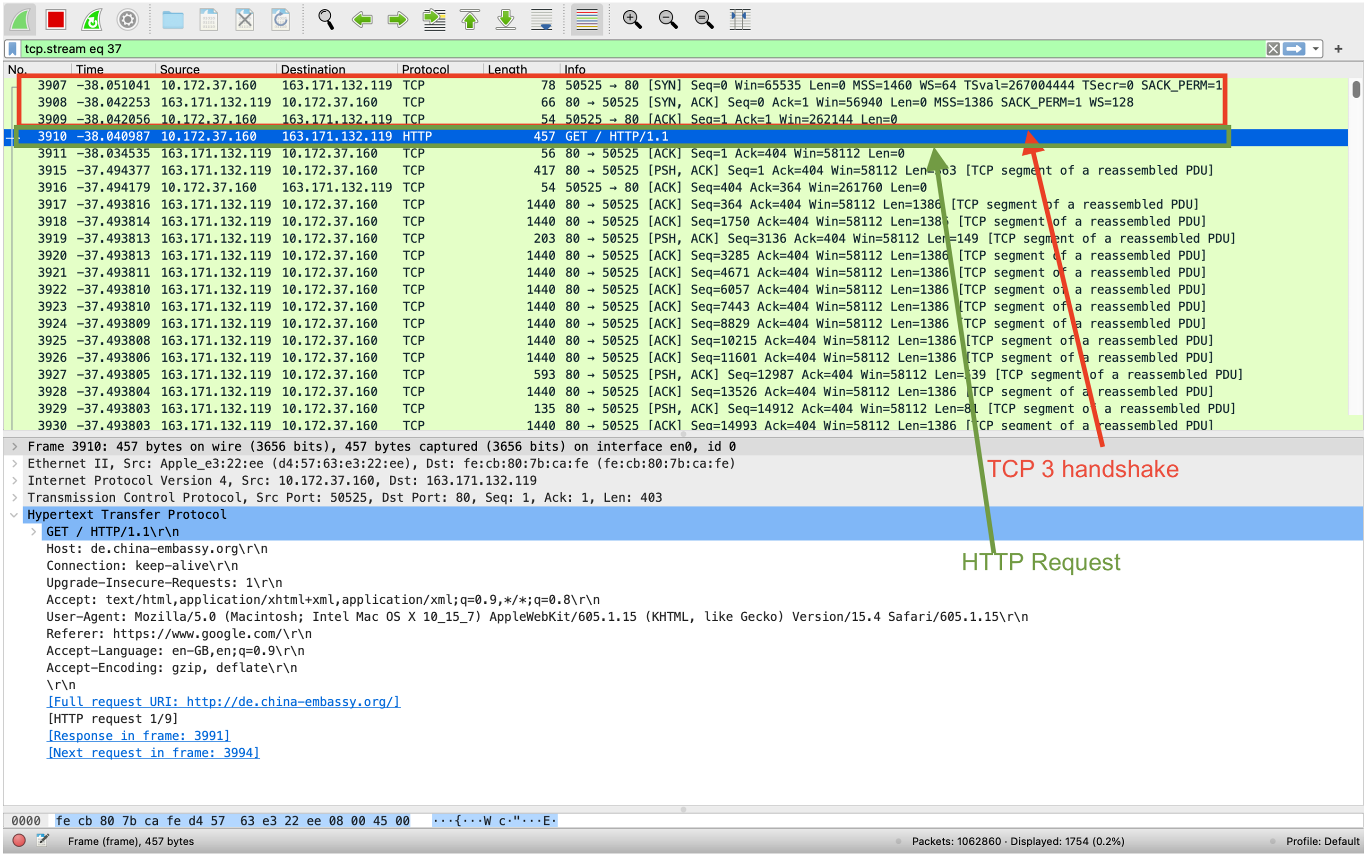
Report

NAME: Zhilun LI MATRICULATION NO.: 68572

§1 4-step HTTP flow

For this experiment of HTTP, I choose the official website of the embassy of the People's Republic of China in the Federal Republic of Germany because it is a website without using the HTTPS protocol.

