

Assignment 2: Understanding the Protocols of Application Layer

By:

Member 1 - Ayush Bansal, Roll No - 15CS30006

Member 2 - Krushna Gaurkar, Roll No - 15CS30018

1)

a)

Port	Type of HTTP Connection
8111	HTTP 1.1 with persistent connection
8110	HTTP 1.1 with non-persistent connection
8100	HTTP 1.0

Justification -

We came to our conclusions based on the content of response headers -

For Port 8111, we received HTTP/1.1 and Connection: keep-alive thus HTTP 1.1 with persistent connection.

For Port 8110, we received HTTP/1.1 and Connection: close thus HTTP 1.1 with non-persistent connection.

For Port 8100, we received HTTP/1.0 thus HTTP 1.0

b)

Port	No. of GET Requests
8111	17
8110	17
8100	18

c)

Port No.	Packet No.	Time
8111	1	0.008743305
	2	0.006982827
	3	0.007172844
	4	0.005053683
	5	0.028747431
	6	0.056613582
	7	0.054169535
	8	0.056305747
	9	0.083803793
	10	0.057849979
	11	0.032968266
	12	0.031296893
	13	0.020167933
	14	0.020622097
	15	0.129971799
	16	0.156900618
	17	0.010143506
8110	1	0.035866793
	2	0.010866241
	3	0.012042253
	4	0.011637728
	5	0.019090065
	6	0.024209787
	7	0.033840627
	8	0.05678728
	9	0.075731013
	10	0.076761111
	11	0.055103923
	12	0.135705658
	13	0.067764591

	14	0.075903306
	15	0.077262473
	16	0.116275385
	17	0.227803629
8100	1	0.007665
	2	0.00667387
	3	0.005940054
	4	0.00737717
	5	0.009778843
	6	0.066724234
	7	0.100741118
	8	0.129721349
	9	0.143584697
	10	0.160056326
	11	0.069086219
	12	0.052707222
	13	0.046636693
	14	0.279639685
	15	0.049930958
	16	0.307373083
	17	0.19850915
	18	0.002583959

d)

Port No.	Time of Last Response	Time of first GET request	Total page download time
8111	18.5451	18.205	0.3401
8110	34.7486	34.387	0.3616
8100	2.9032	2.2759	0.6273

e)

User Agent Field contains the following for every hit -

Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)

