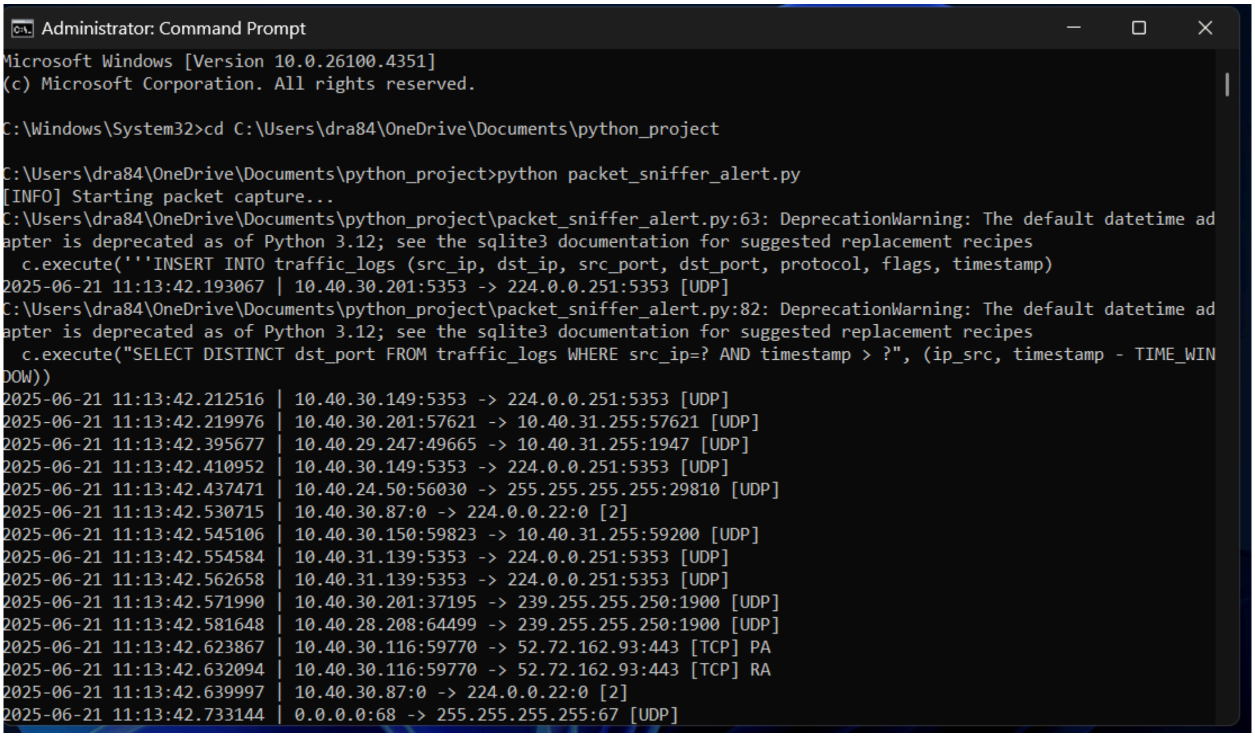
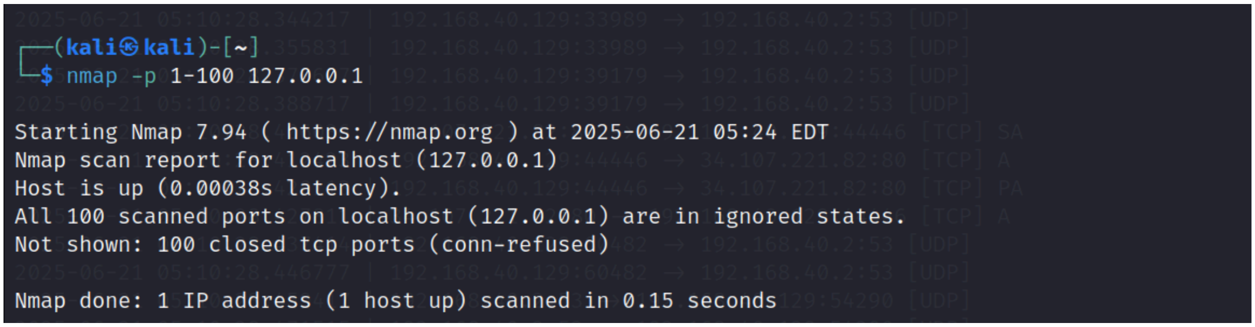
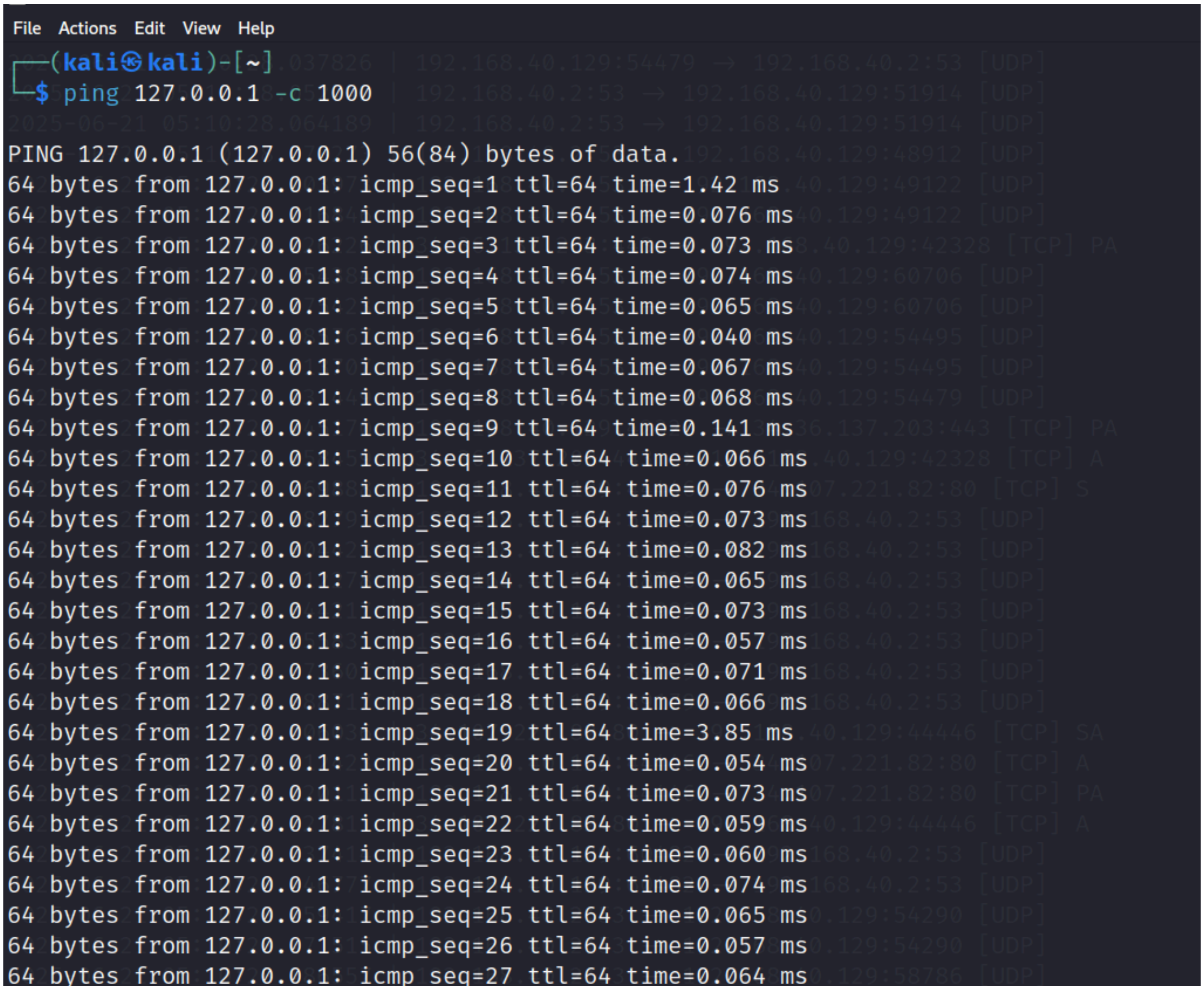
Terminal Output



```
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\Users\dra84\OneDrive\Documents\python_project

C:\Users\dra84\OneDrive\Documents\python_project>python packet_sniffer_alert.py
[INFO] Starting packet capture...
C:\Users\dra84\OneDrive\Documents\python_project\packet_sniffer_alert.py:63: DeprecationWarning: The default datetime ad
apter is deprecated as of Python 3.12; see the sqlite3 documentation for suggested replacement recipes
  c.execute('''INSERT INTO traffic_logs (src_ip, dst_ip, src_port, dst_port, protocol, flags, timestamp)
2025-06-21 11:13:42.193067 | 10.40.30.201:5353 -> 224.0.0.251:5353 [UDP]
