МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ   
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

Отчет по лабораторной работе № 2

по дисциплине «Компьютерные сети»

студента 2 курса группы ПИ-б-о-233(1)  
Иващенко Дениса Олеговича

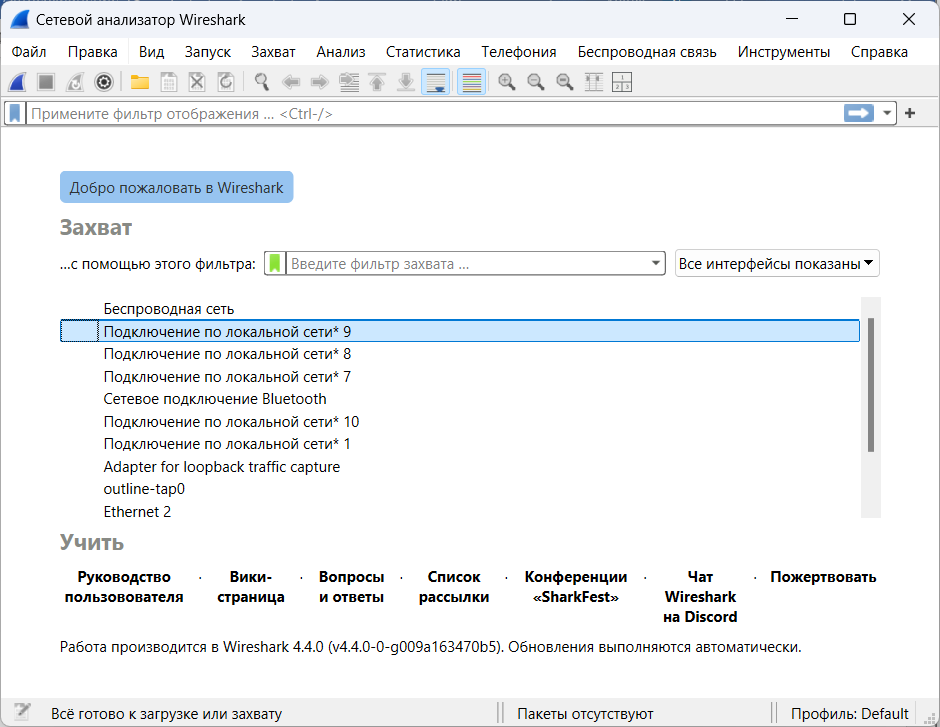
Направления подготовки 09.03.04«Программная инженерия»

Симферополь, 2024

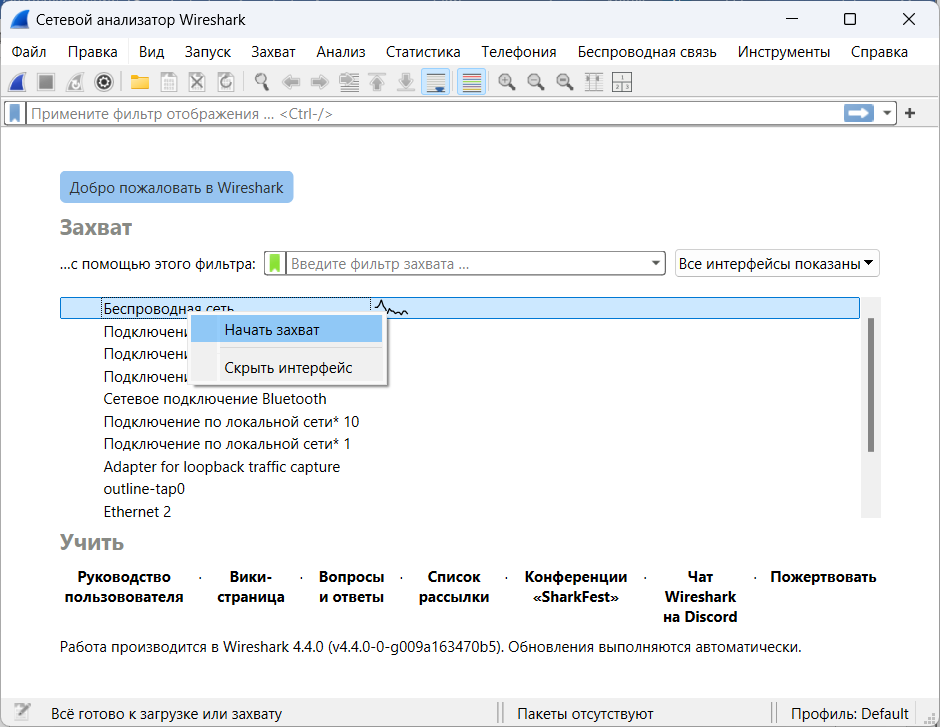
# 2. Анализ сетевого трафика с помощью программы «Wireshark»

Ход работы:

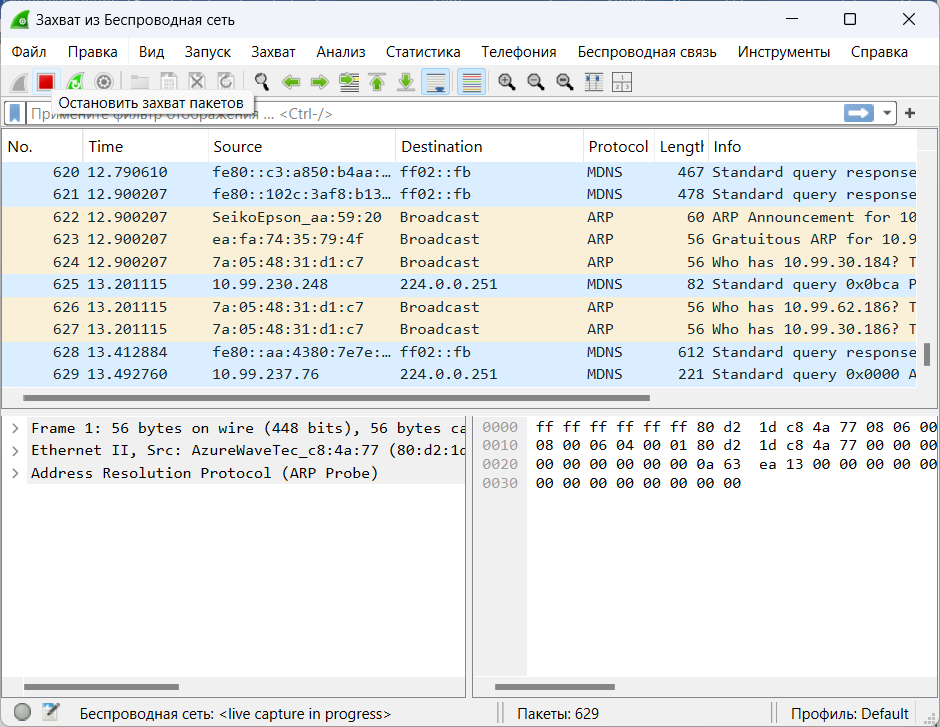
Шаг 1. Запустить программу Wireshark.



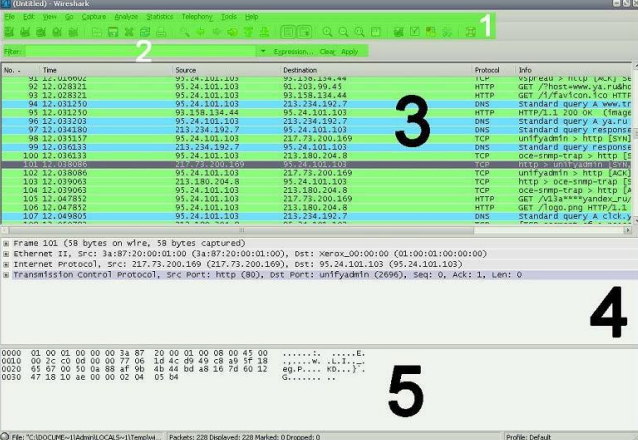
Шаг 2. Запустить процесс захвата трафика.

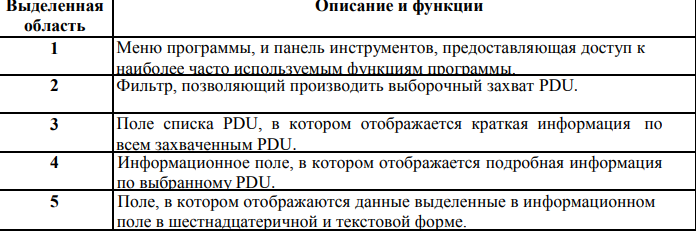


Шаг 3. Остановить процесс захвата трафика.

