TCPDUMP - the tool you will find by googling for "The Interface From Hell":

-By GUHAN SENTHILKUMAR

TcpDump:

TcpDump is also the place where LibPcap lives; LibPcap is the standard API and CaptureFile format used by Wireshark and TShark as well as many many other tools.

TcpDump has been ported to Windows; the port is called WinDump, and it lives at www.winpcap.org/windump.

TCPdump is a UNIX tool used to gather data from the network, decipher the bits, and display the output in a semi coherent fashion. The semi coherent output becomes fully coherent output with a little explanation and exposure to the tool.

Downloading TCPDUMP:

Need to download software known as libpcap, which implements a portable framework for capturing low-level network traffic. You can find it at ftp://ftp.ee.lbl.gov/libpcap.tar.Z

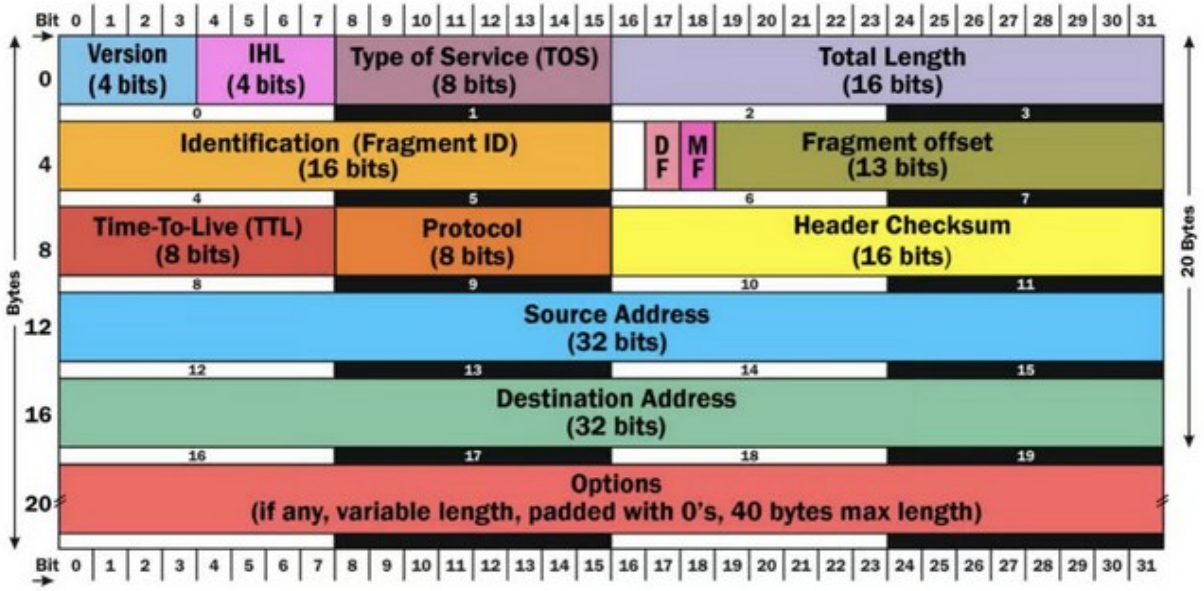
More feature-rich versions are being developed and can be found at www.tcpdump.org Windump is a Windows variant of TCPdump.

You can download it from http://netgroupserv.polito.it/windump.

TCPdump Behavior:

After TCPdump has been installed, most operating systems require root access to run it. This is because reading packets requires access to devices accessible to root-only.

IP Packet Header:



The TCP/IP Header

ASCII CODE:

Standard Characters ASCII Code Table

ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol
0	0	NUL	16	10	DLE	32	20	(space)	48	30	0
1	1	SOH	17	11	DC1	33	21	!	49	31	1
2	2	STX	18	12	DC2	34	22	"	50	32	2
3	3	ETX	19	13	DC3	35	23	#	51	33	3
4	4	EOT	20	14	DC4	36	24	$	52	34	4
5	5	ENQ	21	15	NAK	37	25	%	53	35	5
6	6	ACK	22	16	SYN	38	26	&	54	36	6
7	7	BEL	23	17	ETB	39	27	'	55	37	7
8	8	BS	24	18	CAN	40	28	(	56	38	8
9	9	TAB	25	19	EM	41	29	)	57	39	9
10	A	LF	26	1A	SUB	42	2A	*	58	3A	:
11	B	VT	27	1B	ESC	43	2B	+	59	3B	;
12	C	FF	28	1C	FS	44	2C	,	60	3C	<
13	D	CR	29	1D	GS	45	2D	-	61	3D	=
14	E	SO	30	1E	RS	46	2E	.	62	3E	>
15	F	SI	31	1F	US	47	2F	/	63	3F	?

ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol
64	40	@	80	50	P	96	60	`	112	70	p
65	41	A	81	51	Q	97	61	a	113	71	q
66	42	B	82	52	R	98	62	b	114	72	r
67	43	C	83	53	S	99	63	c	115	73	s
68	44	D	84	54	T	100	64	d	116	74	t
69	45	E	85	55	U	101	65	e	117	75	u
70	46	F	86	56	V	102	66	f	118	76	v
71	47	G	87	57	W	103	67	g	119	77	w
72	48	H	88	58	X	104	68	h	120	78	x
73	49	I	89	59	Y	105	69	i	121	79	y
74	4A	J	90	5A	Z	106	6A	j	122	7A	z
75	4B	K	91	5B	[	107	6B	k	123	7B	{
76	4C	L	92	5C	\	108	6C	l	124	7C	|
77	4D	M	93	5D	]	109	6D	m	125	7D	}
78	4E	N	94	5E	^	110	6E	n	126	7E	~
79	4F	O	95	5F	_	111	6F	o	127	7F	DEL

