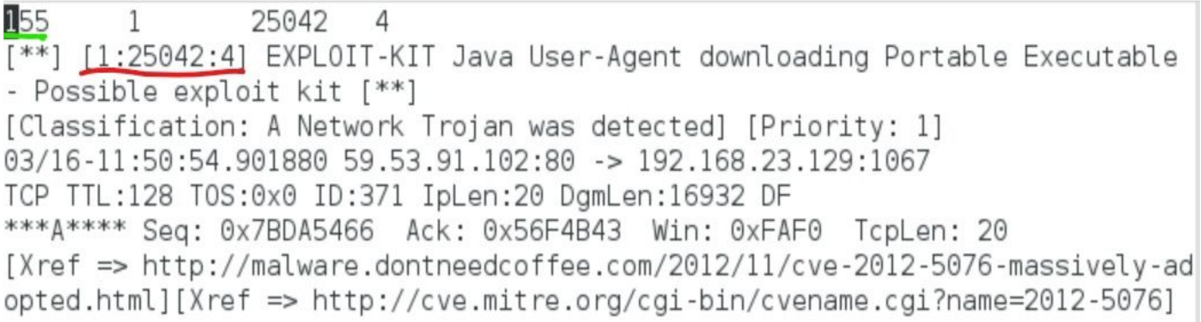
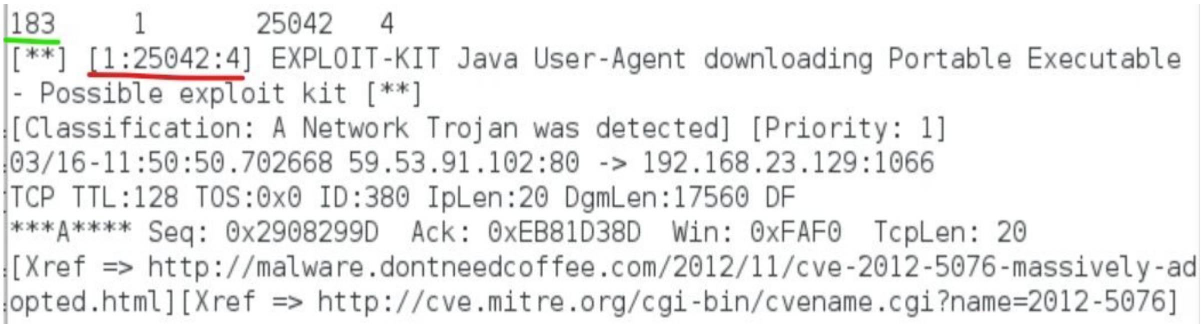
Lab #4 - SNORT
Sam Mishra
N12140743

command : sudo snort -c /etc/snort/snort.conf -r /home/student/InfectedPcaps/infected.pcap -A fast -A full -A test

