

Faculty of Engineering & Technology Electrical & Computer Engineering Department

ENCS4130

Wireshark HTTP ToDo

Prepared by : Tareq Shannak

ID Number : 1181404

Instructor : Dr. Ahmad Alsadeh

Teaching Assistant : Katy Sadi

Section : 2

Date : August 17, 2021

The Basic HTTP GET/response interaction

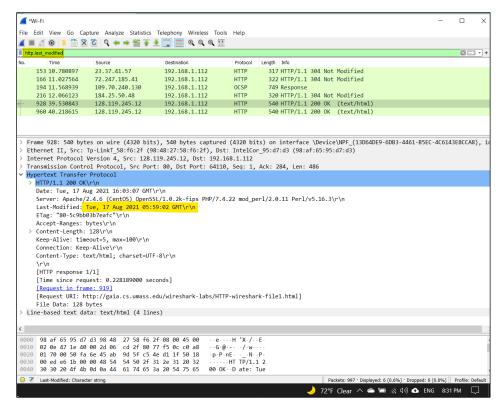
By looking at the information in the HTTP GET and response messages, answer the following questions. If you're doing this lab as part of class, your teacher will provide details about how to hand in assignments, whether written or in an LMS.

	Wi-Fi				- [) X
-			s Telephony Wireless To			
_		🙆 ९ 🗢 🔿 🖺 🕯	ં 🛃 📃 🗐 લ, લ, લ, 🫉	<u> </u>		
htt	<u> </u>					
No.	Time	Source	Destination	Protocol	Length Info	
	212 11.973072	192.168.1.112	184.25.50.48	HTTP	334 GET /msdownload/update/v3/static/trustedr/en/authroots	:1.c
	216 12.066123	184.25.50.48	192.168.1.112	HTTP	320 HTTP/1.1 304 Not Modified	
	919 39.302654	192.168.1.112	128.119.245.12	HTTP	337 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1	
	928 39.530843	128.119.245.12	192.168.1.112	HTTP	540 HTTP/1.1 200 OK (text/html)	
•	956 39.976137	192.168.1.112	128.119.245.12	HTTP	530 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1	
	960 40.218615	128.119.245.12	192.168.1.112	HTTP	540 HTTP/1.1 <mark>200 OK</mark> (text/html) 476 GET /favicon.ico HTTP/1.1	
	961 40.270538	192.168.1.112	128.119.245.12	HITP	4/0 GET /TAVICON.ICO HTTP/1.1	
						>
	Host: gaia.cs.u			r\n		
	Connection: keep Upgrade-Insecur User-Agent: Moz Accept: text/htm Accept-Encoding Accept-Language \r\n	<pre>b-alive\r\n a-Requests: 1\r\n illa/5.0 (Windows N ml,application/xhtm : gzip, deflate\r\n : en-U5,en;q=0.9\r\ RI: http://gaia.cs. /2] ame: 960]</pre>	l+xml,application/xml	opleWebKit/5;q=0.9,image	537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36∖ /avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch reshark-file1.html]	
002(003(004(Connection: kee Upgrade-Insecur- User-Agent: Moz Accept: text/htt Accept-Encoding full request u [HTIP request 1] [HTIP request 1] [Next request 1] [Next request 1] 02 04 bl ad 40 f5 0c c3 51 00 01 04 39 30 00 68 61 72 6b 2d	2-alive\r\n =-Requests: 1\r\n mllaf5.0 (Windows N ml,application/xhtm : grip, deflate\r\n : en-US,en;q=0.9\r\ 31: http://gaia.cs. /2] ame: 960] 1 frame: 961] 21 98 af 65 95 d7 00 80 06 00 00 cc 50 7a 09 70 ff c5 50 7a 09 70 ff c5 50 74 24 24 24 22 6c 61 62 73 2f 48	(d3 08 00 45 00 (11) a 0 (11) a 0 (11) a 8 01 70 80 77 a b 61 49 50 18	opleWebKit/5;q=0.9,image	<pre>:/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch reshark-file1.html] E E</pre>	ange;v-
2000 2010 2020 2030	Connection: kee Upgrade-Insecur- User-Agent: Moz Accept: text/htt Accept-Encoding Accept-Language \r\n [Full request 1] [HTP request 1] [HTP request 1] [Next request 1] [Next request 1] 02 04 bl ad 40 f5 0c c3 51 00 01 04 39 30 00 68 61 72 6b 2d	2-alive\r\n =-Requests: 1\r\n mllaf5.0 (Windows N ml,application/xhtm : grip, deflate\r\n : en-US,en;q=0.9\r\ 31: http://gaia.cs. /2] ame: 960] 1 frame: 961] 21 98 af 65 95 d7 00 80 06 00 00 cc 50 7a 09 70 ff c5 50 7a 09 70 ff c5 50 74 24 24 24 22 6c 61 62 73 2f 48	(d3 08 00 45 00 (11) a 0 (11) a 0 (11) a 8 01 70 80 77 a b 61 49 50 18	>p]e₩ebKit/; ;q=0.9,image abs/HTTP-wir @ @ Q.P2: pai	<pre>:/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch reshark-file1.html] E>w F>w F>w F>w</pre>	ange;v