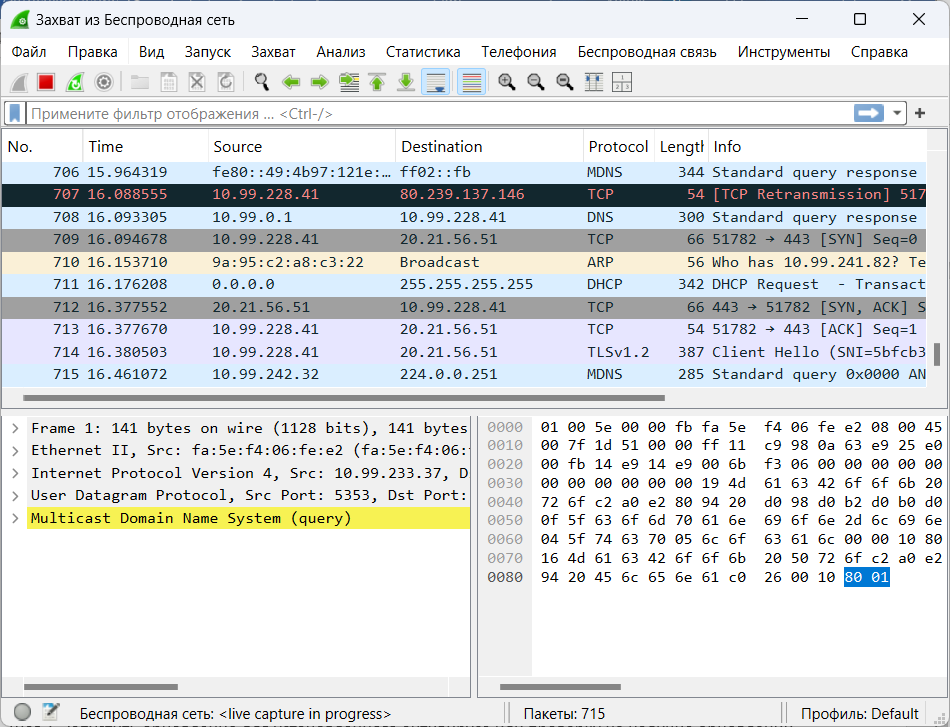


Шаг 4. Изучите интерфейс главного окна

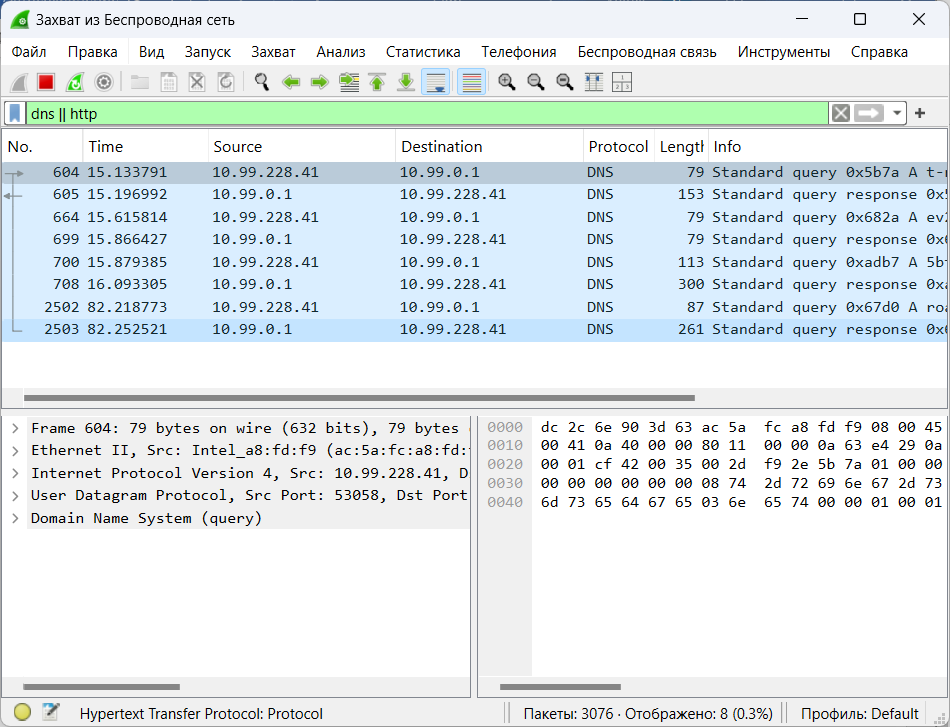




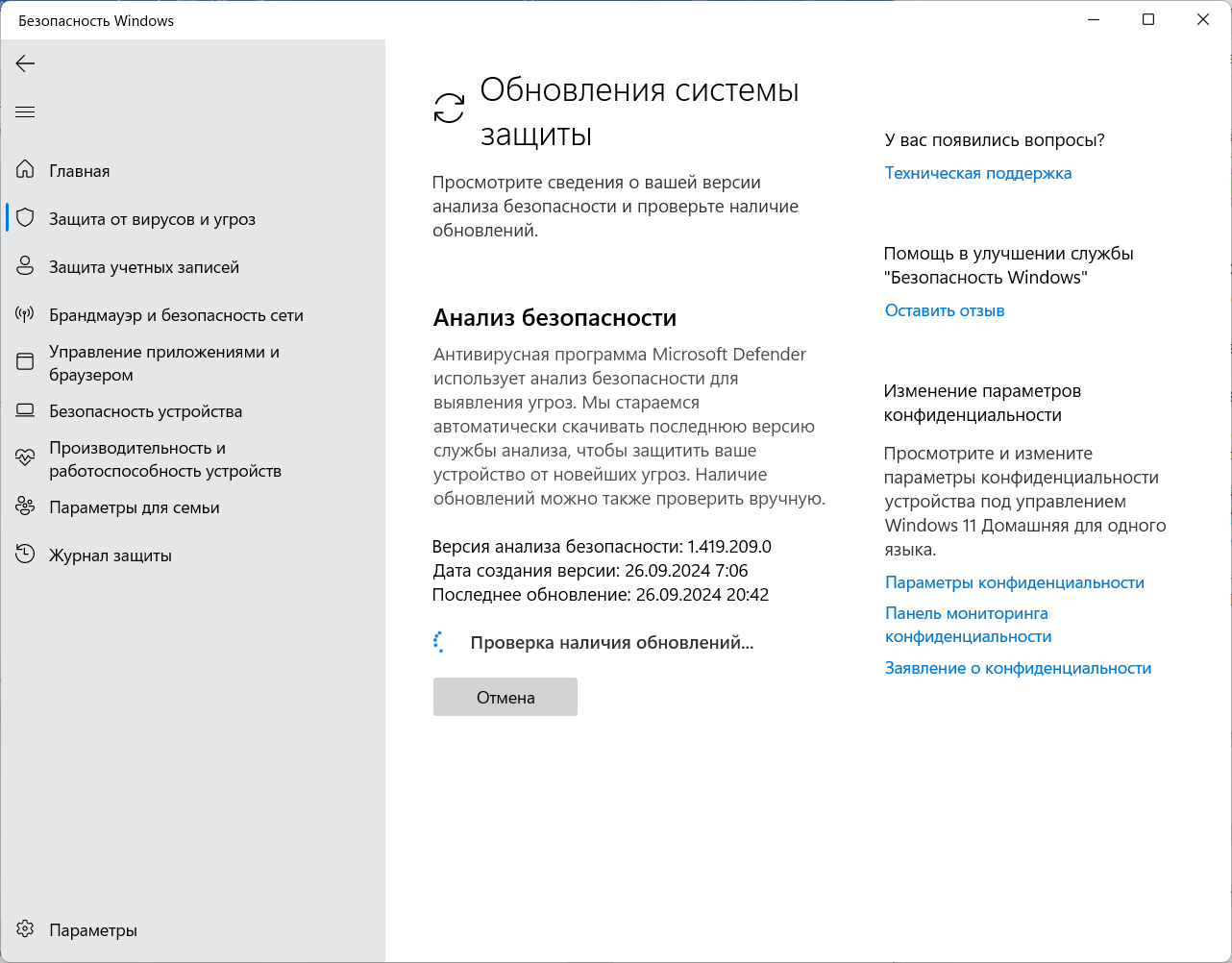
Шаг 5. Запустить процесс захвата трафика заново.