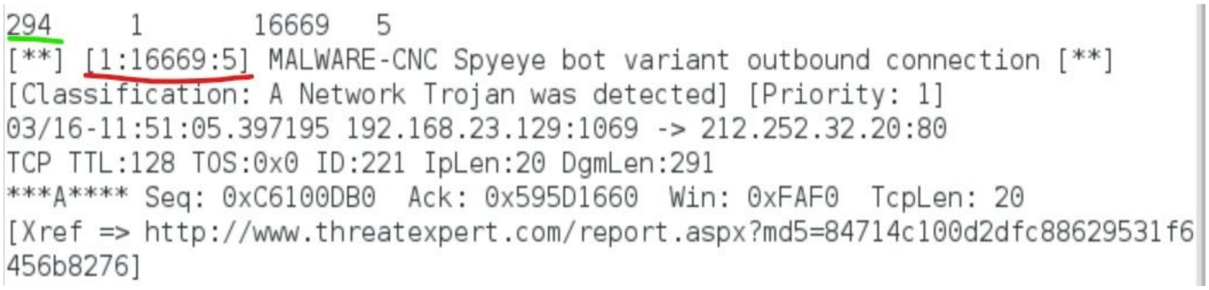
1. /var/log/snort/alert:



```
155     1       25042   4
[**] [1:25042:4] EXPLOIT-KIT Java User-Agent downloading Portable Executable
- Possible exploit kit [**]
[Classification: A Network Trojan was detected] [Priority: 1]
03/16-11:50:54.901880 59.53.91.102:80 -> 192.168.23.129:1067
TCP TTL:128 TOS:0x0 ID:371 IpLen:20 DgmLen:16932 DF
***A**** Seq: 0x7BDA5466  Ack: 0x56F4B43  Win: 0xFAF0  TcpLen: 20
[Xref => http://malware.dontneedcoffee.com/2012/11/cve-2012-5076-massively-ad
opted.html][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-5076]
```



```
183     1       25042   4
[**] [1:25042:4] EXPLOIT-KIT Java User-Agent downloading Portable Executable
- Possible exploit kit [**]
[Classification: A Network Trojan was detected] [Priority: 1]
03/16-11:50:50.702668 59.53.91.102:80 -> 192.168.23.129:1066
TCP TTL:128 TOS:0x0 ID:380 IpLen:20 DgmLen:17560 DF
***A**** Seq: 0x2908299D  Ack: 0xEB81D38D  Win: 0xFAF0  TcpLen: 20
[Xref => http://malware.dontneedcoffee.com/2012/11/cve-2012-5076-massively-ad
opted.html][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-5076]
```



```
294     1       16669   5
[**] [1:16669:5] MALWARE-CNC Spyeye bot variant outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
03/16-11:51:05.397195 192.168.23.129:1069 -> 212.252.32.20:80
TCP TTL:128 TOS:0x0 ID:221 IpLen:20 DgmLen:291
***A**** Seq: 0xC6100DB0  Ack: 0x595D1660  Win: 0xFAF0  TcpLen: 20
[Xref => http://www.threatexpert.com/report.aspx?md5=84714c100d2dfc88629531f6
456b8276]
```

Snort alerted us three times.

Alert #1: **GID** = 1; **SID** = 25042; **RID** = 4; https://www.snort.org/rule_docs/1-25042

Summary: This event is generated when an attempt is made to exploit a known vulnerability in jdk.

Impact: Denial of Service. Information disclosure. Loss of integrity.

