Оглавление

Тема и цель работы

Тема лабораторной работы: «Настройка Telnet и SSH. Перехват трафика средствами Wireshark».

Цель работы: Научиться устанавливать, проводить удаленное подключение по ssh и telnet, следить за трафиком через wireshark

Вариант №25

Оборудование, ПО

Таблица 1 – Оборудование, ПО.

Устройство	Операционная система	IP адрес/Маска	Шлюз	DNS
CLI_A1	Astra Linux SE 1.8.x	10.0.25.10/24	-	-
CLI_A2	Astra Linux SE 1.8.x	10.0.25.20/24	-	-

Ход лабораторной работы

1.Для того, чтобы обеспечить машинам доступ в Интернет, необходимо включить второй адаптер с типом подключения «NAT».

Перейти в настройки VirtualBox (см. рис. 1)

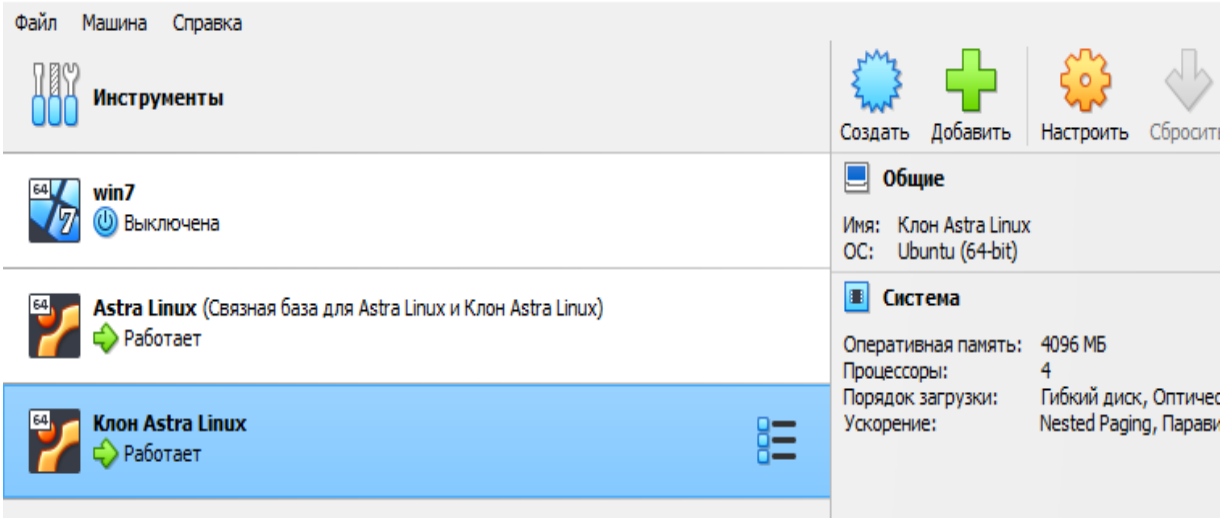

Рисунок 1 – Интерфейс VIrtualBox

На вкладке «Сеть» включить адаптер 2 и настроить его на тип подключения «NAT» (см. рис. 2).

