Wireshark Lab #1, Intro

He Tianyang, 3022001441

September 20, 2024

Problem 1.Protocols

List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Solves:

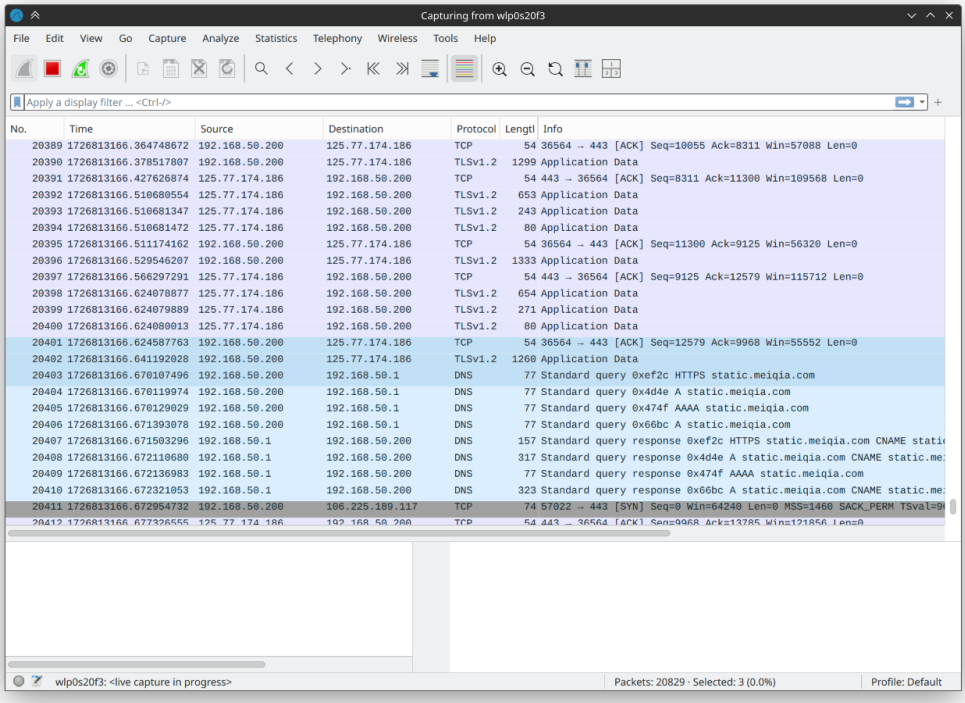

Figure 1: The protocol column in the unfiltered packet-listing window

Open Wireshark and wait for the packet sniffer to start. The three protocols that appear in the protocol column are

1. DNS

2. HTTP
3. TLSv1.2

The details are showned in the Fig. 1:

Problem 2. Request Timing

> How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

Solves:

I used the Linux command `curl` to send a simple HTTP request and observed the updates in Wireshark.

```
curl www.baidu.com
```

