

1-) BASIC HTTP GET/ RESPINSE INTERACTION

The image shows a Wireshark network traffic capture on a Wi-Fi interface. The packet list pane displays four packets related to an HTTP GET request and its response. The packet details pane shows the structure of the selected packet (No. 173), including the GET request line, host, connection, cache control, upgrade-insecure-requests, user agent, accept headers, accept-encoding, accept-language, and the 200 OK response line. The packet bytes pane shows the raw data of the response body, which is an HTML document.

No.	Time	Source	Destination	Protocol	Length	Info
173	11.671213	192.168.0.12	128.119.245.12	HTTP	548	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
187	11.839554	128.119.245.12	192.168.0.12	HTTP	540	HTTP/1.1 200 OK (text/html)
223	13.109016	192.168.0.12	128.119.245.12	HTTP	494	GET /favicon.ico HTTP/1.1
232	13.285706	128.119.245.12	192.168.0.12	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36
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=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,tr;q=0.8,af;q=0.7

HTTP/1.1 200 OK
Date: Wed, 21 Apr 2021 16:44:21 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Wed, 21 Apr 2021 05:59:01 GMT
ETag: "80-5c075426772cf"
Accept-Ranges: bytes
Content-Length: 128
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
Congratulations. You've downloaded the file
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!
</html>
```

1-1)

Both of them are 1.1

1-2)

Accepted languages are: en-us, tr, af

1-3)

My IP is: 192.168.0.12

Gaia.cs.umass.edu ip is: 128.119.245.12

1-4)

Status code is: 200

1-5)

Last modified: Wed, 21 Apr 2021 05:59:01 GMT

1-6)

128 bytes

1-7)

No.

2-)

8

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The top toolbar contains icons for various functions like opening files, saving, and zooming. The main window is divided into three panes:

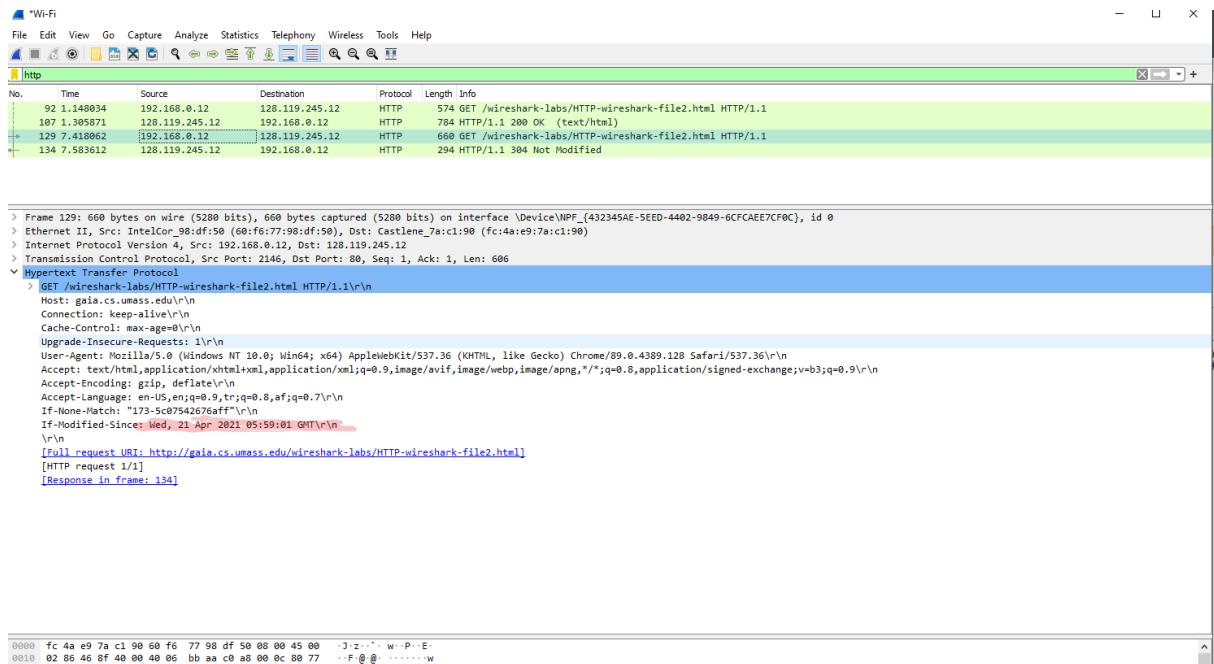
- Packet List:** Shows a list of captured packets. The selected packet is #107, an HTTP GET request to `http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html`.
