

Assignment 5

Computer Networks Lab

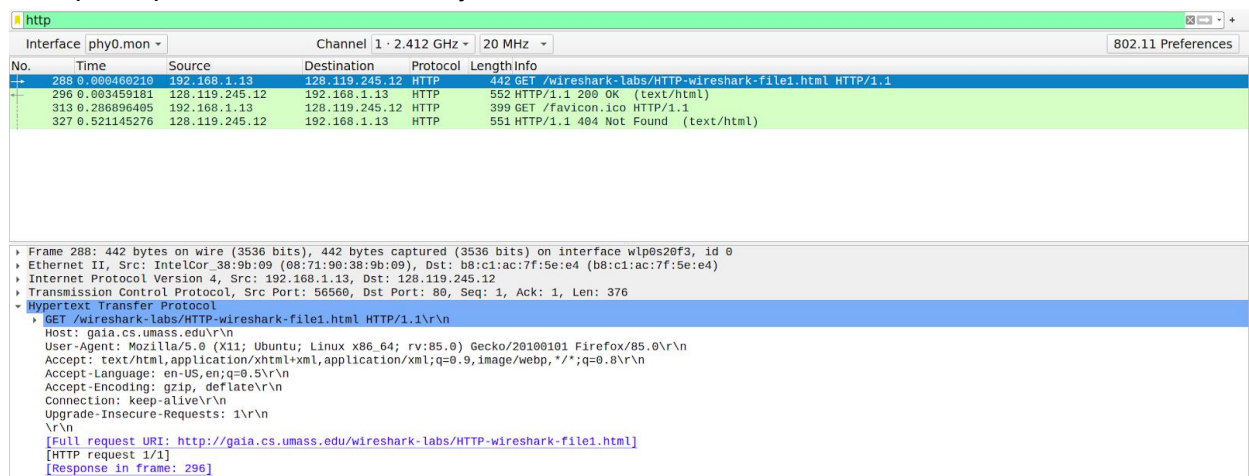
T Satwik

Roll no: 190030043

IP Address: 192.168.1.13

Q1. The Basic HTTP GET/response interaction.

- 1) The browser is running the HTTP 1.1 version as we can see in the first line in the Hypertext Transfer Protocol section in the GET request message. The server is also using HTTP 1.1 version as we can see in the first line of Hypertext Transfer Protocol section in the response message.
- 2) The languages accepted are en-US, en, which means US english and english. This can be seen in the Accept-Language line in the Hypertext Transfer Protocol section in the GET request message.
- 3) The IP address of my computer is 192.168.1.13, as we can see in the Source Address line in the Internet Protocol Section. The IP address of gaia.cs.umass.edu server is 128.119.245.12, as we can see in the Destination Address line in the Internet Protocol Section.
- 4) Status Code returned by the server to the browser is 200 OK, as we can see in the first line of Hypertext Transfer Protocol section in the response message.
- 5) The HTML file was last modified Thu, 04 Mar 2021 06:59:01 GMT, as we can see in the Last Modified line of Hypertext Transfer Protocol section in the response message.
- 6) 128 bytes of data is being returned by the server to the browser, as we can see in the Content Length line of Hypertext Transfer Protocol section in the response message.
- 7) No, there are no headers in the packet content window that are not listed in the packet-listing window. I have attached the screenshot of the packet content window in the zip file, please refer if necessary.



The screenshot shows a Wireshark packet capture on the 'http' filter. The packet list shows three packets: a GET request (288 bytes), a 200 OK response (552 bytes), and a 309 GET for a favicon (399 bytes). The packet details pane is expanded for the first packet (288 bytes), showing the Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol sections. The Hypertext Transfer Protocol section shows the request line 'GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1' and various headers including Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Connection, and Upgrade-Insecure-Requests. The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
288	0.000460210	192.168.1.13	128.119.245.12	HTTP	442	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
296	0.003459131	128.119.245.12	192.168.1.13	HTTP	552	HTTP/1.1 200 OK (text/html)
313	0.286896405	192.168.1.13	128.119.245.12	HTTP	399	GET /favicon.ico HTTP/1.1
327	0.521145276	128.119.245.12	192.168.1.13	HTTP	551	HTTP/1.1 404 Not Found (text/html)

