|  |  |
| --- | --- |
| Министерство образования Республики Беларусь | |
| Учреждение образования | |
| БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ | |
| ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ | |
|  | |
|  | |
| Факультет компьютерных систем и сетей | |
| Кафедра программного обеспечения информационных технологий | |
| Дисциплина: **Название дисциплины (АББРЕВИАТУРА)** | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
| **ОТЧЁТ** | |
| по лабораторной работе № **X** | |
|  | |
| Тема работы: **Название темы** | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
| Выполнил: | Фамилия И.О. |
|  | гр. **XXXXXX** |
|  | Вариант **X** |
|  |  |
| Проверил: | Фамилия И.О. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| Минск **202X** | |

**Вариант 7**

## Задание 5 Ethernet

1) очистить кэш браузера;

2) запустить Wireshark;

3) запустить процесс захвата трафика;

4) Найти URL c протоколом http. Для этого можно выполнить поисковый запрос в Google: inurl:http -inurl:https

В URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции, либо выбрать URL по номеру результата поиска, совпадающего с номером в группе.

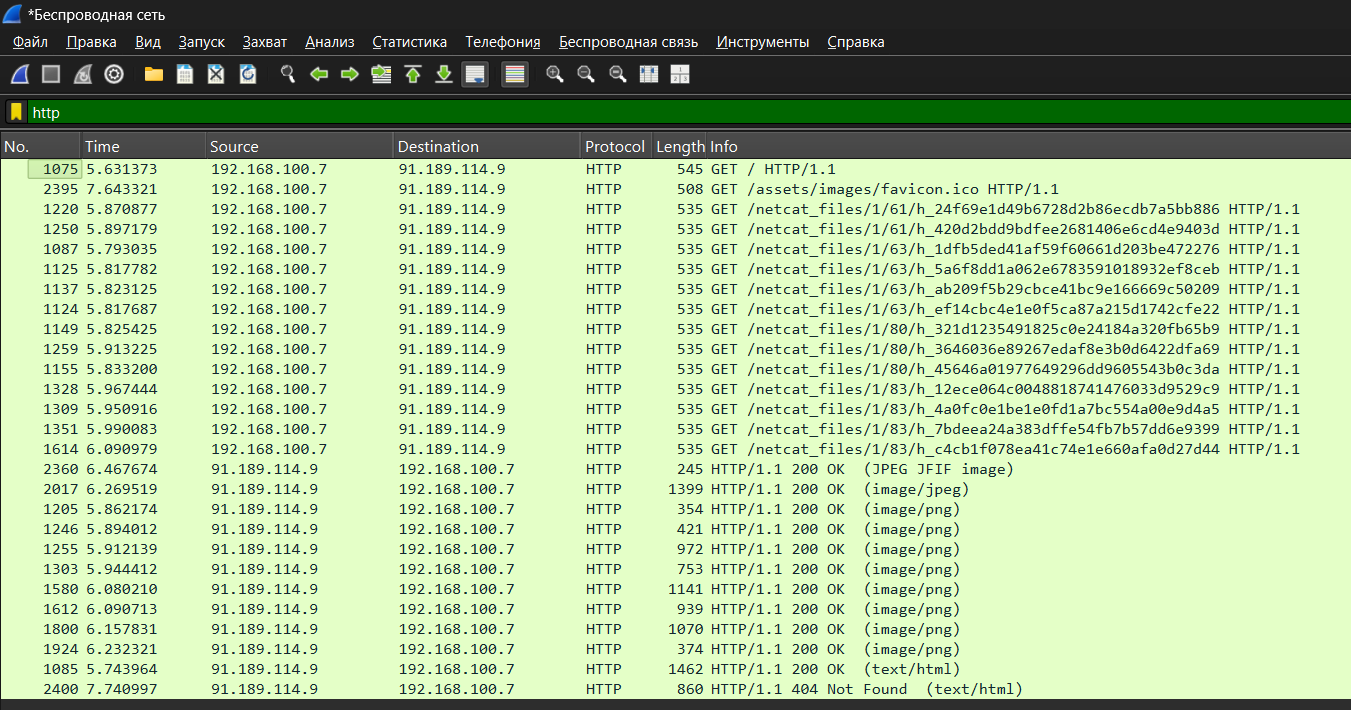
В моём случае, фамилия ----ky, выбираю три буквы — sky. Http-сайт с такими буквами будет найти достаточно просто.

