Introduction

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. In this lab, you will use the NIDS mode.

Lab

1. **List the alerts (from the alerts) and list the corresponding Generator ID, Snort ID and Revision ID of each alert and their significance. (20 points)**
   the command for test mode is:
   sudo snort -dev -A test -c /etc/snort/etc/snort.conf -r /home/student/snort_src/ InfectedPcaps/infected.pcap

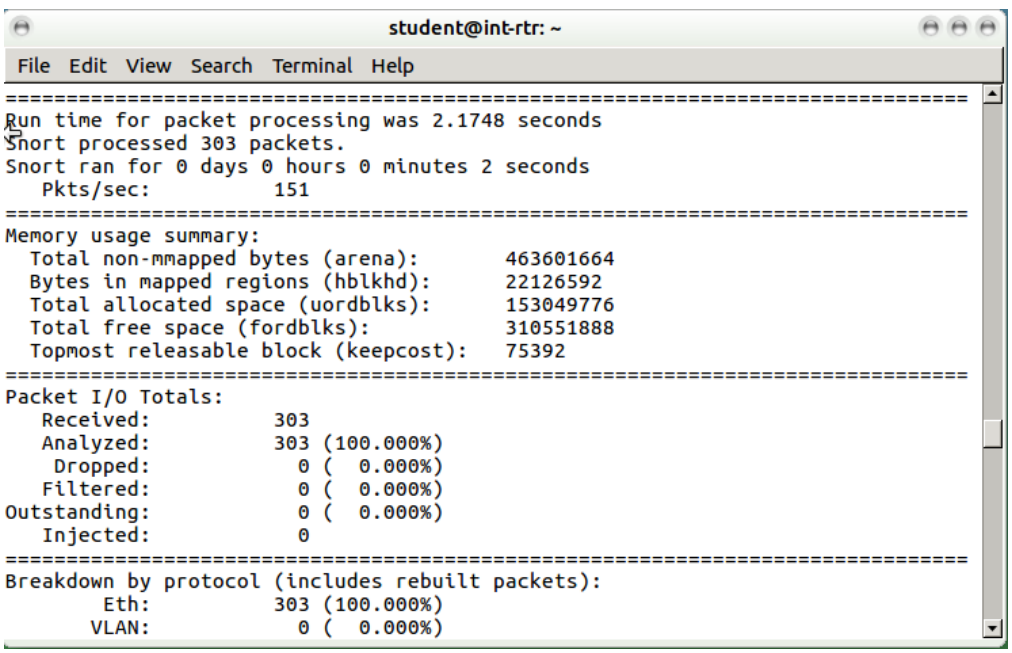

Figure 1: test mode snort and pcap

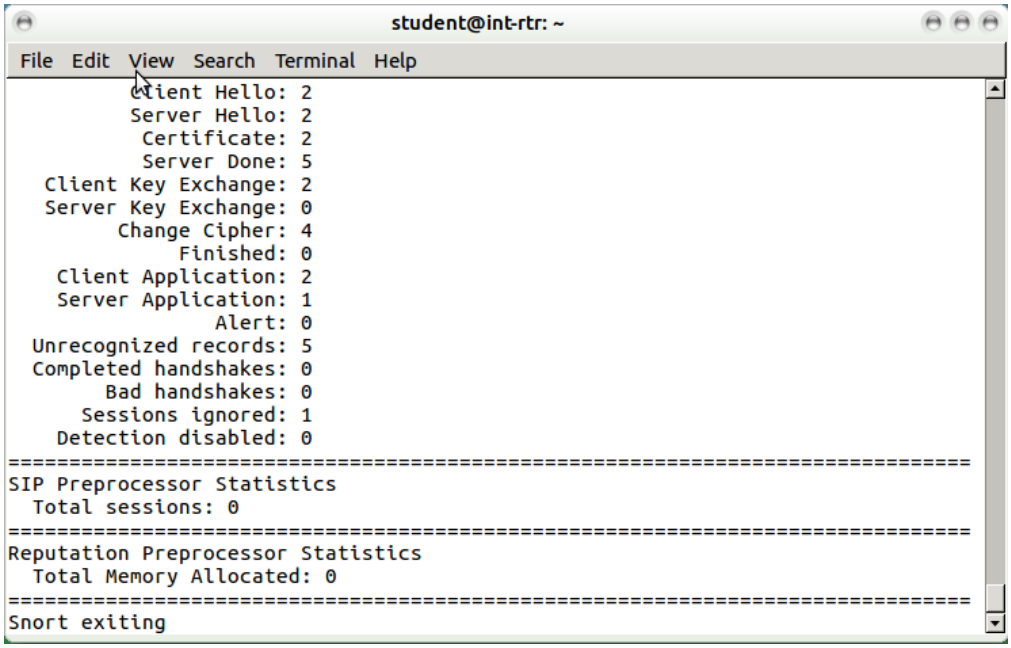

Figure 2: test mode snort and pcap

After test mode, we can vim the alert file, and figure out the three alerts:

(a) the first two
[1 : 25042 : 4]
Generator ID: 1 → snort general alert
Snort ID: 16669 → will be 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.