1) To capture packets from a specific network interface:

```
sudo tcpdump -i wlp58s0
```

```
guhan@Workstation:~$ sudo tcpdump -i wlp58s0
[sudo] password for guhan:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:14:38.396872 IP Workstation.46354 > ec2-52-205-179-80.compute-1.amazonaws.com.https: Flags [P.], seq 2894423798:2894424543, ack 4059294930, win 467, options [nop,nop,TS val 2328209020 ecr 3352194246],
length 745
06:14:38.456730 IP Workstation.33598 > local.airtelfiber.com.domain: 42308+ [1au] PTR? 80.179.205.52.in-addr.arpa. (55)
06:14:38.510445 IP local.airtelfiber.com.domain > Workstation.33598: 42308 1/4/1 PTR ec2-52-205-179-80.compute-1.amazonaws.com. (243)
06:14:38.511092 IP Workstation.51394 > local.airtelfiber.com.domain: 11754+ [1au] PTR? 7.1.168.192.in-addr.arpa. (53)
06:14:38.525848 IP local.airtelfiber.com.domain > Workstation.51394: 11754 NXDomain 0/1/1 (130)
06:14:38.526011 IP Workstation.51394 > local.airtelfiber.com.domain: 11754+ PTR? 7.1.168.192.in-addr.arpa. (42)
06:14:38.533828 IP local.airtelfiber.com.domain > Workstation.51394: 11754 NXDomain 0/1/0 (119)
06:14:38.552587 IP Workstation.55180 > local.airtelfiber.com.domain: 50404+ [1au] PTR? 1.1.168.192.in-addr.arpa. (53)
06:14:38.558060 IP local.airtelfiber.com.domain > Workstation.55180: 50404* 1/0/0 PTR local.airtelfiber.com. (77)
06:14:38.559123 IP Workstation.55180 > local.airtelfiber.com.domain: 30563+ PTR? 1.1.168.192.in-addr.arpa. (42)
06:14:38.565437 IP local.airtelfiber.com.domain > Workstation.55180: 30563* 1/0/0 PTR local.airtelfiber.com. (77)
06:14:38.654338 IP ec2-52-205-179-80.compute-1.amazonaws.com.https > Workstation.46354: Flags [P.], seq 1:60, ack 745, win 425, options [nop,nop,TS val 3352195265 ecr 2328209020], length 59
06:14:38.654372 IP Workstation.46354 > ec2-52-205-179-80.compute-1.amazonaws.com.https: Flags [.], ack 60, win 467, options [nop,nop,TS val 2328209278 ecr 3352195265], length 0
06:14:39.376695 IP Workstation.46354 > ec2-52-205-179-80.compute-1.amazonaws.com.https: Flags [P.], seq 745:1559, ack 60, win 467, options [nop,nop,TS val 2328210000 ecr 3352195265], length 814
06:14:39.637016 IP ec2-52-205-179-80.compute-1.amazonaws.com.https > Workstation.46354: Flags [P.], seq 60:119, ack 1559, win 425, options [nop,nop,TS val 3352196247 ecr 2328210000], length 59
06:14:39.637056 IP Workstation.46354 > ec2-52-205-179-80.compute-1.amazonaws.com.https: Flags [.], ack 119, win 467, options [nop,nop,TS val 2328210260 ecr 3352196247], length 0
06:14:39.831241 IP Workstation.37506 > 69.173.158.64.https: Flags [.], ack 2573236550, win 459, options [nop,nop,TS val 1623641726 ecr 2628046502], length 0
06:14:39.870250 IP 69.173.158.64.https > Workstation.37506: Flags [.], ack 1, win 8520, options [nop,nop,TS val 2628049060 ecr 1623600728], length 0
06:14:39.904137 IP Workstation.50283 > local.airtelfiber.com.domain: 13637+ PTR? 64.158.173.69.in-addr.arpa. (44)
06:14:39.915153 IP local.airtelfiber.com.domain > Workstation.50283: 13637 NXDomain 0/1/0 (98)
```

2) To capture specific number of packets:

```
guhan@Workstation:~$ sudo tcpdump -c 4 -i wlp58s0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:17:16.751030 IP6 del12s05-in-x0a.1e100.net.https > Workstation.44157: UDP, length 164
06:17:16.751522 IP6 Workstation.44157 > del12s05-in-x0a.1e100.net.https: UDP, length 32
06:17:16.770118 IP Workstation.49972 > local.airtelfiber.com.domain: 48036+ PTR? 0.4.4.d.5.5.1.d.2.5.4.9.a.0.2.1.e.d.8.c.f.9.8.8.0.0.9.4.1.0.4.2.ip6.arpa. (90)
06:17:16.779197 IP local.airtelfiber.com.domain > Workstation.49972: 48036 NXDomain 0/0/0 (90)
4 packets captured
8 packets received by filter
0 packets dropped by kernel
guhan@Workstation:~$
```

3) To print captured packets in ASCII format:

```
guhan@Workstation:~$ sudo tcpdump -A -i wlp58s0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:19:10.798724 IP6 Workstation.39731 > del11s08-in-x0e.1e100.net.https: UDP, length 1232
`

O...@$.I.....
.R.U.@$.h.@..... ..3.............:.
oV:.R..@F.:.U.5.....R..B....8.Aa.R.w{..]"...........!k.@..zK...'........%..V#Dt;=Ky.......*.;e... .!P.
.I,.....k.%...R.l.uq).(..........A.......R......z..          2klW#.t...V.!`.H<.........:.>...R...zk ..>.....Q5.cT..V......W.,...~..c....l/..       ......2..\@.J..P.;Q@KImF.......<... ..._.8uI>._.r..5.P:.-....
p....G.f........#.}.v'L..-.M.W...<..n.V..S#.t.....-...@.......S...zO....v A...8..7w....G.......4s.B...A..L..6.{..g}`.....v0.....C.....>..+..Q.......|.5.......{.C...Q.&..O.k....+..MKF..`_*...O..........-.}.
...B.u'+.....WU..bN.C..H/.....x.....v.....  .y...I.....".W.vq.....tZF.:...q...S...=?>.,.....K.....^.=G...I.......T...E..l.....\....<.k.=..%....H..7E.L.T...C...k...
..4C.zp...yq.....8.......g.x..5 .Cz.,..^....=.....cP...9..R..>|..S...O]$....f..........&t....].4].|Tq....d..AW....#.Y.D...r.....\.        .....a..L]     ....'zV.........#...i.`.......V.01...J.V..}(#.C.....
)IVV.3.....=}..L....>.QI.sd...I7..6...Z..........-m.k....2.Lh.ey.X...K.K.G.&....A{c..4.A....cxw..#......Z.S.[Q.id.m}..M.~d.CC.......2...  p.:...tSz:UW...Ri..v..Poe.,......}.9?..4....w....+W...@{.x.!.V.?
.v,o...G...&.....T..D....!D...P..h..KuDT.A...Q.l.....>.p:;..V....4.(m.}.\<..[)O. @.V.]...C..g ixDB3...V...(...r.Iy'...2.S.+4U #....Y_+..U.WU....J..<
06:19:10.798877 IP6 Workstation.39731 > del11s08-in-x0e.1e100.net.https: UDP, length 1232
`

O...@$.I.....
.R.U.@$.h.@..... ..3.............:.
oV:.R..@F.:.U.5.....R..B....8.Aa.R.w{..]"...........!k.@..zK...'........%..V#@.SY^...{.....v4[...jw....d......C...@...
.n|.1U.A..5.8|
/5..`.E`.....J[G..l........3./._]wq.LXP....E..}hX..8.(`.f.G..,.;e/..z..+
.T...T...* Sgdw;.........
oV:.R..@R..../....{$..d.</i...f....o.4..9yG...8.:.6...Y..h.Dc..V.{..c..o.....LI\....we.I9.....
.....
.....
.....
.....
06:19:10.798960 IP6 Workstation.39731 > del11s08-in-x0e.1e100.net.https: UDP, length 1232
`
```