Нашёлся сайт <http://sky-group.aero/>

5) остановить захват трафика;

6) в меню «Анализ» → «Enabled Protocols» можно снять галочку IP:тогда в списке пакетов не будет отображаться информация по протоколам верхнего уровня (после IP) — (необязательный пункт).

 Выберите кадр Ethernet, содержащий сообщение HTTP GET.



Ответьте на следующие вопросы.

* Укажите 48-битный Ethernet адрес вашего компьютера.

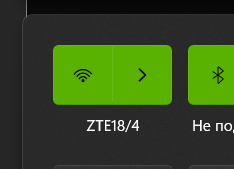


* Укажите 48-битный Ethernet адрес назначения.



* Что это за адрес? (Адрес сервера?)

Судя по названию zte, я предполагаю, что это мой роутер вайфая.



* Укажите 16-чное значение двухбайтового поля «Type»: какому протоколу верхнего уровня оно соответствует?



Оно соответствует HTTP.

Выберите кадр Ethernet, содержащий ответ HTTP. Ответьте на следующие вопросы.

* Укажите значение Ethernet адреса источника. Какое устройство имеет такой адрес?



Я думаю, что это мой роутер вайфая.

* Укажите Ethernet адрес назначения: это адрес вашего компьютера?



Да, это адрес моего компьютера.

* Укажите 16-чное значение двухбайтового поля «Type»: какому протоколу верхнего уровня оно соответствует?



Это HTTP.

## Задание 8. UDP

1) запустить Wireshark;

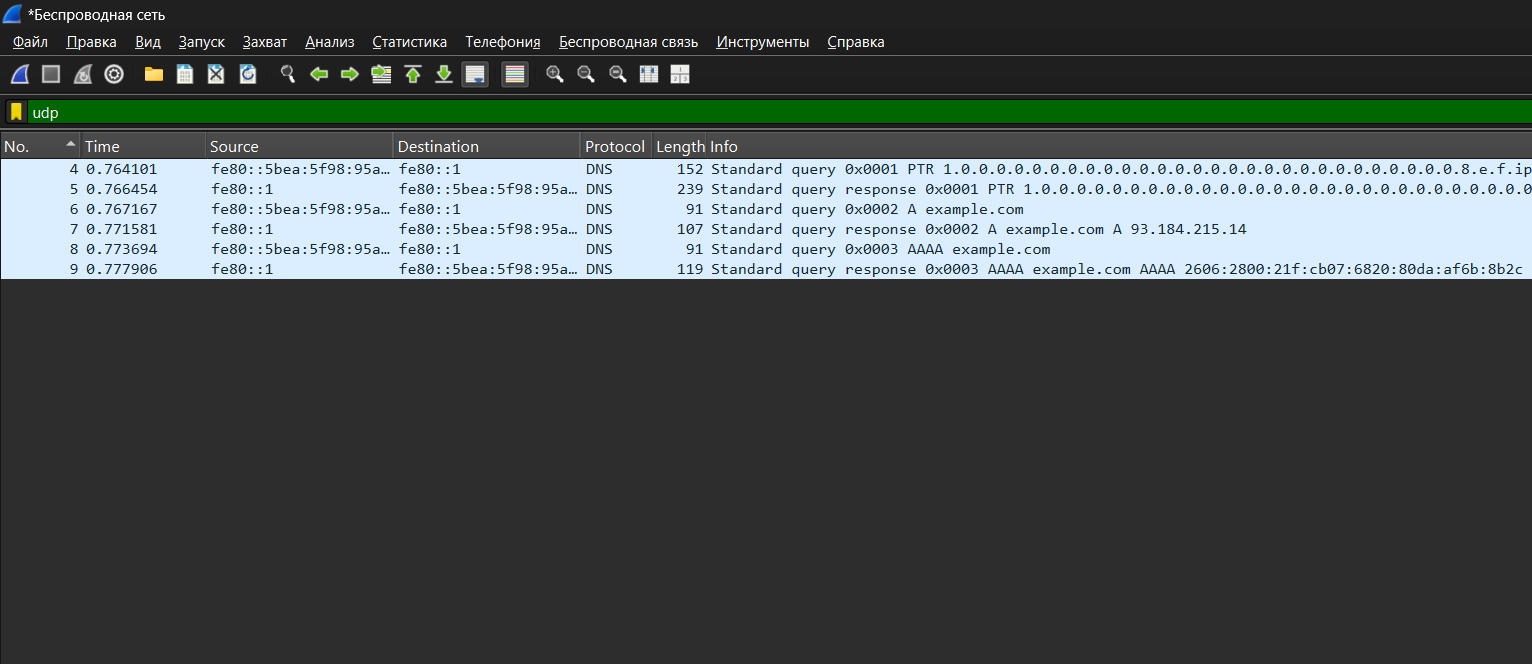
2) настроить фильтр (udp);

