Wireshark Assignment

- **College:** College of Computing
- **Major:** Computer Science
- **Supervisor:** Man Hon Michael CHEUNG
- **Student Name:** CHEN Xian
- **Student Number:** [redacted]

September 16th 2025

Problem 1: Capturing Web Browser HTTP Traffic

Questions

1. What languages (if any) does your browser indicate that it can accept to the server in HTTP Get message? (3 marks)

```
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6\r\n
```

2. What application layer protocol does your web browser access above website? (3 marks)

   The application layer protocol is HTTP.

3. What transport layer protocol does this HTTP GET packet use? (3 marks)

   The HTTP GET packet uses TCP.

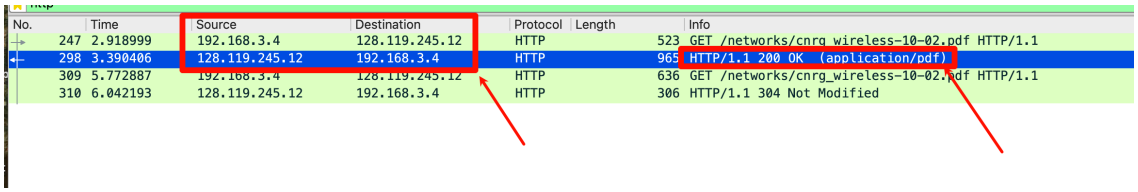
4. What is the destination IP address and port of the HTTP GET message? (3 marks)

   IP: 128.119.245.12; Port: 80

5. For the HTTP GET message, what is the next sequence number in the TCP header? (3 marks)

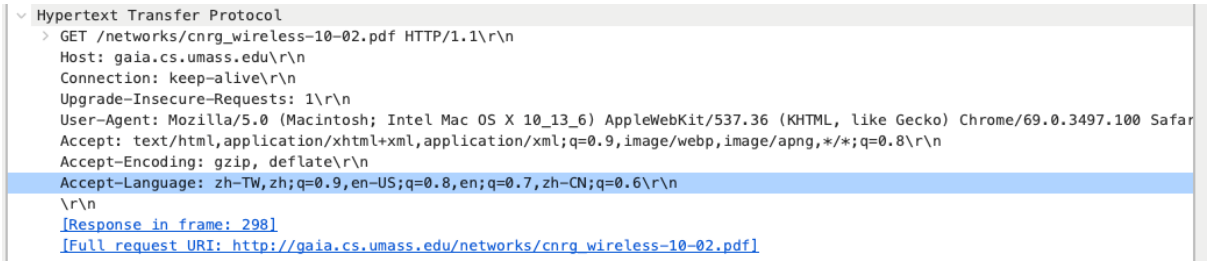
   The next sequence number is 458.

6. Find the response packet corresponding to the HTTP GET message. Take a screenshot. Briefly describe how you are able to tell this packet corresponds to the HTTP GET message. (3 marks)



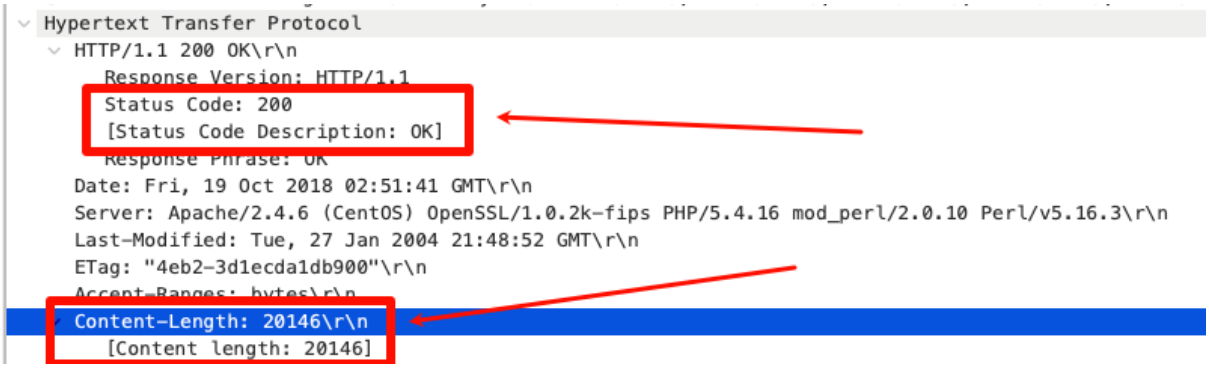
The Info field shows HTTP/1.1 200 OK, and you can see the related IP source and destination and port.

7. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET? (1 mark)



No.

