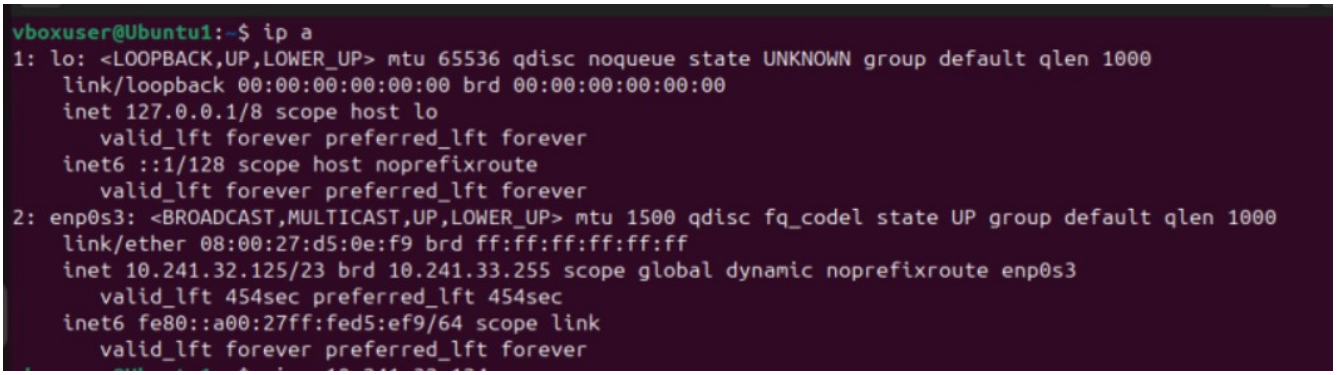
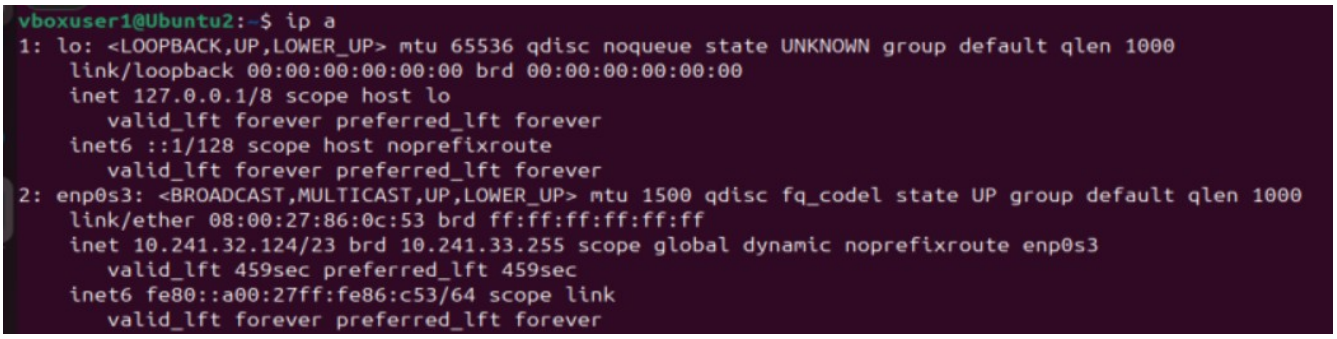
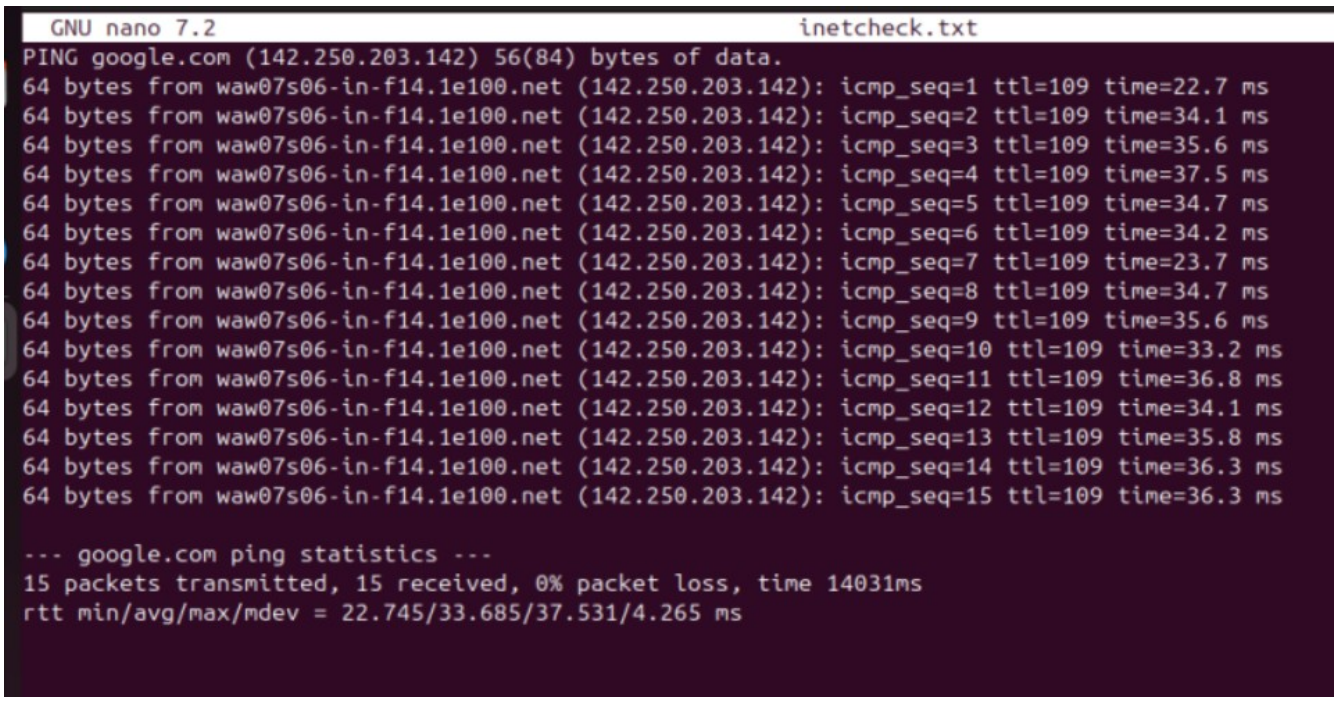
1. Создать сервер t2.micro(Ubuntu), он должен иметь публичный ip и доступ в интернет. Также можно использовать две виртуальные машины (Ubuntu), поднятые на одном компьютере. Либо виртуальную машину и основной компьютер (если ОС твоего основного компьютера Ubuntu). Главное, чтобы два хоста находились в одной сети и имели доступ друг к другу.
   Далее в заданиях будет использована терминология основной хост и удаленный хост. Нет особой разницы какой ты сделаешь основным, главное чтобы далее ты не путался в формулировках.



