Student:	Email:
Loksharan Saravanan	loksharan.soc@gmail.com

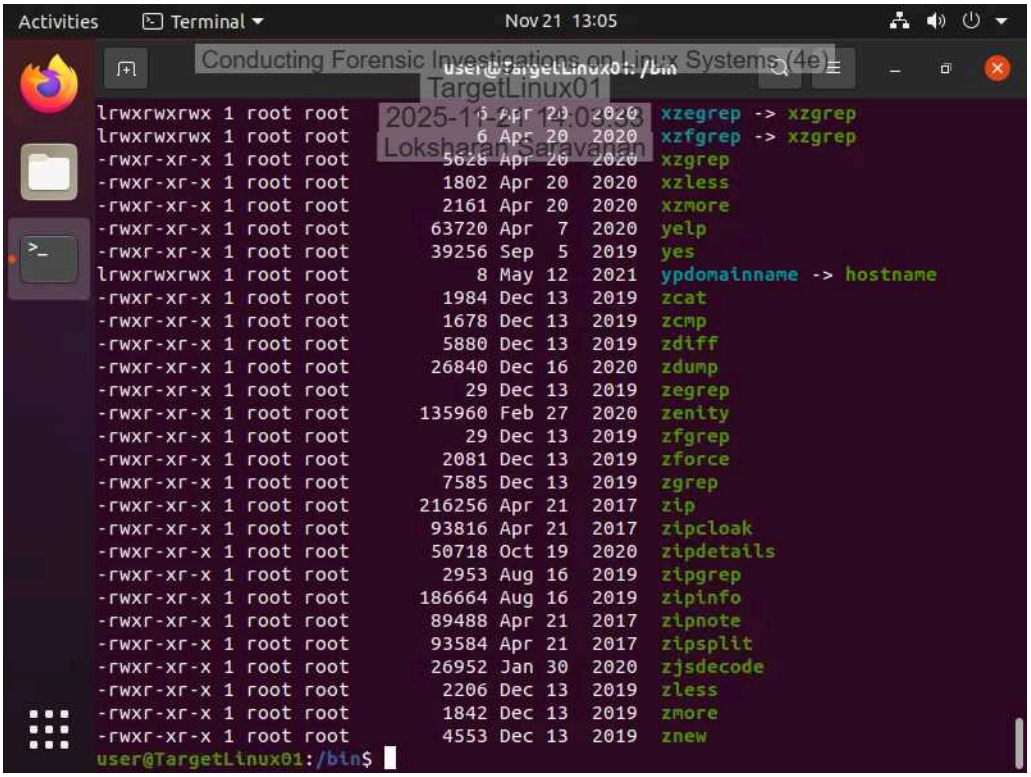
Time on Task:	Progress:
0 hours, 48 minutes	100%