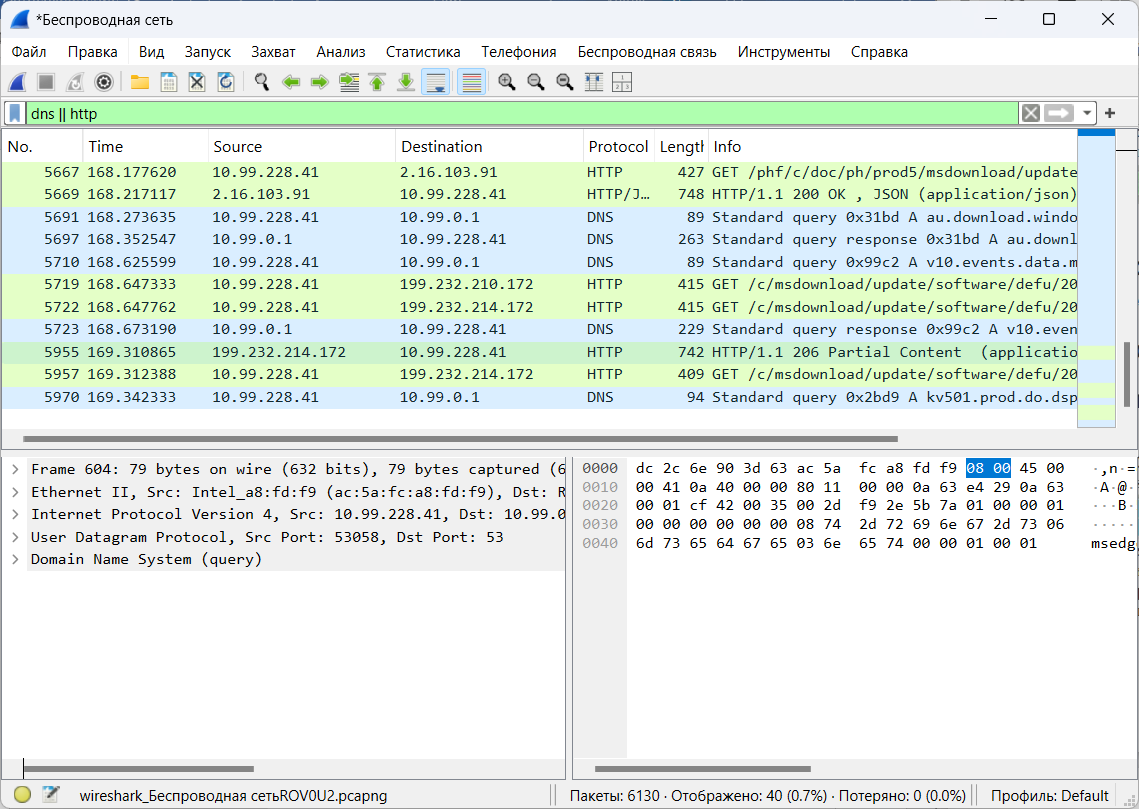
Шаг 6. Настроить фильтрацию вывода по протоколам DNS и HTTP.



Шаг 7. Запустить обновление для установленного антивируса или проверку на наличие обновлений встроенного Защитника Windows.



Шаг 8. Остановить захват трафика.

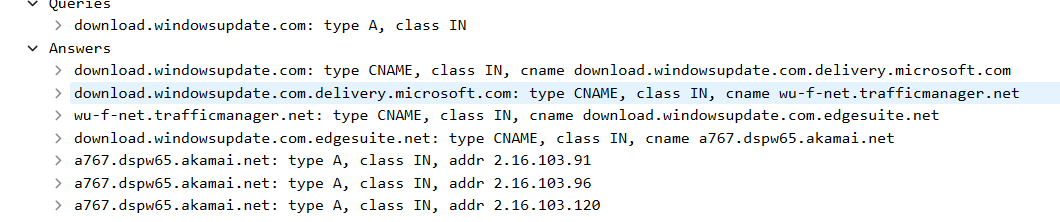


Шаг 9. Проанализировать трафик, захваченный программой.

9.1 Среди PDU, захваченных программой, найти DNS-запрос (query) и DNS-ответ



9.2 Посмотрев содержимое DNS-запроса и DNS-ответа выяснить и записать в отчёт следующую информацию: • DNS имя сервера обновлений антивируса. • Любые 5 сетевых адресов сервера обновлений



9.3 Среди PDU, захваченных программой, найти HTTP-запрос (HTTP GET).



9.4 Посмотрев содержимое PDU выяснить и записать в отчёт следующую информацию:

• Сетевой адрес сервера обновлений.

2.16.103.91

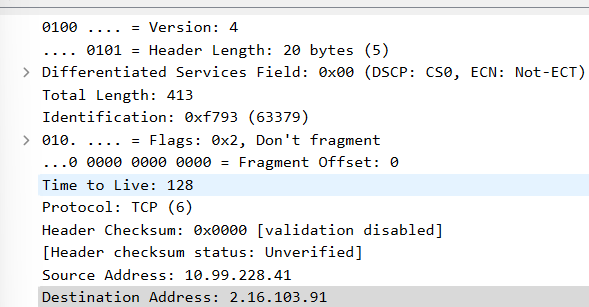
• Данные о вашем компьютере, которые программа обновления передала на сервер: версию Windows, месторасположение компьютера (Страна).

Современные версии не передают явно эти данные.

9.5 Изучив содержимое DNS-запроса, HTTP-запрос и DNS-ответа выяснить и записать в отчёт следующую информацию:

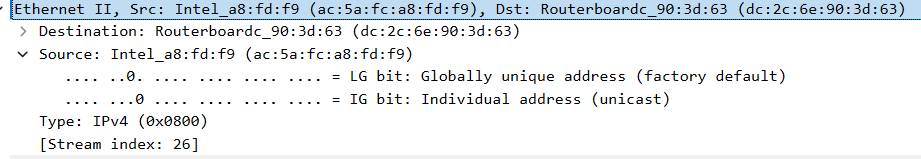
• Сетевой адрес компьютера.

10.99.228.41



• MAC-адрес компьютера.

ac:5a:fc:a8:fd:f9



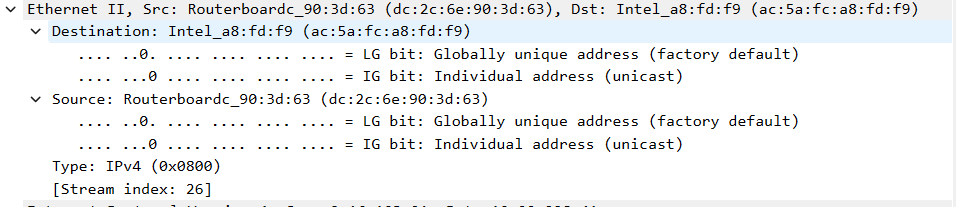
• Сетевой адрес шлюза.

10.99.0.1



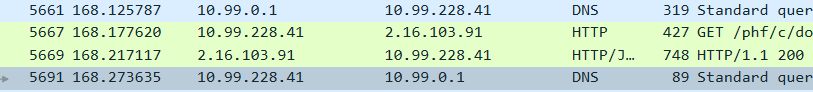
• MAC-адрес шлюза.

ac:5a:fc:a8:fd:f9

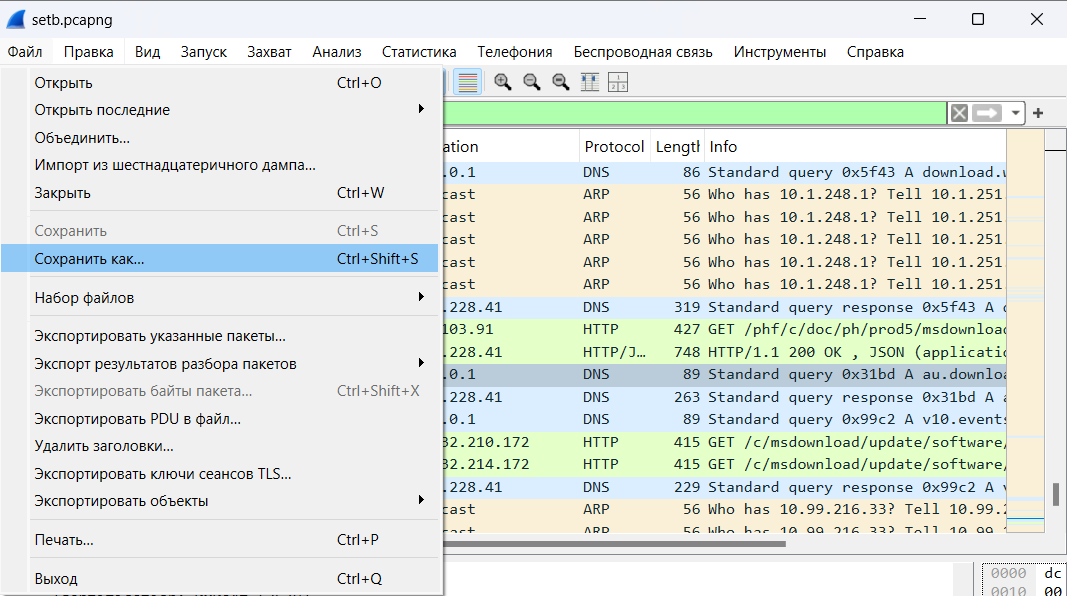


• Сетевой адрес DNS-сервера.