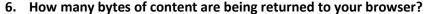
- 1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running? HTTP1.1
- 2. What languages (if any) does your browser indicate that it can accept to the server? en-US (US English)
- 3. What is the IP address of your computer? What is the IP address of the gaia.cs.umass.edu server? IP address of my computer: 192.168.1.112

IP address of the gaia.cs.umass.edu server: 128.119.245.12

- 4. What is the status code returned from the server to your browser? 200 OK
- 5. When the HTML file that you are retrieving was last modified at the server?



Tue, August 17, 2021 5:59:02 GMT



_ *	*Wi-Fi				- 🗆 X
File	Edit View Go Cap	oture Analyze Statistics	Telephony Wireless Tools	Help	
	🔳 🖉 🛞 📜 🛅 🗙	🙆 । ९ 🔶 🔿 🕾 🖌 🖢) 📑 📄 @ @ @ 🎹		
htt	tp				
No.	Time	Source	Destination	Protocol	Length Info
	2609 21.394015	192.168.1.112	93.184.220.29	HTTP	294 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Zt1%2Bz8SiPI7wEW
	2729 21.556347	93.184.220.29	192.168.1.112	OCSP	853 Response
+	5011 29.961685	192.168.1.112	128.119.245.12	HTTP	337 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
-	5014 30.190799	128.119.245.12	192.168.1.112	HTTP	540 HTTP/1.1 200 OK (text/html)
> E > I > T > H	thernet II, Src: T internet Protocol V ransmission Contro Aypertext Transfer	<pre>Tp-LinkT_58:f6:2f (98 Version 4, Src: 128.1 Dl Protocol, Src Port Protocol</pre>		: IntelCo 58.1.112	
	Server: Apache/2 Last-Modified: T ETag: "80-Sc9bb Accept-Ranges: b Ocntent-Length: Keep-Alive: time Connection: Keep Content-Type: te (\n\n [HTTP response 1 [Time since requ [Request in fram	<pre>ug 2021 17:36:46 GMT\/ .4.6 (CentOS) OpenSS Uue, 17 Aug 2021 05:59 03b7eafc"\r\n ytes\r\n 128\r\n out=5, max=100\r\n o-Alive\r\n ext/html; charset=UTF 1/1] uest: 0.229114000 seco ue: 5011 tp://gaia.cs.umass.eu</pre>	L/1.0.2k-fips PHP/7.4. 9:02 GMT\r\n -8\r\n	_	perl/2.0.11 Perl/v5.16.3\r\n ark-file1.html]
> L	ine-based text dat	ta: text/html (4 line	s)		
<					
000	08 af 65 05 d7	43 98 48 27 58 f6 2	F 08 00 15 00	.н. 'Y./.	

128 Bytes

 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.

