

# In Class 4 : HTTP Lab1

- Exercise นี้นำมายจาก HTTP Lab ของ Kurose

Computer lab .....224

LAN หรือ WiFi (ให้ใช้ network สถาบัน) .....LAN

Section .....1 ..... Group Name .....Lan

รหัสนักศึกษา .....65050368 ..... ชื่อ สกุล .....ชนลักษณ์ เกิดปี戌

เครื่องคอมพิวเตอร์ที่ใช้ (หมายเลขครุภัณฑ์) .....65091.7440-29-01-0029

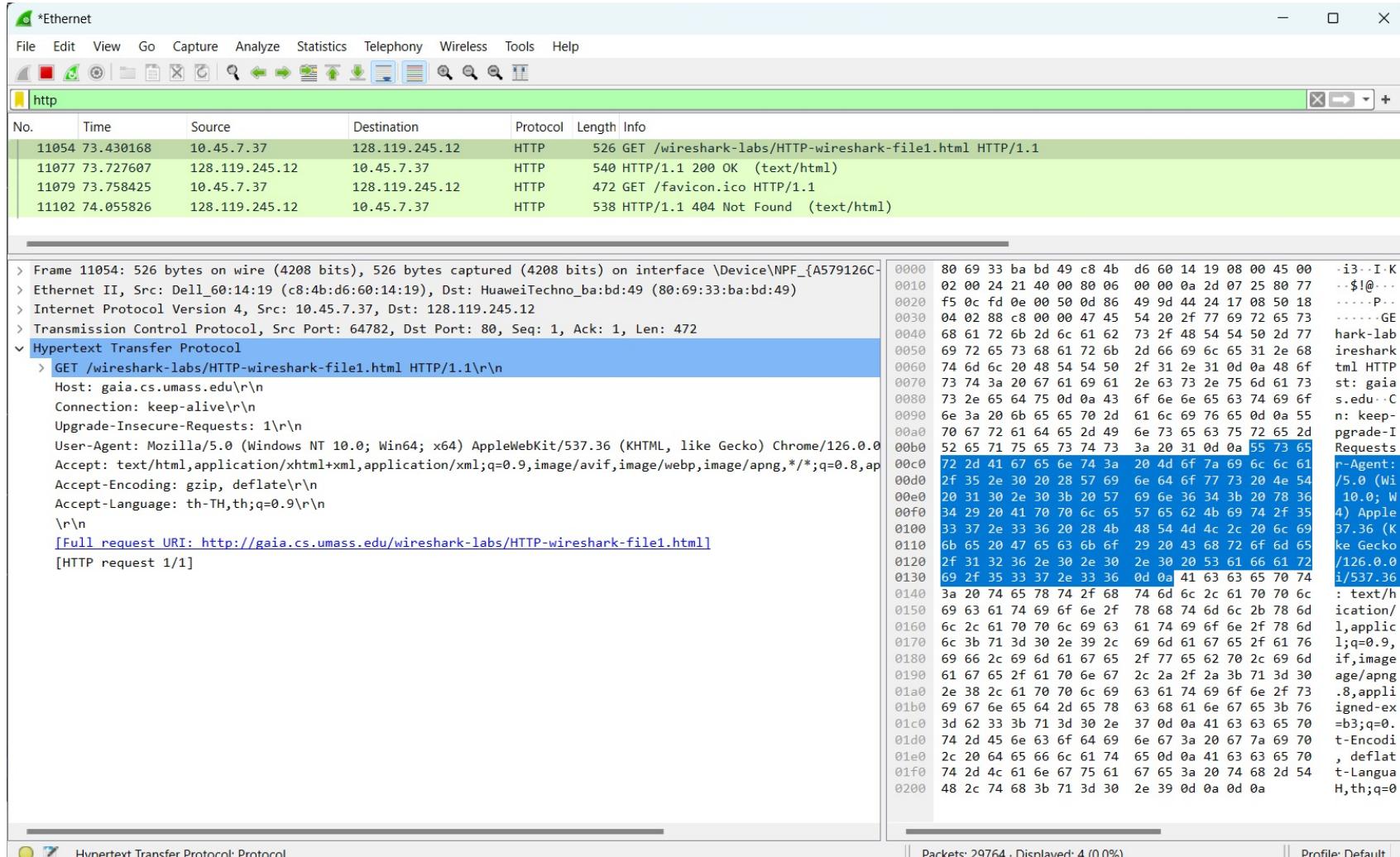
หมายเลข IP ของเครื่องที่นักศึกษาใช้ (CIDR Format) .....10.45.7.37

MAC Address ของเครื่องนักศึกษา .....C8-4B-D6-60-14-19

# A. Instruction

1. Start up your web browser.
2. Start up the Wireshark packet sniffer, as described in the Introductory lab (but don't yet begin packet capture).
  - Enter “http” (just the letters, not the quotation marks, and in lower case) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).
3. Wait a bit more than one minute (we'll see why shortly), and then begin Wireshark packet capture.
4. Enter the following to your browser  
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>  
Your browser should display the very simple, one-line HTML file.
5. Stop Wireshark packet capture.