With the help of the "Follow the TCP steam" functionality, I filtered out the TCP steam as follow:



```
tcp.stream eq 37

No.   Time       Source          Destination     Protocol  Length Info
 3907 -38.051041 10.172.37.160   163.171.132.119 TCP           78 50525 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=267004444 TSecr=0 SACK_PERM=1
 3908 -38.042253 163.171.132.119 10.172.37.160   TCP           66 80 → 50525 [SYN, ACK] Seq=0 Ack=1 Win=56940 Len=0 MSS=1386 SACK_PERM=1 WS=128
 3909 -38.042056 10.172.37.160   163.171.132.119 TCP           54 50525 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
 3910 -38.040987 10.172.37.160   163.171.132.119 HTTP         457 GET / HTTP/1.1
 3911 -38.034535 163.171.132.119 10.172.37.160   TCP           56 80 → 50525 [ACK] Seq=1 Ack=404 Win=58112 Len=0
 3915 -37.494377 163.171.132.119 10.172.37.160   TCP          417 80 → 50525 [PSH, ACK] Seq=1 Ack=404 Win=58112 Len=363 [TCP segment of a reassembled PDU]
 3916 -37.494179 10.172.37.160   163.171.132.119 TCP           54 50525 → 80 [ACK] Seq=404 Ack=364 Win=261760 Len=0
 3917 -37.493816 163.171.132.119 10.172.37.160   TCP         1440 80 → 50525 [ACK] Seq=364 Ack=404 Win=58112 Len=1386 [TCP segment of a reassembled PDU]
 3918 -37.493814 163.171.132.119 10.172.37.160   TCP         1440 80 → 50525 [ACK] Seq=1750 Ack=404 Win=58112 Len=1386 [TCP segment of a reassembled PDU]
 3919 -37.493813 163.171.132.119 10.172.37.160   TCP          203 80 → 50525 [PSH, ACK] Seq=3136 Ack=404 Win=58112 Len=149 [TCP segment of a reassembled PDU]
 3920 -37.493813 163.171.132.119 10.172.37.160   TCP         1440 80 → 50525 [ACK] Seq=3285 Ack=404 Win=58112 Len=1386 [TCP segment of a reassembled PDU]
 3921 -37.493811 163.171.132.119 10.172.37.160   TCP         1440 80 → 50525 [ACK] Seq=4671 Ack=404 Win=58112 Len=1386 [TCP segment of a reassembled PDU]
 3922 -37.493810 163.171.132.119 10.172.37.160   TCP         1440 80 → 50525 [ACK] Seq=6057 Ack=404 Win=58112 Len=1386 [TCP segment of a reassembled PDU]
 3923 -37.493810 163.171.132.119 10.172.37.160   TCP         1440 80 → 50525 [ACK] Seq=7443 Ack=404 Win=58112 Len=1386 [TCP segment of a reassembled PDU]
 3924 -37.493809 163.171.132.119 10.172.37.160   TCP         1440 80 → 50525 [ACK] Seq=8829 Ack=404 Win=58112 Len=1386 [TCP segment of a reassembled PDU]
 3925 -37.493808 163.171.132.119 10.172.37.160   TCP         1440 80 → 50525 [ACK] Seq=10215 Ack=404 Win=58112 Len=1386 [TCP segment of a reassembled PDU]
 3926 -37.493806 163.171.132.119 10.172.37.160   TCP         1440 80 → 50525 [ACK] Seq=11601 Ack=404 Win=58112 Len=1386 [TCP segment of a reassembled PDU]
 3927 -37.493805 163.171.132.119 10.172.37.160   TCP          593 80 → 50525 [PSH, ACK] Seq=12987 Ack=404 Win=58112 Len=539 [TCP segment of a reassembled PDU]
 3928 -37.493804 163.171.132.119 10.172.37.160   TCP         1440 80 → 50525 [ACK] Seq=13526 Ack=404 Win=58112 Len=1386 [TCP segment of a reassembled PDU]
 3929 -37.493803 163.171.132.119 10.172.37.160   TCP          135 80 → 50525 [PSH, ACK] Seq=14912 Ack=404 Win=58112 Len=81 [TCP segment of a reassembled PDU]
 3930 -37.493803 163.171.132.119 10.172.37.160   TCP         1440 80 → 50525 [ACK] Seq=14993 Ack=404 Win=58112 Len=1386 [TCP segment of a reassembled PDU]

> Frame 3910: 457 bytes on wire (3656 bits), 457 bytes captured (3656 bits) on interface en0, id 0
> Ethernet II, Src: Apple_e3:22:ee (d4:57:63:e3:22:ee), Dst: fe:cb:80:7b:ca:fe (fe:cb:80:7b:ca:fe)
> Internet Protocol Version 4, Src: 10.172.37.160, Dst: 163.171.132.119
> Transmission Control Protocol, Src Port: 50525, Dst Port: 80, Seq: 1, Ack: 1, Len: 403
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: de.china-embassy.org\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.4 Safari/605.1.15\r\n
    Referer: https://www.google.com/\r\n
    Accept-Language: en-GB,en;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    \r\n
    [Full request URI: http://de.china-embassy.org/]
    [HTTP request 1/9]
    [Response in frame: 3991]
    [Next request in frame: 3994]

0000  fe cb 80 7b ca fe d4 57  63 e3 22 ee 08 00 45 00   ···{···W c·"···E·

Frame (frame), 457 bytes          Packets: 1062860 · Displayed: 1754 (0.2%)          Profile: Default
```

