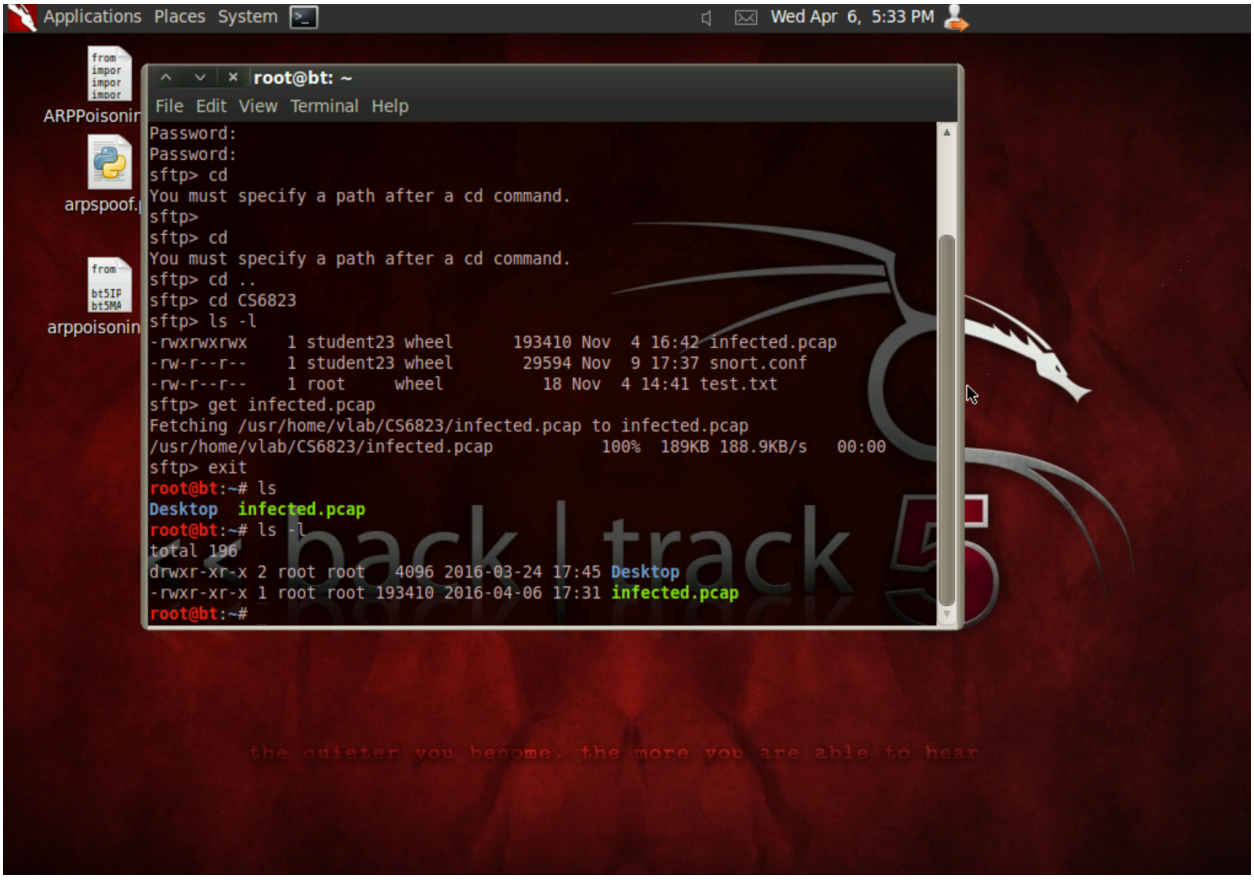
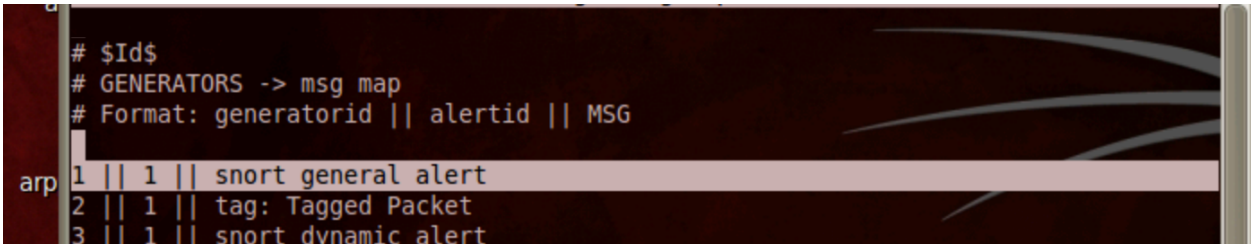
Lab 3: Snort
Masato Anzai
N12725403
ma3156

Downloading infected.pcap from SFTP



1.

