Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра интеллектуальных информационных технологий

**Отчет по лабораторной работе №3**

**по курсу «СиМОИБ»**

**на тему: «Наблюдение за стеком TCP/IP»**

|  |  |
| --- | --- |
| Выполнил студент группы 021702: | Локтев К.А. |
| Проверил: | Захаров В. В. |

**МИНСК**

**2022**

**Задания:**   
1. Установите программы, необходимые для перехвата сетевого трафика.   
2. Изучите различные параметры работы программ для перехвата сетевого трафика. 3.Выполните анализ трафика (с различными параметрами детализации):  
 1. Ping-запроса,   
 2. HTTP трафика при загрузке любого веб-ресурса,   
 3. аутентификацию в веб-ресурсе, на котором не настроен HTTPS,   
 4. SSH, SCP трафика,  
 5. FTP трафика и т. д.   
4. Определите, к каким портам и адресам были выполнены обращения.   
5. Используя дополнительную литературу, расшифруйте содержание перехваченных пакетов.

**Ход работы**

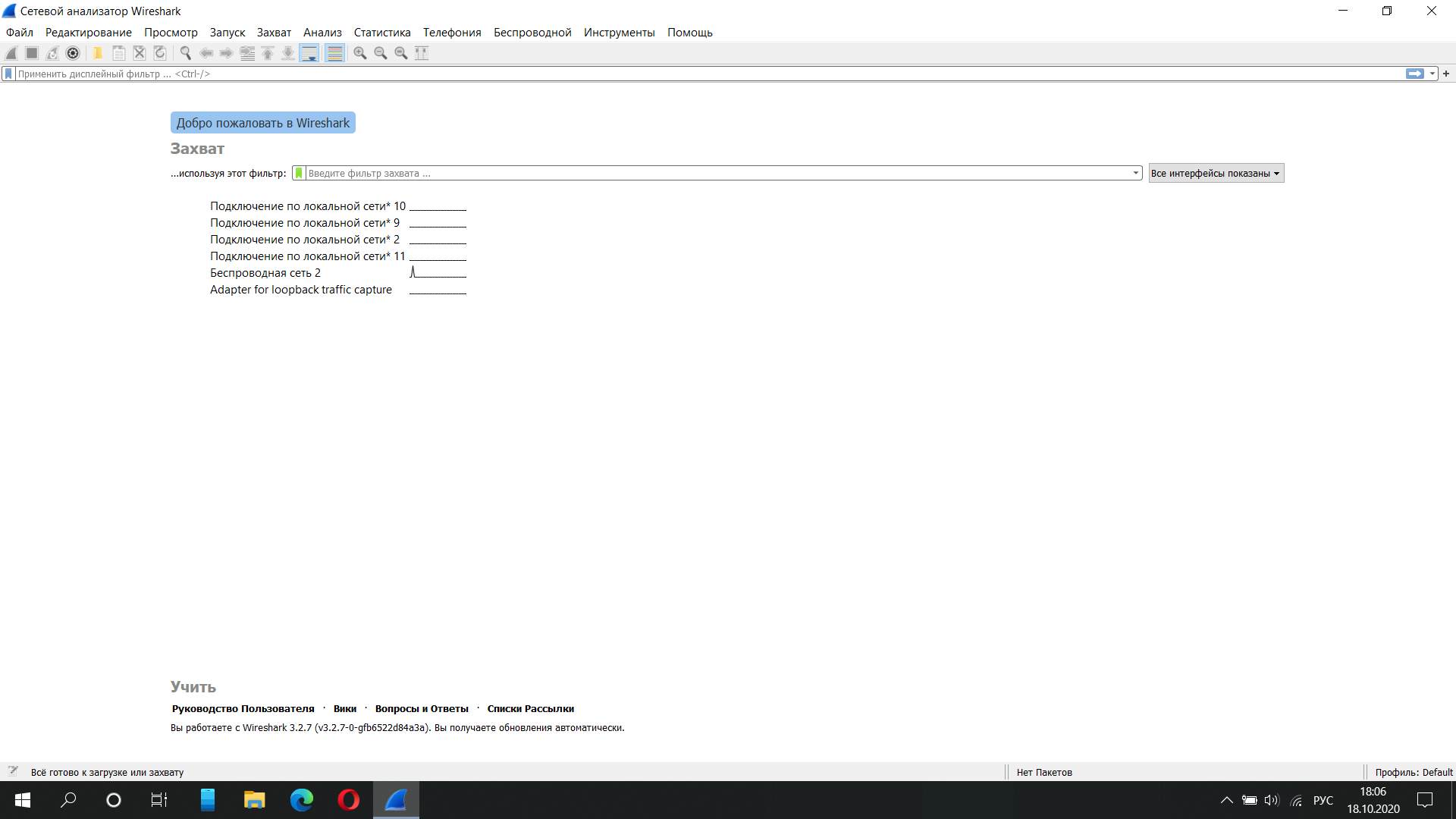
**1.** Для выполнения лабораторной работы скачана и установлена программа Wireshark.

