Student:	Email:
Vishal Singh Bhardvaj	

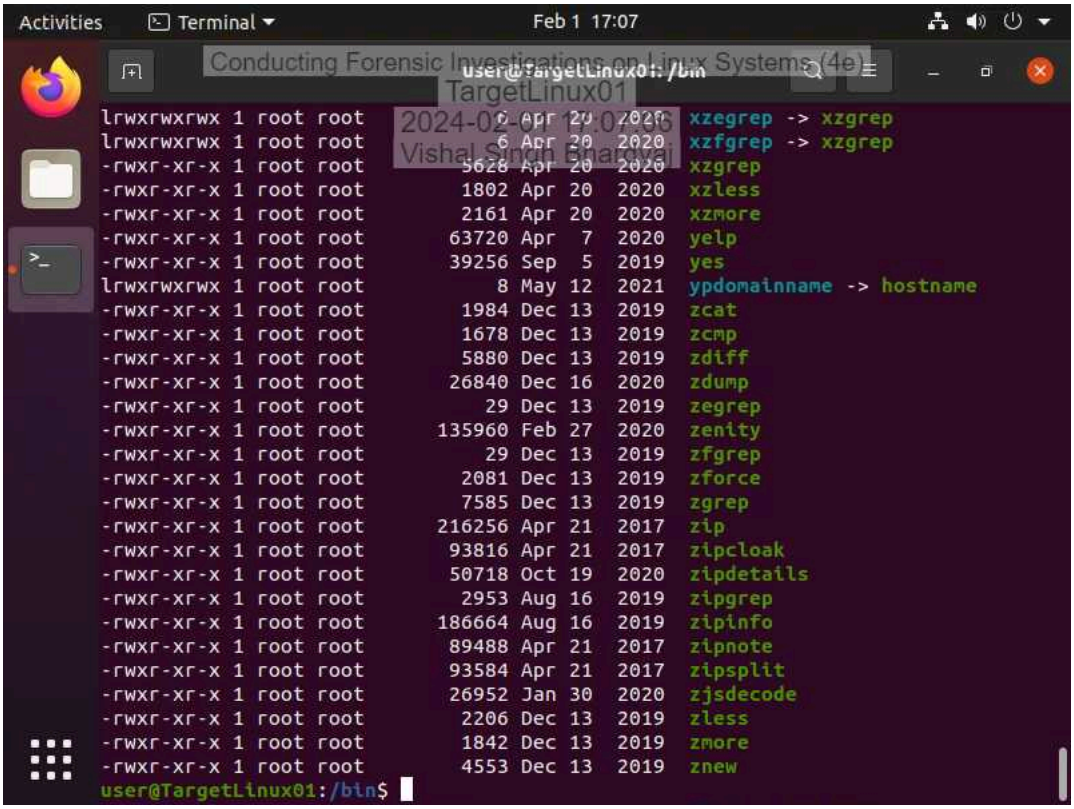
Time on Task:	Progress:
2 hours, 2 minutes	100%

