1 (a)

8100:HTTP/1.0,

8110 : HTTP/1.1, non - persistent

Also, it is mentioned in http header : Connection : close

8111 : HTTP/1.1, persistent - FINAL closure is after all GET requests and receiving

Also, connection type is mentioned KEEP-ALIVE

1 (b)

using filter - http.request.method == "GET"

17 GET requests in all cases

1 (c)

//we are calculating the time b/w the GET request and first packet of the response (http response may span span multiple packets)

Filter ip.addr == 10.112.3.78 && ip.addr ==10.5.20.222 && http

And making Time since request as a column

Time since request

8100
0.001517035
0.000980491
0.001604682
0.003573254
0.003621407
0.004543013
0.008423669
0.009203393
0.008036772
0.005241198
0.004486188
0.012322585
0.003285948
0.00393297
0.044045677
Avg : 0.00765455

8110
Time since request

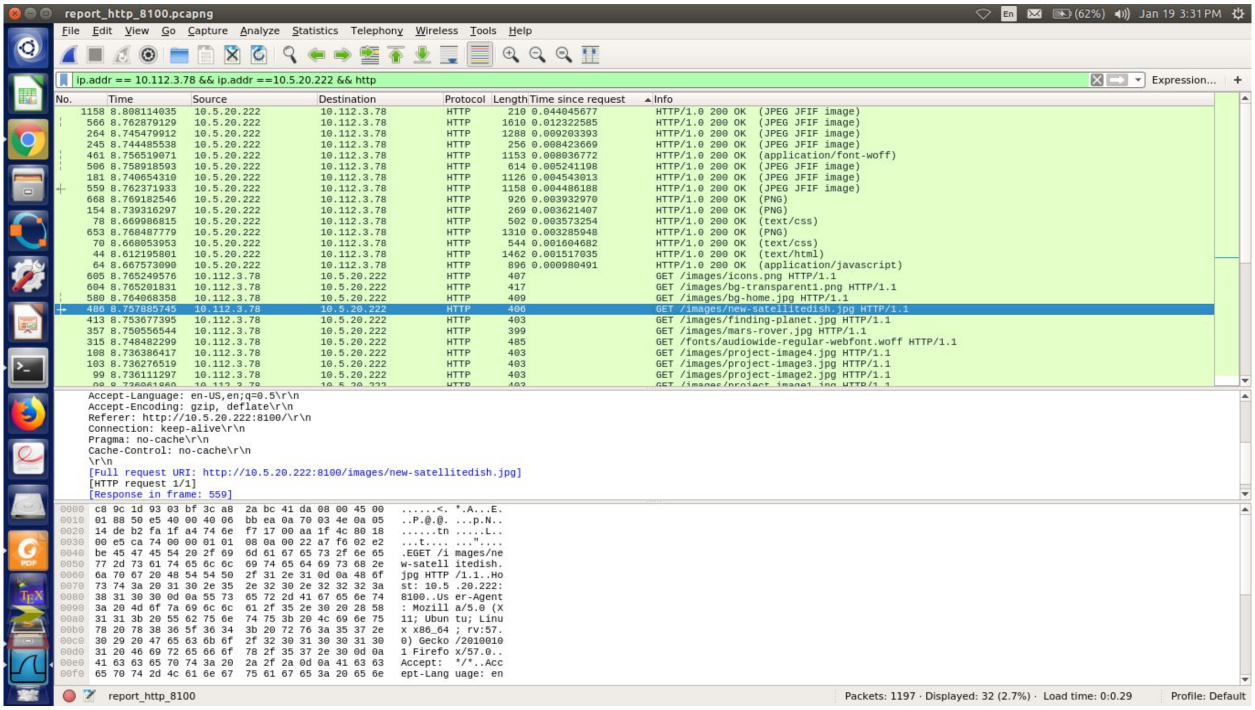
0.001540271

0.000859411
0.001254054
0.002155039
0.000923308
0.004663759
0.005130475
0.004944557
0.008908998
0.00953964
0.010855678
0.004476052
0.005449665
0.012696049
0.031814386
0.002987486
0.057322729

Average : 0.00973656

8111
Time since request
0.001446562
0.00104325
0.001527033
0.00260565
0.002217595
0.004745289
0.011553254
0.004207627
0.004709334
0.004559895
0.004150658
0.035898898
0.054446572
0.20857638
Avg : 0.0244063

