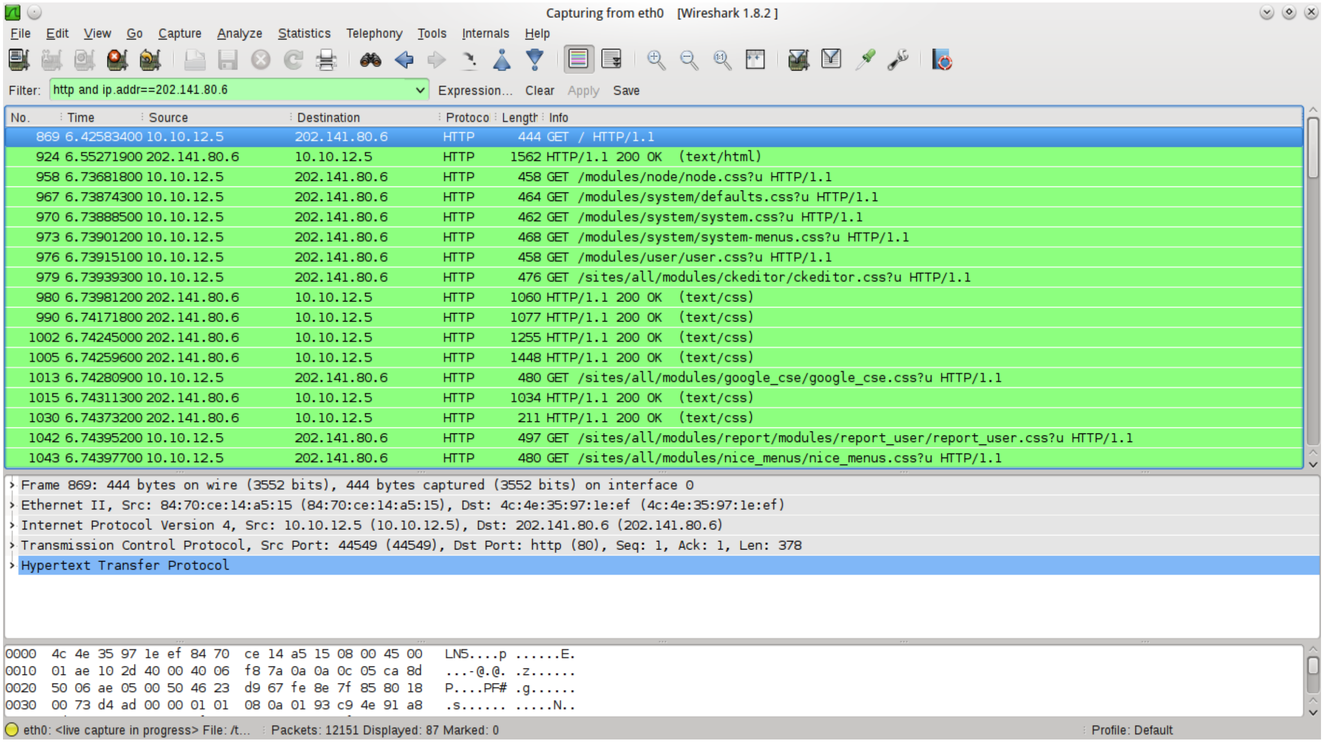
Assignment 4: Packet Capturing Using Wireshark

Simrat Singh Chhabra 11010165

N M Harsha 11010144

Part A : Initial

7. Take a screenshot of this result. How many packets were transmitted from the IITG web server to your client in this.


Capturing from eth0 [Wireshark 1.8.2]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: http and ip.addr==202.141.80.6