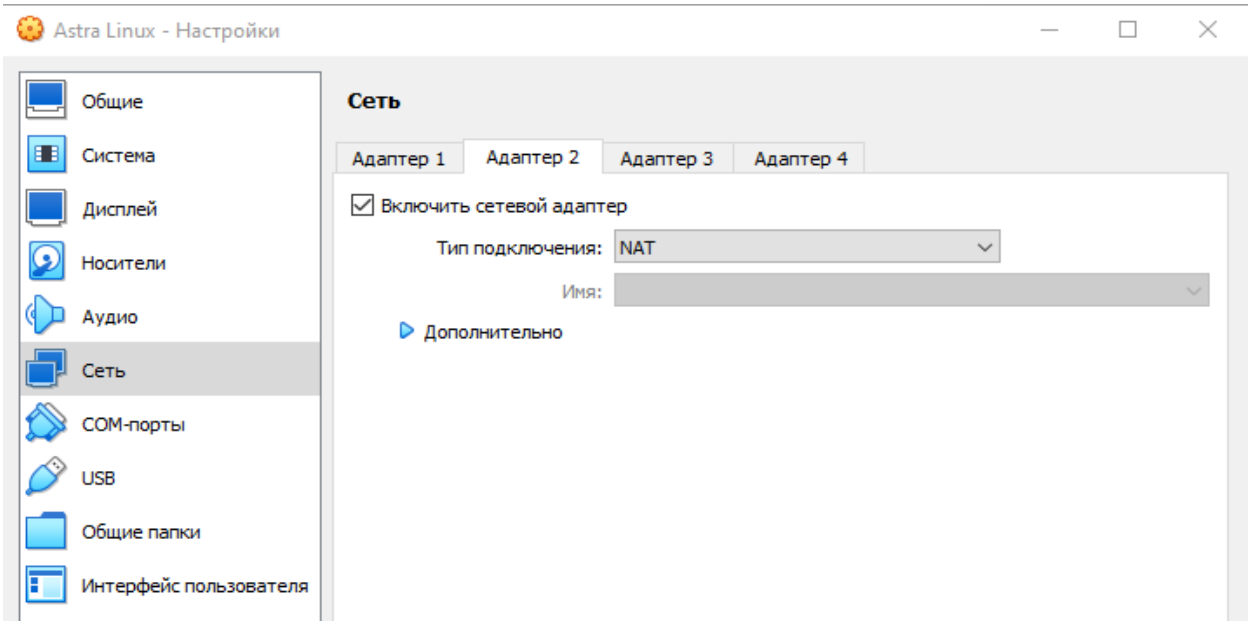

Рисунок 2 – Вкладка «Сеть»

2. Отредактировать etc/network/interfaces (см. рис. 3) .

Рисунок 3 – открытие редактора Vim

Добавить данные строки (см. рис. 4).

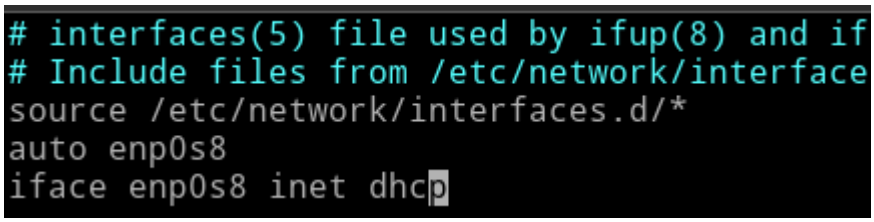

Рисунок 4 – строки добавленные в файл

3. Установить сетевую утилиту Telnet.

Изменить файл etc/apt/sources.list (см. рис. 5).

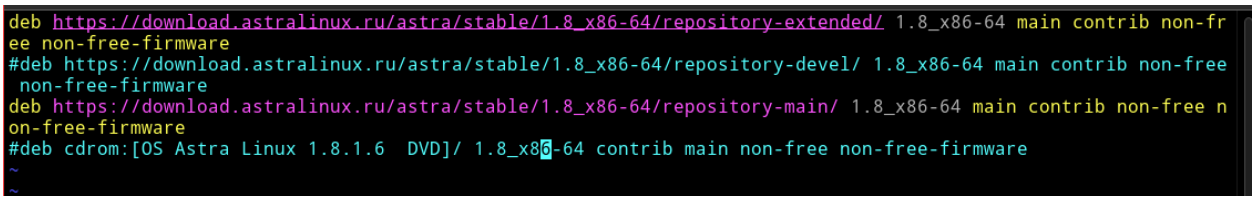

Рисунок 5 – etc/apt/sources.lost

Для установки telnet ввести данные команды:

apt-get update

apt-get install xinetd telnet telnetd

4. Настроить telnet.

Создать файл /etc/xinetd.d/telnet и добавить следующие строки. (см. рис. 6).

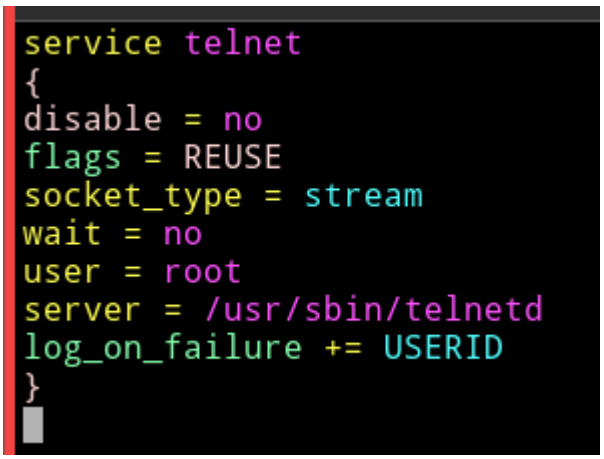

Рисунок 6 – etc/xinetd.d/telnet

Перезагрузить сервис telnet командой **systemctl restart xinetd** и проверить его работоспособность командой **telnet localhost** (см. рис. 7).