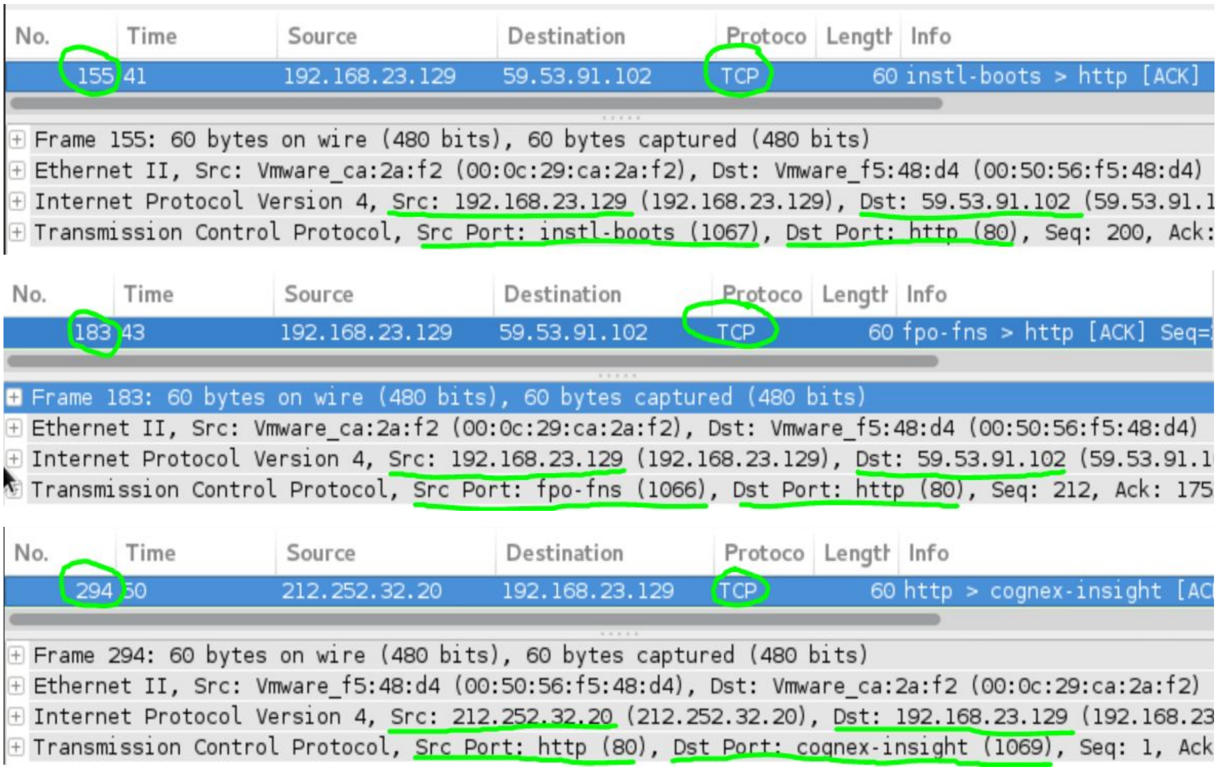
Alert #2: **GID** = 1; **SID** = 25042; **RID** = 4

Alert #3: **GID** = 1; **SID** = 16669; **RID** = 5; https://www.snort.org/rule_docs/1-16669

Summary: This event is generated when activity relating to the spyware application "Spyeye bot" is detected.

Impact: This event is generated when an attempt is made to exploit a known vulnerability in jdk.

2. Suspicious Packets Viewed In Wireshark:



```
No.     Time   Source            Destination     Protoco  Lengtt  Info
155     41     192.168.23.129    59.53.91.102    TCP      60 instl-boots > http [ACK]

⊞ Frame 155: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: Vmware_ca:2a:f2 (00:0c:29:ca:2a:f2), Dst: Vmware_f5:48:d4 (00:50:56:f5:48:d4)
⊞ Internet Protocol Version 4, Src: 192.168.23.129 (192.168.23.129), Dst: 59.53.91.102 (59.53.91.1
⊞ Transmission Control Protocol, Src Port: instl-boots (1067), Dst Port: http (80), Seq: 200, Ack:
```

```
No.     Time   Source            Destination     Protoco  Lengtt  Info
183     43     192.168.23.129    59.53.91.102    TCP      60 fpo-fns > http [ACK] Seq=

⊞ Frame 183: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: Vmware_ca:2a:f2 (00:0c:29:ca:2a:f2), Dst: Vmware_f5:48:d4 (00:50:56:f5:48:d4)
⊞ Internet Protocol Version 4, Src: 192.168.23.129 (192.168.23.129), Dst: 59.53.91.102 (59.53.91.1
⊞ Transmission Control Protocol, Src Port: fpo-fns (1066), Dst Port: http (80), Seq: 212, Ack: 175
```

