IT PROJECT
DOCUMENTATION

DHCP Discover Flood Attack – Detection, Analysis & Recovery

MORGAN BURERA

Google IT Support Professional Certificate

JULY 2025

Ubuntu, Terminal

Screenshots of the first part

🗝️ Key Takeaways

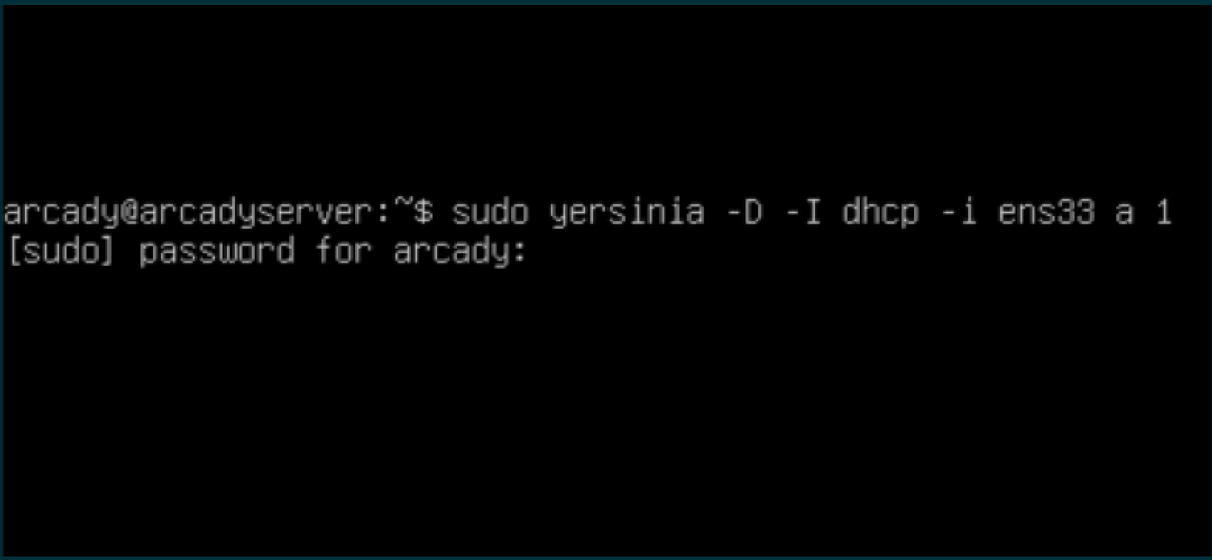
```
morgan@morganclient:~$ sudo ip link set ens33 up
morgan@morganclient:~$ sudo dhclient -v ens33
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Corrupt lease file - possible data loss!
Listening on LPF/ens33/00:0c:29:82:f2:2c
Sending on   LPF/ens33/00:0c:29:82:f2:2c
Sending on   Socket/fallback
xid: warning: no netdev with useable HWADDR found for seed's uniqueness enforcem
ent
xid: rand init seed (0x68112ef2) built using gethostid
DHCPREQUEST for 192.168.251.135 on ens33 to 255.255.255.255 port 67 (xid=0x4521e
f0a)
DHCPACK of 192.168.251.135 from 192.168.251.254 (xid=0xaef2145)
bound to 192.168.251.135 -- renewal in 879 seconds.
morgan@morganclient:~$
```

I started by setting up the environment correctly:

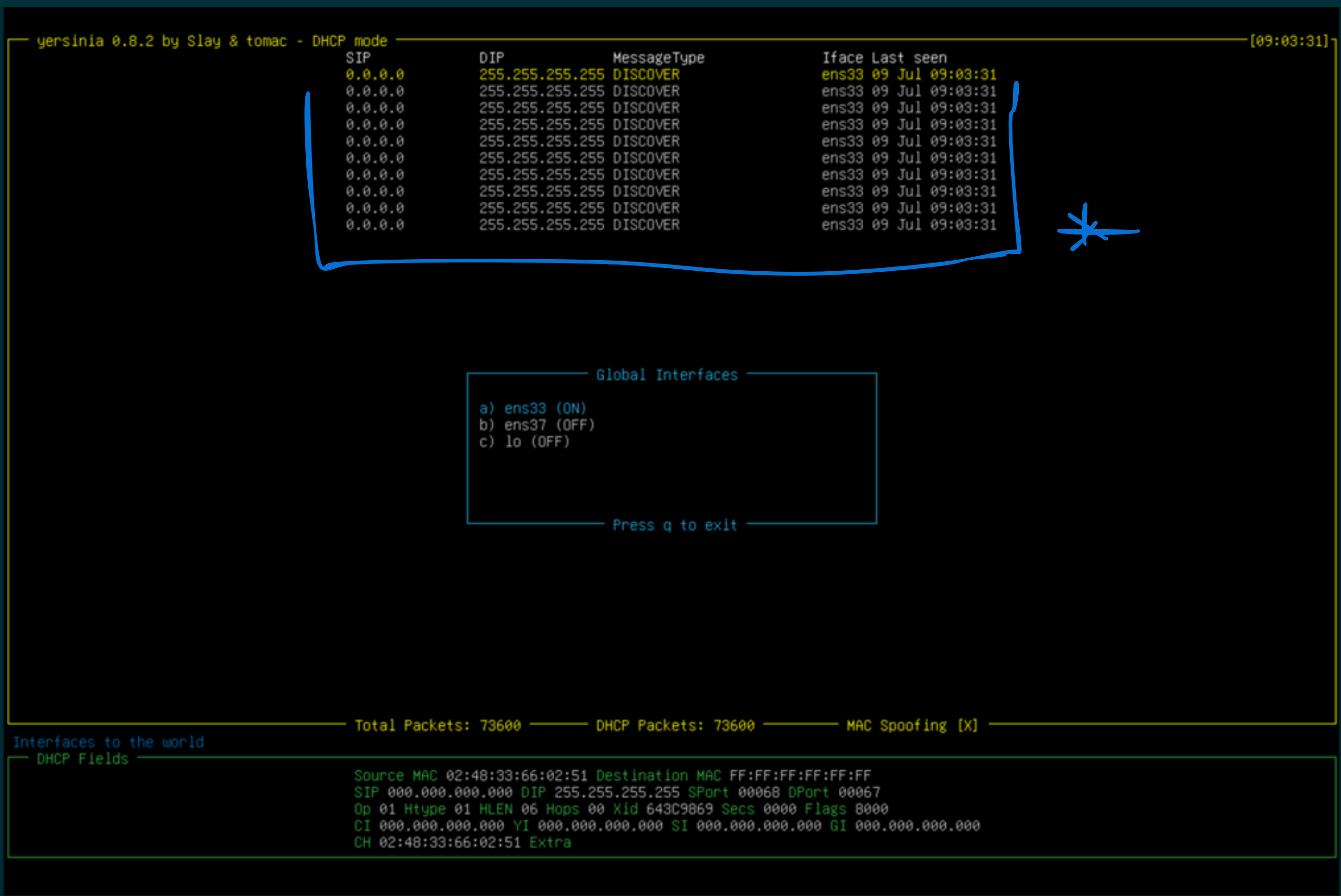
- Put the network interface down, then up
- Renew the IP address

```
2: ens33: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc fq_codel stat
e UP group default qlen 1000
    link/ether 00:0c:29:82:f2:2c brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.251.136/24 brd 192.168.251.255 scope global dynamic noprefixrou
te ens33
       valid_lft 1762sec preferred_lft 1762sec
    inet 192.168.251.135/24 brd 192.168.251.255 scope global secondary dynamic e
ns33
       valid_lft 1770sec preferred_lft 1770sec
    inet6 fe80::20c:29ff:fe82:f22c/64 scope link
       valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:82:f2:36 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 172.16.199.129/24 brd 172.16.199.255 scope global dynamic ens37
       valid_lft 1583sec preferred_lft 1583sec
    inet6 fe80::20c:29ff:fe82:f236/64 scope link
       valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
 UNKNOWN group default qlen 500
    link/none
    inet 10.8.0.1/24 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::a483:6d2d:bfed:31a5/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
morgan@morganclient:~$
```

