tcpdump

capturing network traffic

Lev Walkin
@levwalkin

What is tcpdump?

Capture

[Save]

Filter

Show and explain

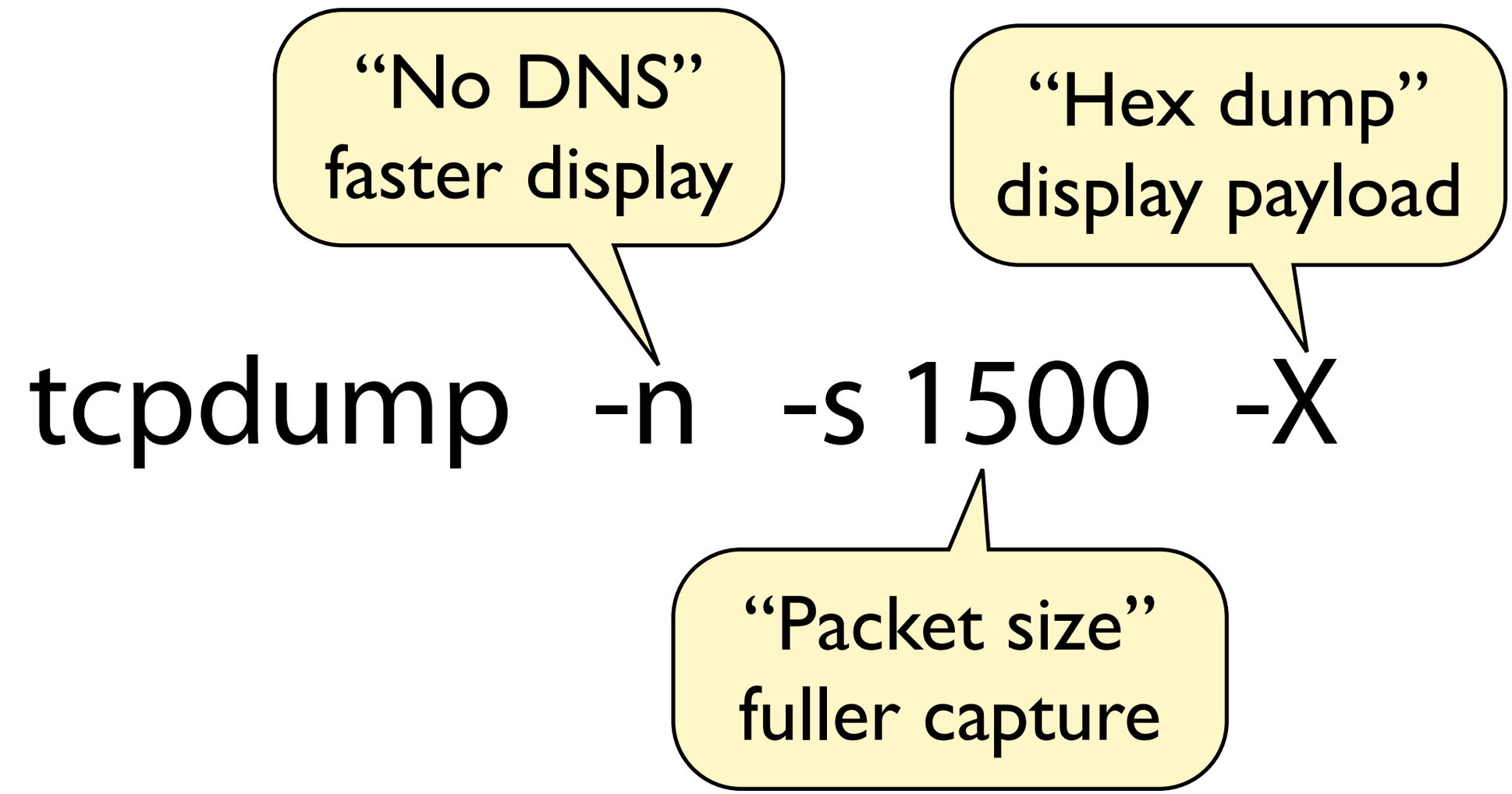
Why tcpdump?