Frame 288: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface wlp8s20f3, id 0
Ethernet II, Src: IntelCor_38:9b:09 (08:71:98:38:9b:09), Dst: b8:c1:ac:7f:5e:e4 (b8:c1:ac:7f:5e:e4)
Internet Protocol Version 4, Src: 192.168.1.13, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56560, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
[HTTP request 1/1]
[Response in frame: 296]

Q1 HTTP GET request

http						
Interface phy0.mon		Channel 1 - 2.412 GHz		20 MHz		
No.	Time	Source	Destination	Protocol	Length	Info
288	0.000460210	192.168.1.13	128.119.245.12	HTTP	442	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
296	0.003459181	128.119.245.12	192.168.1.13	HTTP	552	HTTP/1.1 200 OK (text/html)
313	0.266896405	192.168.1.13	128.119.245.12	HTTP	399	GET /favicon.ico HTTP/1.1
327	0.521145276	128.119.245.12	192.168.1.13	HTTP	551	HTTP/1.1 404 Not Found (text/html)

<p>Frame 296: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface wlp0s20f3, id 0</p> <p>Ethernet II, Src: b8:c1:ac:7f:5e:e4 (b8:c1:ac:7f:5e:e4), Dst: IntelCor_38:9b:09 (08:71:90:38:9b:09)</p> <p>Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.13</p> <p>Transmission Control Protocol, Src Port: 80, Dst Port: 56560, Seq: 1, Ack: 377, Len: 486</p> <p>Hypertext Transfer Protocol</p> <p>HTTP/1.1 200 OK\r\n</p> <p>Date: Fri, 05 Mar 2021 04:26:20 GMT\r\n</p> <p>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</p> <p>Last-Modified: Thu, 04 Mar 2021 06:59:01 GMT\r\n</p> <p>Etag: "80-5bcb808a2bb28"\r\n</p> <p>Accept-Ranges: bytes\r\n</p> <p>Content-Length: 128\r\n</p> <p>Keep-Alive: timeout=5, max=100\r\n</p> <p>Connection: Keep-Alive\r\n</p> <p>Content-Type: text/html; charset=UTF-8\r\n</p> <p>\r\n</p> <p>[HTTP response 1/1]</p> <p>[Time since request: 0.317718195 seconds]</p> <p>[Request in frame: 288]</p> <p>[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]</p> <p>File Data: 128 bytes</p> <p>Line-based text data: text/html (4 lines)</p> <p><html>\n</p> <p>Congratulations. You've downloaded the file \n</p> <p>http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html\n</p> <p></html>\n</p>

Q1 HTTP OK response

Q2. The HTTP CONDITIONAL GET/response interaction.

- 8) No, there is no "IF-MODIFIED-SINCE" line in the first HTTP GET request packet.
- 9) Yes, the server explicitly returned the contents of the file to the browser, as the Line-based text data section in the response message shows the whole content of the html file.
- 10) Yes, there is a "IF-MODIFIED-SINCE" line in the second HTTP GET request packet. The information that follows is the date and time at which the browser first downloaded the resource, in my case the value was Thu, 04 Mar 2021 06:59:01 GMT.
- 11) The HTTP status code and phrase returned from the server in response to this second HTTP GET is 304 Not Modified. The server didn't return the content explicitly, as there is no Line-based text data section. Since the webpage is not modified, the browser displays the previously downloaded web page from the cache.

http						
Interface phy0.mon		Channel 1 - 2.412 GHz		20 MHz		
No.	Time	Source	Destination	Protocol	Length	Info
113	0.000381864	192.168.1.13	128.119.245.12	HTTP	442	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
121	0.002493902	128.119.245.12	192.168.1.13	HTTP	796	HTTP/1.1 200 OK (text/html)
127	0.034615063	192.168.1.13	128.119.245.12	HTTP	399	GET /favicon.ico HTTP/1.1
140	0.001854926	128.119.245.12	192.168.1.13	HTTP	551	HTTP/1.1 404 Not Found (text/html)
250	0.000422103	192.168.1.13	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
264	0.001450557	128.119.245.12	192.168.1.13	HTTP	306	HTTP/1.1 304 Not Modified

