Farhad Ahmed

Network Security

Professor McCoy

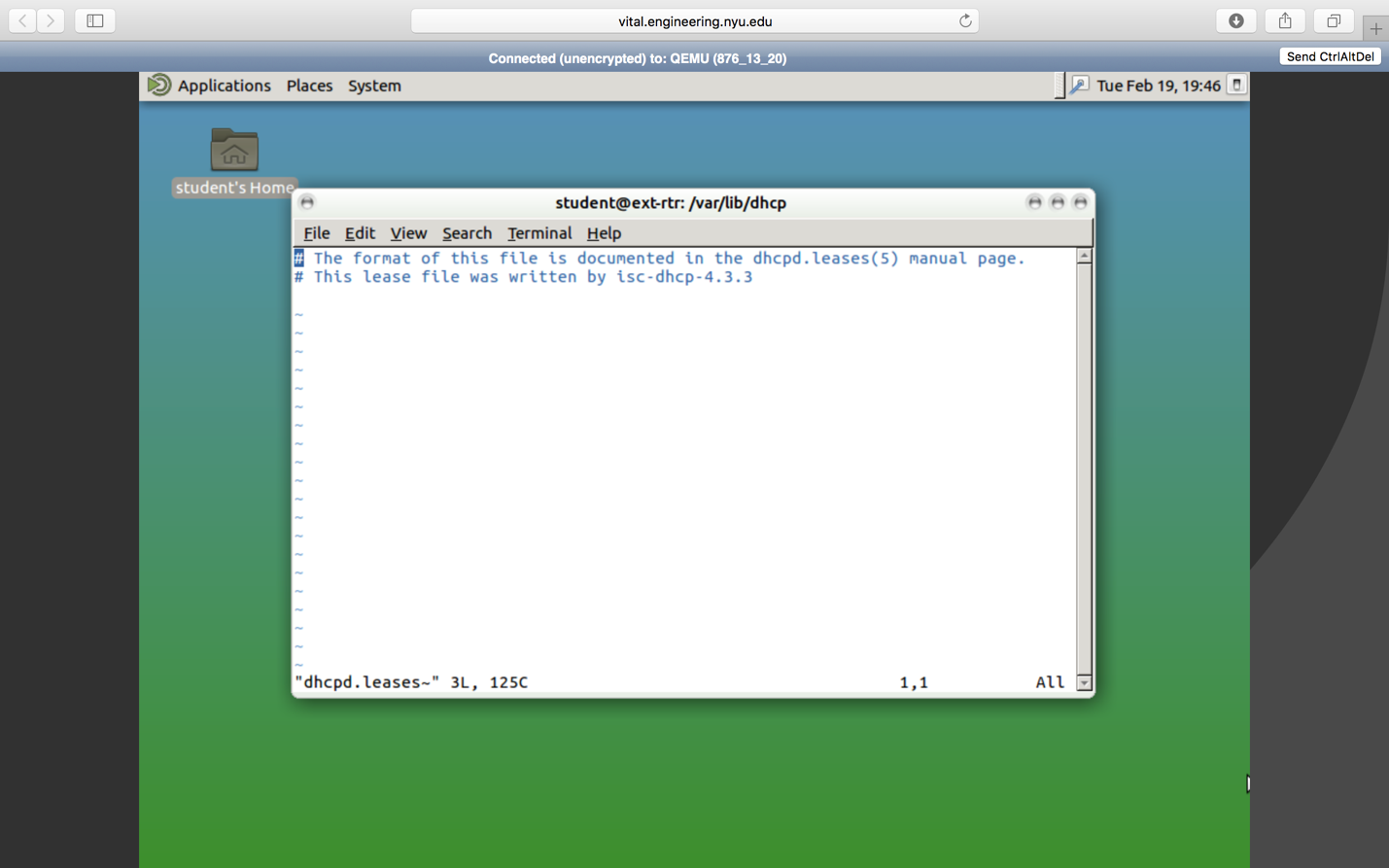
02/19/19

**Lab 01 – DHCP Starvation Attack Using Python/ScaPy**

This lab was designed to show the effectiveness of launching a DoS attack on a DHCP server by starving it of available IP’s within a range. To start this lab, the first thing that needed to be done was reset the EXT-Router’s dhcpd.leases files. Before the attack these files appeared as shown below.