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

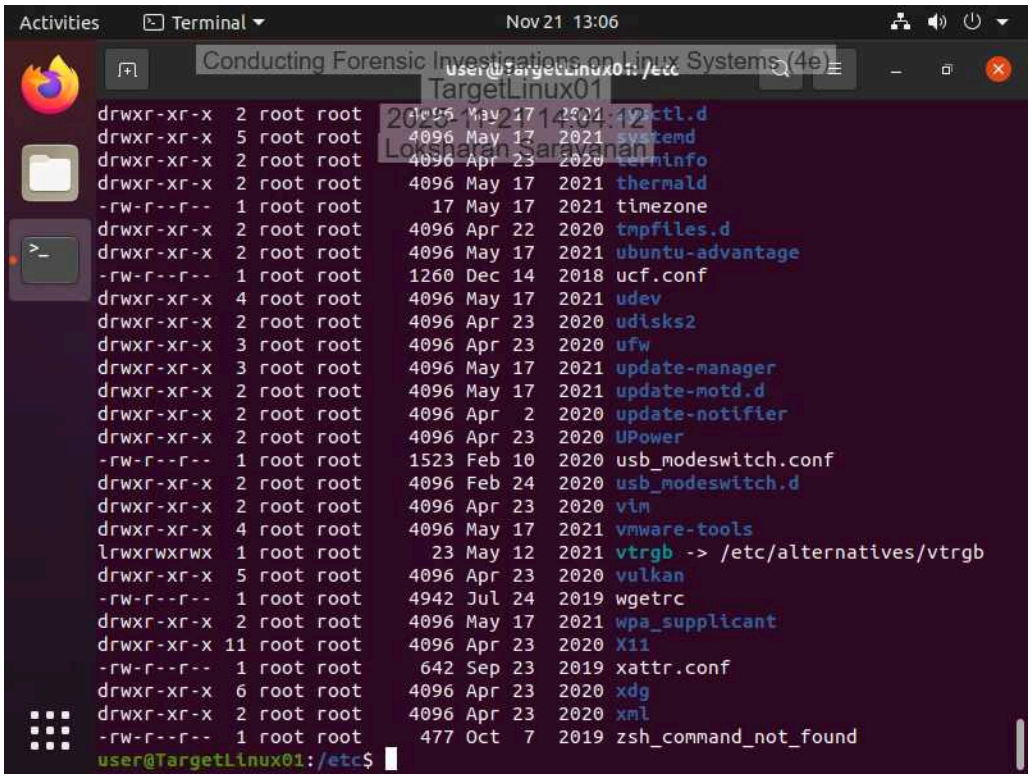
Section 1: Hands-On Demonstration

Part 1: Explore a Live Linux System

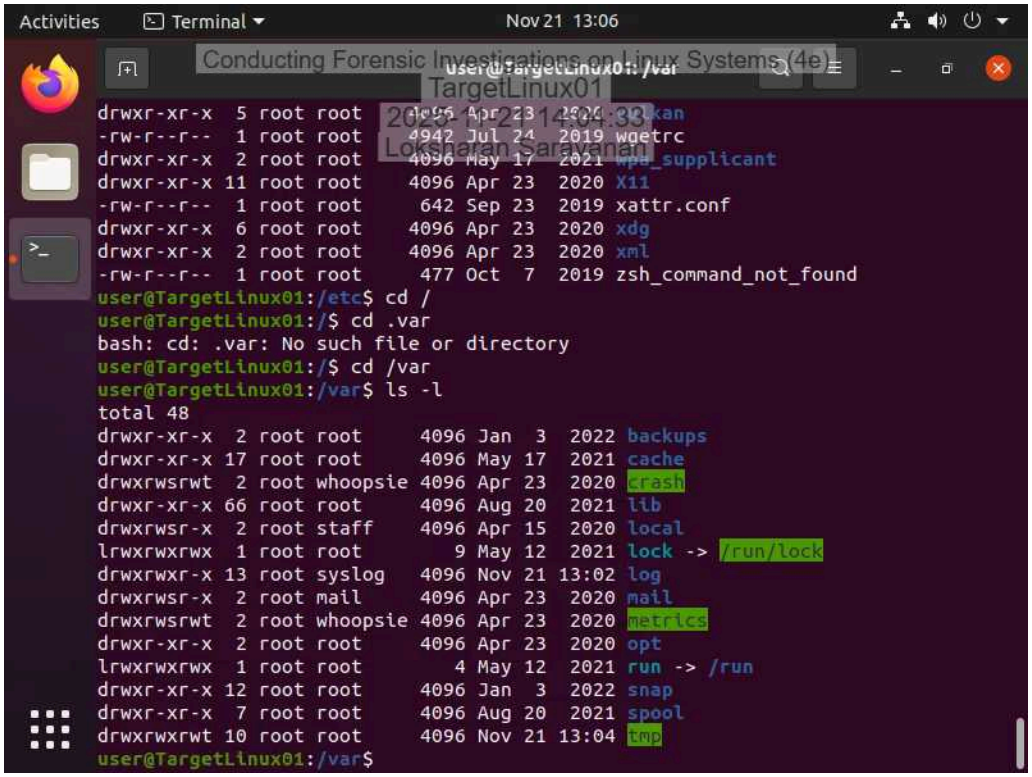
17. **Make a screen capture** showing the **contents of the /bin directory**.