<p>Frame 250: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface wlp0s20f3, id 0</p> <p>Ethernet II, Src: IntelCor_38:9b:09 (08:71:90:38:9b:09), Dst: b8:c1:ac:7f:5e:e4 (b8:c1:ac:7f:5e:e4)</p> <p>Internet Protocol Version 4, Src: 192.168.1.13, Dst: 128.119.245.12</p> <p>Transmission Control Protocol, Src Port: 57214, Dst Port: 80, Seq: 1, Ack: 1, Len: 488</p> <p>Hypertext Transfer Protocol</p> <p>GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n</p> <p>Host: gaia.cs.umass.edu\r\n</p> <p>User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0\r\n</p> <p>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n</p> <p>Accept-Language: en-US,en;q=0.5\r\n</p> <p>Accept-Encoding: gzip, deflate\r\n</p> <p>Connection: keep-alive\r\n</p> <p>Upgrade-Insecure-Requests: 1\r\n</p> <p>If-Modified-Since: Thu, 04 Mar 2021 06:59:01 GMT\r\n</p> <p>If-None-Match: "1f3-5bcb808a2af78"\r\n</p> <p>Cache-Control: max-age=0\r\n</p> <p>\r\n</p> <p>[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]</p> <p>[HTTP request 1/1]</p> <p>[Response in frame: 254]</p>
--

Q2 Second GET request

http						
Interface phy0.mon		Channel 1 · 2.412 GHz		20 MHz		802.11 Preferences
No.	Time	Source	Destination	Protocol	LengthInfo	
113	0.000381864	192.168.1.13	128.119.245.12	HTTP	442 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1	
121	0.002493982	128.119.245.12	192.168.1.13	HTTP	796 HTTP/1.1 200 OK (text/html)	
127	0.034615063	192.168.1.13	128.119.245.12	HTTP	399 GET /favicon.ico HTTP/1.1	
140	0.001854926	128.119.245.12	192.168.1.13	HTTP	551 HTTP/1.1 404 Not Found (text/html)	
250	0.000422183	192.168.1.13	128.119.245.12	HTTP	554 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1	
254	0.001458557	128.119.245.12	192.168.1.13	HTTP	306 HTTP/1.1 304 Not Modified	

▶ Frame 254: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on interface wlp0s20f3, id 0
 ▶ Ethernet II, Src: b8:c1:ac:7f:5e:e4 (b8:c1:ac:7f:5e:e4), Dst: IntelCor_38:9b:09 (08:71:90:38:9b:09)
 ▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.13
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 57214, Seq: 1, Ack: 489, Len: 240
 ▶ Hypertext Transfer Protocol
 ▶ HTTP/1.1 304 Not Modified\r\n
 Date: Fri, 05 Mar 2021 05:18:51 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
 Connection: Keep-Alive\r\n
 Keep-Alive: timeout=5, max=100\r\n
 ETag: "173-5bcb00a2af70"\r\n
 \r\n
 [HTTP response 1/1]
 [Time since request: 0.299202434 seconds]
 [Request in frame: 250]
 [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

Q2 Response to the second GET request

Q3. Retrieving Long Documents

- 12) Only 1 HTTP GET request message(If we consider favicon packets then there are 2 packets) was sent from my browser. Packet number 103 in the trace contains the GET message for the Bill of Rights.
- 13) Packet Number of the response(OK packet) to the HTTP GET request is 110.
- 14) The status code and phrase associated are 200 OK.
- 15) 2 data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights, as we can see in the 2 reassembled TCP segments section and the size of segments are 2880 bytes and 1981 bytes(total=4861bytes).

