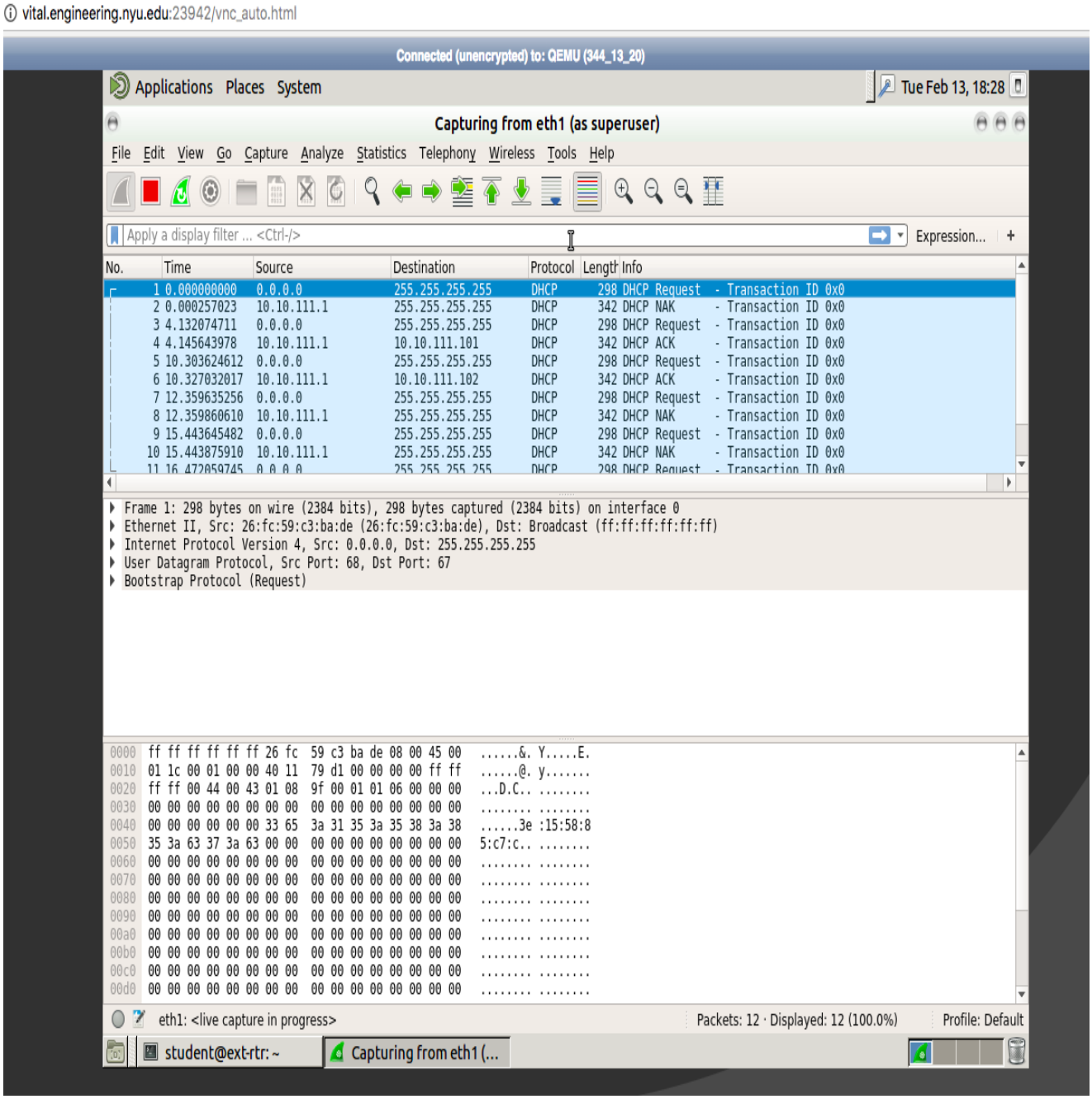
LAB 1 : DHCP Starvation using Python/Scapy

DHCP Starvation attack is when attacker binds all usable IP addresses on a DHCP server and perform Denial of Service on the network. In our lab we performed this attack on External Router. DHCP consists of four steps : DHCP discover, DHCP offer, DHCP request and DHCP ACK. Instead of completing the entire DHCP handshake/protocol, we can just step in to sending request to the external router from spoofed MAC address and receiving ACK back from the router. This will need to be done per IP address in range 10.10.111.100 to 10.10.100.200.