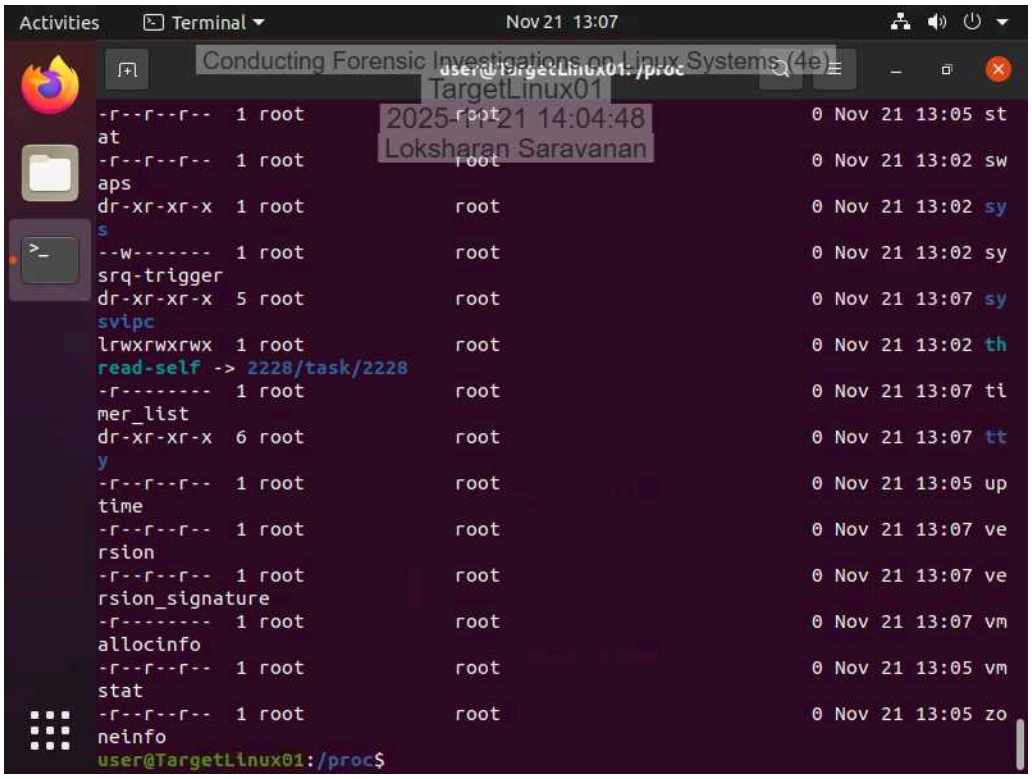
20. **Make a screen capture** showing the **contents of the /etc directory**.



