TCPDUMP

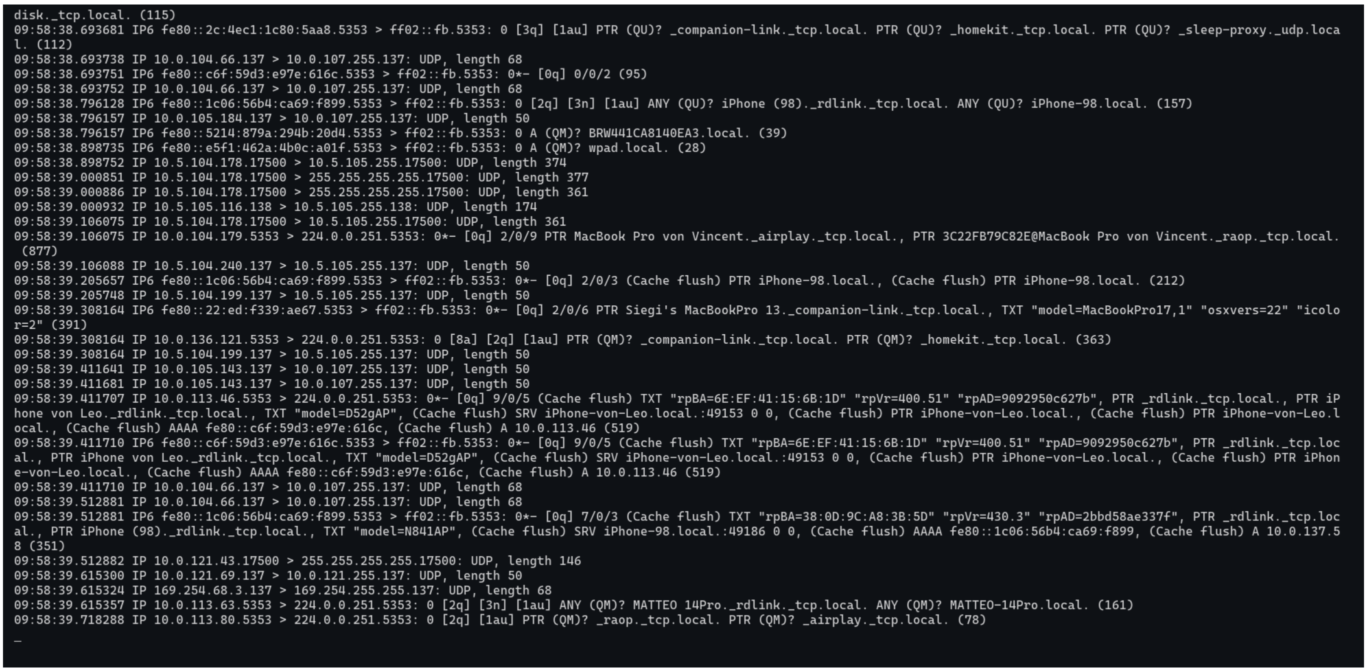
Christof Zlabinger

17.2.2023

Your IP = 10.0.106.107 Your Interface = wlan0

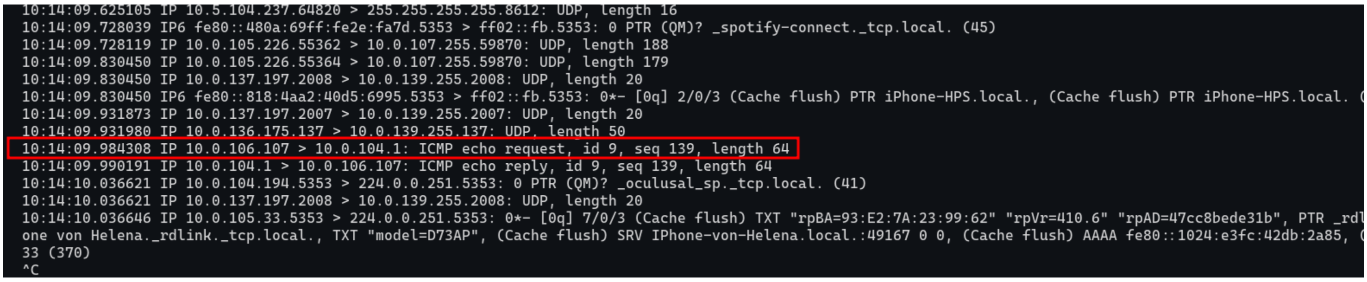
Open a terminal window and type the following command to start capturing TCP/IP packets from the active interface. Do not close this terminal window.