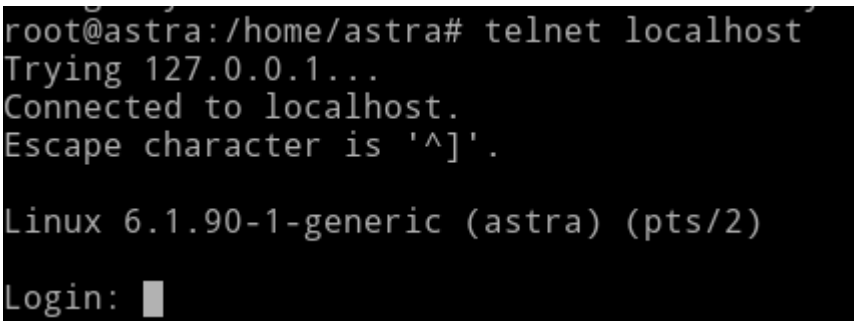

Рисунок 7 – проверка работоспособности telnet

5. Настройка и подключение SSH.

Установить пакет ssh командой **`apt-get install ssh`** (см. рис. 8).

```
root@astra:/home/astra# apt-get install ssh
Чтение списков пакетов… Готово
Построение дерева зависимостей… Готово
Чтение информации о состоянии… Готово
Будут установлены следующие дополнительные пакеты:
  openssh-client openssh-server openssh-sftp-server
Предлагаемые пакеты:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
Следующие НОВЫЕ пакеты будут установлены:
  openssh-server openssh-sftp-server ssh
Следующие пакеты будут обновлены:
  openssh-client
Обновлено 1 пакетов, установлено 3 новых пакетов, для удаления отмечено 0 пакетов, и 564 пакетов не обновлено.
Необходимо скачать 1 998 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 2 444 kB.
Хотите продолжить? [Д/н] y
```

Рисунок 8 – установка SSH

Запустить службу SSH и добавить ее в автозагрузку командами:

`systemctl start ssh`

`systemctl enable ssh`

Проверить службу ssh командой **`systemctl status ssh`** (см. рис. 9).

```
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Thu 2024-10-24 00:23:34 MSK; 3min 48s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 16332 (sshd)
      Tasks: 1 (limit: 4599)
     Memory: 1.6M
        CPU: 32ms
     CGroup: /system.slice/ssh.service
             └─16332 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

окт 24 00:23:34 astra systemd[1]: Starting ssh.service - OpenBSD Secure Shell server.
окт 24 00:23:34 astra sshd[16332]: Server listening on 0.0.0.0 port 22.
окт 24 00:23:34 astra sshd[16332]: Server listening on :: port 22.
окт 24 00:23:34 astra systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
~
```

Рисунок 9 – вывод команды systemctl status ssh

Создать ssh ключ командой **ssh-keygen** (см. рис. 10).

```
root@astra:/home/astra/Desktop# ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519): 123321
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in 123321
Your public key has been saved in 123321.pub
The key fingerprint is:
SHA256:uSaSrq/NN+NopSqbj7Kir9o6x1rVzLhsCGd5sGb+5Ro root@astra
The key's randomart image is:
+--[ED25519 256]--+
|                 |
|                 |
|   .             |
|    + =   .      |
|. B + + S        |
| B = o.  .       |
| .+ Eoo o        |
|==o*o*+o         |
|/%B*O+oo         |
+----[SHA256]-----+
```

Рисунок 10 – ключ SSH

Скопировать ключ на вторую машину командой **ssh-copy-id astra@10.0.25.10** (см. рис. 11).

```
root@astra:/home/astra# ssh-copy-id astra@10.0.25.20
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_ed25519.pub"
The authenticity of host '10.0.25.20 (10.0.25.20)' can't be established.
ED25519 key fingerprint is SHA256:/GRHhIUExXVhS8dazjgYx8iBv6BlmTqo5nUGIGpi63g.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'astra@10.0.25.20'"
and check to make sure that only the key(s) you wanted were added.
```

Рисунок 11 – копирование ключа на вторую машину

Подключиться к второй машине командой **ssh astra@10.0.25.20** (см. рис. 12).

```
root@astra:/home/astra# ssh astra@10.0.25.20
Last login: Thu Nov 28 12:51:41 2024
astra@astra-2:~$
```

Рисунок 12 – подключение к второй машине

Создать файл командой **touch** и отключиться от машины командой **exit** (см. рис. 13).