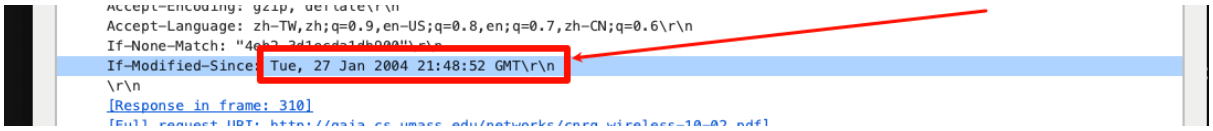
8. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell? (4 marks)



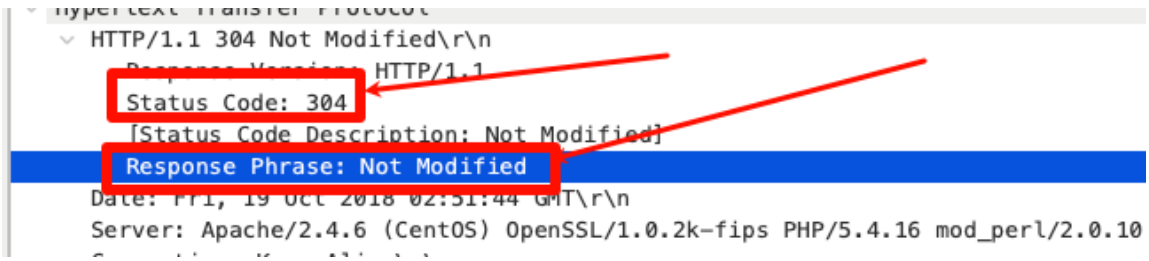
Yes, it did, and you can know how I tell that from the screenshot.

9. Now inspect the contents of the second HTTP GET request that requests the pdf file. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:"header? (3 marks)

Yes.



10. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain. (4 marks)



The server does not return the file content because the client indicates IF-MODIFIED-SINCE and the file has not changed.

Problem 2: Capturing DNS Traffic

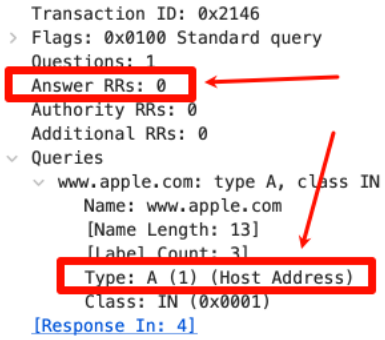
Questions

1. Are they sent over UDP or TCP? (2 marks) How can you tell? (2 marks)

   UDP, the packet has User Datagram Protocol as its transport layer protocol.

   ```
   > Internet Protocol Version 4, Src: 192.168.1.39, Dst: 223.5.5.5
   > User Datagram Protocol, Src Port: 52717, Dst Port: 53
   ```

2. In the Packet List panel, look for the DNS query packet (Standard query 0x???? A www.openrice.com) from the Info column. What "Type" of DNS query is it? Does the query message contain any "answers"? (6 marks)

   The answer shown in the screenshot. The DNS query contains no answers.

3. Look for the DNS response packet (Standard query response 0x???? A www.openrice.com). Examine the DNS response message. What is the source port of DNS response message? (2 mark) What is the type of address in the answer of the response message? (2 marks)

   Source Port = 53
   Type: A (1) –》 (IPv4 address).

4. List the IP address of www.openrice.com. (3 marks)

   170.33.8.214

5. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server (If you are using OSX, you may check it in "System preferences/ Network/ Advanced/DNS"). Are these two IP addresses the same? (3 marks)

   The DNS query is sent to 223.5.5.5
   My local DNS server is 223.5.5.5
   Yes, the IP addresses match.

Problem 3: Capturing SSL Traffic

Questions

1. Find a pair of client and server. Find the first 8 Ethernet frames in their session. For each frame, specify the source address and destination address, determine the number of SSL records that are included in the frame, and list the SSL record types that are included in the frame. Draw a table to show the packet exchange between client and server. An example of the table is shown as follows. (There might be segments missed by Wireshark, e.g., "TCP Previous segment not captured, Ignored Unknown Record". Find a session that has no missing segment.) (12 marks)

Frame	Source address	Destination address	SSL count	SSL Type
155	240e:3b4:2c41:2750:34f8:810b:d003:b445	240e:97c:38:600:3::3dd	1	Handshake (22)
158	240e:97c:38:600:3::3dd	240e:3b4:2c41:2750:34f8:810b:d003:b445	3	Handshake (22)、Change Cipher Spec (20)、Application Data (23)
162	240e:97c:38:600:3::3dd	240e:3b4:2c41:2750:34f8:810b:d003:b445	1	Application Data (23)
164	240e:97c:38:600:3::3dd	240e:3b4:2c41:2750:34f8:810b:d003:b445	1	Application Data (23)
166	240e:3b4:2c41:2750:34f8:810b:d003:b445	240e:97c:38:600:3::3dd	2	Change Cipher Spec (20)、Application Data (23)
167	240e:3b4:2c41:2750:34f8:810b:d003:b445	240e:97c:38:600:3::3dd	1	Application Data (23)
168	240e:3b4:2c41:2750:34f8:810b:d003:b445	240e:97c:38:600:3::3dd	1	Application Data (23)
169	240e:97c:38:600:3::3dd	240e:3b4:2c41:2750:34f8:810b:d003:b445	1	Application Data (23)
170	240e:97c:38:600:3::3dd	240e:3b4:2c41:2750:34f8:810b:d003:b445	2	Application Data (23)