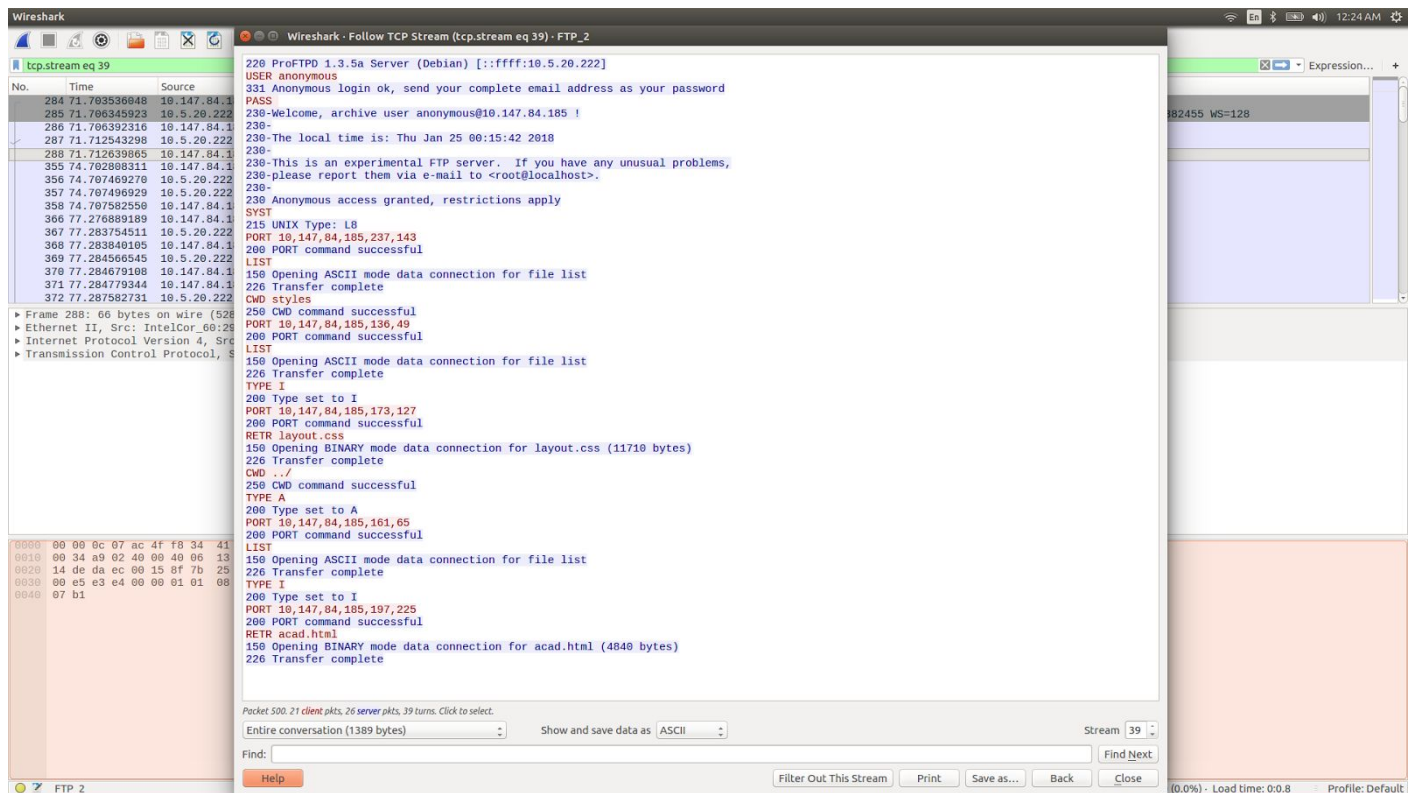
Chrome/63.0.3239.132 Safari/537.36

We conclude the following information regarding the OS and browser

OS - Linux x86-64

Browser - Chrome 63.0

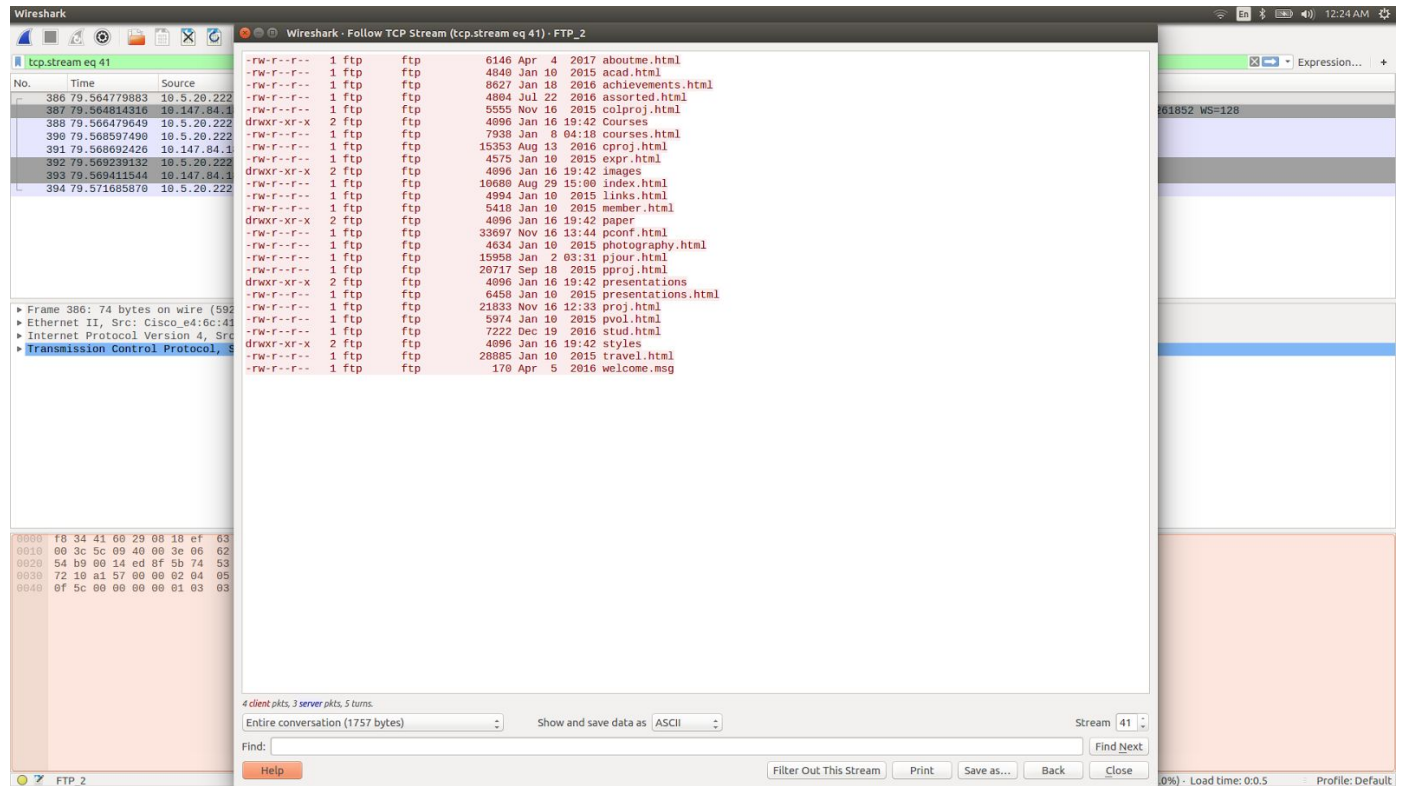
2)
a)
i) Active Mode -



Command - open 10.5.20.222, followed by username and password.

Observed FTP Headers - 1. Response 2. Request

Source IP -	For Request - 10.147.84.185	For Response - 10.5.20.222
Destination IP -	For Request - 10.5.20.222	For Response - 10.147.84.185
Source port -	For Request - 56044	For Response - 21
Destination port -	For Request - 21	For Response - 56044



