CS526 Information Security- Project 2

hegde12@purdue.edu

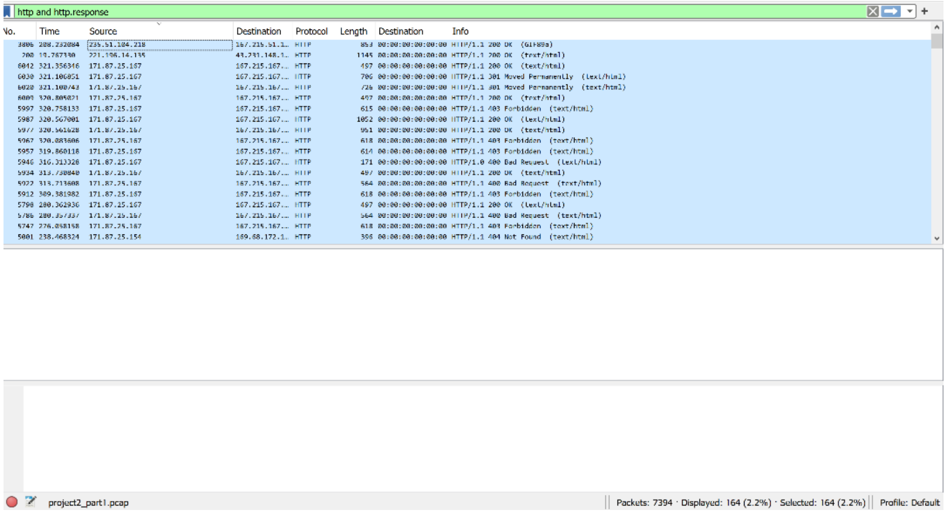
Problem 1

a. HTTPS Session
Successfully visited ips:

235.51.104.218
221.196.14.135
171.87.25.167
171.87.25.154
171.87.25.134
171.54.85.171
171.38.206.203
171.38.206.134
171.38.194.75
171.118.85.218
169.231.16.199
169.215.245.198
169.215.245.165
169.102.199.170
169.100.175.166
169.100.167.250
167.87.119.134
167.86.245.153
167.70.230.107
167.119.105.170
167.103.51.138
157.54.163.75
157.54.163.135
137.79.61.203
137.54.75.155
137.245.108.202
135.54.222.170
109.85.130.234
109.85.130.199
107.70.210.154
107.70.10.71
107.39.238.234
105.71.216.186
105.55.89.170
105.55.3.171
103.245.209.202

(Count – 36)

Filter used – "http and http.response"
What it does – Displays only the http packets where the server has sent back some response code
Rationale – If servers are 'successfully visited', they must have sent some response code

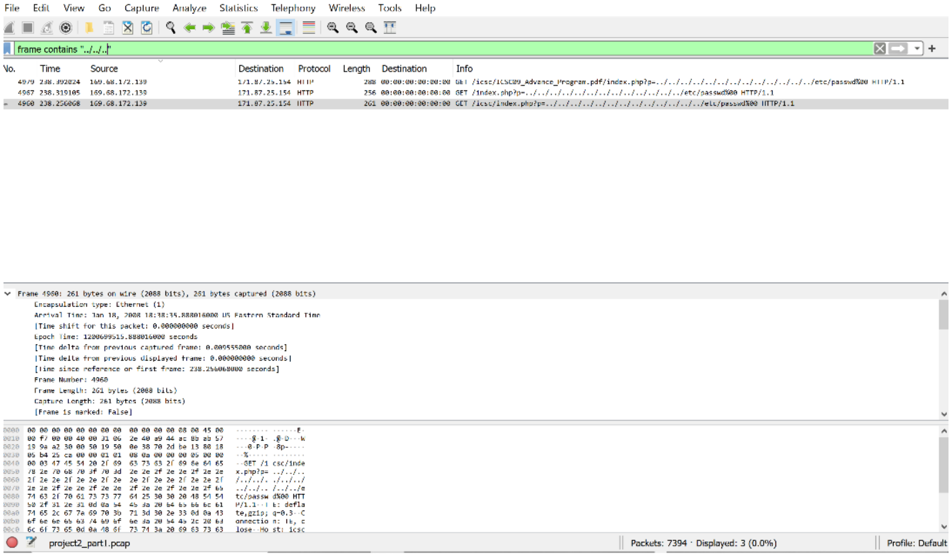


http and http.response

```
No.   Time         Source            Destination     Protocol  Length  Destination        Info
 3806 208.232084   235.51.104.218    167.215.51.1..  HTTP         853  00:00:00:00:00:00  HTTP/1.1 200 OK  (GIF89a)
  200 19.767330    221.196.14.135    43.231.148.1..  HTTP        1145  00:00:00:00:00:00  HTTP/1.1 200 OK  (text/html)
 6042 321.356346   171.87.25.167     167.215.167...  HTTP         497  00:00:00:00:00:00  HTTP/1.1 200 OK  (text/html)
 6030 321.106051   171.87.25.167     167.215.167...  HTTP         706  00:00:00:00:00:00  HTTP/1.1 301 Moved Permanently  (text/html)
 6020 321.100743   171.87.25.167     167.215.167...  HTTP         726  00:00:00:00:00:00  HTTP/1.1 301 Moved Permanently  (text/html)
 6009 320.805021   171.87.25.167     167.215.167...  HTTP         497  00:00:00:00:00:00  HTTP/1.1 200 OK  (text/html)
 5997 320.758133   171.87.25.167     167.215.167...  HTTP         615  00:00:00:00:00:00  HTTP/1.1 403 Forbidden  (text/html)
 5987 320.567001   171.87.25.167     167.215.167...  HTTP        1052  00:00:00:00:00:00  HTTP/1.1 200 OK  (text/html)
 5977 320.561628   171.87.25.167     167.215.167...  HTTP         951  00:00:00:00:00:00  HTTP/1.1 200 OK  (text/html)
 5967 320.083606   171.87.25.167     167.215.167...  HTTP         618  00:00:00:00:00:00  HTTP/1.1 403 Forbidden  (text/html)
 5957 319.860118   171.87.25.167     167.215.167...  HTTP         614  00:00:00:00:00:00  HTTP/1.1 403 Forbidden  (text/html)
 5946 316.313326   171.87.25.167     167.215.167...  HTTP         171  00:00:00:00:00:00  HTTP/1.0 400 Bad Request  (text/html)
 5934 313.730840   171.87.25.167     167.215.167...  HTTP         497  00:00:00:00:00:00  HTTP/1.1 200 OK  (text/html)
 5922 313.713608   171.87.25.167     167.215.167...  HTTP         564  00:00:00:00:00:00  HTTP/1.1 400 Bad Request  (text/html)
 5912 309.381982   171.87.25.167     167.215.167...  HTTP         618  00:00:00:00:00:00  HTTP/1.1 403 Forbidden  (text/html)
 5798 280.362936   171.87.25.167     167.215.167...  HTTP         497  00:00:00:00:00:00  HTTP/1.1 200 OK  (text/html)
 5786 280.357337   171.87.25.167     167.215.167...  HTTP         564  00:00:00:00:00:00  HTTP/1.1 400 Bad Request  (text/html)
 5747 276.058158   171.87.25.167     167.215.167...  HTTP         618  00:00:00:00:00:00  HTTP/1.1 403 Forbidden  (text/html)
 5001 238.468324   171.87.25.154     169.68.172.1..  HTTP         396  00:00:00:00:00:00  HTTP/1.1 404 Not Found  (text/html)
```

project2_part1.pcap | Packets: 7394 · Displayed: 164 (2.2%) · Selected: 164 (2.2%) | Profile: Default

2. Directory Traversal
   Host - 169.68.172.139
   Filter used – 'frame contains "../../.." '
   What it does – Displays only the packets that would have the particular string in it's frame
   Rationale – For directory traversal, the attacker must have sent traversal string "../../.." at some point.



frame contains "../../.."