# A1. Capture หน้าจอ Wireshark ของนักศึกษา (หน้าตาประมาณนี้) แล้ว Copy ทั้งรูปนี้เลยค่ะ => HTTP Request



# A2. Capture នៃការ Wireshark ទូទៅនៃកម្រិត = > HTTP Response

The screenshot shows the Wireshark interface with the following details:

- Panels:** Top: \*Ethernet menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help). Bottom: Line-based text data (data-text-lines), 0 bytes(s) selected.
- Packet List:** Shows four captured packets:
  - 11054: 73.430168, Source: 10.45.7.37, Destination: 128.119.245.12, Protocol: HTTP, Info: 526 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  - 11077: 73.727607, Source: 128.119.245.12, Destination: 10.45.7.37, Protocol: HTTP, Info: 540 HTTP/1.1 200 OK (text/html)
  - 11079: 73.758425, Source: 10.45.7.37, Destination: 128.119.245.12, Protocol: HTTP, Info: 472 GET /favicon.ico HTTP/1.1
  - 11102: 74.055826, Source: 128.119.245.12, Destination: 10.45.7.37, Protocol: HTTP, Info: 538 HTTP/1.1 404 Not Found (text/html)
- Details:** Shows the expanded details for the 540 OK response. It includes:
  - Frame 11077: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF\_{A579126C}
  - Ethernet II, Src: HuaweiTechno\_ba:bd:49 (80:69:33:ba:bd:49), Dst: Dell\_60:14:19 (c8:4b:d6:60:14:19)
  - Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.45.7.37
  - Transmission Control Protocol, Src Port: 80, Dst Port: 64782, Seq: 1, Ack: 473, Len: 486
  - Hypertext Transfer Protocol
    - HTTP/1.1 200 OK\r\nDate: Tue, 23 Jul 2024 04:54:23 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3\r\nLast-Modified: Mon, 22 Jul 2024 05:59:01 GMT\r\nETag: "80-61dcfbdea7fbb"\r\nAccept-Ranges: bytes\r\nContent-Length: 128\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/2]  
[Time since request: 0.297439000 seconds]  
[Request in frame: 11054]  
[Next request in frame: 11079]  
[Next response in frame: 11102]  
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]  
File Data: 128 bytes
- Bytes:** Shows the raw hex and ASCII representation of the captured data, corresponding to the selected packet.

# A3. ตอบคำถามต่อไปนี้ พร้อมนำคำตอบไปเติมใน Sheet

1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?