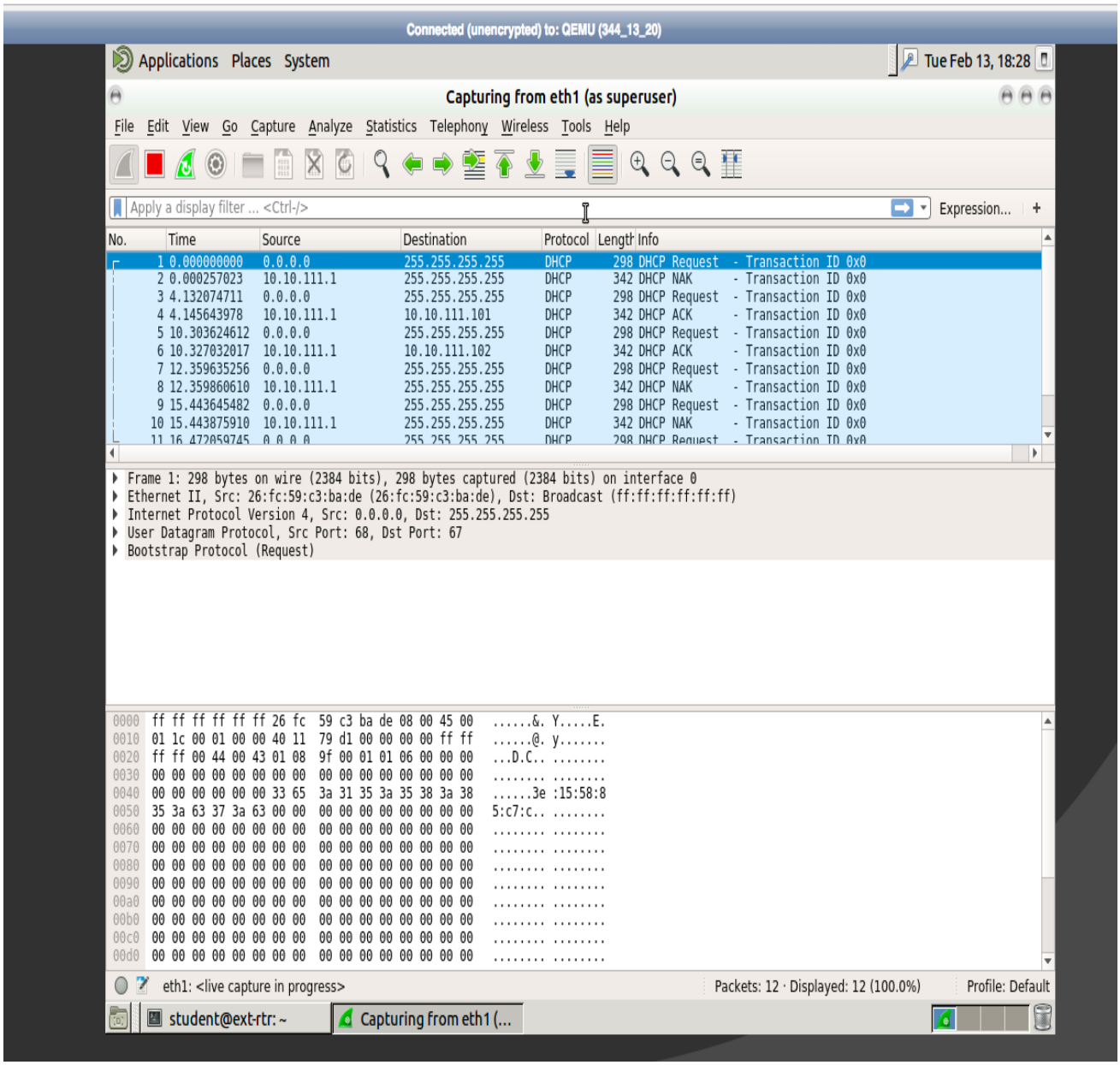
Before attack we can look in to dhcpd.leases files entry. This dhcpd.leases file is located at path /var/lib.dhcp in external router. We have to delete any previous entries in the file. This removes any static or old IP/MAC binding pre-configured in router.