Average time since request is more in persistent connection


report_http_8100.pcapng
En
(62%)
Jan 19 3:31 PM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
ip.addr == 10.112.3.78 && ip.addr ==10.5.20.222 && http
```

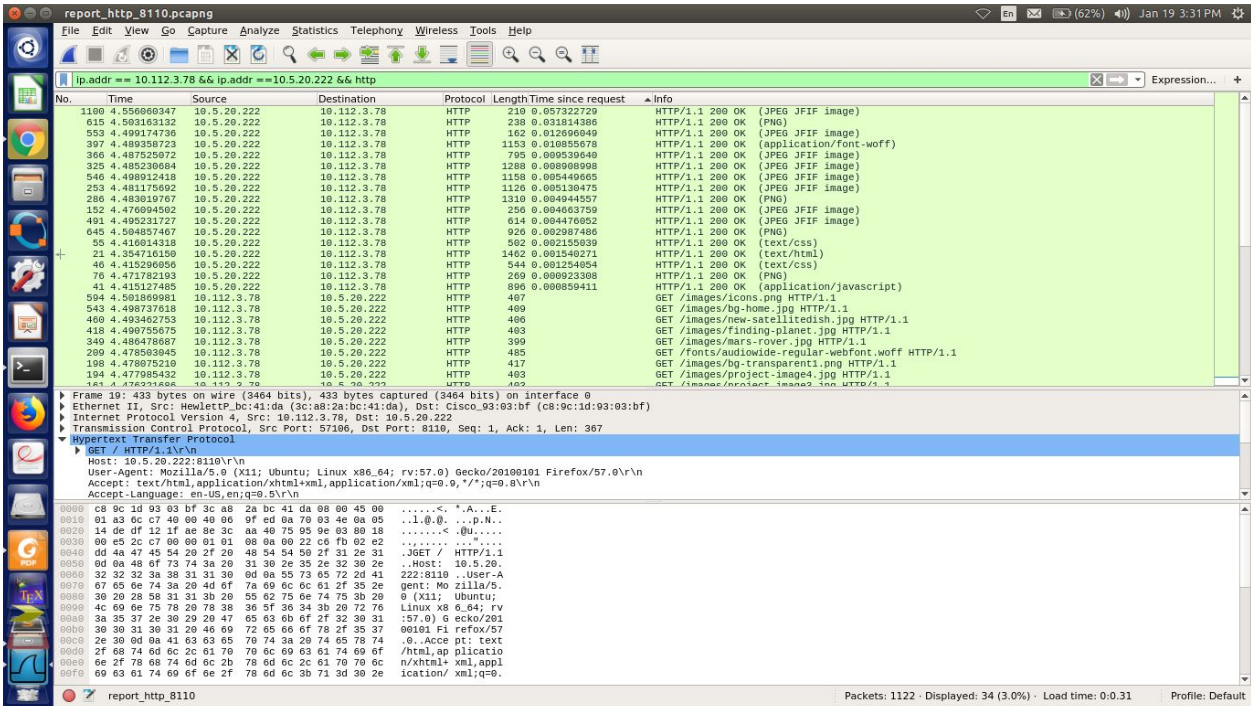
```
No.    Time         Source         Destination    Protocol Length Time since request  Info
 1158 8.808114035  10.5.20.222    10.112.3.78    HTTP      210 0.044045677   HTTP/1.0 200 OK  (JPEG JFIF image)
  566 8.762879129  10.5.20.222    10.112.3.78    HTTP     1610 0.012322585   HTTP/1.0 200 OK  (JPEG JFIF image)
  264 8.745479912  10.5.20.222    10.112.3.78    HTTP     1288 0.009203393   HTTP/1.0 200 OK  (JPEG JFIF image)
  245 8.744485538  10.5.20.222    10.112.3.78    HTTP      256 0.008423669   HTTP/1.0 200 OK  (JPEG JFIF image)
  461 8.756519071  10.5.20.222    10.112.3.78    HTTP     1153 0.008036772   HTTP/1.0 200 OK  (application/font-woff)
  506 8.758918593  10.5.20.222    10.112.3.78    HTTP      614 0.005241198   HTTP/1.0 200 OK  (JPEG JFIF image)
  181 8.740654310  10.5.20.222    10.112.3.78    HTTP     1126 0.004543013   HTTP/1.0 200 OK  (JPEG JFIF image)
  559 8.762371933  10.5.20.222    10.112.3.78    HTTP     1158 0.004486188   HTTP/1.0 200 OK  (JPEG JFIF image)
  668 8.769182546  10.5.20.222    10.112.3.78    HTTP      926 0.003932970   HTTP/1.0 200 OK  (PNG)
  154 8.739316297  10.5.20.222    10.112.3.78    HTTP      269 0.003621407   HTTP/1.0 200 OK  (PNG)
   78 8.669986815  10.5.20.222    10.112.3.78    HTTP      502 0.003573254   HTTP/1.0 200 OK  (text/css)
  653 8.768487779  10.5.20.222    10.112.3.78    HTTP     1310 0.003285948   HTTP/1.0 200 OK  (PNG)
   70 8.668053953  10.5.20.222    10.112.3.78    HTTP      544 0.001604682   HTTP/1.0 200 OK  (text/css)
   44 8.612195801  10.5.20.222    10.112.3.78    HTTP     1462 0.001517035   HTTP/1.0 200 OK  (text/html)
   64 8.667573090  10.5.20.222    10.112.3.78    HTTP      896 0.000980491   HTTP/1.0 200 OK  (application/javascript)
  605 8.765249576  10.112.3.78    10.5.20.222    HTTP      407               GET /images/icons.png HTTP/1.1
  604 8.765201831  10.112.3.78    10.5.20.222    HTTP      417               GET /images/bg-transparent1.png HTTP/1.1
  580 8.764068358  10.112.3.78    10.5.20.222    HTTP      409               GET /images/bg-home.jpg HTTP/1.1
  486 8.757885745  10.112.3.78    10.5.20.222    HTTP      406               GET /images/new-satellitedish.jpg HTTP/1.1
  413 8.753677395  10.112.3.78    10.5.20.222    HTTP      403               GET /images/finding-planet.jpg HTTP/1.1
  357 8.750556544  10.112.3.78    10.5.20.222    HTTP      399               GET /images/mars-rover.jpg HTTP/1.1
  315 8.748482299  10.112.3.78    10.5.20.222    HTTP      485               GET /fonts/audiowide-regular-webfont.woff HTTP/1.1
  108 8.736386417  10.112.3.78    10.5.20.222    HTTP      403               GET /images/project-image4.jpg HTTP/1.1
  103 8.736276519  10.112.3.78    10.5.20.222    HTTP      403               GET /images/project-image3.jpg HTTP/1.1
   99 8.736111297  10.112.3.78    10.5.20.222    HTTP      403               GET /images/project-image2.jpg HTTP/1.1
   98 8.736061860  10.112.3.78    10.5.20.222    HTTP      403               GET /images/project-image1.jpg HTTP/1.1
```

```
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://10.5.20.222:8100/\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://10.5.20.222:8100/images/new-satellitedish.jpg]
    [HTTP request 1/1]
    [Response in frame: 559]
```

```
0000  c8 9c 1d 93 03 bf 3c a8  2a bc 41 da 08 00 45 00   ......<. *.A...E.
0010  01 88 50 e5 40 00 40 06  bb ea 0a 70 03 4e 0a 05   ..P.@.@. ...p.N..
0020  14 de b2 fa 1f a4 74 6e  f7 17 00 aa 1f 4c 80 18   ......tn .....L..
0030  00 e5 ca 74 00 00 01 01  08 0a 00 22 a7 f6 02 e2   ...t.... ..."....
0040  be 45 47 45 54 20 2f 69  6d 61 67 65 73 2f 6e 65   .EGET /i mages/ne
0050  77 2d 73 61 74 65 6c 6c  69 74 65 64 69 73 68 2e   w-satell itedish.
0060  6a 70 67 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   jpg HTTP /1.1..Ho
0070  73 74 3a 20 31 30 2e 35  2e 32 30 2e 32 32 32 3a   st: 10.5 .20.222:
0080  38 31 30 30 0d 0a 55 73  65 72 2d 41 67 65 6e 74   8100..Us er-Agent
0090  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 58   : Mozill a/5.0 (X
00a0  31 31 3b 20 55 62 75 6e  74 75 3b 20 4c 69 6e 75   11; Ubun tu; Linu
00b0  78 20 78 38 36 5f 36 34  3b 20 72 76 3a 35 37 2e   x x86_64 ; rv:57.
00c0  30 29 20 47 65 63 6b 6f  2f 32 30 31 30 30 31 30   0) Gecko /2010010
00d0  31 20 46 69 72 65 66 6f  78 2f 35 37 2e 30 0d 0a   1 Firefo x/57.0..
00e0  41 63 63 65 70 74 3a 20  2a 2f 2a 0d 0a 41 63 63   Accept:  */*..Acc
00f0  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a 20 65 6e   ept-Lang uage: en
```

```
report_http_8100        Packets: 1197 · Displayed: 32 (2.7%) · Load time: 0:0.29        Profile: Default
```

8110


report_http_8110.pcapng
En
(62%)
Jan 19 3:31 PM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
ip.addr == 10.112.3.78 && ip.addr ==10.5.20.222 && http
```

