

Ethical Hacking And Vulnerability Assessment

21bce301 Thakkar Krisha

LabPractical 1: Wireshark Packet Sniffer the Basics

I. The Basic HTTP GET/response interaction

Url : <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

By looking at the information in the HTTP GET and response messages, answer the following questions.

The Request : ➡

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The middle pane shows the details of the selected packet (No. 50), which is an HTTP GET request. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
50	7.347751360	192.168.40.129	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
55	8.120432395	128.119.245.12	192.168.40.129	HTTP	542	HTTP/1.1 200 OK (text/html)
65	8.157900287	192.168.40.129	128.119.245.12	HTTP	437	GET /favicon.ico HTTP/1.1
83	9.143725305	128.119.245.12	192.168.40.129	HTTP	540	HTTP/1.1 404 Not Found (text/html)

Details of Packet 50:

- Frame 50: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface any, id 0
- Linux cooked capture v1
- Internet Protocol Version 4, Src: 192.168.40.129, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 45372, Dst Port: 80, Seq: 1, Ack: 424
- Hypertext Transfer Protocol
 - GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
 - Request Method: GET
 - Request URI: /wireshark-labs/HTTP-wireshark-file1.html
 - Request Version: HTTP/1.1
 - Host: gaia.cs.umass.edu\r\n
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
 - Accept-Language: en-US,en;q=0.5\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Connection: keep-alive\r\n
 - Upgrade-Insecure-Requests: 1\r\n
 - Pragma: no-cache\r\n
 - Cache-Control: no-cache\r\n
 - \r\n
 - [Full request URI: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>]
 - [HTTP request 1/2]
 - [Response in frame: 55]
 - [Next request in frame: 65]

Raw Data (Hex/ASCII):

```

0000  00 04 00 01 00 06 00 0c 29 82 9a 35 00 00 08 00 .....).5...
0010  45 00 01 d0 d7 2e 40 00 40 06 03 4c c0 a8 28 81 E....@. @.L.(:
0020  80 77 f5 0c b1 3c 00 50 9d 46 fb f4 32 5a 73 30 .w...<P .F. 2Zs0
0030  50 18 7d 78 60 70 00 00 47 45 54 20 2f 77 69 72 P }x'p. . GET /wir
0040  65 73 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 eshark-l abs/HTTP
0050  2d 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 -wiresha rk-file1
0060  2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HT TP/1.1
0070  48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d Host: ga ia.cs.um
0080  61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 ass.edu. User-Ag
0090  65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Moz illa/5.0
00a0 20 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 38 36 (X11; L inux x86
00b0 5f 36 34 3b 20 72 76 3a 31 30 39 2e 30 29 20 47 _64; rv: 109.0) G
00c0 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 ecko/201 00101 Fi
00d0 72 65 66 6f 78 2f 31 31 35 2e 30 0d 0a 41 63 63 refox/11 5.0 .Acc
00e0 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 ept: tex t/html,a
00f0 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c pplicati on/xhtml
0100 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e +xml,app lication
0110 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 /xml;q=0 .9,image
0120 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 /avif,im age/webp
0130 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 ,/*;q=0 .8 Acce
0140 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d pt-Langu age: en
0150 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 US,en;q= 0.5 Acc
0160 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a ept-Enco ding: gz
0170 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e ip, defl ate Con
0180 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c nection: keep-al
0190 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 ive Upg rade-Ins
01a0 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 ecore-Re quests:
01b0 31 0d 0a 50 72 61 67 6d 61 3a 20 6e 6f 2d 63 61 1 Pragm a: no-ca
01c0 63 68 65 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 che Cac he-Contr
01d0 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 0d 0a ol: no-c ache....
  
