ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

*Московский институт электроники и математики им. А.Н.Тихонова*

**Домашнее задание по теме 2. Защита компьютерных сетей и систем**

По направлению 10.04.01 – «Информационная безопасность»

Проверил:

преп. Денис Бубнов

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Выполнил:

Новиков В. С. МКБ 241

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

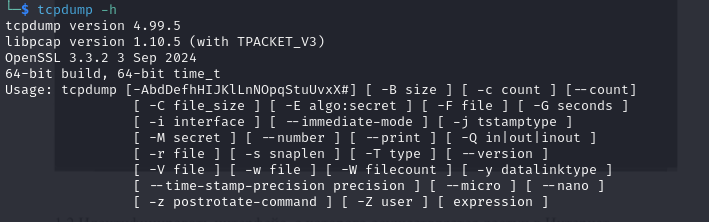
Москва 2024

# Задание 1. Захват трафика и использование инструментов фильтрации в TCPDump/Windump

## Запустить TCPDump или Windump в зависимости от платформы. Ознакомиться с встро.енной справкой консольной утилиты.

**Решение:**

*tcpdump –h*



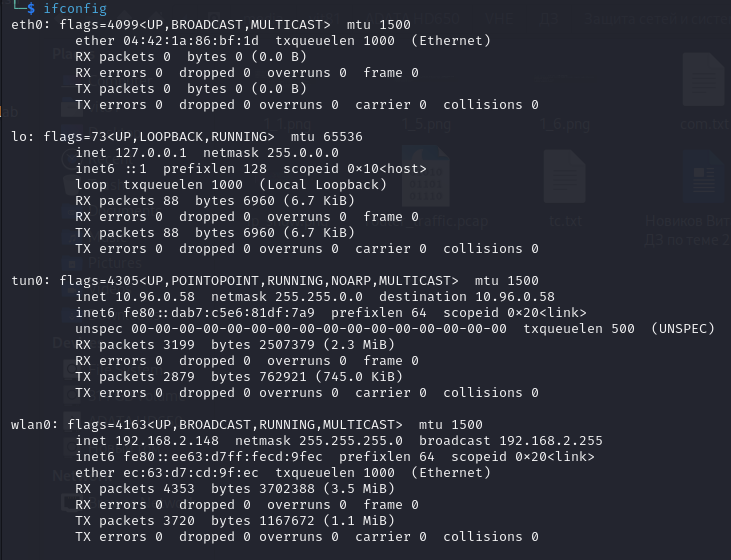
## Идентифицировать интерфейс, с которого осуществляется доступ в Интернет.

Решение:

*ip route show*

default via 192.168.2.1 dev wlan0 proto dhcp src 192.168.2.148 metric 600

*ifconfig*



Выполнить захват трафика, убедиться, что захват происходит.

Далее в п.1.3 показан захват трафика.

## 1.3. Настроить захват трафика с выводом в консоль следующим образом:

- детализация захвата -vv

- количество пакетов – 200

- не использовать разрешение имен DNS

- отображать заголовки Ethernet.

Решение:

*sudo tcpdump -i wlan0 -c 200 -nn -e –vv*

*Параметры:*

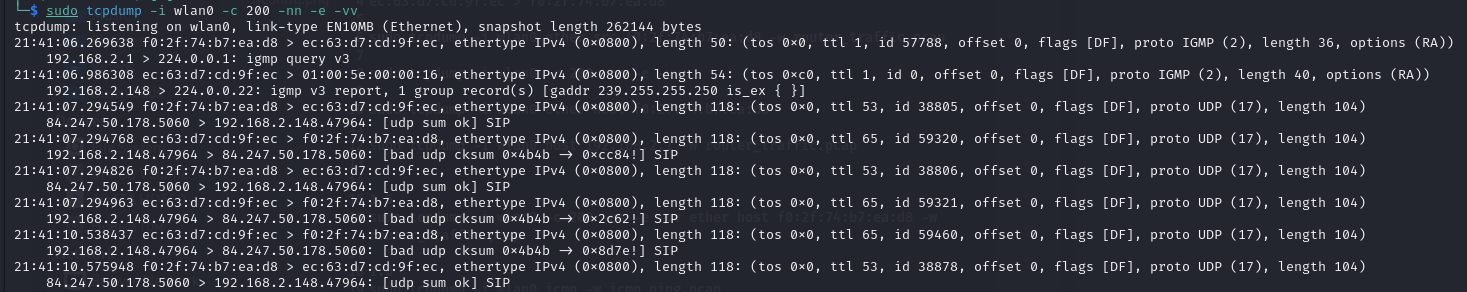
-i <интерфейс> — указать интерфейс (например, wlan0).

