

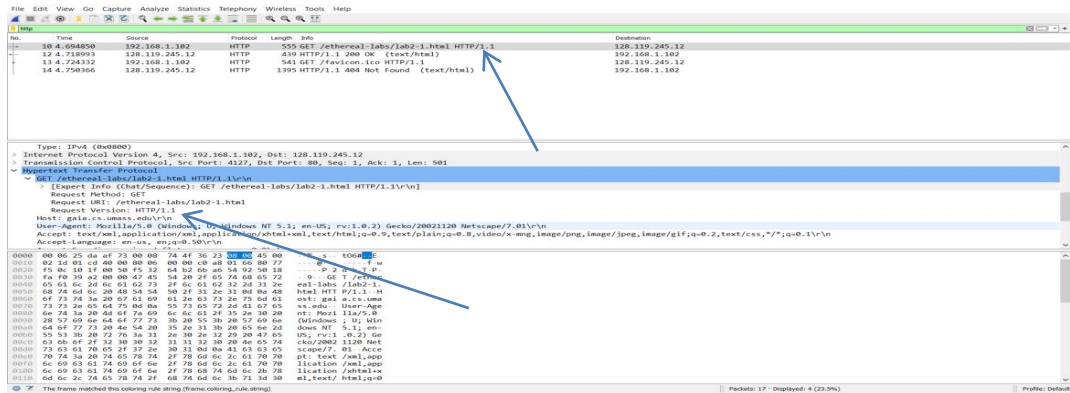
Name: Kazi Farhan Hasan Tanjim

ID: 18701018

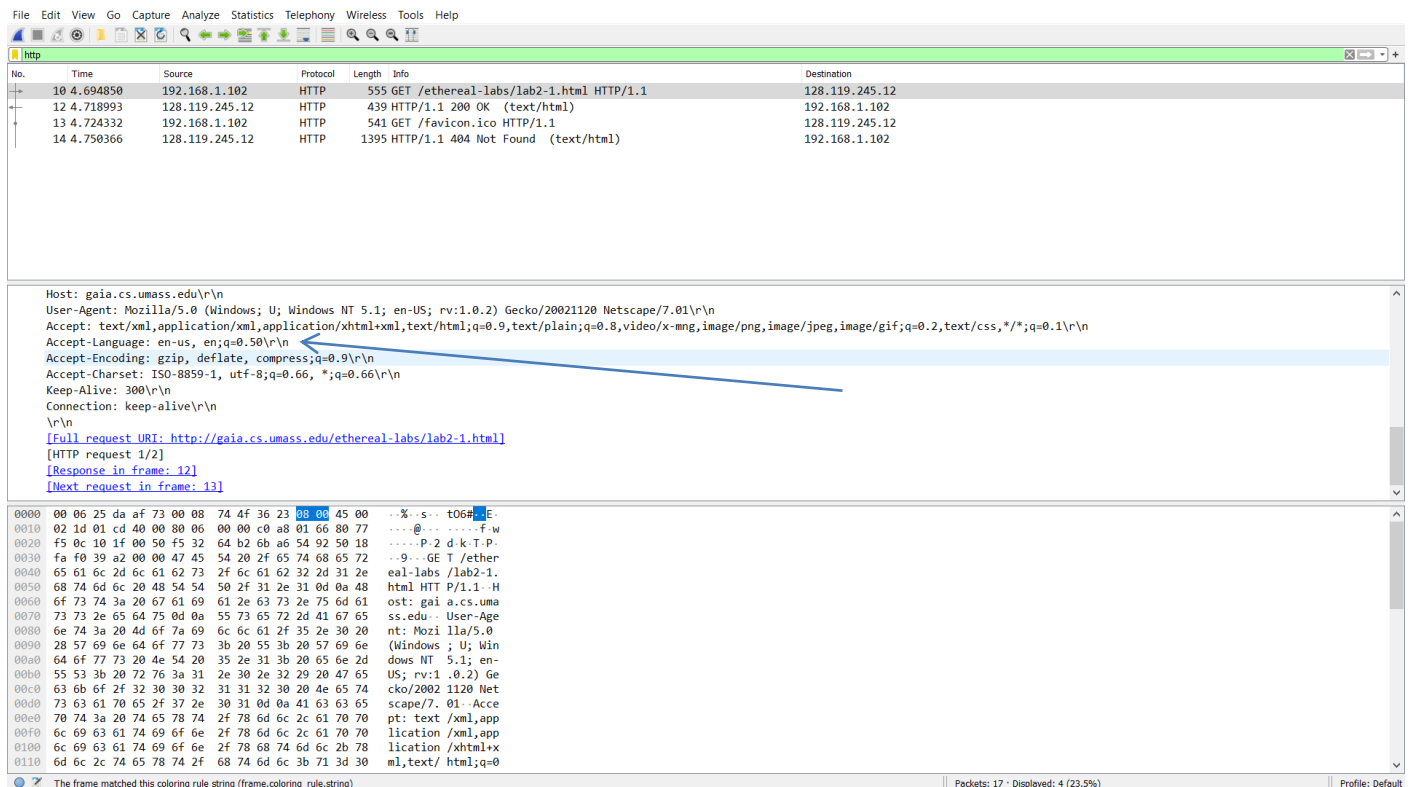
Assignment Name: Lab Assignment-1.