GID:



SID:

EXPLOIT-KIT Java User-Agent downloading Portable Executable - Possible exploit kit

Sid 1-25402

Summary:

BLACKLIST DNS request for known malware domain csrss-update-new.com

Sid 1-16669

Summary

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

Impact

Unkown. Possible information disclosure, violation of privacy, possible violation of policy.

Detailed information

Spyware is malicious software running on a host that may intercept or take information from the host system without a users consent or knowledge. Spyware is also capable of using a hosts Internet connection without the knowlege or consent of the user, in order to deliver that information to an unauthorized third party.

This software not only uses available bandwidth on a network connection but also consumes system resources to the point of making the host unusable in some cases.

Spyware can be classified into multiple categories depending on the behavior of the software.

Alert Tags Explained:
GID 1 = snort general alert.
SID 25402 = EXPLOIT-KIT Java User-Agent downloading Portable Executable
SID 16669 = MALWARE-CNC Spyeye bot variant outbound connection
Revision ID 3 = Revision 3
Revision ID 5 = Revision 5

ALERTS:
Alert #1:

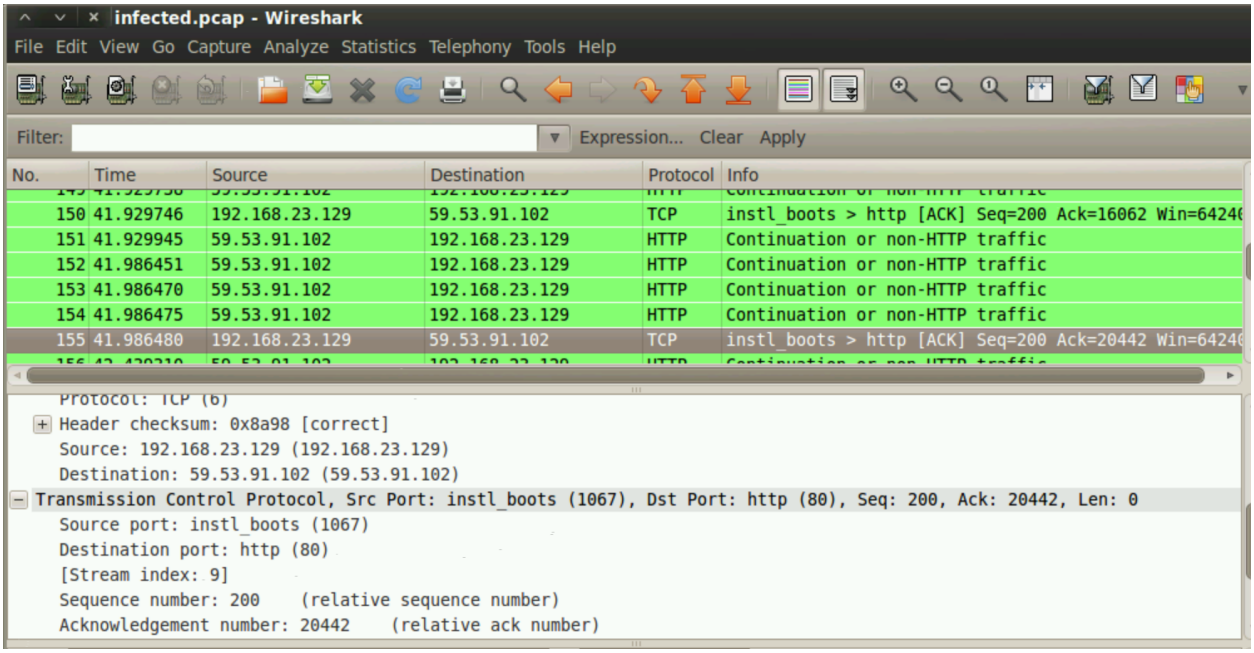
Generator ID: 1
Snort ID: 25402
Revision ID: 3