(b) the last one
[1 : 16669 : 5]
Generator ID: 1 → snort general alert
Snort ID: 16669 → will be generated when a spyware application related activity is detected.
Revision ID: 5 → This denotes the number of times an alert is revised.

Also, if we use the full mode for the snort, we will get the Figure 4, with more details.

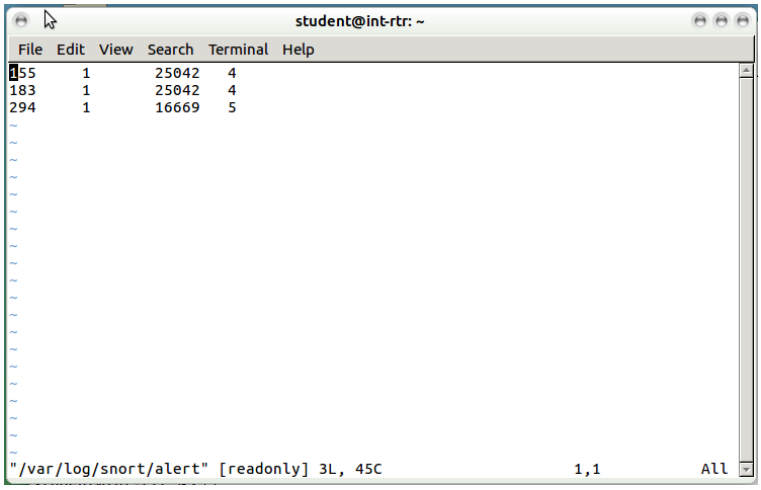

Figure 3: alert after test mode

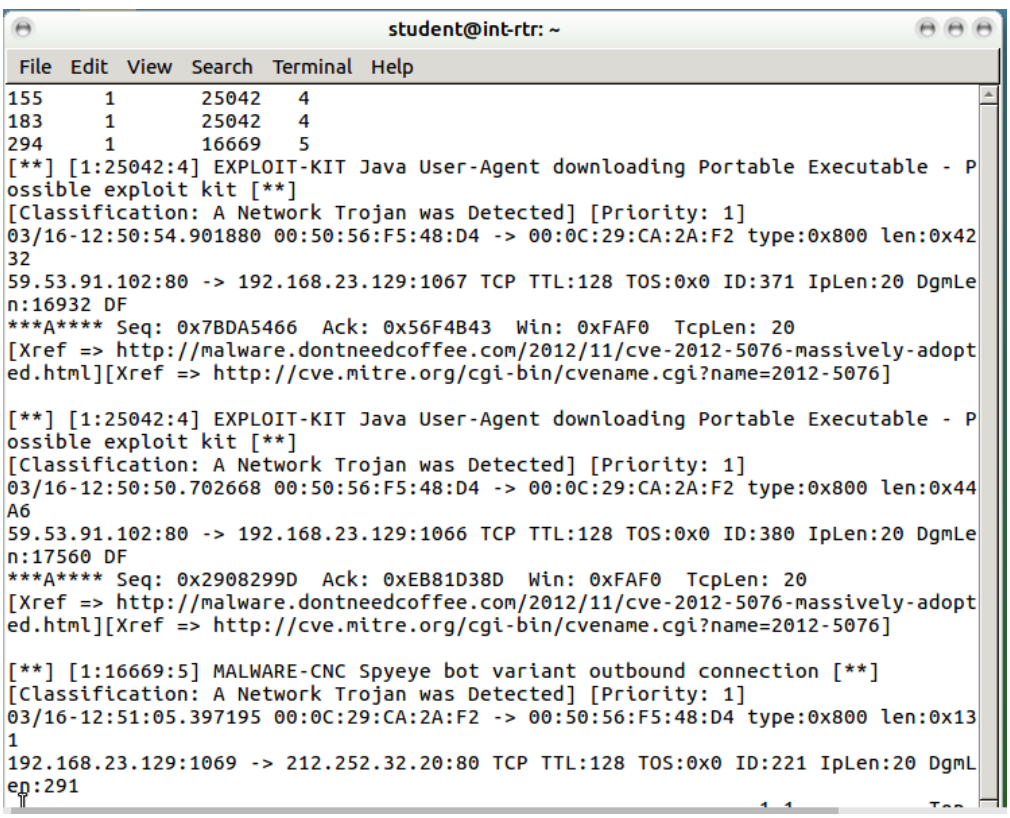

Figure 4: alert after full mode