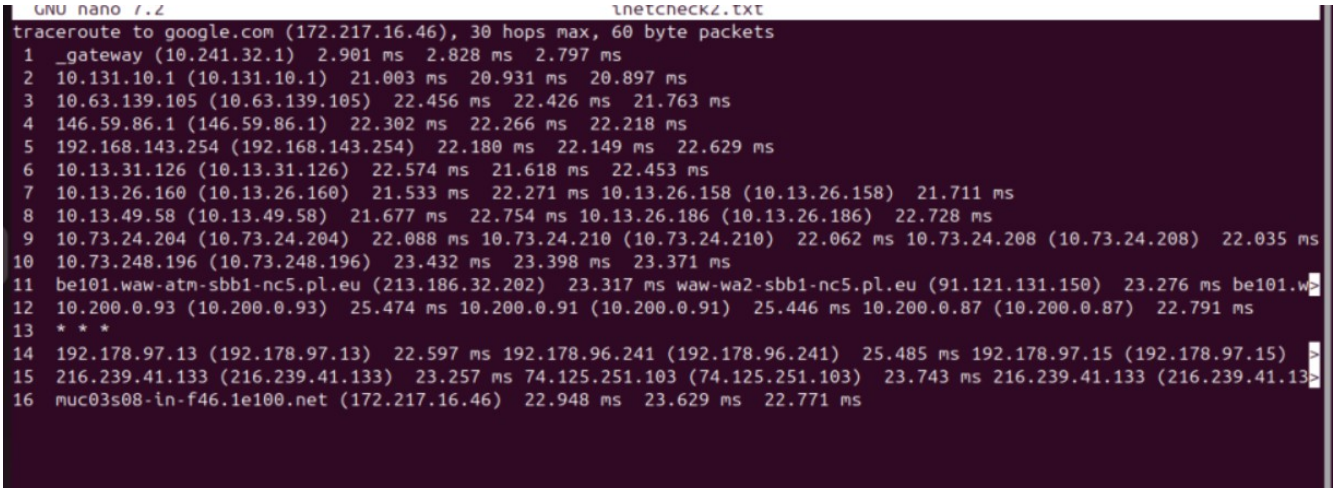


2. Проверь доступность интернета на основном хосте, воспользовавшись командой ping. Для этого нужно пропинговать доверенный адрес в интернете, который точно будет доступен (например, google.com). Запиши вывод в файл.

