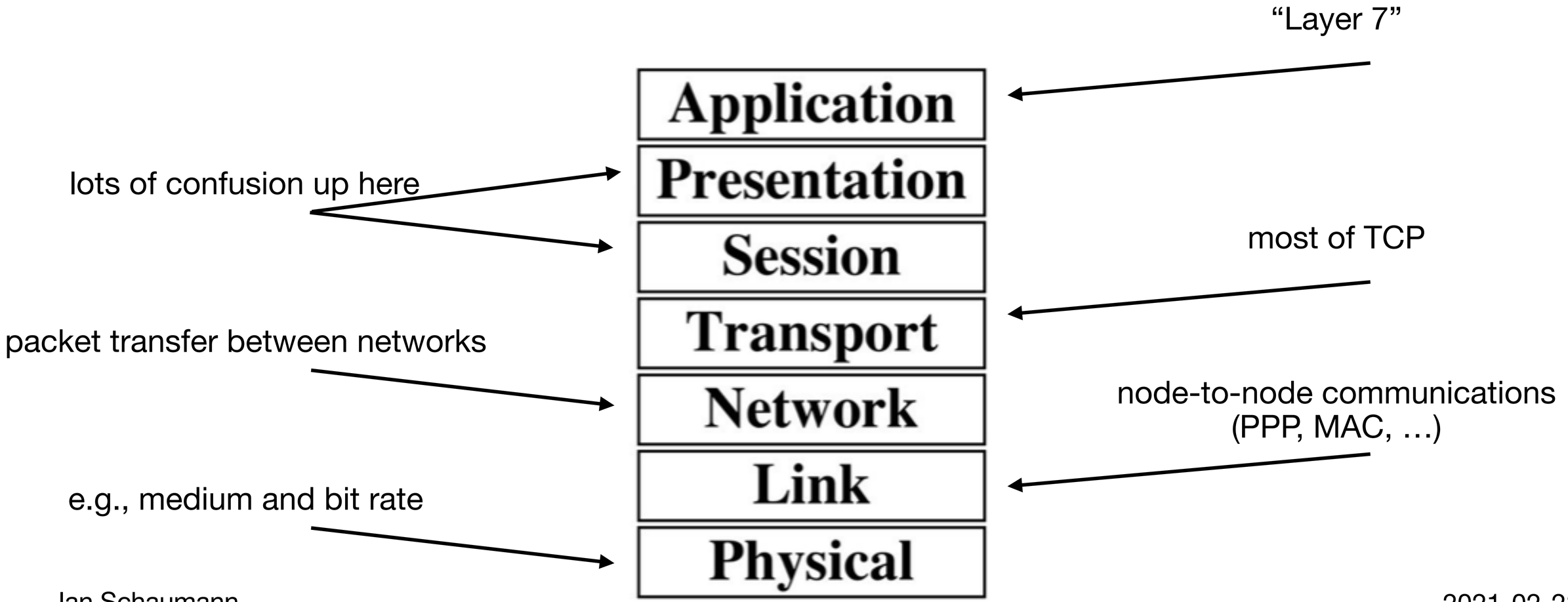

# System Administration

## Week 05, Segment 1
## Networking I: Layers

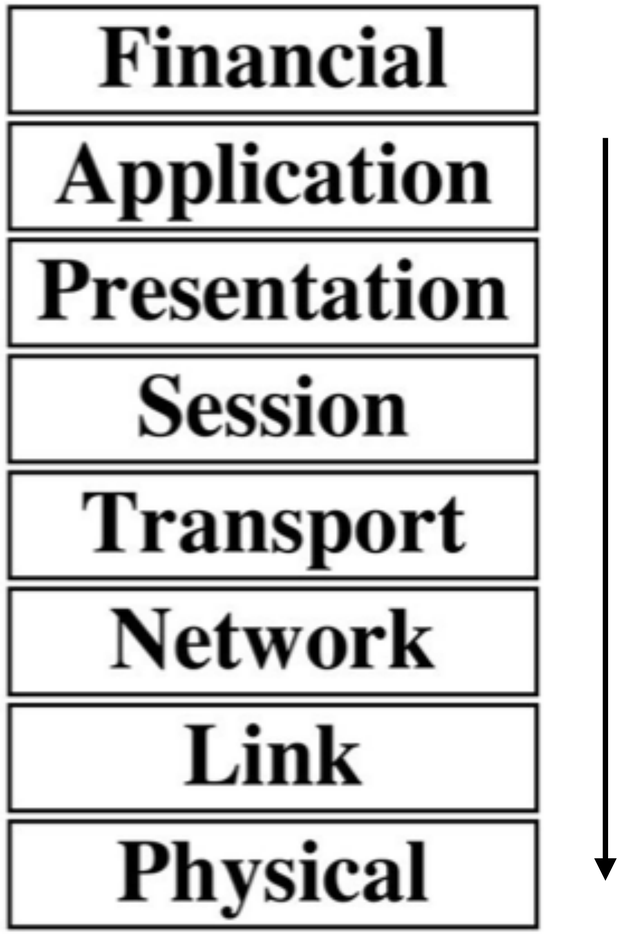
**Department of Computer Science**
**Stevens Institute of Technology**