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)**

   (a) packet 155
   source IP address: 192.168.23.129
   destination IP address: 59.53.91.102
   source port numbers: 1067
   destination port numbers: 80
   protocol: TCP

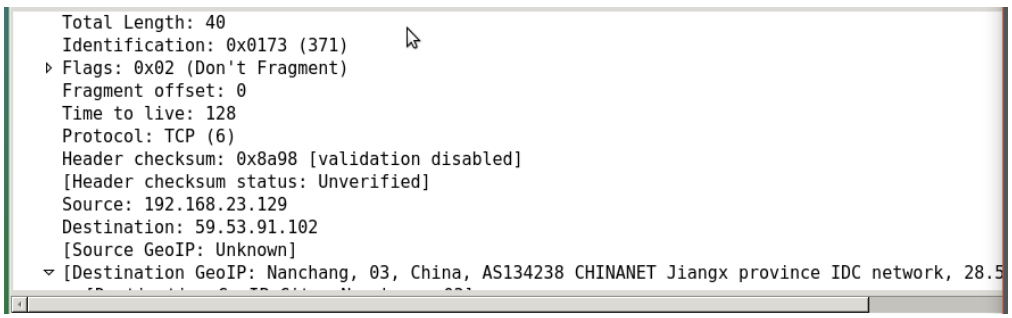

Figure 5: packet 155

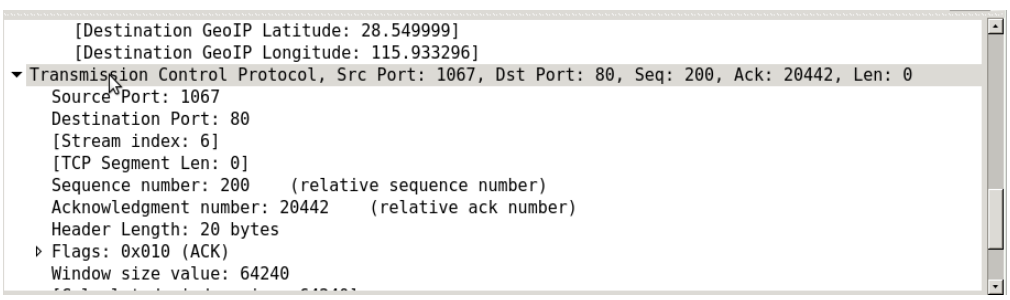

Figure 6: packet 155

   (b) packet 183
   source IP address: 192.168.23.129
   destination IP address: 59.53.91.102
   source port numbers: 1067

