

Lab 2: Comp Networks

Shrey Kharbanda, Sep 26 2024

```
▼ Hypertext Transfer Protocol
  ▼ 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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36\r\n
    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;c\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Response in frame: 55]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

1. Both my browser and the server are running version: HTTP 1.1
2. It indicates that my browser can accept en-US and en, which are English (US) and English with priority given to en-US and en given a preference weight of 0.9

Source Address: 10.188.136.105

Destination Address: 128.119.245.12

3. My IP Address is 10.188.136.105 and the IP address of the gaia.cs.umass.edu server is 128.119.245.12

```
▼ HTTP/1.1 200 OK\r\n
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
```

4. Status code received from the server to my browser is 200

```
Last-Modified: Thu, 26 Sep 2024 05:59:01 GMT\r\n
```

5. It was last modified on Thursday, September 26, 2024 at 05:59:01 GMT

```
▼ Content-Length: 128\r\n
  [Content length: 128]
```

File Data: 128 bytes

6. 128 bytes are being returned to my browser

7. None, I verified all headers on the packet content window and they're all displayed in the packet-listing window.

No.	Time	Source	Destination	Protocol	Length	Info
53	4.010422	10.188.136.105	128.119.245.12	HTTP	532	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
55	4.092484	128.119.245.12	10.188.136.105	HTTP	540	HTTP/1.1 200 OK (text/html)

<ul style="list-style-type: none"> > Frame 55: 540 bytes on wire (4320 bits), 540 bytes captured > Ethernet II, Src: Dell_82:55:10 (28:47:47:82:55:10), Dst: A > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.1 > Transmission Control Protocol, Src Port: 80, Dst Port: 5617 > Hypertext Transfer Protocol <ul style="list-style-type: none"> > HTTP/1.1 200 OK\r\n Date: Thu, 26 Sep 2024 15:32:32 GMT\r\n Last-Modified: Thu, 26 Sep 2024 05:59:01 GMT\r\n Etag: "80-622ff6f6ad2eb"\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 [Request in frame: 53] [Time since request: 0.082062000 seconds] [Request URI: /wireshark-labs/HTTP-wireshark-file1.html] [Full request URI: http://gaia.cs.umass.edu/wireshark-lab File Data: 128 bytes > Line-based text data: text/html (4 lines) 	<pre> 0010 02 0e ad ee 40 00 2c 06 96 52 80 77 15 0c 0a bc ...@...R-w... 0020 88 69 00 50 db 6d 67 1b 0e 67 17 62 39 a1 58 18 ...i-P mg g b9-P 0030 00 ed 28 f4 00 00 48 54 54 50 2f 31 2e 31 20 32 ...(-...HT P/1.1 2 0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75 ...00 OK--D ate: Thu 0050 2c 20 32 36 20 53 65 70 20 32 30 32 34 20 31 35 ... 26 Sep 2024 15 0060 3a 33 32 3a 33 32 20 47 4d 54 0d 0a 53 65 72 76 ...:32:32 G MT--Serv 0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 ...err: Apac he/2.4.6 0080 20 20 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 ... (CentOS) openSS 0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 .../1.0.2k -fips PH 00a0 50 2f 37 2e 34 2e 33 33 20 6d 6f 64 5f 70 65 72 ...P/7.4.33 mod_per 00b0 6e 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 .../2.0.11 Perl/v5 00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 ...16.3.1 Last-Modi 00d0 60 69 65 64 3a 20 54 68 75 2c 20 32 36 20 53 65 ...fied: Thu, 26 Se 00e0 70 20 32 30 32 34 20 30 35 3a 35 39 3a 30 31 20 ... p 2024 0 5:59:01 00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 36 ...GMT--Etag: "80-6 0100 32 32 66 66 36 66 36 61 64 32 65 38 22 0d 0a 41 ...22ff6f6a d2eb"--A 0110 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 ...ccept-Ra nges: by 0120 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e ...tes--Con tent-Len 0130 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41 ...gth: 128 --Keep-A 0140 60 69 70 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c ...Live: ti meout=5, 0150 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 ...max=100 --Connecc 0160 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 ...tion: Ke ep-Alive 0170 0d 0a 43 6f 6e 74 65 6e 74 2d 54 70 65 3a 20 ...