

NETWORK LAB

LAB ASSIGNMENT for Week # 2

Usirikayala Likhith

20223295, D2

HTTP

1. The Basic HTTP GET/response interaction

Note: Answer the following questions using the http-ethereal-trace-1 packet trace to answer the

questions below

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

ANS:

No.	Time	Source	Destination	Protocol	Length	Info
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)	0000	00 06 25 da af 73 00 08	74 4f 36 23 08 00 45 00	.X.s - t06# E
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)	0010	02 1d 01 cd 40 00 00 06	00 00 c0 a8 01 66 80 77	...@... ..f.w
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12	0020	f5 0c 10 1f 00 50 f5 32	64 b2 6b a6 54 92 50 18P 2 d k.T.P.
Transmission Control Protocol, Src Port: 4127, Dst Port: 80, Seq: 1, Ack: 1, Len: 501	0030	fa f0 39 a2 00 00 47 45	54 20 2f 65 74 68 65 72	- 9 - GE T /ether
Hypertext Transfer Protocol	0040	65 61 6c 2d 6c 61 62 73	2f 6c 61 62 32 2d 31 2e	eal-lab/ /lab2-1.
	0050	68 74 6d 6c 20 48 54 54	50 2f 31 2e 31 0d 0a 48	html HTTP/1.1 H
	0060	6f 73 74 3a 20 67 61 69	61 2e 63 73 2e 75 6d 61	ost: gai a.c.s.uma
	0070	73 73 2e 65 64 75 0d 0a	55 73 65 72 2d 41 67 65	ss.edu - User-Age
	0080	6e 74 3a 20 4d 6f 7a 69	6c 6c 61 2f 35 2e 30 20	nt: Mozilla/5.0
	0090	28 57 69 6e 64 6f 77 73	3b 20 55 3b 20 57 69 6e	(Windows ; U; Win
	00a0	64 6f 77 73 20 4e 54 20	35 2e 31 3b 20 65 6e 2d	dows NT 5.1; en-
	00b0	55 53 3b 20 72 76 3a 31	2e 30 2e 32 29 20 47 65	US; rv:1.0.2) Ge
	00c0	63 6b 6f 2f 32 30 30 32	31 31 32 30 20 4e 65 74	cko/2002.1120 Net
	00d0	73 63 61 70 65 2f 37 2e	30 31 0d 0a 41 63 63 65	scape/7.01 Acce
	00e0	70 74 3a 20 74 65 70 74	2f 78 6d 6c 2c 61 70 70	pt: text/xml,app
	00f0	6c 69 63 61 74 69 6f 6e	2f 78 6d 6c 2c 61 70 70	lication /xml,app
	0100	6c 69 63 61 74 69 6f 6e	2f 78 6d 74 6d 6c 2b 78	lication /xhtml+x
	0110	6d 6c 2c 74 65 78 74 2f	68 74 6d 6c 3b 71 3d 30	ml;text/ html;q=0
	0120	2e 39 2c 74 65 78 74 2f	70 6c 61 69 6e 3b 71 3d	.9;text/plain;q=
	0130	30 2e 38 2c 76 69 64 65	6f 2f 78 2d 6d 6e 67 2c	0.9;vide o/x-mng,
	0140	69 6d 61 67 65 2f 70 6e	67 2c 69 6d 61 67 65 2f	image/png,image/
	0150	6a 70 65 67 2c 69 6d 61	67 65 2f 67 69 66 3b 71	jpeg,image/gif;q

My browser is running HTTP version 1.1 and HTTP version of the server is also 1.1.

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

ANS:

American English and English of weight 0.5 were accepted by the server.

No.	Time	Source	Destination	Protocol	Length	Info
10	4.694950	192.168.1.102	128.119.245.12	HTTP	555	GET /etherreal-labs/lab2-1.html HTTP/1.1
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

<p>Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)</p> <p>Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)</p> <p>Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12</p> <p>Transmission Control Protocol, Src Port: 80, Dst Port: 4127, Seq: 1, Ack: 1, Len: 501</p> <p>Hypertext Transfer Protocol</p> <p>GET /etherreal-labs/lab2-1.html HTTP/1.1\r\n</p> <p>Host: gaia.cs.umass.edu\r\n</p> <p>User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n</p> <p>Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng;q=0.5,image/png,gif;q=0.3,*/*;q=0.1\r\n</p> <p>Accept-Language: en-us,en;q=0.50\r\n</p> <p>Accept-Encoding: gzip, deflate, compress;q=0.9\r\n</p> <p>Accept-Charset: ISO-8859-1, utf-8;q=0.66,*;q=0.66\r\n</p> <p>Keep-Alive: 300\r\n</p> <p>Connection: keep-alive\r\n</p> <p>\r\n</p> <p>[Full request URI: http://gaia.cs.umass.edu/etherreal-labs/lab2-1.html]</p> <p>[HTTP request 1/2]</p> <p>[Response in frame 12]</p> <p>[Next request in frame 13]</p>	<pre> 0000 73 63 61 70 65 2f 37 2e 30 31 0d 0a 41 63 63 65 scape/7. 01 Acce 0000 70 74 3a 20 74 65 78 74 2f 78 6d 6c 2c 61 70 70 pt: text/xml,app 0000 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c 61 70 70 lication/xml,app 0000 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 lication/xhtml;x 0000 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 71 3d 30 ml;text/html;q= 0000 2e 39 2c 74 65 78 74 2f 70 6c 61 69 6e 3b 71 3d .5;text/plain;q= 0000 30 2c 38 2c 76 69 64 65 6f 2f 78 2d 6d 6e 67 2c 0.8,video/x-mng; 0000 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65 2f image/png,gimage/ 0000 6a 70 65 67 2c 69 6d 61 67 65 2f 67 69 66 3b 71 jpeg,image/gif;q 0000 3d 30 2e 32 2c 74 65 78 74 2f 63 73 73 2c 2a 2f =0.2;text/css,/* 0000 2a 3b 71 3d 30 2e 31 0d 0a 41 63 63 65 70 74 2d *q=0.1 Accept- 0000 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 2c Language: en-us, 0000 20 65 6e 3b 71 3d 30 2e 35 30 0d 0a 41 63 63 65 en;q=0.50 Acce 0000 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 p-encod ing: gzi 0000 70 2c 20 64 65 66 6e 61 74 65 2c 20 63 6f 6d 70 p, defla te, comp 0000 72 65 73 73 3b 71 3d 30 2e 39 0d 0a 41 63 63 65 ross;q=0.9 Acce 0000 70 74 2d 43 68 61 72 73 65 74 3a 20 49 53 4f 2d pt-Chara et: ISO- 0000 38 35 39 2d 31 2c 20 75 74 66 2d 38 3b 71 3d 3d 8859-1, utf-8;q= 0000 30 26 36 3e 2c 20 2a 3b 71 3d 30 2e 38 36 0d 0a 0.66,*;q=0.66 0000 4b 65 65 70 2d 41 6e 69 76 65 3a 20 33 30 30 0d Keep-Alive: 300 0000 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 .Connect ion: kee 0000 70 2d 61 6c 69 76 65 0d 0a 0d 0a p-alive: </pre>
--	---

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

ANS:

The IP address of my computer is 192.168.1.102 and the IP address of the server is 128.119.245.12 .

