

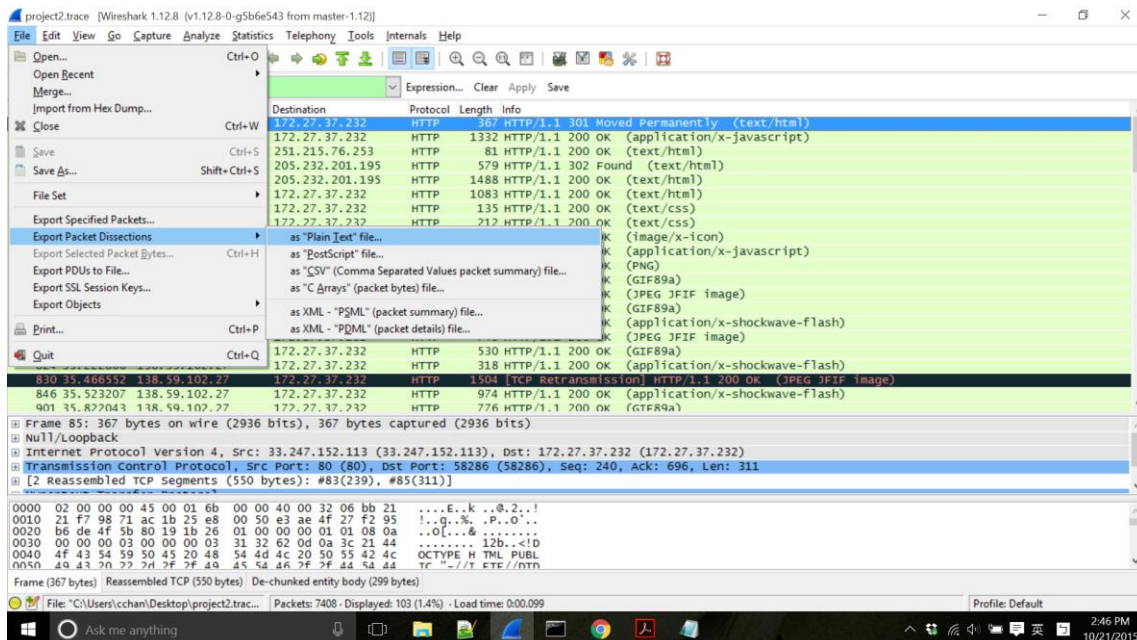
1.

Filter: http.response

I examine the IP address only for http response which includes the servers that engaged in a valid instance of the HTTP protocol, for the status code returned were 404, 200 and other types. I also export the information into txt file (q1.txt) and then write a Python script (question1.py) to find the IP address.

The IP list is following (in Wireshark shown order not script order but they are the same):

- | | | | |
|---------------------|---------------------|---------------------|---------------------|
| 1) 143.138.4.147 | 2) 33.247.152.113 | 3) 33.247.152.101 | 4) 44.131.48.102 |
| 5) 34.30.235.180 | 6) 97.145.19.119 | 7) 37.199.226.67 | 8) 143.138.66.97 |
| 9) 37.120.175.85 | 10) 44.111.85.82 | 11) 44.131.51.48 | 12) 248.78.109.66 |
| 13) 138.59.102.27 | 14) 154.87.109.40 | 15) 154.87.109.177 | 16) 93.119.134.44 |
| 17) 155.231.237.70 | 18) 35.183.215.204 | 19) 159.70.229.173 | 20) 251.235.172.148 |
| 21) 205.232.201.218 | 22) 44.131.51.161 | 23) 155.111.186.252 | 24) 136.93.4.213 |
| 25) 93.199.112.45 | 26) 143.179.11.189 | 27) 154.27.68.55 | 28) 111.4.186.50 |
| 29) 40.187.57.142 | 30) 142.165.192.177 | 31) 142.165.192.188 | 32) 205.234.49.157 |
| 33) 159.79.22.194 | 34) 159.79.22.198 | 35) 205.232.203.30 | 36) 159.79.22.249 |



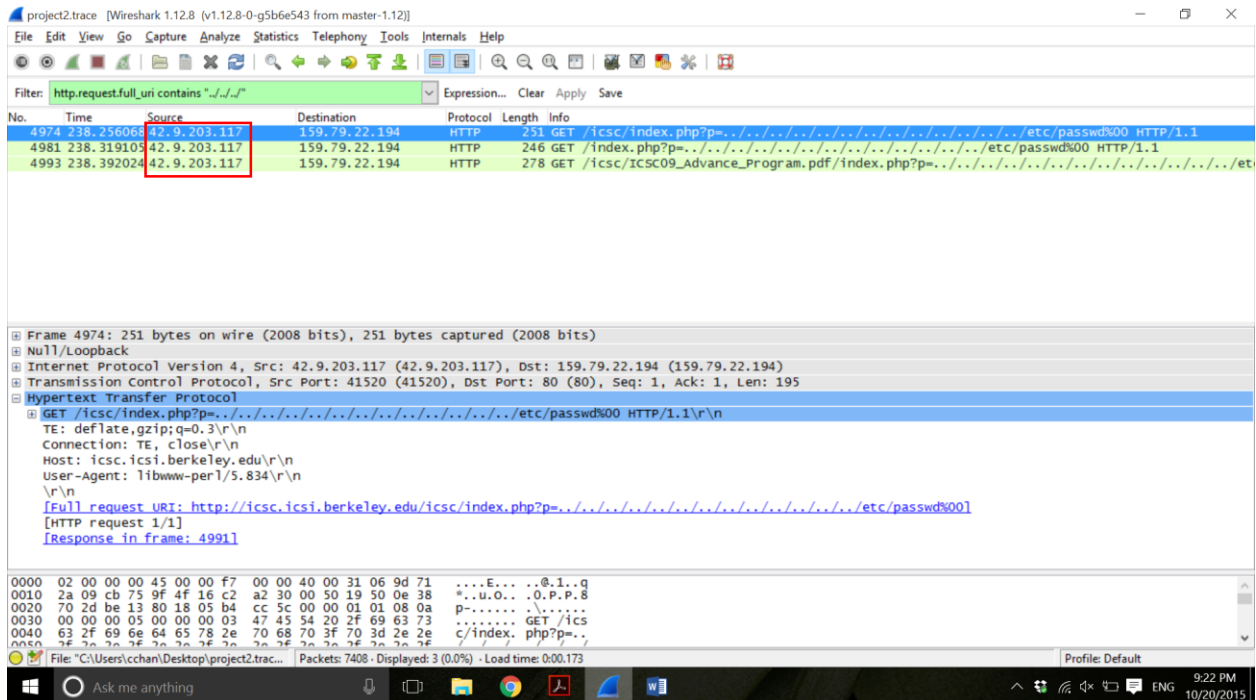
```
Command Prompt
source ip: 44.154.102.10 ['200']
source ip: 205.232.201.195 ['200']

C:\Users\cchan\Desktop\Python>question1.py
source ip: 155.111.186.252 ['200']
source ip: 40.187.57.142 ['302']
source ip: 93.119.134.44 ['302']
source ip: 155.231.237.70 ['301']
source ip: 159.79.22.249 ['403']
source ip: 159.70.229.173 ['200']
source ip: 35.183.215.204 ['302']
source ip: 205.232.201.218 ['200']
source ip: 93.199.112.45 ['200']
source ip: 33.247.152.113 ['301']
source ip: 142.165.192.188 ['200']
source ip: 136.93.4.213 ['200']
source ip: 143.138.66.97 ['200']
source ip: 97.145.19.119 ['200']
source ip: 44.111.85.82 ['200']
source ip: 159.79.22.198 ['404']
source ip: 205.234.49.157 ['302']
source ip: 154.87.109.177 ['200']
source ip: 44.131.48.102 ['200']
source ip: 33.247.152.101 ['200']
source ip: 159.79.22.194 ['404']
source ip: 154.87.109.40 ['200']
source ip: 248.78.109.66 ['302']
source ip: 142.165.192.177 ['302']
source ip: 34.30.235.180 ['200']
source ip: 154.27.68.55 ['200']
source ip: 111.4.186.50 ['200']
source ip: 143.138.4.147 ['200']
source ip: 37.199.226.67 ['200']
source ip: 37.120.175.85 ['304']
source ip: 205.232.203.30 ['302']
source ip: 138.59.102.27 ['200']
source ip: 143.179.11.189 ['200']
source ip: 251.235.172.148 ['200']
source ip: 44.131.51.48 ['200']
source ip: 44.131.51.161 ['200']
```

2.