```

Bytes 28-31: Source Address (ip.src) | Packets: 307 · Displayed: 4 (1.3%) | Profile: Default

The Response : ←

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The middle pane shows the details of the selected packet (No. 55), and the bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
50	7.347751360	192.168.40.129	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
55	8.120432395	128.119.245.12	192.168.40.129	HTTP	542	HTTP/1.1 200 OK (text/html)
65	8.157900287	192.168.40.129	128.119.245.12	HTTP	437	GET /favicon.ico HTTP/1.1
83	9.143725305	128.119.245.12	192.168.40.129	HTTP	540	HTTP/1.1 404 Not Found (text/html)

Packet 55 Details:

- Frame 55: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface any, id 0
- Linux cooked capture v1
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.40.129
- Transmission Control Protocol, Src Port: 80, Dst Port: 45372, Seq: 1, Ack: 425, Len: 486
- 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: Tue, 13 Aug 2024 06:34:21 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
 - Last-Modified: Tue, 13 Aug 2024 05:59:02 GMT\r\n
 - Etag: "80-61f8a4e721164"\r\n
 - Accept-Ranges: bytes\r\n
 - Content-Length: 128\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 1/2]
 - [Time since request: 0.772681035 seconds]
 - [Request in frame: 50]
 - [Next request in frame: 65]
 - [Next response in frame: 83]
 - [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
 - File Data: 128 bytes
 - Line-based text data: text/html (4 lines)
 - <html>\n
 - Congratulations. You've downloaded the file\n
 - http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
 - </html>\n

Raw Data (Hex/ASCII):

```

0000 00 00 00 01 00 06 00 50 56 eb 67 19 00 00 08 00 .....P V g ....
0010 45 00 02 0e e7 5a 00 00 80 06 f2 e1 80 77 f5 0c E...Z...w...
0020 c0 a8 28 81 00 50 b1 3c 32 5a 73 30 9d 46 fd 9c ..(.P.<22so.F..
0030 50 18 fa f0 2c 4d 00 00 48 54 54 50 2f 31 2e 31 P...M...HTTP/1.1
0040 20 32 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 200 OK..Date: T
0050 75 65 2c 20 31 33 20 41 75 67 20 32 30 32 34 20 ue, 13 A ug 2024
0060 30 36 3a 33 34 3a 32 31 20 47 4d 54 0d 0a 53 65 06:34:21 GMT..Se
0070 72 76 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 rver: Ap ache/2.4
0080 2e 36 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e .6 (Cent OS) Open
0090 53 53 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 SSL/1.0. 2k-fips
00a0 50 48 50 2f 37 2e 34 2e 33 33 20 6d 6f 64 5f 70 PHP/7.4. 33 mod_p
00b0 65 72 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f erl/2.0. 11 Perl/
00c0 76 35 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f v5.16.3. Last-Mo
00d0 64 69 66 69 65 64 3a 20 54 75 65 2c 20 31 33 20 dified: Tue, 13
00e0 41 75 67 20 32 30 32 34 20 30 35 3a 35 39 3a 30 Aug 2024 05:59:0
00f0 32 20 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2 GMT. E Tag: "80
0100 2d 36 31 66 38 61 34 65 37 32 31 31 36 34 22 0d -61f8a4e 721164".
0110 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 Accept- Ranges:
0120 62 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c bytes .C ontent-L
0130 65 6e 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 length: 1 28..Keep
0140 2d 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d -Alive: timeout=
0150 35 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 5, max=1 00..Conn
0160 65 63 74 09 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 ection: Keep-Ali
0170 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 ve..Cont ent-Type
0180 3a 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 : text/h tml; cha
0190 72 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 rset=UTF -8...<h
01a0 74 6d 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 tml> Con gratulat
01b0 69 6f 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f ions. Y ou've do
01c0 77 6e 6c 6f 61 64 65 64 20 74 68 65 20 66 69 6c wnloaded the fil
01d0 65 20 0a 68 74 74 70 3a 2f 2f 67 61 69 61 2e 63 e http: //gaia.c
01e0 73 2e 75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 s.umass. edu/wire
01f0 73 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d shark-la bs/HTTP-
0200 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.
0210 68 74 6d 6c 21 0a 3c 2f 68 74 6d 6c 3e 0a html! </ html>..
  