3) запустить процесс захвата трафика;

4) использовать команду nslookup (см. DNS);

Я использовал nslookup <https://example.com/>

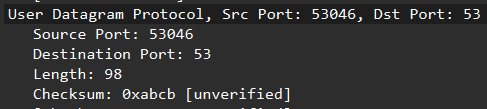
5) остановить захват трафика.



Ответьте на следующие вопросы.

* Выберите один UDP пакет из списка пакетов. Сколько полей в UDP заголовке? Что это за поля?

Их четыре, вот они



* Какова длина (в байтах) каждого поля заголовка?









Протыкав каждое поле, можно заметить, что везде подсвечиваются два байта.

* Длина чего указана в поле «Length»?

Указывает общую длину UDP заголовка и данных в байтах.

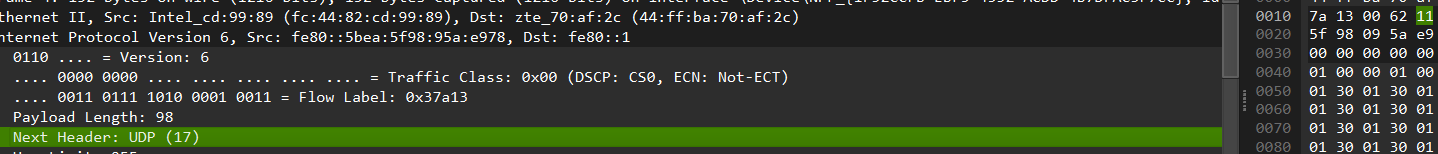
* Какова максимальная длина поля данных UDP?

Максимальная длина поля данных UDP составляет **65,507 байт** (вместе с заголовком 65,535 байт, минус 8 байт заголовка UDP).

* Какой максимально возможный номер порта источника?

Максимально возможный номер порта источника составляет **65,535**.

* Укажите номер протокола для UDP (см. соответствующее поле IP- дейтаграммы) в 10-чном и 16-чном виде.



17 (11)

## Задание 9. TCP

1) запустить Wireshark;

2) запустить процесс захвата трафика;