Filter: http.request.full_uri contains "../../../../"

I look at the request contains the "../../../../", we can see the IP address is the 42.9.203.117 which is trying to exploit the web server.



3.

Filter: ftp.request.command contains "PASS" || ftp.request.command contains "USER"

We can see that the IP address: 248.35.162.92 tried many times I assume it is the brutal force attack.

The 172.27.37.232, 251.215.184.138 also have log in record but they didn't try and try again.

The screenshot shows a Wireshark packet capture of an FTP session. The filter is set to 'ftp.request.command contains "PASS" || ftp.request.command contains "USER"'. The packet list shows several FTP requests from 248.35.162.92 to 159.79.22.194. The packet details pane shows the structure of a frame (5035) containing a NULL/Loopback, an Internet Protocol version 4 header, a Transmission Control Protocol header, and a File Transfer Protocol (FTP) header. The packet bytes pane shows the raw data of the frame, including the FTP command 'Adminis trator..'. The status bar at the bottom indicates that 7408 packets were captured and 17 were displayed.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|-----------------|----------------|----------|--------|-----------------------------|
| 1159 | 41.663858 | 251.215.184.138 | 251.215.76.253 | FTP | 60 | Request: USER anonymous |
| 1173 | 42.033685 | 251.215.184.138 | 251.215.76.253 | FTP | 51 | Request: PASS |
| 1680 | 64.840026 | 172.27.37.232 | 151.37.121.114 | FTP | 72 | Request: USER calrules |
| 1759 | 75.894046 | 172.27.37.232 | 151.37.121.114 | FTP | 80 | Request: PASS thisissecure |
| 5035 | 242.415069 | 248.35.162.92 | 159.79.22.194 | FTP | 64 | Request: USER Administrator |
| 5039 | 242.604139 | 248.35.162.92 | 159.79.22.194 | FTP | 57 | Request: PASS volley |
| 5049 | 242.784042 | 248.35.162.92 | 159.79.22.194 | FTP | 64 | Request: USER Administrator |
| 5053 | 242.968408 | 248.35.162.92 | 159.79.22.194 | FTP | 64 | Request: USER Administrator |
| 5056 | 243.149250 | 248.35.162.92 | 159.79.22.194 | FTP | 57 | Request: PASS ashley |
| 5060 | 243.328988 | 248.35.162.92 | 159.79.22.194 | FTP | 57 | Request: PASS ashley |
| 5064 | 243.507090 | 248.35.162.92 | 159.79.22.194 | FTP | 64 | Request: USER Administrator |
| 5113 | 247.450545 | 248.35.162.92 | 159.79.22.194 | FTP | 64 | Request: USER Administrator |
| 5121 | 247.635976 | 248.35.162.92 | 159.79.22.194 | FTP | 55 | Request: PASS bear |
| 5124 | 247.817190 | 248.35.162.92 | 159.79.22.194 | FTP | 64 | Request: USER Administrator |
| 5128 | 247.997132 | 248.35.162.92 | 159.79.22.194 | FTP | 64 | Request: USER Administrator |
| 5133 | 248.174534 | 248.35.162.92 | 159.79.22.194 | FTP | 57 | Request: PASS calvin |
| 5137 | 248.353616 | 248.35.162.92 | 159.79.22.194 | FTP | 57 | Request: PASS calvin |

Frame 5035: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on *Null/Loopback*

Internet Protocol version 4, Src: 248.35.162.92 (248.35.162.92), Dst: 159.79.22.194 (159.79.22.194)

Transmission Control Protocol, Src Port: 49378 (49378), Dst Port: 21 (21), Seq: 1, Ack: 1, Len: 20

File Transfer Protocol (FTP)

0000 02 00 00 00 45 00 00 3c 00 00 40 00 2a 06 00 2bE...<..@.*..+

0010 f8 23 a2 5c 9f 4f 16 c2 c0 e2 00 15 14 2a 8d bb .#. \.O.%.

0020 78 5b 97 04 50 18 00 40 ec a9 00 00 55 53 45 52 x[.P..@USER

0030 20 41 64 6d 69 6e 69 73 74 72 61 74 6f 72 0d 0a Adminis trator..

File: "C:\Users\cchan\Desktop\project2.trac..." Packets: 7408 - Displayed: 17 (0.2%) - Load time: 0:00:161 Profile: Default

Ask me anything

9:24 PM 10/20/2015

4.

Filter: ftp && ip.src == 172.27.37.232 || ip.dst == 172.27.37.232

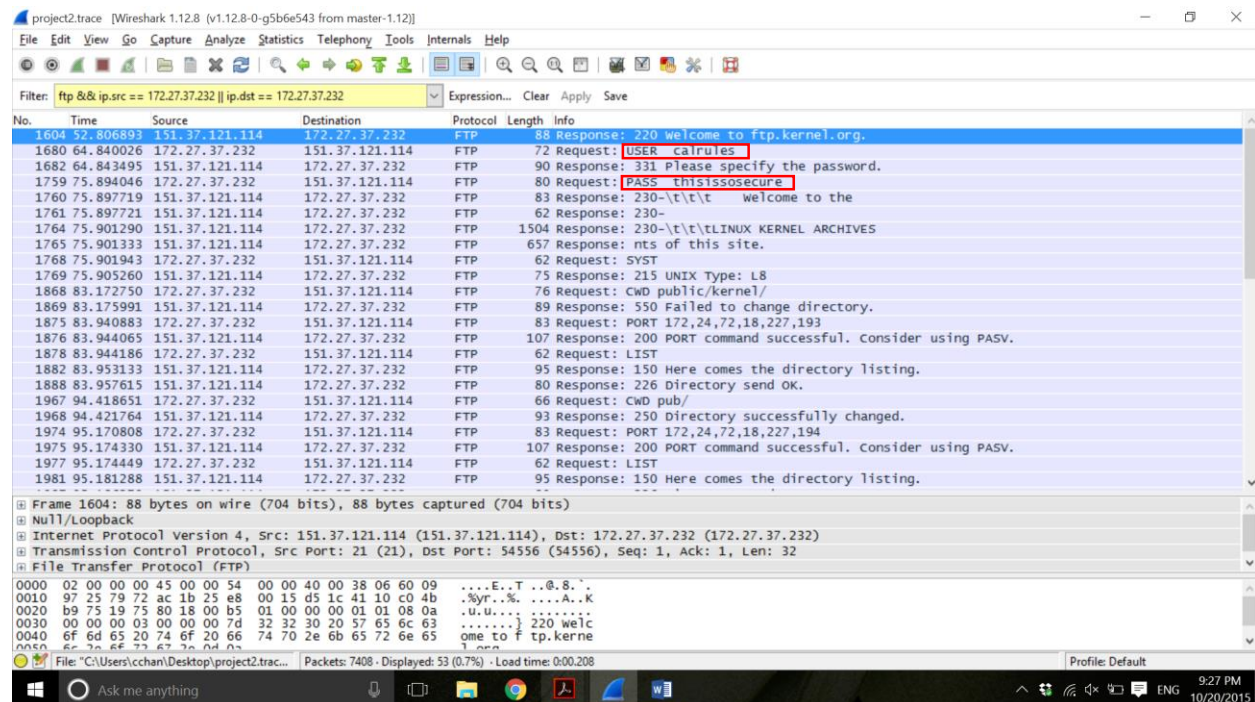
Filter: ftp && ip.src == 251.215.184.138 || ip.dst == 251.215.184.138

I use the last question search result to set the filter.