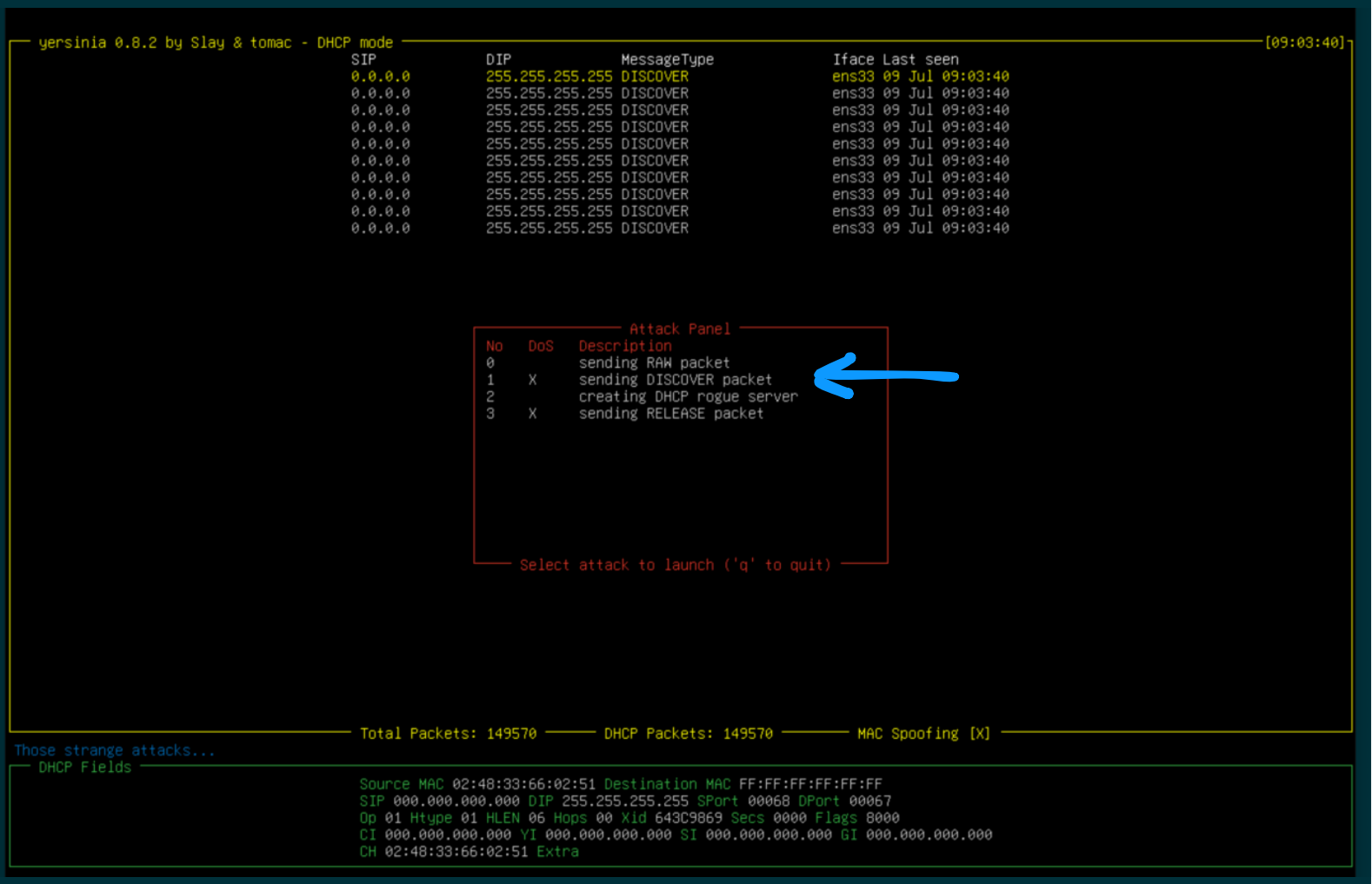
Verifying the network interface.



