**Самостоятельная работа студентов 3**

**Работа с Wireshark**

Wireshark – это мощный инструмент для анализа сетевого трафика, который позволяет углубленно изучить данные, передаваемые по сети. Основной инструмент для наблюдения за сообщениями, которыми обмениваются элементы исполняемого протокола, называется анализатор пакетов(или сниффер). Как следует из названия, он анализирует (перехватывает) сообщения, которые отправляются или получаются вашим компьютером; он также обычно сохраняет и/или отображает содержимое различных полей протокола этих перехваченных сообщений. Анализатор пакетов является пассивной программой. Он только следит за сообщениями, отправленными и полученными приложениями и протоколами, запущенными на вашем компьютере, но сам никогда не отправляет пакеты.

Интерфейс программы представлен на рис. 1.

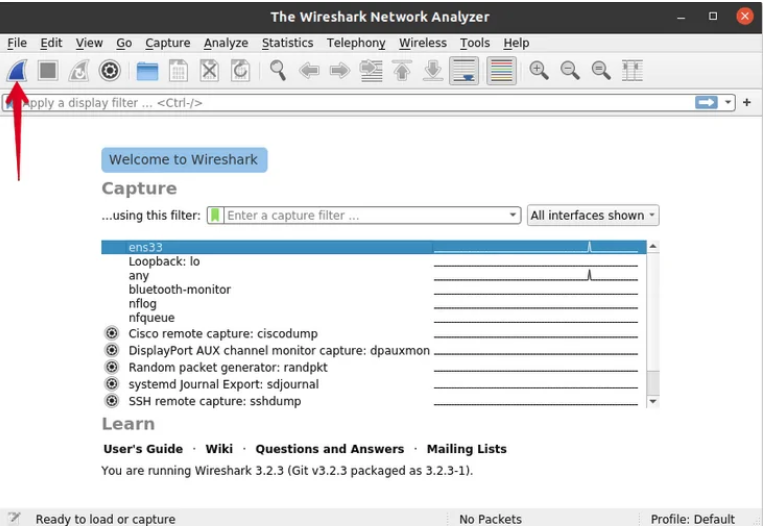
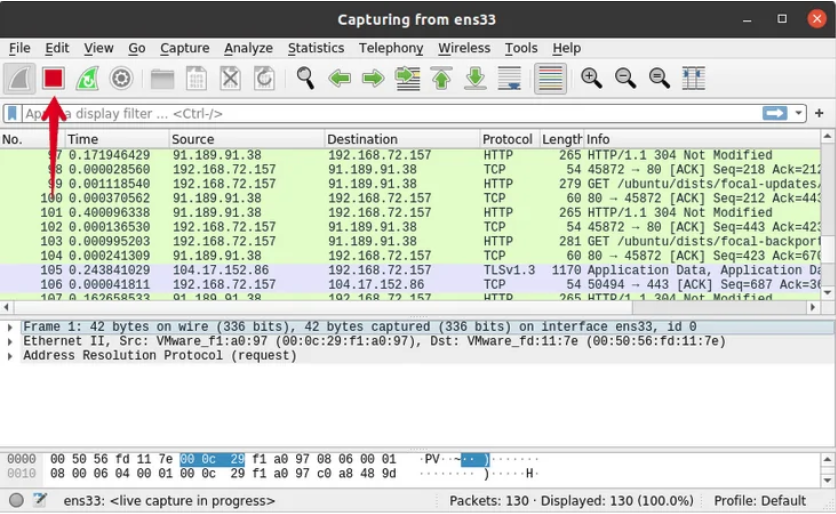


Рисунок 1 – Окно программы Wireshark



Мы будем считать, что ваш компьютер подключен к Интернету через проводной интерфейс Ethernet. Мы рекомендуем вам для первой лабораторной работы использовать именно на Ethernet-соединение, а не беспроводную связь. Выполните следующее:

1. Запустите ваш любимый браузер, и в нем откроется домашняя страница.

2. Запустите программу Wireshark. Чтобы начать работу, выберите в меню **Capture** (Захват) команду **Interfaces** (Интерфейсы). Откроется окно **Wireshark: Capture Interfaces** (Wireshark: Интерфейсы для захвата), показанное на рис. 2.