**Jan Schaumann**
jschauma@stevens.edu
https://stevens.netmeister.org/615/

# The OSI Stack

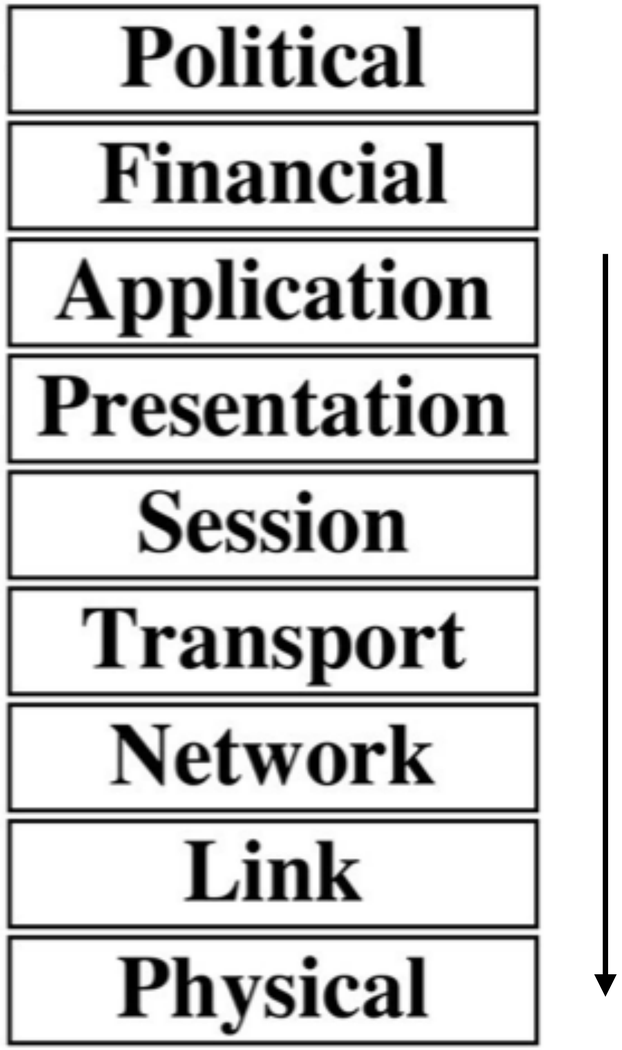


# The OSI Stack

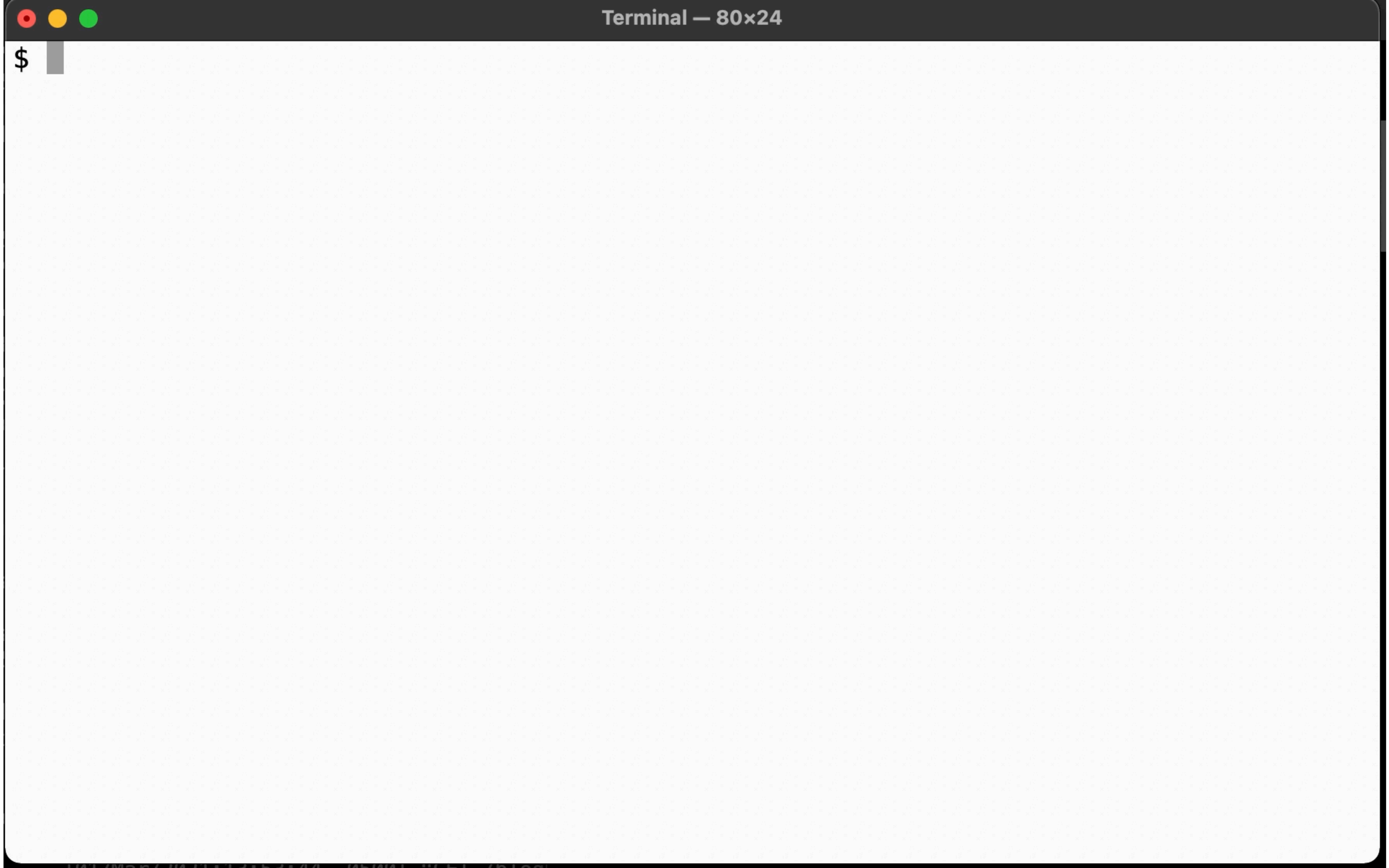


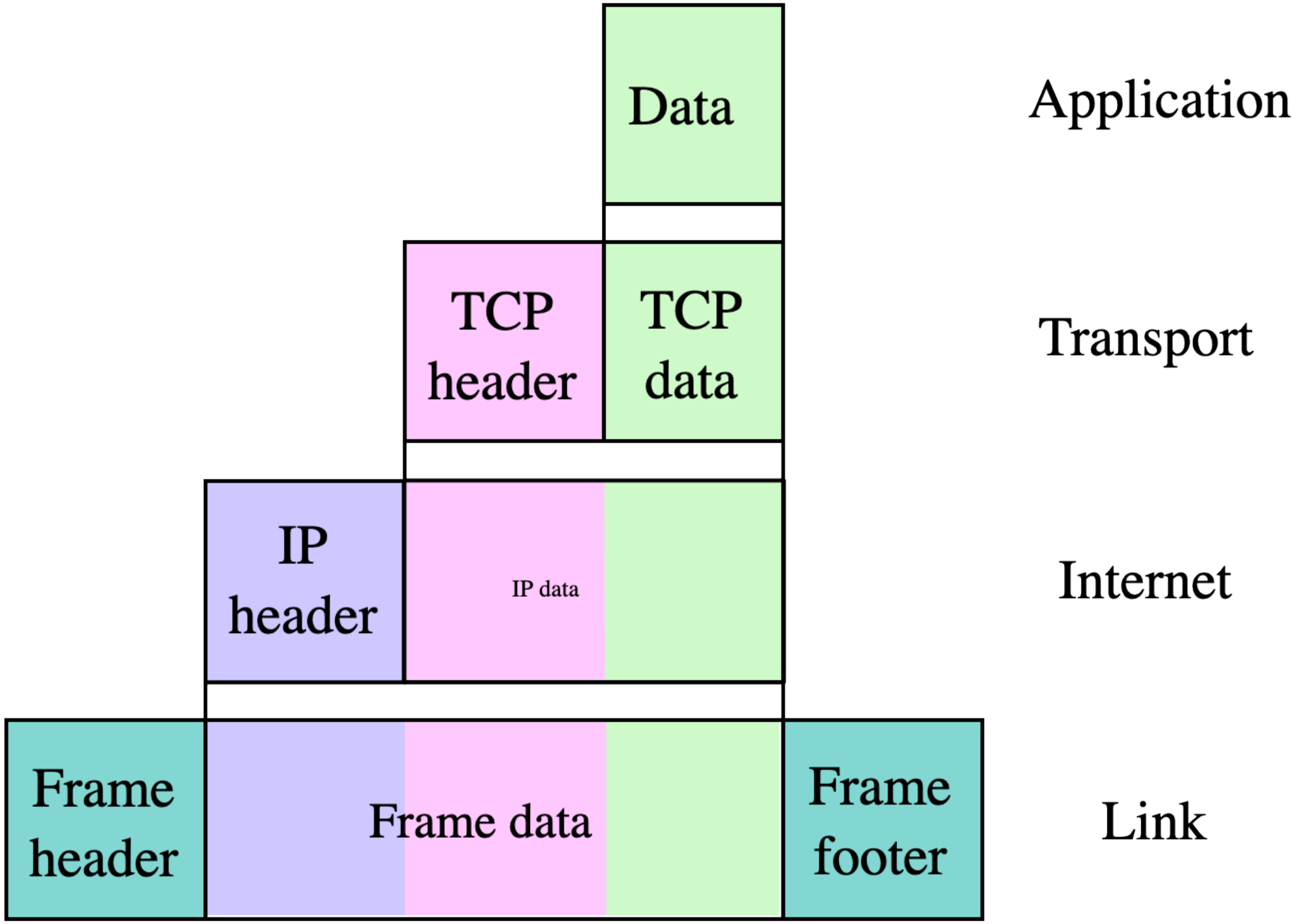

💰 pays for all of this