destination port numbers: 80
protocol: TCP

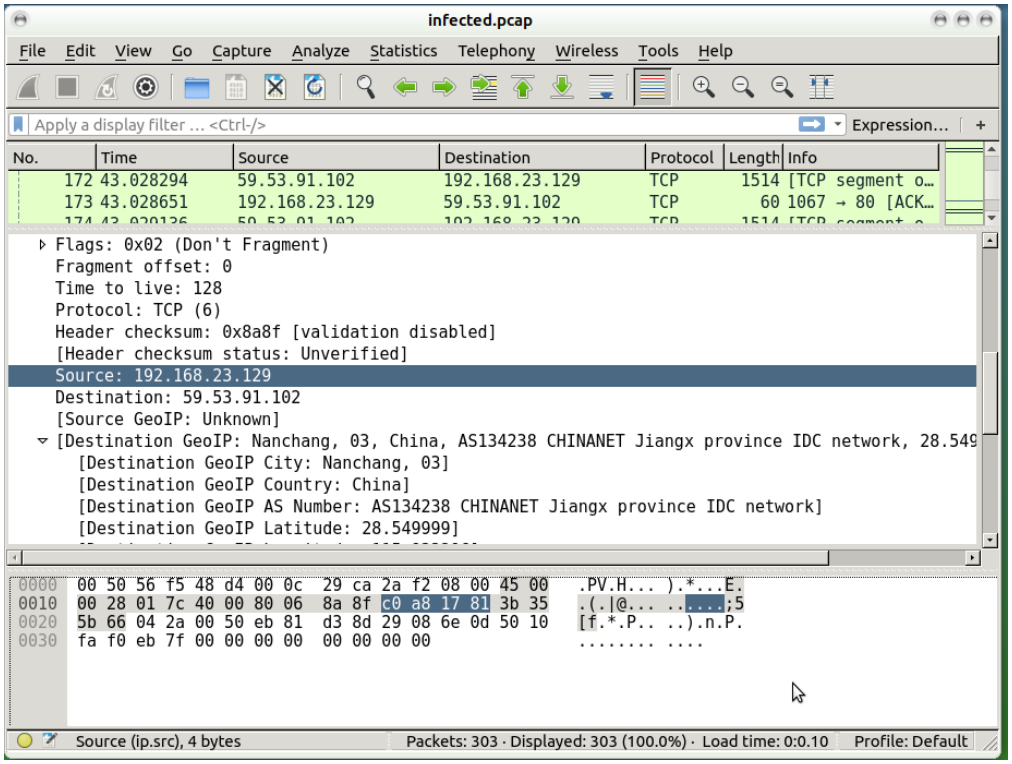

Figure 7: packet 183

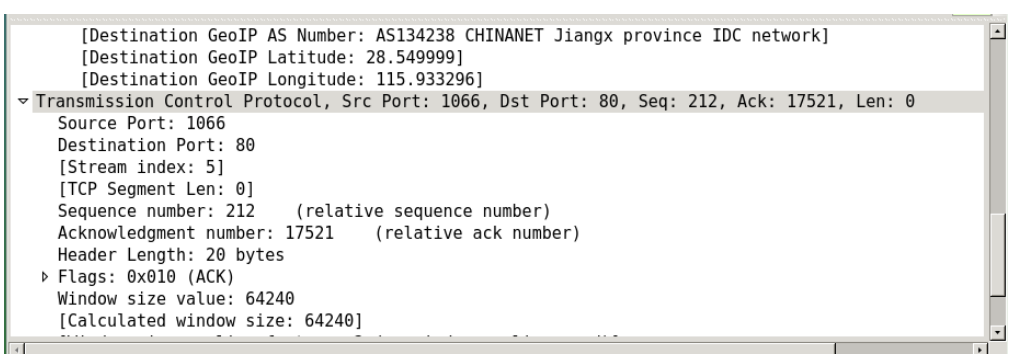

Figure 8: packet 183

(c) packet 294
source IP address: 212.252.32.20
destination IP address: 192.168.23.129
source port numbers: 80
destination port numbers: 1069
protocol: TCP