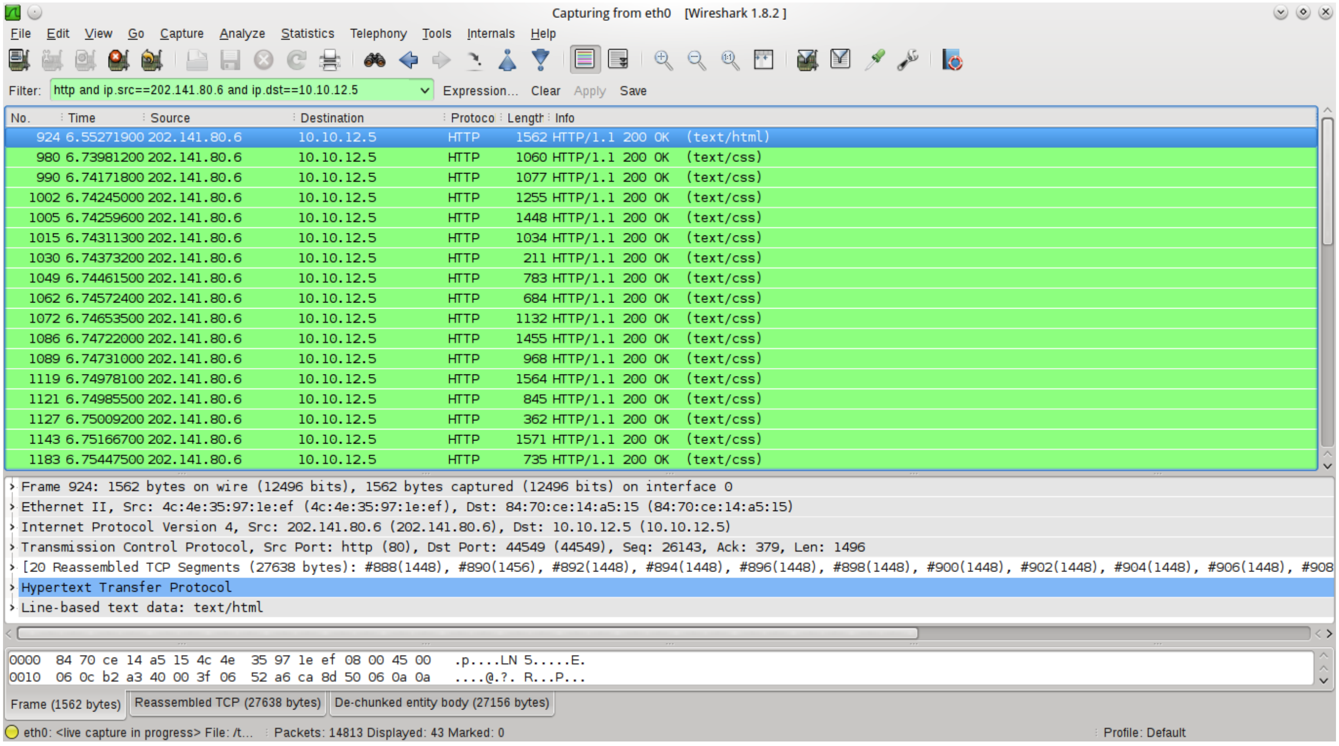
```
No.   Time       Source        Destination   Protoco Length Info
  869 6.42583400 10.10.12.5    202.141.80.6  HTTP     444 GET / HTTP/1.1
  924 6.55271900 202.141.80.6  10.10.12.5    HTTP    1562 HTTP/1.1 200 OK  (text/html)
  958 6.73681800 10.10.12.5    202.141.80.6  HTTP     458 GET /modules/node/node.css?u HTTP/1.1
  967 6.73874300 10.10.12.5    202.141.80.6  HTTP     464 GET /modules/system/defaults.css?u HTTP/1.1
  970 6.73888500 10.10.12.5    202.141.80.6  HTTP     462 GET /modules/system/system.css?u HTTP/1.1
  973 6.73901200 10.10.12.5    202.141.80.6  HTTP     468 GET /modules/system/system-menus.css?u HTTP/1.1
  976 6.73915100 10.10.12.5    202.141.80.6  HTTP     458 GET /modules/user/user.css?u HTTP/1.1
  979 6.73939300 10.10.12.5    202.141.80.6  HTTP     476 GET /sites/all/modules/ckeditor/ckeditor.css?u HTTP/1.1
  980 6.73981200 202.141.80.6  10.10.12.5    HTTP    1060 HTTP/1.1 200 OK  (text/css)
  990 6.74171800 202.141.80.6  10.10.12.5    HTTP    1077 HTTP/1.1 200 OK  (text/css)
 1002 6.74245000 202.141.80.6  10.10.12.5    HTTP    1255 HTTP/1.1 200 OK  (text/css)
 1005 6.74259600 202.141.80.6  10.10.12.5    HTTP    1448 HTTP/1.1 200 OK  (text/css)
 1013 6.74280900 10.10.12.5    202.141.80.6  HTTP     480 GET /sites/all/modules/google_cse/google_cse.css?u HTTP/1.1
 1015 6.74311300 202.141.80.6  10.10.12.5    HTTP    1034 HTTP/1.1 200 OK  (text/css)
 1030 6.74373200 202.141.80.6  10.10.12.5    HTTP     211 HTTP/1.1 200 OK  (text/css)
 1042 6.74395200 10.10.12.5    202.141.80.6  HTTP     497 GET /sites/all/modules/report/modules/report_user/report_user.css?u HTTP/1.1
 1043 6.74397700 10.10.12.5    202.141.80.6  HTTP     480 GET /sites/all/modules/nice_menus/nice_menus.css?u HTTP/1.1
```

```
> Frame 869: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface 0
> Ethernet II, Src: 84:70:ce:14:a5:15 (84:70:ce:14:a5:15), Dst: 4c:4e:35:97:1e:ef (4c:4e:35:97:1e:ef)
> Internet Protocol Version 4, Src: 10.10.12.5 (10.10.12.5), Dst: 202.141.80.6 (202.141.80.6)
> Transmission Control Protocol, Src Port: 44549 (44549), Dst Port: http (80), Seq: 1, Ack: 1, Len: 378
> Hypertext Transfer Protocol
```

```
0000  4c 4e 35 97 1e ef 84 70  ce 14 a5 15 08 00 45 00   LN5....p ......E.
0010  01 ae 10 2d 40 00 40 06  f8 7a 0a 0a 0c 05 ca 8d   ...-@.@. .z......
0020  50 06 ae 05 00 50 46 23  d9 67 fe 8e 7f 85 80 18   P....PF# .g......
0030  00 73 d4 ad 00 00 01 01  08 0a 01 93 c9 4e 91 a8   .s...... .....N..
```

eth0: <live capture in progress> File: /t... Packets: 12151 Displayed: 87 Marked: 0 Profile: Default

Packets belonging to the http session between host and IITG web server


Capturing from eth0   [Wireshark 1.8.2]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

```
Filter: http and ip.src==202.141.80.6 and ip.dst==10.10.12.5

No.   Time       Source        Destination  Protoco Length Info
  924 6.55271900 202.141.80.6  10.10.12.5   HTTP    1562 HTTP/1.1 200 OK  (text/html)
  980 6.73981200 202.141.80.6  10.10.12.5   HTTP    1060 HTTP/1.1 200 OK  (text/css)
  990 6.74171800 202.141.80.6  10.10.12.5   HTTP    1077 HTTP/1.1 200 OK  (text/css)
 1002 6.74245000 202.141.80.6  10.10.12.5   HTTP    1255 HTTP/1.1 200 OK  (text/css)
 1005 6.74259600 202.141.80.6  10.10.12.5   HTTP    1448 HTTP/1.1 200 OK  (text/css)
 1015 6.74311300 202.141.80.6  10.10.12.5   HTTP    1034 HTTP/1.1 200 OK  (text/css)
 1030 6.74373200 202.141.80.6  10.10.12.5   HTTP     211 HTTP/1.1 200 OK  (text/css)
 1049 6.74461500 202.141.80.6  10.10.12.5   HTTP     783 HTTP/1.1 200 OK  (text/css)
 1062 6.74572400 202.141.80.6  10.10.12.5   HTTP     684 HTTP/1.1 200 OK  (text/css)
 1072 6.74653500 202.141.80.6  10.10.12.5   HTTP    1132 HTTP/1.1 200 OK  (text/css)
 1086 6.74722000 202.141.80.6  10.10.12.5   HTTP    1455 HTTP/1.1 200 OK  (text/css)
 1089 6.74731000 202.141.80.6  10.10.12.5   HTTP     968 HTTP/1.1 200 OK  (text/css)
 1119 6.74978100 202.141.80.6  10.10.12.5   HTTP    1564 HTTP/1.1 200 OK  (text/css)
 1121 6.74985500 202.141.80.6  10.10.12.5   HTTP     845 HTTP/1.1 200 OK  (text/css)
 1127 6.75009200 202.141.80.6  10.10.12.5   HTTP     362 HTTP/1.1 200 OK  (text/css)
 1143 6.75166700 202.141.80.6  10.10.12.5   HTTP    1571 HTTP/1.1 200 OK  (text/css)
 1183 6.75447500 202.141.80.6  10.10.12.5   HTTP     735 HTTP/1.1 200 OK  (text/css)

> Frame 924: 1562 bytes on wire (12496 bits), 1562 bytes captured (12496 bits) on interface 0
> Ethernet II, Src: 4c:4e:35:97:1e:ef (4c:4e:35:97:1e:ef), Dst: 84:70:ce:14:a5:15 (84:70:ce:14:a5:15)
> Internet Protocol Version 4, Src: 202.141.80.6 (202.141.80.6), Dst: 10.10.12.5 (10.10.12.5)
> Transmission Control Protocol, Src Port: http (80), Dst Port: 44549 (44549), Seq: 26143, Ack: 379, Len: 1496
> [20 Reassembled TCP Segments (27638 bytes): #888(1448), #890(1456), #892(1448), #894(1448), #896(1448), #898(1448), #900(1448), #902(1448), #904(1448), #906(1448), #908
> Hypertext Transfer Protocol
> Line-based text data: text/html

0000  84 70 ce 14 a5 15 4c 4e  35 97 1e ef 08 00 45 00   .p....LN 5.....E.
0010  06 0c b2 a3 40 00 3f 06  52 a6 ca 8d 50 06 0a 0a   ....@.?. R...P...

Frame (1562 bytes) | Reassembled TCP (27638 bytes) | De-chunked entity body (27156 bytes)

eth0: <live capture in progress> File: /t...   Packets: 14813 Displayed: 43 Marked: 0   Profile: Default
```

