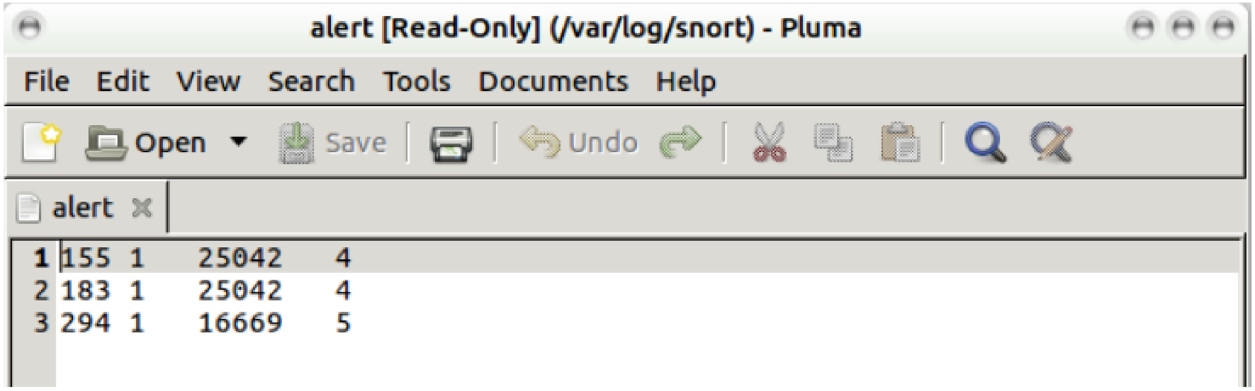
Brian Chan
April 21st, 2021

CS-UY 3933 Network Security
Lab 4

Part 1:



```
155 1    25042    4
183 1    25042    4
294 1    16669    5
```

Generator ID/Snort ID/Revision ID for 155: 1, 25042, 4

1: Snort default alert.

25042: Attempt to exploit unknown Java vulnerability. Downloading portable executable.

4: Number of revisions the alert has undergone.

Generator ID/Snort ID/Revision ID for 183: 1, 25042, 4

1: Snort default alert.

25042: Attempt to exploit unknown Java vulnerability. Downloading portable executable.

4: Number of revisions the alert has undergone.

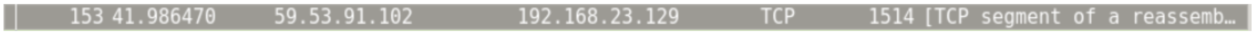
Generator ID/Snort ID/Revision ID for 294: 1, 16669, 5

1: Snort default alert.

16669: Spyeye bot variant outbound connection.

5: Number of revisions the alert has undergone.

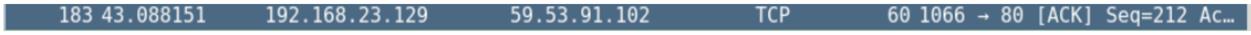
Packet 155



```
153 41.986470    59.53.91.102    192.168.23.129    TCP    1514 [TCP segment of a reassemb…
```

Source IP: 192.168.23.129, Destination IP: 59.53.91.102, Source port: 1067, Destination port: 80, Protocol: TCP

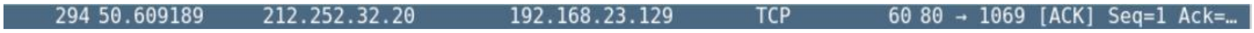
Packet 183



```
183 43.088151    192.168.23.129    59.53.91.102    TCP    60 1066 → 80 [ACK] Seq=212 Ac…
```

Source IP: 192.168.23.129, Destination IP: 59.53.91.102, Source port: 1066, Destination port: 80, Protocol: TCP

