Marl Rico

CPSC 353

Mr. Heckathorn

Final Project: Wireshark

1. List 3 different protocols that appear in the protocol column in the unfiltered

packet-listing window in step 7 above.

a) MDNS

b) TCP

c) TLSv1.2

2. How long did it take from when the HTTP GET message was sent until the HTTP

OK reply was received? (By default, the value of the Time column in the packetlisting window is the amount of time, in seconds, since Wireshark tracing began.

To display the Time field in time-of-day format, select the Wireshark View pull

down menu, then select Time Display Format, then select Time-of-day.)

a) 0.092857 seconds

3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

a) gaia.cs.umass.edu : 128.119.245.12

b) my address: 192.168.0.61

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To

do so, select Print from the Wireshark File command menu, and select the

“Selected Packet Only” and “Print as displayed” radial buttons, and then click

OK.

```
C:\Users\mrmar\AppData\Local\Temp\wireshark_Wi-FiPCNRD1.pcapng 56 total packets, 2 shown

No.     Time               Source                Destination           Protocol Length Info
     20 15:24:20.165019    192.168.0.61          128.119.245.12        HTTP     641    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 20: 641 bytes on wire (5128 bits), 641 bytes captured (5128 bits) on interface \Device\NPF_{28039E94-B44D-42AF-
AB6C-2E368514CE2C}, id 0
Ethernet II, Src: IntelCor_e5:ae:d4 (a0:51:0b:e5:ae:d4), Dst: Motorola_e6:bc:39 (c8:c7:50:e6:bc:39)
Internet Protocol Version 4, Src: 192.168.0.61, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49916, Dst Port: 80, Seq: 1, Ack: 1, Len: 587
Hypertext Transfer Protocol
No.     Time               Source                Destination           Protocol Length Info
     23 15:24:20.257876    128.119.245.12        192.168.0.61          HTTP     293    HTTP/1.1 304 Not Modified
Frame 23: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{28039E94-B44D-42AF-
AB6C-2E368514CE2C}, id 0
Ethernet II, Src: Motorola_e6:bc:39 (c8:c7:50:e6:bc:39), Dst: IntelCor_e5:ae:d4 (a0:51:0b:e5:ae:d4)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.61
Transmission Control Protocol, Src Port: 80, Dst Port: 49916, Seq: 1, Ack: 588, Len: 239
Hypertext Transfer Protocol
```

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

a) HTTP version 1.1
b) HTTP version 1.1

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

a) en-US

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

a) my computer: 192.168.0.61

b) gaia.cs.umass.edu: 128.119.245.12

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

a) 200 OK

```
No.     Time               Source                Destination           Protocol Length Info
    293 16:02:55.913252    128.119.245.12        192.168.0.61          HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 293: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{28039E94-B44D-42AF-
AB6C-2E368514CE2C}, id 0
Ethernet II, Src: 39:bc:e6:50:c7:c8 (39:bc:e6:50:c7:c8), Dst: IntelCor_e5:ae:d4 (a0:51:0b:e5:ae:d4)
```

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

a) Last-Modified: Tue, 07 Dec 2021 06:59:01 GMT

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

a) 128 bytes

11. 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.

a) **There's no headers within the data that are not displayed in the packet-listing window**.

12. 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?

a) There's no "IF-MODIFIED-SINCE" line if the first HTTP GET

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

a) Yes, the server explicitly return the contents of the file. It is under the Line-based text data.

```
    [Request in frame: 17]
    [Next request in frame: 25]
    [Next response in frame: 26]
    [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. <br>\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 <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

14. 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?

a) Yes, there is a "IF-MODDED-SINCE:" line in the second HTTP GET

b) Tue, 07 Dec 2021 06:59:01 GMT

```
    Request Version: HTTP/1.1
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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36\r
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-5d288e8841b70"\r\n
If-Modified-Since: Tue, 07 Dec 2021 06:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 2/2]
[Prev request in frame: 17]
[Response in frame: 26]
```

15. 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

a) **The HTTP status code and phrase return from the server in response to the second HTTP GET is HTTP/1.1 305 Not Modified**
b) **The server didn't explicitly return the contents of the file thus, making it shorter and just reusing the first HTTP GET since the file is "Not Modified"**

No.	Time	Source	Destination	Protocol	Length	Info
17	16:29:00.024009	192.168.0.61	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
19	16:29:00.121066	128.119.245.12	192.168.0.61	HTTP	784	HTTP/1.1 200 OK (text/html)
25	16:29:03.967347	192.168.0.61	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
26	16:29:04.057370	128.119.245.12	192.168.0.61	HTTP	293	HTTP/1.1 304 Not Modified