C:\Users\dra84\OneDrive\Documents\python_project\packet_sniffer_alert.py:82: DeprecationWarning: The default datetime ad
apter is deprecated as of Python 3.12; see the sqlite3 documentation for suggested replacement recipes
  c.execute("SELECT DISTINCT dst_port FROM traffic_logs WHERE src_ip=? AND timestamp > ?", (ip_src, timestamp - TIME_WIN
DOW))
2025-06-21 11:13:42.212516 | 10.40.30.149:5353 -> 224.0.0.251:5353 [UDP]
2025-06-21 11:13:42.219976 | 10.40.30.201:57621 -> 10.40.31.255:57621 [UDP]
2025-06-21 11:13:42.395677 | 10.40.29.247:49665 -> 10.40.31.255:1947 [UDP]
2025-06-21 11:13:42.410952 | 10.40.30.149:5353 -> 224.0.0.251:5353 [UDP]
2025-06-21 11:13:42.437471 | 10.40.24.50:56030 -> 255.255.255.255:29810 [UDP]
2025-06-21 11:13:42.530715 | 10.40.30.87:0 -> 224.0.0.22:0 [2]
2025-06-21 11:13:42.545106 | 10.40.30.150:59823 -> 10.40.31.255:59200 [UDP]
2025-06-21 11:13:42.554584 | 10.40.31.139:5353 -> 224.0.0.251:5353 [UDP]
2025-06-21 11:13:42.562658 | 10.40.31.139:5353 -> 224.0.0.251:5353 [UDP]
2025-06-21 11:13:42.571990 | 10.40.30.201:37195 -> 239.255.255.250:1900 [UDP]
2025-06-21 11:13:42.581648 | 10.40.28.208:64499 -> 239.255.255.250:1900 [UDP]
2025-06-21 11:13:42.623867 | 10.40.30.116:59770 -> 52.72.162.93:443 [TCP] PA
2025-06-21 11:13:42.632094 | 10.40.30.116:59770 -> 52.72.162.93:443 [TCP] RA
2025-06-21 11:13:42.639997 | 10.40.30.87:0 -> 224.0.0.22:0 [2]
2025-06-21 11:13:42.733144 | 0.0.0.0:68 -> 255.255.255.255:67 [UDP]
```

