

ECE361 – Computer Networks

Wireshark Lab 1: HTTP

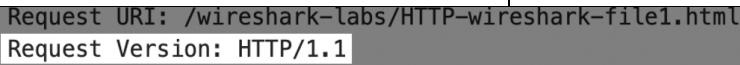
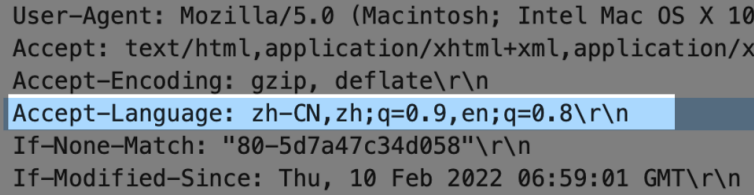
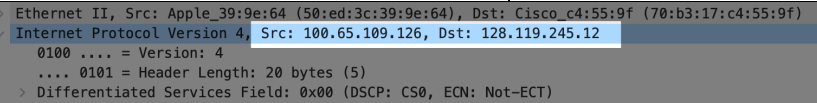
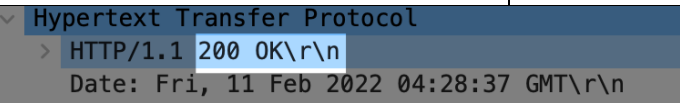
First Name: Yuhe Last Name: Chen

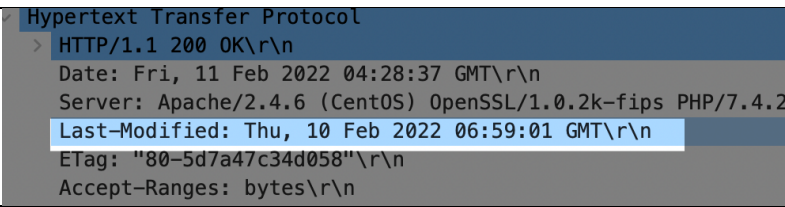
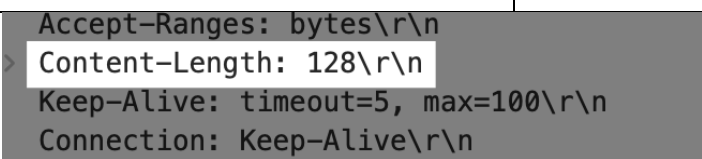
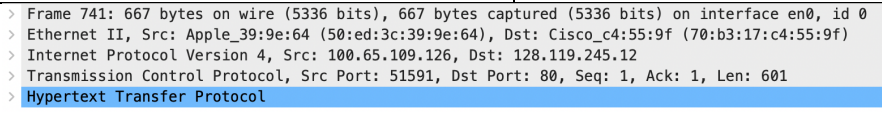
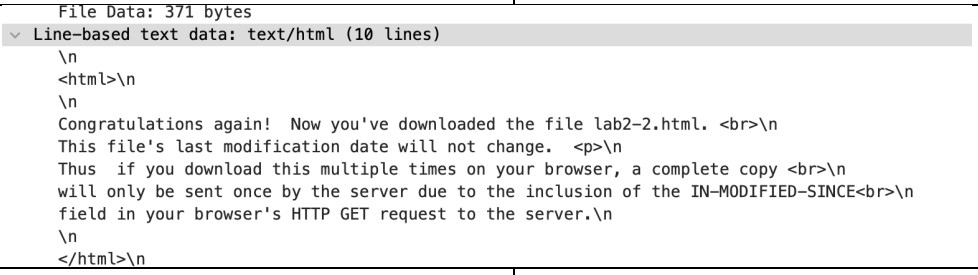
First Name: Leting Last Name: Ni

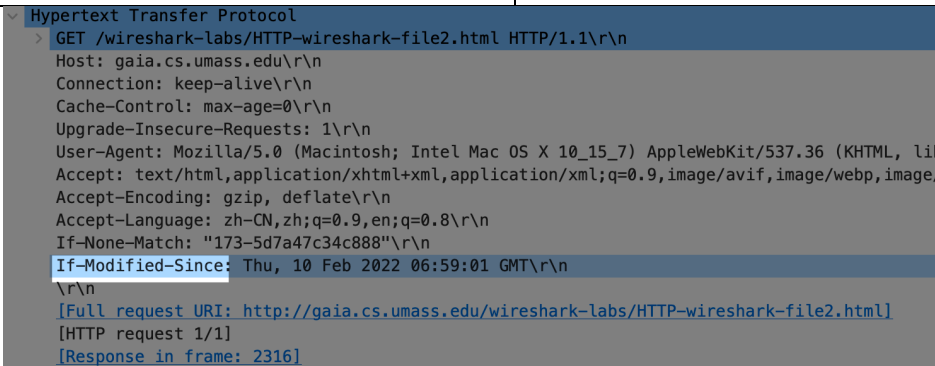
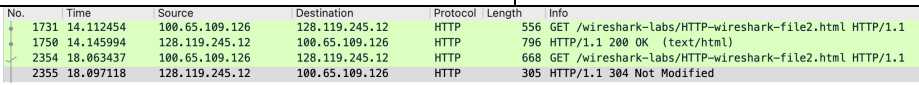
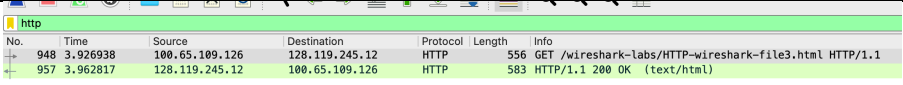
Group Details:

Student #: _1005689480_____ Student #: _1006255446_____

Mark:

	Question	Answer
1	Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?	My browser is running version 1.1
Annotated Screenshot (if needed)		
2	What languages (if any) does your browser indicate that it can accept to the server?	My browser indicates it will accept Chinese(zh) and English (en).
Annotated Screenshot (if needed)		
3	What is the IP address of your computer? Of the gaia.cs.umass.edu server?	My computer: 100.65.109.126 Server: 128.119.245.12
Annotated Screenshot (if needed)		
4	What is the status code returned from the server to your browser?	200
Annotated Screenshot (if needed)		
5	When was the HTML file that you are retrieving last modified at the server?	Thu, 10 Feb 2022 06:59:01

Annotated Screenshot (if needed)		
6	How many bytes of content are being returned to your browser?	128
Annotated Screenshot (if needed)		
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.	NO.
Annotated Screenshot (if needed)		
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?	NO
Annotated Screenshot (if needed)		
9	Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?	Yes, because we can see that in the line-base text data.
Annotated Screenshot (if needed)		
10	Now inspect the contents of the second HTTP GET request from your	Yes. The information is Thu, 10 Feb

	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?	2022 06:59:01 GMT\r\n																																			
Annotated Screenshot (if needed)	 <pre>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, li Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image Accept-Encoding: gzip, deflate\r\n Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n If-None-Match: "173-5d7a47c34c888"\r\n If-Modified-Since: Thu, 10 Feb 2022 06:59:01 GMT\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: 2316]</pre>																																				
11	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.	304 not modified The server didn’t return the contents of the file. The file is not modified so server doesn’t need to send the file again.																																			
Annotated Screenshot (if needed)	 <table><thead><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>1731</td><td>14.112454</td><td>100.65.109.126</td><td>128.119.245.12</td><td>HTTP</td><td>556</td><td>GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1</td></tr><tr><td>1750</td><td>14.145994</td><td>128.119.245.12</td><td>100.65.109.126</td><td>HTTP</td><td>796</td><td>HTTP/1.1 200 OK (text/html)</td></tr><tr><td>2354</td><td>18.063437</td><td>100.65.109.126</td><td>128.119.245.12</td><td>HTTP</td><td>668</td><td>GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1</td></tr><tr><td>2355</td><td>18.097118</td><td>128.119.245.12</td><td>100.65.109.126</td><td>HTTP</td><td>305</td><td>HTTP/1.1 304 Not Modified</td></tr></tbody></table>		No.	Time	Source	Destination	Protocol	Length	Info	1731	14.112454	100.65.109.126	128.119.245.12	HTTP	556	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1	1750	14.145994	128.119.245.12	100.65.109.126	HTTP	796	HTTP/1.1 200 OK (text/html)	2354	18.063437	100.65.109.126	128.119.245.12	HTTP	668	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1	2355	18.097118	128.119.245.12	100.65.109.126	HTTP	305	HTTP/1.1 304 Not Modified
No.	Time	Source	Destination	Protocol	Length	Info																															
1731	14.112454	100.65.109.126	128.119.245.12	HTTP	556	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1																															
1750	14.145994	128.119.245.12	100.65.109.126	HTTP	796	HTTP/1.1 200 OK (text/html)																															
2354	18.063437	100.65.109.126	128.119.245.12	HTTP	668	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1																															
2355	18.097118	128.119.245.12	100.65.109.126	HTTP	305	HTTP/1.1 304 Not Modified																															
12 ¹	How many HTTP GET request messages were sent by your browser?	1																																			
Annotated Screenshot (if needed)	 <table><thead><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>948</td><td>3.926938</td><td>100.65.109.126</td><td>128.119.245.12</td><td>HTTP</td><td>556</td><td>GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1</td></tr><tr><td>957</td><td>3.962817</td><td>128.119.245.12</td><td>100.65.109.126</td><td>HTTP</td><td>583</td><td>HTTP/1.1 200 OK (text/html)</td></tr></tbody></table>		No.	Time	Source	Destination	Protocol	Length	Info	948	3.926938	100.65.109.126	128.119.245.12	HTTP	556	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1	957	3.962817	128.119.245.12	100.65.109.126	HTTP	583	HTTP/1.1 200 OK (text/html)														
No.	Time	Source	Destination	Protocol	Length	Info																															
948	3.926938	100.65.109.126	128.119.245.12	HTTP	556	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1																															
957	3.962817	128.119.245.12	100.65.109.126	HTTP	583	HTTP/1.1 200 OK (text/html)																															
13	How many data-containing TCP segments were needed to carry the single HTTP response?	4																																			