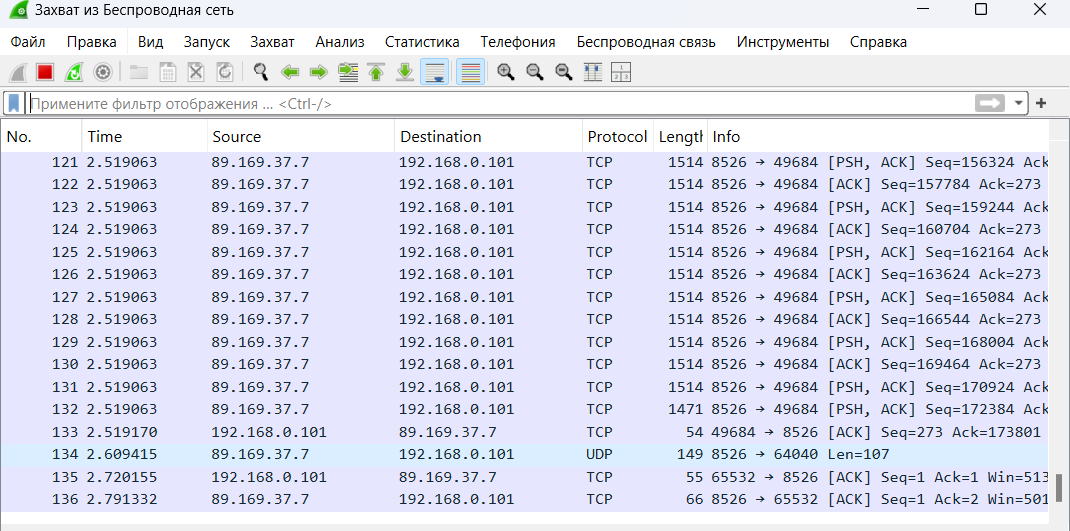
10.99.0.1



Шаг 10. Сохранить захваченный трафик.



Шаг 11. Заново запустить захват трафика.



Шаг 12. Настроить фильтрацию вывода по протоколу FTP.

• Протокол транспортного уровня, который использует сервис DNS.

• Порт, на который осуществляется DNS-запрос.

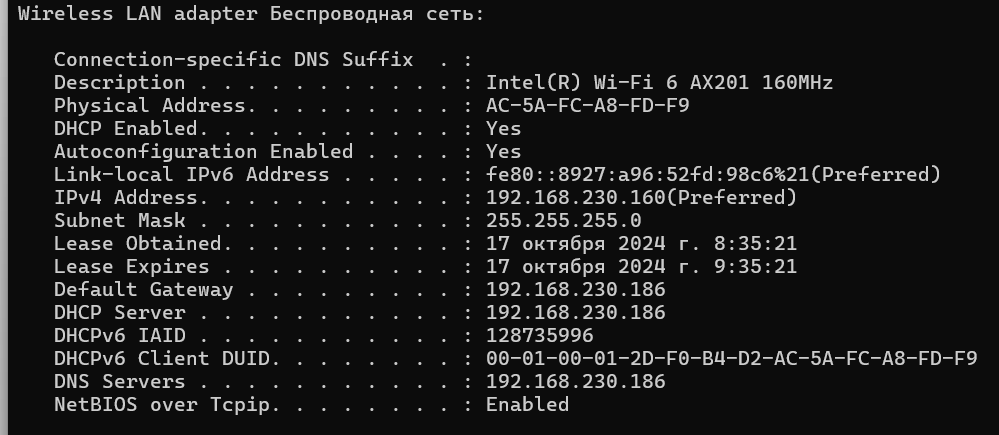
• Протокол транспортного уровня, который использует протокол HTTP.

• Порт, на который осуществляется запрос обновления антивируса по протоколу HTTP.

Часть 3

Шаг 1. Узнайте адреса интерфейсов своего ПК.

1. Откройте окно командной строки Windows. a. В окне командной строки введите ipconfig/all, чтобы узнать IP-адрес интерфейса компьютера, его описание и MAC-адрес (физический).



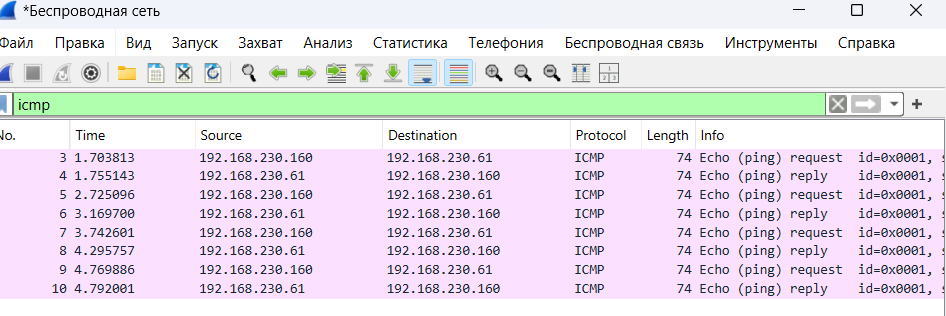
Ip-адрес другого студента

192.168.230.61

Шаг 2. Запустите программу Wireshark и начните сбор данных.

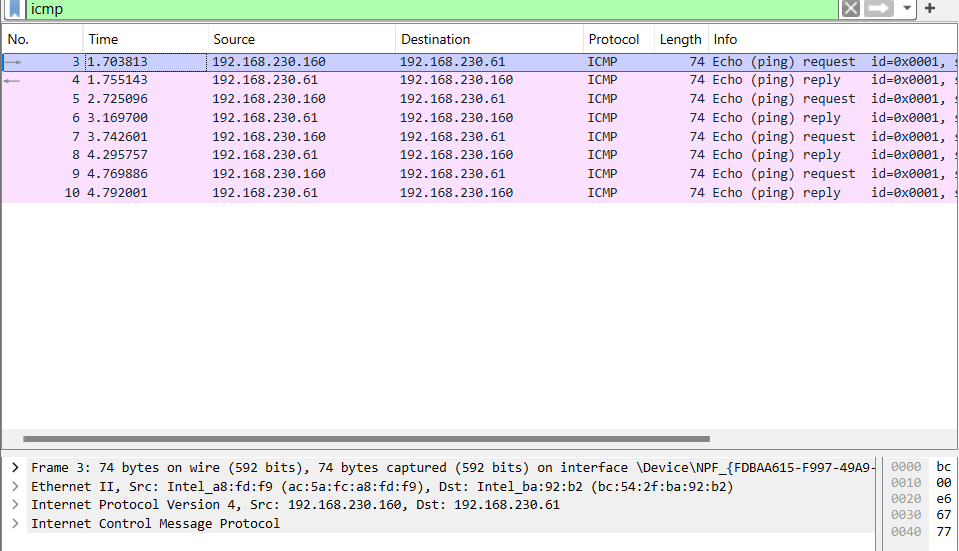
Откройте окно командной строки и отправьте эхо-запрос с помощью команды ping на IP-адрес, полученный от другого учащегося.

В верхней части окна программы Wireshark снова появятся данные.

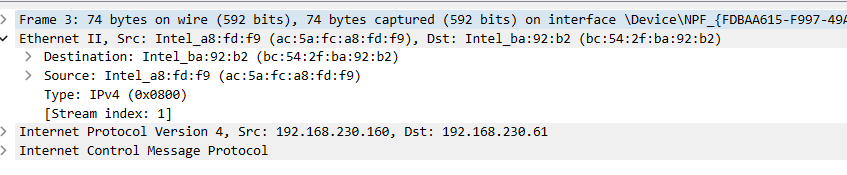


Шаг 3. Изучите полученные данные.

