

Zachary Waters

Ellen Zegura

1/31/2019

CS 3251

Homework 1:

1.

1.1:

HTTP, ICMPv6, UDP

1.2:

The GET message was sent at 18:01:51:456053 and the RESPONSE message was received at 18:01:51:506744 so it took 0.50691 seconds.

1.3:

The URL of the server is: </wireshark-labs/INTRO-wireshark-file1.html>

The URL of my computer is: /1.1

The IP address of the server is: 128.119.245.12

The IP address of my computer is: 10.0.0.171

1.4:

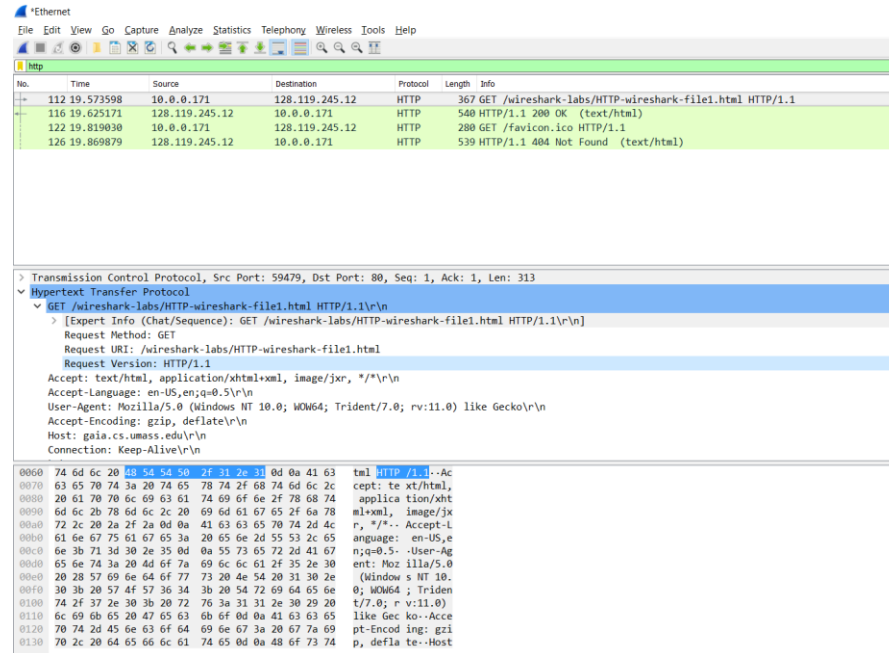
The two print pages for the GET and RESPONSE messages are attached separately in the submission.

2.

2.1:

My browser is running version 1.1 of HTTP, while the server is running version 1.1

Screen Shot of the GET message with the Highlighted Portion Below:



Screen Shot of the RESPONSE message with the Highlighted Portion Below:

*Ethernet						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
112	19.573598	10.0.0.171	128.119.245.12	HTTP	367	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
116	19.625171	128.119.245.12	10.0.0.171	HTTP	540	HTTP/1.1 200 OK (text/html)
122	19.819030	10.0.0.171	128.119.245.12	HTTP	280	GET /favicon.ico HTTP/1.1
126	19.869879	128.119.245.12	10.0.0.171	HTTP	539	HTTP/1.1 404 Not Found (text/html)
> Transmission Control Protocol, Src Port: 80, Dst Port: 59479, Seq: 1, Ack: 314, Len: 486 > Hypertext Transfer Protocol > HTTP/1.1 200 OK\r\n > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n] Response Version: HTTP/1.1 Status Code: 200 [Status Code Description: OK] Response Phrase: OK Date: Thu, 31 Jan 2019 21:10:32 GMT\r\n Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n Last-Modified: Thu, 31 Jan 2019 06:59:02 GMT\r\n ETag: "8b-580bbfb8d0a"\r\n Accept-Ranges: bytes\r\n						
0030	00 ed 36 68 00 00	48 54 54 50 2f 31 2e 31	20 32	--6h--	41	TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 54 68 75	00 OK--D	ate: Thu		
0050	2c 20 33 31 20 4a 61 6e	20 32 30 31 39 20 32 31	,	31 Jan 2019 21		
0060	3a 31 30 3a 33 32 20 47	4d 54 0d 0a 53 65 72 76	:	10:32 G MT--Serv		
0070	65 72 3a 20 41 70 61 63	68 65 2f 32 2e 34 2e 36	er: Apac	he/2.4.6		
0080	20 28 43 65 6e 74 4f 53	29 20 4f 70 65 6e 53 53	(CentOS)	OpenSS		
0090	4c 2f 31 2e 30 2e 32 6b	2d 66 69 70 73 20 50 48	L/1.0.2k	-fips PH		
00a0	50 2f 35 2e 34 2e 31 36	20 6d 6f 64 5f 70 65 72	P/5.4.16	mod_per		
00b0	6c 2f 32 2e 30 2e 31 30	20 50 65 72 6c 2f 76 35	1/2.0.10	Perl/v5		
00c0	2e 31 36 2e 33 0d 0a 4c	61 73 74 2d 4d 6f 64 69	.16.3--L	ast-Modi		
00d0	66 69 65 64 3a 20 54 68	75 2c 20 33 31 20 4a 61	fied: Th	u, 31 Ja		
00e0	6e 20 32 30 31 39 20 30	36 3a 35 39 3a 30 32 20	n 2019 0	6:59:02		
00f0	47 4d 54 0d 0a 45 54 61	67 3a 20 22 38 30 2d 35	GMT--Etag:	g: "80-5		
0100	38 30 62 62 38 66 62 38	64 30 34 61 22 0d 0a 41	80bbfb8	d0a"--A		

2.2:

My browser indicates that it can accept English.