This command was done on the server vm to start the dhcp rogue attack on ‘yersinia’ but i had to do it manually on it’s interface.

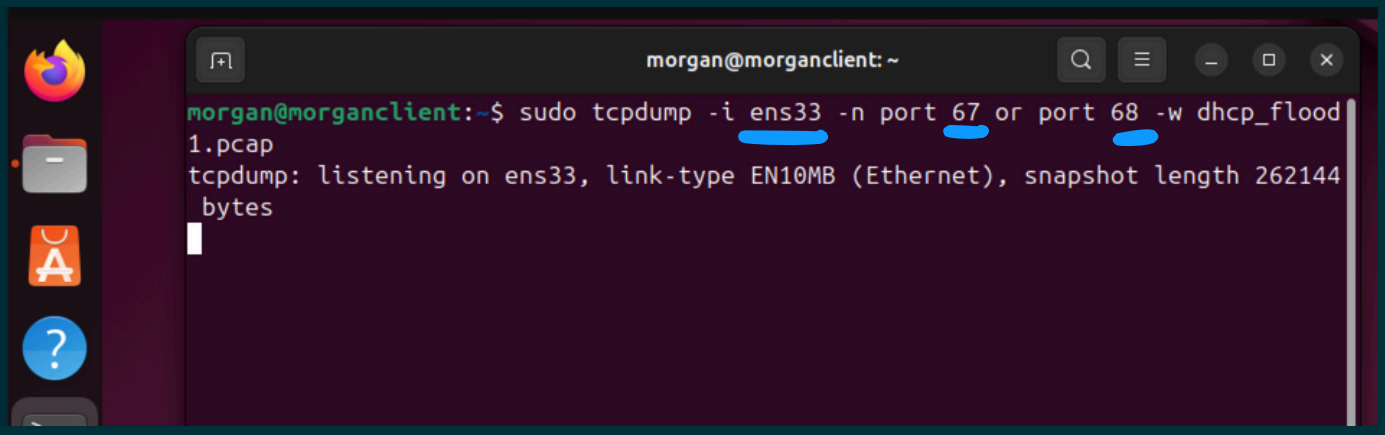


Testing of the attack on yersinia

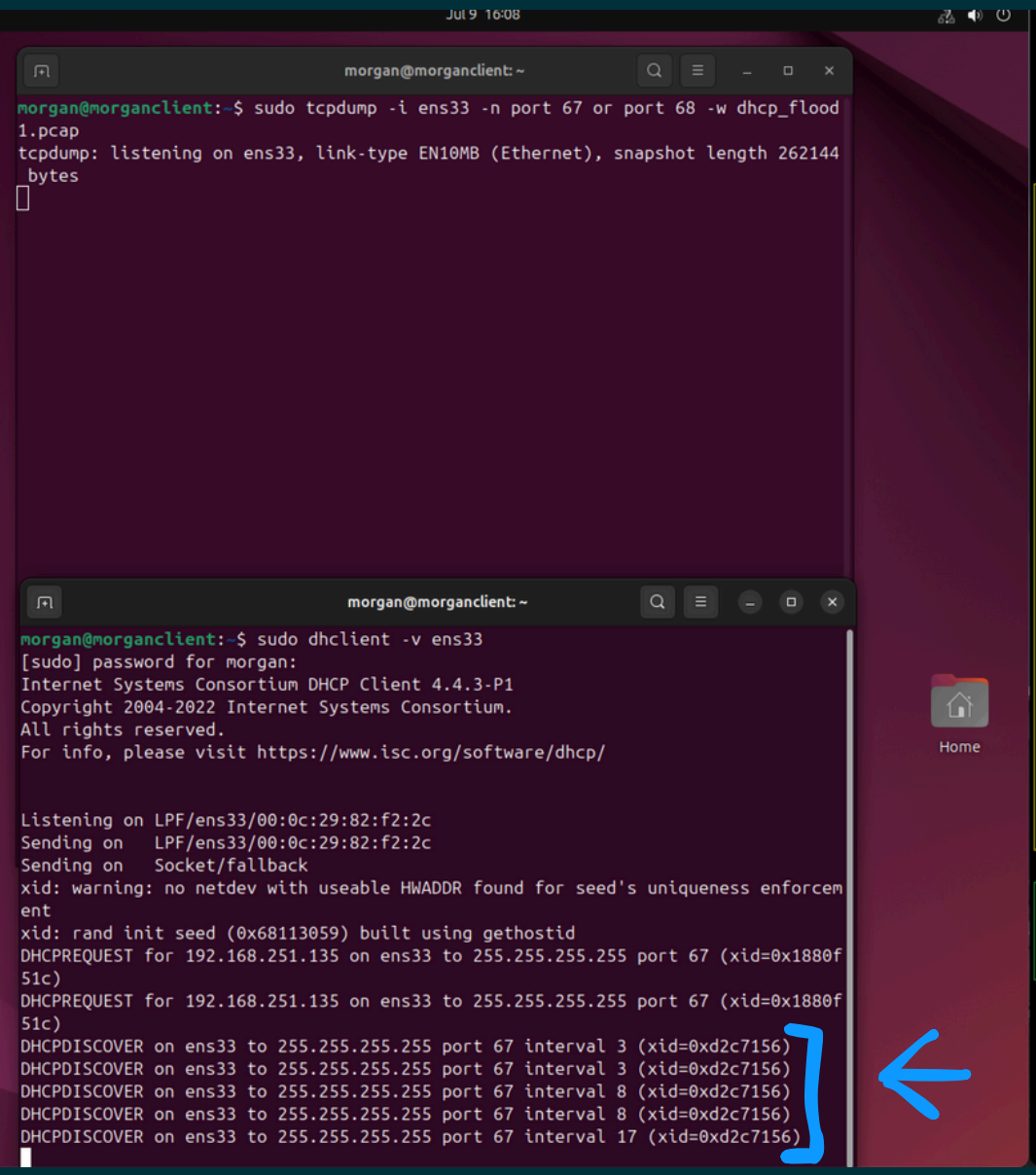


I repeated the attack :