Packet 294

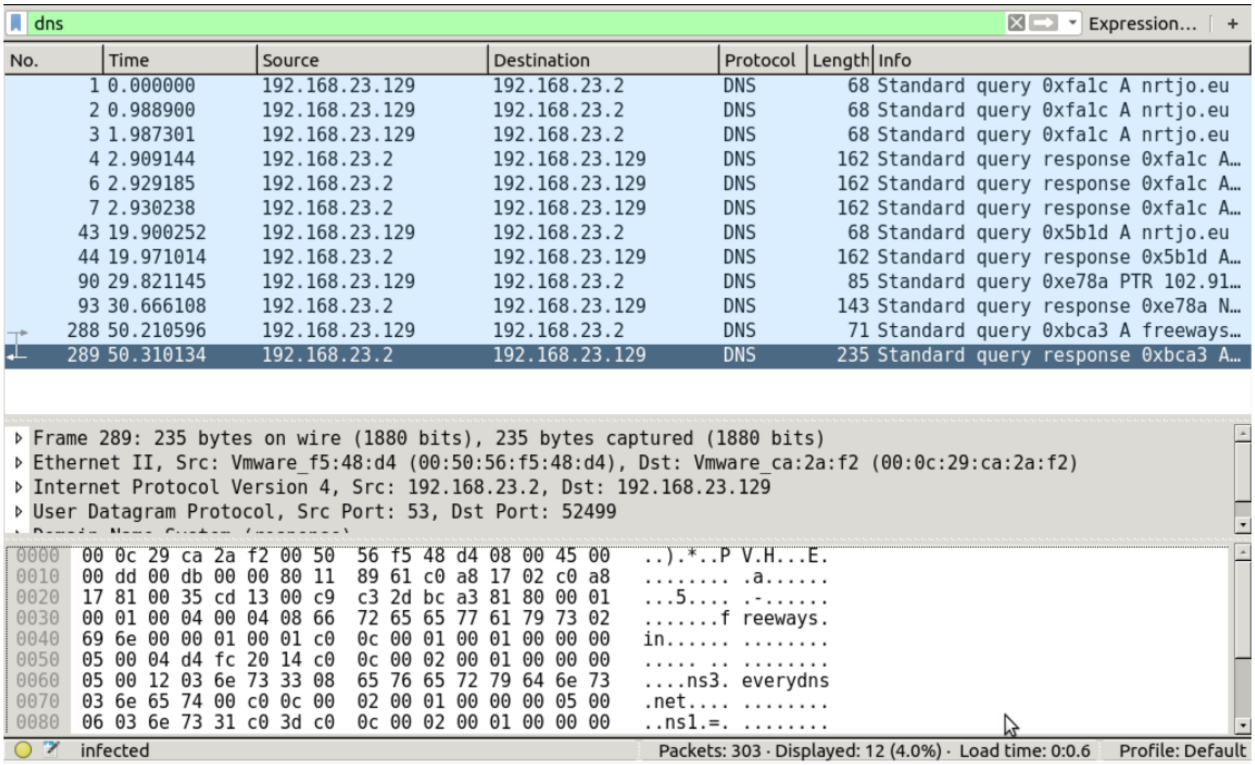


```
294 50.609189    212.252.32.20    192.168.23.129    TCP    60 80 → 1069 [ACK] Seq=1 Ack=…
```

Source IP: 212.252.32.20, Destination IP: 192.168.23.129, Source port: 80, Destination port: 1069, Protocol: TCP

Part 2:

3.