Answering the question:

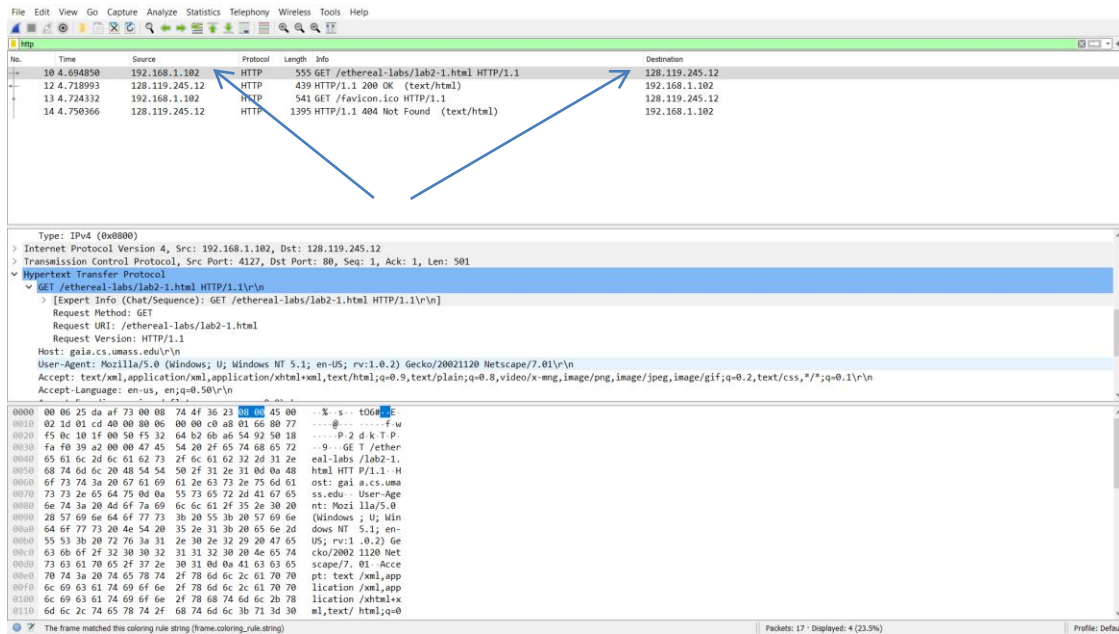
1 : 1.1 and 1.1



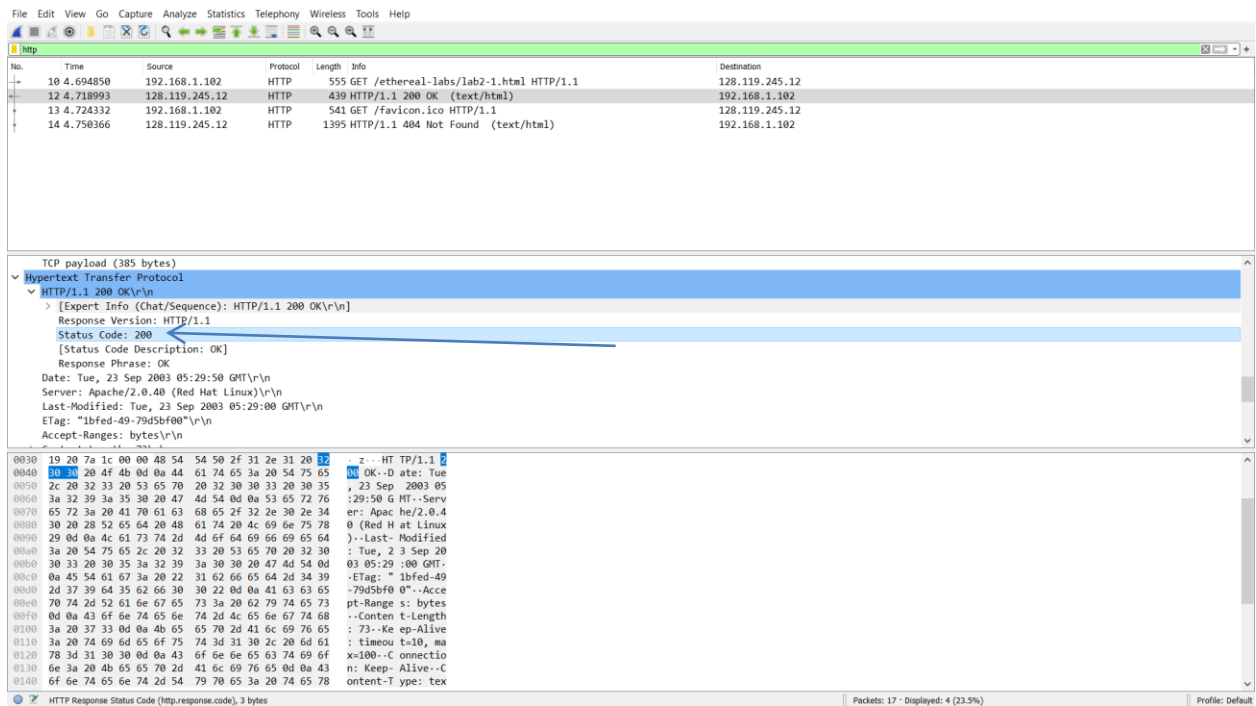
2: language: en-us



3: computer: 192.168.1.102, server: 128.119.245.12



#### 4: status code: 200



#### 5: last modified: tue, 23 sep 2003 05:29:00 GMT

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

Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
Server: Apache/2.0.40 (Red Hat Linux)\r\n
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
ETag: "1bfed-49-79d5bf00"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 73\r\n
Keep-Alive: timeout=10, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=ISO-8859-1\r\n
\r\n

```

0000 00 00 74 4f 36 23 00 06 25 da af 73 00 00 45 00  --106#...%.-s.-E-
0010 01 a9 b6 fa 40 00 37 06 53 c2 80 77 f5 0c c0 a8  --...@-7- S-u....
0020 01 66 00 50 10 1f 6b a6 54 92 f5 32 66 a7 50 18  --f-P-.k. T.-2f-P-
0030 19 20 7a 1c 00 00 48 54 54 50 2f 31 2e 31 20 32  --z...HT TP/1.1.2