```

any: <live capture in progress> | Packets: 405 - Displayed: 4 (1.0%) | Profile: Default

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

- The browser is running **HTTP/1.1**, as indicated in the request line:

```
‣ Frame 50: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface any, id 0
‣ Linux cooked capture v1
‣ Internet Protocol Version 4, Src: 192.168.40.129, Dst: 128.119.245.12
‣ Transmission Control Protocol, Src Port: 45372, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
‣ Hypertext Transfer Protocol
  ‣ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    ‣ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
```

- The server is also running **HTTP/1.1**, as indicated in the response line:

```
‣ Frame 55: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface any, id 0
‣ Linux cooked capture v1
‣ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.40.129
‣ Transmission Control Protocol, Src Port: 80, Dst Port: 45372, Seq: 1, Ack: 425, Len: 486
‣ 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
```

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

- Languages Accepted: The browser indicates it can accept English (`en-US, en;q=0.5`) as shown in the `Accept-Language` header: `Accept-Language: en-US,en;q=0.5`.

```

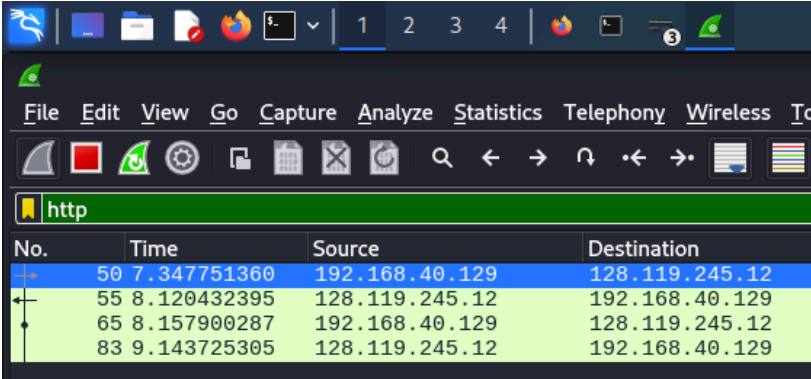
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
  Request Method: GET
  Request URI: /wireshark-labs/HTTP-wireshark-file1.html
  Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n

```

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

- The IP address of the computer is **192.168.40.129**.
- The IP address of the **gaia.cs.umass.edu** server is **128.119.245.12**.

○



No.	Time	Source	Destination
50	7.347751360	192.168.40.129	128.119.245.12
55	8.120432395	128.119.245.12	192.168.40.129
65	8.157900287	192.168.40.129	128.119.245.12
83	9.143725305	128.119.245.12	192.168.40.129

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

- **Status Code:** The status code is `200 OK` i.e., the request was successful.

```
▸ Frame 55: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.40.129
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 45372, Seq: 1, Ack: 425, Len: 486
▾ 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: Tue, 13 Aug 2024 06:34:21 GMT\r\n
```

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

- The HTML file was last modified on **Tue, 13 Aug 2024 05:59:02 GMT**, as indicated by the **Last-Modified** header in the response.

```
▾ 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: Tue, 13 Aug 2024 06:34:21 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
      Last-Modified: Tue, 13 Aug 2024 05:59:02 GMT\r\n
      ETag: "80-61f8a4e721164"\r\n
```

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

- The content length returned to your browser is **128 bytes**, as indicated by the **Content-Length: 128** header in the response.

```
Date: Tue, 13 Aug 2024 06:34:21 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
Last-Modified: Tue, 13 Aug 2024 05:59:02 GMT\r\n
ETag: "80-61f8a4e721164"\r\n
Accept-Ranges: bytes\r\n
▼ Content-Length: 128\r\n
  [Content length: 128]
Keep-Alive: timeout=5, max=100\r\n
```