dns

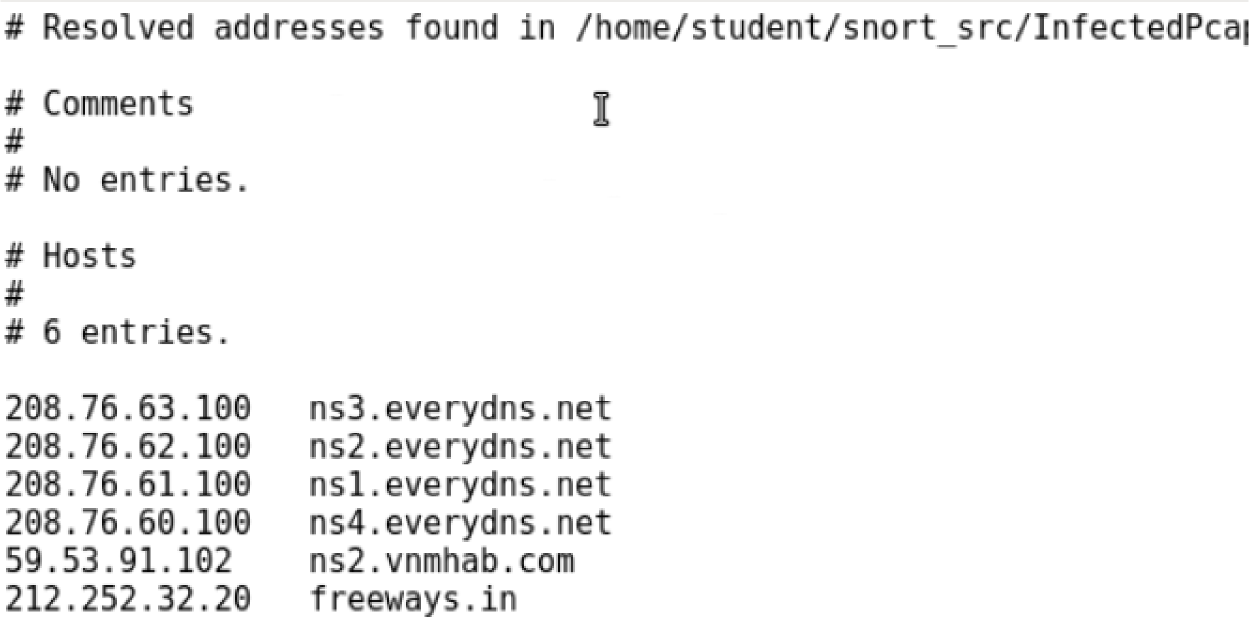
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfa1c A nrtjo.eu
2	0.988900	192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfa1c A nrtjo.eu
3	1.987301	192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfa1c A nrtjo.eu
4	2.909144	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfa1c A…
6	2.929185	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfa1c A…
7	2.930238	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfa1c A…
43	19.900252	192.168.23.129	192.168.23.2	DNS	68	Standard query 0x5b1d A nrtjo.eu
44	19.971014	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0x5b1d A…
90	29.821145	192.168.23.129	192.168.23.2	DNS	85	Standard query 0xe78a PTR 102.91…
93	30.666108	192.168.23.2	192.168.23.129	DNS	143	Standard query response 0xe78a N…
288	50.210596	192.168.23.129	192.168.23.2	DNS	71	Standard query 0xbca3 A freeways…
289	50.310134	192.168.23.2	192.168.23.129	DNS	235	Standard query response 0xbca3 A…

```
▷ Frame 289: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits)
▷ Ethernet II, Src: Vmware_f5:48:d4 (00:50:56:f5:48:d4), Dst: Vmware_ca:2a:f2 (00:0c:29:ca:2a:f2)
▷ Internet Protocol Version 4, Src: 192.168.23.2, Dst: 192.168.23.129
▷ User Datagram Protocol, Src Port: 53, Dst Port: 52499
▷ Domain Name System (response)
```

```
0000  00 0c 29 ca 2a f2 00 50  56 f5 48 d4 08 00 45 00   ..).*..P V.H...E.
0010  00 dd 00 db 00 00 80 11  89 61 c0 a8 17 02 c0 a8   ........ .a......
0020  17 81 00 35 cd 13 00 c9  c3 2d bc a3 81 80 00 01   ...5.... .-......
0030  00 01 00 04 00 04 08 66  72 65 65 77 61 79 73 02   .......f reeways.
0040  69 6e 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   in...... ........
0050  05 00 04 d4 fc 20 14 c0  0c 00 02 00 01 00 00 00   ..... .. ........
0060  05 00 12 03 6e 73 33 08  65 76 65 72 79 64 6e 73   ....ns3. everydns
0070  03 6e 65 74 00 c0 0c 00  02 00 01 00 00 00 05 00   .net.... ........
0080  06 03 6e 73 31 c0 3d c0  0c 00 02 00 01 00 00 00   ..ns1.=. ........
```

infected   Packets: 303 · Displayed: 12 (4.0%) · Load time: 0:0.6   Profile: Default

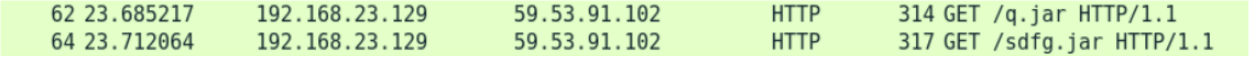
DNS filter



```
# Resolved addresses found in /home/student/snort_src/InfectedPca

# Comments
#
# No entries.

# Hosts
#
# 6 entries.

208.76.63.100   ns3.everydns.net
208.76.62.100   ns2.everydns.net
208.76.61.100   ns1.everydns.net
208.76.60.100   ns4.everydns.net
59.53.91.102    ns2.vnmhab.com
212.252.32.20   freeways.in
```

6 resolved addresses listed.