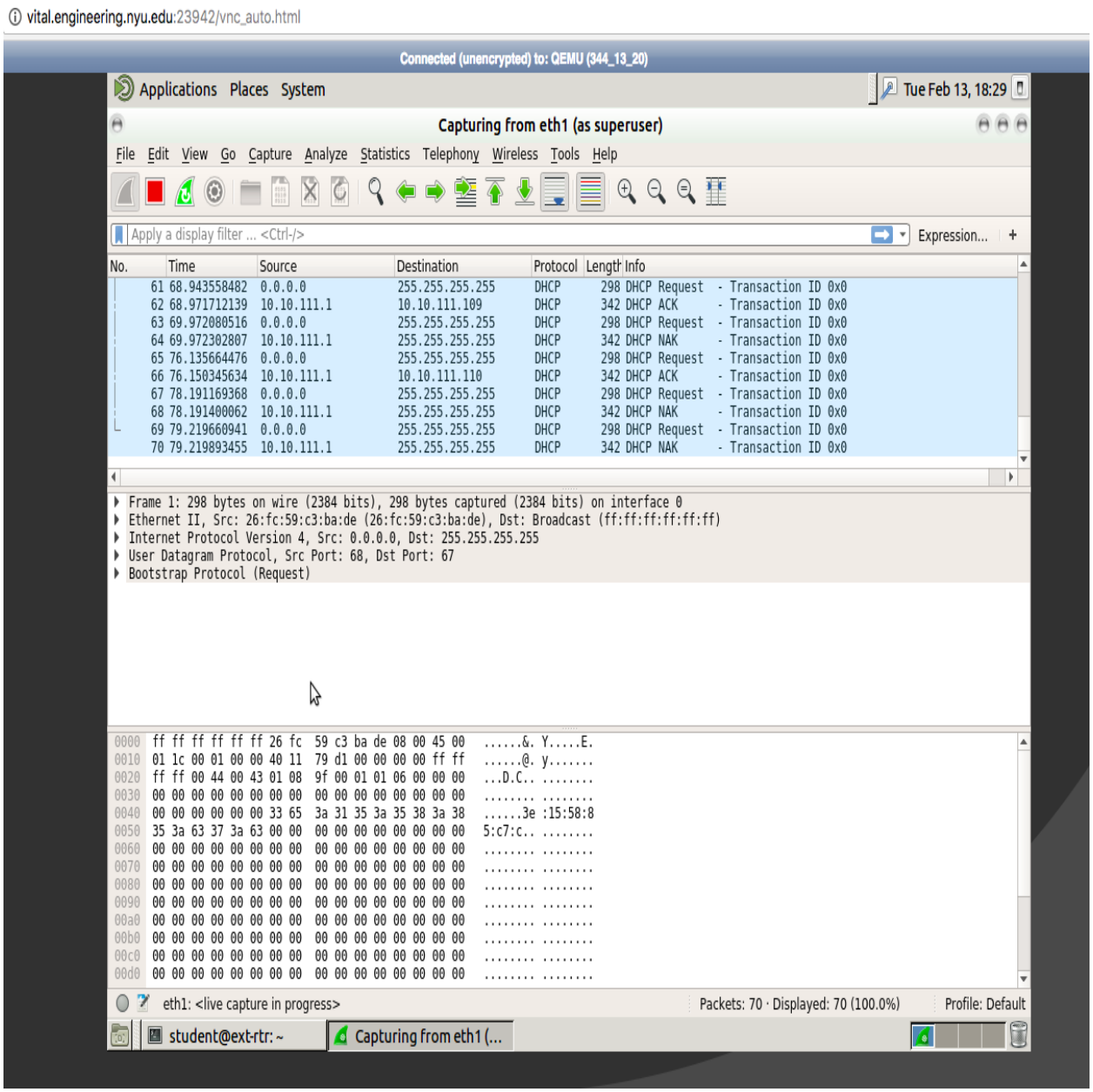
The python script has to be executed on kali machine. We can use scapy for DHCP starvation. ScaPy is python library which is used for networking and security. When script runs on kali machine the dhcp_starvation method send DHCP requests for certain IP in a loop to external router. Everytime we are generating a new MAC address and checking whether current IP address is already registered. We are also using sleep to avoid congesting the link with DHCP, which decreases the efficiency of attack. All the available IP addresses will be bound after the attack and dhcpd.leases file will now have entries for them.

