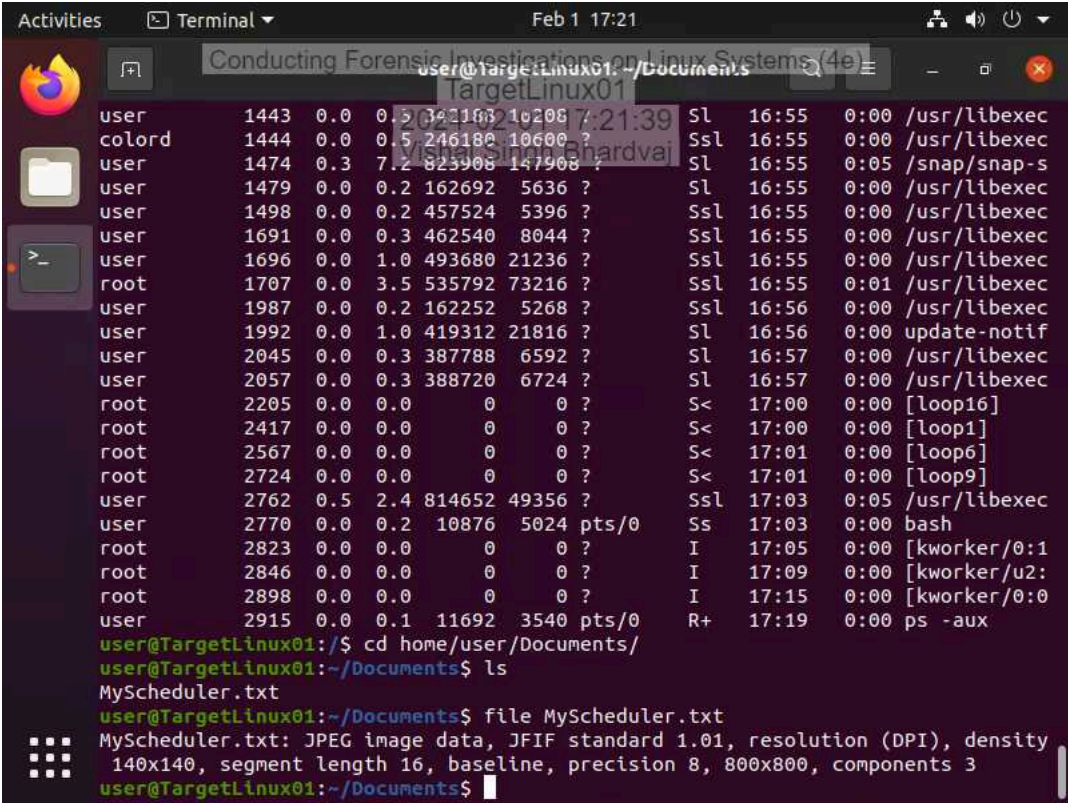
```
user@TargetLinux01:~$ history
1  sudo apt update
2  ifconfig
3  ip a
4  ip set link ens192 down
5  ip link set ens192 down
6  sudo ip link set ens192 down
7  sudo ip link set ens192 up
8  ls
9  ifconfig
10 ip a
11 apt update
12 suod pat update
13 sudo apt update
14 sudo apt install open-vm-tools-desktop
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
```

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

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

[illegible]