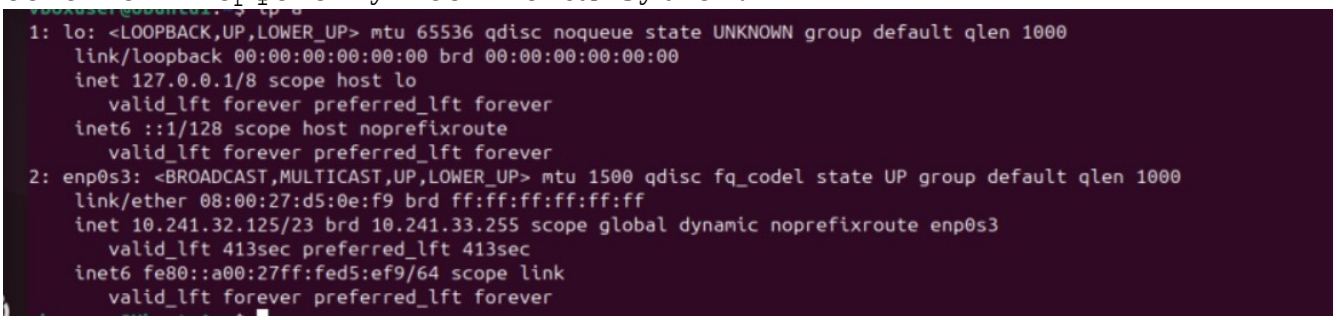


3. Выполни команду traceroute до доверенного адреса в интернете, который точно будет доступен (например, google.com). Изучи вывод команды. Запиши вывод в файл.

```
vboxuser@Ubuntu1:~$ traceroute google.com > inetcheck2.txt
vboxuser@Ubuntu1:~$ sudo nano inetcheck2.txt
```

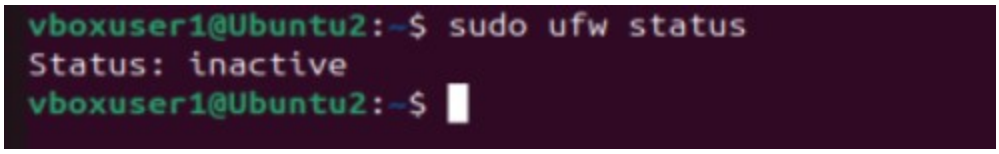


4. Узнай IP-адрес основного и удаленного хостов. Посмотри какие сетевые интерфейсы у тебя используются.