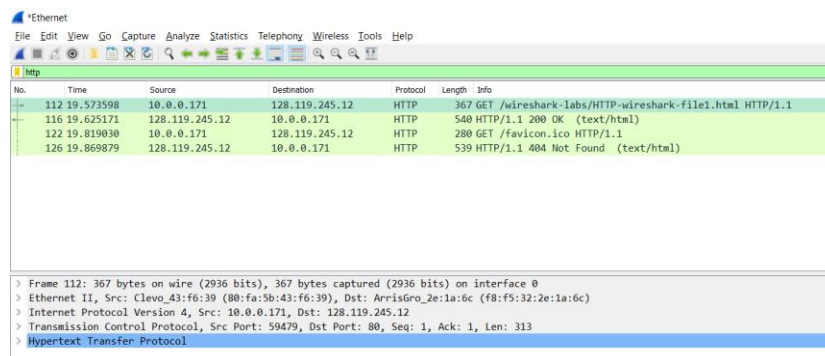
Screen Shot of the GET message with the Highlighted Portion Below:

*Ethernet						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
112	19.573598	10.0.0.171	128.119.245.12	HTTP	367	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
116	19.625171	128.119.245.12	10.0.0.171	HTTP	540	HTTP/1.1 200 OK (text/html)
122	19.819030	10.0.0.171	128.119.245.12	HTTP	280	GET /favicon.ico HTTP/1.1
126	19.869879	128.119.245.12	10.0.0.171	HTTP	539	HTTP/1.1 404 Not Found (text/html)
> Transmission Control Protocol, Src Port: 59479, Dst Port: 80, Seq: 1, Ack: 1, Len: 313 > Hypertext Transfer Protocol > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n] Request Method: GET Request URI: /wireshark-labs/HTTP-wireshark-file1.html Request Version: HTTP/1.1 Accept: text/html,application/xhtml+xml,image/jpeg,*/*\r\n Accept-Language: en-US,en;q=0.5\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n Accept-Encoding: gzip, deflate\r\n Host: gaia.cs.umass.edu\r\n Connection: Keep-Alive\r\n						
0090	6d 6c 2b 78 6d 6c 2c 20	69 6d 61 67 65 2f 6a 78	ml+xml,	image/jx		
00a0	72 2c 20 2a 2f 2a 0d 0a	41 63 63 65 70 7a 2d 4c	r,*/*--	Accept-1		
00b0	01 6e 67 75 61 67 65 3a	20 65 6e 2d 55 53 2c 65	language:	en-US,e		
00c0	6e 3b 71 3d 30 2e 35 0d	0a 55 73 65 72 2d 41 67	q;q=0.5,	User-Ag		
00d0	65 6e 74 3a 20 4d 6f 7a	69 6c 6c 61 2f 35 2e 30	ent: Moz	illa/5.0		
00e0	20 28 57 69 6e 64 6f 77	73 20 4e 54 20 31 30 2e	(window	s NT 10.		
00f0	30 3b 20 57 4f 57 36 3a	3b 20 54 72 69 64 65 6e	0; WOW64	; Triden		
0100	74 2f 32 2e 30 3b 20 72	76 3a 31 31 2e 30 29 20	t/7.0; r	v:11.0)		
0110	6c 69 6b 65 20 47 65 63	6b 6f 0d 0a 41 63 63 65	like Gec	ko-Acce		
0120	70 74 2d 45 6e 63 6f 64	69 6e 67 3a 20 67 7a 69	pt-Encod	ing: gzi		
0130	70 2c 20 64 65 66 6c 61	74 65 0d 0a 48 6f 73 74	p, defla	te--Host		
0140	3a 20 67 61 69 61 2e 63	73 2e 75 6d 61 73 73 2e	: gaia.c	s.umass.		
0150	65 64 75 0d 0a 43 6f 6e	6e 65 63 74 69 6f 6e 3a	edu--Con	nection:		
0160	20 4b 65 65 70 2d 41 6c	69 76 65 0d 0a 0d 0a	Keep-Al	ive...		

2.3:

My computer's IP address is 10.0.0.171, while the IP address of the server is 128.119.245.12

Screen Shot of the GET message with the Highlighted Portion Below:



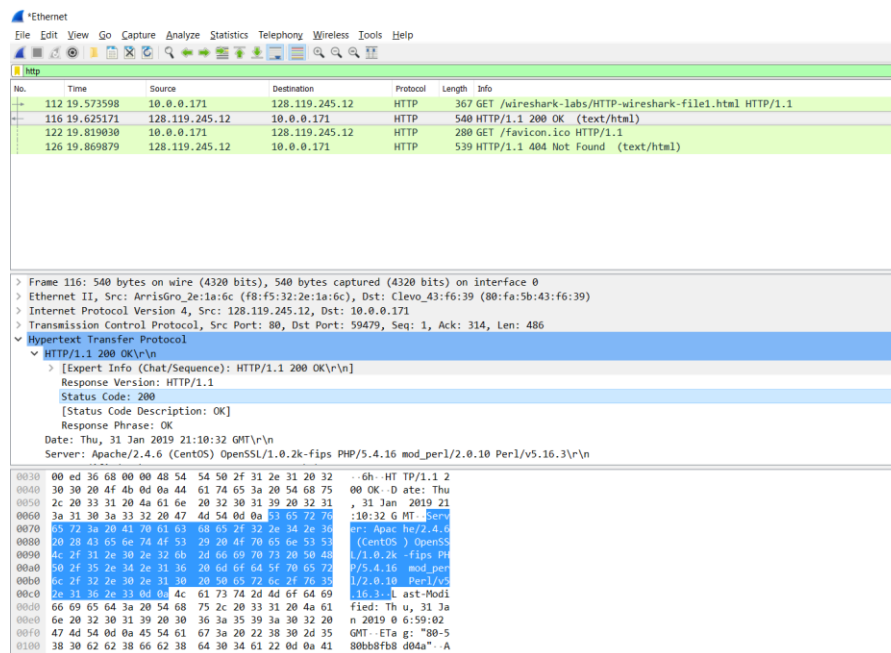
No.	Time	Source	Destination	Protocol	Length	Info
112	19.573598	10.0.0.171	128.119.245.12	HTTP	367	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
116	19.625171	128.119.245.12	10.0.0.171	HTTP	540	HTTP/1.1 200 OK (text/html)
122	19.819030	10.0.0.171	128.119.245.12	HTTP	280	GET /favicon.ico HTTP/1.1
126	19.869879	128.119.245.12	10.0.0.171	HTTP	539	HTTP/1.1 404 Not Found (text/html)

> Frame 112: 367 bytes on wire (2936 bits), 367 bytes captured (2936 bits) on interface 0
> Ethernet II, Src: Clevo_43:f6:39 (80:fa:5b:43:f6:39), Dst: ArriaGro_2e:1a:6c (f8:f5:32:2e:1a:6c)
> Internet Protocol Version 4, Src: 10.0.0.171, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59479, Dst Port: 80, Seq: 1, Ack: 1, Len: 313
> Hypertext Transfer Protocol

2.4:

The status code returned from the server is 200.

Screen Shot of the RESPONSE message with the Highlighted Portion Below:



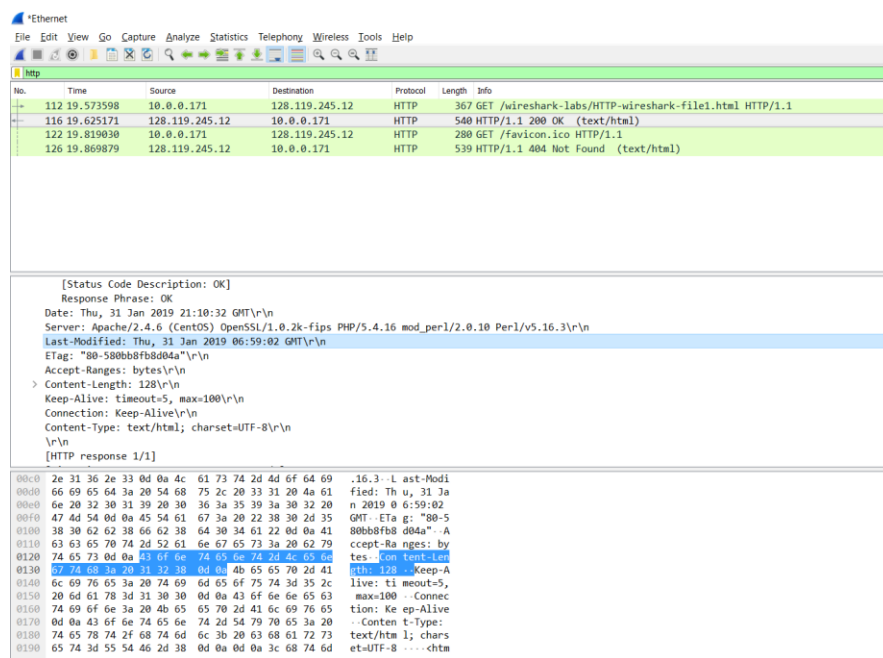
No.	Time	Source	Destination	Protocol	Length	Info
112	19.573598	10.0.0.171	128.119.245.12	HTTP	367	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
116	19.625171	128.119.245.12	10.0.0.171	HTTP	540	HTTP/1.1 200 OK (text/html)
122	19.819030	10.0.0.171	128.119.245.12	HTTP	280	GET /favicon.ico HTTP/1.1
126	19.869879	128.119.245.12	10.0.0.171	HTTP	539	HTTP/1.1 404 Not Found (text/html)

> Frame 116: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: ArriaGro_2e:1a:6c (f8:f5:32:2e:1a:6c), Dst: Clevo_43:f6:39 (80:fa:5b:43:f6:39)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.171
> Transmission Control Protocol, Src Port: 80, Dst Port: 59479, Seq: 1, Ack: 314, Len: 486
> Hypertext Transfer Protocol
 > HTTP/1.1 200 OK\r\n
 > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n
 Response Version: HTTP/1.1
 Status Code: 200
 [Status Code Description: OK]
 Response Phrase: OK
 Date: Thu, 31 Jan 2019 21:10:32 GMT\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n