tcpdump -nn



```
disk._tcp.local. (115)
09:58:38.693681 IP6 fe80::2c:4ec1:1c80:5aa8.5353 > ff02::fb.5353: 0 [3q] [1au] PTR (QU)? _companion-link._tcp.local. PTR (QU)? _homekit._tcp.local. PTR (QU)? _sleep-proxy._udp.loca
l. (112)
09:58:38.693738 IP 10.0.104.66.137 > 10.0.107.255.137: UDP, length 68
09:58:38.693751 IP6 fe80::c6f:59d3:e97e:616c.5353 > ff02::fb.5353: 0*- [0q] 0/0/2 (95)
09:58:38.693752 IP 10.0.104.66.137 > 10.0.107.255.137: UDP, length 68
09:58:38.796128 IP6 fe80::1c06:56b4:ca69:f899.5353 > ff02::fb.5353: 0 [2q] [3n] [1au] ANY (QU)? iPhone (98)._rdlink._tcp.local. ANY (QU)? iPhone-98.local. (157)
09:58:38.796157 IP 10.0.105.184.137 > 10.0.107.255.137: UDP, length 50
09:58:38.796157 IP6 fe80::5214:879a:294b:20d4.5353 > ff02::fb.5353: 0 A (QM)? BRW441CA8140EA3.local. (39)
09:58:38.898735 IP6 fe80::e5f1:462a:4b0c:a01f.5353 > ff02::fb.5353: 0 A (QM)? wpad.local. (28)
09:58:38.898752 IP 10.5.104.178.17500 > 10.5.105.255.17500: UDP, length 374
09:58:39.000851 IP 10.5.104.178.17500 > 255.255.255.255.17500: UDP, length 377
09:58:39.000886 IP 10.5.104.178.17500 > 255.255.255.255.17500: UDP, length 361
09:58:39.000932 IP 10.5.105.116.138 > 10.5.105.255.138: UDP, length 174
09:58:39.106075 IP 10.5.104.178.17500 > 10.5.105.255.17500: UDP, length 361
09:58:39.106075 IP 10.0.104.179.5353 > 224.0.0.251.5353: 0*- [0q] 2/0/9 PTR MacBook Pro von Vincent._airplay._tcp.local., PTR 3C22FB79C82E@MacBook Pro von Vincent._raop._tcp.local.
 (877)
09:58:39.106088 IP 10.5.104.240.137 > 10.5.105.255.137: UDP, length 50
09:58:39.205657 IP6 fe80::1c06:56b4:ca69:f899.5353 > ff02::fb.5353: 0*- [0q] 2/0/3 (Cache flush) PTR iPhone-98.local., (Cache flush) PTR iPhone-98.local. (212)
09:58:39.205748 IP 10.5.104.199.137 > 10.5.105.255.137: UDP, length 50
09:58:39.308164 IP6 fe80::22:ed:f339:ae67.5353 > ff02::fb.5353: 0*- [0q] 2/0/6 PTR Siegi's MacBookPro 13._companion-link._tcp.local., TXT "model=MacBookPro17,1" "osxvers=22" "icolo
r=2" (391)
09:58:39.308164 IP 10.0.136.121.5353 > 224.0.0.251.5353: 0 [8a] [2q] [1au] PTR (QM)? _companion-link._tcp.local. PTR (QM)? _homekit._tcp.local. (363)
09:58:39.308164 IP 10.5.104.199.137 > 10.5.105.255.137: UDP, length 50
09:58:39.411641 IP 10.0.105.143.137 > 10.0.107.255.137: UDP, length 50
09:58:39.411681 IP 10.0.105.143.137 > 10.0.107.255.137: UDP, length 50
09:58:39.411707 IP 10.0.113.46.5353 > 224.0.0.251.5353: 0*- [0q] 9/0/5 (Cache flush) TXT "rpBA=6E:EF:41:15:6B:1D" "rpVr=400.51" "rpAD=9092950c627b", PTR _rdlink._tcp.local., PTR iP
hone von Leo._rdlink._tcp.local., TXT "model=D52gAP", (Cache flush) SRV iPhone-von-Leo.local.:49153 0 0, (Cache flush) PTR iPhone-von-Leo.local., (Cache flush) PTR iPhone-von-Leo.l
ocal., (Cache flush) AAAA fe80::c6f:59d3:e97e:616c, (Cache flush) A 10.0.113.46 (519)
09:58:39.411710 IP6 fe80::c6f:59d3:e97e:616c.5353 > ff02::fb.5353: 0*- [0q] 9/0/5 (Cache flush) TXT "rpBA=6E:EF:41:15:6B:1D" "rpVr=400.51" "rpAD=9092950c627b", PTR _rdlink._tcp.loc
al., PTR iPhone von Leo._rdlink._tcp.local., TXT "model=D52gAP", (Cache flush) SRV iPhone-von-Leo.local.:49153 0 0, (Cache flush) PTR iPhone-von-Leo.local., (Cache flush) PTR iPhon
e-von-Leo.local., (Cache flush) AAAA fe80::c6f:59d3:e97e:616c, (Cache flush) A 10.0.113.46 (519)
09:58:39.411710 IP 10.0.104.66.137 > 10.0.107.255.137: UDP, length 68
09:58:39.512881 IP 10.0.104.66.137 > 10.0.107.255.137: UDP, length 68
09:58:39.512881 IP6 fe80::1c06:56b4:ca69:f899.5353 > ff02::fb.5353: 0*- [0q] 7/0/3 (Cache flush) TXT "rpBA=38:0D:9C:A8:3B:5D" "rpVr=430.3" "rpAD=2bbd58ae337f", PTR _rdlink._tcp.loc
al., PTR iPhone (98)._rdlink._tcp.local., TXT "model=N841AP", (Cache flush) SRV iPhone-98.local.:49186 0 0, (Cache flush) AAAA fe80::1c06:56b4:ca69:f899, (Cache flush) A 10.0.137.5
8 (351)
09:58:39.512882 IP 10.0.121.43.17500 > 255.255.255.255.17500: UDP, length 146
09:58:39.615300 IP 10.0.121.69.137 > 10.0.121.255.137: UDP, length 50
09:58:39.615324 IP 169.254.68.3.137 > 169.254.255.255.137: UDP, length 68
09:58:39.615357 IP 10.0.113.63.5353 > 224.0.0.251.5353: 0 [2q] [3n] [1au] ANY (QM)? MATTEO 14Pro._rdlink._tcp.local. ANY (QM)? MATTEO-14Pro.local. (161)
09:58:39.718288 IP 10.0.113.80.5353 > 224.0.0.251.5353: 0 [2q] [1au] PTR (QM)? _raop._tcp.local. PTR (QM)? _airplay._tcp.local. (78)
_
```