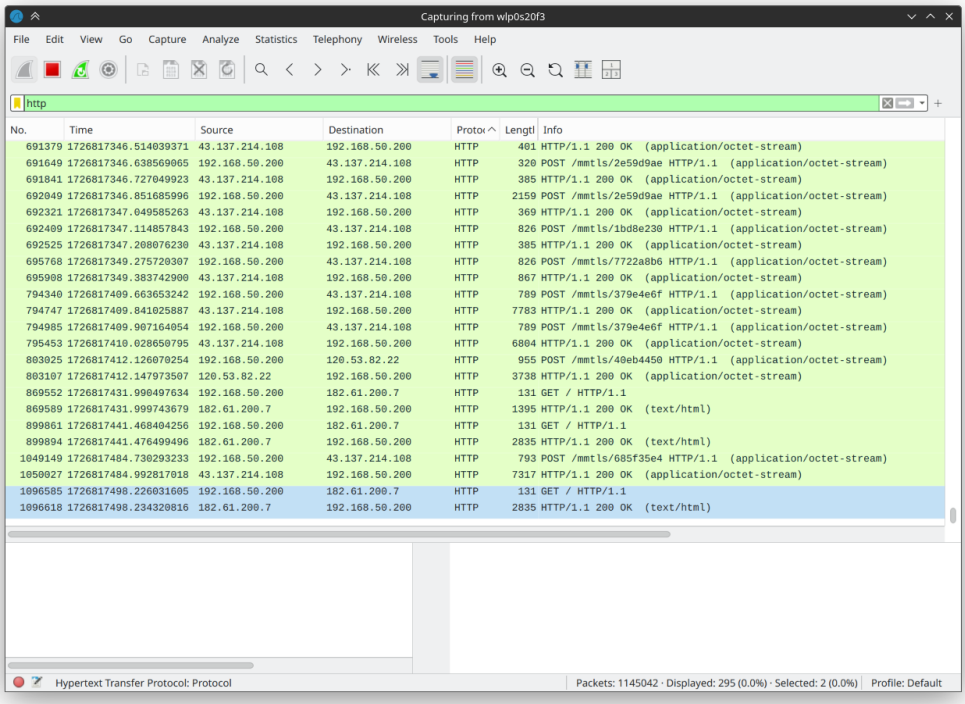

Figure 2: The time from HTTP GET to HTTP OK

There are two rows in the packet-listing window: one represents the HTTP GET request, and the other shows the HTTP OK reply. By observing the time column for these two rows, we can

measure the time difference, which is the duration from the HTTP GET to HTTP OK response. The result is shown in Fig. 2.

The time column displays the timestamp of each packet, based on the configured settings. It represents the total number of seconds since 1970-01-01 00:00:00 UTC.

Therefore, the time from HTTP GET to HTTP OK can be calculated as:

$$\begin{aligned} t_{GET-OK} &= t_{OK} - t_{GET} \\ &= 1726817498.234320816\ \mathbf{s} - 1726817498.226031605\ \mathbf{s} \\ &\boxed{= 0.008289211\ \mathbf{s}} \end{aligned}$$

Problem 3. Internet Address

> What is the Internet address of the gaia.cs.umass.edu
> (also known as www-net.cs.umass.edu)?
> What is the Internet address of your computer?

Solves:

Also, use the `curl` command to send a simple HTTP request:

```
curl gaia.cs.umass.edu
```

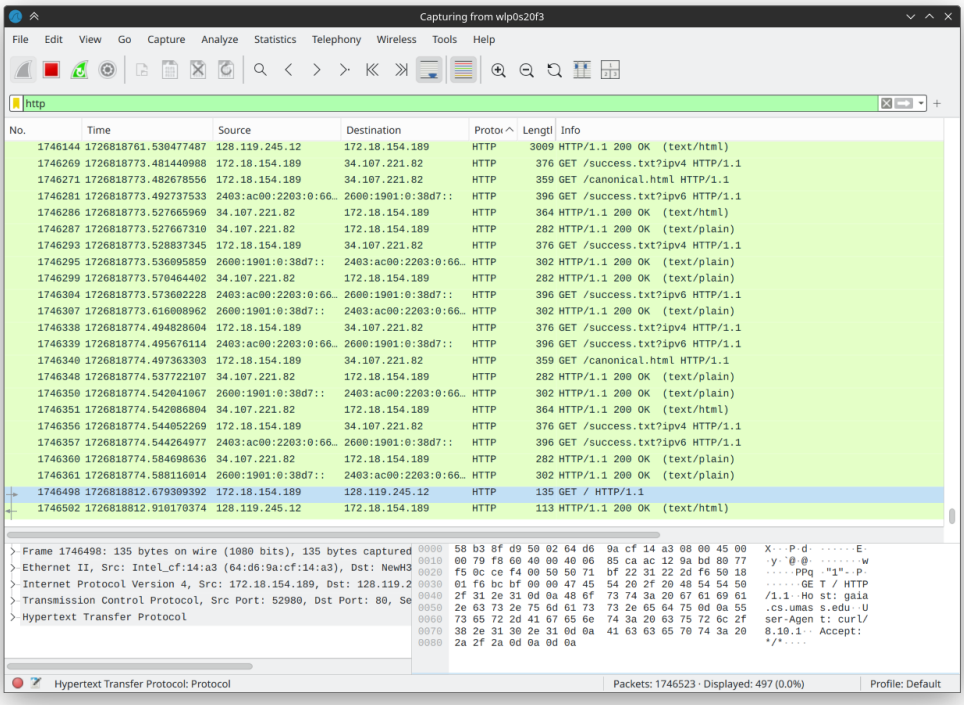

Figure 3: Internet Address

We can observe the source and destination columns.