0040 30 30 20 4f 4b 00 0a 44 61 74 65 3a 20 54 75 65  00 OK--D ate: Tue
0050 2c 20 32 33 20 53 65 70 20 32 30 30 33 20 30 35  --, 23 Sep 2003 05
0060 3a 32 39 3a 35 30 20 47 4d 54 0d 0a 53 65 72 76  --:29:50 6 MT--Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34  er: Apac he/2.0.4
0080 30 20 28 52 65 64 20 40 61 74 20 4c 69 6e 75 70  0 (Red H at Linux
0090 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64  )--Last- Modified
00a0 3a 20 54 75 65 2c 20 32 33 20 53 65 70 20 32 30  : Tue, 2 3 Sep 20
00b0 30 33 20 30 35 3a 32 39 3a 30 30 20 47 4d 54 0d  03 05:29 :00 GMT-
00c0 0a 45 54 61 67 3a 20 22 31 62 66 65 64 2d 34 39  -ETag: " 1bfed-49
00d0 2d 37 39 64 35 62 66 30 30 22 0d 0a 41 63 63 65  --79d5bf0 0"--Acce
00e0 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73  pt-Range s: bytes
00f0 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68  --Content t-length
0100 3a 20 37 31 0d 0a 4b 65 65 70 2d 41 6c 69 76 65  : 73--Ke ep-Alive
0110 3a 20 74 69 6d 65 6f 75 74 3d 31 30 2c 20 6d 61  : timeou t=10, ma

