

# Network Traffic Analysis Report

## 1. Introduction

This report presents the results of a network traffic analysis performed using packet capture (PCAP) files and screenshots from Wireshark and browser sessions. The objective is to analyze different protocols including DNS, TCP, and ICMP, as well as HTTP(S) traffic related to Facebook login and google.com by using ping command in terminal.

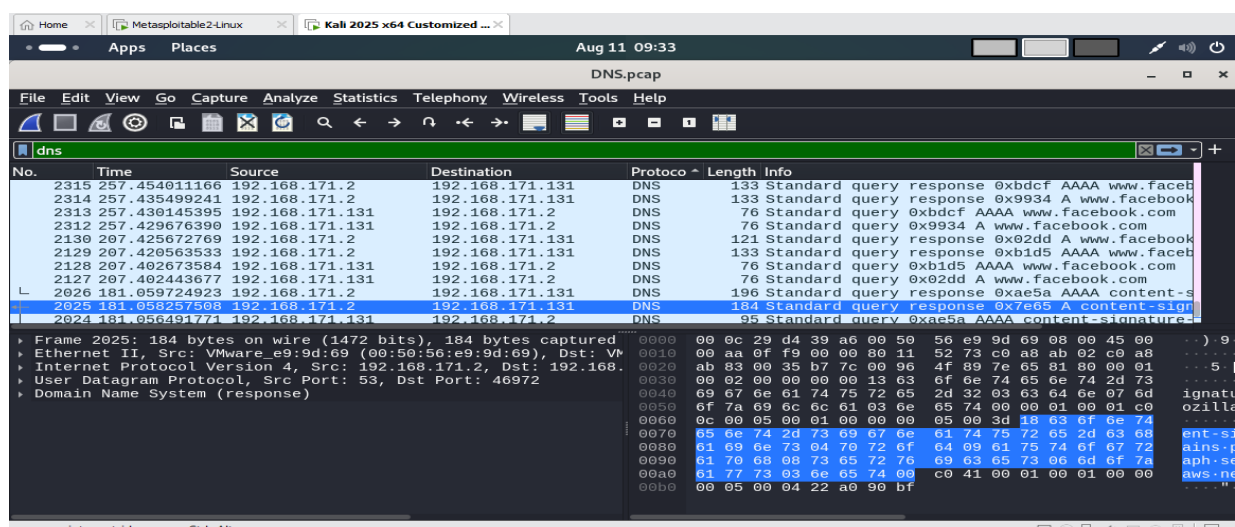
## 2. Methodology

The analysis was conducted using Wireshark to open and inspect the provided PCAP files. Screenshots were taken to highlight relevant findings for each protocol or network event. The following captures are included:

- DNS Query and Response
- Facebook login page visit
- TCP handshake and data exchange
- ICMP ping to google.com

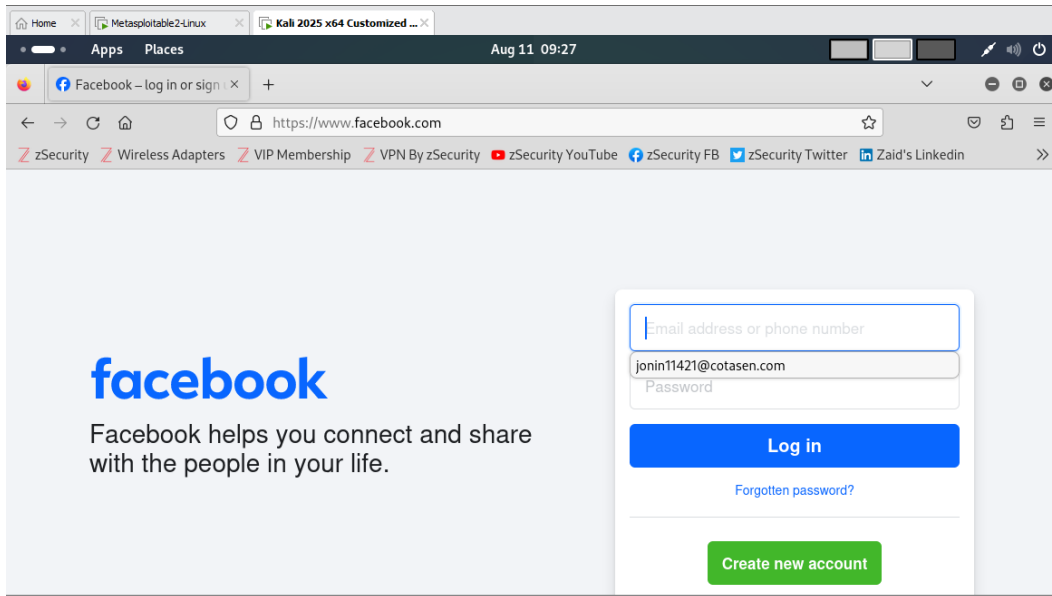
## 3. DNS Traffic Analysis

The DNS analysis shows standard query and response packets, including lookups for domains such as www.facebook.com. These indicate that the host resolved domain names to IP addresses before initiating TCP/HTTP(S) connections.