It shows that the source is `172.18.154.189`, and the destination is `128.119.245.12`. Therefore, the Internet address of that website is `128.119.245.12`, and the Internet address of my computer is `172.18.154.189`, which is a `LAN` address.

Problem 4. Print HTTP messages

> Print the two HTTP messages (GET and OK) referred to in question 2 above To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.

Solves:

Follow the instructions, and you will get a menu similar to Fig. 4. Press `OK` to confirm the operation.

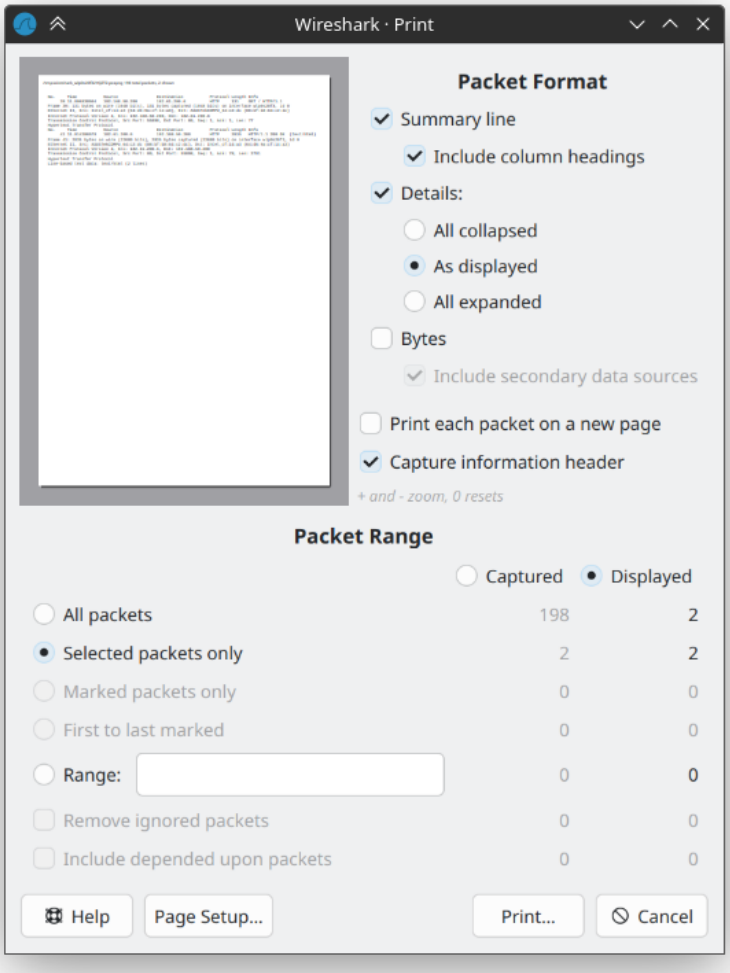

Figure 4: Print HTTP messages

And choose `Print to PDF` as the printer. This will generate a PDF file as shown in Fig. 5."

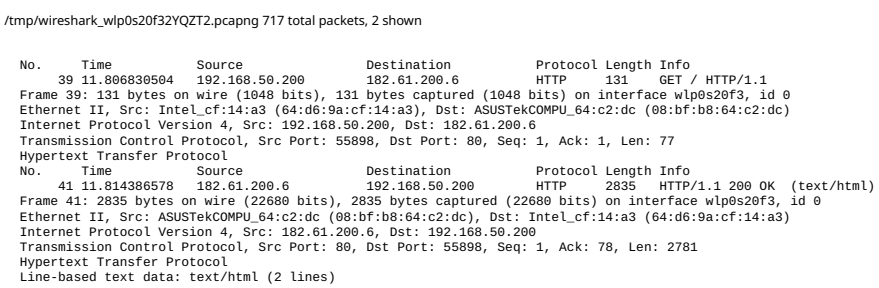

Figure 5: Print Result