Introduction to Computer Networks

Lab 1: Wireshark

1. Description

Learn the fundamentals of packet capturing using Wireshark, including setup, filter techniques, and analysis. The primary objective is to help students comprehend the transmission and reception processes while observing the structure of packets.

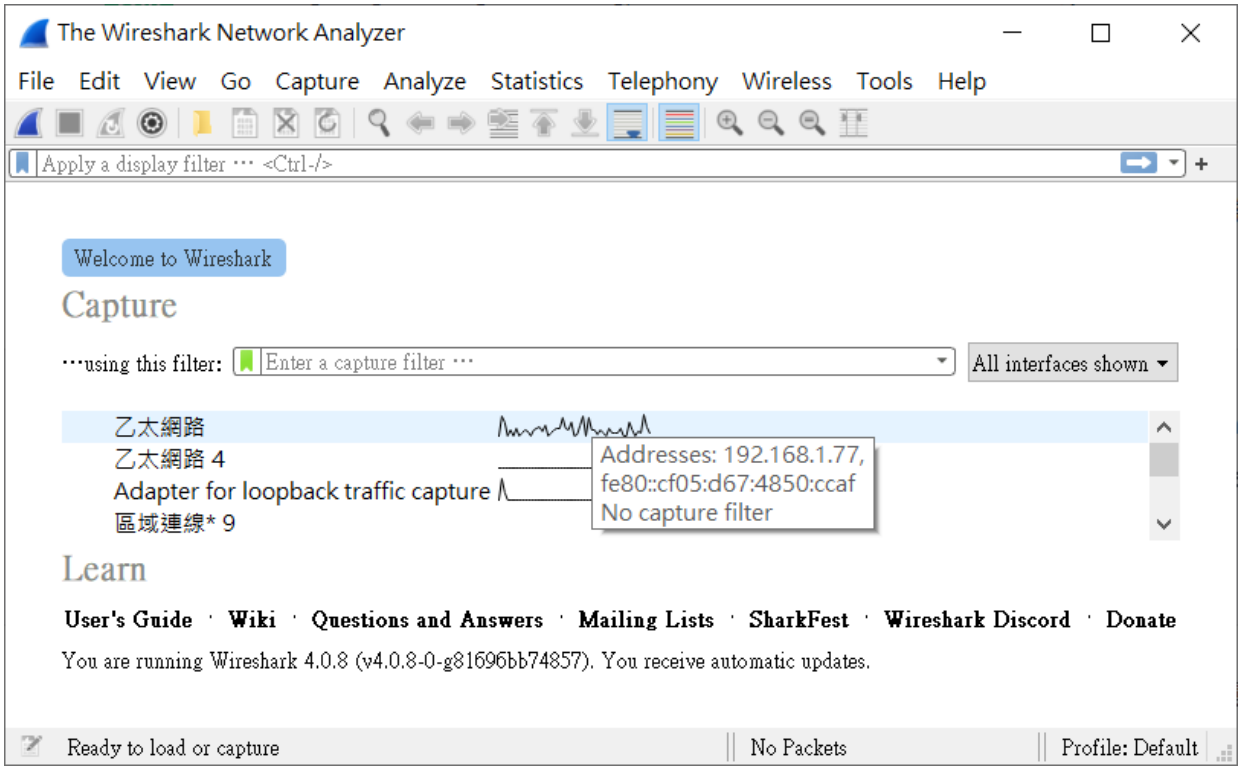
2. Install Wireshark

Visit https://www.wireshark.org/ and download the appropriate installation file for your OS.
If you are using Windows, the installation process will include Npcap, which is a packet capture library. Please follow the prompts to install it step by step.

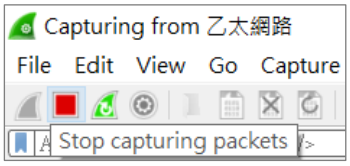
Before we start, we recommend you disable your VPN, proxy, antivirus, and ad-blocking software.

3. Capture HTTP Traffic

Open Wireshark and select the network interface you would like to capture.

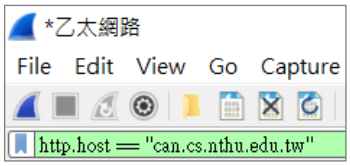


Next, open your web browser and access http://can.cs.nthu.edu.tw/. Then, return to the Wireshark and click the red stop button in the top left corner to stop capturing packets.

