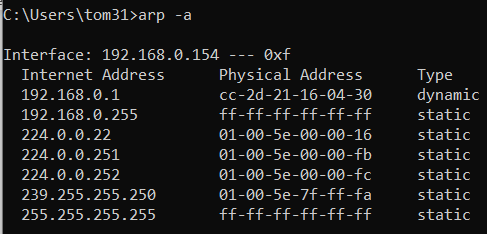
**Московка Артём, ИКБО-20-19, Лабораторная работа №9**

**Часть 1: Подготовка операционной системы компьютера**

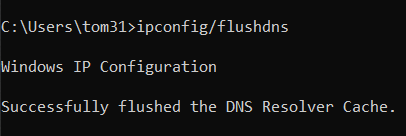
В части 1 потребуется подготовить операционную систему к захвату пакетов.

**Шаг 1:** Удаление результатов обращения к устройствам в сети.

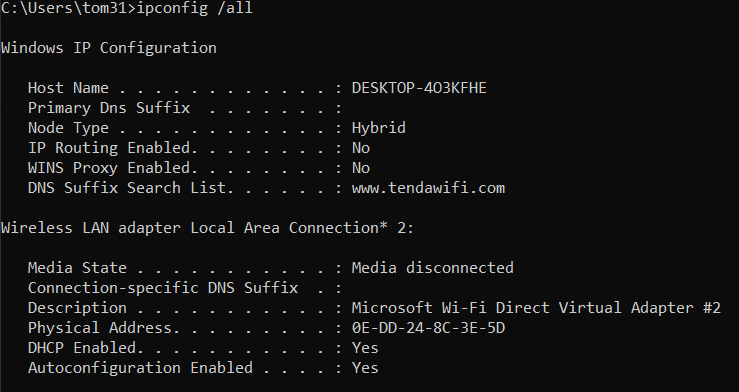
a. Очистите кеш ARP на компьютере.



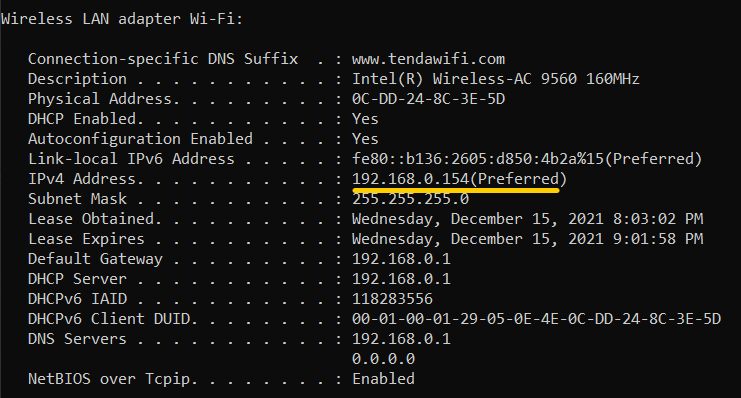
b. Очистите кеш DNS на компьютере.



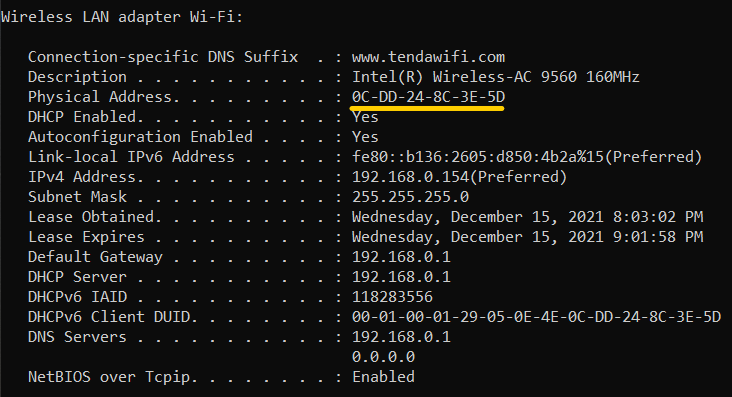
**Шаг 2:** Узнайте адреса интерфейсов ПК.



