МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра информатики и систем управления

# ОТЧЕТ

по лабораторной работе №3

по дисциплине

Сети и телекоммуникации

РУКОВОДИТЕЛЬ:

_____ Гай В.Е.
(подпись) (фамилия, и.,о.)

СТУДЕНТ:

_____ Береснева М.А.
(подпись) (фамилия, и.,о.)

18-АС
(шифр группы)

Работа защищена «___» _____

С оценкой _____

Нижний Новгород 2020

## Задание

Для экспериментов использовать схему из первой лабораторной работы. Все ip-адреса (или маски) необходимо поменять так, чтобы адрес сети у всех компьютеров был один. Все действия должны быть выполнены в симуляторе сетей CORE.

## Часть 1. Формирование запроса и получение ответа

1. Начать захват пакетов при помощи WireShark.

2. Сформировать кадр ARP-запроса с помощью утилиты PackETH и отправить его в сеть (компьютеры выбрать самостоятельно).

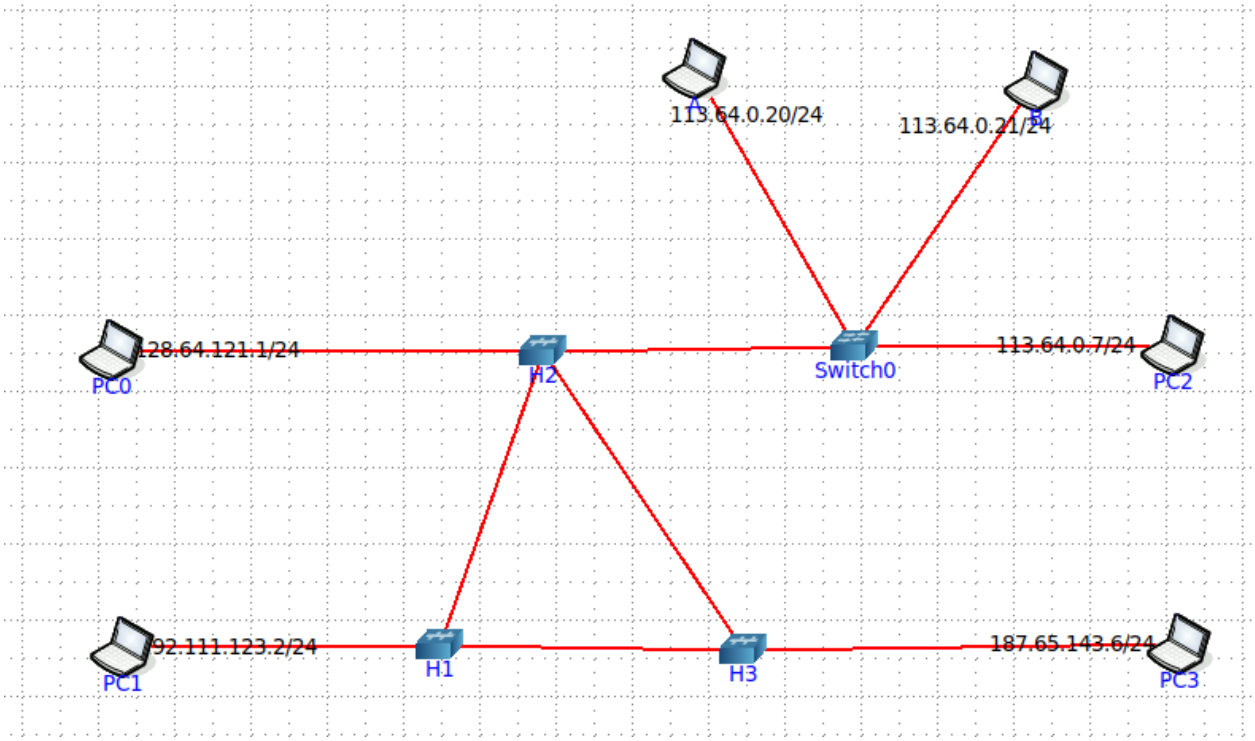
3. Убедиться, что был получен кадр ARP-ответа, соответствующий посланному запросу. Захваченные пакеты сохранить для отчета. Вывести arp таблицу (команда «arp»).

4. Прекратить захват пакетов.