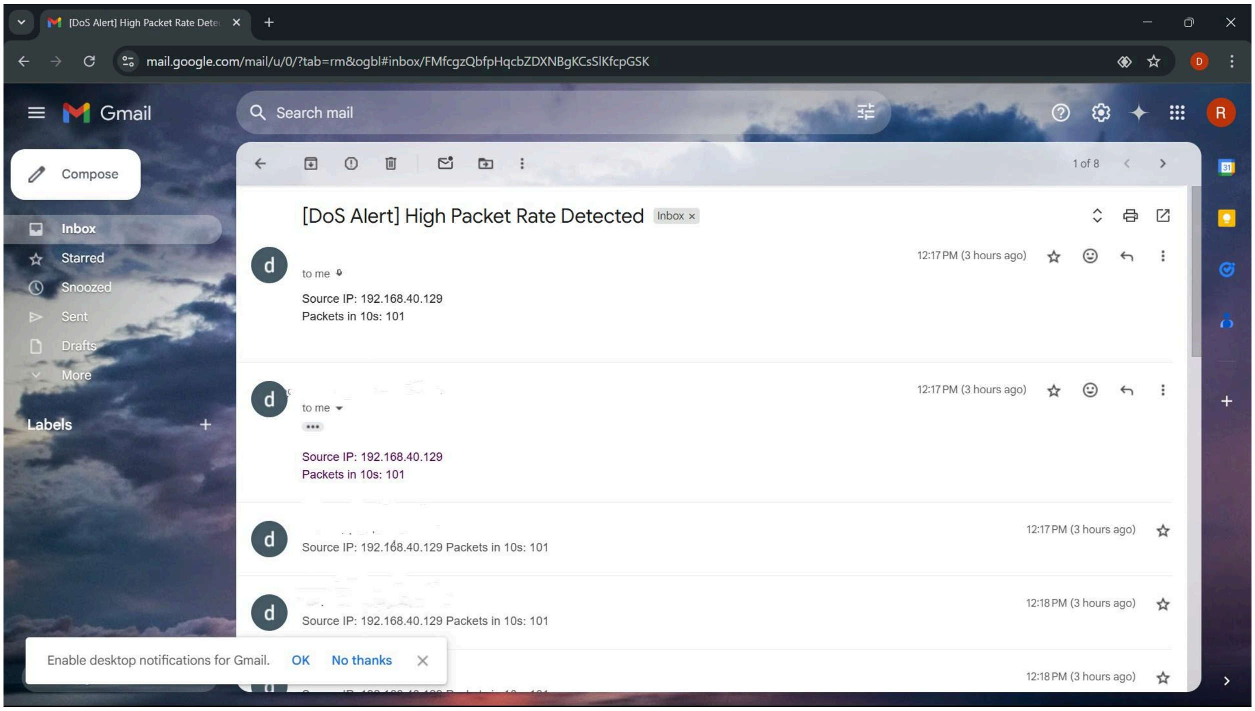


```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1-100 127.0.0.1

Starting Nmap 7.94 ( https://nmap.org ) at 2025-06-21 05:24 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00038s latency).
All 100 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ ping 127.0.0.1 -c 1000

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=1.42 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.076 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.073 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.074 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.065 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.067 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.068 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.141 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.066 ms
64 bytes from 127.0.0.1: icmp_seq=11 ttl=64 time=0.076 ms
64 bytes from 127.0.0.1: icmp_seq=12 ttl=64 time=0.073 ms
64 bytes from 127.0.0.1: icmp_seq=13 ttl=64 time=0.082 ms
64 bytes from 127.0.0.1: icmp_seq=14 ttl=64 time=0.065 ms
64 bytes from 127.0.0.1: icmp_seq=15 ttl=64 time=0.073 ms
64 bytes from 127.0.0.1: icmp_seq=16 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=17 ttl=64 time=0.071 ms
64 bytes from 127.0.0.1: icmp_seq=18 ttl=64 time=0.066 ms
64 bytes from 127.0.0.1: icmp_seq=19 ttl=64 time=3.85 ms
64 bytes from 127.0.0.1: icmp_seq=20 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=21 ttl=64 time=0.073 ms
64 bytes from 127.0.0.1: icmp_seq=22 ttl=64 time=0.059 ms
64 bytes from 127.0.0.1: icmp_seq=23 ttl=64 time=0.060 ms
64 bytes from 127.0.0.1: icmp_seq=24 ttl=64 time=0.074 ms
64 bytes from 127.0.0.1: icmp_seq=25 ttl=64 time=0.065 ms
64 bytes from 127.0.0.1: icmp_seq=26 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=27 ttl=64 time=0.064 ms
```