2.5:

The retrieved HTML file was last modified Thu, 31 Jan 2019 06:59:02

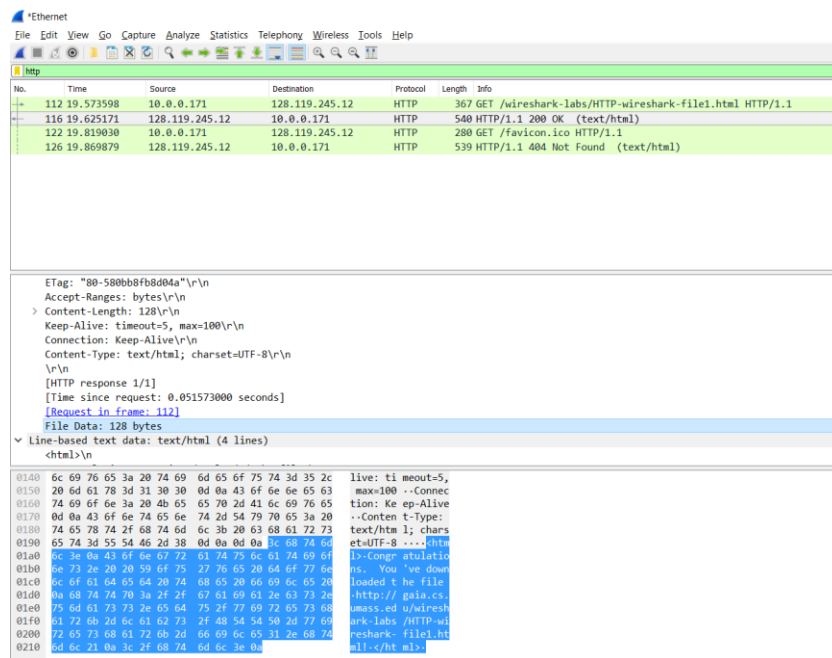
Screen Shot of the RESPONSE message with the Highlighted Portion Below:



2.6:

The retrieved file was 128 bytes.

Screen Shot of the RESPONSE message with the Highlighted Portion Below:



2.7:

I was unable to find anything that was not displayed in the packet-listing window.

2.8:

I do not see a “IF-MODIFIED-SINCE” line

2.9:

The Server explicitly returned the contents of the file, you can see this by looking at the Line-based text data field.

Screen Shot of the RESPONSE message with the Highlighted Portion Below:

*Ethernet						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
20	2.092891	2601:c0:c67f:e09f:1...	2600:1402:2000::17d...	HTTP	75	Continuation
29	2.905230	10.0.0.171	72.21.91.29	HTTP	55	Continuation
93	4.592847	10.0.0.171	128.119.245.12	HTTP	432	GET /wireshack-labs/HTTP-wireshark-file2.html HTTP/1.1
> Frame 96: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface 0 > Ethernet II, Src: ArrisGro_2e:1a:6c (f8:f5:32:2e:1a:6c), Dst: Clevo_43:f6:39 (80:fa:5b:43:f6:39) > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.171 > Transmission Control Protocol, Src Port: 80, Dst Port: 65473, Seq: 1, Ack: 379, Len: 730 > Hypertext Transfer Protocol						
Line-based text data: text/html (10 lines) <pre> \n <html>\n \n Congratulations again! Now you've downloaded the file lab2-2.html.
\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
\n will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\n field in your browser's HTTP GET request to the server.\n \n </html>\n </pre>						
0000	50 2f 35 2e 34 2e 31 36	20 6d 6f 64 5f 70 65 72	P/5.4.16 mod_per			
0000	6c 2f 32 2e 30 2e 31 30	20 50 65 72 6c 2f 76 35	1/2.0.10 Perl/v5			
0000	2e 31 36 2e 33 0d 0a 4c	61 73 74 2d 4d 6f 64 69	.16.3.1 Last-Modi			
0000	66 69 65 64 3a 20 54 68	75 2c 20 33 31 20 4a 61	fied: Thu, 31 Jan			
0000	6e 20 32 30 31 39 20 30	36 3a 35 39 3a 30 32 20	n 2019 0 6:59:02			
0000	47 4d 54 8d 0a 45 54 61	67 3a 20 22 31 37 33 2d	GMT. Eta g: "173-			
0100	35 38 30 62 62 38 66 62	38 63 34 39 32 22 0d 0a	580bbbfb 8c492"			
0110	41 63 63 65 70 74 2d 52	61 6e 67 65 73 3a 20 62	Accept-Ranges: b			
0120	79 74 65 73 0d 0a 43 6f	6e 74 65 6e 74 2d 4c 65	ytes. Content-Le			
0130	6e 67 74 68 3a 20 33 37	31 0d 0a 4b 65 65 70 2d	ngth: 37.1. Keep-			
0140	41 6c 69 76 65 3a 20 74	69 6d 65 6f 75 74 3d 35	Alive: timeout=5			
0150	2c 20 6d 61 78 3d 31 30	30 0d 0a 43 6f 6e 65	, max=10.0. Conne			
0160	63 74 69 6f 6e 3a 20 4b	65 65 70 2d 41 6c 69 76	ction: Keep-Alive			
0170	65 0d 0a 43 6f 6e 74 65	6e 74 2d 54 79 70 65 3a	e. Content-Type:			
0180	20 74 65 78 74 2f 68 74	6d 6c 3b 20 63 68 61 72	text/html; char			
0190	73 65 74 3d 55 54 46 2d	38 0d 0a 0d 0a 0a 3c 68	set-UTF-8... 			
01a0	78 6d 65 3a 20 0d 0a 43 6f	6e 67 72 61 74 75 6c 61	ml">Congratulations			
01b0	74 69 6f 6e 73 20 61 67	61 69 6e 21 20 20 4a 61	tions again! Now			
01c0	77 20 79 6f 75 27 76 65	20 64 6f 77 6e 6c 6f 61	w you've downloa			
01d0	64 65 64 20 74 68 65 20	66 69 6c 65 20 6c 61 62	ded the file lab			