http						
Interface phy0.mon		Channel 1 · 2.412 GHz		20 MHz		802.11 Preferences
No.	Time	Source	Destination	Protocol	LengthInfo	
103	0.000312688	192.168.1.13	128.119.245.12	HTTP	442 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1	
110	0.000265993	128.119.245.12	192.168.1.13	HTTP	2047 HTTP/1.1 200 OK (text/html)	
119	0.035565633	192.168.1.13	128.119.245.12	HTTP	399 GET /favicon.ico HTTP/1.1	
133	0.002358683	128.119.245.12	192.168.1.13	HTTP	551 HTTP/1.1 404 Not Found (text/html)	

▶ Frame 103: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface wlp0s20f3, id 0
 ▶ Ethernet II, Src: IntelCor_38:9b:09 (08:71:90:38:9b:09), Dst: b8:c1:ac:7f:5e:e4 (b8:c1:ac:7f:5e:e4)
 ▶ Internet Protocol Version 4, Src: 192.168.1.13, Dst: 128.119.245.12
 ▶ Transmission Control Protocol, Src Port: 58272, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
 ▶ Hypertext Transfer Protocol
 ▶ GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
 Host: gaia.cs.umass.edu\r\n
 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0\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
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
 [HTTP request 1/1]
 [Response in frame: 110]

Q3 GET request

http						
Interface phy0.mon		Channel 1 - 2.412 GHz		20 MHz		
No.	Time	Source	Destination	Protocol	LengthInfo	
103	0.000312688	192.168.1.13	128.119.245.12	HTTP	442 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1	
110	0.000265993	128.119.245.12	192.168.1.13	HTTP	2047 HTTP/1.1 200 OK (text/html)	
119	0.035565633	192.168.1.13	128.119.245.12	HTTP	399 GET /favicon.ico HTTP/1.1	
133	0.002358683	128.119.245.12	192.168.1.13	HTTP	551 HTTP/1.1 404 Not Found (text/html)	

Frame 110: 2047 bytes on wire (16376 bits), 2047 bytes captured (16376 bits) on interface wlp0s20f3, id 0 Ethernet II, Src: b8:c1:ac:7f:5e:e4 (b8:c1:ac:7f:5e:e4), Dst: IntelCor_38:9b:09 (08:71:90:38:9b:09) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.13 Transmission Control Protocol, Src Port: 80, Dst Port: 58272, Seq: 2881, Ack: 377, Len: 1981 [2 Reassembled TCP Segments (4861 bytes): #108(2880), #110(1981)] [Frame: 108, payload: 0-2879 (2880 bytes)] [Frame: 110, payload: 2880-4860 (1981 bytes)] [Segment count: 2] [Reassembled TCP length: 4861] [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204672692c203035204d61722032...]						
Hypertext Transfer Protocol HTTP/1.1 200 OK\r\n Date: Fri, 05 Mar 2021 06:04:42 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: Fri, 05 Mar 2021 06:04:01 GMT\r\n ETag: "1194-bacc3d9bd0993"\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]						

Q3 Response

Q4. HTML Documents with Embedded Objects.

16) 3 HTTP GET request messages (If we consider favicon packets then there are 4 HTTP request packets) were sent from the browser. 1 for the web page and 2 for the images. The HTTP webpage and the pearson image were sent to 128.119.245.12 and the 8E small cover image request was sent to 178.79.137.164.

17) The 2 images were downloaded serially, one after the other. The GET request for the first message was sent and the OK message was received, then the GET request for the second image was sent to 178.79.137.164, and a response message was received. Hence they are downloaded serially.

http						
Interface phy0.mon		Channel 1 - 2.412 GHz		20 MHz		
No.	Time	Source	Destination	Protocol	LengthInfo	
3405	0.000311334	192.168.1.13	128.119.245.12	HTTP	442 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1	
3419	0.003618018	128.119.245.12	192.168.1.13	HTTP	1367 HTTP/1.1 200 OK (text/html)	
3427	0.016933367	192.168.1.13	128.119.245.12	HTTP	399 GET /pearson.png HTTP/1.1	
3433	0.057293839	192.168.1.13	128.119.245.12	HTTP	399 GET /favicon.ico HTTP/1.1	
3447	0.003505779	128.119.245.12	192.168.1.13	HTTP	2238 HTTP/1.1 200 OK (PNG)	
3463	0.000060268	128.119.245.12	192.168.1.13	HTTP	551 HTTP/1.1 404 Not Found (text/html)	
3508	0.000285185	192.168.1.13	178.79.137.164	HTTP	406 GET /8E_cover_small.jpg HTTP/1.1	
3510	0.000459322	178.79.137.164	192.168.1.13	HTTP	237 HTTP/1.1 301 Moved Permanently	
3558	0.000473594	192.168.1.13	23.48.226.43	OCSP	444 Request	
3565	0.00001413	23.48.226.43	192.168.1.13	OCSP	955 Response	