Alert #2
Generator ID: 1
Snort ID: 25402
Revision ID: 3

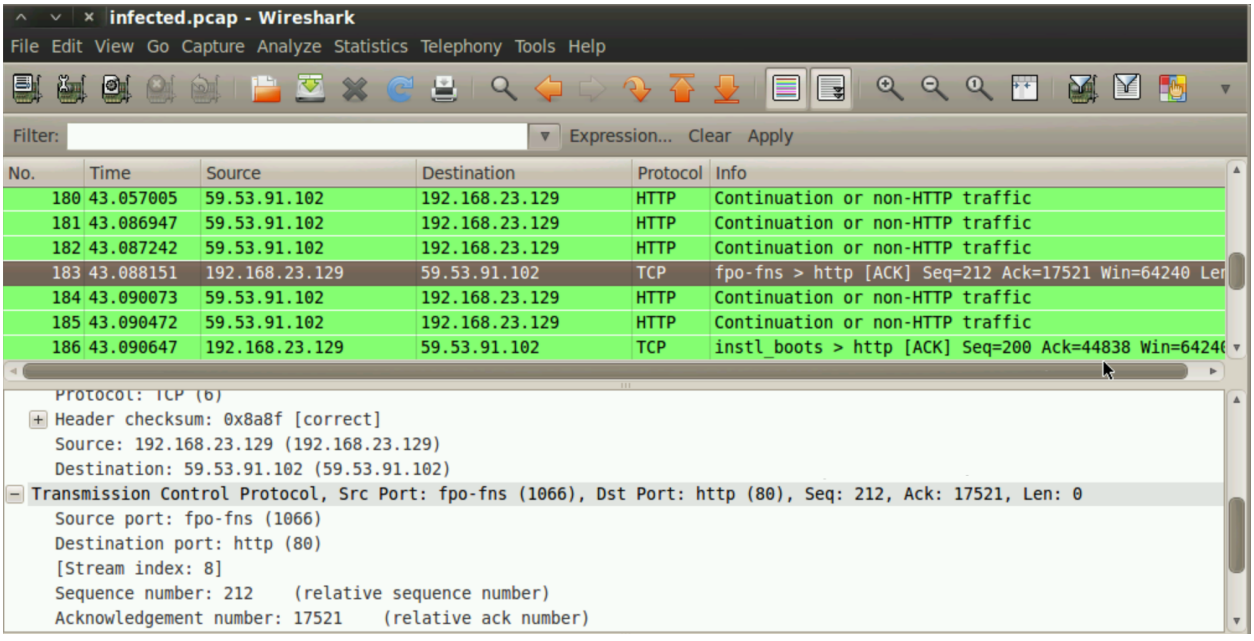
Alert #3
Generator ID: 1
Snort ID: 16669
Revision ID: 5

2.

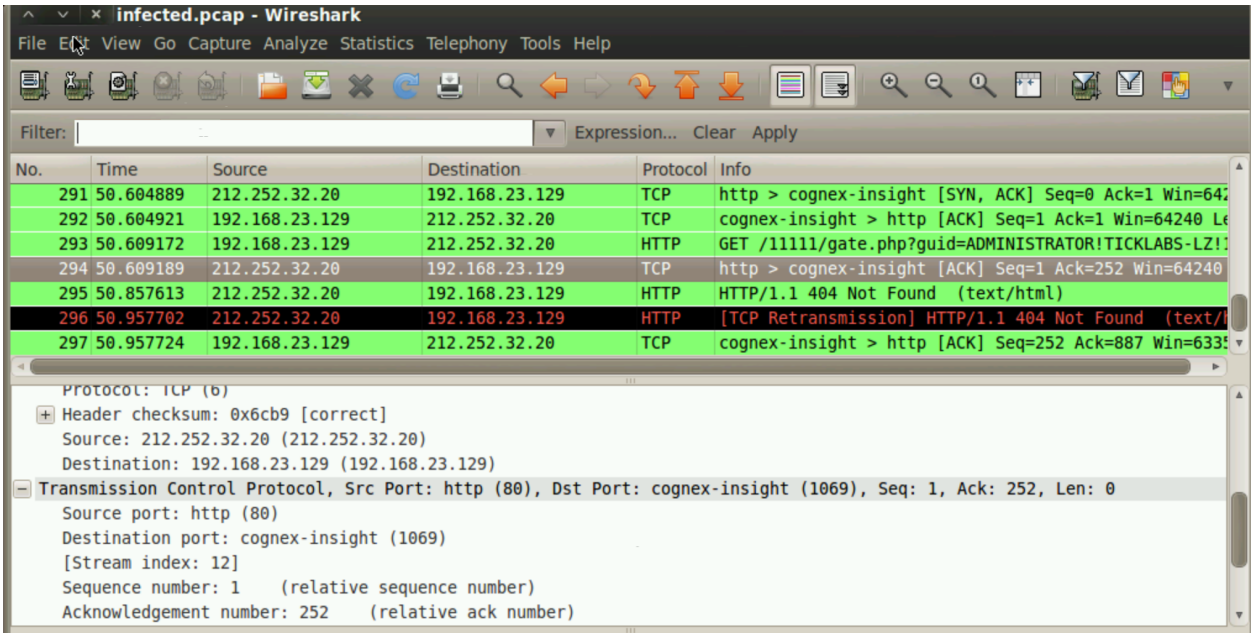
Packet 155:
Source IP: 192.168.23.129
Destination IP: 59.53.91.102
Source Port: 1067
Destination Port: 80
TCP Protocol