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

ANS:

The Status Code returned from the server to browser is 200 OK.

No.	Time	Source	Destination	Protocol	Length	Info
10	4.694950	192.168.1.102	128.119.245.12	HTTP	555	GET /etherreal-labs/lab2-1.html HTTP/1.1
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

<p>Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)</p> <p>Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)</p> <p>Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102</p> <p>Transmission Control Protocol, Src Port: 80, Dst Port: 4127, Seq: 1, Ack: 502, Len: 385</p> <p>Hypertext Transfer Protocol</p> <p>HTTP/1.1 200 OK\r\n</p> <p>Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n</p> <p>Server: Apache/2.0.40 (Red Hat Linux)\r\n</p> <p>Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n</p> <p>ETag: "1bfed-49-79d5bf00"\r\n</p> <p>Accept-Ranges: bytes\r\n</p> <p>Content-Length: 73\r\n</p> <p>Keep-Alive: timeout=10, max=100\r\n</p> <p>Connection: Keep-Alive\r\n</p> <p>Content-Type: text/html; charset=ISO-8859-1\r\n</p> <p>\r\n</p> <p>[HTTP response 1/2]</p> <p>[Time since request: 0.024143000 seconds]</p> <p>[Request in frame 10]</p> <p>[Next request in frame 13]</p> <p>[Next response in frame 14]</p>	<pre> 0000 19 20 7a 1c 00 00 48 54 54 50 2f 31 2e 31 20 32 2 HT TP/1.1 2 0000 30 20 2f 4b 0d 0d 44 61 74 65 3a 20 54 75 65 00 OK: Date: Tue 0000 2c 20 32 33 20 53 65 70 20 32 30 33 20 30 35 , 23 Sep 2003 05 0000 3a 32 39 3a 35 30 20 47 4d 54 0d 0a 53 65 72 76 :29:50 GMT- Serv 0000 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34 er: Apac he/2.0.4 0000 30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78 0 (Red Hat Linux 0000 20 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64)-Last-Modified 0000 3a 20 54 75 65 2c 20 32 33 20 53 65 70 20 32 30 : Tue, 23 Sep 20 0000 30 33 20 30 35 3a 32 39 3a 30 20 47 4d 54 0d 0a 03 05:29 :00 GMT- 0000 0a 45 54 61 67 3a 20 22 31 62 66 65 64 2d 34 39 -ETag: " 1bfed-49 0000 2d 37 39 64 35 62 66 30 30 22 0d 0a 41 63 63 65 -79d5bf00"-Acce 0000 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 pt-Range s: bytes 0000 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 .Content t-Length 0000 3a 20 37 33 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 : 73--Ke ep-Alive 0000 3a 20 74 69 6d 65 67 75 74 31 30 2c 20 6d 61 : timeout=10, ma 0000 78 3d 31 30 30 0d 0a 43 6f 6e 65 63 7a 69 6f x:100--C connectio 0000 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 n: Keep-Alive--C 0000 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 ontent-T ype: tex 0000 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3a t/html; charsets 0000 49 53 4f 2d 38 38 35 39 2d 31 0d 0a 0d 0a 3c 68 ISO-8859 -1----ch 0000 74 6d 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 tml> Con gratulat 0000 69 6f 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f ions . You've do </pre>
---	---

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

ANS:

The HTML file was last modified on Tuesday , 23 September 2003 05:29:00 GMT.

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

ANS:

73 bytes of content are being returned to my browser.

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.

ANS:

NO Additional headers were listed in raw data window.

2. The HTTP CONDITIONAL GET/response interaction

Note: Answer the following questions using the http-ethereal-trace-2 packet trace to answer the questions below

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?

ANS:

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP/1.1
14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP/1.1
10	2.357902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

Frame 8: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)	0000	00 06 25 da af 73 00 08	74 4f 36 23 08 00 45 00	...X s...tO6W...E...
Ethernet II, Src: Dell_Af:36:23 (00:08:74:4f:36:23), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)	0010	02 1d 02 5a 40 00 80 06	00 00 c0 ad 01 66 80 77	...2B...f w...
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12	0020	f5 6c 10 37 00 40 fa 88	01 31 81 6a b3 81 5a 18	...P...1.1.P...
Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 1, Ack: 1, Len: 501	0030	fa f0 39 a2 00 00 47 45	54 20 2f 65 74 68 65 72	...9...GE T /ether...
Hypertext Transfer Protocol	0040	65 61 6c 2d 6c 61 62 73	2f 6c 61 62 32 2d 32 2e	eal-labs /lab2-2...
GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n	0050	68 74 6d 6c 20 4b 54 54	50 2f 31 2e 31 0d 0e 48	html HT /1.1. H...
Host: gais.cs.umass.edu\r\n	0060	6f 73 74 3a 20 67 61 69	61 2e 63 73 2e 75 6d 61	ost: gai a.c.s.uma...
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n	0070	73 73 2e 65 64 75 0d 0a	55 73 65 72 2d 41 67 65	ss.edu User-Age...
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng;q=0.5\r\n	0080	6e 74 3a 20 4d 6f 7a 69	6c 6c 61 2f 35 2e 30 20	nt: Mozi lla/5.0...
Accept-Language: en-us,en;q=0.50\r\n	0090	28 57 69 6e 64 6f 77 73	3b 20 55 3b 20 57 69 6e	(Windows ; U; Win...
Accept-Encoding: gzip, deflate, compress;q=0.9\r\n	00a0	64 6f 77 73 20 4e 54 20	35 2e 31 3b 20 65 6e 2d	ows NT 5.1; en;
Accept-Charset: ISO-8859-1, utf-8;q=0.66,*q=0.66\r\n	00b0	55 53 3b 20 72 76 3a 31	2e 30 2e 32 23 20 47 65	US; rv:1.0.2) Ge...
Keep-Alive: 300\r\n	00c0	63 6b 6f 2f 32 30 30 32	31 31 32 30 20 4e 65 74	cko/2002 1120 Net
Connection: keep-alive\r\n	00d0	73 63 61 70 65 2f 37 2e	30 31 0d 0a 41 63 63 65	scape/7.01; Acce...
\r\n	00e0	70 74 3a 20 74 65 78 74	2f 78 6d 6c 2c 61 70 70	pt: text /xml,app...
[HTTP request 1/2] http://gais.cs.umass.edu/ethereal-labs/lab2-2.html	00f0	6c 69 63 61 74 69 6f 6e	2f 78 6d 6c 2c 61 70 70	lication /xml,app...
[Response in frame 10]	0100	6c 69 63 61 74 69 6f 6e	2f 78 6d 6c 2c 61 70 70	lication /html-x...
[Next request in frame 14]	0110	6d 6c 2c 74 65 78 74 2f	68 74 6d 6c 3b 71 3d 30	ml;text/html;q=0...
	0120	2e 39 2c 74 65 78 74 2f	70 6c 61 69 6e 3b 71 3d	.9;text/plain;q=...
	0130	30 2e 38 2c 76 69 64 65	6f 2f 78 2d 6d 6e 67 2c	0.8;vide o/x-mng...
	0140	69 6d 61 67 65 2f 70 6e	67 2c 69 6d 61 67 65 2f	image/pn g,image/...
	0150	6a 70 65 67 2c 69 6d 61	67 65 2f 67 69 66 3b 71	jpeg,ima gn/gif;q...