Выберите кадры PDU первого запроса ICMP в верхнем разделе окна программы Wireshark. Обратите внимание на то, что в столбце Source (Источник) указывается IP-адрес вашего компьютера, а в столбце Destination (Назначение) — IP-адрес ПК другого участника, на который вы отправили ping-запрос.



b. Не меняя выбор кадра PDU в верхнем разделе окна, перейдите в средний раздел. Нажмите символ + слева от строки Ethernet II, чтобы просмотреть МАС-адреса источника и назначения.



Вопросы:

Совпадает ли MAC-адрес источника с интерфейсом компьютера?

Да, совпадает, ac:5a:fc:a8:fd:f9

Совпадает ли MAC-адрес назначения в программе Wireshark с MAC-адресом другого участника рабочей группы?

Да, совпадает, bs:54:2f:ba:92:b2

Как ваш ПК определил MAC-адрес другого ПК, на который был отправлен эхо-запрос с помощью команды ping?

ПК использует протокол ARP (Address Resolution Protocol) для определения MAC-адреса другого ПК. Протокол ARP опрашивает все хосты в локальной сети и только один отвечает на этот запрос.

Часть 2. Сбор и анализ данных протокола ICMP по удаленным узлам в программе Wireshark

Шаг 1. Запустите захват данных в интерфейсе.

a. Снова начните захват данных.

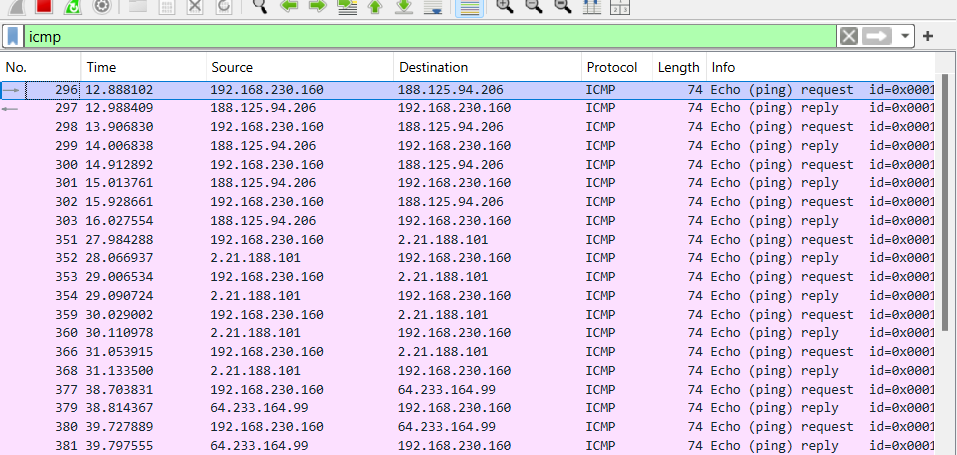
b. Появится окно с предложением сохранить полученные ранее данные перед началом нового захвата. Сохранять эти данные необязательно. Нажмите Continue without Saving (Продолжить без сохранения).

c. Активировав захват данных, отправьте эхо-запрос с помощью команды ping на следующие три URL-адреса веб-сайтов с командной строки Windows: Откройте окно командной строки Windows.

1) [www.yahoo.com](http://www.yahoo.com)

2) [www.cisco.com](http://www.cisco.com)

3) [www.google.com](http://www.google.com)



Шаг 2. Изучите и проанализируйте данные, полученные от удаленных узлов.

Просмотрите собранные данные в программе Wireshark и изучите IP- и MAC-адреса трех веб-сайтов, на которые вы отправили ping-запросы. Ниже в оставленном месте укажите IP- и MAC-адреса назначения для всех трех веб-сайтов.

Вопросы:

IP-адрес для [www.yahoo.com](http://www.yahoo.com): 188.125.94.206

MAC-адрес для [www.yahoo.com](http://www.yahoo.com): 22:73:a4:34:5f:64

IP-адрес для [www.cisco.com](http://www.cisco.com): 2.21.188.101

MAC-адрес для [www.cisco.com](http://www.cisco.com): 22:73:a4:34:5f:64

IP-адрес для [www.google.com](http://www.google.com): 64.233.164.99

MAC-адрес для [www.google.com](http://www.google.com): 22:73:a4:34:5f:64

Какова существенная особенность этих данных? Как эта информация отличается от данных, полученных в результате эхо-запросов локальных узлов в части 1?

Публичные ip адреса удаленных хостов,

В случае локальных узлов MAC-адреса являются уникальными для каждого устройства в локальной сети и используются для передачи данных внутри этой сети. Для удаленных веб-сайтов, как правило, отображается MAC-адрес ближайшего маршрутизатора или шлюза, который обрабатывает запросы.

Закройте окно командной строки Windows

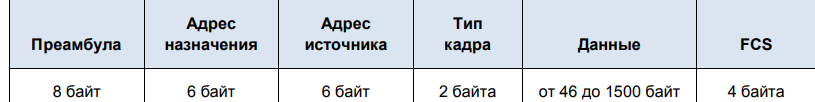
Почему программа Wireshark показывает фактические MAC-адреса локальных узлов, но не показывает фактические MAC-адреса удаленных узлов?

MAC-адреса удаленных хостов не известны в локальной сети, поэтому используется. MAC-адрес шлюза по умолчанию.

