|  |  |  |  |
| --- | --- | --- | --- |
| МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН  СЕВЕРО-КАЗАХСТАНСКИЙ УНИВЕРСИТЕТ ИМ. М. КОЗЫБАЕВА  ФАКУЛЬТЕТ ИНЖЕНЕРИИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ  КАФЕДРА «ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ» | | | |
|  | | | |
|  | | |  |
| ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №8  Тема: Контроль доступа к Web-сайтам с помощью программы Wireshark. | | | |
| Выполнил студент  группы АПО-22 |  | Захаров Д.М. | |
| Проверил  преподаватель |  | Куликов В.П. | |
|  |  |  | |
|  |  |  | |

Петропавловск, 2024

**Цель**

Приобрести навыки для мониторинга доступа к веб-сайтам.

**Инструменты необходимые для выполнения лабораторной работы**

* Анализатор трафика Wireshark;
* Браузер

**Задание**

1. Захватить трафик;
2. Рассмотреть способы мониторинга доступа к веб-сайтам;
3. Подготовить отчет в виде скриншотов каждого шага с краткими пояснениями.

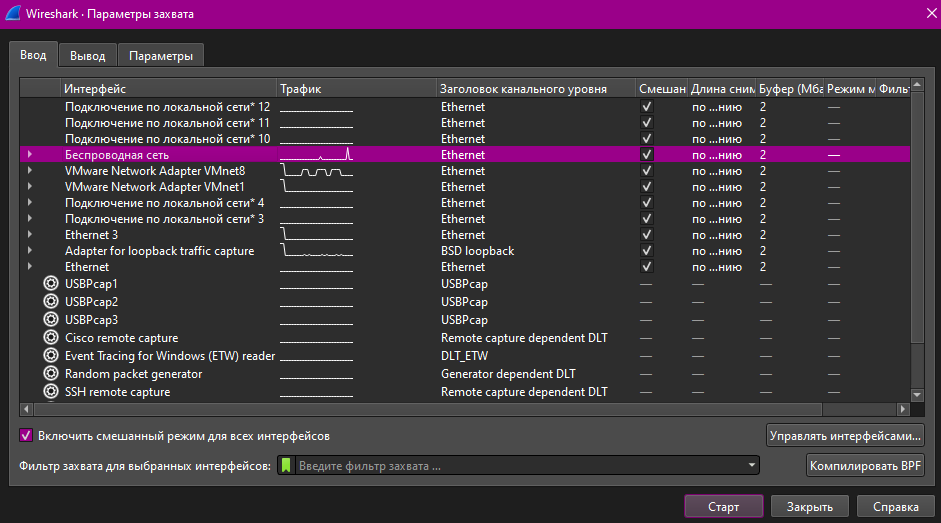
***Этап 1. Захват трафика***

Для выполнения этапа 1 нам потребуется:

* Запустить захват трафика;
* Перейти на сайт http://www.sfu-kras.ru/. В результате перехода на сайт, между сервером и клиентом начнется обмен HTTP-пакетами, которые захватит Wireshark;
* Остановить захват трафика.