2.10:

Yes, there is now a “IF-MODIFIED-SINCE” line in the GET request, what follows is “Thu, 31 Jan 2019 06:59:02 GMT/r/n”.

Screen Shot of the GET message with the Highlighted Portion Below:

Ethernet

File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help

HTTP

No.	Time	Source	Destination	Protocol	Length	Info
20	2.092891	2601:c0:c67f:e09f:1...	2600:1402:2000::17d...	HTTP	75	Continuation
20	2.905230	10.0.0.171	72.21.91.29	HTTP	55	Continuation
93	4.592847	10.0.0.171	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
96	4.643432	128.119.245.12	10.0.0.171	HTTP	784	HTTP/1.1 200 OK (text/html)
97	4.673184	10.0.0.171	128.119.245.12	HTTP	373	GET /favicon.ico HTTP/1.1
98	4.719475	128.119.245.12	10.0.0.171	HTTP	538	HTTP/1.1 404 Not Found (text/html)
178	20.490229	10.0.0.171	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
182	20.556899	128.119.245.12	10.0.0.171	HTTP	294	HTTP/1.1 304 Not Modified
209	21.161785	10.0.0.171	72.21.91.29	OCSP	506	Request
211	21.176397	72.21.91.29	10.0.0.171	OCSP	842	Response
231	21.910258	2601:c0:c67f:e09f:1...	2600:1402:2000::17d...	HTTP	372	GET /success.txt HTTP/1.1
235	21.924668	2600:1402:2000::17d...	2601:c0:c67f:e09f:1...	HTTP	458	HTTP/1.1 200 OK (text/plain)

Frame 178: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface 0
Ethernet II, Src: Clevo_43:f6:39 (80:fa:5b:43:f6:39), Dst: ArrisGro_2e:1a:6c (f8:f5:32:2e:1a:6c)
Internet Protocol Version 4, Src: 10.0.0.171, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 65476, Dst Port: 80, Seq: 1, Ack: 1, Len: 490
Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0\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

If-Modified-Since: Thu, 31 Jan 2019 06:59:02 GMT\r\n

If-None-Match: "173-580bb8fb8c492"\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 1/1]

[Response in frame: 182]

01a0

2d 52 65 71 75 65 73 74

73 3a 20 31 0d 0a 40 66

-Request s: 1..

01b0

40 6d 65 69 66 69 65 64

2d 53 69 66 63 65 3a

If-Modified-Since:

01c0

20 54 68 75 2c 20 33 31

20 4a 61 60 20 32 38 31

Thu, 31 Jan 201

01d0

39 20 30 36 3a 35 39 3a

30 32 20 47 4d 54 0d 0a

0 06:59:02 GMT-

01e0

49 66 2d 4e 6f 6e 65 2d

4d 61 74 63 68 3a 20 22

If-None-Match: "

01f0

31 37 33 2d 35 38 30 62

62 38 66 62 38 63 34 39

173-580bb8fb8c49

2.11:

The Server Sent a 304-status code with the phrase NOT MODIFIED. And did not return the content of the file.

http						
No.	Time	Source	Destination	Protocol	Length	Info
20	2.092891	2601:c0:c67f:e09f:1...	2600:1402:2000::17d...	HTTP	75	Continuation
29	2.905230	10.0.0.171	72.21.91.29	HTTP	55	Continuation
93	4.592847	10.0.0.171	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
96	4.643432	128.119.245.12	10.0.0.171	HTTP	784	HTTP/1.1 200 OK (text/html)
97	4.673184	10.0.0.171	128.119.245.12	HTTP	373	GET /favicon.ico HTTP/1.1
98	4.719475	128.119.245.12	10.0.0.171	HTTP	538	HTTP/1.1 404 Not Found (text/html)
178	20.490229	10.0.0.171	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
182	20.556899	128.119.245.12	10.0.0.171	HTTP	294	HTTP/1.1 304 Not Modified
209	21.161785	10.0.0.171	72.21.91.29	OCSP	506	Request
211	21.176397	72.21.91.29	10.0.0.171	OCSP	842	Response
231	21.910258	2601:c0:c67f:e09f:1...	2600:1402:2000::17d...	HTTP	372	GET /success.txt HTTP/1.1
235	21.924668	2600:1402:2000::17d...	2601:c0:c67f:e09f:1...	HTTP	458	HTTP/1.1 200 OK (text/plain)