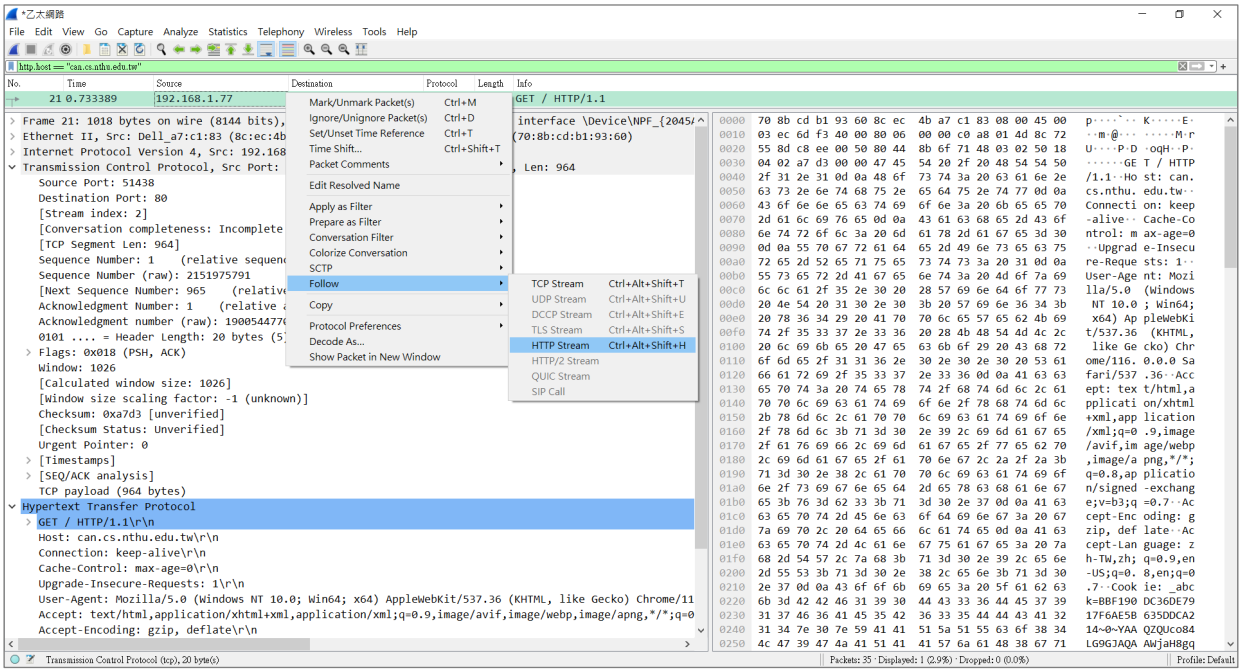


In the filter field, enter the rule:

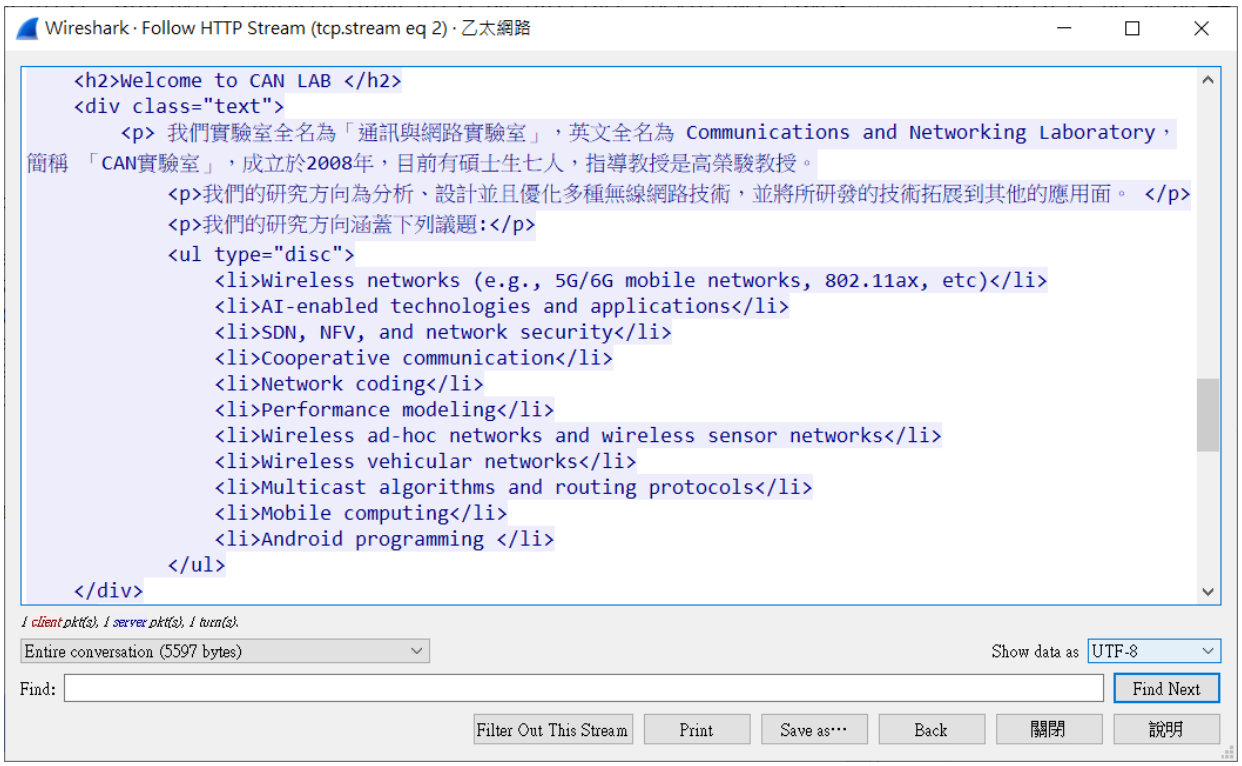
```
http.host == "can.cs.nthu.edu.tw"
```



