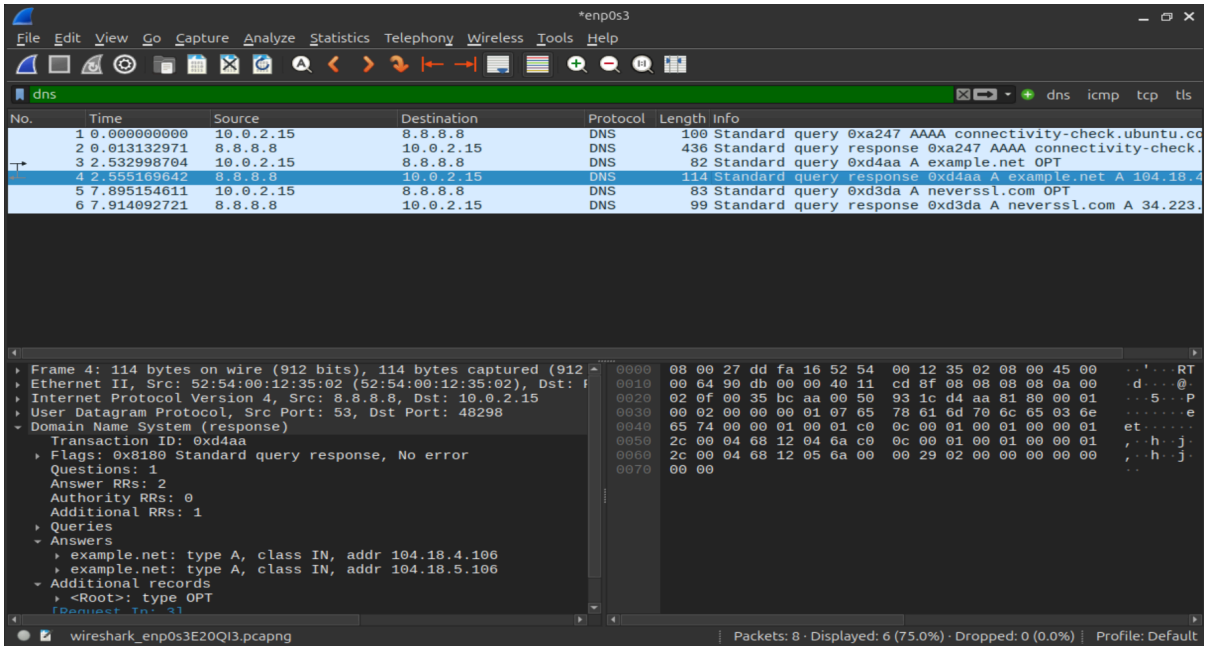
Wireshark week02

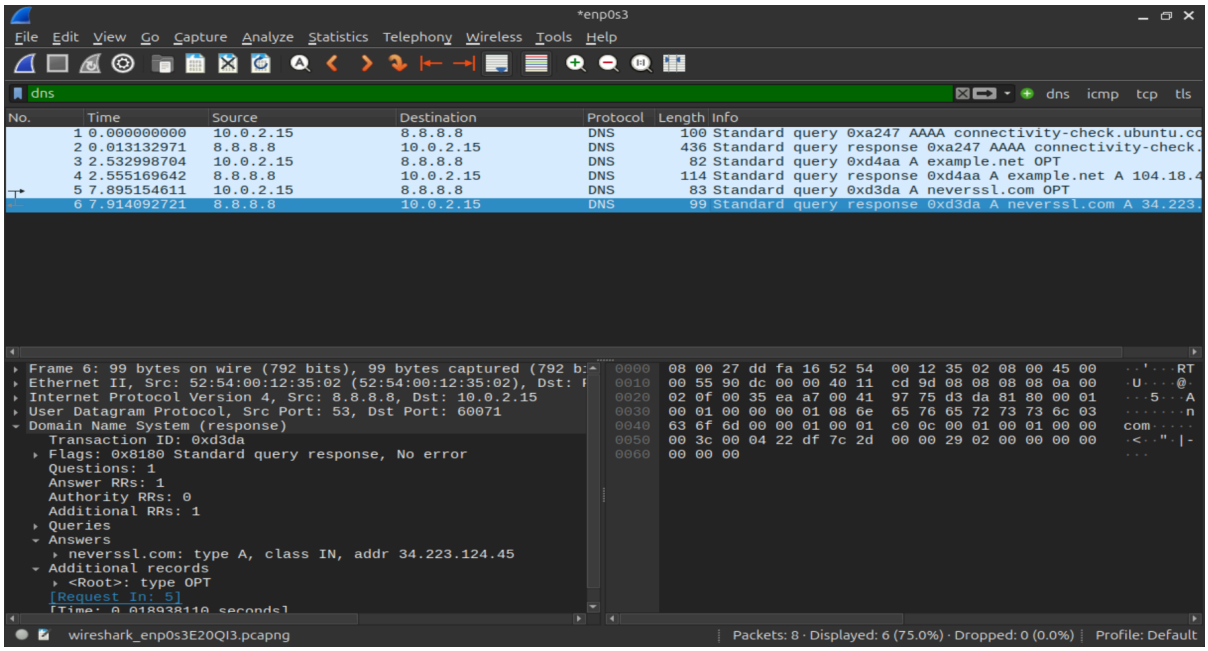
DNS traffic was captured in Wireshark using the `dig` command. Standard DNS A record queries and responses were observed for both example.net and neverssl.com, including source and destination IP addresses. Some domains returned multiple IP addresses, indicating load balancing.