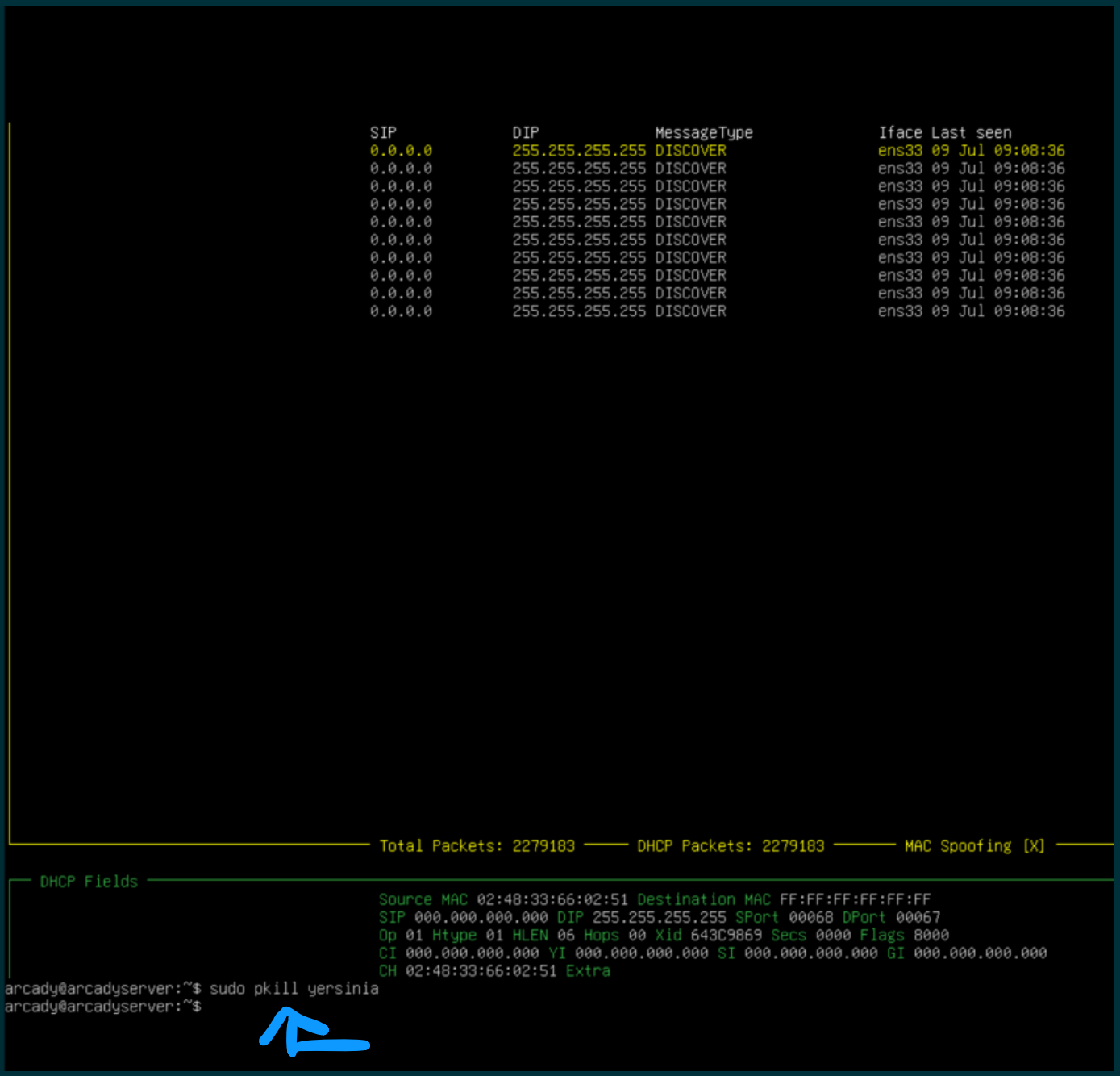
- 1 : Sending Discover packet



Start of the capture on the right ports using tcpdump and saving the capture on : dhcp_flood1.pcap (for auditing)



Start of the issue, due to the dhcp rogue attack every IPs addresses are taken so using ‘sudo dhclient -v ens33’ to assign an IP address to my client is failing.