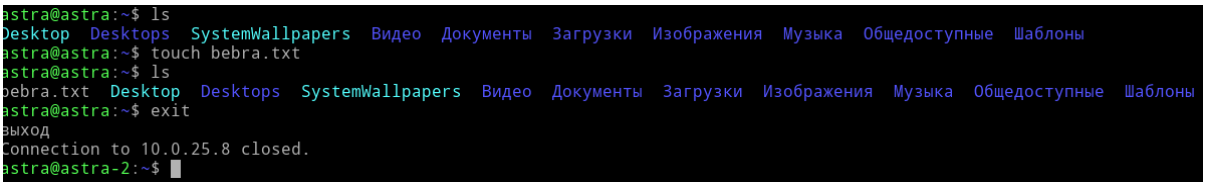

Рисунок 13 – создание файла и отключение

Открыть вторую машину и проверить наличие данного файла (см. рис. 14)

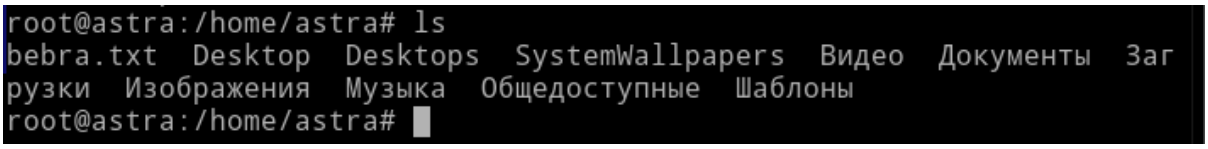

Рисунок 14 – созданный файл присутствует

6. Установить и использовать сетевой анализатор wireshark.

Установить пакет командой **apt-get install wireshark** (см. рис. 15).

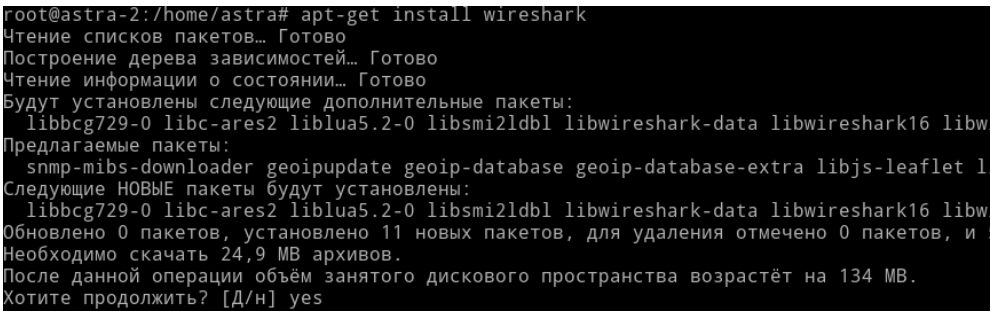

Рисунок 15 – установка пакета

Во время установки синем окне нажать <Да> (см. рис. 16).

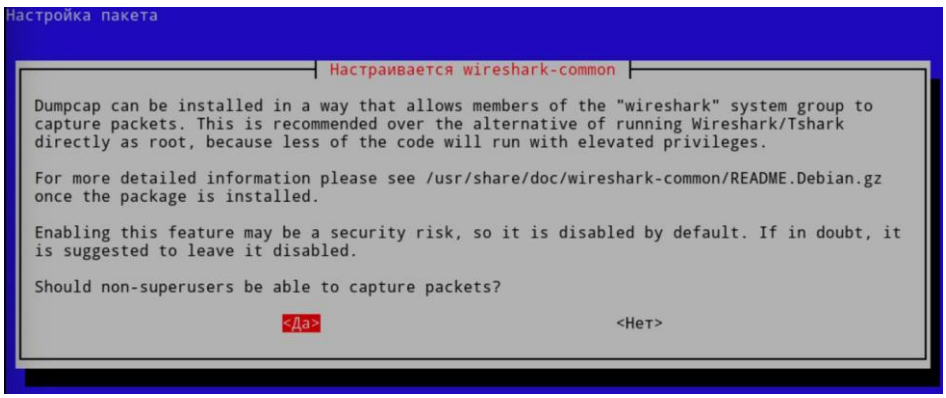

Рисунок 16 – настройка wireshark-common

Выдать права на выполнение командой **`chmod +x /usr/bin/dumpcap`** и открыть утилиту командой **`wireshark`** (см. рис. 17).

```
root@astra-2:/home/astra# chmod +x ../../usr/bin/dumpcap
root@astra-2:/home/astra# wireshark
 ** (wireshark:5914) 22:39:37.237377 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
^C
```

Рисунок 17 – выдача прав доступа и открытие утилиты

В интерфейсе утилиты wireshark выберем интерфейс enp0s3 для анализа (см. рис. 18).