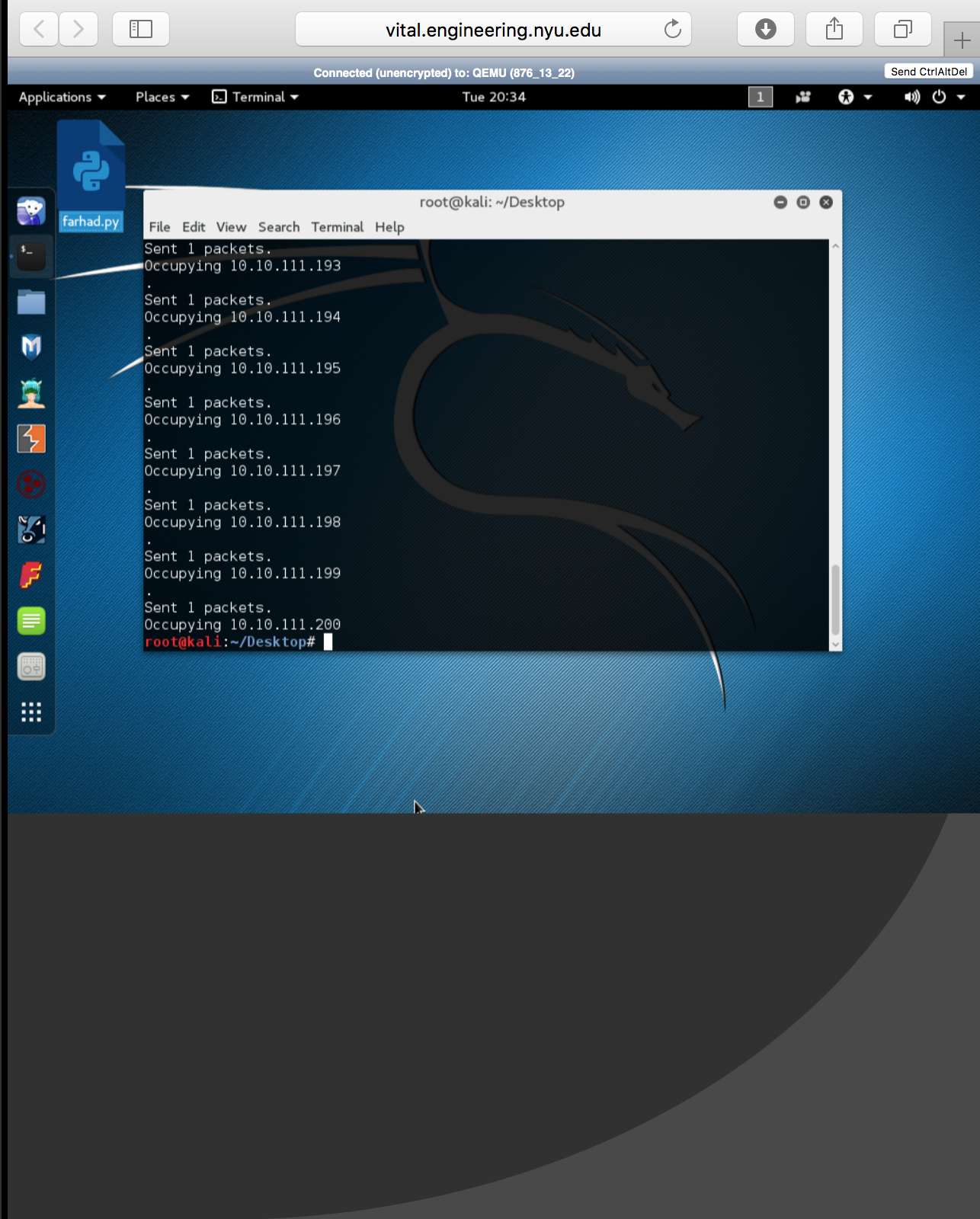
**Figure 1***. dhcpd.leases file contents*



