

**Лабораторная работа №9. Изучение пакетов с помощью программы Wireshark**

**Топология**

**Задачи**

**Часть 1. Подготовка операционной системы компьютера Часть 2. Захват поиск и изучение пакетов**

**Часть 3. Защита лабораторной работы (ответы на контрольные вопросы и вопросы преподавателя)**

**Необходимые ресурсы**

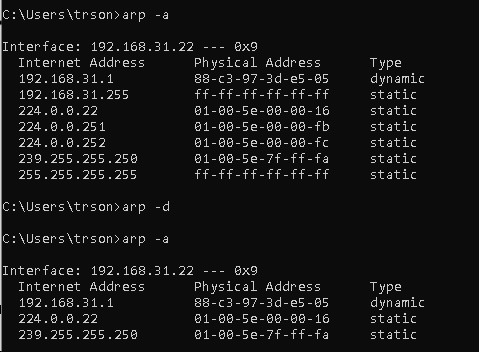
 1 ПК с доступом к командной строке, Интернету и установленному анализатору пакетов Wireshark.

**Часть 1: Подготовка операционной системы компьютера**

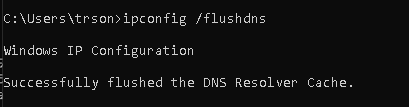
В части 1 потребуется подготовить операционную систему к захвату пакетов.

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

1. Очистите кеш ARP на компьютере.

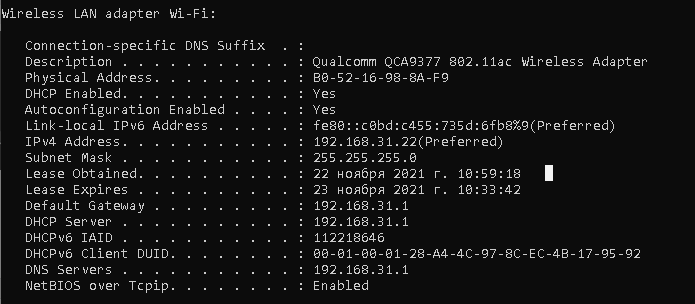


1. Очистите кеш DNS на компьютере.



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

1. Определите ip адрес компьютера.



b. 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](http://www.yandex.ru/) в браузере.