From the screenshot shown above, I can see that there was a TCP 3-way handshake process before the HTTP request. The request has a structure as follows:

1. A starter line
2. HTTP headers
3. A blank line

In the HTTP headers, I can find information such as

1. The Host is de.china-embassy.org

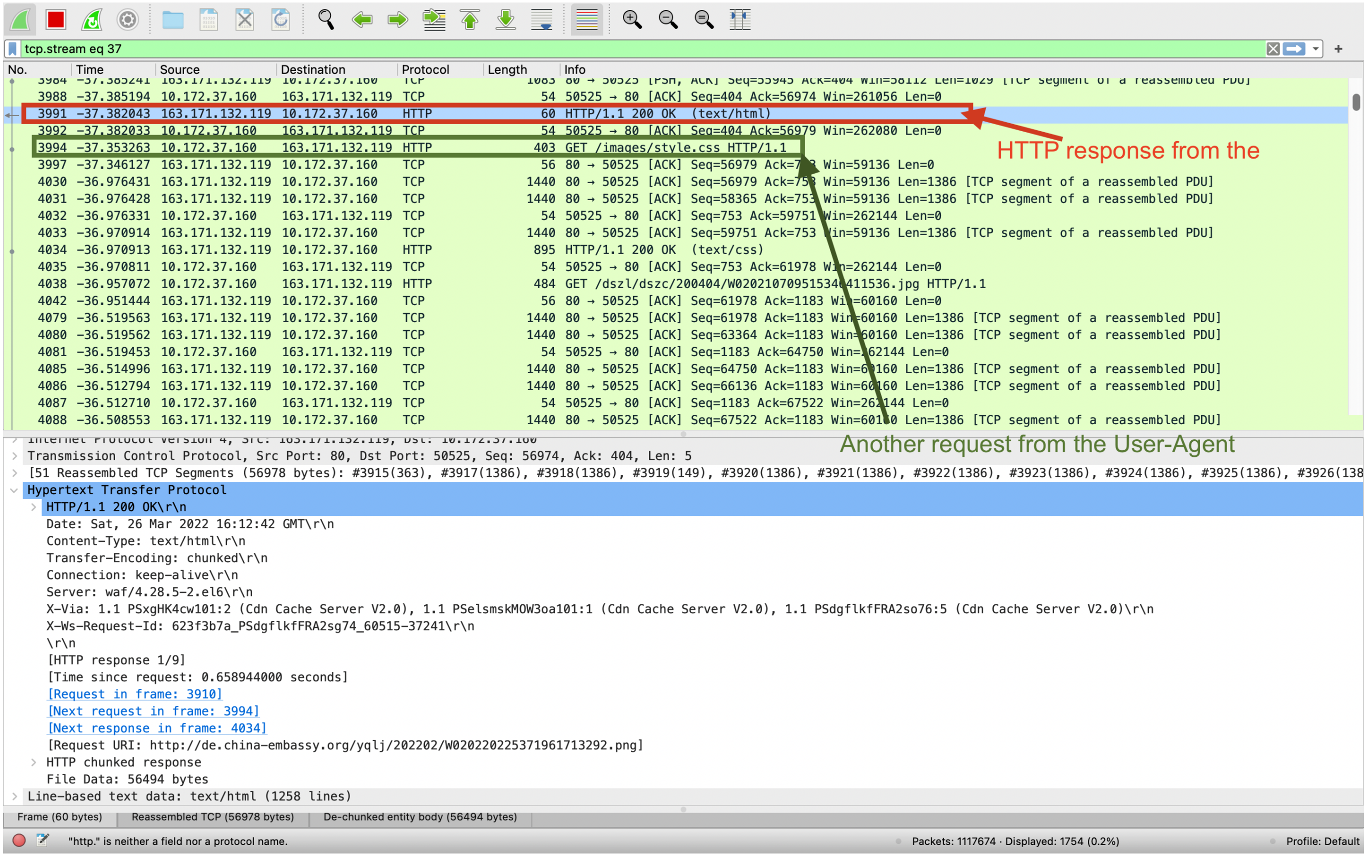
2. The connection support "keep-alive."