**Figure 2**. *dhcpd.leases~ file contents*

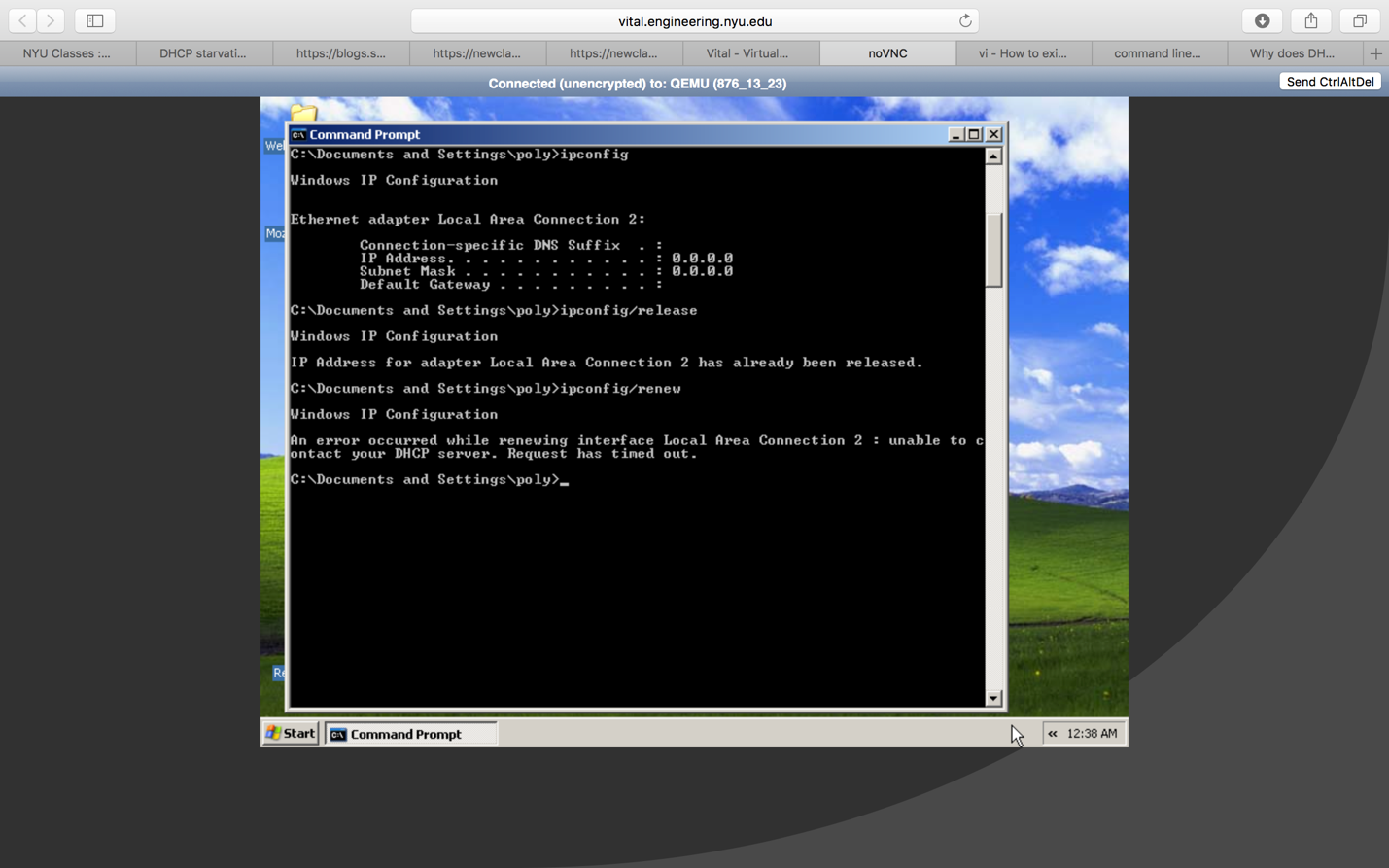
The next step was to boot the Kali Linux machine and write a Python script using the ScaPy library. This script loops through a range of 100 to 200 and adds that to the subnet to assemble a proper IP address (10.10.11.xxx). A new MAC address is also generated and a packet is put together using these two. The packets are sent to the server and the handshake results as incomplete which bounds the packet to the IP. After doing this for 100 addresses, there is none left for legitimate users.