Рисунок 1 Окно приложения

Запрос пинга для yandex.ru

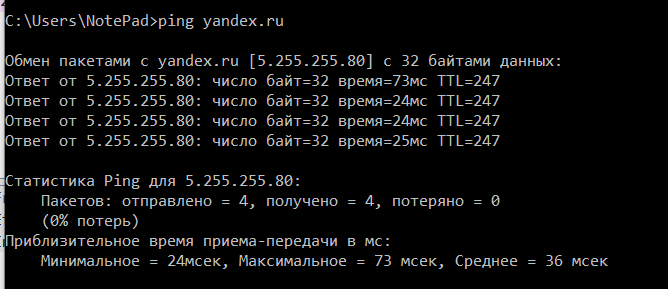


Рисунок 2 Интерфейс редактора групповой политики

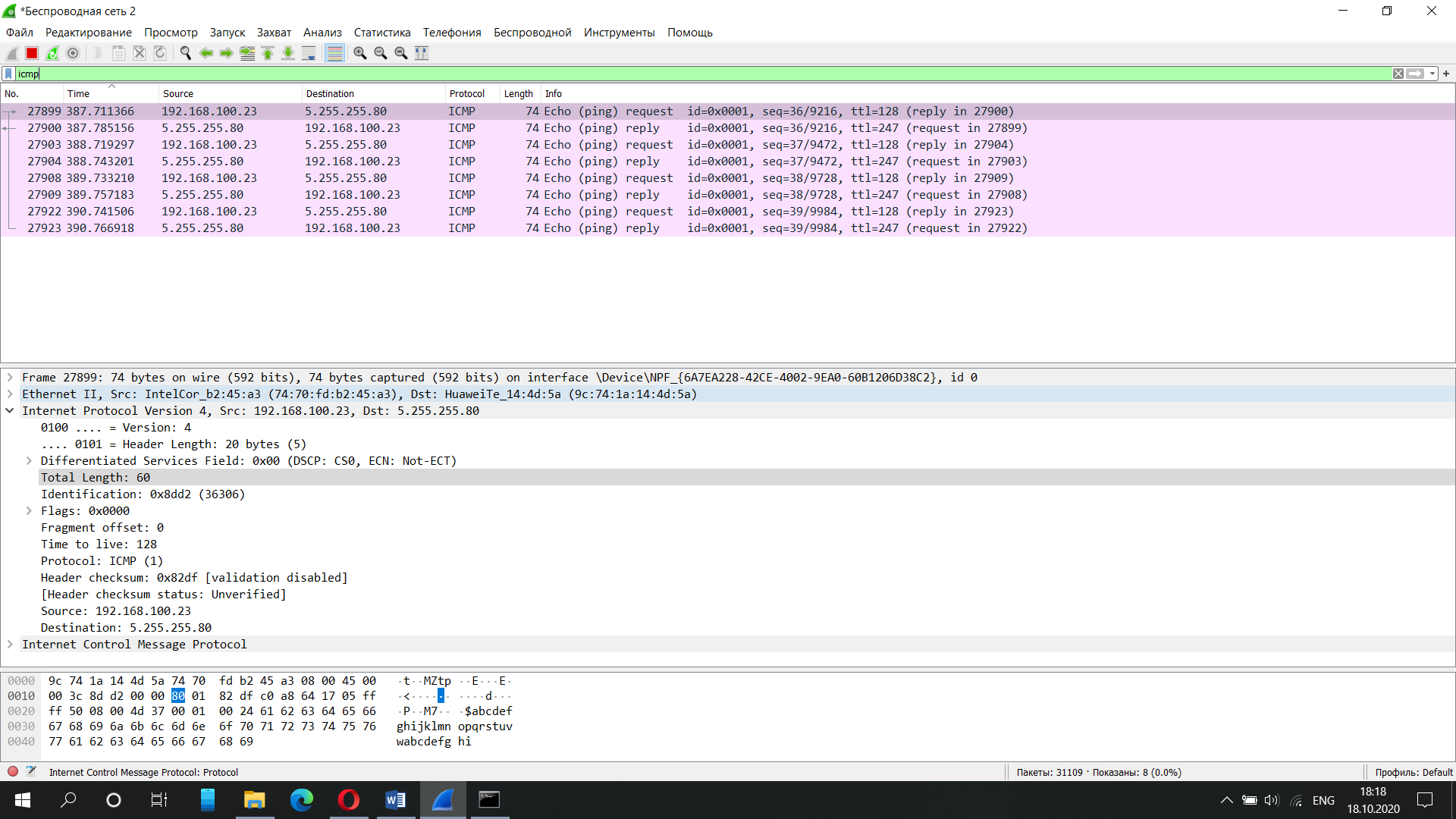