```

6. byte of content: 73

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

[Status Code Description: OK]
Response Phrase: OK
Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
Server: Apache/2.0.40 (Red Hat Linux)\r\n
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
ETag: "1bfed-49-79d5bf00"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 73\r\n
Keep-Alive: timeout=10, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=ISO-8859-1\r\n
\r\n
[HTTP response 1/2]

```

0000 3a 20 54 75 65 2c 20 32 33 20 53 65 70 20 32 30  : Tue, 2 3 Sep 20
0010 30 33 20 30 35 3a 32 39 3a 30 30 20 47 4d 54 0d  03 05:29 :00 GMT-
0020 0a 45 54 61 67 3a 20 22 31 62 66 65 64 2d 34 39  -ETag: " 1bfed-49
0030 2d 37 39 64 35 62 66 30 30 22 0d 0a 41 63 63 65  --79d5bf0 0"--Acce
0040 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73  pt-Range s: bytes
0050 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68  --Content t-length
0060 3a 20 37 31 0d 0a 4b 65 65 70 2d 41 6c 69 76 65  : 73--Ke ep-Alive
0070 3a 20 74 69 6d 65 6f 75 74 3d 31 30 2c 20 6d 61  : timeou t=10, ma
0080 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f  x=100--C connectio
0090 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43  n: Keep- Alive--C
00a0 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78  tent-T ype: tex
00b0 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d  t/html; charset=
00c0 49 53 4f 2d 38 38 35 39 2d 31 0d 0a 0d 0a 3c 68  ISO-8859 -1....ch
00d0 74 6d 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74  tml> Con gratulat
00e0 69 6f 6e 73 2e 20 59 6f 75 27 76 65 20 64 6f  ions. Y ou've do
00f0 77 6e 6c 6f 61 64 65 64 20 74 68 65 20 66 69 6c  nloaded the fill
0100 65 20 6c 61 62 32 2d 31 2e 68 74 6d 6c 21 0a 3c  e lab2-1 .html! <
0110 2f 68 74 6d 6c 3e 0a

```

7. No.

8. No.

9. Yes. In the section ‘Line-Based Text Data’ that shows what the server sent back to my browser .



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Protocol	Length	Info	Destination
8	2.331268	192.168.1.102	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP/1.1	128.119.245.12
10	2.357982	128.119.245.12	HTTP	739	HTTP/1.1 200 OK (text/html)	192.168.1.102
14	5.517390	192.168.1.102	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP/1.1	128.119.245.12
15	5.540216	128.119.245.12	HTTP	243	HTTP/1.1 304 Not Modified	192.168.1.102

HTTP/1.1 304 Not Modified\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]

Response Version: HTTP/1.1

Status Code: 304

[Status Code Description: Not Modified]

Response Phrase: Not Modified

Date: Tue, 23 Sep 2003 05:35:53 GMT\r\n

Server: Apache/2.0.40 (Red Hat Linux)\r\n

Connection: Keep-Alive\r\n

Keep-Alive: timeout=10, max=99\r\n

ETag: "1bfeef-173-8f4ae900"\r\n

\r\n

[HTTP response 2/2]

0000 00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 00 ...tOG#...%...s...E-  
0010 00 e5 dc 88 40 00 37 06 2e f8 80 77 f5 0c c0 a8 ...:..@.7...w...  
0020 01 66 00 50 10 97 81 6a b6 2e fa 88 05 8c 50 18 ...f.P...j...P  
0030 1f 2e 89 37 00 00 48 54 54 50 2f 31 2e 31 20 33 ...-7..HT TP/1.1  
0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d ...Not Modified-  
0050 0a 44 61 74 65 3a 20 54 75 65 2c 20 32 33 20 53 ...Date: Tue, 23 S  
0060 65 70 20 32 30 30 32 20 30 35 3a 33 35 3a 35 33 ...ep 2003 05:35:53  
0070 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 ...GMT-Se rver: Ap  
0080 61 63 68 65 2f 32 2e 30 2e 34 30 20 28 52 65 64 ...ache/2.0 .40 (Red  
0090 20 48 61 74 20 4c 69 6e 75 78 29 0d 0a 43 6f 6e ...at Lin ux)..Con  
00a0 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c ...nection: Keep-AL  
00b0 69 76 65 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a ...ive-Keep p-Alive  
00c0 20 74 69 6d 65 6f 75 74 3d 31 30 2c 20 6d 61 78 ...timeout =10, max  
00d0 3d 39 39 0d 0a 45 54 61 67 3a 20 22 31 62 66 65 ...=99-.ETa g: "1bfe  
00e0 66 2d 31 37 33 2d 38 66 34 61 65 39 30 30 22 0d ...f-173-8f 4ae900".  
00f0 0a 0d 0a ...

HTTP Response Status Code (http.response.code), 3 bytes

Packets: 20 - Displayed: 4 (20.0%)

Profile: Default

## 12. 1, packet number: 8

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Protocol	Length	Info	Destination
8	2003-09-23 11:36:59.501408	192.168.1.102	HTTP	555	GET /ethereal-labs/lab2-3.html HTTP/1.1	128.119.245.12
14	2003-09-23 11:36:59.558596	128.119.245.12	HTTP	490	HTTP/1.1 200 OK (text/html)	192.168.1.102

Frame 8: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)

Ethernet II, Src: Dell\_4f:36:23 (00:08:74:4f:36:23), Dst: Linksys\_6d:af:73 (00:06:25:da:af:73)