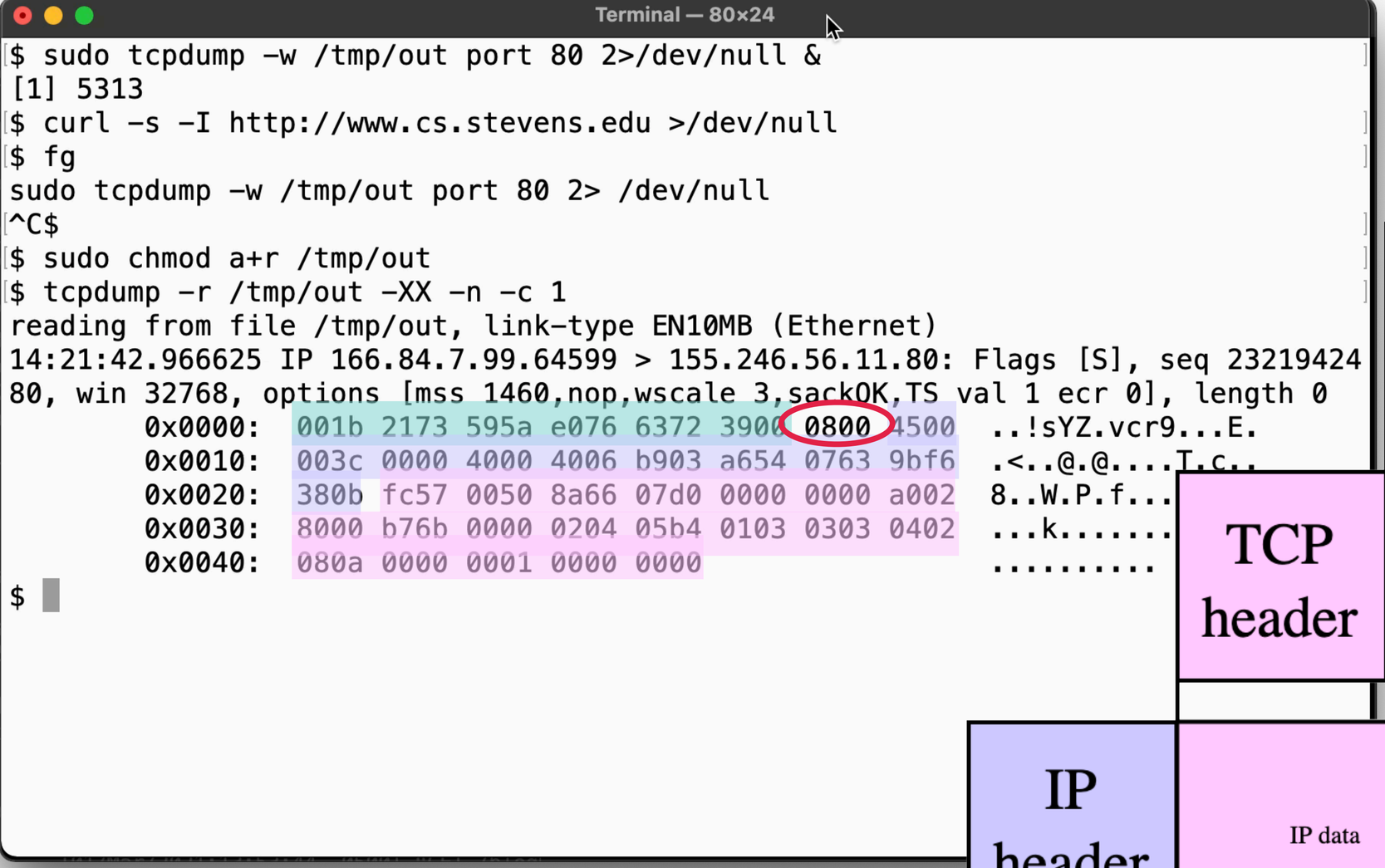
# The OSI Stack

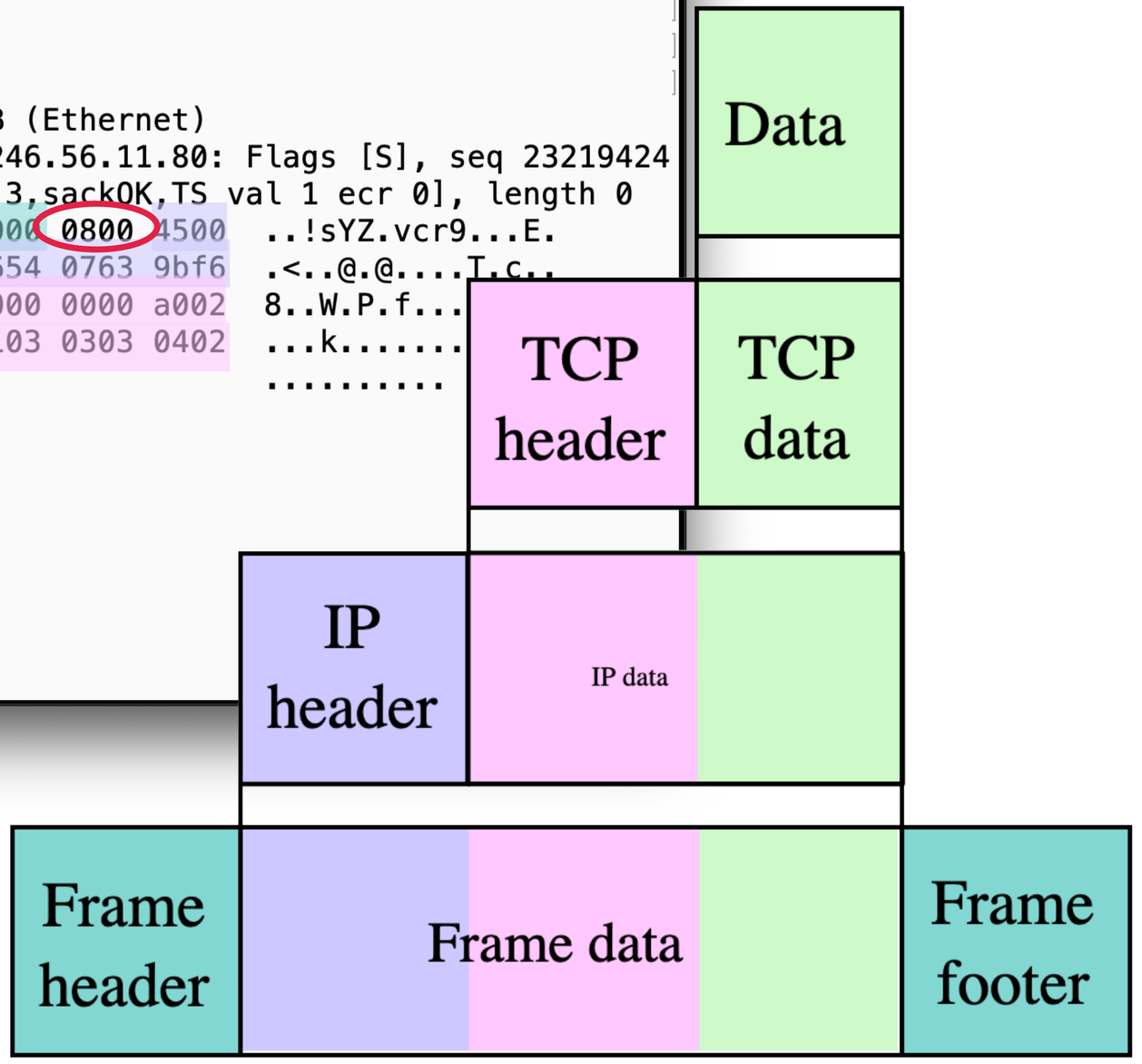



💰 pays for all of this


Terminal — 80×24
$


Data
Application
TCP header
TCP data
Transport
IP header
IP data
Internet
Frame header
Frame data
Frame footer
Link