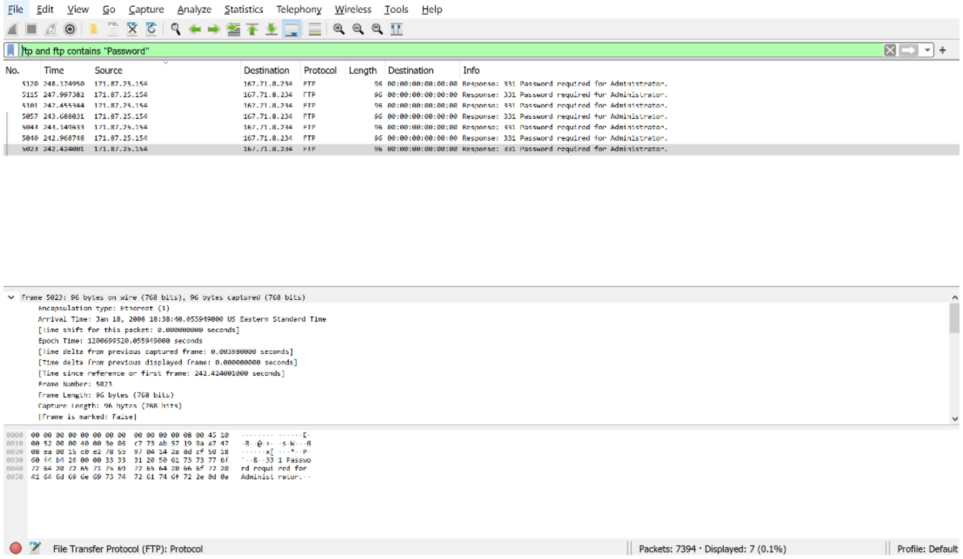
```
No.   Time         Source            Destination     Protocol  Length  Destination        Info
 4979 238.392824   169.68.172.139    171.87.25.154   HTTP         288  00:00:00:00:00:00  GET /icsc/ICSC09_Advance_Program.pdf/index.php?p=../../../../../../../../../../../../../etc/passwd%00 HTTP/1.1
 4967 238.319105   169.68.172.139    171.87.25.154   HTTP         256  00:00:00:00:00:00  GET /index.php?p=../../../../../../../../../../../../../etc/passwd%00 HTTP/1.1
 4960 238.256068   169.68.172.139    171.87.25.154   HTTP         261  00:00:00:00:00:00  GET /icsc/index.php?p=../../../../../../../../../../../../../etc/passwd%00 HTTP/1.1
```

```
Frame 4960: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 18, 2008 18:38:35.888016000 US Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1200699515.888016000 seconds
    [Time delta from previous captured frame: 0.009555000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 238.256068000 seconds]
    Frame Number: 4960
    Frame Length: 261 bytes (2088 bits)
    Capture Length: 261 bytes (2088 bits)
    [Frame is marked: False]
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ········ ······E·
0010  00 f7 00 00 40 00 31 06  2e 40 a9 44 ac 0b ab 57   ····@·1· .@·D···W
0020  19 9a a2 30 00 50 19 50  0e 38 70 2d be 13 80 18   ···0·P·P ·8p-····
0030  05 b4 25 ca 00 00 01 01  08 0a 00 00 00 05 00 00   ··%····· ········
0040  00 03 47 45 54 20 2f 69  63 73 63 2f 69 6e 64 65   ··GET /i csc/inde
0050  78 2e 70 68 70 3f 70 3d  2e 2e 2f 2e 2e 2f 2e 2e   x.php?p= ../../..
0060  2f 2e 2e 2f 2e 2e 2f 2e  2e 2f 2e 2e 2f 2e 2e 2f   /../../. ./../../
0070  2e 2e 2f 2e 2e 2f 2e 2e  2f 2e 2e 2f 2e 2e 2f 65   ../../.. /../../e
0080  74 63 2f 70 61 73 73 77  64 25 30 30 20 48 54 54   tc/passw d%00 HTT
0090  50 2f 31 2e 31 0d 0a 54  45 3a 20 64 65 66 6c 61   P/1.1··T E: defla
00a0  74 65 2c 67 7a 69 70 3b  71 3d 30 2e 33 0d 0a 43   te,gzip; q=0.3··C
00b0  6f 6e 6e 65 63 74 69 6f  6e 3a 20 54 45 2c 20 63   onnectio n: TE, c
00c0  6c 6f 73 65 0d 0a 48 6f  73 74 3a 20 69 63 73 63   lose··Ho st: icsc
```

project2_part1.pcap | Packets: 7394 · Displayed: 3 (0.0%) | Profile: Default

3. Password Guessing
   Host – '167.71.8.234'
   Filter used – 'ftp and ftp contains "Password" '
   What it does – Displays only the ftp packets that have the word 'Password' in it
   Rationale – For password guessing, there must be requests/responses with the word "Pass" in it



```
ftp and ftp contains "Password"
```

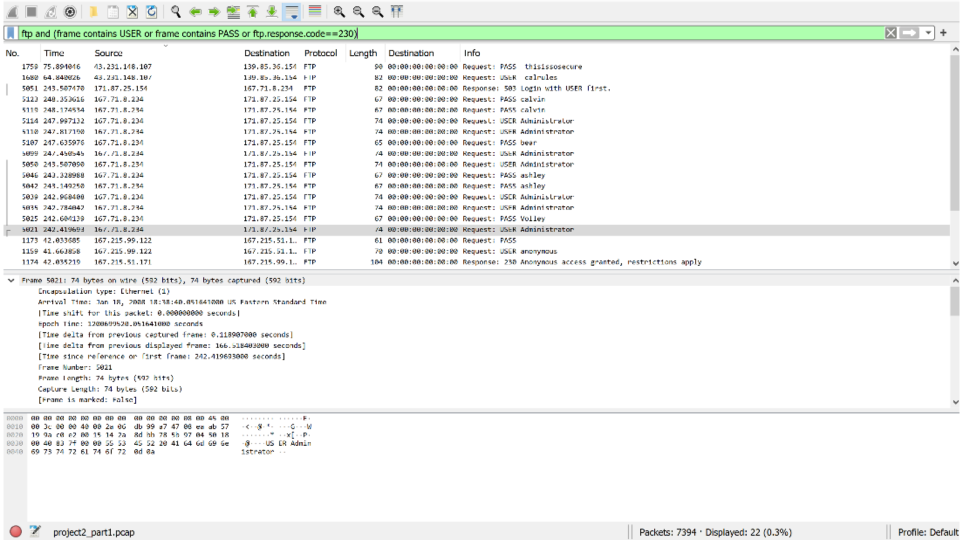
```
No.   Time        Source          Destination   Protocol Length Destination       Info
 5120 248.174950  171.87.25.154   167.71.8.234  FTP          96 00:00:00:00:00:00 Response: 331 Password required for Administrator.
 5115 247.997382  171.87.25.154   167.71.8.234  FTP          96 00:00:00:00:00:00 Response: 331 Password required for Administrator.
 5101 247.455344  171.87.25.154   167.71.8.234  FTP          96 00:00:00:00:00:00 Response: 331 Password required for Administrator.
 5057 243.688031  171.87.25.154   167.71.8.234  FTP          96 00:00:00:00:00:00 Response: 331 Password required for Administrator.
 5043 243.149633  171.87.25.154   167.71.8.234  FTP          96 00:00:00:00:00:00 Response: 331 Password required for Administrator.
 5040 242.968746  171.87.25.154   167.71.8.234  FTP          96 00:00:00:00:00:00 Response: 331 Password required for Administrator.
 5023 242.424001  171.87.25.154   167.71.8.234  FTP          96 00:00:00:00:00:00 Response: 331 Password required for Administrator.
```

```
Frame 5023: 96 bytes on wire (768 bits), 96 bytes captured (768 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 18, 2008 18:38:40.055949000 US Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1200699520.055949000 seconds
    [Time delta from previous captured frame: 0.003980000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 242.424001000 seconds]
    Frame Number: 5023
    Frame Length: 96 bytes (768 bits)
    Capture Length: 96 bytes (768 bits)
    [Frame is marked: False]
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 10   ········ ······E·
0010  00 52 00 00 40 00 3e 06  c7 73 ab 57 19 9a a7 47   ·R··@·>· ·s·W···G
0020  08 ea 00 15 c0 e2 78 5b  97 04 14 2a 8d cf 50 18   ······x[ ···*··P·
0030  60 f4 b4 26 00 00 33 33  31 20 50 61 73 73 77 6f   `··&··33 1 Passwo
0040  72 64 20 72 65 71 75 69  72 65 64 20 66 6f 72 20   rd requi red for 
0050  41 64 6d 69 6e 69 73 74  72 61 74 6f 72 2e 0d 0a   Administ rator.··
```

