Student:	Email:
Jose Cruz	jose.cruz2@udc.edu

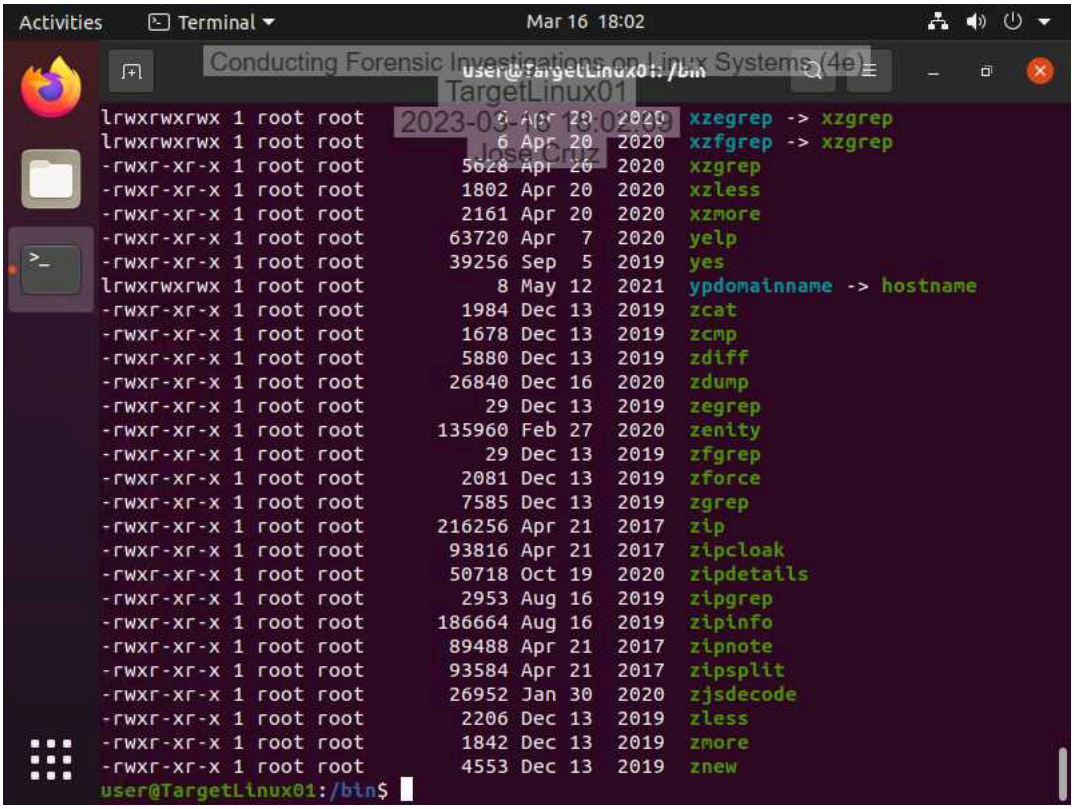
Time on Task:	Progress:
9 hours, 20 minutes	100%

