

COMPUTER NETWORKS LAB2

Achintya Bhavaraju

SE20UARI020

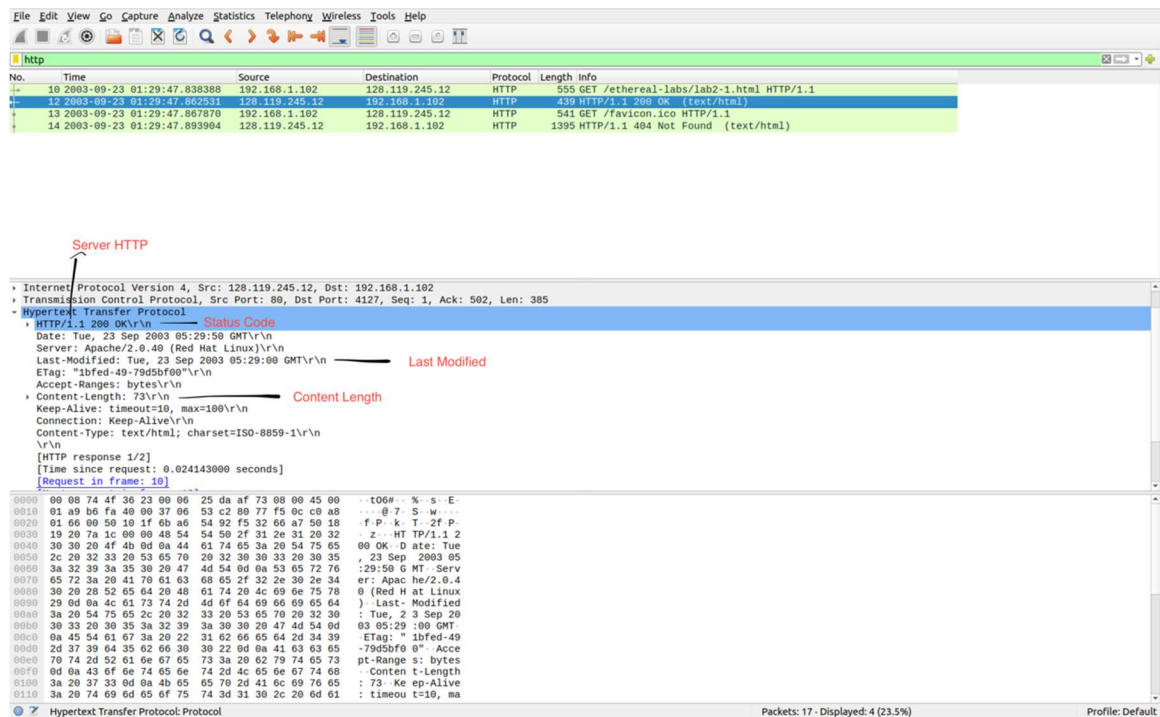
1. The Basic HTTP GET/response interaction

The image shows a Wireshark packet capture titled "http-ethereal-trace-1". The top pane displays a list of captured packets. The second pane shows the details of the selected packet (No. 12), which is an HTTP GET request. The third pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
10	2003-09-23 01:29:47.830388	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
12	2003-09-23 01:29:47.862531	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	2003-09-23 01:29:47.867870	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	2003-09-23 01:29:47.893904	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) on interface eth0
Ethernet II, Src: Dell 4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG 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: 4127, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
Hypertext Transfer Protocol
GET /ethereal-labs/lab2-1.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,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1
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=0.60
Keep-Alive: 300
Connection: keep-alive
Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-1.html
[HTTP request 1/2]

0000 00 06 25 da af 73 00 08 74 4f 36 23 08 00 45 00 ... s... t06# E-
0010 02 1d 01 cd 40 00 00 06 00 00 c0 a8 01 66 00 77 ... @... f.w
0020 f5 0c 10 1f 00 50 f5 32 64 b2 0b a6 54 92 50 18 ... P 2 d k T 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 0c 61 62 73 2f 6c 61 62 32 2d 31 2e eal-labs /lab2-1.
0050 68 74 6d 6c 28 48 54 54 50 2f 31 2e 31 6d 0a 48 html HT P/1.1 H
0060 6f 73 74 3a 20 07 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 la/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 05 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 61 70 70 lication /html+x
0110 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 71 3d 30 ml, text/ html;q=0