Running the script, output to the terminal everytime a packet was sent and also displayed the IP address that the loop was on.



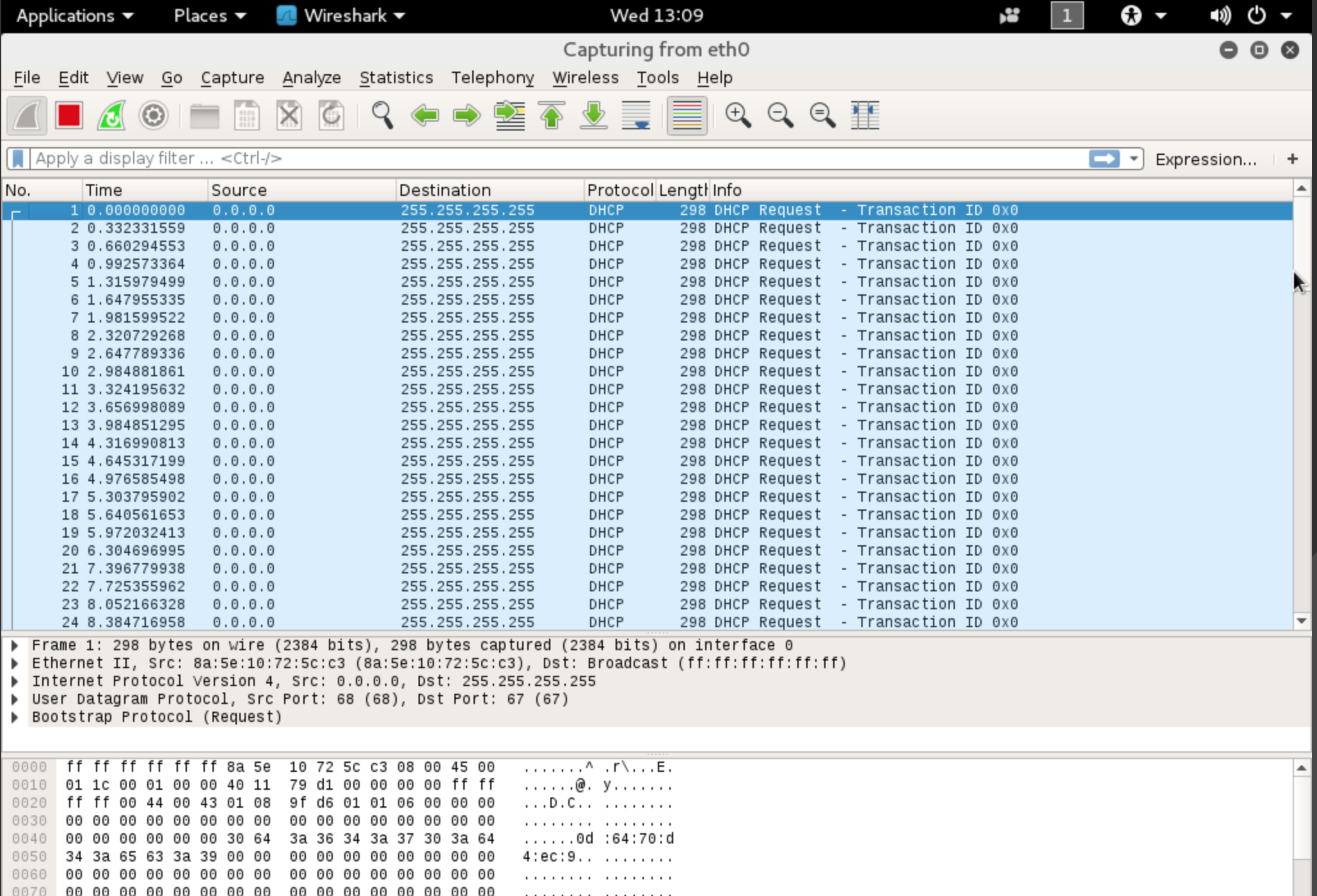
**Figure 3.** *Terminal output from running starve.py*