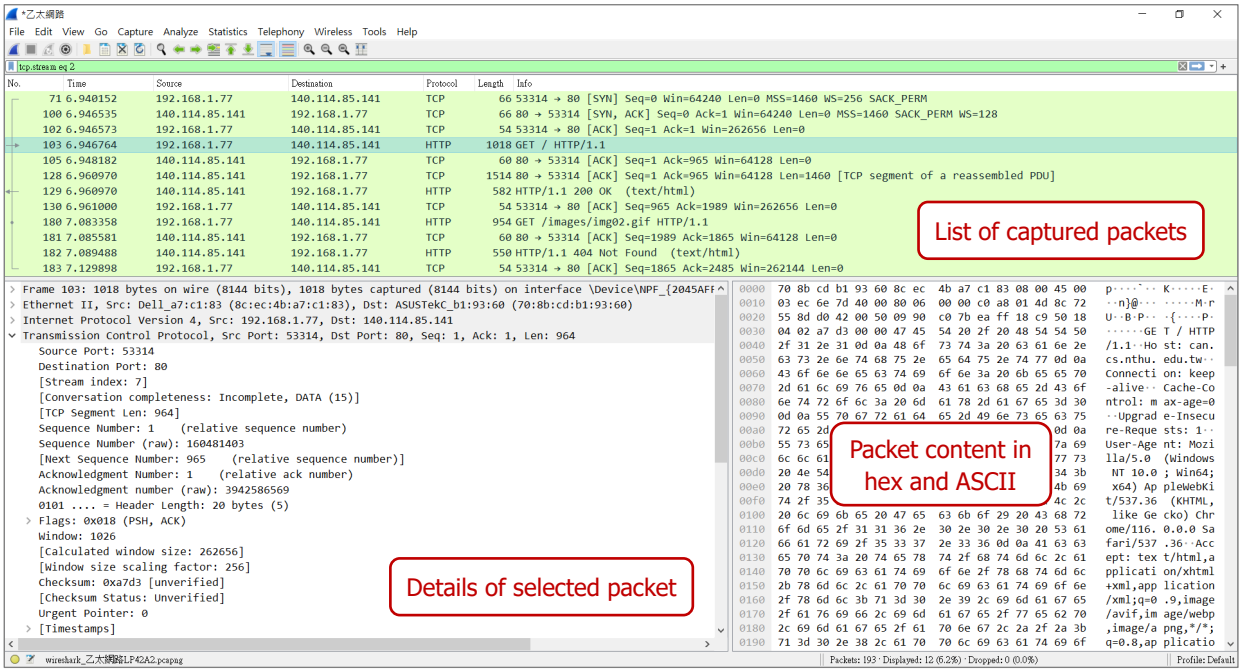
Find the record where the request is "`GET /`", which typically represents the main web page. Right-click on it, then select [Follow] → [HTTP Stream].



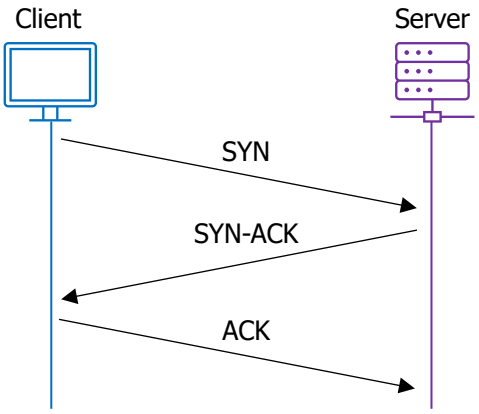
You will see the data of that HTTP Stream. The default encoding will be ASCII, so it won't be able to display Chinese characters. Please select [UTF-8] in [Show data as], and you will be able to view Chinese characters. Please note that some older web pages may use Big5 encoding.

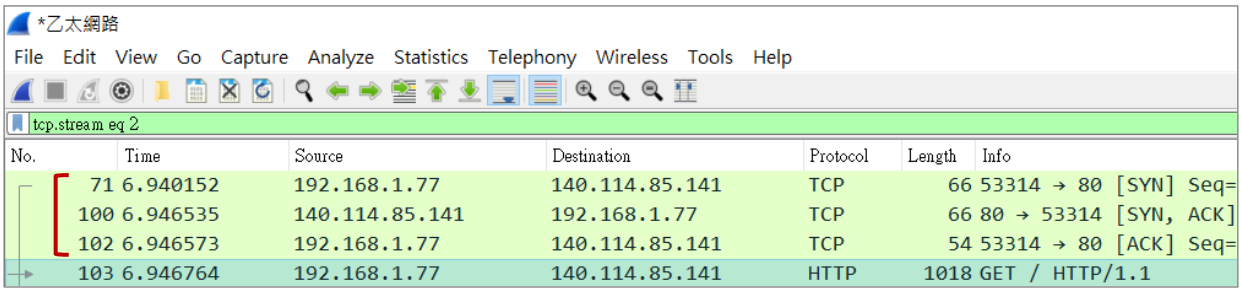


You will notice that the filter field changes to "`tcp.stream eq N`", and it will display packet records related to this specific stream.



We can observe that before the browser sends an HTTP GET request to the server, there are three packet records. These three packets are involved in what is known as the Three-way Handshake. The Three-way Handshake is a fundamental process that establishes a TCP connection between two devices. It involves three steps: SYN (synchronize), SYN-ACK (synchronize-acknowledge), and ACK (acknowledge), ensuring a reliable and synchronized connection setup.

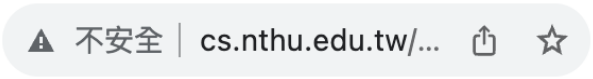




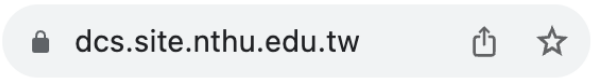
4. Capture HTTPS Traffic

The HTTPS protocol encrypts packets to secure our data transmission, so packets captured by Wireshark will be in ciphertext. To observe the contents of HTTPS packets, we need to get the SSL keys for decrypting the packets. Below are instructions on how to obtain SSL keys using Chrome.

HTTP “Not Secure” warning



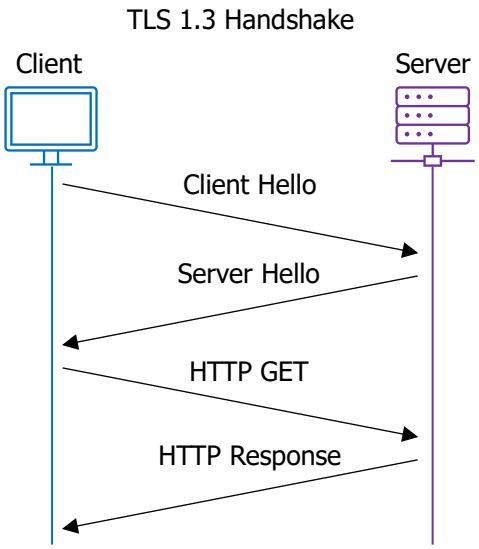
HTTPS lock icon



Although SSL (Secure Sockets Layer) has been deprecated, this term is still commonly used due to historical reasons. Except for a few outdated systems that still use SSL, the term SSL actually refers to TLS (Transport Layer Security) in most cases.