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

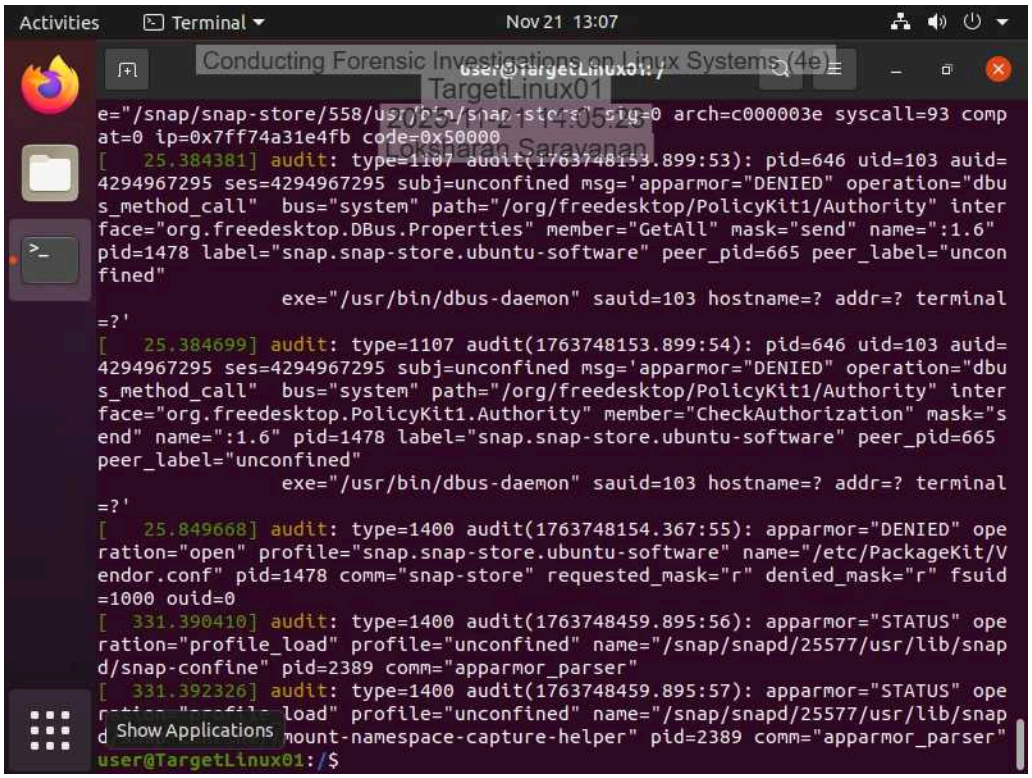


22. **Make a screen capture** showing the **contents of the /proc directory**.