-c 200 — захватить только 200 пакетов.

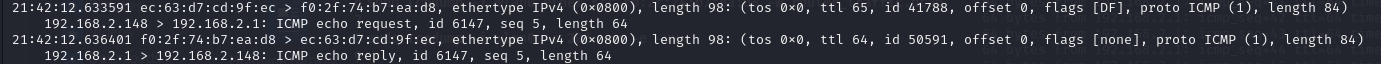
-nn — не разрешать имена хостов и служб (IP и порты остаются в числовом виде).

-e — отображать Ethernet-заголовки.

-vv — максимальная детализация информации о захвате.



## 1.4. Из дампа трафика, выявить MAC адреса компьютера и маршрутизатора (основного шлюза). Включить данные в отчет.

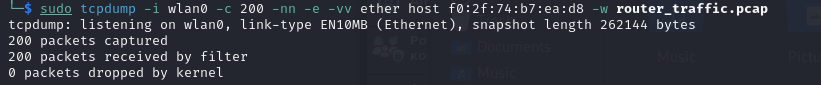


По результату команды ifconfig, мы видим, что MAC хоста ec:63:d7:cd:9f:ec, соответственно MAC шлюза f0:2f:74:b7:ea:d8

## 1.5. С помощью средств фильтрации трафика, захватить трафик, формируемый маршрутизатором. Сохранить дамп трафика в файл. Включить полученный файл в отчет.

Решение:

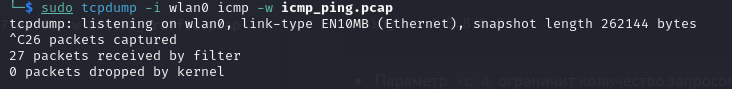
*sudo tcpdump -i wlan0 -c 200 -nn -e -vv ether host f0:2f:74:b7:ea:d8 -w router\_traffic.pcap*



## 1.6. С помощью средств фильтрации трафика выполнить захват ICMP пакетов

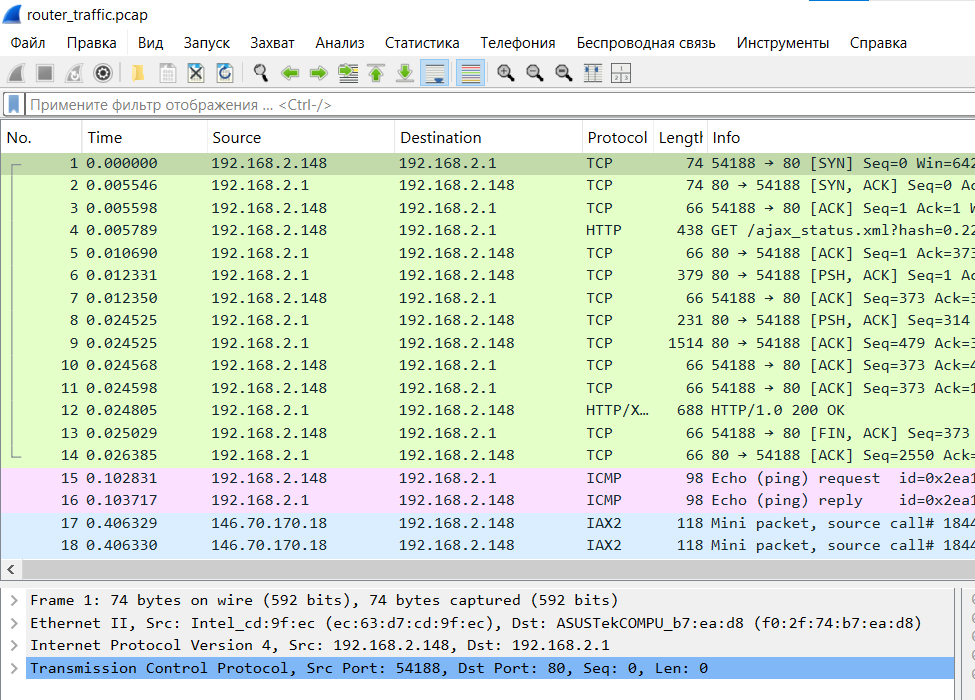
(ping) на адрес 8.8.8.8. Сформировать трафик командой ping 8.8.8.8. Сохранить дамп трафика в файл. Включить полученный файл в отчет.