Client and Server : HTTP 1.1

2. What languages (if any) does your browser indicate that it can accept to the server?

th-TH, th; q=0.9

3. What is the IP address of your computer? What is the IP address of the gaia.cs.umass.edu server?

Client: 128.119.245.12 | Server: 10.45.7.57

4. What is the status code returned from the server to your browser?

200 OK

5. When was the HTML file that you are retrieving last modified at the server?

Mon 22 Jul 2024 05:59:01 GMT

6. How many bytes of content are being returned to your browser?

128

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

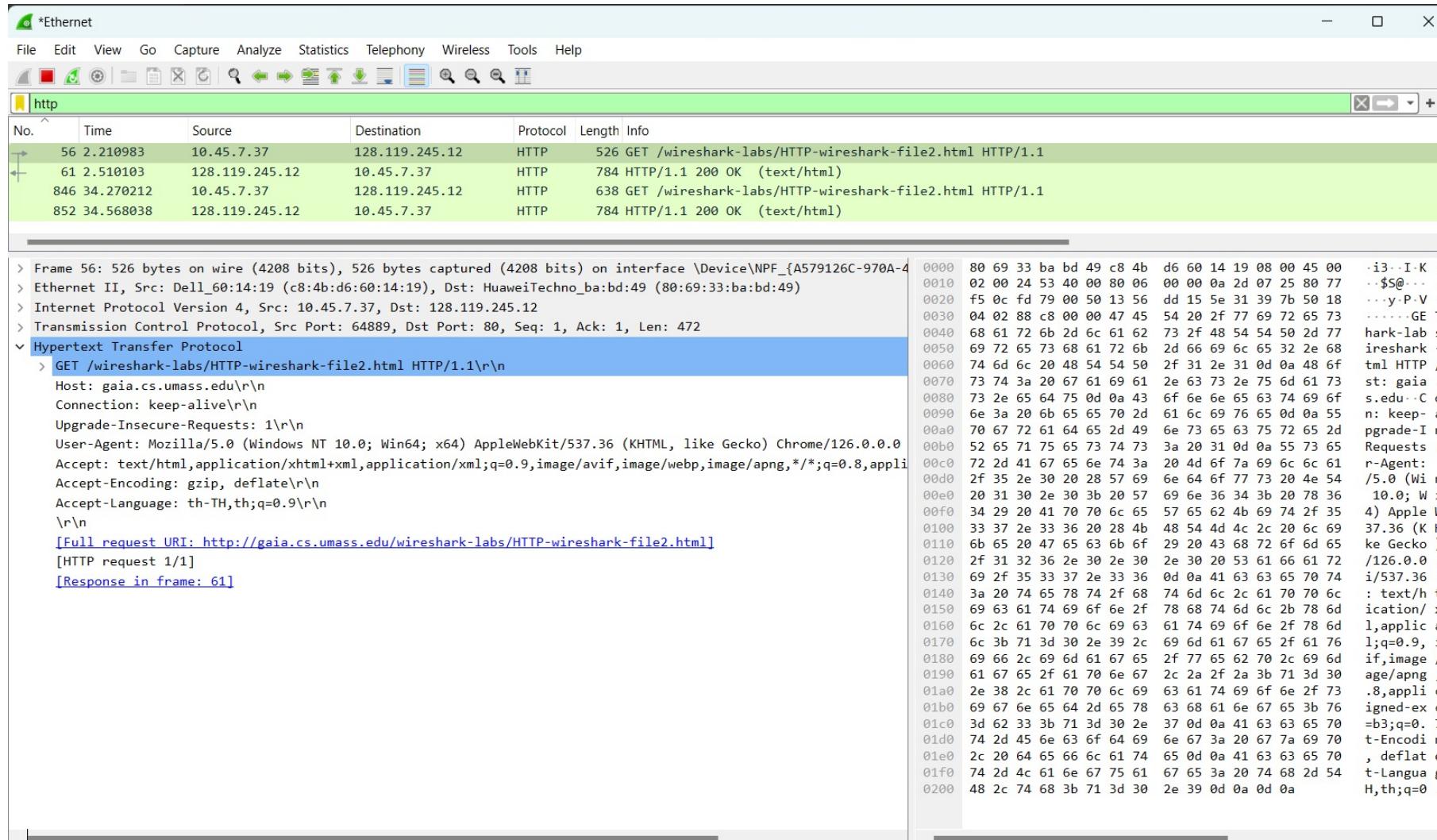
ไม่พบ