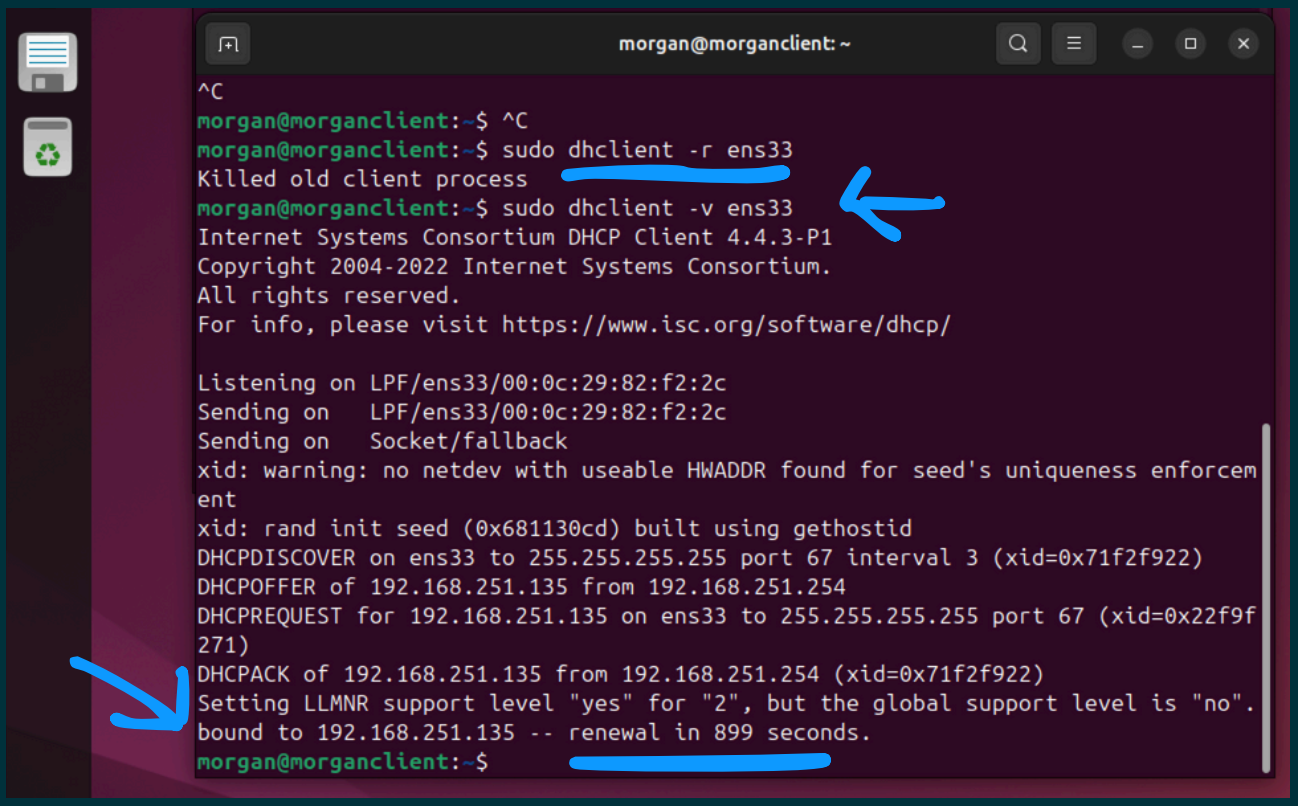


Stoping the dhcp flood on yersinia using :

- sudo pkill Yersinia

or

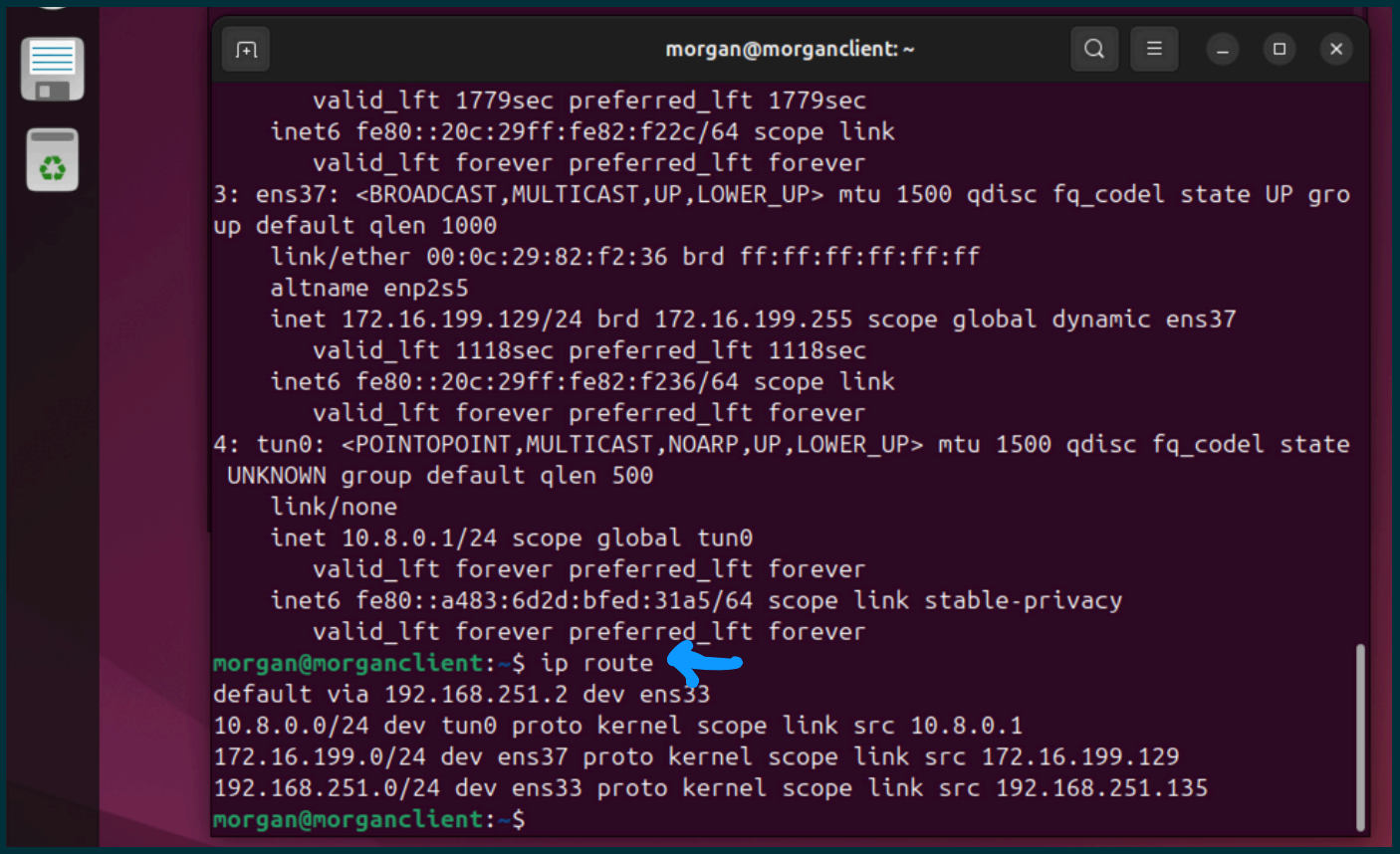
- q (from it’s interactive interface)



Alright, although my laptop was heavily loaded — running the DHCP flood on the VM server, capturing packets on the client VM, and executing commands on another terminal; the capture process still ran without crashing.