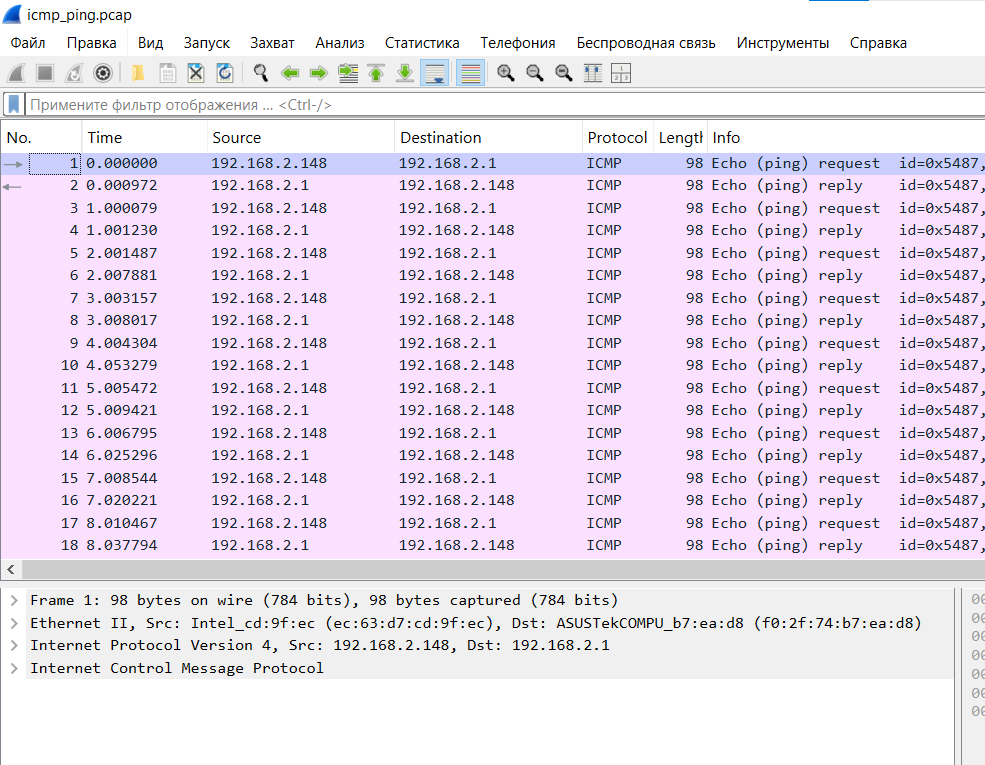
sudo tcpdump -i wlan0 icmp -w icmp\_ping.pcap



# Задание 2. Захват трафика и использование инструментов фильтрации в Wireshark

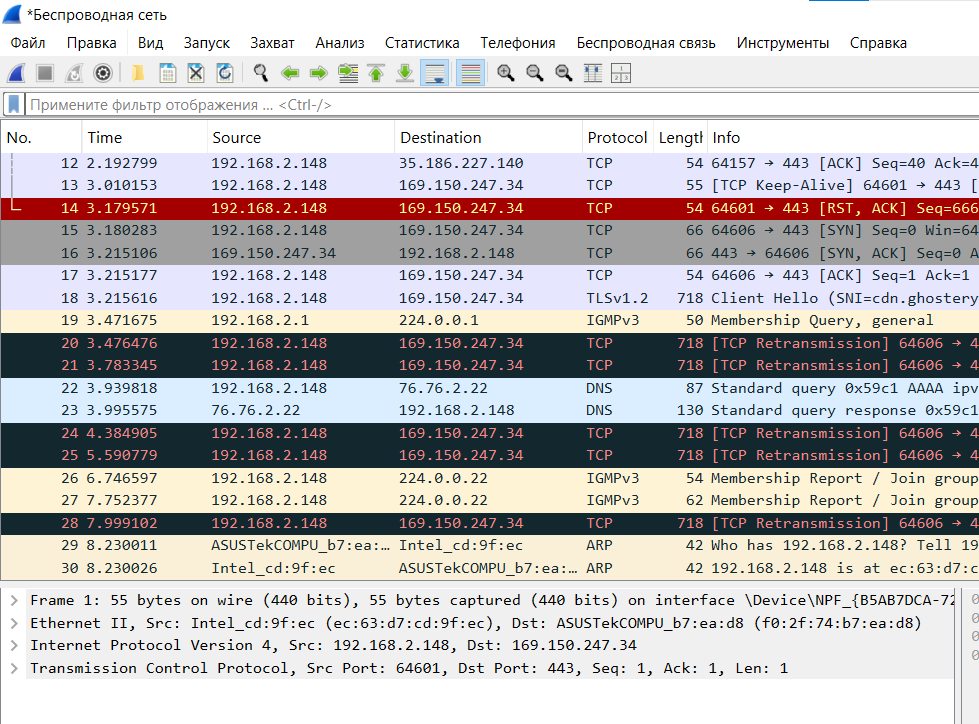
## 2.1. Открыть файлы, сохраненные в Задании 1. Убедиться, что дамп трафика корректно отображается в Wireshark. Убедиться в совместимости форматов дампа.