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

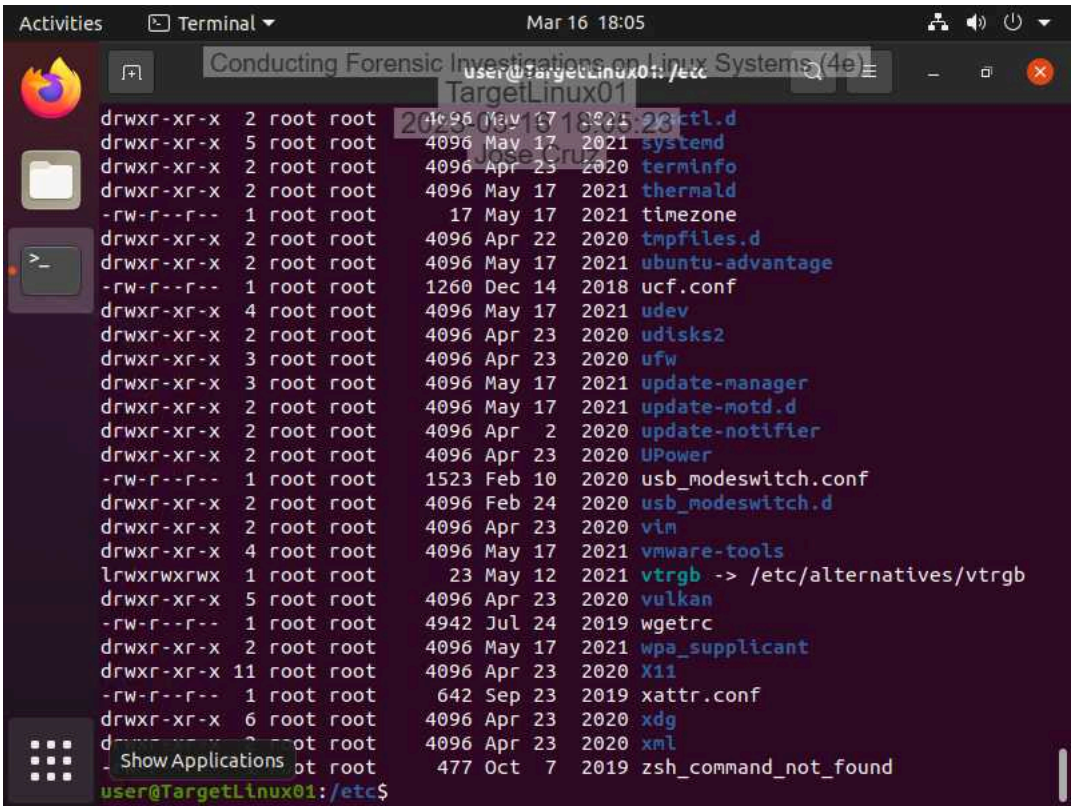
Section 1: Hands-On Demonstration

Part 1: Explore a Live Linux System

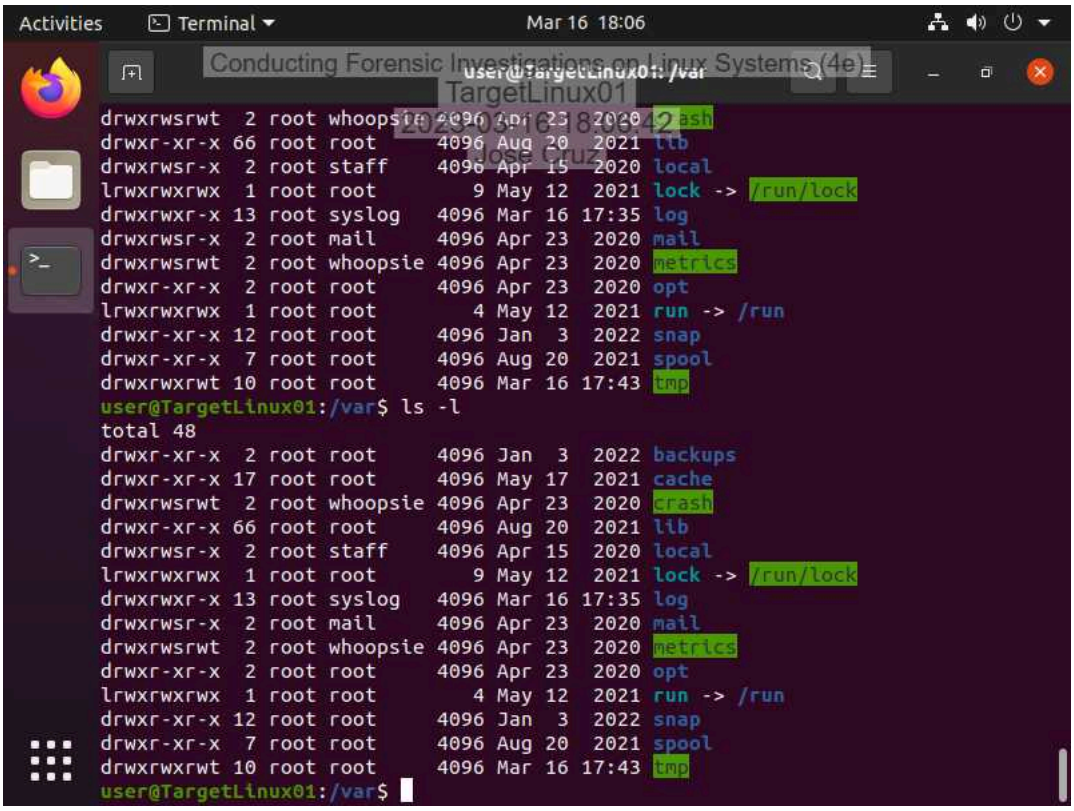
17. **Make a screen capture** showing the **contents of the /bin directory**.



