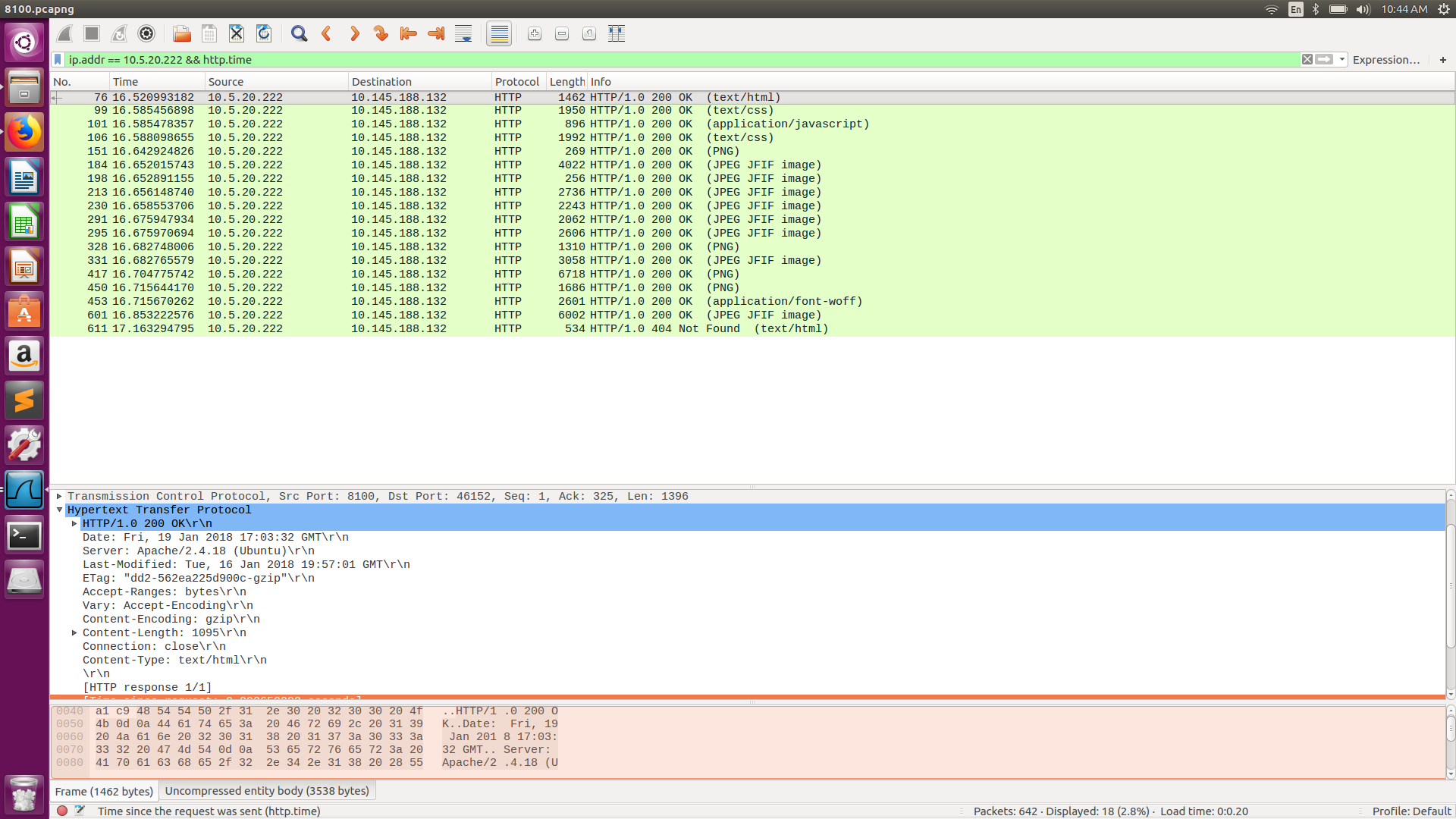
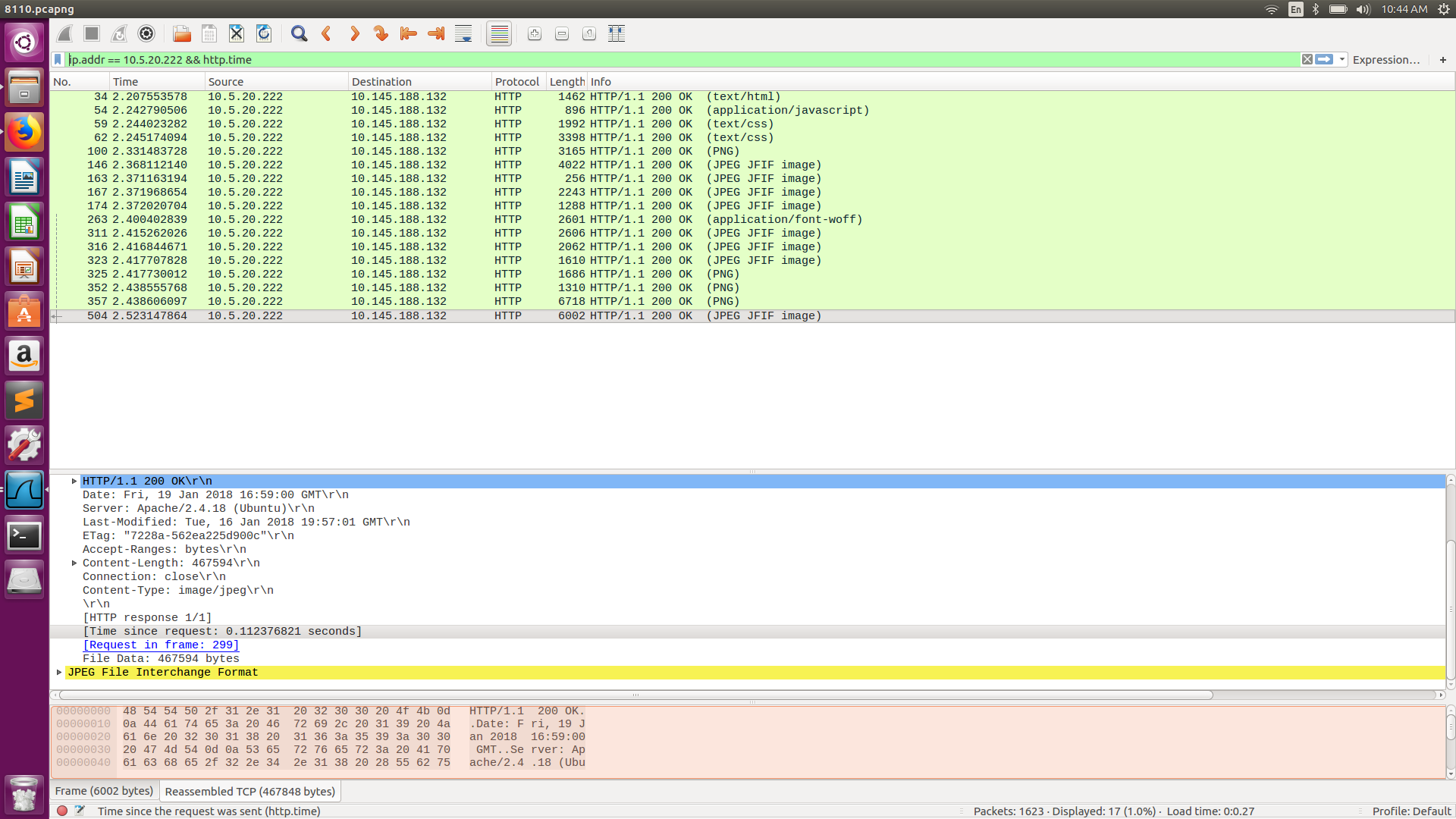
**NETWORKS LAB ASSIGNMENT 2 (15CS30042 and 15CS30008)**