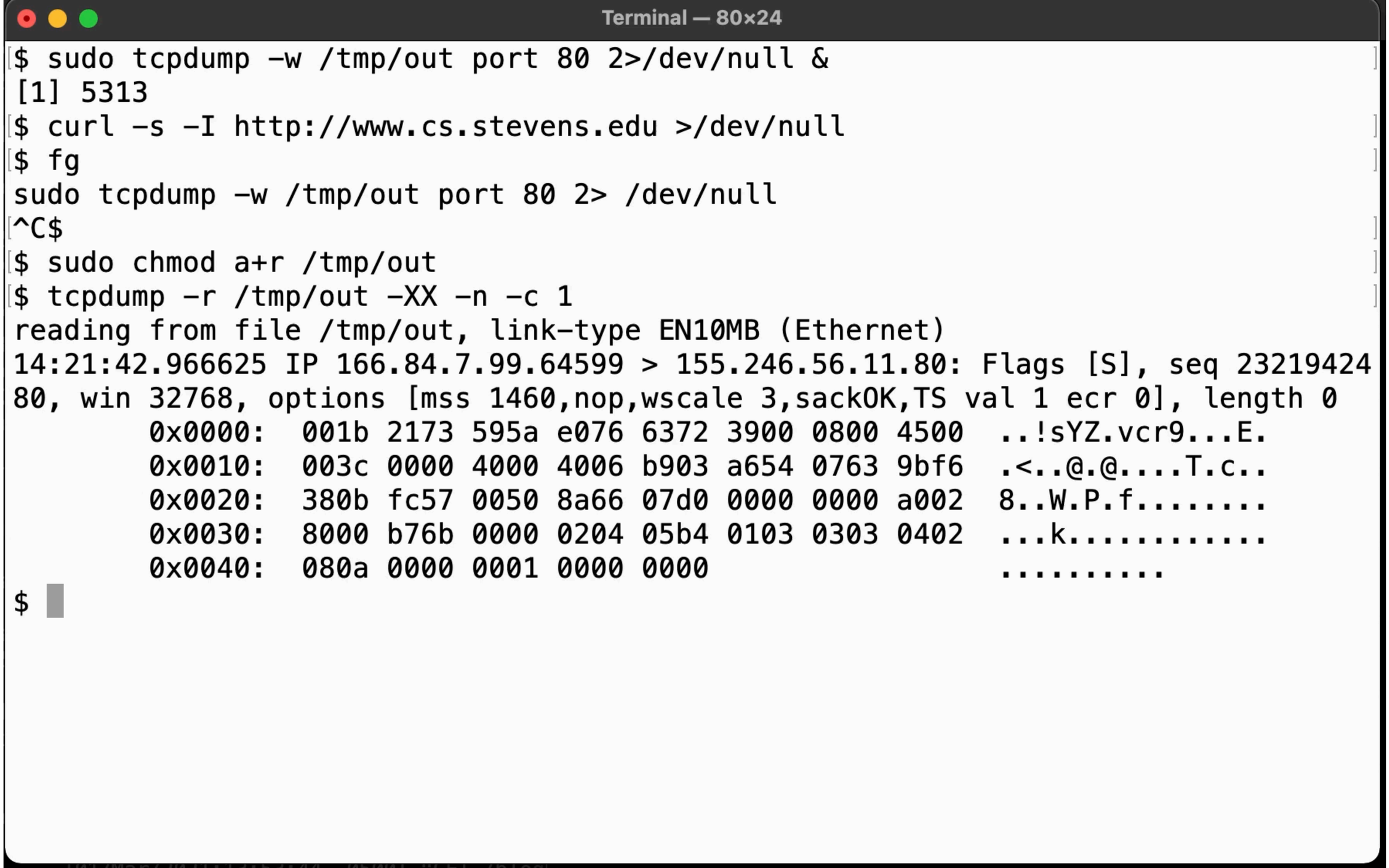



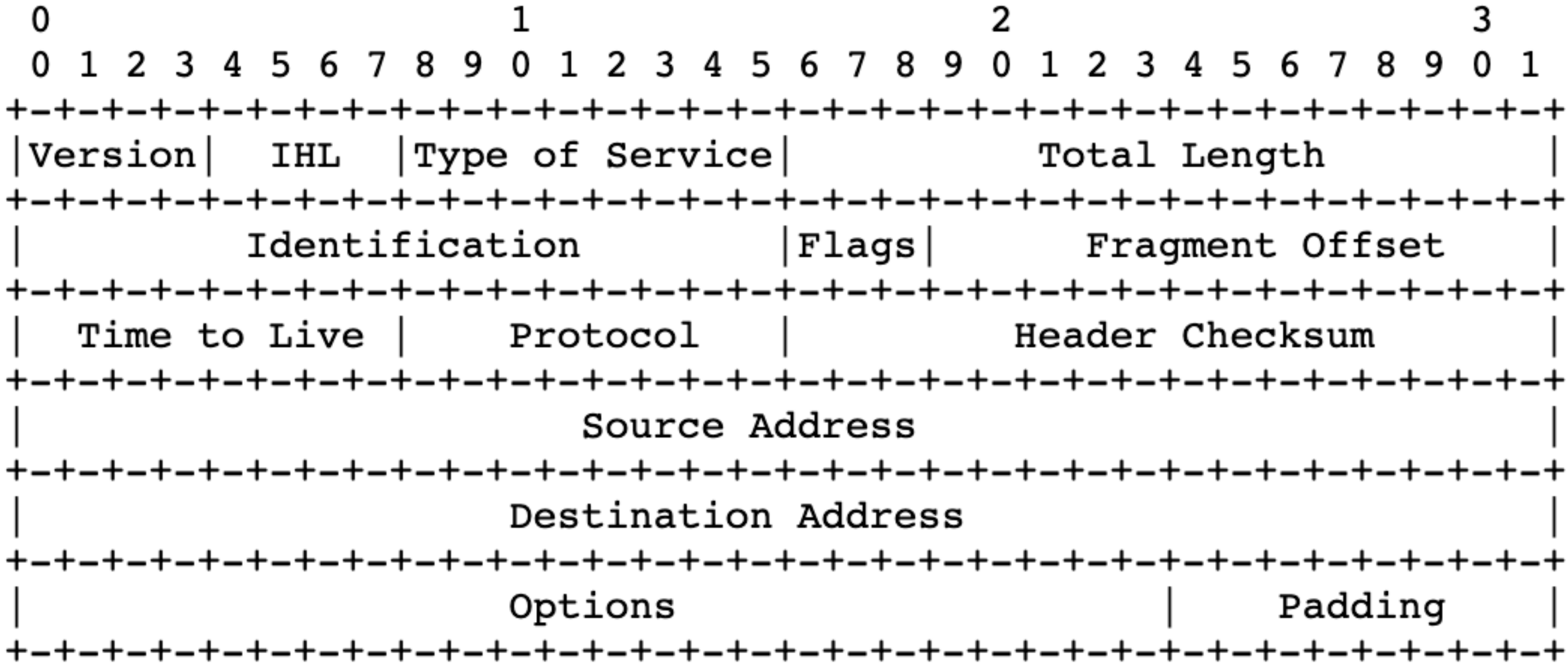

Application

Transport

Internet

Link


Terminal — 80×24
$ sudo tcpdump -w /tmp/out port 80 2>/dev/null &
[1] 5313
$ curl -s -I http://www.cs.stevens.edu >/dev/null
$ fg
sudo tcpdump -w /tmp/out port 80 2> /dev/null
^C$
$ sudo chmod a+r /tmp/out
$ tcpdump -r /tmp/out -XX -n -c 1
reading from file /tmp/out, link-type EN10MB (Ethernet)
14:21:42.966625 IP 166.84.7.99.64599 > 155.246.56.11.80: Flags [S], seq 23219424
80, win 32768, options [mss 1460,nop,wscale 3,sackOK,TS val 1 ecr 0], length 0
0x0000: 001b 2173 595a e076 6372 3900 0800 4500 ..!sYZ.vcr9...E.
0x0010: 003c 0000 4000 4006 b903 a654 0763 9bf6 .<..@.@....T.c..
0x0020: 380b fc57 0050 8a66 07d0 0000 0000 a002 8..W.P.f........
0x0030: 8000 b76b 0000 0204 05b4 0103 0303 0402 ...k............
0x0040: 080a 0000 0001 0000 0000 ..........
$