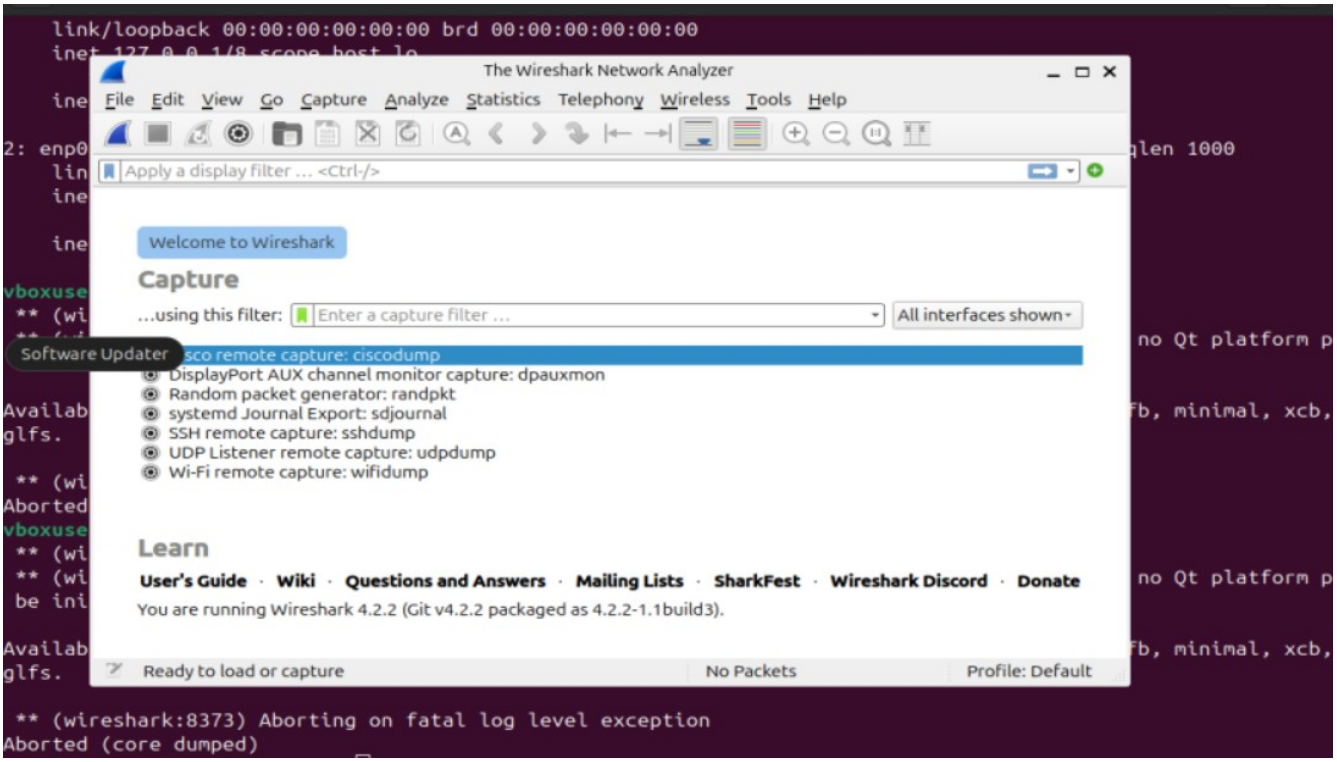


Enp0s3 и lo

5. Проверь статус межсетевого экрана на удаленном хосте. Используй команду “sudo ufw status”. В случае если он включен, отключи его.



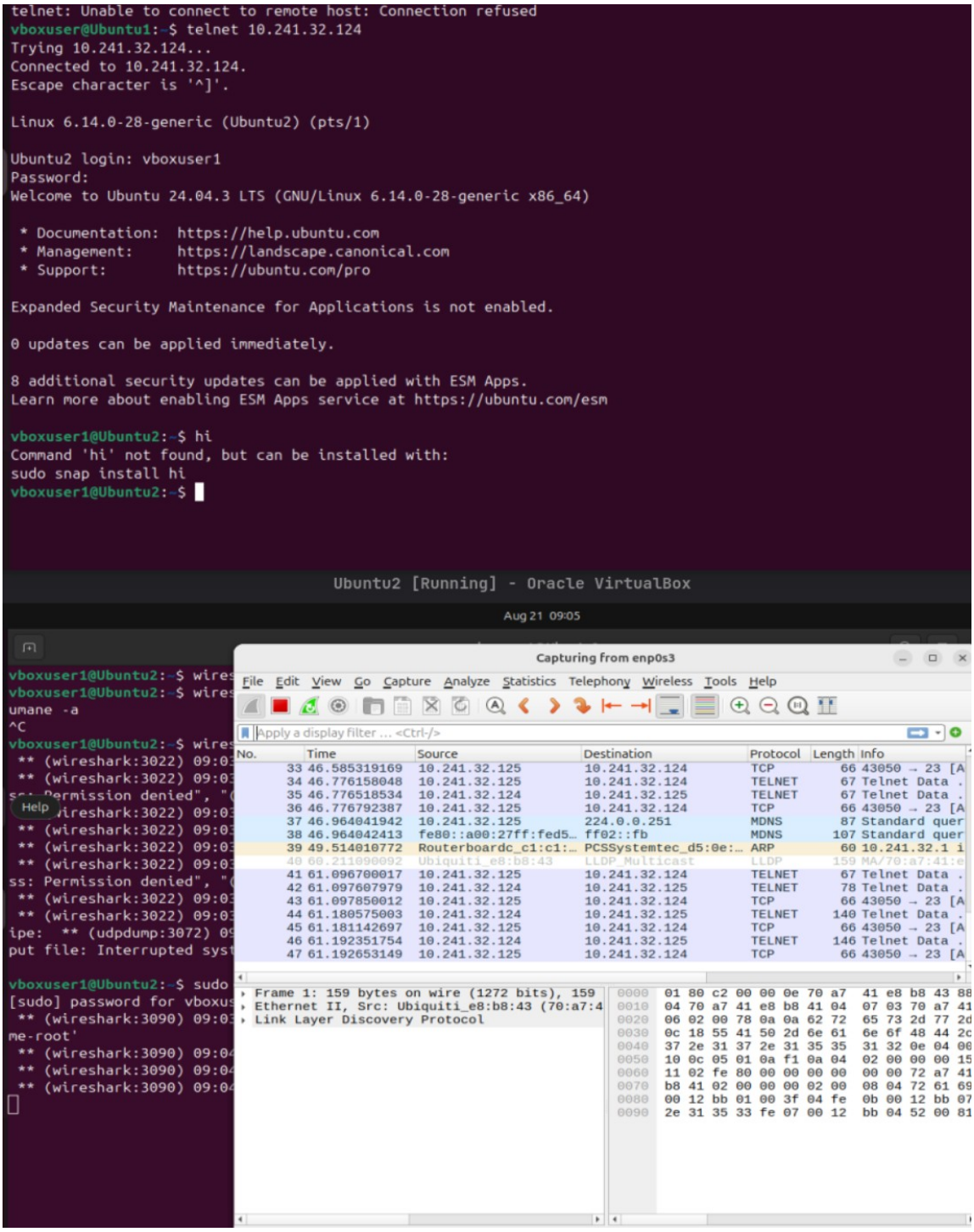
6. Установи себе на основной хост wireshark. Запусти его, ознакомься с интерфейсом.



