

LAB 4

Question 1.2

- 1) Browser - HTTP Version 1.1
Server - HTTP Version 1.1
- 2) Language Supported - English (US)
- 3) Computer IP Address - 192.168.43.119 (IPv4)
Server IP Address - 128.119.245.12 (IPv4)
- 4) Status Code returned - 200
- 5) Last Modified - Sat, 26 Sep 2020 05:59:01 GMT
- 6) Content Length - 128 Bytes

```
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 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
```

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 26 Sep 2020 09:53:21 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sat, 26 Sep 2020 05:59:01 GMT\r\n
    ETag: "80-5b0312148b021"\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
```

Question 2.2

- 1) No such line present.
- 2) Yes. Status Code is 200 hence it is explicitly sent from the server.

```
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. <br>\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 <br>\r\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\r\n
field in your browser's HTTP GET request to the server.\r\n
\r\n
</html>\r\n
```

3) No IF-MODIFIED in 1st GET.

Second GET Request has an IF-MODIFIED followed by Last Modified - Sat, 26 Sep 2020 05:59:01 GMT.

4) Status Code is 304 (Description - Not Modified). The server explicitly didn't explicitly return the file as it was already present in the cache.

No.	Time	Source	Destination	Protocol	Length	Info
2432	11.741885	192.168.43.119	128.119.245.12	HTTP	440	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2521	12.049136	128.119.245.12	192.168.43.119	HTTP	784	HTTP/1.1 200 OK (text/html)
2585	12.312647	192.168.43.119	128.119.245.12	HTTP	321	GET /favicon.ico HTTP/1.1
2643	12.624327	128.119.245.12	192.168.43.119	HTTP	539	HTTP/1.1 404 Not Found (text/html)
2996	14.609999	192.168.43.119	128.119.245.12	HTTP	552	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
3054	14.997308	128.119.245.12	192.168.43.119	HTTP	293	HTTP/1.1 304 Not Modified

> Frame 2996: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \Device\NPF_{BF9054D7-661E-47B7-ADE5-50DDC93A1E9B}, id 0
> Ethernet II, Src: c6:d2:90:e1:ef:05 (c6:d2:90:e1:ef:05), Dst: ce:bf:58:81:ac:42 (ce:bf:58:81:ac:42)
> Internet Protocol Version 4, Src: 192.168.43.119, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55582, Dst Port: 80, Seq: 387, Ack: 731, Len: 498
▼ 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 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
DNT: 1\r\n
If-Modified-Since: Sat, 26 Sep 2020 05:59:01 GMT\r\n
If-None-Match: "173-5b03121488528"\r\n
Cache-Control: max-age=0\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 2/2]

Question 3.2

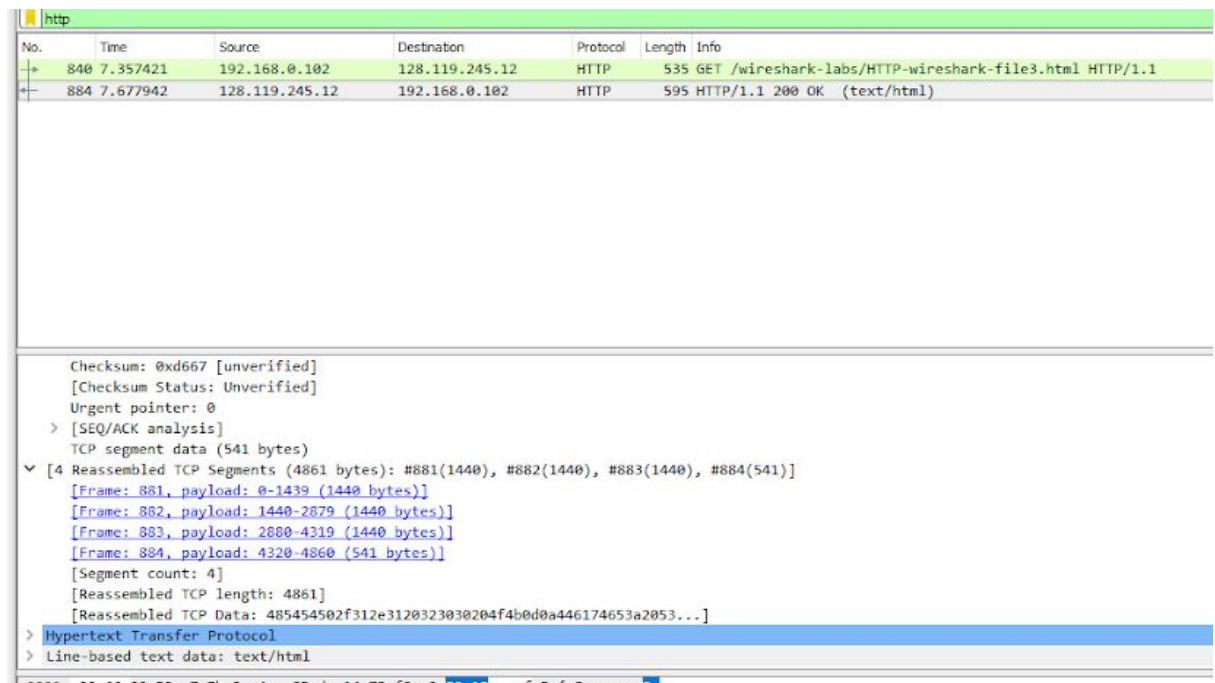
1. Just one HTTP sent request message was sent by the browser.



The screenshot shows a Wireshark packet capture window titled "Wi-Fi". The packet list on the left shows two packets. The first packet is an HTTP GET request from 192.168.1.9 to 128.119.245.12. The second packet is an HTTP 200 OK response from 128.119.245.12 to 192.168.1.9. The packet details pane on the right shows the structure of the HTTP response, including the status line "HTTP/1.1 200 OK (text/html)".

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000000	192.168.1.9	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
4	0.000000	128.119.245.12	192.168.1.9	HTTP	679	HTTP/1.1 200 OK (text/html)

2. There are 4 TCP segments.