Packet 183:
Source IP: 192.168.23.129
Destination IP: 59.53.91.102
Source Port: 1067
Destination Port: 80
TCP Protocol

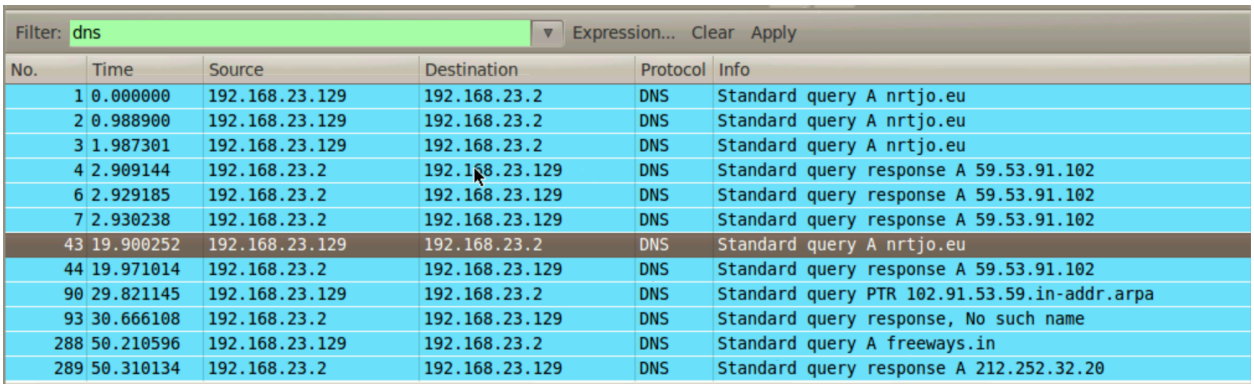


Packet 294:
Source IP: 212.252.32.20
Destination IP: 192.168.23.129
Source Port: 80
Destination Port: 1069
TCP Protocol

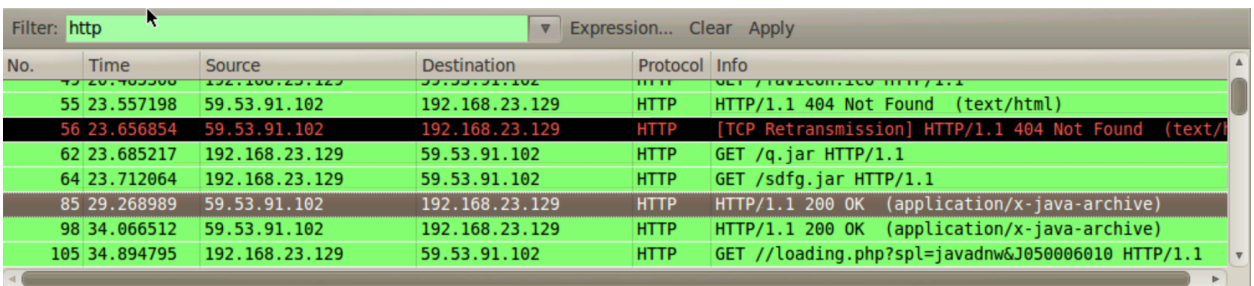


Wireshark Exercises:

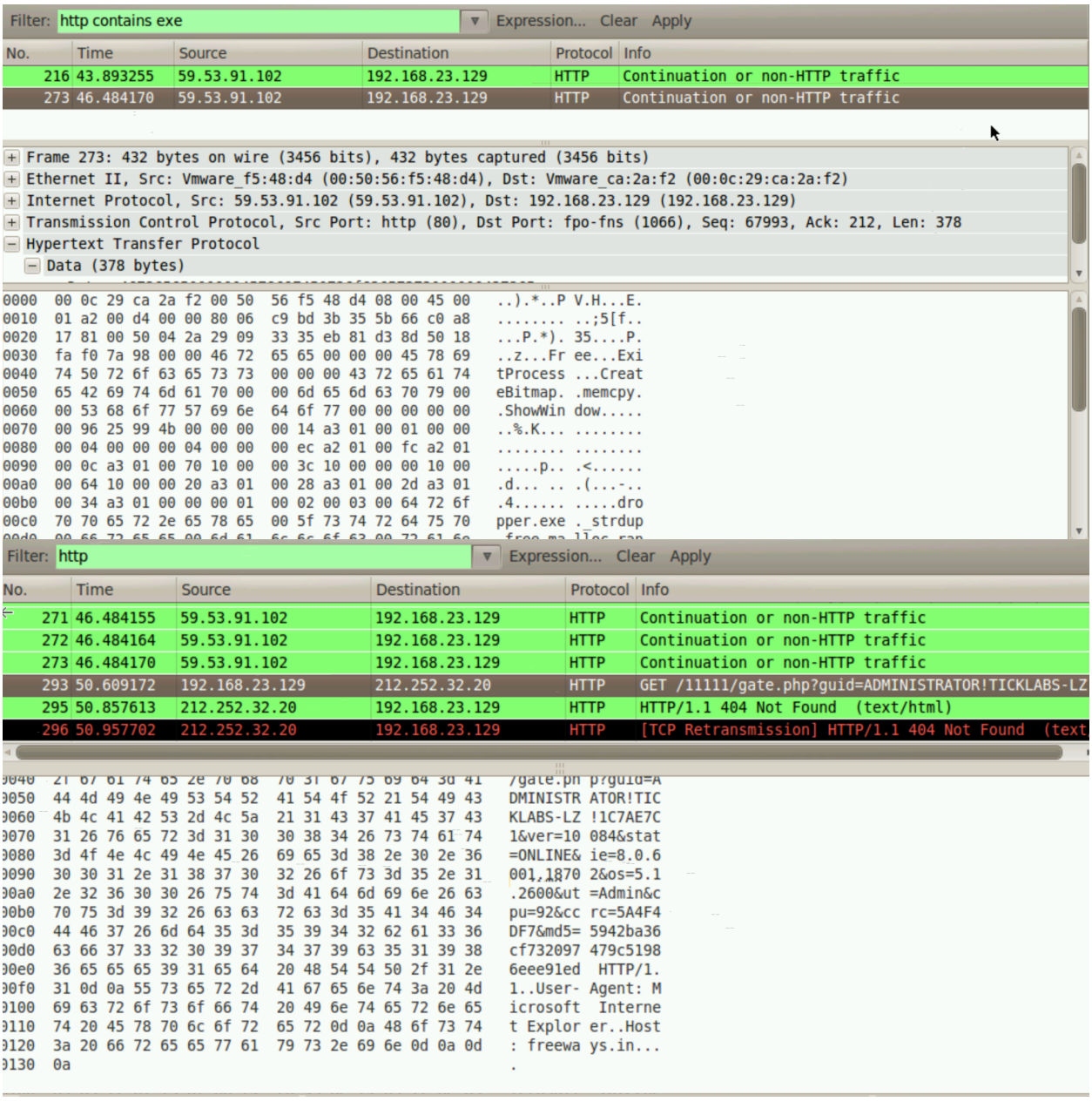
1.



2.
q.jar, sdfg.jar



3. md5hash: 5942ba36cf732097479c51986eee91ed



4. Microsoft Internet Explorer (Image Above)