Email sent:


[DoS Alert] High Packet Rate Dete
mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FMfcgzQbfpHqcbZDXNBgKCsSlKfcpGSK
Gmail
Search mail
Compose
Inbox
Starred
Snoozed
Sent
Drafts
More
Labels
1 of 8
Inbox ×
Enable desktop notifications for Gmail.
OK
No thanks

[DoS Alert] High Packet Rate Detected

d

to me

12:17 PM (3 hours ago)

Source IP: 192.168.40.129
Packets in 10s: 101

d

to me

12:17 PM (3 hours ago)

Source IP: 192.168.40.129
Packets in 10s: 101

d

Source IP: 192.168.40.129 Packets in 10s: 101

12:17 PM (3 hours ago)

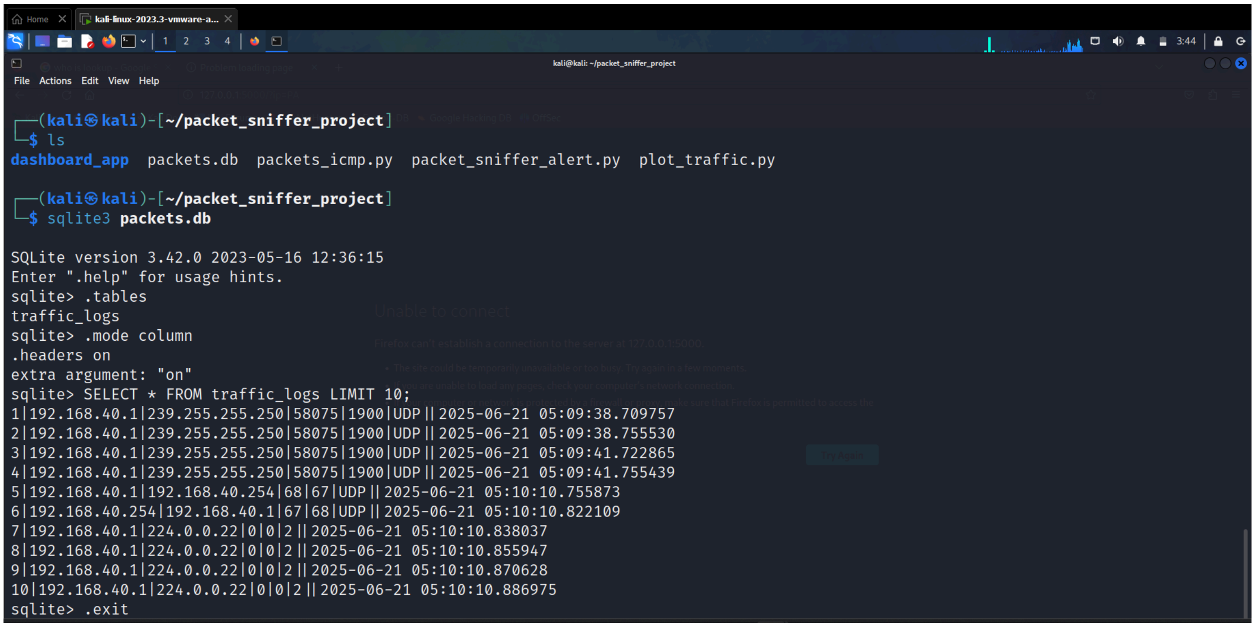
d

Source IP: 192.168.40.129 Packets in 10s: 101

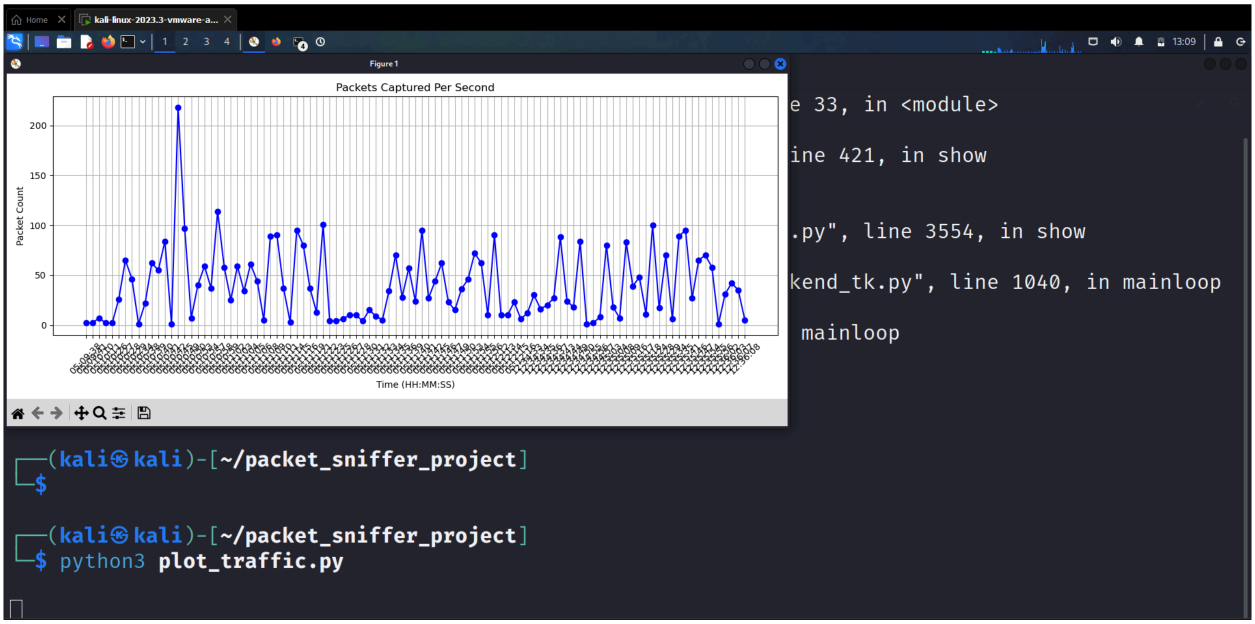
12:18 PM (3 hours ago)

12:18 PM (3 hours ago)

DATABASE

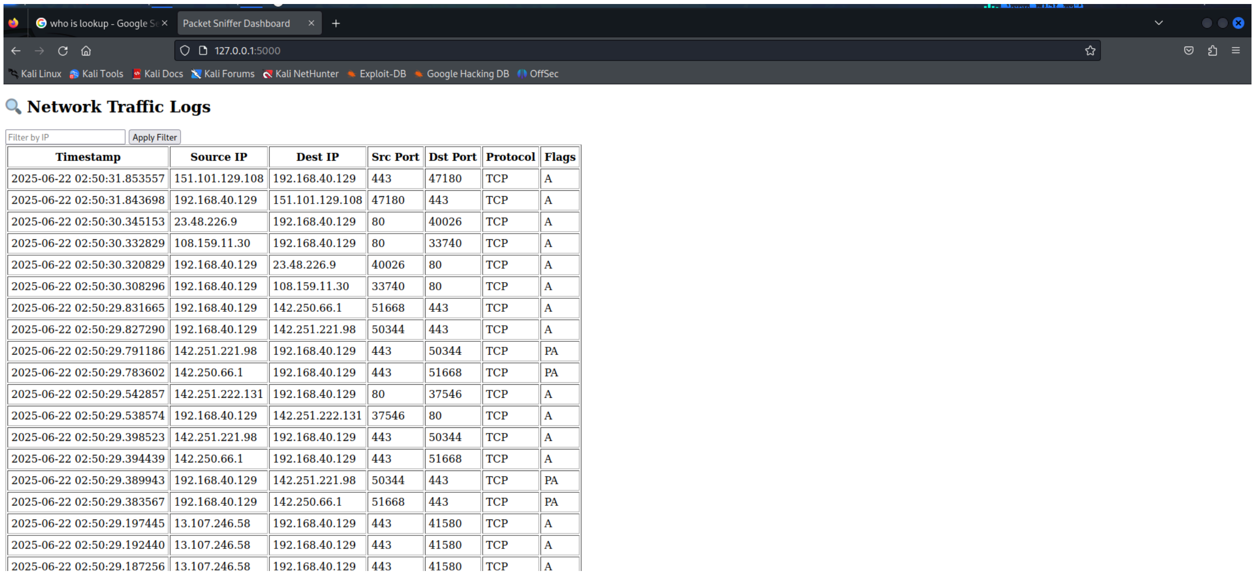

Home
kali-linux-2023.3-vmware-a...
3:44
kali@kali: ~/packet_sniffer_project
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/packet_sniffer_project]
└─$ ls
dashboard_app  packets.db  packets_icmp.py  packet_sniffer_alert.py  plot_traffic.py

