Wireshark Network Traffic Analysis – Mini Report

# Objective

To capture and analyze real-time network traffic using Wireshark on Linux. Focused on identifying and understanding the behavior of core internet protocols like DNS, TCP, and HTTPS by observing traffic from visits to ChatGPT and Instagram.

# Tools & Environment

- Operating System: Linux

- Tool Used: Wireshark

- Network Interface: eth0 (active interface detected via `ip a`)

- Websites Visited During Capture:  
 • https://chat.openai.com  
 • https://www.instagram.com

# Steps Performed

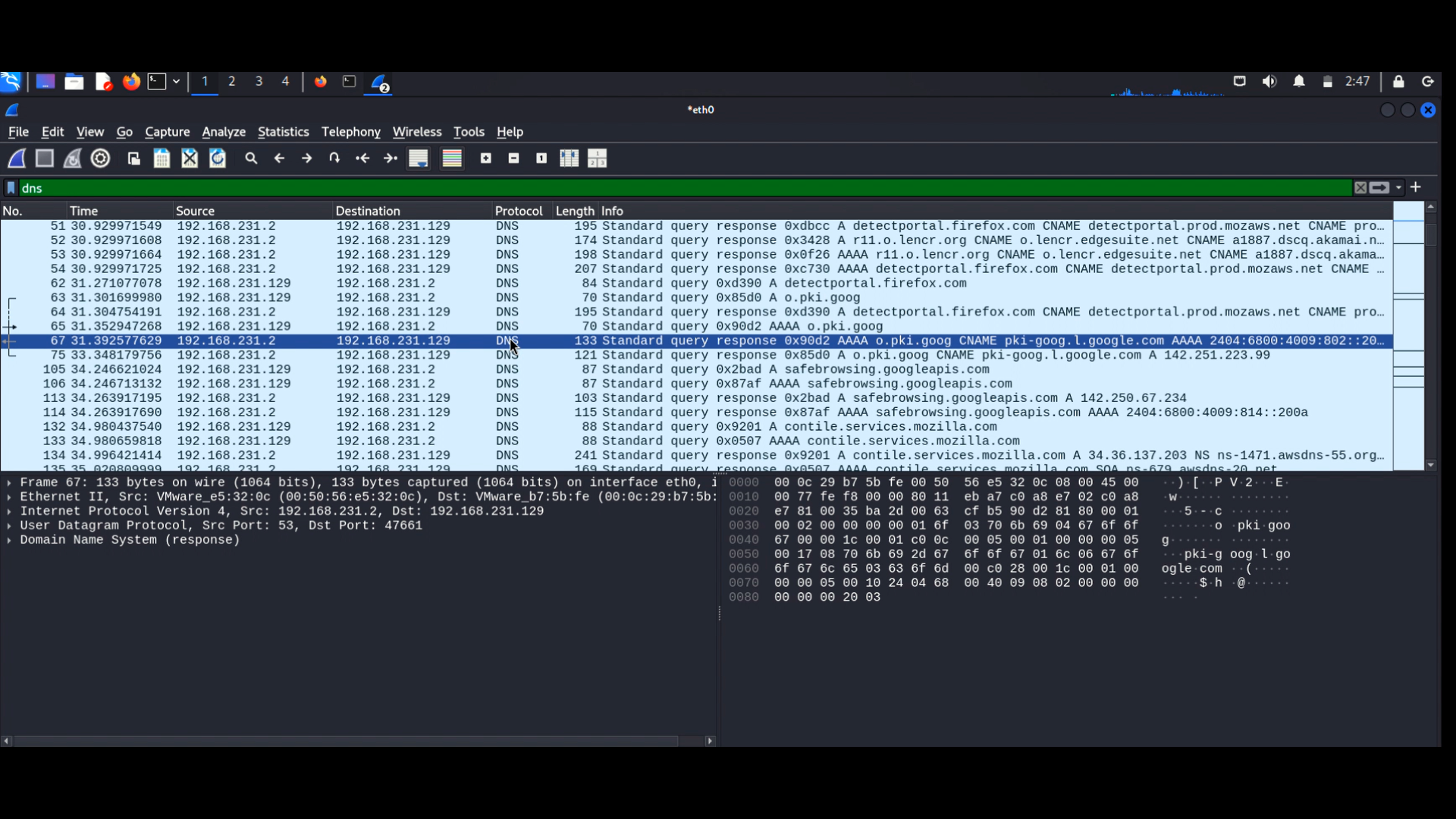
1. Installed Wireshark using the terminal:  
 sudo apt install wireshark -y  
 sudo usermod -aG wireshark $USER  
2. Opened Wireshark and selected interface eth0.  
3. Began packet capture, then opened ChatGPT and Instagram in the browser.  
4. Stopped capture after 5 minutes.  
5. Used filters (dns, tcp, tls) to focus on relevant traffic.  
6. Analyzed:  
 - DNS lookups and responses  
 - TCP handshake packets (SYN, SYN-ACK, ACK)  
 - TLS handshake metadata (e.g., Server Name Indication)

