Практическая работа №2

Анализ сетевого трафика с помощью программы Wireshark

Цель работы: ознакомление с сетевым анализатором Wireshark.

Ход работы:

При запуске программы Wireshark появится стартовый интерфейс программы.

Для старта программы и перехвата данных нажмите кнопку «Interface List» (Список интерфейсов), которая помогает вывести весь список сетевых адаптеров для перехвата трафика.

В открывшемся окне «Capture Interface» (Перехват интерфейсов) программы Wireshark, установите флажок рядом с интерфейсом, подключенным к вашей локальной сети и нажмите кнопку «Start», чтобы начать перехват данных.

По завершению процесса перехвата пакеты, которые были захвачены, будут отображены в окне программы. Строки данных выделяются различными цветами в зависимости от протокола (рис. 2.1).

Для того чтобы произвести фильтрацию по пакетам и выбрать необходимый фильтр, нажмите на кнопку «Filter» в окне программы. Появится окно с опциями на выбор: Только TCP; только UDP; только HTTP. Пример приведен на рис. 2.2.

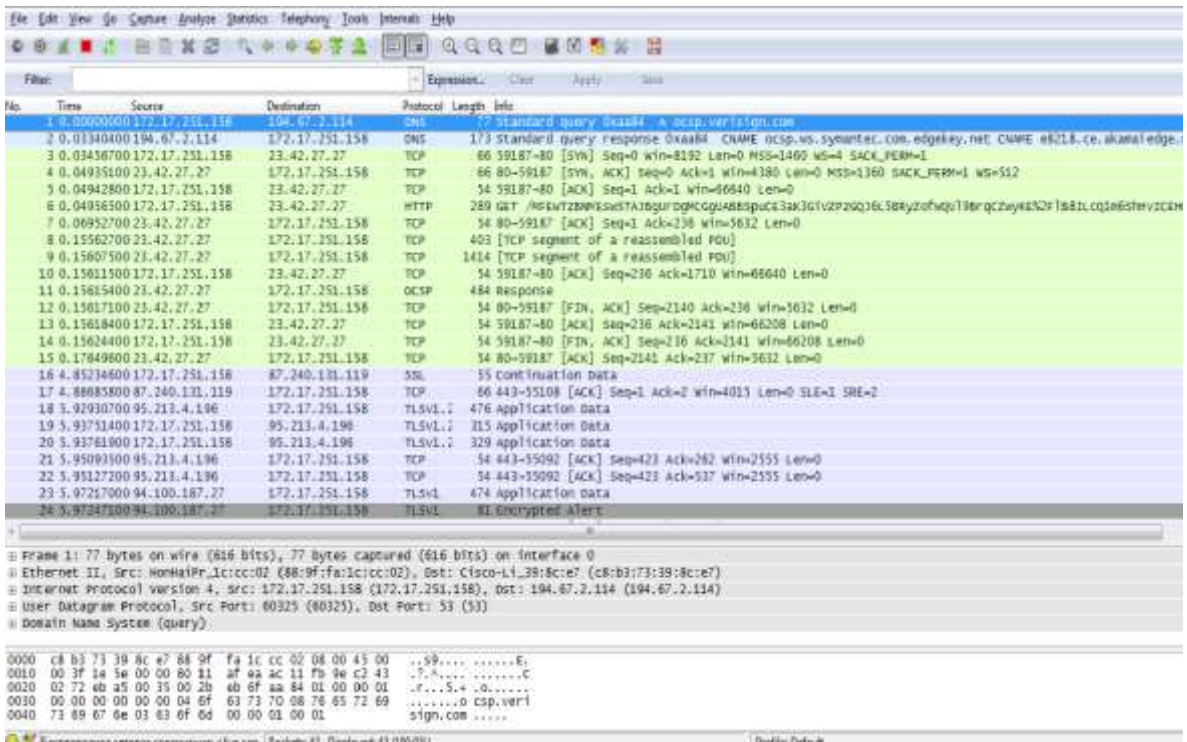

Рис. 2.1. Вид главного рабочего окна программы Wireshark

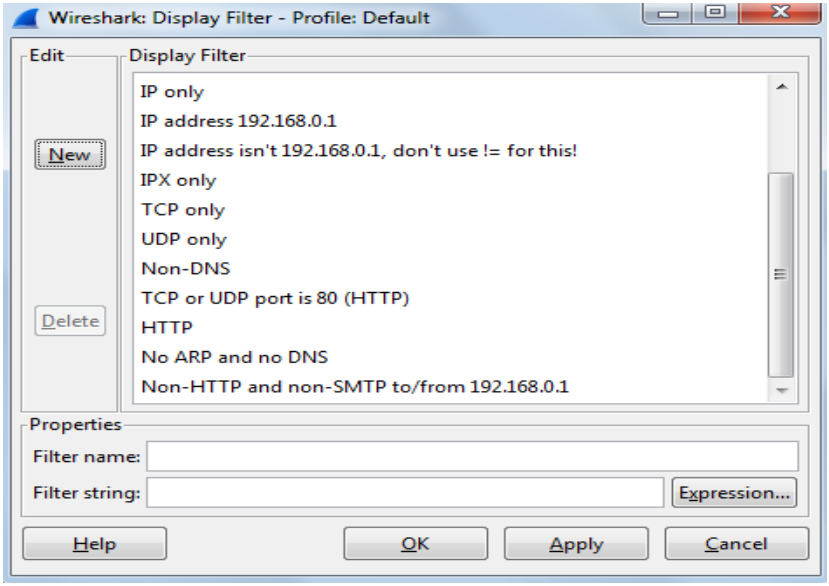

Рис. 2.2. Окно фильтра программы Wireshark

Таким образом, осуществим поиск пакета, используя фильтр и определим только пакеты TCP. Для этого в меню программы Wireshark открываем «Edit» нажмите кнопку «Find Packet», откройте «Filter» и выберите параметр «TCP only». Пример поиска пакета приведен на рис. 2.3.

Протоколы расположены в виде иерархического дерева, от низкоуровневых к более высокоуровневым, согласно стеку протоколов и очередности инкапсуляции. Информация о каждом протоколе может быть развернута до подробного описания всех полей и их значений. Пример представлен на рис. 2.4.