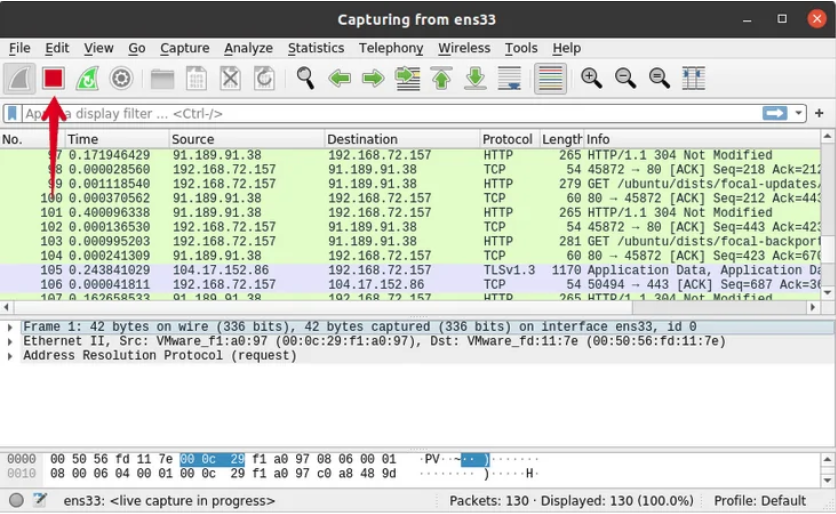


Рисунок 2 – Захват пакетов Wireshark

После того, как ваш браузер отобразил веб-страницу, остановите захват пакетов, выбрав в меню **Capture** (Захват) команду **Stop** (Стоп). Теперь у вас есть реальные данные по пакетам, которыми обменивался ваш компьютер с другим объектом сети. HTTP-сообщения обмена с веб-сервером должны быть где-то в списке захваченных пакетов. Но там присутствует также множество других типов пакетов. Даже если кроме загрузки веб-страницы вы больше ничего не делали, все равно на вашем компьютере работает множество других протоколов, скрытых с глаз.

Для того чтобы отобразить страницу, ваш браузер связывается с HTTP-сервером и обменивается HTTP-сообщениями с сервером, чтобы загрузить эту страницу. Кадры Ethernet, содержащие эти HTTP-сообщения (а также все другие кадры, проходящие через адаптер Ethernet) будут перехвачены программой Wireshark.

Укажите значение **http** (все имена протоколов в Wireshark пишутся в нижнем регистре) в поле фильтра отображения. Затем нажмите кнопку **Apply** (Применить) (справа от этого поля). Это приведет к тому, что в окне списка пакетов будут отображаться только HTTP-сообщения.

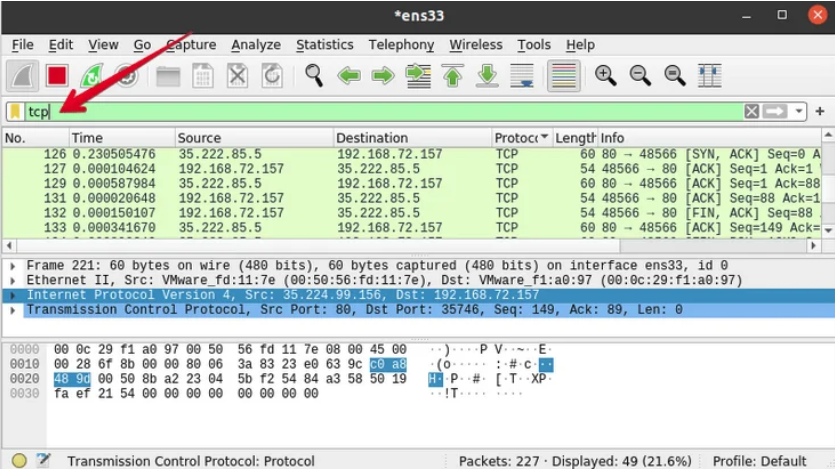


Рисунок 3 - Фильтрация пакетов

* Запустите программу еще несколько раз, откройте различные веб-страницы.
* Сделайте захват трафика.
* Проанализируйте трафик и сделайте различные фильтрации.