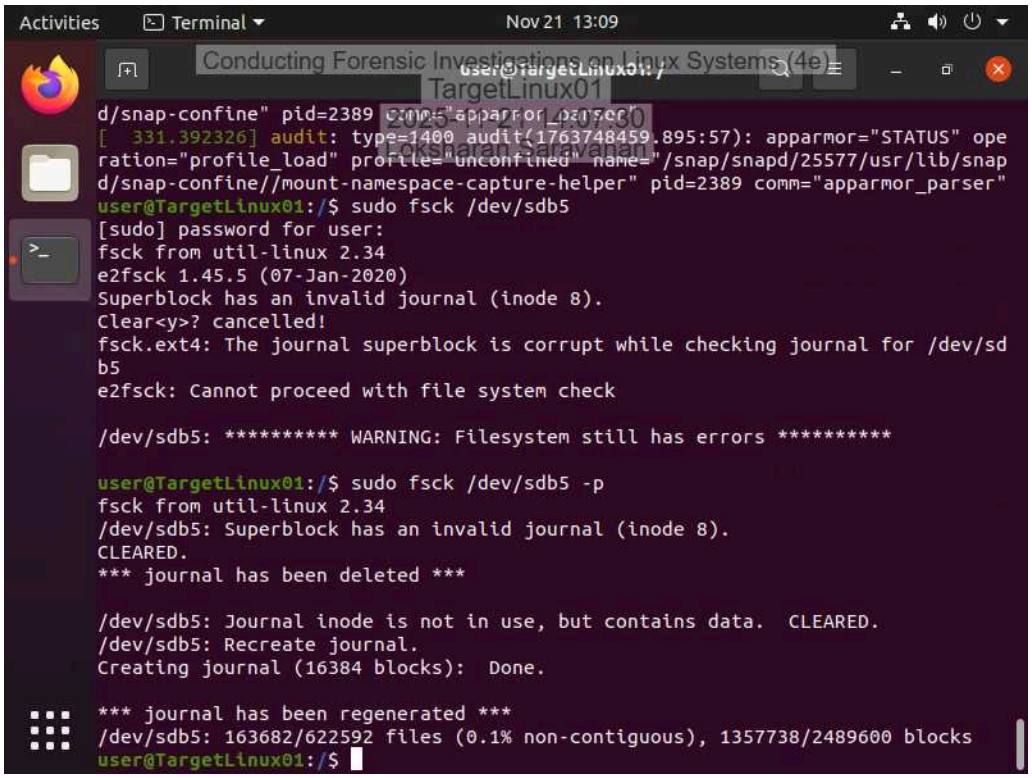


Part 2: Use Linux Shell Commands for Forensic Investigations

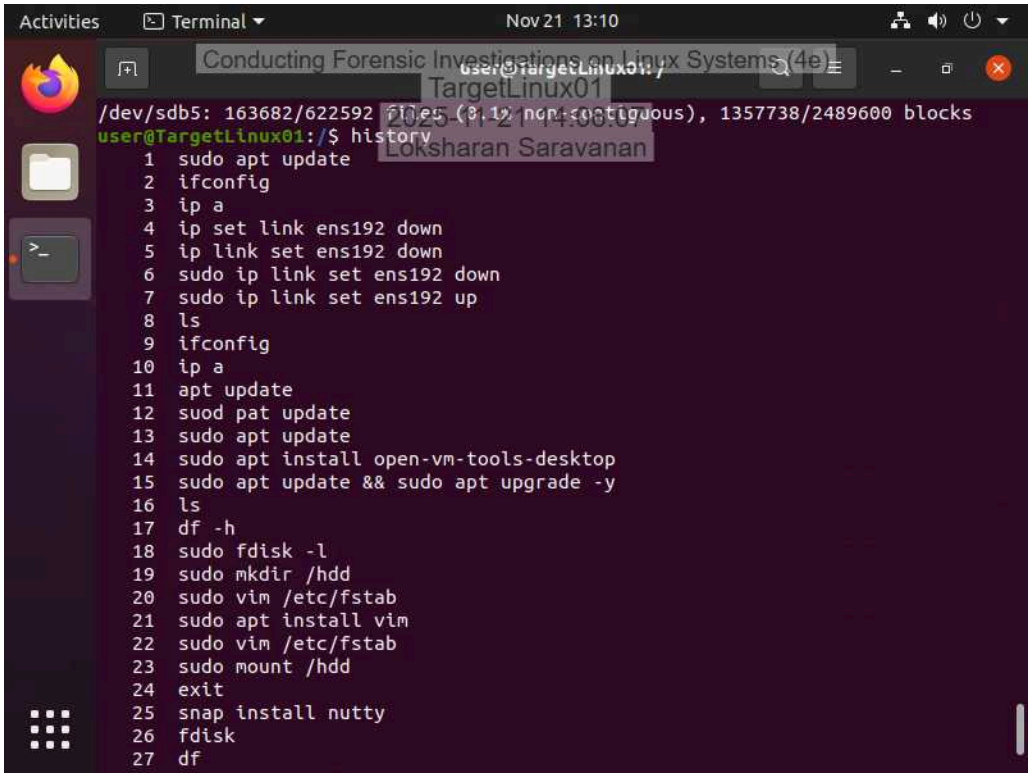
2. **Make a screen capture** showing the **results of the dmesg command**.



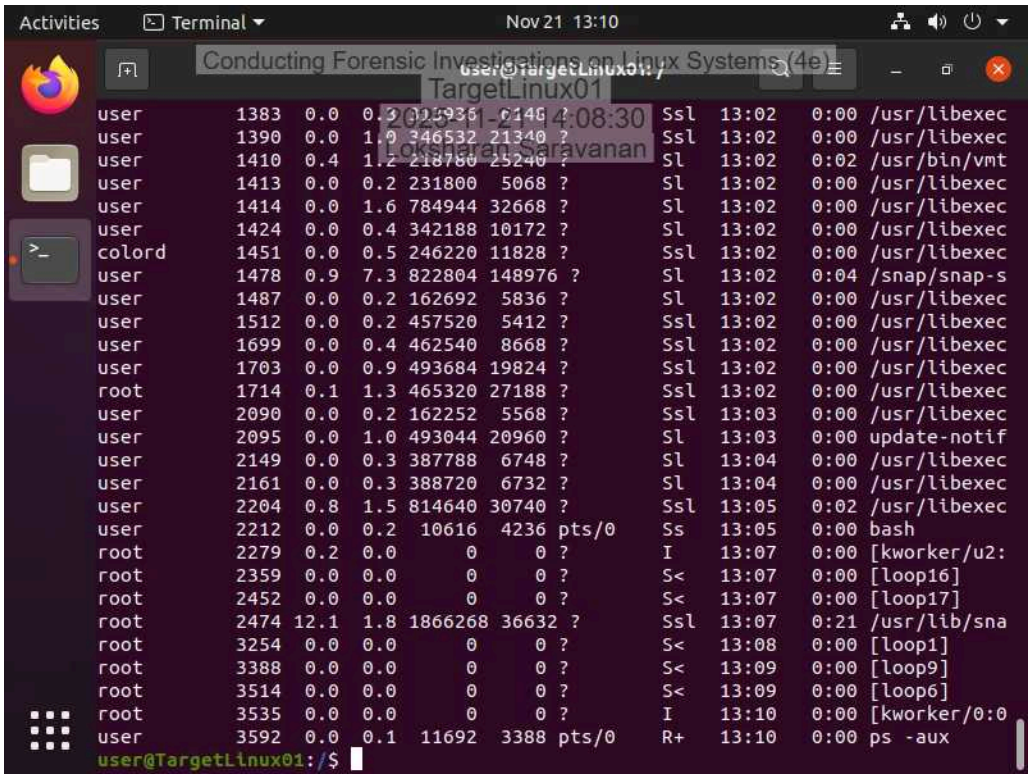
7. **Make a screen capture** showing the **results of the fsck command.**