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

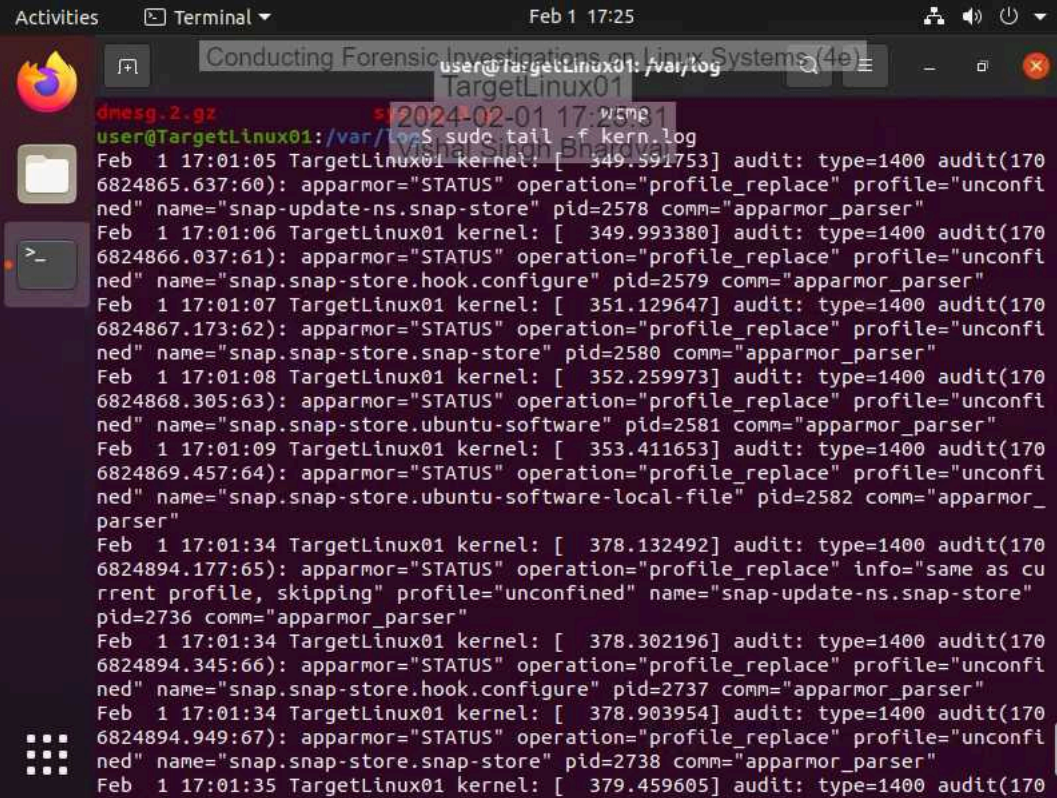


The screenshot shows a terminal window titled 'Terminal' with the date 'Feb 1 17:21'. The user is logged in as 'user' on a system named 'TargetLinux01'. The terminal displays the output of the 'file' command on a file named 'MyScheduler.txt'. The output indicates that the file is a JPEG image with the following details: JFIF standard 1.01, resolution (DPI), density 140x140, segment length 16, baseline, precision 8, 800x800, components 3.

```
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
```

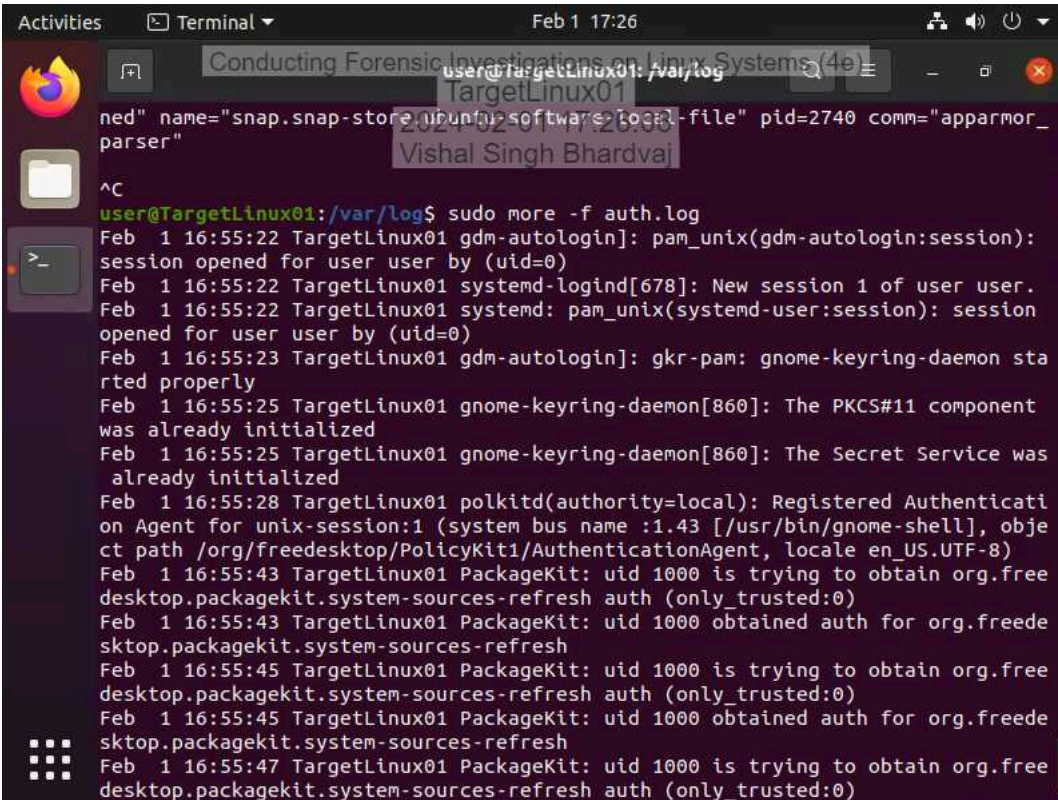
Part 3: Retrieve Logs Files on a Live Linux System