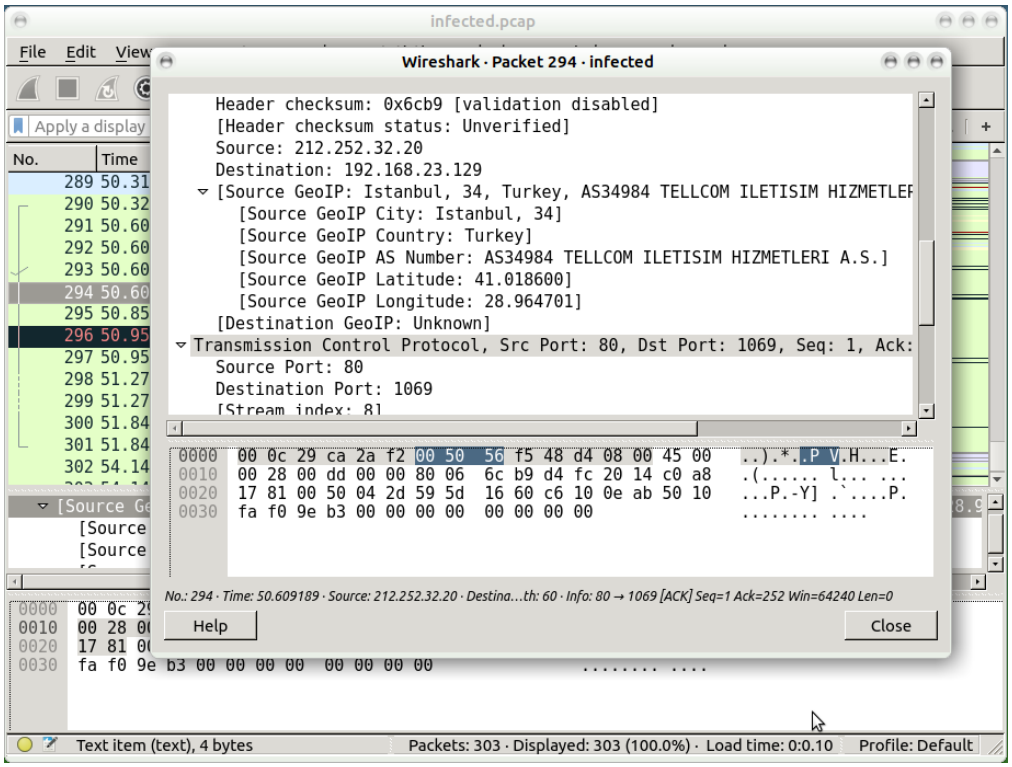

Figure 9: packet 294

3. **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 directly use 'dns' to filter.

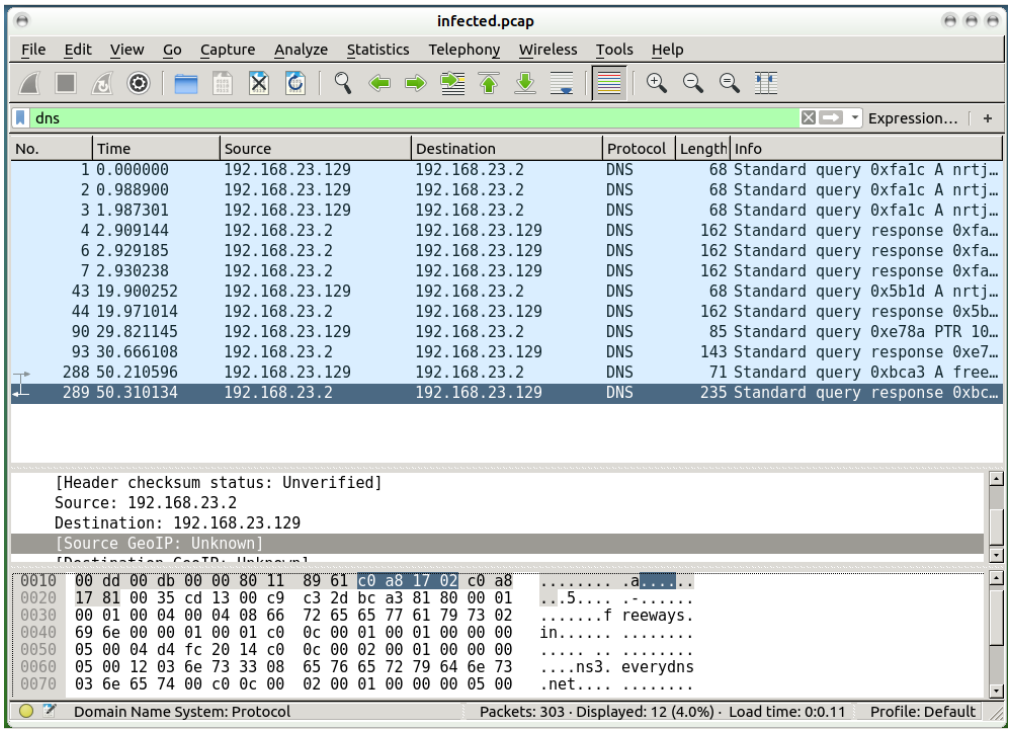

Figure 10: dns queries

4. **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)**
We can use 'http' to filter and then we will notice that there are two jar files: q.jar and sdfg.jar.