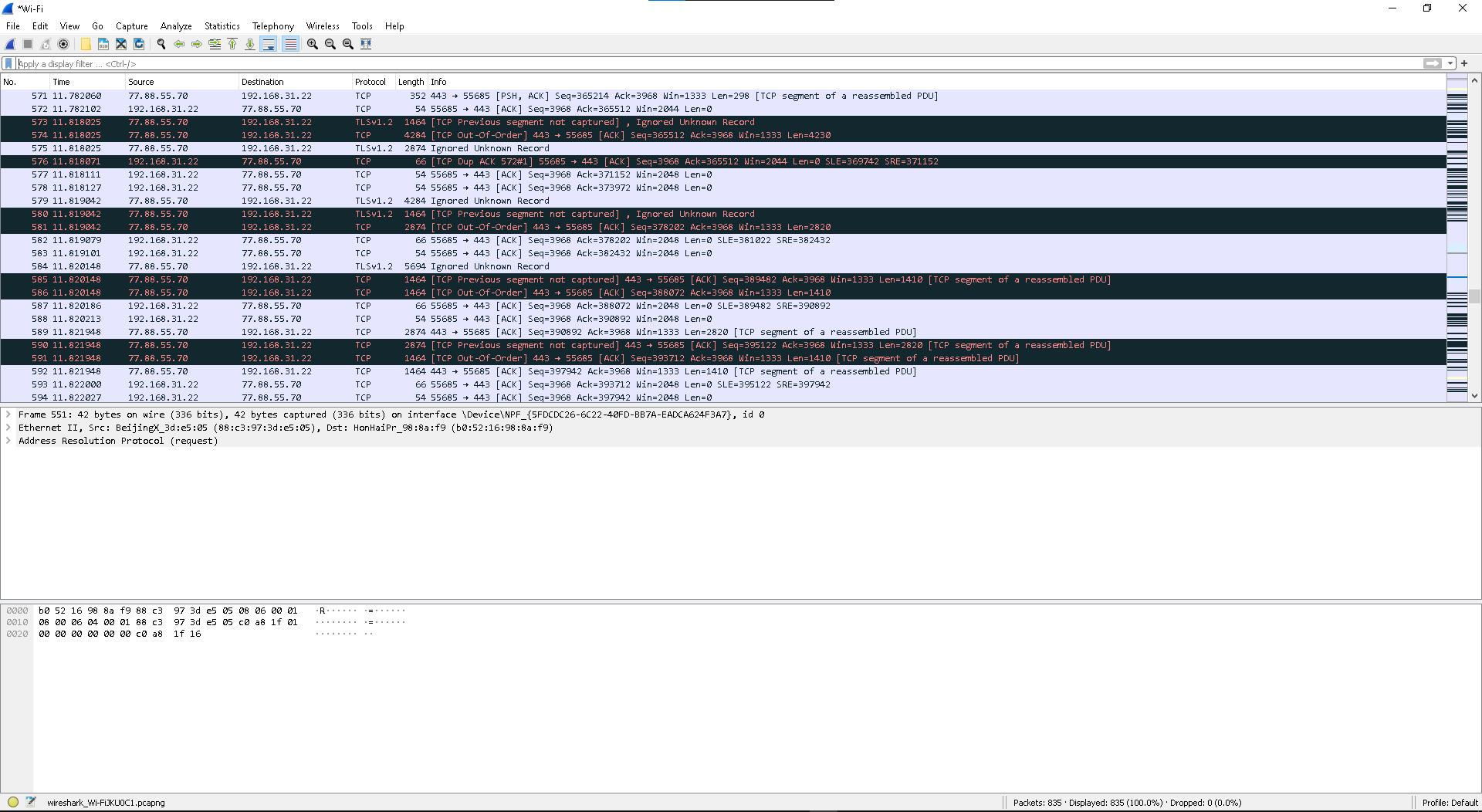
© Компания Cisco и/или ее дочерние компании, 2019 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco. Страница **1** из **3**

**Лабораторная работа. Изучение пакетов с помощью программы Wireshark**

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

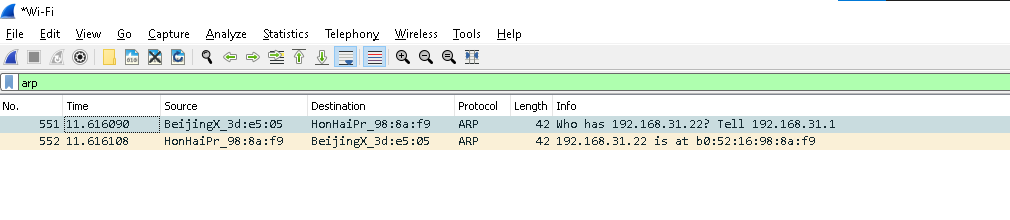
Вы увидите захваченный трафик.

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



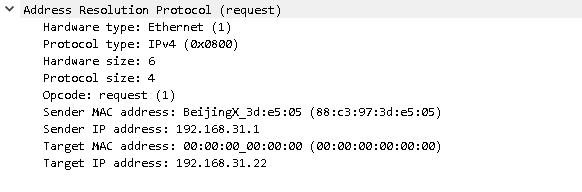
**Шаг 3: Анализ пакетов ARP.**

1. Отфильтруйте перехваченные данные оставив только кадры ARP.



