NetID : iv447
UniID : N17385760

LAB 4 : SNORT

Snort is free and open source network intrusion prevention system (IPS) and network intrusion detection system (NIDS).

Snort can be run in three modes:
1. Sniffer mode: which simply reads the packets off of the network and displays them for you in a continuous stream on the console.
2. Packet logged mode: which logs the packets to disk.
3. Network Intrusion Detection system (NIDS): which performs detection and analysis on network traffic. This is the most complex and configurable mode.

The snort configuration file for this lab is located at : /etc/conf/etc

An example command line for snort used in NIDS mode is shown below:

snort -dev -A test -c -i eth0
(-dev instructs packet to display the packet data as well as headers.)

This configuration file will include the rules configured for each packet to decide if an action should be triggered based on the rule type. The output is stored in the alert file (if you use -A test) which is located at /var/log/snort and also displayed on the screen in the following format:

[**] [116:56:1] (snort_decoder): T/TCP Detected [**]

The first number is the Generator ID; this tells the user what component of Snort generated this alert. For a list of GIDs, please read etc/generators in the Snort source. In this case, we know that this event came from the “decode” (116) component of Snort.

The second number is the Snort ID (sometimes referred to as Signature ID). To learn about preprocessor SIDs, please see https://www.snort.org/rule_docs. Rule-based SIDs are written directly into the rules with the sid option.

The third number is the revision ID. This number is primarily used when writing signatures, as each rendition of the rule should increment this number with the rev option.

There are a number of alert modes which can be used using '–A' to append it to the command. We will be making use of the **fast, full and test.**

The pcap file used for this lab is located at :
/home/student/snort_src/InfectedPcaps/infected.pcap.

To read a pcap file using Snort, we can use one of the following options:
$ sudo snort -r <file>
$ sudo snort --pcap-single= <file>

Wait for the message "Snort exiting" before reading the results.

Answer the following questions using the alert log file provided. Please provide screenshots wherever necessary.

1. List the alerts (from the alerts) and list the corresponding Generator ID, Snort ID and Revision ID of each alert and their significance. If an alert ID repeats multiple times only include it once. (20 points)

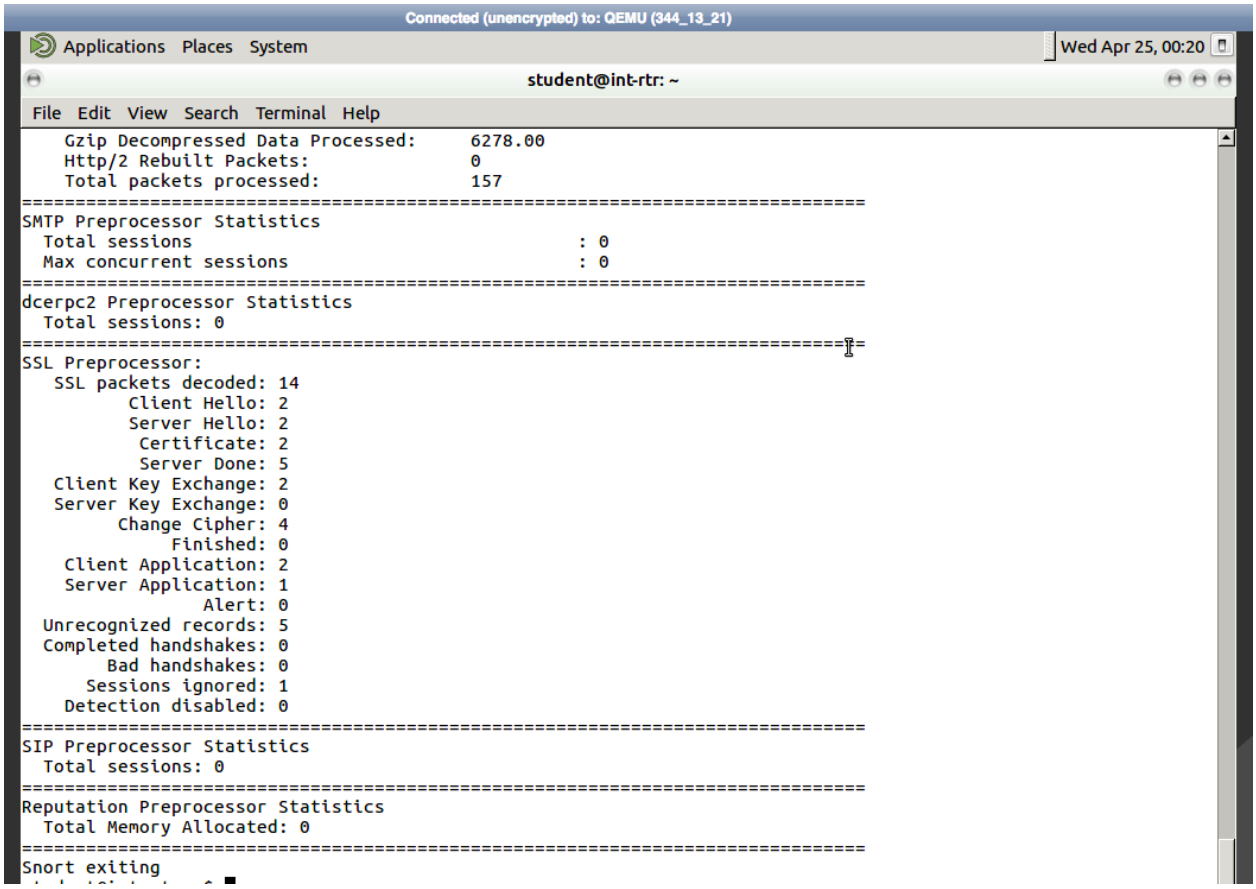
There are three alert modes :

1. **test mode**

Command :

sudo snort -dev -A test -c /etc/snort/etc/snort.conf -r /home/student/snort_src/InfectedPcaps/infected.pcap

Screenshot while snort is running :



Now the alerts are logged in alert file which is located at following location : /var/log/snort

The three alerts logged in the file are :

[1:25042:4]

•Generator ID: 1 -> snort general alert

•Snort ID: 16669 -> This event is generated when an attempt is made to exploit a known vulnerability in jdk.

•Revision ID: 4 -> This denotes the number of times an alert is revised. Here it is 4.

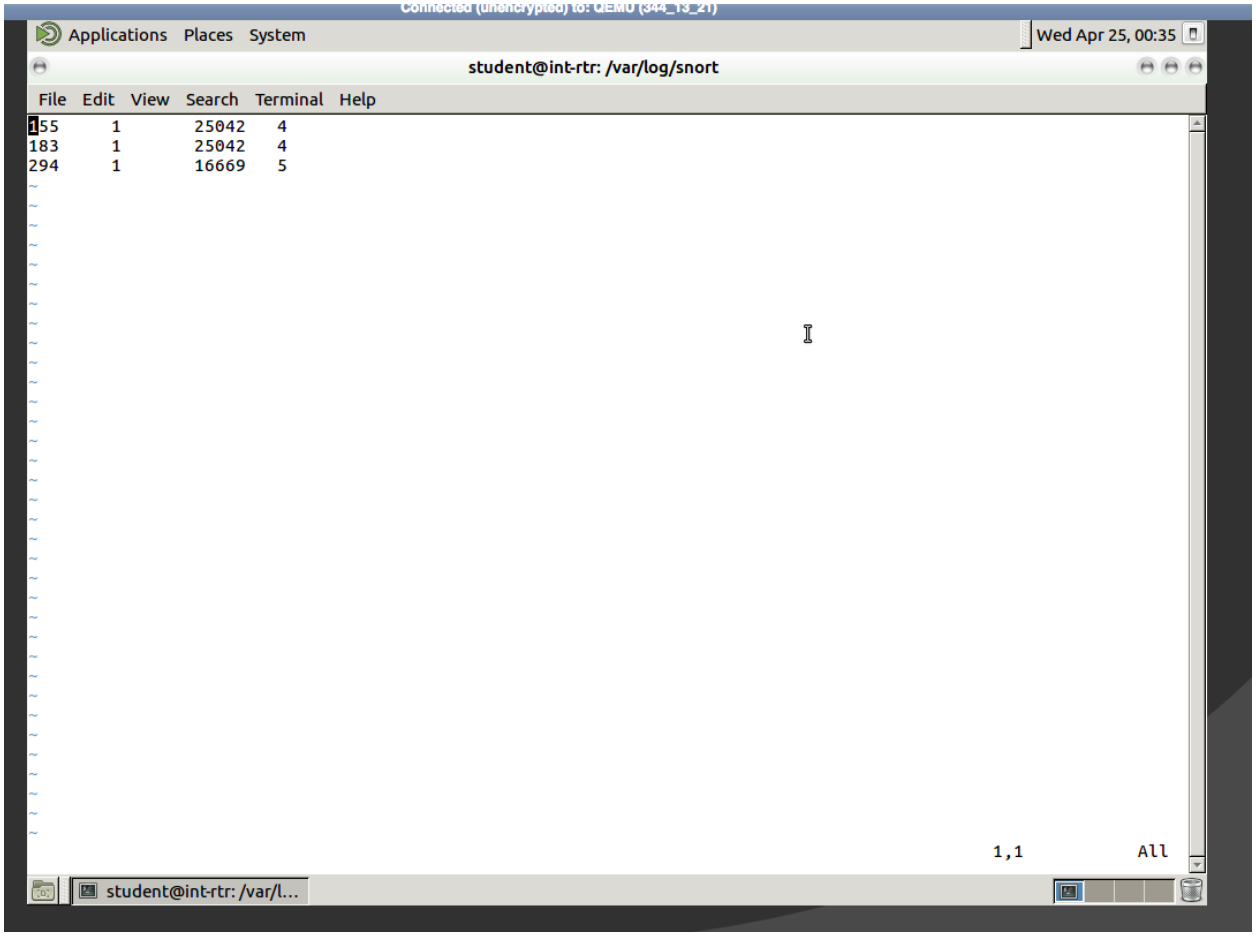
[1:25042:4] Same as above

[1:16669:5]

•Generator ID: 1 -> snort general alert

•Snort ID: 16669 -> This event is generated when a spyware application related activity is detected such as application like "Spyeye bot".