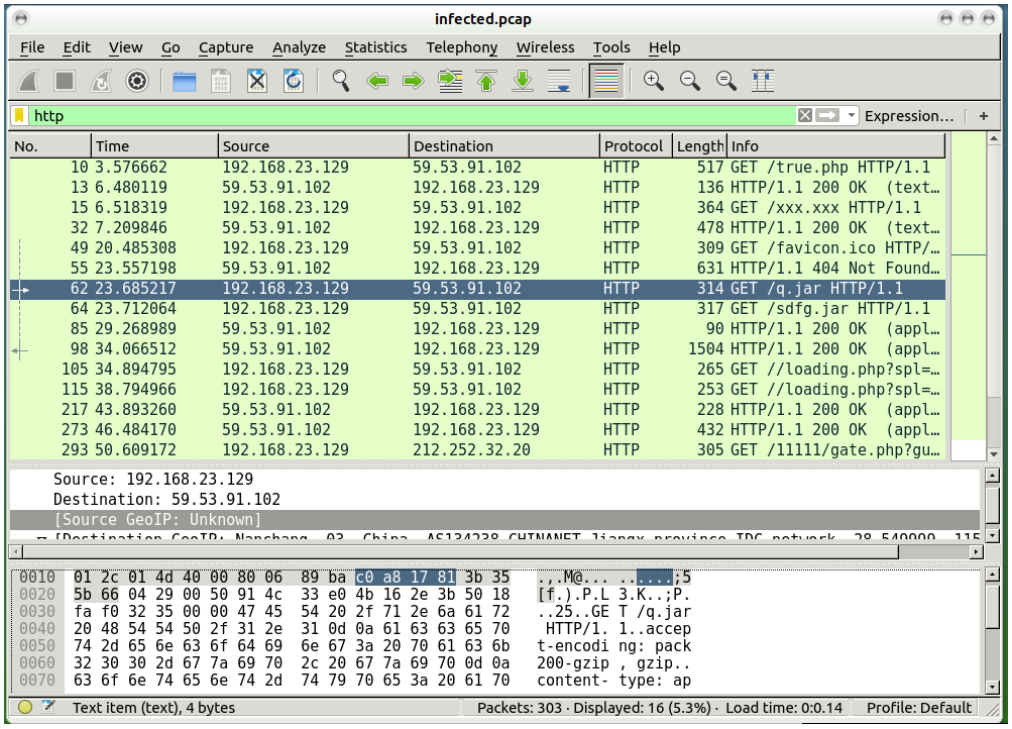

Figure 11: two download jar file

5. **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)**
   According to the hint, the md5 will end with '91ed', and packet 293 has that. And the md5 hash is: 5942ba36cf732097479c51986eee91ed

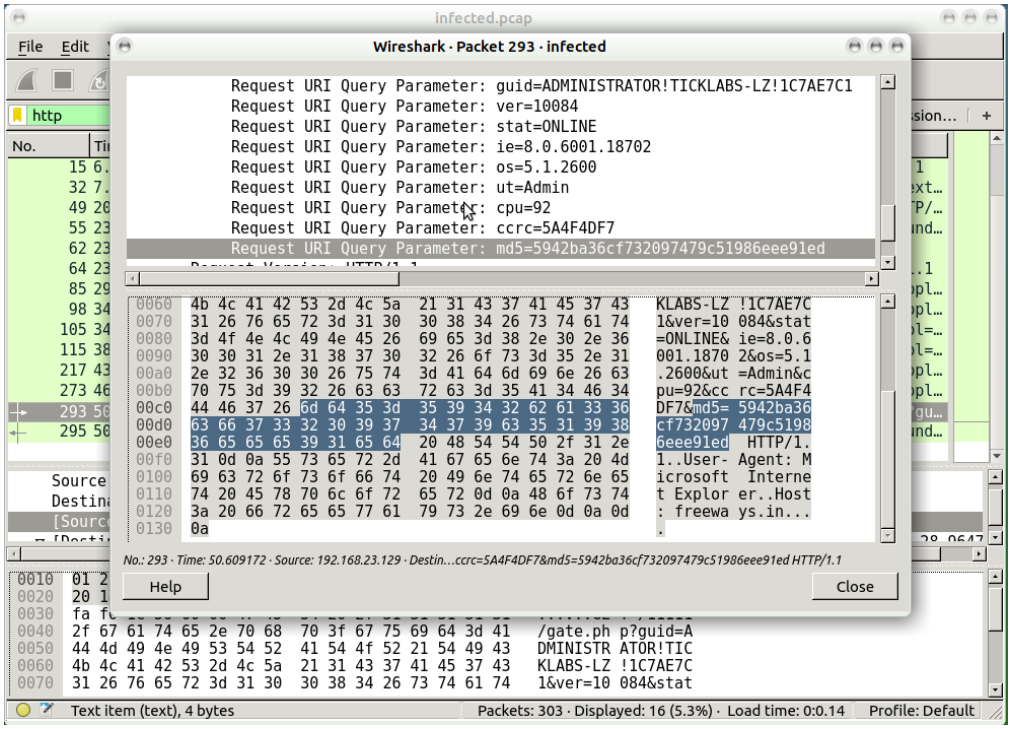

Figure 12: md5 hash

6. **Which browser is being used by the client? (5 points)**
   The client uses Microsoft Internet Explorer.