1. Определите ip адрес компьютера.

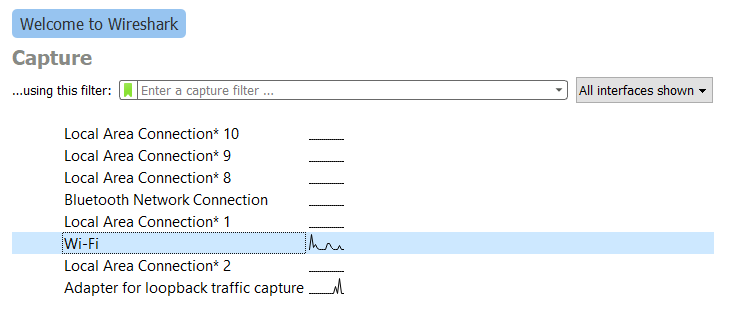


1. Определите MAC адрес компьютера.



**Часть 2: Захват, поиск и изучение пакетов**

**Шаг 1:** запустите программу Wireshark и выберите подходящий интерфейс.



**Шаг 2:** Захват пакетов.

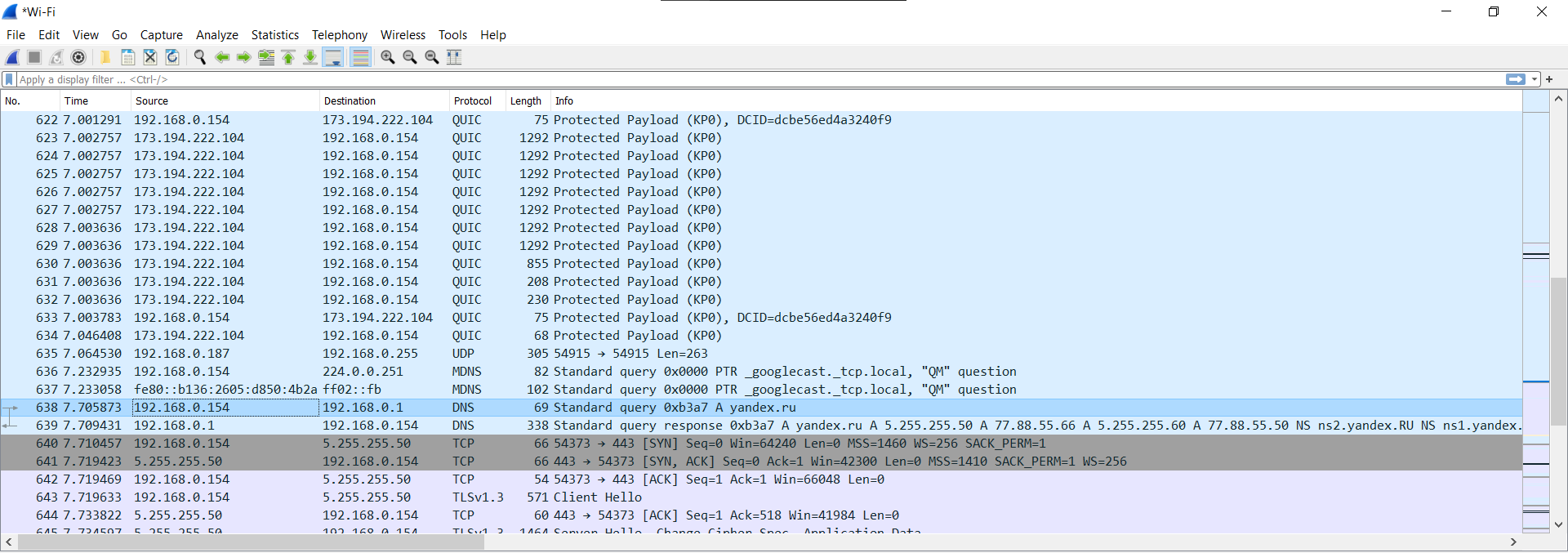
a. Нажмите кнопку Start (Старт), чтобы начать захват данных.

b. Откройте веб-сайт www.yandex.ru в браузере.

c. Сверните окно браузера и вернитесь в программу Wireshark. Остановите процесс захвата данных.