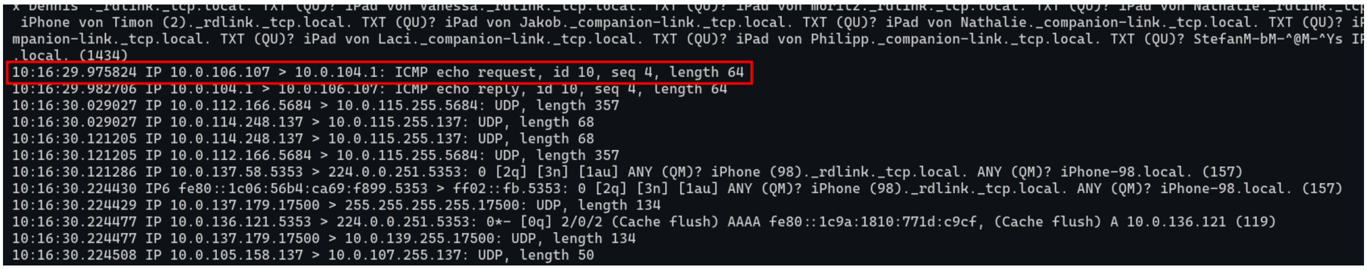
Go to the terminal window where tcpdump is running. You should see ICMP echo packets between your computer and host 10.0.0.4 as shown in the figure below.



```
10:14:09.625105 IP 10.5.104.237.64820 > 255.255.255.255.8612: UDP, length 16
10:14:09.728039 IP6 fe80::480a:69ff:fe2e:fa7d.5353 > ff02::fb.5353: 0 PTR (QM)? _spotify-connect._tcp.local. (45)
10:14:09.728119 IP 10.0.105.226.55362 > 10.0.107.255.59870: UDP, length 188
10:14:09.830450 IP 10.0.105.226.55364 > 10.0.107.255.59870: UDP, length 179
10:14:09.830450 IP 10.0.137.197.2008 > 10.0.139.255.2008: UDP, length 20
10:14:09.830450 IP6 fe80::818:4aa2:40d5:6995.5353 > ff02::fb.5353: 0*- [0q] 2/0/3 (Cache flush) PTR iPhone-HPS.local., (Cache flush) PTR iPhone-HPS.local. (
10:14:09.931873 IP 10.0.137.197.2007 > 10.0.139.255.2007: UDP, length 20
10:14:09.931980 IP 10.0.136.175.137 > 10.0.139.255.137: UDP, length 50
10:14:09.984308 IP 10.0.106.107 > 10.0.104.1: ICMP echo request, id 9, seq 139, length 64
10:14:09.990191 IP 10.0.104.1 > 10.0.106.107: ICMP echo reply, id 9, seq 139, length 64
10:14:10.036621 IP 10.0.104.194.5353 > 224.0.0.251.5353: 0 PTR (QM)? _oculusal_sp._tcp.local. (41)
10:14:10.036621 IP 10.0.137.197.2008 > 10.0.139.255.2008: UDP, length 20
10:14:10.036646 IP 10.0.105.33.5353 > 224.0.0.251.5353: 0*- [0q] 7/0/3 (Cache flush) TXT "rpBA=93:E2:7A:23:99:62" "rpVr=410.6" "rpAD=47cc8bede31b", PTR _rdl
one von Helena._rdlink._tcp.local., TXT "model=D73AP", (Cache flush) SRV IPhone-von-Helena.local.:49167 0 0, (Cache flush) AAAA fe80::1024:e3fc:42db:2a85, (
33 (370)
^C
```