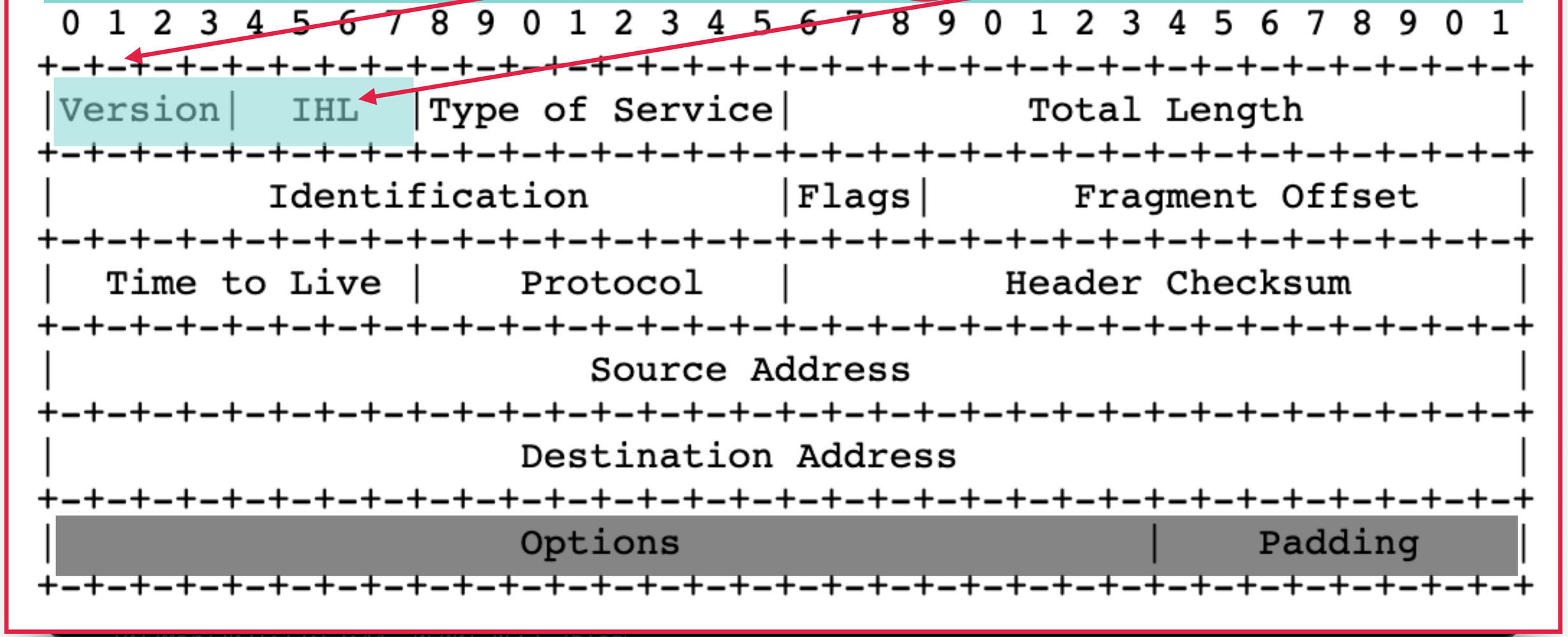



https://tools.ietf.org/html/rfc791

Terminal — 80×24

```
0x0000:  001b 2173 595a e076 6372 3900 0800 4500  ..!sYZ.vcr9...E.
0x0010:  003c 0000 4000 4006 b903 a654 0763 9bf6  .<..@.@....T.c..
0x0020:  380b fc57 0050 8a66 07d0 0000 0000 a002  8..W.P.f........
0x0030:  8000 b76b 0000 0204 05b4 0103 0303 0402  ...k............
0x0040:  080a 0000 0001 0000 0000                 ..........
```

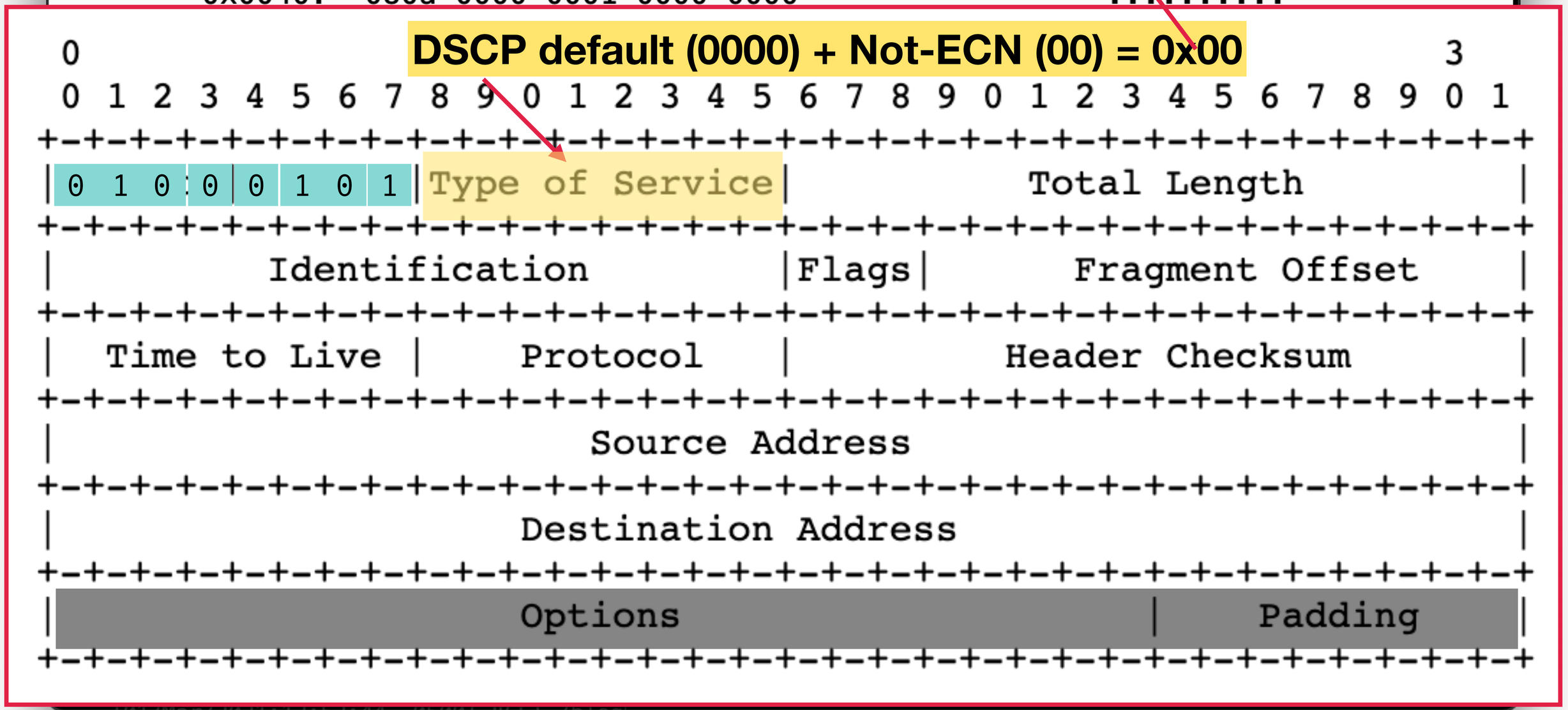
**Version 4 (0100) + Header Length 20 bytes = 5 (0101) * 32 = 01000101 = 0x45**



Terminal — 80×24

```
0x0000:  001b 2173 595a e076 6372 3900 0800 4500  ..!sYZ.vcr9...E.
0x0010:  003c 0000 4000 4006 b903 a654 0763 9bf6  .<..@.@....T.c..
0x0020:  380b fc57 0050 8a66 07d0 0000 0000 a002  8..W.P.f........
0x0030:  8000 b76b 0000 0204 05b4 0103 0303 0402  ...k............
0x0040:  080a 0000 0001 0000 0000                 ..........
```