The user of 172.27.37.232 is "calrules" and password is "thisisosecure".

The user of 251.215.184.138 is "anonymous" and password is ""(none).

When enter the other protocol, we could not find any other username and password.



project2.trace [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ftp && ip.src == 251.215.184.138 || ip.dst == 251.215.184.138 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-----------------|-----------------|----------|--------|---|
| 1141 | 39.485769 | 251.215.76.253 | 251.215.184.138 | FTP | 103 | Response: 220 ProFTPD 1.3.2 Server (Debian) [::ffff:128.32.153.219] |
| 1159 | 41.663858 | 251.215.184.138 | 251.215.76.253 | FTP | 60 | Request: USER anonymous |
| 1160 | 41.691446 | 251.215.76.253 | 251.215.184.138 | FTP | 119 | Response: 331 Anonymous login ok, send your complete email address as your password |
| 1173 | 42.033685 | 251.215.184.138 | 251.215.76.253 | FTP | 51 | Request: PASS |
| 1174 | 42.035219 | 251.215.76.253 | 251.215.184.138 | FTP | 94 | Response: 230 Anonymous access granted, restrictions apply |
| 1175 | 42.035507 | 251.215.184.138 | 251.215.76.253 | FTP | 50 | Request: SYST |
| 1176 | 42.035597 | 251.215.76.253 | 251.215.184.138 | FTP | 63 | Response: 215 UNIX Type: L8 |
| 1177 | 42.035888 | 251.215.184.138 | 251.215.76.253 | FTP | 52 | Request: TYPE I |
| 1178 | 42.035990 | 251.215.76.253 | 251.215.184.138 | FTP | 63 | Response: 200 Type set to I |
| 1219 | 43.433952 | 251.215.184.138 | 251.215.76.253 | FTP | 71 | Request: PORT 128,32,48,187,187,64 |
| 1220 | 43.434150 | 251.215.76.253 | 251.215.184.138 | FTP | 73 | Response: 200 PORT command successful |
| 1221 | 43.434425 | 251.215.184.138 | 251.215.76.253 | FTP | 52 | Request: TYPE A |
| 1222 | 43.434511 | 251.215.76.253 | 251.215.184.138 | FTP | 63 | Response: 200 Type set to A |
| 1223 | 43.434768 | 251.215.184.138 | 251.215.76.253 | FTP | 50 | Request: NLST |

Frame 1972: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)

Null/Loopback

Internet Protocol Version 4, Src: 251.215.76.253 (251.215.76.253), Dst: 251.215.184.138 (251.215.184.138)

Transmission Control Protocol, Src Port: 21 (21), Dst Port: 47935 (47935), Seq: 4145214463, Ack: 4140747606, Len: 14

File Transfer Protocol (FTP)

0000 02 00 00 00 45 00 00 36 00 00 40 00 40 06 3d 8bE..6 ..@.@.=.

0010 fb d7 4c fd fb d7 b8 8a 00 15 bb 3f f7 12 f3 ff ..L.....?....

0020 f6 ce cb 56 50 18 00 2e 49 cc 00 00 32 32 31 20 ...VP... I...221

0030 47 6f 6f 64 62 79 65 2e 0d 0a Goodbye. ..

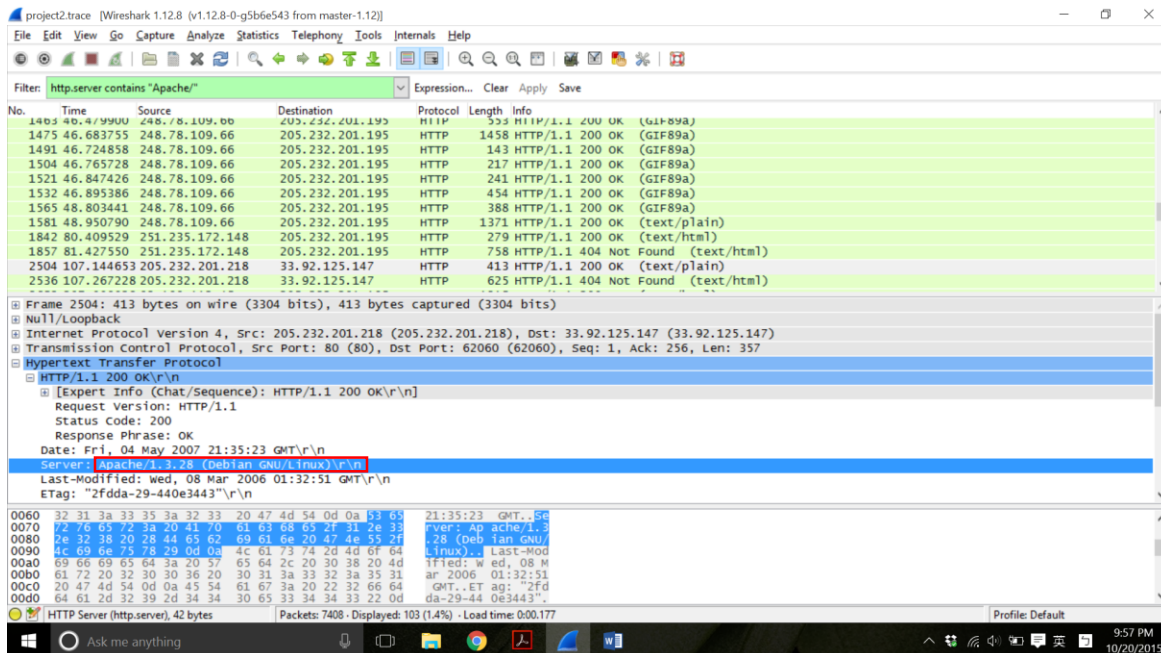
File: "C:\Users\cchan\Desktop\project2.trace..." Packets: 7408 · Displayed: 171 (2.3%) · Load time: 0:00.115 Profile: Default

4:32 PM 10/25/2015

5.

Filter: http.server contains "Apache/"

After enter the filter, I export the information into a plain txt file (q5.txt) and use a python script to print out all the frame and sever type. Then I sort the server type. The 1.3.28 is the oldest. We could see there are 4 different frame used the 1.3.28 server. They all are the same IP address: 205.232.201.218. I use the Python script (question5.py) to search. I first put the server version into the dictionary as a key and then put the IP address as the value. On the other hand, I stored the server version into an array, then sort it. Use the minimum number as the key to print out its source IP.