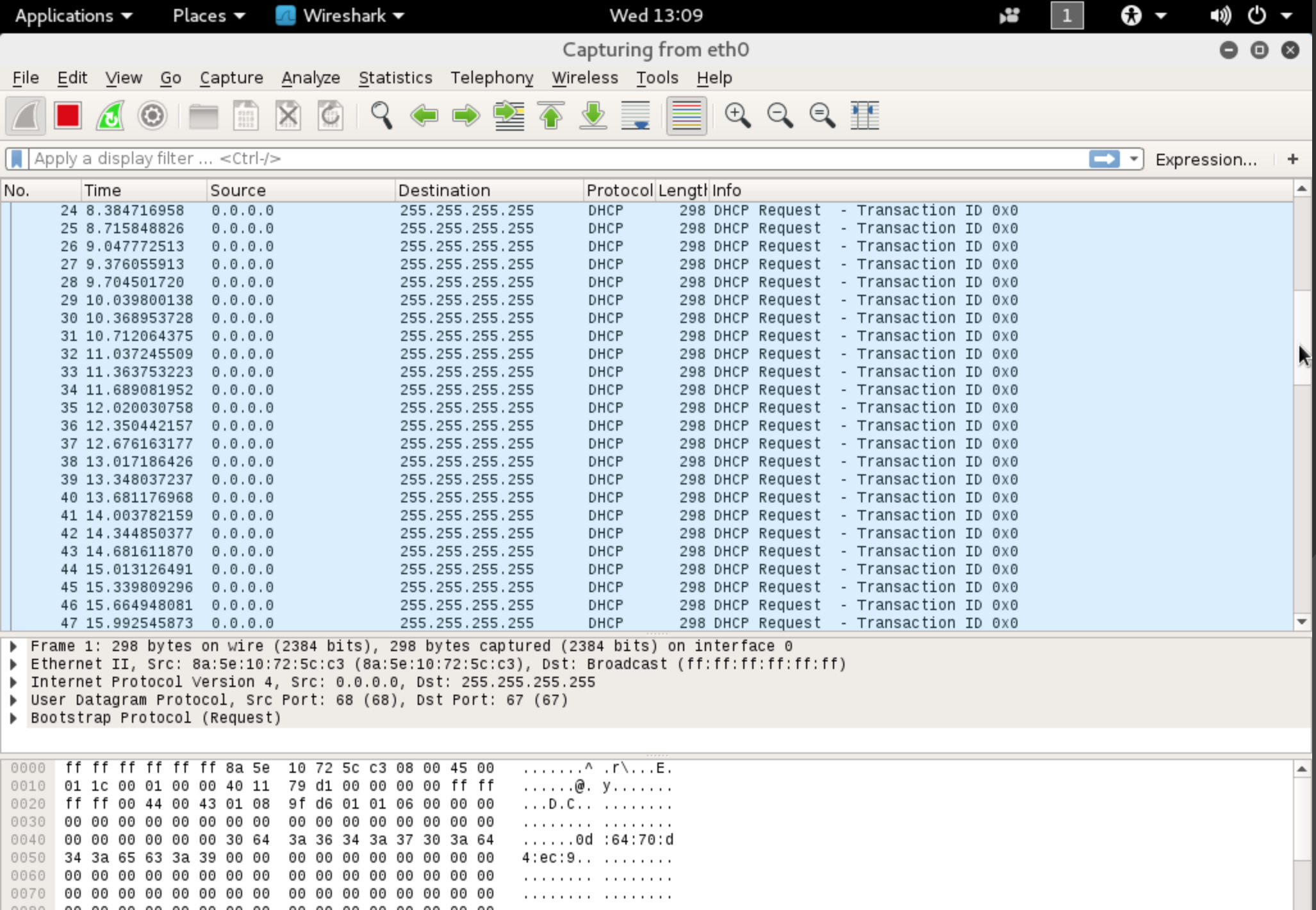
Trying to access the server through ipconfig on the Windows XP VM, revealed that the IP address and subnet was 0.0.0.0. Running ipconfig/renew returned a message indicating that the request had timed out.