****

Рисунок 3 ping запрос

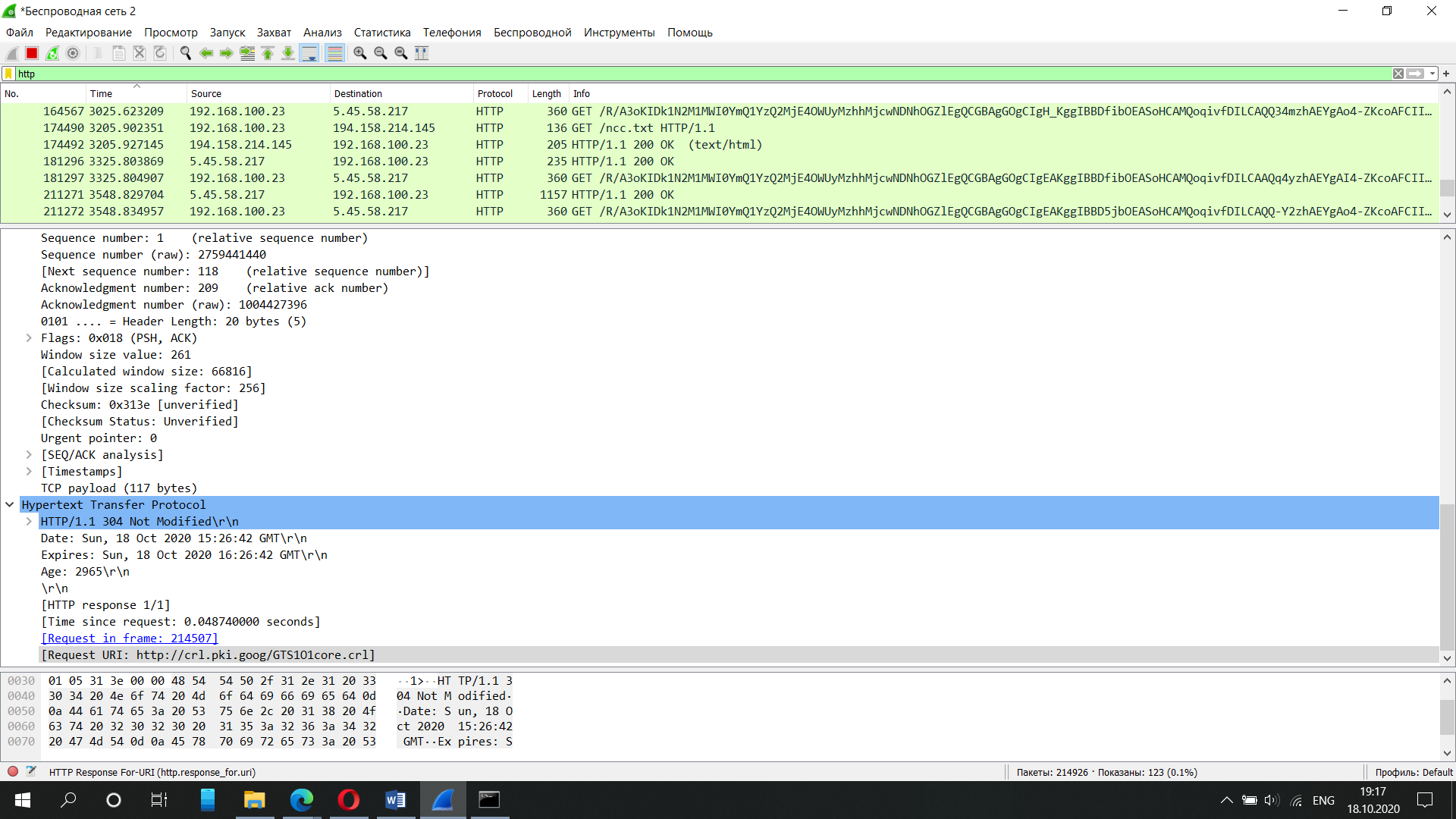
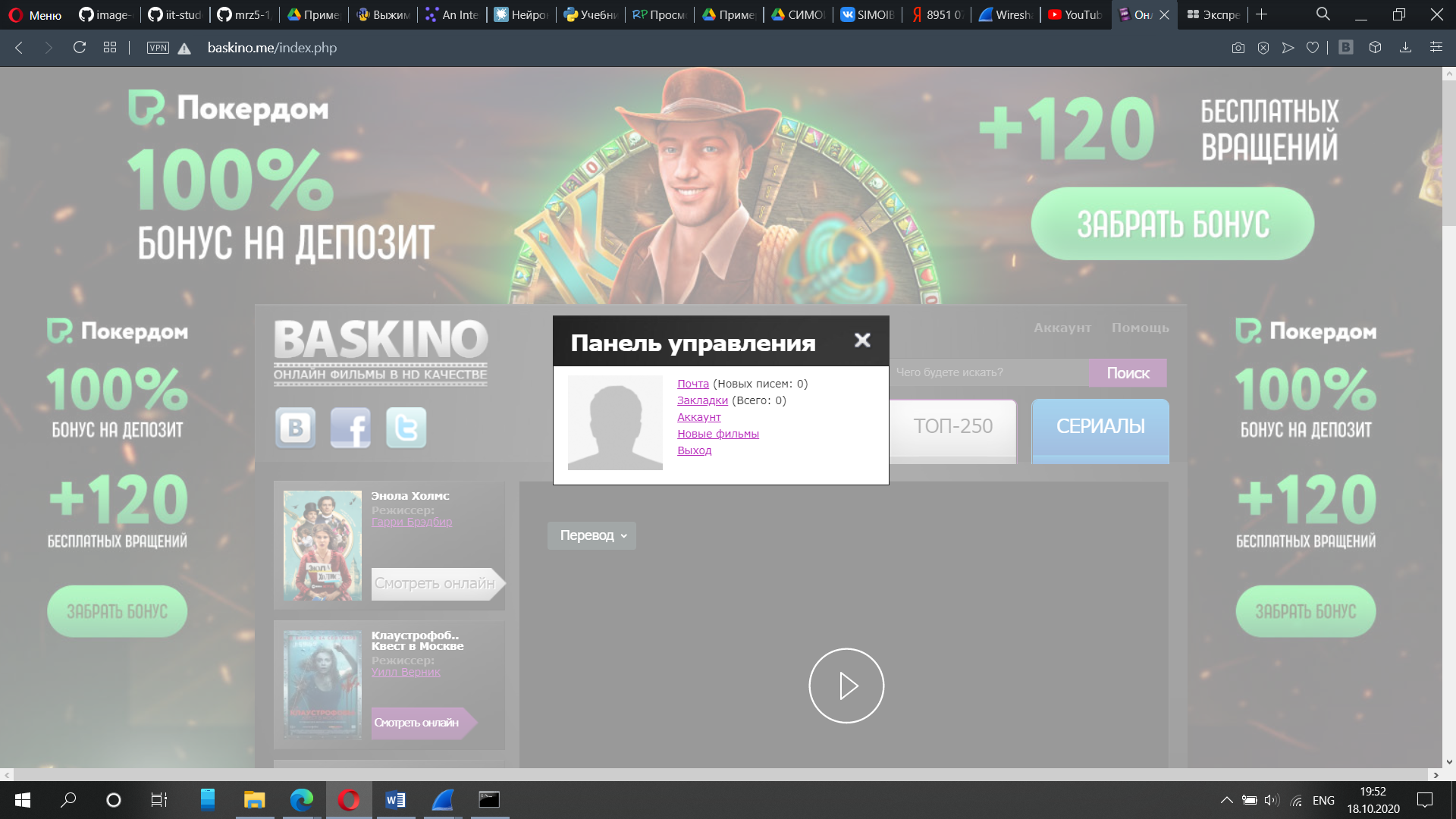