Вы увидите захваченный трафик.

Какие запросы выполнил компьютер прежде, чем обратился к серверу yandex.ru?



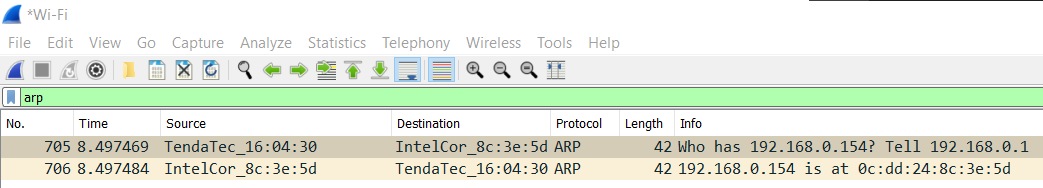
Обращение от моего компьютера с IP 192.168.0.154 к шлюзу по умолчанию с IP 192.168.0.1, далее от шлюза приходит ответ.

**Шаг 3:** Анализ пакетов ARP.

a. Отфильтруйте перехваченные данные оставив только кадры ARP.

Какой фильтр вы применили?

*Фильтр* ***arp*** *по протоколу ARP.*



b. Изучите поля в кадре ARP MAC адрес назначения которого является адресом компьютера.

Для чего нужен протокол ARP?

*Он определяет физический адрес при посылке пакета и отвечает на запросы других станций.*

Чей MAC адрес указан в кадре ARP?

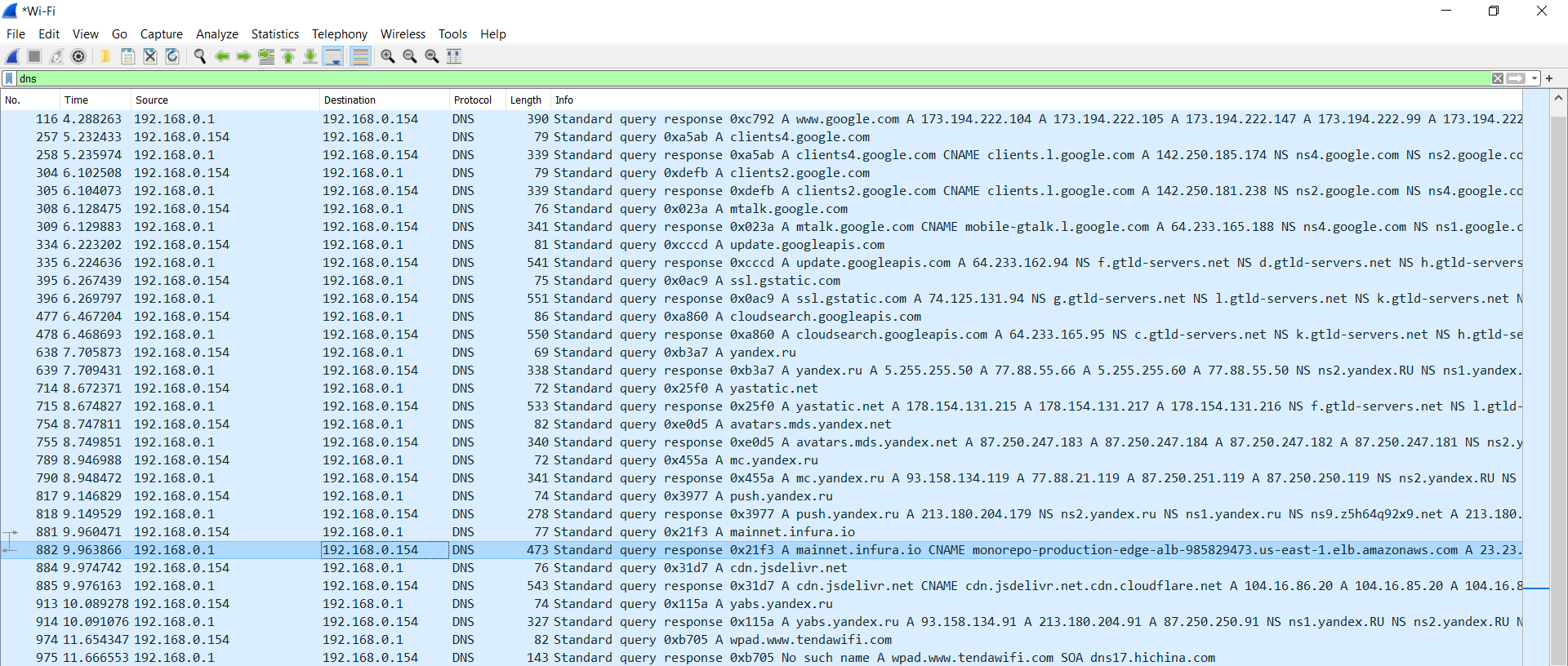
*Похоже, это MAC адрес серверного устройства сайта www.yandex.ru.*