3. My browser's some features, such as supporting "Upgrade-insecure-requests", "Accept-Language" and "Accept-Encoding"

4. HTTP request nine contents in total, and this is the first content.

5. The response from the host is at the frame 3991 and the request (2/9) is in the frame 3994

Then I went to the frame 3991, and got a screenshot as shown below:



tcp.stream eq 37

```
No.   Time       Source          Destination     Protocol Length Info
3984 -37.385241 163.171.132.119 10.172.37.160   TCP     1083 80 → 50525 [PSH, ACK] Seq=55945 Ack=404 Win=58112 Len=1029 [TCP segment of a reassembled PDU]
3988 -37.385194 10.172.37.160   163.171.132.119 TCP       54 50525 → 80 [ACK] Seq=404 Ack=56974 Win=261056 Len=0
3991 -37.382043 163.171.132.119 10.172.37.160   HTTP      60 HTTP/1.1 200 OK  (text/html)
3992 -37.382033 10.172.37.160   163.171.132.119 TCP       54 50525 → 80 [ACK] Seq=404 Ack=56979 Win=262080 Len=0
3994 -37.353263 10.172.37.160   163.171.132.119 HTTP     403 GET /images/style.css HTTP/1.1
3997 -37.346127 163.171.132.119 10.172.37.160   TCP       56 80 → 50525 [ACK] Seq=56979 Ack=753 Win=59136 Len=0
4030 -36.976431 163.171.132.119 10.172.37.160   TCP     1440 80 → 50525 [ACK] Seq=56979 Ack=753 Win=59136 Len=1386 [TCP segment of a reassembled PDU]
4031 -36.976428 163.171.132.119 10.172.37.160   TCP     1440 80 → 50525 [ACK] Seq=58365 Ack=753 Win=59136 Len=1386 [TCP segment of a reassembled PDU]
4032 -36.976331 10.172.37.160   163.171.132.119 TCP       54 50525 → 80 [ACK] Seq=753 Ack=59751 Win=262144 Len=0
4033 -36.970914 163.171.132.119 10.172.37.160   TCP     1440 80 → 50525 [ACK] Seq=59751 Ack=753 Win=59136 Len=1386 [TCP segment of a reassembled PDU]
4034 -36.970913 163.171.132.119 10.172.37.160   HTTP     895 HTTP/1.1 200 OK  (text/css)
4035 -36.970811 10.172.37.160   163.171.132.119 TCP       54 50525 → 80 [ACK] Seq=753 Ack=61978 Win=262144 Len=0
4038 -36.957072 10.172.37.160   163.171.132.119 HTTP     484 GET /dszl/dszc/200404/W020210709515340411536.jpg HTTP/1.1
4042 -36.951444 163.171.132.119 10.172.37.160   TCP       56 80 → 50525 [ACK] Seq=61978 Ack=1183 Win=60160 Len=0
4079 -36.519563 163.171.132.119 10.172.37.160   TCP     1440 80 → 50525 [ACK] Seq=61978 Ack=1183 Win=60160 Len=1386 [TCP segment of a reassembled PDU]
4080 -36.519562 163.171.132.119 10.172.37.160   TCP     1440 80 → 50525 [ACK] Seq=63364 Ack=1183 Win=60160 Len=1386 [TCP segment of a reassembled PDU]
4081 -36.519453 10.172.37.160   163.171.132.119 TCP       54 50525 → 80 [ACK] Seq=1183 Ack=64750 Win=262144 Len=0
4085 -36.514996 163.171.132.119 10.172.37.160   TCP     1440 80 → 50525 [ACK] Seq=64750 Ack=1183 Win=60160 Len=1386 [TCP segment of a reassembled PDU]
4086 -36.512794 163.171.132.119 10.172.37.160   TCP     1440 80 → 50525 [ACK] Seq=66136 Ack=1183 Win=60160 Len=1386 [TCP segment of a reassembled PDU]
4087 -36.512710 10.172.37.160   163.171.132.119 TCP       54 50525 → 80 [ACK] Seq=1183 Ack=67522 Win=262144 Len=0
4088 -36.508553 163.171.132.119 10.172.37.160   TCP     1440 80 → 50525 [ACK] Seq=67522 Ack=1183 Win=60160 Len=1386 [TCP segment of a reassembled PDU]
```

```
> Internet Protocol Version 4, Src: 163.171.132.119, Dst: 10.172.37.160
> Transmission Control Protocol, Src Port: 80, Dst Port: 50525, Seq: 56974, Ack: 404, Len: 5
> [51 Reassembled TCP Segments (56978 bytes): #3915(363), #3917(1386), #3918(1386), #3919(149), #3920(1386), #3921(1386), #3922(1386), #3923(1386), #3924(1386), #3925(1386), #3926(138
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 26 Mar 2022 16:12:42 GMT\r\n
    Content-Type: text/html\r\n
    Transfer-Encoding: chunked\r\n
    Connection: keep-alive\r\n
    Server: waf/4.28.5-2.el6\r\n
    X-Via: 1.1 PSxgHK4cw101:2 (Cdn Cache Server V2.0), 1.1 PSelsmskMOW3oa101:1 (Cdn Cache Server V2.0), 1.1 PSdgflkfFRA2so76:5 (Cdn Cache Server V2.0)\r\n
    X-Ws-Request-Id: 623f3b7a_PSdgflkfFRA2sg74_60515-37241\r\n
    \r\n
    [HTTP response 1/9]
    [Time since request: 0.658944000 seconds]
    [Request in frame: 3910]
    [Next request in frame: 3994]
    [Next response in frame: 4034]
    [Request URI: http://de.china-embassy.org/yqlj/202202/W020220225371961713292.png]
  > HTTP chunked response
    File Data: 56494 bytes
> Line-based text data: text/html (1258 lines)
```