Q1) My browser on HTTP/1.1 and server is also running HTTP/1.1

Q2) The browser can accept en-US

Q3) IP Address of my computer 128.119.245.12

IP Address of gaia Server 172.16.98.128

Q4) Status Code – 200 :OK (passed)

Q5) Last Modified – Tue, 23 September 2003 05:29:00 GMT (old document)

Q6) 73 Bytes

Q7) No headers present

2. The HTTP CONDITIONAL GET/response interaction

The image shows a Wireshark capture of an HTTP interaction. The top pane displays a list of packets, with packet 8 selected. The middle pane shows the details of the selected packet, which is an HTTP GET request for /ethereal-labs/lab2-2.html. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
8	2003-09-23 01:35:47.812260	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP/1.1
10	2003-09-23 01:35:47.838894	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	2003-09-23 01:35:50.999382	192.168.1.102	128.119.245.12	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP/1.1
15	2003-09-23 01:35:51.021208	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

Packet 8 Details:

- Hypertext Transfer Protocol:**
 - 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,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1
 - 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=0.60
 - Keep-Alive: 300
 - Connection: keep-alive
 - Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html
 - HTTP request 1/2

Raw Data:

```
0000 00 06 25 da af 73 00 08 74 4f 36 23 08 00 45 00  - %..s...t06#..E-
0010 02 1d 02 5a 40 00 00 06 00 00 c0 a8 01 06 80 77  - ...20...f.w
0020 f5 0c 10 97 00 50 fa 09 01 31 81 6a b3 01 50 10  - ...P...1.j..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 0c 01 02 73 2f 6c 61 62 32 2d 32 2e  eal-labs /lab2-2.
0050 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 40  html HTTP 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 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 29 47 65  US; rv:1.0.2) Ge
00c0 63 0b 0f 2f 32 30 30 32 31 31 32 30 29 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 01 70 70  pt: text /xml,app
00f0 6c 09 63 61 74 69 6f 6e 2f 78 6d 6c 2c 61 70 70  lication /xml,app
0100 6c 09 63 61 74 69 6f 6e 2f 78 6d 74 6d 6c 2b 78  lication /html,x
0110 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 71 3d 30  ml;text/ html;q=0
```

http-ethereal-trace-2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

h http

No.	Time	Source	Destination	Protocol	Length	Info
8	2003-09-23 01:35:47.812260	192.168.1.102	128.119.245.12	HTTP	555	GET /etherreal-labs/lab2-2.html HTTP/1.1
10	2003-09-23 01:35:47.838894	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	2003-09-23 01:35:50.998382	192.168.1.102	128.119.245.12	HTTP	668	GET /etherreal-labs/lab2-2.html HTTP/1.1
15	2003-09-23 01:35:51.021208	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

[Time since request: 0.026634000 seconds]
[Request in frame: 8]
[Next request in frame: 14]
[Next response in frame: 15]
[Request URI: http://gaia.cs.umass.edu/etherreal-labs/lab2-2.html]
File Data: 371 bytes

Line-based text data: text/html (10 lines)

Line-based text data

0000 00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 00 ... t06#... % s E-
0010 02 d5 dc 87 40 00 37 06 2d 09 80 77 f5 0c c0 a8 ... 0 7: ... w...
0020 01 66 00 50 10 97 81 6a b3 81 fa 88 03 26 50 18 ... f P... j ... &P
0030 19 20 58 95 00 00 48 54 54 50 2f 31 2e 31 20 32 ... X ... HT TP/1.1 2
0040 30 30 20 4f 4b 0d 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 33 35 3a 35 30 20 47 4d 54 0d 0a 53 65 72 76 ... :35:50 G MT: Serv
0070 65 72 3a 20 41 70 61 63 68 05 2f 32 20 2e 34 ... er: Apac he/2.0.4
0080 30 20 28 52 65 64 20 48 61 74 20 4c 09 6e 75 78 ... 0 (Red H at Linux
0090 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 09 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 33 35 3a 30 20 47 4d 54 0d ... 03 05:35 :00 GMT
00c0 0a 45 54 61 67 3a 20 22 31 62 66 65 66 2d 31 37 ... -Etag: " 1bfef-17
00d0 33 2d 38 66 34 61 65 39 30 30 22 0d 0a 41 63 63 ... 3-8f4ae9 00"-Acc
00e0 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 ... ept-Rang es: byte
00f0 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 ... s Conte nt-Lengt
0100 68 3a 20 33 37 31 0d 0a 4b 65 65 70 2d 41 6c 69 ... h: 371... Keep-All
0110 76 65 3a 20 74 69 6d 65 6f 75 74 3d 31 30 2c 20 ... ve: time out=10,

