# TCP Dump

tcpdump is the world’s premier network analysis tool—combining both power and simplicity into a single command-line interface.

## Install

**apt install tcpdump (Ubuntu)  
yum install tcpdump (Redhat/Centos)**

Expression Types:  
**host**, **net**, and **port**.  
Directions:  
**src** and **dst**.  
Types:  
**host**, **net**, and **port**.  
Protocols:  
**tcp**, **udp**, icmp, and many more.

You can get a single packet with **-c 1**, or n number with **-c n**

Get information from and interface : **tcpdump -i eth0**

Get information from a host 2 direction : **tcpdump host 1.1.1.1**

Get information from a host 1 direction : **tcpdump src 1.1.1.1**

Get information from a host 1 direction : **tcpdump dst 1.1.1.1**

You can combine **net** with the **src** and **dst** options as well.

Get information from a net 1 direction : **tcpdump dst net 1.1.1.0/24**

Get information from a host 1 direction for protocol **ICMP**: **tcpdump src 1.1.1.1** ICMP

Get traffic of specific port : **tcpdump** **port** **3389** (desination port)  
Get traffic of specific port : **tcpdump** **src** **port** **1025** (source port)

Get traffic of range of ports **tcpdump** **portrange** **21-23** (desination port)  
get just ICMP protocol : **tcpdump** **icmp**

Common Options:  
**-nn** : Don’t resolve hostnames or port names.  
**-S** : Get the entire packet.

**-S** : Print absolute sequence numbers  
**-X** : Get hex output.

**-e** : Get the ethernet header as well.

**-t** : Give human-readable timestamp output.

-tt : very human readable time stamp

-v : verbose

-vv : very verbose

Find traffic of particular size :

* **tcpdump** **less** **32**  
  **tcpdump** **greater** **64**  
  **tcpdump** **<=** **128**

write to file : **tcpdump** **port** **80** **-w** capture\_file

read from a pcap file : **tcpdump -r** **capture\_file**

## combination of options

1. **AND**  
   *and* or &&
2. **OR**  
   *or* or ||
3. **EXCEPT**  
   *not* or !

Example :

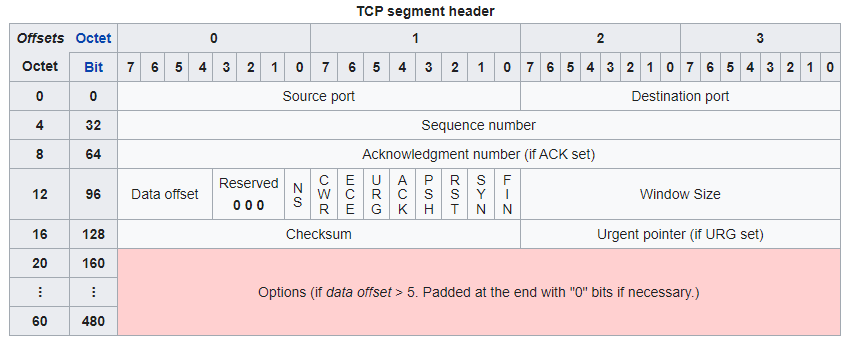
1- **tcpdump** -nvX **src net** **192.168.0.0/16** **and** dst net **10.0.0.0/8** **or** 172.16.0.0/16

* Let’s look for all traffic coming from 192.168.x.x and going to the 10.x or 172.16.x.x networks

2- **tcpdump** **dst 192.168.0.2 and** **not icmp**

3- **tcpdump** **'src 10.0.2.4 and** **(dst port 3389 or 22)'**

## Analyzing TCP flags



* FIN - sudo tcpdump 'tcp[13] & 1 != 0'
* SYN - sudo tcpdump 'tcp[13] & 2 != 0'
* RST - sudo tcpdump 'tcp[13] & 4 != 0'
* PSH - sudo tcpdump 'tcp[13] & 8 != 0'
* ACK - sudo tcpdump 'tcp[13] & 16 != 0'
* URG - sudo tcpdump 'tcp[13] & 32 != 0'

Another notation

tcpdump **'tcp[13]** & **1**!=**0**'  
tcpdump **'tcp[tcpflags]** **== tcp-fin**'

tcpdump **'tcp[13]** & **2**!=**0**'  
tcpdump **'tcp[tcpflags]** **== tcp-syn**'

tcpdump **'tcp[13]** & **4**!=**0**'  
tcpdump **'tcp[tcpflags]** **== tcp-rst**'

tcpdump **'tcp[13]** & **8**!=**0**'  
tcpdump **'tcp[tcpflags]** **== tcp-push**'

tcpdump **'tcp[13]** & **16**!=**0**'  
tcpdump **'tcp[tcpflags]** **== tcp-ack**'

tcpdump **'tcp[13]** & **32**!=**0**'  
tcpdump **'tcp[tcpflags]** **== tcp-urg**'

**we can set some bits and unset some others**

* Isolate packets that have both the SYN and ACK flags set : **tcpdump** **'tcp[13]=18**'
* Both SYN and RST Set : tcpdump **'tcp[13] = 6'**

## Find HTTP User Agents

The -l switch lets you see the traffic as you’re capturing it, and helps when sending to commands like grep.

-A let us to capture L2 traffics

tcpdump **-vvAls0** | **grep** **'User-Agent:'**

Cleartext GET Requests : **tcpdump** **-vvAls0** | **grep** **'GET'**

Find HTTP Host Headers : **tcpdump** **-vvAls0** | **grep** **'Host:'**

Find HTTP Cookies : **tcpdump** **-vvAls0** | **grep** **'Set-Cookie|Host:|Cookie:'**

Find SSH Connections (This one works regardless of what port the connection comes in on, because it’s getting the banner response.) : **tcpdump** **'tcp[(tcp[12]>>2):4] = 0x5353482D'**

Find DNS Traffic : **tcpdump** **-vvAs0** **port** **53**

Find FTP Traffic : **tcpdump** **-vvAs0** **port** **ftp or ftp-data**

Find NTP Traffic : **tcpdump** **-vvAs0** **port** **123**