**Review Test Submission: Homework3**

### Question 3

In the HW2\_Lab, explain what is happening in the TCP Stream from Frame 35.  Remember, you need to right click on Frame 35 and select "Follow TCP Stream."  Your answer should include at least 6 items that you noticed based on your analysis.

Enumeration of the victim’s browser is taking place to determine if they have Java installed, which version, and if it is a vulnerable version.

The URL to the browser exploits of amor1.jar and java7.jar (danieldelaney.com) are shown in this stream as well, albeit somewhat obfuscated.

Also, a URL (blogtcl.com.ar) to send the payload rh.exe to the victim is shown.

### Question 5

In the HW\_2 Lab, create a filter that only shows traffic from any host using the HTTP protocol but eliminate the SSDP traffic .  Type the filter as the answer to this question.

http and tcp.port==80

### Question 10

What is the difference between Viruses, Worms, and Trojans?  You answer should include details about propation method and payloads.

Virus - Can't propagate on its own.  Payload may overwrite other software, erase files and programs, reformat hard disk, etc.

Worm - Can propagate on its own.  Payload may include backdoor, spam engine, DoS attacks, etc.

Trojan - Does not self replicate like worms or reproduce by infecting other files like viruses.  Payload may include data theft, backdoor, downloading of other malware, etc.