Лабораторная работа №27

**Тема:** Установка и использование программы Wireshark.

**Цель:** научиться устанавливать и использовать программу Wireshark.

**Ход работы:**

**Часть 1.** Изучить теоретический материал.

**Часть 2.** Использование программы Wireshark.

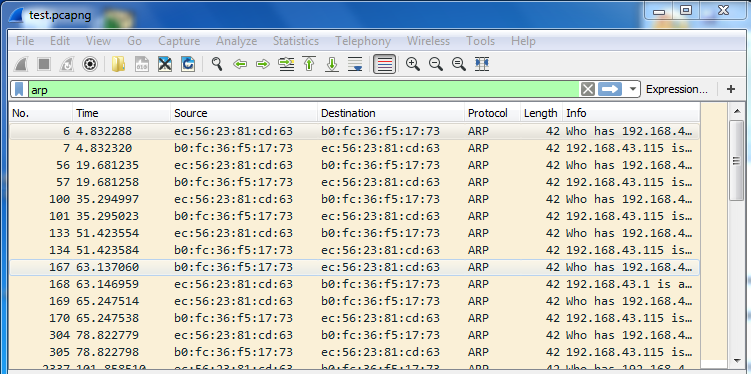
Изучить принципы работы и проанализировать пакеты.

Схема анализа:

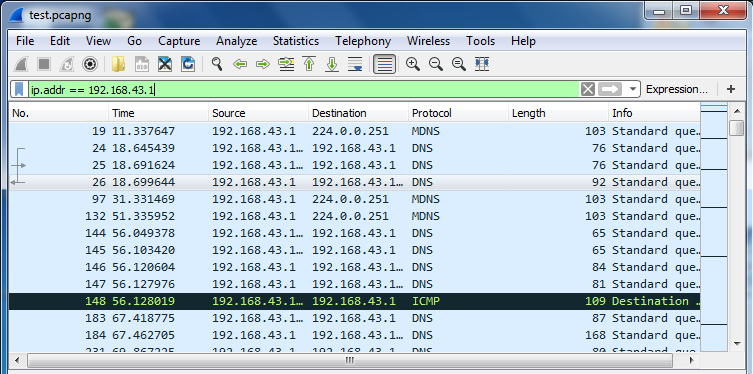
Начать захват. Эмулировать сетевую активность, чтобы получить пакеты нужного типа (веб-браузер, команды). Остановить захват. Проанализировать результаты.

\* В скобках указан утилиты командной строки, которые надо использовать при эмуляции сетевой активности, чтобы получить пакеты нужного типа.

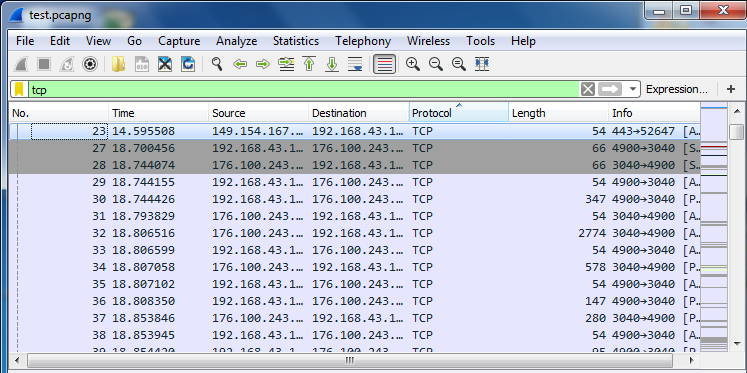
-ARP (arp)