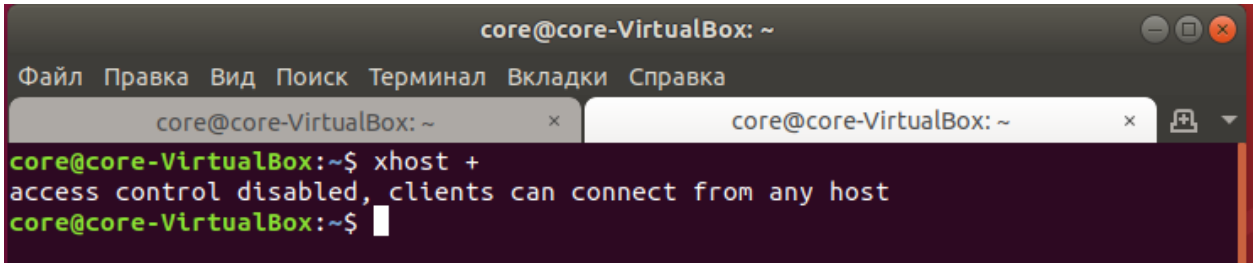
## Часть 2. ARP-спуфинг

1. Выделить на схеме и обозначить три компьютера: A, B, Сервер.

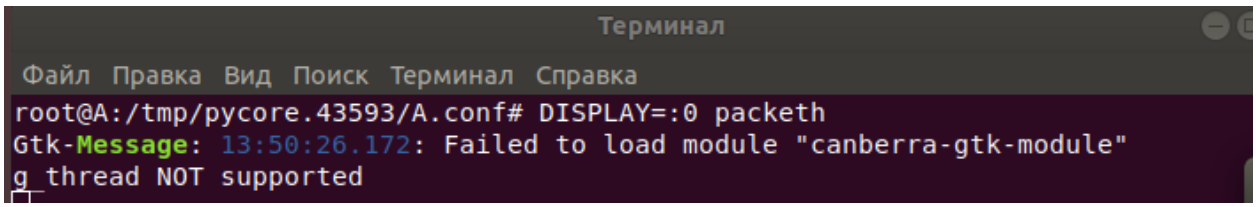
2. Подготовить кадр ARP-ответа, направляемый Сервером хосту A с помощью программы PackETH. Кадр должен быть составлен так, чтобы MAC-адресу Сервера соответствовал IP-адрес хоста B. Вывести arp таблицу на хосте A. Отправить сформированный пакет от Сервера хосту A.