```
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
Date: Wed, 08 Dec 2021 00:29:04 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=99\r\n
ETag: "173-5d288e8841b70"\r\n
\r\n
[HTTP response 2/2]
[Time since request: 0.090023000 seconds]
[Prev request in frame: 17]
[Prev response in frame: 19]
[Request in frame: 25]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

16. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

a) **My browser only sent one HTTP GET request message.**

b) **Packet number 16 in the trace contains the GET message for the Bill of Rights**

No.	Time	Source	Destination	Protocol	Length	Info
16	20:53:10.631591	192.168.0.61	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
21	20:53:10.725809	128.119.245.12	192.168.0.61	HTTP	535	HTTP/1.1 200 OK (text/html)

17. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

a) **Packet number 21 in the trace contains the status code and phrase associated with the response of the HTTP GET request.**

No.	Time	Source	Destination	Protocol	Length	Info
16	20:53:10.631591	192.168.0.61	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
21	20:53:10.725809	128.119.245.12	192.168.0.61	HTTP	535	HTTP/1.1 200 OK (text/html)

18. What is the status code and phrase in the response?

a) The status code and phrase in the response is 200 OK

No.	Time	Source	Destination	Protocol	Length	Info
16	20:53:10.631591	192.168.0.61	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
21	20:53:10.725809	128.119.245.12	192.168.0.61	HTTP	535	HTTP/1.1 200 OK (text/html)

19. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

a) 4 data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.

```
Transmission Control Protocol, Src Port: 80, Dst Port: 55300, Seq: 4381, Ack: 476, Len: 481
[4 Reassembled TCP Segments (4861 bytes): #18(1460), #19(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]
```

20. How many HTTP GET request messages did your browser send? To which

Internet addresses were these GET requests sent?

a) 3 HTTP GET request messages were sent by my browser.

b) The internet addresses were 128.119.245.12 and 178.79.137.164

No.	Time	Source	Destination	Protocol	Length	Info
7	21:11:56.948165	192.168.0.61	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
13	21:11:57.042764	128.119.245.12	192.168.0.61	HTTP	1355	HTTP/1.1 200 OK (text/html)
15	21:11:57.118026	192.168.0.61	128.119.245.12	HTTP	475	GET /pearson.png HTTP/1.1
22	21:11:57.207332	128.119.245.12	192.168.0.61	HTTP	745	HTTP/1.1 200 OK (PNG)
28	21:11:57.380523	192.168.0.61	178.79.137.164	HTTP	442	GET /8E_cover_small.jpg HTTP/1.1
35	21:11:57.519536	178.79.137.164	192.168.0.61	HTTP	225	HTTP/1.1 301 Moved Permanently

21. Can you tell whether your browser downloaded the two images serially, or

whether they were downloaded from the two web sites in parallel? Explain.

a) The browser downloaded the two images serially it is because after the first image was requested and send, that was when the browser requested and sent the second photo. This means that the two images were not downloaded from two website in parallel.

22. What is the server's response (status code and phrase) in response to the initial

HTTP GET message from your browser?

a) The initial response to the HTTP GET message from my browser is 401 Unauthorized

No.	Time	Source	Destination	Protocol	Length	Info
8	21:27:18.953270	192.168.0.61	128.119.245.12	HTTP	545	GET /wireshark-labs/protected_pages/HTTP-wireshark-file
12	21:27:19.049090	128.119.245.12	192.168.0.61	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
39	21:27:28.518306	192.168.0.61	128.119.245.12	HTTP	630	GET /wireshark-labs/protected_pages/HTTP-wireshark-file
43	21:27:28.612404	128.119.245.12	192.168.0.61	HTTP	544	HTTP/1.1 200 OK (text/html)

23. When your browser's sends the HTTP GET message for the second time, what

new field is included in the HTTP GET message?

a) **When the browser sends the second HTTP GET message the new field that is included in the message is Authorization: means that my browser is authorized to grab the information.**

```
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36\r
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\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: 43]
```