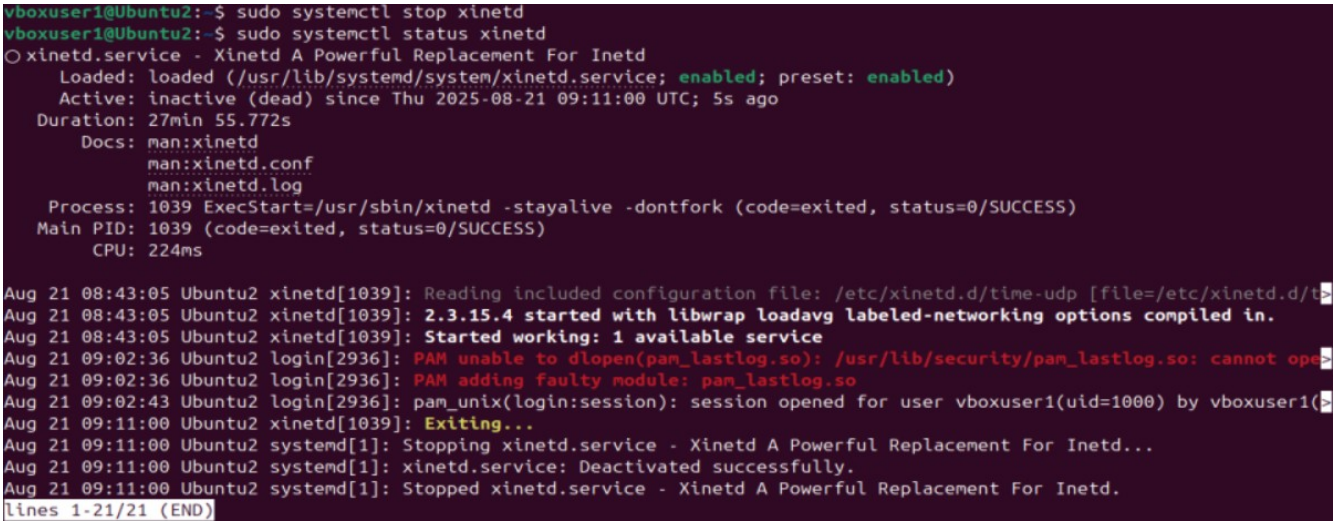
7. Установи на удаленный хост telnet и подключись по telnet с основного к локальному хосту (в случае с AWS тебе необходимо будет создать нового юзера на удаленном хосте под кредами которого ты будешь подключаться).

```
root@Ubuntu1:~# telnet 10.241.32.124
Trying 10.241.32.124...
Connected to 10.241.32.124.
Escape character is '^]'.

Linux 6.14.0-28-generic (Ubuntu2) (pts/3)

Ubuntu2 login: vboxuser
Login timed out after 60 seconds.
Connection closed by foreign host.
root@Ubuntu1:~# telnet 10.241.32.124
Trying 10.241.32.124...
Connected to 10.241.32.124.
Escape character is '^]'.

Linux 6.14.0-28-generic (Ubuntu2) (pts/3)

Ubuntu2 login: vboxuser
Password:

Login incorrect
Ubuntu2 login: vboxuser1
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.
```