There wasn't any IF-MODIFIED SINCE line in HTTP GET.

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

ANS:

Yes the Server explicitly return the contents of the file. The status word of the response message is 200 OK. So the server sent the response for the request that has been sent .

No.	Time	Source	Destination	Protocol	Length	Info
10	4.044850	192.168.1.102	128.119.245.12	HTTP	555	GET /etherreal-labs/lab2-1.html HTTP/1.1
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /Favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)	0030	19 20 7a 1c 00 00 48 54 54 50 2f 31 2e 31 20 32	z HT TP/1.1 2
Ethernet II, Src: LinksysGroup.daf:73 (00:06:25:daf:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)	0040	30 30 20 4f 4b 0d 04 44 61 74 65 3a 20 54 75 65	00 OK Date: Tue
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102	0050	2c 20 32 33 20 53 65 70 20 32 30 33 20 30 35	, 23 Sep 2003 05
Transmission Control Protocol, Src Port: 80, Dst Port: 4127, Seq: 1, Ack: 502, Len: 385	0060	3a 32 39 3a 35 30 20 47 4d 54 0d 0a 53 65 72 76	:29:50 G MT--Serv
Hypertext Transfer Protocol	0070	65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34	er: Apac he/2.0.4
HTTP/1.1 200 OK\r\n	0080	30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78	0 (Red Hat Linux
Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n	0090	29 0d 0a 4c 61 73 7a 2d 4d 64 69 66 69 65 64):-Last-Modified
Server: Apache/2.0.40 (Red Hat Linux)\r\n	00a0	3a 20 54 75 65 2c 20 32 33 20 53 65 70 20 32 30	: Tue, 2 3 Sep 20
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n	00b0	30 33 20 30 35 3a 32 39 3a 30 20 47 4d 54 0d	03 05:29 :00 GMT-
ETag: "1bfed-49-79d5bf00"\r\n	00c0	0a 45 54 61 67 3a 20 22 31 62 66 65 64 2d 34 39	-ETag: " 1bfed-49
Accept-Ranges: bytes\r\n	00d0	70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73	pt-Range s: bytes
Content-Length: 73\r\n	00e0	0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68	..Conten t-Length
Keep-Alive: timeout=10, max=100\r\n	0100	3a 20 37 33 0d 0a 4b 65 65 70 2d 41 6c 69 76 65	: 73--Ke ep-Alive
Connection: Keep-Alive\r\n	0110	3a 20 74 69 6d 65 6f 75 74 3d 31 30 2c 20 6d 61	: timeout t=10, ma
Content-Type: text/html; charset=ISO-8859-1\r\n	0120	78 3d 31 30 30 0d 0a 43 6f 6e 65 63 74 69 6f	x=100--c connectio
\r\n	0130	6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43	n: Keep- Alive--C
[HTTP response 1/2]	0140	6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78	ontent-T ype: tex
[Time since request: 0.024143000 seconds]	0150	74 2f 68 74 6d 6c 30 20 63 68 61 72 73 65 74 3d	t/html; charset=
[Unpack in frame 14]	0160	49 53 4f 2d 38 38 35 39 2d 31 0d 0a 0d 0a 3c 68	ISO-8859 -1----ch
[Next request in frame 13]	0170	74 6d 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74	tml; con gratulat
[Next response in frame 14]	0180	69 6f 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f	ions. You've do

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?

ANS:

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /etherreal-labs/lab2-2.html HTTP/1.1
14	5.517390	192.168.1.102	128.119.245.12	HTTP	658	GET /etherreal-labs/lab2-2.html HTTP/1.1
10	2.357902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12	0140	69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65 2f	image/pn g,image/
Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 502, Ack: 686, Len: 614	0150	6a 70 65 67 2c 69 6d 61 67 65 2f 67 69 66 3b 71	jpeg,ima ge/gif;q
Hypertext Transfer Protocol	0160	3d 30 2e 32 2c 74 65 78 74 2f 63 73 73 2c 2a 2f	=0.2,tes t/css,*f
GET /etherreal-labs/lab2-2.html HTTP/1.1\r\n	0170	2a 3b 71 3d 30 2e 31 0d 0a 41 63 63 65 70 74 2d	*,q=0.1.-Accep-
Host: gaia.cs.umass.edu\r\n	0180	4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 2c	Language : en-us,
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n	0190	20 65 6e 3b 71 3d 30 2e 35 30 0d 0a 41 63 63 65	en;q=0.50--Acce
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng	01a0	70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69	pt-encod ing: gzi
Accept-Language: en-us, en;q=0.50\r\n	01b0	70 2c 20 64 65 66 6c 61 74 65 2c 20 63 6f 6d 70	p, defla te, comp
Accept-Encoding: gzip, deflate, compress;q=0.9\r\n	01c0	72 65 73 73 3b 71 3d 30 2e 39 0d 0a 41 63 63 65	ress;q=0.9--Acce
Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n	01d0	38 38 35 39 2d 31 2c 20 75 74 66 2d 38 3b 71 3d	pt-Chars et: ISO-
Keep-Alive: 300\r\n	01e0	30 2e 36 3e 2c 20 2a 3b 71 3d 30 2e 36 3e 0d	8859-1, utf-8;q=
Connection: keep-alive\r\n	01f0	4b 65 65 70 2d 41 6c 69 76 65 3a 20 33 30 30	0.66, *, q=0.66--
If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n	0200	0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65	Keep-Ali ve: 300-
If-None-Match: "1bfef-173-8f4ae900"\r\n	0210	70 2d 61 6c 69 76 65 0d 0a 49 66 2d 4d 6f 64 69	.Connect ion: kee
Cache-Control: max-age=0\r\n	0220	66 69 65 64 2d 53 69 6e 63 65 3a 20 54 75 65 2c	p-ali ve. If-Modi
\r\n	0230	2d 32 33 20 53 65 70 20 32 30 33 20 30 35 3a	fied-Sin ce: Tue,
[Full request URI: http://gaia.cs.umass.edu/etherreal-labs/lab2-2.html]	0240	33 35 3a 30 30 20 47 4d 54 0d 0a 49 66 2d 4e 6f	23 Sep 2003 05:
[HTTP request 2/2]	0250	6e 65 2d 4d 61 74 63 68 3a 20 22 31 62 66 65 66	35:00 GM T-If-No
[Unpack request in frame 8]	0260	2d 31 37 33 2d 38 66 3a 61 65 39 30 30 2d 0d 0a	ne-Match : "1bfef
[Response in frame 15]	0270	43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d	-173-8f4 ae900"-
	0280	61 78 2d 61 67 65 3d 30 0d 0a 0d 0a	Cache-Co ntrol: m
	0290		ax-age=0

Yes there is an IF-MODIFIED-SINCE header in the HTTP GET. It indicates the last date and time the file has been received a response from the server. For this file the information is Tue, 23 sep 2003 05:35:00 GMT.

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.

ANS:

The HTTP status code and phrase returned from the server in response is 304 Not Modified.

The server doesn't explicitly return the contents of the file because the file wasn't modified since the last response. So server tells to check the cache which is still valid.

3. Retrieving Long Documents

Note: Answer the following questions using the http-ethereal-trace-3 packet trace to answer the questions below

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?

ANS:

No.	Time	Source	Destination	Protocol	Length	Info
8	4.623732	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-3.html HTTP/1.1

Frame 8: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)	0000	00 06 25 da af 73 00 08	74 4f 36 23 08 00 45 00	..% s...t06# .E
Ethernet II, Src: Dell 4f:36:23 (00:08:74:4f:36:23), Dst: LinksysGroup da:af:73 (00:06:25:da:af:73)	0010	02 1d 02 04 40 00 80 06	00 00 c0 a8 01 66 80 77	...@...f.w
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12	0020	f5 0c 10 b0 00 50 fb 98	de ea 85 b2 aa 64 50 18P.....dP
Transmission Control Protocol, Src Port: 4272, Dst Port: 80, Seq: 1, Ack: 1, Len: 501	0030	fa f0 39 a2 00 00 47 45	54 20 2f 65 74 68 65 72	...9...GE T /ether
Hypertext Transfer Protocol	0040	65 61 6c 2d 6c 61 62 73	2f 6c 61 62 32 2d 33 2e	eal-labs /lab2-3,
	0050	68 74 6d 6c 20 48 54 54	50 2f 31 2e 31 0d 0a 48	html HT P/1.1. H
	0060	6f 73 74 3a 20 67 61 69	61 2e 63 73 2e 75 6d 61	ost: gai a.cs.uma
	0070	73 73 2e 65 64 75 0d 0a	55 73 65 72 2d 41 67 65	ss.edu. User-Age
	0080	6e 74 3a 20 4d 6f 7a 69	6c 6c 61 2f 35 2e 30 20	nt: Mozilla/5.0
	0090	20 57 69 6e 64 6f 77 73	3b 20 55 3b 20 57 69 6e	(Windows ; U; Win
	00a0	64 6f 77 73 20 4e 54 20	35 2e 31 3b 20 65 6e 2d	dows NT 5.1; en-
	00b0	55 53 3b 20 72 76 3a 31	2e 30 2e 32 29 20 47 65	US; rv:1.0.2) Ge
	00c0	63 6b 6f 2f 32 30 30 32	31 31 32 30 20 4e 65 74	cko/2002 1120 Net
	00d0	73 63 61 70 65 2f 37 2e	30 31 0d 0a 41 63 65 65	scape/7.01. ACce
	00e0	70 74 3a 20 74 65 78 74	2f 78 6d 6c 2c 61 70 70	pt: text /xml,app
	00f0	6c 69 63 61 74 69 6f 6e	2f 78 6d 6c 2c 61 70 70	lication /xml,app
	0100	6c 69 63 61 74 69 6f 6e	2f 78 68 74 6d 6c 2b 78	lication /html+ex
	0110	6d 6c 2c 74 65 78 74 2f	68 74 6d 6c 3b 71 3d 30	ly;text/ html;q=0
	0120	2e 39 2c 74 65 78 74 2f	70 6c 61 69 6a 3b 71 3d	;text/ plain;q=
	0130	30 2e 38 2c 76 69 64 65	6f 2f 78 2d 6d 6e 67 2c	0.8;vide o/x-mng;
	0140	69 6d 61 67 65 2f 70 6e	67 2c 69 6d 61 67 65 2f	image/png,image/
	0150	6a 70 65 67 2c 69 6d 61	67 65 2f 67 69 66 3b 74	jpeg,image/gif;q

Only one HTTP GET request has been send by the browser. The Packet number is 8.