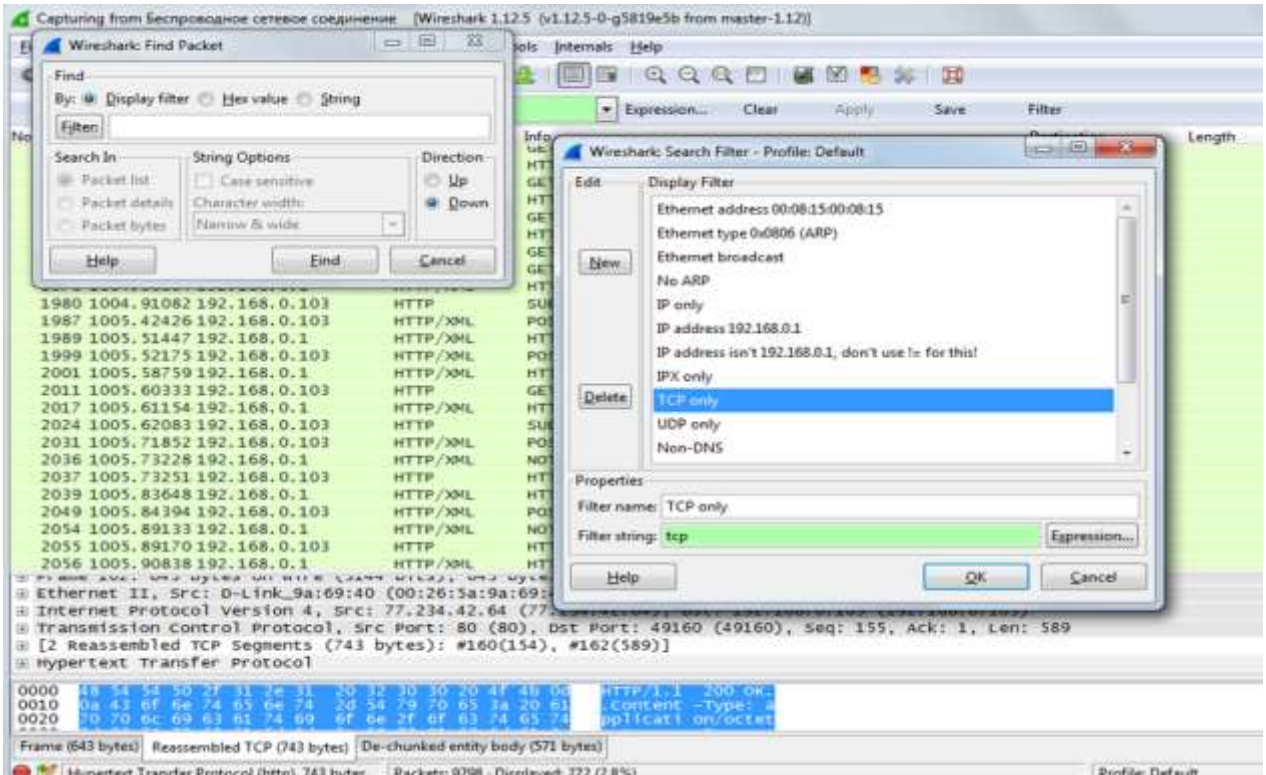

Рис. 2.3. Окно программы поиска пакета через фильтр

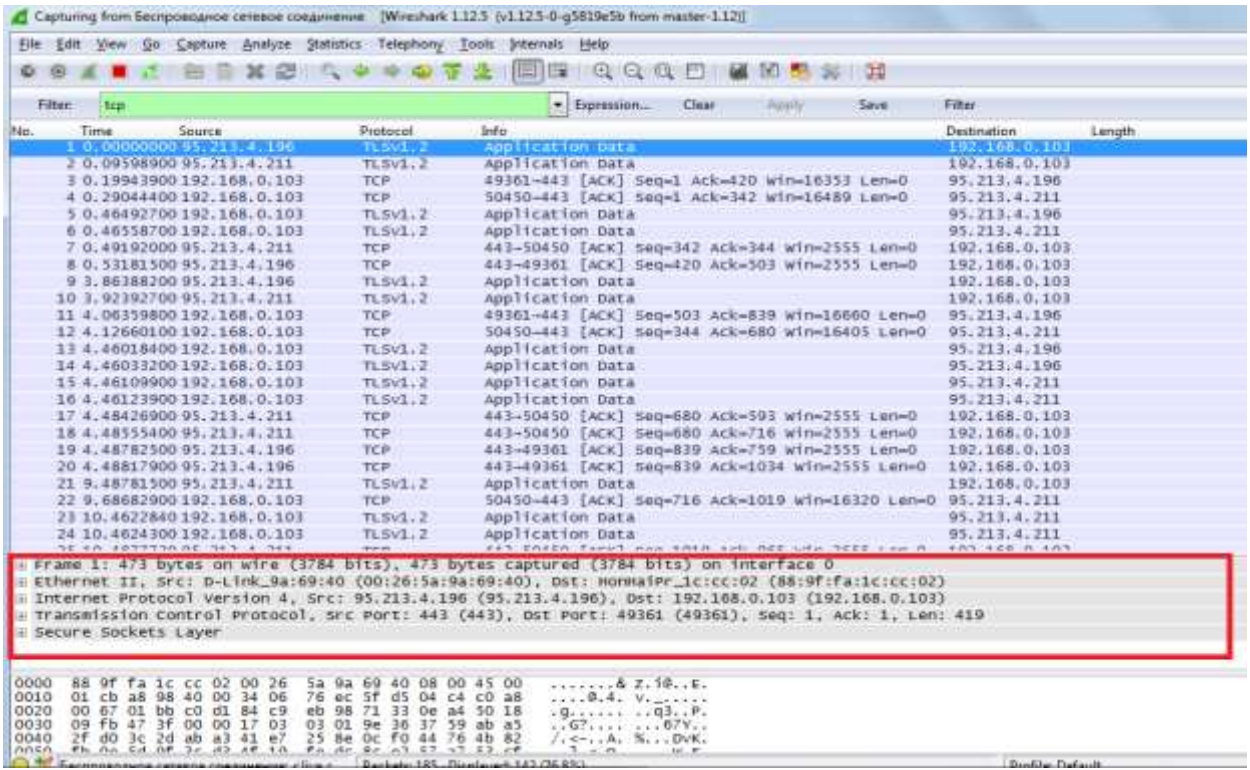

Рис. 2.4. Окно инкапсуляции пакета программы Wireshark

Панель «байты пакетов» показывает данные текущего пакета. Слева показывается смещение данных пакета, по центру данные пакета показаны в шестнадцатеричной системе исчисления и справа показывается соответствующий вид код вида ASCII. Пример приведен на рис. 2.5.

Пакет характеризуется следующими параметрами:

- No – номер пакета;
- Time – временная отметка пакета показывает время, в которое захвачен пакет;
- Source – адрес отправителя (откуда пришел пакет);
- Protocol – название протокола в сокращенной версии;
- Info – краткое содержание пакета;
- Destination – адрес получателя (куда пойдет пакет);
- Length – размер пакета.

Далее вся информация протоколов записывается в окне статистики программы Wireshark. Перейдите в меню «Statistics» и выберите «Converstations» (рис. 2.6). Wireshark также может выводить полученную информацию в графическом режиме, что облегчает ее восприятие. Перейдя в «Graphs tool», в меню «Statistics», вы можете выбрать до пяти фильтров для сравнения файлов с помощью выделения различными цветами. Пример графика зависимости разного типа приведен на рис. 2.7.