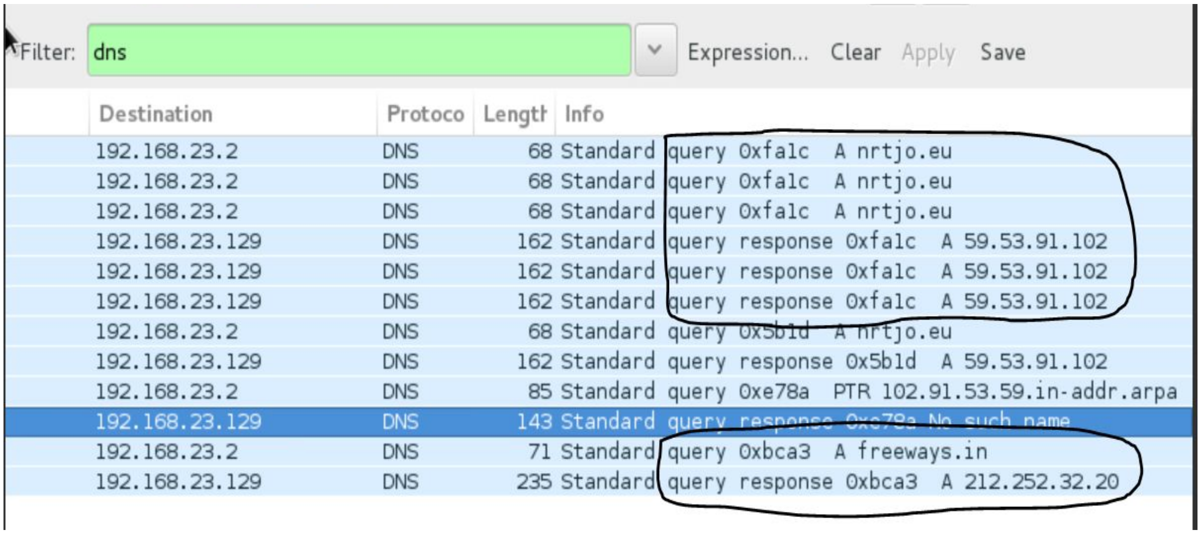
```
No.     Time   Source            Destination     Protoco  Lengtt  Info
294     50     212.252.32.20     192.168.23.129  TCP      60 http > cognex-insight [AC

⊞ Frame 294: 60 bytes on wire (480 bits), 60 bytes captured (480 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: 212.252.32.20 (212.252.32.20), Dst: 192.168.23.129 (192.168.23
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: cognex-insight (1069), Seq: 1, Ack
```

Packet #155 -	**Src**:	192.168.23.129
	Src Port:	1067
	Dst:	59.53.91.102
	Dst Port:	80
	Protocol:	TCP
Packet #183 -	**Src**:	192.168.23.129
	Src Port:	1066
	Dst:	59.53.91.102
	Dst Port:	80
	Protocol:	TCP
Packet #294 -	**Src**:	212.252.32.20
	Src Port:	80
	Dst:	192.168.23.129
	Dst Port:	1069
	Protocol:	TCP