Hypertext Transfer Protocol: Protocol

Packets: 20 · Displayed: 4 (20.0%)

Profile: Default

http-ethereal-trace-2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

h http

No.	Time	Source	Destination	Protocol	Length	Info
8	2003-09-23 01:35:47.812260	192.168.1.102	128.119.245.12	HTTP	555	GET /etherreal-labs/lab2-2.html HTTP/1.1
10	2003-09-23 01:35:47.838894	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	2003-09-23 01:35:50.998382	192.168.1.102	128.119.245.12	HTTP	668	GET /etherreal-labs/lab2-2.html HTTP/1.1
15	2003-09-23 01:35:51.021208	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

Frame 14: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits)
Ethernet II, Src: Dell 4f:36:23 (00:08:74:4f:36:23), Dst: Linksys G, 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: 4247, Dst Port: 80, Seq: 502, Ack: 686, Len: 614

Hypertext Transfer Protocol

GET /etherreal-labs/lab2-2.html HTTP/1.1\r\n
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=0.60\r\n
Keep-Alive: 300\r\n
Connection: keep-alive\r\n
If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n
If-None-Match: "1bfef-173-8f4ae900"\r\n
Cache-Control: max-age=0\r\n

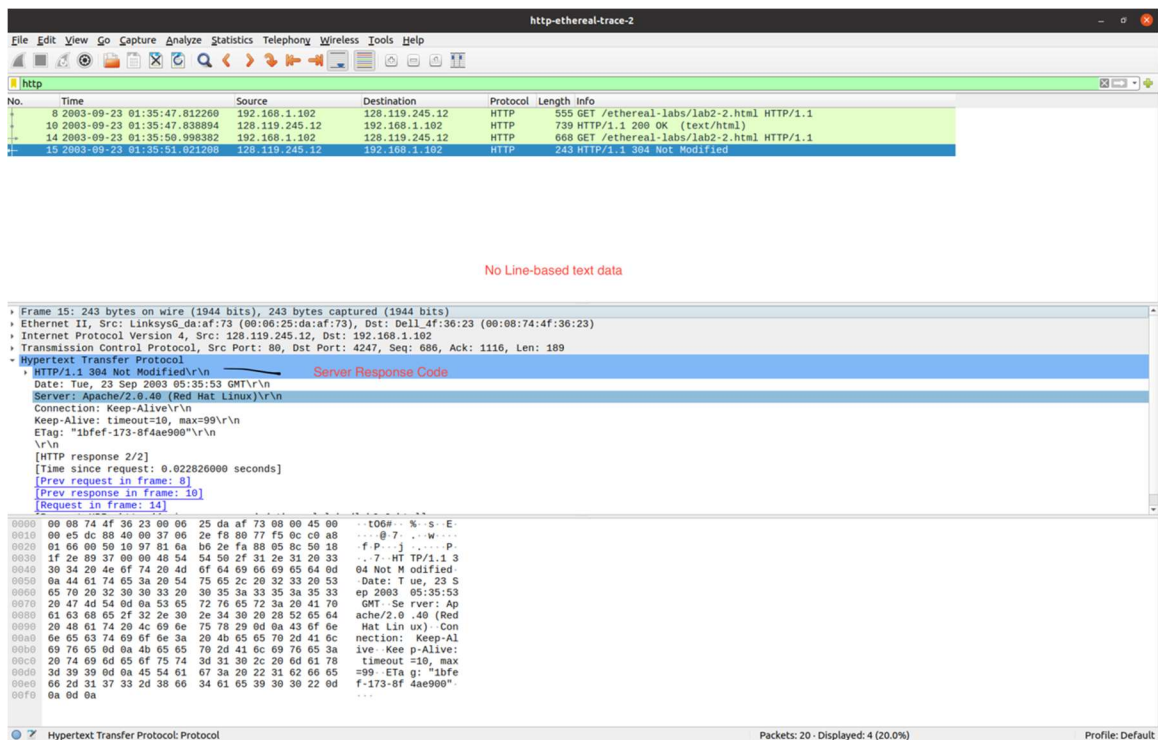
IF-MODIFIED-SINCE

0000 00 06 25 da af 73 00 08 74 4f 36 23 00 00 45 00 ... % s... t06#... E-
0010 02 0e 02 61 40 00 00 06 00 00 c0 a0 01 66 00 77 aB f w
0020 f5 0c 10 97 00 50 fa 88 03 26 81 6a b6 2e 50 18 P... & j . P
0030 f8 43 3a 13 00 00 47 45 54 20 2f 65 74 68 05 72 ... C:... GE T /ether
0040 65 61 6c 2d 0c 01 62 73 2f 6c 01 62 32 2d 32 2e ... eal-labs /lab2-2.
0050 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 4b ... 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 74 69 6c 6c 61 2f 35 2e 30 20 ... nt: Mozil la/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 0b 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,x
0100 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 ... lication /html;x
0110 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 71 3d 30 ... ml,text/ html;q=0

Hypertext Transfer Protocol: Protocol

Packets: 20 · Displayed: 4 (20.0%)

Profile: Default



Q8) No I do not see and IF-MODIFIED-SINCE line

Q9) Yes and I can tell because of the Line-based text data field

Q10) Yes, I see an IF-MODIFIED-SINCE line in the second HTTP GET.
IF-MODIFIED-SINCE: Tue, 23 Sep 2003 05:35:00 GMT

Q11) Status Code in 2nd HTTP GET – 304 Not Modified

No, the server did not return the contents of the file since it already exists in the cache

3. Retrieving Long Documents

The screenshot shows a Wireshark packet capture of an HTTP GET request. The packet list pane at the top shows two packets: packet 8 (555 bytes) and packet 14 (490 bytes). Packet 14 is selected, and its details pane shows the Hypertext Transfer Protocol section. A red arrow points to the 'Packet Number' column header. The packet bytes pane shows the raw data of the HTTP request.

No.	Time	Source	Destination	Protocol	Length	Info