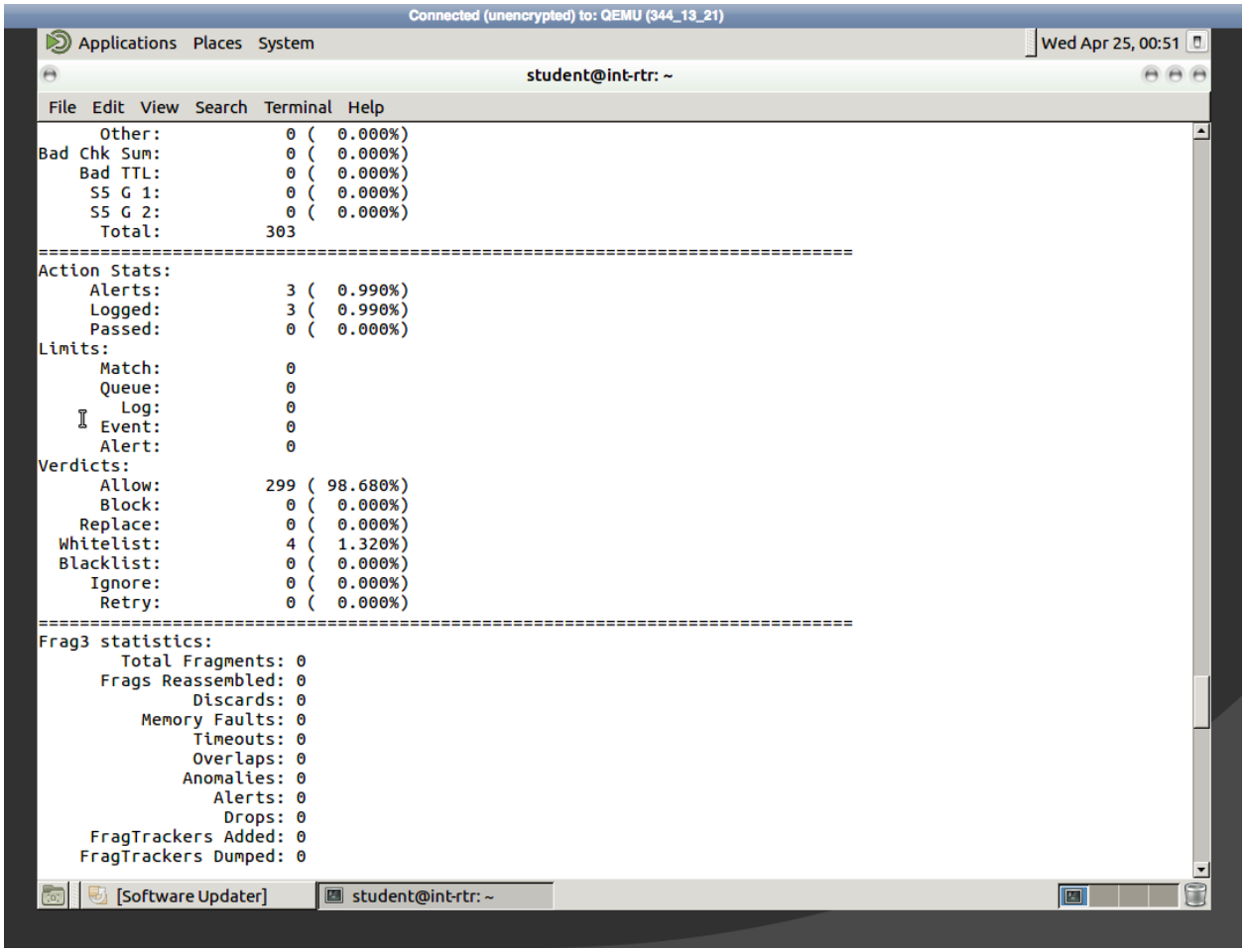
•Revision ID: 5 -> This denotes the number of times an alert is revised. Here it is 5.



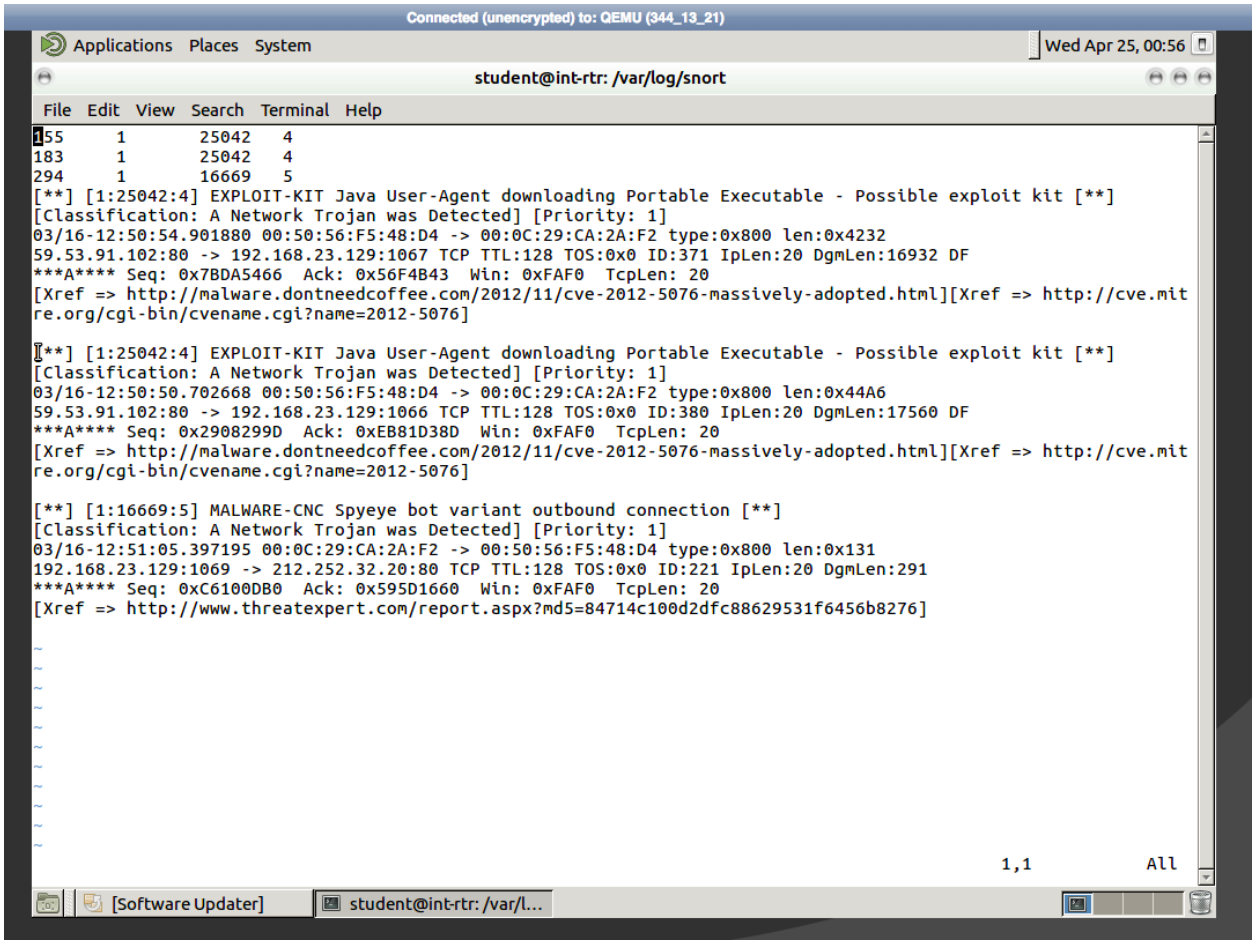
2. **full mode**
***Command*:**

sudo snort -dev -A full -c /etc/snort/etc/snort.conf -r /home/student/snort_src/InfectedPcaps/infected.pcap

When snort is running :



