Networks Assignment-4

Packet Capturing Using Wireshark

Prepared by:

Nikhil Agarwal
11012323

Himanshu Upreti
11012315

Instructors:

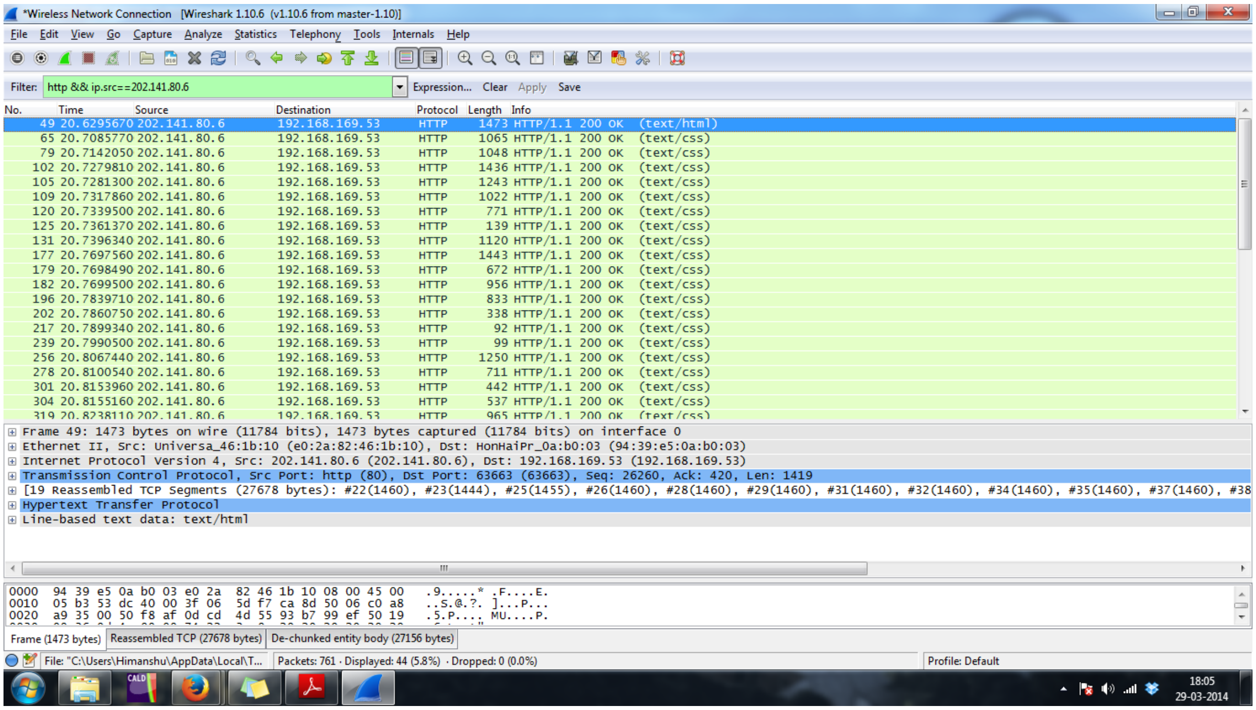
Dr. Sukumar Nandi
T. Venkatesh

March 31, 2014

PartA: Initials

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

Ans: 44.



*Wireless Network Connection [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: http && ip.src==202.141.80.6

```
No.     Time        Source            Destination       Protocol Length Info
     49 20.6295670 202.141.80.6      192.168.169.53    HTTP     1473 HTTP/1.1 200 OK  (text/html)
     65 20.7085770 202.141.80.6      192.168.169.53    HTTP     1065 HTTP/1.1 200 OK  (text/css)
     79 20.7142050 202.141.80.6      192.168.169.53    HTTP     1048 HTTP/1.1 200 OK  (text/css)
    102 20.7279810 202.141.80.6      192.168.169.53    HTTP     1436 HTTP/1.1 200 OK  (text/css)
    105 20.7281300 202.141.80.6      192.168.169.53    HTTP     1243 HTTP/1.1 200 OK  (text/css)
    109 20.7317860 202.141.80.6      192.168.169.53    HTTP     1022 HTTP/1.1 200 OK  (text/css)
    120 20.7339500 202.141.80.6      192.168.169.53    HTTP      771 HTTP/1.1 200 OK  (text/css)
    125 20.7361370 202.141.80.6      192.168.169.53    HTTP      139 HTTP/1.1 200 OK  (text/css)
    131 20.7396340 202.141.80.6      192.168.169.53    HTTP     1120 HTTP/1.1 200 OK  (text/css)
    177 20.7697560 202.141.80.6      192.168.169.53    HTTP     1443 HTTP/1.1 200 OK  (text/css)
    179 20.7698490 202.141.80.6      192.168.169.53    HTTP      672 HTTP/1.1 200 OK  (text/css)
    182 20.7699500 202.141.80.6      192.168.169.53    HTTP      956 HTTP/1.1 200 OK  (text/css)
    196 20.7839710 202.141.80.6      192.168.169.53    HTTP      833 HTTP/1.1 200 OK  (text/css)
    202 20.7860750 202.141.80.6      192.168.169.53    HTTP      338 HTTP/1.1 200 OK  (text/css)
    217 20.7899340 202.141.80.6      192.168.169.53    HTTP       92 HTTP/1.1 200 OK  (text/css)
    239 20.7990500 202.141.80.6      192.168.169.53    HTTP       99 HTTP/1.1 200 OK  (text/css)
    256 20.8067440 202.141.80.6      192.168.169.53    HTTP     1250 HTTP/1.1 200 OK  (text/css)
    278 20.8100540 202.141.80.6      192.168.169.53    HTTP      711 HTTP/1.1 200 OK  (text/css)
    301 20.8153960 202.141.80.6      192.168.169.53    HTTP      442 HTTP/1.1 200 OK  (text/css)
    304 20.8155160 202.141.80.6      192.168.169.53    HTTP      537 HTTP/1.1 200 OK  (text/css)
    319 20.8238110 202.141.80.6      192.168.169.53    HTTP      965 HTTP/1.1 200 OK  (text/css)
```

```
⊞ Frame 49: 1473 bytes on wire (11784 bits), 1473 bytes captured (11784 bits) on interface 0
⊞ Ethernet II, Src: Universa_46:1b:10 (e0:2a:82:46:1b:10), Dst: HonHaiPr_0a:b0:03 (94:39:e5:0a:b0:03)
⊞ Internet Protocol Version 4, Src: 202.141.80.6 (202.141.80.6), Dst: 192.168.169.53 (192.168.169.53)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 63663 (63663), Seq: 26260, Ack: 420, Len: 1419
⊞ [19 Reassembled TCP Segments (27678 bytes): #22(1460), #23(1444), #25(1455), #26(1460), #28(1460), #29(1460), #31(1460), #32(1460), #34(1460), #35(1460), #37(1460), #38
⊞ Hypertext Transfer Protocol
⊞ Line-based text data: text/html
```

```
0000  94 39 e5 0a b0 03 e0 2a  82 46 1b 10 08 00 45 00   .9.....* .F....E.
0010  05 b3 53 dc 40 00 3f 06  5d f7 ca 8d 50 06 c0 a8   ..S.@.?. ]...P...
0020  a9 35 00 50 f8 af 0d cd  4d 55 93 b7 99 ef 50 19   .5.P.... MU....P.
```

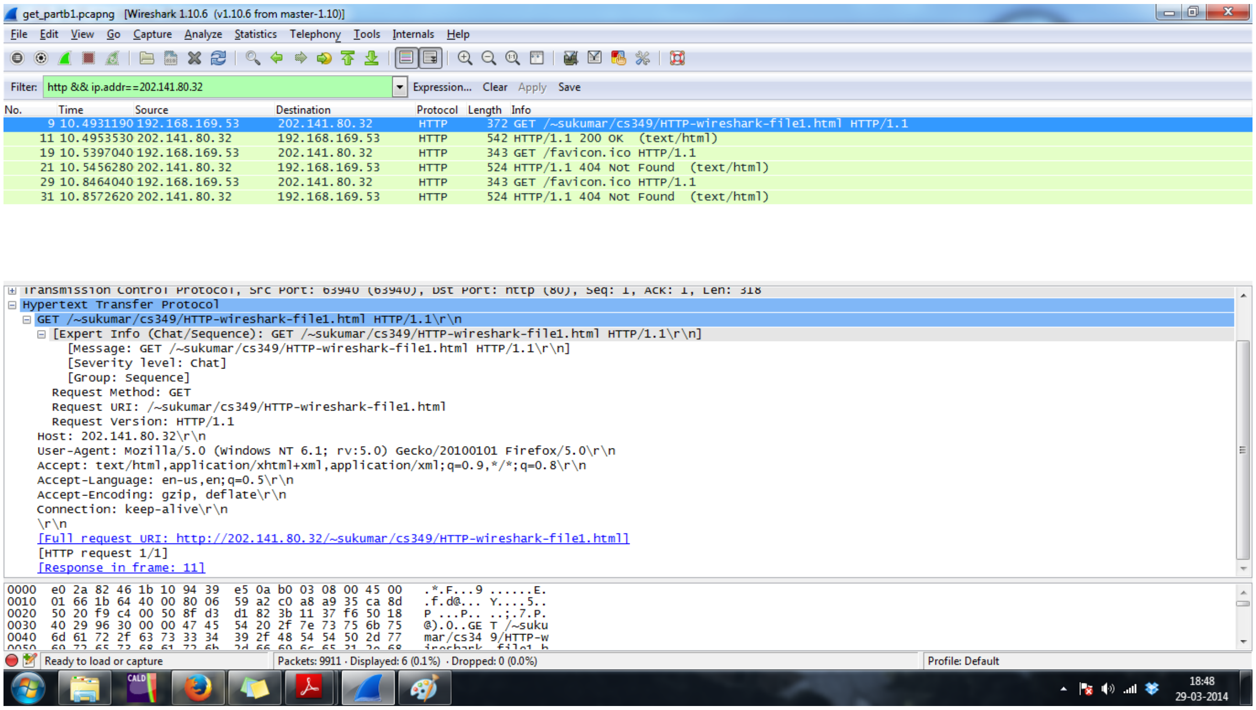
Frame (1473 bytes) | Reassembled TCP (27678 bytes) | De-chunked entity body (27156 bytes)