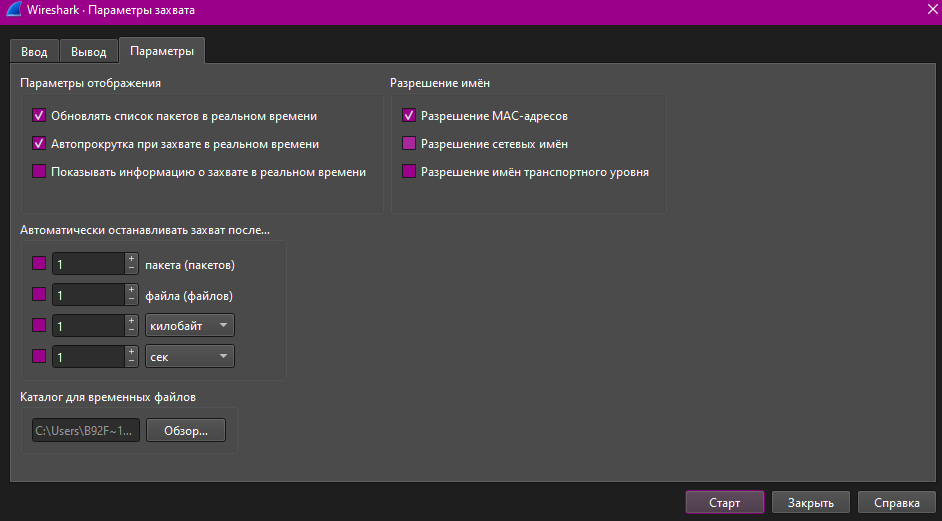
**Запуск захвата трафика**

1. Запустите программу Wireshark, расположенную в Пуск\Wireshark;
2. Подготовьте Wireshark для захвата трафика. Напомним, что подготовка завершается выбором сетевого интерфейса в окне «Интерфейсы Захвата»;

  
Рисунок 1. Окно «Параметры захвата».

1. В окне «Интерфейсы Захвата» перейдите во вкладку «Опции» и установите флажок «Разрешить сетевые имена»;

**Примечание.** Установка флажка «Разрешить сетевые имена» позволит заменить IP-адреса всех веб-сайтов на символьные имена (в том числе это касается и того сайта, который мы будем использовать).

  
Рисунок 2. Вкладка «Параметры».

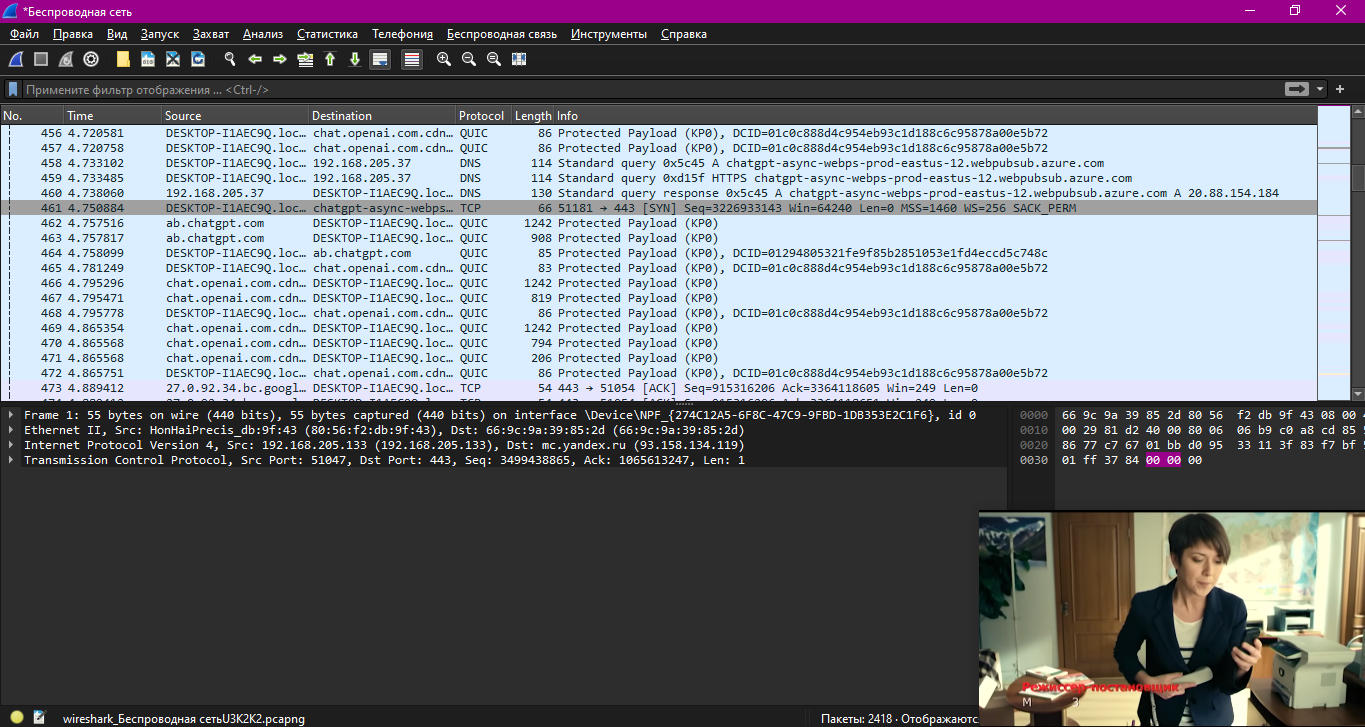
1. Нажмите кнопку «Старт» для запуска захвата трафика;