Wireshark capture on router when attack is in progress (i.e Python script is running on kali machine)


vital.engineering.nyu.edu:23942/vnc_auto.html
Connected (unencrypted) to: QEMU (344_13_20)
Applications Places System
Tue Feb 13, 18:28
Capturing from eth1 (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
1 0.000000000 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
2 0.000257023 10.10.111.1 255.255.255.255 DHCP 342 DHCP NAK - Transaction ID 0x0
3 4.132074711 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
4 4.145643978 10.10.111.1 10.10.111.101 DHCP 342 DHCP ACK - Transaction ID 0x0
5 10.303624612 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
6 10.327032017 10.10.111.1 10.10.111.102 DHCP 342 DHCP ACK - Transaction ID 0x0
7 12.359635256 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
8 12.359860610 10.10.111.1 255.255.255.255 DHCP 342 DHCP NAK - Transaction ID 0x0
9 15.443645482 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
10 15.443875910 10.10.111.1 255.255.255.255 DHCP 342 DHCP NAK - Transaction ID 0x0
Frame 1: 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface 0
Ethernet II, Src: 26:fc:59:c3:ba:de (26:fc:59:c3:ba:de), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Bootstrap Protocol (Request)
0000 ff ff ff ff ff ff 26 fc 59 c3 ba de 08 00 45 00 ......&. Y.....E.
0010 01 1c 00 01 00 00 40 11 79 d1 00 00 00 00 ff ff ......@. y.......
0020 ff ff 00 44 00 43 01 08 9f 00 01 01 06 00 00 00 ...D.C.. ....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0040 00 00 00 00 00 00 33 65 3a 31 35 3a 35 38 3a 38 ......3e :15:58:8
0050 35 3a 63 37 3a 63 00 00 00 00 00 00 00 00 00 00 5:c7:c.. ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
eth1: <live capture in progress>
Packets: 12 · Displayed: 12 (100.0%)
Profile: Default
student@ext-rtr: ~
Capturing from eth1 (...