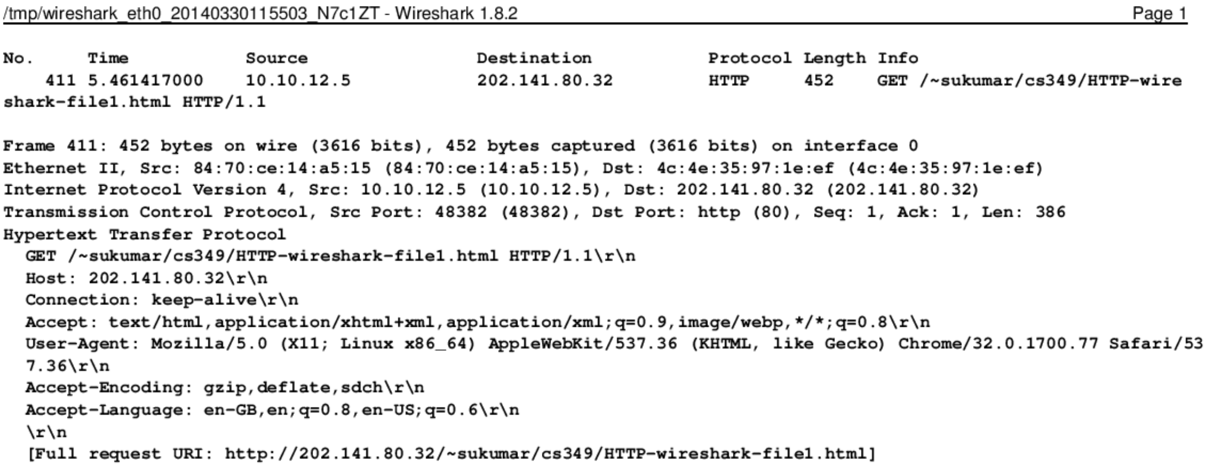
Packets sent from IITG web server to client

43 packets were transmitted from IITG web server to client.

Part B : HTTP

I. The Basic HTTP GET/response Interaction

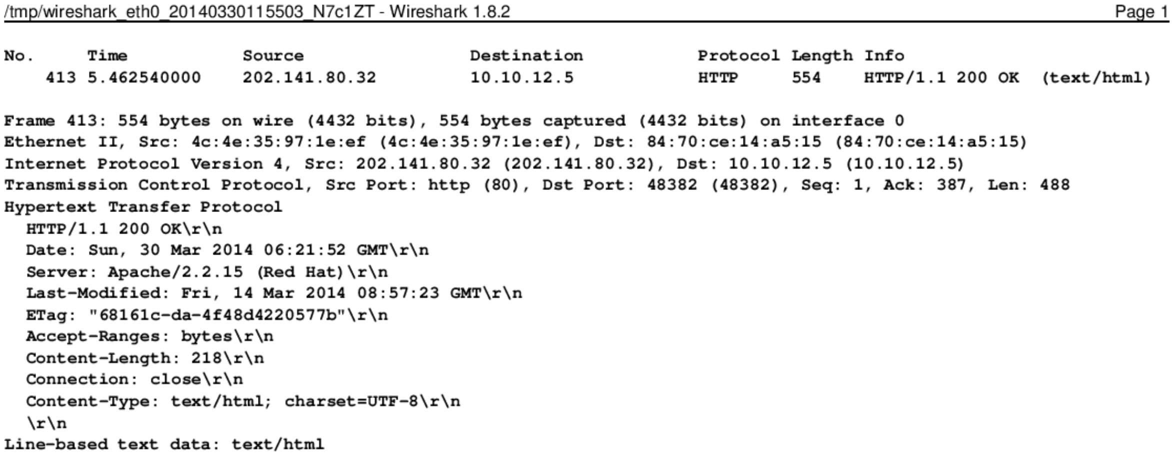
Request



/tmp/wireshark_eth0_20140330115503_N7c1ZT - Wireshark 1.8.2 Page 1

```
No.     Time           Source                Destination           Protocol Length Info
    411 5.461417000    10.10.12.5            202.141.80.32         HTTP     452    GET /~sukumar/cs349/HTTP-wire
shark-file1.html HTTP/1.1

Frame 411: 452 bytes on wire (3616 bits), 452 bytes captured (3616 bits) on interface 0
Ethernet II, Src: 84:70:ce:14:a5:15 (84:70:ce:14:a5:15), Dst: 4c:4e:35:97:1e:ef (4c:4e:35:97:1e:ef)
Internet Protocol Version 4, Src: 10.10.12.5 (10.10.12.5), Dst: 202.141.80.32 (202.141.80.32)
Transmission Control Protocol, Src Port: 48382 (48382), Dst Port: http (80), Seq: 1, Ack: 1, Len: 386
Hypertext Transfer Protocol
  GET /~sukumar/cs349/HTTP-wireshark-file1.html HTTP/1.1\r\n
  Host: 202.141.80.32\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/53
7.36\r\n
  Accept-Encoding: gzip,deflate,sdch\r\n
  Accept-Language: en-GB,en;q=0.8,en-US;q=0.6\r\n
  \r\n
  [Full request URI: http://202.141.80.32/~sukumar/cs349/HTTP-wireshark-file1.html]
```

Response



```
/tmp/wireshark_eth0_20140330115503_N7c1ZT - Wireshark 1.8.2                                    Page 1

No.     Time           Source                Destination           Protocol Length Info
    413 5.462540000    202.141.80.32         10.10.12.5            HTTP     554    HTTP/1.1 200 OK  (text/html)

Frame 413: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
Ethernet II, Src: 4c:4e:35:97:1e:ef (4c:4e:35:97:1e:ef), Dst: 84:70:ce:14:a5:15 (84:70:ce:14:a5:15)
Internet Protocol Version 4, Src: 202.141.80.32 (202.141.80.32), Dst: 10.10.12.5 (10.10.12.5)
Transmission Control Protocol, Src Port: http (80), Dst Port: 48382 (48382), Seq: 1, Ack: 387, Len: 488
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Sun, 30 Mar 2014 06:21:52 GMT\r\n
  Server: Apache/2.2.15 (Red Hat)\r\n
  Last-Modified: Fri, 14 Mar 2014 08:57:23 GMT\r\n
  ETag: "68161c-da-4f48d4220577b"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 218\r\n
  Connection: close\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
Line-based text data: text/html
```