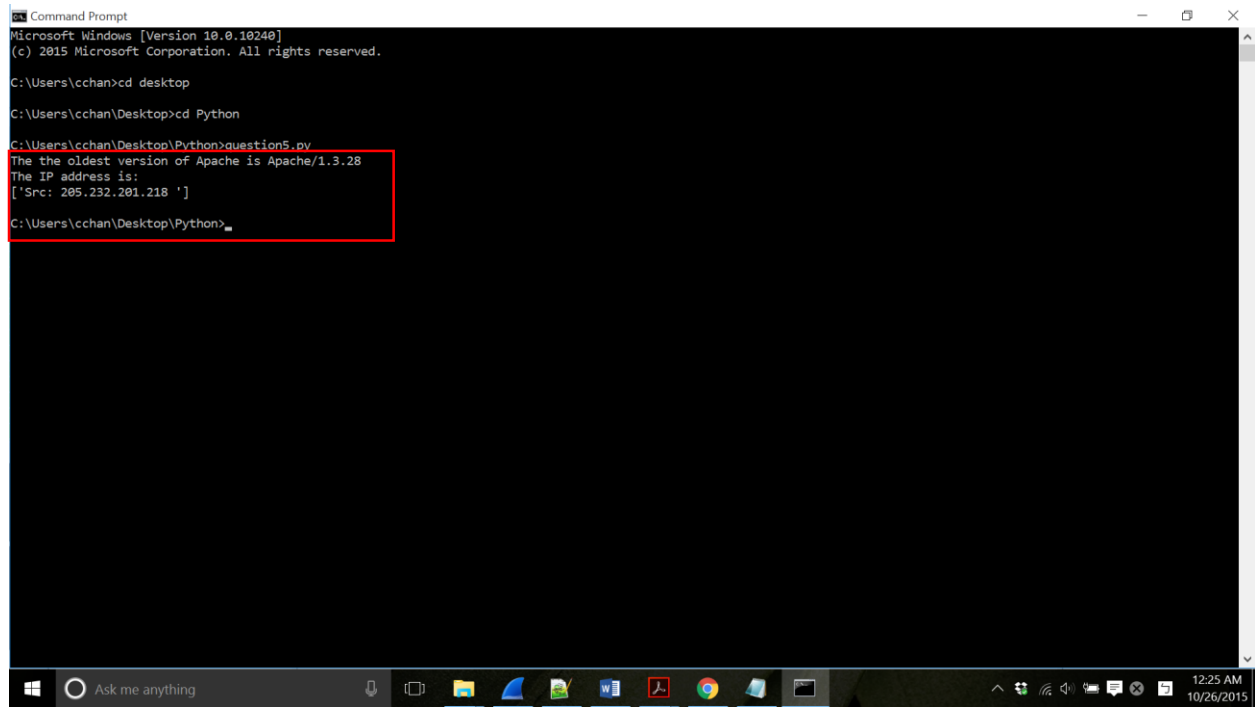
```
Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\cchan>cd desktop

C:\Users\cchan\Desktop>cd Python

C:\Users\cchan\Desktop\Python>question5.py
The the oldest version of Apache is Apache/1.3.28
The IP address is:
['Src: 205.232.201.218 ']

C:\Users\cchan\Desktop\Python>
```

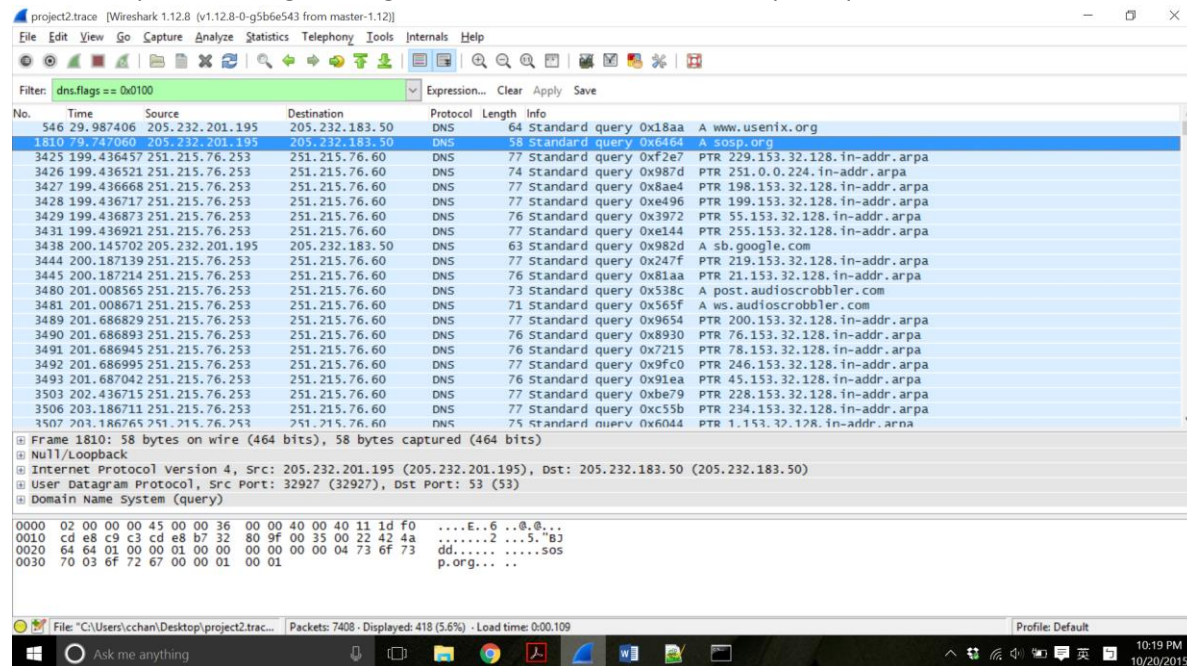


The screenshot shows a Windows Command Prompt window with a black background and white text. The window title is 'Command Prompt'. The text shows the user navigating to the desktop, then to a directory named 'Python', and running a file named 'question5.py'. The script's output is displayed on the next two lines: 'The the oldest version of Apache is Apache/1.3.28' and 'The IP address is:'. The third line shows the output of the script as a list: ['Src: 205.232.201.218 ']. A red rectangular box is drawn around these two lines of output. The Windows taskbar is visible at the bottom, showing the Start button, a search bar with the text 'Ask me anything', and several application icons. The system clock in the bottom right corner indicates the time is 12:25 AM on 10/26/2015.

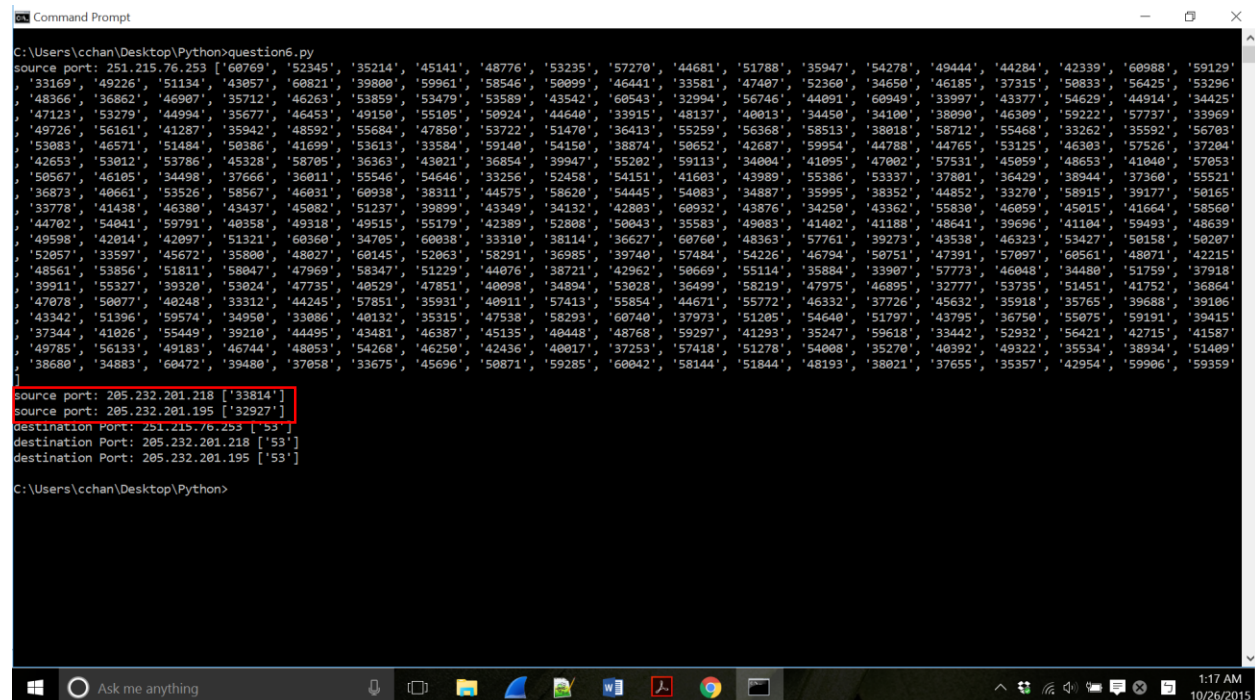
6.