Какой фильтр вы применили? - **arp**

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

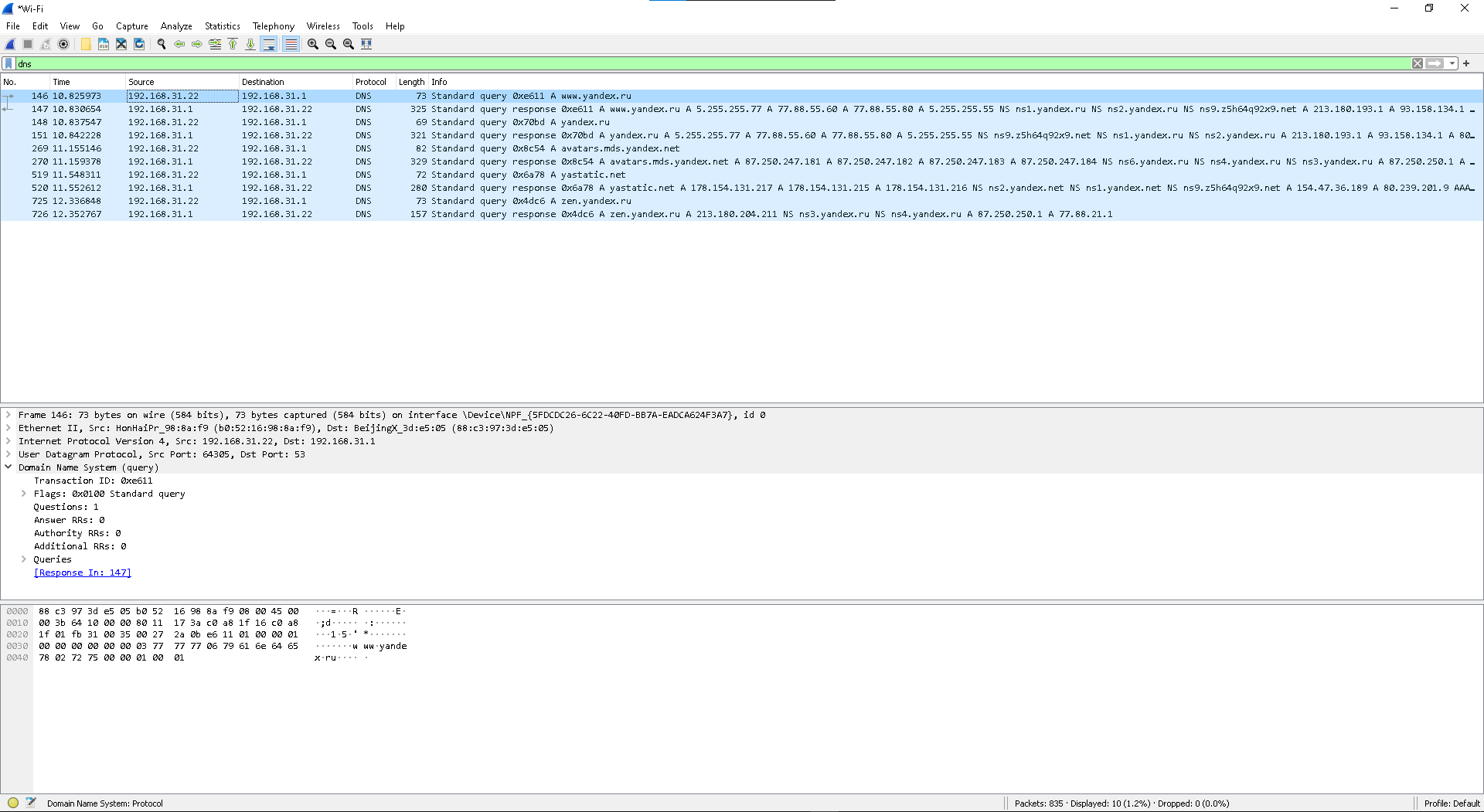


Для чего нужен протокол ARP? **- ARP** **— протокол в компьютерных сетях, предназначенный для определения *MAC-адреса* по IP-адресу другого компьютера**

Чей MAC адрес указан в кадре ARP? - **MAC-адрес компьютера**

**Шаг 4: Анализ пакетов DNS.**

1. Отфильтруйте перехваченные данные оставив только пакеты DNS.



