

Wireshark Lab #1, Intro

He Tianyang, 3022001441

September 25, 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:

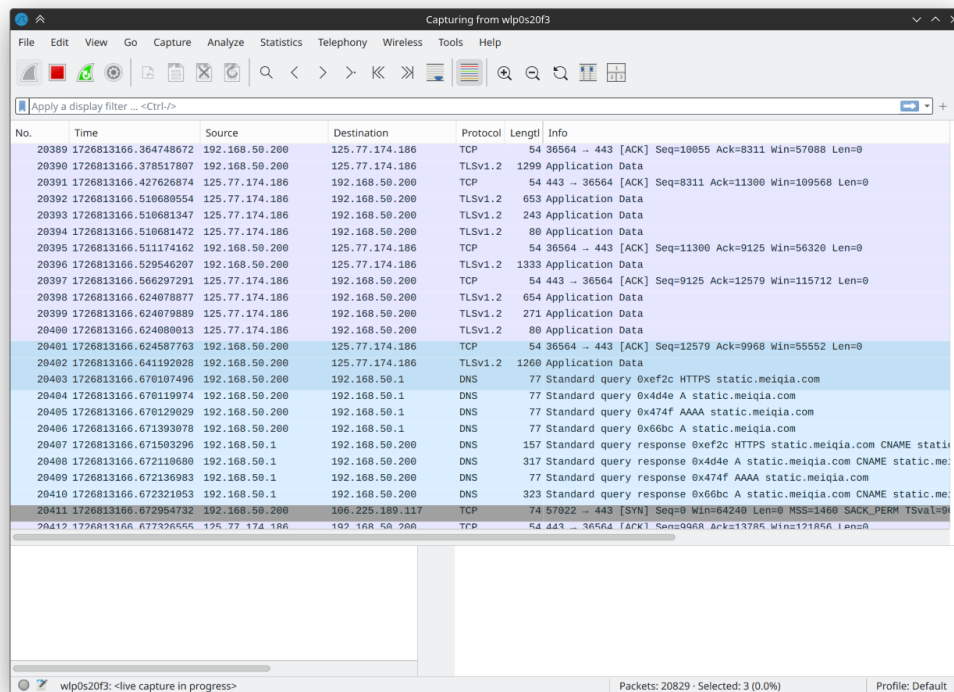


Figure 1: The protocol column in the unfiltered packet-listing window

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
```

No.	Time	Source	Destination	Protocol	Length	Info
691379	1726817346.514039371	43.137.214.108	192.168.50.200	HTTP	401	HTTP/1.1 200 OK (application/octet-stream)
691649	1726817346.638569065	192.168.50.200	43.137.214.108	HTTP	320	POST /mmtls/2e59d9ae HTTP/1.1 (application/octet-stream)
691841	1726817346.727049923	43.137.214.108	192.168.50.200	HTTP	385	HTTP/1.1 200 OK (application/octet-stream)
692049	1726817346.851685996	192.168.50.200	43.137.214.108	HTTP	2159	POST /mmtls/2e59d9ae HTTP/1.1 (application/octet-stream)
692321	1726817347.049585263	43.137.214.108	192.168.50.200	HTTP	369	HTTP/1.1 200 OK (application/octet-stream)
692499	1726817347.114857843	192.168.50.200	43.137.214.108	HTTP	826	POST /mmtls/1bd8e230 HTTP/1.1 (application/octet-stream)
692525	1726817347.208072630	43.137.214.108	192.168.50.200	HTTP	385	HTTP/1.1 200 OK (application/octet-stream)
695768	1726817349.275728307	192.168.50.200	43.137.214.108	HTTP	826	POST /mmtls/7722a8b6 HTTP/1.1 (application/octet-stream)
695988	1726817349.383742900	43.137.214.108	192.168.50.200	HTTP	867	HTTP/1.1 200 OK (application/octet-stream)
794340	1726817409.663653242	192.168.50.200	43.137.214.108	HTTP	789	POST /mmtls/379e4eef HTTP/1.1 (application/octet-stream)
794747	1726817409.841025887	43.137.214.108	192.168.50.200	HTTP	7783	HTTP/1.1 200 OK (application/octet-stream)