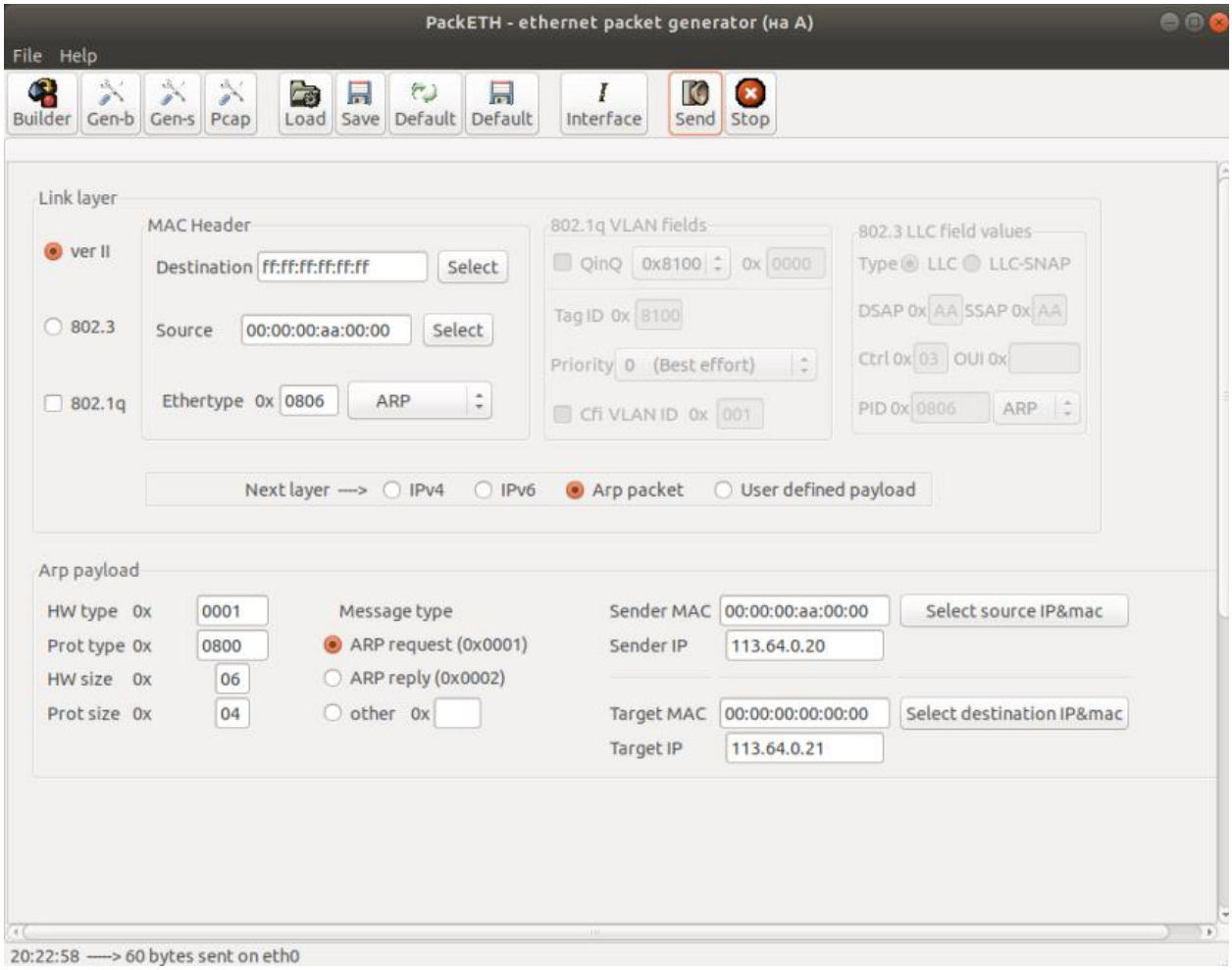



К серверу могут подключаться любые компьютеры




На компьютере A запускаем PackETH






Destination – широковещательный MAC-адрес

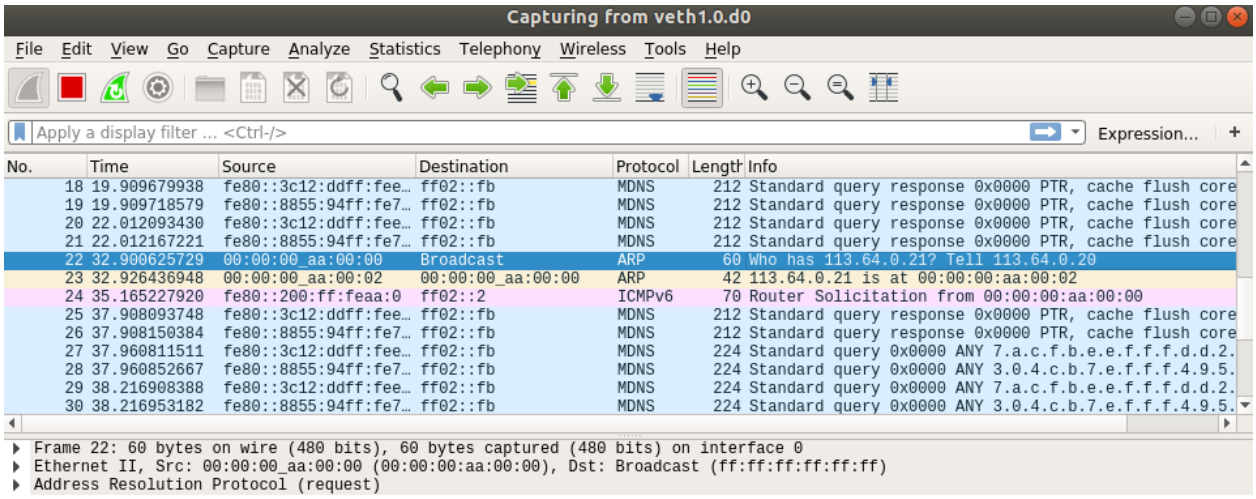
Source – MAC-адрес компьютера A (с помощью ifconfig)