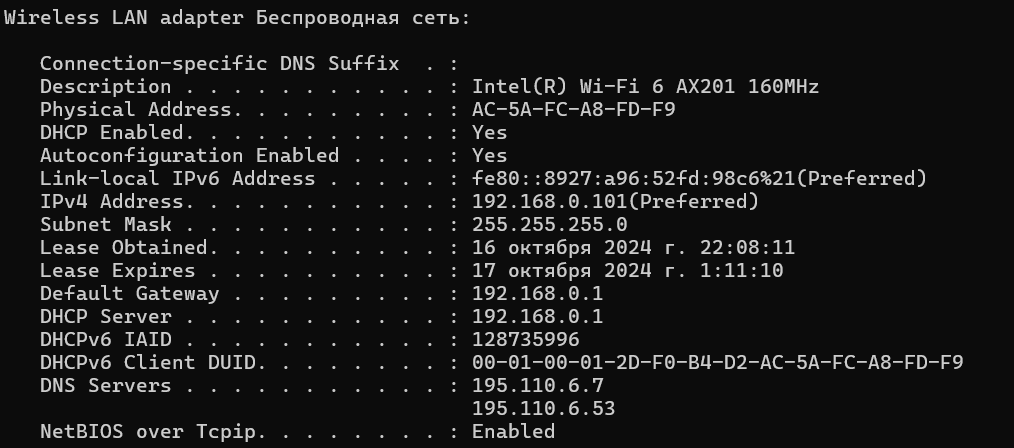
Часть 4

Часть 1

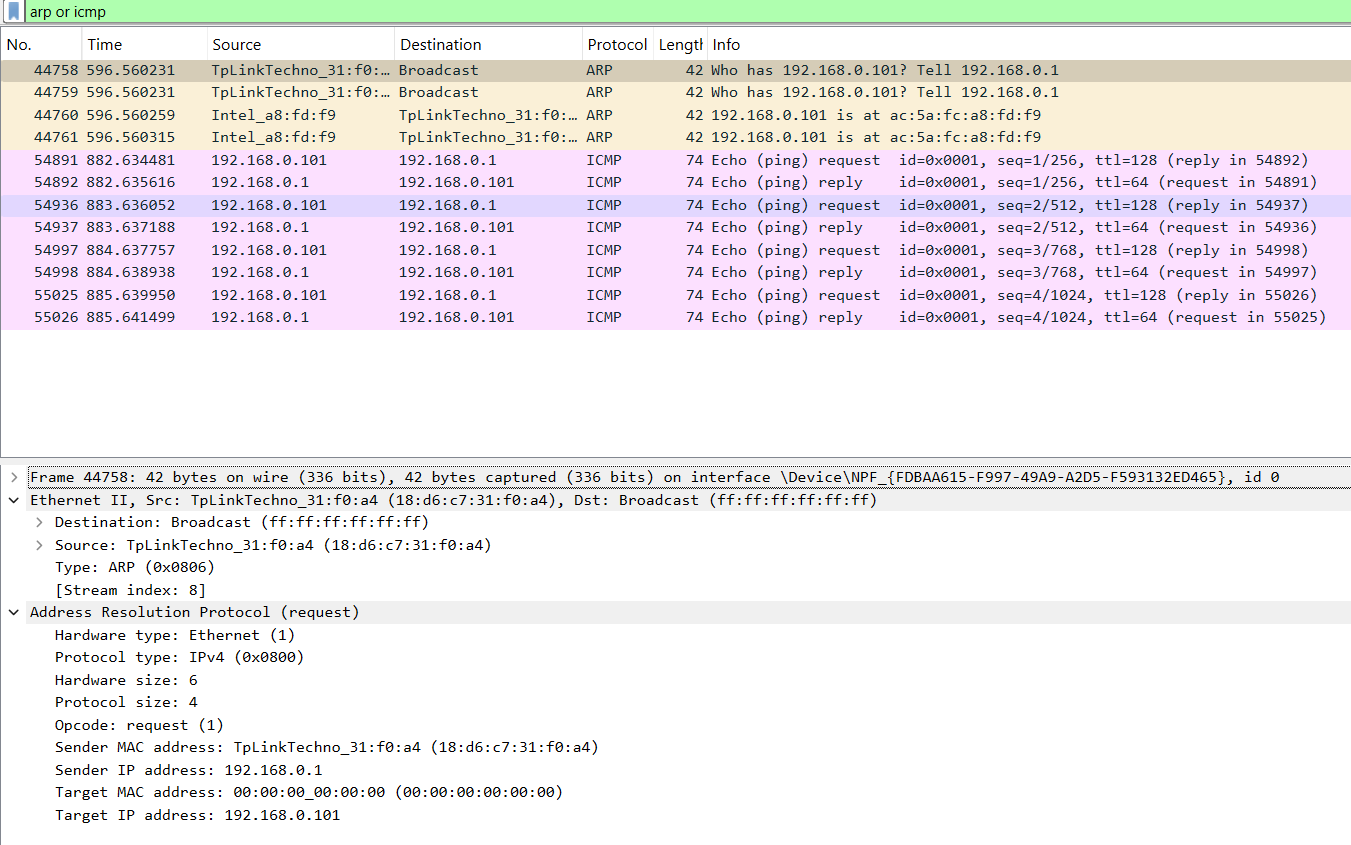
Шаг 1. Просмотрите длины и описания полей заголовков Ethernet II.



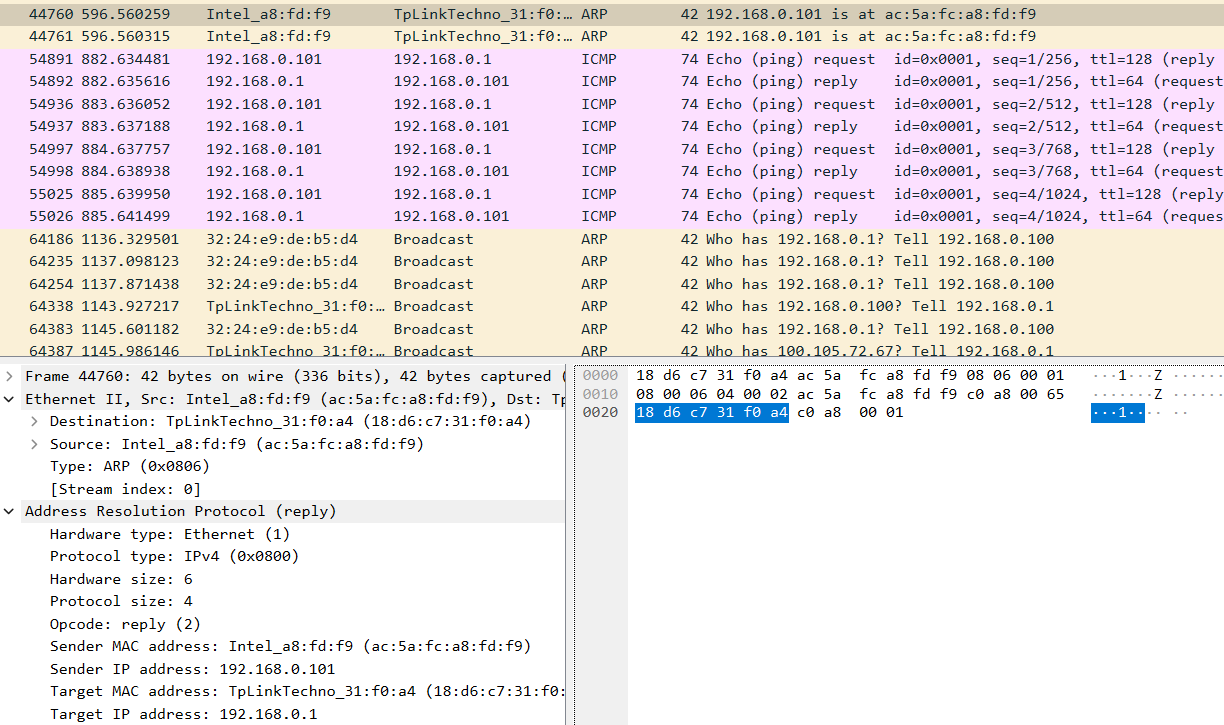
Шаг 2. Изучите конфигурацию сети ПК.



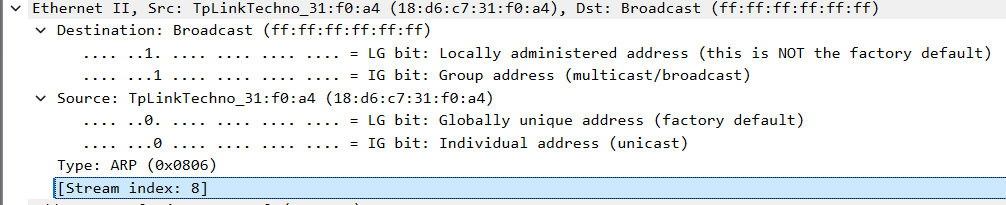
Шаг 3. Изучите кадры Ethernet в данных, перехваченных программой Wireshark.



На этом скриншоте показаны сведения о кадре ответа ARP.



Шаг 4. Изучите содержание заголовков Ethernet II в ARP-запросе.



Какова особенность содержания поля адреса назначения?

Поле адреса назначения в этом кадре содержит широковещательный адрес **ff:ff:ff:ff:ff,** который используется для отправки пакетов всем устройствам в локальной сети. Это типично для ARP-запросов, где отправитель пытается определить MAC-адрес устройства по его IP-адресу.

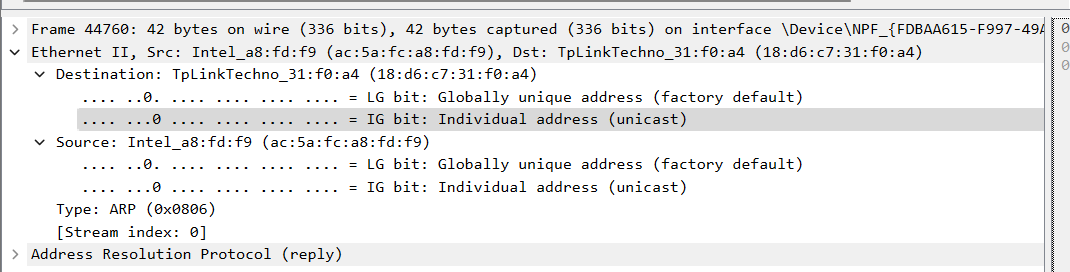
Почему перед первым эхо-запросом ПК отправляет широковещательную рассылку ARP?

Перед тем как отправить эхо-запрос (ICMP запрос), компьютер должен узнать MAC-адрес целевого устройства для построения Ethernet-кадра. Для этого отправляется **ARP-запрос** с широковещательной рассылкой, которая запрашивает у всех устройств в сети, чей IP-адрес соответствует указанному. В ответ ARP предоставляет MAC-адрес целевого устройства.

Назовите MAC-адрес источника в первом кадре.

**18:d6:c7:31:f0:a4**

Назовите идентификатор производителя (OUI) сетевой платы источника в ответе ARP?



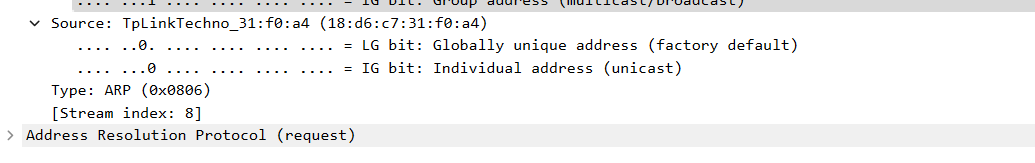
**ac:5a:fc**

Какая часть МАС-адреса соответствует OUI?