## B. The HTTP CONDITIONAL GET/response interaction

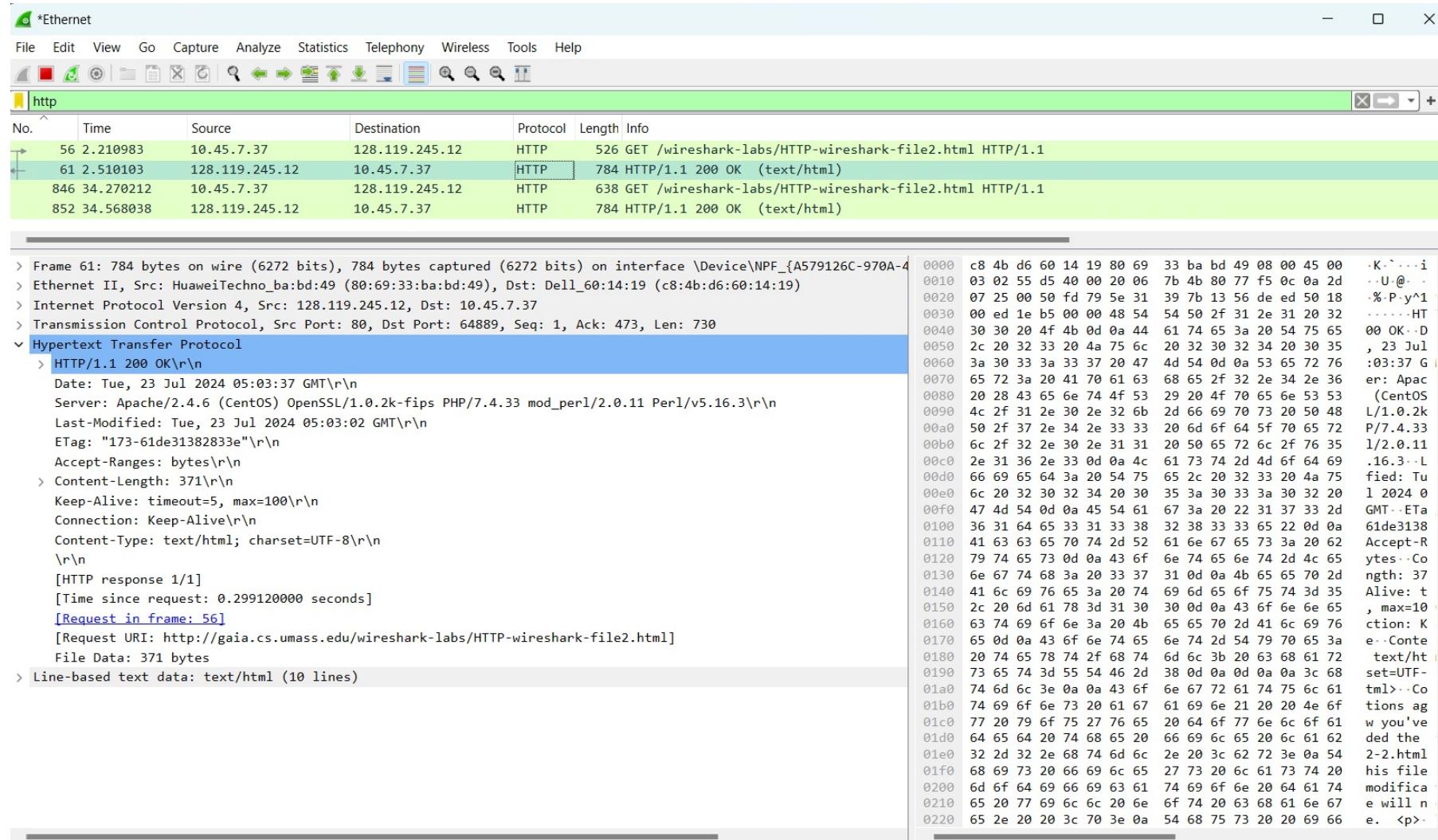
### Instruction

1. Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
2. Start up the Wireshark packet sniffer
3. Enter the following URL into your browser  
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>  
Your browser should display a very simple five-line HTML file.
4. Quickly enter the same URL into your browser again (or simply select the refresh button on your browser)
5. Stop Wireshark packet capture, and enter “http” (again, in lower case without the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

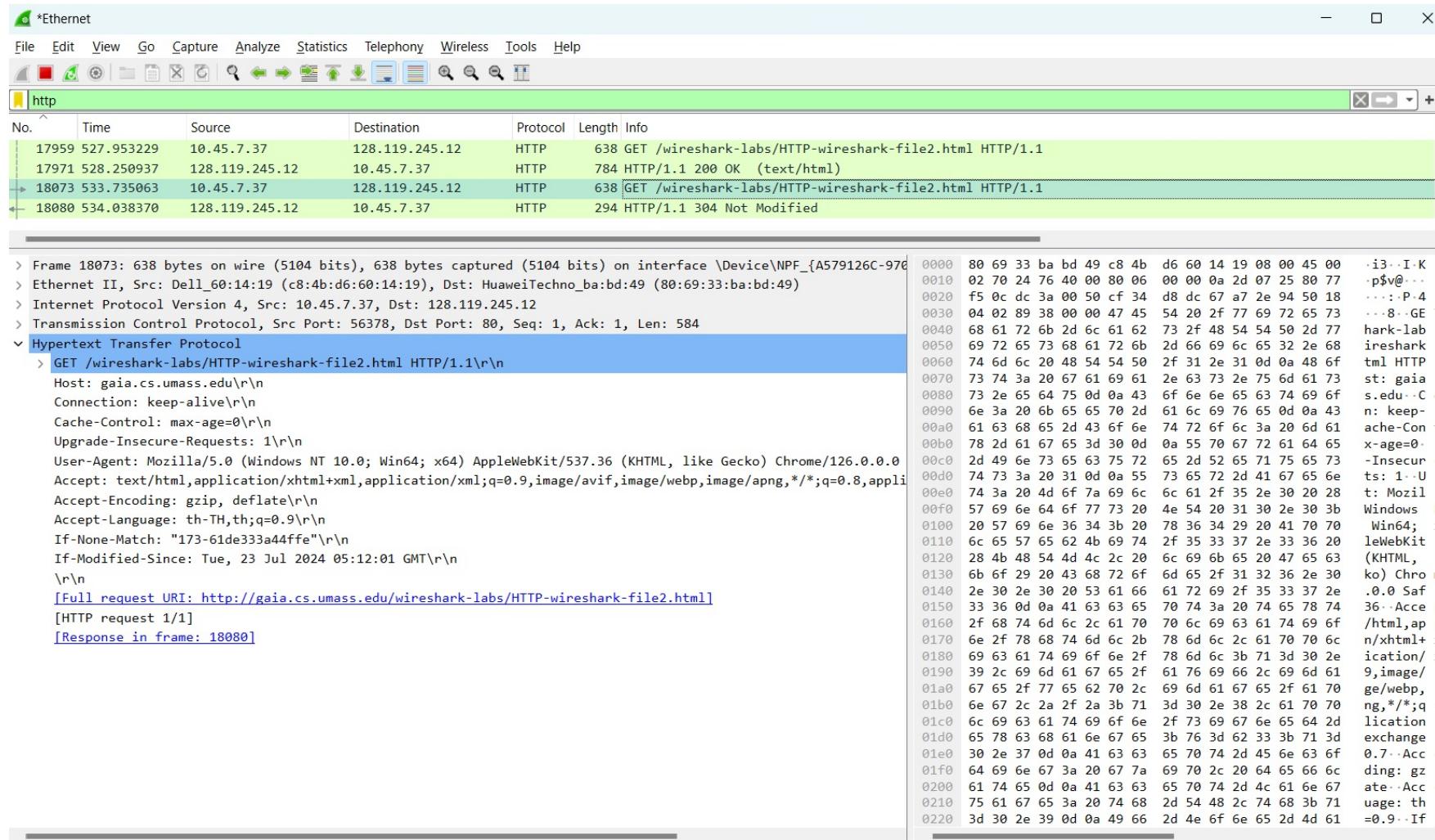
# A1. Capture នៃការ Wireshark : HTTP Get Packet នៅក្នុង