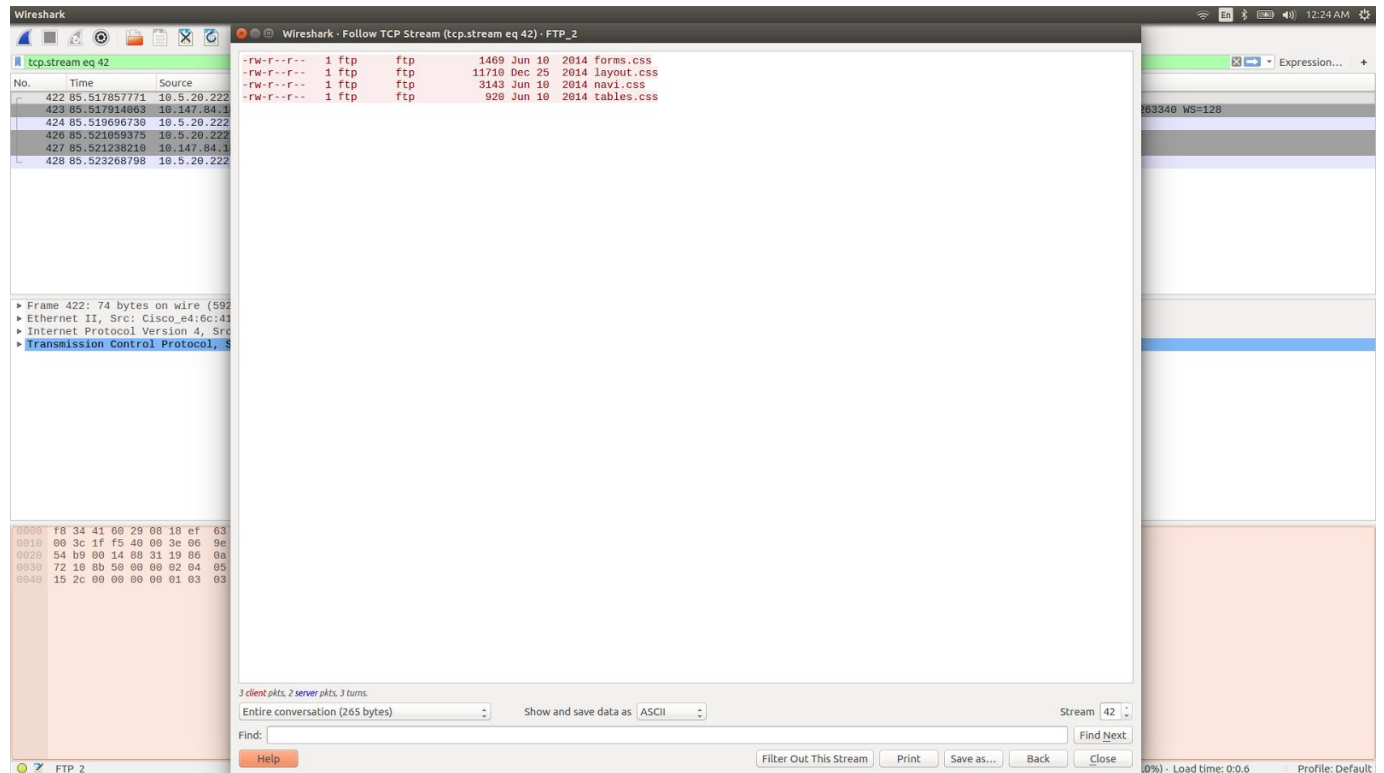
Command - ls

Source IP - 10.5.20.222

Destination IP - 10.147.84.185

Source port - 20

Destination port - 60815



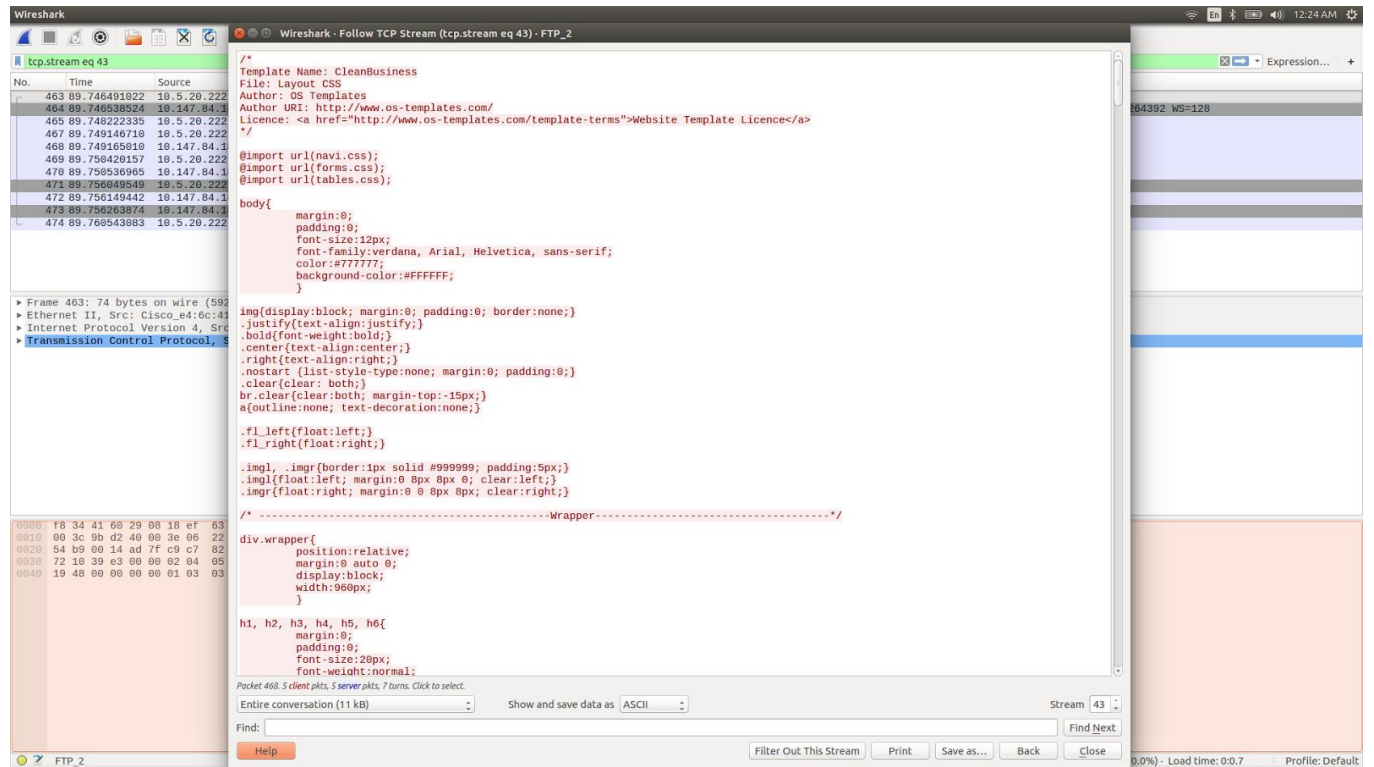
Command - ls

Source IP - 10.5.20.222

Destination IP - 10.147.84.185

Source port - 20

Destination port - 34865



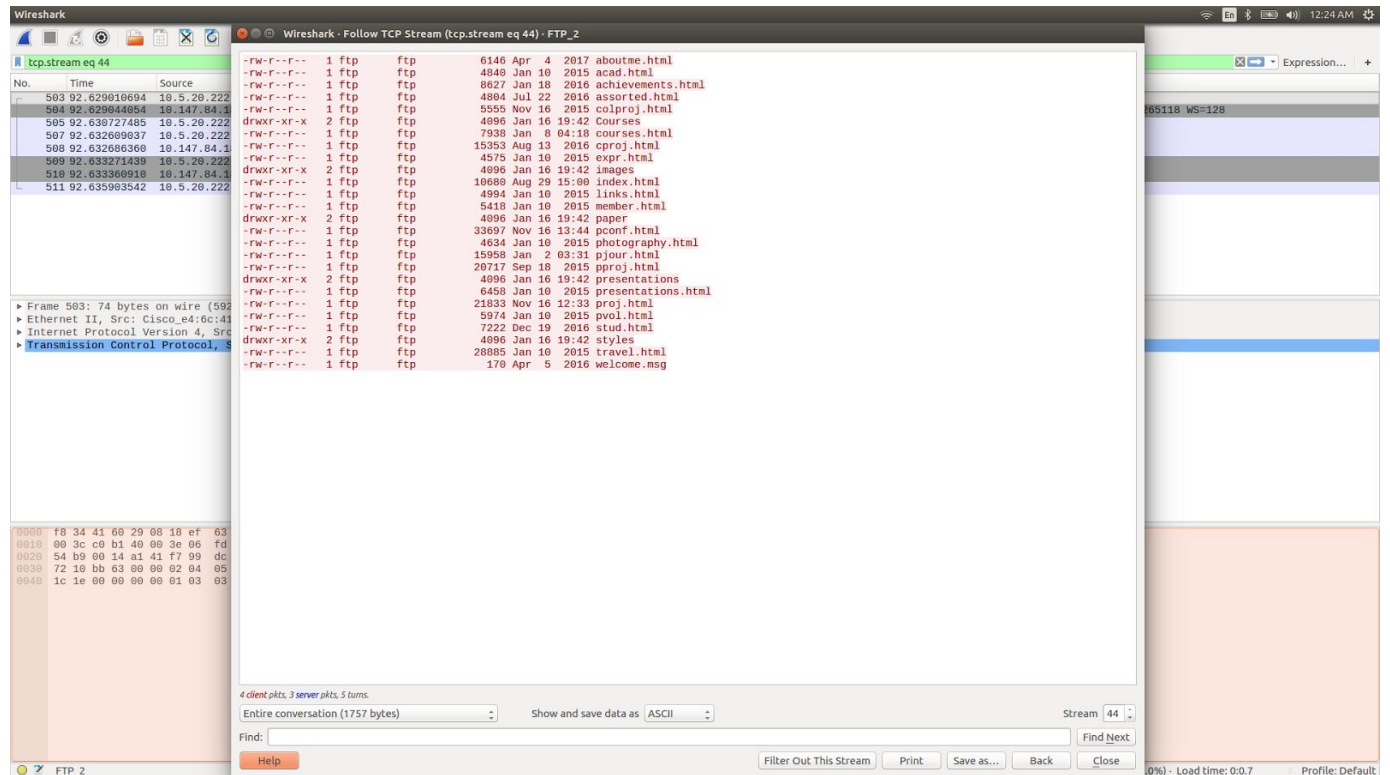
Command - get layout.css

Source IP - 10.5.20.222

Destination IP - 10.147.84.185

Source port - 20

Destination port - 44415



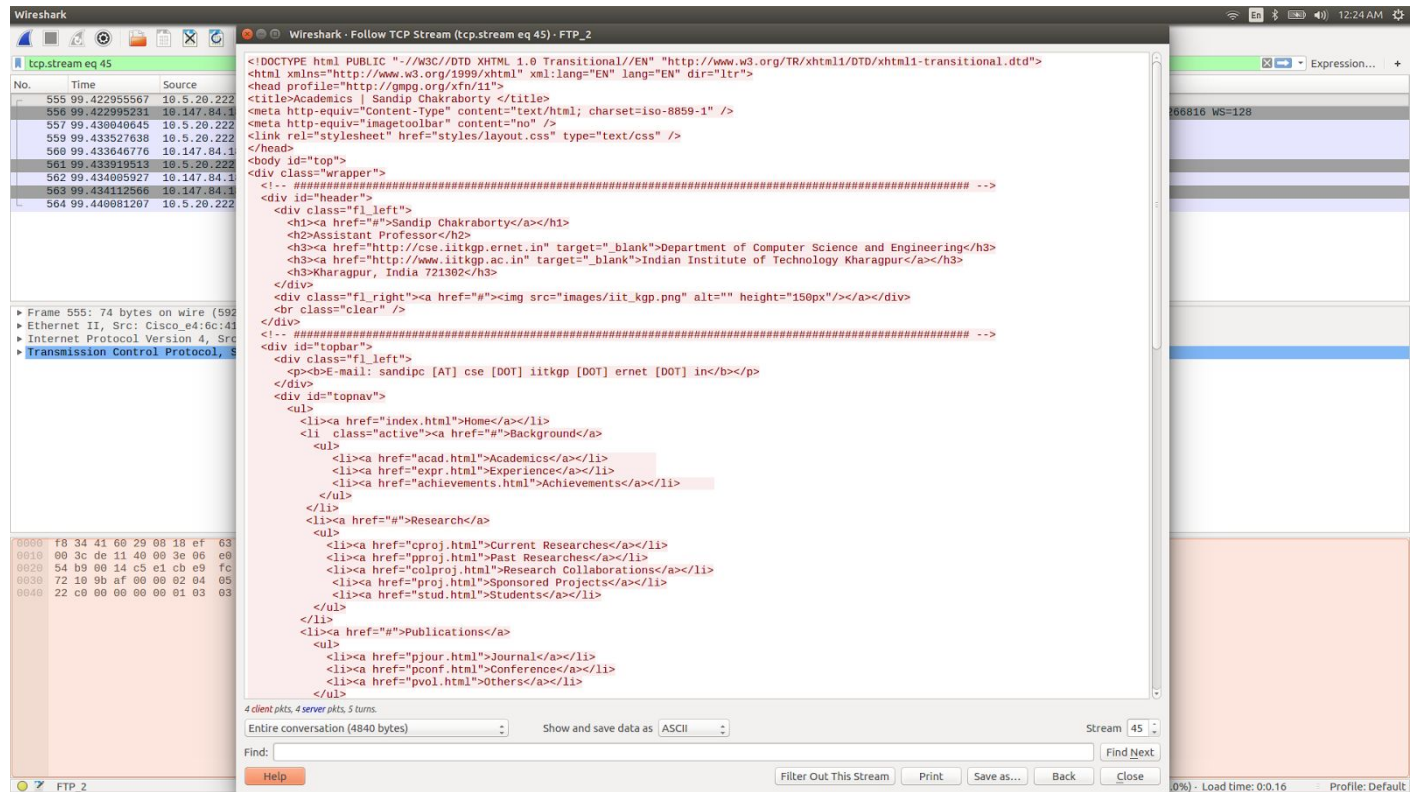
Command - ls

Source IP - 10.5.20.222