File Transfer Protocol (FTP): Protocol | Packets: 7394 · Displayed: 7 (0.1%) | Profile: Default

4. Unencrypted Usernames and Passwords
   Username : ‘calrules’
   Password: ‘thisissosecure’
   Filter used – ‘ftp and (frame contains USER or frame contains PASS or ftp.response.code==230)’
   What it does – Displays only the ftp packets that have either ‘USER’ or ‘PASS’ in it or have an ftp response code of 230
   Rationale – We want all packets that either send username and password or give a success response



```
ftp and (frame contains USER or frame contains PASS or ftp.response.code==230)
```

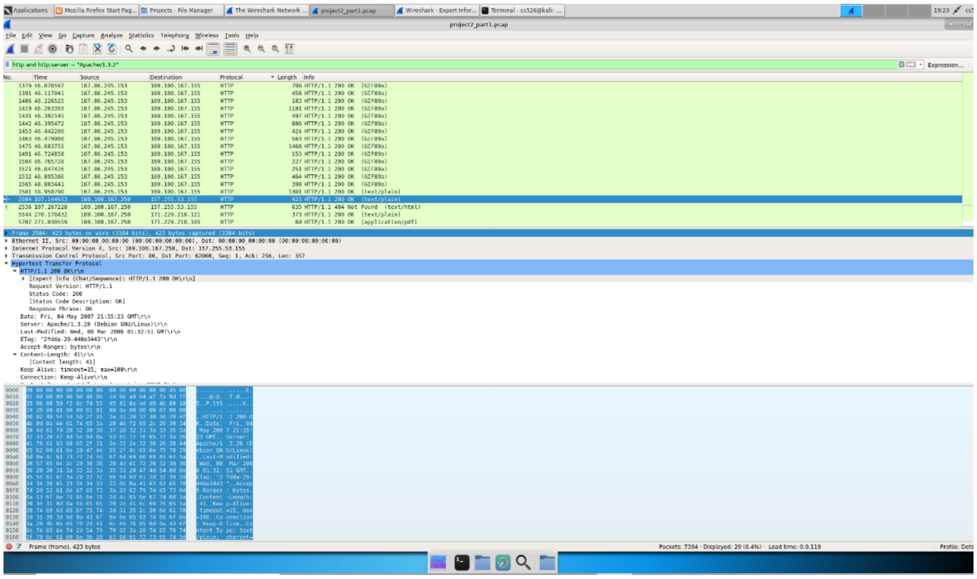
```
No.   Time        Source          Destination     Protocol Length Destination       Info
 1759 75.894046   43.231.148.107  139.85.36.154   FTP          90 00:00:00:00:00:00 Request: PASS  thisissosecure
 1680 64.840026   43.231.148.107  139.85.36.154   FTP          82 00:00:00:00:00:00 Request: USER  calrules
 5051 243.507470  171.87.25.154   167.71.8.234    FTP          82 00:00:00:00:00:00 Response: 503 Login with USER first.
 5123 248.353616  167.71.8.234    171.87.25.154   FTP          67 00:00:00:00:00:00 Request: PASS calvin
 5119 248.174534  167.71.8.234    171.87.25.154   FTP          67 00:00:00:00:00:00 Request: PASS calvin
 5114 247.997132  167.71.8.234    171.87.25.154   FTP          74 00:00:00:00:00:00 Request: USER Administrator
 5110 247.817190  167.71.8.234    171.87.25.154   FTP          74 00:00:00:00:00:00 Request: USER Administrator
 5107 247.635976  167.71.8.234    171.87.25.154   FTP          65 00:00:00:00:00:00 Request: PASS bear
 5099 247.450545  167.71.8.234    171.87.25.154   FTP          74 00:00:00:00:00:00 Request: USER Administrator
 5050 243.507090  167.71.8.234    171.87.25.154   FTP          74 00:00:00:00:00:00 Request: USER Administrator
 5046 243.328988  167.71.8.234    171.87.25.154   FTP          67 00:00:00:00:00:00 Request: PASS ashley
 5042 243.149250  167.71.8.234    171.87.25.154   FTP          67 00:00:00:00:00:00 Request: PASS ashley
 5039 242.968400  167.71.8.234    171.87.25.154   FTP          74 00:00:00:00:00:00 Request: USER Administrator
 5035 242.784042  167.71.8.234    171.87.25.154   FTP          74 00:00:00:00:00:00 Request: USER Administrator
 5025 242.604139  167.71.8.234    171.87.25.154   FTP          67 00:00:00:00:00:00 Request: PASS Volley
 5021 242.419693  167.71.8.234    171.87.25.154   FTP          74 00:00:00:00:00:00 Request: USER Administrator
 1173 42.033685   167.215.99.122  167.215.51.1…   FTP          61 00:00:00:00:00:00 Request: PASS
 1159 41.663858   167.215.99.122  167.215.51.1…   FTP          70 00:00:00:00:00:00 Request: USER anonymous
 1174 42.035219   167.215.51.171  167.215.99.1…   FTP         104 00:00:00:00:00:00 Response: 230 Anonymous access granted, restrictions apply
```

```
Frame 5021: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 18, 2008 18:38:40.051641000 US Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1200699520.051641000 seconds
    [Time delta from previous captured frame: 0.118907000 seconds]
    [Time delta from previous displayed frame: 166.518403000 seconds]
    [Time since reference or first frame: 242.419693000 seconds]
    Frame Number: 5021
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ········ ······E·
0010  00 3c 00 00 40 00 2a 06  db 99 a7 47 00 ea ab 57   ·<··@·*· ···G···W
0020  19 9a c0 e2 00 15 14 2a  8d bb 78 5b 97 04 50 18   ·······* ··x[··P·
0030  00 40 83 7f 00 00 55 53  45 52 20 41 64 6d 69 6e   ·@····US ER Admin
0040  69 73 74 72 61 74 6f 72  0d 0a                    istrator ··
```