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.

```

0000 00 00 00 01 00 06 00 50 56 eb 67 19 00 00 08 00 .....P V.g.....
0010 45 00 02 0e e7 5a 00 00 80 06 f2 e1 80 77 f5 0c E....Z....w...
0020 c0 a8 28 81 00 50 b1 3c 32 5a 73 30 9d 46 fd 9c ..(..P.< 2Zs0.F..
0030 50 18 fa f0 2c 4d 00 00 48 54 54 50 2f 31 2e 31 P...M... HTTP/1.1
0040 20 32 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 200 OK...Date: T
0050 75 65 2c 20 31 33 20 41 75 67 20 32 30 32 34 20 ue, 13 A ug 2024
0060 30 36 3a 33 34 3a 32 31 20 47 4d 54 0d 0a 53 65 06:34:21 GMT...Se
0070 72 76 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 rver: Ap ache/2.4
0080 2e 36 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e .6 (Cent OS) Open
0090 53 53 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 SSL/1.0. 2k-fips
00a0 50 48 50 2f 37 2e 34 2e 33 33 20 6d 6f 64 5f 70 PHP/7.4. 33 mod_p
00b0 65 72 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f erl/2.0. 11 Perl/
00c0 76 35 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f v5.16.3...Last-Mo
00d0 64 69 66 69 65 64 3a 20 54 75 65 2c 20 31 33 20 dified: Tue, 13
00e0 41 75 67 20 32 30 32 34 20 30 35 3a 35 39 3a 30 Aug 2024 05:59:0
00f0 32 20 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2 GMT...E Tag: "80
0100 2d 36 31 66 38 61 34 65 37 32 31 31 36 34 22 0d -61f8a4e 721164".
0110 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 ...Accept- Ranges:
0120 62 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c bytes...C ontent-L
0130 65 6e 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 ength: 1 28...Keep
0140 2d 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d -Alive: timeout=
0150 35 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 5, max=1 00...Conn
0160 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 ection: Keep-Ali
0170 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 ve...Cont ent-Type
0180 3a 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 : text/h tml; cha
0190 72 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 rset=UTF -8...<h
01a0 74 6d 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 tml>...Con gratulat
01b0 69 6f 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f ions. Y ou've do
01c0 77 6e 6c 6f 61 64 65 64 20 74 68 65 20 66 69 6c wnloaded the fil
01d0 65 20 0a 68 74 74 70 3a 2f 2f 67 61 69 61 2e 63 e http: //gaia.c
01e0 73 2e 75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 s.umass. edu/wire
01f0 73 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d shark-la bs/HTTP-
0200 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.
0210 68 74 6d 6c 21 0a 3c 2f 68 74 6d 6c 3e 0a html!.</ html>

```


- **Date:** Tue, 13 Aug 2024 06:34:21 GMT
- **Server:** Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3
- **Last-Modified:** Tue, 13 Aug 2024 05:59:06 GMT
- **ETag:** "80-61f8a4de72164"
- **Accept-Ranges:** bytes
- **Content-Length:** 128
- **Keep-Alive:** timeout=5, max=100
- **Connection:** Keep-Alive
- **Content-Type:** text/html; charset=UTF-8

II. The HTTP CONDITIONAL GET/response interaction

Url : <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

By looking at the information in the HTTP GET and response messages, answer the following questions.

The Request 1 : ➡

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. The second pane shows the details of the selected packet (Frame 9), which is an HTTP GET request. The third pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
9	0.308598477	192.168.40.129	128.119.245.12	HTTP	437	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
12	0.792100902	128.119.245.12	192.168.40.129	HTTP	786	HTTP/1.1 200 OK (text/html)
15	0.814759688	192.168.40.129	128.119.245.12	HTTP	394	GET /favicon.ico HTTP/1.1
17	1.132472682	128.119.245.12	192.168.40.129	HTTP	541	HTTP/1.1 404 Not Found (text/html)
29	8.895747500	192.168.40.129	128.119.245.12	HTTP	523	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
33	9.300235606	128.119.245.12	192.168.40.129	HTTP	296	HTTP/1.1 304 Not Modified