Frame (60 bytes)
Reassembled TCP (56978 bytes)
De-chunked entity body (56494 bytes)

"http." is neither a field nor a protocol name.

Packets: 1117674 · Displayed: 1754 (0.2%)

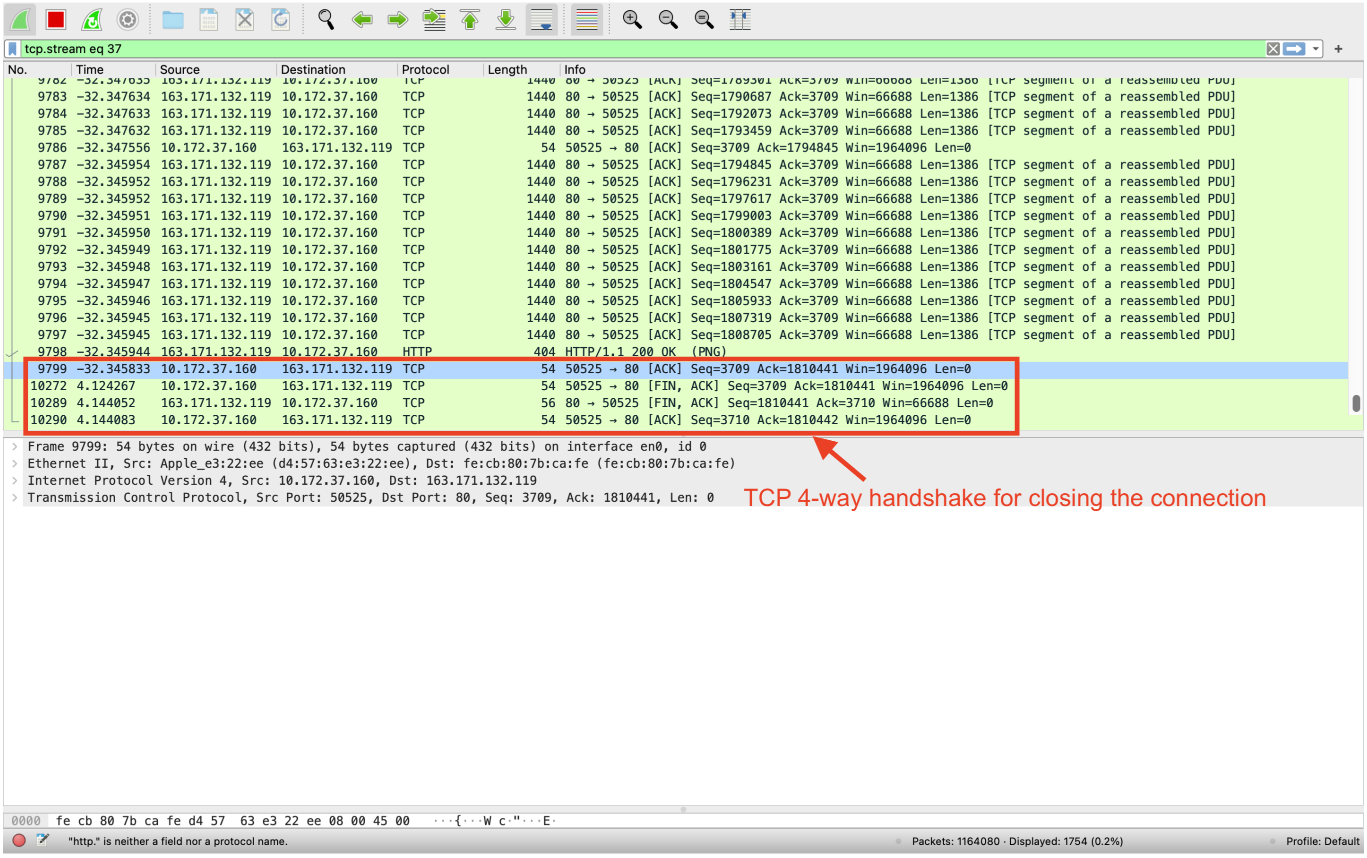
Profile: Default

From the screenshot shown above, I can see a response from the host and another request from the User-agent. Between the two requests from the User-agent, there is no close of the TCP connection because the protocol HTTP 1.1 is used so that the efficiency is hereby got improved.

The response has a structure as follows:

1. A status line including a. The protocol version HTTP/1.1; b. A status code 200, indicating the success of the request; c. A status text, OK, a brief description of the status code.
2. Headers, including a. the requested content has a type of text/html b. transfer coding information and so on
3. A blank line

