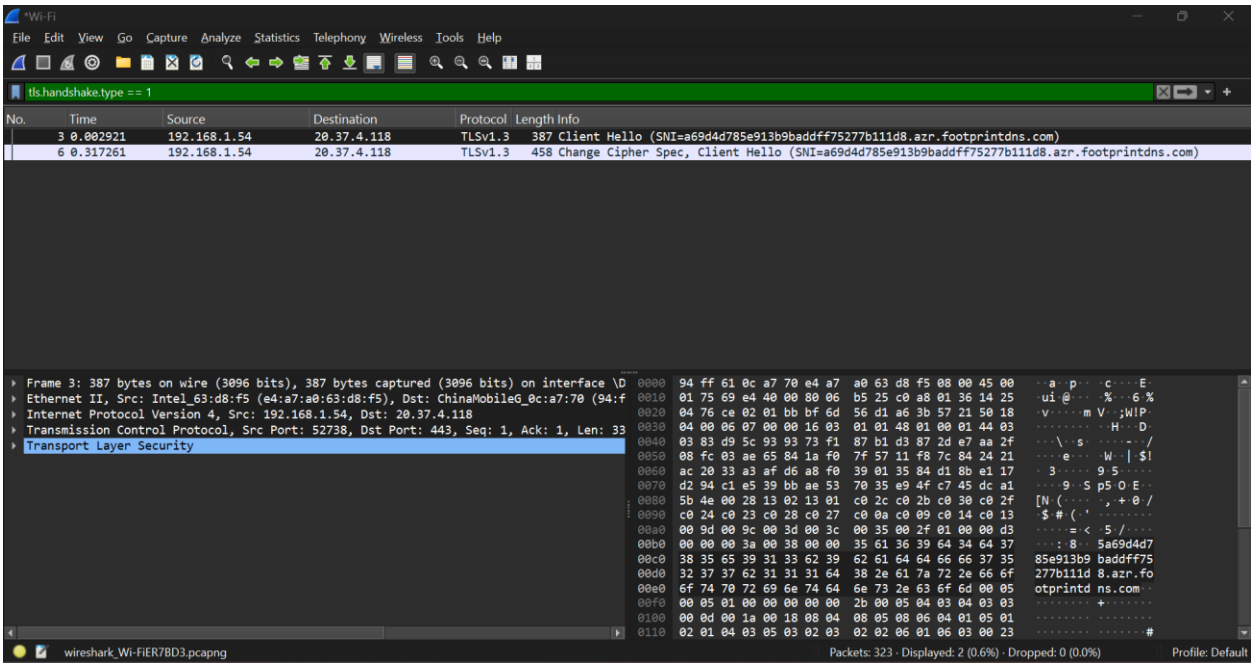
HTTPS :

Task : 1

The website is: **https://www.wikipedia.com**

Task : 2

tls.handshake.type == 1



Task : 3

Host: lushglowingquietrain.neverssl.com

Connection: Keep-Alive

Content-Length: 256

Content-Type: text/html; charset=iso-8859-1

The request is a GET request for /online.