**HTTP Server**

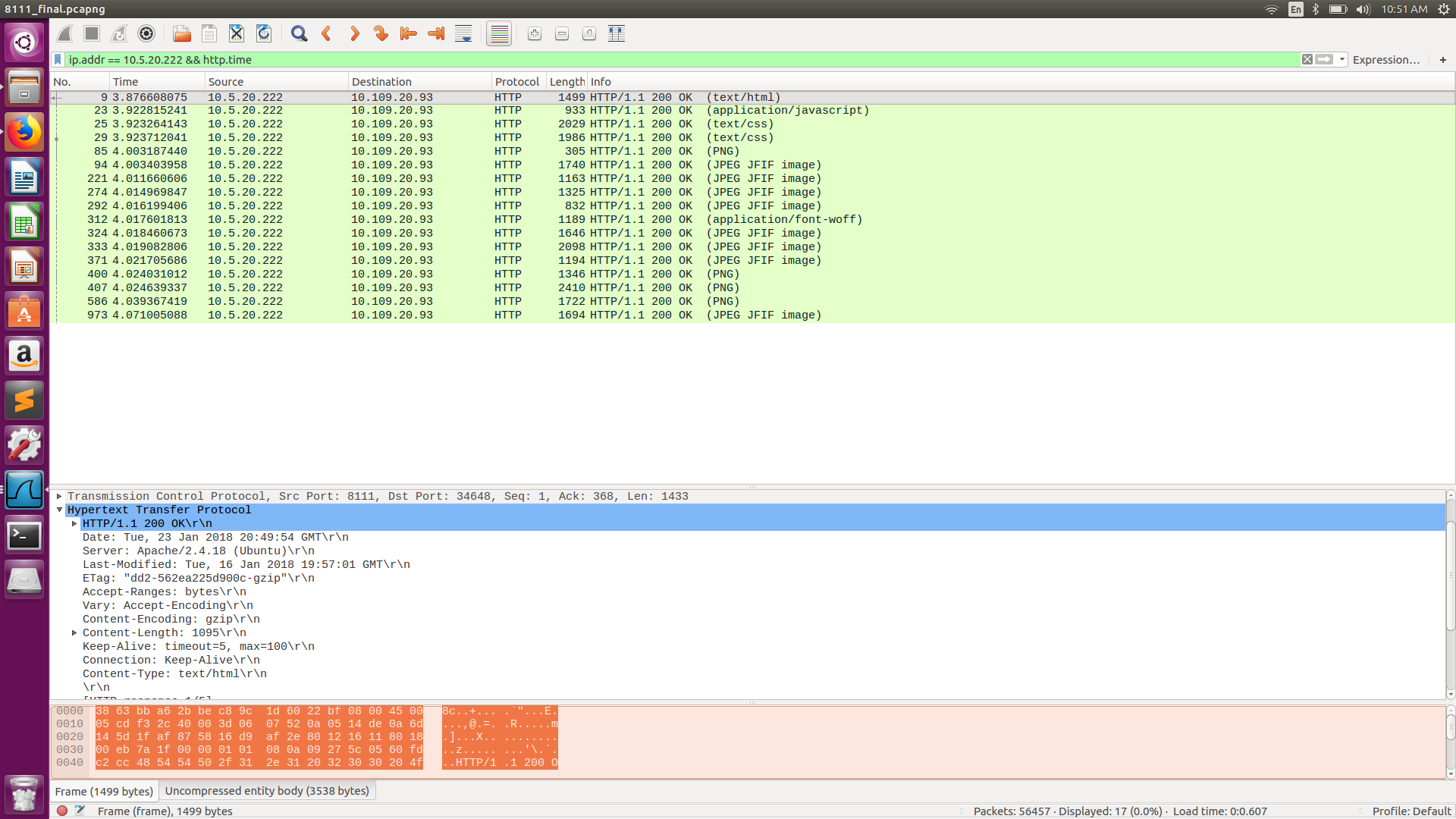
1. 8100 case



8110 case



8111 case



* 1. Analysis
     1. At port 8111.
        1. Steps : Open <http://10.5.20.222:8111> in a browser and track the packets in wireshark after applying filter. Analyse the HTTP Headers to know about the protocol used. Analyse the sequence of the TCP packets.
        2. Observation : A web server with IP 10.5.20.222 is running HTTP 1.1 protocol on 8111 port. Keep Alive is on. Persistent connection.
        3. Justification : The message sent from server has the HTTP header with protocol version 1.1 and Connection: keep alive.
        4. Other Observations : The browser has an optimization technique that makes parallel connections for faster retrieval of packets from the server. This is observed from the fact that there are SYN requests(TCP connection 3-way handshakes) even before the previous connection finished.
     2. At port 8110.
        1. Steps : Open <http://10.5.20.222:8110> in a browser and track the packets in wireshark after applying filter. Analyse the HTTP Headers to know about the protocol used. Analyse the sequence of the TCP packets.
        2. Observation : A web server with IP 10.5.20.222 is running HTTP 1.1 protocol on 8110 port. Non Persistent connection.
        3. Justification : The message sent from server has the HTTP header with protocol version 1.1 and Connection: close and pattern of TCP packets.
     3. At port 8100.
        1. Steps : Open [http://10.5.20.222:8100](http://10.5.20.222:8110) in a browser and track the packets in wireshark after applying filter. Analyse the HTTP Headers to know about the protocol used. Analyse the sequence of the TCP packets.
        2. Observation : A web server with IP 10.5.20.222 is running HTTP 1.0 protocol on 8100 port.
        3. The message sent from server has the HTTP header with protocol version 1.0.

General observation in all 3 cases: The get request is made by the browser to the best available HTTP, that is HTTP 1.1 with keep alive on, but the server may restrict the protocol to the version implemented in it.

* 1. Ans

8111,8110,8100

* + - 1. Steps : Open <http://10.5.20.222:8111>/<http://10.5.20.222:8110>/<http://10.5.20.222:8100> with cache off and use wireshark with filters ‘ip.src == 10.109.20.93 && ip.dst == 10.5.20.222 && http’ to monitor the HTTP GET requests sent.
      2. Observation: 17 HTTP GET requests are sent.
      3. Justification: There are only 16 URI in the HTML page. So total 17 requests.
  1. Ans

Step :

1. Steps: Open <http://10.5.20.222:8111>/ <http://10.5.20.222:8110>/ <http://10.5.20.222:8100> with cache off and use wireshark with filters ‘ip.src == 10.109.20.93 && ip.dst == 10.5.20.222 && http’ to monitor the HTTP GET requests sent.
2. HTTP GET Requests and the corresponding OK Response from the server and check the response time in the HTTP Header.
3. Justification: Difference between GET request and the corresponding response is shown in the HTTP Header named response time.
   * 1. 8111

|  |  |
| --- | --- |
| text/html | 0.001614226 |
| /css/style.css | 0.002675759 |
| /css/mobile.css | 0.001629051 |
| /js/mobile.js | 0.001151157 |
| /images/logo.png | 0.003543476 |
| /images/satellite.png | 0.039426158 |
| /images/project-image1.jpg | 0.003321640 |
| /images/project-image2.jpg | 0.010861050 |
| /images/project-image3.jpg | 0.012237937 |
| /fonts/audiowide-regular-webfont.woff | 0.014348860 |
| /images/project-image4.jpg | 0.012906402 |
| /images/mars-rover.jpg | 0.015027203 |
| /images/finding-planet.jpg | 0.007368466 |
| /images/new-satellitedish.jpg | 0.006672797 |
| /images/bg-home.jpg | 0.054747969 |
| /images/bg-transparent1.png | 0.006377572 |
| /images/icons.png | 0.006120459 |