The screenshot shows a Wireshark packet capture window titled "http". The packet list on the left shows two packets. The first packet is an HTTP GET request from 192.168.0.102 to 128.119.245.12. The second packet is an HTTP 200 OK response from 128.119.245.12 to 192.168.0.102. The packet details pane on the right shows the structure of the HTTP response, including the status line "HTTP/1.1 200 OK (text/html)".

No.	Time	Source	Destination	Protocol	Length	Info
840	7.357421	192.168.0.102	128.119.245.12	HTTP	535	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
884	7.677942	128.119.245.12	192.168.0.102	HTTP	595	HTTP/1.1 200 OK (text/html)

Checksum: 0xd667 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> [SEQ/ACK analysis]
TCP segment data (541 bytes)
[4 Reassembled TCP Segments (4861 bytes): #881(1440), #882(1440), #883(1440), #884(541)]
[Frame: 881, payload: 0-1439 (1440 bytes)]
[Frame: 882, payload: 1440-2879 (1440 bytes)]
[Frame: 883, payload: 2880-4319 (1440 bytes)]
[Frame: 884, payload: 4320-4860 (541 bytes)]
[Segment count: 4]
[Reassembled TCP length: 4861]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053...]
> Hypertext Transfer Protocol
> Line-based text data: text/html

3. HTTP/1.1 200 OK (Above screenshot).

Question 4.2

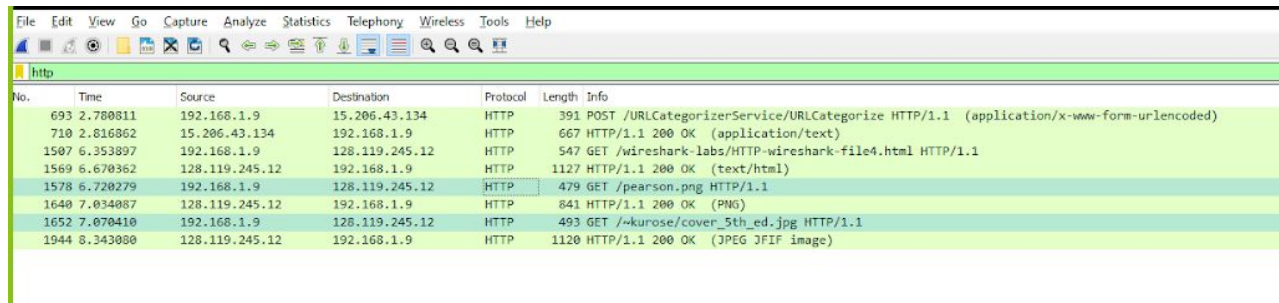
- 3 GET requests were sent:

GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n

GET /pearson.png HTTP/1.1\r\n

GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\n

They were sent to the destination: 128.119.245.12



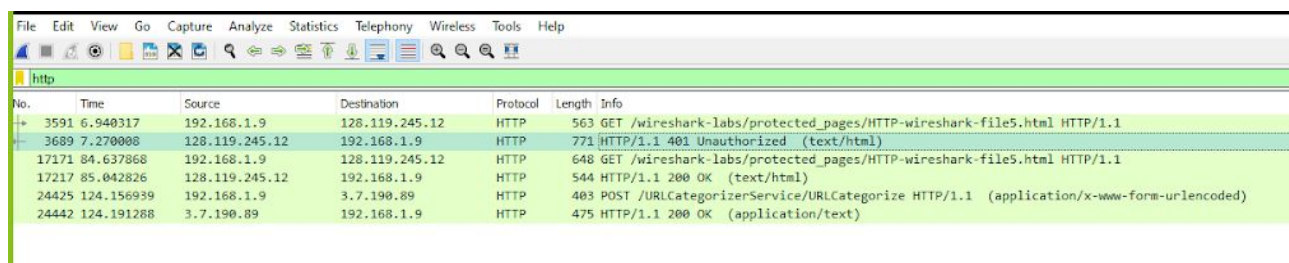
No.	Time	Source	Destination	Protocol	Length	Info
693	2.760811	192.168.1.9	15.206.43.134	HTTP	391	POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
710	2.816862	15.206.43.134	192.168.1.9	HTTP	667	HTTP/1.1 200 OK (application/text)
1507	6.353897	192.168.1.9	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
1569	6.670362	128.119.245.12	192.168.1.9	HTTP	1127	HTTP/1.1 200 OK (text/html)
1578	6.720279	192.168.1.9	128.119.245.12	HTTP	479	GET /pearson.png HTTP/1.1
1640	7.034087	128.119.245.12	192.168.1.9	HTTP	841	HTTP/1.1 200 OK (PNG)
1652	7.070410	192.168.1.9	128.119.245.12	HTTP	493	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
1944	8.343000	128.119.245.12	192.168.1.9	HTTP	1120	HTTP/1.1 200 OK (JPEG JFIF image)

- The two images were downloaded serially because the timestamps were different and also, the source port is incrementing each time which means that the images were received serially over separate TCP connections.

Question 5.2

- The server's response to initial GET request was:

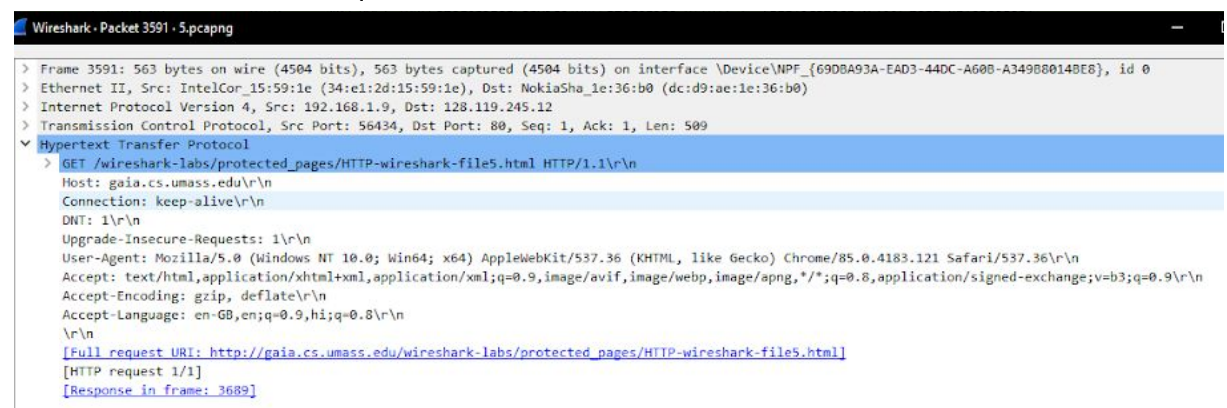
HTTP/1.1 401 Unauthorized



No.	Time	Source	Destination	Protocol	Length	Info
3591	6.940317	192.168.1.9	128.119.245.12	HTTP	563	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
3689	7.270008	128.119.245.12	192.168.1.9	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
17171	84.637868	192.168.1.9	128.119.245.12	HTTP	648	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
17217	85.042826	128.119.245.12	192.168.1.9	HTTP	544	HTTP/1.1 200 OK (text/html)
24425	124.156939	192.168.1.9	3.7.190.89	HTTP	403	POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
24442	124.191288	3.7.190.89	192.168.1.9	HTTP	475	HTTP/1.1 200 OK (application/text)

- The second GET message contains an authorization field which is not present in the first GET message.

Screenshot of first GET request