File: "C:\Users\Himanshu\AppData\Local\T... Packets: 761 · Displayed: 44 (5.8%) · Dropped: 0 (0.0%) Profile: Default

Figure 1: Packets transmitted from iitg web server

PartB: HTTP

The Basic HTTP GET/response Interaction



get_partb1.pcapng [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http && ip.addr==202.141.80.32

Expression... Clear Apply Save

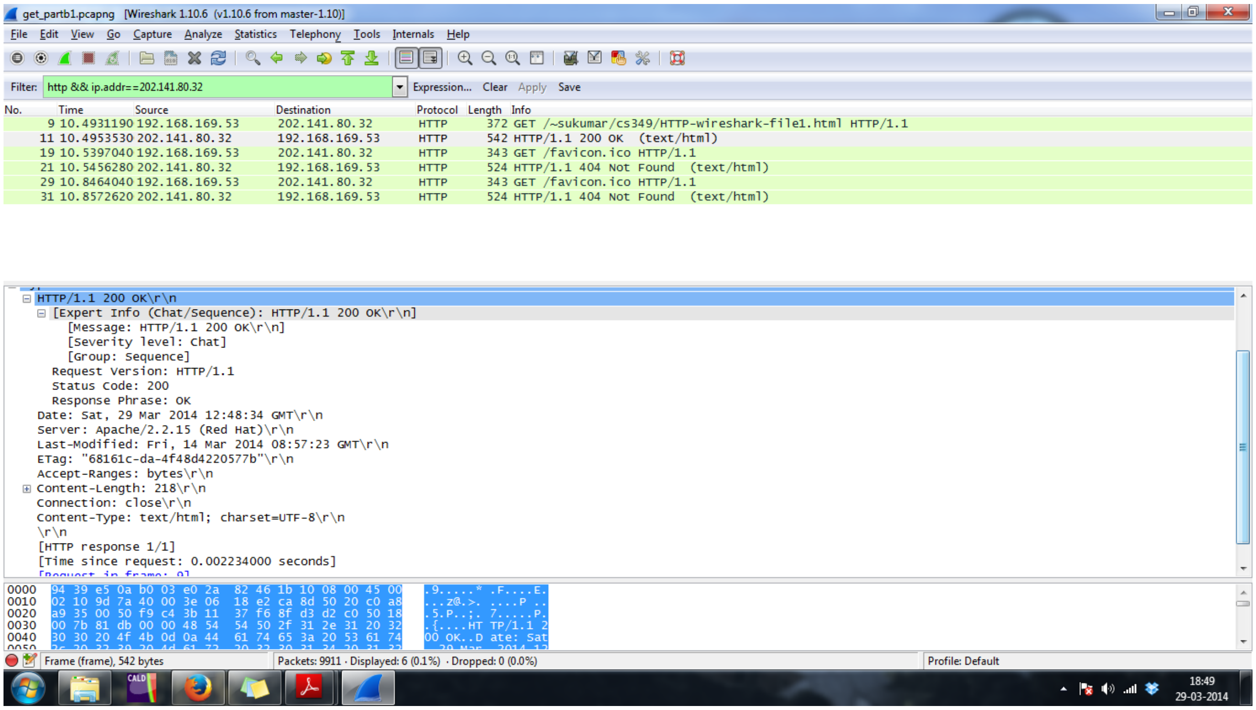
```
No.   Time       Source          Destination     Protocol Length Info
    9 10.4931190 192.168.169.53  202.141.80.32   HTTP     372 GET /~sukumar/cs349/HTTP-wireshark-file1.html HTTP/1.1
   11 10.4953530 202.141.80.32   192.168.169.53  HTTP     542 HTTP/1.1 200 OK  (text/html)
   19 10.5397040 192.168.169.53  202.141.80.32   HTTP     343 GET /favicon.ico HTTP/1.1
   21 10.5456280 202.141.80.32   192.168.169.53  HTTP     524 HTTP/1.1 404 Not Found  (text/html)
   29 10.8464040 192.168.169.53  202.141.80.32   HTTP     343 GET /favicon.ico HTTP/1.1
   31 10.8572620 202.141.80.32   192.168.169.53  HTTP     524 HTTP/1.1 404 Not Found  (text/html)
```

```
⊞ Transmission Control Protocol, Src Port: 63940 (63940), Dst Port: http (80), Seq: 1, Ack: 1, Len: 318
⊟ Hypertext Transfer Protocol
  ⊟ GET /~sukumar/cs349/HTTP-wireshark-file1.html HTTP/1.1\r\n
    ⊟ [Expert Info (Chat/Sequence): GET /~sukumar/cs349/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Message: GET /~sukumar/cs349/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /~sukumar/cs349/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: 202.141.80.32\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0\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-file1.html]
    [HTTP request 1/1]
    [Response in frame: 11]
```

```
0000  e0 2a 82 46 1b 10 94 39  e5 0a b0 03 08 00 45 00   .*.F...9 ......E.
0010  01 66 1b 64 40 00 80 06  59 a2 c0 a8 a9 35 ca 8d   .f.d@... Y....5..
0020  50 20 f9 c4 00 50 8f d3  d1 82 3b 11 37 f6 50 18   P ...P.. ..;.7.P.
0030  40 29 96 30 00 00 47 45  54 20 2f 7e 73 75 6b 75   @).0..GE T /~suku
0040  6d 61 72 2f 63 73 33 34  39 2f 48 54 54 50 2d 77   mar/cs34 9/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
```

Ready to load or capture | Packets: 9911 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

Figure 2: Get message display


get_partb1.pcapng [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Profile: Default
18:49
29-03-2014

Filter: http && ip.addr==202.141.80.32

```
No.    Time       Source          Destination     Protocol Length Info
     9 10.4931190 192.168.169.53  202.141.80.32   HTTP     372 GET /~sukumar/cs349/HTTP-wireshark-file1.html HTTP/1.1
    11 10.4953530 202.141.80.32   192.168.169.53  HTTP     542 HTTP/1.1 200 OK  (text/html)
    19 10.5397040 192.168.169.53  202.141.80.32   HTTP     343 GET /favicon.ico HTTP/1.1
    21 10.5456280 202.141.80.32   192.168.169.53  HTTP     524 HTTP/1.1 404 Not Found  (text/html)
    29 10.8464040 192.168.169.53  202.141.80.32   HTTP     343 GET /favicon.ico HTTP/1.1
    31 10.8572620 202.141.80.32   192.168.169.53  HTTP     524 HTTP/1.1 404 Not Found  (text/html)
```

```
⊟ HTTP/1.1 200 OK\r\n
  ⊟ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [Message: HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 200
    Response Phrase: OK
  Date: Sat, 29 Mar 2014 12:48:34 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
  [HTTP response 1/1]
  [Time since request: 0.002234000 seconds]
```

```
0000  94 39 e5 0a b0 03 e0 2a  82 46 1b 10 08 00 45 00   .9.....* .F....E.
0010  02 10 9d 7a 40 00 3e 06  18 e2 ca 8d 50 20 c0 a8   ...z@.>. ....P ..
0020  a9 35 00 50 f9 c4 3b 11  37 f6 8f d3 d2 c0 50 18   .5.P..;. 7.....P.
0030  00 7b 81 db 00 00 48 54  54 50 2f 31 2e 31 20 32   .{....HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 61 74   00 OK..D ate: Sat
```

Frame (frame), 542 bytes | Packets: 9911 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%)

Figure 3: Response message display

```
No.     Time           Source                Destination
    Protocol Length Info
      9 10.493119000   192.168.169.53        202.141.80.32         HTTP
             372     GET /~sukumar/cs349/HTTP-wireshark-file1.html HTTP/1.1

Frame 9: 372 bytes on wire (2976 bits), 372 bytes captured (2976 bits) on
    interface 0
Ethernet II, Src: HonHaiPr_0a:b0:03 (94:39:e5:0a:b0:03), Dst: Universa_46
    :1b:10 (e0:2a:82:46:1b:10)
Internet Protocol Version 4, Src: 192.168.169.53 (192.168.169.53), Dst:
    202.141.80.32 (202.141.80.32)
Transmission Control Protocol, Src Port: 63940 (63940), Dst Port: http
    (80), Seq: 1, Ack: 1, Len: 318
Hypertext Transfer Protocol
     GET /~sukumar/cs349/HTTP-wireshark-file1.html HTTP/1.1\r\n
     Host: 202.141.80.32\r\n
     User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101
        Firefox/5.0\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-
        file1.html]
     [HTTP request 1/1]
     [Response in frame: 11]

 No.     Time           Source                Destination
    Protocol Length Info
      11 10.495353000   202.141.80.32         192.168.169.53        HTTP
             542    HTTP/1.1 200 OK  (text/html)

 Frame 11: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on
     interface 0
 Ethernet II, Src: Universa_46:1b:10 (e0:2a:82:46:1b:10), Dst: HonHaiPr_0a:
    b0:03 (94:39:e5:0a:b0:03)
 Internet Protocol Version 4, Src: 202.141.80.32 (202.141.80.32), Dst:
    192.168.169.53 (192.168.169.53)
 Transmission Control Protocol, Src Port: http (80), Dst Port: 63940
    (63940), Seq: 1, Ack: 319, Len: 488
 Hypertext Transfer Protocol
     HTTP/1.1 200 OK\r\n
     Date: Sat, 29 Mar 2014 12:48:34 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
     [HTTP response 1/1]
     [Time since request: 0.002234000 seconds]
     [Request in frame: 9]
 Line-based text data: text/html
```