Какой фильтр вы применили? - **dns**

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

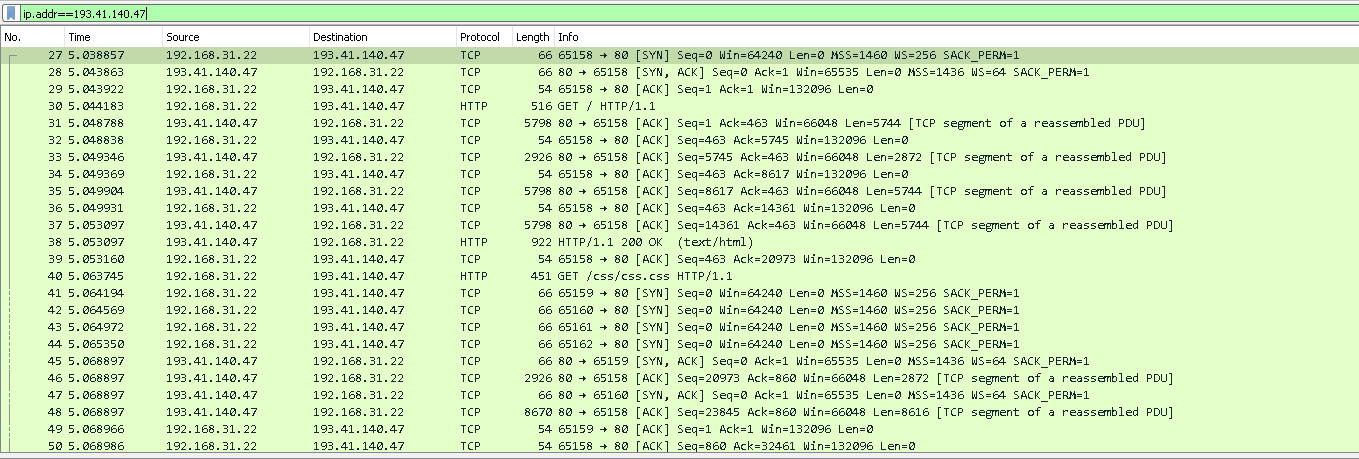
Для чего нужен протокол DNS? - **DNS — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты и/или обслуживающих узлах для протоколов в домене**

Какой IP адрес указан в поле протоколы DNS и чему он принадлежит? **указанный IP-адрес является IP-адресом сервера**

**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? – **ip.addr==193.41.140.47**

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



Какую роль выполняет данный пакет? - **отправить запрос с компьютера на сервер, чтобы запросить соединение (установлен флаг SYN)**

Назовите номер порта источника TCP. - **65158**

Как бы вы классифицировали порт источника? **Динамический**

Назовите номер порта назначения TCP. - **80**

Как бы вы классифицировали порт назначения? **- HTTP**

Какие установлены флаги? **– Флаг SYN**

На какое значение настроен относительный последовательный номер? **– seq = 0**

1. Выберите следующий кадр в трёхстороннем рукопожатии. **- Это веб-сервер, отвечающий на исходный запрос для начала сеанса.**



Назовите значения портов источника и назначения. - **Источник: 80, Назначение 65158**

Какие установлены флаги? **- SYN и ACK**

На какие значения настроены относительный последовательный номер и номер подтверждения?**– Последовательность: 0 и Подтверждение: 1**

1. Изучите третий и последний пакет трёхстороннего рукопожатия.