Первые шесть шестнадцатеричных чисел обозначают производителя сетевой платы, а последние — ее серийный номер

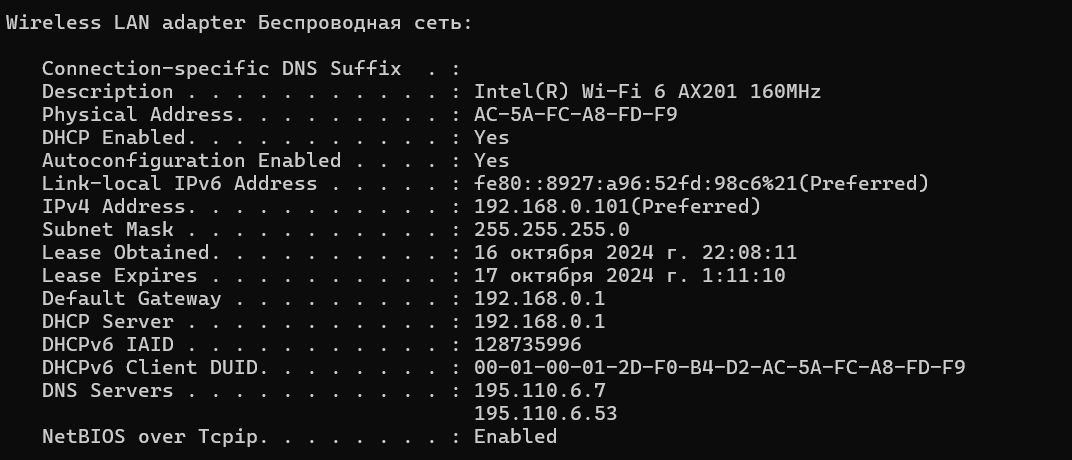
31:f0:a4

Назовите серийный номер сетевой интерфейсной платы (NIC) источника



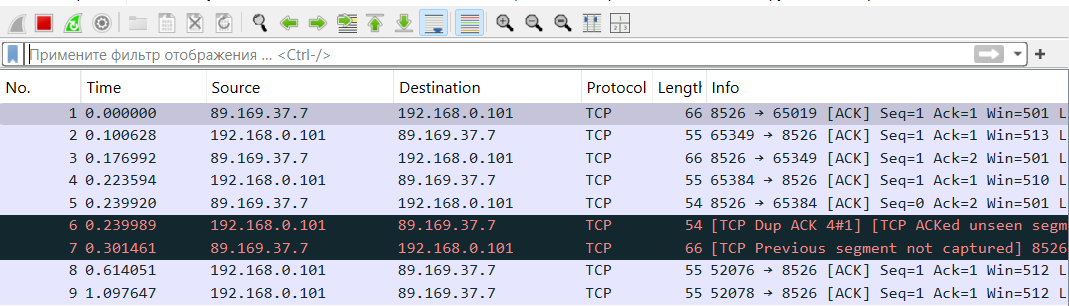
Часть 2. Перехват и анализ кадров Ethernet с помощью программы Wireshark.

Шаг 1. Определите IP-адрес шлюза по умолчанию на своем ПК.

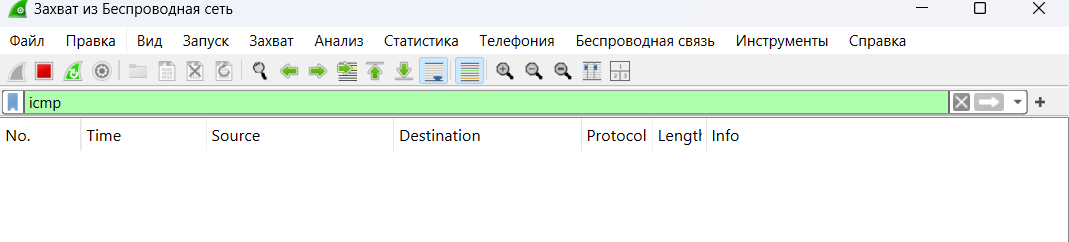


192.168.0.1

Шаг 2. Начните захват трафика на сетевой интерфейсной плате своего ПК.

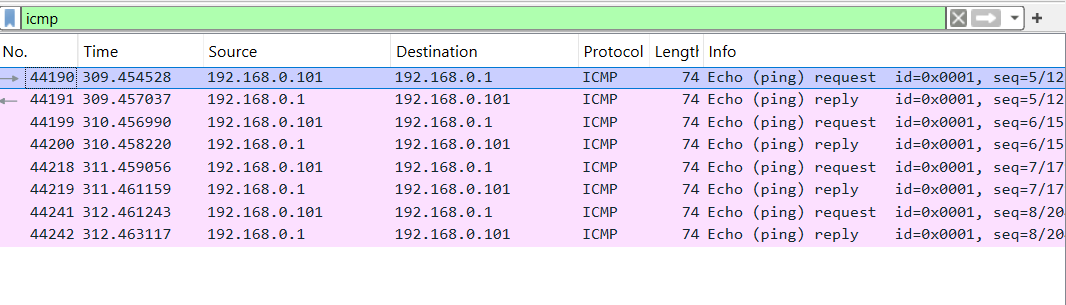


Шаг 3. С помощью фильтров программы Wireshark отобразите на экране только трафик ICMP.



Шаг 4. Из окна командной строки отправьте эхо-запрос на шлюз ПК по умолчанию.

Шаг 5. Остановите захват трафика на сетевой плате.

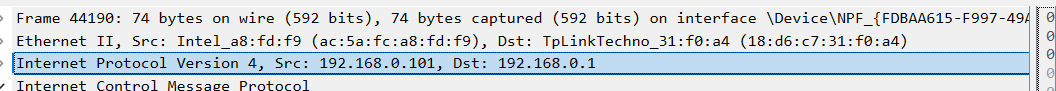


Шаг 6. Изучите первый эхозапрос в программе Wireshark.

1.На панели списка пакетов (верхний раздел) выберите первый указанный кадр. В столбце Info (Информация) появится значение Echo (ping) request (Эхо-запрос с помощью команды ping). Теперь линия должна быть выделена.



2.. Изучите первую строку на панели сведений о пакете в средней части экрана. В этой строке показана длина кадра.



3. Вторая строка на панели сведений о пакете показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника и назначения.

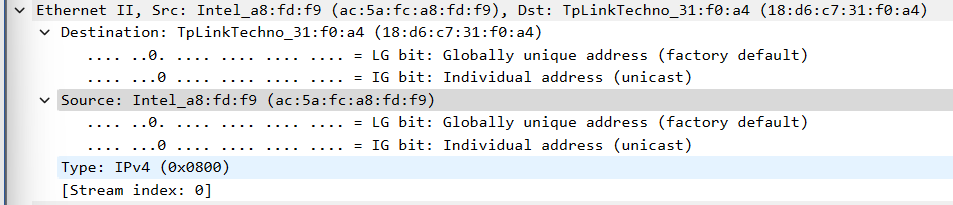
Вопросы: Назовите MAC-адрес сетевой интерфейсной платы этого ПК.

ac:5a:fc:a8:fd:f9

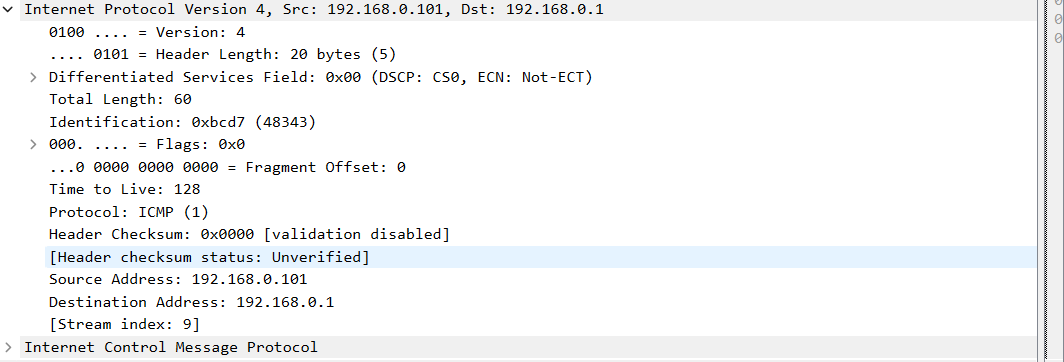
Назовите MAC-адрес шлюза по умолчанию.