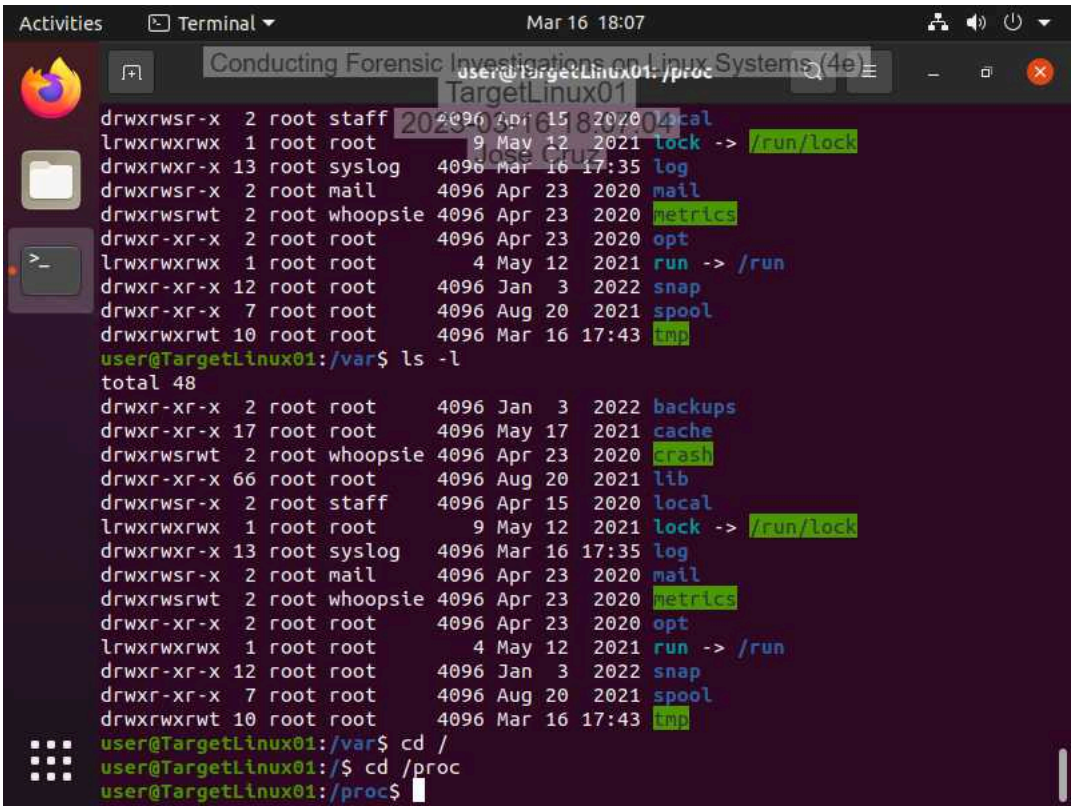
20. **Make a screen capture** showing the **contents of the /etc directory**.