--Content t-type: 0180 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 ...text/html; chars 0190 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d ...et=UTF-8 --...chtn 01a0 6e 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f ...l- Congratulation 01b0 6e 73 2e 20 59 6f 75 27 76 65 20 64 6f 77 6e ...ns. You 've down 01c0 6c 6f 61 64 65 64 20 74 68 65 20 60 69 6c 65 20 ...loaded t he file 01d0 0a 6d 74 74 7a 3a 2f 2f 61 69 61 2e 63 73 2e ...http:// gaia.cs. 01e0 75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 73 68 ...umass.ed u/wiresh 01f0 61 72 6b 2d 6c 61 62 73 2f 48 54 54 5d 2d 77 69 ...ark-labs /HTTP-wi 0200 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 ...reshark- file1.ht 0210 6d 6c 21 0a 3c 2f 68 74 6d 6c 3e 0a ...ml!</ht ml>-> </pre>
--	---

- Hypertext Transfer Protocol
 - GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1
 - Host: gaia.cs.umass.edu\r\n
 - Connection: keep-alive\r\n
 - Upgrade-Insecure-Requests: 1\r\n
 - User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 1
 - Accept: text/html,application/xhtml+xml,application/
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: en-US,en;q=0.9\r\n
 - \r\n

[Response in frame: 35]

[Full request URI: http://gaia.cs.umass.edu/wireshar

8.

No, there is no

“IF-MODIFIED-SINCE” line in the first HTTP GET request.

<ul style="list-style-type: none"> <ul style="list-style-type: none"> 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 [Request in frame: 33] [Time since request: 0.096175000 seconds] [Request URI: /wireshark-labs/HTTP-wireshark-file2.html] [Full request URI: http://gaia.cs.umass.edu/wireshark-lab File Data: 371 bytes > Line-based text data: text/html (10 lines) \n <html>\n \n Congratulations again! Now you've downloaded the file. This file's last modification date will not change. <p> Thus if you download this multiple times on your brows will only be sent once by the server due to the inclusio field in your browser's HTTP GET request to the server. \n </html>\n 	<pre> 0190 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 set=UTF-8 --...<h 01a0 74 6d 6c 3e 0a 0a 43 6f 6e 67 72 61 74 75 6c 61 tml>-> Co ngratula 01b0 74 69 6f 6e 73 20 61 67 61 69 6e 21 20 20 4e 6f tions ag ain! No 01c0 77 20 79 6f 75 27 76 65 20 64 6f 77 6e 6c 6f 61 w you've downloa 01d0 64 65 64 20 74 68 65 20 66 69 6c 65 20 6c 61 62 ded the file lab 01e0 32 2d 32 2e 68 74 6d 6c 2e 20 3c 62 72 3e 0a 54 2-2.html.
T 01f0 68 69 73 20 66 69 6c 65 27 73 20 6c 61 73 74 20 his file 's last 0200 6d 6f 64 69 66 69 63 61 74 69 6f 6e 20 64 61 74 modifia tion dat 0210 65 20 77 69 6c 6c 20 6e 6f 74 20 63 68 61 6e 67 e will n ot chang 0220 65 2e 20 20 3c 70 3e 0a 54 68 75 73 20 20 69 66 e. <p> Thus if 0230 20 79 6f 75 20 64 6f 77 6e 6c 6f 61 64 20 74 68 you down load th 0240 69 73 20 6d 75 6c 74 69 70 6c 65 20 74 69 6d 65 is multi ple time 0250 73 20 6f 6e 20 79 6f 75 72 20 62 72 6f 77 73 65 s on you r browse 0260 72 2c 20 61 20 63 6f 6d 70 6c 65 74 65 20 63 6f r, a com plete co 0270 70 79 20 3c 62 72 3e 0a 77 69 6c 6c 20 6f 6e 6c py
 will onl 0280 79 20 62 65 20 73 65 6e 74 20 6f 6e 63 65 20 62 y be sen t once b 0290 79 20 74 68 65 20 73 65 72 76 65 72 20 64 75 65 y the se rver due 02a0 20 74 6f 20 74 68 65 20 69 6e 63 6c 75 73 69 6f to the inclusio 02b0 6e 20 6f 66 20 74 68 65 20 49 4e 2d 4d 4f 44 49 n of the IN-MODI 02c0 46 49 45 44 2d 53 49 4e 43 45 3c 62 72 3e 0a 66 FIED-SIN CE-br> f 02d0 69 65 6c 64 20 69 6e 20 79 6f 75 72 20 62 72 6f ield in your bro 02e0 77 73 65 72 27 73 20 48 54 54 5d 2d 47 45 54 20 user's H TTP GET 02f0 72 65 71 75 65 73 74 20 74 6f 20 74 68 65 20 73 request to the s 0300 65 72 76 65 72 2e 0a 0a 3c 2f 68 74 6d 6c 3e 0a erver...</html>-> </pre>
---	---

9.

The server explicitly returned the file contents since the headers File Data and Content-Length are present with the actual text data under “Line-based text data” section of Wireshark’s packet listings window along with the content seen in the packet contents window

