Анализ трафика сети на примере tcpdump

1. Ловим весь входящий трафик из локальной сети на сервер. Здесь все просто.

```
# /usr/sbin/tcpdump -i eth0 -n -nn -ttt dst host 192.168.2.254
```

Если вы запускаете его в SSH сессии, то подготовьтесь — польется очень много и очень быстро…
2. Ловим весь входящий трафик, исключая трафик генерируемый нашей SSH-сессией.

```
# /usr/sbin/tcpdump -i eth0 -n -nn -ttt 'dst host 192.168.2.254 and not ( src host 192.168.2.100 and dst port 22 )'
```

Вот теперь в потоке пакетов можно разобраться.
3. Нужна информация об DNS-общении между сервером и каким-нибудь узлом сети.

```
# /usr/sbin/tcpdump -i eth0 -n -nn -ttt 'host 192.168.2.13 and ip proto \udp'
```

Здесь, кстати будет бегать не только DNS-трафик. А вообще весь, который идет по UDP. Исправить это можно следующим:

```
# /usr/sbin/tcpdump -i eth0 -n -nn -ttt 'host 192.168.2.13 and port 53'
```

4. Отлавливаем исключительно icmp пакеты.

```
# /usr/sbin/tcpdump -i eth0 -n -nn -ttt 'ip proto \icmp'
```