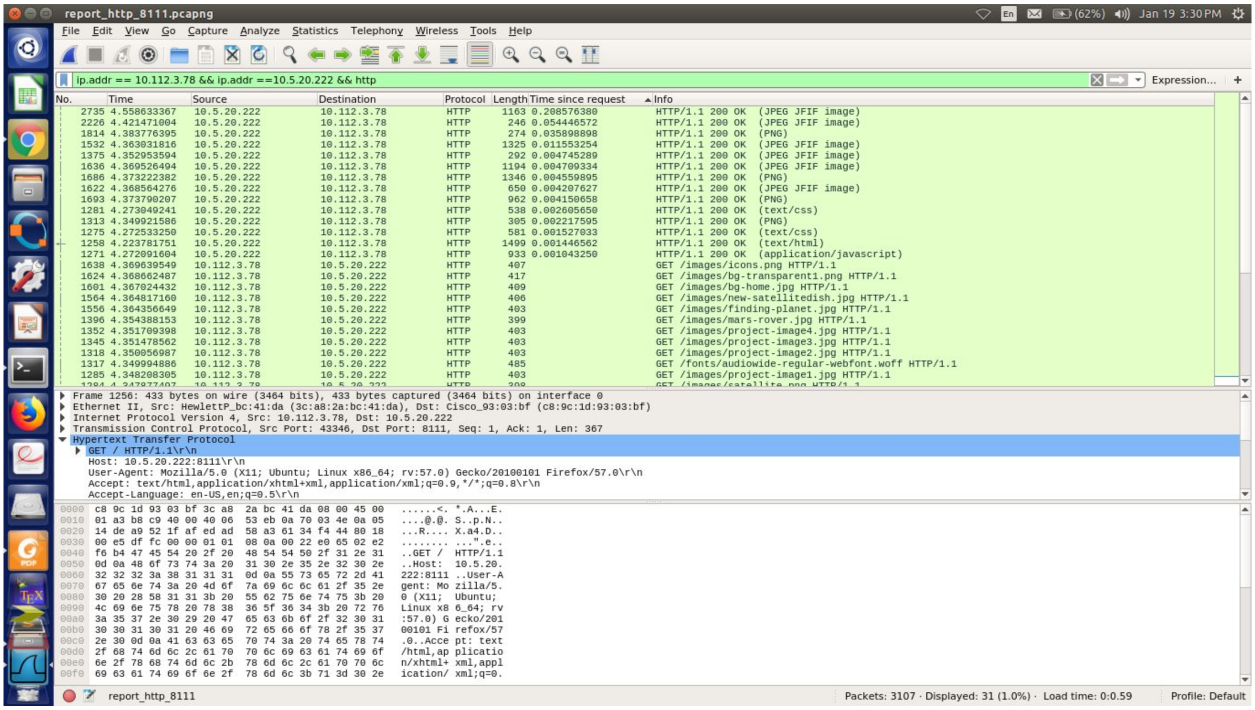
```
No.    Time         Source         Destination    Protocol Length Time since request  Info
 1100 4.556060347  10.5.20.222    10.112.3.78    HTTP      210 0.057322729   HTTP/1.1 200 OK  (JPEG JFIF image)
  615 4.503163132  10.5.20.222    10.112.3.78    HTTP      238 0.031814386   HTTP/1.1 200 OK  (PNG)
  553 4.499174736  10.5.20.222    10.112.3.78    HTTP      162 0.012696049   HTTP/1.1 200 OK  (JPEG JFIF image)
  397 4.489358723  10.5.20.222    10.112.3.78    HTTP     1153 0.010855678   HTTP/1.1 200 OK  (application/font-woff)
  366 4.487525072  10.5.20.222    10.112.3.78    HTTP      795 0.009539640   HTTP/1.1 200 OK  (JPEG JFIF image)
  325 4.485230684  10.5.20.222    10.112.3.78    HTTP     1288 0.008908998   HTTP/1.1 200 OK  (JPEG JFIF image)
  546 4.498912418  10.5.20.222    10.112.3.78    HTTP     1158 0.005449665   HTTP/1.1 200 OK  (JPEG JFIF image)
  253 4.481175692  10.5.20.222    10.112.3.78    HTTP     1126 0.005130475   HTTP/1.1 200 OK  (JPEG JFIF image)
  286 4.483019767  10.5.20.222    10.112.3.78    HTTP     1310 0.004944557   HTTP/1.1 200 OK  (PNG)
  152 4.476094502  10.5.20.222    10.112.3.78    HTTP      256 0.004663759   HTTP/1.1 200 OK  (JPEG JFIF image)
  491 4.495231727  10.5.20.222    10.112.3.78    HTTP      614 0.004476052   HTTP/1.1 200 OK  (JPEG JFIF image)
  645 4.504857467  10.5.20.222    10.112.3.78    HTTP      926 0.002987486   HTTP/1.1 200 OK  (PNG)
   55 4.416014318  10.5.20.222    10.112.3.78    HTTP      502 0.002155039   HTTP/1.1 200 OK  (text/css)
   21 4.354716150  10.5.20.222    10.112.3.78    HTTP     1462 0.001540271   HTTP/1.1 200 OK  (text/html)
   46 4.415296056  10.5.20.222    10.112.3.78    HTTP      544 0.001254054   HTTP/1.1 200 OK  (text/css)
   76 4.471782193  10.5.20.222    10.112.3.78    HTTP      269 0.000923308   HTTP/1.1 200 OK  (PNG)
   41 4.415127485  10.5.20.222    10.112.3.78    HTTP      896 0.000859411   HTTP/1.1 200 OK  (application/javascript)
  594 4.501869981  10.112.3.78    10.5.20.222    HTTP      407               GET /images/icons.png HTTP/1.1
  543 4.498737618  10.112.3.78    10.5.20.222    HTTP      409               GET /images/bg-home.jpg HTTP/1.1
  460 4.493462753  10.112.3.78    10.5.20.222    HTTP      406               GET /images/new-satellitedish.jpg HTTP/1.1
  418 4.490755675  10.112.3.78    10.5.20.222    HTTP      403               GET /images/finding-planet.jpg HTTP/1.1
  349 4.486478687  10.112.3.78    10.5.20.222    HTTP      399               GET /images/mars-rover.jpg HTTP/1.1
  209 4.478503045  10.112.3.78    10.5.20.222    HTTP      485               GET /fonts/audiowide-regular-webfont.woff HTTP/1.1
  198 4.478075210  10.112.3.78    10.5.20.222    HTTP      417               GET /images/bg-transparent1.png HTTP/1.1
  194 4.477985432  10.112.3.78    10.5.20.222    HTTP      403               GET /images/project-image4.jpg HTTP/1.1
  161 4.476221686  10.112.3.78    10.5.20.222    HTTP      403               GET /images/project-image3.jpg HTTP/1.1
```

```
▶ Frame 19: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface 0
▶ Ethernet II, Src: HewlettP_bc:41:da (3c:a8:2a:bc:41:da), Dst: Cisco_93:03:bf (c8:9c:1d:93:03:bf)
▶ Internet Protocol Version 4, Src: 10.112.3.78, Dst: 10.5.20.222
▶ Transmission Control Protocol, Src Port: 57106, Dst Port: 8110, Seq: 1, Ack: 1, Len: 367
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: 10.5.20.222:8110\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:57.0) Gecko/20100101 Firefox/57.0\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
```

```
0000  c8 9c 1d 93 03 bf 3c a8  2a bc 41 da 08 00 45 00   ......<. *.A...E.
0010  01 a3 6c c7 40 00 40 06  9f ed 0a 70 03 4e 0a 05   ..l.@.@. ...p.N..
0020  14 de df 12 1f ae 8e 3c  aa 40 75 95 9e 03 80 18   .......< .@u.....
0030  00 e5 2c c7 00 00 01 01  08 0a 00 22 c6 fb 02 e2   ..,..... ..."....
0040  dd 4a 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   .JGET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  31 30 2e 35 2e 32 30 2e   ..Host:  10.5.20.
0060  32 32 32 3a 38 31 31 30  0d 0a 55 73 65 72 2d 41   222:8110 ..User-A
0070  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
0080  30 20 28 58 31 31 3b 20  55 62 75 6e 74 75 3b 20   0 (X11;  Ubuntu;
0090  4c 69 6e 75 78 20 78 38  36 5f 36 34 3b 20 72 76   Linux x8 6_64; rv
00a0  3a 35 37 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   :57.0) G ecko/201
00b0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 35 37   00101 Fi refox/57
00c0  2e 30 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   .0..Acce pt: text
00d0  2f 68 74 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   /html,ap plicatio
00e0  6e 2f 78 68 74 6d 6c 2b  78 6d 6c 2c 61 70 70 6c   n/xhtml+ xml,appl
00f0  69 63 61 74 69 6f 6e 2f  78 6d 6c 3b 71 3d 30 2e   ication/ xml;q=0.
```

```
report_http_8110        Packets: 1122 · Displayed: 34 (3.0%) · Load time: 0:0.31        Profile: Default
```