Universal file format (.pcap)

Universal filter expression

Can work on remote hosts

Quick start


"No DNS"
faster display
"Hex dump"
display payload
tcpdump -n -s 1500 -X
"Packet size"
fuller capture

tcpdump -Xns0

Header

HEX
(-X)

ASCII
(-A)

...next

vlm — 80×28

```
01:45:38.094148 IP 216.218.215.245.49663 > 50.18.56.119.80: Flags [P.], seq 1:24
8, ack 1, win 8265, options [nop,nop,TS val 803565308 ecr 2125048095], length 24
7
        0x0000:  ff03 0021 4500 012b 0ea3 4000 4006 0fd1  ...!E..+..@.@...
        0x0010:  d8da d7f5 3212 3877 c1ff 0050 816e bf16  ....2.8w...P.n..
        0x0020:  06ef 30d6 8018 2049 966d 0000 0101 080a  ..0....I.m......
        0x0030:  2fe5 6efc 7ea9 a91f 4745 5420 2f61 7069  /.n.~...GET./api
        0x0040:  2f76 312f 7365 6172 6368 3f61 7070 6b65  /v1/search?appke
        0x0050:  793d 6533 2e6a 736b 6974 2671 3d63 6869  y=e3.jskit&q=chi
        0x0060:  6c64 7265 6e6f 663a 6874 7470 3a2f 2f61  ldrenof:http://a
        0x0070:  626f 7574 6563 686f 2e63 6f6d 2f25 3241  boutecho.com/%2A
        0x0080:  2532 3069 7465 6d73 5065 7250 6167 653a  %20itemsPerPage:
        0x0090:  3125 3230 6368 696c 6472 656e 3a30 2048  1%20children:0.H
        0x00a0:  5454 502f 312e 310d 0a55 7365 722d 4167  TTP/1.1..User-Ag
        0x00b0:  656e 743a 2063 7572 6c2f 372e 3234 2e30  ent:.curl/7.24.0
        0x00c0:  2028 7838 365f 3634 2d61 7070 6c65 2d64  .(x86_64-apple-d
        0x00d0:  6172 7769 6e31 322e 3029 206c 6962 6375  arwin12.0).libcu
        0x00e0:  726c 2f37 2e32 342e 3020 4f70 656e 5353  rl/7.24.0.OpenSS
        0x00f0:  4c2f 302e 392e 3872 207a 6c69 622f 312e  L/0.9.8r.zlib/1.
        0x0100:  322e 350d 0a48 6f73 743a 2061 7069 2e65  2.5..Host:.api.e
        0x0110:  6368 6f65 6e61 626c 6564 2e63 6f6d 0d0a  choenabled.com..
        0x0120:  4163 6365 7074 3a20 2a2f 2a0d 0a0d 0a    Accept:.*/*....
01:45:38.344774 IP 50.18.56.119.80 > 216.218.215.245.49663: Flags [.], ack 248,
win 2772, options [nop,nop,TS val 2125048120 ecr 803565308], length 0
        0x0000:  ff03 0021 4500 0034 99e1 4000 3706 8e89  ...!E..4..@.7...
        0x0010:  3212 3877 d8da d7f5 0050 c1ff 06ef 30d6  2.8w.....P....0.
        0x0020:  816e c00d 8010 0ad4 4e3b 0000 0101 080a  .n......N;......
        0x0030:  7ea9 a938 2fe5 6efc                      ~..8/.n.
```

Workflow 1:
Online analysis

Fast (-n), full (-s0), with dump (-X), ...and filter:

tcpdump -Xns0 port 80

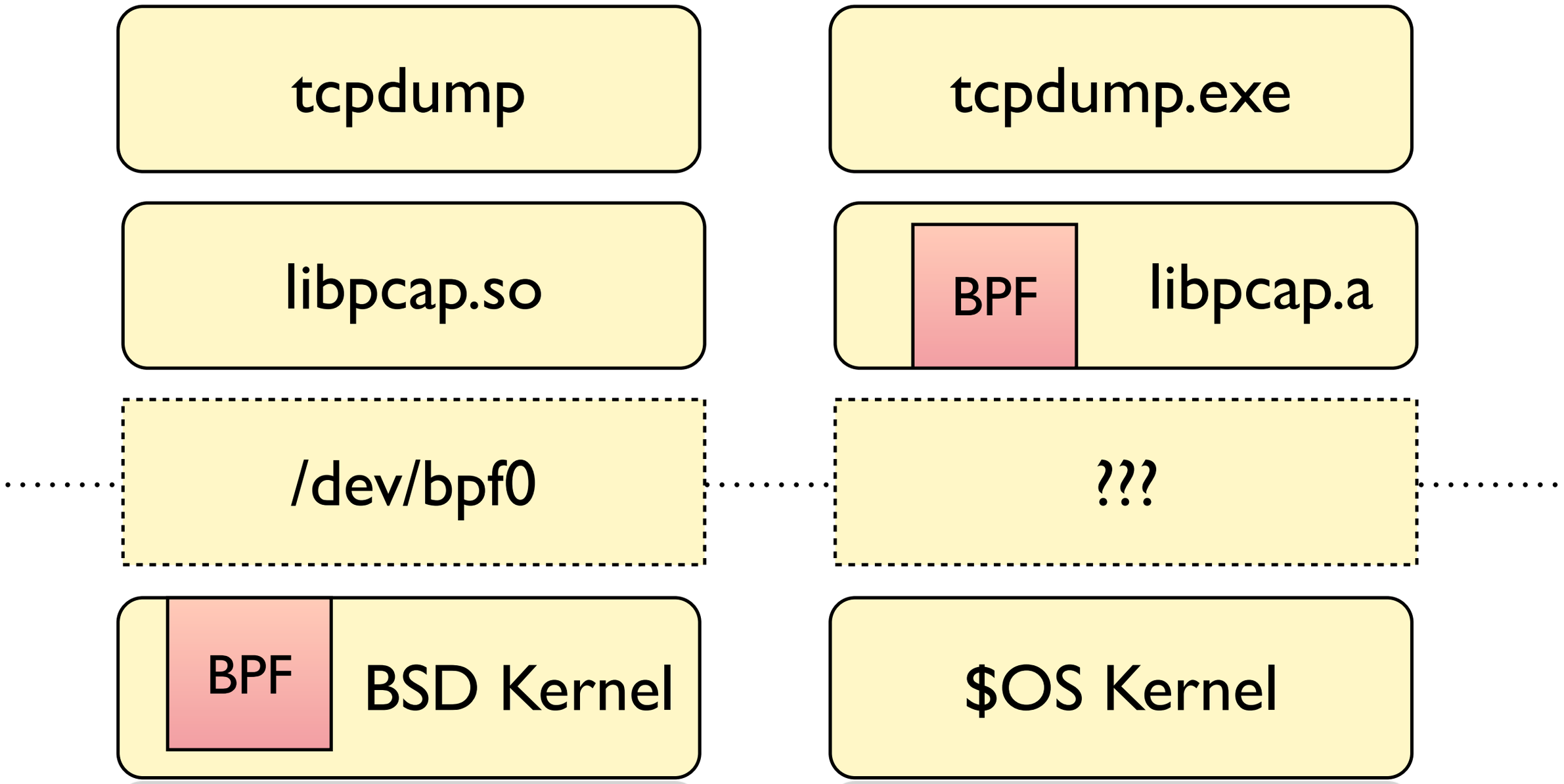
Workflow 2: Offline analysis

Full (-s0), write to a file (-w), then read:

tcpdump -s0 -w *abc.pcap* port 80

tcpdump -nXr *abc.pcap* host nweb30

Architecture



BPF: Berkeley Packet Filter

The human readable filter is converted to a bytecode (-d), sent to kernel. Efficient.

http://www.tcpdump.org/papers/bpf-usenix93.pdf

Filter language

and, or

port 80

host nweb30

‘src host localhost and dst port 80’

Output

Timestamp (-tt, -ttt, -tttt)

L3 protocol

Relative TCP ack number

TCP Flags (S, F, R)

Relative TCP sequence number

Advertised TCP window size

```
216.2 8.215.245.61966 > 50.18.0 102.80:
Flags [P.], seq 1:473, ack 1, win 8265,
options [nop,nop,TS val 808617737 ecr
1091126708], length 472
```

List of TCP options (e.g. wscale)

Payload length

WTFs (0/3)

tcpdump: no suitable device found

Use sudo or check /dev/bpf* permissions

WTFs (1/3)

Output is laggy?

Disable DNS resolution (-n)

Or save to a file (-w)

WTFs (2/3)

Nothing happens?

Select a proper interface
(-i ppp0)

WTFs (3/3)

Want to cut-n-paste HTML?

Use ASCII output (-A), or save to .pcap (-r) and fire up vim.

RFCs

IP: RFC791

TCP: RFC793, 1122

DNS: RFC1034, 1035

Many short overviews exist!

See also

WireShark (GUI)

SSLdump (decrypt HTTPS)

tcpflow (split by TCP flow)

libpcap (C interface)

lionet.info/ipcad

RTFM

man pcap-filter

man tcpdump

man pcap

man bpf

Questions?