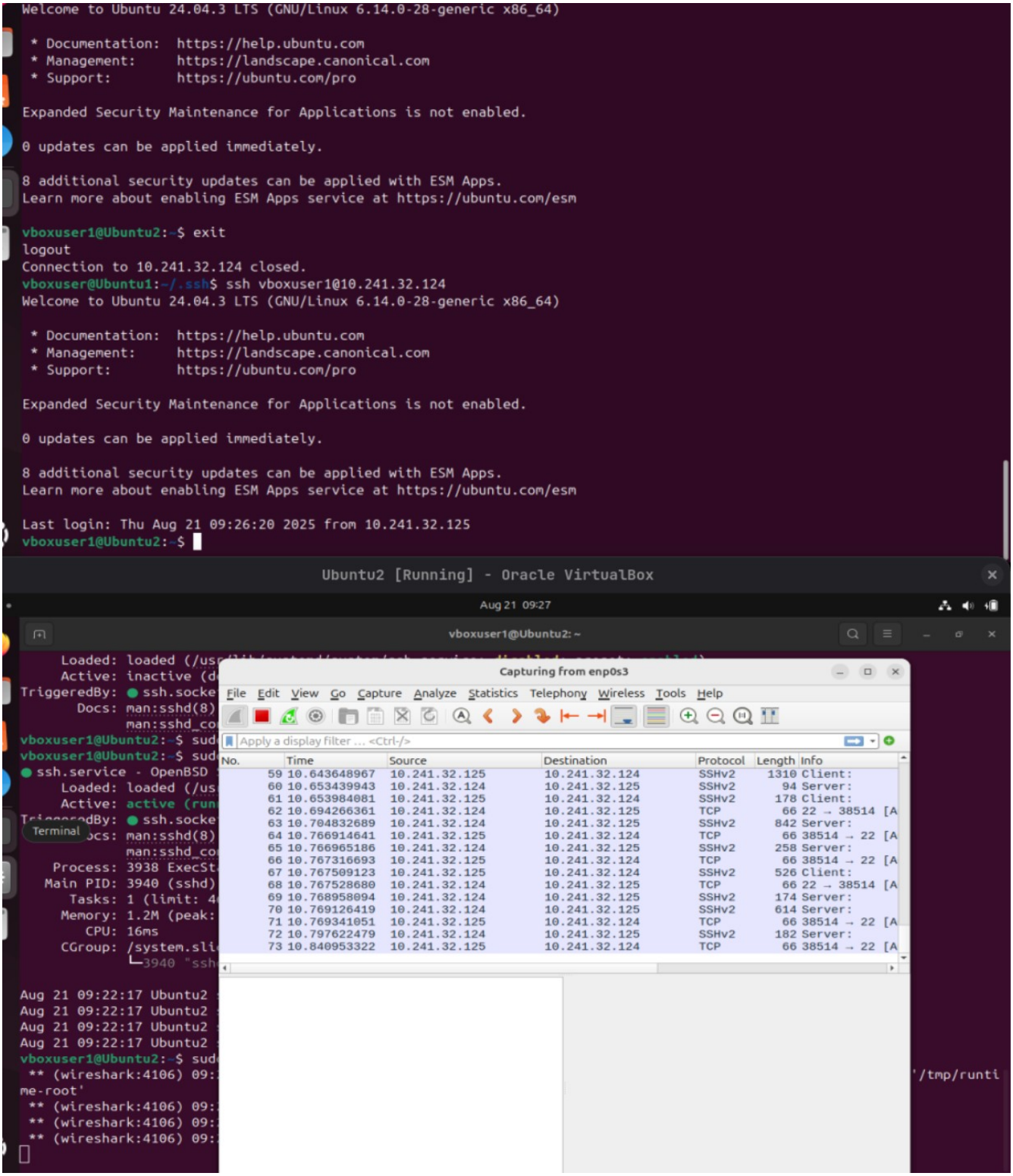
8.Запусти Wireshark на основном хосте. При запущенном Wireshark введи команду “umane -a” в терминале с открытой telnet сессией. Отыщи информацию передаваемую по telnet протоколу в wireshark. Проанализируй что ты видишь.