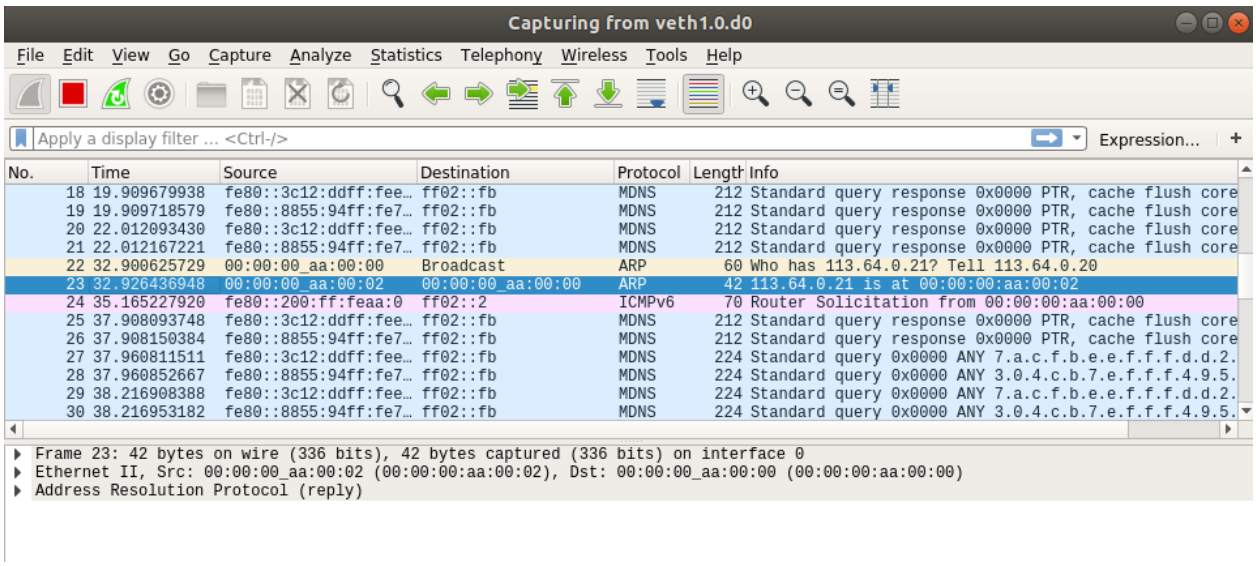
Sender MAC – MAC-адрес компьютера A

Sender IP – IP компьютера A

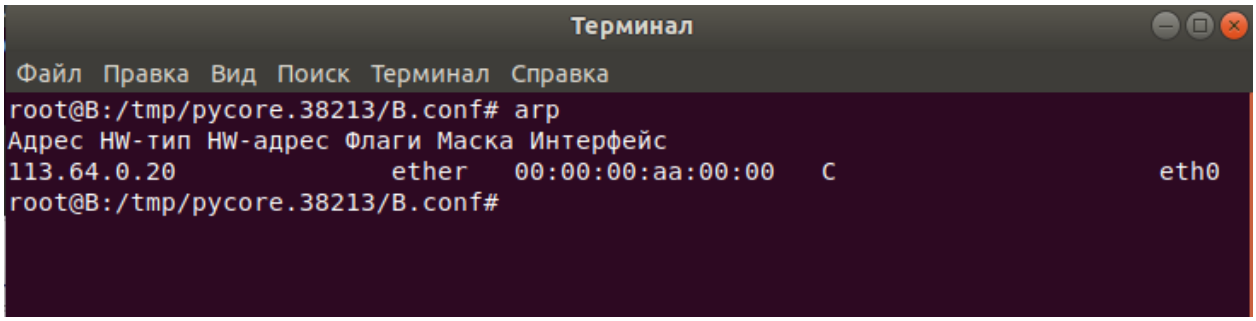
Target IP - IP компьютера B

Запускаем Wireshark и видим, что компьютер A посылает запрос и получает ответ.