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

Ans : My browser is running HTTP version 1.1.
[GET /~sukumar/cs349/HTTP-wireshark-file1.html **HTTP/1.1**\r\n]

The server is also running HTTP 1.1.
[**HTTP/1.1** 200 OK\r\n]

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

Ans : The browser indicates that it can accept the following languages :
English (United Kingdom), English, English (United States)
[Accept-Language: **en-GB**,**en**;q=0.8,**en-US**;q=0.6\r\n]

3. What is the IP address of your computer?

Ans : The IP address of my computer is 10.10.12.5
[Internet Protocol Version 4, **Src: 10.10.12.5 (10.10.12.5),** Dst: 202.141.80.32 (202.141.80.32)]

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

Ans: The status returned from the server to my browser is 200 OK which means '*The request has succeeded.'*
[HTTP/1.1 **200 OK**\r\n]
5. When was the HTML file that you are retrieving last modified at the server?

Ans : The HTML file was last modified on Fri, 14 Mar 2014 08:57:23 GMT**.**
[Last-Modified: **Fri, 14 Mar 2014 08:57:23 GMT**\r\n]

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

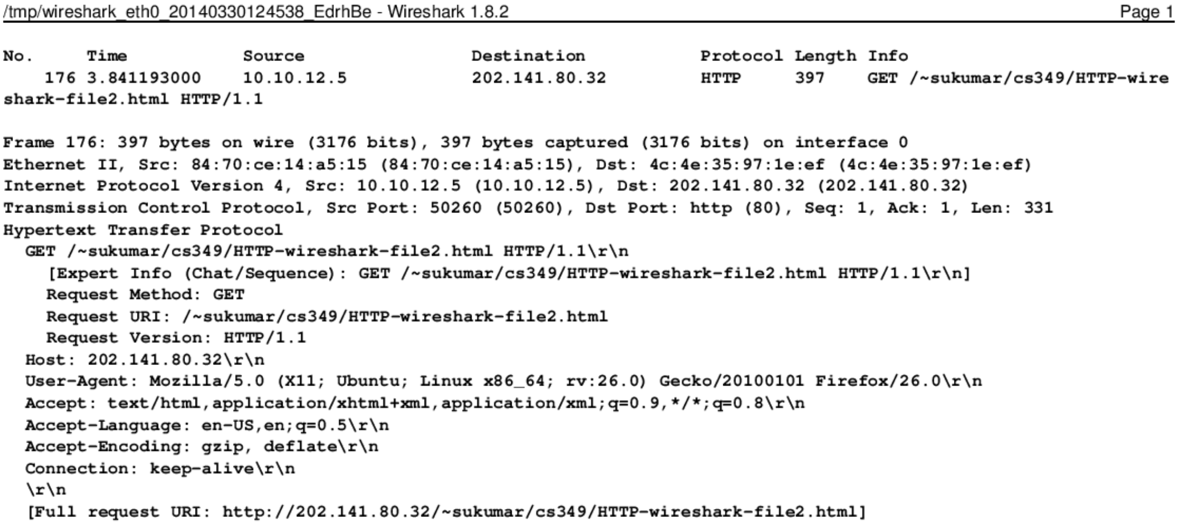
Ans : 218 bytes are returned to the browser.
[Content-Length: **218**\r\n]

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 :

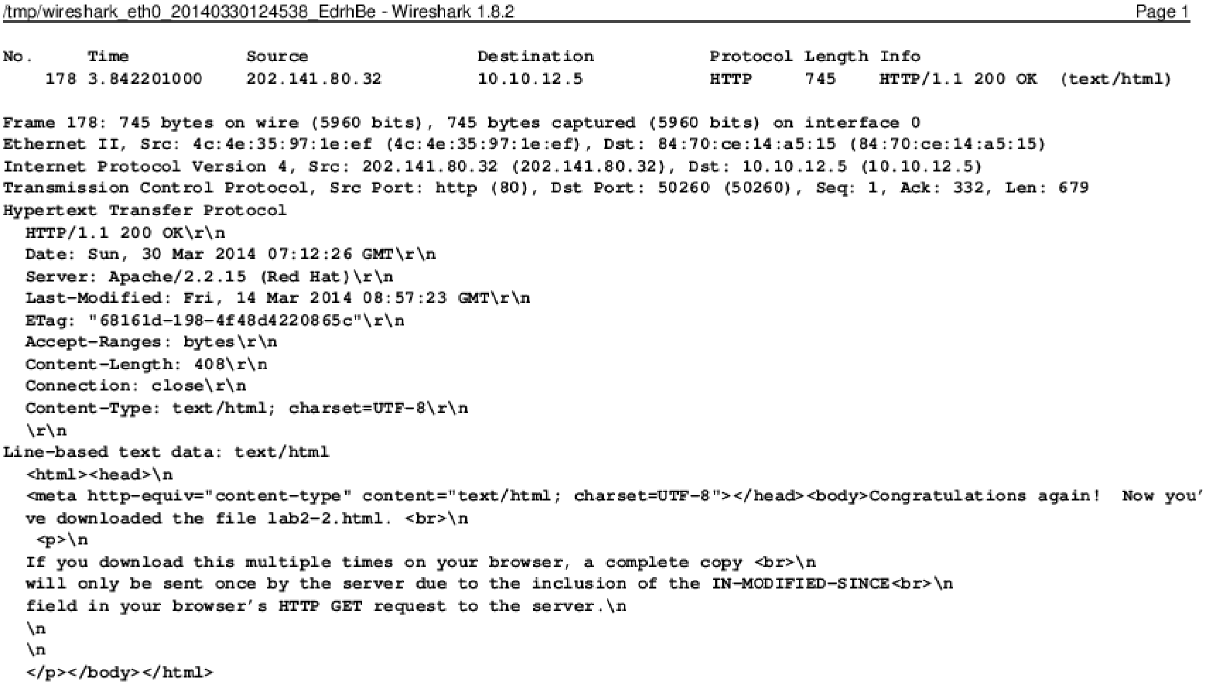
II. The HTTP CONDITIONAL GET/response Interaction