**Шаг 4:** Анализ пакетов DNS.

a. Отфильтруйте перехваченные данные оставив только пакеты DNS.

Какой фильтр вы применили?

*Фильтр* ***dns*** *по протоколу DNS.*



b. Изучите поля в пакете DNS идущем от сервера к компьютеру.

Для чего нужен протокол DNS?

*Он нужен для хранения данных о соответствии имени домена конкретному IP-адресу, кэширования ресурсных записей прочих DNS-серверов.*

Какой IP адрес указан в поле протокола DNS и чему он принадлежит?

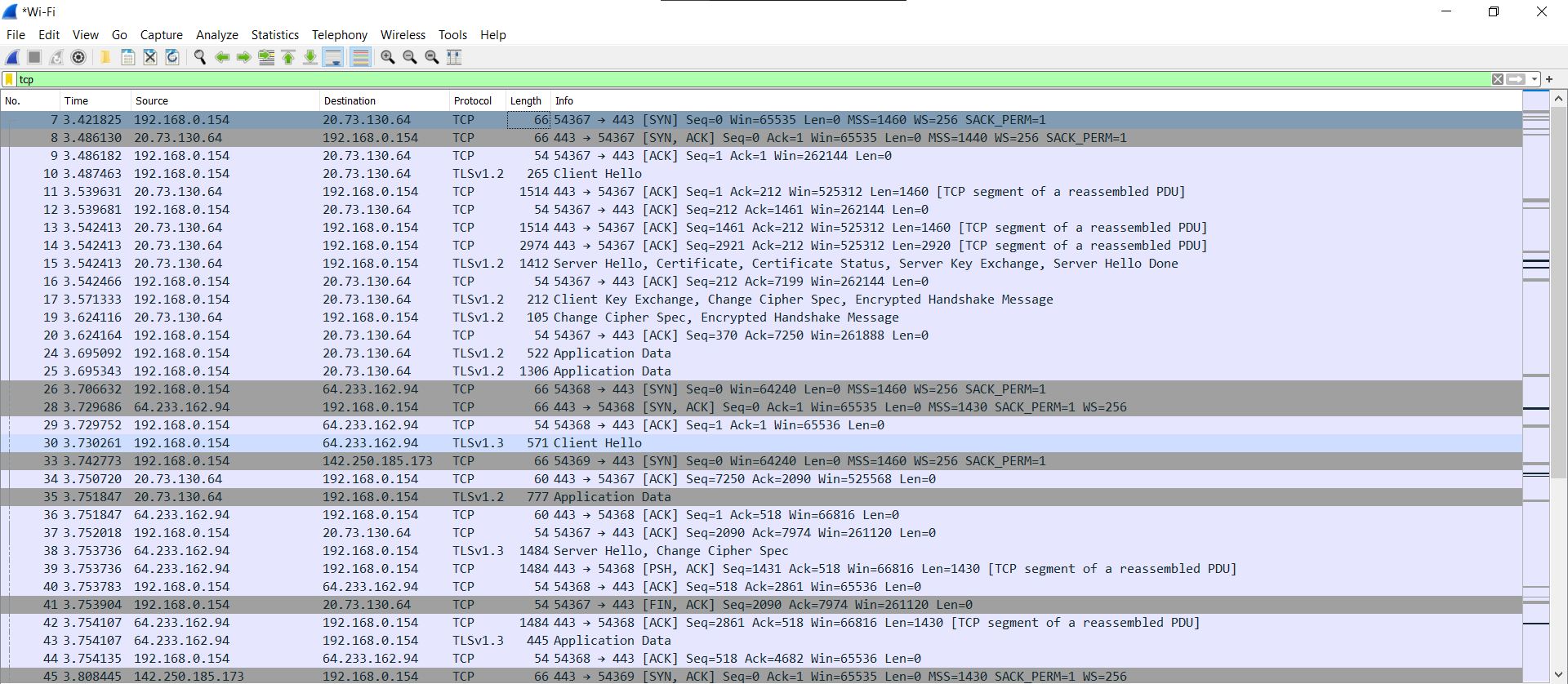
***192.168.0.1*** *– шлюз по умолчанию на моем маршрутизаторе,* ***192.168.1.154*** *– мой компьютер*

**Шаг 5: изучите трафик между компьютером и веб сервером.**

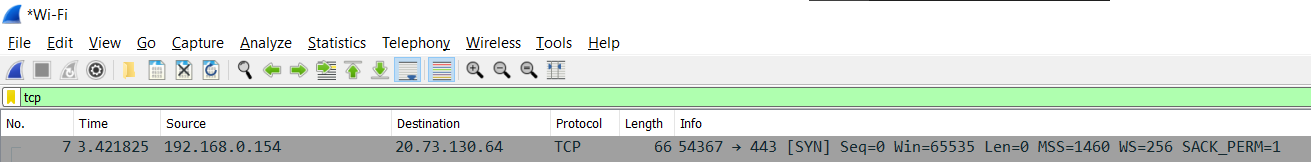