Frame 3427: 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface wlp0s20f3, id 0 Ethernet II, Src: IntelCor_38:9b:09 (08:71:90:38:9b:09), Dst: b8:c1:ac:7f:5e:e4 (b8:c1:ac:7f:5e:e4) Internet Protocol Version 4, Src: 192.168.1.13, Dst: 128.119.245.12 Transmission Control Protocol, Src Port: 58496, Dst Port: 80, Seq: 1, Ack: 1, Len: 333 Hypertext Transfer Protocol GET /pearson.png HTTP/1.1\r\n Host: gaia.cs.umass.edu\r\n User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0\r\n Accept: image/webp,*/*\r\n Accept-Language: en-US,en;q=0.5\r\n Accept-Encoding: gzip, deflate\r\n Connection: keep-alive\r\n Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n \r\n [Full request URI: http://gaia.cs.umass.edu/pearson.png] [HTTP request 1/1] [Response in frame: 3447]						
---	--	--	--	--	--	--

Q4 first Image GET request

http						
Interface phy0.mon		Channel 1 - 2.412 GHz		20 MHz		
No.	Time	Source	Destination	Protocol	LengthInfo	
3405	0.000311334	192.168.1.13	128.119.245.12	HTTP	442 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1	
3418	0.003618018	128.119.245.12	192.168.1.13	HTTP	1367 HTTP/1.1 200 OK (text/html)	
3427	0.016933367	192.168.1.13	128.119.245.12	HTTP	399 GET /pearson.png HTTP/1.1	
3433	0.057293939	192.168.1.13	128.119.245.12	HTTP	399 GET /favicon.ico HTTP/1.1	
3447	0.003355779	128.119.245.12	192.168.1.13	HTTP	2233 HTTP/1.1 200 OK (PNG)	
3463	0.000909268	128.119.245.12	192.168.1.13	HTTP	551 HTTP/1.1 404 Not Found (text/html)	
3508	0.000285185	192.168.1.13	178.79.137.164	HTTP	406 GET /8E_cover_small.jpg HTTP/1.1	
3510	0.000458322	178.79.137.164	192.168.1.13	HTTP	237 HTTP/1.1 301 Moved Permanently	
3558	0.000473594	192.168.1.13	23.48.226.43	OCSP	444 Request	
3565	0.000901413	23.48.226.43	192.168.1.13	OCSP	955 Response	

[Frame: 3447, payload: 1440-3611 (2172 bytes)]						
[Segment count: 2]						
[Reassembled TCP length: 3612]						
[Reassembled TCP Data: 485454502f312e3120323036204f4b0d0a446174653a204672692c203035204d61722032_-]						
Hypertext Transfer Protocol						
HTTP/1.1 200 OK\r\n Date: Fri, 05 Mar 2021 06:22:51 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: Sat, 06 Aug 2016 10:08:14 GMT\r\n ETag: "cc3-539645c7f1ee7"\r\n Accept-Ranges: bytes\r\n Content-Length: 3267\r\n Keep-Alive: timeout=5, max=100\r\n Connection: Keep-Alive\r\n Content-Type: image/png\r\n \r\n [HTTP response 1/1]\n [Time since request: 0.315093304 seconds]\n [Request in frame: 3427]\n [Request URI: http://gaia.cs.umass.edu/pearson.png]\n File Data: 3267 bytes						
Portable Network Graphics						

Q4 first Image response

Q5. HTTP Authentication.

18) The server's response (status code and phrase) in response to the initial HTTP GET message from my browser is 401 Unauthorized.