Filter: dns.flags == 0x0100

I filter the packets using dns flags 0x0100. We can see all the request queries as shown below:



Then I used a Python script (question6.py) to map the different source ports used to their source IP address in the export txt file (q6.txt). We can see the first IP has many destination IP. And the 205.232.201.218 and 205.232.201.195 only have one connection.



7.

Filter: tcp.flags == 0x02

After using the script (question7.py) to search the IP endpoint in q7.txt more than 5 times, I examine the seq number to see which IP endpoints connection provide the broadest 32-bit coverage in their ISNs.

Filter: tcp.flags == 0x02 && ip.src == 205.232.201.195 && ip.dst == 248.78.109.66

205.232.201.195 & 248.78.109.66 with a range 3,152,737,232 – 3,122,016,130= 30,721,102

Filter: tcp.flags == 0x02 && ip.src == 251.215.153.250 && ip.dst == 159.79.22.249

251.215.153.250 & 159.79.22.249 range from 3,783,016,653 to 42,319,747. The range is 3,740,696,906. Obviously, the range of 251.215.153.250 & 159.79.22.249 is bigger. That's what we need.

```

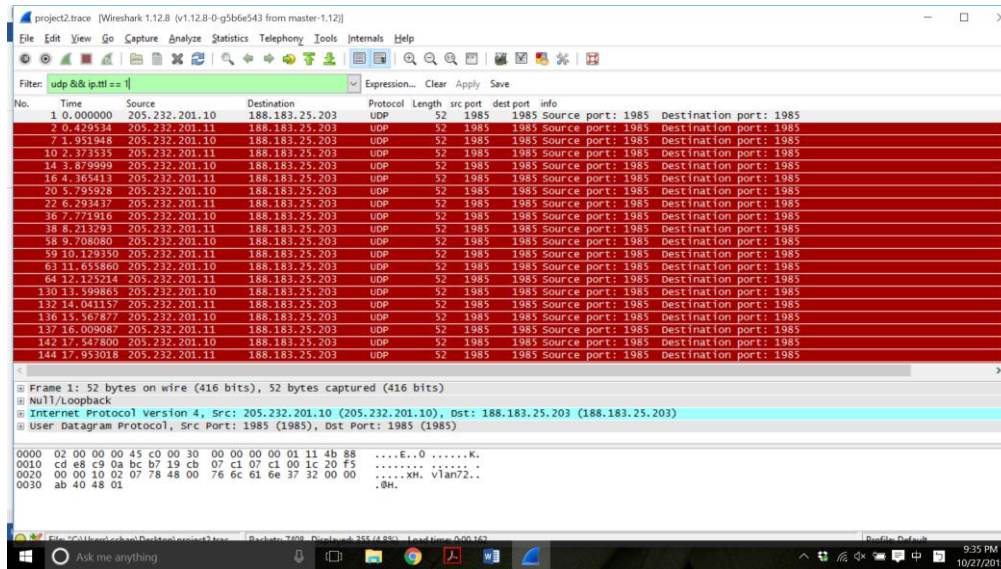
1 f = open('q7.txt')
2 count =
3 dict =
4 for word in open('q7.txt').readlines():
5     dic(c) 2015 Microsoft Corporation. All rights reserved.
6     word
7     if C:\Users\cchan>cd desktop
8
9     C:\Users\cchan\Desktop>cd Python
10
11     C:\Users\cchan\Desktop\Python>question7.py
12     251.215.153.250 159.79.22.249 16
13     205.232.201.195 248.78.109.66 26
14
15     C:\Users\cchan\Desktop\Python>
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30 f.close

```

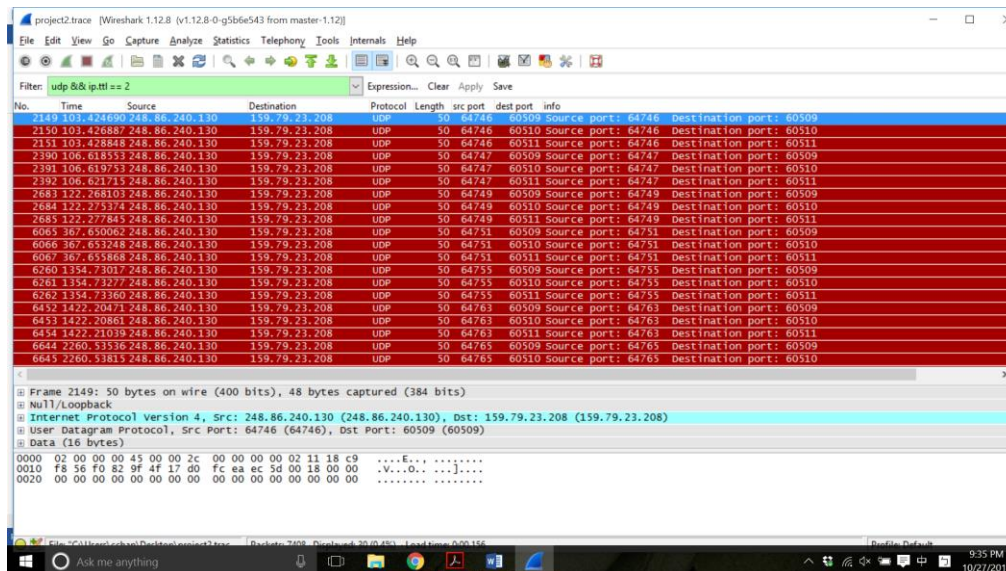
8.

I tried to look for a host performing trace route. The trace route scanning will send UDP packets with incrementing ttl and receives ICMP packets in return. So I enter the filter shown as following.

Filter: udp && ip.ttl == 1



Filter: udp && ip.ttl == 2



We could see that IP: 248.86.240.130 and 159.79.23.208 are running traceroute for detecting routers on a path.