Destination: Linksys\_6d:af:73 (00:06:25:da:af:73)

Source: Dell\_4f:36:23 (00:08:74:4f:36:23)

Type: IPv4 (0x0000)

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

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 541

Identification: 0x0284 (644)

Flags: 0x4000, Don't fragment

...0 0000 0000 0000 = Fragment offset: 0

0000 00 06 25 da af 73 08 00 45 00 ...s...tOG#...E-  
0010 02 1d 02 84 40 00 00 0c 00 00 c0 a8 01 66 80 77 ...@.....Fw  
0020 15 0c 10 b0 00 50 fb 98 de ea 85 b2 aa 64 50 18 .....P.....dP  
0030 fa f0 39 a2 00 00 47 45 54 20 2f 65 74 68 65 72 ...-GE T /ether  
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: Mozil lla/s.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 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 6d 6c 2c 2b 78 ...lication /xml+xs  
0110 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 71 3d 30 ...ml,text/ html;q=0

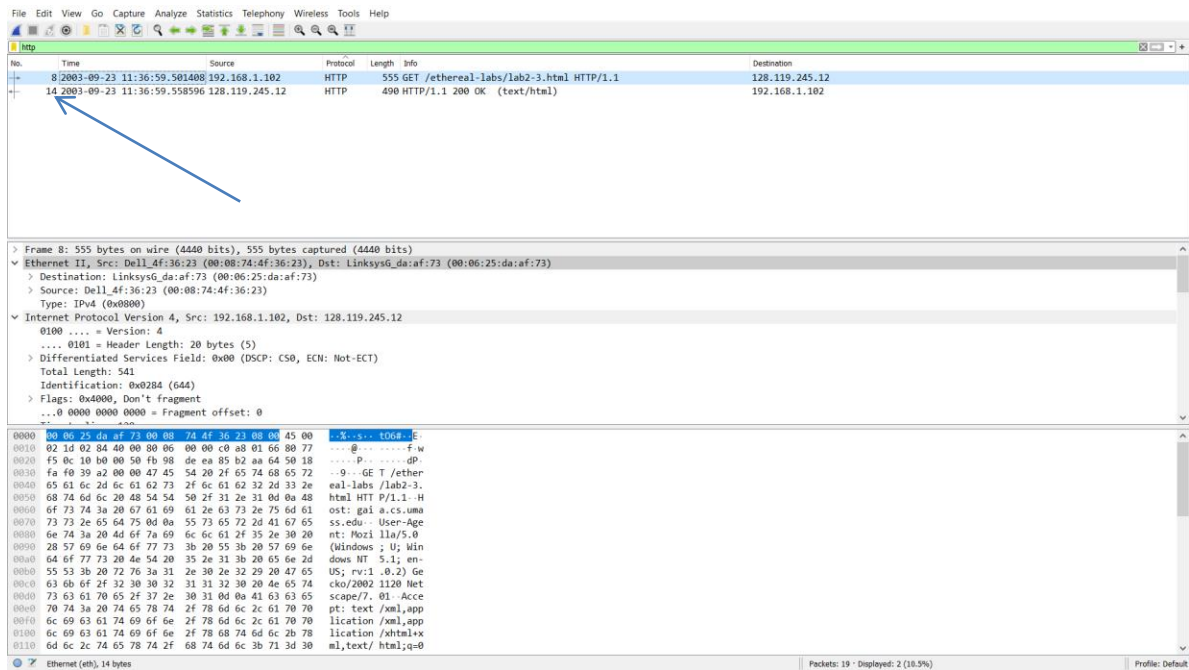
Ethernet (eth), 14 bytes

Packets: 19 - Displayed: 2 (10.5%)