a. Отсортируйте данные таким образом, чтобы отображался только поток между компьютером и веб сервером.

Какой фильтр вы применили?

*Фильтр* ***tcp*** *по протоколу TCP.*



b. Найдите первый пакет, отправленный с компьютера на сервер yandex.ru.



Какую роль выполняет данный пакет?

*Запрос на создание TCP-сессии.*

Назовите номер порта источника TCP.

***192.168.0.154***

Как бы вы классифицировали порт источника?

*Частные – не регистрируются.*

Назовите номер порта назначения TCP.

*У первого TCP пакета* ***20.73.130.64***

Как бы вы классифицировали порт назначения?

*Общеизвестные.*

Какие установлены флаги?

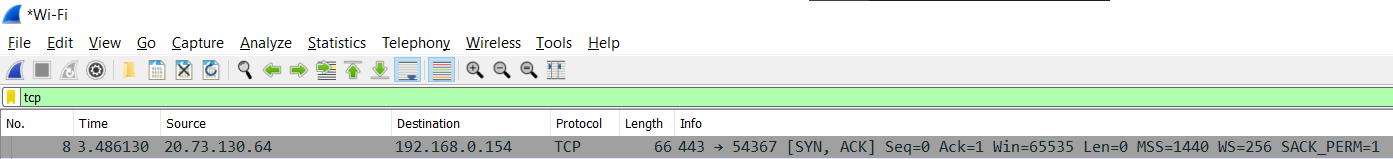
*Флаг* ***SYN*** *для установки сеанса между сервером и клиентом.*

На какое значение настроен относительный последовательный номер?