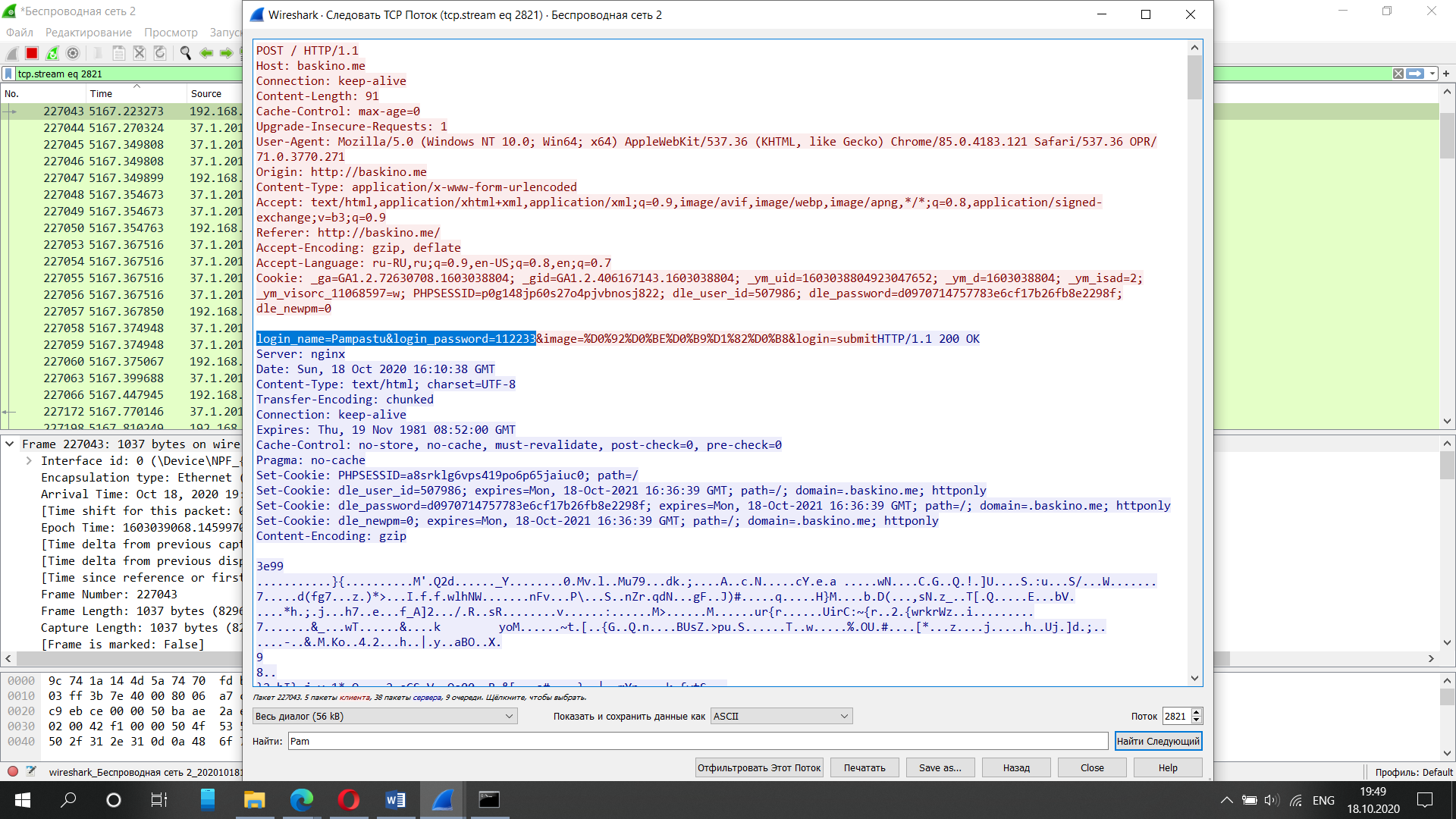
Рисунок 4 Перехват http протокола

Была произведена авторизация на сайте незащищенном протоколом https.

2

2

Рисунок 5 Незащищенный сайт

Потом был произведен поиск отправленных данных через фильтр http.request.method==”POST”. После этого, проследив за TCP, можем увидеть введённые при авторизации данные.