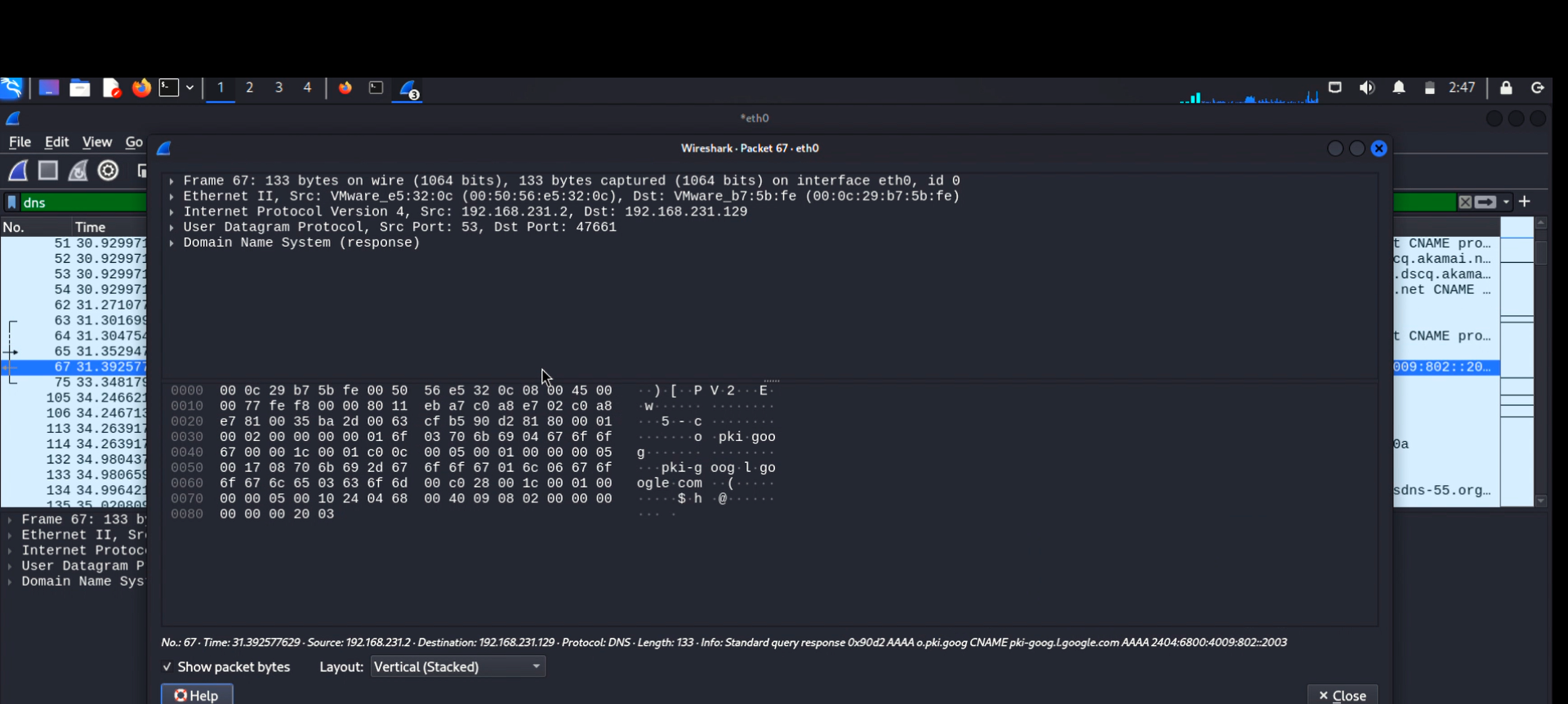
# Key Findings

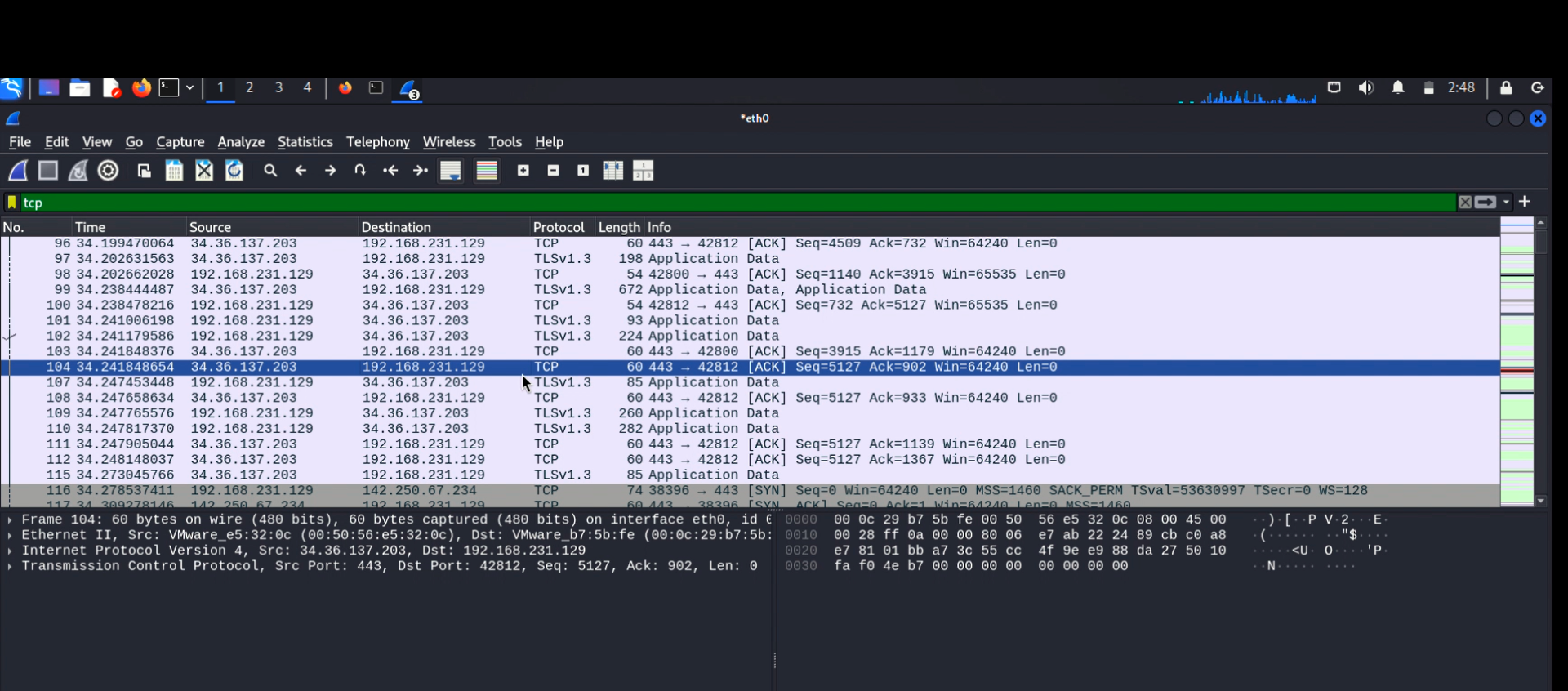
|  |  |
| --- | --- |
| Protocol | Observation |
| DNS | DNS requests were sent to resolve chat.openai.com and www.instagram.com. Responses returned IPs owned by OpenAI and Meta's CDN. |
| TCP | Multiple TCP handshakes observed between local IP and external servers. Verified successful connection setup using SYN → SYN-ACK → ACK sequence. |
| HTTPS / TLS | Most web traffic was encrypted. HTTP headers were not visible, but TLS Client Hello packets revealed SNI values, confirming domain names like www.instagram.com. |