¹ Yes, questions 12 through 15 are different in this document than the lab handout. **You must answer the questions found in *this* document.**

Annotated Screenshot (if needed)	<div>> Frame 957: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface en0, id 0</div> <div>> Ethernet II, Src: Cisco_c4:55:9f (70:b3:17:c4:55:9f), Dst: Apple_39:9e:64 (50:ed:3c:39:9e:64)</div> <div>> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 100.65.109.126</div> <div>> Transmission Control Protocol, Src Port: 80, Dst Port: 52001, Seq: 4345, Ack: 491, Len: 517</div> <div>✓ [4 Reassembled TCP Segments (4861 bytes): #954(1448), #955(1448), #956(1448), #957(517)]</div> <div>[Frame: 954, payload: 0-1447 (1448 bytes)]</div> <div>[Frame: 955, payload: 1448-2895 (1448 bytes)]</div> <div>[Frame: 956, payload: 2896-4343 (1448 bytes)]</div> <div>[Frame: 957, payload: 4344-4860 (517 bytes)]</div> <div>[Segment count: 4]</div> <div>[Reassembled TCP length: 4861]</div> <div>[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a204672692c203131204665622032...]</div> <div>> Hypertext Transfer Protocol</div> <div>> Line-based text data: text/html (98 lines)</div>																																																		
14	What is the status code and phrase associated with the response to the HTTP GET request?	200																																																	
Annotated Screenshot (if needed)	<div>✓ Hypertext Transfer Protocol</div> <div>✓ HTTP/1.1 200 OK\r\n</div> <div>> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]</div> <div>Response Version: HTTP/1.1</div> <div>Status Code: 200</div> <div>[Status Code Description: OK]</div>																																																		
15	Are there any HTTP status lines in the transmitted data associated with a TCP induced “Continuation”?	No																																																	
Annotated Screenshot (if needed)	<table><thead><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>906</td><td>4.113095</td><td>100.65.109.126</td><td>128.119.245.12</td><td>HTTP</td><td>477</td><td>GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1</td></tr><tr><td>911</td><td>4.147459</td><td>128.119.245.12</td><td>100.65.109.126</td><td>HTTP</td><td>583</td><td>HTTP/1.1 200 OK (text/html)</td></tr></tbody></table>		No.	Time	Source	Destination	Protocol	Length	Info	906	4.113095	100.65.109.126	128.119.245.12	HTTP	477	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1	911	4.147459	128.119.245.12	100.65.109.126	HTTP	583	HTTP/1.1 200 OK (text/html)																												
No.	Time	Source	Destination	Protocol	Length	Info																																													
906	4.113095	100.65.109.126	128.119.245.12	HTTP	477	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1																																													
911	4.147459	128.119.245.12	100.65.109.126	HTTP	583	HTTP/1.1 200 OK (text/html)																																													
16	How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?	3 The first and the second GET requests are sent to the IP address 128.119.245.12. The third GET request is sent to the IP address 178.79.137.164.																																																	
Annotated Screenshot (if needed)	<table><thead><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>1427</td><td>5.169011</td><td>100.65.109.126</td><td>128.119.245.12</td><td>HTTP</td><td>556</td><td>GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1</td></tr><tr><td>1438</td><td>5.204385</td><td>128.119.245.12</td><td>100.65.109.126</td><td>HTTP</td><td>1367</td><td>HTTP/1.1 200 OK (text/html)</td></tr><tr><td>1515</td><td>5.366708</td><td>100.65.109.126</td><td>128.119.245.12</td><td>HTTP</td><td>502</td><td>GET /pearson.png HTTP/1.1</td></tr><tr><td>1521</td><td>5.400664</td><td>128.119.245.12</td><td>100.65.109.126</td><td>HTTP</td><td>781</td><td>HTTP/1.1 200 OK (PNG)</td></tr><tr><td>1545</td><td>5.525437</td><td>100.65.109.126</td><td>178.79.137.164</td><td>HTTP</td><td>469</td><td>GET /BE_cover_small.jpg HTTP/1.1</td></tr><tr><td>1565</td><td>5.612327</td><td>178.79.137.164</td><td>100.65.109.126</td><td>HTTP</td><td>237</td><td>HTTP/1.1 301 Moved Permanently</td></tr></tbody></table>		No.	Time	Source	Destination	Protocol	Length	Info	1427	5.169011	100.65.109.126	128.119.245.12	HTTP	556	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1	1438	5.204385	128.119.245.12	100.65.109.126	HTTP	1367	HTTP/1.1 200 OK (text/html)	1515	5.366708	100.65.109.126	128.119.245.12	HTTP	502	GET /pearson.png HTTP/1.1	1521	5.400664	128.119.245.12	100.65.109.126	HTTP	781	HTTP/1.1 200 OK (PNG)	1545	5.525437	100.65.109.126	178.79.137.164	HTTP	469	GET /BE_cover_small.jpg HTTP/1.1	1565	5.612327	178.79.137.164	100.65.109.126	HTTP	237	HTTP/1.1 301 Moved Permanently