Filter: (ip.src == 248.86.240.130 && ip.dst == 159.79.23.208) || (ip.dst == 248.86.240.130 && ip.src == 159.79.23.208)

project2.trace [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (ip.src == 248.86.240.130 && ip.dst == 159.79.23.208) || (ip.dst == 248.86.240.130 && ip.src == 159.79.23.208) Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | src port | dest port | info |
|------|------------|----------------|---------------|----------|--------|----------|-----------|---|
| 2163 | 103.446961 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60523 | Source port: 64746 Destination port: 60523 |
| 2162 | 103.445058 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60522 | Source port: 64746 Destination port: 60522 |
| 2161 | 103.443085 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60521 | Source port: 64746 Destination port: 60521 |
| 2160 | 103.441117 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60520 | Source port: 64746 Destination port: 60520 |
| 2159 | 103.439215 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60519 | Source port: 64746 Destination port: 60519 |
| 2158 | 103.437279 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60518 | Source port: 64746 Destination port: 60518 |
| 2157 | 103.435716 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60517 | Source port: 64746 Destination port: 60517 |
| 2156 | 103.434207 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60516 | Source port: 64746 Destination port: 60516 |
| 2155 | 103.432544 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60515 | Source port: 64746 Destination port: 60515 |
| 2154 | 103.431961 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60514 | Source port: 64746 Destination port: 60514 |
| 2153 | 103.431488 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60513 | Source port: 64746 Destination port: 60513 |
| 2152 | 103.430882 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60512 | Source port: 64746 Destination port: 60512 |
| 2151 | 103.428848 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60511 | Source port: 64746 Destination port: 60511 |
| 2150 | 103.426887 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60510 | Source port: 64746 Destination port: 60510 |
| 2149 | 103.424690 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60509 | Source port: 64746 Destination port: 60509 |
| 2148 | 103.424211 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60508 | Source port: 64746 Destination port: 60508 |
| 2147 | 103.423833 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60507 | Source port: 64746 Destination port: 60507 |
| 2146 | 103.423167 | 248.86.240.130 | 159.79.23.208 | UDP | 50 | 64746 | 60506 | Source port: 64746 Destination port: 60506 |
| 2084 | 99.882986 | 248.86.240.130 | 159.79.23.208 | ICMP | 88 | | | Echo (ping) request id=0x2a12, seq=256/1, ttl=64 (no response found!) |
| 2069 | 98.867687 | 248.86.240.130 | 159.79.23.208 | ICMP | 88 | | | Echo (ping) request id=0x2a12, seq=0/0, ttl=64 (no response found!) |

Frame 2149: 50 bytes on wire (400 bits), 48 bytes captured (384 bits)

Null/Loopback

Internet Protocol Version 4, Src: 248.86.240.130 (248.86.240.130), Dst: 159.79.23.208 (159.79.23.208)

User Datagram Protocol, Src Port: 64746 (64746), Dst Port: 60509 (60509)