TLS handshake is a secure process for establishing a connection between a client and server. It begins with the client sending a “Client Hello” message, including supported cryptographic algorithms called cipher suites. The server selects a mutually supported cipher suite and responds with a “Server Hello” message. The client and server exchange key information and verify their identities.

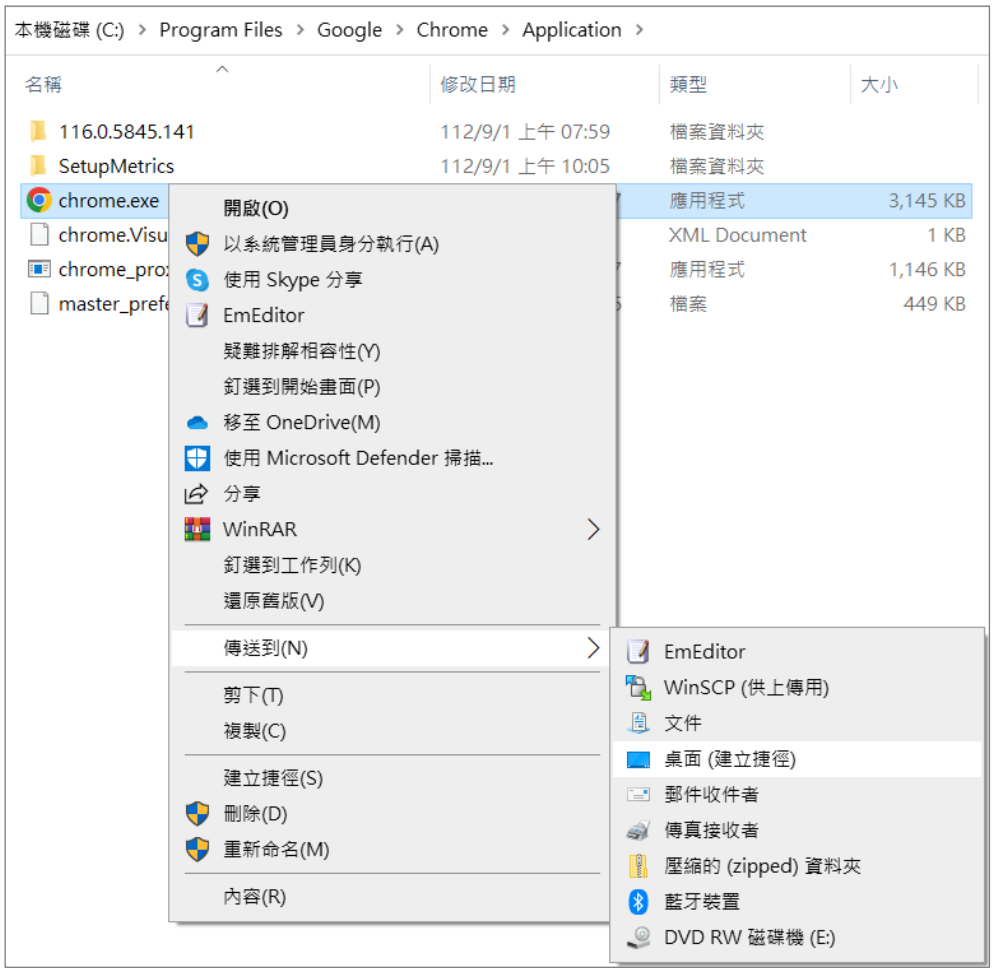
For different TLS versions, there may be some differences in details, but the fundamental concept of the TLS handshake remains as described above.



(1) Windows

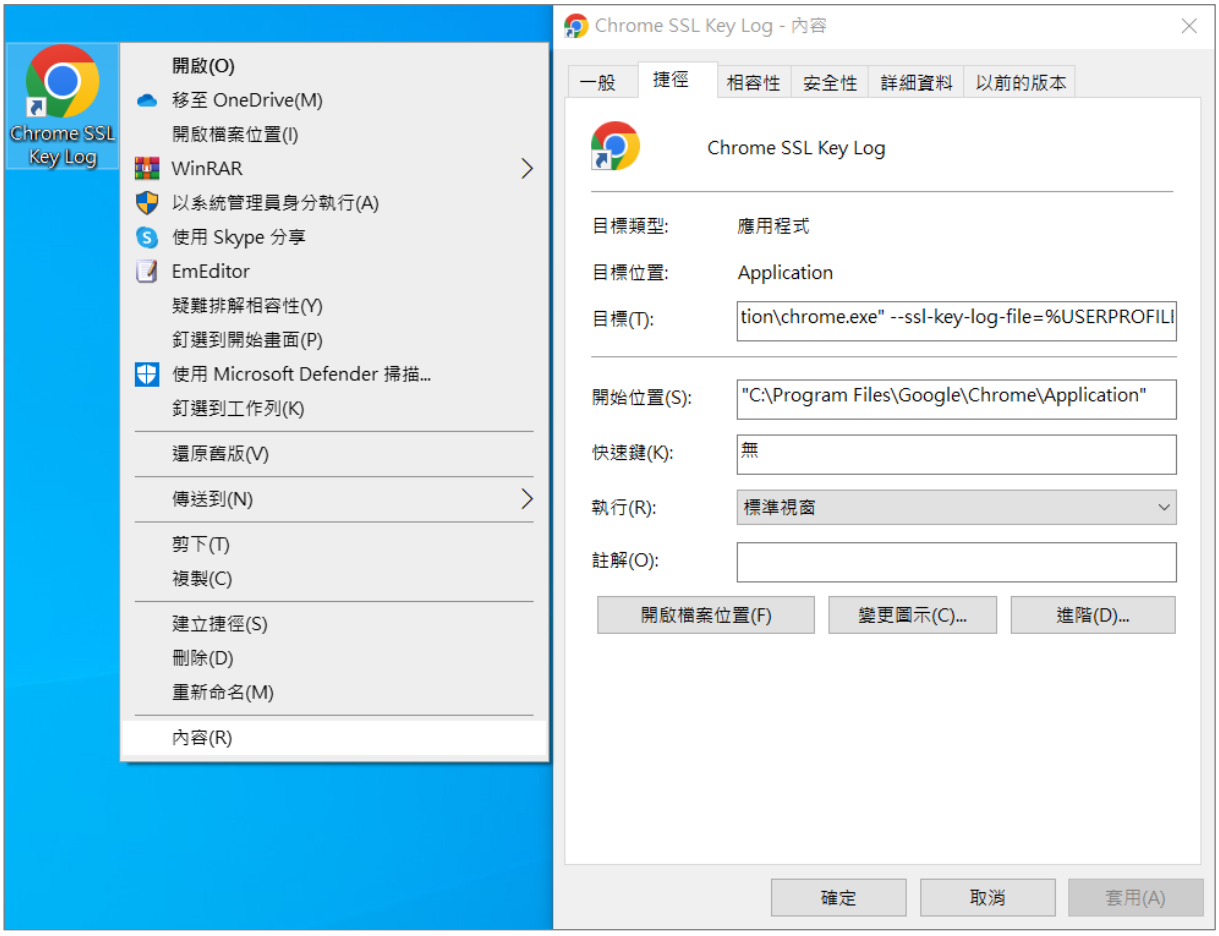
Most tutorials on capturing HTTPS packets with Wireshark involve setting the `SSLKEYLOGFILE` environment variable. However, we are concerned that you may forget to remove it after completing the assignment, potentially causing security risks. Therefore, we recommend launching Chrome with an argument called `--ssl-key-log-file`, as both methods achieve the same result.