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

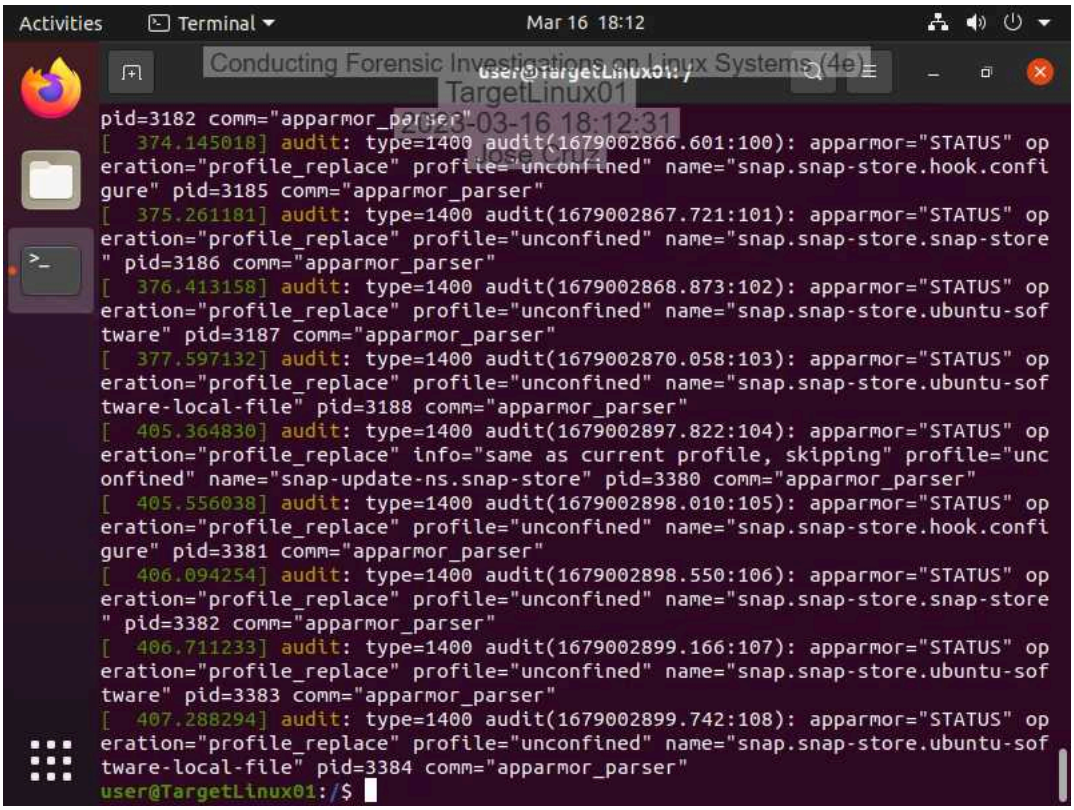


22. **Make a screen capture** showing the **contents of the /proc directory**.