Data (16 bytes)

```

0000 02 00 00 00 00 45 00 00 2c 00 00 00 00 02 11 18 c9 .....E.....
0010 f8 56 f0 82 9f 4f 17 d0 fc ea ec 5d 00 18 00 00 .V...O...].
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

File: C:\Users\chao\Desktop\project2.trace [Packets: 7108, Displayed: 1033 (15.0%), Load time: 0:00:14]

9:36 PM 10/27/2015

I find a host that incrementing its ttl: source IP 248.86.240.130 and destination IP 159.79.23.208.

9.

I use the filter to search the URL that contains a script inside the URL itself.

Filter: http.request.full_uri contains "script"

IP: dst=37.120.175.85 (Vulnerable Server)

project2.trace [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

Filter: `http.request.full_uri contains "script"` Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|-----------------|-----------------|----------|--------|---|
| 293 | 25.570342 | 251.215.76.253 | 37.120.175.85 | HTTP | 663 | GET /index.php?language=en&partner=%22%3E%3Cscript%3Ealert(123456789)%3C/script%3E HTTP/1.1 |
| 496 | 29.337059 | 251.215.76.253 | 44.111.85.82 | HTTP | 682 | GET /%3Cscript%3Ealert(123456789)%3Cscript%3E HTTP/1.1 |
| 657 | 32.768037 | 172.27.37.232 | 138.59.102.27 | HTTP | 500 | GET /scripts/core.js HTTP/1.1 |
| 3590 | 204.324088 | 251.215.76.253 | 136.93.19.97 | HTTP | 710 | GET /includes/blq/resources/gv1/r61/script/blq_core.js HTTP/1.1 |
| 3779 | 208.101297 | 251.215.76.253 | 128.136.239.153 | HTTP | 485 | GET /assets/A8/N24/M8481/P17/q45482/script_970_250.js?&0.3852269649505615 HTTP/1.1 |
| 3794 | 208.147362 | 251.215.76.253 | 128.136.239.153 | HTTP | 445 | GET /script/V3.00/select.js?350.0 HTTP/1.1 |
| 4033 | 211.647341 | 251.215.76.253 | 128.136.239.153 | HTTP | 446 | [TCP ACKed unseen segment] GET /script/V3.00/deliver.js?350.0 HTTP/1.1 |
| 4034 | 211.648766 | 251.215.76.253 | 128.136.239.153 | HTTP | 1003 | GET /script/V3.00/deliver2.html?pid=45482&cid=8481&pub=17&a=182442&vwDebug=false&pc=1823 HTTP/1.1 |
| 4140 | 212.327727 | 251.215.76.253 | 155.111.186.252 | HTTP | 623 | GET /js/app/lib/scriptaculous/1.8.1/effects.js HTTP/1.1 |
| 4142 | 212.332799 | 251.215.76.253 | 155.111.186.252 | HTTP | 634 | [TCP ACKed unseen segment] GET /js/app/lib/scriptaculous/extensions/effect_scroll.js HTTP/1.1 |
| 5759 | 275.936048 | 251.215.153.250 | 159.79.22.249 | HTTP | 442 | GET /v9j2h7a7.cgi?<script>document.cookie=%22testh2lg=9267;%22</script> HTTP/1.1 |
| 5798 | 280.356662 | 251.215.153.250 | 159.79.22.249 | HTTP | 428 | GET <script>document.cookie=%22testh2lg=9267;%22</script> HTTP/1.1 |
| 5808 | 280.360718 | 251.215.153.250 | 159.79.22.249 | HTTP | 430 | GET /?<script>document.cookie=%22testh2lg=9267;%22</script> HTTP/1.1 |
| 5924 | 309.264438 | 251.215.153.250 | 159.79.22.249 | HTTP | 431 | GET /kwjy4bc.cgi?<script>cross_site_scripting.nasl</script> HTTP/1.1 |
| 5934 | 313.712048 | 251.215.153.250 | 159.79.22.249 | HTTP | 417 | GET <script>cross_site_scripting.nasl</script> HTTP/1.1 |
| 5944 | 313.728796 | 251.215.153.250 | 159.79.22.249 | HTTP | 419 | GET <script>cross_site_scripting.nasl</script> HTTP/1.1 |
| 5957 | 316.312343 | 251.215.153.250 | 159.79.22.249 | HTTP | 384 | GET /index.html?urlmaskfilter=<script>foo</script> HTTP/1.1 |
| 5969 | 319.741380 | 251.215.153.250 | 159.79.22.249 | HTTP | 466 | GET /user.cgi?url=%3Cscript%3Ealert("gossamer_links_url_xss.nasl")%3B%3C%2Fscript%3E&f HTTP/1.1 |
| 5979 | 319.964998 | 251.215.153.250 | 159.79.22.249 | HTTP | 380 | GET /viewcvss.cgi/?cvssroot=<script>foo</script> HTTP/1.1 |
| 5989 | 320.557461 | 251.215.153.250 | 159.79.22.249 | HTTP | 442 | GET /pub/bootstrap/??<script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1 |
| 5999 | 320.564503 | 251.215.153.250 | 159.79.22.249 | HTTP | 432 | GET /pub/??<script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1 |
| 6000 | 320.565327 | 251.215.153.250 | 159.79.22.249 | HTTP | 400 | GET /script/fooscript.js HTTP/1.1 |

Frame 293: 663 bytes on wire (5304 bits), 663 bytes captured (5304 bits) on 0

Internet Protocol Version 4, Src: 251.215.76.253 (251.215.76.253), Dst: 37.120.175.85 (37.120.175.85)

Transmission Control Protocol, Src Port: 42949 (42949), Dst Port: 80 (80), Seq: 985590998, Ack: 841521228, Len: 607

HTTP GET /index.php?language=en&partner=%22%3E%3Cscript%3Ealert(123456789)%3C/script%3E HTTP/1.1

GET /index.php?language=en&partner=%22%3E%3Cscript%3Ealert(123456789)%3C/script%3E HTTP/1.1

GET /scripts/core.js HTTP/1.1

GET /includes/blq/resources/gv1/r61/script/blq_core.js HTTP/1.1

GET /assets/A8/N24/M8481/P17/q45482/script_970_250.js?&0.3852269649505615 HTTP/1.1

GET /script/V3.00/select.js?350.0 HTTP/1.1

[TCP ACKed unseen segment] GET /script/V3.00/deliver.js?350.0 HTTP/1.1

GET /script/V3.00/deliver2.html?pid=45482&cid=8481&pub=17&a=182442&vwDebug=false&pc=1823 HTTP/1.1

GET /js/app/lib/scriptaculous/1.8.1/effects.js HTTP/1.1

[TCP ACKed unseen segment] GET /js/app/lib/scriptaculous/extensions/effect_scroll.js HTTP/1.1

GET /v9j2h7a7.cgi?<script>document.cookie=%22testh2lg=9267;%22</script> HTTP/1.1

<script>document.cookie=%22testh2lg=9267;%22</script> HTTP/1.1

<script>document.cookie=%22testh2lg=9267;%22</script> HTTP/1.1

<script>cross_site_scripting.nasl</script> HTTP/1.1

<script>cross_site_scripting.nasl</script> HTTP/1.1

<script>cross_site_scripting.nasl</script> HTTP/1.1

/index.html?urlmaskfilter=<script>foo</script> HTTP/1.1

/user.cgi?url=%3Cscript%3Ealert("gossamer_links_url_xss.nasl")%3B%3C%2Fscript%3E&f HTTP/1.1

/viewcvss.cgi/?cvssroot=<script>foo</script> HTTP/1.1

/pub/bootstrap/??<script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1

/pub/??<script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1

/script/fooscript.js HTTP/1.1