4) To display all available interfaces:

```
guhan@Workstation:~$ sudo tcpdump -D
1.wlp58s0 [Up, Running, Wireless, Associated]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.enp0s31f6 [Up, Disconnected]
5.virbr0 [Up, Disconnected]
6.br-fdccf0ce8055 [Up, Disconnected]
7.docker0 [Up, Disconnected]
8.br-8c16ee636dd2 [Up, Disconnected]
9.bluetooth0 (Bluetooth adapter number 0) [Wireless, Association status unknown]
10.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
11.nflog (Linux netfilter log (NFLOG) interface) [none]
12.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
13.dbus-system (D-Bus system bus) [none]
14.dbus-session (D-Bus session bus) [none]
guhan@Workstation:~$
```

5) To display packets in HEX and ASCII values:

```
guhan@Workstation:~$ sudo tcpdump -XX -i wlp58s0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:22:18.974179 IP Workstation.45416 > local.airtelfiber.com.domain: 40866+ A? connectivity-check.ubuntu.com. (47)
        0x0000:  b4a7 c60a 8088 50eb 71aa f965 0800 4500  ......P.q..e..E.
        0x0010:  004b 1e35 0000 4011 d914 c0a8 0107 c0a8  .K.5..@.........
        0x0020:  0101 b168 0035 0037 83a1 9fa2 0100 0001  ...h.5.7........
        0x0030:  0000 0000 0000 1263 6f6e 6e65 6374 6976  .......connectiv
        0x0040:  6974 792d 6368 6563 6b06 7562 756e 7475  ity-check.ubuntu
        0x0050:  0363 6f6d 0000 0100 01                   .com.....
06:22:18.986099 IP local.airtelfiber.com.domain > Workstation.45416: 40866 12/3/0 A 91.189.91.48, A 185.125.190.18, A 91.189.91.98, A 185.125.190.96, A 91.189.91.96, A 185.125.190.49, A 91.189.91.49, A 91
.189.91.97, A 185.125.190.17, A 185.125.190.48, A 185.125.190.97, A 185.125.190.98 (303)
        0x0000:  50eb 71aa f965 b4a7 c60a 8088 0800 4500  P.q..e.......E.
        0x0010:  014b 5279 4000 4011 63d0 c0a8 0101 c0a8  .KRy@.@.c.......
        0x0020:  0107 0035 b168 0137 fc90 9fa2 8180 0001  ...5.h.7........
        0x0030:  000c 0003 0000 1263 6f6e 6e65 6374 6976  .......connectiv
        0x0040:  6974 792d 6368 6563 6b06 7562 756e 7475  ity-check.ubuntu
        0x0050:  0363 6f6d 0000 0100 01c0 0c00 0100 0100  .com............
        0x0060:  0000 1300 045b bd5b 30c0 0c00 0100 0100  .....[.[0.......
        0x0070:  0000 1300 04b9 7dbe 12c0 0c00 0100 0100  ......}.........
        0x0080:  0000 1300 045b bd5b 62c0 0c00 0100 0100  .....[.[b.......
        0x0090:  0000 1300 04b9 7dbe 60c0 0c00 0100 0100  ......}.`.......
        0x00a0:  0000 1300 045b bd5b 60c0 0c00 0100 0100  .....[.[`.......
        0x00b0:  0000 1300 04b9 7dbe 31c0 0c00 0100 0100  ......}.1.......
        0x00c0:  0000 1300 045b bd5b 31c0 0c00 0100 0100  .....[.[1.......
        0x00d0:  0000 1300 045b bd5b 61c0 0c00 0100 0100  .....[.[a.......
        0x00e0:  0000 1300 04b9 7dbe 11c0 0c00 0100 0100  ......}.........
        0x00f0:  0000 1300 04b9 7dbe 30c0 0c00 0100 0100  ......}.0.......
        0x0100:  0000 1300 04b9 7dbe 61c0 0c00 0100 0100  ......}.a.......
        0x0110:  0000 1300 04b9 7dbe 62c0 1f00 0200 0100  ......}.b.......
        0x0120:  023b 6d00 1003 6e73 3109 6361 6e6f 6e69  .;m...ns1.canoni
        0x0130:  6361 6cc0 26c0 1f00 0200 0100 023b 6d00  cal.&........;m.
        0x0140:  0603 6e73 32c0 ffc0 1f00 0200 0100 023b  ..ns2..........;
```

6) To save captured packets into a file :

```
guhan@Workstation:~$ sudo tcpdump -w captured_packets.pcap -i wlp58s0
tcpdump: listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C123 packets captured
123 packets received by filter
0 packets dropped by kernel
guhan@Workstation:~$
```