8	2003-09-23 01:36:59.501408	192.168.1.102	128.119.245.12	HTTP	555	GET /etheral-labs/lab2-3.html HTTP/1.1
14	2003-09-23 01:36:59.558596	128.119.245.12	192.168.1.102	HTTP	490	HTTP/1.1 200 OK (text/html)

1 HTTP GET

Packet Number

Frame 8: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
Ethernet II, Src: Dell_4f:36:23 (08:00:74:4f:36:23), Dst: Linksys_d8: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: 4272, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
Hypertext Transfer Protocol

0000 00 06 25 da af 73 00 08 74 4f 36 23 08 00 45 00 -- %..s..t06..E..
0010 02 1d 02 84 40 00 00 00 00 00 c0 a8 01 60 80 77 --- @... ..f.w
0020 f5 9c 19 b0 00 50 fb 98 de e0 65 b2 aa 64 50 18 --- P... ..dP
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 33 2e eal-labs /lab2-3.
0050 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 6d 0a 40 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.c.s.uma
0070 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 05 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 53 3b 20 72 76 3a 31 2e 30 2e 32 29 20 47 65 US; rv:1.0.2) Ge
00c0 63 0b 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 74 6d 6c 2b 78 lication /html+
0110 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 71 3d 30 ml,text/ html;q=0

Hypertext Transfer Protocol: Protocol

Packets: 19 - Displayed: 2 (10.5%)

Profile: Default

The screenshot shows a Wireshark packet capture of an HTTP 200 OK response. The packet list pane at the top shows two packets: packet 8 (555 bytes) and packet 14 (490 bytes). Packet 14 is selected, and its details pane shows the Hypertext Transfer Protocol section. A red arrow points to the 'Packet Number' column header. The packet bytes pane shows the raw data of the HTTP response.

No.	Time	Source	Destination	Protocol	Length	Info
8	2003-09-23 01:36:59.501408	192.168.1.102	128.119.245.12	HTTP	555	GET /etheral-labs/lab2-3.html HTTP/1.1
14	2003-09-23 01:36:59.558596	128.119.245.12	192.168.1.102	HTTP	490	HTTP/1.1 200 OK (text/html)

Packet Number

Status Code

Frame 14: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits)
Ethernet II, Src: Linksys_d8:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (08:00:74:4f: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 (90 lines)

Number of TCP Segments

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 -!q@ 7...W...
0020 01 66 00 50 10 b0 85 b2 bb 08 fb 98 e0 df 50 18 -f P... ..P
0030 19 29 25 ab 00 00 3e 3c 68 33 3e 41 6d 65 6e 64 %..>c h3>Amend
0040 6d 65 6e 74 20 49 58 3c 2f 68 33 3e 3c 2f 73 74 ment IXc /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>>pThe enuera
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 6e 20 63 65 72 titution , of cer
0090 74 61 69 6e 20 72 69 67 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 deny 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 6e 64 20 62 79 20 74 68 65 20 retained by the
00e0 70 65 6f 70 6c 6e 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 <st