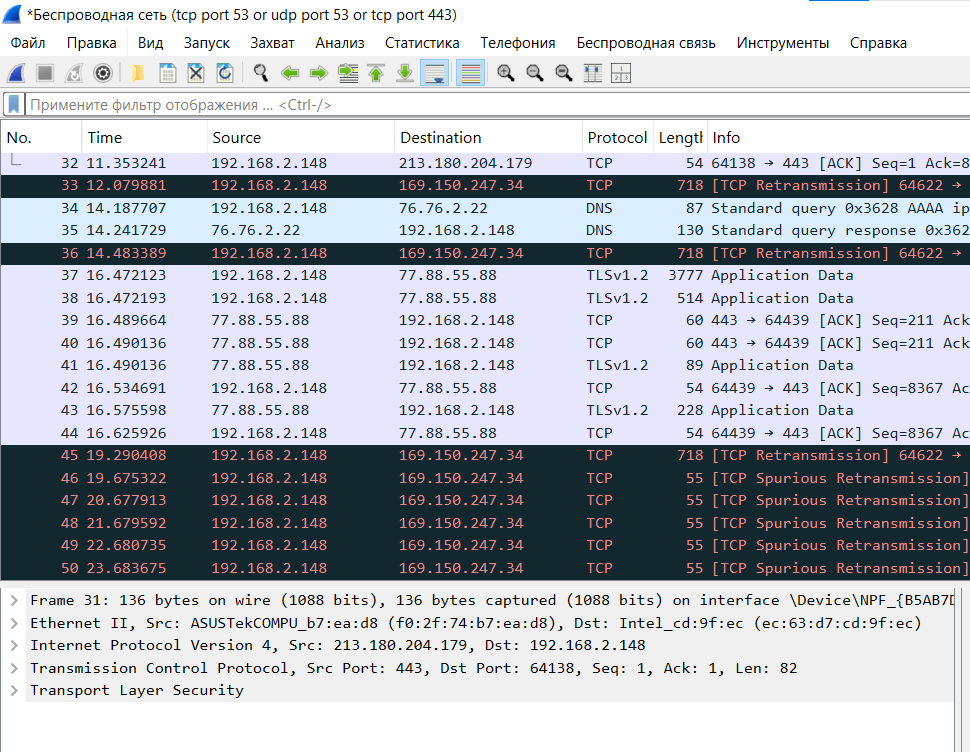


Закрыть файлы дампа.