8111



```
ip.addr == 10.112.3.78 && ip.addr ==10.5.20.222 && http
```

```
No.    Time         Source        Destination   Protocol Length Time since request  Info
  2735 4.558633367  10.5.20.222   10.112.3.78   HTTP     1163 0.208576380   HTTP/1.1 200 OK  (JPEG JFIF image)
  2226 4.421471004  10.5.20.222   10.112.3.78   HTTP      246 0.054446572   HTTP/1.1 200 OK  (JPEG JFIF image)
  1814 4.383776395  10.5.20.222   10.112.3.78   HTTP      274 0.035898898   HTTP/1.1 200 OK  (PNG)
  1532 4.363031816  10.5.20.222   10.112.3.78   HTTP     1325 0.011553254   HTTP/1.1 200 OK  (JPEG JFIF image)
  1375 4.352953594  10.5.20.222   10.112.3.78   HTTP      292 0.004745289   HTTP/1.1 200 OK  (JPEG JFIF image)
  1636 4.369526494  10.5.20.222   10.112.3.78   HTTP     1194 0.004709334   HTTP/1.1 200 OK  (JPEG JFIF image)
  1686 4.373222382  10.5.20.222   10.112.3.78   HTTP     1346 0.004559895   HTTP/1.1 200 OK  (PNG)
  1622 4.368564276  10.5.20.222   10.112.3.78   HTTP      650 0.004207627   HTTP/1.1 200 OK  (JPEG JFIF image)
  1693 4.373790207  10.5.20.222   10.112.3.78   HTTP      962 0.004150658   HTTP/1.1 200 OK  (PNG)
  1281 4.273049241  10.5.20.222   10.112.3.78   HTTP      538 0.002605650   HTTP/1.1 200 OK  (text/css)
  1313 4.349921586  10.5.20.222   10.112.3.78   HTTP      305 0.002217595   HTTP/1.1 200 OK  (PNG)
  1275 4.272533250  10.5.20.222   10.112.3.78   HTTP      581 0.001527033   HTTP/1.1 200 OK  (text/css)
  1258 4.223781751  10.5.20.222   10.112.3.78   HTTP     1499 0.001446562   HTTP/1.1 200 OK  (text/html)
  1271 4.272091604  10.5.20.222   10.112.3.78   HTTP      933 0.001043250   HTTP/1.1 200 OK  (application/javascript)
  1638 4.369639549  10.112.3.78   10.5.20.222   HTTP      407               GET /images/icons.png HTTP/1.1
  1624 4.368662487  10.112.3.78   10.5.20.222   HTTP      417               GET /images/bg-transparent1.png HTTP/1.1
  1601 4.367024432  10.112.3.78   10.5.20.222   HTTP      409               GET /images/bg-home.jpg HTTP/1.1
  1564 4.364817160  10.112.3.78   10.5.20.222   HTTP      406               GET /images/new-satellitedish.jpg HTTP/1.1
  1556 4.364356649  10.112.3.78   10.5.20.222   HTTP      403               GET /images/finding-planet.jpg HTTP/1.1
  1396 4.354388153  10.112.3.78   10.5.20.222   HTTP      399               GET /images/mars-rover.jpg HTTP/1.1
  1352 4.351709398  10.112.3.78   10.5.20.222   HTTP      403               GET /images/project-image4.jpg HTTP/1.1
  1345 4.351478562  10.112.3.78   10.5.20.222   HTTP      403               GET /images/project-image3.jpg HTTP/1.1
  1318 4.350056987  10.112.3.78   10.5.20.222   HTTP      403               GET /images/project-image2.jpg HTTP/1.1
  1317 4.349994886  10.112.3.78   10.5.20.222   HTTP      485               GET /fonts/audiowide-regular-webfont.woff HTTP/1.1
  1285 4.348208305  10.112.3.78   10.5.20.222   HTTP      403               GET /images/project-image1.jpg HTTP/1.1
  1284 4.347877407  10.112.3.78   10.5.20.222   HTTP      308               GET /images/satellite.png HTTP/1.1
```

```
▶ Frame 1256: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface 0
▶ Ethernet II, Src: HewlettP_bc:41:da (3c:a8:2a:bc:41:da), Dst: Cisco_93:03:bf (c8:9c:1d:93:03:bf)
▶ Internet Protocol Version 4, Src: 10.112.3.78, Dst: 10.5.20.222
▶ Transmission Control Protocol, Src Port: 43346, Dst Port: 8111, Seq: 1, Ack: 1, Len: 367
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: 10.5.20.222:8111\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:57.0) Gecko/20100101 Firefox/57.0\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
```

```
0000  c8 9c 1d 93 03 bf 3c a8  2a bc 41 da 08 00 45 00   ......<. *.A...E.
0010  01 a3 b8 c9 40 00 40 06  53 eb 0a 70 03 4e 0a 05   ....@.@. S..p.N..
0020  14 de a9 52 1f af ed ad  58 a3 61 34 f4 44 80 18   ...R.... X.a4.D..
0030  00 e5 df fc 00 00 01 01  08 0a 00 22 e0 65 02 e2   ........ ...".e..
0040  f6 b4 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   ..GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  31 30 2e 35 2e 32 30 2e   ..Host:  10.5.20.
0060  32 32 32 3a 38 31 31 31  0d 0a 55 73 65 72 2d 41   222:8111 ..User-A
0070  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
0080  30 20 28 58 31 31 3b 20  55 62 75 6e 74 75 3b 20   0 (X11;  Ubuntu;
0090  4c 69 6e 75 78 20 78 38  36 5f 36 34 3b 20 72 76   Linux x8 6_64; rv
00a0  3a 35 37 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   :57.0) G ecko/201
00b0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 35 37   00101 Fi refox/57
00c0  2e 30 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   .0..Acce pt: text
00d0  2f 68 74 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   /html,ap plicatio
00e0  6e 2f 78 68 74 6d 6c 2b  78 6d 6c 2c 61 70 70 6c   n/xhtml+ xml,appl
00f0  69 63 61 74 69 6f 6e 2f  78 6d 6c 3b 71 3d 30 2e   ication/ xml;q=0.
```

report_http_8111 | Packets: 3107 · Displayed: 31 (1.0%) · Load time: 0:0.59 | Profile: Default