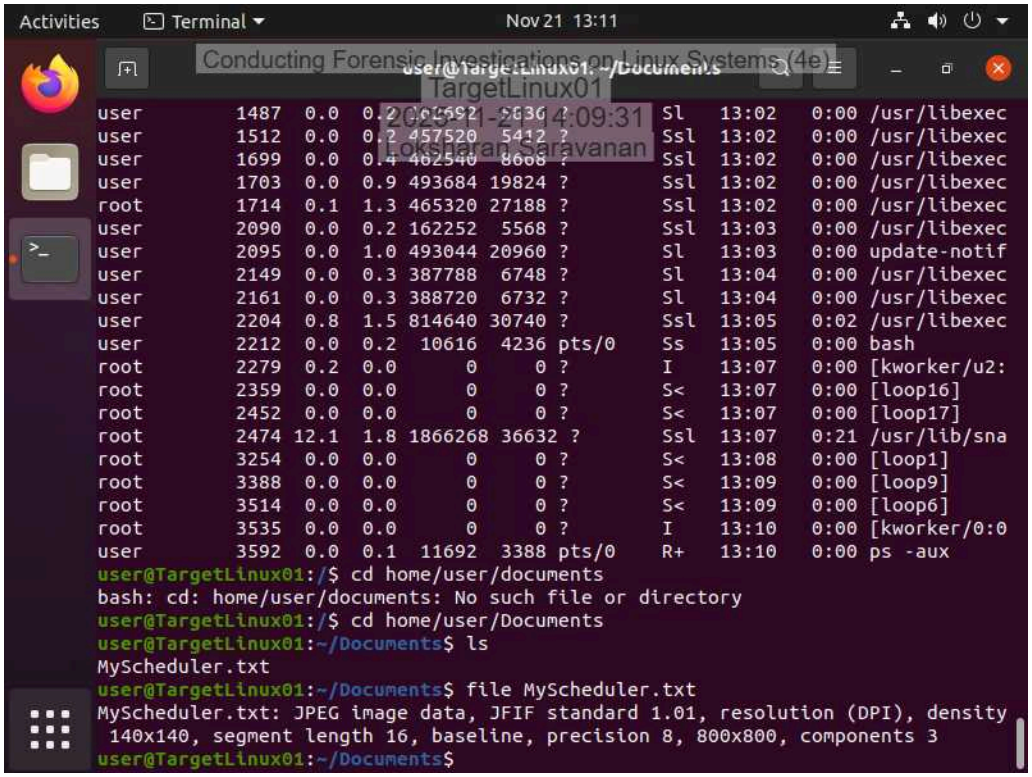
9. **Make a screen capture** showing the **results of the history command**.