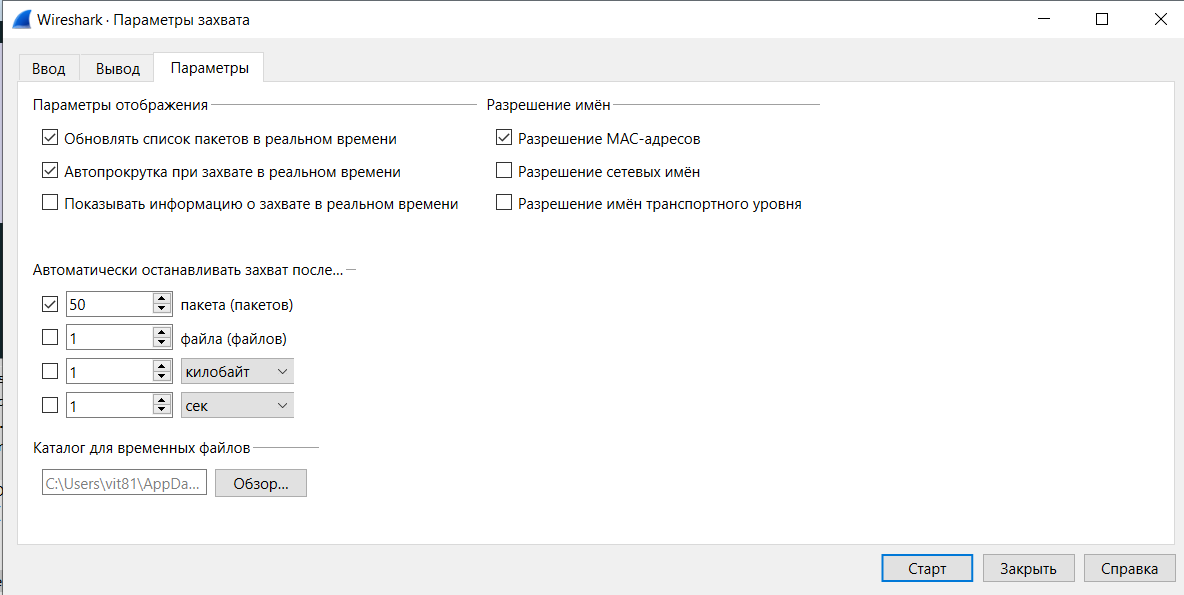
## 2.2. В Wireshark выбрать интерфейс ОС, с которого осуществляется доступ в Интернет. Запустить захват дампа трафика. Убедиться в наличии трафика на экране.



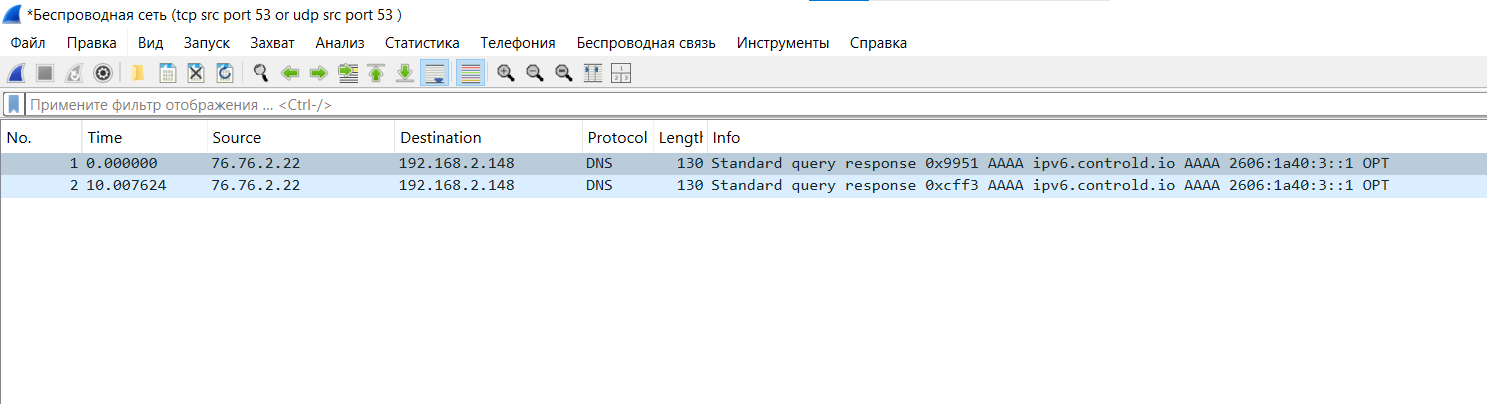
## 2.3. Создать фильтр захвата трафика, предусматривающий захват только трафика протоколов DNS и HTTPS. Установить размер дампа трафика в 50 пакетов.



Настройка ограничения по количеству пакетов:



## 2.4. Использовать фильтр отображения пакетов в текущем дампе трафика.



Отобразить только трафик, направленный от DNS сервера к клиенту. Сохранить дамп трафика в формате pcapng. Включить полученный файл в отчет.