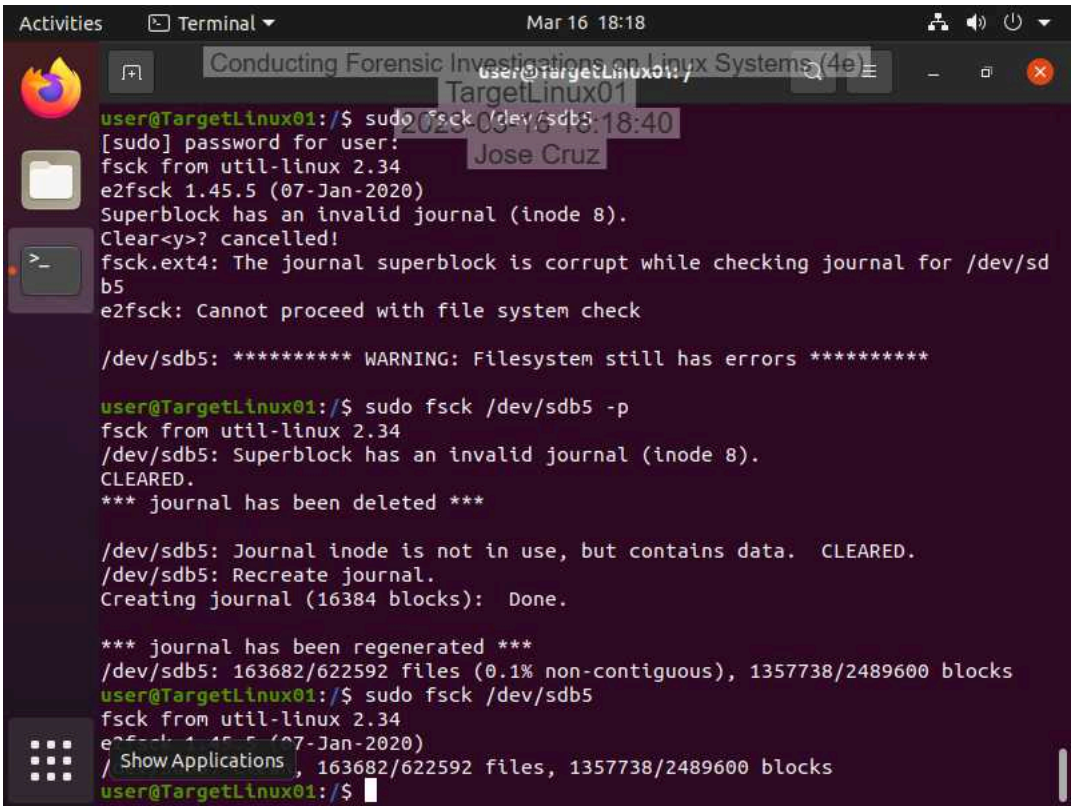


Part 2: Use Linux Shell Commands for Forensic Investigations

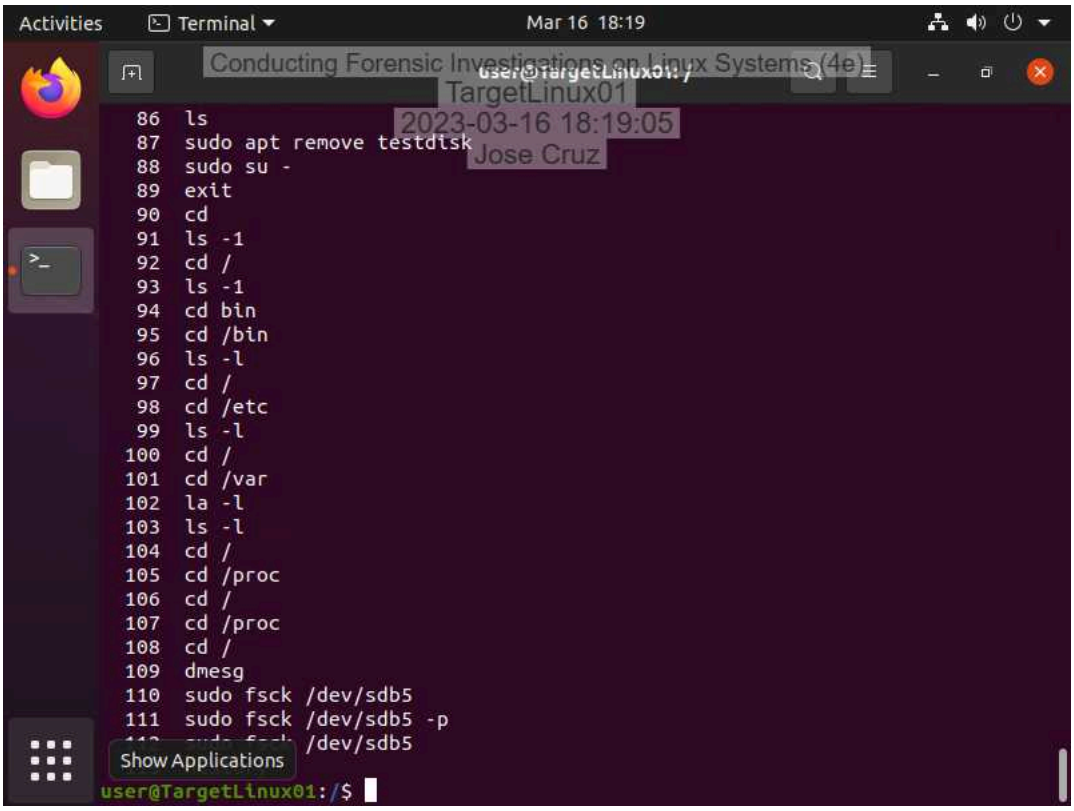
2. **Make a screen capture** showing the **results of the dmesg command**.