Frame 9: 437 bytes on wire (3496 bits), 437 bytes captured (3496 bits) on interface any, id 0

- Linux cooked capture v1
- Internet Protocol Version 4, Src: 192.168.40.129, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 33236, Dst Port: 80, Seq: 1, Ack: 1, Len: 381
- Hypertext Transfer Protocol
 - GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
 - [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Request Method: GET
 - Request URI: /wireshark-labs/HTTP-wireshark-file2.html
 - Request Version: HTTP/1.1
 - Host: gaia.cs.umass.edu\r\n
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
 - Accept-Language: en-US,en;q=0.5\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Connection: keep-alive\r\n
 - Upgrade-Insecure-Requests: 1\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: 12]

0000 00 04 00 01 00 06 00 0c 29 82 9a 35 00 00 08 00) 5 ...
 0010 45 00 01 a5 7b 25 40 00 40 06 5f 80 c0 a8 28 81 E...{ } @ _...(
 0020 80 77 f5 0c 81 d4 00 50 3e ea 45 20 6b 9b 78 dd .w...P >E k x
 0030 50 18 7d 78 60 45 00 00 47 45 54 20 2f 77 69 72 P }x'E... GET /wir
 0040 65 73 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 eshark-l abs/HTTP
 0050 2d 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 -wiresha rk-file2
 0060 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HT TP/1.1
 0070 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d Host: ga ia.cs.um
 0080 61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 ass.edu User-Ag
 0090 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Moz illa/5.0
 00a0 20 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 38 36 (X11; L inux x86
 00b0 5f 36 34 3b 20 72 76 3a 31 30 39 2e 30 29 20 47 _64; rv: 109.0) G
 00c0 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 ecko/201 00101 Fi
 00d0 72 65 66 6f 78 2f 31 31 35 2e 30 0d 0a 41 63 63 refox/11 5.0 Acc
 00e0 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 ept: tex t/html,a
 00f0 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c pplicati on/xhtmll
 0100 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e +xml,app lication
 0110 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 /xml;q=0 .9,image
 0120 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 /avif,im age/webp
 0130 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 ,/*;q=0 .8 Acc
 0140 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d pt-Langu age: en-
 0150 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 US,en;q= 0.5 Acc
 0160 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a ept-Enco ding: gz
 0170 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e ip, defl ate Con
 0180 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c nection: keep-al
 0190 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 ive Upg rade-Ins
 01a0 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 ecore-Re quests:
 01b0 31 0d 0a 0d 0a 1...

Hypertext Transfer Protocol: Protocol Packets: 41 - Displayed: 6 (14.6%) - Dropped: 0 (0.0%) Profile: Default

The Response : ←

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
9	0.308598477	192.168.40.129	128.119.245.12	HTTP	437	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
12	0.792100962	128.119.245.12	192.168.40.129	HTTP	786	HTTP/1.1 200 OK (text/html)
15	0.814759688	192.168.40.129	128.119.245.12	HTTP	394	GET /favicon.ico HTTP/1.1
17	1.132472682	128.119.245.12	192.168.40.129	HTTP	541	HTTP/1.1 404 Not Found (text/html)
29	8.895747500	192.168.40.129	128.119.245.12	HTTP	523	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
33	9.300235606	128.119.245.12	192.168.40.129	HTTP	296	HTTP/1.1 304 Not Modified

Frame 12: 786 bytes on wire (6288 bits), 786 bytes captured (6288 bits) on interface any, id 0