> Frame 182: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface 0

> Ethernet II, Src: ArrisGro_2e:1a:6c (f8:f5:32:2e:1a:6c), Dst: Clevo_43:f6:39 (80:fa:5b:43:f6:39)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.171

> Transmission Control Protocol, Src Port: 80, Dst Port: 65476, Seq: 1, Ack: 491, Len: 240

> Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

Date: Thu, 31 Jan 2019 22:28:04 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n

Connection: Keep-Alive\r\n

Keep-Alive: timeout=5, max=100\r\n

ETag: "173-580bb8fb8c492"\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.066670000 seconds]

[Request in frame: 178]

0030	00 ed 2c 95 00 00 48 54	54 50 2f 31 2e 31 20 32	... HTTP/1.1 3
0040	30 34 20 4e 6f 74 20 4d	6f 64 69 66 69 65 64 0e	304 Not Modified
0050	00 44 61 74 65 3a 20 54	68 75 2c 20 33 31 20 4a	Date: Thu, 31 J
0060	61 6e 20 32 30 31 39 20	32 32 3a 32 38 3a 30 34	en 2019 22:28:04
0070	20 47 4d 54 0d 0a 53 65	72 76 65 72 3a 20 41 70	GMT-Server: Ap
0080	61 63 68 65 2f 32 2e 34	2e 36 20 28 43 65 6e 74	ache/2.4.6 (Cent

2.12:

3 GET requests were sent. The Packet with number 35 was the GET message for the bill of rights.

*Ethernet						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
35	19:58:09.050729	10.0.0.171	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
41	19:58:09.100771	128.119.245.12	10.0.0.171	HTTP	535	HTTP/1.1 200 OK (text/html)
43	19:58:09.130710	10.0.0.171	128.119.245.12	HTTP	373	GET /favicon.ico HTTP/1.1
45	19:58:09.174950	128.119.245.12	10.0.0.171	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1047	19:58:15.581001	2601:c0:c67f:e09f:b...	2600:1403:15::17c8:...	HTTP	372	GET /success.txt HTTP/1.1
1054	19:58:15.608129	2600:1403:15::17c8:...	2601:c0:c67f:e09f:b...	HTTP	458	HTTP/1.1 200 OK (text/plain)

2.13:

The packet with number 41 contains the status code and phrase associated with the response to the GET request.

2.14:

The status code is 200, and the response phrase is “OK”.

http						
No.	Time	Source	Destination	Protocol	Length	Info
2049	20:01:25.751505	10.0.0.1	10.0.0.171	HTTP/X...	249	HTTP/1.1 200 OK
2079	20:01:35.565512	10.0.0.171	10.0.0.1	HTTP	137	GET /IGDdevicedesc_br1an0.xml HTTP/1.1
2085	20:01:35.580842	10.0.0.1	10.0.0.171	HTTP/X...	249	HTTP/1.1 200 OK
2091	20:01:35.586426	10.0.0.171	10.0.0.1	HTTP/X...	564	POST /upnp/control/WANIPConnection0 HTTP/1.1
2096	20:01:35.615995	10.0.0.1	10.0.0.171	HTTP/X...	396	HTTP/1.1 200 OK
2338	20:02:16.097409	10.0.0.171	128.119.245.12	HTTP	483	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
2345	20:02:16.151588	128.119.245.12	10.0.0.171	HTTP	535	HTTP/1.1 200 OK (text/html)

> Frame 41: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0 > Ethernet II, Src: ArrisGro_2e:1a:6c (f8:f5:32:2e:1a:6c), Dst: Clevo_43:f6:39 (80:fa:5b:43:f6:39) > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.171 > Transmission Control Protocol, Src Port: 80, Dst Port: 49632, Seq: 4381, Ack: 379, Len: 481 > [4 Reassembled TCP Segments (4861 bytes): #37(1460), #38(1460), #40(1460), #41(481)] > Hypertext Transfer Protocol						
> HTTP/1.1 200 OK\r\n > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]						
Response Version: HTTP/1.1 Status Code: 200 [Status Code Description: OK] Response Phrase: OK Date: Fri, 01 Feb 2019 00:58:08 GMT\r\n Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n Last-Modified: Thu, 31 Jan 2019 06:59:02 GMT\r\n ETag: "1194-580bb8fb87e41"\r\n Accept-Ranges: bytes\r\n > Content-Length: 4500\r\n Keep-Alive: timeout=5, max=100\r\n						

0000	48	54	54	50	2f	31	2e	31	20	32	30	30	20	4f	4b	0d	HTTP/1.1	200	OK
0010	0a	44	61	74	65	3a	20	46	72	69	2c	20	30	31	20	46	Date: Fri, 01 Feb		
0020	65	62	20	32	30	31	39	20	30	30	3a	35	38	3a	30	38	eb 2019 00:58:08		
0030	20	47	4d	54	0d	0a	53	65	72	76	65	72	3a	20	41	70	GMT-Se rver: Ap		
0040	61	63	68	65	2f	32	2e	34	2e	36	20	28	43	65	6e	74	ache/2.4 .6 (Cent		
0050	4f	53	29	20	4f	70	65	6e	53	53	4c	2f	31	2e	30	2e	OS) Open SSL/1.0.		
0060	32	6b	2d	66	69	70	73	20	50	48	50	2f	35	2e	34	2e	2k-fips PHP/5.4.		
0070	31	36	20	6d	6f	64	5f	70	65	72	6c	2f	32	2e	30	2e	16 mod_p erl/2.0.		
0080	31	30	20	50	65	72	6c	2f	76	35	2e	31	36	2e	33	0d	10 Perl/ v5.16.3		
0090	0a	4c	61	73	74	2d	4d	6f	64	69	66	69	65	64	3a	20	Last-Mo dified:		
00a0	54	68	75	2c	20	33	31	20	4a	61	6e	20	32	30	31	39	Thu, 31 Jan 2019		
00b0	20	30	36	3a	35	39	3a	30	32	20	47	4d	54	0d	0a	45	06:59:0 2 GMT-E		