```
Wireshark - Packet 3591 - 5.pcapng

> Frame 3591: 563 bytes on wire (4504 bits), 563 bytes captured (4504 bits) on interface \Device\NPF_{69DDA93A-EAD3-44DC-A600-A349B8014BE8}, id 0
> Ethernet II, Src: IntelCor_15:59:1e (34:e1:2d:15:59:1e), Dst: NokiaSha_1e:36:b0 (dc:d9:ae:1e:36:b0)
> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56434, Dst Port: 80, Seq: 1, Ack: 1, Len: 509
  > Hypertext Transfer Protocol
    > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      DNT: 1\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/85.0.4183.121 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;q=0.9\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-GB,en;q=0.9,hi;q=0.8\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
      [HTTP request 1/1]
      [Response in frame: 3689]
```

Screenshot of the second GET request

```
Wireshark - Packet 17171 - 5.pcapng

> Frame 17171: 648 bytes on wire (5184 bits), 648 bytes captured (5184 bits) on interface \Device\NPF_{69DBA93A-EAD3-44DC-A60B-A349B80148E8}, id 0
> Ethernet II, Src: IntelCor_15:59:1e (34:e1:2d:15:59:1e), Dst: NokiaSha_1e:36:b0 (dc:d9:ae:1e:36:b0)
> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56440, Dst Port: 80, Seq: 1, Ack: 1, Len: 594
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.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
  ▼ Authorization: Basic d2lyZXNoYXJrLXN8dWRlbnRzOm5ldHdvcm5=\r\n
    Credentials: wireshark-students:network
    DNT: 1\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/85.0.4183.121 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;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en;q=0.9,hi;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
    [Response in frame 17217]
```