***54367***

c. Выберите следующий кадр в трёхстороннем рукопожатии.

*Отправка от сервера клиенту* ***SYN*** *и* ***ACK*** *флагов.*

**

Назовите значения портов источника и назначения.

***20.73.130.64*** *и* ***192.168.0.154***

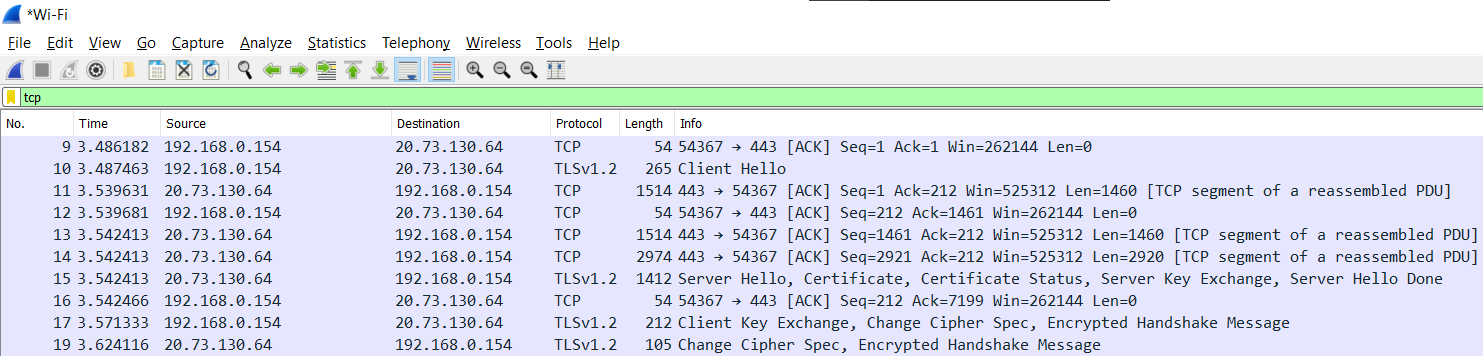
Какие установлены флаги?

***SYN*** *и* ***ACK***

На какие значения настроены относительный последовательный номер и номер подтверждения?

*Когда сообщение содержит флаг* ***ACK****, то значение в номере подтверждения должно соответствовать следующему порядковому номеру, которое отправитель сообщения с флагом* ***ACK*** *ожидает получить от передающей системы. Таким образом, отправка одного номера подтверждения способна подтвердить получение всех байтов с информацией, полученных до этого.*

d. Изучите третий и последний пакет трёхстороннего рукопожатия.



Какие установлены флаги?