The HTTP CONDITIONAL GET/response interaction

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

📕 *W																	
	/1-11														-		\times
File	Edit	View Go	Capture	Analyze	e Statistics	Telephony	Wireles	ss Tools	Help								
	a	0 1		Q 🦛	. ≩ 🕾 🔶		0 Q	Q 11									
http	1 (86:4)			• •				• 1444									- +
10.		Time		ource		Destinati	ion		Protocol	Length Inf	<u>`````````````````````````````````````</u>						
		101.47124		28.119.3	245 12		58.1.11	2	HTTP	-	, TP/1.1 200 OI	(text/k	(1m1)				
		101.61938		92.168.			19.245.		HTTP		T /kurose ro:						
		101.86609		28.119.			58.1.11		HTTP		TP/1.1 200 0						
		102.25329		2.168.			19.245.		HTTP		T /kurose ro			ok 8E 2.i	pg HTTP/1	.1	
5	5433	103.42502	29 1	28.119.3	245.12	192.16	58.1.11	2	HTTP		TP/1.1 200 O						
- 5	5496	112.46092	21 1	92.168.	1.112	128.11	19.245.	12	HTTP	337 GE	T /wireshark	labs/HTTF	-wireshark	-file2.ht	ml HTTP/1	.1	
- 5	5499	112.69842	26 1	28.119.3	245.12	192.16	58.1.11	2	HTTP	784 HT	TP/1.1 200 0	(text/h	tml)				
																>	•
En	ame '	5499 . 784	bytes	on wire	(6272 bi	ts). 784	hytes o	antured	(6272	hits) on iu	terface \Dev	ice\NPE {	13D64DE9-6	DB3-4461-F	35EC-4C61	43E8CC/	A8}. †
											(98:af:65:9						
					Src: 128.						(,					
										, Ack: 284	Len: 730						
						· · · ·											
> Hvt	perte	ext Trans	fer Pro	tocol													
					tml (10 li	nes)											
/ Li	ne-ba <htm <htm \n Cong This Thus</htm </htm 	ased text nl>\n gratulations file's i s if you	data: ons aga last mo downlo	text/ht in! No dificat ad this	w you've (ion date) multiple	downloade vill not times on	change. your b	\n rowser,	a compl	lete copy «	br>\n -SINCE \n						
Y Li	ne-ba <htm <htm \n Cong This Thus will</htm </htm 	ased text nl>\n gratulatid file's i if you l only be	data: ons aga last mo downlo sent c	text/ht in! No dificat ad this nce by	w you've (ion date) multiple	downloade vill not times on due to	change. your b the inc	\n rowser, lusion d	a compl	lete copy «							
Y Li	\n <htm <htm \n Cong This Thus will fiel \n</htm </htm 	ased text al>\n gratulation file's file's if you l only be ld in you	data: ons aga last mo downlo sent c	text/ht in! No dificat ad this nce by	w you've o ion date o multiple the serve	downloade vill not times on due to	change. your b the inc	\n rowser, lusion d	a compl	lete copy «							
Y Li	\n <htm <htm \n Cong This Thus will fiel \n</htm </htm 	ased text al>\n gratulation file's if you l only be ld in you	data: ons aga last mo downlo sent c	text/ht in! No dificat ad this nce by	w you've o ion date o multiple the serve	downloade vill not times on due to	change. your b the inc	\n rowser, lusion d	a compl	lete copy «							
Y Li	\n <htm <htm \n Cong This Thus will fiel \n</htm </htm 	ased text al>\n gratulation file's file's if you l only be ld in you	data: ons aga last mo downlo sent c	text/ht in! No dificat ad this nce by	w you've o ion date o multiple the serve	downloade vill not times on due to	change. your b the inc	\n rowser, lusion d	a compl	lete copy «							
Y Li	\n <htm <htm \n Cong This Thus will fiel \n</htm </htm 	ased text al>\n gratulation file's file's if you l only be ld in you	data: ons aga last mo downlo sent c	text/ht in! No dificat ad this nce by	w you've o ion date o multiple the serve	downloade vill not times on due to	change. your b the inc	\n rowser, lusion d	a compl	lete copy «							
Y Li	\n <htm <htm \n Cong This Thus will fiel \n</htm </htm 	ased text al>\n gratulation file's file's if you l only be ld in you	data: ons aga last mo downlo sent c	text/ht in! No dificat ad this nce by	w you've o ion date o multiple the serve	downloade vill not times on due to	change. your b the inc	\n rowser, lusion d	a compl	lete copy «							
Y Li	\n <htm <htm \n Cong This Thus will fiel \n</htm </htm 	ased text al>\n gratulation file's file's if you l only be ld in you	data: ons aga last mo downlo sent c	text/ht in! No dificat ad this nce by	w you've o ion date o multiple the serve	downloade vill not times on due to	change. your b the inc	\n rowser, lusion d	a compl	lete copy «							
Y Lin	\n <htm <htm \n Cong This Thus will fiel \n</htm </htm 	ased text al>\n gratulation file's file's if you l only be ld in you	data: ons aga last mo downlo sent c	text/ht in! No dificat ad this nce by	w you've o ion date o multiple the serve	downloade vill not times on due to	change. your b the inc	\n rowser, lusion d	a compl	lete copy «							2