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

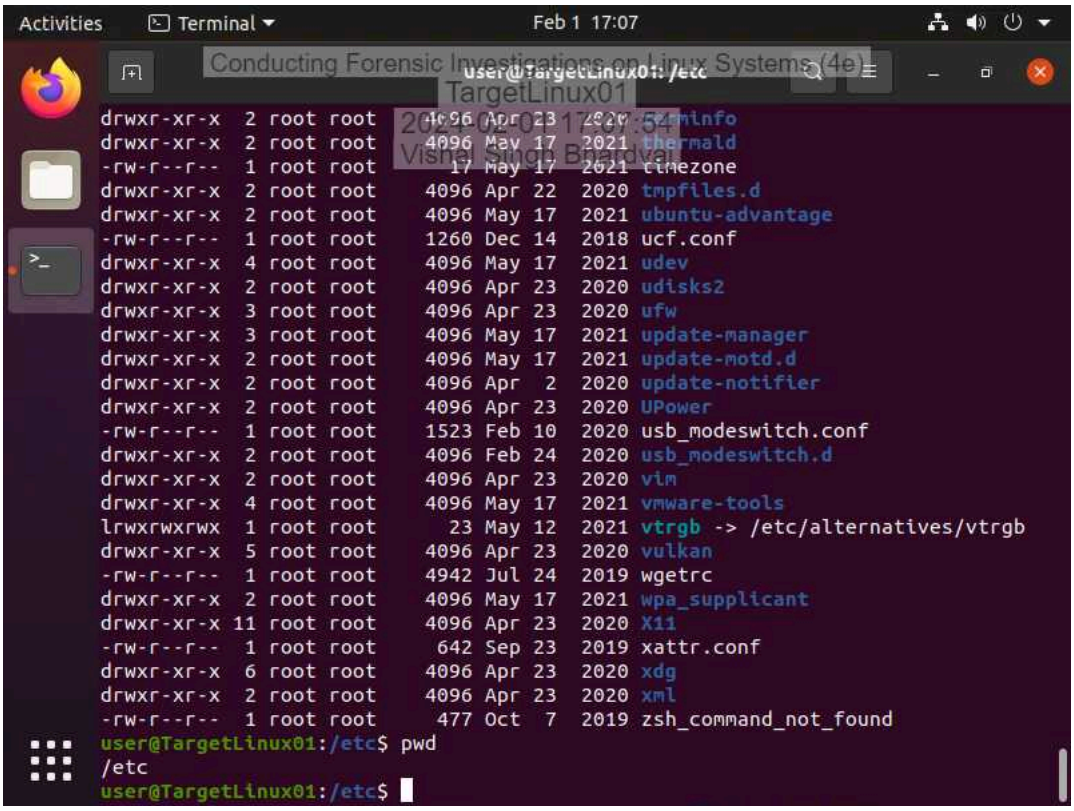
Section 1: Hands-On Demonstration

Part 1: Explore a Live Linux System

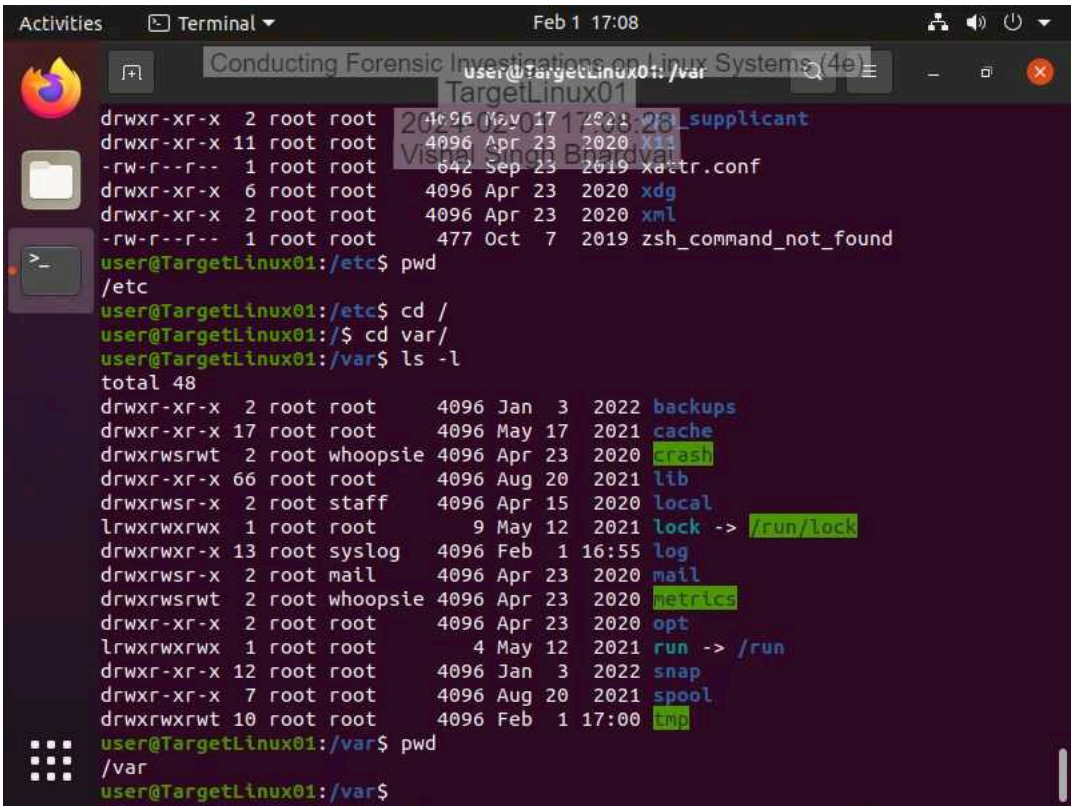
17. **Make a screen capture** showing the **contents of the /bin directory**.