Listing 1: HTTP GET/RESPONSE interaction

Q1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running.
Ans: Both are running HTTP 1.1

Q2. What languages (if any) does your browser indicate that it can accept to the server?
Ans: Accept-Language: en-us

Q3. What is the IP address of your computer?
Ans: The IP address of our computer is 192.168.169.53

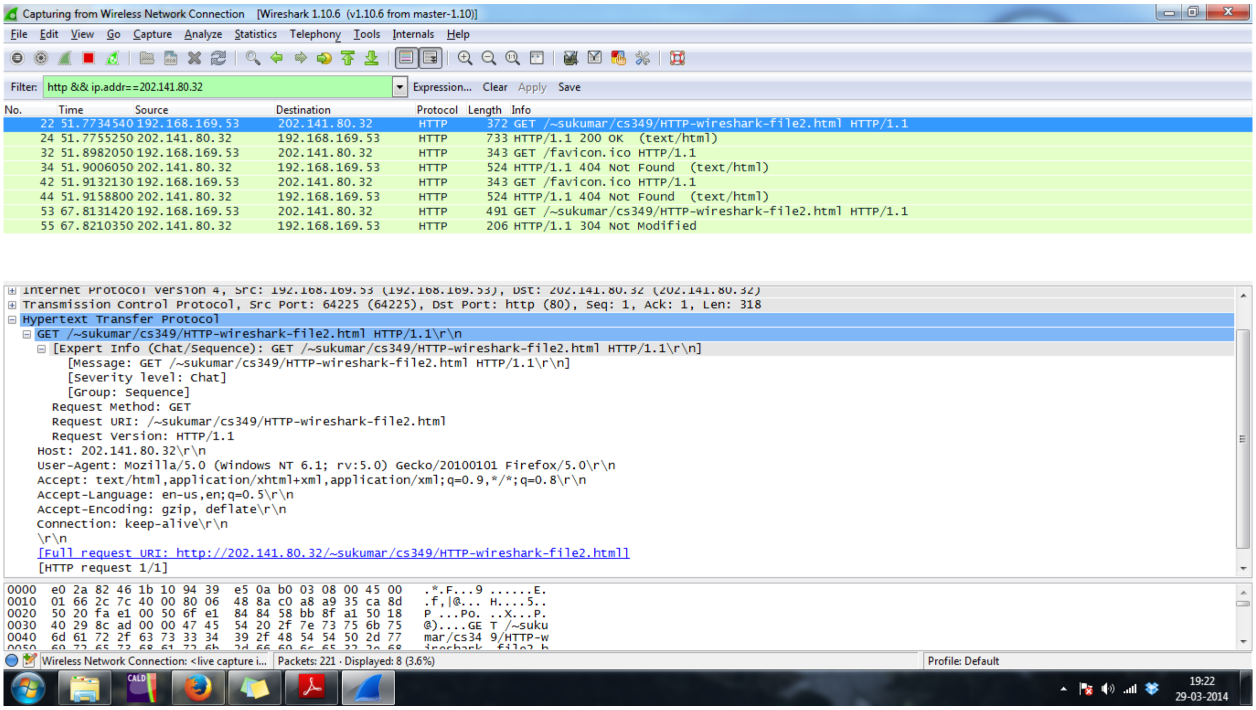
Q4. What is the status code returned from the server to your browser?
Ans: 200 OK (text/html)

Q5. When was the HTML file that you are retrieving last modified at the server?
Ans: Last-Modified: Fri , 14 Mar 2014 08:57:23 GMT

Q6. How many bytes of content are being returned to your browser?
Ans: Content-Length: 218

Q7. 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 all of the headers can be found in the raw data.

The HTTP CONDITIONAL GET/response Interaction


Capturing from Wireless Network Connection [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Wireless Network Connection: <live capture i...
Packets: 221 · Displayed: 8 (3.6%)
Profile: Default
CALD
19:22
29-03-2014

Filter: http && ip.addr==202.141.80.32

```
No.     Time          Source             Destination        Protocol Length Info
     22 51.7734540    192.168.169.53     202.141.80.32      HTTP     372    GET /~sukumar/cs349/HTTP-wireshark-file2.html HTTP/1.1
     24 51.7755250    202.141.80.32      192.168.169.53     HTTP     733    HTTP/1.1 200 OK  (text/html)
     32 51.8982050    192.168.169.53     202.141.80.32      HTTP     343    GET /favicon.ico HTTP/1.1
     34 51.9006050    202.141.80.32      192.168.169.53     HTTP     524    HTTP/1.1 404 Not Found  (text/html)
     42 51.9132130    192.168.169.53     202.141.80.32      HTTP     343    GET /favicon.ico HTTP/1.1
     44 51.9158800    202.141.80.32      192.168.169.53     HTTP     524    HTTP/1.1 404 Not Found  (text/html)
     53 67.8131420    192.168.169.53     202.141.80.32      HTTP     491    GET /~sukumar/cs349/HTTP-wireshark-file2.html HTTP/1.1
     55 67.8210350    202.141.80.32      192.168.169.53     HTTP     206    HTTP/1.1 304 Not Modified
```

```
⊞ Internet Protocol Version 4, Src: 192.168.169.53 (192.168.169.53), Dst: 202.141.80.32 (202.141.80.32)
⊞ Transmission Control Protocol, Src Port: 64225 (64225), Dst Port: http (80), Seq: 1, Ack: 1, Len: 318
⊟ 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]
        [Message: GET /~sukumar/cs349/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      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 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0\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]
    [HTTP request 1/1]
```

```
0000  e0 2a 82 46 1b 10 94 39  e5 0a b0 03 08 00 45 00   .*.F...9 ......E.
0010  01 66 2c 7c 40 00 80 06  48 8a c0 a8 a9 35 ca 8d   .f,|@... H....5..
0020  50 20 fa e1 00 50 6f e1  84 84 58 bb 8f a1 50 18   P ...Po. ..X...P.
0030  40 29 8c ad 00 00 47 45  54 20 2f 7e 73 75 6b 75   @)....GE T /~suku
0040  6d 61 72 2f 63 73 33 34  39 2f 48 54 54 50 2d 77   mar/cs34 9/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 32 2e 68   ireshark -file2.h
```

Figure 4: First get message display

```
No.     Time           Source                Destination
    Protocol Length Info
     22 51.773454000   192.168.169.53        202.141.80.32         HTTP
            372    GET /~sukumar/cs349/HTTP-wireshark-file2.html HTTP/1.1

Frame 22: 372 bytes on wire (2976 bits), 372 bytes captured (2976 bits) on
    interface 0
Ethernet II, Src: HonHaiPr_0a:b0:03 (94:39:e5:0a:b0:03), Dst: Universa_46
    :1b:10 (e0:2a:82:46:1b:10)
Internet Protocol Version 4, Src: 192.168.169.53 (192.168.169.53), Dst:
    202.141.80.32 (202.141.80.32)
Transmission Control Protocol, Src Port: 64225 (64225), Dst Port: http
    (80), Seq: 1, Ack: 1, Len: 318
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]
```

```
            [Message: GET /~sukumar/cs349/HTTP-wireshark-file2.html HTTP
               /1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        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 (Windows NT 6.1; rv:5.0) Gecko/20100101
       Firefox/5.0\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]
    [HTTP request 1/1]
    [Response in frame: 24]

No.     Time           Source                Destination
   Protocol Length Info
     24 51.775525000   202.141.80.32         192.168.169.53        HTTP
            733    HTTP/1.1 200 OK  (text/html)

Frame 24: 733 bytes on wire (5864 bits), 733 bytes captured (5864 bits) on
    interface 0
Ethernet II, Src: Universa_46:1b:10 (e0:2a:82:46:1b:10), Dst: HonHaiPr_0a:
   b0:03 (94:39:e5:0a:b0:03)
Internet Protocol Version 4, Src: 202.141.80.32 (202.141.80.32), Dst:
   192.168.169.53 (192.168.169.53)
Transmission Control Protocol, Src Port: http (80), Dst Port: 64225
   (64225), Seq: 1, Ack: 319, Len: 679
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [Message: HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
    Date: Sat, 29 Mar 2014 13:41:21 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
    [HTTP response 1/1]
    [Time since request: 0.002071000 seconds]
    [Request in frame: 22]
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>

No.     Time           Source                Destination
   Protocol Length Info
     53 67.813142000   192.168.169.53        202.141.80.32         HTTP
            491    GET /~sukumar/cs349/HTTP-wireshark-file2.html HTTP/1.1

Frame 53: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on
    interface 0
Ethernet II, Src: HonHaiPr_0a:b0:03 (94:39:e5:0a:b0:03), Dst: Universa_46
   :1b:10 (e0:2a:82:46:1b:10)
Internet Protocol Version 4, Src: 192.168.169.53 (192.168.169.53), Dst:
   202.141.80.32 (202.141.80.32)
Transmission Control Protocol, Src Port: 64232 (64232), Dst Port: http
   (80), Seq: 1, Ack: 1, Len: 437
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]
            [Message: GET /~sukumar/cs349/HTTP-wireshark-file2.html HTTP
               /1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        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 (Windows NT 6.1; rv:5.0) Gecko/20100101
       Firefox/5.0\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]
    [HTTP request 1/1]
    [Response in frame: 55]

No.     Time           Source                Destination
   Protocol Length Info
     55 67.821035000   202.141.80.32         192.168.169.53        HTTP
            206    HTTP/1.1 304 Not Modified

Frame 55: 206 bytes on wire (1648 bits), 206 bytes captured (1648 bits) on
    interface 0
Ethernet II, Src: Universa_46:1b:10 (e0:2a:82:46:1b:10), Dst: HonHaiPr_0a:
   b0:03 (94:39:e5:0a:b0:03)
Internet Protocol Version 4, Src: 202.141.80.32 (202.141.80.32), Dst:
   192.168.169.53 (192.168.169.53)
Transmission Control Protocol, Src Port: http (80), Dst Port: 64232
   (64232), Seq: 1, Ack: 438, Len: 152
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
            [Message: HTTP/1.1 304 Not Modified\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.1
        Status Code: 304
        Response Phrase: Not Modified
    Date: Sat, 29 Mar 2014 13:41:38 GMT\r\n
    Server: Apache/2.2.15 (Red Hat)\r\n
    Connection: close\r\n
    ETag: "68161d-198-4f48d4220865c"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.007893000 seconds]
    [Request in frame: 53]
```