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

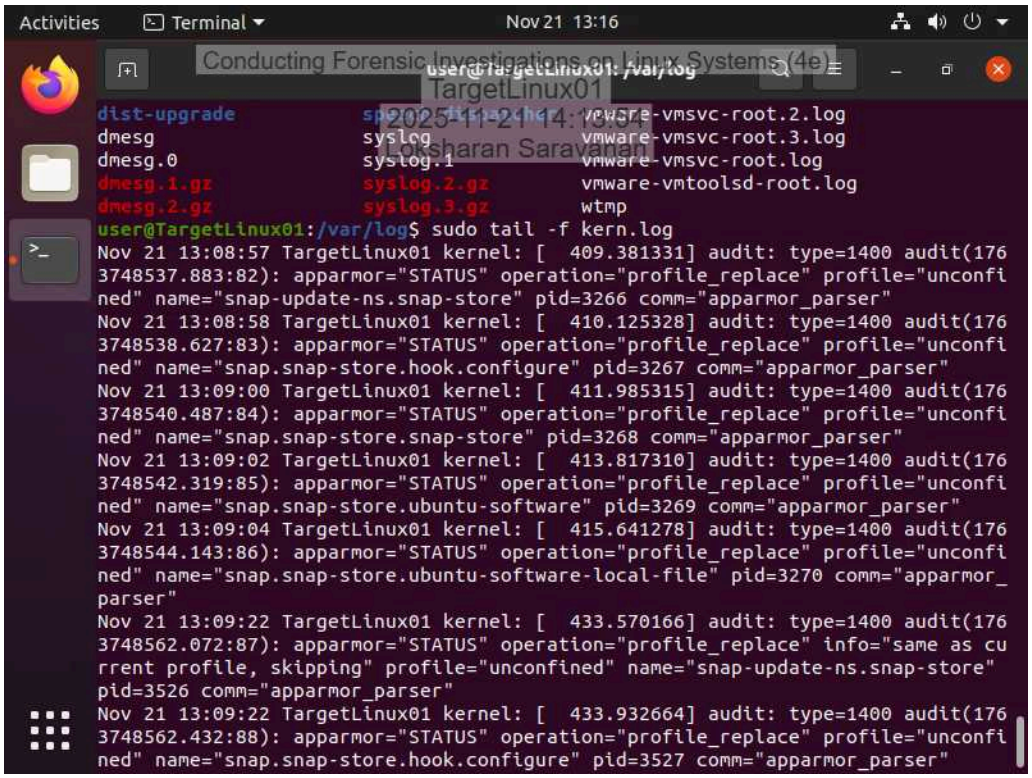


15. **Make a screen capture** showing the **results of the file command**.

