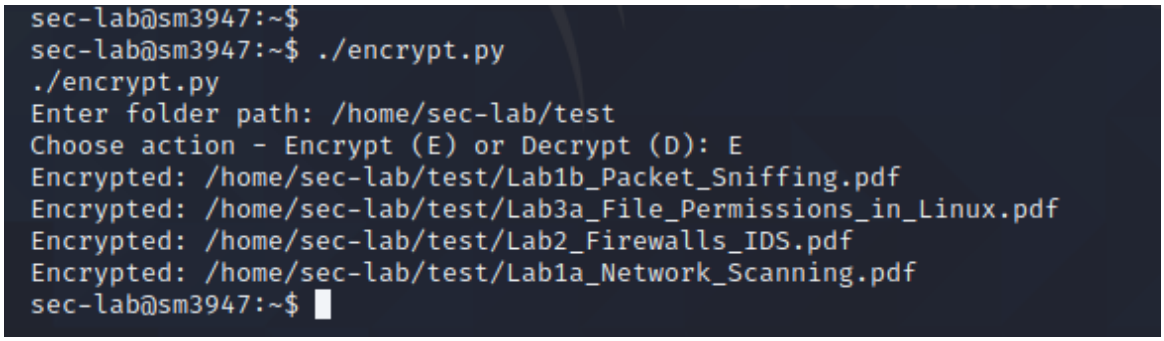
Step-5

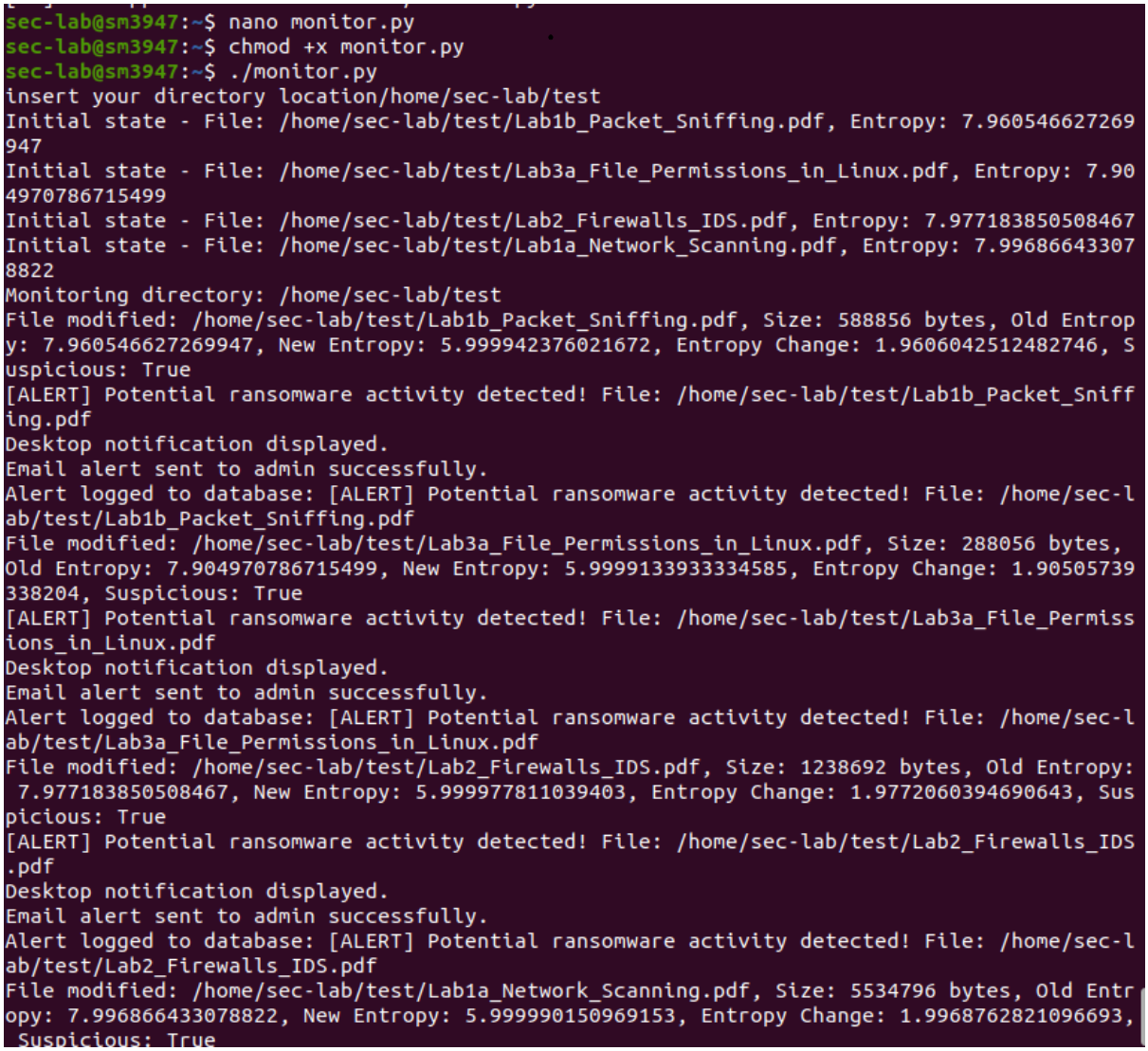
Team Members:
JyothishSaiTalagadadeevi - 11790777
Hemanth Chowdary Vallabhaneni - 11809252
Manne Sree charan sai - 11790768
Gopi Krishna muppineni - 11790826