Open the folder `C:\Program Files\Google\Chrome\Application` and right-click on chrome.exe, then select [Send to 傳送到] → [Desktop (create shortcut) 桌面 (建立捷徑)]. Rename the shortcut as “Chrome SSL Key Log”.



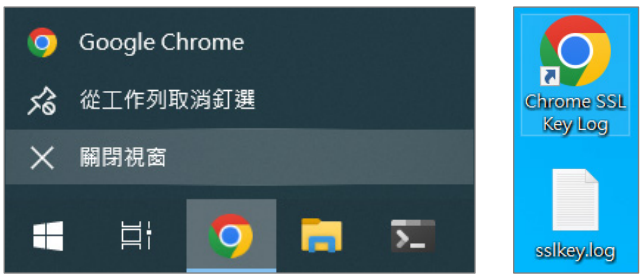
Right-click on the shortcut, click [Properties 內容] → [Shortcut 捷徑], and add the argument `--ssl-key-log-file` after the executable path in the [Target 目標] field (after the double quotes):

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --ssl-key-log-file=%USERPROFILE%\Desktop\sslkey.log
```

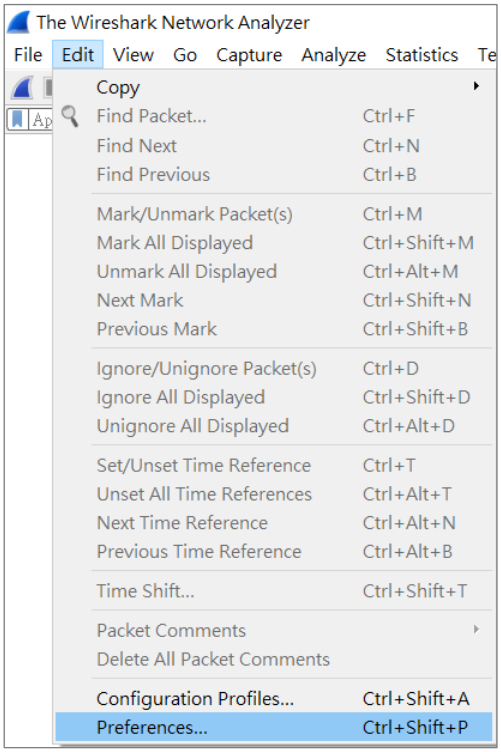


Before launching "Chrome SSL Key Log", make sure to completely close any existing Chrome instances. You can also check in the "Task Manager (工作管理員)" for any background Chrome processes to avoid issues such as no log output.

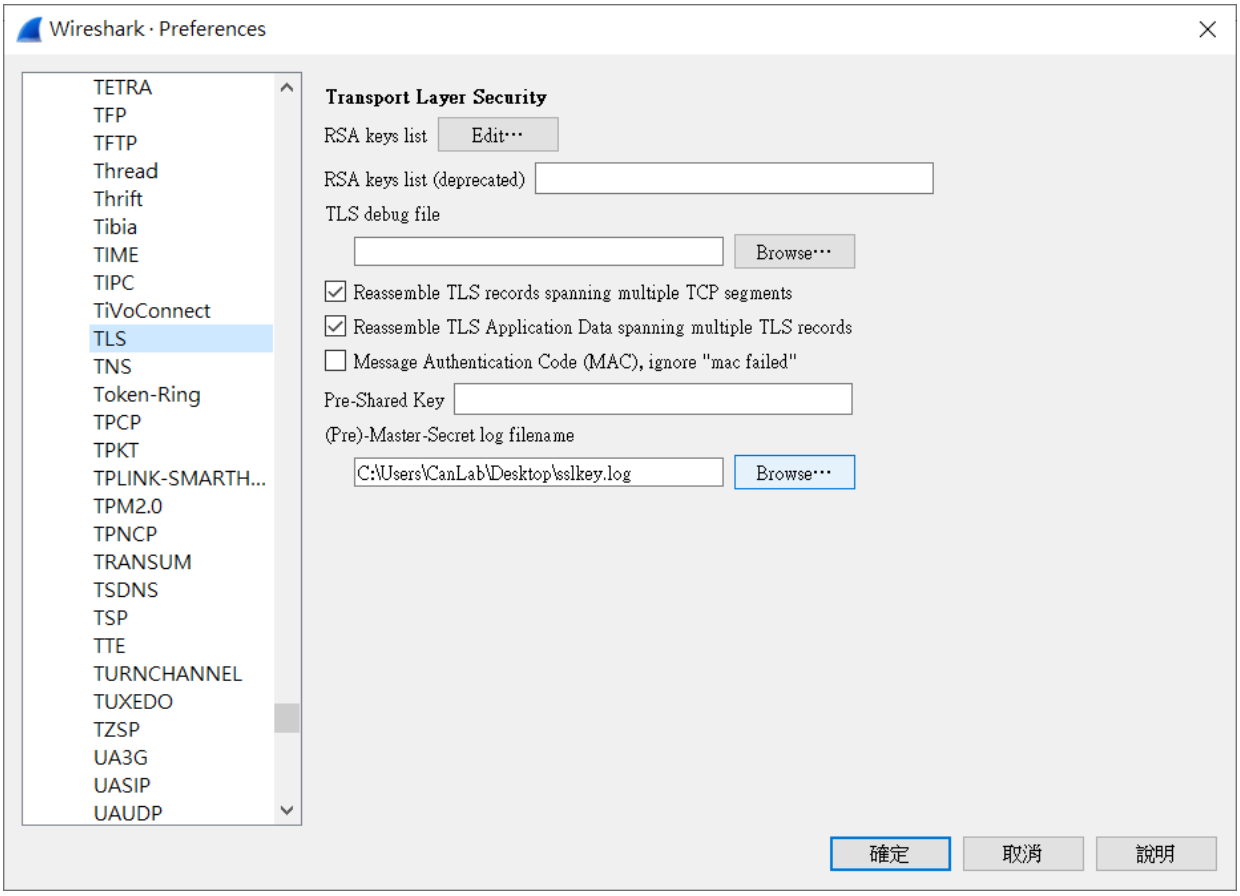
Next, double-click the Chrome SSL Key Log shortcut to launch Chrome. You will notice that it created a sslkey.log file on your desktop.



Open Wireshark and click [Edit] → [Preferences…].