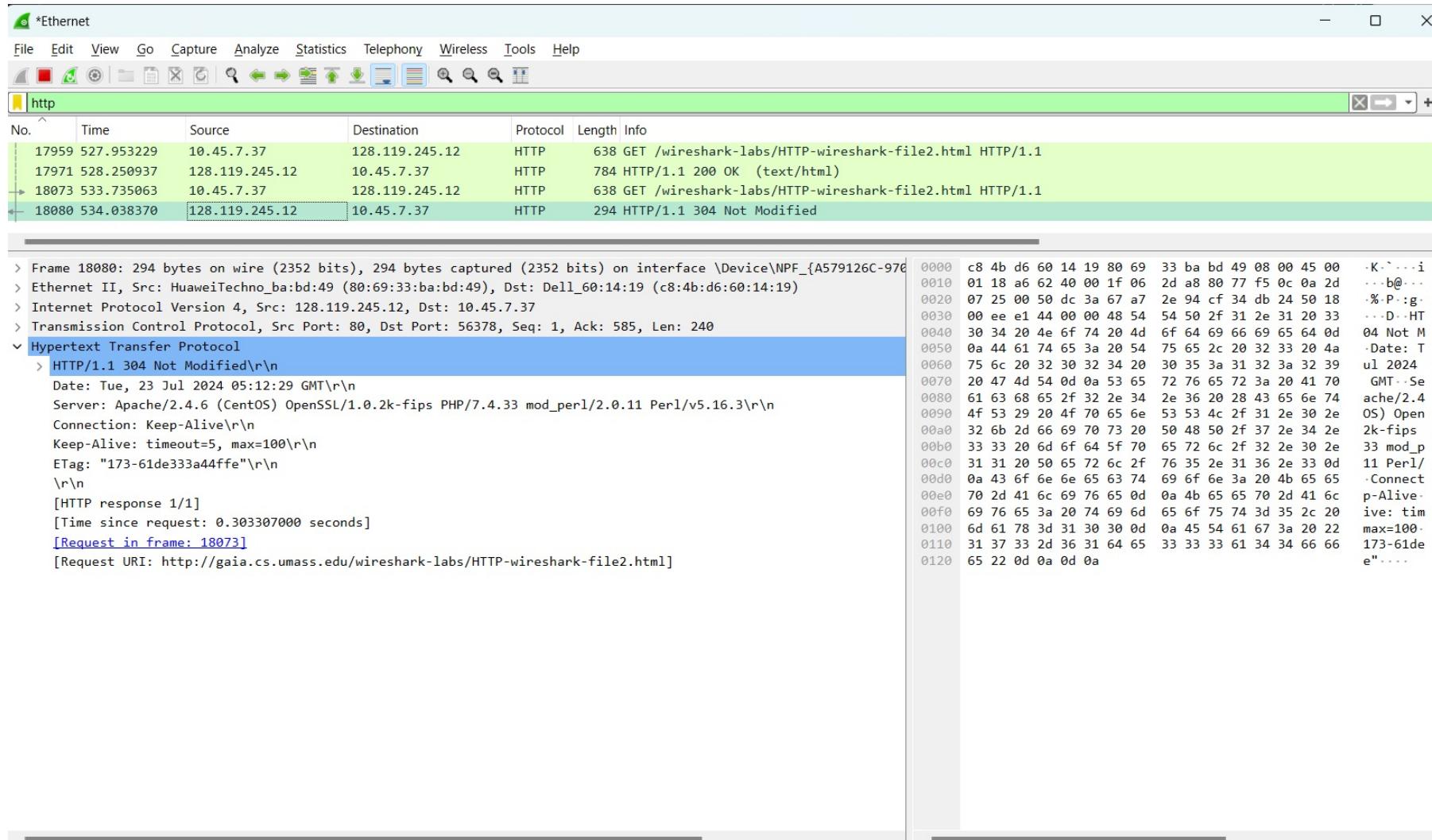
# A2. Capture នៃការ Wireshark : HTTP Response packet នៅក្នុង