1 d) total page download time from each of these three HTTP server Instances

After allowing subdissector to allow reassemble of tcp stream

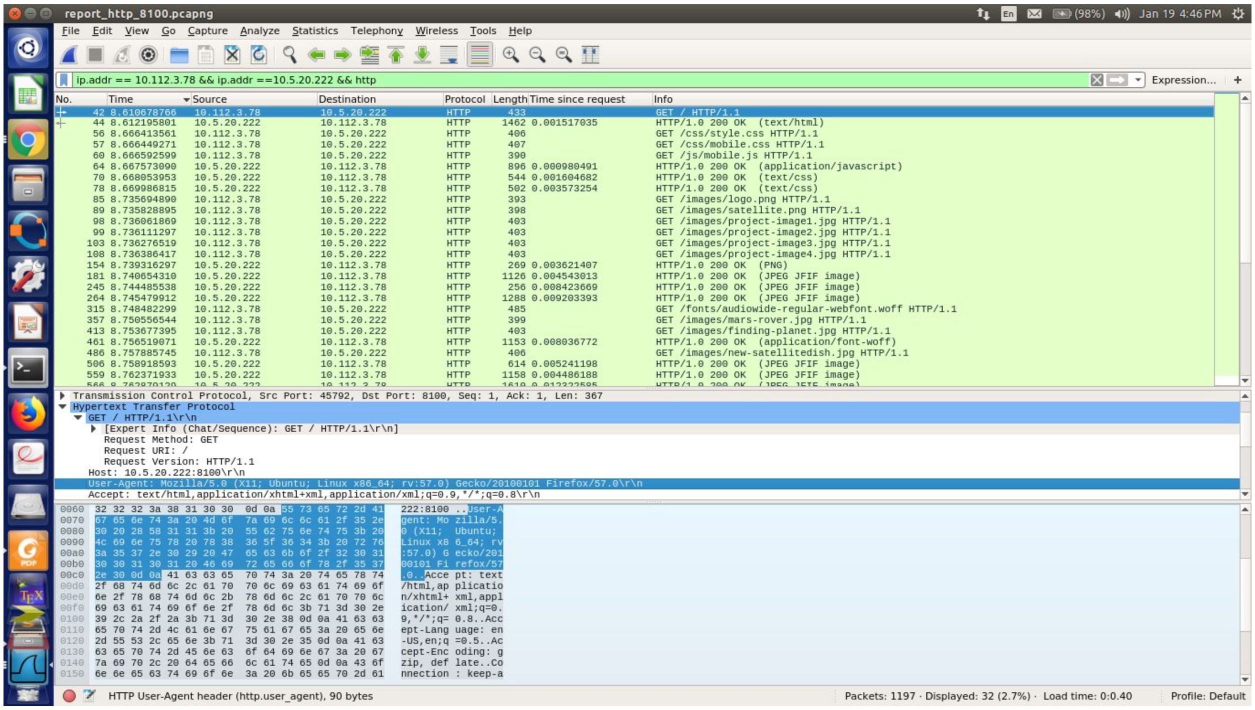
8100: 8.808114035 - 8.610678766 = 0.197435269 sec
8110: 4.556060347 - 4.353175879 = 0.202884468 sec
8111: 4.558633367 - 4.222335189 = 0.336298178 sec

1 (e)

User agent

: Browser

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:57.0) Gecko/20100101 Firefox/57.0\r\n



report_http_8100.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
(98%) Jan 19 4:46 PM
Expression… +

```
ip.addr == 10.112.3.78 && ip.addr ==10.5.20.222 && http
```

```
No.   Time         Source         Destination    Protocol  Length Time since request  Info
   42 8.610678766  10.112.3.78    10.5.20.222    HTTP      433                        GET / HTTP/1.1
   44 8.612195801  10.5.20.222    10.112.3.78    HTTP      1462 0.001517035           HTTP/1.0 200 OK  (text/html)
   56 8.666413561  10.112.3.78    10.5.20.222    HTTP      406                        GET /css/style.css HTTP/1.1
   57 8.666449271  10.112.3.78    10.5.20.222    HTTP      407                        GET /css/mobile.css HTTP/1.1
   60 8.666592599  10.112.3.78    10.5.20.222    HTTP      390                        GET /js/mobile.js HTTP/1.1
   64 8.667573090  10.5.20.222    10.112.3.78    HTTP      896 0.000980491            HTTP/1.0 200 OK  (application/javascript)
   70 8.668053953  10.5.20.222    10.112.3.78    HTTP      544 0.001604682            HTTP/1.0 200 OK  (text/css)
   78 8.669986815  10.5.20.222    10.112.3.78    HTTP      502 0.003573254            HTTP/1.0 200 OK  (text/css)
   85 8.735694890  10.112.3.78    10.5.20.222    HTTP      393                        GET /images/logo.png HTTP/1.1
   89 8.735828895  10.112.3.78    10.5.20.222    HTTP      398                        GET /images/satellite.png HTTP/1.1
   98 8.736061869  10.112.3.78    10.5.20.222    HTTP      403                        GET /images/project-image1.jpg HTTP/1.1
   99 8.736111297  10.112.3.78    10.5.20.222    HTTP      403                        GET /images/project-image2.jpg HTTP/1.1
  103 8.736276519  10.112.3.78    10.5.20.222    HTTP      403                        GET /images/project-image3.jpg HTTP/1.1
  108 8.736386417  10.112.3.78    10.5.20.222    HTTP      403                        GET /images/project-image4.jpg HTTP/1.1
  154 8.739316297  10.5.20.222    10.112.3.78    HTTP      269 0.003621407            HTTP/1.0 200 OK  (PNG)
  181 8.740654310  10.5.20.222    10.112.3.78    HTTP      1126 0.004543013           HTTP/1.0 200 OK  (JPEG JFIF image)
  245 8.744485538  10.5.20.222    10.112.3.78    HTTP      256 0.008423669            HTTP/1.0 200 OK  (JPEG JFIF image)
  264 8.745479912  10.5.20.222    10.112.3.78    HTTP      1288 0.009203393           HTTP/1.0 200 OK  (JPEG JFIF image)
  315 8.748482299  10.112.3.78    10.5.20.222    HTTP      485                        GET /fonts/audiowide-regular-webfont.woff HTTP/1.1
  357 8.750556544  10.112.3.78    10.5.20.222    HTTP      399                        GET /images/mars-rover.jpg HTTP/1.1
  413 8.753677395  10.112.3.78    10.5.20.222    HTTP      403                        GET /images/finding-planet.jpg HTTP/1.1
  461 8.756519071  10.5.20.222    10.112.3.78    HTTP      1153 0.008036772           HTTP/1.0 200 OK  (application/font-woff)
  486 8.757885745  10.112.3.78    10.5.20.222    HTTP      406                        GET /images/new-satellitedish.jpg HTTP/1.1
  506 8.758918593  10.5.20.222    10.112.3.78    HTTP      614 0.005241198            HTTP/1.0 200 OK  (JPEG JFIF image)
  559 8.762371933  10.5.20.222    10.112.3.78    HTTP      1158 0.004486188           HTTP/1.0 200 OK  (JPEG JFIF image)
```

```
▶ Transmission Control Protocol, Src Port: 45792, Dst Port: 8100, Seq: 1, Ack: 1, Len: 367
▼ Hypertext Transfer Protocol
  ▼ GET / HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: 10.5.20.222:8100\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:57.0) Gecko/20100101 Firefox/57.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
```

```
0060  32 32 32 3a 38 31 30 30  0d 0a 55 73 65 72 2d 41   222:8100 ..User-A
0070  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
0080  30 20 28 58 31 31 3b 20  55 62 75 6e 74 75 3b 20   0 (X11;  Ubuntu; 
0090  4c 69 6e 75 78 20 78 38  36 5f 36 34 3b 20 72 76   Linux x8 6_64; rv
00a0  3a 35 37 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   :57.0) G ecko/201
00b0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 35 37   00101 Fi refox/57
00c0  2e 30 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   .0..Acce pt: text
00d0  2f 68 74 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   /html,ap plicatio
00e0  6e 2f 78 68 74 6d 6c 2b  78 6d 6c 2c 61 70 70 6c   n/xhtml+ xml,appl
00f0  69 63 61 74 69 6f 6e 2f  78 6d 6c 3b 71 3d 30 2e   ication/ xml;q=0.
0100  39 2c 2a 2f 2a 3b 71 3d  30 2e 38 0d 0a 41 63 63   9,*/*;q= 0.8..Acc
0110  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a 20 65 6e   ept-Lang uage: en
0120  2d 55 53 2c 65 6e 3b 71  3d 30 2e 35 0d 0a 41 63   -US,en;q =0.5..Ac
0130  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
0140  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 43 6f   zip, def late..Co
0150  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
```