- Packet Details:** Displays the structure of the selected packet. It shows the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The Hypertext Transfer Protocol section is expanded, showing the request details:
 - Host: `gaia.cs.umass.edu`
 - Connection: `keep-alive`
 - Cache-Control: `max-age=0`
 - Upgrade-Insecure-Requests: `1`
 - User-Agent: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36`
 - 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=0.9`
 - Accept-Encoding: `gzip, deflate`
 - Accept-Language: `en-US,en;q=0.9,tr;q=0.8,af;q=0.7`
- Packet Bytes:** Shows the raw data of the packet in hexadecimal and ASCII format.

A red question mark icon is visible in the bottom left corner of the image.

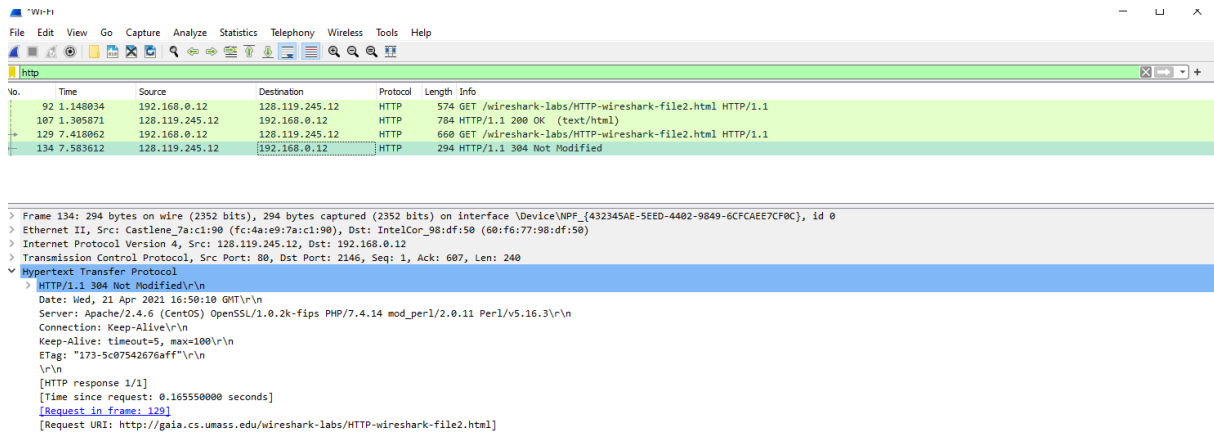
9

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.12
 Transmission Control Protocol, Src Port: 80, Dst Port: 2145, Seq: 1, Ack: 521, Len: 730
 Hypertext Transfer Protocol
 > HTTP/1.1 200 OK\r\n\r\n
 Date: Wed, 21 Apr 2021 16:50:04 GMT\r\n\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n\r\n
 Last-Modified: Wed, 21 Apr 2021 05:59:01 GMT\r\n\r\n
 ETag: "173-5c07542676aff"\r\n\r\n
 Accept-Ranges: bytes\r\n\r\n
 > Content-Length: 371\r\n\r\n
 Keep-Alive: timeout=5, max=100\r\n\r\n
 Connection: Keep-Alive\r\n\r\n
 Content-Type: text/html; charset=UTF-8\r\n\r\n
 \r\n\r\n
 [HTTP response 1/1]
 [Time since request: 0.157837000 seconds]
 [Request in frame: 92]
 [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)
 \r\n
 <html>\r\n
 \r\n
 Congratulations again! Now you've downloaded the file lab2-2.html.