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

ANS:

No.	Time	Source	Destination	Protocol	Length	Info
8	4.623732	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-3.html HTTP/1.1
14	4.680920	128.119.245.12	192.168.1.102	HTTP	490	HTTP/1.1 200 OK (text/html)

Frame 14: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits)

Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102

Transmission Control Protocol, Src Port: 80, Dst Port: 4272, Seq: 4381, Ack: 502, Len: 436

[4 Reassembled TCP Segments (4816 bytes): #10(1460), #11(1460), #13(1460), #14(436)]

Hypertext Transfer Protocol

Line-based text data: text/html (98 lines)

0000 00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 00 t06# . % . s . E
0010 01 dc 21 71 40 00 37 06 e9 18 80 77 f5 0c c0 a8 l06 7 w . . .
0020 01 66 00 50 10 b0 85 b2 bb 80 fb 98 e0 df 50 18 f p P
0030 19 20 25 ab 00 00 3e 3c 68 33 3e 41 6d 65 6e 64 . % . >X h3>Amend
0040 6d 65 6e 74 20 49 58 3c 2f 68 33 3e 3c 2f 73 74 ment IX< /h3><st
0050 72 6f 6e 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f rong> . <p></
0060 70 3e 3c 70 3e 54 68 65 20 65 6e 75 6d 65 72 61 p>>p>The enumera
0070 74 69 6f 6e 20 69 6e 20 74 68 65 20 43 6f 6e 73 tion in the Cons
0080 74 69 74 75 74 69 6f 6e 2c 20 6f 66 20 63 65 72 titution , of cer
0090 74 61 69 6e 20 72 69 6f 68 74 73 2c 20 73 68 61 tain rig hts, sha
00a0 6c 6c 0a 6e 6f 74 20 62 65 20 63 6f 6e 73 74 72 ll not b e constr
00b0 75 65 64 20 74 6f 20 64 65 6e 79 20 6f 72 20 64 ued to d eny or d
00c0 69 73 70 61 72 61 67 65 20 6f 74 68 65 72 73 20 isparage others
00d0 72 65 74 61 69 6e 65 64 20 62 79 20 74 68 65 20 retained by the
00e0 70 65 6f 70 6c 65 2e 0a 0a 3c 2f 70 3e 3c 70 3e people . . </p><p>
00f0 3c 61 20 6e 61 6d 65 3d 22 31 30 22 3e 3c 73 74 xt
0100 72 6f 6e 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 rong><h3 >Amendme
0110 6e 74 20 58 3c 2f 68 33 3e 3c 2f 73 74 72 6f 6e nt X</h3 ><stron
0120 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f 70 3e 0a g> . . <p></p>
0130 3c 70 3e 54 68 65 20 70 6f 77 65 72 73 20 6e 6f <p>The p owers no
0140 74 20 64 65 6c 65 67 61 74 65 64 20 74 6f 20 74 t delega ted to t

Frame (490 bytes) Reassembled TCP (4816 bytes)

The packet number is 14 which contains the status code and phrase associated with the response for HTTP GET request

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

ANS:

The Status code and phrase in response is 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?

ANS:

No.	Time	Source	Destination	Protocol	Length	Info
5	4.602642	192.168.1.102	128.119.245.12	TCP	62	4272 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
6	4.623285	128.119.245.12	192.168.1.102	TCP	62	80 → 4272 [SYN, ACK] Seq=0 Ack=1 Win=0 MSS=1460 SACK_PERM
7	4.623313	192.168.1.102	128.119.245.12	TCP	54	4272 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
8	4.623732	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-3.html HTTP/1.1
9	4.652711	128.119.245.12	192.168.1.102	TCP	60	80 → 4272 [ACK] Seq=1 Ack=502 Win=6432 Len=0
10	4.657569	128.119.245.12	192.168.1.102	TCP	1514	80 → 4272 [ACK] Seq=1 Ack=502 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
11	4.658792	128.119.245.12	192.168.1.102	TCP	1514	80 → 4272 [ACK] Seq=1461 Ack=502 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
12	4.658828	192.168.1.102	128.119.245.12	TCP	54	4272 → 80 [ACK] Seq=502 Ack=2921 Win=64240 Len=0
13	4.680438	128.119.245.12	192.168.1.102	TCP	1514	80 → 4272 [ACK] Seq=2921 Ack=502 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
14	4.680920	128.119.245.12	192.168.1.102	HTTP	490	HTTP/1.1 200 OK (text/html)
15	4.680948	192.168.1.102	128.119.245.12	TCP	54	4272 → 80 [ACK] Seq=502 Ack=4817 Win=64240 Len=0

Frame 14: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits)

Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102

Transmission Control Protocol, Src Port: 80, Dst Port: 4272, Seq: 4381, Ack: 502, Len: 436

Source Port: 80

Destination Port: 4272

[Stream index: 0]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 436]

Sequence Number: 4381 (relative sequence number)

Sequence Number (raw): 221083130

[Next Sequence Number: 4817 (relative sequence number)]

Acknowledgment Number: 502 (relative ack number)

Acknowledgment Number (raw): 4221100255

0101 = Header Length: 20 bytes (5)

Flags: 0x015 (PSH, ACK)

Window: 6432

[Calculated window size: 6432]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x25ab [unverified]

Checksum Status: Unverified

0020 01 66 00 50 10 b0 85 b2 bb 80 fb 98 e0 df 50 18 f p P
0030 19 20 25 ab 00 00 3e 3c 68 33 3e 41 6d 65 6e 64 . % . >X h3>Amend
0040 6d 65 6e 74 20 49 58 3c 2f 68 33 3e 3c 2f 73 74 ment IX< /h3><st
0050 72 6f 6e 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f rong> . <p></
0060 70 3e 3c 70 3e 54 68 65 20 65 6e 75 6d 65 72 61 p>>p>The enumera
0070 74 69 6f 6e 20 69 6e 20 74 68 65 20 43 6f 6e 73 tion in the Cons
0080 74 69 74 75 74 69 6f 6e 2c 20 6f 66 20 63 65 72 titution , of cer
0090 74 61 69 6e 20 72 69 6f 68 74 73 2c 20 73 68 61 tain rig hts, sha
00a0 6c 6c 0a 6e 6f 74 20 62 65 20 63 6f 6e 73 74 72 ll not b e constr
00b0 75 65 64 20 74 6f 20 64 65 6e 79 20 6f 72 20 64 ued to d eny or d
00c0 69 73 70 61 72 61 67 65 20 6f 74 68 65 72 73 20 isparage others
00d0 72 65 74 61 69 6e 65 64 20 62 79 20 74 68 65 20 retained by the
00e0 70 65 6f 70 6c 65 3d 22 31 30 22 3e 3c 73 74 xt
0100 72 6f 6e 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 rong><h3 >Amendme
0110 6e 74 20 58 3c 2f 68 33 3e 3c 2f 73 74 72 6f 6e nt X</h3 ><stron
0120 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f 70 3e 0a g> . . <p></p>
0130 3c 70 3e 54 68 65 20 70 6f 77 65 72 73 20 6e 6f <p>The p owers no
0140 74 20 64 65 6c 65 67 61 74 65 64 20 74 6f 20 74 t delega ted to t
0150 68 65 20 55 6e 69 74 65 64 20 53 74 61 74 65 73 he Unite d States
0160 20 62 79 20 74 68 65 20 63 6f 6e 73 74 69 74 75 by the Constitu

Frame (490 bytes) Reassembled TCP (4816 bytes)

TCP Segment Len (tcp.len)

Packets: 19 - Displayed: 11 (57.9%)

Segment count is 4.