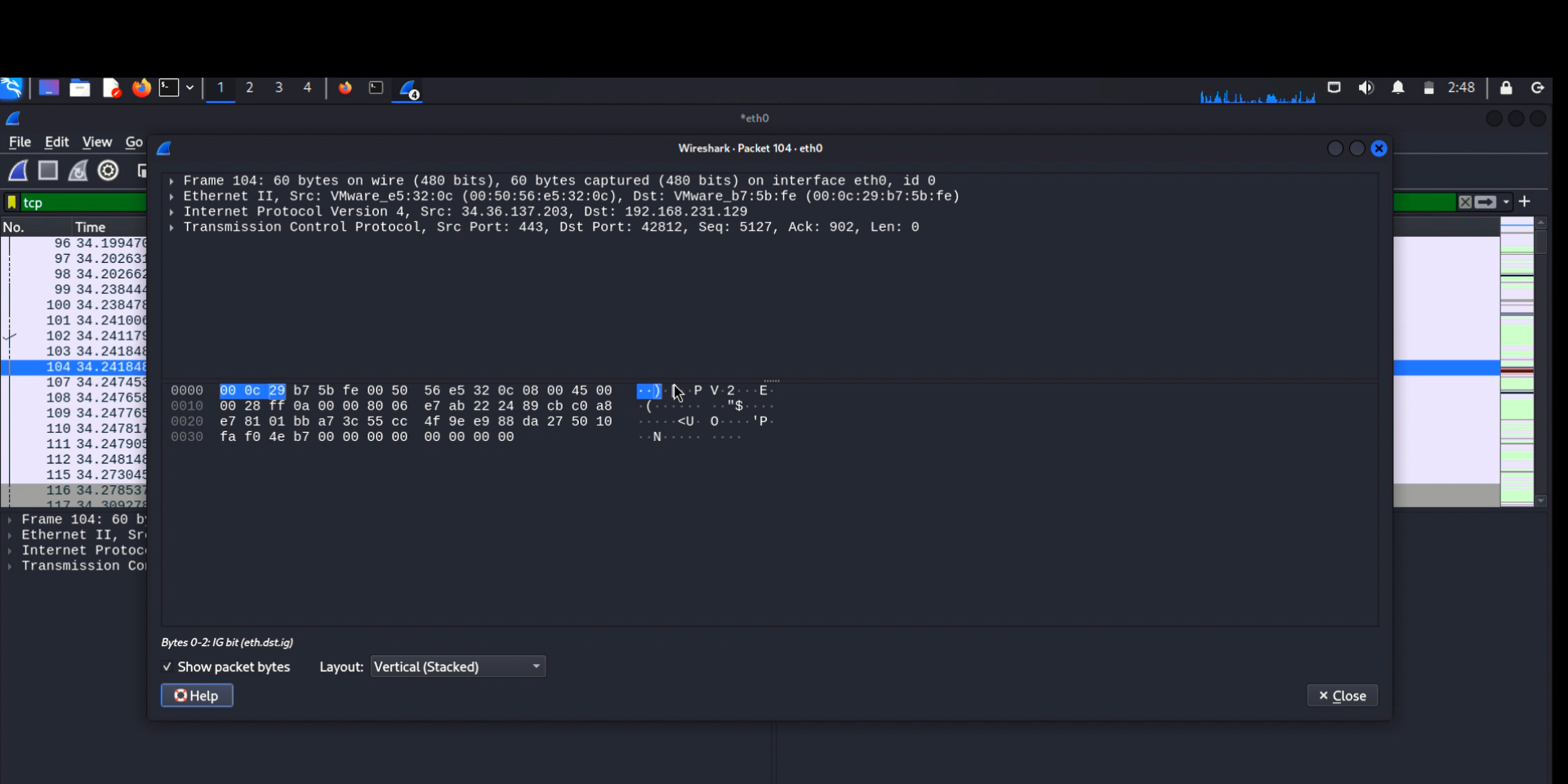
# Screenshots

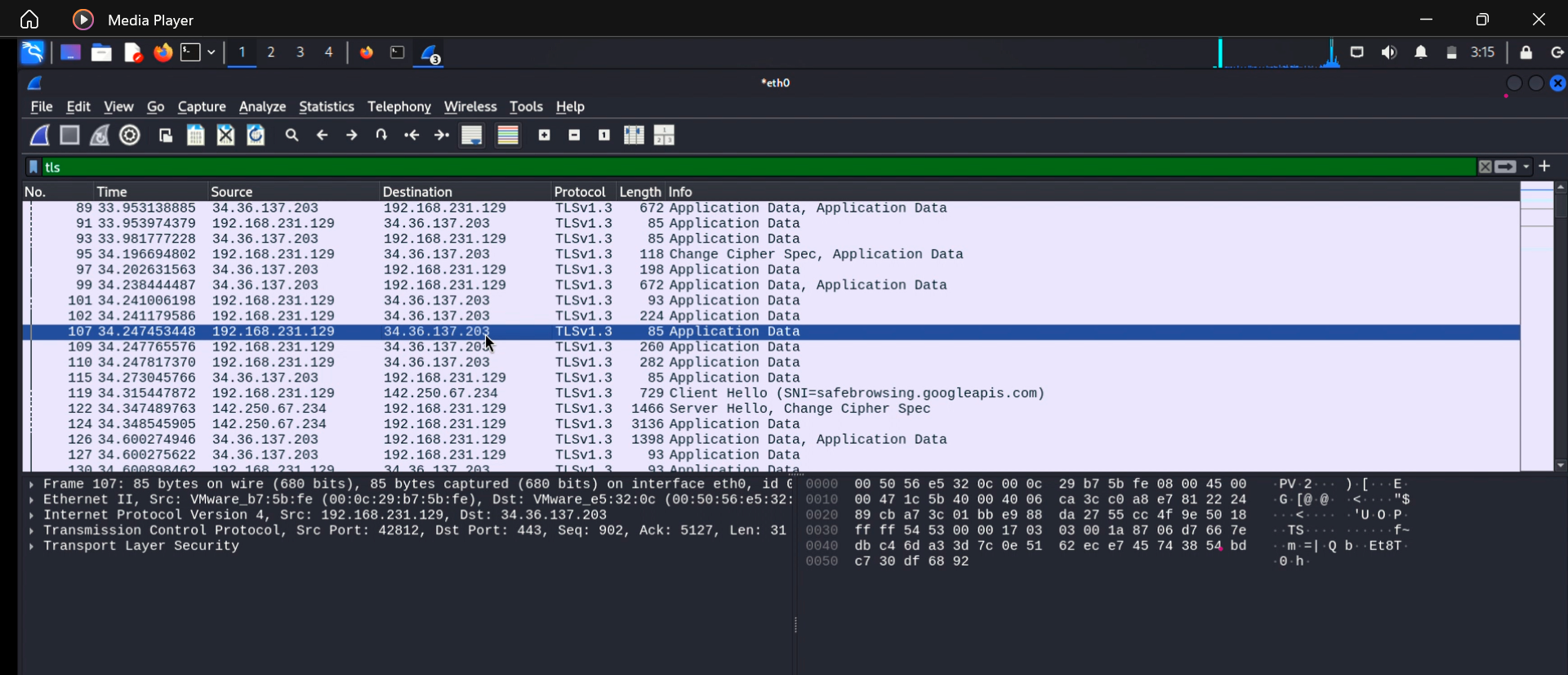
- A filtered dns packet showing query for chat.openai.com





- TCP 3-way handshake captured for a remote server



- TLS handshake showing SNI (Server Name Indication) 

# Conclusion

This analysis successfully demonstrates the following skills:  
- Live packet capture and interface selection in Linux  
- Use of Wireshark filters to isolate protocols  
- Understanding of the role of DNS in domain resolution  
- Identifying TCP connection setup patterns  
- Observing domain-level metadata in TLS-encrypted connections  
  
The traffic captured from ChatGPT and Instagram reflects standard modern internet communication: encrypted, efficient, and layered across multiple protocols.