Under [Protocols], choose [TLS], and in the [Pre-Master-Secret log filename] field, select the sslkey.log on your desktop.

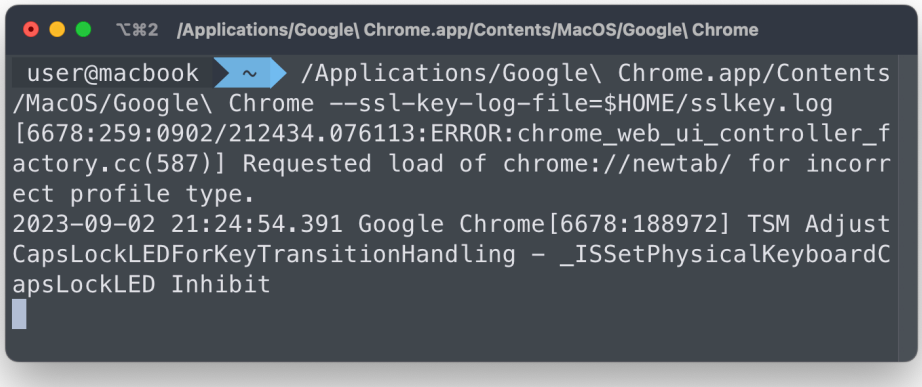


(2) macOS

Please make sure to fully close the existing Chrome. On macOS, closing the window does not actually quit the application; you need to press Command (⌘) + Q. If there is a “dot” underneath the icon in the dock, it means Chrome is still running in the background. Please right-click and quit it. You can also check in the “Activity Monitor (活動監視器)” for any background processes.

Open the terminal and enter the following command. The reason for using command-line arguments to launch an executable rather than relying solely on environment variables is that it provides a more intuitive way to check for error messages directly in the terminal. This makes debugging much easier.

```
/Applications/Google\ Chrome.app/Contents/MacOS/Google\ Chrome --ssl-key-log-file=$HOME/sslkey.log
```

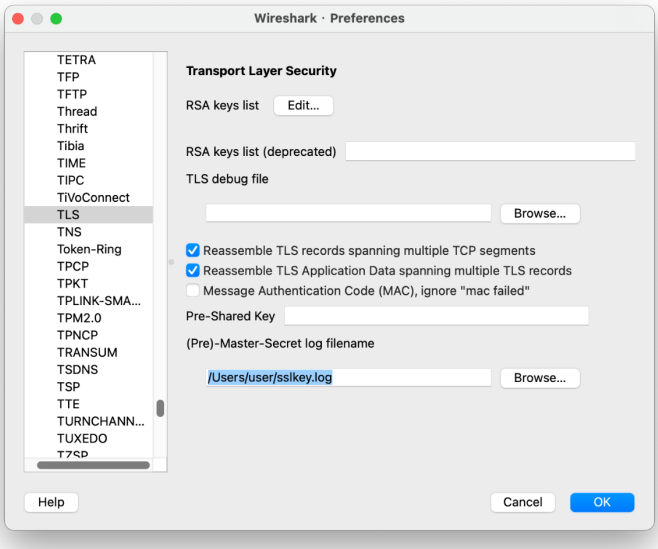


If you don’t want to see the messages displayed in the terminal output, you can also use one of the following two commands.