9.Выключи или удали telnet на удаленном хосте.

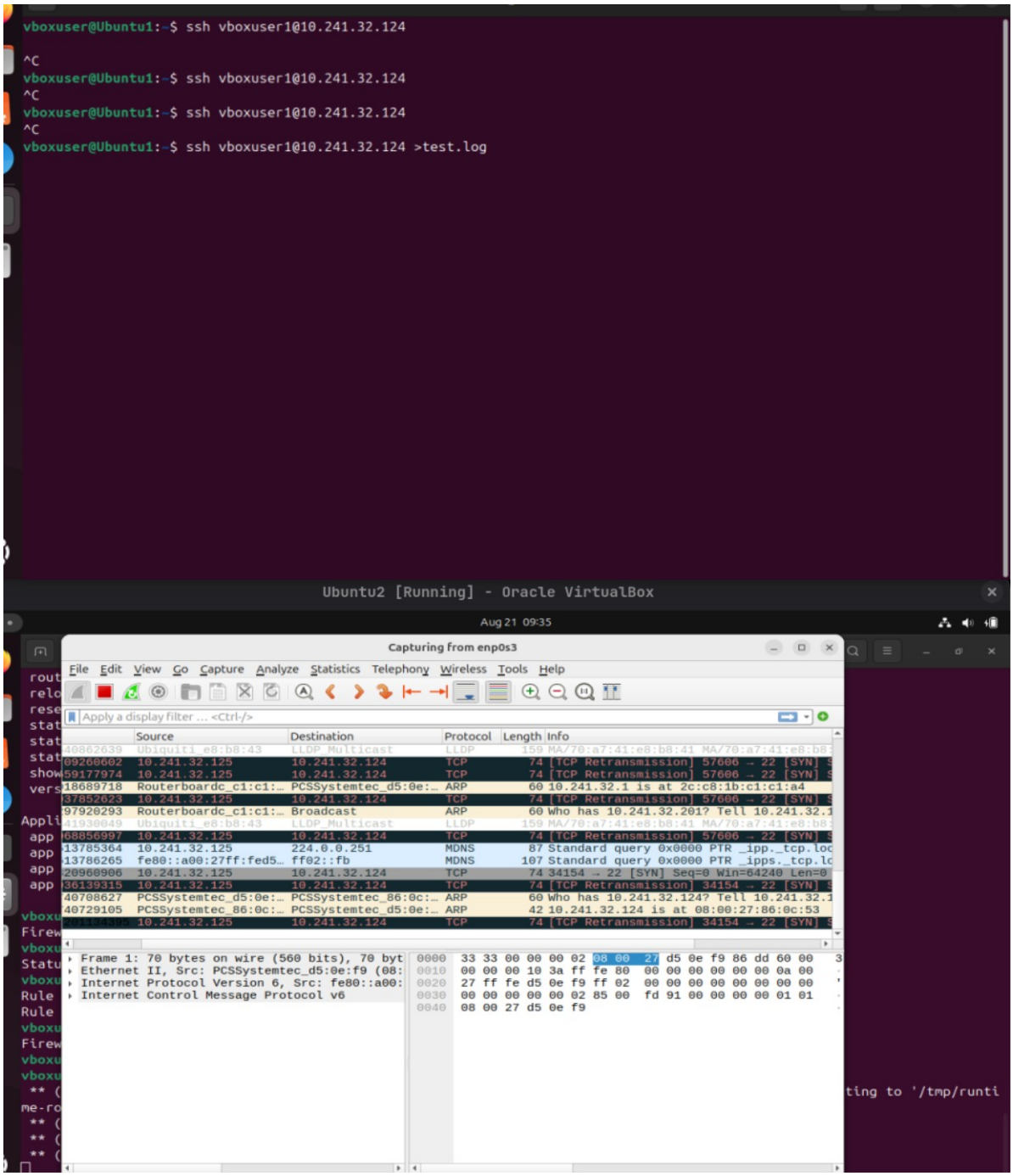


10.Далее повтори то же самое, однако для подключения к удаленному хосту используя ssh. Сравни результаты анализа. Запиши свои выводы (логические выводы) в файл.