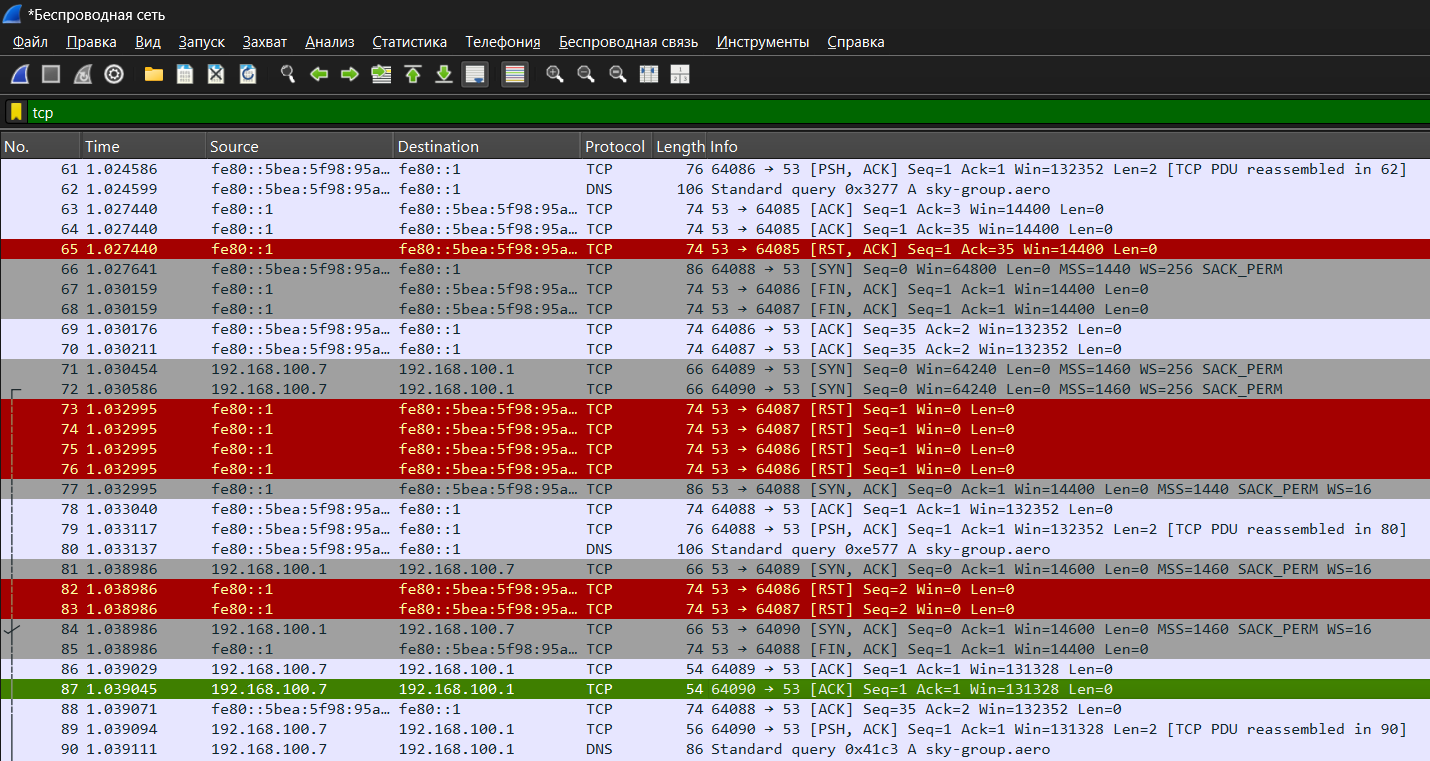
3) открыть любой сайт; в URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции;

В моём случае, фамилия Burbovsky, выбираю три буквы — sky. Http-сайт с такими буквами будет найти достаточно просто.

Нашёлся сайт <http://sky-group.aero/>

4) остановить захват трафика;

5) настроить фильтр просмотра для просмотра сегментов tcp.



Пояснить каким образом происходит начало TCP-сессии (процесс трехэтапного рукопожатия).

1) Клиент отправляет сегмент с установленным флагом синхронизации.

2) Сервер получает запрос и отправляет ответный сегмент с одновременно установленными флагами синхронизации и подтверждения.

3) После получения клиентом сегмента с флагами синхронизации и подтверждения соединение считается установленным. Клиент, в свою очередь, отправляет в ответ сегмент с флагом подтверждения.

4) Начинается передача данных.