Destination IP - 10.147.84.185

Source port - 20

Destination port - 41281



Command - get acad.html

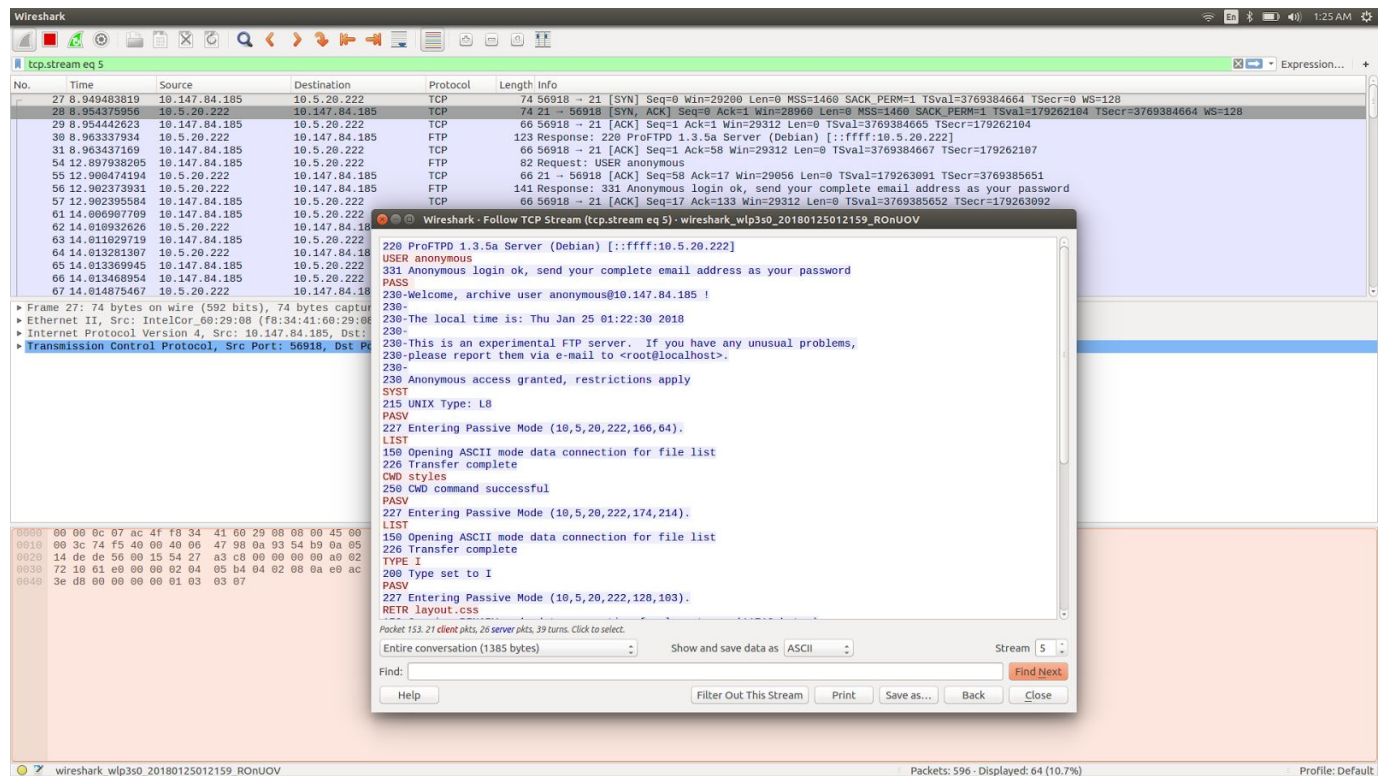
Source IP - 10.5.20.222

Destination IP - 10.147.84.185

Source port - 20

Destination port - 50657

ii) Passive Mode -



Command - open 10.5.20.222, followed by username and password, passive

Observed FTP Headers - 1. Response 2. Request

Source IP -	For Request - 10.147.84.185	For Response - 10.5.20.222
Destination IP -	For Request - 10.5.20.222	For Response - 10.147.84.185
Source port -	For Request - 56918	For Response - 21
Destination port -	For Request - 21	For Response - 56918

The image shows a Wireshark packet capture window. The top pane displays a list of packets. The second pane shows the details of the selected packet (Frame 121), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The third pane shows the raw packet data in hexadecimal and ASCII. A fourth pane, titled 'Wireshark - Follow TCP Stream (tcp.stream eq 14) - wireshark_wlp3s0_20180125012159_RONuOV', displays the stream data in a table format, showing the sequence of data received from the client and sent to the server.