project2_part1.pcap | Packets: 7394 · Displayed: 22 (0.3%) | Profile: Default

5. Service Versions
   Host ip – 169.100.167.250
   Version – Apache/1.3.29
   Filter Used – ‘http and http.server ~ "Apache/1.3.2"’
   What it does –Displays only the http packets that have an Apache server whose name matches a part of the string ‘*Apache/1.3.2’*
   Rationale – Oldest version of Apache is 1.3



```
http and http.server ~ "Apache/1.3.2"
No.   Time        Source           Destination      Protocol  Length Info
 1379 46.076597   167.86.245.153   169.100.167.155  HTTP       708 HTTP/1.1 200 OK  (GIF89a)
 1391 46.117041   167.86.245.153   169.100.167.155  HTTP       458 HTTP/1.1 200 OK  (GIF89a)
 1406 46.226525   167.86.245.153   169.100.167.155  HTTP       183 HTTP/1.1 200 OK  (GIF89a)
 1419 46.263393   167.86.245.153   169.100.167.155  HTTP      1101 HTTP/1.1 200 OK  (GIF89a)
 1431 46.302145   167.86.245.153   169.100.167.155  HTTP       497 HTTP/1.1 200 OK  (GIF89a)
 1442 46.395472   167.86.245.153   169.100.167.155  HTTP       806 HTTP/1.1 200 OK  (GIF89a)
 1453 46.442280   167.86.245.153   169.100.167.155  HTTP       424 HTTP/1.1 200 OK  (GIF89a)
 1463 46.479900   167.86.245.153   169.100.167.155  HTTP       563 HTTP/1.1 200 OK  (GIF89a)
 1475 46.683755   167.86.245.153   169.100.167.155  HTTP      1468 HTTP/1.1 200 OK  (GIF89a)
 1491 46.724858   167.86.245.153   169.100.167.155  HTTP       153 HTTP/1.1 200 OK  (GIF89a)
 1504 46.765728   167.86.245.153   169.100.167.155  HTTP       227 HTTP/1.1 200 OK  (GIF89a)
 1521 46.847426   167.86.245.153   169.100.167.155  HTTP       251 HTTP/1.1 200 OK  (GIF89a)
 1532 46.895386   167.86.245.153   169.100.167.155  HTTP       464 HTTP/1.1 200 OK  (GIF89a)
 1565 48.803441   167.86.245.153   169.100.167.155  HTTP       398 HTTP/1.1 200 OK  (GIF89a)
 1581 48.950790   167.86.245.153   169.100.167.155  HTTP      1301 HTTP/1.1 200 OK  (text/plain)
 2504 107.144653  169.100.167.250  157.255.53.155   HTTP       423 HTTP/1.1 200 OK  (text/plain)
 2536 107.267228  169.100.167.250  157.255.53.155   HTTP       635 HTTP/1.1 404 Not Found  (text/html)
 5544 270.178432  169.100.167.250  171.229.218.121  HTTP       373 HTTP/1.1 200 OK  (text/plain)
 5782 271.830559  169.100.167.250  171.229.218.185  HTTP        69 HTTP/1.1 200 OK  (application/pdf)

▸ Frame 2504: 423 bytes on wire (3384 bits), 423 bytes captured (3384 bits)
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 169.100.167.250, Dst: 157.255.53.155
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 62060, Seq: 1, Ack: 256, Len: 357
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    ▸ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Fri, 04 May 2007 21:35:23 GMT\r\n
    Server: Apache/1.3.28 (Debian GNU/Linux)\r\n
    Last-Modified: Wed, 08 Mar 2006 01:32:51 GMT\r\n
    ETag: "2fdda-29-440e3443"\r\n
    Accept-Ranges: bytes\r\n
  ▾ Content-Length: 41\r\n
      [Content length: 41]
    Keep-Alive: timeout=15, max=100\r\n
    Connection: Keep-Alive\r\n

0000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 45 00   ........ ......E.
0010  01 99 00 00 40 00 40 06  14 66 a9 64 a7 fa 9d ff   ....@.@. .f.d....
0020  35 9b 00 50 f2 6c 74 53  d5 81 8e ad d9 4b 80 18   5..P.ltS .....K..
0030  19 20 00 01 00 00 01 01  08 0a 00 00 00 07 00 00   . ...... ........
0040  00 02 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   ..HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 46 72 69 2c 20 30 34   K..Date:  Fri, 04
0060  20 4d 61 79 20 32 30 30  37 20 32 31 3a 33 35 3a    May 200 7 21:35:
0070  32 33 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   23 GMT.. Server: 
0080  41 70 61 63 68 65 2f 31  2e 33 2e 32 38 20 28 44   Apache/1 .3.28 (D
0090  65 62 69 61 6e 20 47 4e  55 2f 4c 69 6e 75 78 29   ebian GN U/Linux)
00a0  0d 0a 4c 61 73 74 2d 4d  6f 64 69 66 69 65 64 3a   ..Last-M odified:
00b0  20 57 65 64 2c 20 30 38  20 4d 61 72 20 32 30 30    Wed, 08  Mar 200
00c0  36 20 30 31 3a 33 32 3a  35 31 20 47 4d 54 0d 0a   6 01:32: 51 GMT..
00d0  45 54 61 67 3a 20 22 32  66 64 64 61 2d 32 39 2d   ETag: "2 fdda-29-
00e0  34 34 30 65 33 34 34 33  22 0d 0a 41 63 63 65 70   440e3443 "..Accep

Frame (frame), 423 bytes        Packets: 7394 · Displayed: 29 (0.4%) · Load time: 0:0.119        Profile: Defa
```

6. DNS and Source Port Randomization

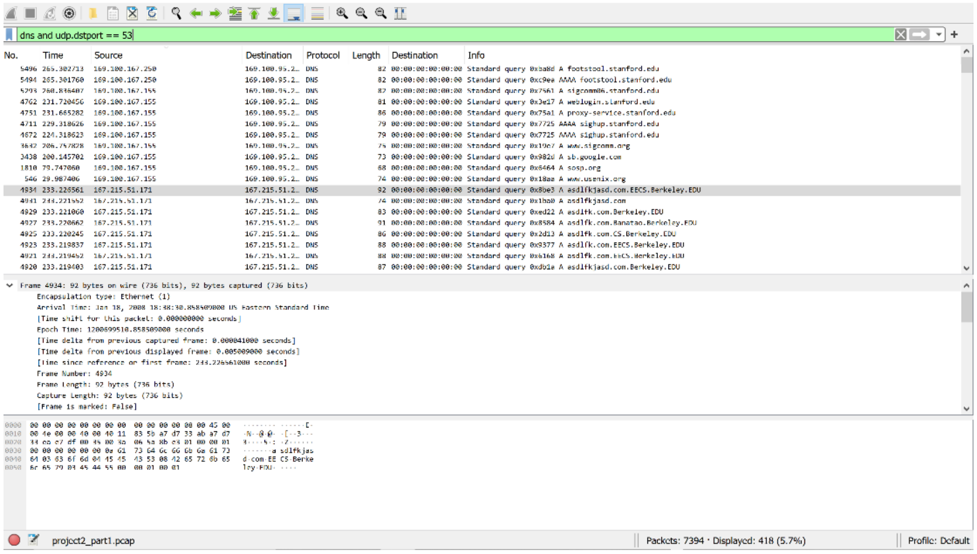
Host ip - 169.100.167.155 and 169.100.167.250