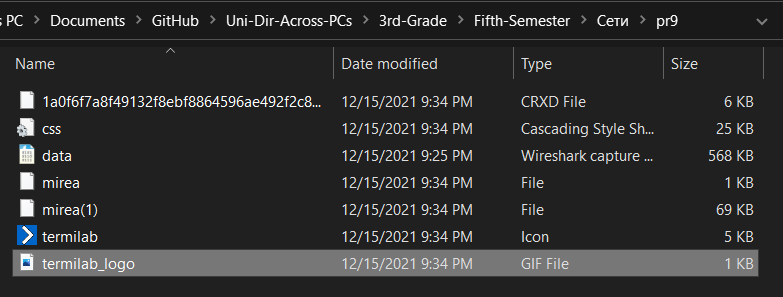
*Флаг* ***ACK****.*

**Шаг 6:** Восстановление сайта из собранных данных.

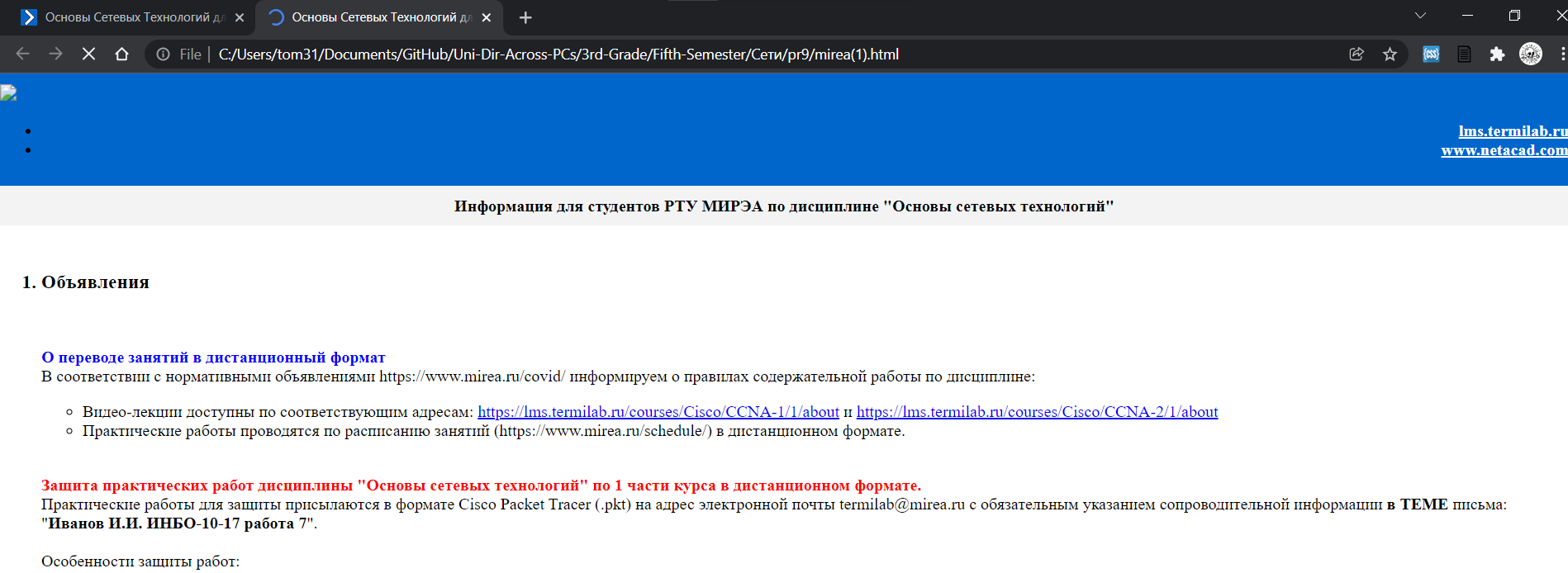
a. Повторите захват пакетов выполнив запрос в браузере к сайту по протоколу HTTP: http://termilab.ru/

или http://mirea.org/ или любой другой сайт, доступный по http://

b. Сохраните перехваченные данные от веб-сервера (HTTP трафик) на жесткий диск.



c. Запустите сайт с жесткого диска.



**Часть 3: Защита лабораторной работы**

1. В программе Wireshark доступны сотни фильтров. В большой сети может быть множество фильтров и различных типов трафика. Какие три фильтра в списке будут наиболее полезны для сетевого администратора?

*TCP,*

*конкретные IP-адреса (источник или место назначения);*

*протоколы, такие как HTTP.*

2. Как ещё можно использовать программу Wireshark в производственной сети?

*Wireshark часто используется в целях безопасности для анализа обычного трафика или после сетевой атаки. Может потребоваться захват новых протоколов или служб, чтобы определить, какой порт или порты используются.*