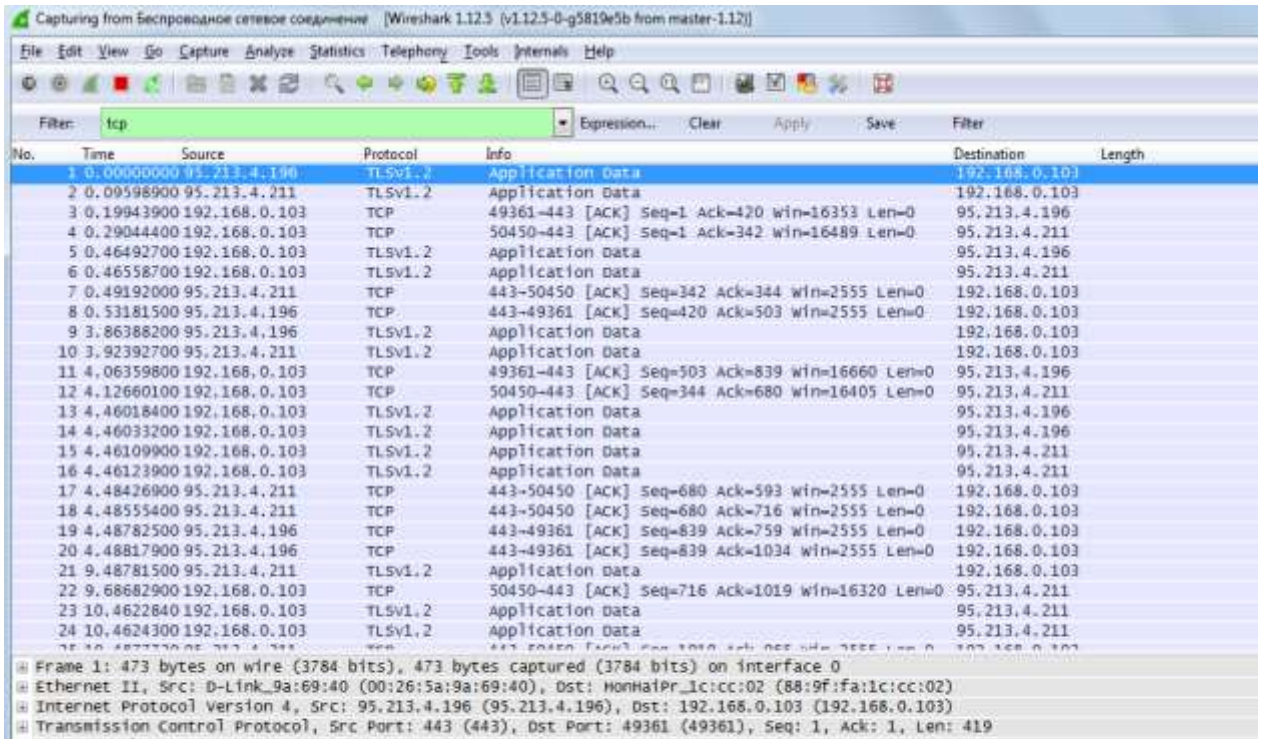

Рис. 2.5. Окно «байты пакетов» программы Wireshark

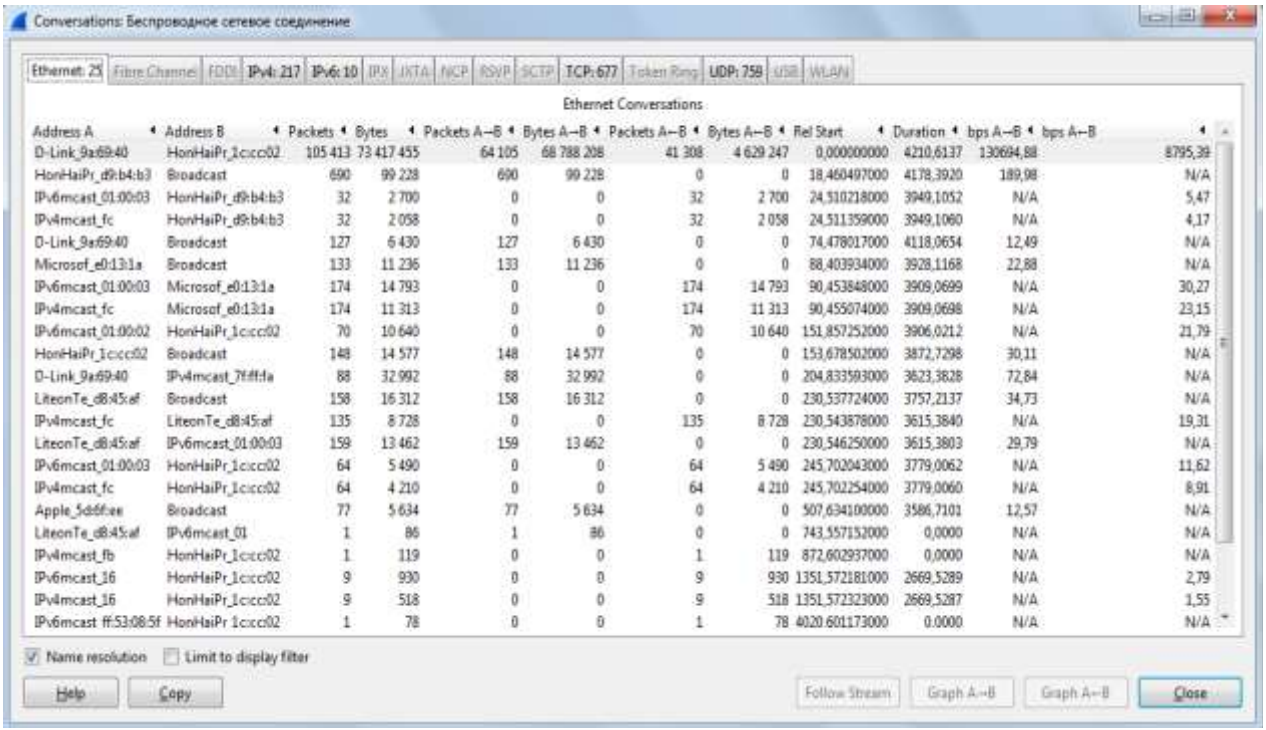

Рис. 2.6. Окно статистики программы Wireshark

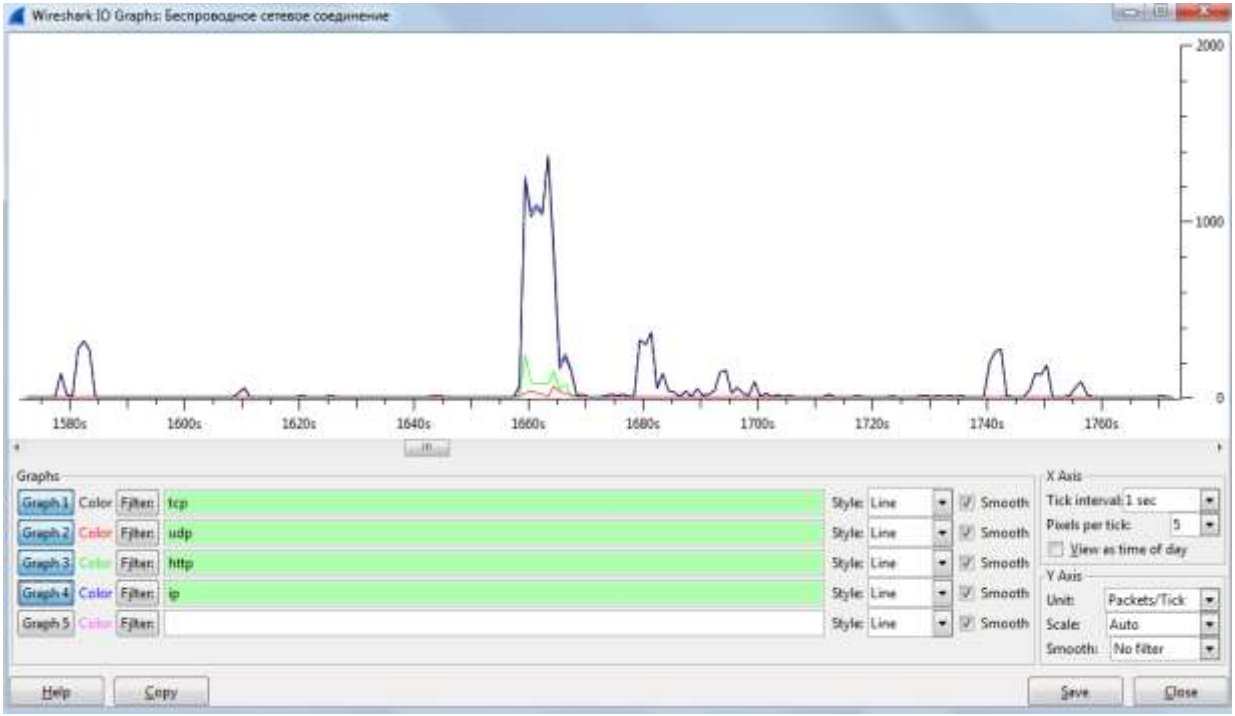

Рис. 2.7. Окно графика зависимости разного типа программы Wireshark

Задание:

- осуществить перехват трафика;
- произвести фильтрацию трафика по пакетам типа: TCP, UDP, HTTP;
- произвести поиск пакета в соответствии с заданием преподавателя и расшифровать его содержимое;
- сделать анализ по выполненной работе.