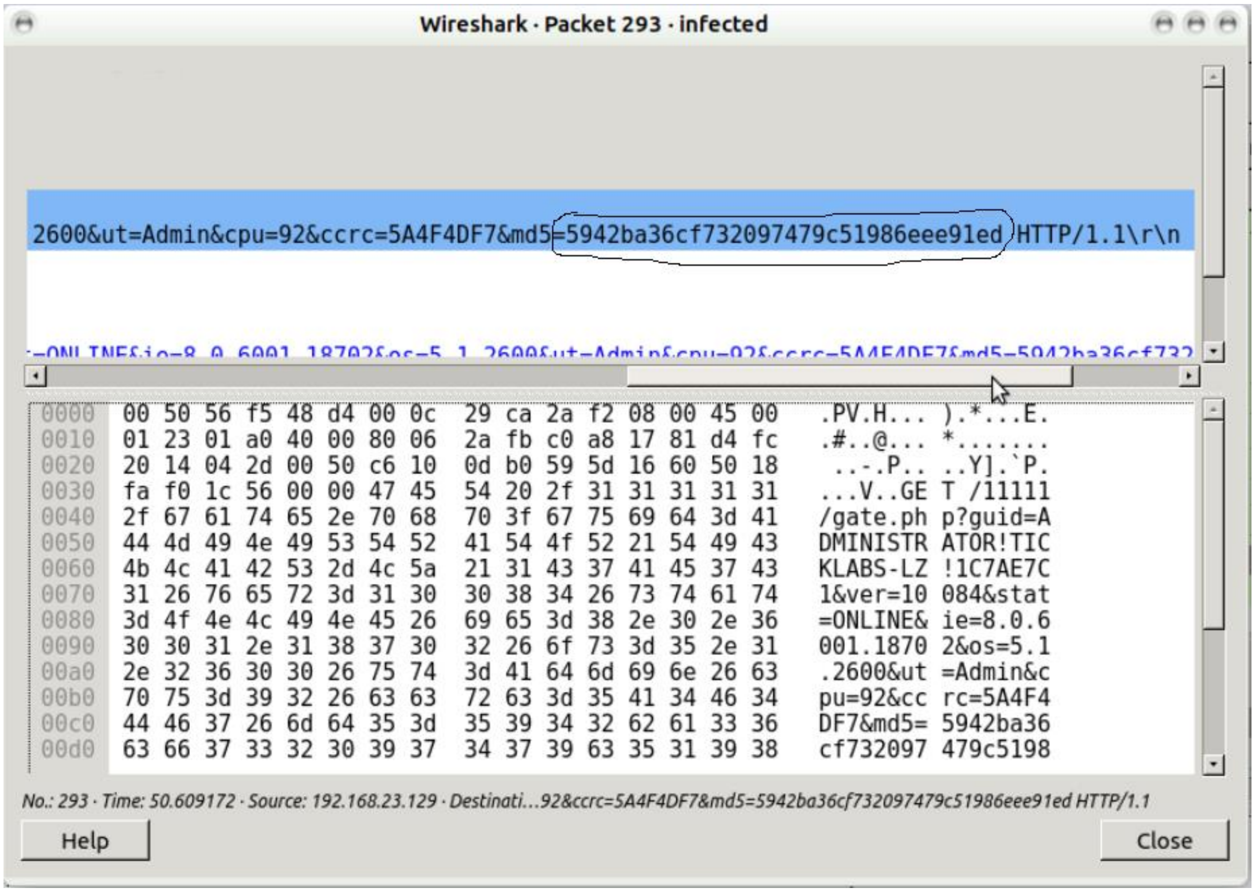
4.



```
   62 23.685217     192.168.23.129      59.53.91.102        HTTP      314 GET /q.jar HTTP/1.1
   64 23.712064     192.168.23.129      59.53.91.102        HTTP      317 GET /sdfg.jar HTTP/1.1
```

Two .jar packets: q.jar, qdfg.jar

5.