ⓘ vital.engineering.nyu.edu:23942/vnc_auto.html

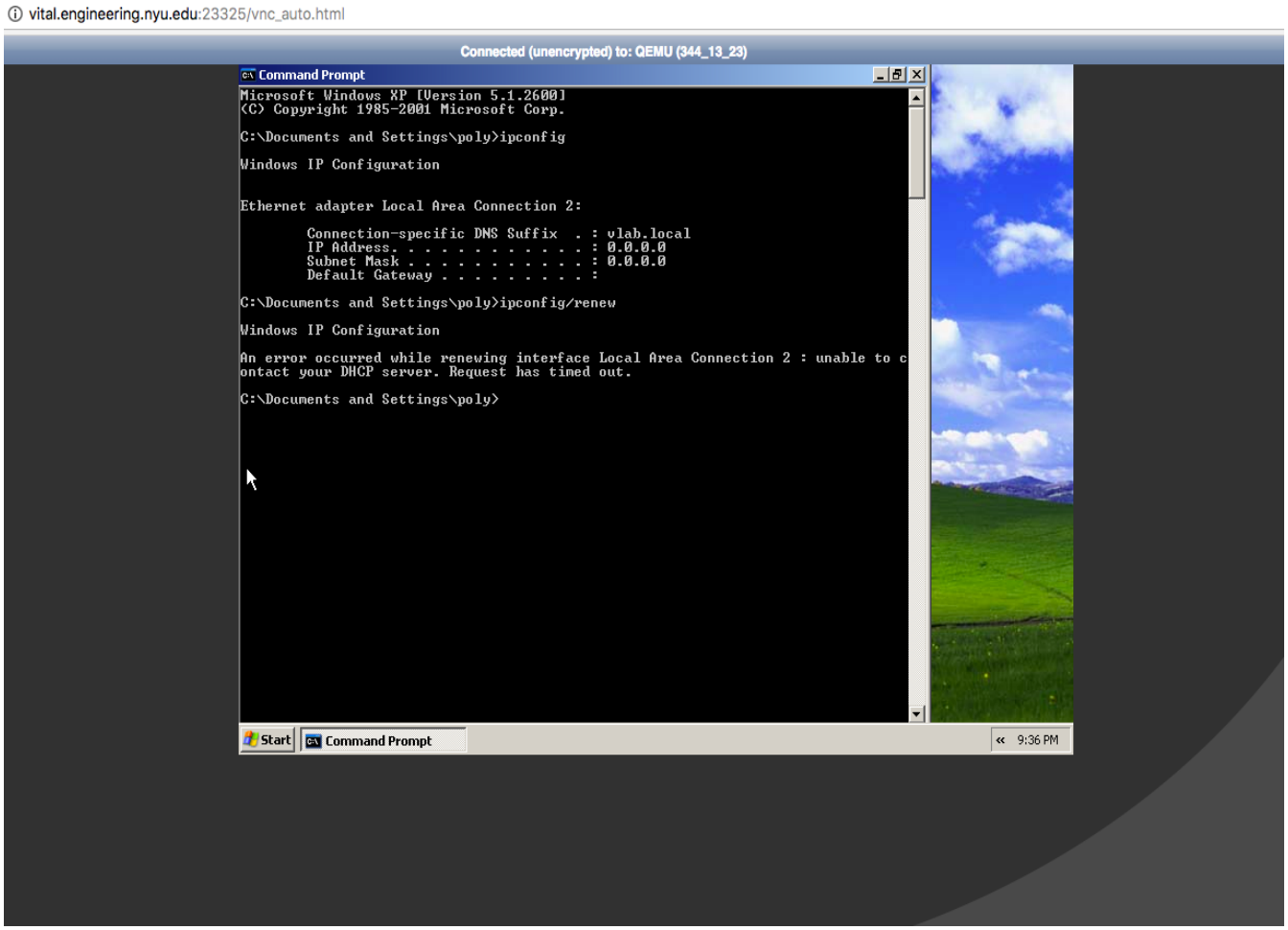




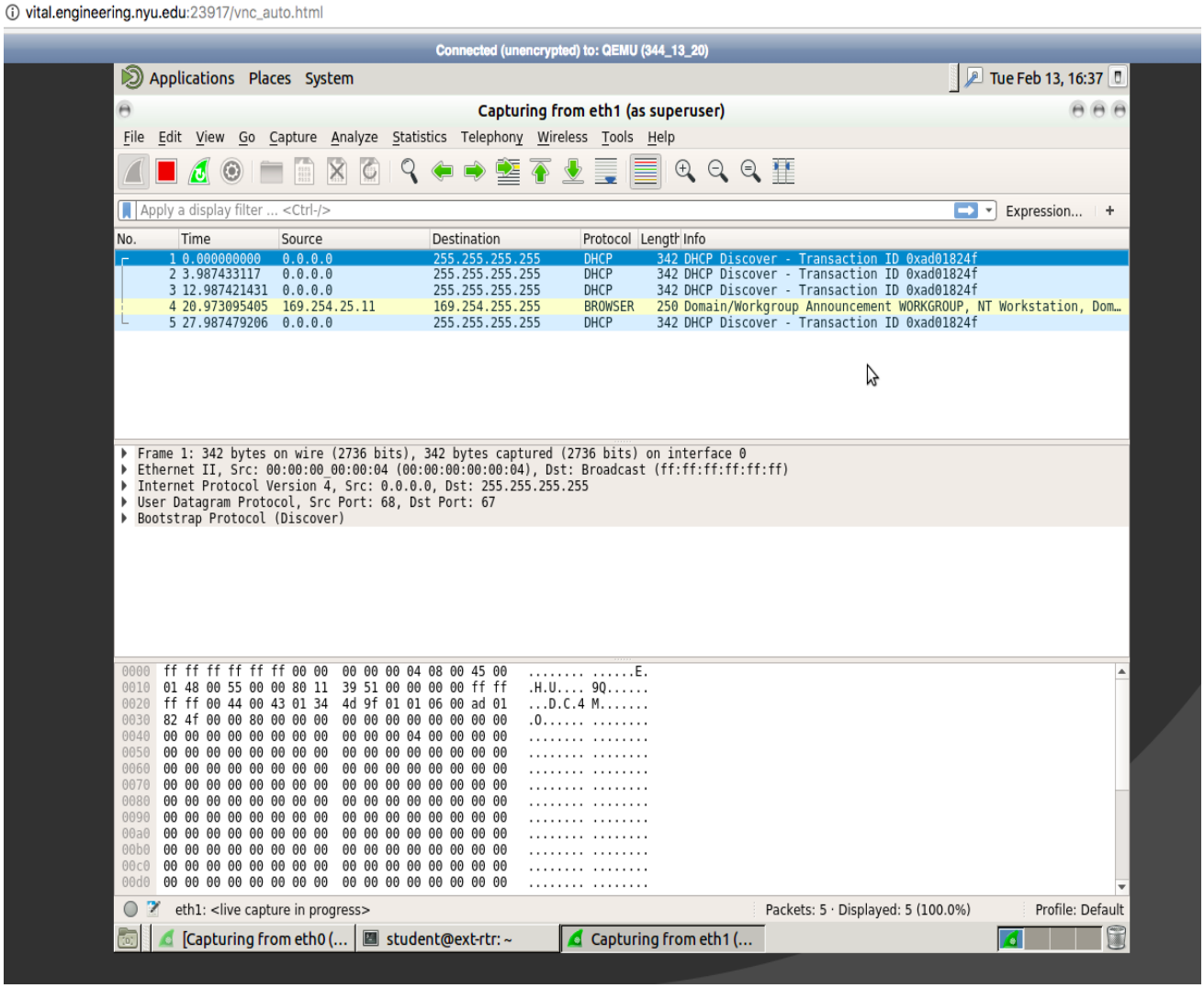
After the attack is done. We have to start window xp machine and check it's ip address.
We can do this by running ipconfig command on cmd.exe. The IP address and subnet mask is 0.0.0.0. This means that Windows XP machine is unable to get IP address from DHCP server.

Now we type ipconfig/renew to try to get an IP address from the router.

The output comes as follows :



Wireshark capture at ext-router when ipconfig/renew command is issued from windows xp machine :



Since, the machine is not able to get the IP from router, that means our DHCP starvation attack was successful.