First GET Message



```
/tmp/wireshark_eth0_20140330124538_EdrhBe - Wireshark 1.8.2                                          Page 1

No.     Time           Source                Destination           Protocol Length Info
    176 3.841193000    10.10.12.5            202.141.80.32         HTTP     397    GET /~sukumar/cs349/HTTP-wire
shark-file2.html HTTP/1.1

Frame 176: 397 bytes on wire (3176 bits), 397 bytes captured (3176 bits) on interface 0
Ethernet II, Src: 84:70:ce:14:a5:15 (84:70:ce:14:a5:15), Dst: 4c:4e:35:97:1e:ef (4c:4e:35:97:1e:ef)
Internet Protocol Version 4, Src: 10.10.12.5 (10.10.12.5), Dst: 202.141.80.32 (202.141.80.32)
Transmission Control Protocol, Src Port: 50260 (50260), Dst Port: http (80), Seq: 1, Ack: 1, Len: 331
Hypertext Transfer Protocol
  GET /~sukumar/cs349/HTTP-wireshark-file2.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /~sukumar/cs349/HTTP-wireshark-file2.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /~sukumar/cs349/HTTP-wireshark-file2.html
    Request Version: HTTP/1.1
  Host: 202.141.80.32\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:26.0) Gecko/20100101 Firefox/26.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
  \r\n
  [Full request URI: http://202.141.80.32/~sukumar/cs349/HTTP-wireshark-file2.html]
```

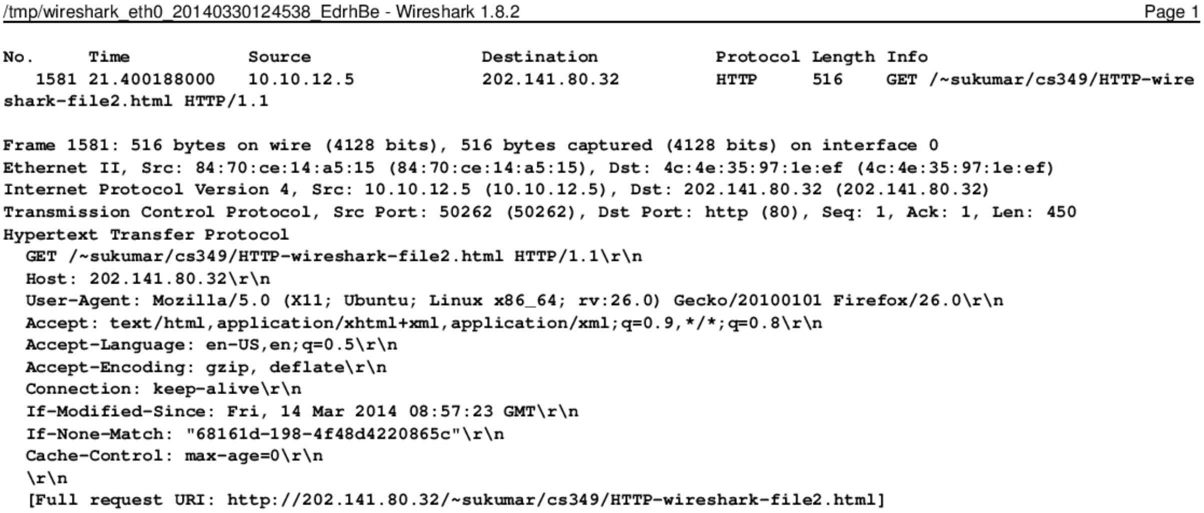
First Response



/tmp/wireshark_eth0_20140330124538_EdrhBe - Wireshark 1.8.2 Page 1

```
No.     Time           Source                Destination           Protocol Length Info
    178 3.842201000    202.141.80.32         10.10.12.5            HTTP     745    HTTP/1.1 200 OK  (text/html)

Frame 178: 745 bytes on wire (5960 bits), 745 bytes captured (5960 bits) on interface 0
Ethernet II, Src: 4c:4e:35:97:1e:ef (4c:4e:35:97:1e:ef), Dst: 84:70:ce:14:a5:15 (84:70:ce:14:a5:15)
Internet Protocol Version 4, Src: 202.141.80.32 (202.141.80.32), Dst: 10.10.12.5 (10.10.12.5)
Transmission Control Protocol, Src Port: http (80), Dst Port: 50260 (50260), Seq: 1, Ack: 332, Len: 679
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Sun, 30 Mar 2014 07:12:26 GMT\r\n
  Server: Apache/2.2.15 (Red Hat)\r\n
  Last-Modified: Fri, 14 Mar 2014 08:57:23 GMT\r\n
  ETag: "68161d-198-4f48d4220865c"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 408\r\n
  Connection: close\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
Line-based text data: text/html
  <html><head>\n
  <meta http-equiv="content-type" content="text/html; charset=UTF-8"></head><body>Congratulations again!  Now you'
  ve downloaded the file lab2-2.html. <br>\n
   <p>\n
  If you download this multiple times on your browser, a complete copy <br>\n
  will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
  field in your browser's HTTP GET request to the server.\n
  \n
  \n
  </p></body></html>
```

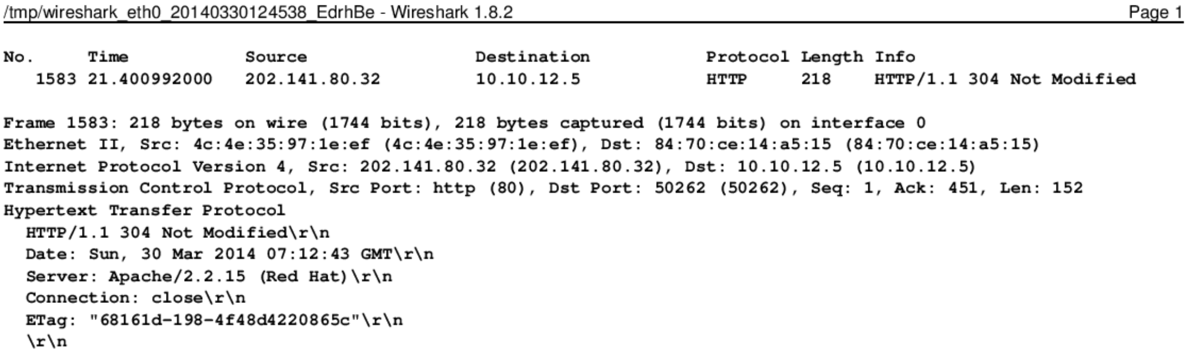
Second GET Message



/tmp/wireshark_eth0_20140330124538_EdrhBe - Wireshark 1.8.2 Page 1

```
No.     Time           Source                Destination           Protocol Length Info
   1581 21.400188000   10.10.12.5            202.141.80.32         HTTP     516    GET /~sukumar/cs349/HTTP-wire
shark-file2.html HTTP/1.1

Frame 1581: 516 bytes on wire (4128 bits), 516 bytes captured (4128 bits) on interface 0
Ethernet II, Src: 84:70:ce:14:a5:15 (84:70:ce:14:a5:15), Dst: 4c:4e:35:97:1e:ef (4c:4e:35:97:1e:ef)
Internet Protocol Version 4, Src: 10.10.12.5 (10.10.12.5), Dst: 202.141.80.32 (202.141.80.32)
Transmission Control Protocol, Src Port: 50262 (50262), Dst Port: http (80), Seq: 1, Ack: 1, Len: 450
Hypertext Transfer Protocol
  GET /~sukumar/cs349/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: 202.141.80.32\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:26.0) Gecko/20100101 Firefox/26.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
  If-Modified-Since: Fri, 14 Mar 2014 08:57:23 GMT\r\n
  If-None-Match: "68161d-198-4f48d4220865c"\r\n
  Cache-Control: max-age=0\r\n
  \r\n
  [Full request URI: http://202.141.80.32/~sukumar/cs349/HTTP-wireshark-file2.html]
```