┌──(kali㉿kali)-[~/packet_sniffer_project]
└─$ sqlite3 packets.db

SQLite version 3.42.0 2023-05-16 12:36:15
Enter ".help" for usage hints.
sqlite> .tables
traffic_logs
sqlite> .mode column
.headers on
extra argument: "on"
sqlite> SELECT * FROM traffic_logs LIMIT 10;
1|192.168.40.1|239.255.255.250|58075|1900|UDP||2025-06-21 05:09:38.709757
2|192.168.40.1|239.255.255.250|58075|1900|UDP||2025-06-21 05:09:38.755530
3|192.168.40.1|239.255.255.250|58075|1900|UDP||2025-06-21 05:09:41.722865
4|192.168.40.1|239.255.255.250|58075|1900|UDP||2025-06-21 05:09:41.755439
5|192.168.40.1|192.168.40.254|68|67|UDP||2025-06-21 05:10:10.755873
6|192.168.40.254|192.168.40.1|67|68|UDP||2025-06-21 05:10:10.822109
7|192.168.40.1|224.0.0.22|0|0|2||2025-06-21 05:10:10.838037
8|192.168.40.1|224.0.0.22|0|0|2||2025-06-21 05:10:10.855947
9|192.168.40.1|224.0.0.22|0|0|2||2025-06-21 05:10:10.870628
10|192.168.40.1|224.0.0.22|0|0|2||2025-06-21 05:10:10.886975
sqlite> .exit
```