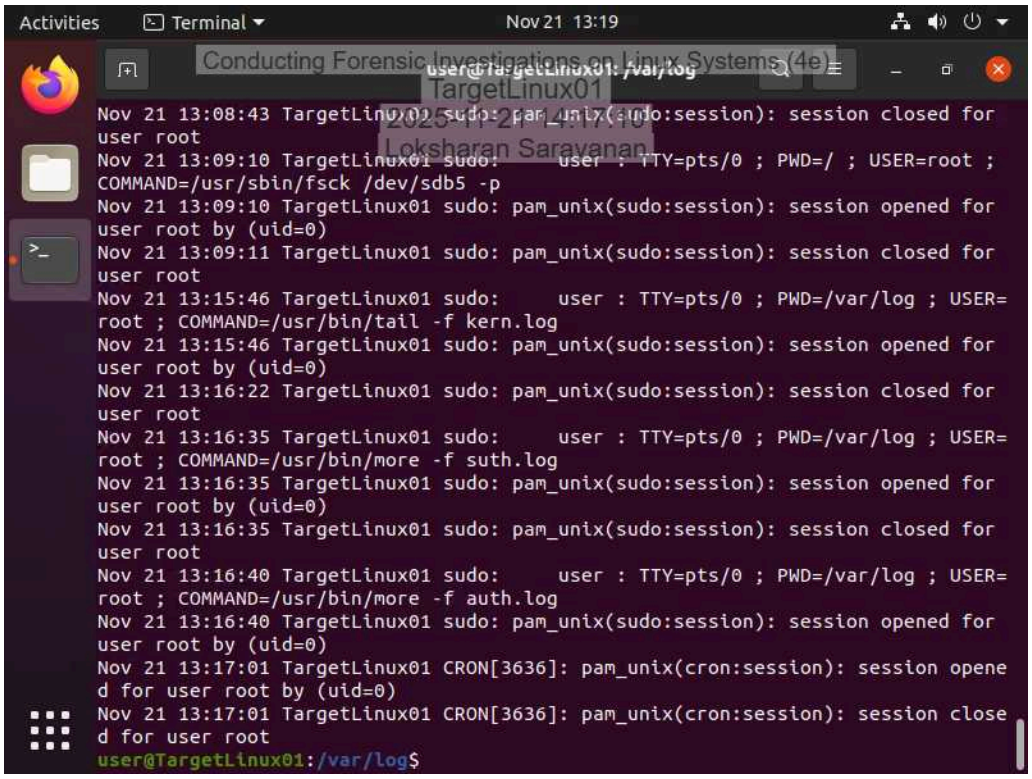


Part 3: Retrieve Logs Files on a Live Linux System

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.

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:htopcurlvimpython3-piplogkeys (suspicious)netcat (potentially suspicious depending on context)Suspicious Items Identified:logkeysCategory: KeyloggerReason 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

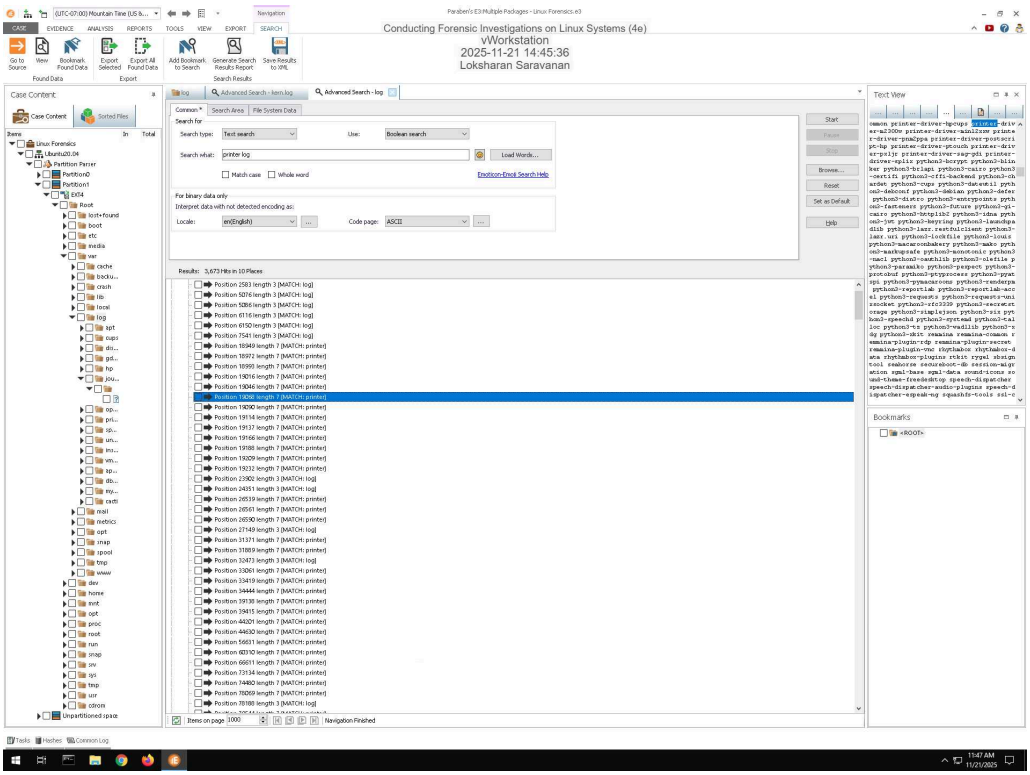
4. **Document** when the USB storage device was connected and its serial number.

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, 2024Time: 13:17:44Log entry example:
Jun 10 13:17:44 ubuntu kernel: [1234.567890] usb 2-1: USB Mass Storage device detectedDevice Serial Number: SN1234ABC567
from the accompanying kern.log entry such as: “Product: USB Flash Drive, Serial Number: SN1234ABC567”

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**.