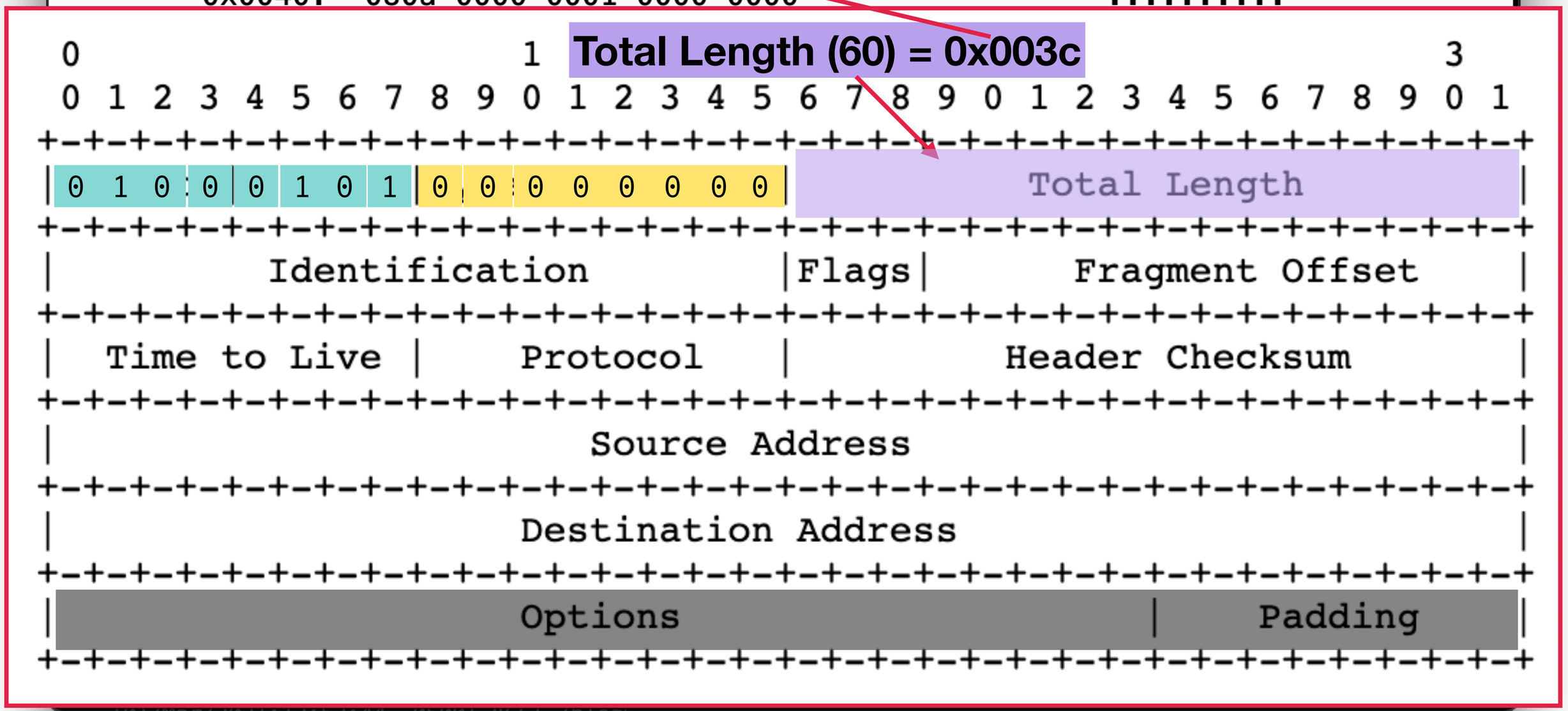
**DSCP default (0000) + Not-ECN (00) = 0x00**



Terminal — 80×24

```
0x0000:  001b 2173 595a e076 6372 3900 0800 4500  ..!sYZ.vcr9...E.
0x0010:  003c 0000 4000 4006 b903 a654 0763 9bf6  .<..@.@....T.c..
0x0020:  380b fc57 0050 8a66 07d0 0000 0000 a002  8..W.P.f........
0x0030:  8000 b76b 0000 0204 05b4 0103 0303 0402  ...k............
0x0040:  080a 0000 0001 0000 0000                 ..........
```

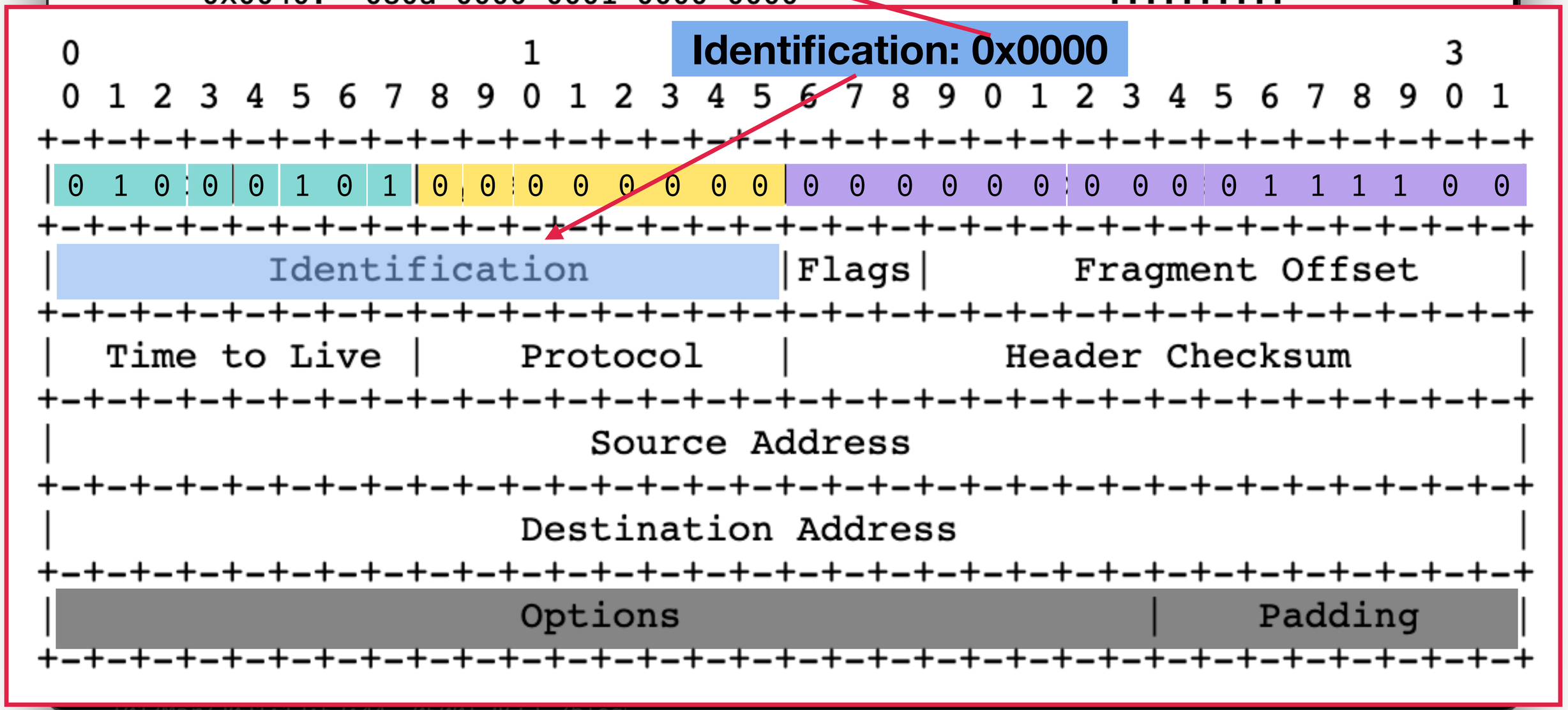
**Total Length (60) = 0x003c**



Terminal — 80×24

```
0x0000:  001b 2173 595a e076 6372 3900 0800 4500  ..!sYZ.vcr9...E.
0x0010:  003c 0000 4000 4006 b903 a654 0763 9bf6  .<..@.@....T.c..
0x0020:  380b fc57 0050 8a66 07d0 0000 0000 a002  8..W.P.f........
0x0030:  8000 b76b 0000 0204 05b4 0103 0303 0402  ...k............
0x0040:  080a 0000 0001 0000 0000                 ..........
```