* + 1. 8110

|  |  |
| --- | --- |
| text/html | 0.009057032 |
| /css/style.css | 0.002382261 |
| /css/mobile.css | 0.003628556 |
| /js/mobile.js | 0.004809953 |
| /images/logo.png | 0.012799586 |
| /images/satellite.png | 0.049299207 |
| /images/project-image1.jpg | 0.052389374 |
| /images/project-image2.jpg | 0.053105719 |
| /images/project-image3.jpg | 0.053181410 |
| /fonts/audiowide-regular-webfont.woff | 0.027874171 |
| /images/project-image4.jpg | 0.018192335 |
| /images/mars-rover.jpg | 0.019932390 |
| /images/finding-planet.jpg | 0.039684798 |
| /images/new-satellitedish.jpg | 0.099012382 |
| /images/bg-home.jpg | 0.007449633 |
| /images/bg-transparent1.png | 0.007447694 |
| /images/icons.png | 0.112376821 |

Iii. 8100

|  |  |
| --- | --- |
| text/html | 0.002650282 |
| /css/style.css | 0.004701859 |
| /css/mobile.css | 0.002808952 |
| /js/mobile.js | 0.005477081 |
| /images/logo.png | 0.007117340 |
| /images/satellite.png | 0.015462930 |
| /images/project-image1.jpg | 0.016361396 |
| /images/project-image2.jpg | 0.019291333 |
| /images/project-image3.jpg | 0.021653907 |
| /fonts/audiowide-regular-webfont.woff | 0.013268016 |
| /images/project-image4.jpg | 0.013252207 |
| /images/mars-rover.jpg | 0.010296789 |
| /images/finding-planet.jpg | 0.026491425 |
| /images/new-satellitedish.jpg | 0.012651072 |
| /images/bg-home.jpg | 0.079174865 |
| /images/bg-transparent1.png | 0.026627512 |
| /images/icons.png | 0.180830317 |

* 1. Page download time in port 8111 case = 0.19601

Page download time in port 8110 case = 0.32465

Page download time in port 8100 case = 0.644952

* 1. Server : Apache/2.4.18 (Ubuntu) , Client Browser : Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:57.0) Gecko/20100101 Firefox/57.0