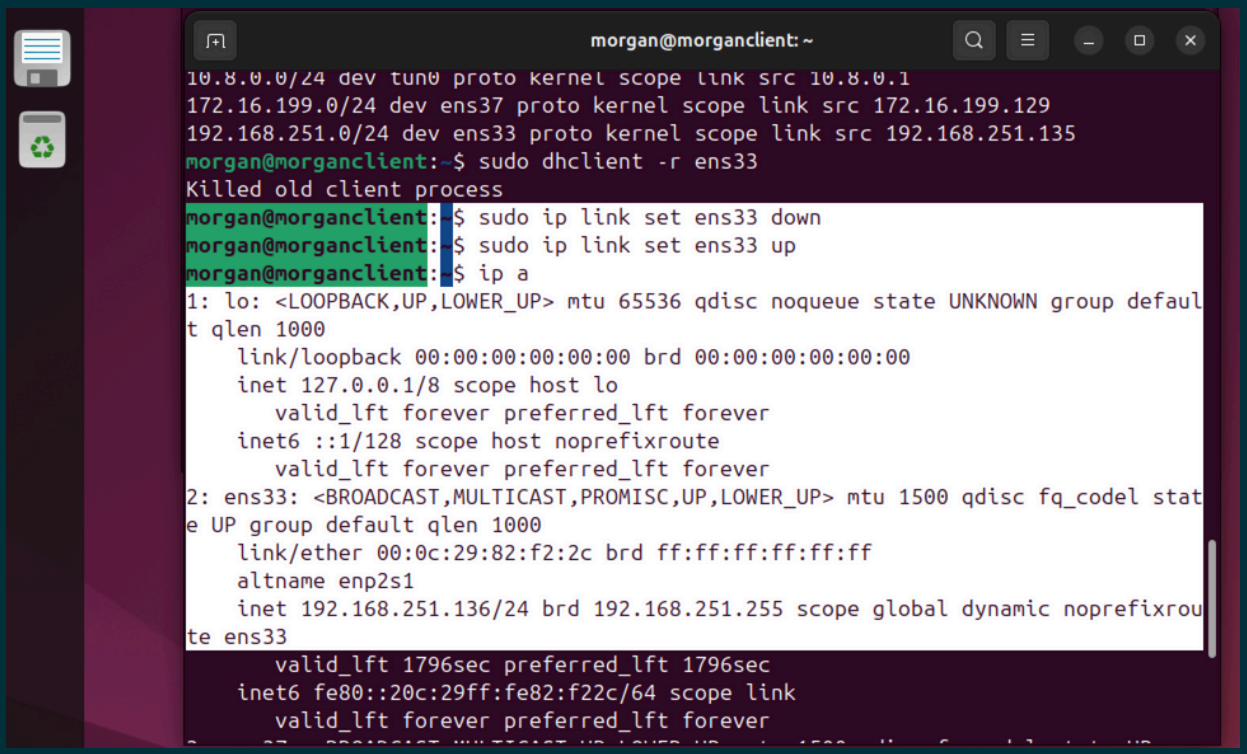
After stopping the DHCP flood attack, the IP addresses that had been held "hostage" by Yersinia were finally released. As a result, my client successfully obtained an IP address: 192.168.251.135.

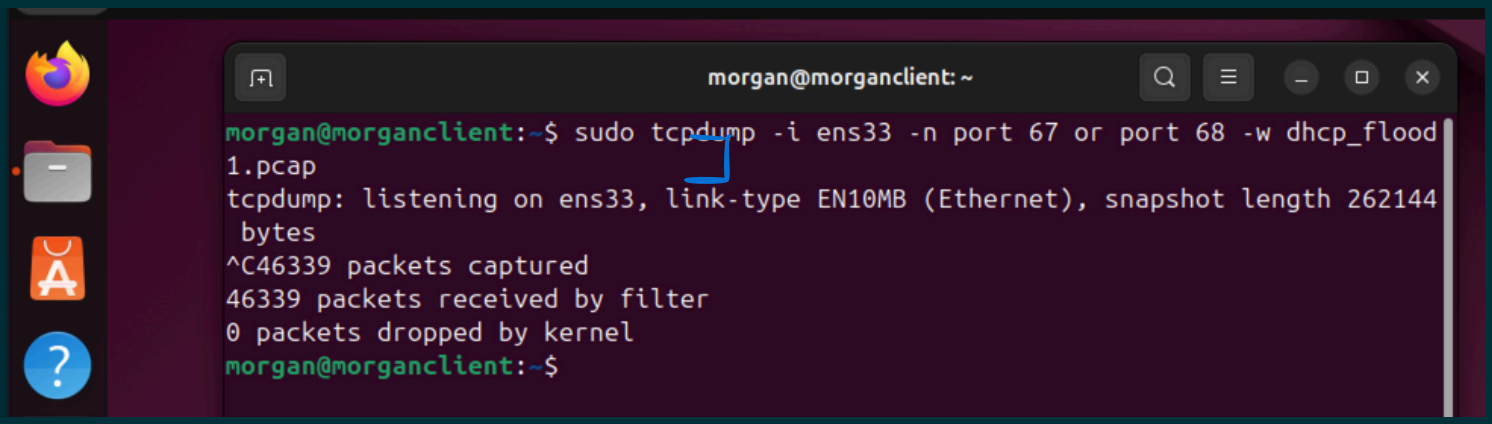
(This IP was dynamically assigned via DHCPv4. If Netplan had been set to static mode, the assignment would have failed unless I ran ‘sudo netplan apply’. Also, every time I bring the ens33 interface down and back up, I have to manually clear the IP address first — otherwise, it won’t refresh properly.)