2.15:

The Response message was broken up into 4 TCP segments.

2.16:

4 GET requests were sent.

http						
No.	Time	Source	Destination	Protocol	Length	Info
17	20:29:06.011311	10.0.0.171	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
20	20:29:06.062424	128.119.245.12	10.0.0.171	HTTP	1127	HTTP/1.1 200 OK (text/html)
21	20:29:06.096634	10.0.0.171	128.119.245.12	HTTP	389	GET /pearson.png HTTP/1.1
26	20:29:06.142851	128.119.245.12	10.0.0.171	HTTP	745	HTTP/1.1 200 OK (PNG)
35	20:29:06.197470	10.0.0.171	128.119.245.12	HTTP	403	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
36	20:29:06.245167	10.0.0.171	128.119.245.12	HTTP	373	GET /favicon.ico HTTP/1.1
53	20:29:06.286999	128.119.245.12	10.0.0.171	HTTP	538	HTTP/1.1 404 Not Found (text/html)
134	20:29:06.344987	128.119.245.12	10.0.0.171	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)

2.17:

I believe they were downloaded serially, as the requests and responses for the two images were at different times.

2.18:

The server's RESPONSE message contains status code 401 and phrase "Unauthorized".

http						
No.	Time	Source	Destination	Protocol	Length	Info
3	20:39:41.955315	2601:c0:c67f:e09f:b...	2600:1403:15::17c8:...	HTTP	75	Continuation
35	20:39:44.316361	10.0.0.171	128.119.245.12	HTTP	447	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
37	20:39:44.368268	128.119.245.12	10.0.0.171	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
120	20:40:01.737131	2601:c0:c67f:e09f:b...	2600:1403:15::17c8:...	HTTP	372	GET /success.txt HTTP/1.1
127	20:40:01.765286	2600:1403:15::17c8:...	2601:c0:c67f:e09f:b...	HTTP	458	HTTP/1.1 200 OK (text/plain)
242	20:40:16.172466	10.0.0.171	128.119.245.12	HTTP	506	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
244	20:40:16.224098	128.119.245.12	10.0.0.171	HTTP	583	HTTP/1.1 404 Not Found (text/html)
246	20:40:16.296074	10.0.0.171	128.119.245.12	HTTP	373	GET /favicon.ico HTTP/1.1
247	20:40:16.339754	128.119.245.12	10.0.0.171	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 37: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface 0

> Ethernet II, Src: ArrisGro_2e:1a:6c (f8:f5:32:2e:1a:6c), Dst: Clevo_43:f6:39 (80:fa:5b:43:f6:39)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.171

> Transmission Control Protocol, Src Port: 80, Dst Port: 49885, Seq: 1, Ack: 394, Len: 717

> Hypertext Transfer Protocol

> HTTP/1.1 401 Unauthorized\r\n

> Date: Fri, 01 Feb 2019 01:39:43 GMT\r\n

> Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 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]

> [Time since request: 0.051907000 seconds]

> [Request in frame: 35]

> File Data: 381 bytes

> Line-based text data: text/html (12 lines)

2.19:

The second GET request has the added phrase "/success.txt" and has the added fields "Cache-Control: no-cache/r/n" and Pragma "no-cache/r/n".

*Ethernet						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
3	20:39:41.955315	2601:c0:c67f:e09f:b...	2600:1403:15::17c8:...	HTTP	75	Continuation
35	20:39:44.316361	10.0.0.171	128.119.245.12	HTTP	447	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
37	20:39:44.368268	128.119.245.12	10.0.0.171	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
120	20:40:01.737131	2601:c0:c67f:e09f:b...	2600:1403:15::17c8:...	HTTP	372	GET /success.txt HTTP/1.1
127	20:40:01.765286	2600:1403:15::17c8:...	2601:c0:c67f:e09f:b...	HTTP	458	HTTP/1.1 200 OK (text/plain)
242	20:40:16.172466	10.0.0.171	128.119.245.12	HTTP	506	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
244	20:40:16.224098	128.119.245.12	10.0.0.171	HTTP	583	HTTP/1.1 404 Not Found (text/html)
246	20:40:16.296074	10.0.0.171	128.119.245.12	HTTP	373	GET /favicon.ico HTTP/1.1
247	20:40:16.339754	128.119.245.12	10.0.0.171	HTTP	538	HTTP/1.1 404 Not Found (text/html)