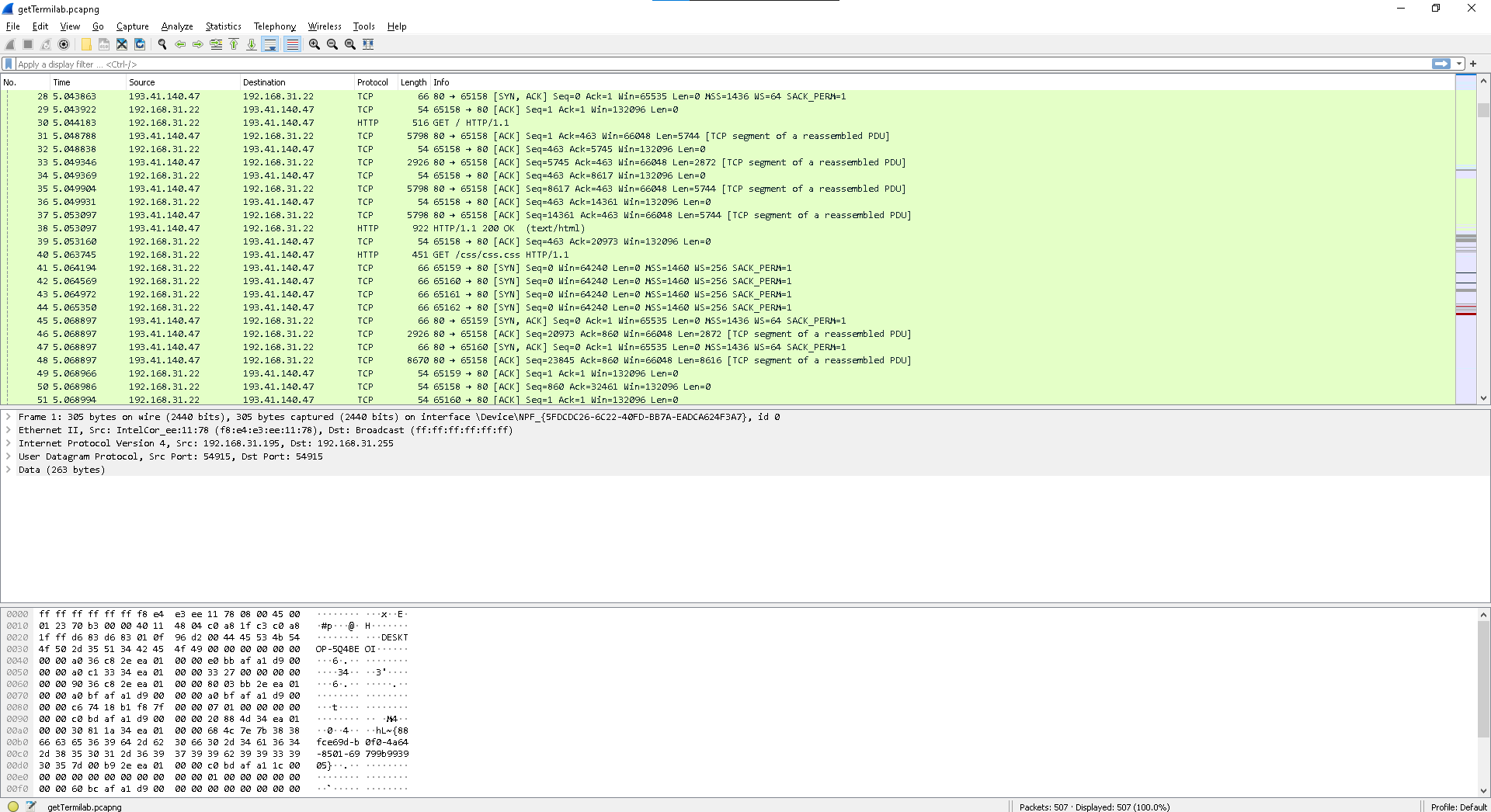


Какие установлены флаги? - **АСК**

**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://

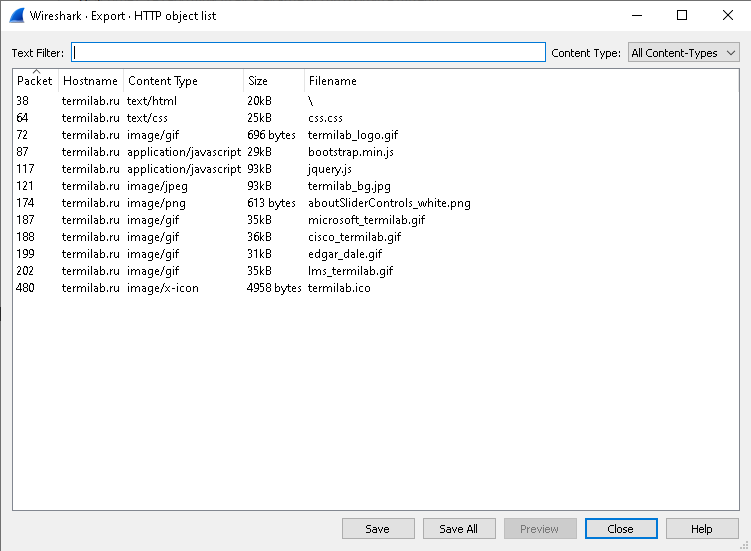


Захват пакетов выполнив запрос в браузере