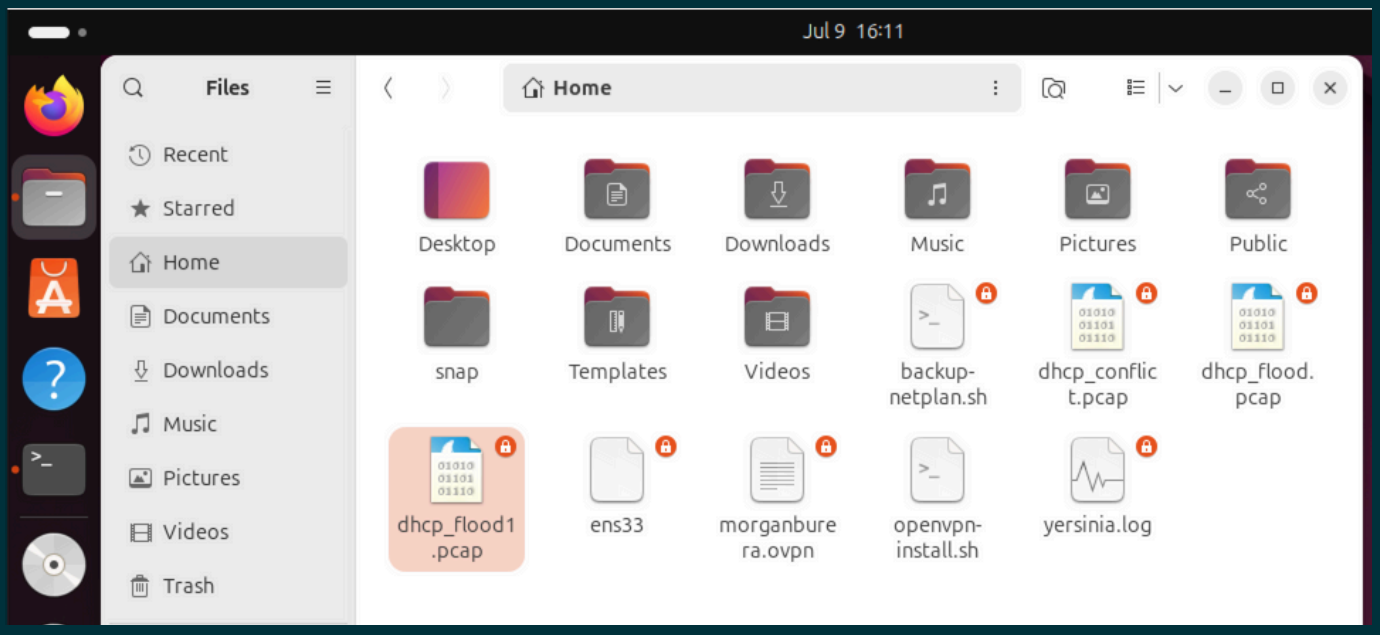
I verified the network interface to see if it was back to a normal state :