Second Response



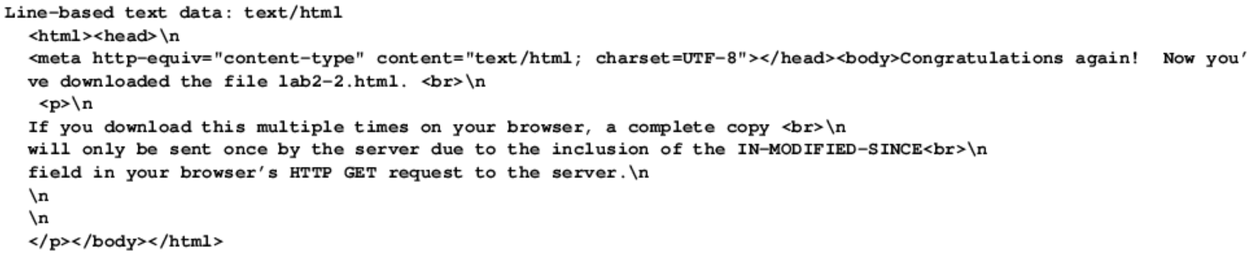
```
/tmp/wireshark_eth0_20140330124538_EdrhBe - Wireshark 1.8.2                                         Page 1

No.     Time           Source                Destination           Protocol Length Info
   1583 21.400992000   202.141.80.32         10.10.12.5            HTTP     218    HTTP/1.1 304 Not Modified

Frame 1583: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface 0
Ethernet II, Src: 4c:4e:35:97:1e:ef (4c:4e:35:97:1e:ef), Dst: 84:70:ce:14:a5:15 (84:70:ce:14:a5:15)
Internet Protocol Version 4, Src: 202.141.80.32 (202.141.80.32), Dst: 10.10.12.5 (10.10.12.5)
Transmission Control Protocol, Src Port: http (80), Dst Port: 50262 (50262), Seq: 1, Ack: 451, Len: 152
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Date: Sun, 30 Mar 2014 07:12:43 GMT\r\n
  Server: Apache/2.2.15 (Red Hat)\r\n
  Connection: close\r\n
  ETag: "68161d-198-4f48d4220865c"\r\n
  \r\n
```

1. 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, there is no “IF-MODIFIED-SINCE” line in the first HTTP GET request.

2. 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 returned the contents of the file.
We can see this here:



```
Line-based text data: text/html
  <html><head>\n
  <meta http-equiv="content-type" content="text/html; charset=UTF-8"></head><body>Congratulations again!  Now you'
  ve downloaded the file lab2-2.html. <br>\n
   <p>\n
  If you download this multiple times on your browser, a complete copy <br>\n
  will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
  field in your browser's HTTP GET request to the server.\n
  \n
  \n
  </p></body></html>
```

3. 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?

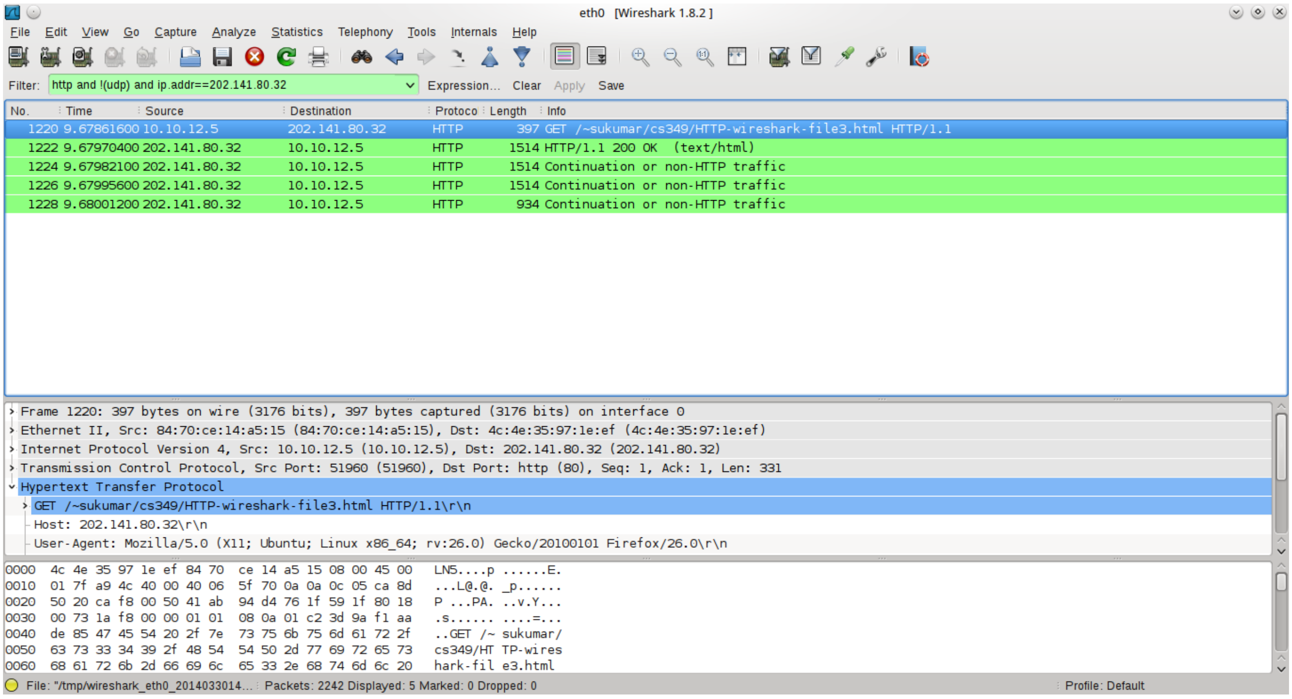
Ans : Yes, there is an “IF-MODIFIED-SINCE:” line in the second HTTP GET request.
[If-Modified-Since: Fri, 14 Mar 2014 08:57:23 GMT\r\n]
It tells the server that it should only return the contents of the file again if they have changed since Fri, 14 Mar 2014 08:57:23 GMT. (The last modified time of the file).

4. 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 server returned the HTTP status code 304 along with the phrase Not Modified.

[HTTP/1.1 304 Not Modified\r\n]
The contents of the file were not explicitly returned.
The reason for this is that the second GET request was a conditional GET request with the header If-Modified-Since. As the contents of the file on the server has not been modified after Fri, 14 Mar 2014 08:57:23 GMT, the server returned a Not Modified response to indicate to the client that the file had not been modified and hence sending the contents again was not required.