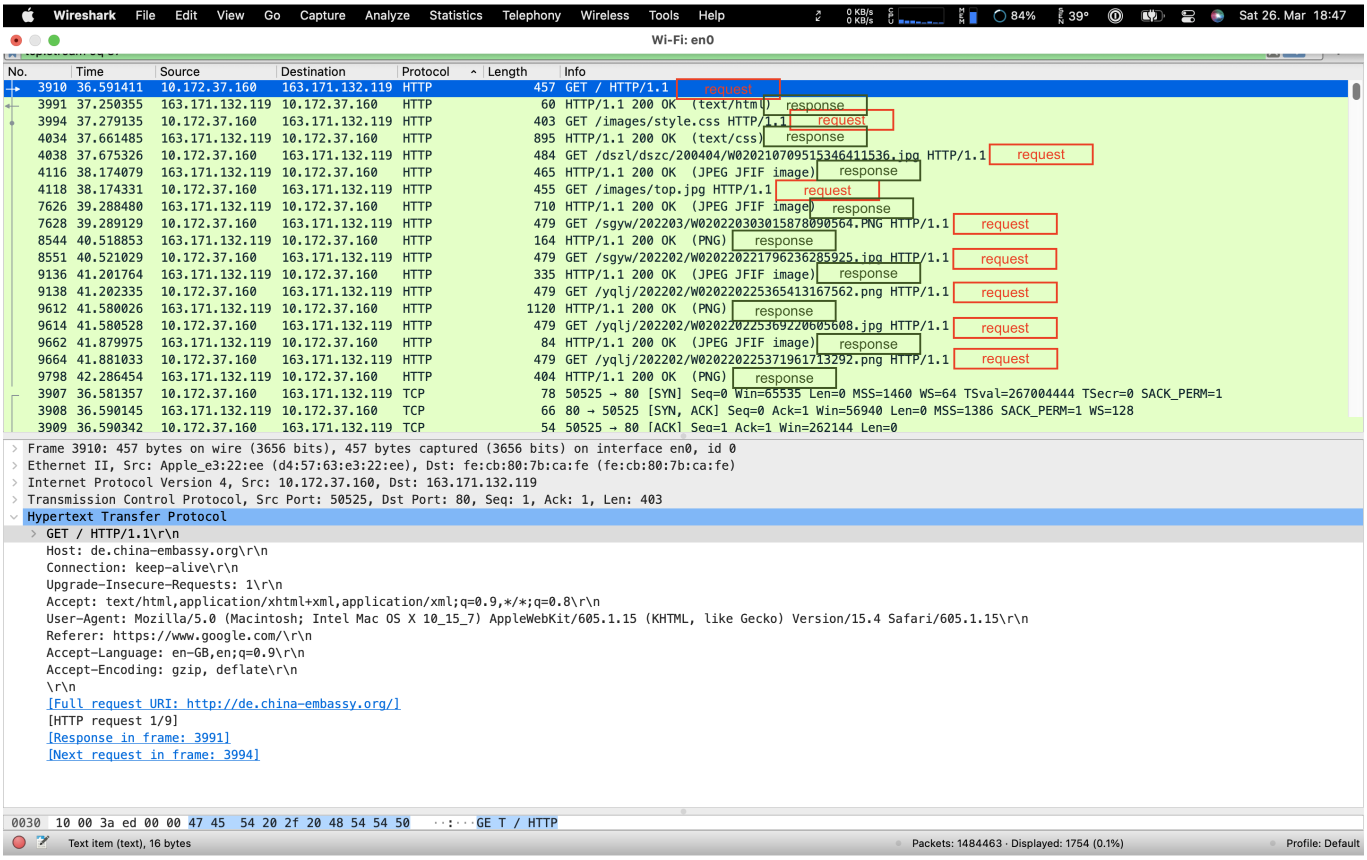
Go to the very end of this TCP stream; I can see a close of connection via TCP 4-way handshake, which is shown below:



```
tcp.stream eq 37

No.    Time       Source          Destination     Protocol  Length Info
 9782 -32.347635 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1789301 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9783 -32.347634 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1790687 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9784 -32.347633 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1792073 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9785 -32.347632 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1793459 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9786 -32.347556 10.172.37.160   163.171.132.119 TCP         54 50525 → 80 [ACK] Seq=3709 Ack=1794845 Win=1964096 Len=0
 9787 -32.345954 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1794845 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9788 -32.345952 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1796231 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9789 -32.345952 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1797617 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9790 -32.345951 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1799003 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9791 -32.345950 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1800389 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9792 -32.345949 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1801775 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9793 -32.345948 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1803161 