Load two websites:

dig example.net



dig nerverssl.com



Expect to Find: DNS A/AAAA query

Found for both websites:

- Source IP
- Destination IP
- Standard DNS query
- Record type: **A**

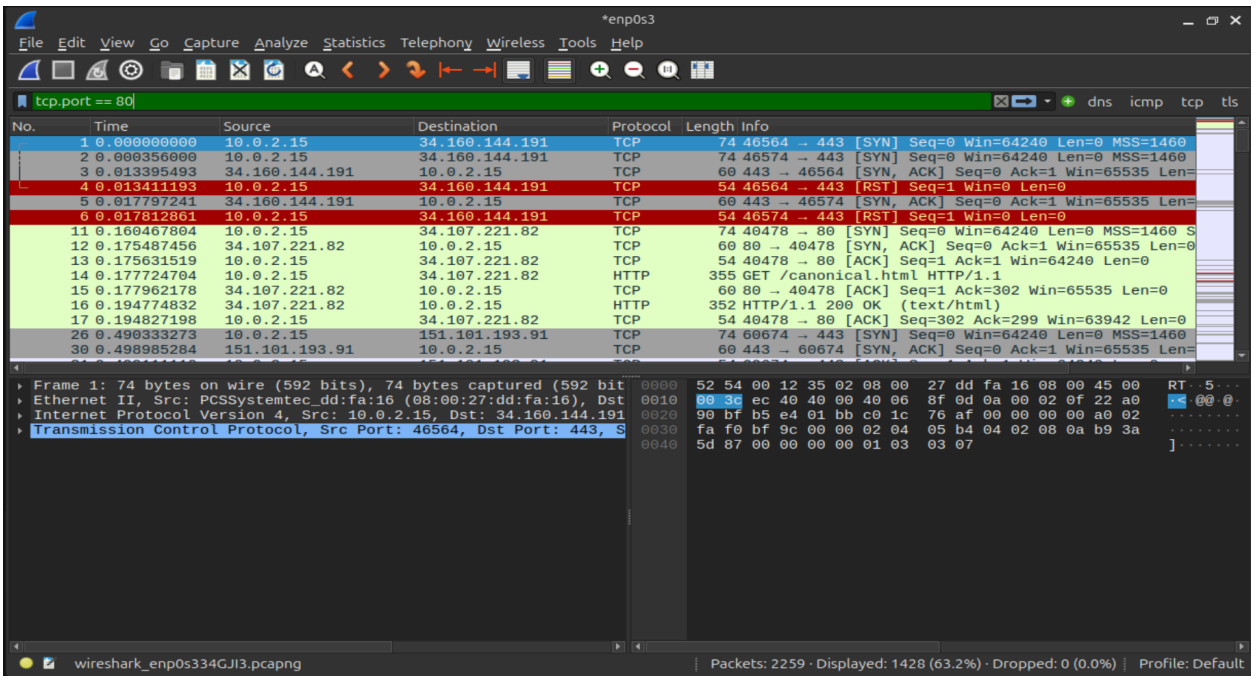
TCP handshake

A TCP three-way handshake (SYN, SYN-ACK, ACK) was successfully observed when loading example.com over HTTPS (port 443), followed by a TLS Client Hello where the Server Name Indication (SNI) revealed the destination domain.