- Linux cooked capture v1
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.40.129
- Transmission Control Protocol, Src Port: 80, Dst Port: 33236, Seq: 1, Ack: 382, Len: 730
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - [HTTP/1.1 200 OK\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Response Version: HTTP/1.1
 - Status Code: 200
 - [Status Code Description: OK]
 - Response Phrase: OK
 - Date: Tue, 20 Aug 2024 09:54:38 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
 - Last-Modified: Tue, 20 Aug 2024 05:59:01 GMT\r\n
 - ETag: "173-620171f4e45ba"\r\n
 - Accept-Ranges: bytes\r\n
 - Content-Length: 371\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: 0.483502425 seconds]
 - [Request in frame: 9]
 - [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)
 - \n
 - <html>\n
 - \n
 - Congratulations again! Now you've downloaded the file lab2-2.html.
\n
 - This file's last modification date will not change. <p>\n
 - Thus if you download this multiple times on your browser, a complete copy
\n
 - will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\n
 - field in your browser's HTTP GET request to the server.\n
 - \n
 - </html>\n

Text item (text), 73 bytes

Packets: 41 · Displayed: 6 (14.6%) · Dropped: 0 (0.0%) Profile: Default

The Request 2 : ➡

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The second pane shows the details of the selected packet (No. 29), which is an HTTP GET request. The third pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
9	0.308598477	192.168.40.129	128.119.245.12	HTTP	437	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
12	0.792100902	128.119.245.12	192.168.40.129	HTTP	786	HTTP/1.1 200 OK (text/html)
15	0.814759688	192.168.40.129	128.119.245.12	HTTP	394	GET /favicon.ico HTTP/1.1
17	1.132472682	128.119.245.12	192.168.40.129	HTTP	541	HTTP/1.1 404 Not Found (text/html)
29	8.895747500	192.168.40.129	128.119.245.12	HTTP	523	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
33	9.300235606	128.119.245.12	192.168.40.129	HTTP	296	HTTP/1.1 304 Not Modified

Packet 29 Details:

- Frame 29: 523 bytes on wire (4184 bits), 523 bytes captured (4184 bits) on interface any, id 0
- Linux cooked capture v1
- Internet Protocol Version 4, Src: 192.168.40.129, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 47700, Dst Port: 80, Seq: 1, Ack: 1, Len: 467
- Hypertext Transfer Protocol
 - GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
 - [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Request Method: GET
 - Request URI: /wireshark-labs/HTTP-wireshark-file2.html
 - Request Version: HTTP/1.1
 - Host: gaia.cs.umass.edu\r\n
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
 - Accept-Language: en-US,en;q=0.5\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Connection: keep-alive\r\n
 - Upgrade-Insecure-Requests: 1\r\n
 - If-Modified-Since: Tue, 20 Aug 2024 05:59:01 GMT\r\n
 - If-None-Match: "173-620171f4e45ba"\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: 33]