Src Port – 32927 and 33814 respectively

Filter Used – 'dns and udp.dstport == 53'

What it does – Displays only the dns packets that have their udp destination port address as 53

Rationale – DNS queries are sent with destination port set to 53



```
dns and udp.dstport == 53
No.   Time        Source           Destination      Protocol  Length Destination        Info
 5496 265.302713  169.100.167.250  169.100.95.2...  DNS       82 00:00:00:00:00:00  Standard query 0xba8d A footstool.stanford.edu
 5494 265.301760  169.100.167.250  169.100.95.2...  DNS       82 00:00:00:00:00:00  Standard query 0xc9ea AAAA footstool.stanford.edu
 5293 260.836407  169.100.167.155  169.100.95.2...  DNS       82 00:00:00:00:00:00  Standard query 0x7561 A sigcomm06.stanford.edu
 4762 231.720456  169.100.167.155  169.100.95.2...  DNS       81 00:00:00:00:00:00  Standard query 0x3e17 A weblogin.stanford.edu
 4751 231.665282  169.100.167.155  169.100.95.2...  DNS       86 00:00:00:00:00:00  Standard query 0x75a1 A proxy-service.stanford.edu
 4711 229.318626  169.100.167.155  169.100.95.2...  DNS       79 00:00:00:00:00:00  Standard query 0x7725 AAAA sighup.stanford.edu
 4672 224.318623  169.100.167.155  169.100.95.2...  DNS       79 00:00:00:00:00:00  Standard query 0x7725 AAAA sighup.stanford.edu
 3642 206.757828  169.100.167.155  169.100.95.2...  DNS       75 00:00:00:00:00:00  Standard query 0x19c7 A www.sigcomm.org
 3438 200.145702  169.100.167.155  169.100.95.2...  DNS       73 00:00:00:00:00:00  Standard query 0x982d A sb.google.com
 1810 79.747060   169.100.167.155  169.100.95.2...  DNS       68 00:00:00:00:00:00  Standard query 0x6464 A sosp.org
  546 29.987406   169.100.167.155  169.100.95.2...  DNS       74 00:00:00:00:00:00  Standard query 0x18aa A www.usenix.org
 4934 233.226561  167.215.51.171   167.215.51.2...  DNS       92 00:00:00:00:00:00  Standard query 0x8be3 A asdlfkjasd.com.EECS.Berkeley.EDU
 4931 233.221552  167.215.51.171   167.215.51.2...  DNS       74 00:00:00:00:00:00  Standard query 0x1ba0 A asdlfkjasd.com
 4929 233.221060  167.215.51.171   167.215.51.2...  DNS       83 00:00:00:00:00:00  Standard query 0xed22 A asdlfk.com.Berkeley.EDU
 4927 233.220662  167.215.51.171   167.215.51.2...  DNS       91 00:00:00:00:00:00  Standard query 0x8584 A asdlfk.com.Banatao.Berkeley.EDU
 4925 233.220245  167.215.51.171   167.215.51.2...  DNS       86 00:00:00:00:00:00  Standard query 0x2d13 A asdlfk.com.CS.Berkeley.EDU
 4923 233.219837  167.215.51.171   167.215.51.2...  DNS       88 00:00:00:00:00:00  Standard query 0x9377 A asdlfk.com.EECS.Berkeley.EDU
 4921 233.219452  167.215.51.171   167.215.51.2...  DNS       88 00:00:00:00:00:00  Standard query 0x6168 A asdlfk.com.EECS.Berkeley.EDU
 4920 233.219403  167.215.51.171   167.215.51.2...  DNS       87 00:00:00:00:00:00  Standard query 0xdb1a A asdlfkjasd.com.Berkeley.EDU

▾ Frame 4934: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 18, 2008 18:38:30.858509000 US Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1200699510.858509000 seconds
    [Time delta from previous captured frame: 0.000041000 seconds]
    [Time delta from previous displayed frame: 0.005009000 seconds]
    [Time since reference or first frame: 233.226561000 seconds]
    Frame Number: 4934
    Frame Length: 92 bytes (736 bits)
    Capture Length: 92 bytes (736 bits)
    [Frame is marked: False]

0000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 45 00   ········ ······E·
0010  00 4e 00 00 40 00 40 11  83 5b a7 d7 33 ab a7 d7   ·N··@·@· ·[··3···
0020  33 ca c7 df 00 35 00 3a  06 5a 8b c3 01 00 00 01   3····5·: ·Z······
0030  00 00 00 00 00 00 0a 61  73 64 6c 66 6b 6a 61 73   ·······a sdlfkjas
0040  64 03 63 6f 6d 04 45 45  43 53 08 42 65 72 6b 65   d·com·EE CS·Berke
0050  6c 65 79 03 45 44 55 00  00 01 00 01               ley·EDU· ····

project2_part1.pcap        Packets: 7394 · Displayed: 418 (5.7%)        Profile: Default
```

7. TCP Sequence Numbers

Filter Used – 'tcp and tcp.flags.syn ==1 and tcp.flags.ack==0'

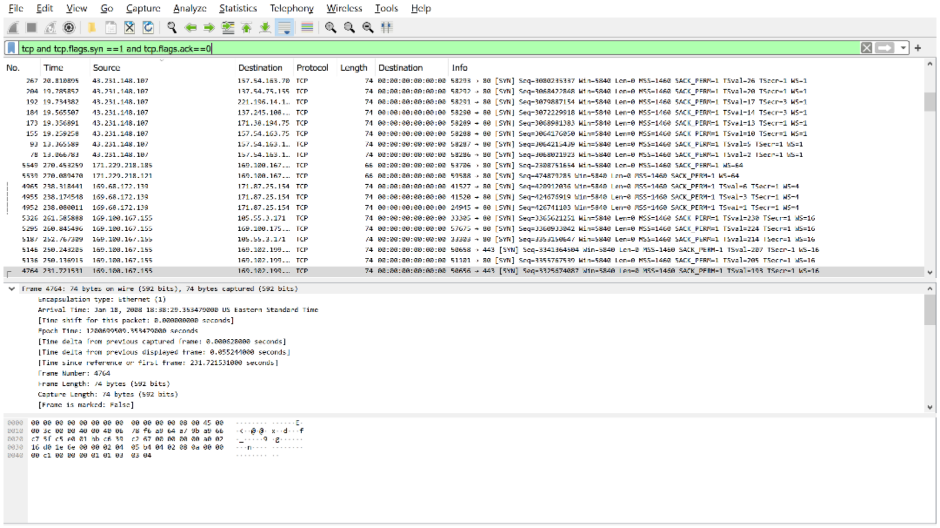
What it does – Displays only the tcp packets that are sending SYN and not ACK

Rationale – We want to find the Ips that participate in 5 or more connections. So it is enough to get the packets participating in the first step of the TCP/IP handshake.