An HTTP connection over port 80 was observed, including a complete TCP three-

way handshake followed by an HTTP GET request and a 200 OK response. To confirm the exact website, the HTTP Host header can be checked.

neverssl.com



source IP

destination IP

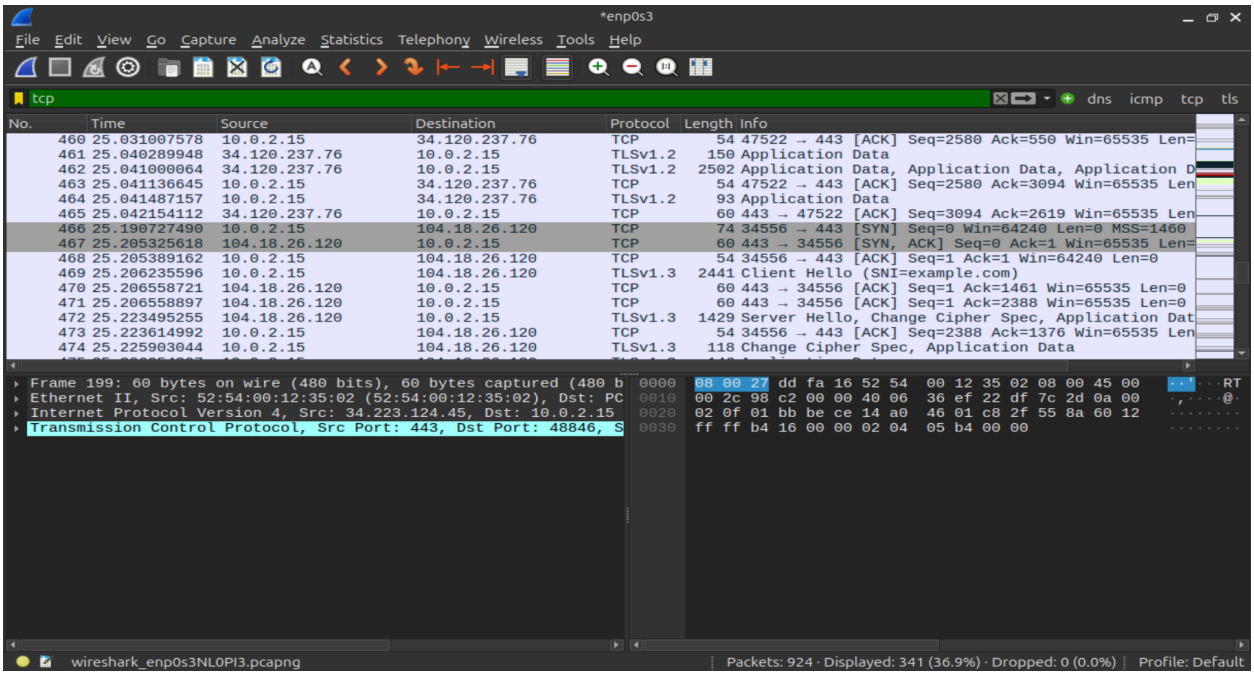
tcp

SYN → SYN-ACK → ACK

port 80

10.0.2.15 → 34.107.221.82 40478 → 80 [SYN]
34.107.221.82 → 10.0.2.15 80 → 40478 [SYN, ACK]
10.0.2.15 → 34.107.221.82 40478 → 80 [ACK]
GET /canonical.html HTTP/1.1
HTTP/1.1 200 OK

example.com



source IP

destination IP

tcp

SYN → SYN-ACK → ACK

port 443

client hello (SNI = example.com)

HTTP (Port 80)

- Full HTTP GET request visible
- Path visible (`/canonical.html`)
- Status code visible (`HTTP/1.1 200 OK`)
- Host header can be inspected

HTTPS (Port 443)

- TCP handshake visible

- TLS Client Hello visible
- **SNI reveals the domain name**
- Payload is encrypted (no HTTP GET visible)

HTTP traffic exposes request paths, headers, and responses in plaintext, while HTTPS encrypts application data, with only metadata such as IP addresses, ports, and SNI remaining visible.