- ip a
- ip route

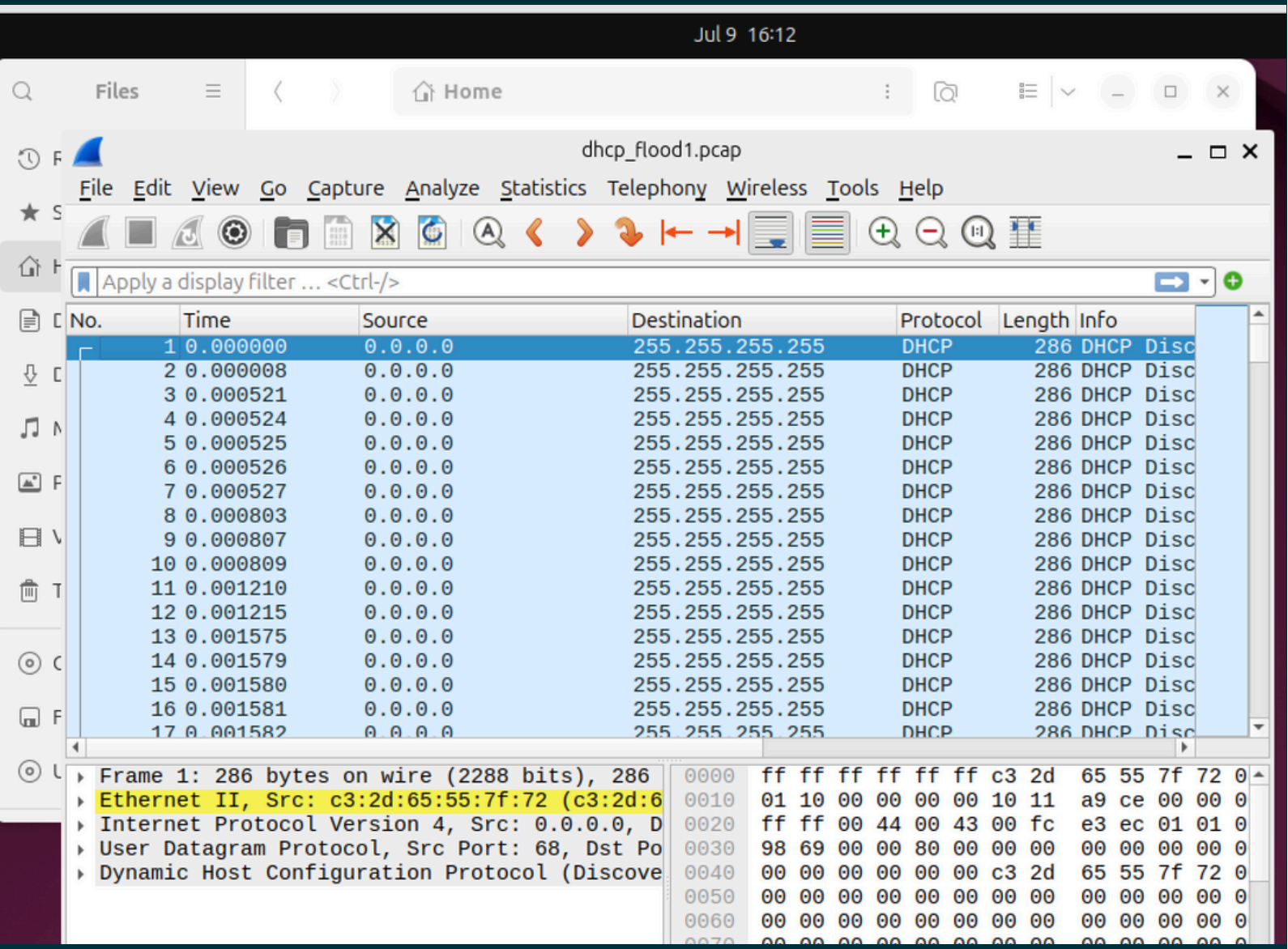




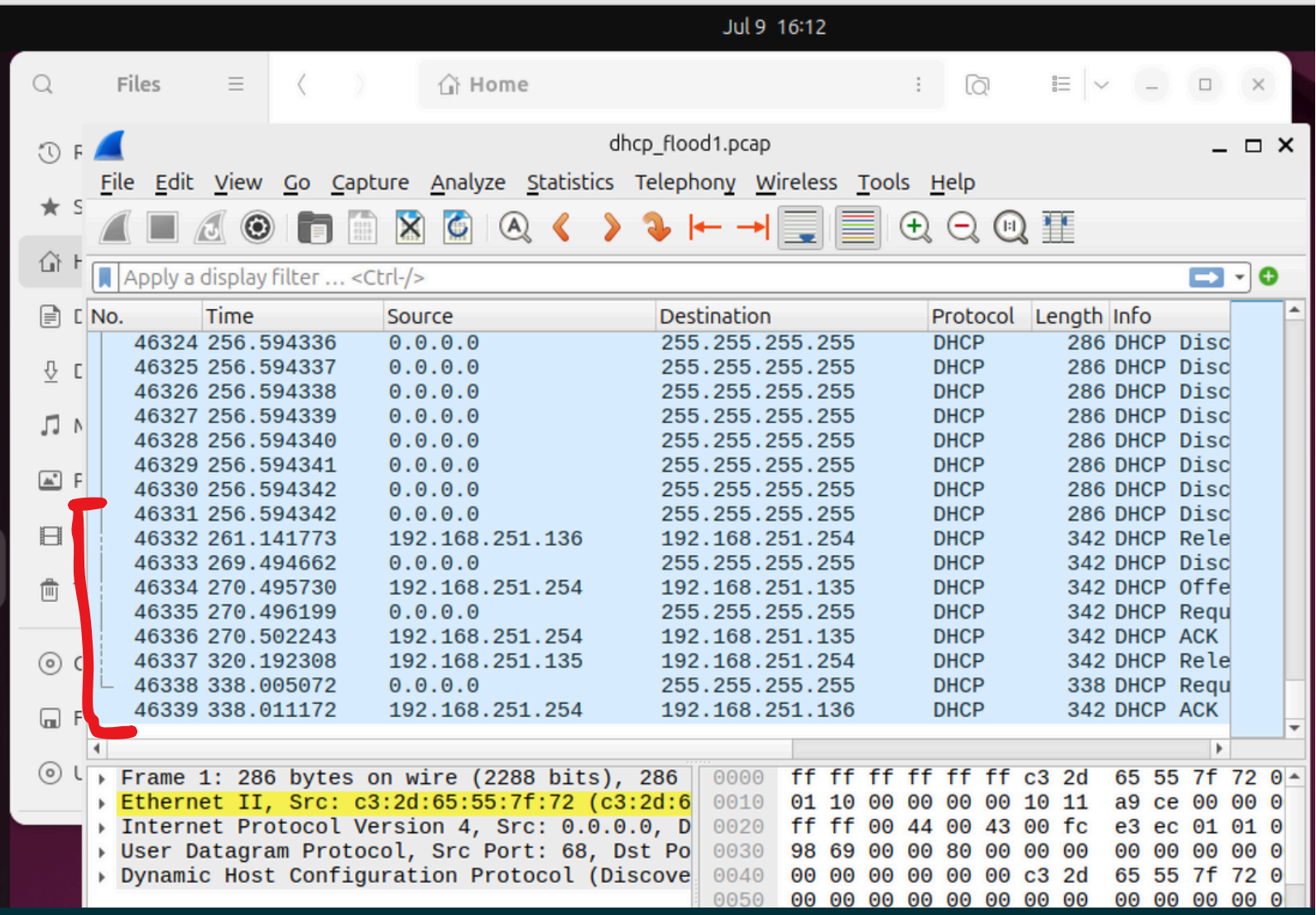
Time to stop the capture, poor machine.



I wanted to inspect the capture from the saved file



We can clearly the interpretation of the DHCP rogue attack numerous attacks (0.0.0.0) overwhelming the server with DHCP Discoveries sent by broadcast.



This is the end of the capture, just after stop Yersinia DHCP attack.We can observe the client was assigned a final IP address : 192.168.251.135.
The communication was terminated by the server's ACK (acknowledgement).

Also The difference in the packet lenght can make us understand that the machine requesting the IP address was different from the last one.

🗝️ Key Takeaways

- DHCP Floods can paralyze a network by exhausting available IP addresses.
- Packet inspection tools (Wireshark, tcpdump) are essential to analyze and verify network behavior during and after an attack.
- Client-side testing on limited hardware (single laptop) is viable but demanding — separating roles across multiple machines improves accuracy and performance.
- Proper interface control (netplan apply, ifdown/ifup, clearing leases) is crucial to reinitialize DHCP communication reliably.