III. Retrieving Long Documents



Filter: http and !(udp) and ip.addr==202.141.80.32

```
No.   Time       Source         Destination    Protoco Length Info
 1220 9.67861600 10.10.12.5     202.141.80.32  HTTP     397 GET /~sukumar/cs349/HTTP-wireshark-file3.html HTTP/1.1
 1222 9.67970400 202.141.80.32  10.10.12.5     HTTP    1514 HTTP/1.1 200 OK  (text/html)
 1224 9.67982100 202.141.80.32  10.10.12.5     HTTP    1514 Continuation or non-HTTP traffic
 1226 9.67995600 202.141.80.32  10.10.12.5     HTTP    1514 Continuation or non-HTTP traffic
 1228 9.68001200 202.141.80.32  10.10.12.5     HTTP     934 Continuation or non-HTTP traffic
```

```
> Frame 1220: 397 bytes on wire (3176 bits), 397 bytes captured (3176 bits) on interface 0
> Ethernet II, Src: 84:70:ce:14:a5:15 (84:70:ce:14:a5:15), Dst: 4c:4e:35:97:1e:ef (4c:4e:35:97:1e:ef)
> Internet Protocol Version 4, Src: 10.10.12.5 (10.10.12.5), Dst: 202.141.80.32 (202.141.80.32)
> Transmission Control Protocol, Src Port: 51960 (51960), Dst Port: http (80), Seq: 1, Ack: 1, Len: 331
v Hypertext Transfer Protocol
  > GET /~sukumar/cs349/HTTP-wireshark-file3.html HTTP/1.1\r\n
    Host: 202.141.80.32\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:26.0) Gecko/20100101 Firefox/26.0\r\n
```

```
0000  4c 4e 35 97 1e ef 84 70  ce 14 a5 15 08 00 45 00   LN5....p ......E.
0010  01 7f a9 4c 40 00 40 06  5f 70 0a 0a 0c 05 ca 8d   ...L@.@. _p......
0020  50 20 ca f8 00 50 41 ab  94 d4 76 1f 59 1f 80 18   P ...PA. ..v.Y...
0030  00 73 1a f8 00 00 01 01  08 0a 01 c2 3d 9a f1 aa   .s...... ....=...
0040  de 85 47 45 54 20 2f 7e  73 75 6b 75 6d 61 72 2f   ..GET /~ sukumar/
0050  63 73 33 34 39 2f 48 54  54 50 2d 77 69 72 65 73   cs349/HT TP-wires
0060  68 61 72 6b 2d 66 69 6c  65 33 2e 68 74 6d 6c 20   hark-fil e3.html
```

File: "/tmp/wireshark_eth0_2014033014... Packets: 2242 Displayed: 5 Marked: 0 Dropped: 0   Profile: Default

1. How many HTTP GET request messages were sent by your browser?

Ans : **1** HTTP GET request message was sent by my browser.

2. How many data-containing TCP segments were needed to carry the single HTTP response?

Ans : **4** TCP segments were needed to carry the single HTTP response.

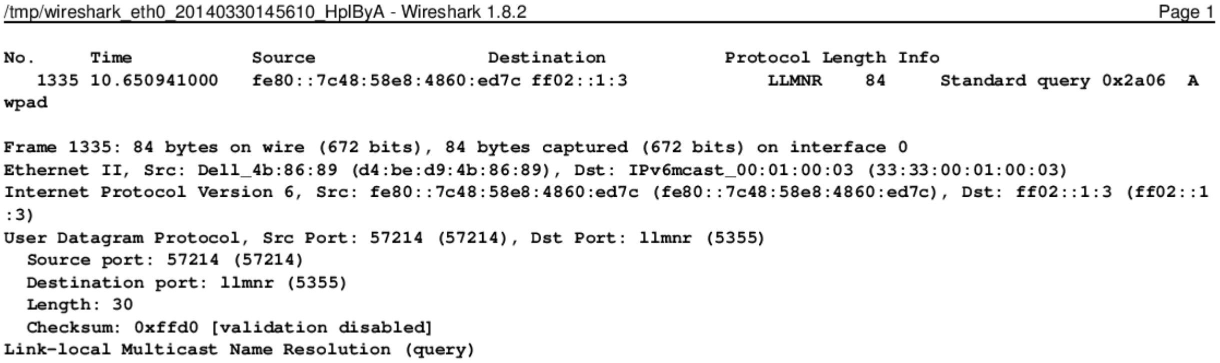
3. What is the status code and phrase associated with the response to the HTTP GET request?

Ans : The status code is 200 and the associated phrase is OK.
[HTTP/1.1 **200 OK**\r\n]

4. Are there any HTTP status lines in the transmitted data associated with a TCP-induced “Continuation”?

Ans : **No**, there is no associated HTTP status line associated with the TCP-induced “Continuation”.

Part C: UDP



```
/tmp/wireshark_eth0_20140330145610_HplByA - Wireshark 1.8.2                                          Page 1

No.     Time           Source                     Destination            Protocol Length Info
   1335 10.650941000   fe80::7c48:58e8:4860:ed7c ff02::1:3                  LLMNR    84     Standard query 0x2a06  A
wpad

Frame 1335: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Ethernet II, Src: Dell_4b:86:89 (d4:be:d9:4b:86:89), Dst: IPv6mcast_00:01:00:03 (33:33:00:01:00:03)
Internet Protocol Version 6, Src: fe80::7c48:58e8:4860:ed7c (fe80::7c48:58e8:4860:ed7c), Dst: ff02::1:3 (ff02::1
:3)
User Datagram Protocol, Src Port: 57214 (57214), Dst Port: llmnr (5355)
  Source port: 57214 (57214)
  Destination port: llmnr (5355)
  Length: 30
  Checksum: 0xffd0 [validation disabled]
Link-local Multicast Name Resolution (query)
```

a. Select one packet. From this packet, determine how many fields there are in the UDP header. (Do not look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields as they are named in the Wireshark display of segment fields.

Ans: There are **4** fields in the UDP header. These are:
[1] Source Port
[2] Destination Port
[3] Length
[4] Checksum

b. What are the source and destination port numbers, in both decimal and hexadecimal format. (Hint: the hexadecimal format is given in the data in the bottommost panel in the wireshark display, and so it’s easier just to read it out from there rather than converting the decimal number to hex).