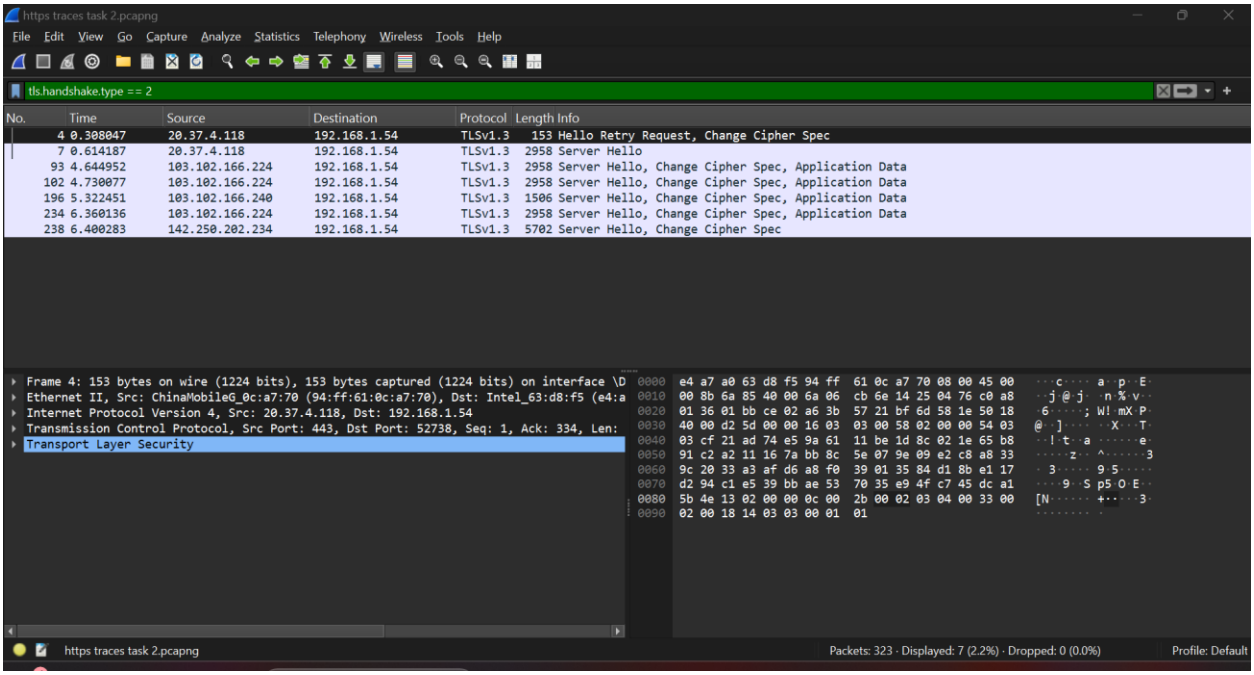
The HTTP version is HTTP/1.1**.**

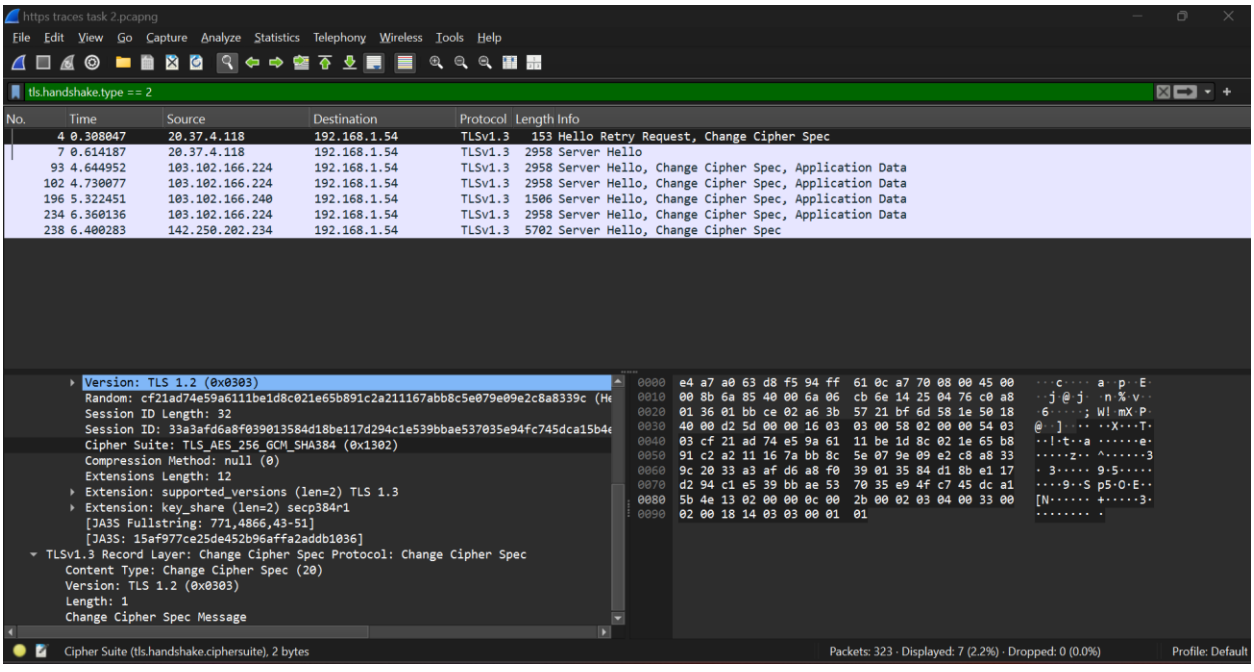
The server is Apache/2.4.62.