<	ne-ba <htm <htm Cong This Thus will fie] \n <td>ased text nl>\n gratulati i file's i if you L only be ld in you cml>\n</td><td>data: ons aga last mo downlo sent c r brows</td><td>text/ht in! No dificat ad this nce by er's HT</td><td>w you've e ion date t multiple the server TP GET rea</td><td>downloade will not times on due to uuest to</td><td>change. your b the inc the ser</td><td>\n prowser, lusion (ver.\n</td><td>a compl of the l</td><td>lete copy ∢ IN-MODIFIED</td><td></td><td></td><td></td><td></td><td></td><td></td><td>3</td></htm </htm 	ased text nl>\n gratulati i file's i if you L only be ld in you cml>\n	data: ons aga last mo downlo sent c r brows	text/ht in! No dificat ad this nce by er's HT	w you've e ion date t multiple the server TP GET rea	downloade will not times on due to uuest to	change. your b the inc the ser	\n prowser, lusion (ver.\n	a compl of the l	lete copy ∢ IN-MODIFIED							3
< Lin 00000	<pre>ne-ba </pre> /n Cong This Thus will fie /n 98	ased text al>\n gratulating file's if you t only be d in you cml>\n af 65 95	data: ons aga last mc downlc sent c r brows d7 d3	text/ht in! No dificat ad this nce by er's HT 98 48	w you've o ion date o multiple the serve	downloade will not times on due to uuest to 2f 08 00	change. your b the inc the ser 45 00	<nowser, incomeser, ilusion of ver.\n ·ver.\n</nowser, 	a compl	lete copy < IN-MODIFIET							
< Lin 0000 0010	<pre>ne-ba <htm 03<="" 98="" <="" \="" cong="" fie="" ht="" n="" pre="" this="" thus="" will=""></htm></pre>	ased text al>\n gratulating s if you is if you id in you cml>\n af 65 95 02 30 82	data: ons aga last mc downlo sent c r brows d7 d3 40 00	text/ht in! No dificat ad this nce by er's HT 98 48 2c 06	w you've tion date t multiple the server TP GET rer 27 58 f6	lownloade will not times on due to quest to 24 08 00 77 f5 0c	change. your b the inc the ser 45 00 c0 a8	<noise< p=""></noise<>	a compi of the I	lete copy < IN-MODIFIED							
c c 0000 0010 0020 0020 0030	ne-ba <htm <htm \n Cong This Thus Thus Will fiel \n <td>ased text al>\n gratulatii s file's i if you t only be d in you cml>\n af 65 95 02 30 82 70 00 50 ed 13 ed</td><td>data: ons agg last mc downlc sent c r brows d7 d3 40 00 cd fa 60 00</td><td>in! No dificat ad this nce by er's HT 98 48 2c 06 f8 10 48 54</td><td>w you've a ion date to multiple the server TP GET rea 27 58 f6 e3 d7 80 23 c1 e8 54 50 26</td><td>downloade vill not times on due to quest to 2f 08 00 77 f5 0c 76 05 9c 76 05 9c 71 2e 31</td><td>change. your b the inc the ser 45 00 c0 a8 50 18 20 32</td><td><</td><td>a compi of the 1 -H 'X./ ,W </td><td>lete copy < IN-MODIFIED</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></htm </htm 	ased text al>\n gratulatii s file's i if you t only be d in you cml>\n af 65 95 02 30 82 70 00 50 ed 13 ed	data: ons agg last mc downlc sent c r brows d7 d3 40 00 cd fa 60 00	in! No dificat ad this nce by er's HT 98 48 2c 06 f8 10 48 54	w you've a ion date to multiple the server TP GET rea 27 58 f6 e3 d7 80 23 c1 e8 54 50 26	downloade vill not times on due to quest to 2f 08 00 77 f5 0c 76 05 9c 76 05 9c 71 2e 31	change. your b the inc the ser 45 00 c0 a8 50 18 20 32	<	a compi of the 1 -H 'X./ ,W 	lete copy < IN-MODIFIED							
Lin 0000 0010 0020	ne-ba <htm <htm \n Cong This Thus Thus Will fiel \n <td>ased text al>\n gratulatii s file's i if you t only be d in you cml>\n af 65 95 02 30 82 70 00 50 ed 13 ed</td><td>data: ons agg last mc downlc sent c r brows d7 d3 40 00 cd fa 60 00</td><td>in! No dificat ad this nce by er's HT 98 48 2c 06 f8 10 48 54</td><td>w you've tion date t multiple the server TP GET rer 27 58 f6 e3 d7 80 23 c1 e8</td><td>downloade vill not times on due to quest to 2f 08 00 77 f5 0c 76 05 9c 76 05 9c 71 2e 31</td><td>change. your b the inc the ser 45 00 c0 a8 50 18 20 32</td><td><</td><td>a compi of the] -H 'X-/ ,W</td><td>lete copy < IN-MODIFIED</td><td></td><td></td><td></td><td></td><td></td><td></td><td>,</td></htm </htm 	ased text al>\n gratulatii s file's i if you t only be d in you cml>\n af 65 95 02 30 82 70 00 50 ed 13 ed	data: ons agg last mc downlc sent c r brows d7 d3 40 00 cd fa 60 00	in! No dificat ad this nce by er's HT 98 48 2c 06 f8 10 48 54	w you've tion date t multiple the server TP GET rer 27 58 f6 e3 d7 80 23 c1 e8	downloade vill not times on due to quest to 2f 08 00 77 f5 0c 76 05 9c 76 05 9c 71 2e 31	change. your b the inc the ser 45 00 c0 a8 50 18 20 32	<	a compi of the] -H 'X-/ ,W	lete copy < IN-MODIFIED							,