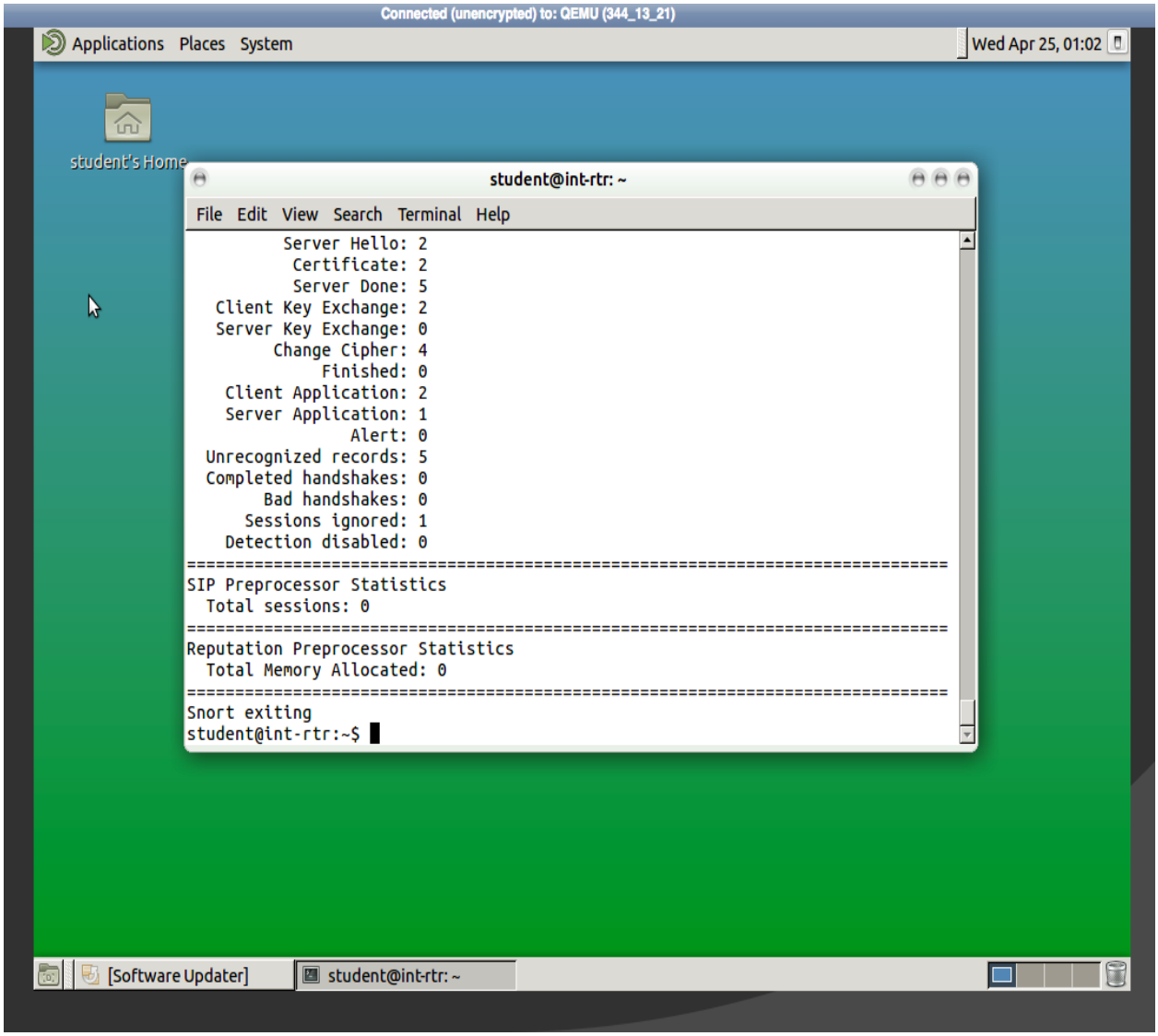
Results are logged in alert file :



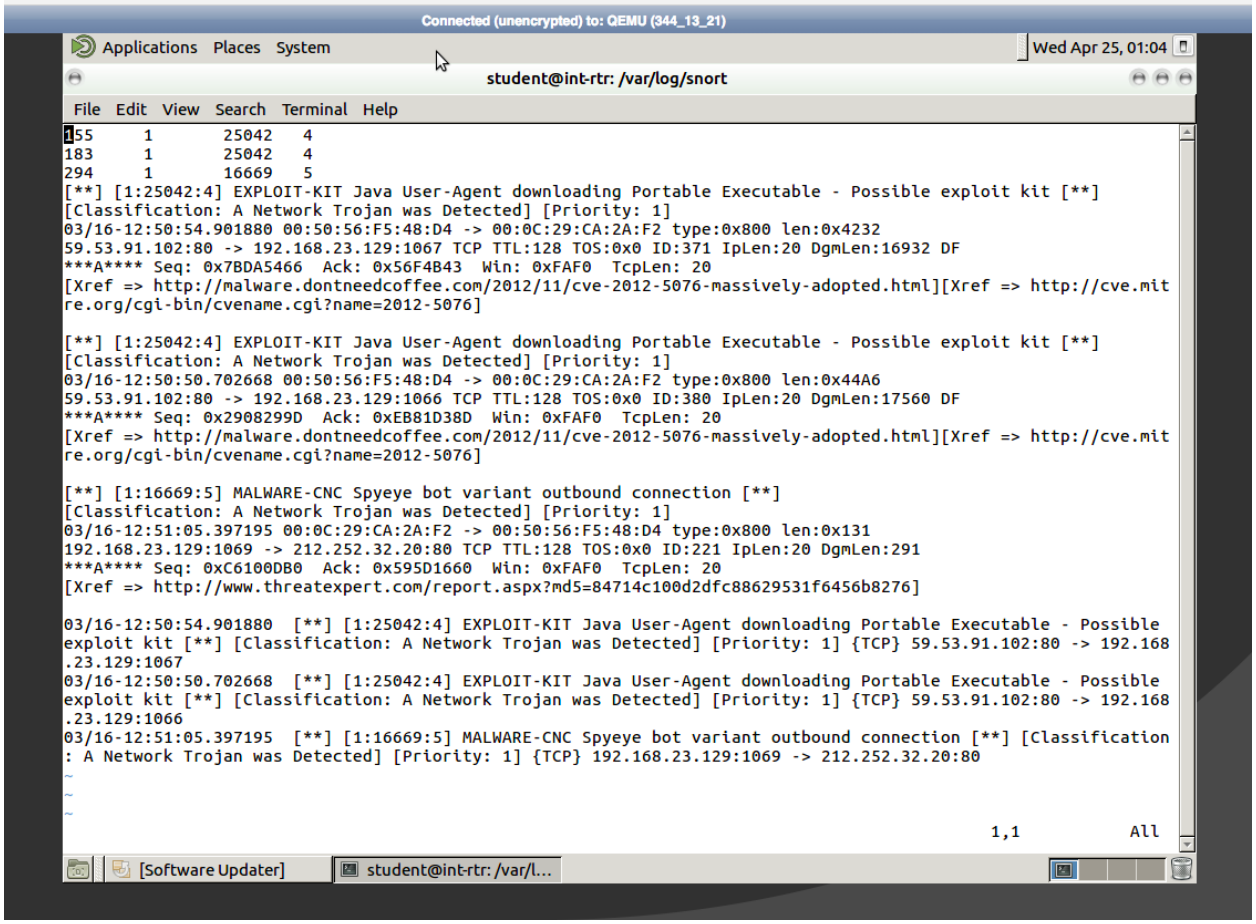
3. **fast mode**
Command **:**

sudo snort -dev -A fast -c /etc/snort/etc/snort.conf -r /home/student/snort_src/InfectedPcaps/infected.pcap

Screenshot while command is running:

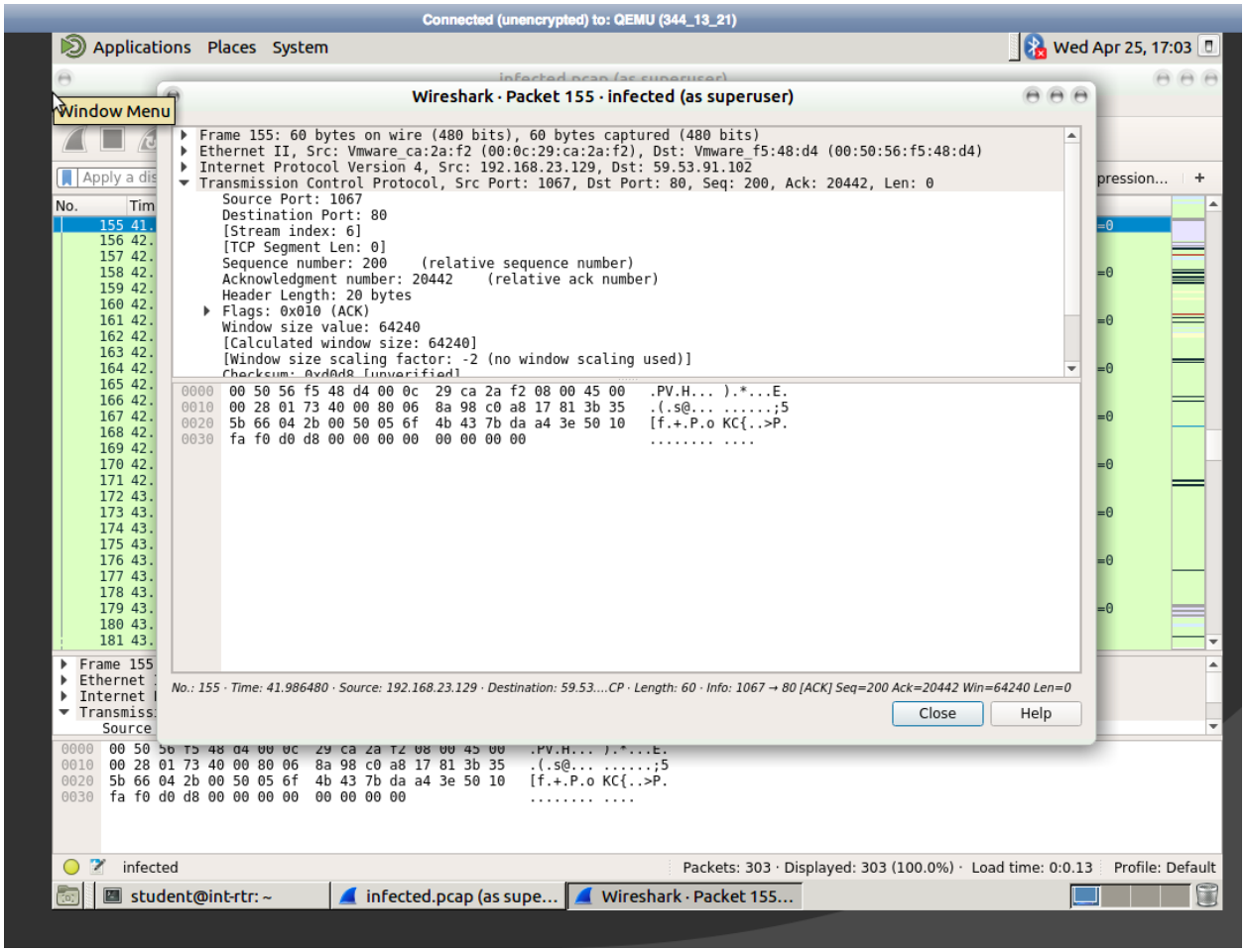


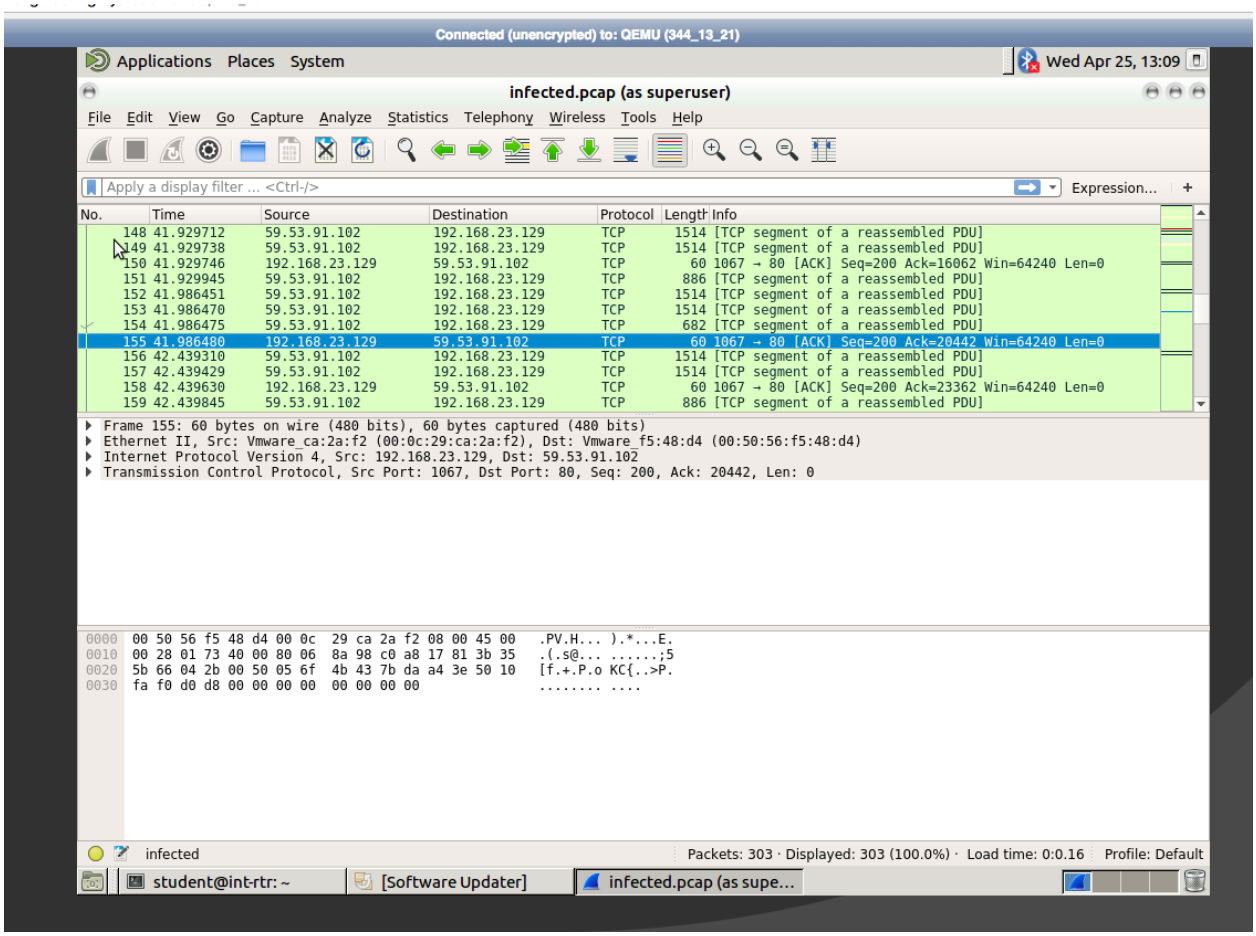
Results are logged in alert file :



2. The alert file contains the output when the file was run using the “–A test” option. This will display the packet numbers of the corresponding packets that triggered alerts. Use Wireshark and locate these packets. List the source and destination IP address, source and destination port numbers and protocol used for each packet. (15 points)