If a computer has multiple interfaces, the interface to capture packets must be specified using the -i option. Type the following command in the terminal

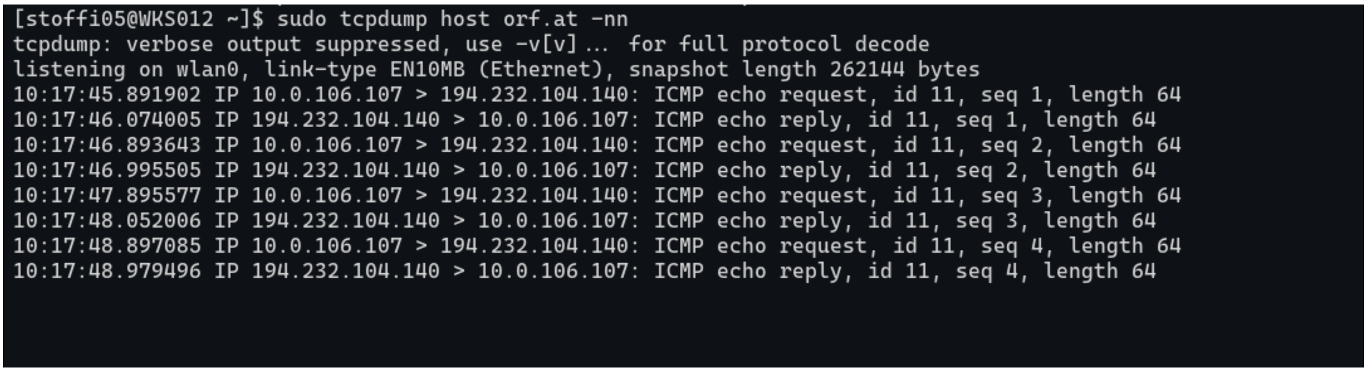
tcpdump -i <your interface> -nn



```
x Dennis ._rdlink._tcp.local. TXT (QU)? iPad von Vanessa._rdlink._tcp.local. TXT (QU)? iPad von Moritz._rdlink._tcp.local. TXT (QU)? iPad von Nathalie._rdlink._tcp
 iPhone von Timon (2)._rdlink._tcp.local. TXT (QU)? iPad von Jakob._companion-link._tcp.local. TXT (QU)? iPad von Nathalie._companion-link._tcp.local. TXT (QU)? iP
mpanion-link._tcp.local. TXT (QU)? iPad von Laci._companion-link._tcp.local. TXT (QU)? iPad von Philipp._companion-link._tcp.local. TXT (QU)? StefanM-bM-^@M-^Ys IP
.local. (1434)
10:16:29.975824 IP 10.0.106.107 > 10.0.104.1: ICMP echo request, id 10, seq 4, length 64
10:16:29.982706 IP 10.0.104.1 > 10.0.106.107: ICMP echo reply, id 10, seq 4, length 64
10:16:30.029027 IP 10.0.112.166.5684 > 10.0.115.255.5684: UDP, length 357
10:16:30.029027 IP 10.0.114.248.137 > 10.0.115.255.137: UDP, length 68
10:16:30.121205 IP 10.0.114.248.137 > 10.0.115.255.137: UDP, length 68
10:16:30.121205 IP 10.0.112.166.5684 > 10.0.115.255.5684: UDP, length 357
10:16:30.121286 IP 10.0.137.58.5353 > 224.0.0.251.5353: 0 [2q] [3n] [1au] ANY (QM)? iPhone (98)._rdlink._tcp.local. ANY (QM)? iPhone-98.local. (157)
10:16:30.224430 IP6 fe80::1c06:56b4:ca69:f899.5353 > ff02::fb.5353: 0 [2q] [3n] [1au] ANY (QM)? iPhone (98)._rdlink._tcp.local. ANY (QM)? iPhone-98.local. (157)
10:16:30.224429 IP 10.0.137.179.17500 > 255.255.255.255.17500: UDP, length 134
10:16:30.224477 IP 10.0.136.121.5353 > 224.0.0.251.5353: 0*- [0q] 2/0/2 (Cache flush) AAAA fe80::1c9a:1810:771d:c9cf, (Cache flush) A 10.0.136.121 (119)
10:16:30.224477 IP 10.0.137.179.17500 > 10.0.139.255.17500: UDP, length 134
10:16:30.224508 IP 10.0.105.158.137 > 10.0.107.255.137: UDP, length 50
```