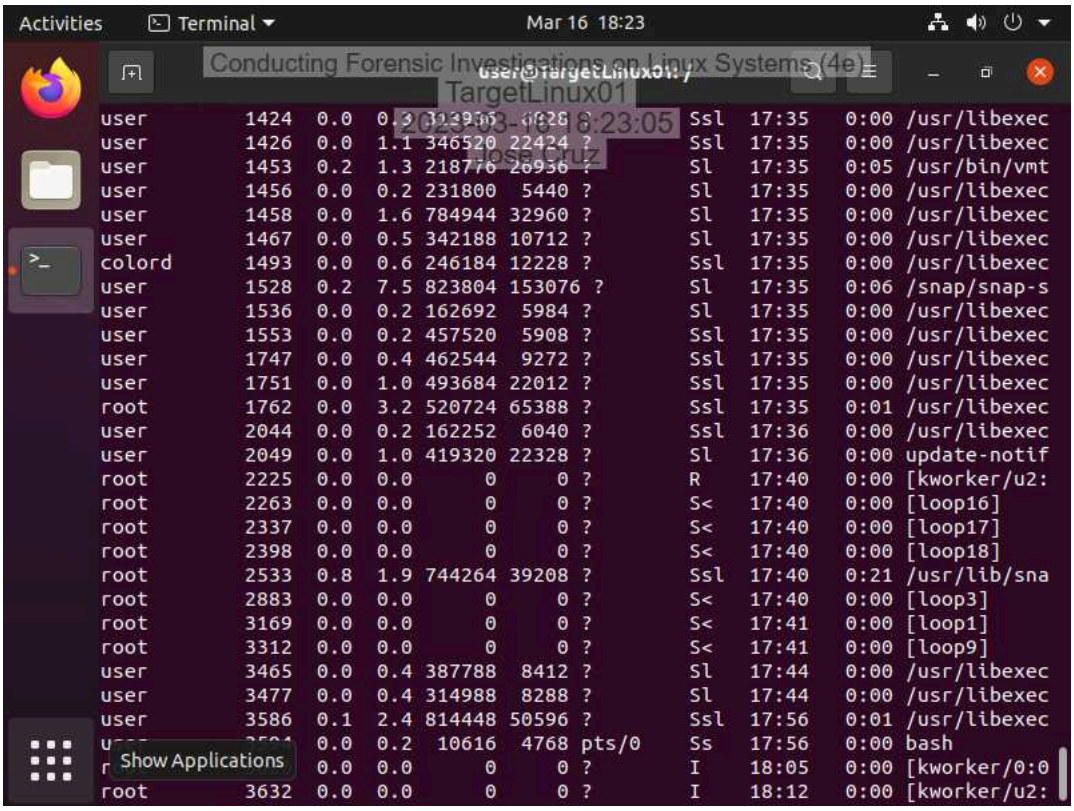
7. **Make a screen capture** showing the **results of the fsck command.**



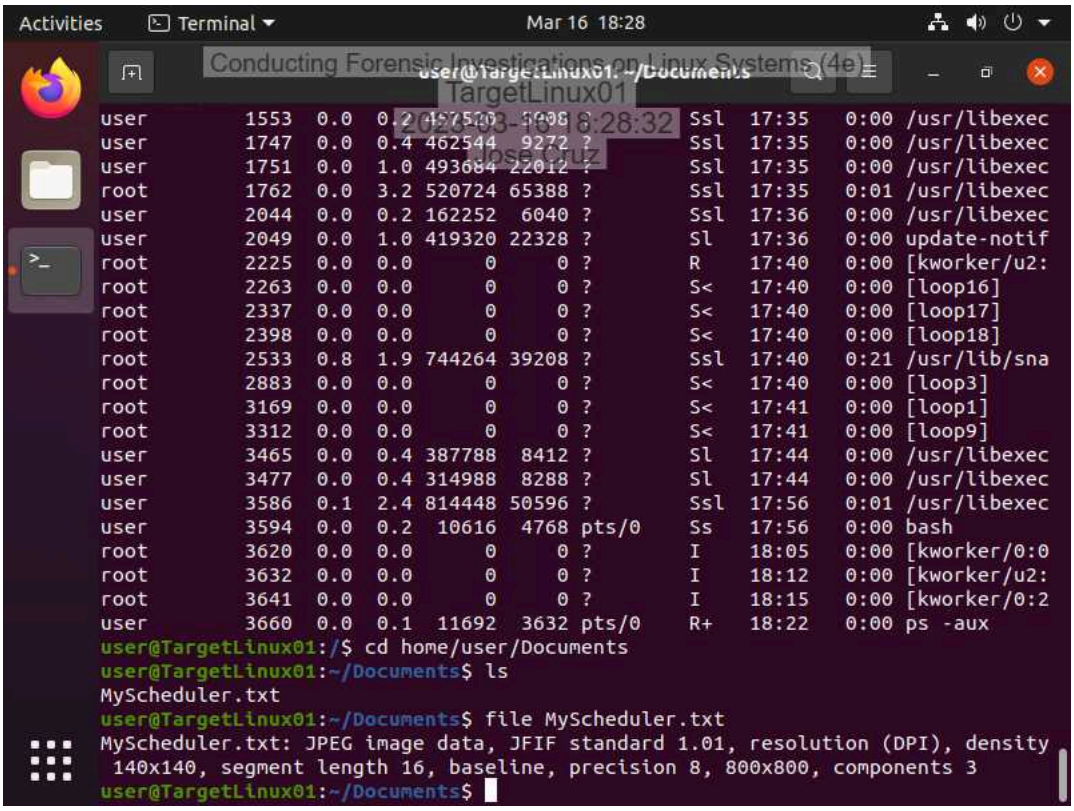
9. **Make a screen capture** showing the **results of the history command**.