The response to this request (as seen in packet 2873) indicates a "301 Moved Permanently" **status.**

Task : 4

tls.handshake.type == 2



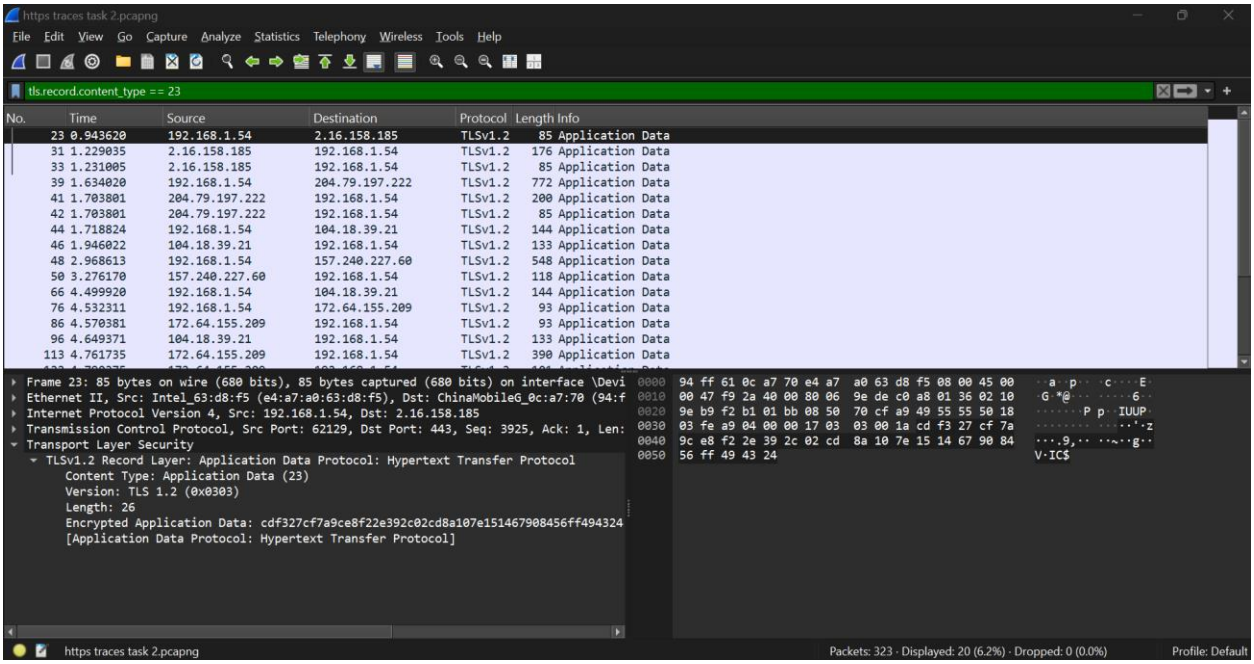


Task : 5

- **Issuer**: GlobalSign ASIA Pacific Infrastructure RSA R2 (or GlobalSign)
- **Subject**: CN = *.wikipedia.org (or CN = www.wikipedia.org)
- **Validity**:
  Not Before: e.g. Mar 1 2025 00:00:00 GMT
  Not After: e.g. Mar 1 2026 23:59:59 GMT

Task : 6

tls.record.content_type == 23



Because all HTTP communication is **encrypted by TLS**.

Without the session key, Wireshark cannot decrypt the HTTP layer.

Because all HTTP communication is **encrypted by TLS**.

- Because all HTTP communication is **encrypted by TLS**.
- Without the session key, Wireshark cannot decrypt the HTTP layer.