You can specify the source and destination address of the packets to be captured by using the host option. For example, type

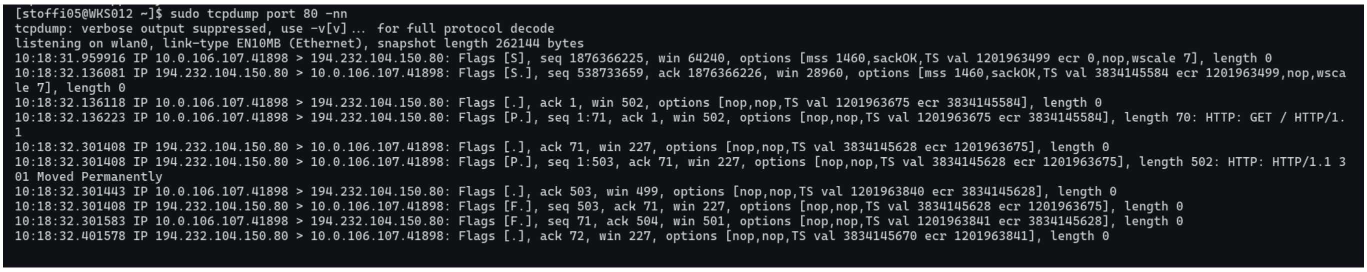
tcpdump host 192.168.1.1 -nn



```
[stoffi05@WKS012 ~]$ sudo tcpdump host orf.at -nn
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:17:45.891902 IP 10.0.106.107 > 194.232.104.140: ICMP echo request, id 11, seq 1, length 64
10:17:46.074005 IP 194.232.104.140 > 10.0.106.107: ICMP echo reply, id 11, seq 1, length 64
10:17:46.893643 IP 10.0.106.107 > 194.232.104.140: ICMP echo request, id 11, seq 2, length 64
10:17:46.995505 IP 194.232.104.140 > 10.0.106.107: ICMP echo reply, id 11, seq 2, length 64
10:17:47.895577 IP 10.0.106.107 > 194.232.104.140: ICMP echo request, id 11, seq 3, length 64
10:17:48.052006 IP 194.232.104.140 > 10.0.106.107: ICMP echo reply, id 11, seq 3, length 64
10:17:48.897085 IP 10.0.106.107 > 194.232.104.140: ICMP echo request, id 11, seq 4, length 64
10:17:48.979496 IP 194.232.104.140 > 10.0.106.107: ICMP echo reply, id 11, seq 4, length 64
```

It is also possible to capture packets based on the source or destination ports. For example, type

