

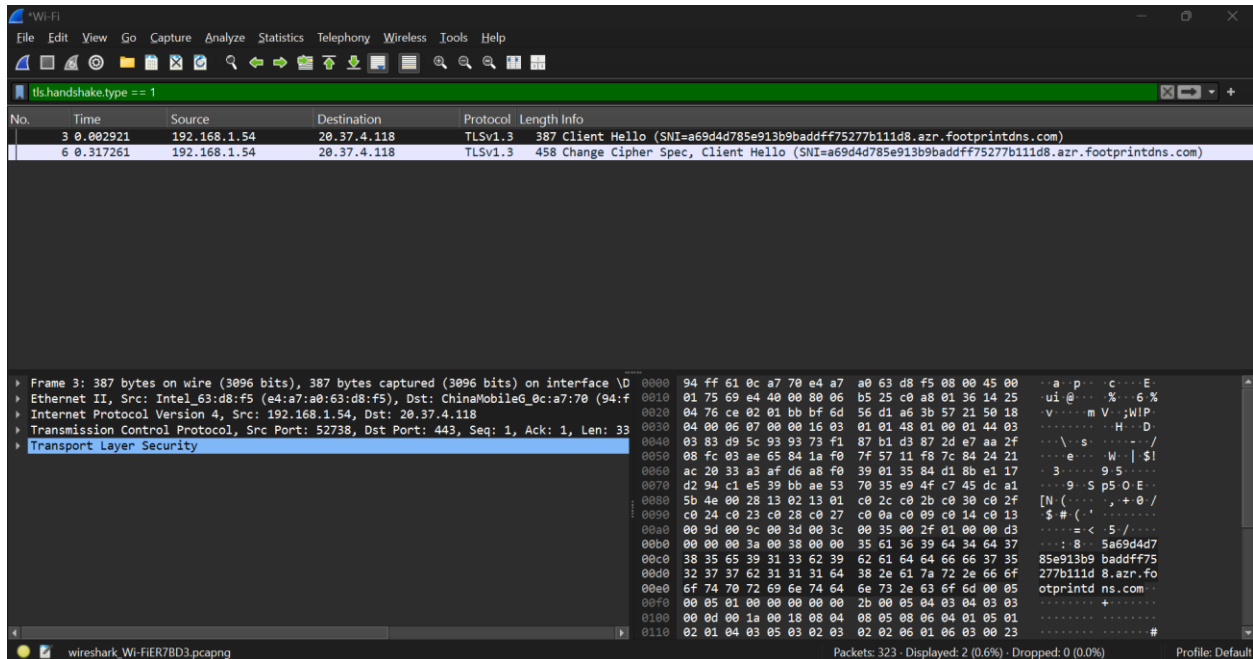
## HTTPS :

### Task : 1

The website is: <https://www.wikipedia.com>

### Task : 2

`tls.handshake.type == 1`



### Task : 3

**Host:** [lushglowingquietrain.neverssl.com](https://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

The screenshot shows a Wireshark capture of a TLS handshake (type 2) on interface eth0. The packet list shows a sequence of frames: a Hello Retry Request (frame 4), followed by several Server Hello frames (frames 7, 93, 102, 196, 234, 238). The packet details pane shows the selected frame 4, which is a Hello Retry Request, Change Cipher Spec. The packet bytes pane shows the raw data of the frame, including the TLS header and the Hello Retry Request structure.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.308847	20.37.4.118	192.168.1.54	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
7	0.614187	20.37.4.118	192.168.1.54	TLSv1.3	2958	Server Hello
93	4.644952	103.102.166.224	192.168.1.54	TLSv1.3	2958	Server Hello, Change Cipher Spec, Application Data
102	4.730077	103.102.166.224	192.168.1.54	TLSv1.3	2958	Server Hello, Change Cipher Spec, Application Data
196	5.322451	103.102.166.240	192.168.1.54	TLSv1.3	1506	Server Hello, Change Cipher Spec, Application Data
234	6.360136	103.102.166.224	192.168.1.54	TLSv1.3	2958	Server Hello, Change Cipher Spec, Application Data
238	6.400283	142.250.202.234	192.168.1.54	TLSv1.3	5702	Server Hello, Change Cipher Spec

The screenshot shows a Wireshark capture of a TLS handshake (type 2) on interface eth0. The packet list shows a sequence of frames: a Hello Retry Request (frame 4), followed by several Server Hello frames (frames 7, 93, 102, 196, 234, 238). The packet details pane shows the selected frame 4, which is a Hello Retry Request, Change Cipher Spec. The packet bytes pane shows the raw data of the frame, including the TLS header and the Hello Retry Request structure. The packet details pane also shows the TLS version (TLS 1.2) and the cipher suite (TLS\_AES\_256\_GCM\_SHA384).