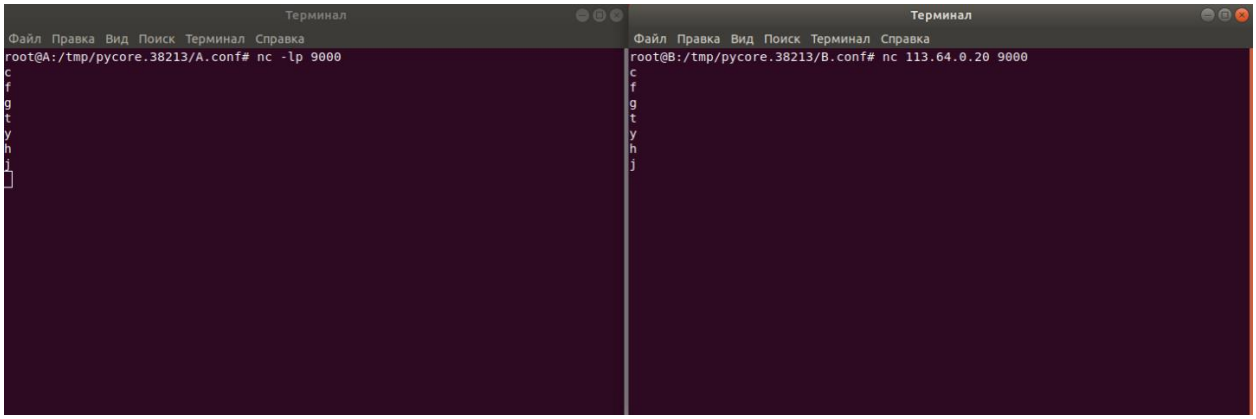



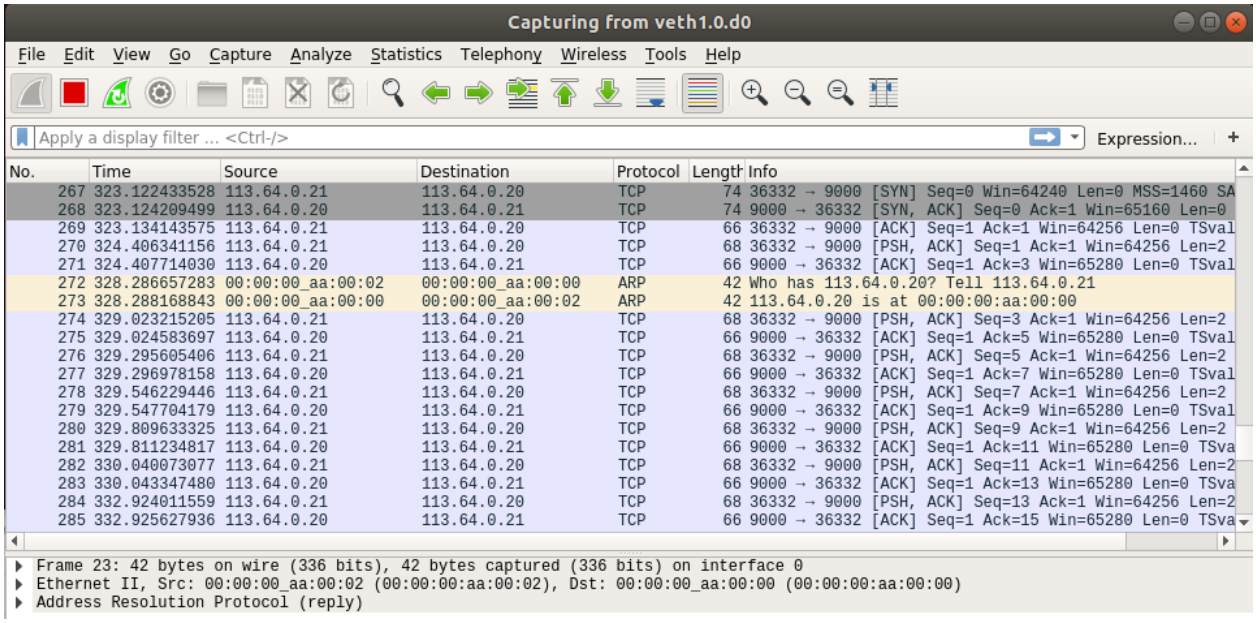

Смотрим arp-таблицу на B и видим, что в ней находится MAC-адрес компьютера A.