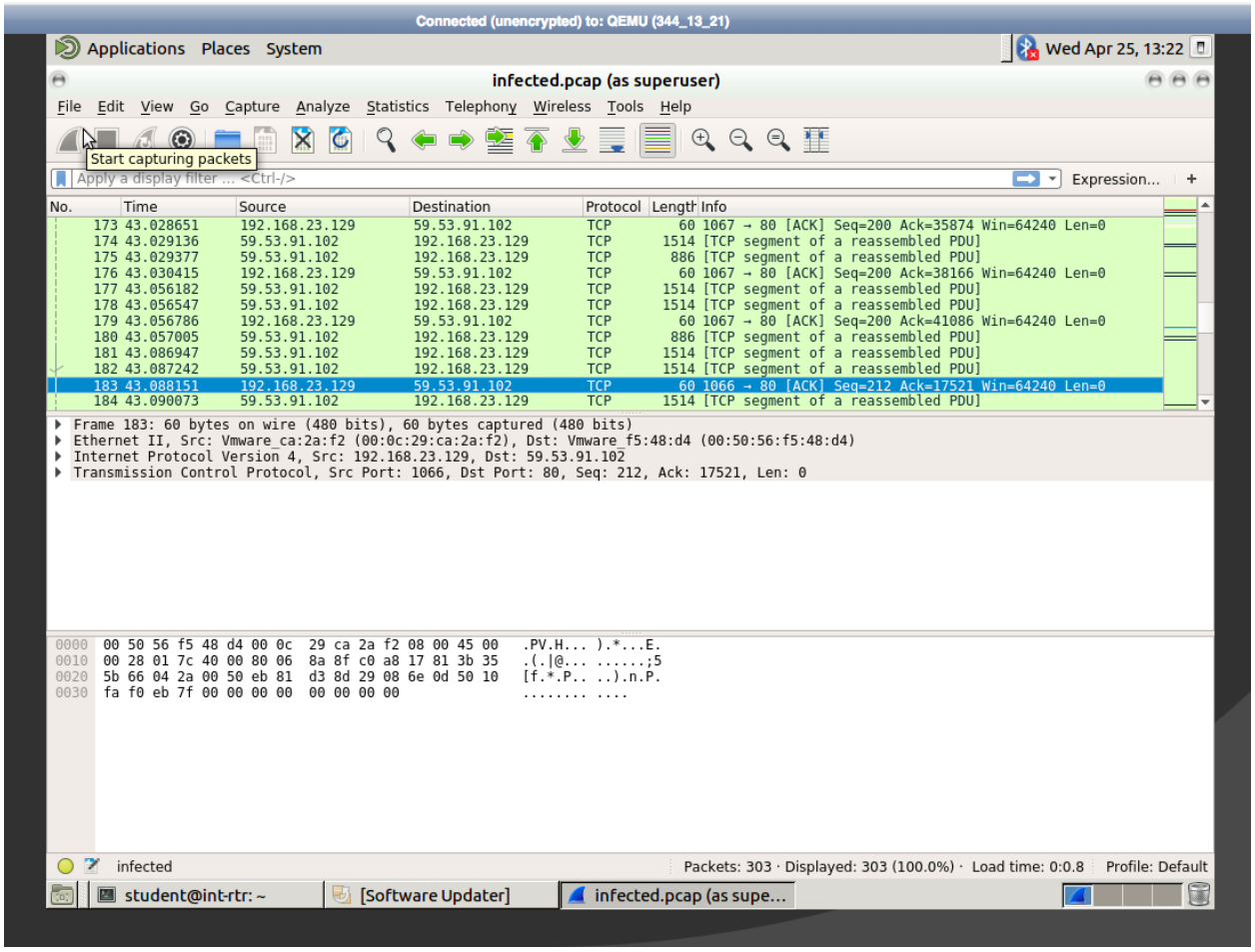
Answer) 1. Packet : 155

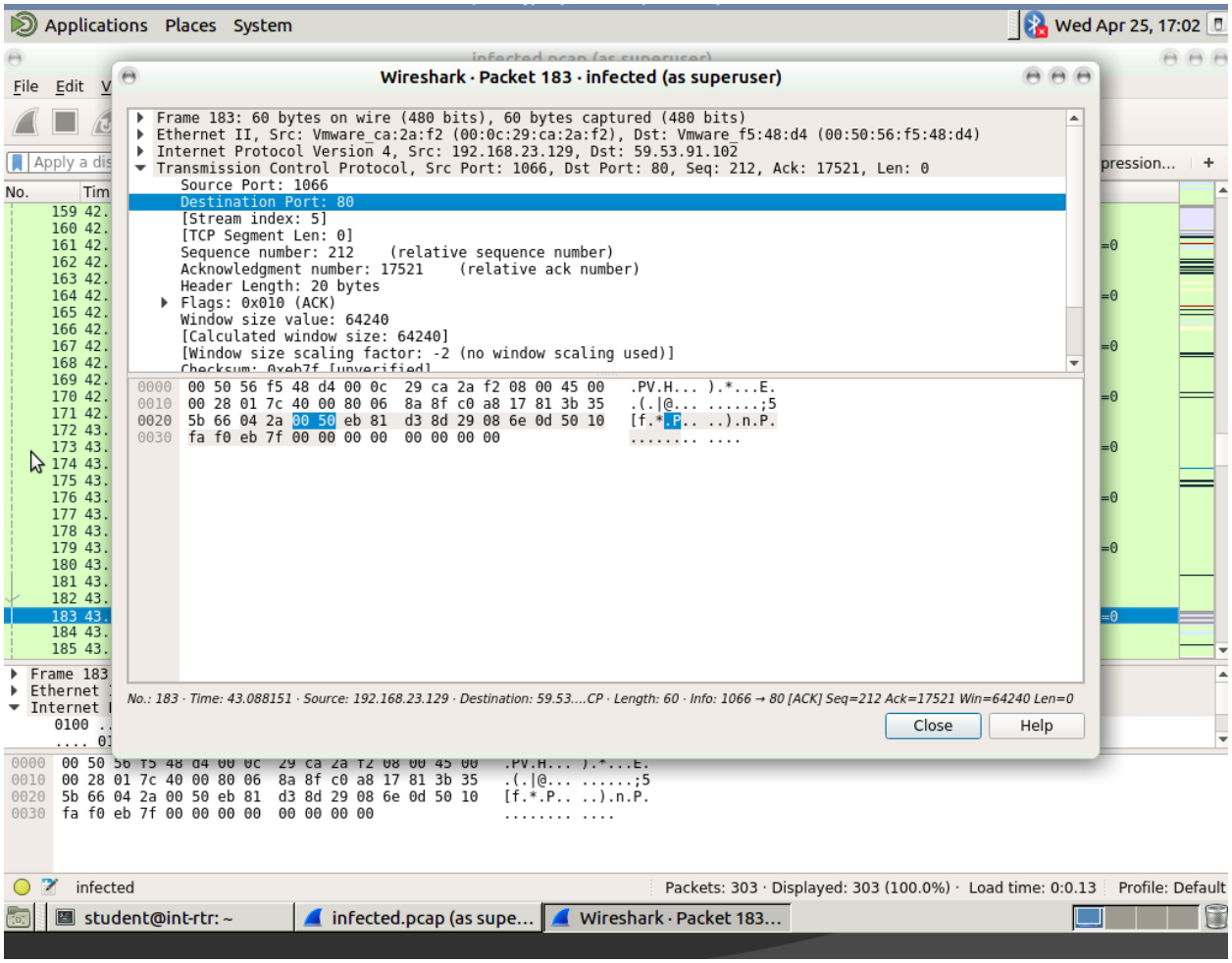

Connected (unencrypted) to: QEMU (344_13_21)
Applications Places System
Wed Apr 25, 17:03
Window Menu
Wireshark · Packet 155 · infected (as superuser)
Frame 155: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Vmware_ca:2a:f2 (00:0c:29:ca:2a:f2), Dst: Vmware_f5:48:d4 (00:50:56:f5:48:d4)
Internet Protocol Version 4, Src: 192.168.23.129, Dst: 59.53.91.102
Transmission Control Protocol, Src Port: 1067, Dst Port: 80, Seq: 200, Ack: 20442, Len: 0
Source Port: 1067
Destination Port: 80
[Stream index: 6]
[TCP Segment Len: 0]
Sequence number: 200 (relative sequence number)
Acknowledgment number: 20442 (relative ack number)
Header Length: 20 bytes
Flags: 0x010 (ACK)
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
0000 00 50 56 f5 48 d4 00 0c 29 ca 2a f2 08 00 45 00 .PV.H...).*...E.
0010 00 28 01 73 40 00 80 06 8a 98 c0 a8 17 81 3b 35 .(.s@... ......;5
0020 5b 66 04 2b 00 50 05 6f 4b 43 7b da a4 3e 50 10 [f.+.P.o KC{..>P.
0030 fa f0 d0 d8 00 00 00 00 00 00 00 00 ....
No.: 155 · Time: 41.986480 · Source: 192.168.23.129 · Destination: 59.53....CP · Length: 60 · Info: 1067 → 80 [ACK] Seq=200 Ack=20442 Win=64240 Len=0
Close
Help
infected
Packets: 303 · Displayed: 303 (100.0%) · Load time: 0:0.13
Profile: Default
student@int-rtr: ~
infected.pcap (as supe...
Wireshark · Packet 155...



Source IP : 192.168.23.129
Destination IP : 59.53.91.102
Source Port : 1067
Destination Port : 80
Protocol : Transmission Control protocol (TCP)