```

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
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  If-None-Match: "173-622ff6f6acb18"\r\n
  If-Modified-Since: Thu, 26 Sep 2024 05:59:01 GMT\r\n
\r\n
[Response in frame: 76]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

```

10.

Yes, there is an “IF-MODIFIED-SINCE:” line in the second HTTP GET. It contains the date and time of the time the file was last accessed by me, in this case, it is Thursday, 26 September 2024, 05:59:01 GMT.

```

Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Response Version: HTTP/1.1
  Status Code: 304
  [Status Code Description: Not Modified]
  Response Phrase: Not Modified
  Date: Thu, 26 Sep 2024 16:48:16 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 m
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=99\r\n
  ETag: "173-622ff6f6acb18"\r\n
\r\n
[Request in frame: 53]
[Time since request: 0.101979000 seconds]
[Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTT

```

11.

The Status code is 304: Not Modified; The server did not explicitly return the contents of the file because the browser simply retrieved the contents from its cache. If the file had been modified since it was last accessed by me, it would return the contents of the file, instead this status code indicated to my browser to simply retrieve the old file from its cached memory.

12. My browser only sent 1 HTTP GET Request with packet number: 261

No.	Time	Source	Destination	Protocol	Length	Info
261	12.075487	10.188.136.105	128.119.245.12	HTTP	532	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1

13. The packet number associated with the response to the GET Request in 12. is 268.

268	12.185089	128.119.245.12	10.188.136.105	HTTP	535	HTTP/1.1 200 OK (text/html)
-----	-----------	----------------	----------------	------	-----	-----------------------------

14. The code was 200 and Phrase was OK

```
  HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
```

15. The data was sent in 4 TCP segments to the browser and were reassembled later.

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 57528, Seq: 4381, Ac
> [4 Reassembled TCP Segments (4861 bytes): #265(1460), #266(1460), #267(1460)
  Hypertext Transfer Protocol
```

16. My browser sent 3 HTTP GET message requests. They were sent to: Initial Page address and Pearson Logo Image address : 128.119.245.12 and the pearson bookcover image address: 178.79.137.164

17. They were downloaded rather parallelly from the two websites since the two GET requests were sent almost simultaneously (with only a small time gap of 0.03 seconds). If they were sent serially, the first GET request would be responded to until the second GET request was sent and responded back to.

No.	Time	Source	Destination	Protocol	Length	Info
351	8.053769	10.188.136.105	128.119.245.12	HTTP	532	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
356	8.135860	128.119.245.12	10.188.136.105	HTTP	1355	HTTP/1.1 200 OK (text/html)
358	8.169345	10.188.136.105	128.119.245.12	HTTP	478	GET /pearson.png HTTP/1.1
403	8.197333	10.188.136.105	178.79.137.164	HTTP	457	GET /8E_cover_small.jpg HTTP/1.1
412	8.208649	178.79.137.164	10.188.136.105	HTTP	237	HTTP/1.1 301 Moved Permanently
493	8.253761	128.119.245.12	10.188.136.105	HTTP	745	HTTP/1.1 200 OK (PNG)

I believe that my browser (Chrome) has the ability to make these simultaneous requests in parallel for resources such as images for a smoother experience.

18. The servers initial response was “401 Unauthorized”

138	5.438975	10.188.136.105	128.119.245.12	HTTP	548	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP...
143	5.534979	128.119.245.12	10.188.136.105	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
384	24.449845	10.188.136.105	128.119.245.12	HTTP	633	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP...
396	24.536637	128.119.245.12	10.188.136.105	HTTP	544	HTTP/1.1 200 OK (text/html)

19. The new field in the second GET Request is the Authorization field. This is included as I sent the server a username and password along with the request such that I was

authorized to receive the page.

```

  ▾ Hypertext Transfer Protocol
    ▾ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      Cache-Control: max-age=0\r\n
    ▾ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=\r\n
      Credentials: wireshark-students:network
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9\r\n
      \r\n

```