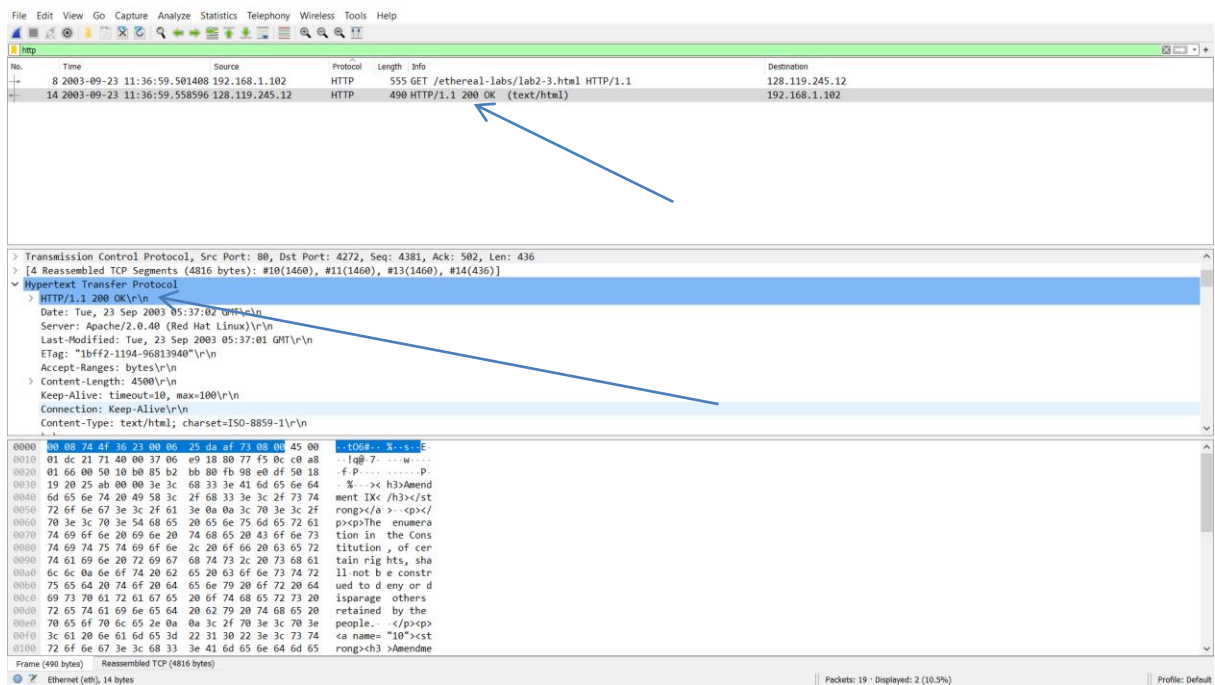
Profile: Default

## 13. packet number: 14





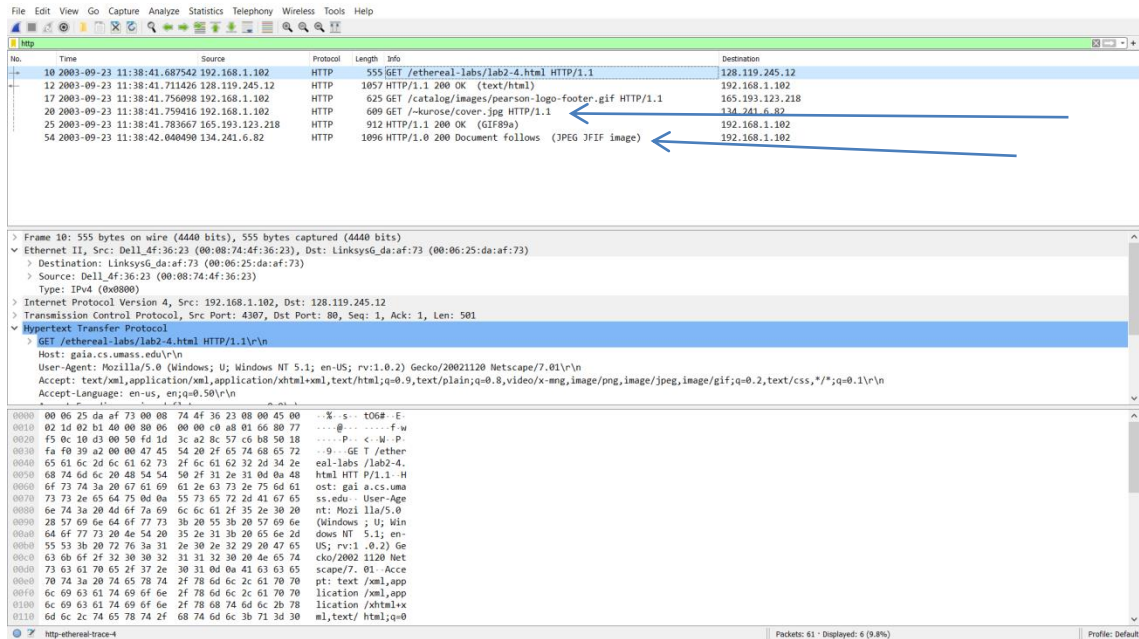
## 14. status code: 200



## 15. 4 TCP segments.



17. The browser downloaded the two images in serially 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.



The screenshot shows a Wireshark packet capture of an HTTP session. The packet list pane at the top shows several HTTP requests. Two specific requests are highlighted with blue arrows pointing to the packet details pane below. The first arrow points to packet 10, which is a GET request for /ethereal-labs/lab2-4.html. The second arrow points to packet 25, which is a GET request for /kurose/cover.jpg. The packet details pane for packet 25 shows the Hypertext Transfer Protocol section, indicating a 200 OK status and a Content-Type of image/jpeg.