No.	Time	Source	Destination	Protocol	Length	Info
121	37.345930794	10.147.84.185	10.5.20.222	TCP	74	33696 → 42560 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3769391763 TSecr=0 WS=128
122	37.347555518	10.5.20.222	10.147.84.185	TCP	74	42560 → 33696 [SYN, ACK] Seq=8 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=179269283 TSecr=3769391763 WS=128
123	37.347621523	10.147.84.185	10.5.20.222	TCP	66	33696 → 42560 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3769391763 TSecr=179269283
126	37.352298088	10.5.20.222	10.147.84.185	FTP-DATA	1823	FTP Data: 1757 bytes
127	37.352422347	10.147.84.185	10.5.20.222	TCP	66	33696 → 42560 [ACK] Seq=1 Ack=1759 Win=32768 Len=0 TSval=3769391764 TSecr=179269284
128	37.352849796	10.147.84.185	10.5.20.222	TCP	66	33696 → 42560 [FIN, ACK] Seq=1 Ack=1759 Win=32768 Len=0 TSval=3769391765 TSecr=179269284
129	37.355951845	10.5.20.222	10.147.84.185	TCP	66	42560 → 33696 [ACK] Seq=1759 Ack=2 Win=29056 Len=0 TSval=179269286 TSecr=3769391765

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

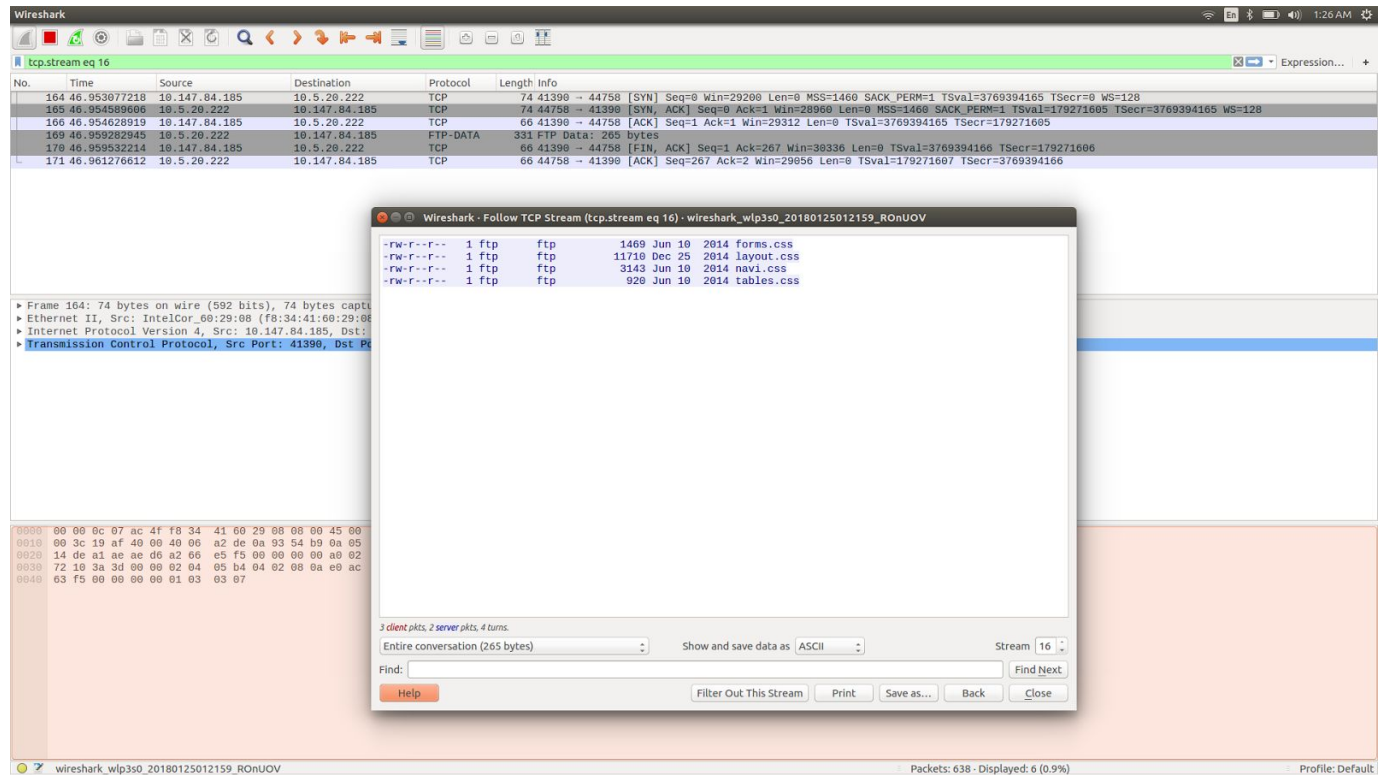
Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	0010	0020	0030	0040
0000	00 00 0c 07 ac 4f f8 34 41 60 29 08 00 00 45 00				
0010	00 3c f2 26 40 00 40 06 ca 66 0a 93 54 b9 0a 05				
0020	14 de 83 a0 a6 40 b9 13 00 de 00 00 00 00 a0 02				
0030	72 10 38 ae 00 00 02 04 05 b4 04 02 08 0a e0 ac				
0040	5a 93 00 00 00 00 01 03 03 07				