Specify the IP addresses of client and server respectively. How can you tell? (3 marks)

The client IP address is 240e:3b4:2c41:2750:34f8:810b:d003:b445, because this host sent the first TLS handshake message (Client Hello).
The server IP address is 240e:97c:38:600:3::3dd, because it responded with the Server Hello message.
You can see it in Info.

2. Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is "content type" and has length of one byte. List all three fields and their lengths. (3 marks)

Content Type: 1 byte
Version: 2 bytes
Length: 2 bytes

3. Expand a ClientHello record. What is the value of the content type? What is it used for? (3 marks)

Value: 22

It indicates that this record contains a handshake message, which is used to establish a secure connection.

4. Does the ClientHello record advertise the cipher suites it supports? Show the first cipher suite. (2 mark)

Yes. The ClientHello advertises supported cipher suites. The first listed cipher suite is Reserved (GREASE).

5. Find the corresponding ServerHello SSL record. Does this record specify a chosen cipher suite? Show the chosen cipher suite. (3 mark)

The ServerHello specifies the chosen cipher suite: TLS_AES_256_GCM_SHA384 (0x1302)

6. Does the ServerHello SSL record include a nonce? If so, how long is it? What is the purpose of the client and server nonces in SSL? (3 mark)

Yes. ServerHello includes a 32 byte nonce (Random). It used as Session Keys and used to prevent replay attacks.

7. Does the ServerHello SSL record include a session ID? What is the purpose of the session ID? (3 mark)

   Yes, it does. It used for session resumption.

8. Does the ServerHello SSL record contain a certificate, or is the certificate included in a separate record. Does the certificate fit into a single Ethernet frame? (3 mark)

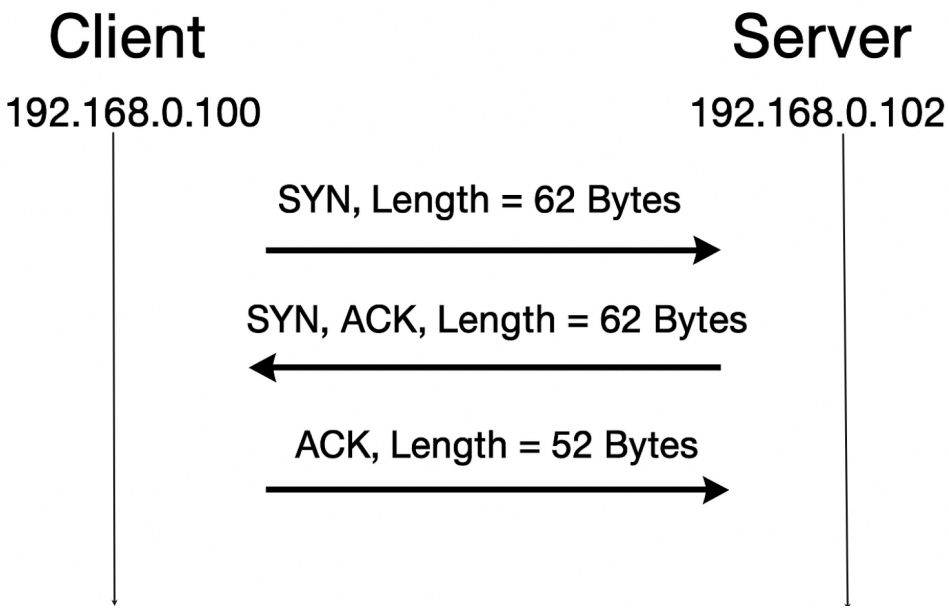
   The Certificate is in a separate record.

   No, it does not fit.

Problem 4: Analyzing TCP Traffic

Questions

1. Draw a diagram to illustrate the handshake between 192.168.0.100:4480 and 192.168.0.102:5001. List the length of the all packets used to complete TCP handshake. (6 marks)



2. Finding the first TCP segment sending from 192.168.0.100:4480 after the handshake of TCP. What's the length of this TCP segment? (3 marks)

   LEN = 1000 Bytes

3. Calculating the RTT value for the TCP segment you found in question 2. (Hint: the value of the Time column in the packet listing window is the amount of the time, in seconds, since Wireshark tracing began.) (6 marks)

T_{sent_time} = 0.000361 seconds;
T_{ack} = 0.142331 seconds;
RTT = T_{ack} - T_{sent_time} = 0.14197 seconds;