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9794 -32.345947 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1804547 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9795 -32.345946 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1805933 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9796 -32.345945 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1807319 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9797 -32.345945 163.171.132.119 10.172.37.160   TCP       1440 80 → 50525 [ACK] Seq=1808705 Ack=3709 Win=66688 Len=1386 [TCP segment of a reassembled PDU]
 9798 -32.345944 163.171.132.119 10.172.37.160   HTTP       404 HTTP/1.1 200 OK  (PNG)
 9799 -32.345833 10.172.37.160   163.171.132.119 TCP         54 50525 → 80 [ACK] Seq=3709 Ack=1810441 Win=1964096 Len=0
10272 4.124267   10.172.37.160   163.171.132.119 TCP         54 50525 → 80 [FIN, ACK] Seq=3709 Ack=1810441 Win=1964096 Len=0
10289 4.144052   163.171.132.119 10.172.37.160   TCP         56 80 → 50525 [FIN, ACK] Seq=1810441 Ack=3710 Win=66688 Len=0
10290 4.144083   10.172.37.160   163.171.132.119 TCP         54 50525 → 80 [ACK] Seq=3710 Ack=1810442 Win=1964096 Len=0

> Frame 9799: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
> Ethernet II, Src: Apple_e3:22:ee (d4:57:63:e3:22:ee), Dst: fe:cb:80:7b:ca:fe (fe:cb:80:7b:ca:fe)
> Internet Protocol Version 4, Src: 10.172.37.160, Dst: 163.171.132.119
> Transmission Control Protocol, Src Port: 50525, Dst Port: 80, Seq: 3709, Ack: 1810441, Len: 0

0000  fe cb 80 7b ca fe d4 57  63 e3 22 ee 08 00 45 00   ···{···W c·"···E·

"http." is neither a field nor a protocol name.        Packets: 1164080 · Displayed: 1754 (0.2%)        Profile: Default
```