10. 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?

Yes.

 Hypertext Transfer Protocol 	
<pre>> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n</pre>	
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 Geo	(ko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image	e/ap
Accept-Encoding: gzip, deflate\r\n	
Accept-Language: en-US,en;q=0.9\r\n	
If-None-Match: "173-5c9bb03b7df44"\r\n	
If-Modified-Since: Tue, 17 Aug 2021 05:59:02 GMT\r\n	
\r\n	
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]	
[HTTP request 2/4]	
[Prev request in frame: 4354]	
[Response in frame: 4370]	

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.

We get a HTTP/1.1 304 Not Modified Response. This is much shorter than the full response packet seen previously.

Section of the secting of the secting of the secting of the secting of the sec

12. 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?

Two, packet numbers = 64 and 89.

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

Packet numbers = 71 and 130

- **14. What is the status code and phrase in the response?** HTTP1.1/200 OK
- 15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

4	*Wi-Fi																-		\times
File	Edit	View Go	Captu	re Analyze	Statistics	Telephony	Wireless	Tools	Help										
4		0	1 1 1	9 🛶 🕯	• 🕾 Ŧ 🗄		0,0,0	11											
								•										X	• +
No.		Time		Source		Destinatio	on		Protocol	Length	Info								
	6	4 9.223886		192.168.1	.112	128.11	9.245.12		HTTP			eshark-	labs/HTTP-	wireshar	k-file3.	html H	ITTP/1	.1	
-	7	1 9.459266		128.119.2	45.12	192.16	8.1.112		HTTP	83	5 HTTP/1.1	200 OK	(text/ht	=1)					
	8	9 9.850226		192.168.1	.112	128.11	9.245.12		HTTP	53	0 GET /wir	eshark-	labs/HTTP-	wireshar	k-file3.	html H	ITTP/1	.1	
	13	0 10.08157	7	128.119.2	45.12	192.16	8.1.112		HTTP	83	5 HTTP/1.1	200 OK	(text/ht	=l)					
> 1	Frame	71 - 835	hytes (on wire ((6680 bits),	835 hvt	tes cantu	uned (6	680 hit	s) on	interface	Device	NPE (130)	54DE9-6D	R3-4461-R	SEC-4	C6143E	800483	id (
					:f6:2f (98													,	,
					Src: 128.11								,						
>	Frans	mission Co	ontrol	Protocol,	, Src Port:	80, Dst	Port: 5	\$1951,	Seq: 40	81, Ad	k: 284, Le	n: 781							
\sim	[4 Re	assembled	TCP Se	egments (4	4861 bytes)	: #66(13	360), #68	8(1360)	, #69(1	360),	#71(781)]								
	LE.	name: 66,	payloa	d: 0-1359) (1360 byt	es)]													
	[F	name: 68,	payloa	d: 1360-2	2719 (1360	bytes)]													
	LE.	name: 69,	payloa	d: 2720-4	1079 (1360	bytes)]													
	[E	name: 71,	payloa	d: 4080-4	1860 (781 b	ytes)]													
	[5	egment cou	int: 4]																
	[R	eassembled	I TCP]	ength: 48	361]														
					454502f312e	31203230	30204f4b	/0d0a44	6174653a	20547	5652c20313	7204175	672032]						
>	lyper	text Trans	sfer Pi	otocol															
>	Line-	based text	t data:	text/htm	ml (98 line	25)													