4. HTML Documents with Embedded Objects

Note: Answer the following questions using the http-ethereal-trace-4 packet trace to answer the questions below

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

ANS:

No.	Time	Source	Destination	Protocol	Length	Info
10	7.236929	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-4.html HTTP/1.1
12	7.260813	128.119.245.12	192.168.1.102	HTTP	1057	HTTP/1.1 200 OK (text/html)
17	7.305485	192.168.1.102	165.193.123.218	HTTP	625	GET /catalog/images/pearson-logo-footer.gif HTTP/1.1
20	7.308803	192.168.1.102	134.241.6.82	HTTP	609	GET /kurose/cover.jpg HTTP/1.1
25	7.333954	165.193.123.218	192.168.1.102	HTTP	912	HTTP/1.1 200 OK (GIF89a)
54	7.589877	134.241.6.82	192.168.1.102	HTTP	1096	HTTP/1.0 200 Document follows (JPEG JFIF image)

0000	00 06 25 da af 73 00 08	74 4f 36 23 08 00 45 00	% s... t06# E
0010	02 1d 02 b1 40 00 80 06	00 00 c0 a9 01 56 80 77	... @... .. f w
0020	f5 0c 10 d3 00 50 fd 1d	3c a2 8c 57 c5 b8 50 18	... P... < W P
0030	fa f0 39 a2 00 00 47 45	54 20 2f 65 74 68 65 72	... 9... GE T /ether
0040	65 61 6c 2d 6c 61 62 73	2f 6c 61 62 32 2d 34 2e	eal-labs /lab2-4.
0050	68 74 6d 6c 20 48 84 54	50 2f 31 2e 31 0d 0a 48	html HT P/1.1 H
0060	6f 73 74 3a 20 67 61 69	61 2e 63 73 2e 75 6d 61	ost: gai a.es,ma
0070	73 73 2e 65 64 75 0d 0a	55 73 65 72 2d 41 67 65	ss.edu User-Age
0080	6e 74 3a 20 4d 6f 7a 69	6c 6c 61 2f 35 2e 30 20	nt: Mozi lla/5.0
0090	28 57 69 6e 64 6f 77 73	3b 20 55 3b 20 57 69 6e	(Windows ; U; Win
00a0	64 6f 77 73 20 4e 54 20	35 2e 31 3b 20 65 6e 2d	dows NT 5.1; en-
00b0	55 51 3b 20 72 76 3a 31	2e 30 2e 32 29 20 47 65	US; rv:1 .0.2) Ge
00c0	63 6b 6f 2f 32 30 30 32	31 31 32 30 20 4e 65 74	cko/2002 1120 Net
00d0	73 63 61 70 65 2f 37 2e	30 31 0d 0a 41 63 63 65	scape/7. 01 Acce
00e0	70 74 3a 20 74 65 78 74	2f 78 6d 6c 2c 61 70 70	pt: text /xml,app
00f0	6c 69 63 61 74 69 6f 6e	2f 78 6d 6c 2c 61 70 70	lication /xml,app
0100	6c 69 63 61 74 69 6f 6e	2f 78 68 74 6d 6c 2b 78	lication /xhtml+x
0110	6d 6c 2c 74 65 78 74 2f	68 74 6d 6c 3b 71 3d 30	ml;text/ html;q=0
0120	2e 39 2c 74 65 78 74 2f	70 6c 61 69 6e 3b 71 3d	9;text/ plain;q=
0130	30 2e 38 2c 76 69 64 65	6f 2f 78 6d 6d 6e 67 2c	0.8,vide o/x-mg,
0140	69 6d 61 67 65 2f 70 6e	67 2c 69 6d 61 67 65 2f	image/pn g,image/
0150	6a 70 65 67 2c 69 6d 61	67 65 2f 67 69 66 3b 71	jpeg,ima ge/gif;q

There were 3 HTTP GET request messages that were sent from the browser. The GET requests were sent to three different IP addresses. They are

128.119.245.12, 165.193.123.218, 134.241.6.82

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.

ANS:

The browser downloaded the two images from the two web sites in parallel. Because the request message for the two images were sent to two different IP addresses. So the response for the two images were sent from two different IP addresses. So we can say they were downloaded from two different web sites in parallel.

5. HTTP Authentications

Note: Answer the following questions using the http-ethereal-trace-5 packet trace to answer the questions below

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

ANS:

No.	Time	Source	Destination	Protocol	Length	Info
6	2.508229	192.168.1.102	128.119.245.12	HTTP	571	GET /etherreal-labs/protected_pages/lab2-5.html HTTP/1.1
9	2.538231	128.119.245.12	192.168.1.102	HTTP	278	HTTP/1.1 401 Authorization Required (text/html)
65	18.516793	192.168.1.102	128.119.245.12	HTTP	622	GET /etherreal-labs/protected_pages/lab2-5.html HTTP/1.1
68	18.541671	128.119.245.12	192.168.1.102	HTTP	499	HTTP/1.1 200 OK (text/html)

Frame 9: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits)
Ethernet II, Src: LinksysGroup, da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 1461, Ack: 518, Len: 224
[2 Reassembled TCP Segments (1684 bytes): #8(1460), #9(224)]
Hypertext Transfer Protocol
Line-based text data: text/html (56 lines)

0000 00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 00 ..t06# % . e .
0010 01 08 d4 cc 40 00 37 06 36 91 80 77 f5 0c c0 a8 ... @ 7 6 w . .
0020 01 66 00 50 10 ef 91 47 21 28 fe 37 f5 ef 50 18 . f P . . G ! (7 . P .
0030 19 20 d9 9c 00 00 45 72 72 6f 72 20 34 30 31 3c ... Er ron 401c
0040 2f 68 32 3e 0a 3c 64 6c 3e 0a 3c 64 64 3e 0a 3c /H2> <dl > <dd> <
0050 61 64 64 72 65 73 3e 0a 20 20 3c 61 20 68 72 address> < a hr
0060 65 66 3d 22 2f 22 3e 77 77 77 2d 6e 65 74 2e 63 ef="/" "sw ww-net.c
0070 73 2e 75 6d 61 73 2e 65 64 75 3c 2f 61 3e 0a s.umass. edu(
0080 20 20 3c 62 72 20 2f 3e 0a 20 20 0a 20 20 3c 73
 <s
0090 6d 61 6c 6c 3e 54 75 65 20 53 65 70 20 32 33 20 mall>Tue Sep 23
00a0 30 31 3a 33 39 3a 35 38 20 32 30 30 33 3c 2f 73 01:39:58 2003/<s
00b0 6d 61 6c 6c 3e 0a 20 20 3c 62 72 20 2f 3e 0a 20 mall>