# A3. Capture หน้าจอ Wireshark : HTTP Get Packet ที่สอง

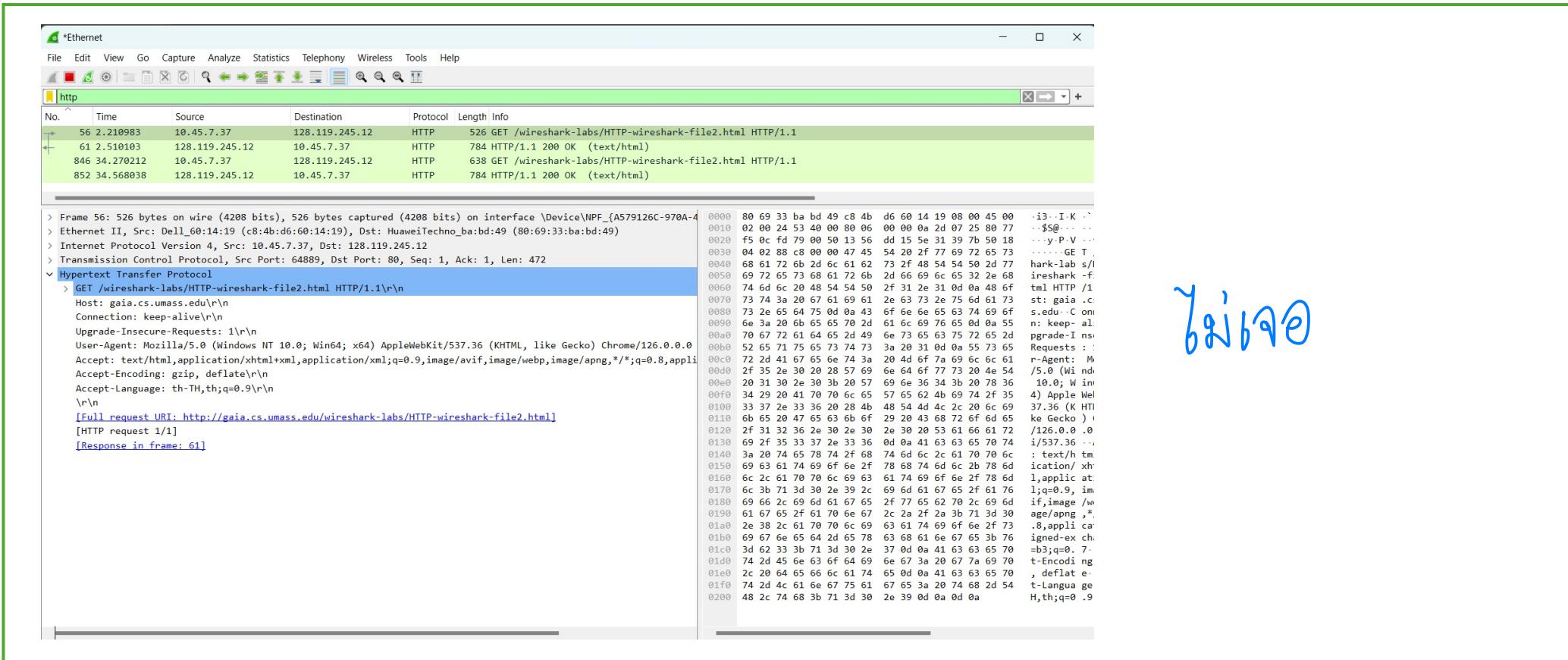


# A4. Capture หน้าจอ Wireshark : HTTP Response packet ที่สอง (หลัง Reload)



# B5.1 ຈົງຕອບກຳດາມຕ່ອໄປນີ້

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? ຕອບ ເຈືອ ໄນເຈືອ ໄທ້ວັງ



Wireshark screenshot showing an HTTP session. The first frame is selected, displaying the following details:

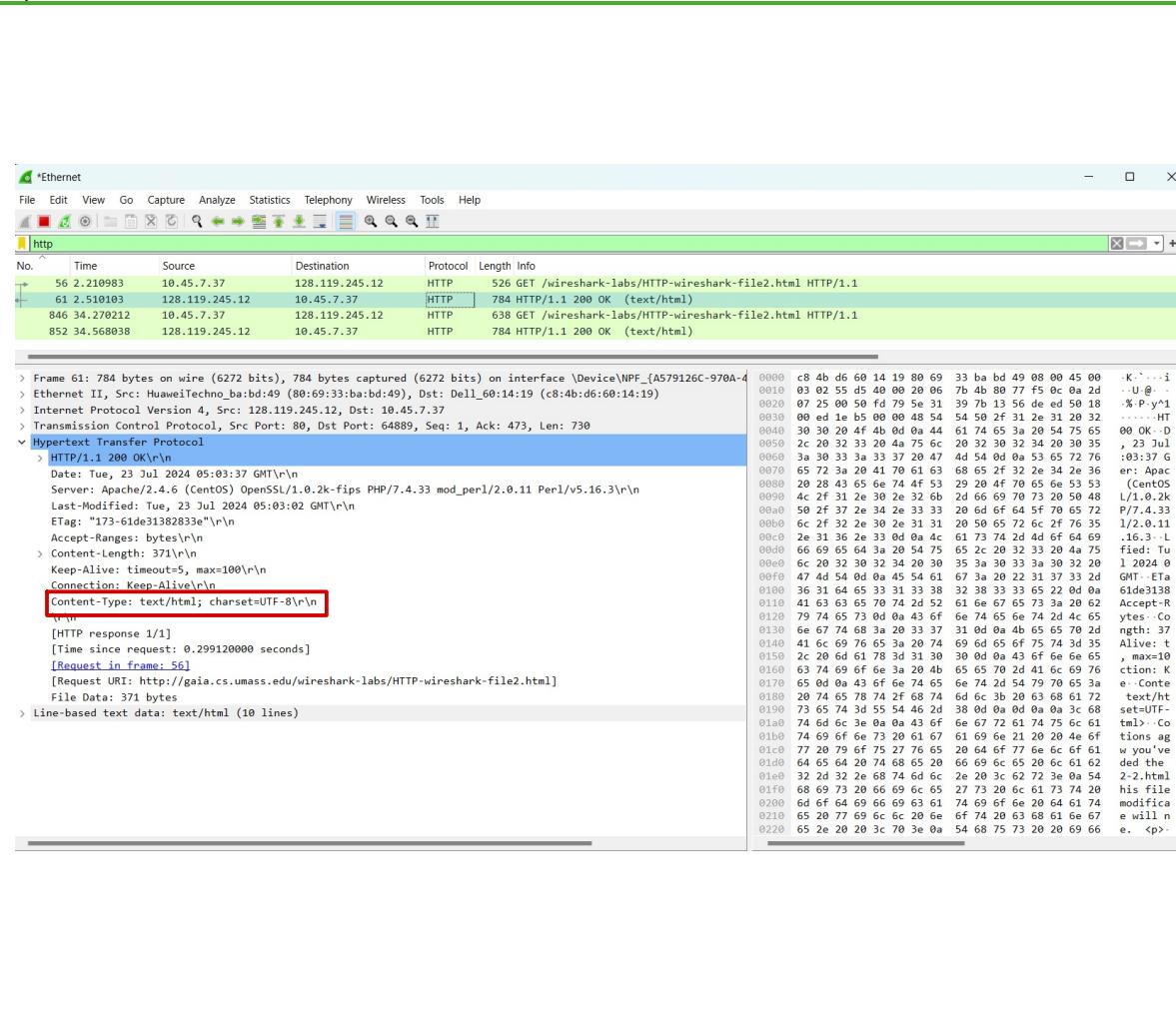
No.	Time	Source	Destination	Protocol	Length	Info
56	2.210983	10.45.7.37	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
61	2.510103	128.119.245.12	10.45.7.37	HTTP	784	HTTP/1.1 200 OK (text/html)
846	34.270212	10.45.7.37	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
852	34.568038	128.119.245.12	10.45.7.37	HTTP	784	HTTP/1.1 200 OK (text/html)

The packet details pane shows the raw bytes of the captured frame, with the first few bytes of the request line highlighted in blue. The text "ຍິນເຈືອ" is handwritten in blue ink over this highlighted area.

```
> Frame 56: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{A579126C-970A-4  
> Ethernet II, Src: Dell_50:14:19 (c8:4b:d6:60:14:19), Dst: HuaweiTechno_ba:bd:49 (80:69:33:ba:bd:49)  
> Internet Protocol Version 4, Src: 10.45.7.37, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 64889, Dst Port: 80, Seq: 1, Ack: 1, Len: 472  
▼ Hypertext Transfer Protocol  
  > [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1]\r\n    Host: gaia.cs.umass.edu\r\n    Connection: keep-alive\r\n    Upgrade-Insecure-Requests: 1\r\n    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0  
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7  
    Accept-Encoding: gzip, deflate\r\n    Accept-Language: th-TH,th;q=0.9\r\n\r\n  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]  
  [HTTP request 1/1]  
  [Response in frame: 61]
```

## B5.2 ຈົງຕອບກຳດາມຕ່ອໄປນີ້

Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?