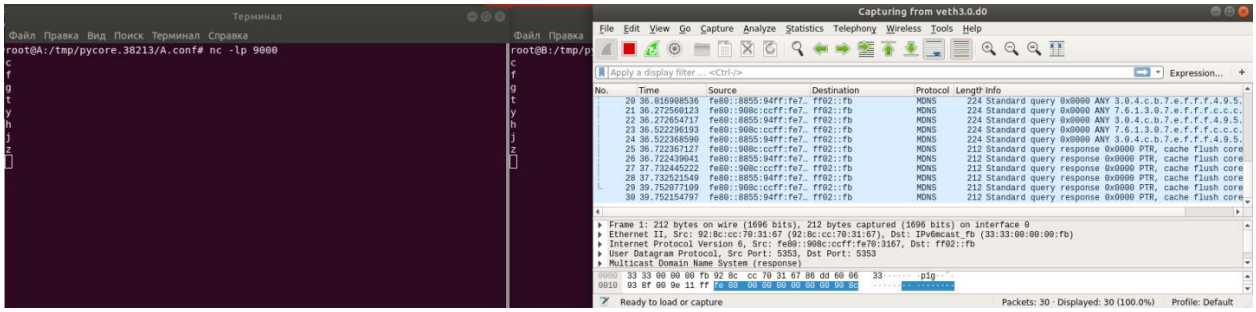

В консоли компьютера A “nc -lp 9000”.

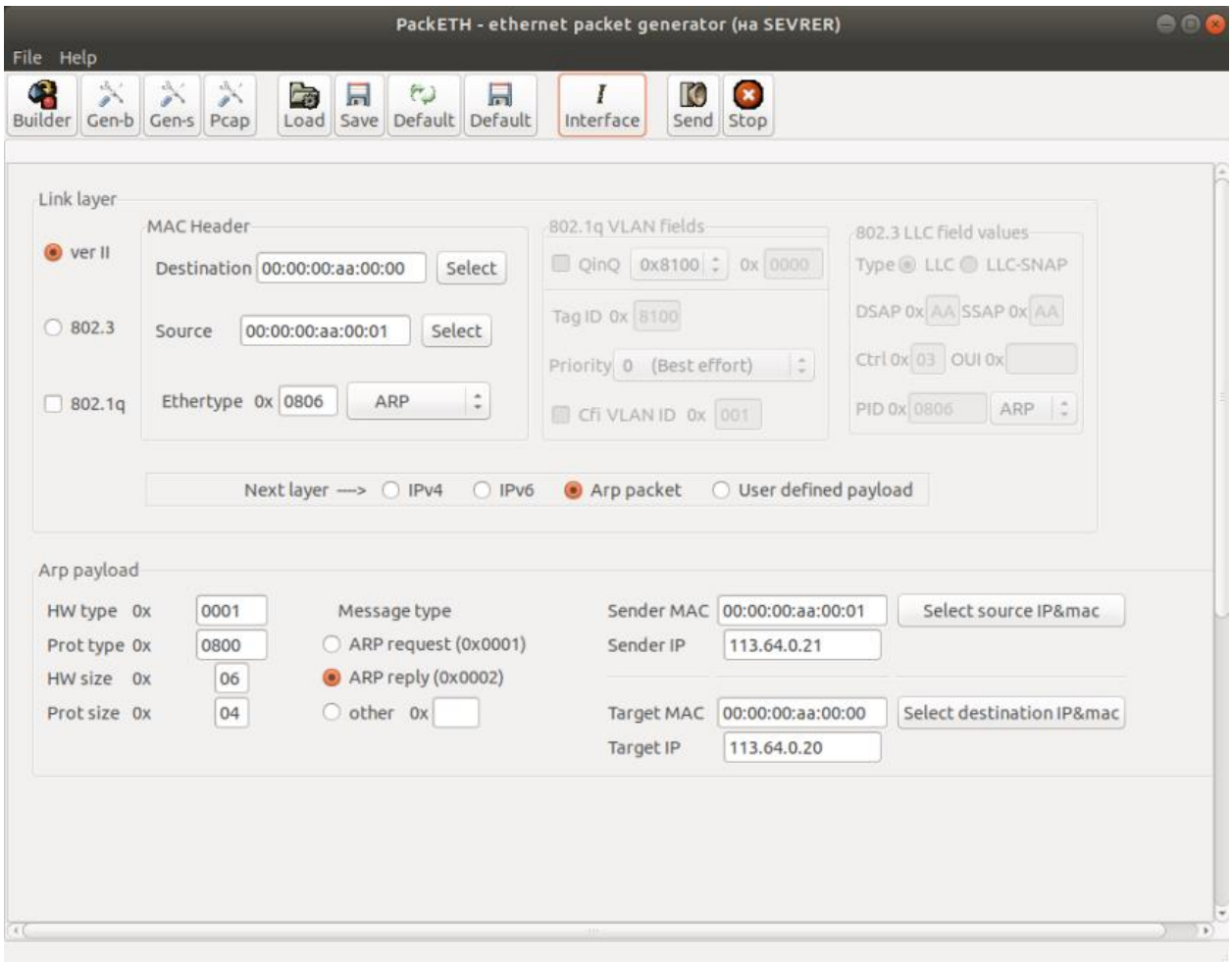
В консоли компьютера В “nc 113.64.0.20 9000”