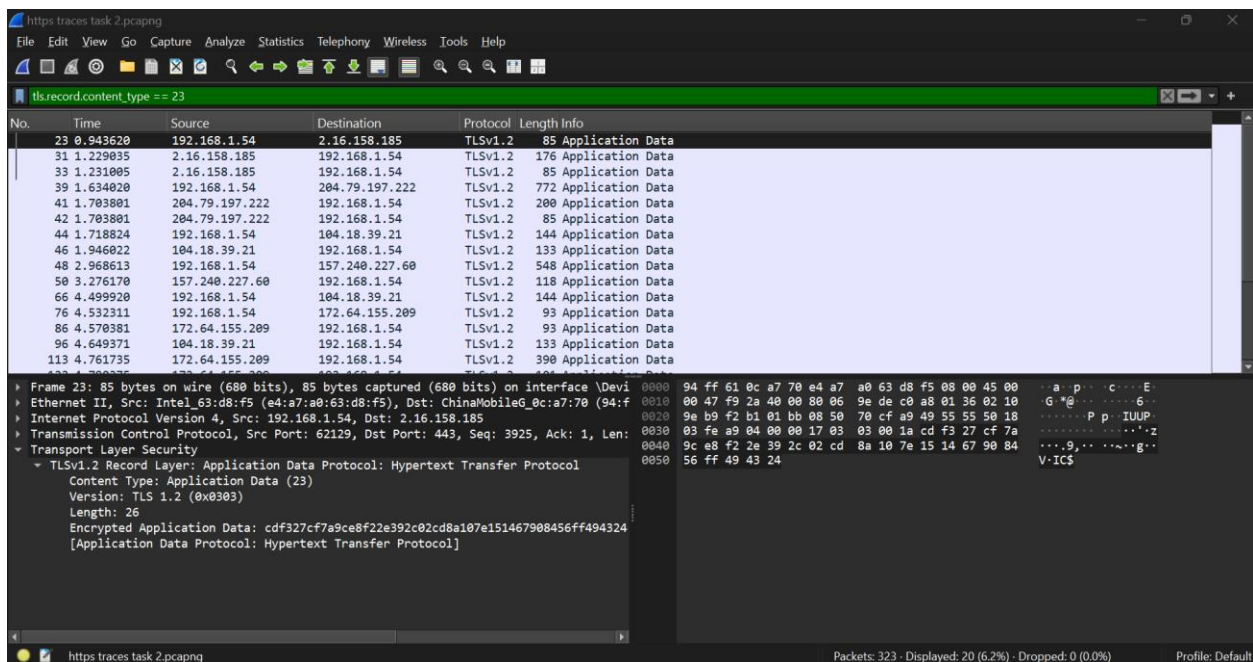
No.	Time	Source	Destination	Protocol	Length	Info
4	0.308847	20.37.4.118	192.168.1.54	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
7	0.614187	20.37.4.118	192.168.1.54	TLSv1.3	2958	Server Hello
93	4.644952	103.102.166.224	192.168.1.54	TLSv1.3	2958	Server Hello, Change Cipher Spec, Application Data
102	4.730077	103.102.166.224	192.168.1.54	TLSv1.3	2958	Server Hello, Change Cipher Spec, Application Data
196	5.322451	103.102.166.240	192.168.1.54	TLSv1.3	1506	Server Hello, Change Cipher Spec, Application Data
234	6.360136	103.102.166.224	192.168.1.54	TLSv1.3	2958	Server Hello, Change Cipher Spec, Application Data
238	6.400283	142.250.202.234	192.168.1.54	TLSv1.3	5702	Server Hello, Change Cipher Spec

## Task : 5

- **Issuer:** GlobalSign ASIA Pacific Infrastructure RSA R2 (or GlobalSign)
- **Subject:** CN = \*.wikipedia.org (or CN = [www.wikipedia.org](http://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.