No.	Time	Source	Destination	Protocol	Length	Info																																													
1427	5.169011	100.65.109.126	128.119.245.12	HTTP	556	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1																																													
1438	5.204385	128.119.245.12	100.65.109.126	HTTP	1367	HTTP/1.1 200 OK (text/html)																																													
1515	5.366708	100.65.109.126	128.119.245.12	HTTP	502	GET /pearson.png HTTP/1.1																																													
1521	5.400664	128.119.245.12	100.65.109.126	HTTP	781	HTTP/1.1 200 OK (PNG)																																													
1545	5.525437	100.65.109.126	178.79.137.164	HTTP	469	GET /BE_cover_small.jpg HTTP/1.1																																													
1565	5.612327	178.79.137.164	100.65.109.126	HTTP	237	HTTP/1.1 301 Moved Permanently																																													
17	Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.	We can tell from the time that the two images are downloaded serially.																																																	
Annotated Screenshot (if needed)	<table><thead><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>1427</td><td>5.169011</td><td>100.65.109.126</td><td>128.119.245.12</td><td>HTTP</td><td>556</td><td>GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1</td></tr><tr><td>1438</td><td>5.204385</td><td>128.119.245.12</td><td>100.65.109.126</td><td>HTTP</td><td>1367</td><td>HTTP/1.1 200 OK (text/html)</td></tr><tr><td>1515</td><td>5.366708</td><td>100.65.109.126</td><td>128.119.245.12</td><td>HTTP</td><td>502</td><td>GET /pearson.png HTTP/1.1</td></tr><tr><td>1521</td><td>5.400664</td><td>128.119.245.12</td><td>100.65.109.126</td><td>HTTP</td><td>781</td><td>HTTP/1.1 200 OK (PNG)</td></tr><tr><td>1545</td><td>5.525437</td><td>100.65.109.126</td><td>178.79.137.164</td><td>HTTP</td><td>469</td><td>GET /BE_cover_small.jpg HTTP/1.1</td></tr><tr><td>1565</td><td>5.612327</td><td>178.79.137.164</td><td>100.65.109.126</td><td>HTTP</td><td>237</td><td>HTTP/1.1 301 Moved Permanently</td></tr></tbody></table>		No.	Time	Source	Destination	Protocol	Length	Info	1427	5.169011	100.65.109.126	128.119.245.12	HTTP	556	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1	1438	5.204385	128.119.245.12	100.65.109.126	HTTP	1367	HTTP/1.1 200 OK (text/html)	1515	5.366708	100.65.109.126	128.119.245.12	HTTP	502	GET /pearson.png HTTP/1.1	1521	5.400664	128.119.245.12	100.65.109.126	HTTP	781	HTTP/1.1 200 OK (PNG)	1545	5.525437	100.65.109.126	178.79.137.164	HTTP	469	GET /BE_cover_small.jpg HTTP/1.1	1565	5.612327	178.79.137.164	100.65.109.126	HTTP	237	HTTP/1.1 301 Moved Permanently
No.	Time	Source	Destination	Protocol	Length	Info																																													
1427	5.169011	100.65.109.126	128.119.245.12	HTTP	556	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1																																													
1438	5.204385	128.119.245.12	100.65.109.126	HTTP	1367	HTTP/1.1 200 OK (text/html)																																													
1515	5.366708	100.65.109.126	128.119.245.12	HTTP	502	GET /pearson.png HTTP/1.1																																													
1521	5.400664	128.119.245.12	100.65.109.126	HTTP	781	HTTP/1.1 200 OK (PNG)																																													
1545	5.525437	100.65.109.126	178.79.137.164	HTTP	469	GET /BE_cover_small.jpg HTTP/1.1																																													
1565	5.612327	178.79.137.164	100.65.109.126	HTTP	237	HTTP/1.1 301 Moved Permanently																																													
Questions 18 and 19 omitted																																																			