18:d6:c7:31:f0:a4

4. Вы можете щелкнуть знак больше (>) в начале второй строки, чтобы получить больше информации о кадре Ethernet II. Вопрос: Назовите отображающийся тип кадра.



5. Последние две строки среднего раздела содержат информацию о поле данных кадра. Обратите внимание на то, что данные содержат IPv4-адреса источника и назначения.



Вопросы:

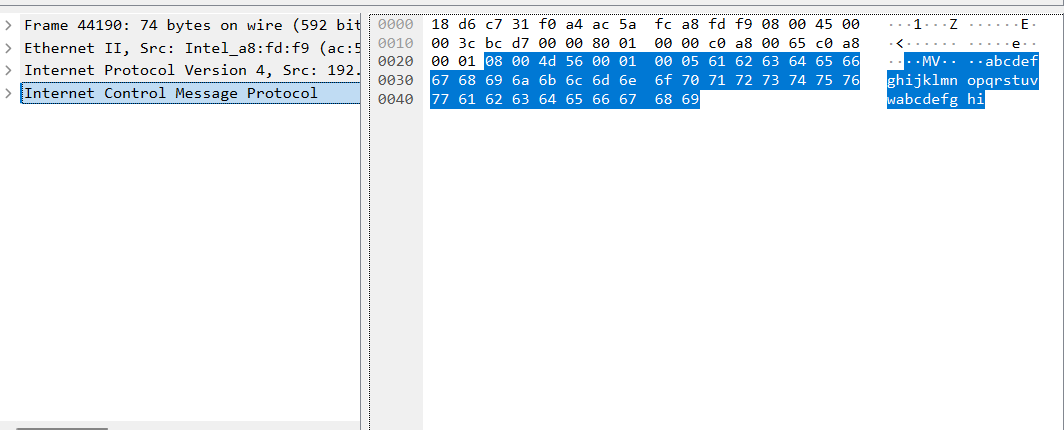
Назовите IP-адрес источника.

192.168.0.101

Назовите IP-адрес назначения.

192.168.0.1

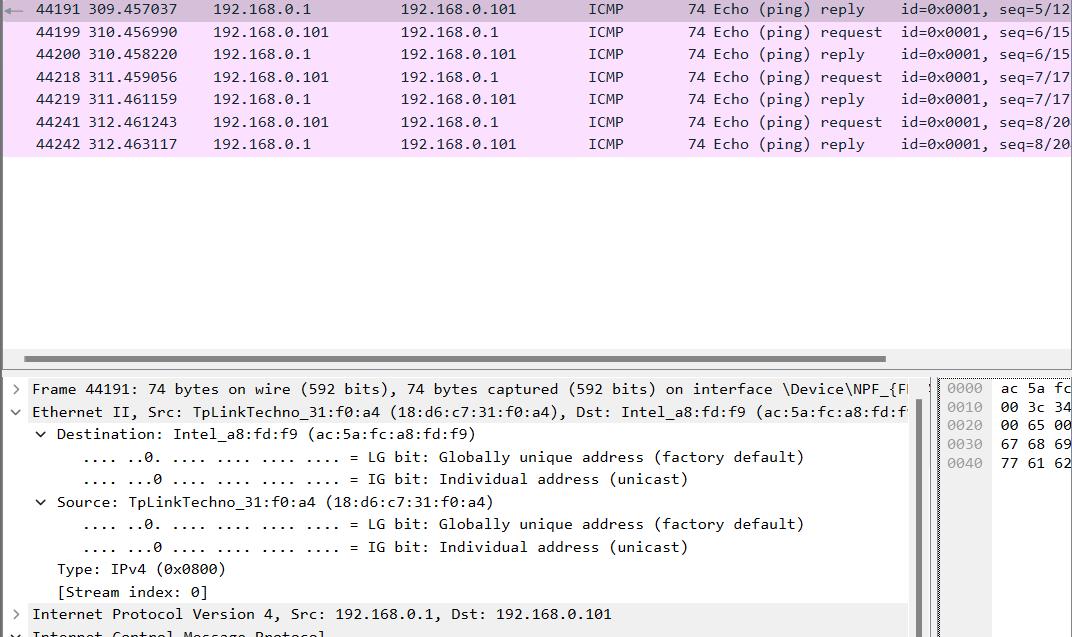
6.Для того чтобы выделить эту часть кадра (в шестнадцатеричной системе и в кодировке ASCII) на панели Packet Bytes (Последовательность байтов пакета) (нижний раздел), щелкните по любой строке в среднем разделе. Щелкните по строке Internet Control Message Protocol (Протокол ICMP) в среднем разделе и посмотрите, что будет выделено на панели Packet Bytes (Последовательность байтов пакета).



Вопрос: Какое слово образуют последние два выделенных октета?

hi

7 Нажмите следующий кадр в верхнем разделе и изучите кадр эхоответа. Обратите внимание на то, что МАС-адреса источника и назначения поменялись местами, поскольку маршрутизатор, который служит шлюзом по умолчанию, отправил этот кадр в ответ на первый эхозапрос.

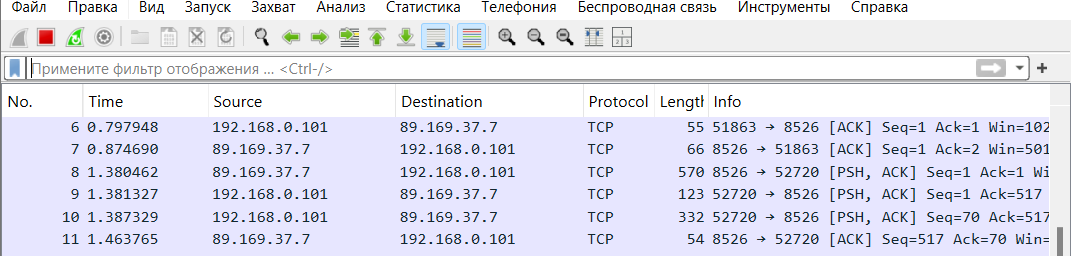


Вопрос: Какое устройство и MAC-адрес отображаются в качестве адреса назначения?

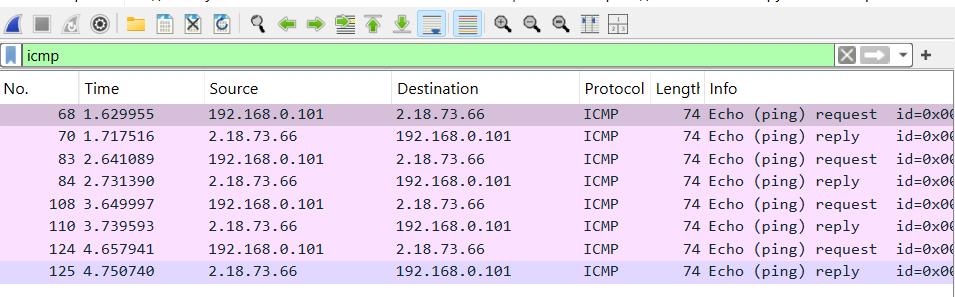
Intel\_a8:fd:f9 (ac:5a:fc:a8:fd:f9)

Шаг 7. Захват пакетов для удаленного узла.

1. Нажмите пиктограмму Start Capture (Начать перехват), чтобы начать новый перехват данных в программе Wireshark. Откроется всплывающее окно с предложением сохранить предыдущие перехваченные пакеты в файл перед началом нового перехвата. Нажмите Continue without Saving (Продолжить без сохранения).



1. Через окно командной строки отправьте эхо-запрос на веб-сайт [www.cisco.com](http://www.cisco.com).
2. Остановите захват пакетов.



1. Изучите новые данные на панели списка пакетов в программе Wireshark.

Вопросы:

Назовите МАС-адреса источника и назначения в первом кадре эхозапроса.

Источник: ac:5a:fc:a8:fd:f9

Назначение: 18:d6:c7:31:f0:a4

Назовите IP-адреса источника и назначения в поле данных кадра.

Источник: 12.168.0.101

Назначение: 2.18.73.66

Сравните эти адреса с адресами, полученными в шаге 6. Изменился только IP-адрес назначения. Почему IP-адрес назначения изменился, а MAC-адрес назначения остался прежним?

MAC-адрес назначения остается прежним, так как он указывает на маршрутизатор, а IP-адрес назначения изменяется, так как он указывает на конкретный сервер, к которому обращаемся.

Вопросы для повторения:

Программа Wireshark не отображает поле преамбулы заголовка кадра. Что содержит преамбула?

В этом поле содержатся синхронизированные биты, обработанные сетевой платой.