**Переход на сайт** [**http://chat.openai.com/**](http://chat.openai.com/)

1. Сверните окно Wireshark. Откройте любой браузер (например, Internet Explorer) и перейдите на сайт <http://chat.openai.com/>;
2. Закройте окно браузера и разверните окно Wireshark;

**Остановка захвата трафика**

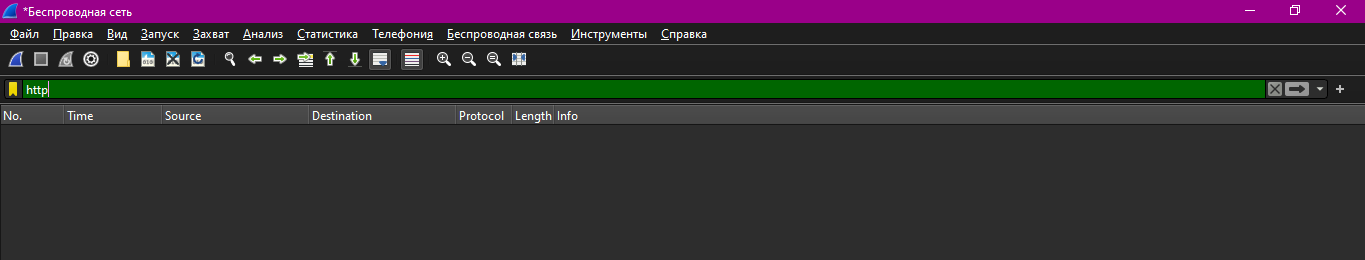
1. Остановите захват пакетов, нажав на кнопку «Остановить захват трафика» на панели инструментов Wireshark;

  
Рисунок 3. Получение захваченного трафика.

**Примечание.** Не закрывая окно программы Wireshark, перейдите к выполнению этапа 2.

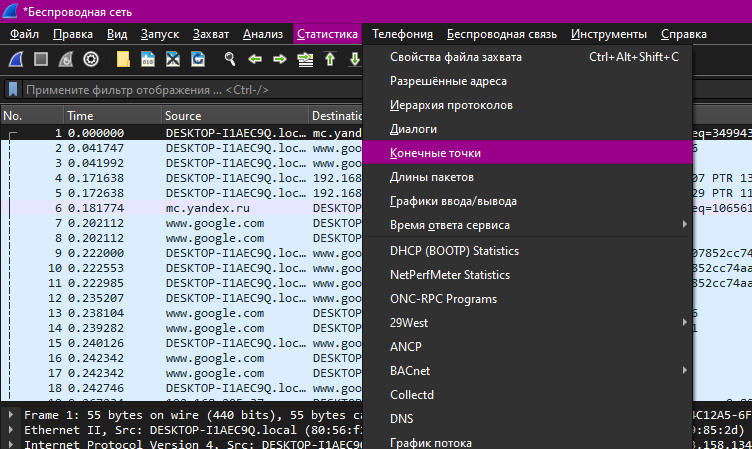
***Этап 2. Мониторинг доступа к веб-сайтам***

1. В главном окне Wireshark в поле «Фильтр» введите правило фильтра «http»;

  
Рисунок 4. Не было найдено ни одного http-пакета.

**Примечание.** На панели «Список пакетов» можно просматривать все сайты, которые посещал пользователь. Этот способ неудобен, так как одному сайту соответствует сразу несколько захваченных пакетов, и, если пользователь обращался к большому количеству сайтов, тогда обнаружить их все будет крайне трудно. Рассмотрим еще один способ мониторинга доступа к веб-сайтам.