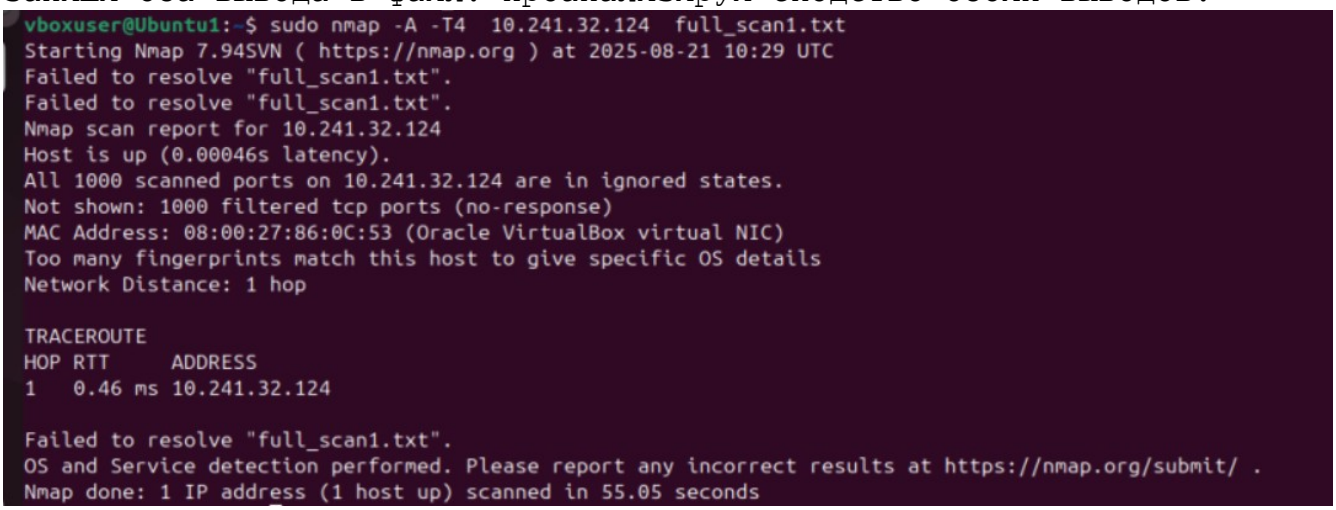


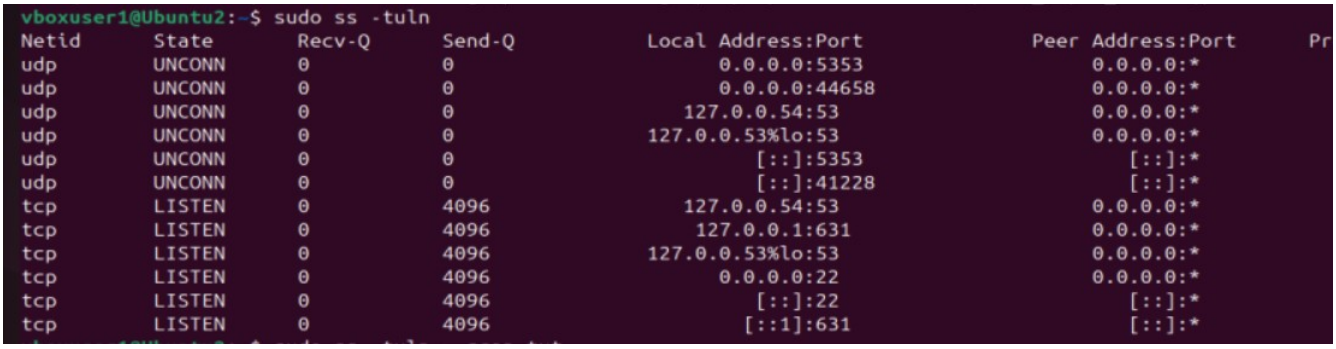
Поменялся протокол передачи данных и роляет то что ssh передает encrypted packet что является более безопасным способом подключения не в локальной сети и убирает возможность перехватить наш трафик как в telnet

11. Включи ufw и настрой запрет на подключение по 22 порту на удаленном хосте. Попробуй подключиться с основного хоста к удаленному по ssh.



12. Скачай nmap на основной хост и сделай полное сканирование удаленного хоста. На удаленном хосте введи команду “sudo ss -tuln”. Запиши оба вывода в файл. Проанализируй сходство обоих выводов.





Ss проверяет изнутри сокеты а nmap работает как внешний клиент который подключается к хосту