Просмотр интерфейсов, доступных tcpdump

```
tcpdump -D
```

Пример вывода:

```
1.enp0s3 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]
```

Пример дампа HTTP трафика

Команда:

```
tcpdump 'tcp port 80' -c 10 -i enp0s3
```

здесь слушаем 80-й порт на интерфейсе `enp0s3` и "дампим" первые 10 пакетов, активируем обмен трафиком с помощью `curl ya.ru`

Вывод:

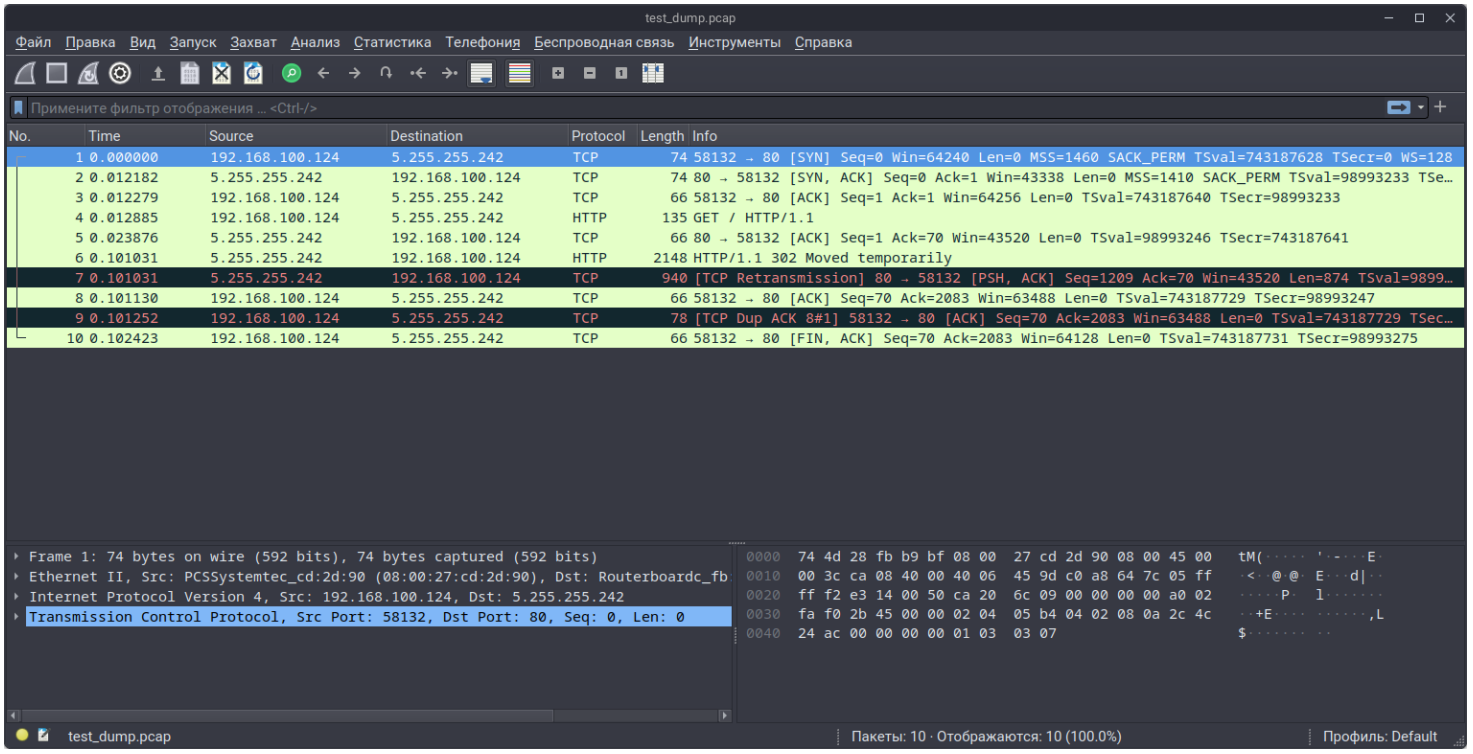
```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
14:11:52.829959 IP ubuntu.46994 > ya.ru.http: Flags [S], seq 1618301429, win 64240,
options [mss 1460,sackOK,TS val 742667806 ecr 0,nop,wscale 7], length 0
14:11:52.851150 IP ya.ru.http > ubuntu.46994: Flags [S.], seq 3379945987, ack
1618301430, win 43338, options [mss 1410,sackOK,TS val 4158969836 ecr
742667806,nop,wscale 8], length 0
14:11:52.851249 IP ubuntu.46994 > ya.ru.http: Flags [.], ack 1, win 502, options
[nop,nop,TS val 742667827 ecr 4158969836], length 0
14:11:52.851993 IP ubuntu.46994 > ya.ru.http: Flags [P.], seq 1:70, ack 1, win 502,
options [nop,nop,TS val 742667828 ecr 4158969836], length 69: HTTP: GET / HTTP/1.1
14:11:52.862785 IP ya.ru.http > ubuntu.46994: Flags [.], ack 70, win 170, options
[nop,nop,TS val 4158969856 ecr 742667828], length 0
14:11:52.864637 IP ya.ru.http > ubuntu.46994: Flags [P.], seq 1:2082, ack 70, win
170, options [nop,nop,TS val 4158969857 ecr 742667828], length 2081: HTTP: HTTP/1.1
302 Moved temporarily
14:11:52.864697 IP ubuntu.46994 > ya.ru.http: Flags [.], ack 2082, win 496, options
[nop,nop,TS val 742667841 ecr 4158969857], length 0
14:11:52.865943 IP ubuntu.46994 > ya.ru.http: Flags [F.], seq 70, ack 2082, win
501, options [nop,nop,TS val 742667842 ecr 4158969857], length 0
14:11:52.876983 IP ya.ru.http > ubuntu.46994: Flags [F.], seq 2082, ack 71, win
```

```
170, options [nop,nop,TS val 4158969870 ecr 742667842], length 0
14:11:52.877093 IP ubuntu.46994 > ya.ru.http: Flags [.], ack 2083, win 501, options
[nop,nop,TS val 742667853 ecr 4158969870], length 0
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

Аналогично с сохранением в файл

```
tcpdump 'tcp port 80' -c 10 -i enp0s3 -w test_dump.pcap
```

Просмотр дампа в Wireshark:



Видим установку TCP соединения: флаги [SYN], [SYN, ACK], [ACK]; HTTP запрос GET, в конце - завершение соединения TCP: [FIN, ACK].