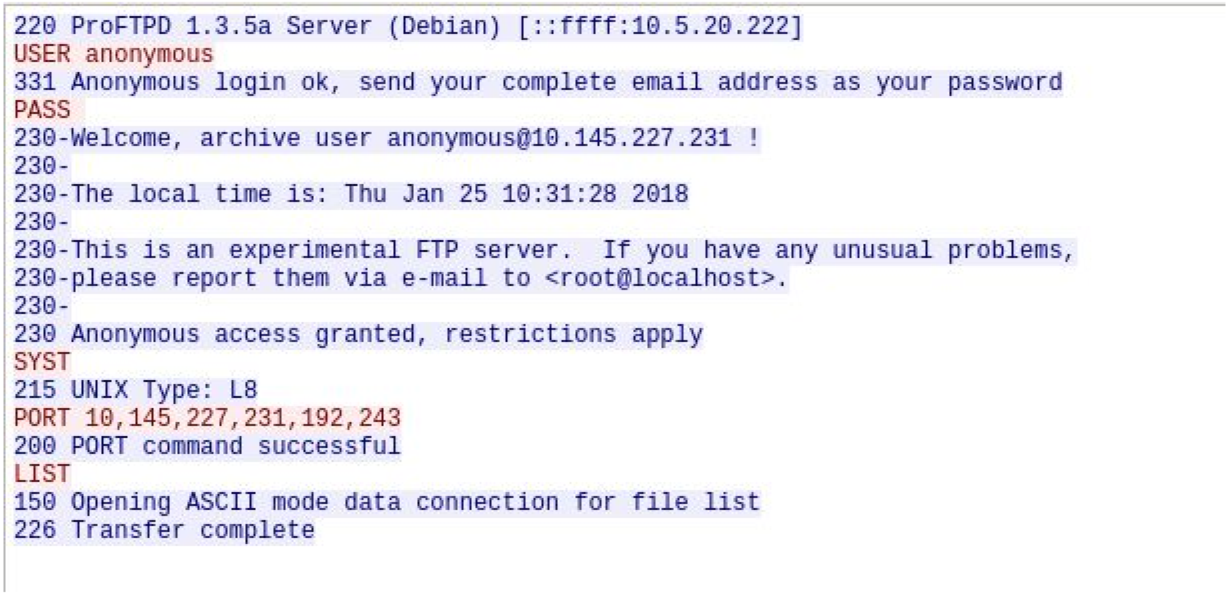
HTTP User-Agent header (http.user_agent), 90 bytes

Packets: 1197 · Displayed: 32 (2.7%) · Load time: 0:0.40

Profile: Default

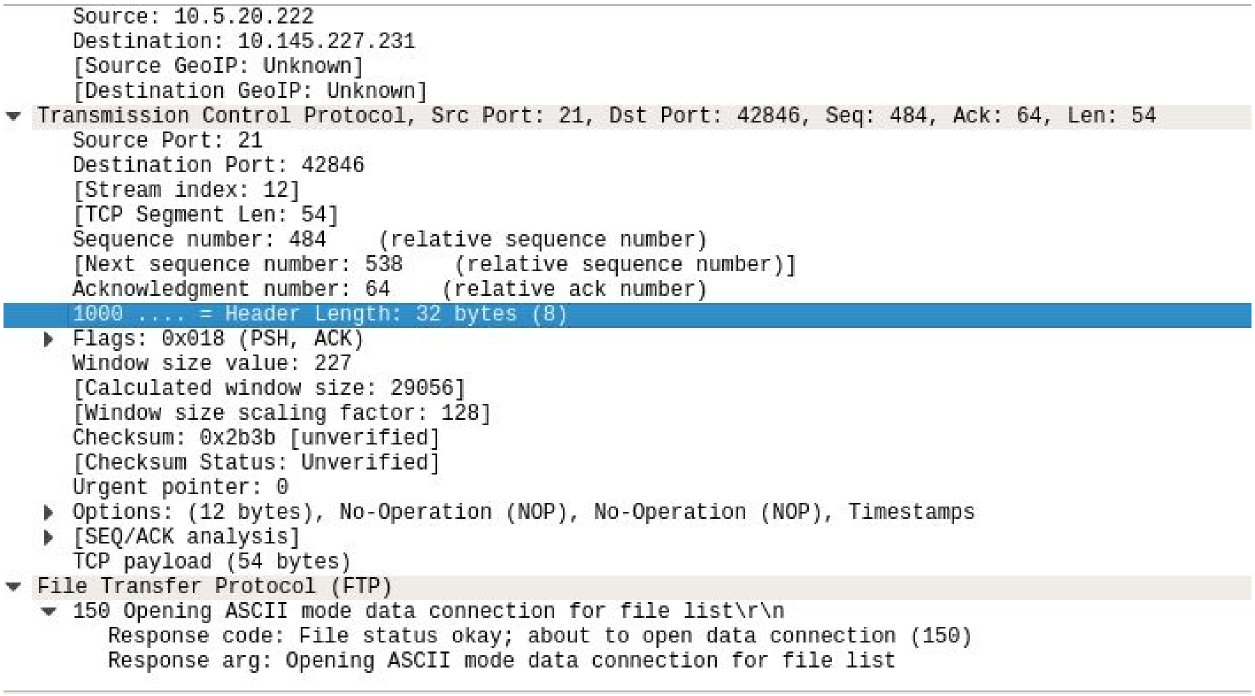
<u>FTP Server :-</u>

2 a) (i) **Active Mode Connection :-**



```
220 ProFTPD 1.3.5a Server (Debian) [::ffff:10.5.20.222]
USER anonymous
331 Anonymous login ok, send your complete email address as your password
PASS 
230-Welcome, archive user anonymous@10.145.227.231 !
230-
230-The local time is: Thu Jan 25 10:31:28 2018
230-
230-This is an experimental FTP server.  If you have any unusual problems,
230-please report them via e-mail to <root@localhost>.
230-
230 Anonymous access granted, restrictions apply
SYST
215 UNIX Type: L8
PORT 10,145,227,231,192,243
200 PORT command successful
LIST
150 Opening ASCII mode data connection for file list
226 Transfer complete
```