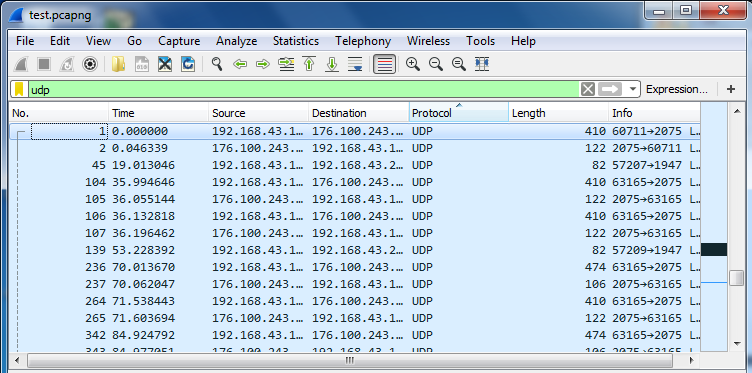
-IP



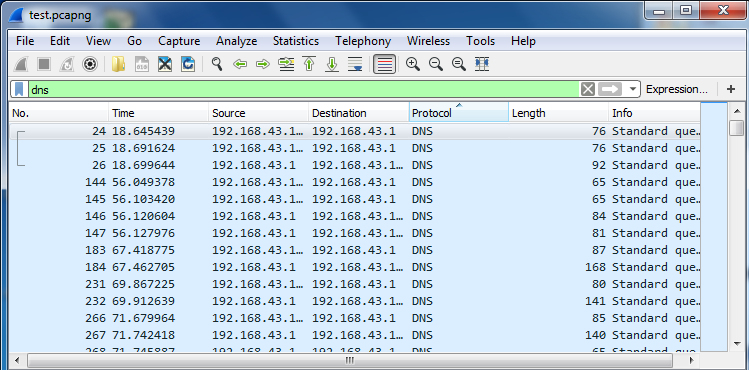
-TCP



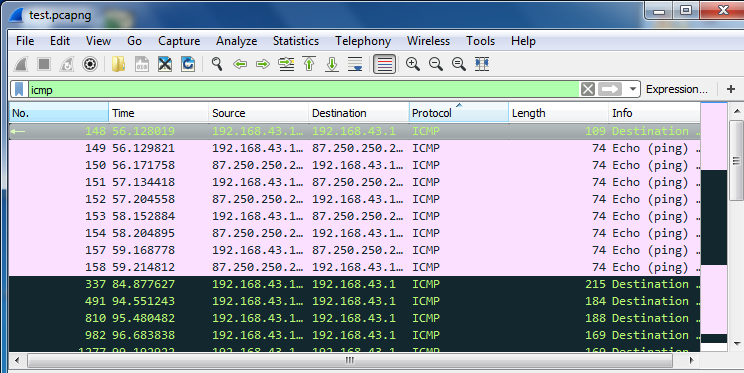
-UDP



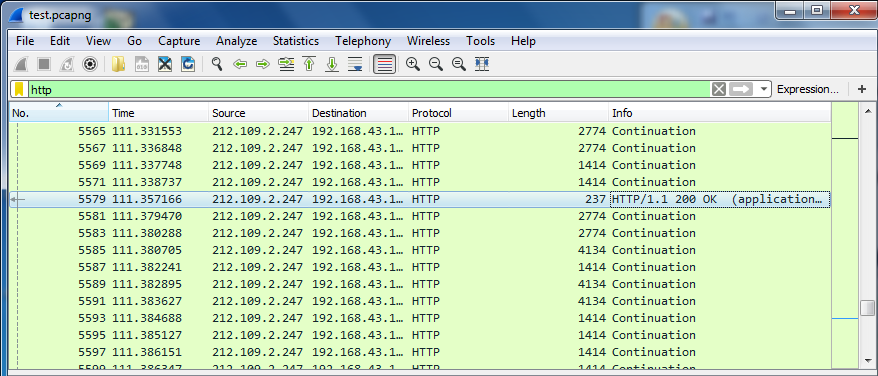
-DNS (nslookup ya.ru)



-ICMP (ping)



-HTTP



**Результаты для каждого протокола занести в отчет.**

Теоретический материал

<http://habrahabr.ru/company/pentestit/blog/204274/>

<http://zyxel.ru/kb/1793>