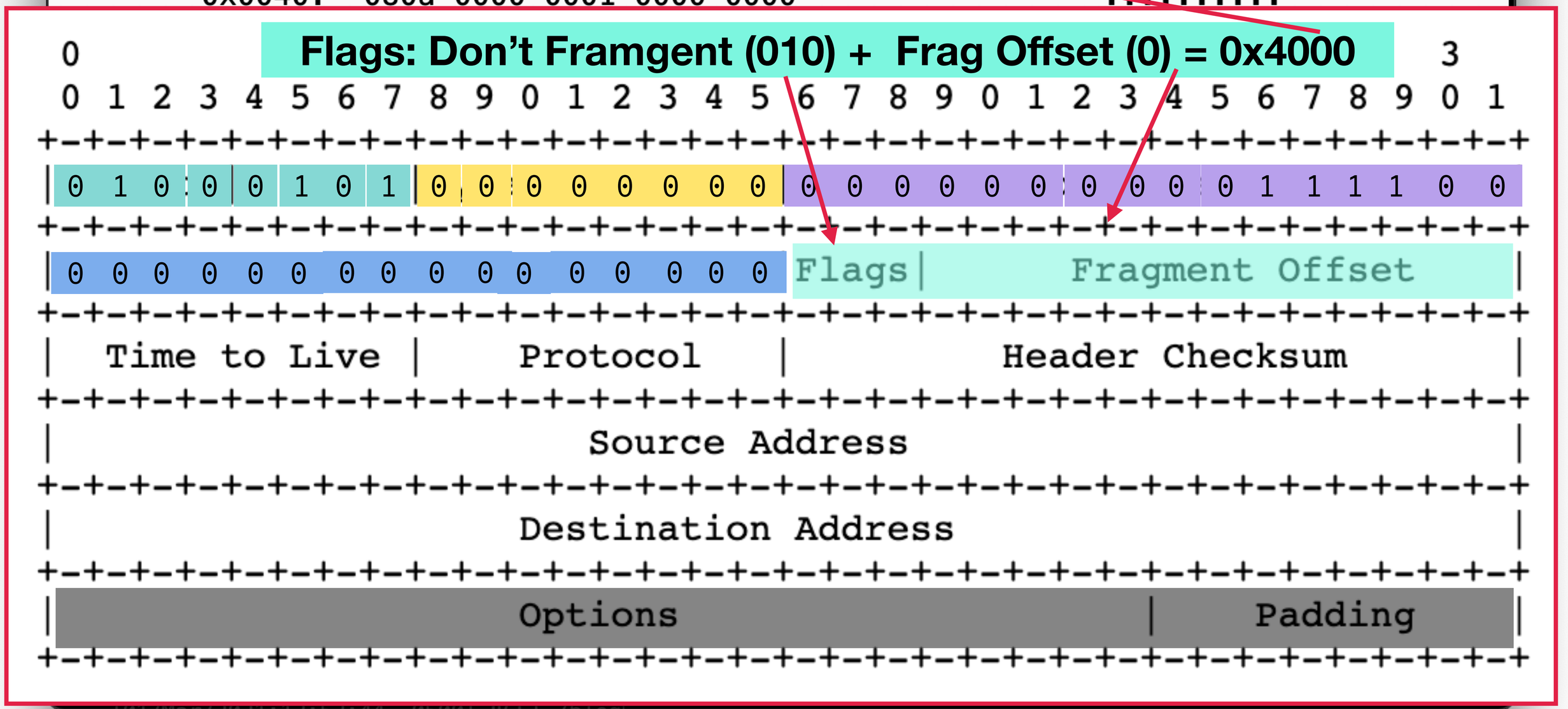
**Identification: 0x0000**



Terminal — 80×24

```
0x0000:  001b 2173 595a e076 6372 3900 0800 4500  ..!sYZ.vcr9...E.
0x0010:  003c 0000 4000 4006 b903 a654 0763 9bf6  .<..@.@....T.c..
0x0020:  380b fc57 0050 8a66 07d0 0000 0000 a002  8..W.P.f........
0x0030:  8000 b76b 0000 0204 05b4 0103 0303 0402  ...k............
0x0040:  080a 0000 0001 0000 0000                 ..........
```

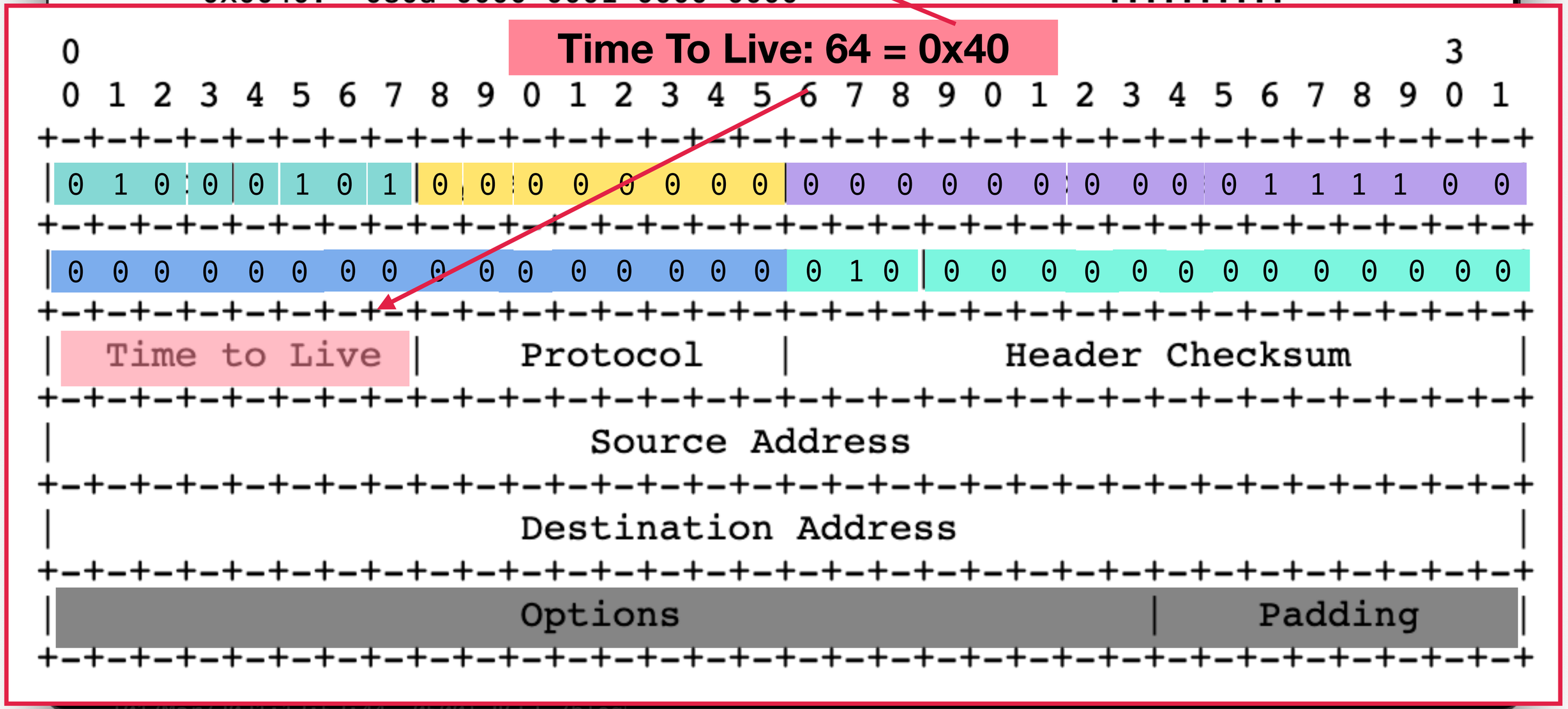
**Flags: Don't Framgent (010) + Frag Offset (0) = 0x4000**