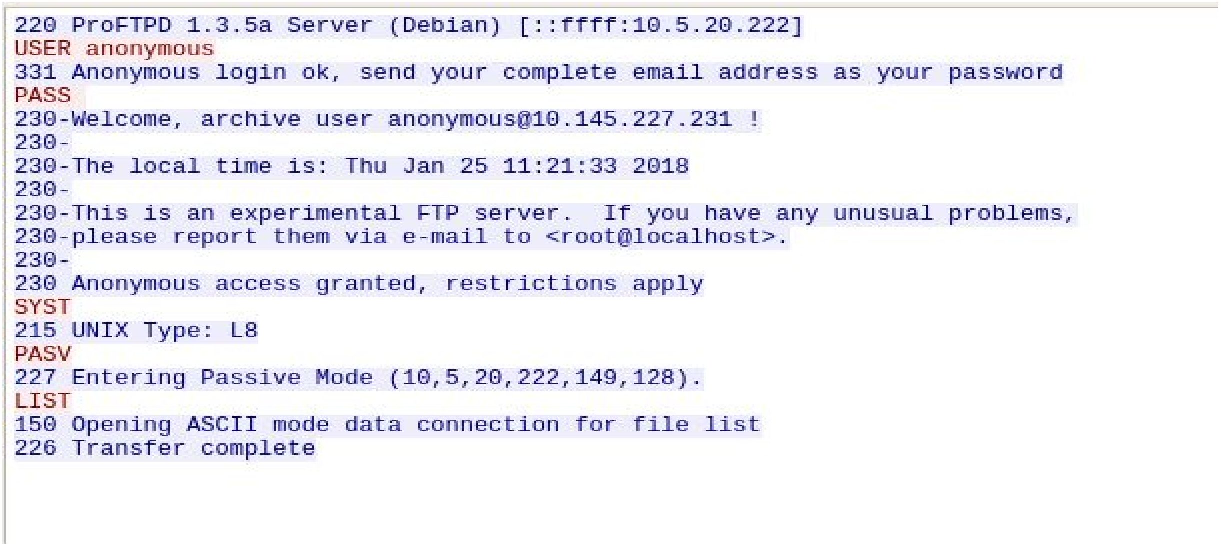
Fig :- Above is the sequence of FTP messages exchanged between server and client along with message type for active mode



```
      Source: 10.5.20.222
      Destination: 10.145.227.231
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
▼ Transmission Control Protocol, Src Port: 21, Dst Port: 42846, Seq: 484, Ack: 64, Len: 54
      Source Port: 21
      Destination Port: 42846
      [Stream index: 12]
      [TCP Segment Len: 54]
      Sequence number: 484    (relative sequence number)
      [Next sequence number: 538    (relative sequence number)]
      Acknowledgment number: 64    (relative ack number)
      1000 .... = Header Length: 32 bytes (8)
   ▶ Flags: 0x018 (PSH, ACK)
      Window size value: 227
      [Calculated window size: 29056]
      [Window size scaling factor: 128]
      Checksum: 0x2b3b [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
   ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
   ▶ [SEQ/ACK analysis]
      TCP payload (54 bytes)
▼ File Transfer Protocol (FTP)
   ▼ 150 Opening ASCII mode data connection for file list\r\n
         Response code: File status okay; about to open data connection (150)
         Response arg: Opening ASCII mode data connection for file list
```

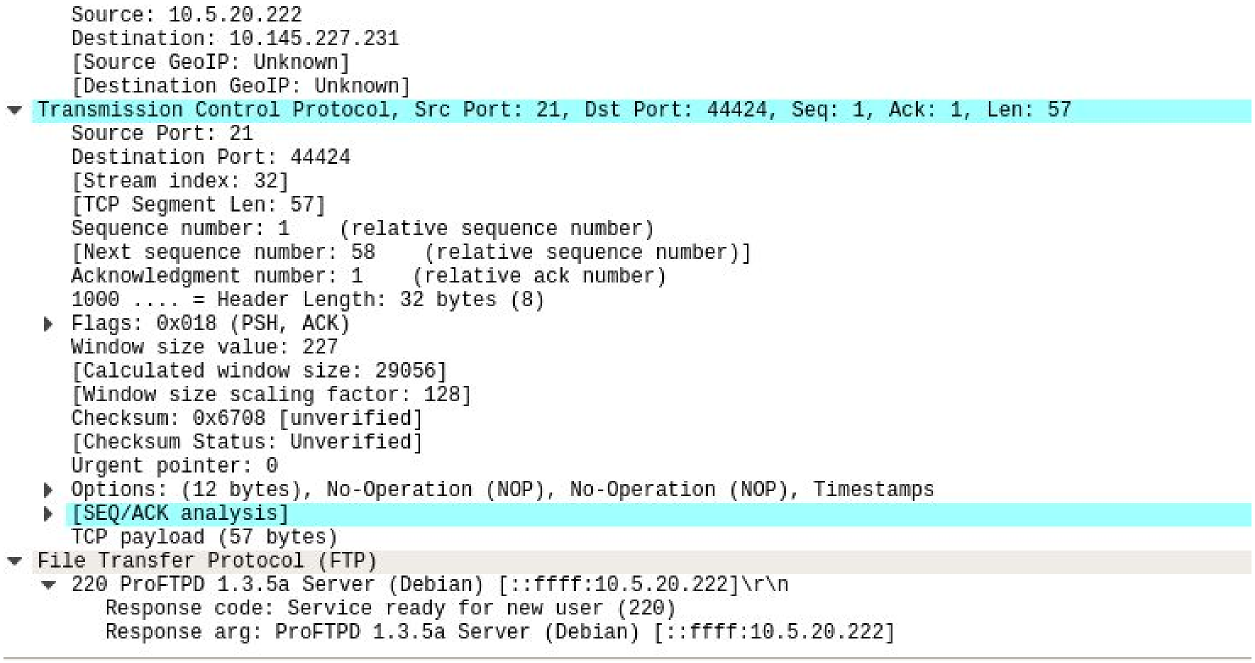
Fig :- FTP header fields, source IP, destination IP, source port and destination port for command channel can be inferred from the above image for active mode

(ii) **Passive Mode Connection :-**



```
220 ProFTPD 1.3.5a Server (Debian) [::ffff:10.5.20.222]
USER anonymous
331 Anonymous login ok, send your complete email address as your password
PASS
230-Welcome, archive user anonymous@10.145.227.231 !
230-
230-The local time is: Thu Jan 25 11:21:33 2018
230-
230-This is an experimental FTP server.  If you have any unusual problems,
230-please report them via e-mail to <root@localhost>.
230-
230 Anonymous access granted, restrictions apply
SYST
215 UNIX Type: L8
PASV
227 Entering Passive Mode (10,5,20,222,149,128).
LIST
150 Opening ASCII mode data connection for file list
226 Transfer complete
```

Fig :- Above is the sequence of FTP messages exchanged between server and client along with message type for passive mode



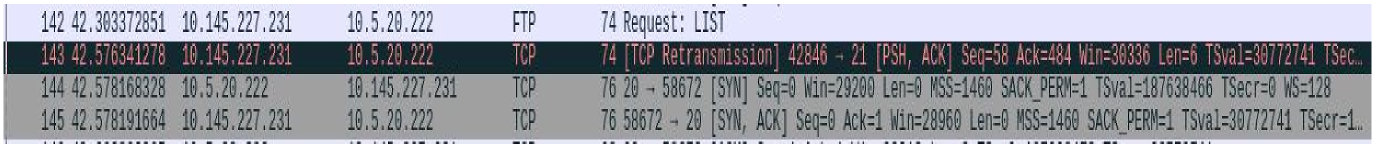
```
    Source: 10.5.20.222
    Destination: 10.145.227.231
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ Transmission Control Protocol, Src Port: 21, Dst Port: 44424, Seq: 1, Ack: 1, Len: 57
    Source Port: 21
    Destination Port: 44424
    [Stream index: 32]
    [TCP Segment Len: 57]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 58    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  ▶ Flags: 0x018 (PSH, ACK)
    Window size value: 227
    [Calculated window size: 29056]
    [Window size scaling factor: 128]
    Checksum: 0x6708 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ [SEQ/ACK analysis]
    TCP payload (57 bytes)
▼ File Transfer Protocol (FTP)
  ▼ 220 ProFTPD 1.3.5a Server (Debian) [::ffff:10.5.20.222]\r\n
      Response code: Service ready for new user (220)
      Response arg: ProFTPD 1.3.5a Server (Debian) [::ffff:10.5.20.222]
```

Fig :- FTP header fields, source IP, destination IP, source port and destination port for command channel can be inferred from the above image for passive mode