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

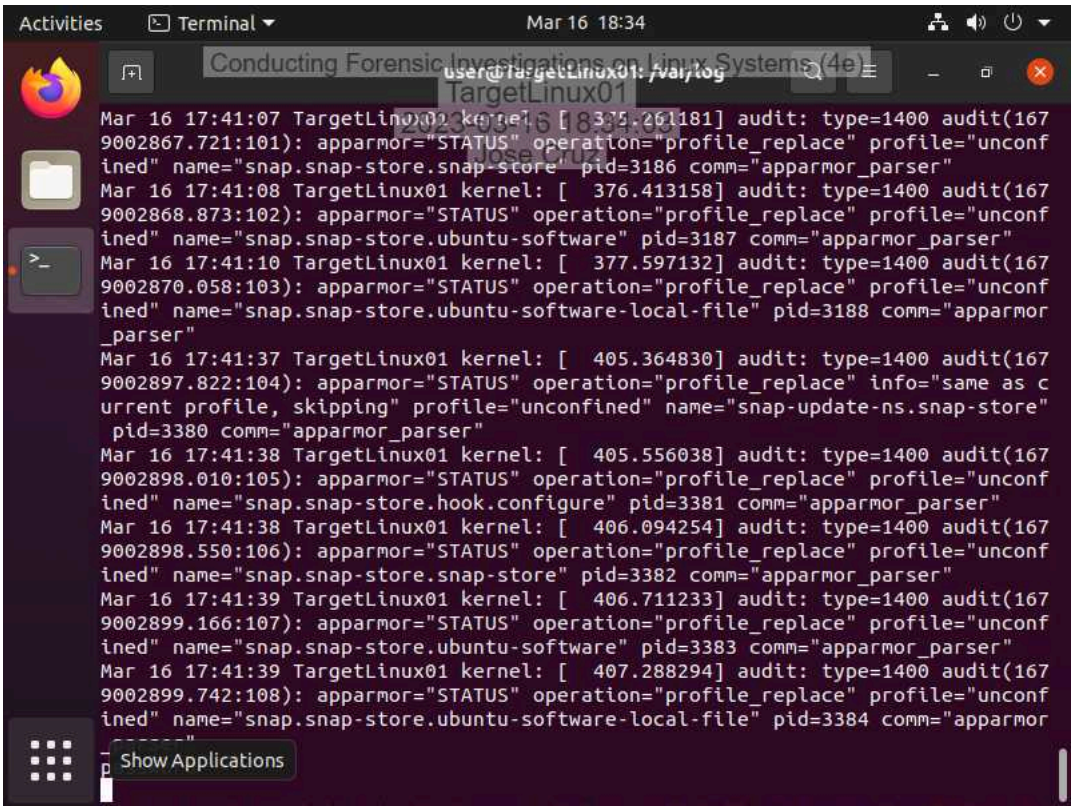


15. **Make a screen capture** showing the **results of the file command**.