к сайту по протоколу HTTP: <http://termilab.ru/>

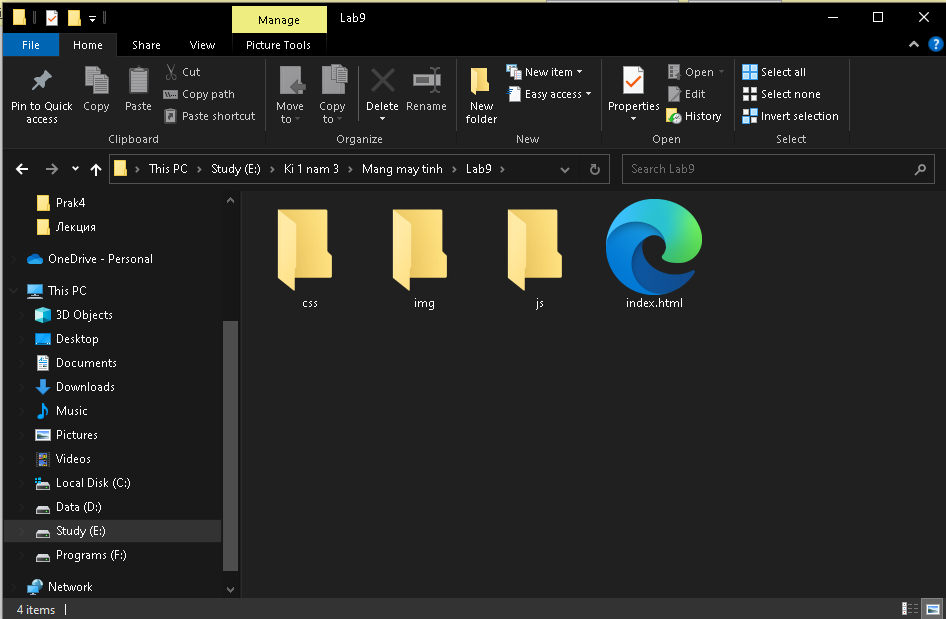
© Компания Cisco и/или ее дочерние компании, 2019 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco. Страница **2** из **3**