00c0 20 3c 73 6d 61 6c 6c 3e 41 70 61 63 68 65 2f 32 <small> Apache/2
00d0 2e 30 2e 3a 30 20 28 52 65 64 20 48 61 74 20 4c .0.40 (R ed Hat L
00e0 69 6e 75 70 29 3c 2f 73 6d 61 6c 6c 3e 0a 3c 2f inux)</s mall> </
00f0 61 64 64 72 65 73 3e 0a 3c 2f 64 64 3e 0a 3c address> </dd> <
0100 2f 64 6c 3e 0a 3c 2f 6f 64 79 3e 0a 3c 2f 68 /dl> </b ody> </h
0110 74 6d 6c 3e 0a 0a tml>..

The servers response for the initial HTTP GET message from the browser is 401 Authorization Required.

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

ANS:

No.	Time	Source	Destination	Protocol	Length	Info
6	2.508229	192.168.1.102	128.119.245.12	HTTP	571	GET /etherreal-labs/protected_pages/lab2-5.html HTTP/1.1
9	2.538231	128.119.245.12	192.168.1.102	HTTP	278	HTTP/1.1 401 Authorization Required (text/html)
65	18.516793	192.168.1.102	128.119.245.12	HTTP	622	GET /etherreal-labs/protected_pages/lab2-5.html HTTP/1.1
68	18.541671	128.119.245.12	192.168.1.102	HTTP	499	HTTP/1.1 200 OK (text/html)

Frame 65: 622 bytes on wire (4976 bits), 622 bytes captured (4976 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysGroup, da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 4342, Dst Port: 80, Seq: 1, Ack: 1, Len: 568
Hypertext Transfer Protocol
GET /etherreal-labs/protected_pages/lab2-5.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,i
Accept-Language: en-us,en;q=0.50
Accept-Encoding: gzip, deflate, compress;q=0.9
Accept-Charset: ISO-8859-1, utf-8;q=0.66,*q=0.66
Keep-Alive: 300
Connection: keep-alive
Authorization: Basic ZXRoLXN0dWw1bm8zOW5ldmVvcmtz
[Full request URI: http://gaia.cs.umass.edu/etherreal-labs/protected_pages/lab2-5.html]
[HTTP request 1/1]
[Response in frame 68]

0130 2e 39 2c 74 65 78 74 2f 70 6c 61 69 6e 3b 71 3d .0,text/plain;q=
0140 30 2e 38 2c 76 69 64 65 6f 2f 78 2d 6d 6e 67 2c 0.8,video o/x-mng,
0150 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65 2f image/png,image/
0160 6a 70 65 67 2c 69 6d 61 67 65 2f 67 69 66 3b 71 jpeg,image/gif;q
0170 3d 30 2e 32 2c 74 65 78 74 2f 63 73 73 2c 2a 2f =0.2,tex t/css,*f
0180 2a 3b 71 3d 30 2e 31 0d 0a 41 63 63 65 70 74 2d *q=0.1 .Accept-
0190 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 2c Language :en-us,
01a0 20 65 6e 3b 71 3d 30 2e 35 30 0d 0a 41 63 63 65 en;q=0.50-Acce
01b0 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Incod ing: gzi
01c0 70 2c 20 64 65 66 6c 61 74 65 2c 20 63 6f 6d 70 p, defla te, comp
01d0 72 65 73 73 3b 71 3d 30 2e 39 0d 0a 41 63 63 65 res;q=0.9-Acce
01e0 70 74 2d 43 68 61 72 73 65 74 3a 20 49 53 4f 2d pt-Chara et: ISO-
01f0 38 38 35 39 2d 31 2c 20 75 74 66 2d 38 3b 71 3d 8859-1, utf-8;q
0200 30 2e 36 36 2c 20 2a 3b 71 3d 30 2e 36 36 0d 0a .0.66,*; q=0.66..
0210 4b 65 65 70 2d 41 6c 69 76 65 3a 20 33 30 30 0d Keep-Ali ve: 300.
0220 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0b 65 65 .Connect ion: kee
0230 70 2d 61 6c 69 76 65 0d 0a 41 75 74 68 6f 72 69 p-alive. Authori
0240 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 5a 58 zation: Basic ZX
0250 52 6f 4c 58 4e 30 64 5f 52 6e 62 6e 52 7a 4f 6d RoLXN0dW w1bm8zOW
0260 35 6e 64 48 64 76 63 6d 74 7a 0d 0a 0d 0a 5ldmVvc mtz...

A new field Authorization was included in the new HTTP GET message.