No.	Time	Source	Protocol	Length	Info	Destination
10	2003-09-23 11:38:41.687542	192.168.1.102	HTTP	555	GET /ethereal-labs/lab2-4.html HTTP/1.1	128.119.245.12
12	2003-09-23 11:38:41.711426	128.119.245.12	HTTP	1057	HTTP/1.1 200 OK (text/html)	192.168.1.102
17	2003-09-23 11:38:41.756098	192.168.1.102	HTTP	625	GET /catalog/images/pearson-logo-footer.gif HTTP/1.1	165.193.123.218
20	2003-09-23 11:38:41.759416	192.168.1.102	HTTP	609	GET /kurose/cover.jpg HTTP/1.1	134.241.6.82
25	2003-09-23 11:38:41.783667	165.193.123.218	HTTP	912	HTTP/1.1 200 OK (GIF89a)	192.168.1.102
54	2003-09-23 11:38:42.040490	134.241.6.82	HTTP	1096	HTTP/1.0 200 Document follows (JPEG JFIF image)	192.168.1.102

Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits) on Ethernet II, Src: Dell\_Af:36:23 (00:08:74:af:36:23), Dst: Linksys6\_da:af:73 (00:06:25:da:af:73)

Ethernet II, Src: Dell\_Af:36:23 (00:08:74:af:36:23), Dst: Linksys6\_da:af:73 (00:06:25:da:af:73)

Type: IPv4 (0x0000)

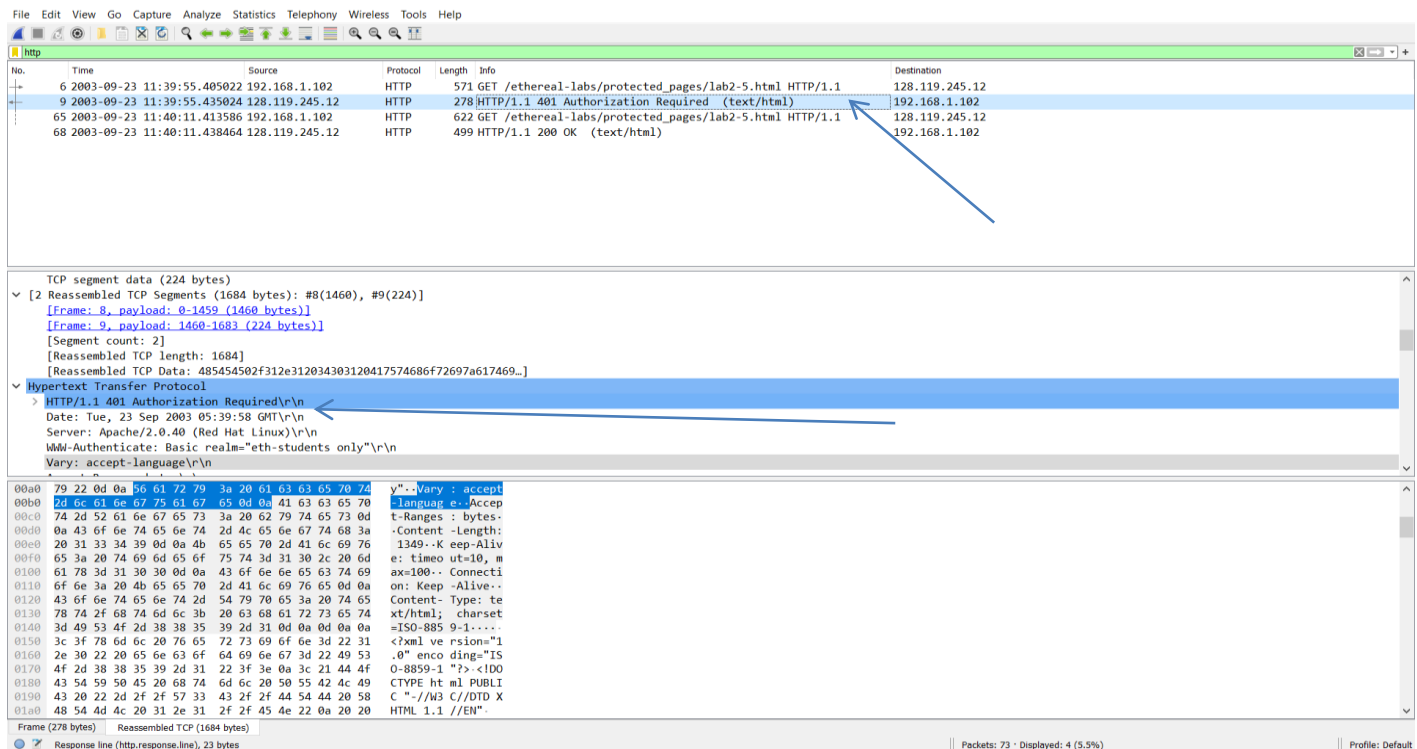
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 4307, Dst Port: 80, Seq: 1, Ack: 1, Len: 501