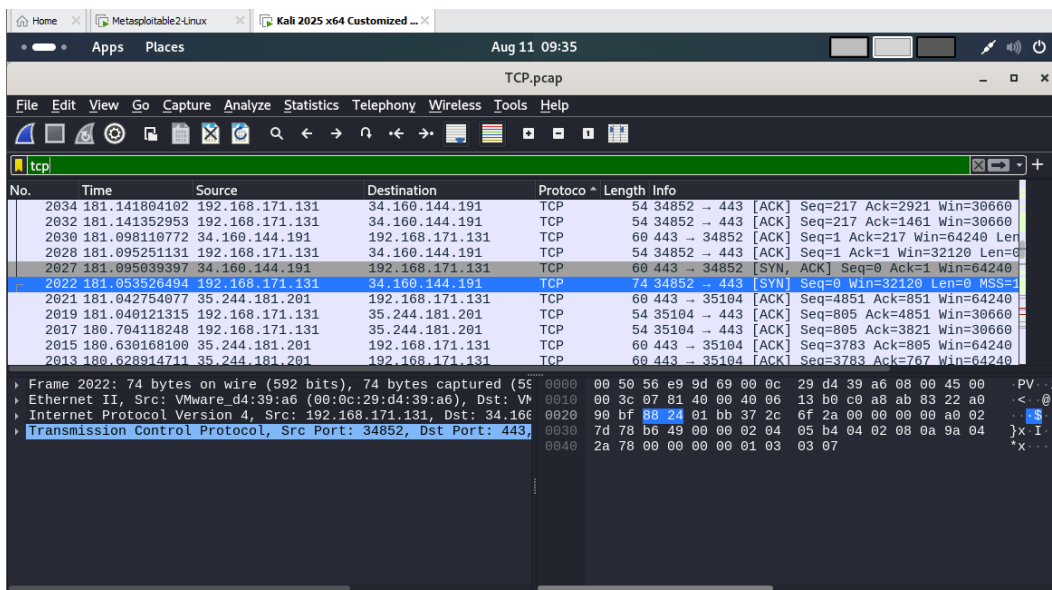
## 4. Facebook Login Observation

The browser screenshot shows a visit to the Facebook login page, where a specific email address was entered in the username field. This demonstrates captured application-level activity.



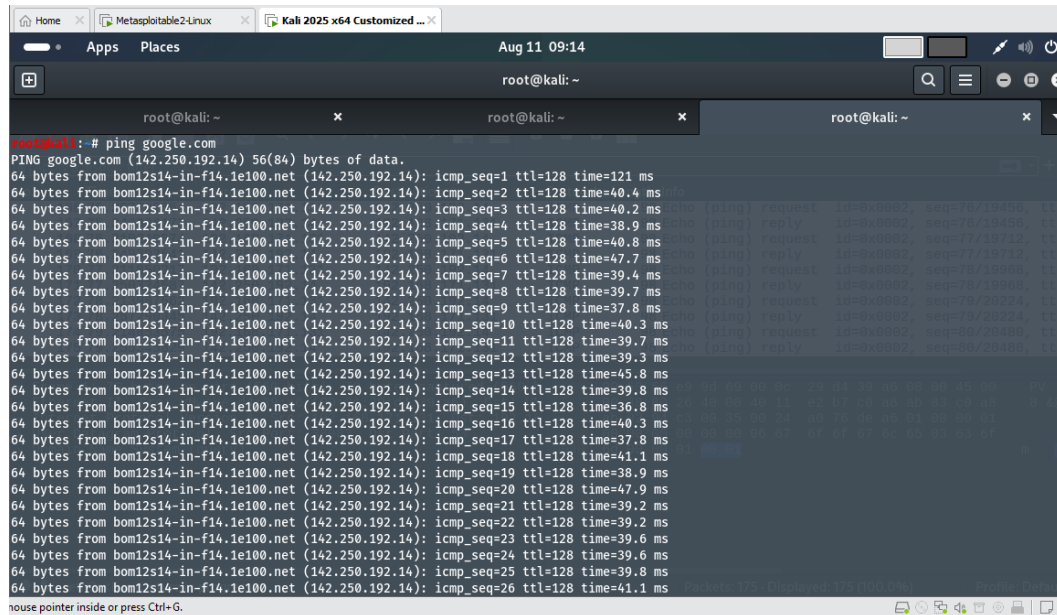
## 5. TCP Traffic Analysis

The TCP capture shows the three-way handshake process and subsequent data packets between the client and remote servers. The SYN, SYN-ACK, and ACK packets confirm successful connection establishment.



## 6. ICMP Ping Analysis

The ICMP capture confirms successful ping requests and replies between the local machine and google.com. This validates connectivity and round-trip response times.



```
root@kali: ~  
root@kali: ~  
root@kali: ~  
root@kali:~# ping google.com  
PING google.com (142.250.192.14) 56(84) bytes of data:  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=1 ttl=128 time=121 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=2 ttl=128 time=40.4 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=3 ttl=128 time=40.2 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=4 ttl=128 time=38.9 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=5 ttl=128 time=40.8 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=6 ttl=128 time=47.7 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=7 ttl=128 time=39.4 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=8 ttl=128 time=39.7 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=9 ttl=128 time=37.8 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=10 ttl=128 time=40.3 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=11 ttl=128 time=39.7 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=12 ttl=128 time=39.3 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=13 ttl=128 time=45.8 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=14 ttl=128 time=39.8 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=15 ttl=128 time=36.8 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=16 ttl=128 time=40.3 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=17 ttl=128 time=37.8 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=18 ttl=128 time=41.1 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=19 ttl=128 time=38.9 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=20 ttl=128 time=47.9 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=21 ttl=128 time=39.2 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=22 ttl=128 time=39.2 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=23 ttl=128 time=39.6 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=24 ttl=128 time=39.6 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=25 ttl=128 time=39.8 ms  
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=26 ttl=128 time=41.1 ms
```

## 7. Conclusion

The analysis demonstrates successful network activity across multiple protocols. DNS queries resolved hostnames, TCP sessions were established for communication, and ICMP verified connectivity. The Facebook login capture confirms higher-layer application activity.