The question says "Find the IP addresses of the 2 TCP endpoints that participate in 5 connections or more". If this is interpreted as "Two different hosts that connect to atleast 5 servers each"

Ips - 167.215.167.186 and 167.86.245.153

If it is interpreted as, “Two hosts that connect with each other atleast 5 times”
Ips - 167.86.245.153 and 169.100.167.155



```
tcp and tcp.flags.syn ==1 and tcp.flags.ack==0

No.   Time        Source             Destination      Protocol Length Destination        Info
 267  20.810895   43.231.148.107     157.54.163.70    TCP      74  00:00:00:00:00:00 58293 → 80 [SYN] Seq=3080235337 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=26 TSecr=1 WS=1
 204  19.785852   43.231.148.107     137.54.75.155    TCP      74  00:00:00:00:00:00 58292 → 80 [SYN] Seq=3068422848 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=20 TSecr=1 WS=1
 192  19.734382   43.231.148.107     221.196.14.1...  TCP      74  00:00:00:00:00:00 58291 → 80 [SYN] Seq=3079887154 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=17 TSecr=3 WS=1
 184  19.565507   43.231.148.107     137.245.108...   TCP      74  00:00:00:00:00:00 58290 → 80 [SYN] Seq=3072229918 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=14 TSecr=3 WS=1
 173  19.356891   43.231.148.107     171.38.194.75    TCP      74  00:00:00:00:00:00 58289 → 80 [SYN] Seq=3068981383 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=13 TSecr=1 WS=1
 155  19.259250   43.231.148.107     157.54.163.75    TCP      74  00:00:00:00:00:00 58288 → 80 [SYN] Seq=3064176050 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=10 TSecr=1 WS=1
  93  13.365589   43.231.148.107     157.54.163.1...  TCP      74  00:00:00:00:00:00 58287 → 80 [SYN] Seq=3064215439 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=5 TSecr=1 WS=1
  78  13.066783   43.231.148.107     157.54.163.1...  TCP      74  00:00:00:00:00:00 58286 → 80 [SYN] Seq=3068021923 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=2 TSecr=1 WS=1
5549  270.453259  171.229.218.185    169.100.167...   TCP      66  00:00:00:00:00:00 53706 → 80 [SYN] Seq=2308751654 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=64
5539  270.089470  171.229.218.121    169.100.167...   TCP      66  00:00:00:00:00:00 59588 → 80 [SYN] Seq=474879285 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=64
4965  238.318441  169.68.172.139     171.87.25.154    TCP      74  00:00:00:00:00:00 41527 → 80 [SYN] Seq=428912036 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=6 TSecr=1 WS=4
4955  238.174548  169.68.172.139     171.87.25.154    TCP      74  00:00:00:00:00:00 41520 → 80 [SYN] Seq=424676919 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3 TSecr=1 WS=4
4952  238.080011  169.68.172.139     171.87.25.154    TCP      74  00:00:00:00:00:00 24945 → 80 [SYN] Seq=426741103 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=1 TSecr=1 WS=4
5326  261.585808  169.100.167.155    105.55.3.171     TCP      74  00:00:00:00:00:00 33305 → 80 [SYN] Seq=3365621251 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=230 TSecr=1 WS=16
5295  260.845496  169.100.167.155    169.100.175...   TCP      74  00:00:00:00:00:00 57675 → 80 [SYN] Seq=3360933042 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=224 TSecr=1 WS=16
5187  252.767309  169.100.167.155    105.55.3.171     TCP      74  00:00:00:00:00:00 33303 → 80 [SYN] Seq=3353150647 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=214 TSecr=1 WS=16
5146  250.243205  169.100.167.155    169.102.199...   TCP      74  00:00:00:00:00:00 50658 → 443 [SYN] Seq=3341364504 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=207 TSecr=1 WS=16
5136  250.136915  169.100.167.155    169.102.199...   TCP      74  00:00:00:00:00:00 51101 → 80 [SYN] Seq=3355767539 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=205 TSecr=1 WS=16
4764  231.721531  169.100.167.155    169.102.199...   TCP      74  00:00:00:00:00:00 50656 → 443 [SYN] Seq=3325674087 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=193 TSecr=1 WS=16

Frame 4764: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 18, 2008 18:38:29.353479000 US Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1200699509.353479000 seconds
    [Time delta from previous captured frame: 0.000628000 seconds]
    [Time delta from previous displayed frame: 0.055244000 seconds]
    [Time since reference or first frame: 231.721531000 seconds]
    Frame Number: 4764
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]

0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ········ ······E·
0010  00 3c 02 00 40 00 40 06  78 f6 a9 64 a7 9b a9 66   ·<··@·@· x··d···f
0020  c7 5f c5 e0 01 bb c6 39  c2 67 00 00 00 00 a0 02   ·_·····9 ·g······
0030  16 d0 1e 6e 00 00 02 04  05 b4 04 02 08 0a 00 00   ···n···· ········
0040  00 c1 00 00 00 01 01 03  03 04                     ········ ··
```

8. Traceroute Scanning

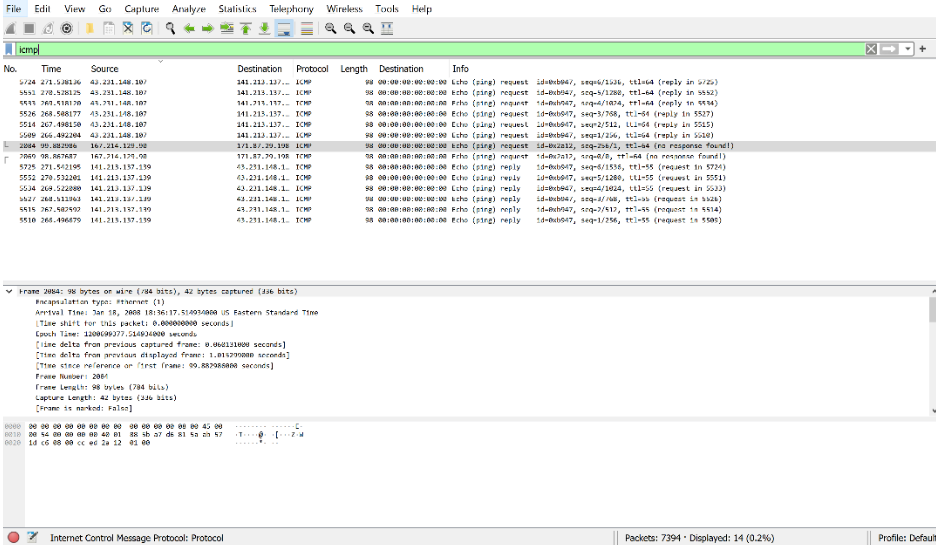
Ip host – 43.231.148.107

Ip destination – 141.231.148.107

Filter Used – ‘icmp’