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



```
Activities Terminal Feb 1 17:25
Conducting Forensic Investigations on Linux Systems (4e)
user@TargetLinux01: /var/log
dmesg.2.gz
user@TargetLinux01: /var/log $ sudo tail -f kern.log
Feb 1 17:01:05 TargetLinux01 kernel: [ 349.591753] audit: type=1400 audit(170
6824865.637:60): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap-update-ns.snap-store" pid=2578 comm="apparmor_parser"
Feb 1 17:01:06 TargetLinux01 kernel: [ 349.993380] audit: type=1400 audit(170
6824866.037:61): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.hook.configure" pid=2579 comm="apparmor_parser"
Feb 1 17:01:07 TargetLinux01 kernel: [ 351.129647] audit: type=1400 audit(170
6824867.173:62): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.snap-store" pid=2580 comm="apparmor_parser"
Feb 1 17:01:08 TargetLinux01 kernel: [ 352.259973] audit: type=1400 audit(170
6824868.305:63): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.ubuntu-software" pid=2581 comm="apparmor_parser"
Feb 1 17:01:09 TargetLinux01 kernel: [ 353.411653] audit: type=1400 audit(170
6824869.457:64): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.ubuntu-software-local-file" pid=2582 comm="apparmor_
parser"
Feb 1 17:01:34 TargetLinux01 kernel: [ 378.132492] audit: type=1400 audit(170
6824894.177:65): apparmor="STATUS" operation="profile_replace" info="same as cu
rrent profile, skipping" profile="unconfined" name="snap-update-ns.snap-store"
pid=2736 comm="apparmor_parser"
Feb 1 17:01:34 TargetLinux01 kernel: [ 378.302196] audit: type=1400 audit(170
6824894.345:66): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.hook.configure" pid=2737 comm="apparmor_parser"
Feb 1 17:01:34 TargetLinux01 kernel: [ 378.903954] audit: type=1400 audit(170
6824894.949:67): apparmor="STATUS" operation="profile_replace" profile="unconfi
ned" name="snap.snap-store.snap-store" pid=2738 comm="apparmor_parser"
Feb 1 17:01:35 TargetLinux01 kernel: [ 379.459605] audit: type=1400 audit(170
```