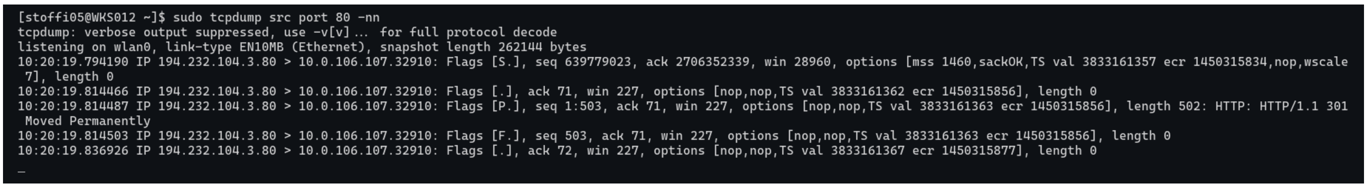
tcpdump port 80 -nn



```
[stoffi05@WKS012 ~]$ sudo tcpdump port 80 -nn
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:18:31.959916 IP 10.0.106.107.41898 > 194.232.104.150.80: Flags [S], seq 1876366225, win 64240, options [mss 1460,sackOK,TS val 1201963499 ecr 0,nop,wscale 7], length 0
10:18:32.136081 IP 194.232.104.150.80 > 10.0.106.107.41898: Flags [S.], seq 538733659, ack 1876366226, win 28960, options [mss 1460,sackOK,TS val 3834145584 ecr 1201963499,nop,wsca
le 7], length 0
10:18:32.136118 IP 10.0.106.107.41898 > 194.232.104.150.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 1201963675 ecr 3834145584], length 0
10:18:32.136223 IP 10.0.106.107.41898 > 194.232.104.150.80: Flags [P.], seq 1:71, ack 1, win 502, options [nop,nop,TS val 1201963675 ecr 3834145584], length 70: HTTP: GET / HTTP/1.
1
10:18:32.301408 IP 194.232.104.150.80 > 10.0.106.107.41898: Flags [.], ack 71, win 227, options [nop,nop,TS val 3834145628 ecr 1201963675], length 0
10:18:32.301408 IP 194.232.104.150.80 > 10.0.106.107.41898: Flags [P.], seq 1:503, ack 71, win 227, options [nop,nop,TS val 3834145628 ecr 1201963675], length 502: HTTP: HTTP/1.1 3
01 Moved Permanently
10:18:32.301443 IP 10.0.106.107.41898 > 194.232.104.150.80: Flags [.], ack 503, win 499, options [nop,nop,TS val 1201963840 ecr 3834145628], length 0
10:18:32.301408 IP 194.232.104.150.80 > 10.0.106.107.41898: Flags [F.], seq 503, ack 71, win 227, options [nop,nop,TS val 3834145628 ecr 1201963675], length 0
10:18:32.301583 IP 10.0.106.107.41898 > 194.232.104.150.80: Flags [F.], seq 71, ack 504, win 501, options [nop,nop,TS val 1201963841 ecr 3834145628], length 0
10:18:32.401578 IP 194.232.104.150.80 > 10.0.106.107.41898: Flags [.], ack 72, win 227, options [nop,nop,TS val 3834145670 ecr 1201963841], length 0
```

It is also possible to specify the source or destination ports. For example, type

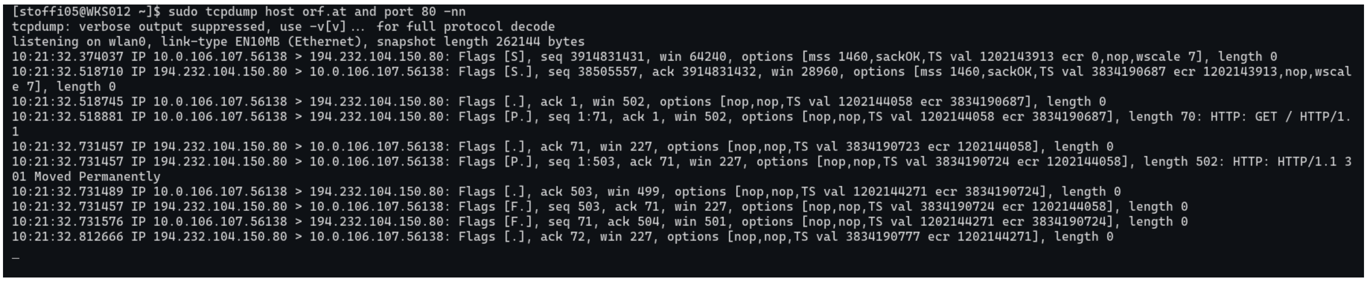
tcpdump src port 80 -nn



```
[stoffi05@WKS012 ~]$ sudo tcpdump src port 80 -nn
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:20:19.794190 IP 194.232.104.3.80 > 10.0.106.107.32910: Flags [S.], seq 639779023, ack 2706352339, win 28960, options [mss 1460,sackOK,TS val 3833161357 ecr 1450315834,nop,wscale
 7], length 0
10:20:19.814466 IP 194.232.104.3.80 > 10.0.106.107.32910: Flags [.], ack 71, win 227, options [nop,nop,TS val 3833161362 ecr 1450315856], length 0
10:20:19.814487 IP 194.232.104.3.80 > 10.0.106.107.32910: Flags [P.], seq 1:503, ack 71, win 227, options [nop,nop,TS val 3833161363 ecr 1450315856], length 502: HTTP: HTTP/1.1 301
 Moved Permanently
10:20:19.814503 IP 194.232.104.3.80 > 10.0.106.107.32910: Flags [F.], seq 503, ack 71, win 227, options [nop,nop,TS val 3833161363 ecr 1450315856], length 0
10:20:19.836926 IP 194.232.104.3.80 > 10.0.106.107.32910: Flags [.], ack 72, win 227, options [nop,nop,TS val 3833161367 ecr 1450315877], length 0
_
```