\r\n
 This file's last modification date will not change. <p>\r\n
 Thus if you download this multiple times on your browser, a complete copy
\r\n
 will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\r\n
 field in your browser's HTTP GET request to the server.\r\n
 \r\n
 </html>\r\n

10



11



?

2-8)

No.

2-9)

Yes, it returned the content of the file. Because we can observe it through browser and line based text data.

2-10)

Yes. Wed, 21 Apr 2021 05:59:01 GMT\r\n

2-11)

304 not modified. It did not return the contents of the file because the browser is not modified and we have it in our cache.

3-)

The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area is divided into three panes. The top pane shows a list of captured packets. The middle pane shows the details of the selected packet (No. 21). The bottom pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.147511	192.168.0.12	128.119.245.12	HTTP	574	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
21	0.319021	128.119.245.12	192.168.0.12	HTTP	535	HTTP/1.1 200 OK (text/html)

Frame 21: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{432345AE-5EED-4402-9849-6CFCCEE7CF0C}, id 0
> Ethernet II, Src: Castlene_7a:c1:90 (fc:4a:e9:7a:c1:90), Dst: IntelCor_98:df:50 (60:f6:77:98:df:50)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.12
> Transmission Control Protocol, Src Port: 80, Dst Port: 2210, Seq: 4381, Ack: 521, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #17(1460), #18(1460), #20(1460), #21(481)]
▼ Hypertext Transfer Protocol
 ▼ HTTP/1.1 200 OK\r\n
 > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n
 Response Version: HTTP/1.1
 Status Code: 200
 [Status Code Description: OK]
 Response Phrase: OK
 Date: Wed, 21 Apr 2021 17:03:16 GMT\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
 Last-Modified: Wed, 21 Apr 2021 05:59:01 GMT\r\n
 ETag: "1194-5c07542672896"\r\n
 Accept-Ranges: bytes\r\n
 Content-Length: 4500\r\n
 Keep-Alive: timeout=5, max=100\r\n
 Connection: Keep-Alive\r\n
 Content-Type: text/html; charset=UTF-8\r\n
 \r\n
 [HTTP response 1/1]
 [Time since request: 0.171510000 seconds]
 [Request in frame: 6]
 [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
 File Data: 4500 bytes
 > Line-based text data: text/html (98 lines)

http						
No.	Time	Source	Destination	Protocol	Length	Info
6	0.147511	192.168.0.12	128.119.245.12	HTTP	574	GET /wireshark-labs/HTTP-v
21	0.319021	128.119.245.12	192.168.0.12	HTTP	535	HTTP/1.1 200 OK (text/htm

> Frame 21: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{4323...}
 > Ethernet II, Src: Castlene_7a:c1:90 (fc:4a:e9:7a:c1:90), Dst: IntelCor_98:df:50 (60:f6:77:98:df:50)
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.12
 > Transmission Control Protocol, Src Port: 80, Dst Port: 2210, Seq: 4381, Ack: 521, Len: 481
 Source Port: 80
 Destination Port: 2210