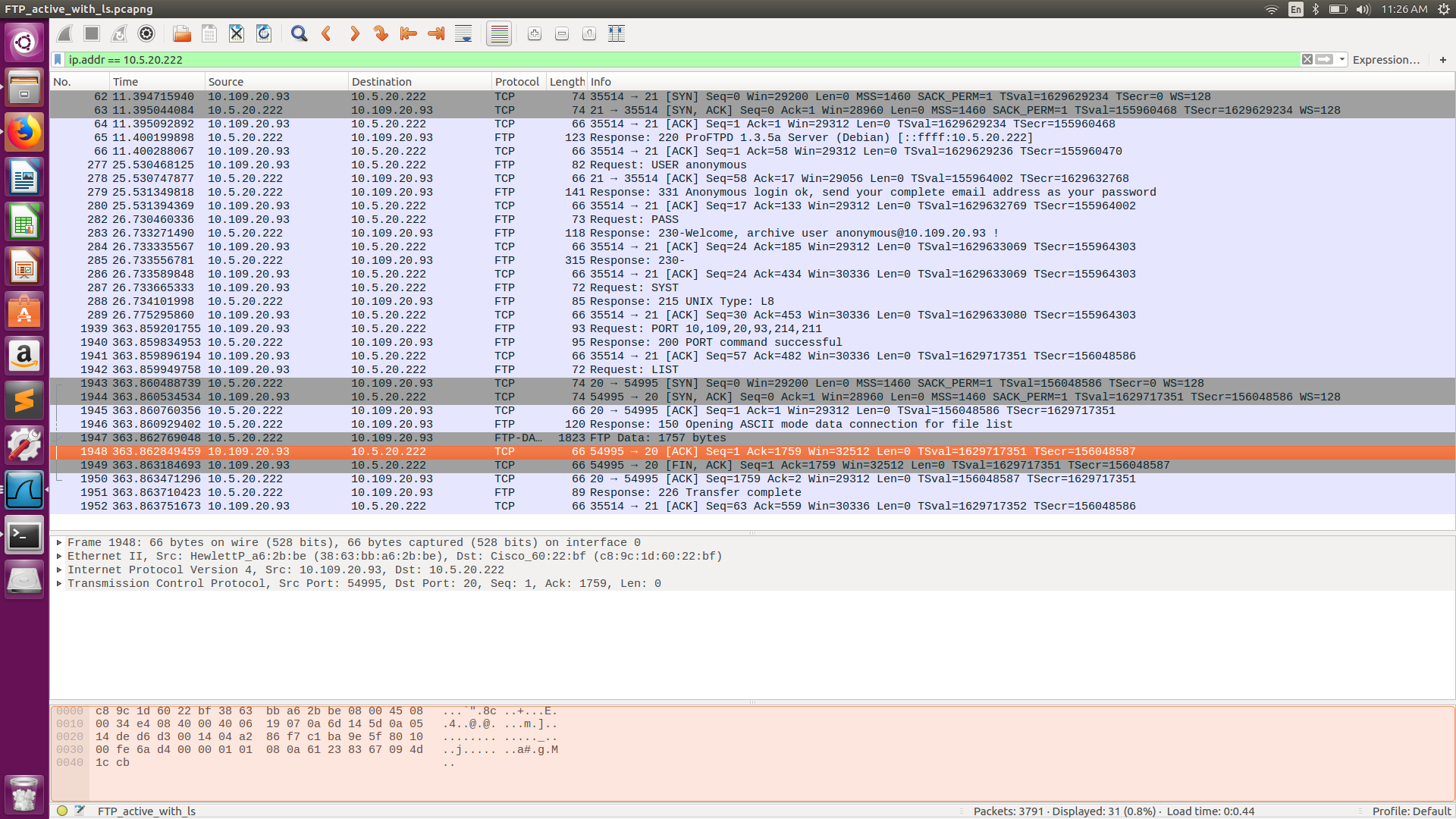
1. Ans

Steps : As mentioned in the question.