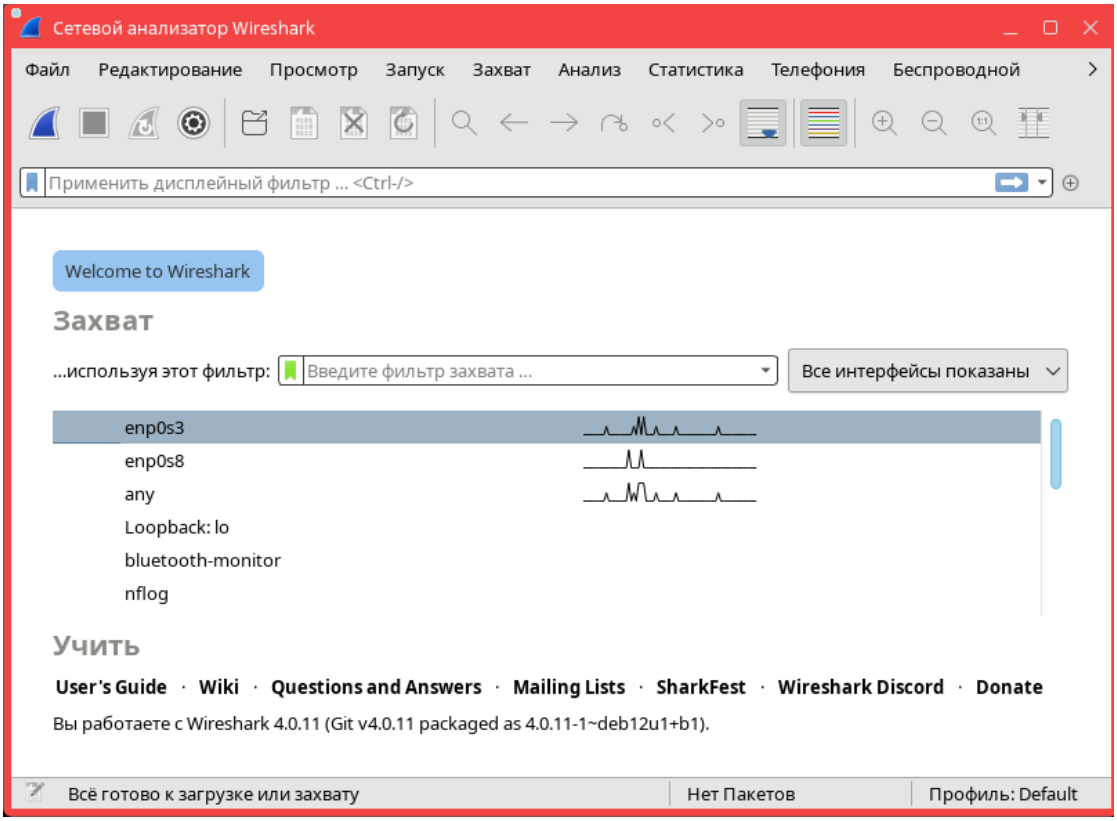

Рисунок 18 – интерфейс команды wireshark

Пингануть вторую машину (см. рис. 19).

```
astra@astra-2:~$ ping 10.0.25.20
PING 10.0.25.20 (10.0.25.20) 56(84) bytes of data.
64 bytes from 10.0.25.20: icmp_seq=1 ttl=64 time=0.036 ms
64 bytes from 10.0.25.20: icmp_seq=2 ttl=64 time=0.330 ms
64 bytes from 10.0.25.20: icmp_seq=3 ttl=64 time=0.100 ms
64 bytes from 10.0.25.20: icmp_seq=4 ttl=64 time=0.090 ms
64 bytes from 10.0.25.20: icmp_seq=5 ttl=64 time=0.056 ms
```

Рисунок 19 – проверка связности с второй машиной

Wireshark увидел передачу пакетов (см. рис. 20).