What it does – Displays only the packets that use ICMP protocol

Rationale – Traceroute packets are sent out using ICMP protocol



```
icmp

No.   Time        Source             Destination      Protocol Length Destination        Info
5724  271.538136  43.231.148.107     141.213.137...   ICMP     98  00:00:00:00:00:00 Echo (ping) request  id=0xb947, seq=6/1536, ttl=64 (reply in 5725)
5551  270.528125  43.231.148.107     141.213.137...   ICMP     98  00:00:00:00:00:00 Echo (ping) request  id=0xb947, seq=5/1280, ttl=64 (reply in 5552)
5533  269.518120  43.231.148.107     141.213.137...   ICMP     98  00:00:00:00:00:00 Echo (ping) request  id=0xb947, seq=4/1024, ttl=64 (reply in 5534)
5526  268.508177  43.231.148.107     141.213.137...   ICMP     98  00:00:00:00:00:00 Echo (ping) request  id=0xb947, seq=3/768, ttl=64 (reply in 5527)
5514  267.498150  43.231.148.107     141.213.137...   ICMP     98  00:00:00:00:00:00 Echo (ping) request  id=0xb947, seq=2/512, ttl=64 (reply in 5515)
5509  266.492204  43.231.148.107     141.213.137...   ICMP     98  00:00:00:00:00:00 Echo (ping) request  id=0xb947, seq=1/256, ttl=64 (reply in 5510)
2084  99.882986   167.214.129.98     171.87.29.198    ICMP     98  00:00:00:00:00:00 Echo (ping) request  id=0x2a12, seq=256/1, ttl=64 (no response found!)
2069  98.867687   167.214.129.98     171.87.29.198    ICMP     98  00:00:00:00:00:00 Echo (ping) request  id=0x2a12, seq=0/0, ttl=64 (no response found!)
5725  271.542195  141.213.137.139    43.231.148.1...  ICMP     98  00:00:00:00:00:00 Echo (ping) reply    id=0xb947, seq=6/1536, ttl=55 (request in 5724)
5552  270.532201  141.213.137.139    43.231.148.1...  ICMP     98  00:00:00:00:00:00 Echo (ping) reply    id=0xb947, seq=5/1280, ttl=55 (request in 5551)
5534  269.522080  141.213.137.139    43.231.148.1...  ICMP     98  00:00:00:00:00:00 Echo (ping) reply    id=0xb947, seq=4/1024, ttl=55 (request in 5533)
5527  268.511963  141.213.137.139    43.231.148.1...  ICMP     98  00:00:00:00:00:00 Echo (ping) reply    id=0xb947, seq=3/768, ttl=55 (request in 5526)
5515  267.502592  141.213.137.139    43.231.148.1...  ICMP     98  00:00:00:00:00:00 Echo (ping) reply    id=0xb947, seq=2/512, ttl=55 (request in 5514)
5510  266.496679  141.213.137.139    43.231.148.1...  ICMP     98  00:00:00:00:00:00 Echo (ping) reply    id=0xb947, seq=1/256, ttl=55 (request in 5509)

Frame 2084: 98 bytes on wire (784 bits), 42 bytes captured (336 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 18, 2008 18:36:17.514934000 US Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1200699377.514934000 seconds
    [Time delta from previous captured frame: 0.060131000 seconds]
    [Time delta from previous displayed frame: 1.015299000 seconds]
    [Time since reference or first frame: 99.882986000 seconds]
    Frame Number: 2084
    Frame Length: 98 bytes (784 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]

0000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 45 00   ········ ······E·
0010  00 54 00 00 00 00 40 01  88 5b a7 d6 81 5a ab 57   ·T····@· ·[···Z·W
0020  1d c6 08 00 cc ed 2a 12  01 00                     ······*· ··

Internet Control Message Protocol: Protocol     Packets: 7394 · Displayed: 14 (0.2%)     Profile: Default
```

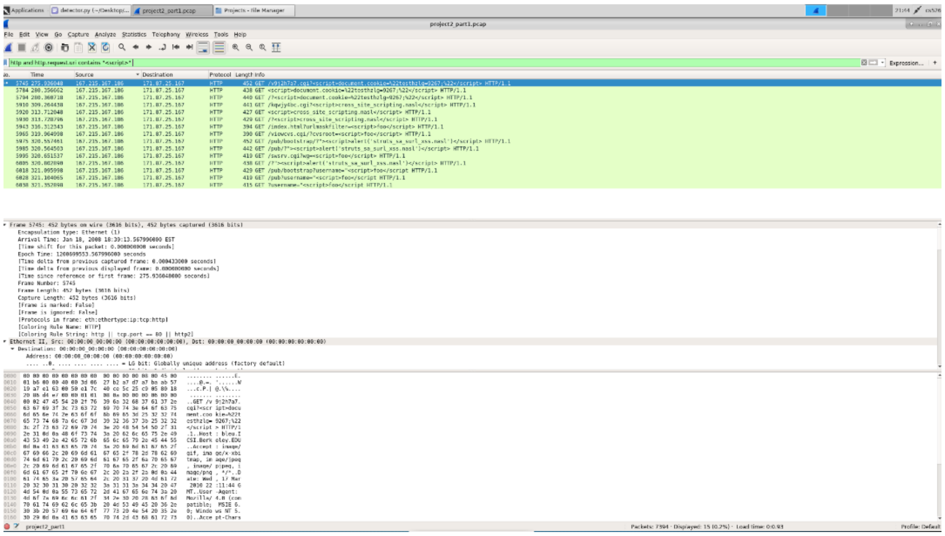
9. Cross-Site Scripting

Server with vulnerability – 171.87.25.167

Filter used – ‘http and http.request.uri contains "<script>"’

What it does – Displays only the http packets that have the string “<script>” in their url