7) To read captured packets from a file:

```
guhan@Workstation:~$ sudo tcpdump -r captured_packets.pcap
reading from file captured_packets.pcap, link-type EN10MB (Ethernet), snapshot length 262144
06:23:58.874658 IP6 Workstation.53956 > del11s22-in-x0a.1e100.net.https: Flags [P.], seq 1980496352:1980496391, ack 3757371102, win 419, options [nop,nop,TS val 519838204 ecr 845359745], length 39
06:23:58.875012 IP6 Workstation.53956 > del11s22-in-x0a.1e100.net.https: Flags [FP.], seq 39:63, ack 1, win 419, options [nop,nop,TS val 519838204 ecr 845359745], length 24
06:23:58.915327 IP6 del11s22-in-x0a.1e100.net.https > Workstation.53956: Flags [.], ack 64, win 1046, options [nop,nop,TS val 845413332 ecr 519838204], length 0
06:23:58.915427 IP6 del11s22-in-x0a.1e100.net.https > Workstation.53956: Flags [F.], seq 1, ack 64, win 1046, options [nop,nop,TS val 845413333 ecr 519838204], length 0
06:23:58.915468 IP6 Workstation.53956 > del11s22-in-x0a.1e100.net.https: Flags [.], ack 2, win 419, options [nop,nop,TS val 519838245 ecr 845413333], length 0
06:23:59.428948 IP6 Workstation.43364 > del11s08-in-x03.1e100.net.https: Flags [P.], seq 2305646999:2305647099, ack 1619227803, win 448, options [nop,nop,TS val 906957628 ecr 2678994347], length 100
06:23:59.472960 IP6 del11s08-in-x03.1e100.net.https > Workstation.43364: Flags [.], ack 100, win 1048, options [nop,nop,TS val 2679025331 ecr 906957628], length 0
06:23:59.536235 IP6 del11s08-in-x03.1e100.net.https > Workstation.43364: Flags [P.], seq 1:97, ack 100, win 1048, options [nop,nop,TS val 2679025396 ecr 906957628], length 96
06:23:59.536766 IP6 del11s08-in-x03.1e100.net.https > Workstation.43364: Flags [P.], seq 97:171, ack 100, win 1048, options [nop,nop,TS val 2679025396 ecr 906957628], length 74
06:23:59.536766 IP6 del11s08-in-x03.1e100.net.https > Workstation.43364: Flags [P.], seq 171:202, ack 100, win 1048, options [nop,nop,TS val 2679025396 ecr 906957628], length 31
06:23:59.536766 IP6 del11s08-in-x03.1e100.net.https > Workstation.43364: Flags [P.], seq 202:241, ack 100, win 1048, options [nop,nop,TS val 2679025396 ecr 906957628], length 39
```

8) To capture packets with ip address:

```
guhan@Workstation:~$ sudo tcpdump -n -i wlp58s0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:26:36.520474 IP6 2404:6800:4002:82d::200a.443 > 2401:4900:889f:c8de:120a:9452:d155:d440.53944: Flags [P.], seq 559264509:559264676, ack 1592672905, win 1016, o
ptions [nop,nop,TS val 845570994 ecr 519975315], length 167
06:26:36.520564 IP6 2401:4900:889f:c8de:120a:9452:d155:d440.53944 > 2404:6800:4002:82d::200a.443: Flags [.], ack 167, win 363, options [nop,nop,TS val 519995850 e
cr 845570994], length 0
06:26:37.143191 IP 192.168.1.7.35430 > 184.51.195.217.443: Flags [.], ack 777865850, win 419, options [nop,nop,TS val 4129579151 ecr 780072309], length 0
06:26:37.151653 IP 184.51.195.217.443 > 192.168.1.7.35430: Flags [.], ack 1, win 501, options [nop,nop,TS val 780082539 ecr 4129516827], length 0
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
guhan@Workstation:~$
```

9) To capture only TCP packets:

```
guhan@Workstation:~$ sudo tcpdump -n -i wlp58s0 tcp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:27:28.343187 IP 192.168.1.7.35430 > 184.51.195.217.443: Flags [.], ack 777865850, win 419, options [nop,nop,TS val 4129630351 ecr 780123519], length 0
06:27:28.349286 IP 184.51.195.217.443 > 192.168.1.7.35430: Flags [.], ack 1, win 501, options [nop,nop,TS val 780133748 ecr 4129516827], length 0
06:27:29.344489 IP6 2401:4900:889f:c8de:120a:9452:d155:d440.56090 > 2404:6800:4002:815::2002.443: Flags [P.], seq 2857456977:2857457016, ack 175802014, win 462, options [nop,nop,TS val 101213945 ecr 22037
18437], length 39
06:27:29.344653 IP6 2401:4900:889f:c8de:120a:9452:d155:d440.36236 > 2404:6800:4002:81c::2001.443: Flags [P.], seq 2115513979:2115514018, ack 2443758244, win 493, options [nop,nop,TS val 2931235889 ecr 214
9709456], length 39
06:27:29.344820 IP6 2401:4900:889f:c8de:120a:9452:d155:d440.59516 > 2606:4700:83b0:3ec6:62fe:370:8a70:1f4a.443: Flags [P.], seq 3010693324:3010693363, ack 1934335519, win 476, options [nop,nop,TS val 1389
019861 ecr 2061057631], length 39
06:27:29.358445 IP6 2606:4700:83b0:3ec6:62fe:370:8a70:1f4a.443 > 2401:4900:889f:c8de:120a:9452:d155:d440.59516: Flags [P.], seq 1:40, ack 39, win 9, options [nop,nop,TS val 2061116239 ecr 1389019861], len
gth 39
06:27:29.358528 IP6 2401:4900:889f:c8de:120a:9452:d155:d440.59516 > 2606:4700:83b0:3ec6:62fe:370:8a70:1f4a.443: Flags [.], ack 40, win 476, options [nop,nop,TS val 1389019875 ecr 2061116239], length 0
06:27:29.394528 IP6 2404:6800:4002:81c::2001.443 > 2401:4900:889f:c8de:120a:9452:d155:d440.36236: Flags [P.], seq 1:40, ack 39, win 1050, options [nop,nop,TS val 2149768064 ecr 2931235889], length 39
06:27:29.394614 IP6 2401:4900:889f:c8de:120a:9452:d155:d440.36236 > 2404:6800:4002:81c::2001.443: Flags [.], ack 40, win 493, options [nop,nop,TS val 2931235939 ecr 2149768064], length 0
06:27:29.402145 IP6 2404:6800:4002:815::2002.443 > 2401:4900:889f:c8de:120a:9452:d155:d440.56090: Flags [P.], seq 1:40, ack 39, win 1048, options [nop,nop,TS val 2203777046 ecr 101213945], length 39
06:27:29.402228 IP6 2401:4900:889f:c8de:120a:9452:d155:d440.56090 > 2404:6800:4002:815::2002.443: Flags [.], ack 40, win 462, options [nop,nop,TS val 101214003 ecr 2203777046], length 0
^C
11 packets captured
11 packets received by filter
0 packets dropped by kernel
guhan@Workstation:~$
```