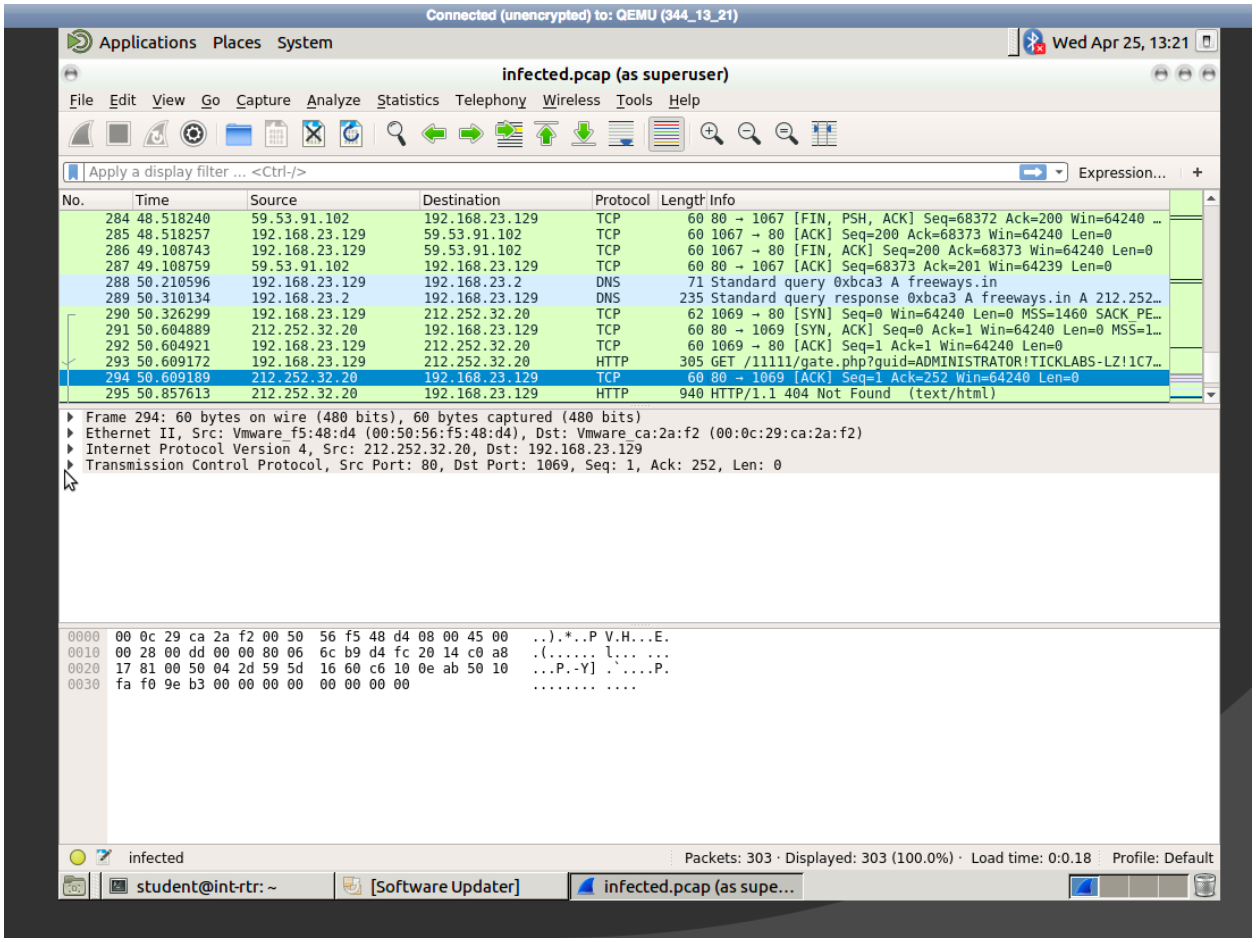
2. Packet : 183

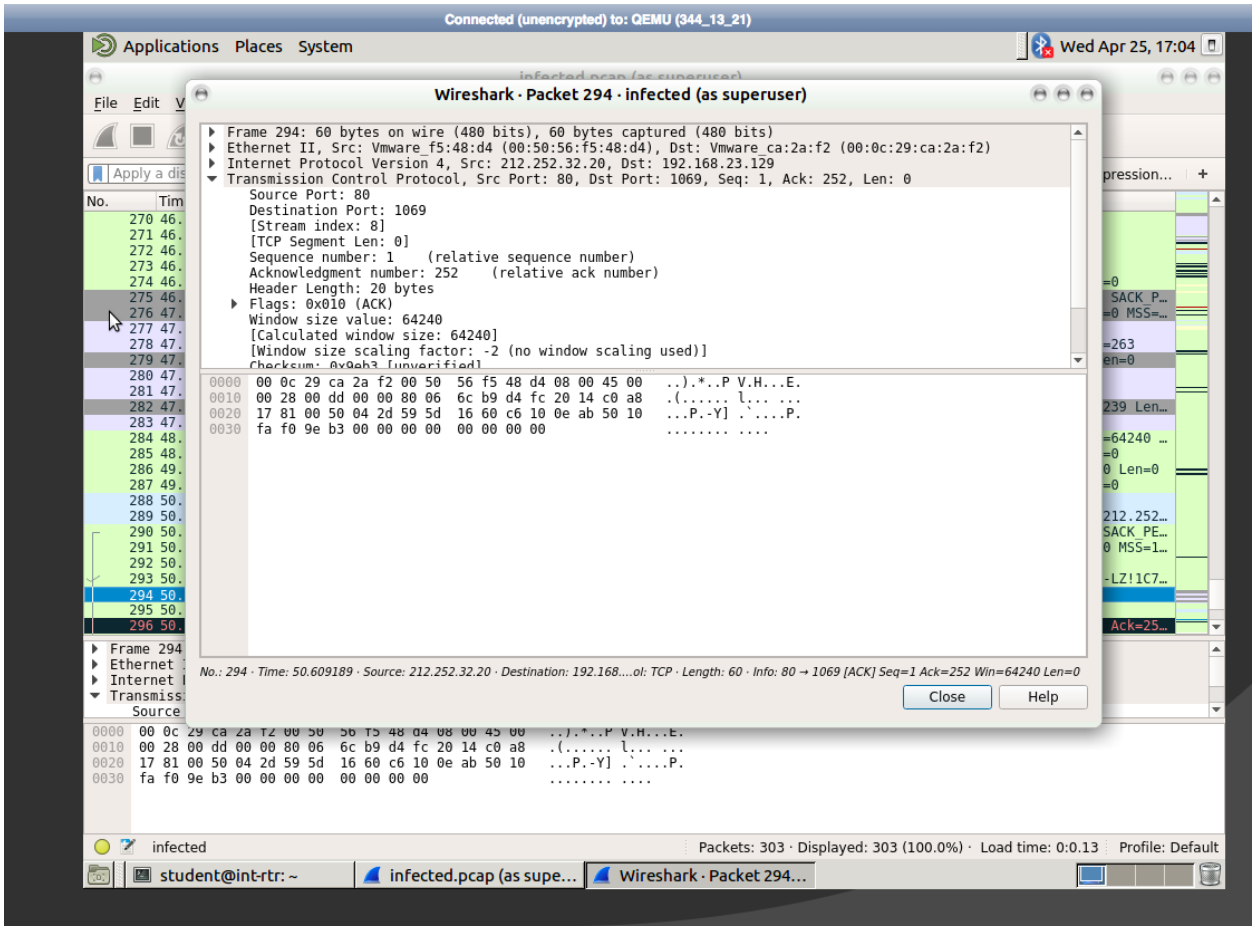

Connected (unencrypted) to: QEMU (344_13_21)
Applications Places System
Wed Apr 25, 13:22
infected.pcap (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Start capturing packets
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
173 43.028651 192.168.23.129 59.53.91.102 TCP 60 1067 → 80 [ACK] Seq=200 Ack=35874 Win=64240 Len=0
174 43.029136 59.53.91.102 192.168.23.129 TCP 1514 [TCP segment of a reassembled PDU]
175 43.029377 59.53.91.102 192.168.23.129 TCP 886 [TCP segment of a reassembled PDU]
176 43.030415 192.168.23.129 59.53.91.102 TCP 60 1067 → 80 [ACK] Seq=200 Ack=38166 Win=64240 Len=0
177 43.056182 59.53.91.102 192.168.23.129 TCP 1514 [TCP segment of a reassembled PDU]
178 43.056547 59.53.91.102 192.168.23.129 TCP 1514 [TCP segment of a reassembled PDU]
179 43.056786 192.168.23.129 59.53.91.102 TCP 60 1067 → 80 [ACK] Seq=200 Ack=41086 Win=64240 Len=0
180 43.057005 59.53.91.102 192.168.23.129 TCP 886 [TCP segment of a reassembled PDU]
181 43.086947 59.53.91.102 192.168.23.129 TCP 1514 [TCP segment of a reassembled PDU]
182 43.087242 59.53.91.102 192.168.23.129 TCP 1514 [TCP segment of a reassembled PDU]
183 43.088151 192.168.23.129 59.53.91.102 TCP 60 1066 → 80 [ACK] Seq=212 Ack=17521 Win=64240 Len=0
184 43.090073 59.53.91.102 192.168.23.129 TCP 1514 [TCP segment of a reassembled PDU]
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, Dst: 59.53.91.102
Transmission Control Protocol, Src Port: 1066, Dst Port: 80, Seq: 212, Ack: 17521, Len: 0
0000 00 50 56 f5 48 d4 00 0c 29 ca 2a f2 08 00 45 00 .PV.H...).*...E.
0010 00 28 01 7c 40 00 80 06 8a 8f c0 a8 17 81 3b 35 .(.|@... ......;5
0020 5b 66 04 2a 00 50 eb 81 d3 8d 29 08 6e 0d 50 10 [f.*.P.. ..).n.P.
0030 fa f0 eb 7f 00 00 00 00 00 00 00 00 ....
infected
Packets: 303 · Displayed: 303 (100.0%) · Load time: 0:0.8
Profile: Default
student@int-rtr: ~
[Software Updater]
infected.pcap (as supe...



Source IP : 192.168.23.129
Destination IP : 59.53.91.102
Source Port : 1066
Destination Port : 80
Protocol : Transmission Control protocol (TCP)

3. Packet : 294


Connected (unencrypted) to: QEMU (344_13_21)
Applications Places System
Wed Apr 25, 13:21
infected.pcap (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
284 48.518240 59.53.91.102 192.168.23.129 TCP 60 80 → 1067 [FIN, PSH, ACK] Seq=68372 Ack=200 Win=64240 …
285 48.518257 192.168.23.129 59.53.91.102 TCP 60 1067 → 80 [ACK] Seq=200 Ack=68373 Win=64240 Len=0
286 49.108743 192.168.23.129 59.53.91.102 TCP 60 1067 → 80 [FIN, ACK] Seq=200 Ack=68373 Win=64240 Len=0
287 49.108759 59.53.91.102 192.168.23.129 TCP 60 80 → 1067 [ACK] Seq=68373 Ack=201 Win=64239 Len=0
288 50.210596 192.168.23.129 192.168.23.2 DNS 71 Standard query 0xbca3 A freeways.in
289 50.310134 192.168.23.2 192.168.23.129 DNS 235 Standard query response 0xbca3 A freeways.in A 212.252…
290 50.326299 192.168.23.129 212.252.32.20 TCP 62 1069 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE…
291 50.604889 212.252.32.20 192.168.23.129 TCP 60 80 → 1069 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1…
292 50.604921 192.168.23.129 212.252.32.20 TCP 60 1069 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
293 50.609172 192.168.23.129 212.252.32.20 HTTP 305 GET /11111/gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7…
294 50.609189 212.252.32.20 192.168.23.129 TCP 60 80 → 1069 [ACK] Seq=1 Ack=252 Win=64240 Len=0
295 50.857613 212.252.32.20 192.168.23.129 HTTP 940 HTTP/1.1 404 Not Found (text/html)
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, Dst: 192.168.23.129
Transmission Control Protocol, Src Port: 80, Dst Port: 1069, Seq: 1, Ack: 252, Len: 0
0000 00 0c 29 ca 2a f2 00 50 56 f5 48 d4 08 00 45 00 ..).*..P V.H...E.
0010 00 28 00 dd 00 00 80 06 6c b9 d4 fc 20 14 c0 a8 .(...... l... ...
0020 17 81 00 50 04 2d 59 5d 16 60 c6 10 0e ab 50 10 ...P.-Y] .`....P.
0030 fa f0 9e b3 00 00 00 00 00 00 00 00 ....
infected
Packets: 303 · Displayed: 303 (100.0%) · Load time: 0:0.18
Profile: Default
student@int-rtr: ~
[Software Updater]
infected.pcap (as supe…



Source IP : 212.252.32.20
Destination IP : 192.168.23.129
Source Port : 80
Destination Port : 1069
Protocol : Transmission Control protocol (TCP)

3. Look up the meaning of the alerts and explain which alert you think is actually the one that identifies a likely malware installation attempt. [15 points]

Answer : The alert which identifies malware installation is :

[1:25042:4]

[Classification: A Network Trojan was Detected] [Priority: 1]

03/16-12:50:50.702668 00:50:56:F5:48:D4 -> 00:0C:29:CA:2A:F2 type:0x800 len:0x44A6

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-adopted.html][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-5076]

Here we can see that some portable executable is being downloaded.