Observations:

* 1. FTP analysis :

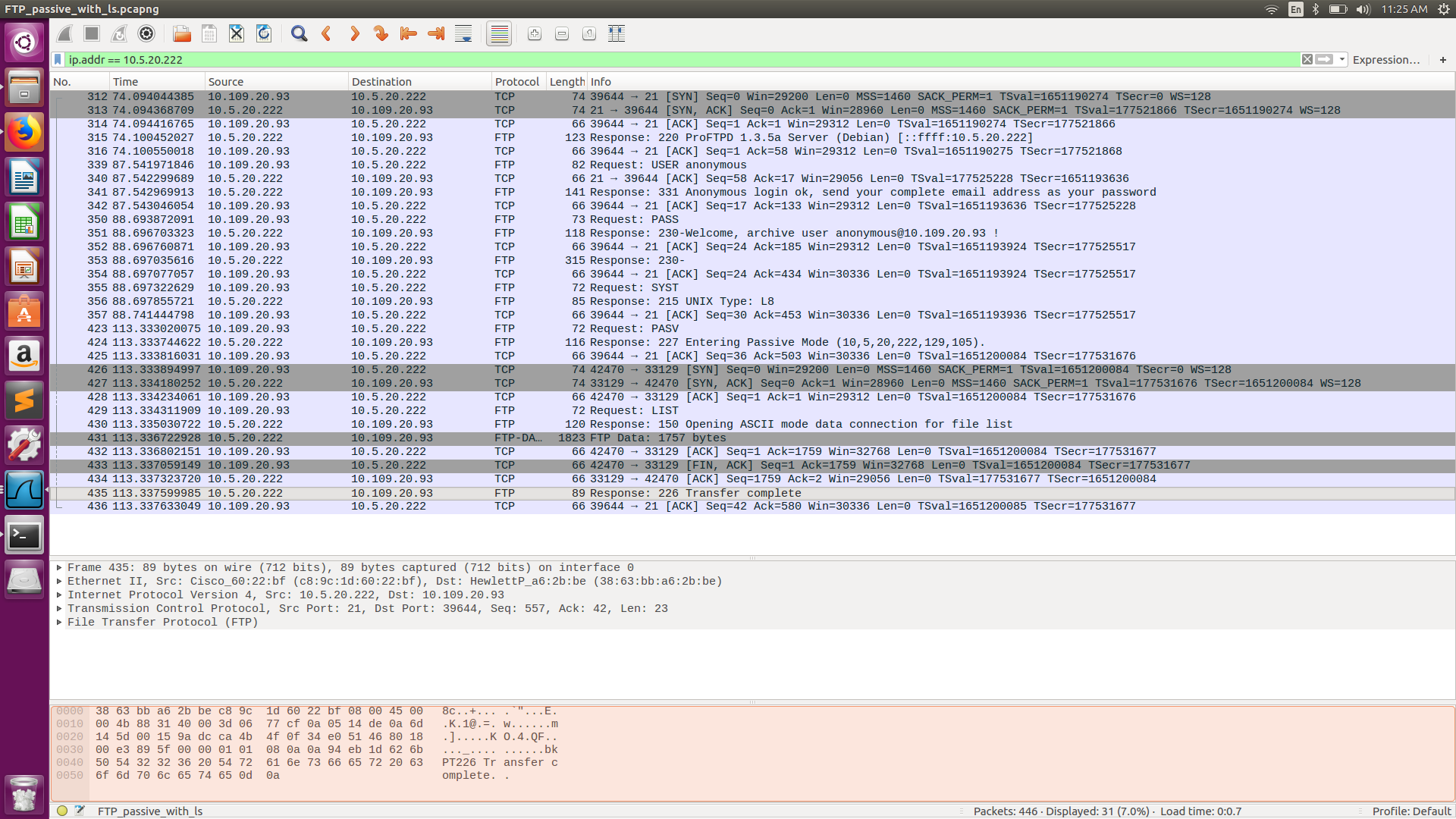
* + 1. Active :