Listing 2: HTTP CONDITIONAL GET/RESPONSE Interaction

Q1. 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 , we don’t see an “IF-MODIFIED-SINCE” line in the HTTP GET as we are loading for first time ; so there is no question of modification.

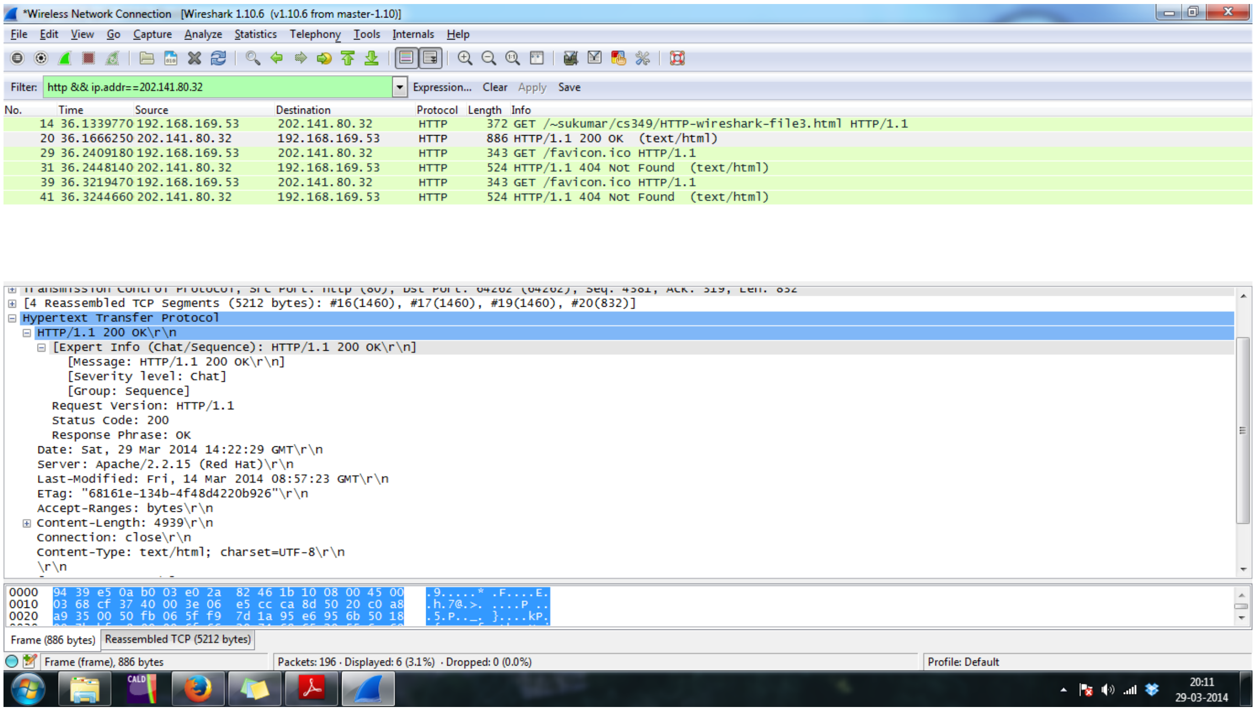
Q2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
Ans: Yes because we can see the contents in the ”Line-based text data” field.

Q3. 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. The information followed is: Fri, 14 Fri 2014 08:57:23 GMT which is the date of the last modification of the file from the previous GET request.

Q4. 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 status code and phrase returned from the server is HTTP/1.1 304 Not Modified. The server didn't explicitly return the contents of the file since the browser loaded it from its cache. (Also , the file was not modified since the first time we requested it)

Retrieving Long Documents



```
Filter: http && ip.addr==202.141.80.32

No.  Time       Source          Destination     Protocol Length Info
  14 36.1339770 192.168.169.53  202.141.80.32   HTTP     372 GET /~sukumar/cs349/HTTP-wireshark-file3.html HTTP/1.1
  20 36.1666250 202.141.80.32   192.168.169.53  HTTP     886 HTTP/1.1 200 OK  (text/html)
  29 36.2409180 192.168.169.53  202.141.80.32   HTTP     343 GET /favicon.ico HTTP/1.1
  31 36.2448140 202.141.80.32   192.168.169.53  HTTP     524 HTTP/1.1 404 Not Found  (text/html)
  39 36.3219470 192.168.169.53  202.141.80.32   HTTP     343 GET /favicon.ico HTTP/1.1
  41 36.3244660 202.141.80.32   192.168.169.53  HTTP     524 HTTP/1.1 404 Not Found  (text/html)
```

```
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 64262 (64262), Seq: 4381, Ack: 319, Len: 832
⊞ [4 Reassembled TCP Segments (5212 bytes): #16(1460), #17(1460), #19(1460), #20(832)]
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 200 OK\r\n
    ⊟ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [Message: HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Sat, 29 Mar 2014 14:22:29 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: "68161e-134b-4f48d4220b926"\r\n
    Accept-Ranges: bytes\r\n
  ⊞ Content-Length: 4939\r\n
    Connection: close\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
```

```
0000  94 39 e5 0a b0 03 e0 2a  82 46 1b 10 08 00 45 00   .9.....* .F....E.
0010  03 68 cf 37 40 00 3e 06  e5 cc ca 8d 50 20 c0 a8   .h.7@.>. ....P ..
0020  a9 35 00 50 fb 06 5f f9  7d 1a 95 e6 95 6b 50 18   .5.P.._. }....kP.
```

Frame (886 bytes) | Reassembled TCP (5212 bytes)

Frame (frame), 886 bytes | Packets: 196 · Displayed: 6 (3.1%) · Dropped: 0 (0.0%) | Profile: Default

*Wireless Network Connection [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
20:11
29-03-2014

Figure 5: response display

```
No.     Time              Source                Destination
    Protocol Length Info
     14 36.133977000    192.168.169.53        202.141.80.32          HTTP
            372     GET /~sukumar/cs349/HTTP-wireshark-file3.html HTTP/1.1

Frame 14: 372 bytes on wire (2976 bits), 372 bytes captured (2976 bits) on
     interface 0
Ethernet II, Src: HonHaiPr_0a:b0:03 (94:39:e5:0a:b0:03), Dst: Universa_46
    :1b:10 (e0:2a:82:46:1b:10)
Internet Protocol Version 4, Src: 192.168.169.53 (192.168.169.53), Dst:
    202.141.80.32 (202.141.80.32)
Transmission Control Protocol, Src Port: 64262 (64262), Dst Port: http
    (80), Seq: 1, Ack: 1, Len: 318
Hypertext Transfer Protocol
     GET /~sukumar/cs349/HTTP-wireshark-file3.html HTTP/1.1\r\n
          [Expert Info (Chat/Sequence): GET /~sukumar/cs349/HTTP-wireshark-
              file3.html HTTP/1.1\r\n]
            [Message: GET /~sukumar/cs349/HTTP-wireshark-file3.html HTTP
               /1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /~sukumar/cs349/HTTP-wireshark-file3.html
        Request Version: HTTP/1.1
     Host: 202.141.80.32\r\n
     User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101
        Firefox/5.0\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-
        file3.html]
     [HTTP request 1/1]
     [Response in frame: 20]

No.     Time           Source                Destination
    Protocol Length Info
     20 36.166625000   202.141.80.32         192.168.169.53        HTTP
            886    HTTP/1.1 200 OK  (text/html)

Frame 20: 886 bytes on wire (7088 bits), 886 bytes captured (7088 bits) on
     interface 0
Ethernet II, Src: Universa_46:1b:10 (e0:2a:82:46:1b:10), Dst: HonHaiPr_0a:
    b0:03 (94:39:e5:0a:b0:03)
Internet Protocol Version 4, Src: 202.141.80.32 (202.141.80.32), Dst:
    192.168.169.53 (192.168.169.53)
Transmission Control Protocol, Src Port: http (80), Dst Port: 64262
    (64262), Seq: 4381, Ack: 319, Len: 832
[4 Reassembled TCP Segments (5212 bytes): #16(1460), #17(1460), #19(1460),
     #20(832)]
Hypertext Transfer Protocol
     HTTP/1.1 200 OK\r\n
          [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [Message: HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
          Request Version: HTTP/1.1
          Status Code: 200
          Response Phrase: OK
     Date: Sat, 29 Mar 2014 14:22:29 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: "68161e-134b-4f48d4220b926"\r\n
     Accept-Ranges: bytes\r\n
     Content-Length: 4939\r\n
          [Content length: 4939]
     Connection: close\r\n
     Content-Type: text/html; charset=UTF-8\r\n
     \r\n
     [HTTP response 1/1]
     [Time since request: 0.032648000 seconds]
     [Request in frame: 14]
Line-based text data: text/html
```

