

Task 4:

For the HTTP based website access, answer the following after analysing collected traces of HTTP:

1. What is the name of website?

neverssl.com

2. Find the packet that contains the first GET request for the website you have accessed.

Packet with GET / HTTP/1.1 from client (10.1.73.246) to server (neverssl.com).

3. Describe all headers and their values in this GET request message.

Host: neverssl.com

User-Agent: (browser info)

Accept: text/html, /

Accept-Language: en-US,en

Accept-Encoding: gzip, deflate

Connection: keep-alive

Upgrade-Insecure-Requests: 1

4. Identify the status code in the first server response.

200 OK

5. How many HTTP response messages are exchanged in total?

2 (main page + favicon)

6. Determine whether the connection is persistent or not. Justify with evidence from packet captures

Persistent → multiple requests/responses use same TCP connection, and Connection: keep-alive header is present.