Raw Data (Hex/ASCII):

```

0000  00 04 00 01 00 06 00 0c 29 82 9a 35 00 00 08 00  ....5...
0010  45 00 01 fb f5 0c 40 00 40 06 e5 42 c0 a8 28 81  E...@...B...
0020  80 77 f5 0c ba 54 00 50 31 04 ae 55 61 cd 1c 68  -w...T P 1...Ua...h
0030  50 18 7d 78 60 9b 00 00 47 45 54 20 2f 77 69 72  P Jx'... GET /wir
0040  65 73 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50  eshark-l abs/HTTP
0050  2d 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32  -wiresha rk-file2
0060  2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a  .html HT TP/1.1..
0070  48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d  Host: ga ia.cs.um
0080  61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67  ass.edu  User-Ag
0090  65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30  ent: Moz illa/5.0
00a0  20 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 38 36  (X11; L inux x86
00b0  5f 36 34 3b 20 72 76 3a 31 30 39 2e 30 29 20 47  _64; rv: 109.0) G
00c0  65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69  ecko/201 00101 Fi
00d0  72 65 66 6f 78 2f 31 31 35 2e 30 0d 0a 41 63 63  refox/11 5.0 .Acc
00e0  65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61  ept: tex t/html,a
00f0  70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c  pplicati on/xhtml
0100  2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e  +xml,app lication
0110  2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65  /xml;q=0 .9,image
0120  2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70  /avif,im age/webp
0130  2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65  , /*;q=0 .8 Acce
0140  70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d  pt-Langu age: en-
0150  55 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63  US,en;q= 0.5 .Acc
0160  65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a  ept-Encod ing: gz
0170  69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e  ip, defl ate .Con
0180  6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c  nection: keep-al
0190  69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73  ive Upg rade-Ins
01a0  65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20  ecur e-Re quests:
01b0  31 0d 0a 49 66 2d 4d 6f 64 69 66 69 65 64 2d 53  1. If-Mo dified-S
01c0  69 6e 63 65 3a 20 54 75 65 2c 20 32 30 20 41 75  ince: Tu e, 20 Au
01d0  67 20 32 30 32 34 20 30 35 3a 35 39 3a 30 31 20  g 2024 0 5:59:01
01e0  47 4d 54 0d 0a 49 66 2d 4e 6f 6e 65 2d 4d 61 74  GMT- If- None-Mat
01f0  63 68 3a 20 22 31 37 33 2d 36 32 30 31 37 31 66  ch: "173 -620171f
0200  34 65 34 35 62 61 22 0d 0a 0d 0a  ....4e45ba" ...
  
```

Summary: Hypertext Transfer Protocol: Protocol | Packets: 41 · Displayed: 6 (14.6%) · Dropped: 0 (0.0%) | Profile: Default

The Response : ←

The screenshot displays the Wireshark interface with a packet capture of an HTTP transaction. The packet list on the left shows several GET requests, with the final packet (No. 33) being a 304 Not Modified response. The packet details pane on the right provides a hierarchical view of the response structure, including the status code and various headers. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
9	0.308598477	192.168.40.129	128.119.245.12	HTTP	437	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
12	0.792100902	128.119.245.12	192.168.40.129	HTTP	786	HTTP/1.1 200 OK (text/html)
15	0.814759688	192.168.40.129	128.119.245.12	HTTP	394	GET /favicon.ico HTTP/1.1
17	1.132472682	128.119.245.12	192.168.40.129	HTTP	541	HTTP/1.1 404 Not Found (text/html)
29	8.895747500	192.168.40.129	128.119.245.12	HTTP	523	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
33	9.300235606	128.119.245.12	192.168.40.129	HTTP	296	HTTP/1.1 304 Not Modified

Frame 33: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface any, id 0

- Linux cooked capture v1
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.40.129
- Transmission Control Protocol, Src Port: 80, Dst Port: 47700, Seq: 1, Ack: 468, Len: 240
- Hypertext Transfer Protocol
 - HTTP/1.1 304 Not Modified\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
 - [HTTP/1.1 304 Not Modified\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Response Version: HTTP/1.1
 - Status Code: 304
 - [Status Code Description: Not Modified]
 - Response Phrase: Not Modified
 - Date: Tue, 20 Aug 2024 09:54:46 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: "173-620171f4e45ba"\r\n
 - \r\n
 - [HTTP response 1/1]
 - [Time since request: 0.404488106 seconds]
 - [Request in frame: 29]
 - [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