Wireshark Exercises

1. DNS



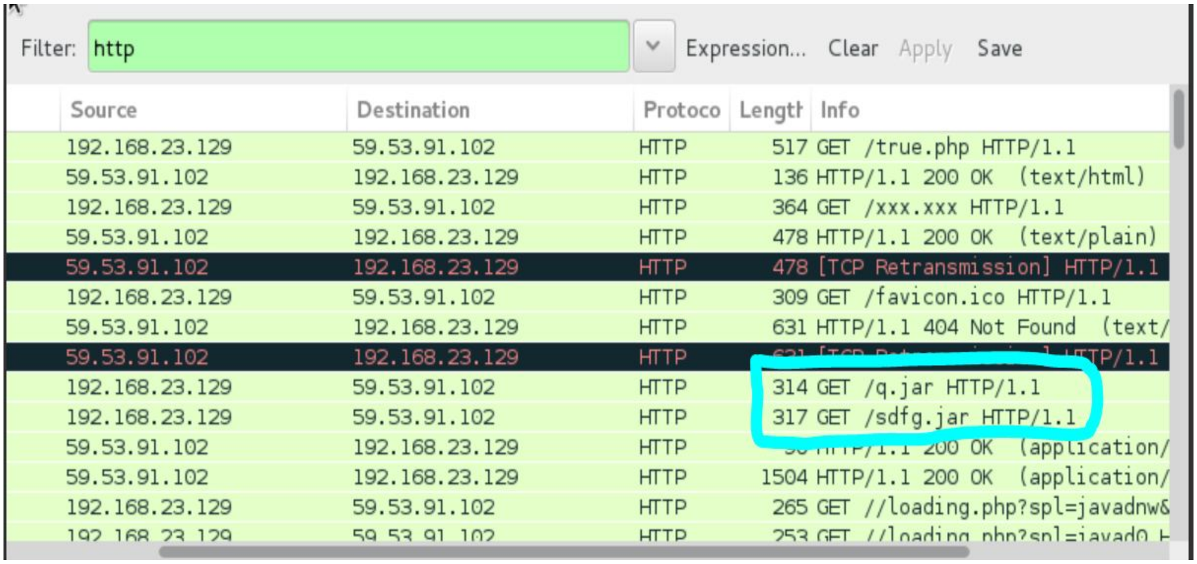
```
Filter: dns                                Expression...  Clear  Apply  Save

Destination        Protoco  Length  Info
192.168.23.2       DNS          68  Standard query 0xfa1c  A nrtjo.eu
192.168.23.2       DNS          68  Standard query 0xfa1c  A nrtjo.eu
192.168.23.2       DNS          68  Standard query 0xfa1c  A nrtjo.eu
192.168.23.129     DNS         162  Standard query response 0xfa1c  A 59.53.91.102
192.168.23.129     DNS         162  Standard query response 0xfa1c  A 59.53.91.102
192.168.23.129     DNS         162  Standard query response 0xfa1c  A 59.53.91.102
192.168.23.2       DNS          68  Standard query 0x5b1d  A nrtjo.eu
192.168.23.129     DNS         162  Standard query response 0x5b1d  A 59.53.91.102
192.168.23.2       DNS          85  Standard query 0xe78a  PTR 102.91.53.59.in-addr.arpa
192.168.23.129     DNS         143  Standard query response 0xe78a No such name
192.168.23.2       DNS          71  Standard query 0xbca3  A freeways.in
192.168.23.129     DNS         235  Standard query response 0xbca3  A 212.252.32.20
```

Two domains were resolved.

Nrjto.eu	resolved to	59.53.91.102
Freeways.in	resolved to	212.252.32.20

2. Java Applets



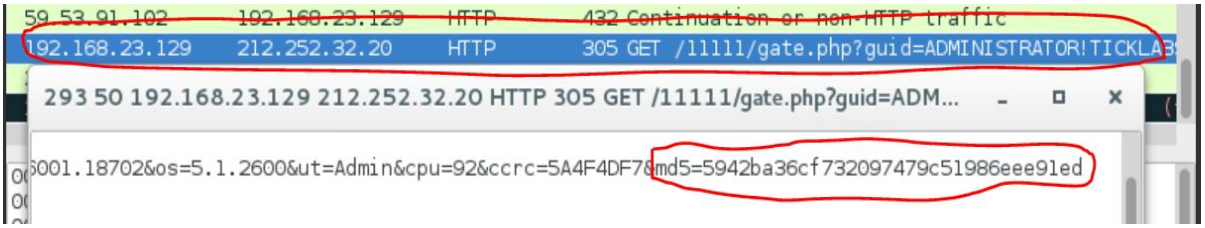
```
Filter: http                               Expression...  Clear  Apply  Save

Source            Destination       Protoco  Length  Info
192.168.23.129    59.53.91.102      HTTP        517  GET /true.php HTTP/1.1
59.53.91.102      192.168.23.129    HTTP        136  HTTP/1.1 200 OK  (text/html)
192.168.23.129    59.53.91.102      HTTP        364  GET /xxx.xxx HTTP/1.1
59.53.91.102      192.168.23.129    HTTP        478  HTTP/1.1 200 OK  (text/plain)
59.53.91.102      192.168.23.129    HTTP        478  [TCP Retransmission] HTTP/1.1
192.168.23.129    59.53.91.102      HTTP        309  GET /favicon.ico HTTP/1.1
59.53.91.102      192.168.23.129    HTTP        631  HTTP/1.1 404 Not Found  (text/
59.53.91.102      192.168.23.129    HTTP        631  [TCP Retransmission] HTTP/1.1
192.168.23.129    59.53.91.102      HTTP        314  GET /q.jar HTTP/1.1
192.168.23.129    59.53.91.102      HTTP        317  GET /sdfg.jar HTTP/1.1
59.53.91.102      192.168.23.129    HTTP         30  HTTP/1.1 200 OK  (application/
59.53.91.102      192.168.23.129    HTTP       1504  HTTP/1.1 200 OK  (application/
192.168.23.129    59.53.91.102      HTTP        265  GET //loading.php?spl=javadnw&
192.168.23.129    59.53.91.102      HTTP        253  GET //loading.php?spl=javad0 H
```