* + - 1. TCP handshake with port 21 of server and client side port 35514(could be any port).

All the below messages are communicated between port 35514 of client with IP 10.109.20.93 and server 10.5.20.222 to port 21 **unless otherwise mentioned.**

* + - 1. Server sends from port 21, Response code 220 (Server ready for new user) along with Response arguments ‘ProFTPD 1.3.5a Server (Debian) [::ffff:10.5.20.222]’. Client sends a acknowledge TCP packet to port 21 of server.
      2. Client sends a Request Command : USER with arguments : anonymous. The server acknowledges this with TCP packet. After which server sends Response code 331 (Username ok need password) with Response args ‘Anonymous login ok, send your complete email address as your password’. Client sends acknowledgement to this using a TCP packet.
      3. Client sends a PASS request to the server and the server sends response with Response code 230 (User logged in , proceed) with response args ‘Welcome, archive user anonymous@10.109.20.93 !’. Client acknowledges this with TCP packet.
      4. Server sends response with Response code 230 (User logged in , proceed) with response args ‘Welcome, archive user anonymous@10.109.20.93 ! The local time is: Tue Jan 23 23:29:14 2018 This is an experimental FTP server. If you have any unusual problems,230-please report them via e-mail to <root@localhost>.Anonymous access granted, restrictions apply’. The client acknowledges this with a TCP packet.
      5. Client sends a SYST request. Server sends Response Code 215(Name System type) with Response args ‘UNIX Type: L8’. Client sends acknowledge TCP packet.
      6. Client sends a Request command ‘PORT’ to server with client ip and newly opened port ‘54995’ and Request arguments ‘10,109,20,93,214,211’ . Server sends response code 200(Command okay) with response args ‘PORT command successful’. Client sends acknowledge TCP packet.
      7. The client sends a Request command ‘LIST’ to server to port 21 from port 35514.
      8. **A TCP handshake between port 20 of server and port 54995 of client happens(Corresponding to the initiation of data channel by the remote server).**
      9. Server sends Response code 150 (File status okay; about to open data connection) with Response args ‘Opening ASCII mode data connection for file list’ from port 21 to port 35514.
      10. Server sends FTP data from port 20 to client port 54995.
      11. Server and client does a TCP handshake to close the pipe between client port 54995 and server port 20.
      12. Server sends a Response Code 226 (Closing data connection) with Response args ‘Transfer complete’ from port 21 to port 35514 which is acknowledged by the client.
    1. Passive:



* + - 1. TCP handshake with port 21 of server and client side port 39644(could be any port).