Сервер пакеты не видит.






Destination – MAC-адрес компьютера A

Source – MAC-адрес сервера

Sender MAC – MAC-адрес сервера

Sender IP – IP компьютера B

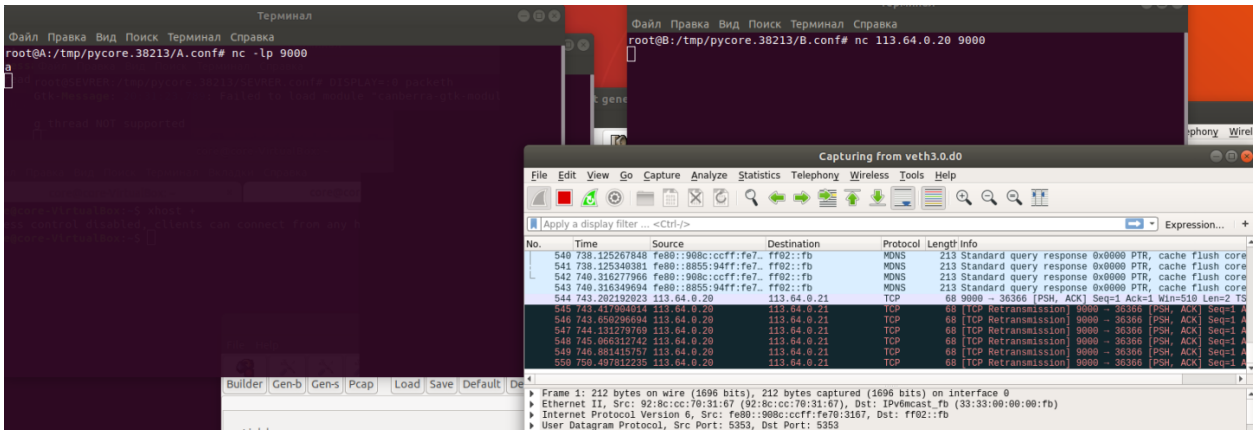
Target MAC - MAC-адрес компьютера A

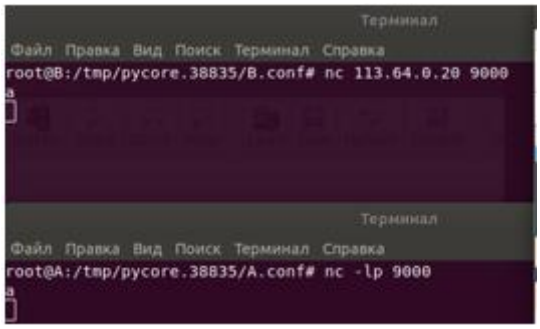
Target IP - IP компьютера A

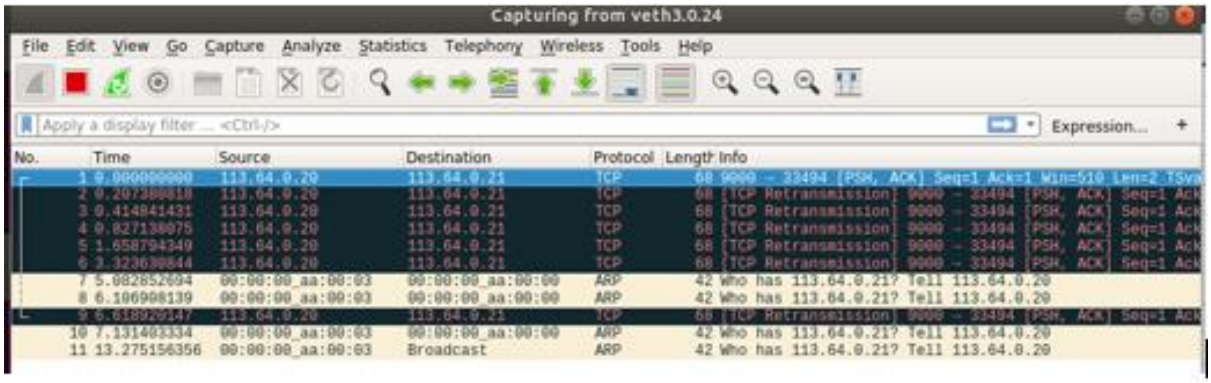
Видим, что в arp-таблице компьютера A сохранился MAC-адрес сервера

```
Терминал
Файл  Правка  Вид  Поиск  Терминал  Справка
root@A:/tmp/pycore.38213/A.conf# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 113.64.0.20  netmask 255.255.255.0  broadcast 0.0.0.0
        inet6 fe80::200:ff:feaa:0  prefixlen 64  scopeid 0x20<link>
        ether 00:00:00:aa:00:00  txqueuelen 1000  (Ethernet)
        RX packets 720  bytes 141463 (141.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 41  bytes 2638 (2.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Локальная петля (Loopback))
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@A:/tmp/pycore.38213/A.conf# arp
Адрес HW-тип HW-адрес Флаги Маска Интерфейс
113.64.0.21              ether   00:00:00:aa:00:01   C                     eth0
root@A:/tmp/pycore.38213/A.conf#
```

Отправляем пакет от A к B.




Терминал
Файл Правка Вид Поиск Терминал Справка