The two .jar files that implemented the applets are:

- q.jar
- sdfg.jar

3. Malicious Executable MD5



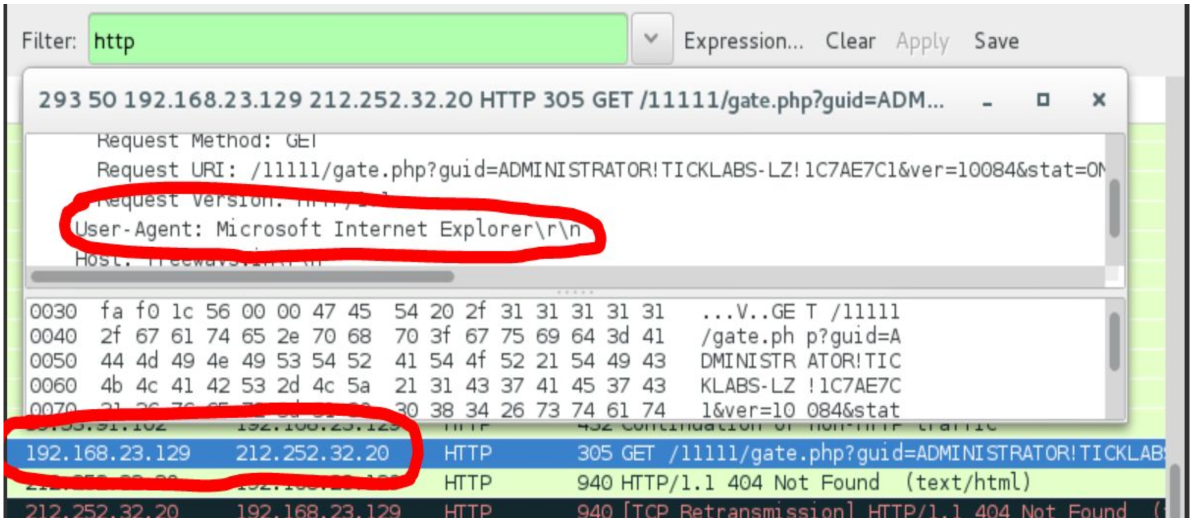
```
59.53.91.102     192.168.23.129    HTTP    432 Continuation or non-HTTP traffic
192.168.23.129   212.252.32.20     HTTP    305 GET /11111/gate.php?guid=ADMINISTRATOR!TICKLAB
```

293 50 192.168.23.129 212.252.32.20 HTTP 305 GET /11111/gate.php?guid=ADM...

```
6001.18702&os=5.1.2600&ut=Admin&cpu=92&ccrc=5A4F4DF7&md5=5942ba36cf732097479c51986eee91ed
```

