



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО  
ОБРАЗОВАНИЯ РФ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

Факультет управления и информатики в технологических системах  
Кафедра информационной безопасности  
Направление подготовки (специальность) 10.05.03 Информационная  
безопасность автоматизированных систем

## Отчет

### по практической работе №1

Выполнил студент гр. УБ-11

Долгих Е.И.

Проверил:  
Денисенко В.В

## **Введение**

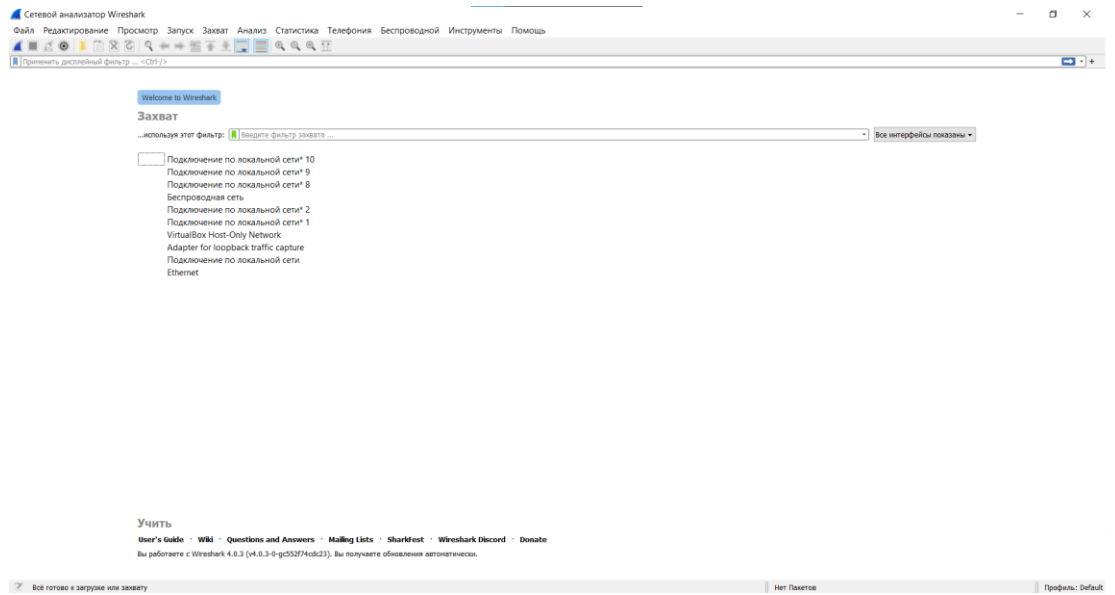
**Цель работы:** отследить и проанализировать трафик приложений, общающихся с сервером по протоколу HTTP

### **Порядок выполнения:**

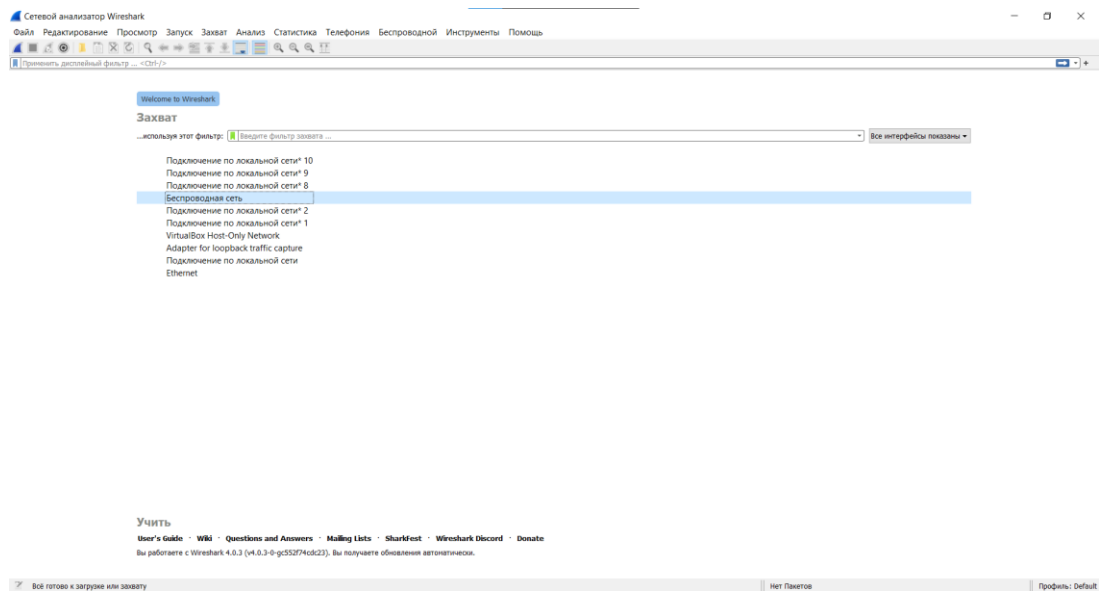
1. Установить программу
  2. Выбрать тип сети
  3. Запустить анализ
  4. Добавить фильтр
  5. Начать серфинг в интернете
  6. Изучить кадры Http в данных, захваченных программой Wireshark.
- Сопоставить результаты