1. В главном окне Wireshark перейдите в «Статистика» -> «Конечные точки»;

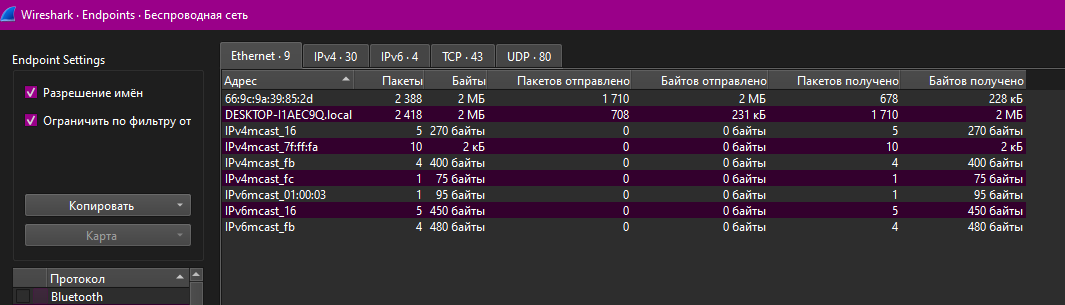
  
Рисунок 5. Открытие окна Endpoints.

1. Появляется окно «Endpoints». В его верхней части отображаются панель, в которой включены вкладки с названием протоколов или семейства протоколов (Ethernet, IPv4, IPv6, TCP и UDP). Рядом с названием протоколов расположены метки. Метка показывает количество захваченных конечных точек (смысл которых определён ниже). Значение метки зависит от текущего сеанса захвата. В данном случае метки имеют следующие значения:

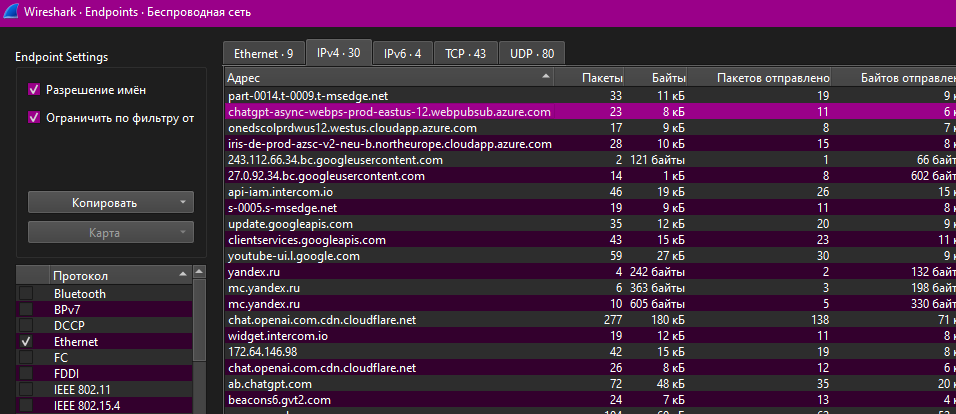
* Для протокола Ethernet - 9;
* Для протокола IPv4 - 30;
* Для протокола TCP - 43.

В нижней части окна расположена кнопка «Endpoint Типы», которая позволяет включать и отключать вкладки протоколов, и 2 флажка:

* **Разрешение имен** - заменить IP-адреса на символьные имена;
* **Ограничить соответственно дисплейному фильтру** - отобразить конечные точки, соответствующие введенному ранее дисплейному фильтру (фильтру отображения). Установите оба флажка, чтобы увидеть символьные адреса вебсайтов и отбросить пакеты, несоответствующие фильтру отображения (т.е. исключаем из рассмотрения ненужную информацию);

  
Рисунок 6. Установка флажков.

1. В верхней части окна кликните по вкладке «IPv4». В ней отображаются конечные точки, соответствующие протоколу IPv4, и их некоторые параметры. В столбце «Address» располагаются адреса веб-ресурсов, с которыми ваш компьютер обменивался пакетами (один из них chatgpt-async-webps-prod-eastus-12.webpubsub.azure.com). Используя эту информацию можно отслеживать доступ к веб-сайтам. Этот способ более удобен, так как одному веб-сайту соответствует одна запись.

  
Рисунок 7. Вкладка IPv4.

**Список использованных ресурсов**

<http://chat.openai.com/>

<https://is.ku.edu.kz/methodpages/qwertyrant/Laboratornuei_praktikum_po_informacionnoi_bezopasnosti.pdf>

<https://networkguru.ru/wireshark/>