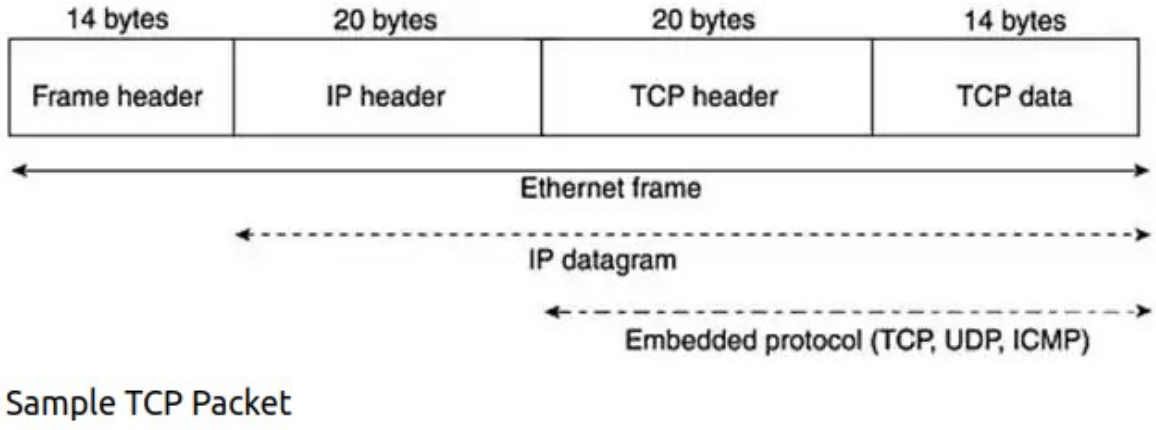
10) Display the version of TCPDUMP:

```
guhan@Workstation:~$ sudo tcpdump --version
tcpdump version 4.99.1
libpcap version 1.10.1 (with TPACKET_V3)
OpenSSL 3.0.2 15 Mar 2022
guhan@Workstation:~$
```

11) In which length is the desired number of bytes to be collected:

```
guhan@Workstation:~$ sudo tcpdump  -i  wlp58s0 -s 39
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 39 bytes
06:55:05.939914  [|ip6]
06:55:05.939914  [|ip6]
06:55:05.940164  [|ip6]
06:55:05.940347  [|ip6]
06:55:05.940347  [|ip6]
06:55:05.940487  [|ip6]
06:55:05.940519  [|ip6]
06:55:05.983911  [|ip6]
06:55:05.983911  [|ip6]
^C
9 packets captured
9 packets received by filter
0 packets dropped by kernel
guhan@Workstation:~$ sudo tcpdump  -i  wlp58s0 -s 1400
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 1400 bytes
06:55:11.701777 IP6 whatsapp-cdn6-shv-02-maa2.fbcdn.net.https > Workstation.46070: Flags [P.], seq 4189448069:4189448140, ack 2243992157, win 619, options [nop,nop,TS val 2974577418 ecr 3714371782],
h 71
06:55:11.701833 IP6 Workstation.46070 > whatsapp-cdn6-shv-02-maa2.fbcdn.net.https: Flags [.], ack 71, win 797, options [nop,nop,TS val 3714372022 ecr 2974577418], length 0
06:55:11.760282 IP Workstation.36709 > local.airtelfiber.com.domain: 6530+ PTR? 0.4.4.d.5.5.1.d.2.5.4.9.a.0.2.1.e.d.8.c.f.9.8.8.0.0.9.4.1.0.4.2.ip6.arpa. (90)
06:55:11.770467 IP local.airtelfiber.com.domain > Workstation.36709: 6530 NXDomain 0/0/0 (90)
06:55:11.863582 IP Workstation.37831 > local.airtelfiber.com.domain: 55083+ PTR? 1.1.168.192.in-addr.arpa. (42)
06:55:11.866410 IP local.airtelfiber.com.domain > Workstation.37831: 55083* 1/0/0 PTR local.airtelfiber.com. (77)
06:55:11.866980 IP Workstation.45473 > local.airtelfiber.com.domain: 46368+ PTR? 7.1.168.192.in-addr.arpa. (42)
06:55:11.885015 IP local.airtelfiber.com.domain > Workstation.45473: 46368 NXDomain 0/1/0 (119)
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
guhan@Workstation:~$
```

Sample Packet and TCP header & Data:



Sample TCP Packet

Basic command that will get us HTTPS traffic:

```
guhan@Workstation:~$ sudo tcpdump -nnSX port 443
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
07:08:28.156134 IP6 2401:4900:889f:c8de:120a:9452:d155:d440.50740 > 2620:1ec:bdf::58.443: Flags [P.], seq 3565117260:3565117299, ack 1646127044, win 461, options [nop,nop,TS val 3372786664 ecr 2745279488]
, length 39
        0x0000:  6006 8555 0047 0640 2401 4900 889f c8de  `..U.G.@$.I.....
        0x0010:  120a 9452 d155 d440 2620 01ec 0bdf 0000  ...R.U.@&.......
        0x0020:  0000 0000 0000 0058 c634 01bb d47f 5f4c  .......X.4...._L
        0x0030:  621d e7c4 8018 01cd 3f03 0000 0101 080a  b.......?.......
        0x0040:  c908 a3e8 a3a1 a400 1703 0300 2204 d218  ............"...
        0x0050:  63f0 0577 d066 ad87 42c4 f425 8d0e 03cf  c..w.f..B..%....
        0x0060:  e6cd 1aef c236 7bce 2690 1919 1df9 87    .....6{.&......
07:08:28.165163 IP6 2620:1ec:bdf::58.443 > 2401:4900:889f:c8de:120a:9452:d155:d440.50740: Flags [.], ack 3565117299, win 83, options [nop,nop,TS val 2745337635 ecr 3372786664], length 0
        0x0000:  6b85 5cbd 0020 0632 2620 01ec 0bdf 0000  k.\....2&......
        0x0010:  0000 0000 0000 0058 2401 4900 889f c8de  .......X$.I.....
        0x0020:  120a 9452 d155 d440 01bb c634 621d e7c4  ...R.U.@...4b...
        0x0030:  d47f 5f73 8010 0053 5a38 0000 0101 080a  .._s...SZ8......
        0x0040:  a3a2 8723 c908 a3e8                      ...#....
07:08:28.165164 IP6 2620:1ec:bdf::58.443 > 2401:4900:889f:c8de:120a:9452:d155:d440.50740: Flags [P.], seq 1646127044:1646127083, ack 3565117299, win 83, options [nop,nop,TS val 2745337635 ecr 3372786664],
 length 39
```

Monitor Traffic to a Suspicious Domain:

```
guhan@Workstation:~$ sudo tcpdump -i wlp58s0 dst host facebook.com
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
07:15:30.787648 IP6 Workstation.52411 > edge-star-mini6-shv-02-maa2.facebook.com.https: UDP, length 1232
07:15:30.787697 IP6 Workstation.52411 > edge-star-mini6-shv-02-maa2.facebook.com.https: UDP, length 1232
07:15:30.800946 IP6 Workstation.52411 > edge-star-mini6-shv-02-maa2.facebook.com.https: UDP, length 46
07:15:30.804452 IP6 Workstation.52411 > edge-star-mini6-shv-02-maa2.facebook.com.https: UDP, length 134
07:15:30.804509 IP6 Workstation.52411 > edge-star-mini6-shv-02-maa2.facebook.com.https: UDP, length 69
07:15:30.810948 IP6 Workstation.52411 > edge-star-mini6-shv-02-maa2.facebook.com.https: UDP, length 34
07:15:31.510354 IP6 Workstation.52411 > edge-star-mini6-shv-02-maa2.facebook.com.https: UDP, length 653
07:15:31.517749 IP6 Workstation.52411 > edge-star-mini6-shv-02-maa2.facebook.com.https: UDP, length 34
07:15:32.279010 IP6 Workstation.52411 > edge-star-mini6-shv-02-maa2.facebook.com.https: UDP, length 43
07:15:32.385906 IP6 Workstation.52411 > edge-star-mini6-shv-02-maa2.facebook.com.https: UDP, length 792
07:15:32.392109 IP6 Workstation.52411 > edge-star-mini6-shv-02-maa2.facebook.com.https: UDP, length 34
07:15:32.582715 IP6 Workstation.52411 > edge-star-mini6-shv-02-maa2.facebook.com.https: UDP, length 560
```

Capture Credentials in Plain Text:

```
guhan@Workstation:~$ sudo tcpdump -A -i wlp58s0 'port http or port ftp or port telnet'
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
07:19:28.094892 IP6 Workstation.45914 > tzdela-bd-in-x03.1e100.net.http: Flags [S], seq 3417879386, win 64952, options [mss 1412,sackOK,TS val 466952649 ecr 0,nop,wscale 7], length 0
 ..G.(.@$.I......
.R.U.@$.h.@......... ..Z.P...Z...................
..!.........
07:19:28.134020 IP6 tzdela-bd-in-x03.1e100.net.http > Workstation.45914: Flags [S.], seq 620497376, ack 3417879387, win 65535, options [mss 1440,sackOK,TS val 2723277519 ecr 466952649,nop,wscale 8], lengt
h 0
k....(.;$.h.@......... .$.I......
.R.U.@.P.Z$.    ....[.....*.........
.Q....!.....
07:19:28.134082 IP6 Workstation.45914 > tzdela-bd-in-x03.1e100.net.http: Flags [.], ack 1, win 508, options [nop,nop,TS val 466952688 ecr 2723277519], length 0
 ..G. .@$.I......
.R.U.@$.h.@......... ..Z.P...[$.        ............
..!..Q..
07:19:28.134832 IP6 Workstation.45914 > tzdela-bd-in-x03.1e100.net.http: Flags [P.], seq 1:436, ack 1, win 508, options [nop,nop,TS val 466952689 ecr 2723277519], length 435: HTTP: POST /wr2 HTTP/1.1
`..G...@$.I......
.R.U.@$.h.@......... ..Z.P...[$.        ......X.....
..!..Q..POST /wr2 HTTP/1.1
Host: o.pki.goog
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/ocsp-request
Content-Length: 83
Connection: keep-alive
Priority: u=2
Pragma: no-cache
Cache-Control: no-cache

0Q0O0M0K0I0     ..+........SB........Mw|.#1.{5.......y..>7$.!..49mB.0..?.....\.
......{
07:19:28.174119 IP6 tzdela-bd-in-x03.1e100.net.http > Workstation.45914: Flags [.], ack 436, win 1053, options [nop,nop,TS val 2723277559 ecr 466952689], length 0
k.... .;$.h.@......... .$.I......
.R.U.@.P.Z$.    .........E.......
.Q....!.
07:19:28.240492 IP6 tzdela-bd-in-x03.1e100.net.http > Workstation.45914: Flags [P.], seq 1:702, ack 436, win 1053, options [nop,nop,TS val 2723277625 ecr 466952689], length 701: HTTP: HTTP/1.1 200 OK
k......;$.h.@......... .$.I......
.R.U.@.P.Z$.    ..........      ......
.Q.9..!.HTTP/1.1 200 OK
Content-Type: application/ocsp-response
Date: Fri, 02 May 2025 01:49:28 GMT
Cache-Control: public, max-age=14400
Server: ocsp_responder
Content-Length: 471
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
```