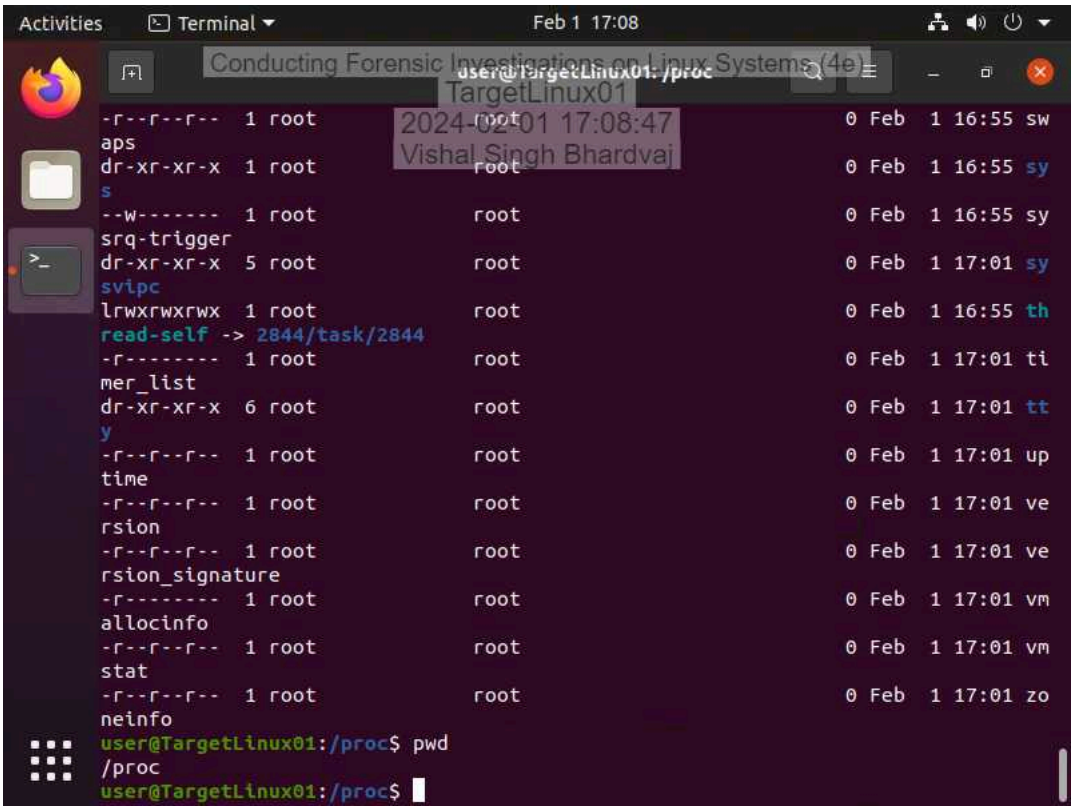
20. **Make a screen capture** showing the **contents of the /etc directory**.