Ans : Source port number -> Decimal : **57214** Hexadecimal : **df7e**
Destination port number -> Decimal : **53555** Hexadecimal : **14eb**

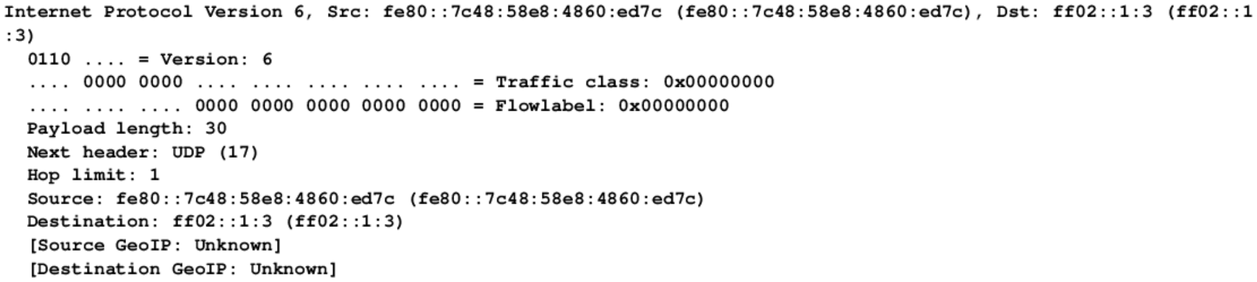
c. What is the value in the Length field in both decimal and hexadecimal format. What is the meaning of this value (i.e., this value is the length of what?)

Ans : Length -> Decimal : **30** Hexadecimal : **1e**

The length field specifies the length of the UDP header and the UDP data (in bytes).

d. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. (To answer this question, you'll need to look into the IP header.)

Ans :



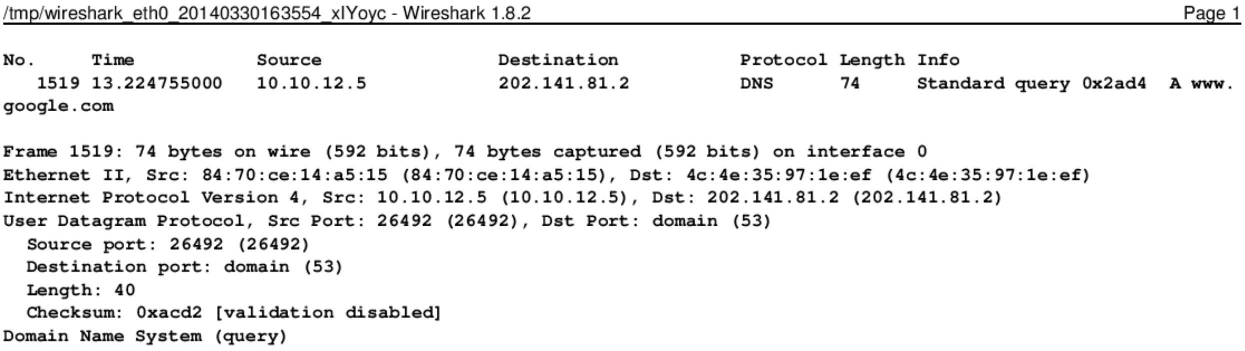
```
Internet Protocol Version 6, Src: fe80::7c48:58e8:4860:ed7c (fe80::7c48:58e8:4860:ed7c), Dst: ff02::1:3 (ff02::1
:3)
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 30
  Next header: UDP (17)
  Hop limit: 1
  Source: fe80::7c48:58e8:4860:ed7c (fe80::7c48:58e8:4860:ed7c)
  Destination: ff02::1:3 (ff02::1:3)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
```

Protocol Number for UDP -> Decimal : **17** Hexadecimal : **11**

e. Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.

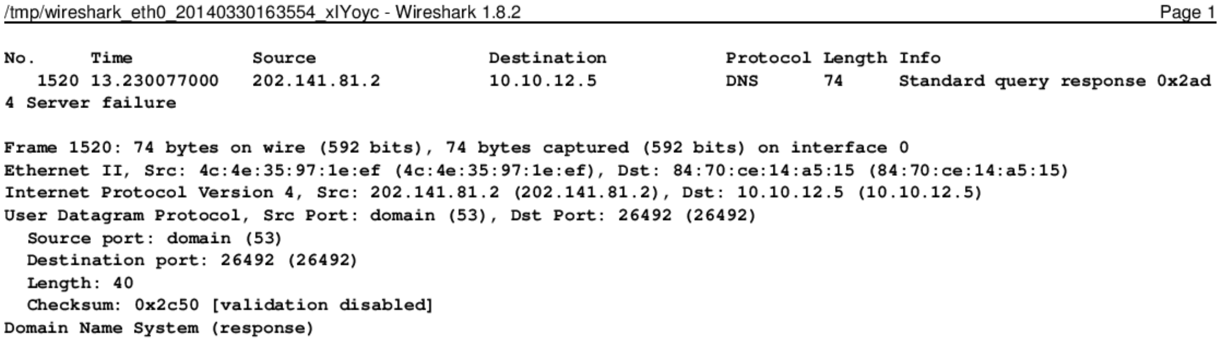
Ans :

Query



```
/tmp/wireshark_eth0_20140330163554_xIYoyc - Wireshark 1.8.2                                    Page 1

No.     Time           Source                Destination           Protocol Length Info
   1519 13.224755000   10.10.12.5            202.141.81.2          DNS      74     Standard query 0x2ad4  A www.
google.com

Frame 1519: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: 84:70:ce:14:a5:15 (84:70:ce:14:a5:15), Dst: 4c:4e:35:97:1e:ef (4c:4e:35:97:1e:ef)
Internet Protocol Version 4, Src: 10.10.12.5 (10.10.12.5), Dst: 202.141.81.2 (202.141.81.2)
User Datagram Protocol, Src Port: 26492 (26492), Dst Port: domain (53)
  Source port: 26492 (26492)
  Destination port: domain (53)
  Length: 40
  Checksum: 0xacd2 [validation disabled]
Domain Name System (query)
```

Response



```
/tmp/wireshark_eth0_20140330163554_xIYoyc - Wireshark 1.8.2                                    Page 1

No.     Time           Source                Destination           Protocol Length Info
   1520 13.230077000   202.141.81.2          10.10.12.5            DNS      74     Standard query response 0x2ad
4 Server failure

Frame 1520: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: 4c:4e:35:97:1e:ef (4c:4e:35:97:1e:ef), Dst: 84:70:ce:14:a5:15 (84:70:ce:14:a5:15)
Internet Protocol Version 4, Src: 202.141.81.2 (202.141.81.2), Dst: 10.10.12.5 (10.10.12.5)
User Datagram Protocol, Src Port: domain (53), Dst Port: 26492 (26492)
  Source port: domain (53)
  Destination port: 26492 (26492)
  Length: 40
  Checksum: 0x2c50 [validation disabled]
Domain Name System (response)
```

Query == Source Port -> **26492**, Dest Port -> **53**
Response == Source Port -> **53**, Dest Port -> **26492**

Therefore, we observe that the source port of the query packet is the destination port for the response packet and the destination port of the query packet is the source port of the response packet.