19) When your browser sends the HTTP GET message for the second time, the Authorization field is newly included in the HTTP GET message. Its value is Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5= which is the encrypted form of the username and password.

http						
Interface phy0.mon		Channel 1 - 2.412 GHz		20 MHz		
No.	Time	Source	Destination	Protocol	LengthInfo	
166	0.000369500	192.168.1.13	128.119.245.12	HTTP	458 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1	
1658	0.000337991	128.119.245.12	192.168.1.13	HTTP	783 HTTP/1.1 401 Unauthorized (text/html)	
3909	0.000335412	192.168.1.13	128.119.245.12	HTTP	517 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1	
3912	0.000000307	128.119.245.12	192.168.1.13	HTTP	556 HTTP/1.1 200 OK (text/html)	
3924	0.000083618	192.168.1.13	128.119.245.12	HTTP	415 GET /favicon.ico HTTP/1.1	
3957	0.000024939	128.119.245.12	192.168.1.13	HTTP	550 HTTP/1.1 404 Not Found (text/html)	

Frame 1056: 783 bytes on wire (6264 bits), 783 bytes captured (6264 bits) on interface wlp0s20f3, id 0 Ethernet II, Src: b8:c1:ac:7f:5e:e4 (b8:c1:ac:7f:5e:e4), Dst: IntelCor_38:9b:09 (08:71:90:38:9b:09) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.13 Transmission Control Protocol, Src Port: 80, Dst Port: 58748, Seq: 1, Ack: 393, Len: 717						
Hypertext Transfer Protocol						
HTTP/1.1 401 Unauthorized\r\n Date: Fri, 05 Mar 2021 06:42:46 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 WWW-Authenticate: Basic realm="wireshark-students only"\r\n Content-Length: 381\r\n Keep-Alive: timeout=5, max=100\r\n Connection: Keep-Alive\r\n Content-Type: text/html; charset=iso-8859-1\r\n \r\n [HTTP response 1/1]\n [Time since request: 0.306061733 seconds]\n [Request in frame: 166]\n [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]\n File Data: 381 bytes						
Line-based text data: text/html (12 lines)						

Q5 Initial Response Message

http					
Interface phy0.mon		Channel 1 · 2.412 GHz		20 MHz	
No.	Time	Source	Destination	Protocol	Length Info
166	0.000368500	192.168.1.13	128.119.245.12	HTTP	458 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1056	0.000337901	128.119.245.12	192.168.1.13	HTTP	783 HTTP/1.1 401 Unauthorized (text/html)
3909	0.000335412	192.168.1.13	128.119.245.12	HTTP	517 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
3912	0.000000307	128.119.245.12	192.168.1.13	HTTP	556 HTTP/1.1 200 OK (text/html)
3924	0.0000003618	192.168.1.13	128.119.245.12	HTTP	415 GET /favicon.ico HTTP/1.1
3957	0.000024939	128.119.245.12	192.168.1.13	HTTP	550 HTTP/1.1 404 Not Found (text/html)

<ul style="list-style-type: none"> Frame 3909: 517 bytes on wire (4136 bits), 517 bytes captured (4136 bits) on interface wlp0s20f3, id 0 Ethernet II, Src: IntelCor_38:9b:09 (08:71:90:38:9b:09), Dst: b8:c1:ac:7f:5e:e4 (b8:c1:ac:7f:5e:e4) Internet Protocol Version 4, Src: 192.168.1.13, Dst: 128.119.245.12 Transmission Control Protocol, Src Port: 58764, Dst Port: 80, Seq: 1, Ack: 1, Len: 451 Hypertext Transfer Protocol <ul style="list-style-type: none"> GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n <ul style="list-style-type: none"> Host: gaia.cs.umass.edu\r\n User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0\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 Authorization: Basic d2lyZXNoYXJRLXN0dWlbnRZOm5ldHdvcmss\r\n

<ul style="list-style-type: none"> \r\n [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html] [HTTP request 1/2] [Response in frame: 3912] [Next request in frame: 3924]

Q5 Second Get Message with authorization field