794985	1726817409.907164054	192.168.50.200	43.137.214.108	HTTP	789	POST /mmtls/379e4eef HTTP/1.1 (application/octet-stream)
795453	1726817410.028658795	43.137.214.108	192.168.50.200	HTTP	6804	HTTP/1.1 200 OK (application/octet-stream)
803025	1726817412.126070254	192.168.50.200	120.53.82.22	HTTP	955	POST /mmtls/48eb4450 HTTP/1.1 (application/octet-stream)
803107	1726817412.147973507	120.53.82.22	192.168.50.200	HTTP	3738	HTTP/1.1 200 OK (application/octet-stream)
809552	1726817431.998497634	192.168.50.200	182.61.208.7	HTTP	131	GET / HTTP/1.1
809589	1726817431.999743679	182.61.208.7	192.168.50.200	HTTP	1395	HTTP/1.1 200 OK (text/html)
809861	1726817441.468484256	192.168.50.200	182.61.208.7	HTTP	131	GET / HTTP/1.1
809894	1726817441.476499496	182.61.208.7	192.168.50.200	HTTP	2835	HTTP/1.1 200 OK (text/html)
1049149	1726817484.738293233	192.168.50.200	43.137.214.108	HTTP	793	POST /mmtls/685f35e4 HTTP/1.1 (application/octet-stream)
1050027	1726817484.992817018	43.137.214.108	192.168.50.200	HTTP	7317	HTTP/1.1 200 OK (application/octet-stream)
1096585	1726817498.226031605	192.168.50.200	182.61.208.7	HTTP	131	GET / HTTP/1.1
1096618	1726817498.234328816	182.61.208.7	192.168.50.200	HTTP	2835	HTTP/1.1 200 OK (text/html)

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:

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

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
```

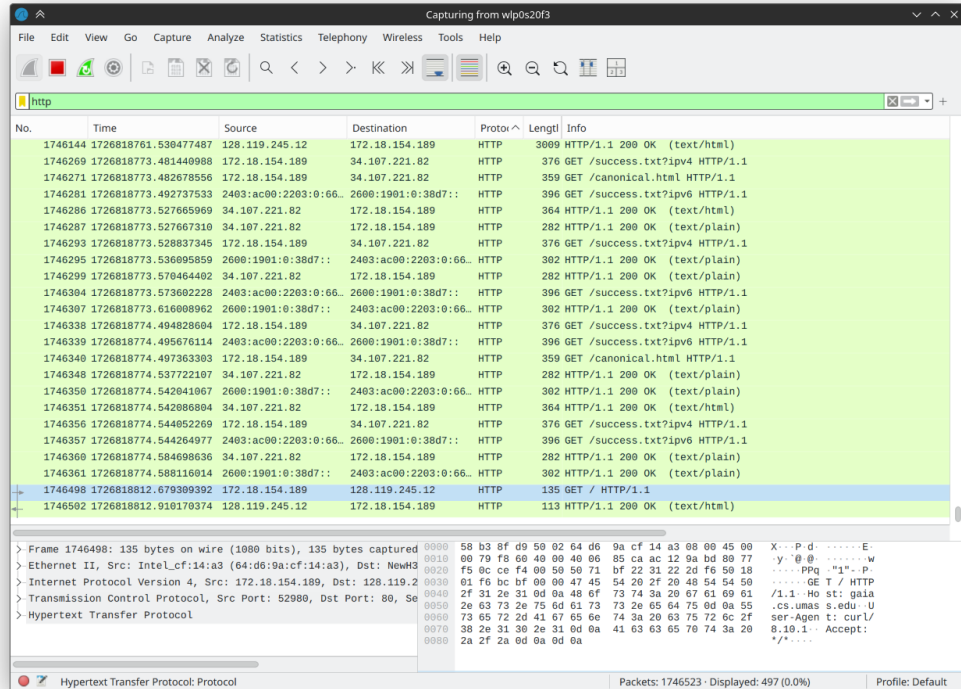


Figure 3: Internet Address

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.