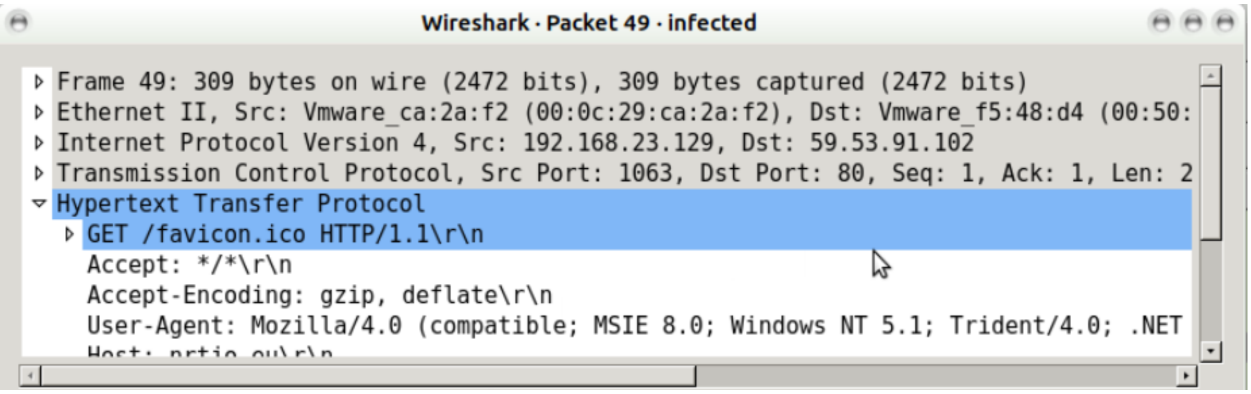
```
2600&ut=Admin&cpu=92&ccrc=5A4F4DF7&md5=5942ba36cf732097479c51986eee91ed HTTP/1.1\r\n

=ONLINE&ie=8.0.6001.18702&os=5.1.2600&ut=Admin&cpu=92&ccrc=5A4F4DF7&md5=5942ba36cf732
```

```
0000  00 50 56 f5 48 d4 00 0c  29 ca 2a f2 08 00 45 00   .PV.H... ).*...E.
0010  01 23 01 a0 40 00 80 06  2a fb c0 a8 17 81 d4 fc   .#..@... *.......
0020  20 14 04 2d 00 50 c6 10  0d b0 59 5d 16 60 50 18    ..-.P.. ..Y].`P.
0030  fa f0 1c 56 00 00 47 45  54 20 2f 31 31 31 31 31   ...V..GE T /11111
0040  2f 67 61 74 65 2e 70 68  70 3f 67 75 69 64 3d 41   /gate.ph p?guid=A
0050  44 4d 49 4e 49 53 54 52  41 54 4f 52 21 54 49 43   DMINISTR ATOR!TIC
0060  4b 4c 41 42 53 2d 4c 5a  21 31 43 37 41 45 37 43   KLABS-LZ !1C7AE7C
0070  31 26 76 65 72 3d 31 30  30 38 34 26 73 74 61 74   1&ver=10 084&stat
0080  3d 4f 4e 4c 49 4e 45 26  69 65 3d 38 2e 30 2e 36   =ONLINE& ie=8.0.6
0090  30 30 31 2e 31 38 37 30  32 26 6f 73 3d 35 2e 31   001.1870 2&os=5.1
00a0  2e 32 36 30 30 26 75 74  3d 41 64 6d 69 6e 26 63   .2600&ut =Admin&c
00b0  70 75 3d 39 32 26 63 63  72 63 3d 35 41 34 46 34   pu=92&cc rc=5A4F4
00c0  44 46 37 26 6d 64 35 3d  35 39 34 32 62 61 33 36   DF7&md5= 5942ba36
00d0  63 66 37 33 32 30 39 37  34 37 39 63 35 31 39 38   cf732097 479c5198
```

No.: 293 · Time: 50.609172 · Source: 192.168.23.129 · Destinati…92&ccrc=5A4F4DF7&md5=5942ba36cf732097479c51986eee91ed HTTP/1.1

MD5 is circled, from packet 293.

6.



```
▷ Frame 49: 309 bytes on wire (2472 bits), 309 bytes captured (2472 bits)
▷ Ethernet II, Src: Vmware_ca:2a:f2 (00:0c:29:ca:2a:f2), Dst: Vmware_f5:48:d4 (00:50:
▷ Internet Protocol Version 4, Src: 192.168.23.129, Dst: 59.53.91.102
▷ Transmission Control Protocol, Src Port: 1063, Dst Port: 80, Seq: 1, Ack: 1, Len: 2
▽ Hypertext Transfer Protocol
  ▷ GET /favicon.ico HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET
    Host: nrtio.ou\r\n
```

Client is using Mozilla.