Packet Bytes:

```

0000  00 00 00 01 00 06 00 50 56 eb 67 19 00 00 08 00  ....P V.g....
0010  45 00 01 18 06 9b 00 00 80 06 d4 97 80 77 f5 0c  E.....w...
0020  c0 a8 28 81 00 50 ba 54 61 cd 1c 68 31 04 b0 28  ..(.P.T a..h1..
0030  50 18 fa f0 0f f5 00 00 48 54 54 50 2f 31 2e 31  P..... HTTP/1.1
0040  20 33 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65  304 Not Modifie
0050  64 0d 0a 44 61 74 65 3a 20 54 75 65 2c 20 32 30  d..Date: Tue, 20
0060  20 41 75 67 20 32 30 32 34 20 30 39 3a 35 34 3a  Aug 202 4 09:54:
0070  34 36 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20  46 GMT.. Server:
0080  41 70 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65  Apache/2 .4.6 (Ce
0090  6e 74 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e  ntOS) Op enSSL/1.
00a0  30 2e 32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e  0.2k-fip s PHP/2.
00b0  34 2e 33 33 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e  4.33 mod _perl/2.
00c0  30 2e 31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e  0.11 Per l/v5.16.
00d0  33 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b  3..Conne ction: K
00e0  65 65 70 2d 41 6c 69 76 65 0d 0a 4b 65 65 70 2d  eep-Aliv e..Keep-
00f0  41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35  Alive: t imeout=5
0100  2c 20 6d 61 78 3d 31 30 30 0d 0a 45 54 61 67 3a  , max=10 0..ETag:
0110  20 22 31 37 33 2d 36 32 30 31 37 31 66 34 65 34  "173-62 0171f4e4
0120  35 62 61 22 0d 0a 0d 0a 5ba"....
  
```

Wireshark status bar: Packets: 41 · Displayed: 6 (14.6%) · Dropped: 0 (0.0%) · Profile: Default

8. 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?

- In the first screenshot, which shows the details of the HTTP GET request, the request is as follows:
 - i. **Request Method:** GET
 - ii. **Request URI:** `/wireshark-labs/HTTP-wireshark-file2.html`
 - iii. **Host:** `gaia.cs.umass.edu`
- After looking at the details of this request, there is no “IF-MODIFIED-SINCE” header line included in this HTTP GET request. This means the client did not check whether the file had been modified since a particular date before requesting it.

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

- In the second screenshot, you can see the server’s response to the HTTP GET request:
 - i. **Response Code:** `200 OK`
 - ii. **Content-Type:** `text/html; charset=UTF-8`
 - iii. **Content-Length:** `371 bytes`

- The server responded with a **200 OK** status, which indicates that the request was successful, and it did return the contents of the requested file. The presence of the "Content-Length" header (371 bytes) and the subsequent "Line-based text data" section, which contains the HTML content of the file, further confirms that the server did indeed return the full content of the file. The HTML content includes messages like "Congratulations again! Now you've downloaded the file lab2-2.html," which is part of the file's content.
- This response shows that the server explicitly returned the file, as evidenced by both the status code and the actual content being included in the response.

10. 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?

- In the second screenshot showing the HTTP GET request, we can observe the following details:
 - i. **Request Method:** GET
 - ii. **Request URI:** /wireshark-labs/HTTP-wireshark-file2.html

- iii. **Host:** `gaia.cs.umass.edu`
- Yes, there is an "IF-MODIFIED-SINCE" line in this HTTP GET request. The information that follows the "IF-MODIFIED-SINCE" header is:
 - i. If-Modified-Since: Tue, 20 Aug 2024 05:59:01 GMT
- This indicates that the client is requesting the resource only if it has been modified since the given date and time, which is "Tue, 20 Aug 2024 05:59:01 GMT."
- The presence of this header means that the server will check the last modified time of the requested resource and only return it if it has been updated after the specified date and time. If the file hasn't been modified since that time, the server would typically respond with a `304 Not Modified` status, indicating that the cached version can be used by the client.

11. What is the HTTP status code and phrase returned from the server in response to this HTTP GET? Did the server explicitly return the contents of the file? Explain.

- The HTTP status code returned from the server in response to this HTTP GET request is `304`, and the associated phrase is "Not Modified."

- The 304 Not Modified status code indicates that the requested resource has not been modified since the last time it was accessed. The server does not return the contents of the file in response to a 304 status. Instead, it relies on the client (usually a web browser) to use the cached version of the file that it already has.
- In this case, the server is confirming that the file has not changed since it was last retrieved, so there is no need to resend the file's contents, which helps reduce bandwidth usage.