```
e 33, in <module>

ine 421, in show

.py", line 3554, in show

kend_tk.py", line 1040, in mainloop

 mainloop

┌──(kali㉿kali)-[~/packet_sniffer_project]
└─$ 

┌──(kali㉿kali)-[~/packet_sniffer_project]
└─$ python3 plot_traffic.py
```

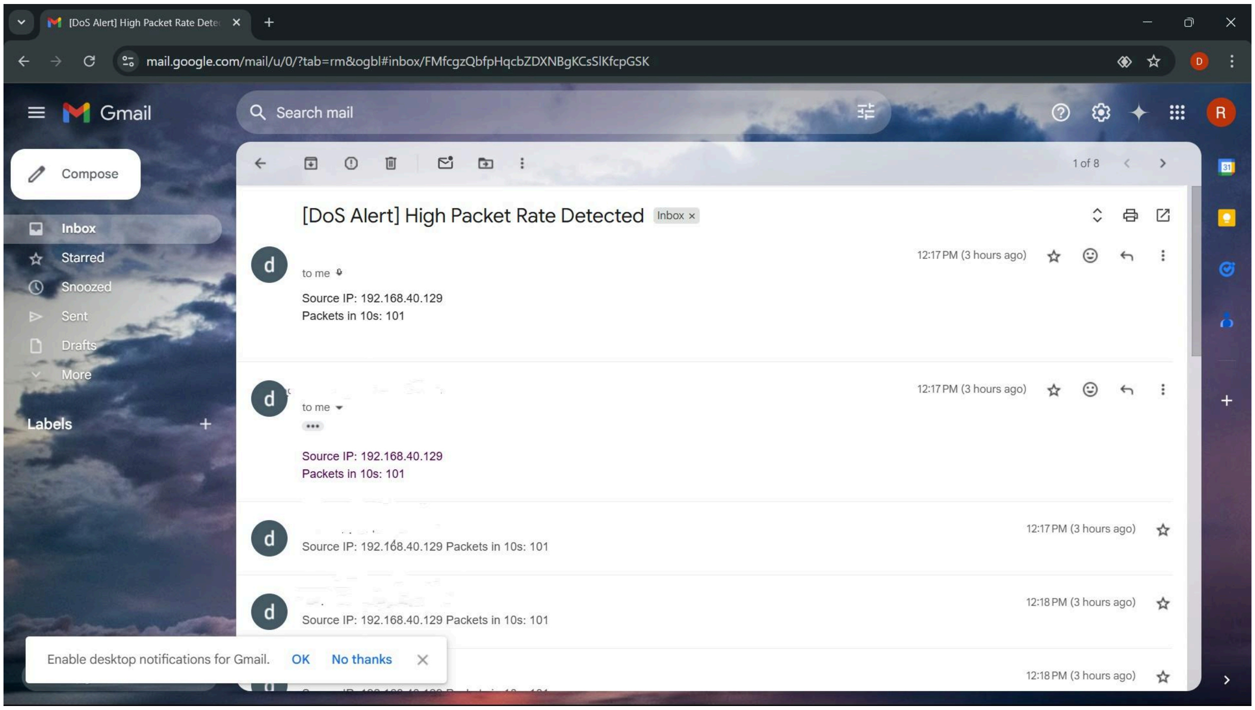
Final dashboard



🔍 Network Traffic Logs

Filter by IP [Apply Filter]

Timestamp	Source IP	Dest IP	Src Port	Dst Port	Protocol	Flags
2025-06-22 02:50:31.853557	151.101.129.108	192.168.40.129	443	47180	TCP	A
2025-06-22 02:50:31.843698	192.168.40.129	151.101.129.108	47180	443	TCP	A
2025-06-22 02:50:30.345153	23.48.226.9	192.168.40.129	80	40026	TCP	A
2025-06-22 02:50:30.332829	108.159.11.30	192.168.40.129	80	33740	TCP	A
2025-06-22 02:50:30.320829	192.168.40.129	23.48.226.9	40026	80	TCP	A
2025-06-22 02:50:30.308296	192.168.40.129	108.159.11.30	33740	80	TCP	A
2025-06-22 02:50:29.831665	192.168.40.129	142.250.66.1	51668	443	TCP	A
2025-06-22 02:50:29.827290	192.168.40.129	142.251.221.98	50344	443	TCP	A
2025-06-22 02:50:29.791186	142.251.221.98	192.168.40.129	443	50344	TCP	PA
2025-06-22 02:50:29.783602	142.250.66.1	192.168.40.129	443	51668	TCP	PA
2025-06-22 02:50:29.542857	142.251.222.131	192.168.40.129	80	37546	TCP	A
2025-06-22 02:50:29.538574	192.168.40.129	142.251.222.131	37546	80	TCP	A
2025-06-22 02:50:29.398523	142.251.221.98	192.168.40.129	443	50344	TCP	A
2025-06-22 02:50:29.394439	142.250.66.1	192.168.40.129	443	51668	TCP	A
2025-06-22 02:50:29.389943	192.168.40.129	142.251.221.98	50344	443	TCP	PA
2025-06-22 02:50:29.383567	192.168.40.129	142.250.66.1	51668	443	TCP	PA
2025-06-22 02:50:29.197445	13.107.246.58	192.168.40.129	443	41580	TCP	A
2025-06-22 02:50:29.192440	13.107.246.58	192.168.40.129	443	41580	TCP	A
2025-06-22 02:50:29.187256	13.107.246.58	192.168.40.129	443	41580	TCP	A



[DoS Alert] High Packet Rate Dete
mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FMfcgzQbfpHqcbZDXNBgKCsSlKfcpGSK
Gmail
Search mail
Compose
Inbox
Starred
Snoozed
Sent
Drafts
More
Labels
1 of 8
Inbox ×
Enable desktop notifications for Gmail.
OK
No thanks

[DoS Alert] High Packet Rate Detected

12:17 PM (3 hours ago)

to me

Source IP: 192.168.40.129
Packets in 10s: 101

12:17 PM (3 hours ago)

to me

Source IP: 192.168.40.129
Packets in 10s: 101

12:17 PM (3 hours ago)

Source IP: 192.168.40.129 Packets in 10s: 101

12:18 PM (3 hours ago)

Source IP: 192.168.40.129 Packets in 10s: 101

12:18 PM (3 hours ago)