The port and host information can be combined using he "and" statement. For example, type

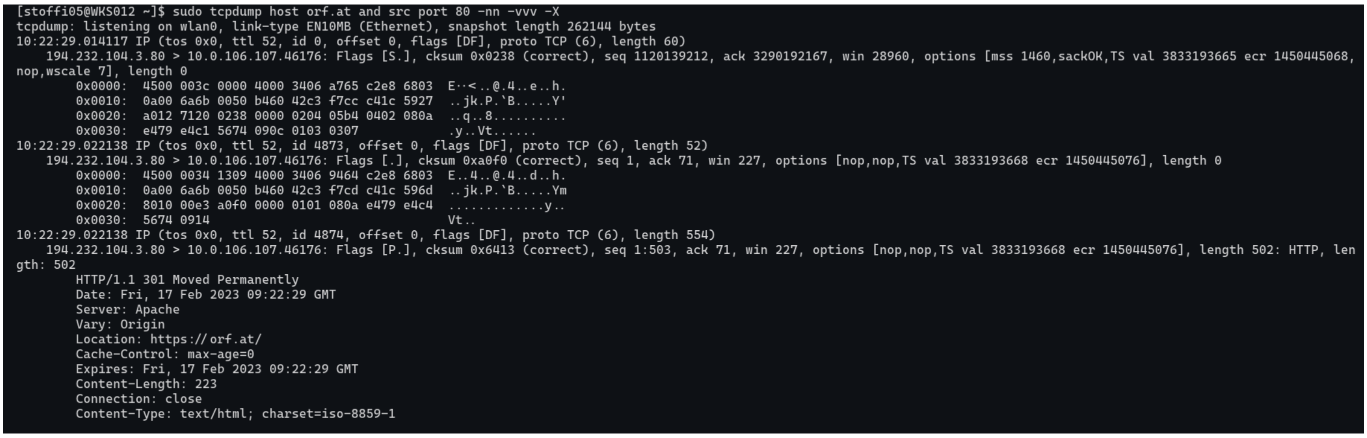
tcpdump host 192.168.1.1 and port 80 -nn



```
[stoffi05@WKS012 ~]$ sudo tcpdump host orf.at and port 80 -nn
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:21:32.374037 IP 10.0.106.107.56138 > 194.232.104.150.80: Flags [S], seq 3914831431, win 64240, options [mss 1460,sackOK,TS val 1202143913 ecr 0,nop,wscale 7], length 0
10:21:32.518710 IP 194.232.104.150.80 > 10.0.106.107.56138: Flags [S.], seq 38505557, ack 3914831432, win 28960, options [mss 1460,sackOK,TS val 3834190687 ecr 1202143913,nop,wscal
e 7], length 0
10:21:32.518745 IP 10.0.106.107.56138 > 194.232.104.150.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 1202144058 ecr 3834190687], length 0
10:21:32.518881 IP 10.0.106.107.56138 > 194.232.104.150.80: Flags [P.], seq 1:71, ack 1, win 502, options [nop,nop,TS val 1202144058 ecr 3834190687], length 70: HTTP: GET / HTTP/1.
1
10:21:32.731457 IP 194.232.104.150.80 > 10.0.106.107.56138: Flags [.], ack 71, win 227, options [nop,nop,TS val 3834190723 ecr 1202144058], length 0
10:21:32.731457 IP 194.232.104.150.80 > 10.0.106.107.56138: Flags [P.], seq 1:503, ack 71, win 227, options [nop,nop,TS val 3834190724 ecr 1202144058], length 502: HTTP: HTTP/1.1 3
01 Moved Permanently
10:21:32.731489 IP 10.0.106.107.56138 > 194.232.104.150.80: Flags [.], ack 503, win 499, options [nop,nop,TS val 1202144271 ecr 3834190724], length 0
10:21:32.731457 IP 194.232.104.150.80 > 10.0.106.107.56138: Flags [F.], seq 503, ack 71, win 227, options [nop,nop,TS val 3834190724 ecr 1202144058], length 0
10:21:32.731576 IP 10.0.106.107.56138 > 194.232.104.150.80: Flags [F.], seq 71, ack 504, win 501, options [nop,nop,TS val 1202144271 ecr 3834190724], length 0
10:21:32.812666 IP 194.232.104.150.80 > 10.0.106.107.56138: Flags [.], ack 72, win 227, options [nop,nop,TS val 3834190777 ecr 1202144271], length 0
_
```