```
open -a "Google Chrome" --args --ssl-key-log-file=$HOME/sslkey.log
```

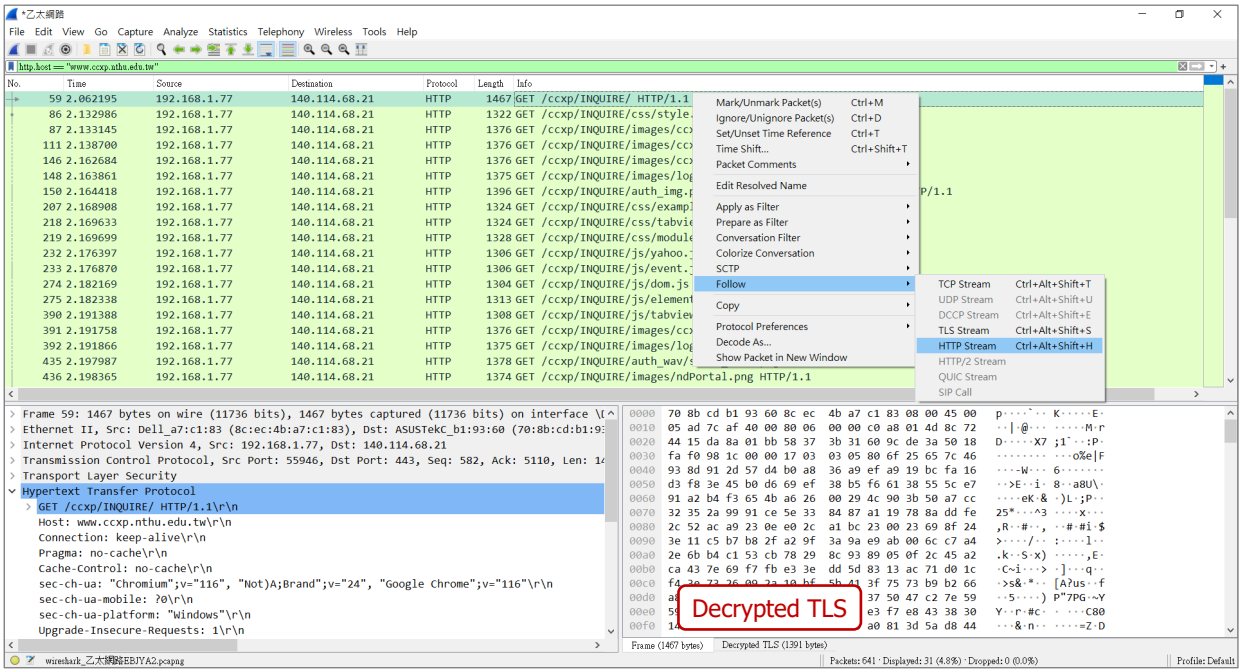
```
export SSLKEYLOGFILE=$HOME/sslkey.log && open -a "Google Chrome"
```

Open Wireshark and click [Wireshark] → [Preferences…]. Under [Protocols], choose [TLS], and in the [Pre-Master-Secret log filename] field, select the sslkey.log located in your home directory.

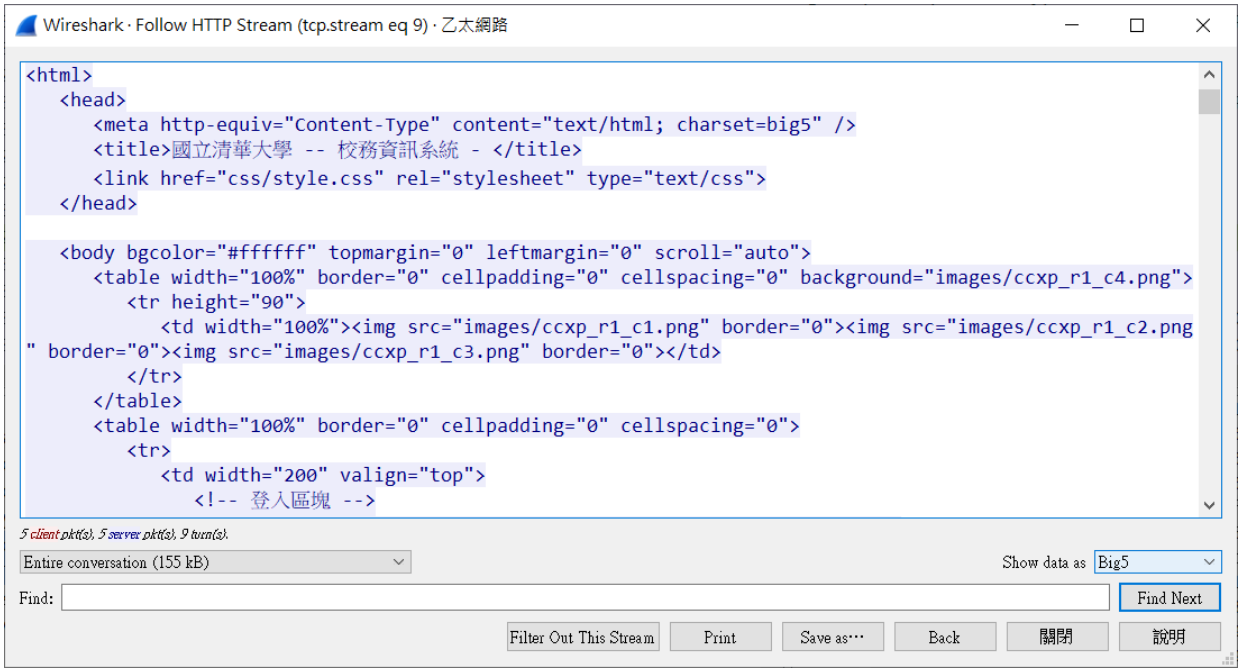


After configuring the TLS secret log path, we can open an HTTPS website to check if the packets can be decrypted. Start capturing and access https://www.ccxp.nthu.edu.tw/ccxp/INQUIRE/ using the Chrome browser that we configured earlier.

Using `http.host == "www.ccxp.nthu.edu.tw"` as the filtering condition, right-click on the main request record, and select [Follow] → [HTTP Stream]. You will also notice an additional [Decrypted TLS] tab appearing in the bottom.



We will be able to see that the packet data is decrypted and readable. Since the system uses the Big5 encoding, you can switch the encoding in the [Show data as] option in the bottom right corner to correctly display Chinese characters.



5. Problems

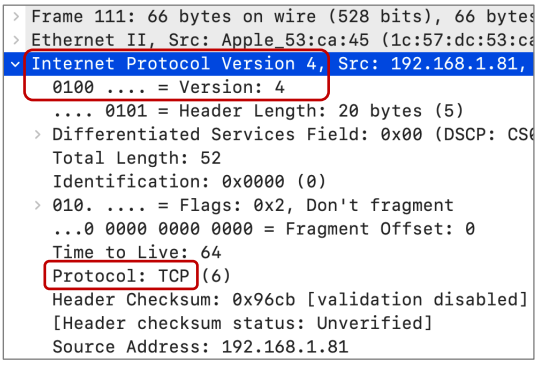
By looking at the information in the Wireshark, answer the following questions. Provide screenshots and highlight the message you found to indicate the information that addresses each question. For example:

Q: Which version of the Internet Protocol is used?

A: IPv4

Q: Which protocol is used, TCP or UDP?

A: TCP



(1) HTTP

Start capturing packets and access http://can.cs.nthu.edu.tw/contact.php

(a) What is your computer's IP address? (5%)

(b) What is the IP address of the domain can.cs.nthu.edu.tw? (5%)

(c) Which port number is used by the web server? (5%)

(d) What is the HTTP status code (a 3-digit integer) returned from the web server? (5%)
Briefly explain what does it mean? (5%)

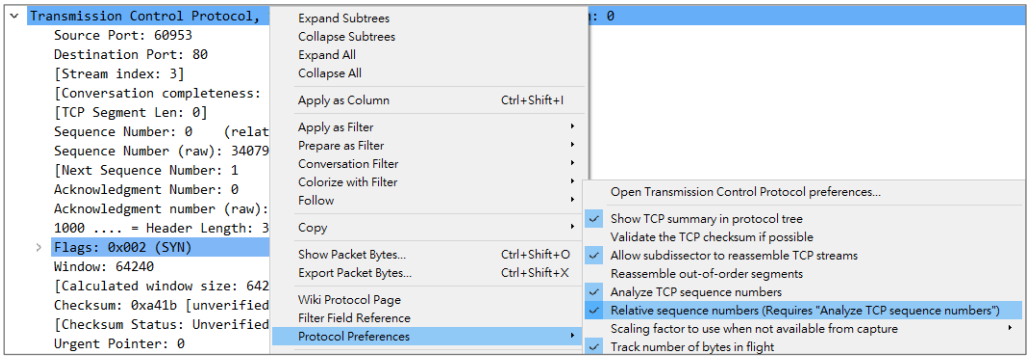
(e) Observe the sequence numbers and acknowledgment numbers in the three packets of the Three-way Handshake, and please provide the **raw values** rather than the relative values. (25%)

1: Client → Server	SEQ number (raw) = _____	
2: Server → Client	SEQ number (raw) = _____	ACK number (raw) = _____