4. There were likely many likely false positive alerts that repeat many times and consumed time in your analysis. Describe your recommendation for reducing these false positives so that they would not consume analysis time in the future. Also include any potential dangers in your proposed method. [10 points]

Answer) Network based intrusion detection systems (NIDS) perform in-depth packet analysis in order to enumerate attackers who are attempting to expose network and service vulnerabilities. A false positive state is when the NIDS identifies an activity as an attack but the activity in actual is benign (it's acceptable behavior). We can implement certain methods to reduce these false positives so that NIDS will not consume analysis time in future such as :

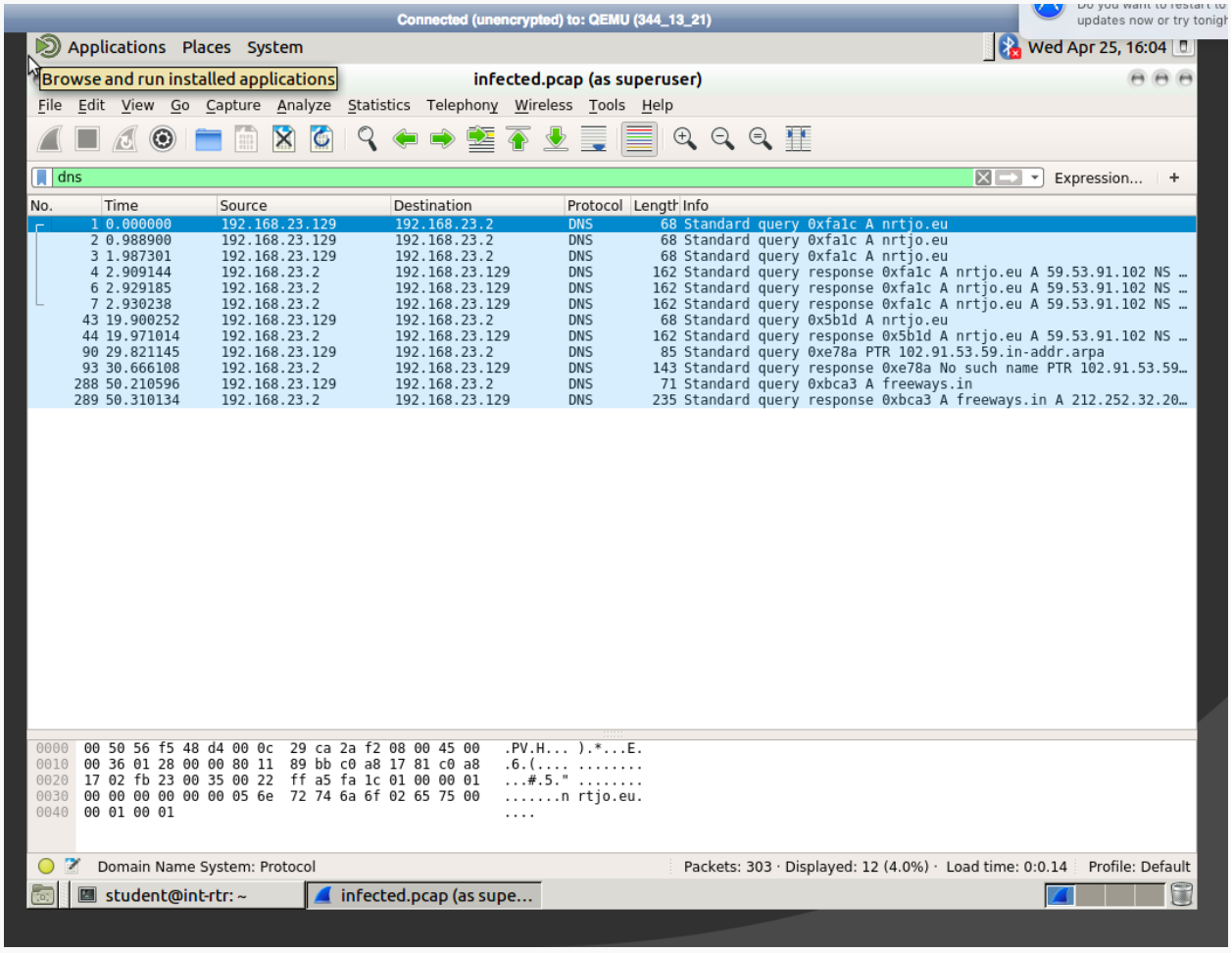
For properly analysing false positive alarms reduction strategies we need to quantify risk and role of NIDS in this risk reduction. There are different formulas to quantify risk. Potential dangers that this method might face is that these formula implemented might not be full proof, mathematics behind these is dubious. Other methods can be placing NIDS behind firewall, Tuning NIDS signature, Network Analysis (this is going to be a laborious task) etc.

Wireshark Exercises :

5. Use a filter and list all the DNS queries and the resolved IP addresses. Include the filter in the lab write up. (15 points)

We can use dns filter to list all the DNS queries and the resolved IP addresses.

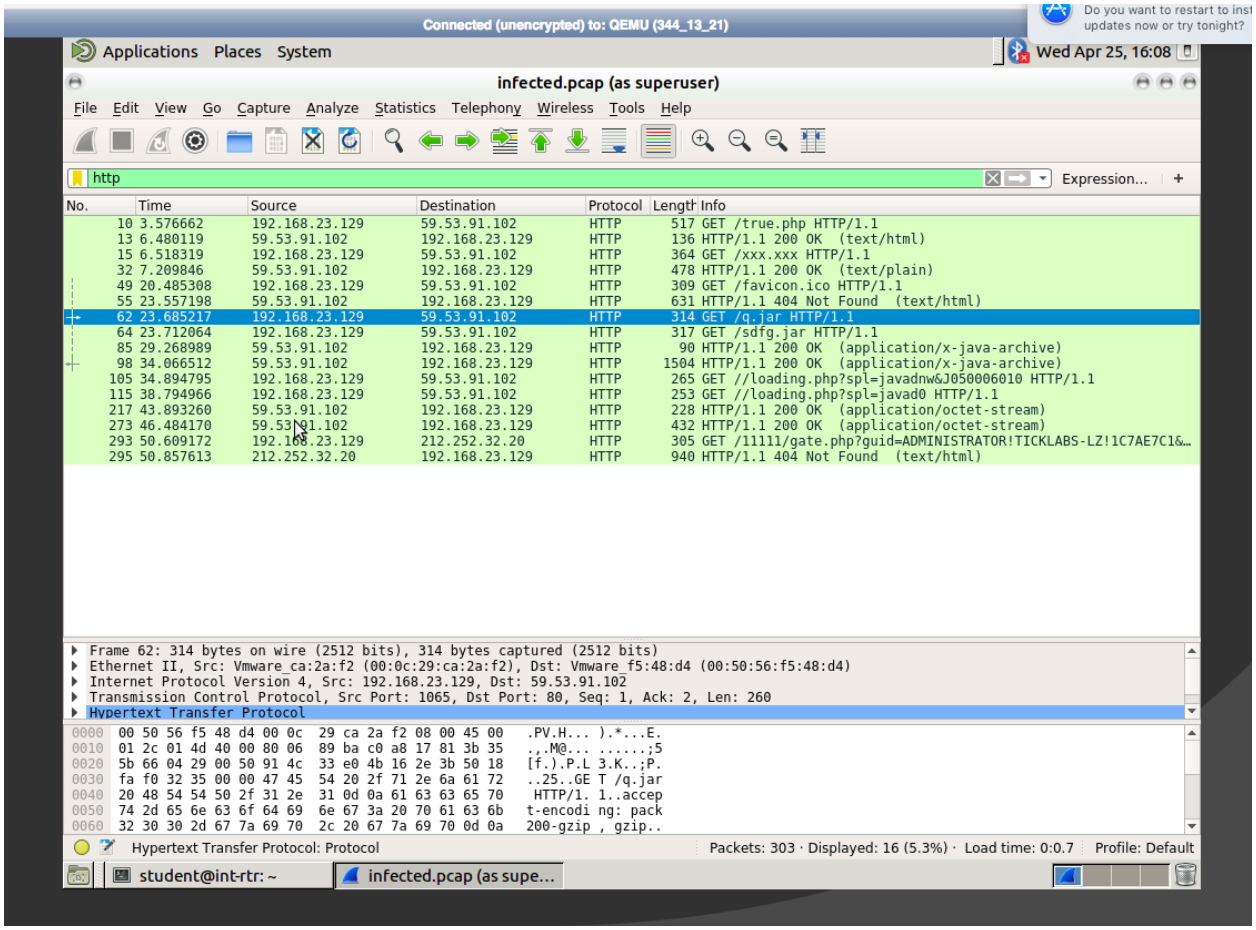
dns



6. There were HTTP sessions established to download 2 java applets. What were the names of the two .jar files that implemented these applets? (10 points)