Offset	0000	001
--------	------	-----



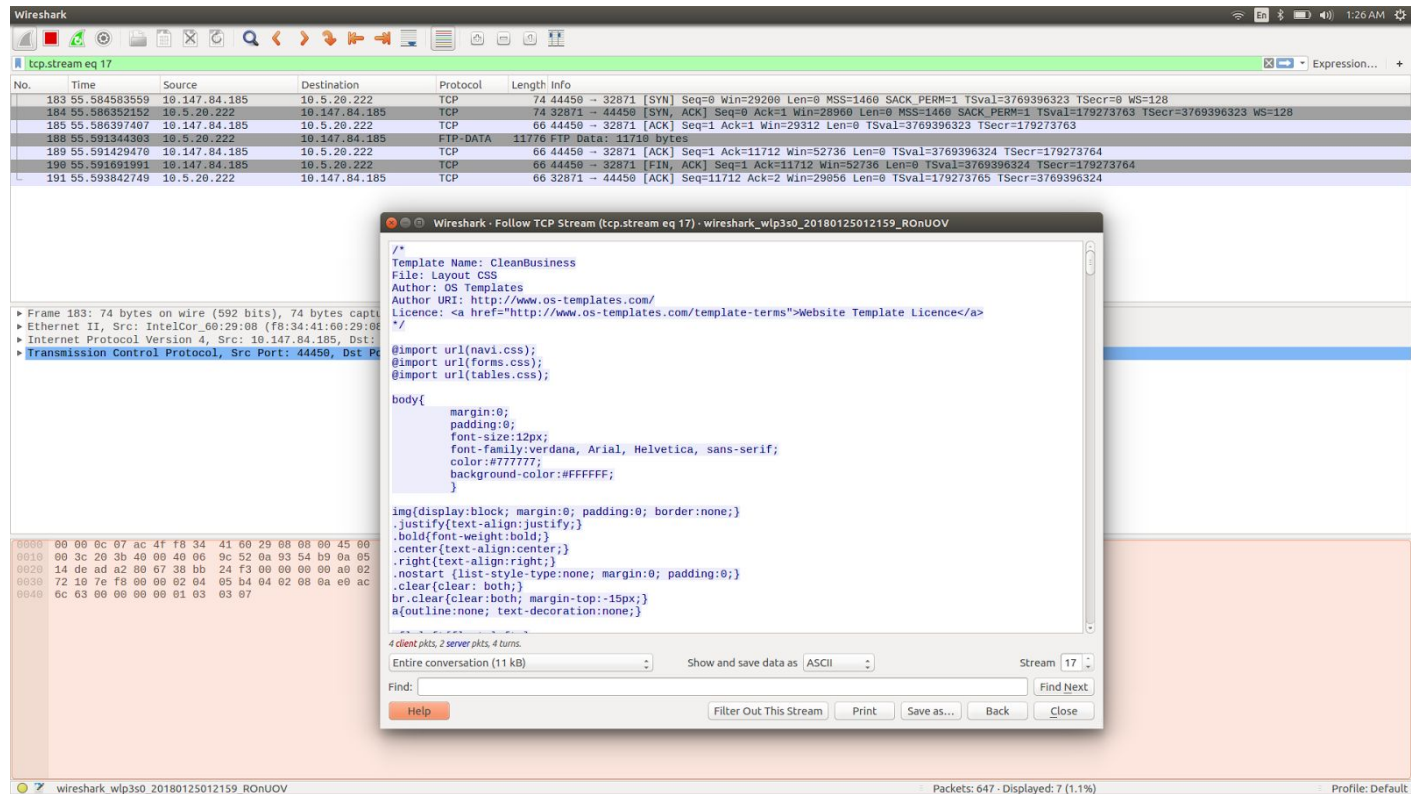
Command - ls

Source IP - 10.5.20.222

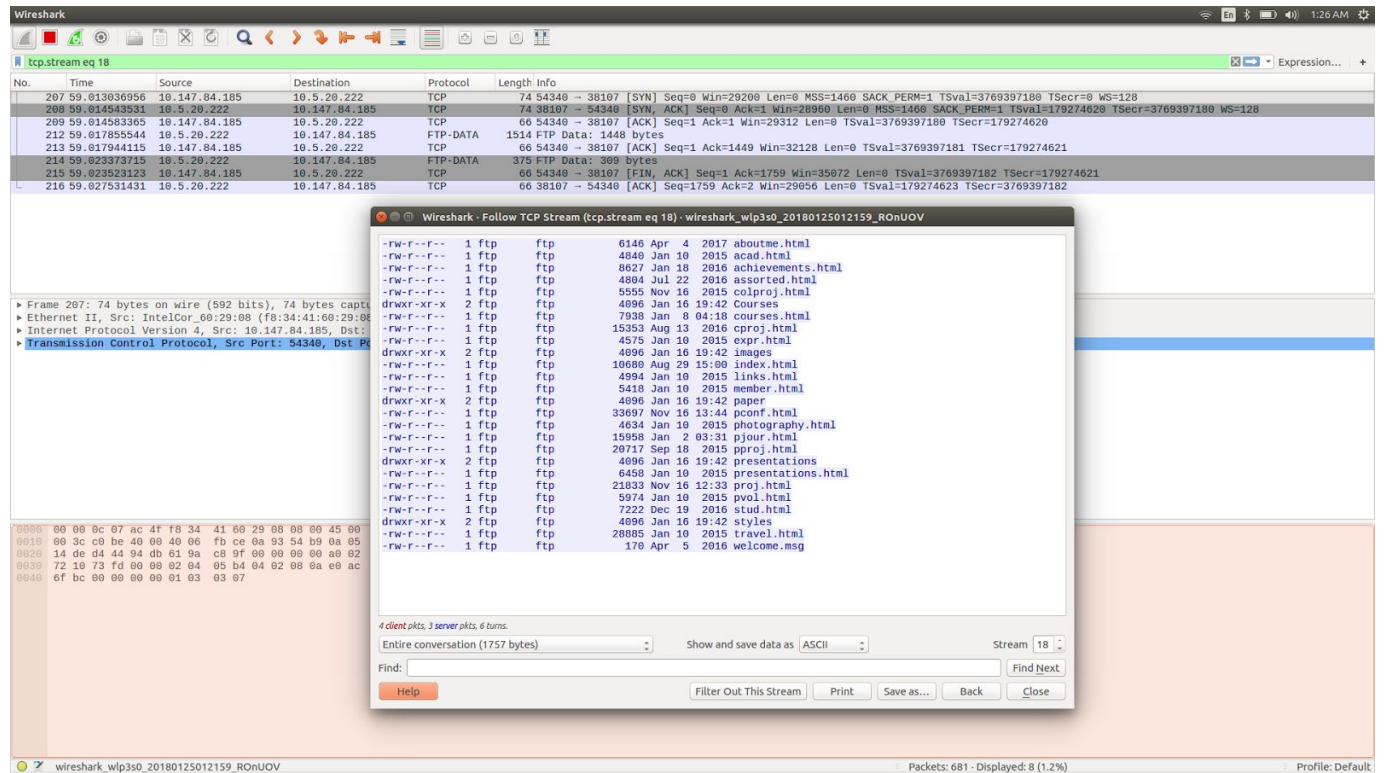
Destination IP - 10.147.84.185

Source port - 44758

Destination port - 41390



Command - get layout.css
 Source IP - 10.5.20.222
 Destination IP - 10.147.84.185
 Source port - 32871
 Destination port - 44450