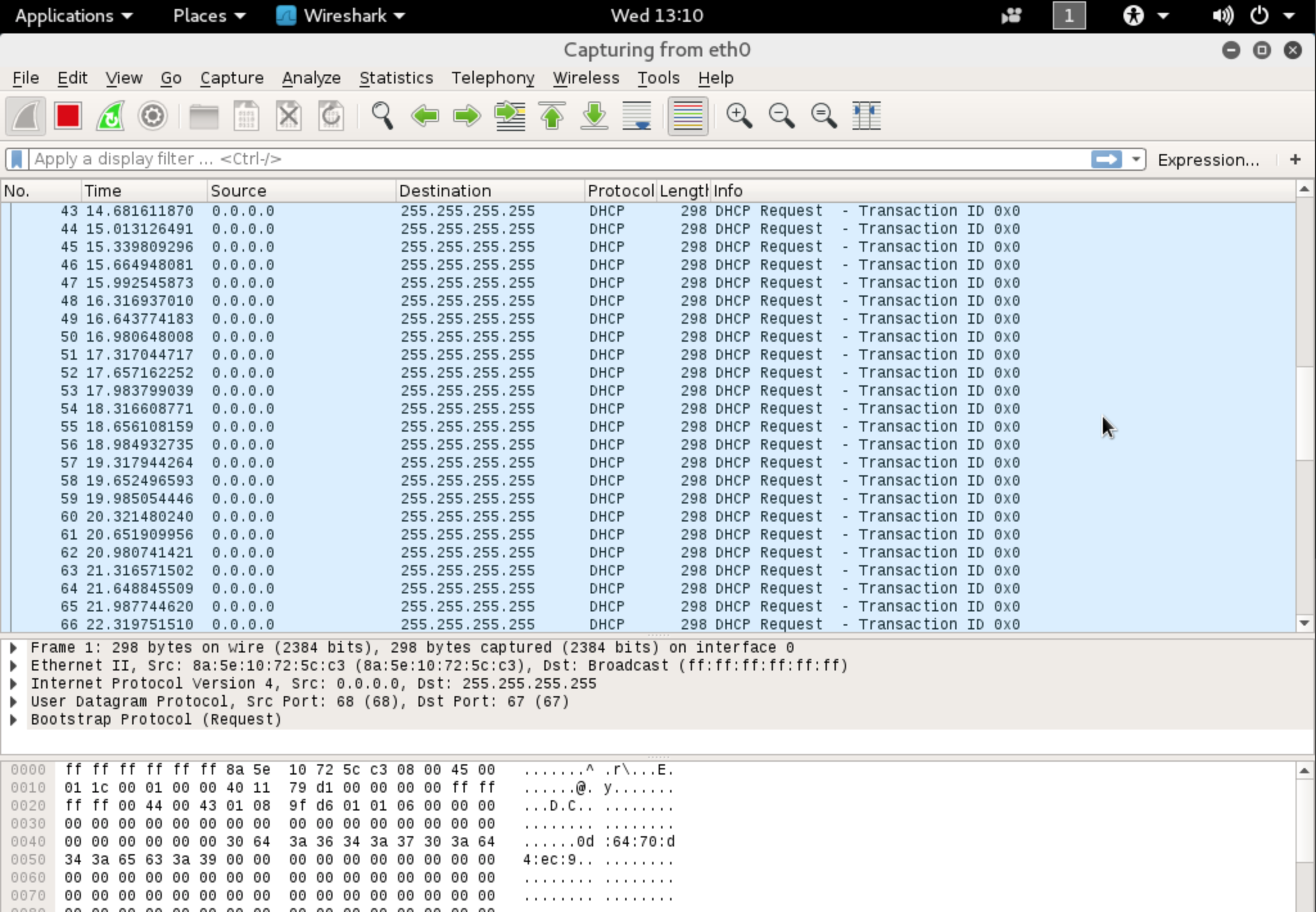


**Figure 4.** *Victim is unable to access server.*

Capturing the packets during the execution of the script was somewhat difficult due to problems with running WireShark within the VM. Wireshark would frequently close after opening the program and selecting the connection to sniff packets on. Sometimes it would even close in the middle of running the starve.py script. However, I was able to screenshot some of the packets before the program could close.