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



The image shows a terminal window titled "Terminal" with the date and time "Feb 1 17:26". The terminal prompt is "user@TargetLinux01: /var/log". The user has entered the command "sudo more -f auth.log". The output of the command is displayed in the terminal, showing system logs for authentication and session management. The logs include entries for "gdm-autologin", "systemd-logind", "gnome-keyring-daemon", and "PackageKit".

```
ned" name="snap.snap-store/ubuntu-software-tool-file" pid=2740 comm="apparmor_
parser"
^C
user@TargetLinux01: /var/log$ sudo more -f auth.log
Feb 1 16:55:22 TargetLinux01 gdm-autologin]: pam_unix(gdm-autologin:session):
session opened for user user by (uid=0)
Feb 1 16:55:22 TargetLinux01 systemd-logind[678]: New session 1 of user user.
Feb 1 16:55:22 TargetLinux01 systemd: pam_unix(systemd-user:session): session
opened for user user by (uid=0)
Feb 1 16:55:23 TargetLinux01 gdm-autologin]: gkr-pam: gnome-keyring-daemon sta
rted properly
Feb 1 16:55:25 TargetLinux01 gnome-keyring-daemon[860]: The PKCS#11 component
was already initialized
Feb 1 16:55:25 TargetLinux01 gnome-keyring-daemon[860]: The Secret Service was
already initialized
Feb 1 16:55:28 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 1 16:55:43 TargetLinux01 PackageKit: uid 1000 is trying to obtain org.free
desktop.packagekit.system-sources-refresh auth (only_trusted:0)
Feb 1 16:55:43 TargetLinux01 PackageKit: uid 1000 obtained auth for org.freede
sktop.packagekit.system-sources-refresh
Feb 1 16:55:45 TargetLinux01 PackageKit: uid 1000 is trying to obtain org.free
desktop.packagekit.system-sources-refresh auth (only_trusted:0)
Feb 1 16:55:45 TargetLinux01 PackageKit: uid 1000 obtained auth for org.freede
sktop.packagekit.system-sources-refresh
Feb 1 16:55:47 TargetLinux01 PackageKit: uid 1000 is trying to obtain org.free
desktop.packagekit.system-sources-refresh auth (only_trusted:0)
```

Section 2: Applied Learning

Part 1: Identify Login Attempts on a Linux Drive Image

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

Name of Non Root user attempted to login- noel, dominic

Number of attempts detected - 18

Date/time range of the attempts - June 11, 00:57:11 - June 11, 05:39:01

Source IP address - 192.168.78.1

Port- 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 - Dominic

Date and Time of most recent successful login -

June 9, 13:31:59

June 11, 05:23:03

User - noel

No successful login

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, autotools.dev, build-essential, autoconf, kbd

Suspicious application - logkeys - It is a key logger that might have been used in spying password.

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

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

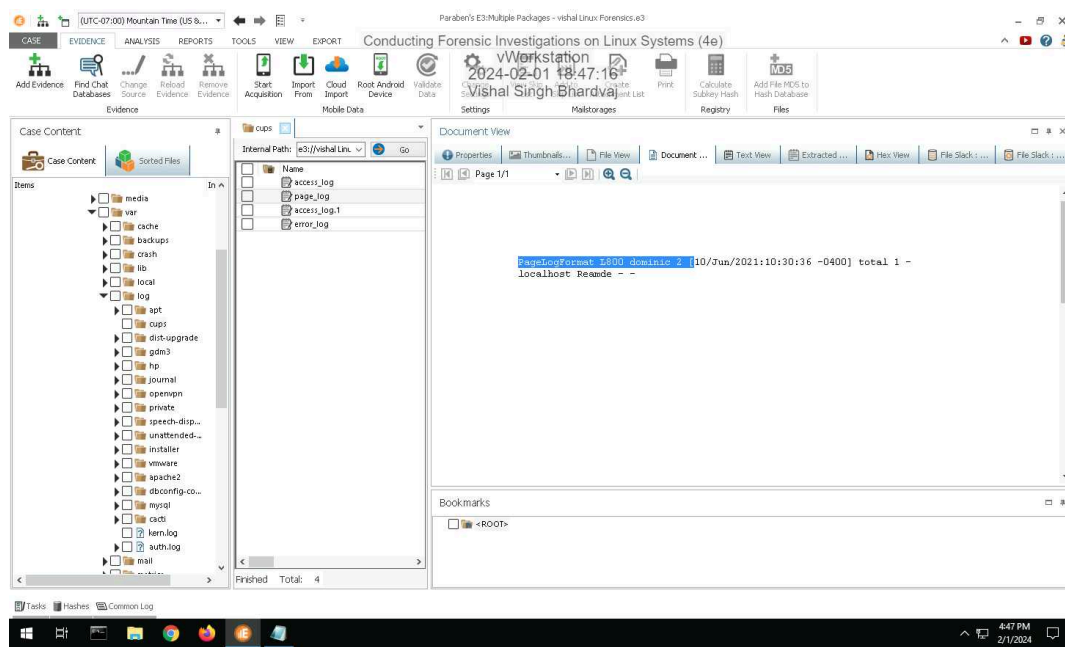
USB storage device connected - Jun 10, 10:24:12

Serial 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.



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.