2 b) (i) **Active Mode Connection :-**

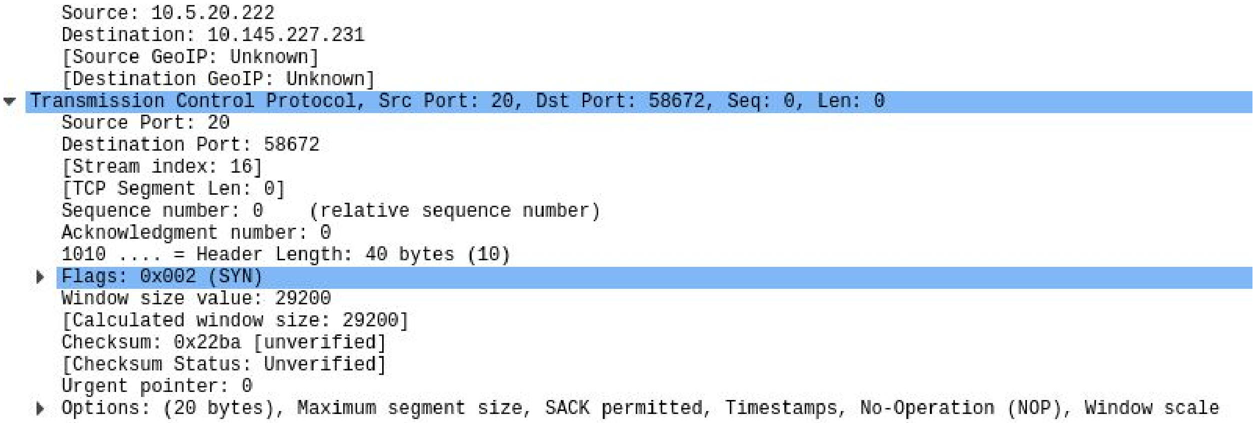
Difference between data channel and communication channel :-

Data channel is used to transfer file data or query data between server and client. Communication channel is used to transfer requests and acknowledgment between server and client.



```
142 42.303372851  10.145.227.231   10.5.20.222      FTP   74 Request: LIST
143 42.576341278  10.145.227.231   10.5.20.222      TCP   74 [TCP Retransmission] 42846 → 21 [PSH, ACK] Seq=58 Ack=484 Win=30336 Len=6 TSval=30772741 TSec…
144 42.578168328  10.5.20.222      10.145.227.231   TCP   76 20 → 58672 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=187638466 TSecr=0 WS=128
145 42.578191664  10.145.227.231   10.5.20.222      TCP   76 58672 → 20 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=30772741 TSecr=1…
```

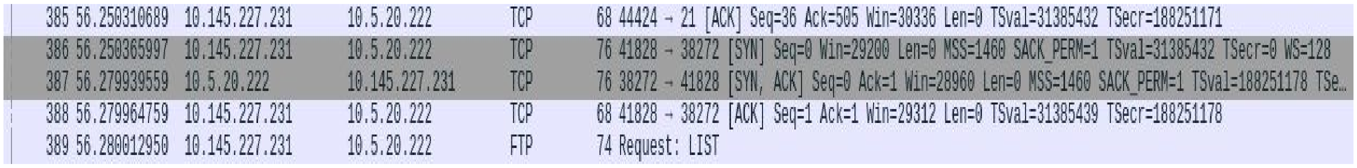
Fig :- The above fig shows that in active mode on getting a List request, the server initiates a data channel from port 20 to port 58672. The client acknowledges this request and a data channel is established.



```
      Source: 10.5.20.222
      Destination: 10.145.227.231
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
▼ Transmission Control Protocol, Src Port: 20, Dst Port: 58672, Seq: 0, Len: 0
      Source Port: 20
      Destination Port: 58672
      [Stream index: 16]
      [TCP Segment Len: 0]
      Sequence number: 0    (relative sequence number)
      Acknowledgment number: 0
      1010 .... = Header Length: 40 bytes (10)
   ▶ Flags: 0x002 (SYN)
      Window size value: 29200
      [Calculated window size: 29200]
      Checksum: 0x22ba [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
   ▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
```

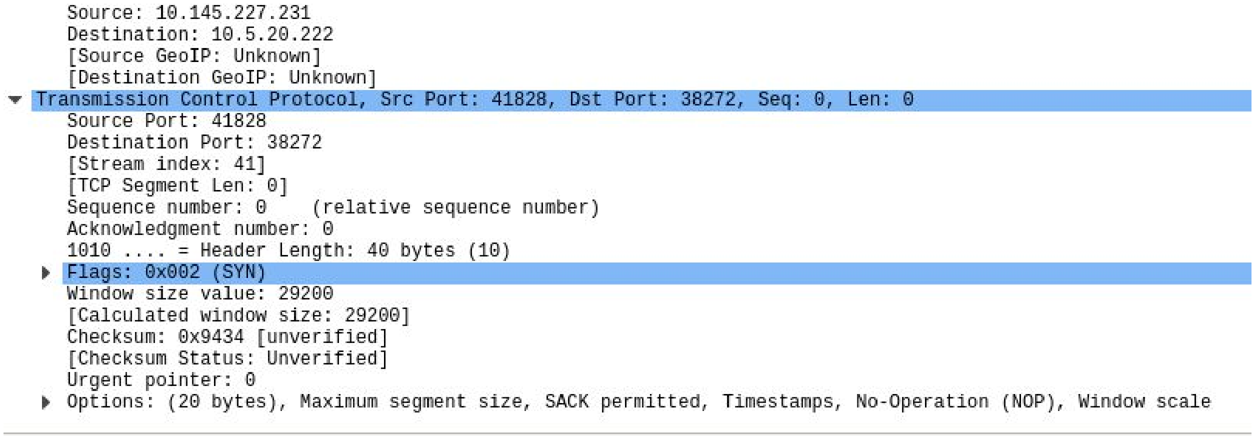
Fig :- The data communication channel established between port 20(server side) and port 58672(client side) in active mode.

(ii) **Passive Mode Communication :-**



```
385 56.250310689  10.145.227.231    10.5.20.222       TCP     68 44424 → 21 [ACK] Seq=36 Ack=505 Win=30336 Len=0 TSval=31385432 TSecr=188251171
386 56.250365997  10.145.227.231    10.5.20.222       TCP     76 41828 → 38272 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=31385432 TSecr=0 WS=128
387 56.279939559  10.5.20.222       10.145.227.231    TCP     76 38272 → 41828 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=188251178 TSe…
388 56.279964759  10.145.227.231    10.5.20.222       TCP     68 41828 → 38272 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=31385439 TSecr=188251178
389 56.280012950  10.145.227.231    10.5.20.222       FTP     74 Request: LIST
```

Fig :- The above fig shows that in passive mode, before sending the List request, the client first initiates a data channel from port 41828 to port 38272. The server acknowledges this request and a data channel is established



```
      Source: 10.145.227.231
      Destination: 10.5.20.222
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
▼ Transmission Control Protocol, Src Port: 41828, Dst Port: 38272, Seq: 0, Len: 0
      Source Port: 41828
      Destination Port: 38272
      [Stream index: 41]
      [TCP Segment Len: 0]
      Sequence number: 0    (relative sequence number)
      Acknowledgment number: 0
      1010 .... = Header Length: 40 bytes (10)
   ▶ Flags: 0x002 (SYN)
      Window size value: 29200
      [Calculated window size: 29200]
      Checksum: 0x9434 [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
   ▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
```

Fig :- The data communication channel established between port 38272(server side) and port 41828(client side) in passive mode.

2 c) **Active Mode Connection :-**

Port used for communication in active mode is :- 20(server side)
58672(client side)

Passive Mode Connection :-

Port used for communication in passive mode is :- 38272(server side)
41828(client side)

When the user enables the passive mode the data channel is initiated by the client in place of the server as in the active connection case. From 2)b) we can see the difference in initiation of the data channel in the case of active connection and passive connection.