Finding Packets by Network:

```
guhan@Workstation: $ sudo tcpdump net 192.168.1.0/24
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
07:30:48.771232 IP Workstation.55120 > local.airtelfiber.com.domain: 22611+ [1au] A? chat.google.com. (44)
07:30:48.781333 IP local.airtelfiber.com.domain > Workstation.55120: 22611 1/0/1 A 142.251.42.46 (60)
07:30:48.832955 IP Workstation.37970 > local.airtelfiber.com.domain: 11154+ [1au] PTR? 1.1.168.192.in-addr.arpa. (53)
07:30:48.835680 IP local.airtelfiber.com.domain > Workstation.37970: 11154* 1/0/0 PTR local.airtelfiber.com. (77)
07:30:48.836025 IP Workstation.37970 > local.airtelfiber.com.domain: 32086+ PTR? 1.1.168.192.in-addr.arpa. (42)
07:30:48.838482 IP local.airtelfiber.com.domain > Workstation.37970: 32086* 1/0/0 PTR local.airtelfiber.com. (77)
07:30:48.839787 IP Workstation.59474 > local.airtelfiber.com.domain: 35363+ PTR? 7.1.168.192.in-addr.arpa. (42)
07:30:48.854606 IP local.airtelfiber.com.domain > Workstation.59474: 35363 NXDomain 0/1/0 (119)
07:30:49.145406 IP local.airtelfiber.com.59217 > 192.168.1.255.9995: UDP, length 321
07:30:49.248135 IP Workstation.37191 > local.airtelfiber.com.domain: 7614+ PTR? 255.1.168.192.in-addr.arpa. (44)
07:30:49.256226 IP local.airtelfiber.com.domain > Workstation.37191: 7614 NXDomain 0/1/0 (121)
^C
```

Raw Output View:

```
guhan@Workstation:~$ sudo tcpdump -ttnnvvS
tcpdump: listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
1746151429.209062 IP6 (flowlabel 0x23785, hlim 64, next-header TCP (6) payload length: 71) 2401:4900:889f:c8de:120a:9452:d155:d440.43840 > 2404:6800:4009:820::2005.443: Flags [P.], cksum 0xfef2 (incorrect
 -> 0xa11a), seq 821428621:821428660, ack 620595568, win 490, options [nop,nop,TS val 1061918207 ecr 4182458490], length 39
1746151429.212595 IP (tos 0x0, ttl 64, id 48092, offset 0, flags [none], proto UDP (17), length 61)
    192.168.1.7.34475 > 192.168.1.1.53: [bad udp cksum 0x8393 -> 0x7c4d!] 40764+ Type65? chat.google.com. (33)
1746151429.219152 IP6 (flowlabel 0x3f9d1, hlim 64, next-header UDP (17) payload length: 1240) 2401:4900:889f:c8de:120a:9452:d155:d440.35201 > 2404:6800:4002:82d::200e.443: [bad udp cksum 0x039e -> 0x4b26!
] UDP, length 1232
1746151429.219309 IP6 (flowlabel 0x3f9d1, hlim 64, next-header UDP (17) payload length: 1240) 2401:4900:889f:c8de:120a:9452:d155:d440.35201 > 2404:6800:4002:82d::200e.443: [bad udp cksum 0x039e -> 0xbdbc!
] UDP, length 1232
1746151429.219402 IP6 (flowlabel 0x3f9d1, hlim 64, next-header UDP (17) payload length: 353) 2401:4900:889f:c8de:120a:9452:d155:d440.35201 > 2404:6800:4002:82d::200e.443: [bad udp cksum 0x0027 -> 0xd6d1!]
 UDP, length 345
```

From specific IP and destined for a specific Port:

```
guhan@Workstation:~$ sudo tcpdump -nnvvS src 192.168.1.7
tcpdump: listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:46:19.658763 IP (tos 0x0, ttl 64, id 26339, offset 0, flags [none], proto UDP (17), length 68)
    192.168.1.7.33737 > 192.168.1.1.53: [bad udp cksum 0x839a -> 0x1725!] 14491+ [1au] Type65? www.inc.com. ar: . OPT UDPsize=1472 (40)
23:46:19.658893 IP (tos 0x0, ttl 64, id 63504, offset 0, flags [none], proto UDP (17), length 68)
    192.168.1.7.39817 > 192.168.1.1.53: [bad udp cksum 0x839a -> 0x6495!] 4971+ [1au] A? www.inc.com. ar: . OPT UDPsize=1472 (40)
23:46:19.658983 IP (tos 0x0, ttl 64, id 54366, offset 0, flags [none], proto UDP (17), length 72)
    192.168.1.7.56351 > 192.168.1.1.53: [bad udp cksum 0x839e -> 0xf074!] 26870+ [1au] A? www.nytimes.com. ar: . OPT UDPsize=1472 (44)
23:46:19.659066 IP (tos 0x0, ttl 64, id 20977, offset 0, flags [none], proto UDP (17), length 72)
    192.168.1.7.58208 > 192.168.1.1.53: [bad udp cksum 0x839e -> 0x2597!] 4499+ [1au] AAAA? www.nytimes.com. ar: . OPT UDPsize=1472 (44)
23:46:19.659147 IP (tos 0x0, ttl 64, id 42064, offset 0, flags [none], proto UDP (17), length 72)
    192.168.1.7.60912 > 192.168.1.1.53: [bad udp cksum 0x839e -> 0xd434!] 13157+ [1au] Type65? www.nytimes.com. ar: . OPT UDPsize=1472 (44)
23:46:19.669250 IP (tos 0x0, ttl 64, id 17595, offset 0, flags [none], proto UDP (17), length 80)
    192.168.1.7.37113 > 192.168.1.1.53: [bad udp cksum 0x83a6 -> 0xd22c!] 37236+ [1au] Type65? mansueto.map.fastly.net. ar: . OPT UDPsize=1472 (52)
23:46:19.674218 IP (tos 0x0, ttl 64, id 27198, offset 0, flags [none], proto UDP (17), length 80)
    192.168.1.7.48165 > 192.168.1.1.53: [bad udp cksum 0x83a6 -> 0xfc3b!] 24889+ [1au] AAAA? mansueto.map.fastly.net. ar: . OPT UDPsize=1472 (52)
23:46:19.682228 IP (tos 0x0, ttl 64, id 41373, offset 0, flags [none], proto UDP (17), length 79)
    192.168.1.7.59706 > 192.168.1.1.53: [bad udp cksum 0x83a5 -> 0x0c33!] 45063+ [1au] AAAA? nytimes.map.fastly.net. ar: . OPT UDPsize=1472 (51)
23:46:19.682440 IP (tos 0x0, ttl 64, id 7246, offset 0, flags [none], proto UDP (17), length 79)
    192.168.1.7.33932 > 192.168.1.1.53: [bad udp cksum 0x83a5 -> 0x2f00!] 61891+ [1au] Type65? nytimes.map.fastly.net. ar: . OPT UDPsize=1472 (51)
^C
9 packets captured
9 packets received by filter
0 packets dropped by kernel
```