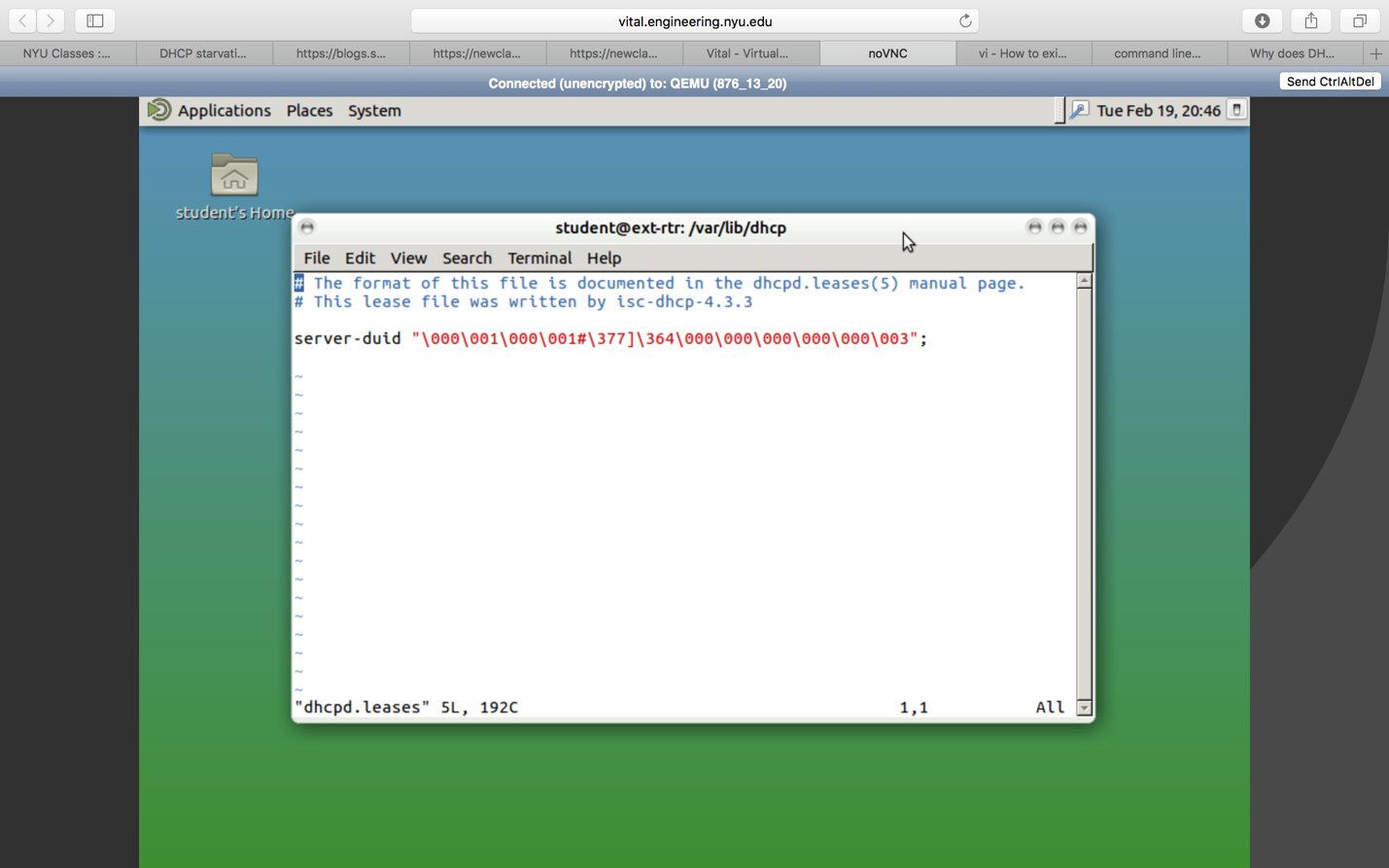


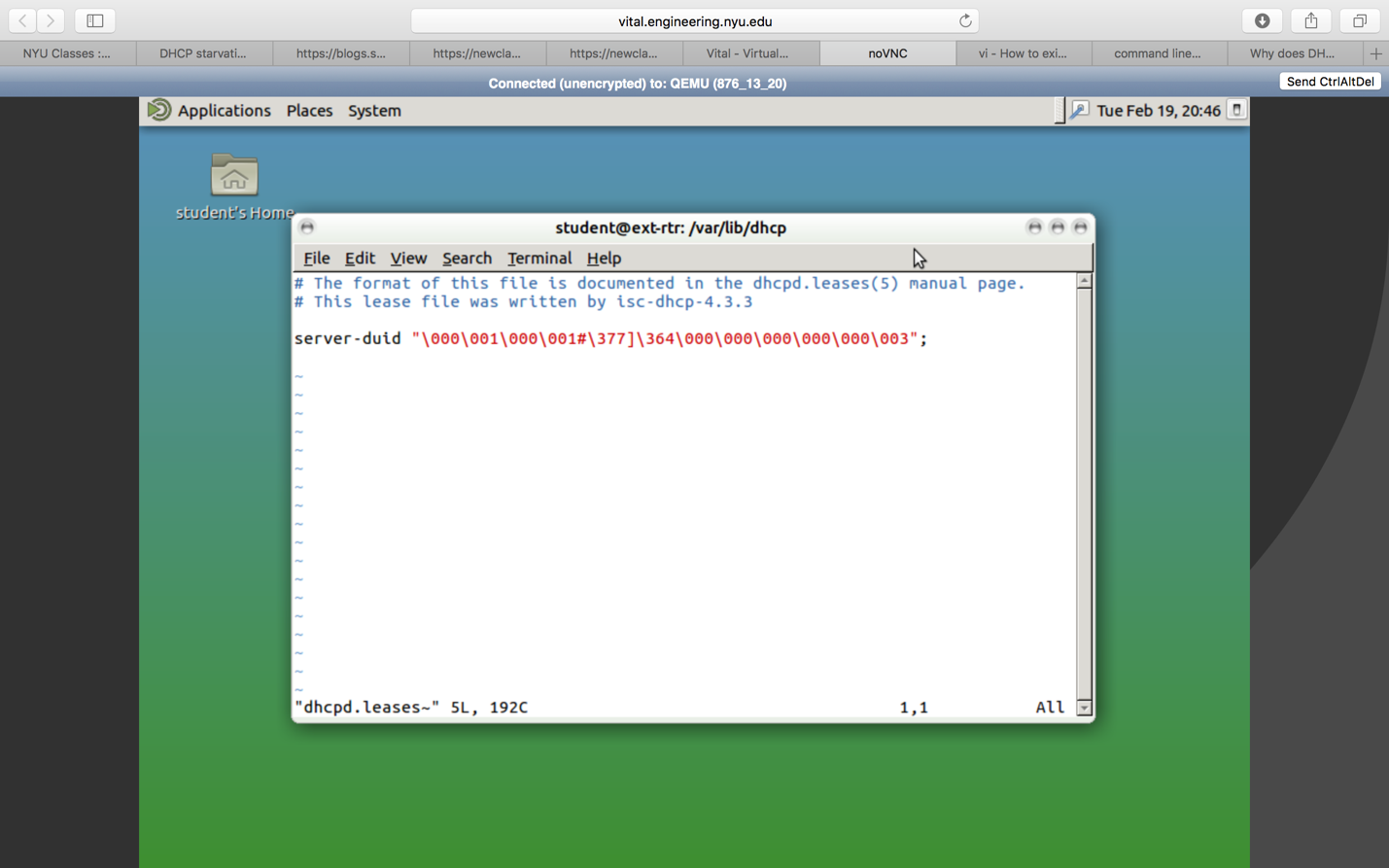




**Figure 5.** *Wireshark packets being captured.*

After running the starvation script, the dhcpd file on the EXT-Router had been updated as seen below.





**Figure 6.** *dhcpd.leases files changed after running attack script.*