By default, tcpdump shows only packet header information. The -X flag is used to display the payload of the captured packets as well. The -v option controls how much information tcpdump provides (-v being the least verborose and -vvv being the most verborose). For example, type

tcpdump host 192.168.1.1 and src port 80 -nn -vvv -X



```
[stoffi05@WKS012 ~]$ sudo tcpdump host orf.at and src port 80 -nn -vvv -X
tcpdump: listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:22:29.014117 IP (tos 0x0, ttl 52, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    194.232.104.3.80 > 10.0.106.107.46176: Flags [S.], cksum 0x0238 (correct), seq 1120139212, ack 3290192167, win 28960, options [mss 1460,sackOK,TS val 3833193665 ecr 1450445068,
nop,wscale 7], length 0
        0x0000:  4500 003c 0000 4000 3406 a765 c2e8 6803  E··<..@.4..e..h.
        0x0010:  0a00 6a6b 0050 b460 42c3 f7cc c41c 5927  ..jk.P.`B.....Y'
        0x0020:  a012 7120 0238 0000 0204 05b4 0402 080a  ..q..8..........
        0x0030:  e479 e4c1 5674 090c 0103 0307            .y..Vt......
10:22:29.022138 IP (tos 0x0, ttl 52, id 4873, offset 0, flags [DF], proto TCP (6), length 52)
    194.232.104.3.80 > 10.0.106.107.46176: Flags [.], cksum 0xa0f0 (correct), seq 1, ack 71, win 227, options [nop,nop,TS val 3833193668 ecr 1450445076], length 0
        0x0000:  4500 0034 1309 4000 3406 9464 c2e8 6803  E..4..@.4..d..h.
        0x0010:  0a00 6a6b 0050 b460 42c3 f7cd c41c 596d  ..jk.P.`B.....Ym
        0x0020:  8010 00e3 a0f0 0000 0101 080a e479 e4c4  ............y..
        0x0030:  5674 0914                                Vt..
10:22:29.022138 IP (tos 0x0, ttl 52, id 4874, offset 0, flags [DF], proto TCP (6), length 554)
    194.232.104.3.80 > 10.0.106.107.46176: Flags [P.], cksum 0x6413 (correct), seq 1:503, ack 71, win 227, options [nop,nop,TS val 3833193668 ecr 1450445076], length 502: HTTP, len
gth: 502
        HTTP/1.1 301 Moved Permanently
        Date: Fri, 17 Feb 2023 09:22:29 GMT
        Server: Apache
        Vary: Origin
        Location: https://orf.at/
        Cache-Control: max-age=0
        Expires: Fri, 17 Feb 2023 09:22:29 GMT
        Content-Length: 223
        Connection: close
        Content-Type: text/html; charset=iso-8859-1
```

```
What will be the tcpdump command to capture web traffic from host 10.0.0.4
(web traffic to and from  host 10.0.0.4)?
tcpdump host 10.0.0.4 and port 80

What will be the tcpdump command to capture web traffic to host 10.0.0.4?
tcpdump dst 10.0.0.4 and port 80

What will be the tcpdump command to capture web traffic from host 10.0.0.4?
tcpdump src 10.0.0.4 and port 80

What will be the tcpdump command to capture all traffic originating from
network 192.168.0.0 and headed to network 10.0.0.0?
tcpdump src net 192.168.0.0 and dst net 10.0.0.0

What will be the tcpdump command to save the output of the previous command
into a file?

tcpdump src net 192.168.0.0 and dst net 10.0.0.0 -w /path/to/file
```