Listing 3: HTTP Retrieving Long Documents

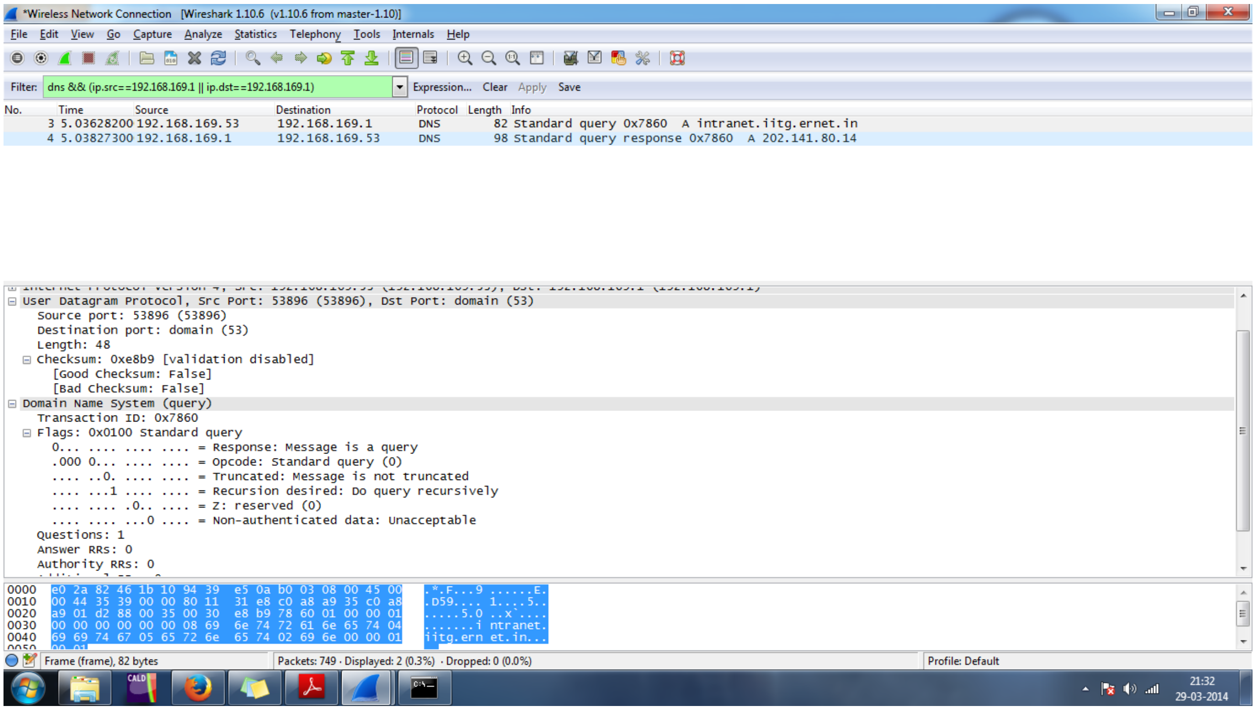
Q1. How many HTTP GET request messages were sent by your browser?
Ans: There was 1 HTTP GET request message sent by my browser.

Q2. How many data-containing TCP segments were needed to carry the single HTTP response?
Ans: There were 4 data containing TCP segments containing 1460 ,1460 ,1460 and 832 bytes respectively for a total of 5212 bytes.

Q3. What is the status code and phrase associated with the response to the HTTP GET request?
Ans: The status code to the response is 200 OK, just like a single packet response.

Q4. Are there any HTTP status lines in the transmitted data associated with a TCP-induced "Continuation"?
Ans: No, the transmitted data of TCP is only the content data. The headers in the GET and OK request are the only two that indicate HTTP status lines.

PARTC: UDP



*Wireless Network Connection [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: dns && (ip.src==192.168.169.1 || ip.dst==192.168.169.1)

```
No.   Time       Source          Destination     Protocol Length Info
    3 5.03628200 192.168.169.53  192.168.169.1   DNS         82 Standard query 0x7860  A intranet.iitg.ernet.in
    4 5.03827300 192.168.169.1   192.168.169.53  DNS         98 Standard query response 0x7860  A 202.141.80.14
```

```
⊟ User Datagram Protocol, Src Port: 53896 (53896), Dst Port: domain (53)
    Source port: 53896 (53896)
    Destination port: domain (53)
    Length: 48
  ⊟ Checksum: 0xe8b9 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
⊟ Domain Name System (query)
    Transaction ID: 0x7860
  ⊟ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
```

```
0000  e0 2a 82 46 1b 10 94 39  e5 0a b0 03 08 00 45 00   .*.F...9 ......E.
0010  00 44 35 39 00 00 80 11  31 e8 c0 a8 a9 35 c0 a8   .D59.... 1....5..
0020  a9 01 d2 88 00 35 00 30  e8 b9 78 60 01 00 00 01   .....5.0 ..x`....
0030  00 00 00 00 00 00 08 69  6e 74 72 61 6e 65 74 04   .......i ntranet.
0040  69 69 74 67 05 65 72 6e  65 74 02 69 6e 00 00 01   iitg.ern et.in...
```

Frame (frame), 82 bytes | Packets: 749 · Displayed: 2 (0.3%) · Dropped: 0 (0.0%) | Profile: Default

Figure 6: UDP segment display

```
No.      Time            Source                  Destination
    Protocol Length Info
      3 5.036282000     192.168.169.53         192.168.169.1          DNS
             82      Standard query 0x7860   A intranet.iitg.ernet.in

Frame 3: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on
    interface 0
Ethernet II, Src: HonHaiPr_0a:b0:03 (94:39:e5:0a:b0:03), Dst: Universa_46
    :1b:10 (e0:2a:82:46:1b:10)
Internet Protocol Version 4, Src: 192.168.169.53 (192.168.169.53), Dst:
    192.168.169.1 (192.168.169.1)
     Version: 4
     Header length: 20 bytes
     Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00:
         Not-ECT (Not ECN-Capable Transport))
     Total Length: 68
     Identification: 0x3539 (13625)
     Flags: 0x00
     Fragment offset: 0
     Time to live: 128
     Protocol: UDP (17)
     Header checksum: 0x31e8 [validation disabled]
     Source: 192.168.169.53 (192.168.169.53)
     Destination: 192.168.169.1 (192.168.169.1)
     [Source GeoIP: Unknown]
     [Destination GeoIP: Unknown]
 User Datagram Protocol, Src Port: 53896 (53896), Dst Port: domain (53)
     Source port: 53896 (53896)
     Destination port: domain (53)
     Length: 48
     Checksum: 0xe8b9 [validation disabled]
         [Good Checksum: False]
         [Bad Checksum: False]
 Domain Name System (query)
     [Response In: 4]
     Transaction ID: 0x7860
     Flags: 0x0100 Standard query
         0... .... .... .... = Response: Message is a query
         .000 0... .... .... = Opcode: Standard query (0)
         .... ..0. .... .... = Truncated: Message is not truncated
         .... ...1 .... .... = Recursion desired: Do query recursively
         .... .... .0.. .... = Z: reserved (0)
         .... .... ...0 .... = Non-authenticated data: Unacceptable
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
     Queries
         intranet.iitg.ernet.in: type A, class IN
             Name: intranet.iitg.ernet.in
             Type: A (Host address)
             Class: IN (0x0001)

 No.     Time           Source                Destination
    Protocol Length Info
       4 5.038273000    192.168.169.1         192.168.169.53        DNS
               98     Standard query response 0x7860  A 202.141.80.14

 Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on
    interface 0
 Ethernet II, Src: Universa_46:1b:10 (e0:2a:82:46:1b:10), Dst: HonHaiPr_0a:
    b0:03 (94:39:e5:0a:b0:03)
 Internet Protocol Version 4, Src: 192.168.169.1 (192.168.169.1), Dst:
    192.168.169.53 (192.168.169.53)
     Version: 4
     Header length: 20 bytes
     Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00:
        Not-ECT (Not ECN-Capable Transport))
     Total Length: 84
     Identification: 0x1508 (5384)
     Flags: 0x00
     Fragment offset: 0
     Time to live: 128
     Protocol: UDP (17)
     Header checksum: 0x5209 [validation disabled]
     Source: 192.168.169.1 (192.168.169.1)
     Destination: 192.168.169.53 (192.168.169.53)
     [Source GeoIP: Unknown]
     [Destination GeoIP: Unknown]
 User Datagram Protocol, Src Port: domain (53), Dst Port: 53896 (53896)
     Source port: domain (53)
     Destination port: 53896 (53896)
     Length: 64
     Checksum: 0x37e8 [validation disabled]
         [Good Checksum: False]
         [Bad Checksum: False]
 Domain Name System (response)
     [Request In: 3]
     [Time: 0.001991000 seconds]
     Transaction ID: 0x7860
     Flags: 0x8580 Standard query response, No error
         1... .... .... .... = Response: Message is a response
         .000 0... .... .... = Opcode: Standard query (0)
         .... .1.. .... .... = Authoritative: Server is an authority for
            domain
         .... ..0. .... .... = Truncated: Message is not truncated
         .... ...1 .... .... = Recursion desired: Do query recursively
         .... .... 1... .... = Recursion available: Server can do recursive
             queries
         .... .... .0.. .... = Z: reserved (0)
         .... .... ..0. .... = Answer authenticated: Answer/authority
            portion was not authenticated by the server
         .... .... ...0 .... = Non-authenticated data: Unacceptable
         .... .... .... 0000 = Reply code: No error (0)
     Questions: 1
     Answer RRs: 1
     Authority RRs: 0
     Additional RRs: 0
     Queries
         intranet.iitg.ernet.in: type A, class IN
             Name: intranet.iitg.ernet.in
             Type: A (Host address)
             Class: IN (0x0001)
     Answers
```