2

2

Рисунок 6 Пароль и Логин

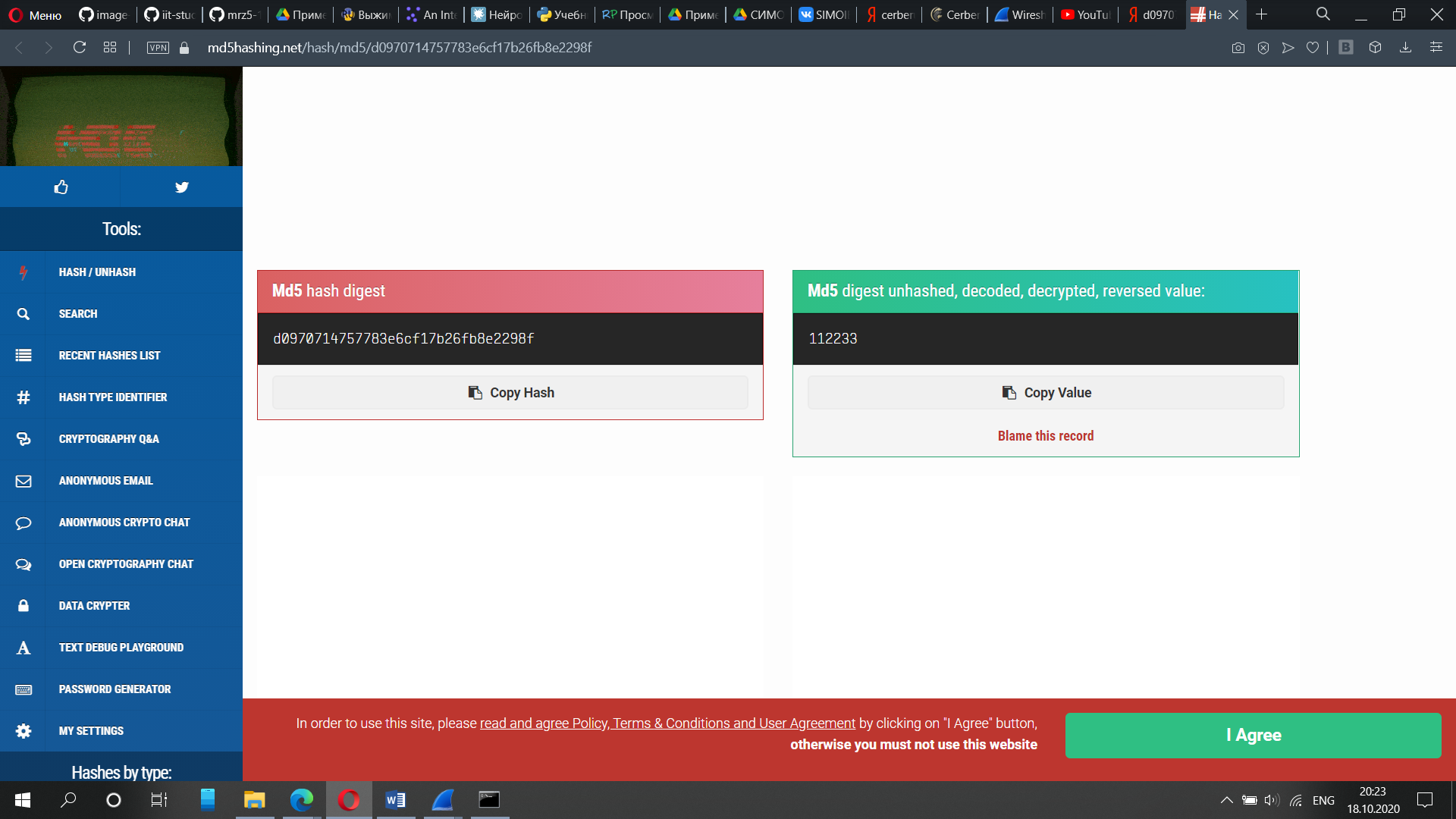
Но, так как данные зашифрованы, их необходимо расшифровать, чтобы получить наши введенные данные.

Рисунок 7 Расшифровка

Пакеты содержат информацию о отправителе и получателе (ip адрес) и о самом запросе  
- Версия   
- Длинна   
- Тип соединения

* Общая длина
* Флаги

вывод

В ходе выполнения работы были изучены базовые основы взаимодействия устройств в сети Интернет и основные способы обеспечения безопасности пользовательских данных.

На скриншотах выше приведены некоторые перехваченные пакеты и их частичная расшифровка. Проведенные опыты показали, что при отсутствии сертификата https у сервера перехват данных пользователя будет не затруднительным, при отсутствии доп. способов защиты, в том числе предоставляемых хостингом. Однако, даже зашифрованные сообщения все еще можно расшифровать, в случае, если удалось встроиться в канал пользователь-сервер.   
  
Не стоит вводить данные кредитных карт и любые иные конфиденциальные данные при пользовании незащищенных каналов связи и без протокола https, так как встроившись в сеть получить данные и с легкость их расшифровать может любой желающий.

Рекомендуется использовать только самые современные и надежные протоколы передачи данных в сети.