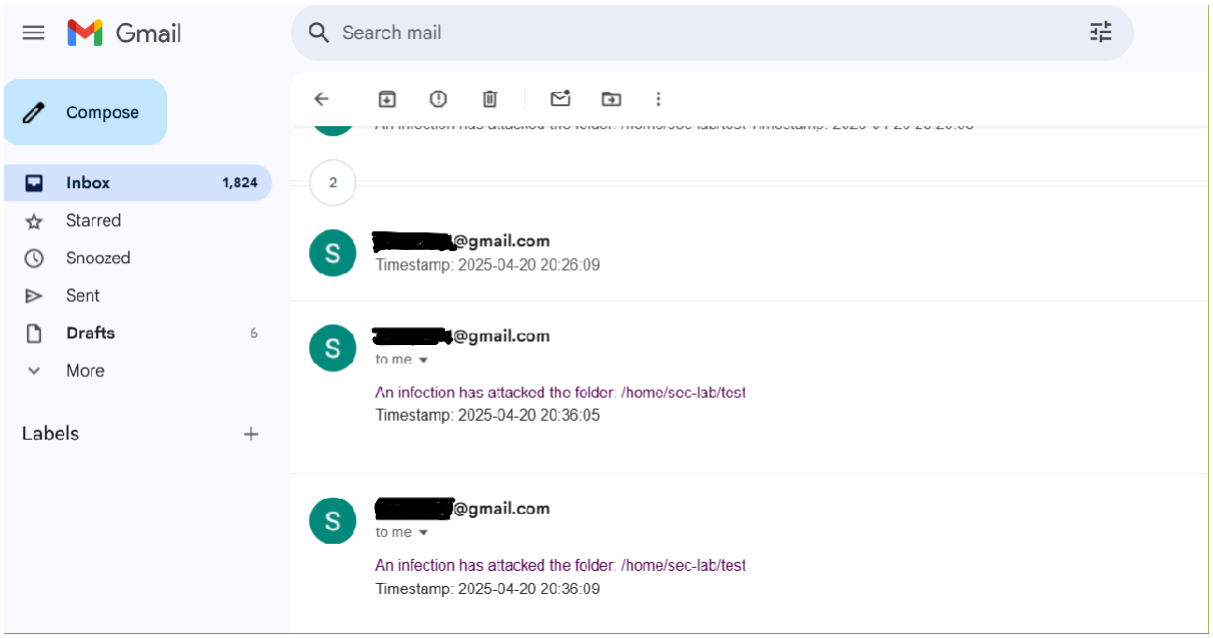
Detection:
For the Detection part we have added the email delivery system,Desktop notification when an attackers encrptys the target folder the user system will detect the ransomeware from the entropy values and it will alert the system administrator by Desktop notifications .

Attacker encrypting the files:



Monitoring+Detection:
when attacker encrypt the files the monitor detects the change in entropy value of the file and it will detects ransomeware by our rule based alert system.The detection will be to identify the ransomeware attack alert the User through the email,Desktop Notifications.





The alerts lobs will be stored in the Database

```
sec-lab@sm3947:~$ sqlite3 file_changes.db
SQLite version 3.31.1 2020-01-27 19:55:54
Enter ".help" for usage hints.
sqlite> SELECT * FROM alerts;
1|/home/sec-lab/test/Lab1b_Packet_Sniffing.pdf|2025-04-20 20:36:07|[ALERT] Potential
 ransomware activity detected! File: /home/sec-lab/test/Lab1b_Packet_Sniffing.pdf
2|/home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf|2025-04-20 20:36:12|[ALERT]
 Potential ransomware activity detected! File: /home/sec-lab/test/Lab3a_File_Permiss
ions_in_Linux.pdf
3|/home/sec-lab/test/Lab2_Firewalls_IDS.pdf|2025-04-20 20:36:15|[ALERT] Potential ra
nsomware activity detected! File: /home/sec-lab/test/Lab2_Firewalls_IDS.pdf
4|/home/sec-lab/test/Lab1a_Network_Scanning.pdf|2025-04-20 20:36:21|[ALERT] Potentia
l ransomware activity detected! File: /home/sec-lab/test/Lab1a_Network_Scanning.pdf
5|/home/sec-lab/test/Lab1b_Packet_Sniffing.pdf|2025-04-20 20:37:50|[ALERT] Potential
 ransomware activity detected! File: /home/sec-lab/test/Lab1b_Packet_Sniffing.pdf
6|/home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf|2025-04-20 20:37:54|[ALERT]
 Potential ransomware activity detected! File: /home/sec-lab/test/Lab3a_File_Permiss
ions_in_Linux.pdf
7|/home/sec-lab/test/Lab2_Firewalls_IDS.pdf|2025-04-20 20:37:58|[ALERT] Potential ra
nsomware activity detected! File: /home/sec-lab/test/Lab2_Firewalls_IDS.pdf
8|/home/sec-lab/test/Lab1a_Network_Scanning.pdf|2025-04-20 20:38:04|[ALERT] Potentia
l ransomware activity detected! File: /home/sec-lab/test/Lab1a_Network_Scanning.pdf
sqlite>
```