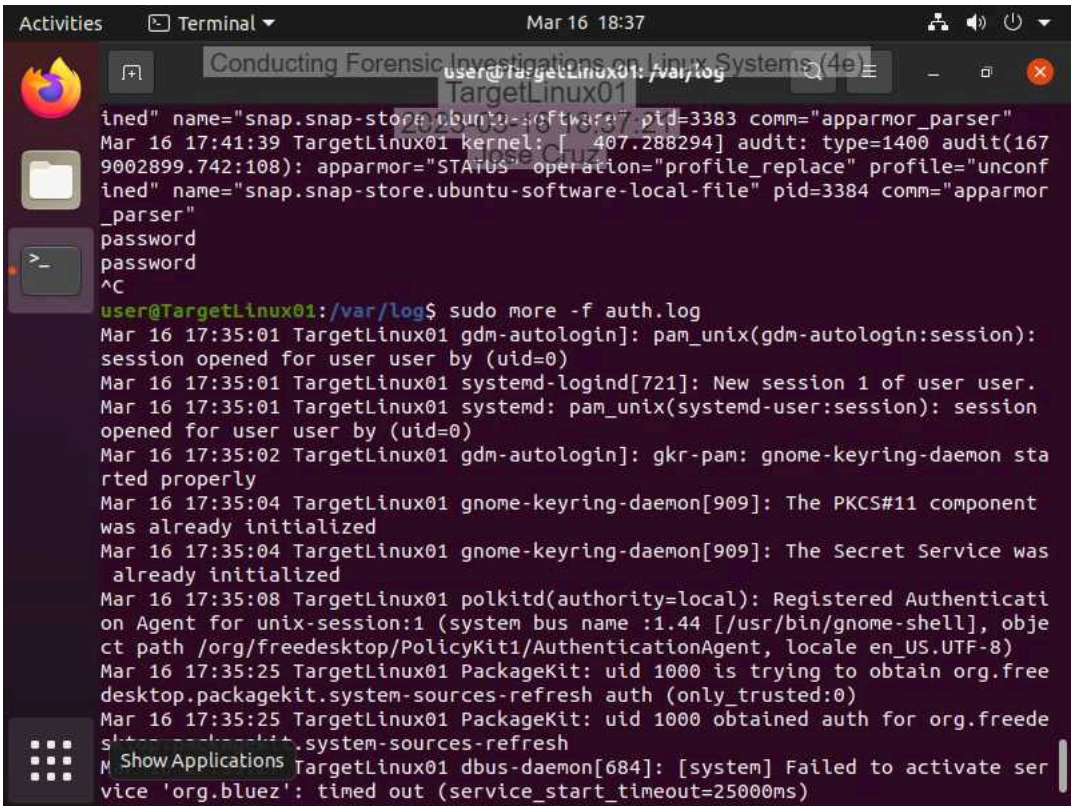


Part 3: Retrieve Logs Files on a Live Linux System

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



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



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

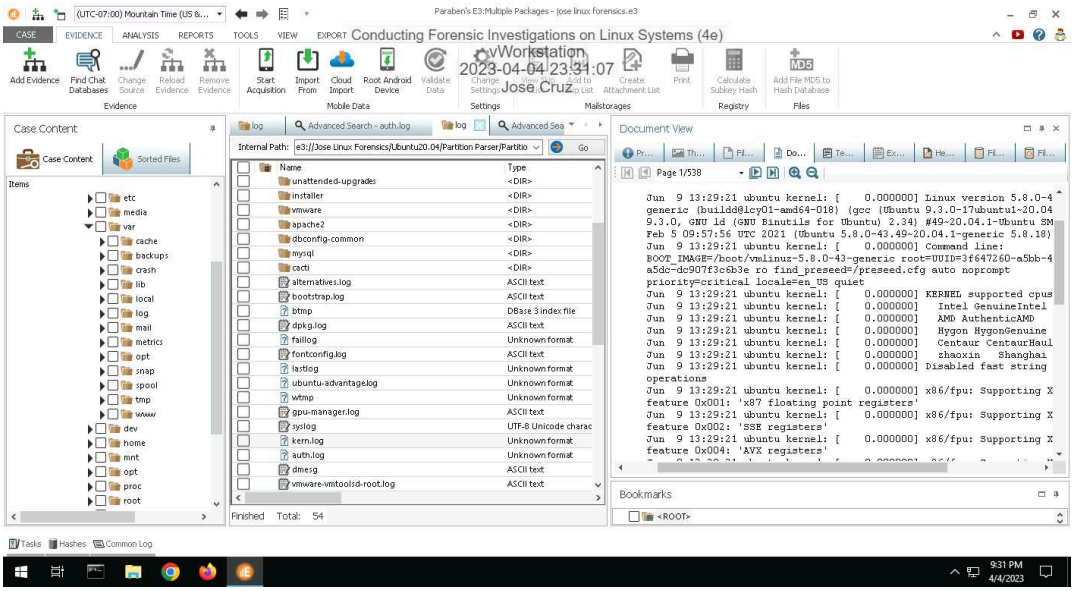
4. **Document** when the USB storage device was connected and its serial number.

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

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**.