<	
> Frame 120: 372 bytes on wire (2976 bits), 372 bytes captured (2976 bits) on interface 0 > Ethernet II, Src: Clevo_A3:f6:39 (80:fa:5b:43:f6:39), Dst: ArrisGro_2e:1a:6c (f8:f5:32:2e:1a:6c) > Internet Protocol Version 6, Src: 2601:c0:c67f:e09f:b028:729a:ae47:e73e, Dst: 2600:1403:15::17c8:ec1a > Transmission Control Protocol, Src Port: 49848, Dst Port: 80, Seq: 2, Ack: 1, Len: 298 > Hypertext Transfer Protocol > GET /success.txt HTTP/1.1\r\n Host: detectportal.firefox.com\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0\r\n Accept: */*\r\n Accept-Language: en-US,en;q=0.5\r\n Accept-Encoding: gzip, deflate\r\n Cache-Control: no-cache\r\n Pragma: no-cache\r\n Connection: keep-alive\r\n \r\n [Full request URI: http://detectportal.firefox.com/success.txt] [HTTP request 1/1] [Response in frame: 127]	

3.

3.1:

The end to end delay is the time it takes for “the whole message” to arrive, in this case it’s the time it takes for the tenth and final car to cross the finish line. We can solve this problem by separating it out into two subproblems. The first subproblem is to figure out how long it would take a car going 100km/hour to travel 150 km. The solution to this is trivial, its 1.5 hours or 90 minutes. The second subproblem is that we need to calculate the time it would take for the final car to get through all three tollbooths. Each tollbooth can only serve a single car and it takes 12 seconds for the car to be served. So, 3 tollbooths multiplied by 12 seconds multiplied by 10 cars gives us the time of 360 seconds (6 minutes) for the final car to complete its final tollbooth. Which means the end to end time for this problem is 6 minutes + 90 minutes = 96 minutes.

3.2:

With 8 cars the only thing that’s changed is the total tollbooth time which we can still solve using 3 tollbooths multiplied by 12 seconds a car multiplied by 8 cars. Which is 288 seconds (4.8 minutes), so our final solution is 4.8 minutes + 90 minutes = 94.8 minutes.

4.

To get a bit from Host A to B it must first be put into a packet, to be put in a packet the bit must wait for all the other bits in the packet to be generated. A packet is 48 bytes, or 384 bits, and host A has a 64-kbps stream. We have 64000 bits a second, or 1 bit per 0.000015625 seconds. So, to fill in all 384 bits of a packet it takes 0.006 seconds. The transmission rate of 2Mbps means we can send 2 million bits per second, so to send our 1 packet of 384 bits it would take 0.000192 seconds. Finally, the propagation delay is 10msec or 0.01 seconds. Our total time is $0.01 + 0.000192 + 0.006 = 0.016192$ seconds.

5.

5.1:

To construct an equation for generating the end to end delay of a packet. We first calculate the time it takes for a packet of length L to be transmitted onto all the links in the system. This can be solved by dividing the length of the packet by the transmission rate of each switch and then summing them all together. Next, we need to calculate the delay caused by the packet propagating through each of the links by summing the length of the link divided by the propagation speed of the same link. finally, we need to account for is the total delay caused by the processing through summing the Dproc's for each of the packet switches. Now our final solution is simply the summation of all the above.

$$\text{End to End Delay} = L/R_1 + L/R_2 + L/R_3 + D_1/S_1 + D_2/S_2 + D_3/S_3 + D_{\text{proc}1} + D_{\text{proc}2}$$

5.2:

The packet is 1,500 bytes or 12000 bits. The transmission rate of all 3 links is 2 Mbps or 2 million bits per second. Which is a bit per 0.0000005 seconds. So, to transmit a packet though a link is 0.006 seconds. It goes through 3 links so it will take a total of 0.018 for the transmission time of all links. The propagation delay of all switches is 3msec or 0.003 seconds and because there are 2 switches it will take 0.006 seconds. Now we simply calculate the time of the length of each link divided by its propagation speed. So $5000\text{km}/2.5 \times 10^8 \text{m/s} + 4000\text{km}/2.5 \times 10^8 \text{m/s} + 1000\text{km}/2.5 \times 10^8 \text{m/s} = 0.02 \text{ seconds} + 0.016 \text{ seconds} + 0.004 \text{ seconds} = 0.04 \text{ seconds}$. Now we simply add it all up. $0.04 + 0.006 + 0.018 = 0.064 \text{ seconds}$

6.

6.1:

Assuming a parallel, non-persistent, connection, we would split it into 10 connections each sharing the 150/bits per second bandwidth connection, meaning they have access to 15 bits per second. Now assuming you are trying to download a packet of 100,000 bits long it would take, the number of bits divided by the download speed of a connection plus the transmission time of the getting that. We simply repeat these 3 times for the number of control packets each of size 200 bits that we also need to receive.

$$\left(\frac{200}{150}\right)3 + \left(\frac{200}{15}\right)3 + \left(\frac{1000000}{150}\right) + \left(\frac{1000000}{15}\right) = 7377 \text{ seconds}$$

6.2:

With a persistent connection:

$$\left(\frac{200}{150}\right)3 + \left(\frac{1000000}{150}\right) + 10\left(\left(\frac{200}{150}\right) + \left(\frac{1000000}{15}\right)\right) = 7351 \text{ seconds}$$

6.3:

The persistent connection is slightly better.