Frame (490 bytes) Reassembled TCP (4816 bytes)

Hypertext Transfer Protocol: Protocol

Packets: 19 - Displayed: 2 (10.5%)

Profile: Default

Q12) The browser sent only 1 HTTP GET message

The packet number – **8**

Q13) The packet number **14** which contains the status code and phrase associated with the response to the HTTP GET request

Q14) Status code and phrase – 200 OK

Q15) The data was sent in 4 TCP segments

4. HTML Documents with Embedded Objects

The image shows a Wireshark capture of an HTTP GET request and response. The packet list on the left shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
10	2003-09-23 01:38:41.687542	192.168.1.102	128.119.245.12	HTTP	555	GET /etherlab-labs/lab2-4.html HTTP/1.1
12	2003-09-23 01:38:41.711426	128.119.245.12	192.168.1.102	HTTP	1057	HTTP/1.1 200 OK (text/html)
17	2003-09-23 01:38:41.750999	192.168.1.102	165.193.123.218	HTTP	625	GET /catalog/images/objectron/logo-feather.gif HTTP/1.1
20	2003-09-23 01:38:41.759416	192.168.1.102	134.241.6.82	HTTP	669	GET /kurose/cover.jpg HTTP/1.1
25	2003-09-23 01:38:41.783667	165.193.123.218	192.168.1.102	HTTP	912	HTTP/1.1 200 OK (GIF89a)
54	2003-09-23 01:38:42.048490	134.241.6.82	192.168.1.102	HTTP	1096	HTTP/1.0 200 Document Follows (JPEG JFIF image)

Annotations on the packet list:

- Initial page IP: points to packet 10 (192.168.1.102)
- Cover IP: points to packet 54 (134.241.6.82)
- Logo IP: points to packet 17 (165.193.123.218)
- 2nd HTTP GET message sent before receiving reply for 1st one: points to packet 20 (134.241.6.82)

The packet details pane shows the following information for the selected packet (10):

- Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
- Ethernet II, Src: Dell_4f:36:23 (08:00:74:4f:36:23), Dst: Linksys6_da:af:73 (08:00:25:da:af:73)
- 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: 581
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the HTTP GET request:

```
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 00 06 00 00 c0 a8 01 66 80 77  ...@...f.w
0020 f5 0c 10 d3 00 50 fd 1d 3c a2 8c 57 c6 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 69 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 6a 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 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 61 70 70  lication /html,x
0110 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 71 3d 30  ml, text/ html;q=0
```

Q16) The browser sent 3 HTTP GET messages

Initial Page address: 128.119.245.12

Pearson Logo: 165.193.123.218

Cover : 134.241.6.82

Q17) The downloads occurred in parallel. The 2nd HTTP GET messages was sent before the reply for the 1st image was received

5. HTTP Authentication

The screenshot displays a Wireshark capture of an HTTP transaction. The packet list at the top shows three HTTP GET requests to the URL `http://gaia.cs.umass.edu/etherlab/protected_pages/lab2-5.html`. The first request (No. 6) is from 192.168.1.102 to 128.119.245.12. The second request (No. 9) is from 128.119.245.12 to 192.168.1.102. The third request (No. 65) is from 128.119.245.12 to 192.168.1.102. The packet details pane for the selected packet (No. 6) shows the full request structure, including the Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Accept-Charset, Keep-Alive, and Connection headers. The packet bytes pane shows the raw data of the request, including the GET method, the URL, and the headers.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
6	2003-09-23 01:39:55.405022	192.168.1.102	128.119.245.12	HTTP	571	GET /etherlab/protected_pages/lab2-5.html HTTP/1.1
9	2003-09-23 01:39:55.435024	128.119.245.12	192.168.1.102	HTTP	278	HTTP/1.1 401 Authorization Required (text/html)
65	2003-09-23 01:40:11.413586	192.168.1.102	128.119.245.12	HTTP	622	GET /etherlab/protected_pages/lab2-5.html HTTP/1.1
68	2003-09-23 01:40:11.438464	128.119.245.12	192.168.1.102	HTTP	499	HTTP/1.1 200 OK (text/html)

Packet Details (No. 6):