All the below messages are communicated between port 39644 of client with IP 10.109.20.93 and server 10.5.20.222 to port 21 **unless otherwise mentioned.**

* + - 1. Server sends from port 21, Response code 220 (Server ready for new user) along with Response arguments ‘ProFTPD 1.3.5a Server (Debian) [::ffff:10.5.20.222]’. Client sends a acknowledge TCP packet to port 21 of server.
      2. Client sends a Request Command : USER with arguments : anonymous. The server acknowledges this with TCP packet. After which server sends Response code 331 (Username ok need password) with Response args ‘Anonymous login ok, send your complete email address as your password’. Client sends acknowledgement to this using a TCP packet.
      3. Client sends a PASS request to the server and the server sends response with Response code 230 (User logged in , proceed) with response args ‘Welcome, archive user anonymous@10.109.20.93 !’. Client acknowledges this with TCP packet.
      4. Server sends response with Response code 230 (User logged in , proceed) with response args ‘Welcome, archive user anonymous@10.109.20.93 ! The local time is: Tue Jan 23 23:29:14 2018 This is an experimental FTP server. If you have any unusual problems,230-please report them via e-mail to <root@localhost>.Anonymous access granted, restrictions apply’. The client acknowledges this with a TCP packet.
      5. Client sends a SYST request. Server sends Response Code 215(Name System type) with Response args ‘UNIX Type: L8’. Client sends acknowledge TCP packet.
      6. Client sends a Request command ‘PASV’ to server with client ip and port 39644 to change the mode to passive. A response is received from the remote server saying “Response Code: 227 (Entering Passive Mode (10,5,20,222,129,105)). “ which is acknowledged by client through a TCP packet.
      7. **A TCP handshake between port 42470 of client and port 33129 of remote server happens(Corresponding to the initiation of data channel by the client server).**
      8. It is observed that Client initiates the data channel in case of passive mode even before a request is made for the data transfer unlike in active mode where the server initiates the data channel only after a request for data transfer is made.
      9. The client sends a Request command ‘LIST’ to server to port 21 from port 39644.
      10. Server sends Response code 150 (File status okay; about to open data connection) with Response args ‘Opening ASCII mode data connection for file list’ from port 21 to port 39644.
      11. The server transfers FTP data to the client from source port 33129 to client’s port 42470.
      12. Server and client does a TCP handshake to close the pipe between client port 42470 and server port 33129.
      13. Server sends a Response Code 226 (Closing data connection) with Response args ‘Transfer complete’ from port 21 to port 39644 which is acknowledged by the client.

* 1. For active mode the command channel is ( 10.109.20.93, 35514, 10.5.20.222, 21). For active mode the data channel is ( 10.109.20.93, 54995, 10.5.20.222, 20). For passive mode the command channel is (10.109.20.93, 39644, 10.5.20.222, 21). For passive mode the data channel is (10.109.20.93, 42470, 10.5.20.222, 33129). The client initiates the data channel connection by sending its port number in active case. In passive case the server initiates the data channel connection by sending the port number.

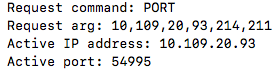
Active mode communication for data channel.



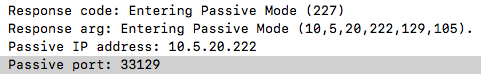
Passive mode communication for data channel.



Client sends the following data in active mode.



Server sends the following data in passive mode.



* 1. For active mode the data channel is ( 10.109.20.93, 54995, 10.5.20.222, 20). For passive mode the data channel is (10.109.20.93, 42470, 10.5.20.222, 33129).