### Диагностика сетей

##### Netstat:

Отслеживание установки соединения через анализатор сетевого трафика Wireshark

**netstat** - выведет открытые или установленные соединение, которые в данный момент времени работают на устройстве

**netstat -n** - показ по конкретным адресам

**netstat -p tcp** - показать только определенный протокол

**netstat -s** - показать статистику

**less /etc/services** - просмотр сопоставлений номеров портов к конкретным службам (в сервисах лежат все конфигурационные файлы для работы с сетью)

### Работа с сетью

Сниферы - программа, которая перехватывает пакеты и данные которые прилетают на сетевой адаптер и которые с него отправляются

Определить ИП адрес по домену: ping www.myipaddress.com

##### Wireshark:

Интерфейс программы:

Каждая строка - сводная информация по отдельно переданному или полученному кусочку данных (инкапсулируемый сегмент)

No - номер кадра

Time - время

Source - IP адрес отправителя

Sestination - IP адрес получателя

Protocol - используемый протокол

Length - длина

Info - номера портов отправителя и получателя

**Команды:**

ip.addr==IP - показывать только соединения с конкретным ИП адресом

##### TCP dump:

tcpdump - анализатор сетевого трафика в консольном варианте

**tcpdump -i en0 -n ip host 8.8.8.8** - интерфейс ен0 ловить протокол ИП и фильтровать весь трафик с хостом 8.8.8.8