Listing 4: UDP segments display

a. Select one packet. From this packet, determine how many fields there are in the UDP header. Name these fields as they are named in the Wireshark display of segment fields.
Ans: The UDP header contains 4 fields: source port, destination port, length, and checksum.

b. What are the source and destination port numbers, in both decimal and hexadecimal format.
Ans: Source Port : 53896 (0xd288)
Destination Port : 53(0x0035)

c. What is the value in the Length field in both decimal and hexadecimal format. What is the meaning of this value ?
Ans: The value in Length field is 48(0x30)
This value in the Length field defines the total length of user datagram (header plus data)

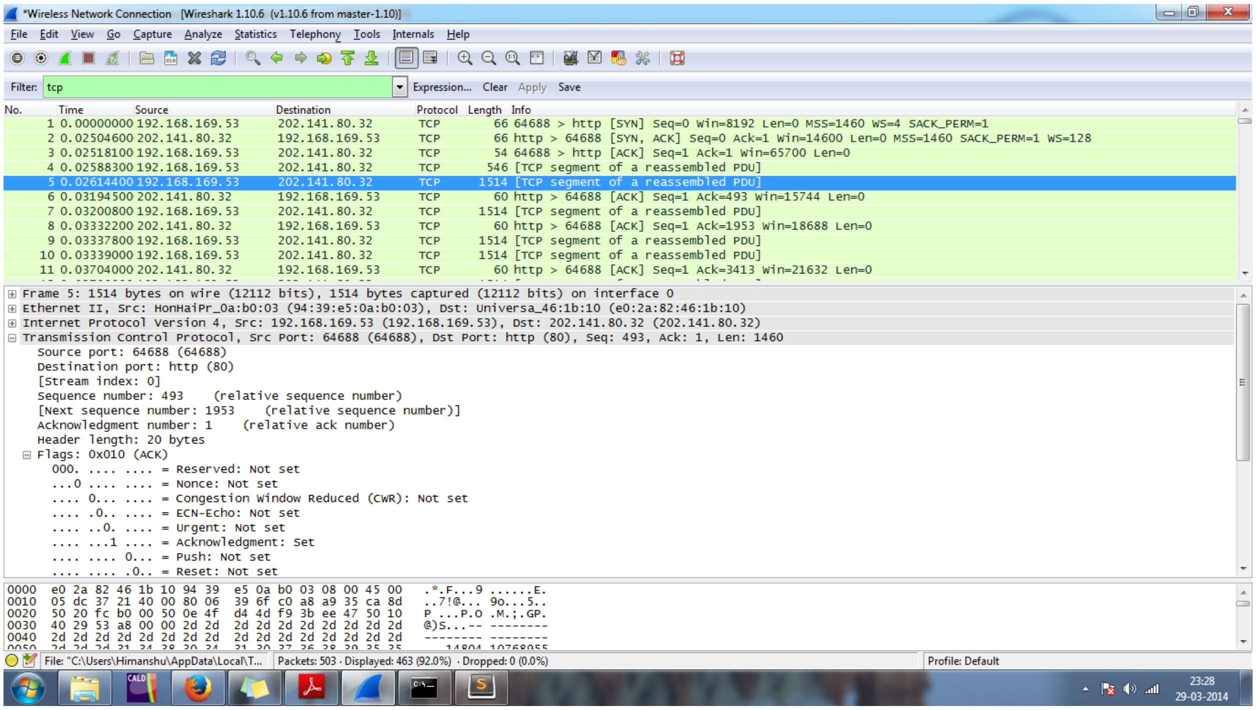
d. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation.

Ans: The protocol number for UDP is 17 (0x11)

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: The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.

PARTD : TCP


*Wireless Network Connection [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp
Expression... Clear Apply Save

```
No.  Time        Source          Destination     Protocol Length Info
  1 0.00000000 192.168.169.53  202.141.80.32   TCP        66 64688 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  2 0.02504600 202.141.80.32   192.168.169.53  TCP        66 http > 64688 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128
  3 0.02518100 192.168.169.53  202.141.80.32   TCP        54 64688 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0
  4 0.02588300 192.168.169.53  202.141.80.32   TCP       546 [TCP segment of a reassembled PDU]
  5 0.02614400 192.168.169.53  202.141.80.32   TCP      1514 [TCP segment of a reassembled PDU]
  6 0.03194500 202.141.80.32   192.168.169.53  TCP        60 http > 64688 [ACK] Seq=1 Ack=493 Win=15744 Len=0
  7 0.03200800 192.168.169.53  202.141.80.32   TCP      1514 [TCP segment of a reassembled PDU]
  8 0.03332200 202.141.80.32   192.168.169.53  TCP        60 http > 64688 [ACK] Seq=1 Ack=1953 Win=18688 Len=0
  9 0.03337800 192.168.169.53  202.141.80.32   TCP      1514 [TCP segment of a reassembled PDU]
 10 0.03339000 192.168.169.53  202.141.80.32   TCP      1514 [TCP segment of a reassembled PDU]
 11 0.03704000 202.141.80.32   192.168.169.53  TCP        60 http > 64688 [ACK] Seq=1 Ack=3413 Win=21632 Len=0
```

```
⊞ Frame 5: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
⊞ Ethernet II, Src: HonHaiPr_0a:b0:03 (94:39:e5:0a:b0:03), Dst: Universa_46:1b:10 (e0:2a:82:46:1b:10)
⊞ Internet Protocol Version 4, Src: 192.168.169.53 (192.168.169.53), Dst: 202.141.80.32 (202.141.80.32)
⊟ Transmission Control Protocol, Src Port: 64688 (64688), Dst Port: http (80), Seq: 493, Ack: 1, Len: 1460
    Source port: 64688 (64688)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 493    (relative sequence number)
    [Next sequence number: 1953    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header length: 20 bytes
  ⊟ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
```

```
0000  e0 2a 82 46 1b 10 94 39  e5 0a b0 03 08 00 45 00   .*.F...9 ......E.
0010  05 dc 37 21 40 00 80 06  39 6f c0 a8 a9 35 ca 8d   ..7!@... 9o...5..
0020  50 20 fc b0 00 50 0e 4f  d4 4d f9 3b ee 47 50 10   P ...P.O .M.;.GP.
0030  40 29 53 a8 00 00 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   @)S...-- --------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
```

```
File: "C:\Users\Himanshu\AppData\Local\T...   Packets: 503 · Displayed: 463 (92.0%) · Dropped: 0 (0.0%)   Profile: Default
```

Figure 7: TCP first few segments

1. Print out a captured packet and indicate where you see the information that answers the following:

a) What is the IP address and TCP port number used by your client computer (source) to transfer the file to 202.141.80.32?

Ans: IP address : 192.168.169.53
Port number : 64688

b) What is the IP address and TCP port number used by the server?

IP address : 202.141.0.32
Port number : 80 (http)

2. Print out a captured packet and indicate where you see the information that answers the following:

```
No.     Time           Source                Destination
   Protocol Length Info
      1 0.000000000    192.168.169.53        202.141.80.32         TCP
              66     64688 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
          SACK_PERM=1

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on
   interface 0
Ethernet II, Src: HonHaiPr_0a:b0:03 (94:39:e5:0a:b0:03), Dst: Universa_46
   :1b:10 (e0:2a:82:46:1b:10)
Internet Protocol Version 4, Src: 192.168.169.53 (192.168.169.53), Dst:
   202.141.80.32 (202.141.80.32)
Transmission Control Protocol, Src Port: 64688 (64688), Dst Port: http
   (80), Seq: 0, Len: 0
    Source port: 64688 (64688)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 0    (relative sequence number)
    Header length: 32 bytes
    Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
    Window size value: 8192
    [Calculated window size: 8192]
    Checksum: 0xecd9 [validation disabled]
    Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window
       scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
```

Listing 5: TCP SYN segment

a) What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and 202.141.80.32?
Ans: Sequence number of the TCP SYN segment is used to initiate the TCP connection between the client computer and 202.141.0.32. The value is 0 in this trace.

b) What is it in the segment that identifies the segment as a SYN segment?
Ans: The SYN flag is set to 1 and it indicates that this segment is a SYN segment.