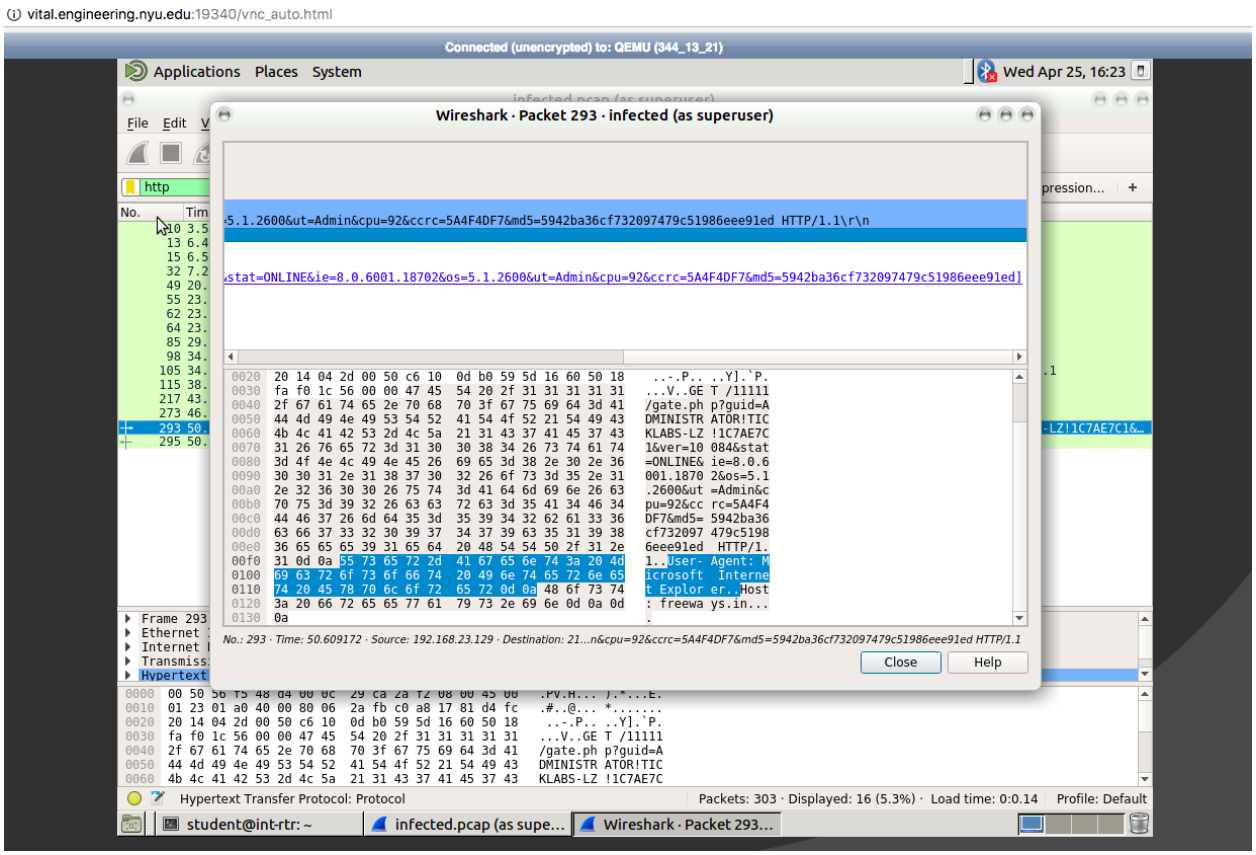
The names of the two .jar files that implemented these applets were :

1. q.jar
2. sdfg.jar



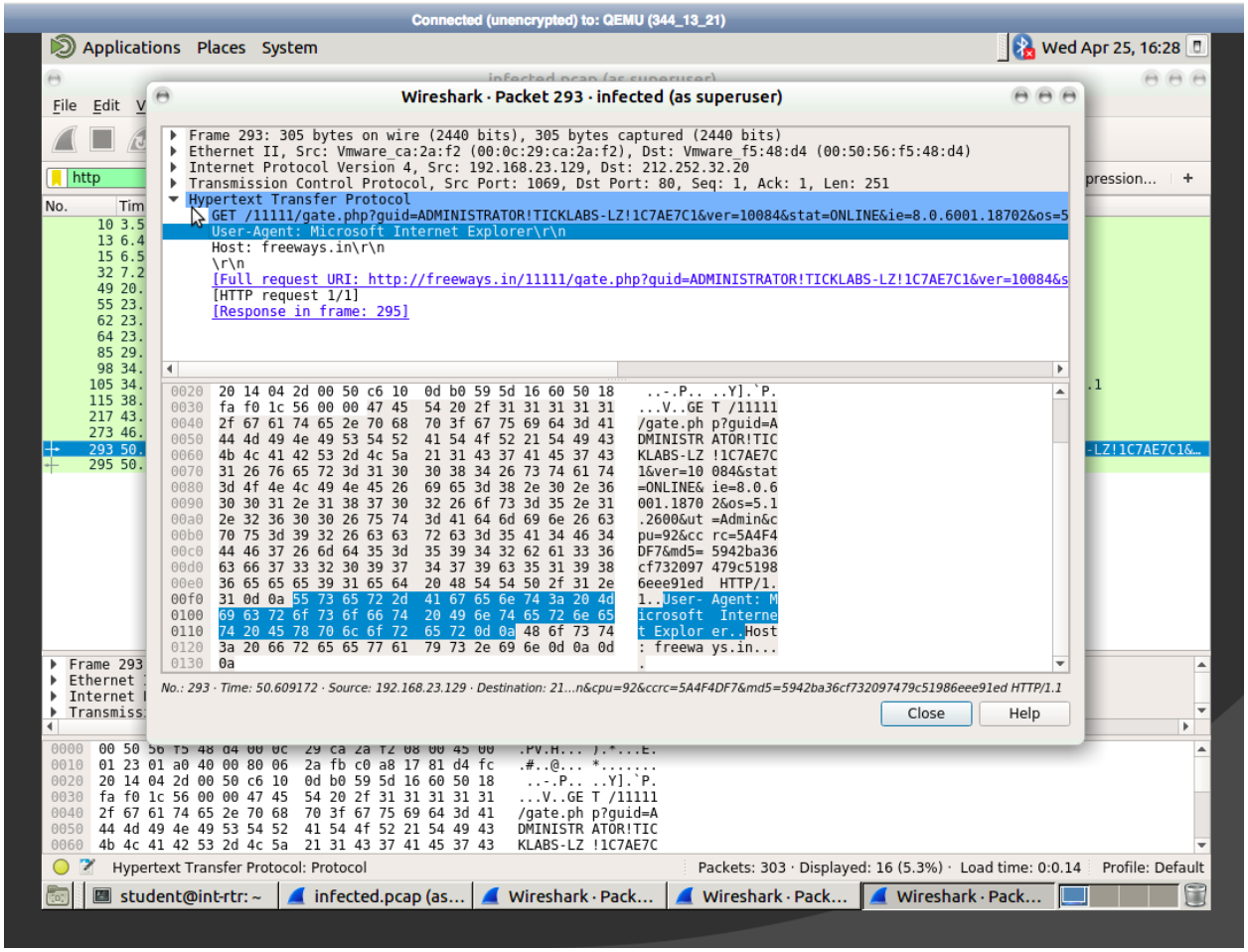
7. As part of the infection, a malicious executable file was downloaded onto the client's computer. What was the file's MD5 hash? Hint: It ends on "91ed". (10 points)

Answer) MD5 hash of the file was : 5942ba36cf732097479c51986eee91ed



8. Which browser is being used by the client? (5 points)

Browser being used by the client is : Microsoft Internet Explorer


Connected (unencrypted) to: QEMU (344_13_21)
Applications Places System
Wed Apr 25, 16:28
Wireshark · Packet 293 · infected (as superuser)
Frame 293: 305 bytes on wire (2440 bits), 305 bytes captured (2440 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, Dst: 212.252.32.20
Transmission Control Protocol, Src Port: 1069, Dst Port: 80, Seq: 1, Ack: 1, Len: 251
Hypertext Transfer Protocol
GET /11111/gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7AE7C1&ver=10084&stat=ONLINE&ie=8.0.6001.18702&os=5
User-Agent: Microsoft Internet Explorer\r\n
Host: freeways.in\r\n
\r\n
[Full request URI: http://freeways.in/11111/gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7AE7C1&ver=10084&s
[HTTP request 1/1]
[Response in frame: 295]
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
00e0 36 65 65 65 39 31 65 64 20 48 54 54 50 2f 31 2e 6eee91ed HTTP/1.
00f0 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 1..User- Agent: M
0100 69 63 72 6f 73 6f 66 74 20 49 6e 74 65 72 6e 65 icrosoft Interne
0110 74 20 45 78 70 6c 6f 72 65 72 0d 0a 48 6f 73 74 t Explor er..Host
0120 3a 20 66 72 65 65 77 61 79 73 2e 69 6e 0d 0a 0d : freewa ys.in...
0130 0a .
No.: 293 · Time: 50.609172 · Source: 192.168.23.129 · Destination: 21...n&cpu=92&ccrc=5A4F4DF7&md5=5942ba36cf732097479c51986eee91ed HTTP/1.1
Close
Help
Hypertext Transfer Protocol: Protocol
Packets: 303 · Displayed: 16 (5.3%) · Load time: 0:0.14
Profile: Default
student@int-rtr: ~
infected.pcap (as...
Wireshark · Pack...
Wireshark · Pack...
Wireshark · Pack...