Rationale – reflected XSS attacks send script inside url



```
http and http.request.uri contains "<script>"
```

```
No.  Time        Source           Destination    Protocol Length Info
5745 275.936048  167.215.167.186  171.87.25.167  HTTP     452 GET /v9j2h7a7.cgi?<script>document.cookie=%22testhzlg=9267;%22</script> HTTP/1.1
5784 280.356662  167.215.167.186  171.87.25.167  HTTP     438 GET <script>document.cookie=%22testhzlg=9267;%22</script> HTTP/1.1
5794 280.360718  167.215.167.186  171.87.25.167  HTTP     440 GET /?<script>document.cookie=%22testhzlg=9267;%22</script> HTTP/1.1
5910 309.264438  167.215.167.186  171.87.25.167  HTTP     441 GET /kqwjy4bc.cgi?<script>cross_site_scripting.nasl</script> HTTP/1.1
5920 313.712048  167.215.167.186  171.87.25.167  HTTP     427 GET <script>cross_site_scripting.nasl</script> HTTP/1.1
5930 313.728796  167.215.167.186  171.87.25.167  HTTP     429 GET /?<script>cross_site_scripting.nasl</script> HTTP/1.1
5943 316.312343  167.215.167.186  171.87.25.167  HTTP     394 GET /index.html?urlmaskfilter=<script>foo</script> HTTP/1.1
5965 319.964998  167.215.167.186  171.87.25.167  HTTP     390 GET /viewcvs.cgi/?cvsroot=<script>foo</script> HTTP/1.1
5975 320.557461  167.215.167.186  171.87.25.167  HTTP     452 GET /pub/bootstrap/?"><script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1
5985 320.564503  167.215.167.186  171.87.25.167  HTTP     442 GET /pub/?"><script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1
5995 320.651537  167.215.167.186  171.87.25.167  HTTP     410 GET /swsrv.cgi?wg=<script>foo</script> HTTP/1.1
6005 320.802890  167.215.167.186  171.87.25.167  HTTP     438 GET /?"><script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1
6018 321.095998  167.215.167.186  171.87.25.167  HTTP     429 GET /pub/bootstrap?username="<script>foo</script HTTP/1.1
6028 321.104065  167.215.167.186  171.87.25.167  HTTP     419 GET /pub?username="<script>foo</script HTTP/1.1
6038 321.352898  167.215.167.186  171.87.25.167  HTTP     415 GET ?username="<script>foo</script HTTP/1.1
```

```
▾ Frame 5745: 452 bytes on wire (3616 bits), 452 bytes captured (3616 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 18, 2008 18:39:13.567996000 EST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1200699553.567996000 seconds
    [Time delta from previous captured frame: 0.000433000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 275.936048000 seconds]
    Frame Number: 5745
    Frame Length: 452 bytes (3616 bits)
    Capture Length: 452 bytes (3616 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
▾ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
  ▾ Destination: 00:00:00_00:00:00 (00:00:00:00:00:00)
      Address: 00:00:00_00:00:00 (00:00:00:00:00:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  01 b6 00 00 40 00 3d 06  27 b2 a7 d7 a7 ba ab 57   ....@.=. '......W
0020  19 a7 e1 63 00 50 e1 7c  40 ce 5c 25 c9 05 80 18   ...c.P.| @.\%....
0030  20 00 d4 e7 00 00 01 01  08 0a 00 00 00 00 00 00    ....... ........
0040  00 02 47 45 54 20 2f 76  39 6a 32 68 37 61 37 2e   ..GET /v 9j2h7a7.
0050  63 67 69 3f 3c 73 63 72  69 70 74 3e 64 6f 63 75   cgi?<scr ipt>docu
0060  6d 65 6e 74 2e 63 6f 6f  6b 69 65 3d 25 32 32 74   ment.coo kie=%22t
0070  65 73 74 68 7a 6c 67 3d  39 32 36 37 3b 25 32 32   esthzlg= 9267;%22
0080  3c 2f 73 63 72 69 70 74  3e 20 48 54 54 50 2f 31   </script > HTTP/1
0090  2e 31 0d 0a 48 6f 73 74  3a 20 62 6c 65 75 2e 49   .1..Host : bleu.I
00a0  43 53 49 2e 42 65 72 6b  65 6c 65 79 2e 45 44 55   CSI.Berk eley.EDU
00b0  0d 0a 41 63 63 65 70 74  3a 20 69 6d 61 67 65 2f   ..Accept : image/
00c0  67 69 66 2c 20 69 6d 61  67 65 2f 78 2d 78 62 69   gif, ima ge/x-xbi
00d0  74 6d 61 70 2c 20 69 6d  61 67 65 2f 6a 70 65 67   tmap, im age/jpeg
00e0  2c 20 69 6d 61 67 65 2f  70 6a 70 65 67 2c 20 69   , image/ pjpeg, i
00f0  6d 61 67 65 2f 70 6e 67  2c 20 2a 2f 2a 0d 0a 44   mage/png , */*..D
0100  61 74 65 3a 20 57 65 64  2c 20 31 37 20 4d 61 72   ate: Wed , 17 Mar
0110  20 32 30 31 30 20 32 32  3a 31 31 3a 34 34 20 47    2010 22 :11:44 G
0120  4d 54 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   MT..User -Agent: 
0130  4d 6f 7a 69 6c 6c 61 2f  34 2e 30 20 28 63 6f 6d   Mozilla/ 4.0 (com
0140  70 61 74 69 62 6c 65 3b  20 4d 53 49 45 20 36 2e   patible;  MSIE 6.
0150  30 3b 20 57 69 6e 64 6f  77 73 20 4e 54 20 35 2e   0; Windo ws NT 5.
0160  30 29 0d 0a 41 63 63 65  70 74 2d 43 68 61 72 73   0)..Acce pt-Chars
```

```
Packets: 7394 · Displayed: 15 (0.2%) · Load time: 0:0.93
```

Problem 2

1.

IP	MAC
10.0.2.1	Apple_e5:66:07 (00:26:08:e5:66:07)
10.0.2.2	Apple_d8:0f:fa (04:0c:ce:d8:04:fa)
10.0.2.3	IntelCor_50:f0:a6 (8c:a9:82:50:f0:a6)

2. This IP range falls under the private IP ranges of Class A IP addresses. Private network addresses are not allocated to any specific organization. These addresses are commonly used for local area networks (LANs) in residential, offices etc. The network shown is a small network with 3 hosts.
3.
    a. Source system – 10.0.2.2, ftp server – 194.109.21.66
    Ans - ftp.mirror.nl
    b. Active Connection
    c. When we follow a tcp stream we can see that the login details are sent in plaintext
    d. In place of FTP we can use SFTP or HTTPS for secure file transfer
4.
    a. The browser is authenticated to facebook through tokens stored in cookies. This is insecure because anybody who gets hold of the cookies will be able to access the user's account without username and password.
    b. The attacker can get the cookies, access user's account and impersonate as the user.
    c. Users can protect themselves by logging out after every session so that the cookies are destroyed
    d. While on facebook, the user searched for users with names starting with 'zak', clicked on 'zakirbpd' and went to that user's profile and visited the timeline. He then opened a new chat message and sent the message 'Остановить нюхают My WiFi'. (Which when translated to English becomes 'stop sniffing my wifi')

Problem 3

Code:

```
import dpkt
import sys
import socket
from dpkt.compat import compat_ord

#f = open('project2_part3.pcap','rb')
f = open(sys.argv[-1],'rb')
pcap = dpkt.pcap.Reader(f)

host_ips_syn={}
host_ips_syn_ack={}

for timestamp,buf in pcap:


    try:
        eth = dpkt.ethernet.Ethernet(buf)
    except (dpkt.dpkt.UnpackError,IndexError):
        continue

    # print(':'.join('%02x' % compat_ord(b) for b in eth.src))



    if not isinstance(eth.data, dpkt.ip.IP):
        #print('Non IP Packet type not supported %s\n' % eth.data.__class__.__name__)
        continue

    ip = eth.data
    ip_src = socket.inet_ntoa(ip.src)
    ip_dst = socket.inet_ntoa(ip.dst)
    #print(ip_src,ip_dst)

   # We are only interested in TCP
    if ip.p != dpkt.ip.IP_PROTO_TCP:
        continue

    tcp = ip.data

    if tcp.flags & dpkt.tcp.TH_SYN and not (tcp.flags & dpkt.tcp.TH_ACK):     #If syn flag in the packet
        if ip_src in host_ips_syn:   #if this ip exists in the src_ips-syn map, add count
            host_ips_syn[ip_src] += 1
        else:
            host_ips_syn[ip_src] = 1          #else add ip to the map and initialize

    if (tcp.flags & dpkt.tcp.TH_SYN) and (tcp.flags & dpkt.tcp.TH_ACK):          #If syn and ack
flags in the packet
        if ip_dst in host_ips_syn_ack:    #if destination ip exists in the dest_ip-syn/ack map, add
count
            host_ips_syn_ack[ip_dst] += 1
        else:
            host_ips_syn_ack[ip_dst] = 1 #else add ip to map initialize




ips = []
# #For every ip in the source ips, compare the count syn+ack it received vs syn it sent
for ip in host_ips_syn:
    #print(ip,":",host_ips_syn[ip])
    if ip in host_ips_syn_ack and host_ips_syn[ip]>=3*host_ips_syn_ack[ip]: #if that ip exists in source
ip list and if the number of syn packets >= 3* number of destination syn+ack packets,
        ips.append(ip)
    elif ip not in host_ips_syn_ack and host_ips_syn[ip]:
        ips.append(ip)




for i in ips:
    print(i)
```

References:

https://dpkt.readthedocs.io/en/latest/_modules/dpkt/ethernet.html

https://dpkt.readthedocs.io/en/latest/api/api_auto.html#dpkt.ethernet.Ethernet.pack_hdr

https://github.com/kbandla/dpkt/issues/232

https://stackoverflow.com/questions/25370010/parsing-ip-address-with-dpkt

https://dpkt.readthedocs.io/en/latest/_modules/examples/print_packets.html

https://dpkt.readthedocs.io/en/latest/print_packets.html