root@B:/tmp/pycore.38835/B.conf# nc 113.64.0.20 9000
a
Терминал
Файл Правка Вид Поиск Терминал Справка
root@A:/tmp/pycore.38835/A.conf# nc -lp 9000
a


Capturing from veth3.0.24
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 113.64.0.20 113.64.0.21 TCP 68 9000 → 33494 [PSH, ACK] Seq=1 Ack=1 Win=510 Len=2 TSva
2 0.207388818 113.64.0.20 113.64.0.21 TCP 68 [TCP Retransmission] 9000 → 33494 [PSH, ACK] Seq=1 Ack
3 0.414841431 113.64.0.20 113.64.0.21 TCP 68 [TCP Retransmission] 9000 → 33494 [PSH, ACK] Seq=1 Ack
4 0.827138075 113.64.0.20 113.64.0.21 TCP 68 [TCP Retransmission] 9000 → 33494 [PSH, ACK] Seq=1 Ack
5 1.658794349 113.64.0.20 113.64.0.21 TCP 68 [TCP Retransmission] 9000 → 33494 [PSH, ACK] Seq=1 Ack
6 3.323630844 113.64.0.20 113.64.0.21 TCP 68 [TCP Retransmission] 9000 → 33494 [PSH, ACK] Seq=1 Ack
7 5.082852694 00:00:00_aa:00:03 00:00:00_aa:00:00 ARP 42 Who has 113.64.0.21? Tell 113.64.0.20
8 6.106908139 00:00:00_aa:00:03 00:00:00_aa:00:00 ARP 42 Who has 113.64.0.21? Tell 113.64.0.20
9 6.618929147 113.64.0.20 113.64.0.21 TCP 68 [TCP Retransmission] 9000 → 33494 [PSH, ACK] Seq=1 Ack
10 7.131403334 00:00:00_aa:00:03 00:00:00_aa:00:00 ARP 42 Who has 113.64.0.21? Tell 113.64.0.20
11 13.275156356 00:00:00_aa:00:03 Broadcast ARP 42 Who has 113.64.0.21? Tell 113.64.0.20