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

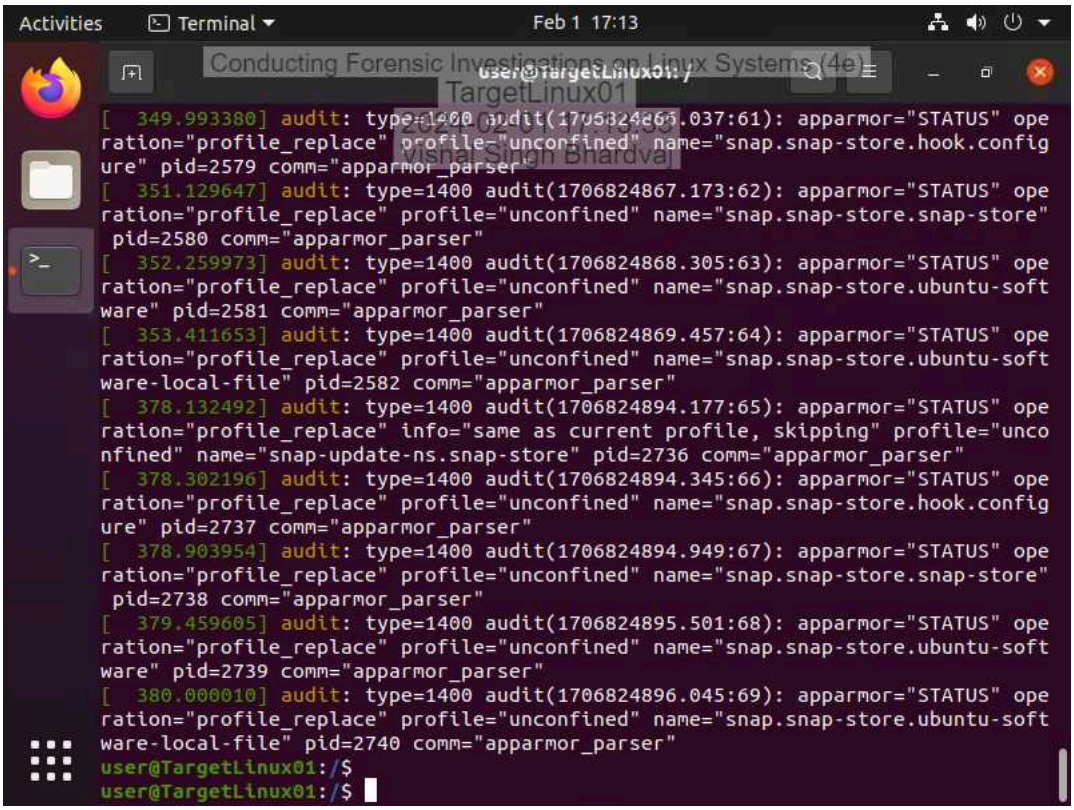


22. **Make a screen capture** showing the **contents of the /proc directory**.