MD5=5942ba36cf732097479c51986eee91ed

4. Browser

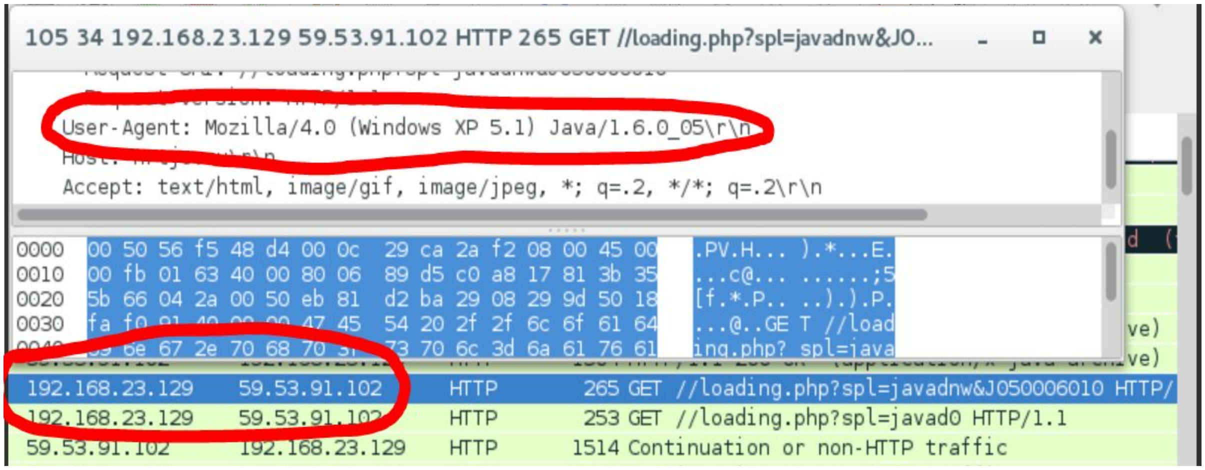


293 50 192.168.23.129 212.252.32.20 HTTP 305 GET /11111/gate.php?guid=ADM...

```
    Request Method: GET
    Request URI: /11111/gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7AE7C1&ver=10084&stat=ON
    Request Version: HTTP/1.1
  User-Agent: Microsoft Internet Explorer\r\n
  Host: [illegible]\r\n
```

```
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  [illegible]              30 38 34 26 73 74 61 74   1&ver=10 084&stat
```

```
59.53.91.102     192.168.23.129    HTTP    432 Continuation or non-HTTP traffic
192.168.23.129   212.252.32.20     HTTP    305 GET /11111/gate.php?guid=ADMINISTRATOR!TICKLAB
212.252.32.20    192.168.23.129    HTTP    940 HTTP/1.1 404 Not Found  (text/html)
212.252.32.20    192.168.23.129    HTTP    940 [TCP Retransmission] HTTP/1.1 404 Not Found
```



105 34 192.168.23.129 59.53.91.102 HTTP 265 GET //loading.php?spl=javadnw&JO...

```
  Request URI: //loading.php?spl=javadnw&J050006010
  Request Version: HTTP/1.1
  User-Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_05\r\n
  Host: [illegible]\r\n
  Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2\r\n
```

```
0000  00 50 56 f5 48 d4 00 0c  29 ca 2a f2 08 00 45 00   .PV.H... ).*...E.
0010  00 fb 01 63 40 00 80 06  89 d5 c0 a8 17 81 3b 35   ...c@... ......;5
0020  5b 66 04 2a 00 50 eb 81  d2 ba 29 08 29 9d 50 18   [f.*.P.. ..).).P.
0030  fa f0 91 40 00 00 47 45  54 20 2f 2f 6c 6f 61 64   ...@..GE T //load
0040  69 6e 67 2e 70 68 70 3f  73 70 6c 3d 6a 61 76 61   ing.php? spl=java
```

```
192.168.23.129   59.53.91.102      HTTP    265 GET //loading.php?spl=javadnw&J050006010 HTTP/
192.168.23.129   59.53.91.102      HTTP    253 GET //loading.php?spl=javad0 HTTP/1.1
59.53.91.102     192.168.23.129    HTTP    1514 Continuation or non-HTTP traffic
```

There seems to be two browsers in use:

Internet Explorer
Mozilla