**Лабораторная работа. Изучение пакетов с помощью программы Wireshark**

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

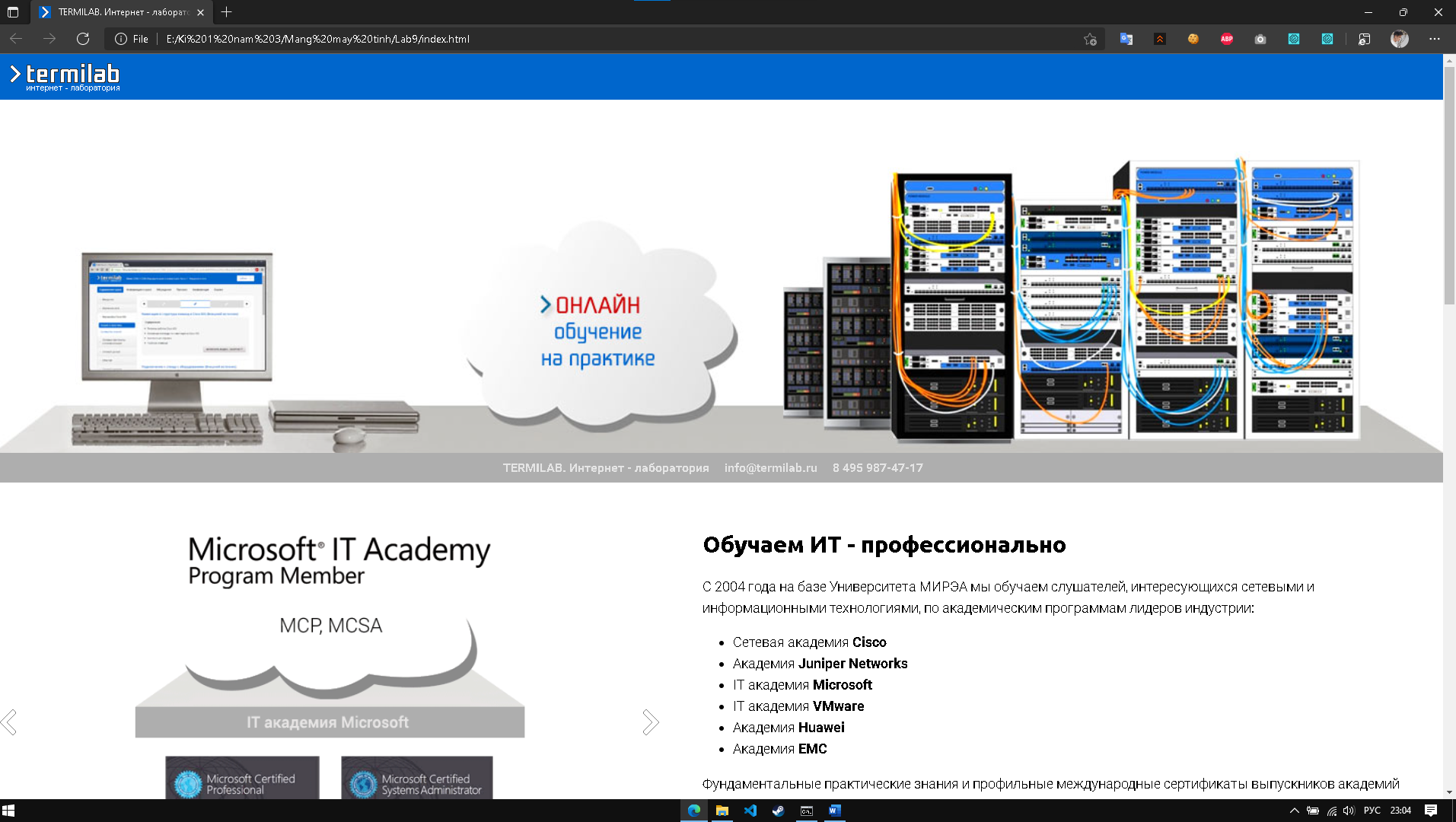


Перехваченные данные от веб-сервера



Сохранит на жесткий диск.

1. Запустите сайт с жесткого диска.



**Часть 3: Защита лабораторной работы (ответы на контрольные**

**вопросы и вопросы преподавателя)**

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? - **contains, arp, dns, ip**

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

- Администраторы сетей используют ее для выявления причин неполадок в сетях.

- Специалисты по безопасности сетей используют ее для поиска проблем с безопасностью.

- Разработчики используют ее для отладки реализаций протоколов.

- Пользователи используют ее для изучения принципов работы сетевых протоколов.

© Компания Cisco и/или ее дочерние компании, 2019 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco. Страница **3** из **3**