Hypertext Transfer Protocol

GET /ethereal-labs/lab2-4.html HTTP/1.1\r\n\r\nHost: gaia.cs.umass.edu\r\nUser-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\nAccept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,css/\*;q=0.1\r\nAccept-Language: en-us,en;q=0.50\r\n\r\n

18. status code: 401, phrase: "Authentication Required"



The screenshot shows a Wireshark packet capture of an HTTP session. The packet list pane at the top shows several HTTP requests. A specific request is highlighted with a blue arrow pointing to the packet details pane below. The arrow points to packet 6, which is a GET request for /ethereal-labs/protected\_pages/lab2-5.html. The packet details pane for packet 6 shows the Hypertext Transfer Protocol section, indicating a 401 Authorization Required status and a Content-Type of text/html.

No.	Time	Source	Protocol	Length	Info	Destination
6	2003-09-23 11:39:55.405022	192.168.1.102	HTTP	571	GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1	128.119.245.12
9	2003-09-23 11:39:55.435024	128.119.245.12	HTTP	278	HTTP/1.1 401 Authorization Required (text/html)	192.168.1.102
65	2003-09-23 11:40:11.413586	192.168.1.102	HTTP	622	GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1	128.119.245.12
68	2003-09-23 11:40:11.438464	128.119.245.12	HTTP	499	HTTP/1.1 200 OK (text/html)	192.168.1.102

TCP segment data (224 bytes)

[2 Reassembled TCP Segments (1684 bytes): #8(1460), #9(224)]

[Frame: 8, payload: 0-1459 (1460 bytes)]

[Frame: 9, payload: 1460-1683 (224 bytes)]

[Segment count: 2]

[Reassembled TCP length: 1684]

[Reassembled TCP Data: 485454502f312e312034303120417574686f72697a617469...]

Hypertext Transfer Protocol

HTTP/1.1 401 Authorization Required\r\n\r\nDate: Tue, 23 Sep 2003 05:39:58 GMT\r\nServer: Apache/2.0.40 (Red Hat Linux)\r\nWWW-Authenticate: Basic realm="eth-students only"\r\n\r\nVary: accept-language\r\n\r\n



## 19. new field: authorization field.

The image shows a Wireshark packet capture of an HTTP transaction. The top pane displays a list of packets. Packet 65 is selected, showing an HTTP GET request for `/etherreal-labs/protected_pages/lab2-5.html` from `192.168.1.102` to `128.119.245.12`. Packet 68 is the corresponding HTTP 200 OK response. The middle pane shows the details of the selected packet (65), which is an HTTP GET request. The 'Authorization' field is highlighted in blue, and a blue arrow points to it from the right. The 'Authorization' field contains the value `Basic ZXRoLXN0bWUuR1bnRzOm5ldkdvcmtz`. The bottom pane shows the raw bytes of the packet, with the 'Authorization' field highlighted in blue.

Host: gaia.cs.umass.edu\r\n  
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n  
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,\*/\*;q=0.1\r\n  
Accept-Language: en-us,en;q=0.50\r\n  
Accept-Encoding: gzip, deflate, compress;q=0.9\r\n  
Accept-Charset: ISO-8859-1, utf-8;q=0.66,\*;q=0.66\r\n  
Keep-Alive: 300\r\n  
Connection: keep-alive\r\n  
Authorization: Basic ZXRoLXN0bWUuR1bnRzOm5ldkdvcmtz\r\n  
[Full request URI: http://gaia.cs.umass.edu/etherreal-labs/protected\_pages/lab2-5.html]  
[HTTP request 1/1]  
[Response in frame 68]

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;text/css,\*  
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-Encod 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-Chars 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 11 73 74 63 6f 72 65 p-alive. Autho  
0240 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 5a 58 ation: Basic ZX  
0250 62 6f 4c 58 4e 30 64 57 52 6c 62 6e 52 7a 4f 6d RoLXN0bWUuR1bnRzOm  
0260 35 6c 64 48 64 76 63 6d 74 7a 0d 0a 0d 0a 5ldkdvcmtz....

HTTP Authorization header (http.authorization), 51 bytes | Packets: 73 - Displayed: 4 (5.5%) | Profile: Default