# Основная часть

## 1. Установили программу:



## 2. Выбираем тип сети:



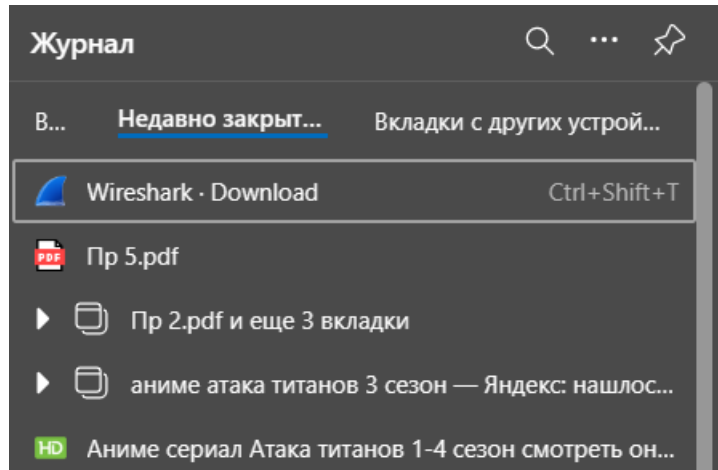
### 3. Запускаем анализ:

The screenshot shows the Wireshark interface with a packet capture on the 'Беспроводная сеть' (Wireless Network) interface. The packet list on the left shows a packet of type 'Simple Service Discovery Protocol' (SSDP) at time 1.216. The packet details pane on the right shows the structure of the SSDP packet, including the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, and the SSDP packet body. The packet body contains a 'M-SEARCH' message for a service named 'urn:uuid:63995864-4328-46e8-b91d-5ac6f4e96fd4'.

### 4. Добавляем фильтр:

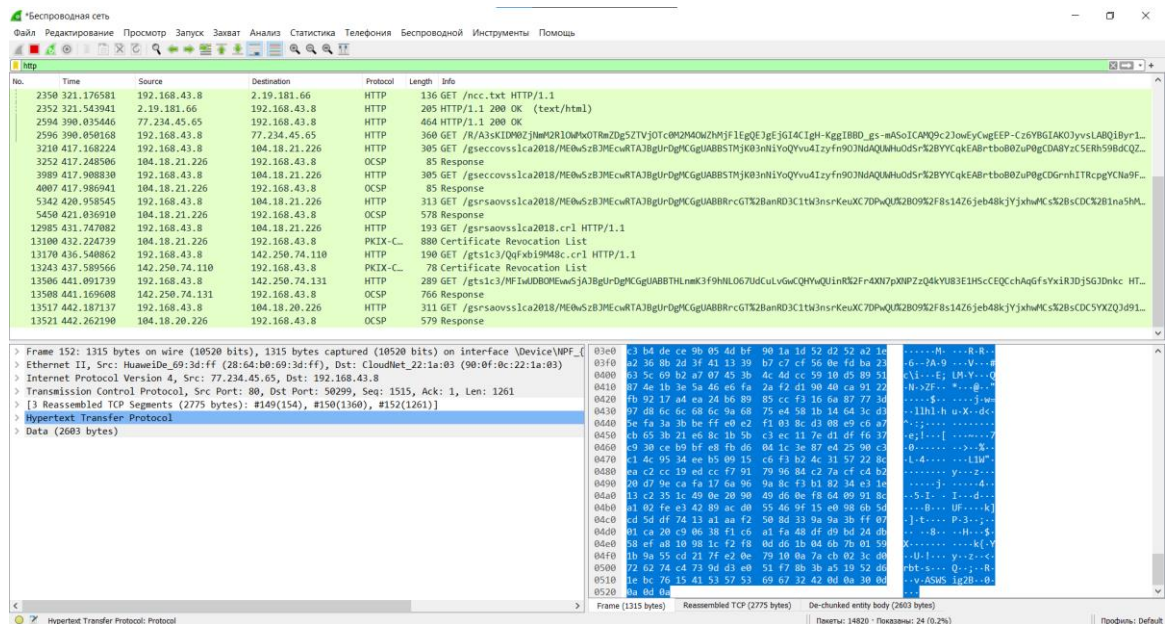
The screenshot shows the Wireshark interface with a packet capture on the 'Беспроводная сеть' (Wireless Network) interface. The packet list on the left shows a filtered list of packets, including HTTP and DSCP packets. The packet details pane on the right shows the structure of the selected packet, which is a 'Data' packet of type 'DSCP' (Differentiated Services Code Point). The packet body contains a 'DSCP' field with a value of 0x28.

## 5. Начинаем серфинг в интернете:



## 6. Изучить кадры Httр в данных, захваченных программой Wireshark.

Сопоставить результаты:



## **Вывод**

Отследили и проанализировали трафик приложений. Установили программу Wireshark. Изучили кадры в данных, захваченных программой Wireshark, сопоставить результаты.