- GET /etherlab/protected_pages/lab2-5.html HTTP/1.1\r\n
- 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=0.56\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
- \r\n
- [Full request URI: http://gaia.cs.umass.edu/etherlab/protected_pages/lab2-5.html]
- [HTTP request 1/1]

Packet Bytes (No. 6):

```
0000 00 06 25 da af 73 00 08 74 4f 36 23 08 00 45 00  --X..s...tO&..E..
0010 02 2d 03 04 00 00 00 06 00 00 c9 a8 01 66 00 77  --...@...f.w
0020 f5 0c 10 ef 00 50 fe 37 f3 ea 91 47 1b 74 50 18  --....P.7...G.tP.
0030 fa f0 39 b2 00 00 47 45 54 20 2f 65 74 08 65 72  --9...GE T /ether
0040 65 61 6c 2d 6c 61 62 73 2f 70 72 6f 74 65 63 74  eal-labs /protect
0050 65 64 5f 70 61 67 65 73 2f 6c 61 62 32 d8 35 2e  ed_pages /lab2-5.
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48  html HT P/1.1-H
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61  ost: gaia.cs.uma
0080 73 73 2e 65 64 75 6d 6a 55 73 65 72 2d 41 67 65  ss.edu User-Age
0090 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20  nt: Mozilla/5.0
00a0 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69 6e  (Windows; U; Win
00b0 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e 2d  dows NT 5.1; en-
00c0 55 53 3b 20 72 70 3a 31 2e 30 2a 32 29 20 47 65  US; rv:1.0.2) Ge
00d0 63 6b 6f 2f 32 30 30 32 31 31 32 30 20 4e 65 74  cko/2002 1120 Net
00e0 73 63 61 70 65 2f 37 2e 30 31 0d 0a 41 63 63 65  scape/7.01-Acce
00f0 70 74 3a 20 74 65 70 74 2f 78 6d 6c 2c 61 70 70  pt: text /xml.app
0100 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c 61 70 70  lication /xml.app
0110 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c 61 70 70  lication /xml+</pre>
```


http-ethereal-trace-5						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
6	2003-09-23 01:39:55.405022	192.168.1.102	128.119.245.12	HTTP	571	GET /etherreal-labs/protected_pages/lab2-5.html HTTP/1.1
9	2003-09-23 01:39:55.435024	128.119.245.12	192.168.1.102	HTTP	278	HTTP/1.1 401 Authorization Required (text/html)
69	2003-09-23 01:40:11.438464	128.119.245.12	192.168.1.102	HTTP	459	HTTP/1.1 200 OK (text/html)

<ul style="list-style-type: none"> 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: LinksysG_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 <ul style="list-style-type: none"> GET /etherreal-labs/protected_pages/lab2-5.html HTTP/1.1\r\n 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,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=0.60\r\n Keep-Alive: 300\r\n Connection: keep-alive\r\n Authorization: Basic ZXRoLXN0dWR1bnRzOm5ldHdvcmtz\r\n Full request URI: http://gaia.cs.umass.edu/etherreal-labs/protected_pages/lab2-5.html] 						
0000	00 06 25 da af 73 00 08 74 4f 36 23 08 00 45 00
0010	02 00 03 20 40 00 00 00 00 c0 a0 01 00 00 77
0020	f5 0c 10 f0 00 50 fe 70 10 ea 92 c4 d1 4e 50 18
0030	fa f0 39 e5 00 00 47 45 54 20 2f 05 74 68 05 72
0040	65 61 6c 2d 6c 61 62 73 2f 70 72 6f 74 65 63 74
0050	65 64 5f 70 61 67 05 73 2f 6c 61 62 32 2d 35 2e
0060	68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0070	6f 73 74 3a 20 07 61 69 61 2e 63 73 2e 75 6d 61
0080	73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 05
0090	6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20
00a0	28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69 6e
00b0	64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e 2d
00c0	55 53 3b 20 72 76 3a 31 2e 30 2e 32 29 20 47 65
00d0	63 6b 6f 2f 32 30 30 32 31 31 32 30 20 4e 65 74
00e0	73 63 61 70 65 2f 37 2e 39 31 00 0a 41 63 63 65
00f0	70 74 3a 20 74 65 70 74 2f 78 6d 6c 2c 61 70 70
0100	6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c 61 70 70
0110	6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78

Q18) The servers initial response was 401 Authorization Required

Q19) The new field in the 2nd HTTP GET message is Authorization