3. Print out a captured packet and indicate where you see the information that answers the following:

```
No.     Time           Source                Destination
   Protocol Length Info
      2 0.025046000    202.141.80.32         192.168.169.53        TCP
             66     http > 64688 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0
         MSS=1460 SACK_PERM=1 WS=128

Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on
   interface 0
Ethernet II, Src: Universa_46:1b:10 (e0:2a:82:46:1b:10), Dst: HonHaiPr_0a:
   b0:03 (94:39:e5:0a:b0:03)
Internet Protocol Version 4, Src: 202.141.80.32 (202.141.80.32), Dst:
   192.168.169.53 (192.168.169.53)
Transmission Control Protocol, Src Port: http (80), Dst Port: 64688
   (64688), Seq: 0, Ack: 1, Len: 0
    Source port: http (80)
    Destination port: 64688 (64688)
    [Stream index: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header length: 32 bytes
    Flags: 0x012 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
    Window size value: 14600
    [Calculated window size: 14600]
    Checksum: 0xec38 [validation disabled]
    Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-
       Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
    [SEQ/ACK analysis]
```

Listing 6: TCP SYNACK segment

a) What is the sequence number of the SYNACK segment sent by 202.141.80.32 to the client computer in reply to the SYN?
Ans: Sequence number of the SYNACK segment from 202.141.80.32 to the client computer in reply to the SYN has the value of 0 in this trace.

b) What is the value of the ACKnowledgement field in the SYNACK segment?
Ans: The value of the ACKnowledgement field in the SYNACK segment is 1.

c) How did 202.141.80.32 server determine that value?

Ans: The value of the ACKnowledgement field in the SYNACK segment is determined by 202.141.80.32 by adding 1 to the initial sequence number of SYN segment from the client computer (i.e. the sequence number of the SYN segment initiated by the client computer is 0).

d) What is it in the segment that identifies the segment as a SYNACK segment?
Ans: The SYN flag and Acknowledgement flag in the segment are set to 1 and they indicate that this segment is a SYNACK segment.

4. Print out a captured packet and indicate where you see the information that answers the following:

```
No.     Time           Source                Destination
   Protocol Length Info
      1 0.000000000    192.168.169.53        202.141.80.32          TCP
             66     64688 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
          SACK_PERM=1

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on
   interface 0
Ethernet II, Src: HonHaiPr_0a:b0:03 (94:39:e5:0a:b0:03), Dst: Universa_46
   :1b:10 (e0:2a:82:46:1b:10)
Internet Protocol Version 4, Src: 192.168.169.53 (192.168.169.53), Dst:
   202.141.80.32 (202.141.80.32)
Transmission Control Protocol, Src Port: 64688 (64688), Dst Port: http
   (80), Seq: 0, Len: 0
    Source port: 64688 (64688)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 0    (relative sequence number)
    Header length: 32 bytes
    Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
            [Expert Info (Chat/Sequence): Connection establish request (
               SYN): server port http]
                [Message: Connection establish request (SYN): server port
                   http]
                [Severity level: Chat]
                [Group: Sequence]
        .... .... ...0 = Fin: Not set
    Window size value: 8192
    [Calculated window size: 8192]
    Checksum: 0xecd9 [validation disabled]
        [Good Checksum: False]
        [Bad Checksum: False]
    Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window
       scale, No-Operation (NOP), No-Operation (NOP), SACK permitted

No.     Time           Source                Destination
   Protocol Length Info
      2 0.025046000    202.141.80.32         192.168.169.53        TCP
              66     http > 64688 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0
         MSS=1460 SACK_PERM=1 WS=128

Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on
   interface 0
Ethernet II, Src: Universa_46:1b:10 (e0:2a:82:46:1b:10), Dst: HonHaiPr_0a:
   b0:03 (94:39:e5:0a:b0:03)
Internet Protocol Version 4, Src: 202.141.80.32 (202.141.80.32), Dst:
   192.168.169.53 (192.168.169.53)
Transmission Control Protocol, Src Port: http (80), Dst Port: 64688
   (64688), Seq: 0, Ack: 1, Len: 0
    Source port: http (80)
    Destination port: 64688 (64688)
    [Stream index: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header length: 32 bytes
    Flags: 0x012 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
            [Expert Info (Chat/Sequence): Connection establish acknowledge
                (SYN+ACK): server port http]
                [Message: Connection establish acknowledge (SYN+ACK):
                   server port http]
                [Severity level: Chat]
                [Group: Sequence]
        .... .... ...0 = Fin: Not set
    Window size value: 14600
    [Calculated window size: 14600]
    Checksum: 0xec38 [validation disabled]
        [Good Checksum: False]
        [Bad Checksum: False]
    Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-
       Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
    [SEQ/ACK analysis]
        [This is an ACK to the segment in frame: 1]
        [The RTT to ACK the segment was: 0.025046000 seconds]

No.     Time           Source                Destination
   Protocol Length Info
      3 0.025181000    192.168.169.53        202.141.80.32         TCP
```

```
              54     64688 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0

Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on
   interface 0
Ethernet II, Src: HonHaiPr_0a:b0:03 (94:39:e5:0a:b0:03), Dst: Universa_46
   :1b:10 (e0:2a:82:46:1b:10)
Internet Protocol Version 4, Src: 192.168.169.53 (192.168.169.53), Dst:
   202.141.80.32 (202.141.80.32)
Transmission Control Protocol, Src Port: 64688 (64688), Dst Port: http
   (80), Seq: 1, Ack: 1, Len: 0
    Source port: 64688 (64688)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header length: 20 bytes
    Flags: 0x010 (ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
    Window size value: 16425
    [Calculated window size: 65700]
    [Window size scaling factor: 4]
    Checksum: 0x25ea [validation disabled]
        [Good Checksum: False]
        [Bad Checksum: False]
    [SEQ/ACK analysis]
        [This is an ACK to the segment in frame: 2]
        [The RTT to ACK the segment was: 0.000135000 seconds]

No.     Time           Source                Destination
   Protocol Length Info
      4 0.025883000    192.168.169.53        202.141.80.32         TCP
              546    [TCP segment of a reassembled PDU]

Frame 4: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on
   interface 0
Ethernet II, Src: HonHaiPr_0a:b0:03 (94:39:e5:0a:b0:03), Dst: Universa_46
   :1b:10 (e0:2a:82:46:1b:10)
Internet Protocol Version 4, Src: 192.168.169.53 (192.168.169.53), Dst:
   202.141.80.32 (202.141.80.32)
Transmission Control Protocol, Src Port: 64688 (64688), Dst Port: http
   (80), Seq: 1, Ack: 1, Len: 492
    Source port: 64688 (64688)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 493    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header length: 20 bytes
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
    Window size value: 16425
    [Calculated window size: 65700]
    [Window size scaling factor: 4]
    Checksum: 0xd9c5 [validation disabled]
        [Good Checksum: False]
        [Bad Checksum: False]
    [SEQ/ACK analysis]
        [Bytes in flight: 492]
    TCP segment data (492 bytes)

No.     Time           Source                Destination
   Protocol Length Info
      5 0.026144000    192.168.169.53        202.141.80.32         TCP
              1514   [TCP segment of a reassembled PDU]

Frame 5: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
    on interface 0
Ethernet II, Src: HonHaiPr_0a:b0:03 (94:39:e5:0a:b0:03), Dst: Universa_46
   :1b:10 (e0:2a:82:46:1b:10)
Internet Protocol Version 4, Src: 192.168.169.53 (192.168.169.53), Dst:
   202.141.80.32 (202.141.80.32)
Transmission Control Protocol, Src Port: 64688 (64688), Dst Port: http
   (80), Seq: 493, Ack: 1, Len: 1460
    Source port: 64688 (64688)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 493    (relative sequence number)
    [Next sequence number: 1953    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header length: 20 bytes
    Flags: 0x010 (ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
    Window size value: 16425
    [Calculated window size: 65700]
    [Window size scaling factor: 4]
    Checksum: 0x53a8 [validation disabled]
        [Good Checksum: False]
        [Bad Checksum: False]
    [SEQ/ACK analysis]
        [Bytes in flight: 1952]
    [Reassembled PDU in frame: 454]
    TCP segment data (1460 bytes)

No.     Time           Source                Destination
   Protocol Length Info
      6 0.031945000    202.141.80.32         192.168.169.53        TCP
              60     http > 64688 [ACK] Seq=1 Ack=493 Win=15744 Len=0

Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on
   interface 0
Ethernet II, Src: Universa_46:1b:10 (e0:2a:82:46:1b:10), Dst: HonHaiPr_0a:
   b0:03 (94:39:e5:0a:b0:03)
Internet Protocol Version 4, Src: 202.141.80.32 (202.141.80.32), Dst:
   192.168.169.53 (192.168.169.53)
Transmission Control Protocol, Src Port: http (80), Dst Port: 64688
   (64688), Seq: 1, Ack: 493, Len: 0
    Source port: http (80)
    Destination port: 64688 (64688)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 493    (relative ack number)
    Header length: 20 bytes
    Flags: 0x010 (ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
    Window size value: 123
    [Calculated window size: 15744]
    [Window size scaling factor: 128]
    Checksum: 0x63ac [validation disabled]
        [Good Checksum: False]
        [Bad Checksum: False]
    [SEQ/ACK analysis]
        [This is an ACK to the segment in frame: 4]
        [The RTT to ACK the segment was: 0.006062000 seconds]
```

Listing 7: TCP first six segments

What is the sequence number of the TCP segment containing the HTTP POST command?
Ans : Segment Number 4 is the TCP segment containing the HTTP POST command. The sequence number of this segment has the value of 1.

Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection.

a) 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?
Ans: The HTTP POST segment is considered as the first segment. The Segments 1 to 6 are Frame No. 4, 5, 7, 9, 10, and 12 in this trace respectively. The sequence numbers along with the time are tabulated below:

Segment no	Frame no.	Sequence no.(Bytes)	Sent time
1	4	1	0.025883
2	5	493	0.02644
3	7	1953	0.032008
4	9	3413	0.033378
5	10	4873	0.03339
6	12	6333	0.037099

b) When was the ACK for each segment received?
Ans: The ACKs of segments 1 – 6 are No. 6, 8, 11, 14, 17, and 20 in this trace. Therefore , the corresponding values when they are received are tabulated below :

Segment no	Frame no.	Ack recvd time
1	6	0.031945
2	8	0.033322
3	11	0.037040
4	14	0.044923
5	17	0.045843
6	20	0.046547

c) Do you see evidence of the use of cumulative ACKs in your trace? Explain.
Ans: Yes we see evidence of the use of cumulative ACKs in our trace. After the server sends an Ack for segment in frame 12, we receive 3 duplicate Acks for the next frame. Since the TCP follows faster retransmission mechanism so, my host sends the frame number 13 again. After receiving frame no. 13 , server directly sends an ACK for the segment in frame 16. Therefore , without acknowledging 13,14,15 it acknowledges the frame no. 16 and hence follow cumulative Acks.

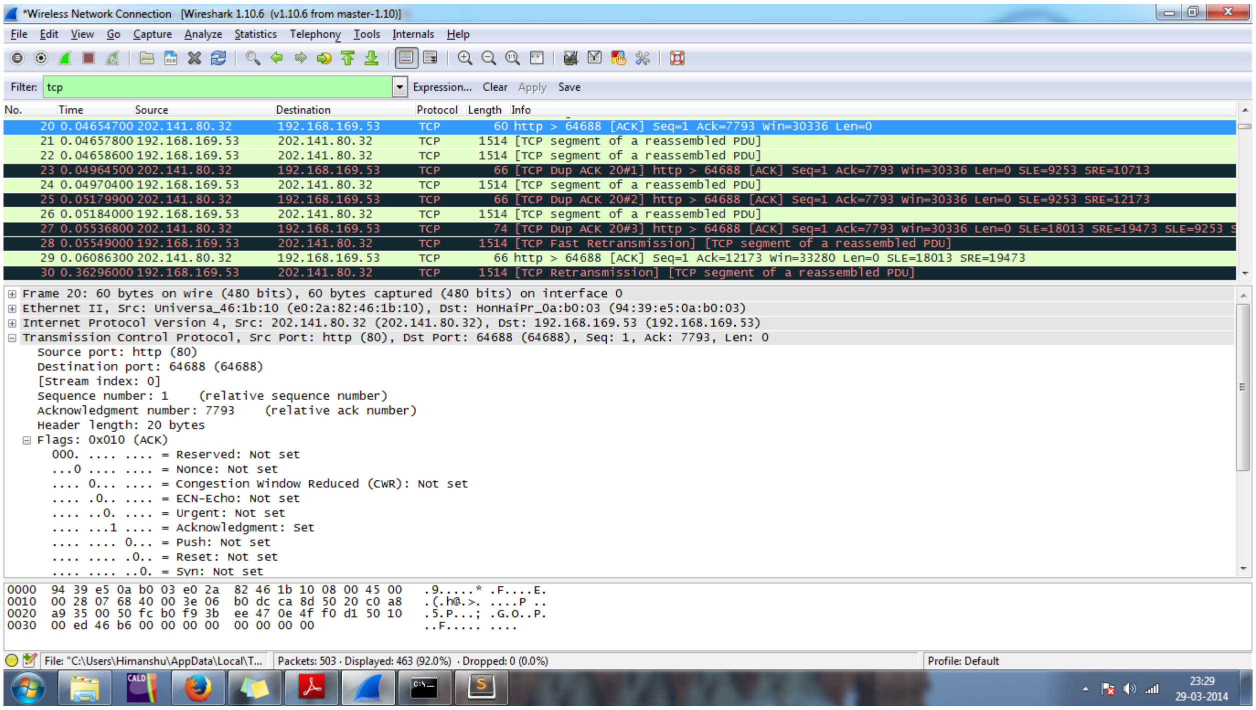
d) Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments?
Ans: The response time for each of them are tabulated below:

Sent time	Received time	RTT time
0.025883	0.031945	0.006062
0.02644	0.033322	0.007178
0.032008	0.037040	0.005032
0.033378	0.044923	0.011545
0.03339	0.045843	0.012453
0.037099	0.046547	0.009448

e) What is the length of each of the first six TCP segments?
Ans: Length of the first TCP segment (containing the HTTP POST): 446 bytes Length of each of the other five TCP segments: 1514 bytes (MSS)

f) What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?
Ans: The minimum amount of buffer space (receiver window) advertised at receiver for the entire trace is 14600 bytes, which shows in the first acknowledgement from the server. This receiver window grows steadily to 15744 for segment 6, 18688 for segment 8 and so on. The maximum window size the server advertises is 139136. Since at each packet acknowledgement server advertises more and more window size, the sender is never throttled.

g) Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question? How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment? Explain.


*Wireless Network Connection [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
23:29
29-03-2014

Filter: tcp

```
No.  Time        Source          Destination     Protocol Length Info
  20 0.04654700 202.141.80.32   192.168.169.53  TCP        60 http > 64688 [ACK] Seq=1 Ack=7793 Win=30336 Len=0
  21 0.04657800 192.168.169.53  202.141.80.32   TCP      1514 [TCP segment of a reassembled PDU]
  22 0.04658600 192.168.169.53  202.141.80.32   TCP      1514 [TCP segment of a reassembled PDU]
  23 0.04964500 202.141.80.32   192.168.169.53  TCP        66 [TCP Dup ACK 20#1] http > 64688 [ACK] Seq=1 Ack=7793 Win=30336 Len=0 SLE=9253 SRE=10713
  24 0.04970400 192.168.169.53  202.141.80.32   TCP      1514 [TCP segment of a reassembled PDU]
  25 0.05179900 202.141.80.32   192.168.169.53  TCP        66 [TCP Dup ACK 20#2] http > 64688 [ACK] Seq=1 Ack=7793 Win=30336 Len=0 SLE=9253 SRE=12173
  26 0.05184000 192.168.169.53  202.141.80.32   TCP      1514 [TCP segment of a reassembled PDU]
  27 0.05536800 202.141.80.32   192.168.169.53  TCP        74 [TCP Dup ACK 20#3] http > 64688 [ACK] Seq=1 Ack=7793 Win=30336 Len=0 SLE=18013 SRE=19473 SLE=9253 S
  28 0.05549000 192.168.169.53  202.141.80.32   TCP      1514 [TCP Fast Retransmission] [TCP segment of a reassembled PDU]
  29 0.06086300 202.141.80.32   192.168.169.53  TCP        66 http > 64688 [ACK] Seq=1 Ack=12173 Win=33280 Len=0 SLE=18013 SRE=19473
  30 0.36296000 192.168.169.53  202.141.80.32   TCP      1514 [TCP Retransmission] [TCP segment of a reassembled PDU]
```

```
⊞ Frame 20: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: Universa_46:1b:10 (e0:2a:82:46:1b:10), Dst: HonHaiPr_0a:b0:03 (94:39:e5:0a:b0:03)
⊞ Internet Protocol Version 4, Src: 202.141.80.32 (202.141.80.32), Dst: 192.168.169.53 (192.168.169.53)
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 64688 (64688), Seq: 1, Ack: 7793, Len: 0
    Source port: http (80)
    Destination port: 64688 (64688)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 7793    (relative ack number)
    Header length: 20 bytes
  ⊟ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
```

```
0000  94 39 e5 0a b0 03 e0 2a  82 46 1b 10 08 00 45 00   .9.....* .F....E.
0010  00 28 07 68 40 00 3e 06  b0 dc ca 8d 50 20 c0 a8   .(.h@.>. ....P ..
0020  a9 35 00 50 fc b0 f9 3b  ee 47 0e 4f f0 d1 50 10   .5.P...; .G.O..P.
0030  00 ed 46 b6 00 00 00 00  00 00 00 00               ..F..... ....
```

File: "C:\Users\Himanshu\AppData\Local\T... Packets: 503 · Displayed: 463 (92.0%) · Dropped: 0 (0.0%) Profile: Default

Figure 8: TCP first few segments

Ans: Yes, there are retransmitted packets in the trace file. We check for TCP Fast Retransmission Packet. Since, after receiving 3 Duplicate Acks, TCP retransmit the packet, I have to search for 3 Duplicate Acks or retransmitted packets. Frame no. 28 is a fast retransmission packet in our output.

Ack Segment no.	Ack Sequence no.	Acknowledged Data
1	493	493
2	1953	1460
3	3413	1460
4	4873	1460
5	6333	1460
6	7793	1460
7	7793	0
8	7793	0
9	7793	0
10	12173	4380
11	13633	1460

From the above table it is clear that receiver typically acknowledges 1460 bytes of data. In my case, receiver is never ACKing every other segment. From the above table, after fast retransmission, receiver ACKs $3 * 1460 = 4380$ *bytes of data together and I searched through the whole file to find 2*1460=2920 bytes of data but I was not able to find it. From the above table receiver directly ACKS 4380 bytes of data due to cumulative ACK.*