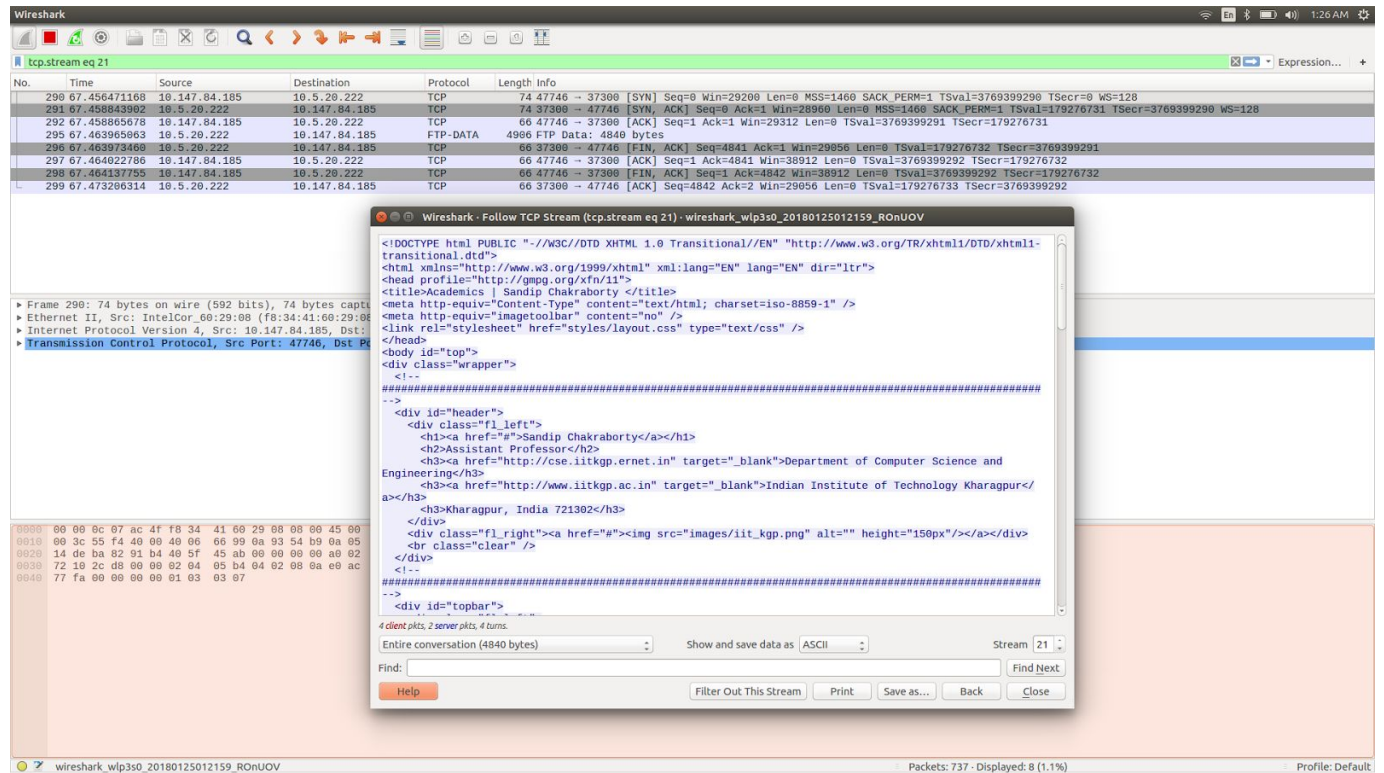
Command - ls

Source IP - 10.5.20.222

Destination IP - 10.147.84.185

Source port - 38107

Destination port - 54340



Command - get acad.html

Source IP - 10.5.20.222

Destination IP - 10.147.84.185

Source port - 37300

Destination port - 47746

b)

i) Active Mode -

Command Channel - 10.147.84.185:56044 - 10.5.20.222:21

Data Channels -

10.5.20.222:20 (Source) - 10.147.84.185:60815 (Destination)

10.5.20.222:20 (Source) - 10.147.84.185:34865 (Destination)

10.5.20.222:20 (Source) - 10.147.84.185:44415 (Destination)

10.5.20.222:20 (Source) - 10.147.84.185:41281 (Destination)

10.5.20.222:20 (Source) - 10.147.84.185:50657 (Destination)

In case of Active mode, the client exposes his data port to server and the Server initiates the data channel connection.

ii) Passive Mode -

Command Channel - 10.147.84.185:56918 - 10.5.20.222:21

Data Channels -

10.5.20.222:42560 (Source) - 10.147.84.185:33696 (Destination)

10.5.20.222:44758 (Source) - 10.147.84.185:41390 (Destination)

10.5.20.222:32871 (Source) - 10.147.84.185:44450 (Destination)

10.5.20.222:38107 (Source) - 10.147.84.185:54340 (Destination)

10.5.20.222:37300 (Source) - 10.147.84.185:47746 (Destination)

In case of Passive mode, the client sends a PASSIVE signal to server and then the client initiates the data channel connection.

c)

For Active mode, the port used for data communication is always port 20 over the FTP server (10.5.20.222) while the port over the client side (10.147.84.185) changes for each stream.

For Passive Mode, the port for data communication changes for each stream for both server and client.

In active mode, the client sends its port number to the server and the server then establishes a connection from its Port 20 to client's specific port.

But during the passive mode, the client sends a Passive message to the Server and the Server responds by exposing its Port to the Client, the connection to which is made by the client using one of its empty Port and the Server's Specified Port.