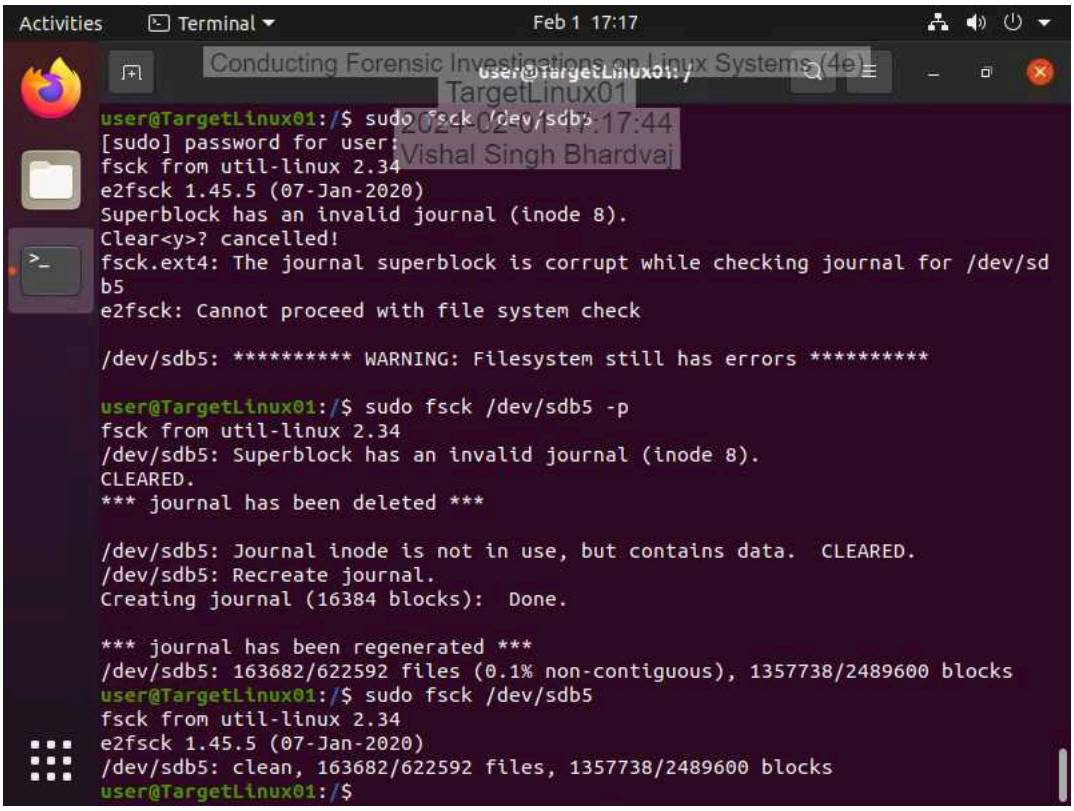


Part 2: Use Linux Shell Commands for Forensic Investigations

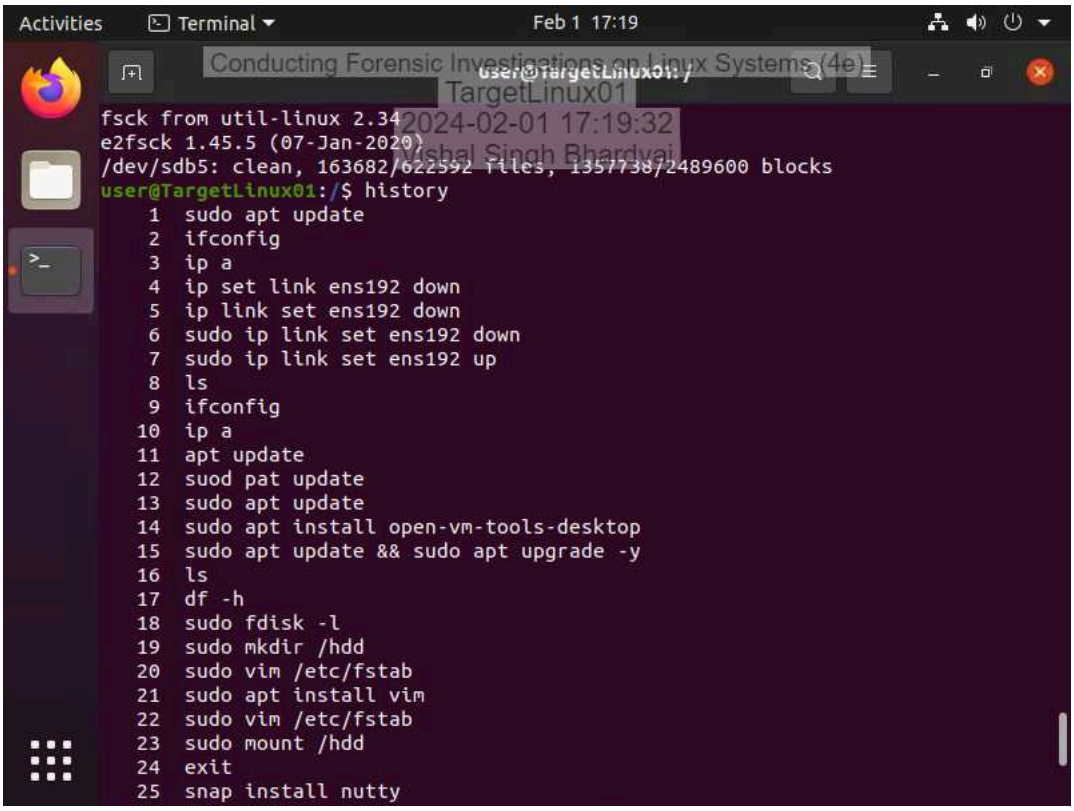
2. **Make a screen capture** showing the **results of the dmesg command**.