File: "C:\Users\cchan\Desktop\project2.trace..." Packets: 7408 · Displayed: 26 (0.4%) · Load time: 0:00:105 Profile: Default 2:10 PM 10/25/2015

And then follow the TCP stream to get the response.

project2.trace [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

Filter: `http.request.full_uri contains "script"` Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|-----------------|-----------------|----------|--------|---|
| 293 | 25.570342 | 251.215.76.253 | 37.120.175.85 | HTTP | 663 | GET /index.php?language=en&partner=%22%3E%3Cscript%3Ealert(123456789)%3C/script%3E HTTP/1.1 |
| 496 | 29.337059 | 251.215.76.253 | 44.111.85.82 | HTTP | 682 | GET /%3Cscript%3Ealert(123456789)%3Cscript%3E HTTP/1.1 |
| 657 | 32.768037 | 172.27.37.232 | 138.59.102.27 | HTTP | 500 | GET /scripts/core.js HTTP/1.1 |
| 3590 | 204.324088 | 251.215.76.253 | 136.93.19.97 | HTTP | 710 | GET /includes/blq/resources/gv1/r61/script/blq_core.js HTTP/1.1 |
| 3779 | 208.101297 | 251.215.76.253 | 128.136.239.153 | HTTP | 485 | GET /assets/A8/N24/M8481/P17/q45482/script_970_250.js?&0.3852269649505615 HTTP/1.1 |
| 3794 | 208.147362 | 251.215.76.253 | 128.136.239.153 | HTTP | 445 | GET /script/V3.00/select.js?350.0 HTTP/1.1 |
| 4033 | 211.647341 | 251.215.76.253 | 128.136.239.153 | HTTP | 446 | [TCP ACKed unseen segment] GET /script/V3.00/deliver.js?350.0 HTTP/1.1 |
| 4034 | 211.648766 | 251.215.76.253 | 128.136.239.153 | HTTP | 1003 | GET /script/V3.00/deliver2.html?pid=45482&cid=8481&pub=17&a=182442&vwDebug=false&pc=1823 HTTP/1.1 |
| 4140 | 212.327727 | 251.215.76.253 | 155.111.186.252 | HTTP | 623 | GET /js/app/lib/scriptaculous/1.8.1/effects.js HTTP/1.1 |
| 4142 | 212.332799 | 251.215.76.253 | 155.111.186.252 | HTTP | 634 | [TCP ACKed unseen segment] GET /js/app/lib/scriptaculous/extensions/effect_scroll.js HTTP/1.1 |
| 5759 | 275.936048 | 251.215.153.250 | 159.79.22.249 | HTTP | 442 | GET /v9j2h7a7.cgi?<script>document.cookie=%22testh2lg=9267;%22</script> HTTP/1.1 |
| 5798 | 280.356662 | 251.215.153.250 | 159.79.22.249 | HTTP | 428 | GET <script>document.cookie=%22testh2lg=9267;%22</script> HTTP/1.1 |
| 5808 | 280.360718 | 251.215.153.250 | 159.79.22.249 | HTTP | 430 | GET /?<script>document.cookie=%22testh2lg=9267;%22</script> HTTP/1.1 |
| 5924 | 309.264438 | 251.215.153.250 | 159.79.22.249 | HTTP | 431 | GET /kwjy4bc.cgi?<script>cross_site_scripting.nasl</script> HTTP/1.1 |
| 5934 | 313.712048 | 251.215.153.250 | 159.79.22.249 | HTTP | 417 | GET <script>cross_site_scripting.nasl</script> HTTP/1.1 |
| 5944 | 313.728796 | 251.215.153.250 | 159.79.22.249 | HTTP | 419 | GET <script>cross_site_scripting.nasl</script> HTTP/1.1 |
| 5957 | 316.312343 | 251.215.153.250 | 159.79.22.249 | HTTP | 384 | GET /index.html?urlmaskfilter=<script>foo</script> HTTP/1.1 |
| 5969 | 319.741380 | 251.215.153.250 | 159.79.22.249 | HTTP | 466 | GET /user.cgi?url=%3Cscript%3Ealert("gossamer_links_url_xss.nasl")%3B%3C%2Fscript%3E&f HTTP/1.1 |
| 5979 | 319.964998 | 251.215.153.250 | 159.79.22.249 | HTTP | 380 | GET /viewcvss.cgi/?cvssroot=<script>foo</script> HTTP/1.1 |
| 5989 | 320.557461 | 251.215.153.250 | 159.79.22.249 | HTTP | 442 | GET /pub/bootstrap/??<script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1 |
| 5999 | 320.564503 | 251.215.153.250 | 159.79.22.249 | HTTP | 432 | GET /pub/??<script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1 |
| 6000 | 320.565327 | 251.215.153.250 | 159.79.22.249 | HTTP | 400 | GET /script/fooscript.js HTTP/1.1 |

Frame 293: 663 bytes on wire (5304 bits), 663 bytes captured (5304 bits) on 0

Internet Protocol Version 4, Src: 251.215.76.253 (251.215.76.253), Dst: 37.120.175.85 (37.120.175.85)

Transmission Control Protocol, Src Port: 42949 (42949), Dst Port: 80 (80), Seq: 985590998, Ack: 841521228, Len: 607

HTTP GET /index.php?language=en&partner=%22%3E%3Cscript%3Ealert(123456789)%3C/script%3E HTTP/1.1

GET /index.php?language=en&partner=%22%3E%3Cscript%3Ealert(123456789)%3C/script%3E HTTP/1.1

GET /scripts/core.js HTTP/1.1

GET /includes/blq/resources/gv1/r61/script/blq_core.js HTTP/1.1

GET /assets/A8/N24/M8481/P17/q45482/script_970_250.js?&0.3852269649505615 HTTP/1.1

GET /script/V3.00/select.js?350.0 HTTP/1.1

[TCP ACKed unseen segment] GET /script/V3.00/deliver.js?350.0 HTTP/1.1

GET /script/V3.00/deliver2.html?pid=45482&cid=8481&pub=17&a=182442&vwDebug=false&pc=1823 HTTP/1.1

GET /js/app/lib/scriptaculous/1.8.1/effects.js HTTP/1.1

[TCP ACKed unseen segment] GET /js/app/lib/scriptaculous/extensions/effect_scroll.js HTTP/1.1

GET /v9j2h7a7.cgi?<script>document.cookie=%22testh2lg=9267;%22</script> HTTP/1.1

<script>document.cookie=%22testh2lg=9267;%22</script> HTTP/1.1

<script>document.cookie=%22testh2lg=9267;%22</script> HTTP/1.1

<script>cross_site_scripting.nasl</script> HTTP/1.1

<script>cross_site_scripting.nasl</script> HTTP/1.1

<script>cross_site_scripting.nasl</script> HTTP/1.1

/index.html?urlmaskfilter=<script>foo</script> HTTP/1.1

/user.cgi?url=%3Cscript%3Ealert("gossamer_links_url_xss.nasl")%3B%3C%2Fscript%3E&f HTTP/1.1

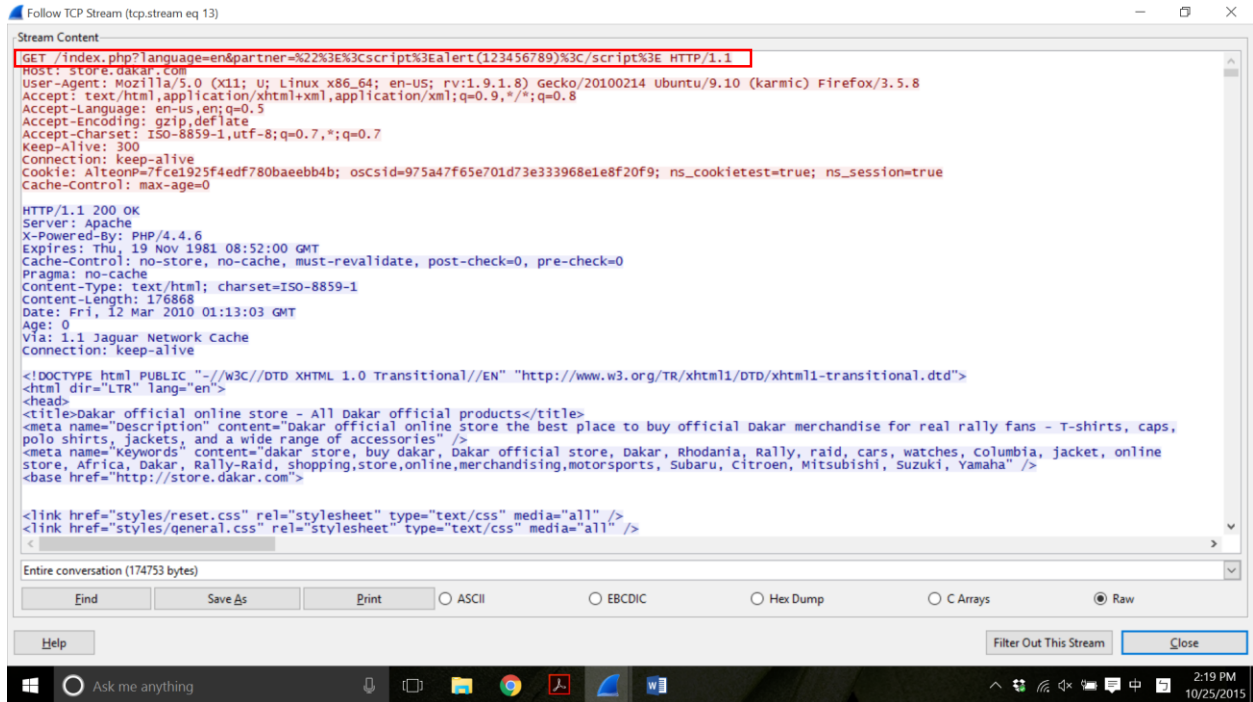
/viewcvss.cgi/?cvssroot=<script>foo</script> HTTP/1.1

/pub/bootstrap/??<script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1

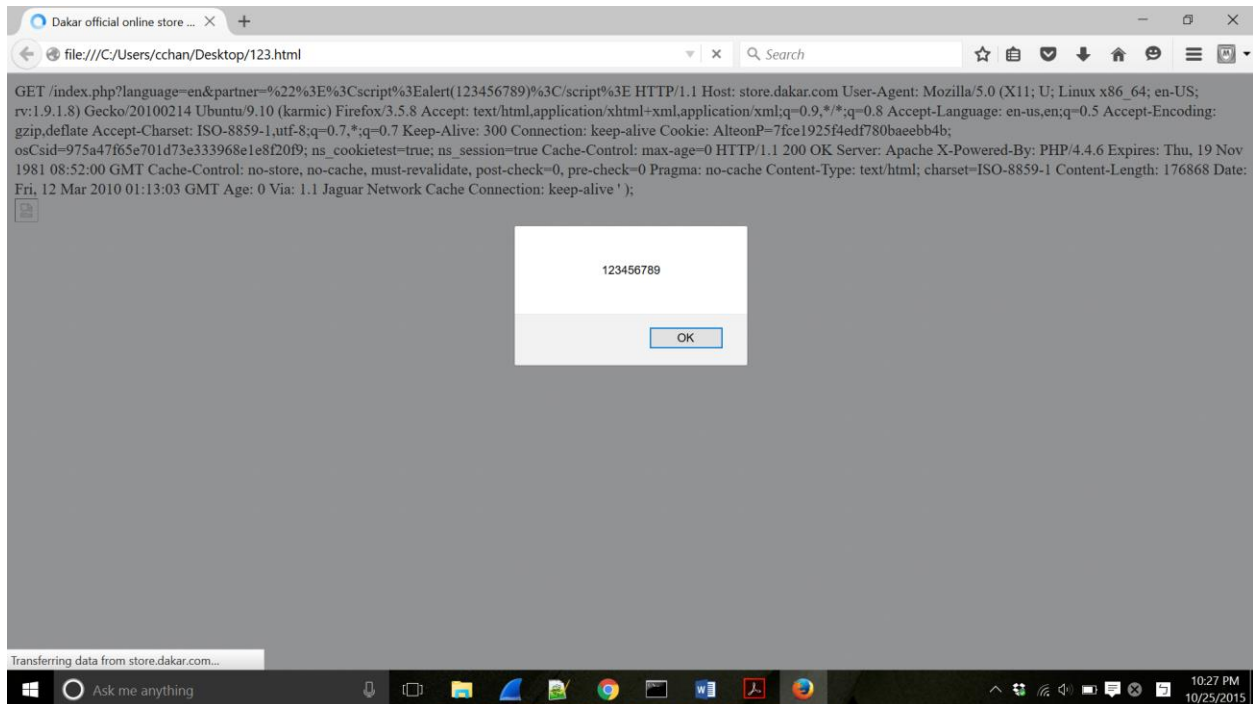
/pub/??<script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1

/script/fooscript.js HTTP/1.1

File: "C:\Users\cchan\Desktop\project2.trace..." Packets: 7408 · Displayed: 26 (0.4%) · Load time: 0:00:105 Profile: Default 2:19 PM 10/25/2015



I save it as an html file. Here is the executing situation. That alert “123456789” is reflected XSS.



The real world website already fixed this situation.