3: Client → Server	SEQ number (raw) = _____	ACK number (raw) = _____

(f) Continuing from the previous question, observe the changes in the values and express the relationship between them using given x and y. (15%)

1: Client → Server	SEQ number = x	
2: Server → Client	SEQ number = y	ACK number = _____
3: Client → Server	SEQ number = _____	ACK number = _____

※ For older versions of Wireshark, if you are unable to see raw values and only see relative values, please right-click, select [Protocol Preferences], and uncheck [Relative sequence numbers].



(2) HTTPS

Start capturing packets and access https://www.ccxp.nthu.edu.tw/ccxp/INQUIRE/. Please enter guest as the username and your student ID as the password, click [Login (登入)], then observe the HTTP POST request. Logging in with the username "guest" does not require password authentication; using your student ID as the password is only for assignment verification purposes.

(a) Briefly explain why HTTPS is more secure than HTTP. (5%)

(b) What is the IP address of the domain www.ccxp.nthu.edu.tw? (5%)

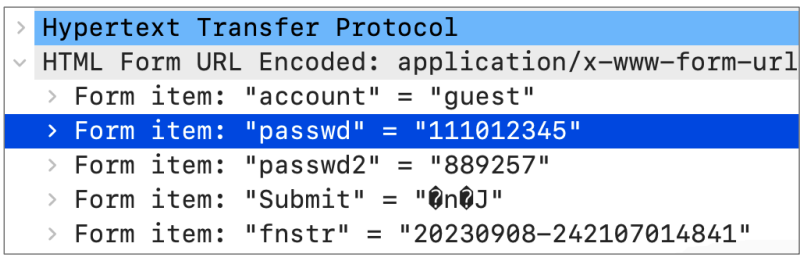
(c) Which port number is used by the HTTPS web server? (5%)

(d) Which security protocol is used, TLS or SSL? (5%)

(e) How many cipher suites does your browser offer for the server to choose from? (5%)
(Hint: in the "Client Hello" message)

(f) Which cipher suite has the server selected to use? (5%)
(Hint: in the "Server Hello" message)

(g) Locate the HTTP POST request packet with the form data and provide a clear screenshot while highlighting your student ID, as shown in the example below: (5%)



In this context, the value of "Submit" appears as gibberish, but you can just ignore it; this is caused by the Big5 encoding resulting in garbled characters.

6. Submission

(a) Please organize your answers and screenshots (clearly marked or highlighted with the corresponding answers) into a PDF file named studentID_lab1.pdf (e.g., 111012345_lab1.pdf)

(b) Upload your PDF file to eeclass.

(c) Discussion is encouraged, but plagiarism is strictly prohibited. Any instances of plagiarism will result in a score of 0.

(d) Make sure to upload your PDF file before the deadline. Late submissions will not be accepted, and a score of 0 will be assigned.