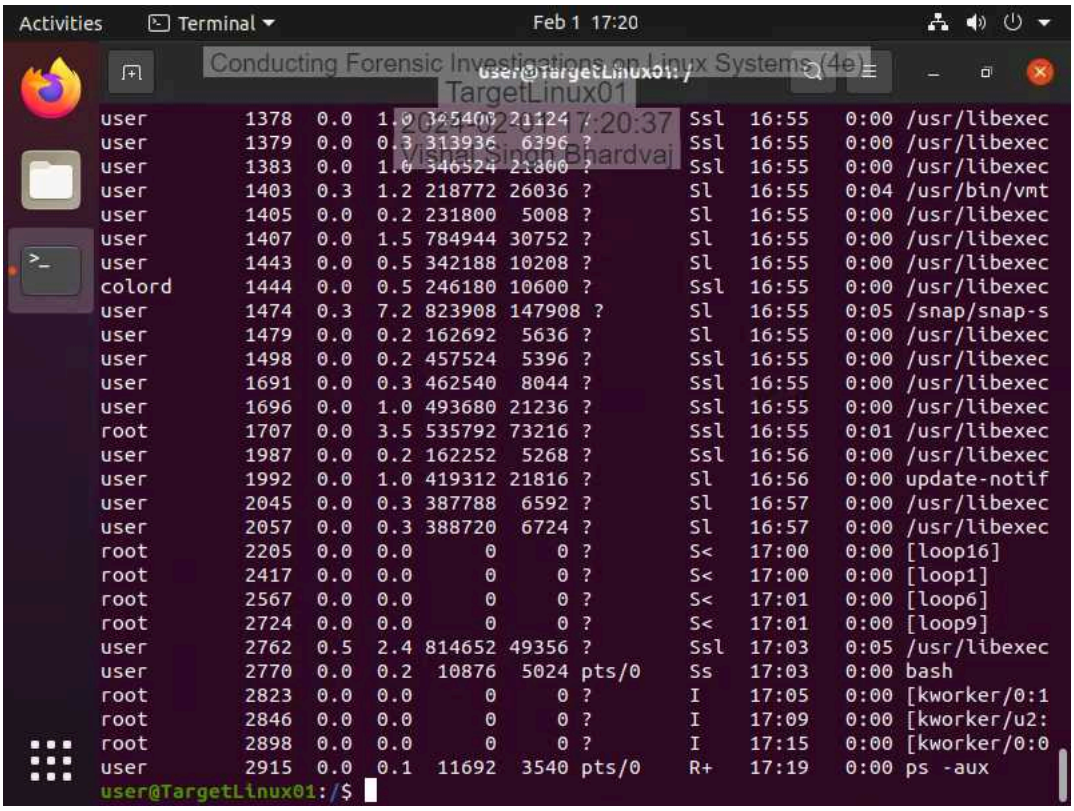
7. **Make a screen capture** showing the **results of the fsck command.**



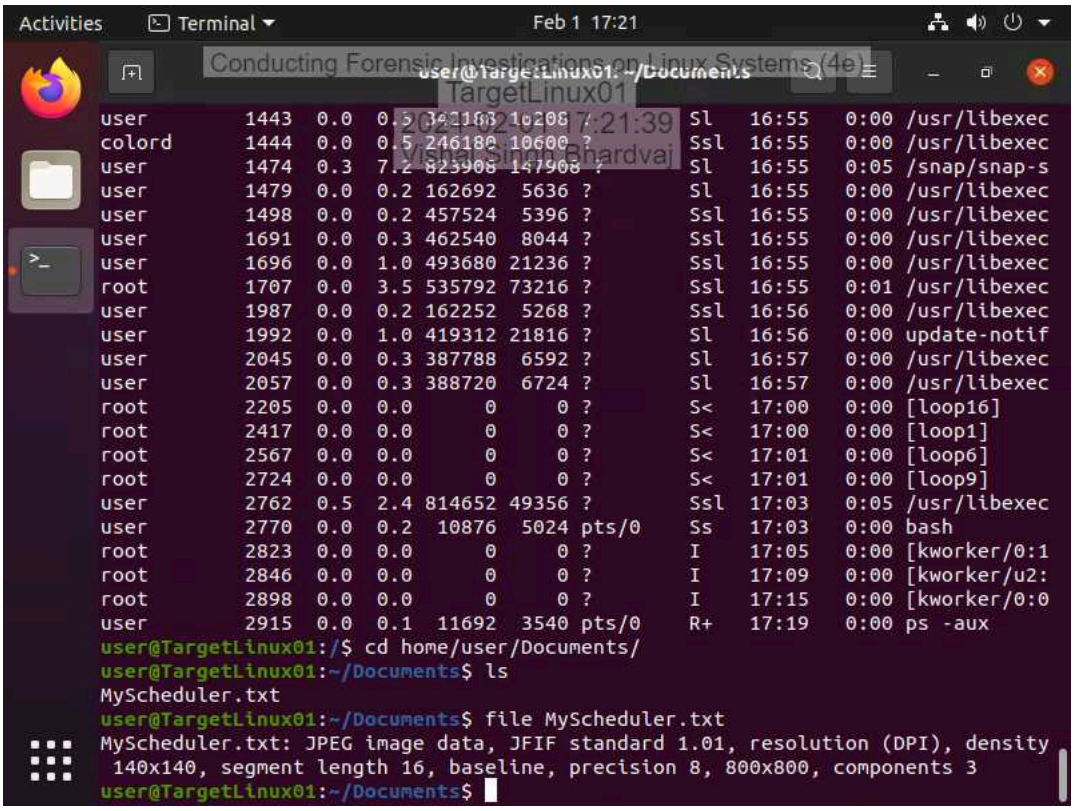
9. **Make a screen capture** showing the **results of the history command**.