 [Stream index: 3]
 [TCP Segment Len: 481]
 Sequence Number: 4381 (relative sequence number)
 Sequence Number (raw): 2695003360
 [Next Sequence Number: 4862 (relative sequence number)]
 Acknowledgment Number: 521 (relative ack number)
 Acknowledgment number (raw): 3073125840
 0101 = Header Length: 20 bytes (5)
 > Flags: 0x018 (PSH, ACK)
 Window: 237
 [Calculated window size: 237]
 [Window size scaling factor: -1 (unknown)]
 Checksum: 0x5073 [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 > [SEQ/ACK analysis]
 > [Timestamps]
 TCP payload (481 bytes)
 TCP segment data (481 bytes)
 > [4 Reassembled TCP Segments (4861 bytes): #17(1460), #18(1460), #20(1460), #21(481)]
 [Frame: 17, payload: 0-1459 (1460 bytes)]
 [Frame: 18, payload: 1460-2919 (1460 bytes)]
 [Frame: 20, payload: 2920-4379 (1460 bytes)]
 [Frame: 21, payload: 4380-4860 (481 bytes)]
 [Segment count: 4]
 [Reassembled TCP length: 4861]
 [Reassembled TCP Data: 485454507f317e3170323030204f4b0d0a4461746553a205765642c203231204170722032 1

3-12)

There is 1 HTTP get request sent by me, 6

3-13)

21

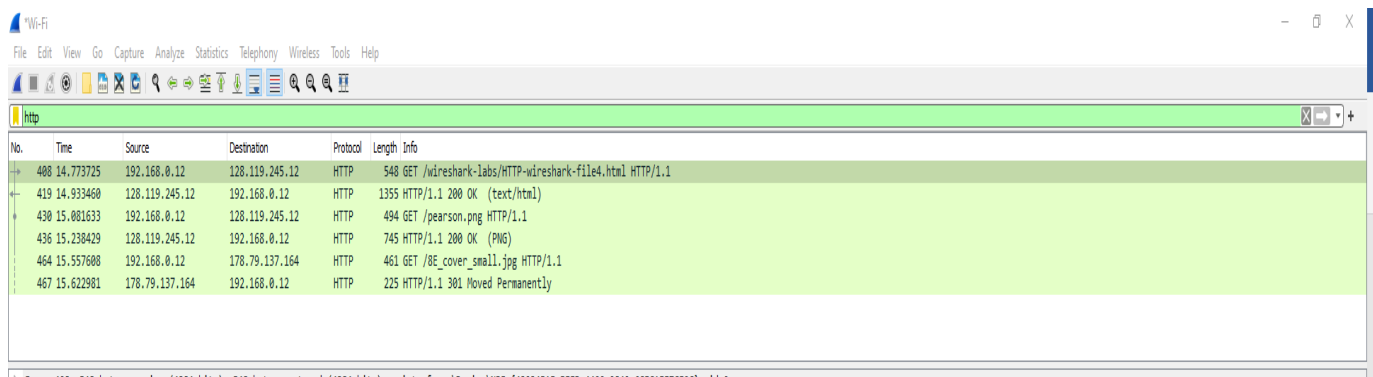
3-14)

200, 'OK'

3-15)

4 segments as 1460,1460,1460,481

4-)



The image shows a Wireshark network traffic capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The main display area shows a list of captured packets, with the first five packets highlighted in green. These packets are all HTTP GET requests. The first packet is a GET request for a file named 'wireshark-file4.html' from 192.168.0.12 to 128.119.245.12. The second packet is a 200 OK response from 128.119.245.12 to 192.168.0.12. The third packet is a GET request for 'pearson.png' from 192.168.0.12 to 128.119.245.12. The fourth packet is a 200 OK response from 128.119.245.12 to 192.168.0.12. The fifth packet is a GET request for '8E_cover_small.jpg' from 192.168.0.12 to 178.79.137.164. The sixth packet is a 301 Moved Permanently response from 178.79.137.164 to 192.168.0.12.

No.	Time	Source	Destination	Protocol	Length	Info
408	14.773725	192.168.0.12	128.119.245.12	HTTP	548	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
419	14.933460	128.119.245.12	192.168.0.12	HTTP	1355	HTTP/1.1 200 OK (text/html)
430	15.081633	192.168.0.12	128.119.245.12	HTTP	494	GET /pearson.png HTTP/1.1
436	15.238429	128.119.245.12	192.168.0.12	HTTP	745	HTTP/1.1 200 OK (PNG)
464	15.557608	192.168.0.12	178.79.137.164	HTTP	461	GET /8E_cover_small.jpg HTTP/1.1
467	15.622981	178.79.137.164	192.168.0.12	HTTP	225	HTTP/1.1 301 Moved Permanently

4-16) There are 3 HTTP GET requests sent by my browser with the order of;

-128.119.245.12

-128.119.245.12

-178.79.137.164

4-17)

I think they are downloaded serially because firstly, first image GET requested and responded. After that, second image requested and responded. So their timestamps are different.