The Wireshark interface is displayed, capturing traffic on the 'Ethernet' interface. The packet list shows three HTTP requests:

- Frame 56: 2.210983 10.45.7.37 → 128.119.245.12 HTTP 526 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
- Frame 61: 2.510103 128.119.245.12 → 10.45.7.37 HTTP 784 HTTP/1.1 200 OK (text/html)
- Frame 846: 34.270212 10.45.7.37 → 128.119.245.12 HTTP 638 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
- Frame 852: 34.568038 128.119.245.12 → 10.45.7.37 HTTP 784 HTTP/1.1 200 OK (text/html)

The details pane shows the server's response to the third request, which includes the file content:

```
> Frame 61: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{A579126C-970A-4  
> Ethernet II, Src: HuaweiTechno_ba:bd:49 (80:69:33:b0:bd:49), Dst: Dell_60:14:19 (c8:4b:d6:60:14:19)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.45.7.37  
> Transmission Control Protocol, Src Port: 80, Dst Port: 64889, Seq: 1, Ack: 473, Len: 730  
HTTP/1.1 200 OK\r\nDate: Tue, 23 Jul 2024 05:03:37 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\nLast-Modified: Tue, 23 Jul 2024 05:03:02 GMT\r\nETag: "173-61de3138283e"\r\nAccept-Ranges: bytes\r\nContent-Length: 371\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/1]  
[Time since request: 0.299120000 seconds]  
[Request in frame: 56]  
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]  
File Data: 371 bytes  
Line-based text data: text/html (10 lines)
```

Answer here

text / html

# B5.3 ຈົງຕອບກຳດາມຕ່ອໄປນີ້

Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE.” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
17959	527.953229	10.45.7.37	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
17971	528.250937	128.119.245.12	10.45.7.37	HTTP	784	HTTP/1.1 200 OK (text/html)
18073	533.735063	10.45.7.37	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
18080	534.038370	128.119.245.12	10.45.7.37	HTTP	294	HTTP/1.1 304 Not Modified

> Frame 18073: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits) on interface \Device\NPF\_{A579126C-97C  
> Ethernet II, Src: Dell\_60:14:19 (c8:4b:d6:60:14:19), Dst: HuaweiTechno\_ba:bd:49 (80:69:33:ba:bd:49)  
> Internet Protocol Version 4, Src: 10.45.7.37, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 56378, Dst Port: 80, Seq: 1, Ack: 1, Len: 584  
HyperText Transfer Protocol  
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,appli  
Accept-Encoding: gzip, deflate\r\nAccept-Language: th-TH,th;q=0.9\r\nIf-None-Match: "173-61de33a44ffe"\r\nIf-Modified-Since: Tue, 23 Jul 2024 05:12:01 GMT\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]  
[HTTP request 1/1]  
[Response in frame: 18080]

Frame 18073 bytes on wire (5104 bits), 638 bytes captured (5104 bits) on interface \Device\NPF\_{A579126C-97C  
Ethernet II, Src: Dell\_60:14:19 (c8:4b:d6:60:14:19), Dst: HuaweiTechno\_ba:bd:49 (80:69:33:ba:bd:49)  
Internet Protocol Version 4, Src: 10.45.7.37, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 56378, Dst Port: 80, Seq: 1, Ack: 1, Len: 584  
HyperText Transfer Protocol  
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,appli  
Accept-Encoding: gzip, deflate\r\nAccept-Language: th-TH,th;q=0.9\r\nIf-None-Match: "173-61de33a44ffe"\r\nIf-Modified-Since: Tue, 23 Jul 2024 05:12:01 GMT\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]  
[HTTP request 1/1]  
[Response in frame: 18080]

Answer here

Tue, 23 Jul 2024

05:12:01 GMT

# B5.4 ຈົງຕອບກຳດາມຕ່ອໄປນີ້

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.

The screenshot shows a Wireshark capture of network traffic on the 'Ethernet' interface. The packet list pane displays four HTTP requests:

- Frame 17959: 638 bytes on wire (2352 bits), 638 bytes captured (2352 bits) on interface \Device\NPF\_{A579126C-97E...  
HTTP/1.1 200 OK (text/html)
- Frame 17971: 784 bytes on wire (2352 bits), 784 bytes captured (2352 bits) on interface \Device\NPF\_{A579126C-97E...  
HTTP/1.1 200 OK (text/html)
- Frame 18073: 638 bytes on wire (2352 bits), 638 bytes captured (2352 bits) on interface \Device\NPF\_{A579126C-97E...  
HTTP/1.1 200 OK (text/html)
- Frame 18080: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF\_{A579126C-97E...  
HTTP/1.1 304 Not Modified

The packet details pane for Frame 18080 shows the following:

```
> Frame 18080: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{A579126C-97E...
> Ethernet II, Src: HuaweiTechno_ba:bd:49 (80:69:33:ba:bd:49), Dst: Dell_60:14:19 (c8:4b:d6:60:14:19)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.45.7.37
> Transmission Control Protocol, Src Port: 80, Dst Port: 56378, Seq: 1, Ack: 585, Len: 240
< Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Tue, 23 Jul 2024 05:12:29 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-61de33a44ffe"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.303307000 seconds]
    [Request in frame: 18073]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

The packet bytes pane shows the raw hex and ASCII data for the selected frame.

Answer here

304 ໄພໍມັກກາ ຮັບການເຄີຍໄວ້

ການຫອ Data ໄປແລ້ວ ຈຶ່ງກຳທົ່ວມດຸ

ເກຳມາໃນໆ ແຮຣອ Catch