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

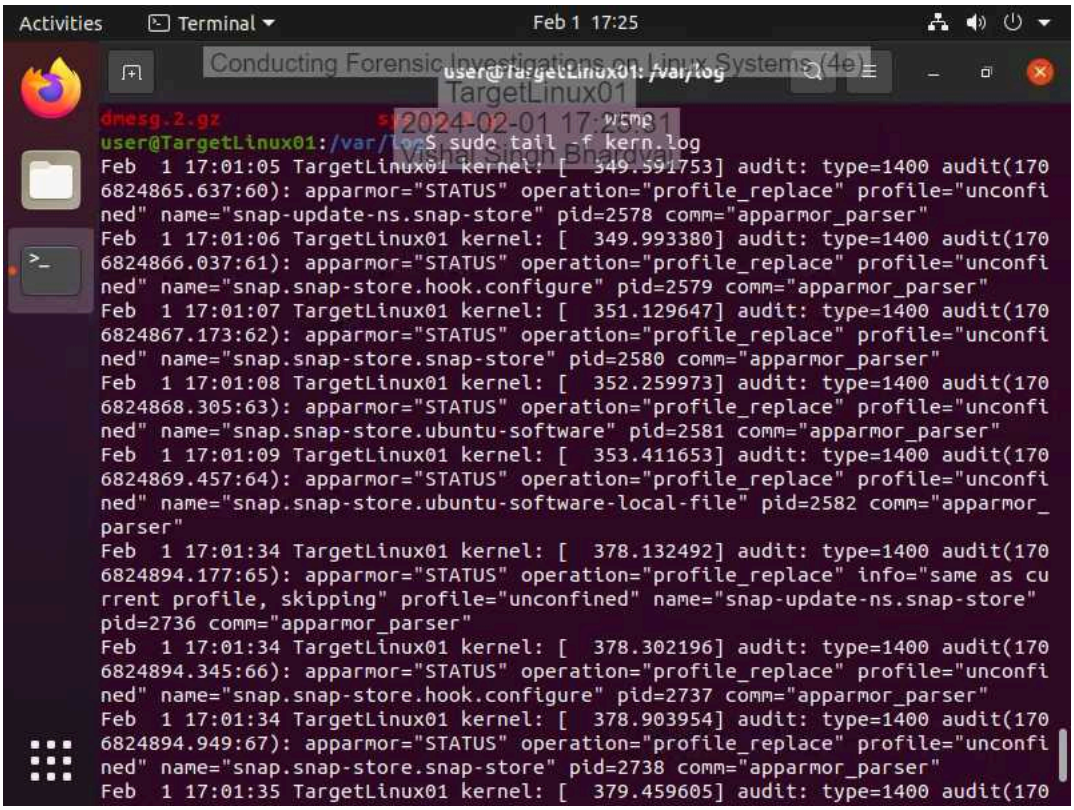


15. **Make a screen capture** showing the **results of the file command**.