From One Network to Another:

```
guhan@Workstation:~$ sudo tcpdump -nvX src net 192.168.1.7 and dst net 192.168.1.1
tcpdump: listening on wlp58s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:50:18.414672 IP (tos 0x0, ttl 64, id 40423, offset 0, flags [none], proto UDP (17), length 73)
    192.168.1.7.37976 > 192.168.1.1.53: 3007+ [1au] Type65? tzm.px-cloud.net. (45)
        0x0000:  4500 0049 9de7 0000 4011 5964 c0a8 0107  E..I....@.Yd....
        0x0010:  c0a8 0101 9458 0035 0035 839f 0bbf 0100  .....X.5.5......
        0x0020:  0001 0000 0000 0001 0374 7a6d 0870 782d  .........tzm.px-
        0x0030:  636c 6f75 6403 6e65 7400 0041 0001 0000  cloud.net..A....
        0x0040:  2905 c000 0000 0000 00                   ).........
23:50:18.414992 IP (tos 0x0, ttl 64, id 9368, offset 0, flags [none], proto UDP (17), length 73)
    192.168.1.7.51229 > 192.168.1.1.53: 60674+ [1au] A? tzm.px-cloud.net. (45)
        0x0000:  4500 0049 2498 0000 4011 d2b3 c0a8 0107  E..I$...@.......
        0x0010:  c0a8 0101 c81d 0035 0035 839f ed02 0100  .......5.5......
        0x0020:  0001 0000 0000 0001 0374 7a6d 0870 782d  .........tzm.px-
        0x0030:  636c 6f75 6403 6e65 7400 0001 0001 0000  cloud.net.......
        0x0040:  2905 c000 0000 0000 00                   ).........
23:50:18.415224 IP (tos 0x0, ttl 64, id 22550, offset 0, flags [none], proto UDP (17), length 73)
    192.168.1.7.54863 > 192.168.1.1.53: 2822+ [1au] AAAA? tzm.px-cloud.net. (45)
        0x0000:  4500 0049 5816 0000 4011 9f35 c0a8 0107  E..IX...@..5....
        0x0010:  c0a8 0101 d64f 0035 0035 839f 0b06 0100  .....O.5.5......
        0x0020:  0001 0000 0000 0001 0374 7a6d 0870 782d  .........tzm.px-
        0x0030:  636c 6f75 6403 6e65 7400 001c 0001 0000  cloud.net.......
        0x0040:  2905 c000 0000 0000 00                   ).........
23:50:19.088125 IP (tos 0x0, ttl 64, id 46870, offset 0, flags [none], proto UDP (17), length 73)
    192.168.1.7.47329 > 192.168.1.1.53: 25590+ [1au] AAAA? tzm.px-cloud.net. (45)
        0x0000:  4500 0049 b716 0000 4011 4035 c0a8 0107  E..I....@.@5....
        0x0010:  c0a8 0101 b8e1 0035 0035 839f 63f6 0100  .......5.5..c...
        0x0020:  0001 0000 0000 0001 0374 7a6d 0870 782d  .........tzm.px-
        0x0030:  636c 6f75 6403 6e65 7400 001c 0001 0000  cloud.net.......
        0x0040:  2905 c000 0000 0000 00                   ).........
```

Additional ways to tweak how you call tcpdump:

- X : Show the packet's *contents* in both hex and ASCII.
- **-XX** : Same as **-X**, but also shows the ethernet header.
- **-D** : Show the list of available interfaces
- **-l** : Line-readable output (for viewing as you save, or sending to other commands)
- **-q** : Be less verbose (more quiet) with your output.
- **-t** : Give human-readable timestamp output.
- **-tttt** : Give maximally human-readable timestamp output.
- **-i eth0** : Listen on the eth0 interface.
- **-vv** : Verbose output (more v's gives more output).
- **-c** : Only get *x* number of packets and then stop.
- **-s** : Define the *snaplength* (size) of the capture in bytes. Use -s0 to get everything, unless you are intentionally capturing less.
- **-S** : Print absolute sequence numbers.
- **-e** : Get the ethernet header as well.
- **-q** : Show less protocol information.
- **-E** : Decrypt IPSEC traffic by providing an encryption key.

TCPDUMP Observatory analysis adds more insightfulness with “combining options” through below Operators:

The ability to **combine options in creative ways** in order to isolate exactly what you’re looking for:

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

Conclusion:

Tcpdump is an essential tool for learning networking and mastering packet analysis due to its raw and precise inspection capabilities. While tools like Wireshark are useful, true expertise begins with tcpdump. This guide offers a strong starting point, but users should refer to the man page for advanced use.

Study Reference Links:

1. **Official Tcpdump Manual (Man Page):** https://www.tcpdump.org/manpages/tcpdump.1.html
2. **Tcpdump Cheat Sheet (PacketLife):** https://packetlife.net/media/library/13/tcpdump.pdf
3. **Tcpdump Tutorial for Beginners (TutorialsPoint):** https://www.tutorialspoint.com/tcpdump/index.htm
4. **Wireshark vs Tcpdump (Comparison Study):** https://danielmiessler.com/study/tcpdump/