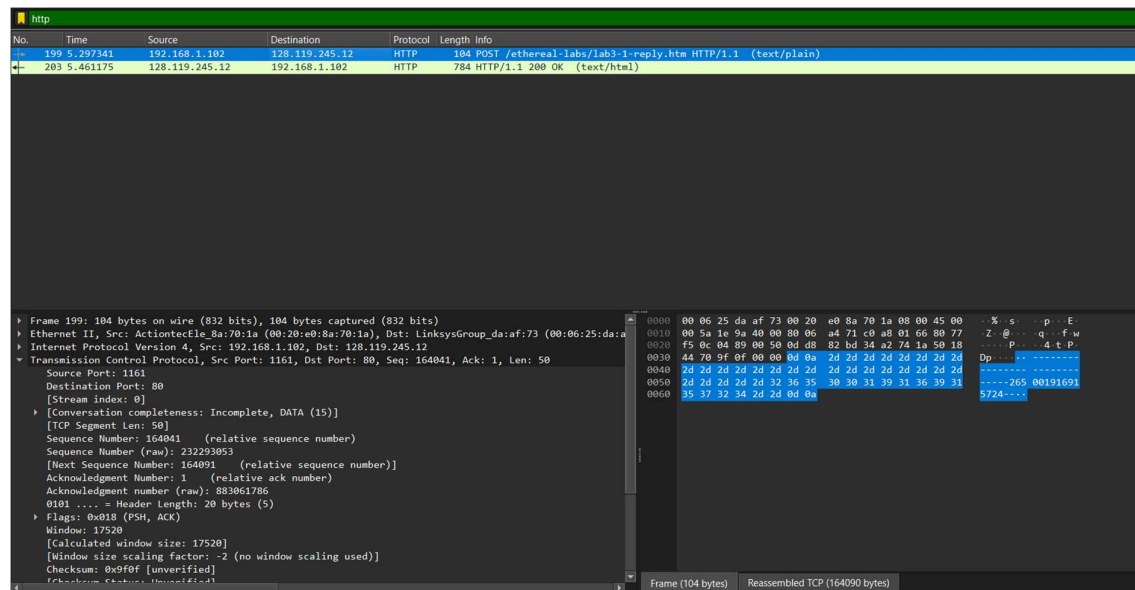
TCP

1. A first look at the captured trace

Note: Answer the following questions using the tcp-ethereal-trace-1 packet trace to answer the questions below

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window".

ANS:



The IP address for the source is 192.168.1.102 and source port number is 1161.

2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

The IP address of the destination is 128.119.245.12 and the destination port number is 80.

2. TCP Basics

Note: Answer the following questions using the tcp-ethereal-trace-1 packet trace to answer the questions below:

3. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

ANS:

tcp.flags.syn == 1 and tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
213	7.595557	192.168.1.102	199.2.53.206	TCP	62	1162 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM

[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 232129012
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0111 = Header Length: 28 bytes (7)
> Flags: 0x0002 (SYN)
0000 = Reserved: Not set
...0 = Accurate ECN: Not set
....0... = Congestion Window Reduced: Not set
....0... = ECN-Echo: Not set
....0... = Urgent: Not set
....0... = Acknowledgment: Not set
....0... = Push: Not set
....0... = Reset: Not set
>0...1... = Syn: Set
....0...0... = Fin: Not set
[TCP Flags:S]
Window: 16384

The sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu is 232129012.

BY the flags we can identify the segment as SYN SEGMENT as the SYN flag is set.

4. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

ANS:

tcp.flags.syn == 1 and tcp.flags.ack == 1

No.	Time	Source	Destination	Protocol	Length	Info
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM

[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 883061785
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 232129013
0111 = Header Length: 28 bytes (7)
> Flags: 0x0012 (SYN, ACK)
0000 = Reserved: Not set
...0 = Accurate ECN: Not set
....0... = Congestion Window Reduced: Not set
....0... = ECN-Echo: Not set
....0... = Urgent: Not set
....0... = Acknowledgment: Set
....0... = Push: Not set
....0... = Reset: Not set
>0...1... = Syn: Set
....0...0... = Fin: Not set
[TCP Flags:A.S]
Window: 5840

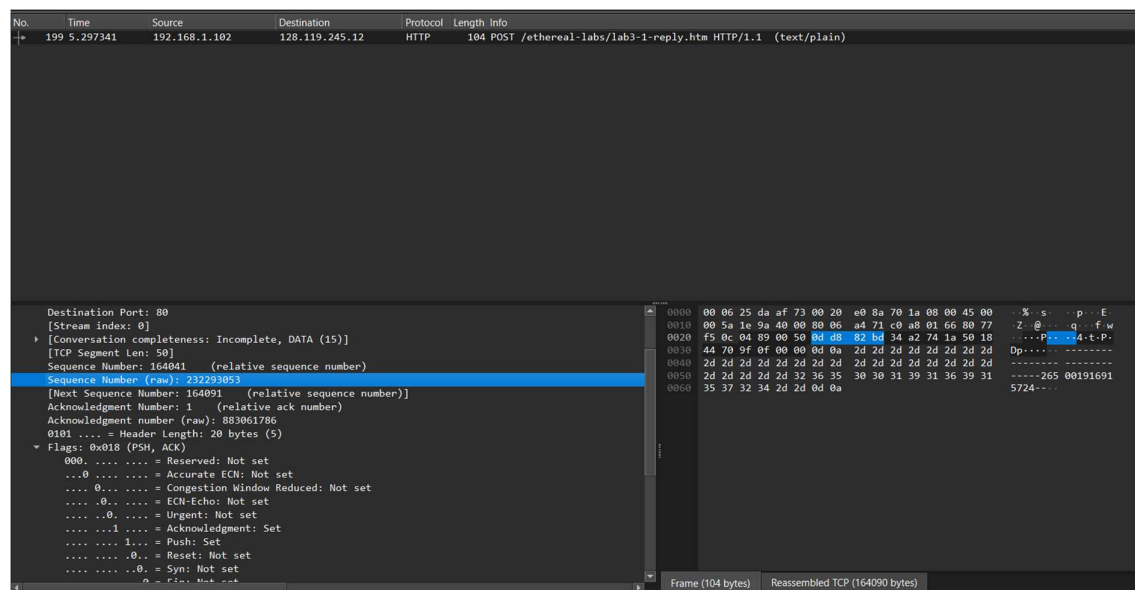
The Sequence number of SYNACK Segment is 883061785.

The Acknowledgment flag is set and the Acknowledge number is 232129013.

Both the SYN flag and Ack flags are set. By the flags we can identify the segment as SYNACK segment.

5. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command; you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

ANS:



Sequence number is 232293053

6. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received?

Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments?

Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the gaia.cs.umass.edu server.

Then select: Statistics->TCP Stream Graph->Round Trip Time Graph.

ANS:

Sequence Number:

1	t=0.026477	ack= 0.053937	rtt=0.02746
566	t=0.041737	ack=0.077294	rtt=0.035557
2026	t=0.054026	ack=0.124085	rtt=0.070059
3486	t=0.054690	ack=0.169118	rtt=0.114428
4946	t=0.077405	ack=0.217299	rtt=0.139894
6406	t=0.078157	ack=0.267802	rtt=0.189645

7. What is the length of each of the first six TCP segments?

ANS:

565, 1460, 1460, 1460, 1460

8. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

ANS:

```
▶ [Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 50]
Sequence Number: 164041 (relative sequence number)
Sequence Number (raw): 232293053
[Next Sequence Number: 164091 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 883061786
0101 .... = Header Length: 20 bytes (5)
▶ Flags: 0x018 (PSH, ACK)
Window: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x9f0f [unverified]
```

9. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

ANS:

NO

10. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment.

ANS:

1460

**11. What is the throughput (bytes transferred per unit time) for the TCP connection?
Explain how you calculated this value.**