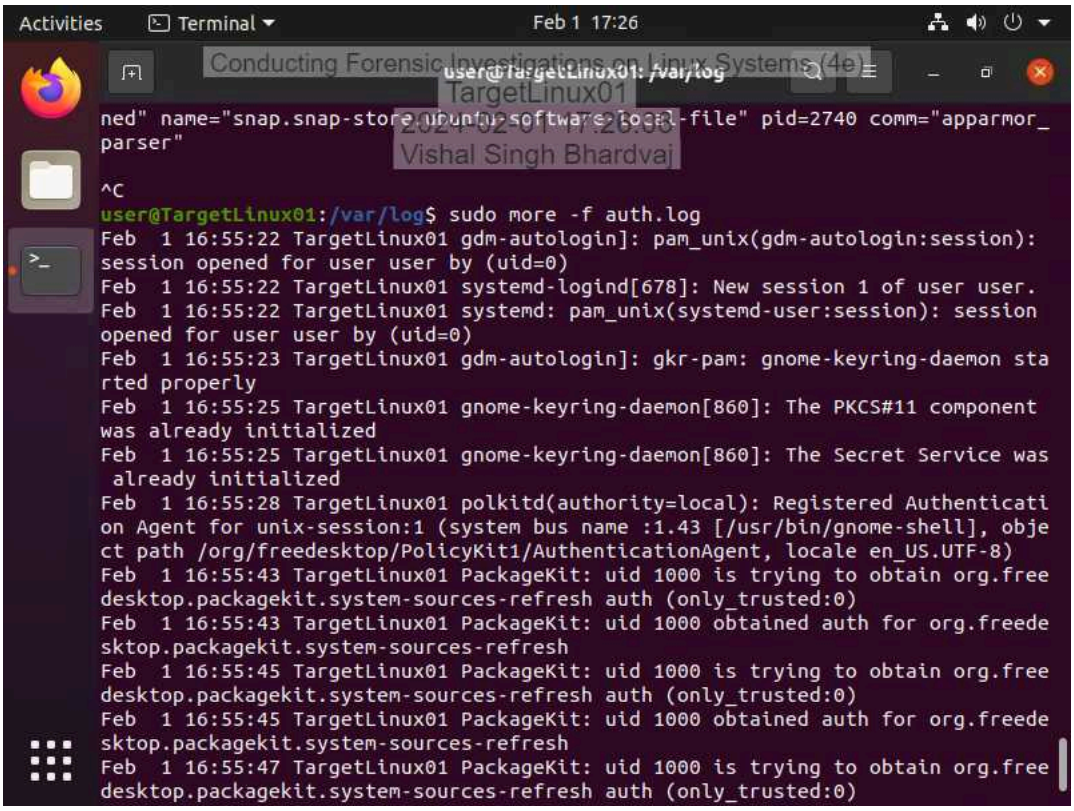


Part 3: Retrieve Logs Files on a Live Linux System

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.

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

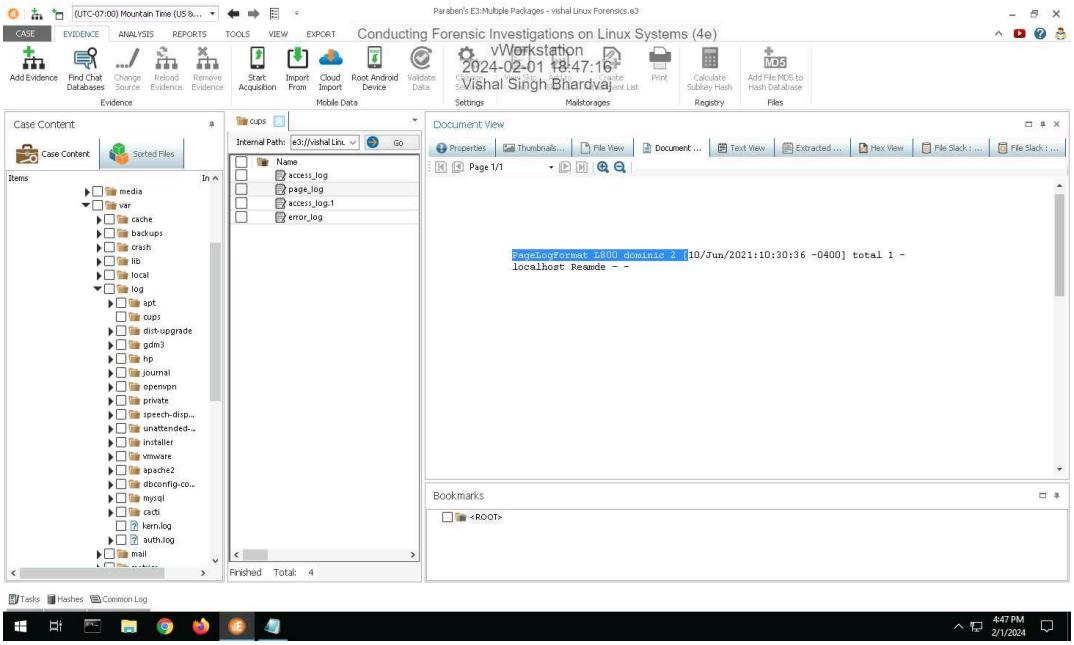
4. **Document** when the USB storage device was connected and its serial number.

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

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