TCP 4-way handshake for closing the connection

§2 All filter results for HTTP



```
No.    Time       Source          Destination     Protocol  Length Info
 3910 36.591411  10.172.37.160   163.171.132.119 HTTP       457 GET / HTTP/1.1
 3991 37.250355  163.171.132.119 10.172.37.160   HTTP        60 HTTP/1.1 200 OK  (text/html)
 3994 37.279135  10.172.37.160   163.171.132.119 HTTP       403 GET /images/style.css HTTP/1.1
 4034 37.661485  163.171.132.119 10.172.37.160   HTTP       895 HTTP/1.1 200 OK  (text/css)
 4038 37.675326  10.172.37.160   163.171.132.119 HTTP       484 GET /dszl/dszc/200404/W020210709515346411536.jpg HTTP/1.1
 4116 38.174079  163.171.132.119 10.172.37.160   HTTP       465 HTTP/1.1 200 OK  (JPEG JFIF image)
 4118 38.174331  10.172.37.160   163.171.132.119 HTTP       455 GET /images/top.jpg HTTP/1.1
 7626 39.288480  163.171.132.119 10.172.37.160   HTTP       710 HTTP/1.1 200 OK  (JPEG JFIF image)
 7628 39.289129  10.172.37.160   163.171.132.119 HTTP       479 GET /sgyw/202203/W020220303015878090564.PNG HTTP/1.1
 8544 40.518853  163.171.132.119 10.172.37.160   HTTP       164 HTTP/1.1 200 OK  (PNG)
 8551 40.521029  10.172.37.160   163.171.132.119 HTTP       479 GET /sgyw/202202/W020220221796236285925.jpg HTTP/1.1
 9136 41.201764  163.171.132.119 10.172.37.160   HTTP       335 HTTP/1.1 200 OK  (JPEG JFIF image)
 9138 41.202335  10.172.37.160   163.171.132.119 HTTP       479 GET /yqlj/202202/W020220225365413167562.png HTTP/1.1
 9612 41.580026  163.171.132.119 10.172.37.160   HTTP      1120 HTTP/1.1 200 OK  (PNG)
 9614 41.580528  10.172.37.160   163.171.132.119 HTTP       479 GET /yqlj/202202/W020220225369220605608.jpg HTTP/1.1
 9662 41.879975  163.171.132.119 10.172.37.160   HTTP        84 HTTP/1.1 200 OK  (JPEG JFIF image)
 9664 41.881033  10.172.37.160   163.171.132.119 HTTP       479 GET /yqlj/202202/W020220225371961713292.png HTTP/1.1
 9798 42.286454  163.171.132.119 10.172.37.160   HTTP       404 HTTP/1.1 200 OK  (PNG)
 3907 36.581357  10.172.37.160   163.171.132.119 TCP         78 50525 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=267004444 TSecr=0 SACK_PERM=1
 3908 36.590145  163.171.132.119 10.172.37.160   TCP         66 80 → 50525 [SYN, ACK] Seq=0 Ack=1 Win=56940 Len=0 MSS=1386 SACK_PERM=1 WS=128
 3909 36.590342  10.172.37.160   163.171.132.119 TCP         54 50525 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0

> Frame 3910: 457 bytes on wire (3656 bits), 457 bytes captured (3656 bits) on interface en0, id 0
> Ethernet II, Src: Apple_e3:22:ee (d4:57:63:e3:22:ee), Dst: fe:cb:80:7b:ca:fe (fe:cb:80:7b:ca:fe)
> Internet Protocol Version 4, Src: 10.172.37.160, Dst: 163.171.132.119
> Transmission Control Protocol, Src Port: 50525, Dst Port: 80, Seq: 1, Ack: 1, Len: 403
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: de.china-embassy.org\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.4 Safari/605.1.15\r\n
    Referer: https://www.google.com/\r\n
    Accept-Language: en-GB,en;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    \r\n
    [Full request URI: http://de.china-embassy.org/]
    [HTTP request 1/9]
    [Response in frame: 3991]
    [Next request in frame: 3994]

0030  10 00 3a ed 00 00 47 45  54 20 2f 20 48 54 54 50   ··:···GE T / HTTP

Text item (text), 16 bytes        Packets: 1484463 · Displayed: 1754 (0.1%)        Profile: Default
```