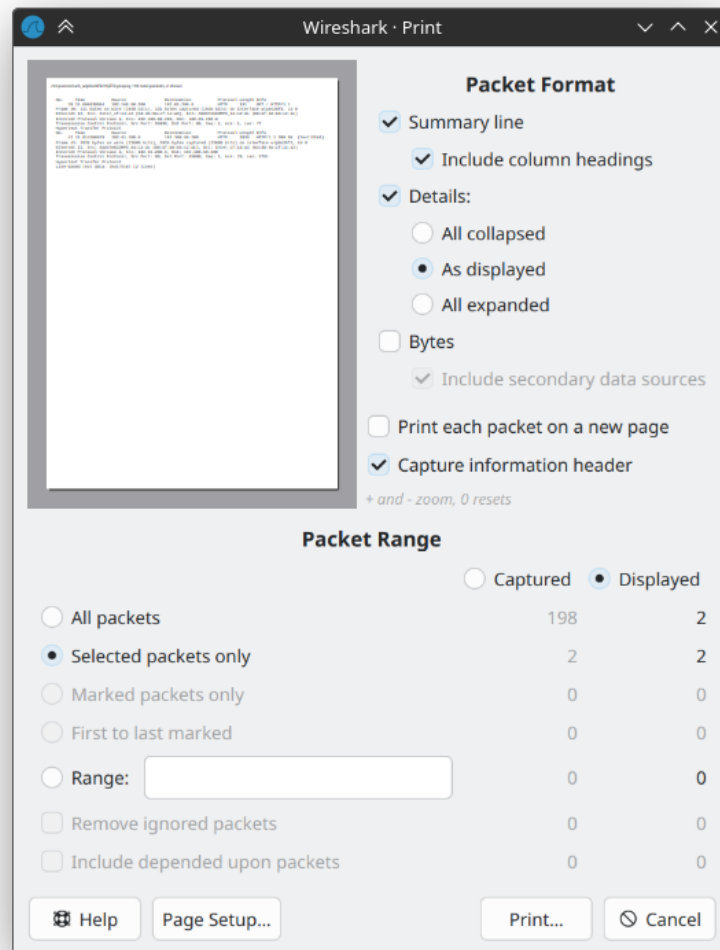


Figure 4: Print HTTP messages

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

```
/tmp/wireshark_wlp0s20f32YQZT2.pcapng 717 total packets, 2 shown

No.      Time                Source                Destination            Protocol Length Info
 39 11.806830504      192.168.50.200        182.61.200.6           HTTP      131    GET / HTTP/1.1
Frame 39: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: Intel_cf:14:a3 (64:d6:9a:cf:14:a3), Dst: ASUSTekCOMPU_64:c2:dc (08:bf:b8:64:c2:dc)
Internet Protocol Version 4, Src: 192.168.50.200, Dst: 182.61.200.6
Transmission Control Protocol, Src Port: 55898, Dst Port: 80, Seq: 1, Ack: 1, Len: 77
Hypertext Transfer Protocol

No.      Time                Source                Destination            Protocol Length Info
 41 11.814386578      182.61.200.6          192.168.50.200        HTTP      2835   HTTP/1.1 200 OK (text/html)
Frame 41: 2835 bytes on wire (22680 bits), 2835 bytes captured (22680 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: ASUSTekCOMPU_64:c2:dc (08:bf:b8:64:c2:dc), Dst: Intel_cf:14:a3 (64:d6:9a:cf:14:a3)
Internet Protocol Version 4, Src: 182.61.200.6, Dst: 192.168.50.200
Transmission Control Protocol, Src Port: 80, Dst Port: 55898, Seq: 1, Ack: 78, Len: 2781
Hypertext Transfer Protocol
Line-based text data: text/html (2 lines)
```

Figure 5: Print Result