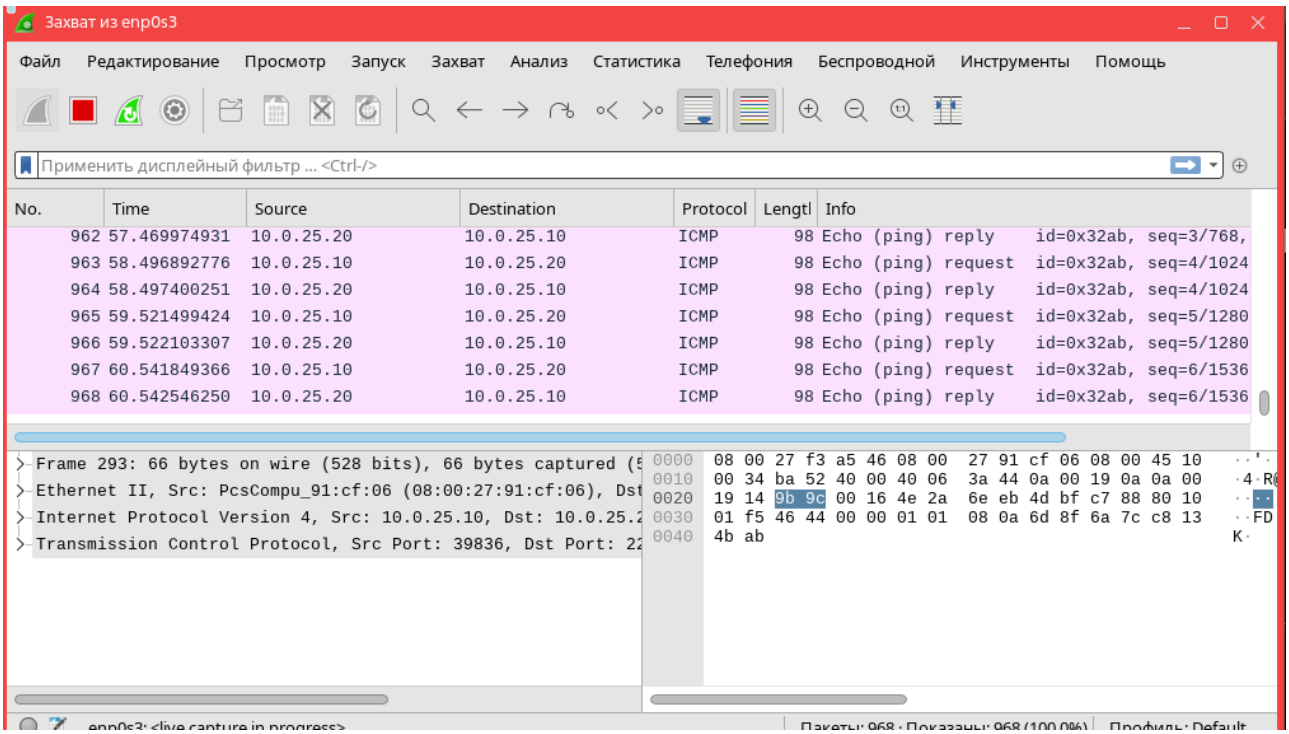

Рисунок 20 – wireshark показывает лог интерфейса.

Вывод

В ходе выполнения описанных шагов была успешно настроена сеть для виртуальных машин, обеспечив их доступ в Интернет через NAT. После конфигурации сетевого адаптера и редактирования файла etc/network/interfaces, была установлена утилита Telnet, что позволило осуществлять удалённое управление. Настройка Telnet и запуск соответствующего сервиса подтвердили его работоспособность. Также была установлена служба SSH, что обеспечило более безопасный способ подключения к удалённым машинам, включая создание и копирование SSH-ключа. В заключение, установка сетевого анализатора Wireshark позволила проанализировать сетевой трафик и убедиться в успешной связи между виртуальными машинами. Все действия подтвердили корректность настройки сети и функциональность инструментов для удалённого доступа и анализа трафика.

Контрольные вопросы

1. Для чего используется telnet?

Telnet используется для удалённого управления устройствами и серверами через текстовый интерфейс, позволяя пользователям выполнять команды на удалённых системах.

2. Для чего используется ssh?

SSH (Secure Shell) используется для безопасного удалённого доступа к устройствам и серверам, обеспечивая шифрование данных и аутентификацию, что делает его более защищённым по сравнению с Telnet.

3. Для чего используется wireshark?

Wireshark используется для анализа сетевого трафика, позволяя захватывать и просматривать пакеты данных, что помогает в диагностике проблем сети и мониторинге её активности.