4 TCP Segments.

HTML Documents with Embedded Objects

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Three, 128.119.245.12 178.79.137.164

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.

No.	Ti	ime	Source	Destination	Protocol	Length Info
	300 57	7.002131	192.168.1.112	128.119.245.12	HTTP	337 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
	302 57	7.236246	128.119.245.12	192.168.1.112	HTTP	1355 HTTP/1.1 200 OK (text/html)
	304 57	7.306597	192.168.1.112	128.119.245.12	HTTP	413 GET /pearson.png HTTP/1.1
	331 57	7.542729	128.119.245.12	192.168.1.112	HTTP	945 HTTP/1.1 200 OK (PNG)
+	336 57	7.617334	192.168.1.112	128.119.245.12	HTTP	530 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
~	344 57	7.848425	128.119.245.12	192.168.1.112	HTTP	1355 HTTP/1.1 200 OK (text/html)

The browser downloaded the two images in serially. I believe this to be the case because the first image was requested and sent before the second image was requested by the browser. Had they been running in parallel, both files would have been requested then would have returned in the same time period. In this case however, the second image was only requested after the first image came back.

HTTP Authentication

ile Edi	t View Go Cap	oture Analyze Statistics	Telephony Wireless Too	ls Help	
	🤊 📄 🖹	🙆 । ९ 👄 🔿 🖀 👔	👲 📃 🔳 @, @, @, 🏢		
ttp					
	Time	Source	Destination	Protocol	Length Info
1	52 24.063369	192.168.1.112	128.119.245.12	HTTP	353 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
16	51 24.286369	128.119.245.12	192.168.1.112	HTTP	771 HTTP/1.1 401 Unauthorized (text/html)
1	75 24.669458	192.168.1.112	128.119.245.12	HTTP	546 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
2:	L0 24.895334	128.119.245.12	192.168.1.112	HTTP	771 HTTP/1.1 401 Unauthorized (text/html)
24	11 33.246068	192.168.1.112	128.119.245.12	HTTP	607 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
24	46 33.496770	128.119.245.12	192.168.1.112	HTTP	771 HTTP/1.1 <mark>401 Unauthorized</mark> (text/html)
29	97 51.239530	192.168.1.112	128.119.245.12	HTTP	631 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
30	02 51.478094	128.119.245.12	192.168.1.112	HTTP	544 HTTP/1.1 2 <mark>00 OK</mark> (text/html)
Ethe	rnet II, Src:	IntelCor_95:d7:d3 (9		t: Tp-Link	its) on interface \Device\NPF_(13D64DE9-6DB3-4461-B5EC-4C6143E8CCA8}, id 0 <t_58:f6:2f (98:48:27:58:f6:2f)<="" th=""></t_58:f6:2f>
			t: 51897, Dst Port: 8		Ack: 1 en: 577
	rtext Transfer		c. 51057, 530 POLC. 6	, ,,	, Nex. 1, Cen. 5/7
			/HTTP-wireshark-file5.	.html HTTF	2/1.1\r\n
	ost: gaia.cs.ur		,		
	onnection: keep				
Ca	ache-Control: r	1ax-age=0\r\n			
> A	uthorization: E	Basic d2lyZXNoYXJrLX	N0dWR1bnRzOm51dHdvcms=	=\r\n	
	grade-Insecure	-Requests: 1\r\n			
U	Brade Insecure				
			10.0; Win64; x64) App	oleWebKit/	'537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36\r\n
U	ser-Agent: Moz	illa/5.0 (Windows NT			'537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36\r\n e/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
U: Ad	ser-Agent: Mozi cept: text/htm	illa/5.0 (Windows NT			

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

HTTP/1.1 401 Unauthorized

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Authorization field as shown in the above picture.