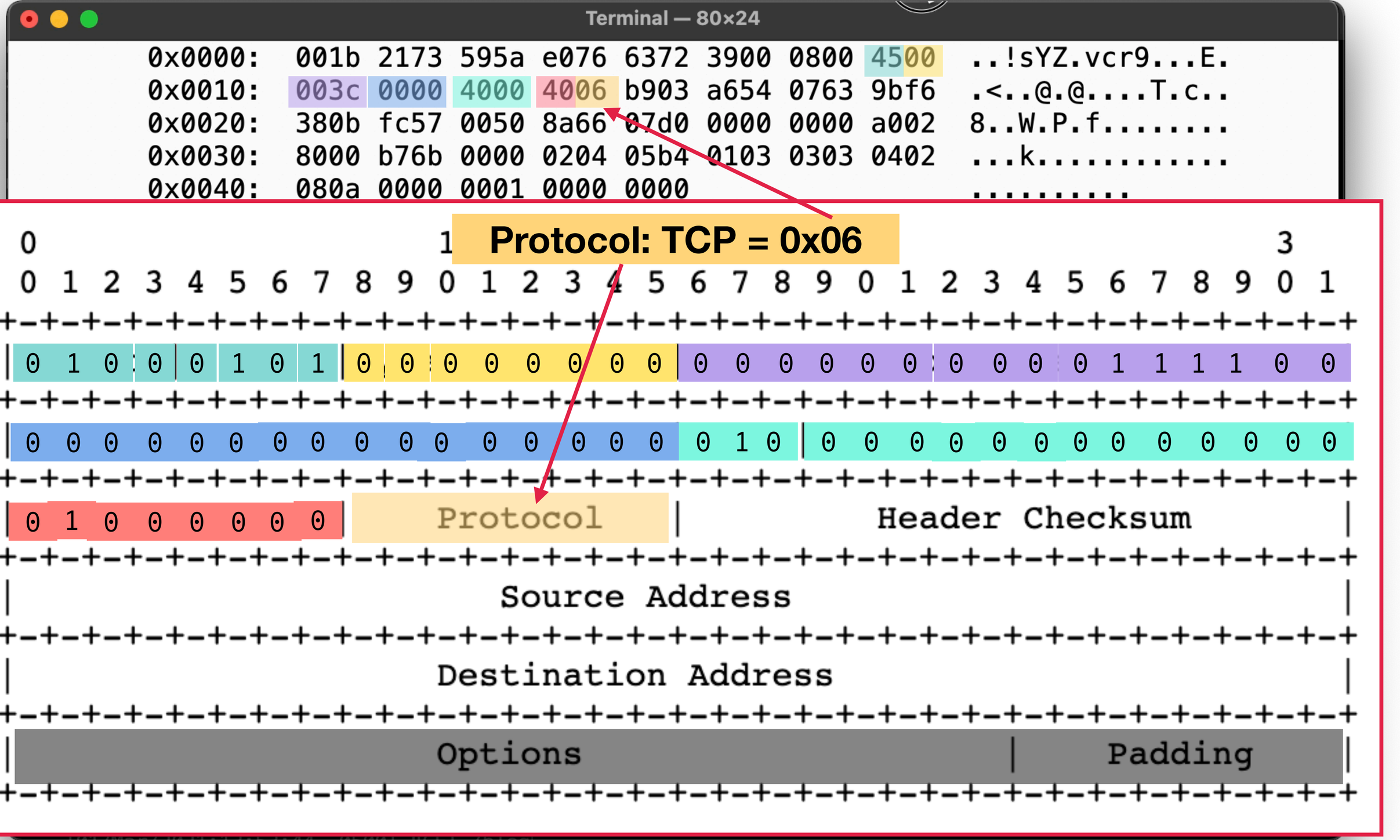


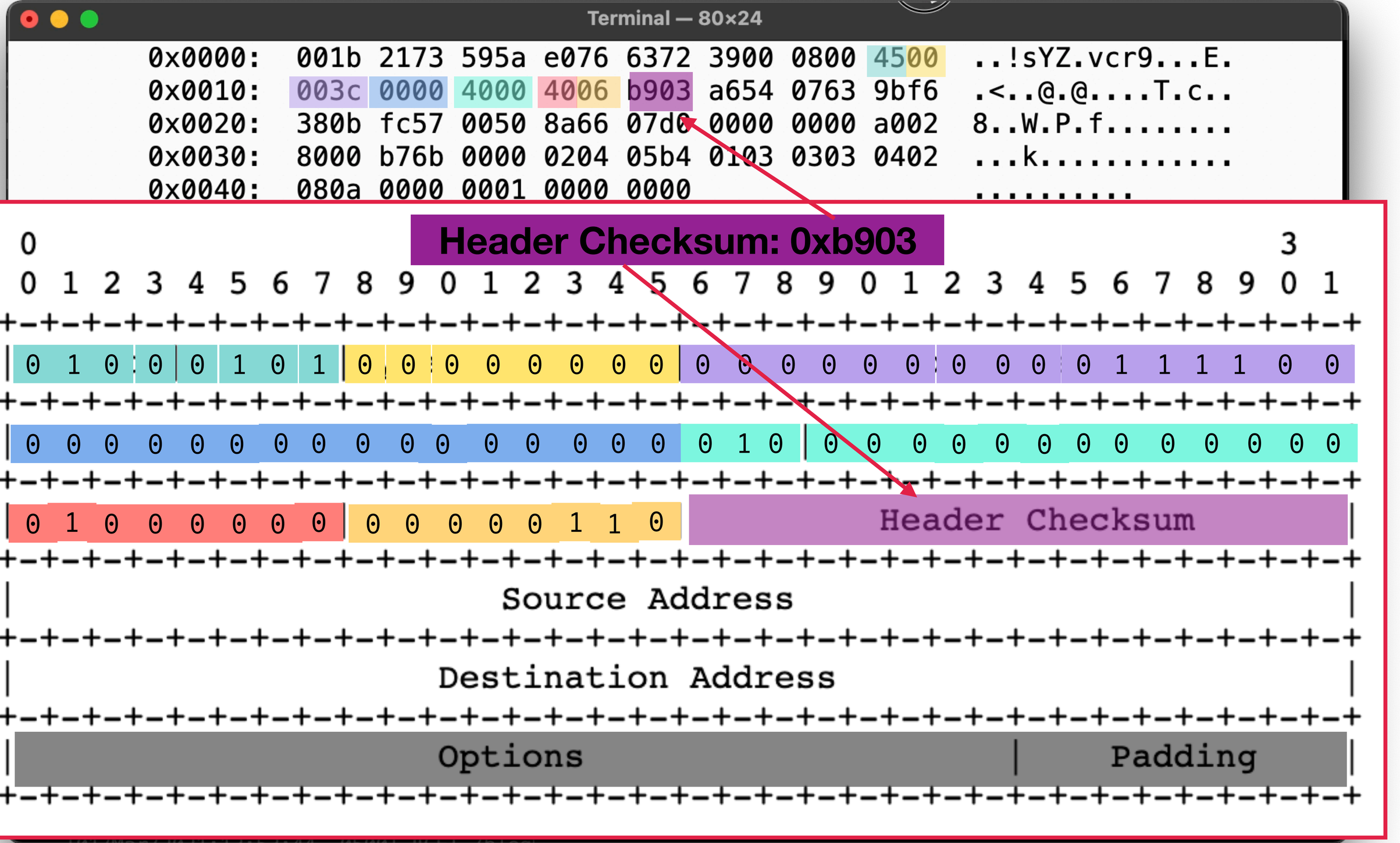
Terminal — 80×24

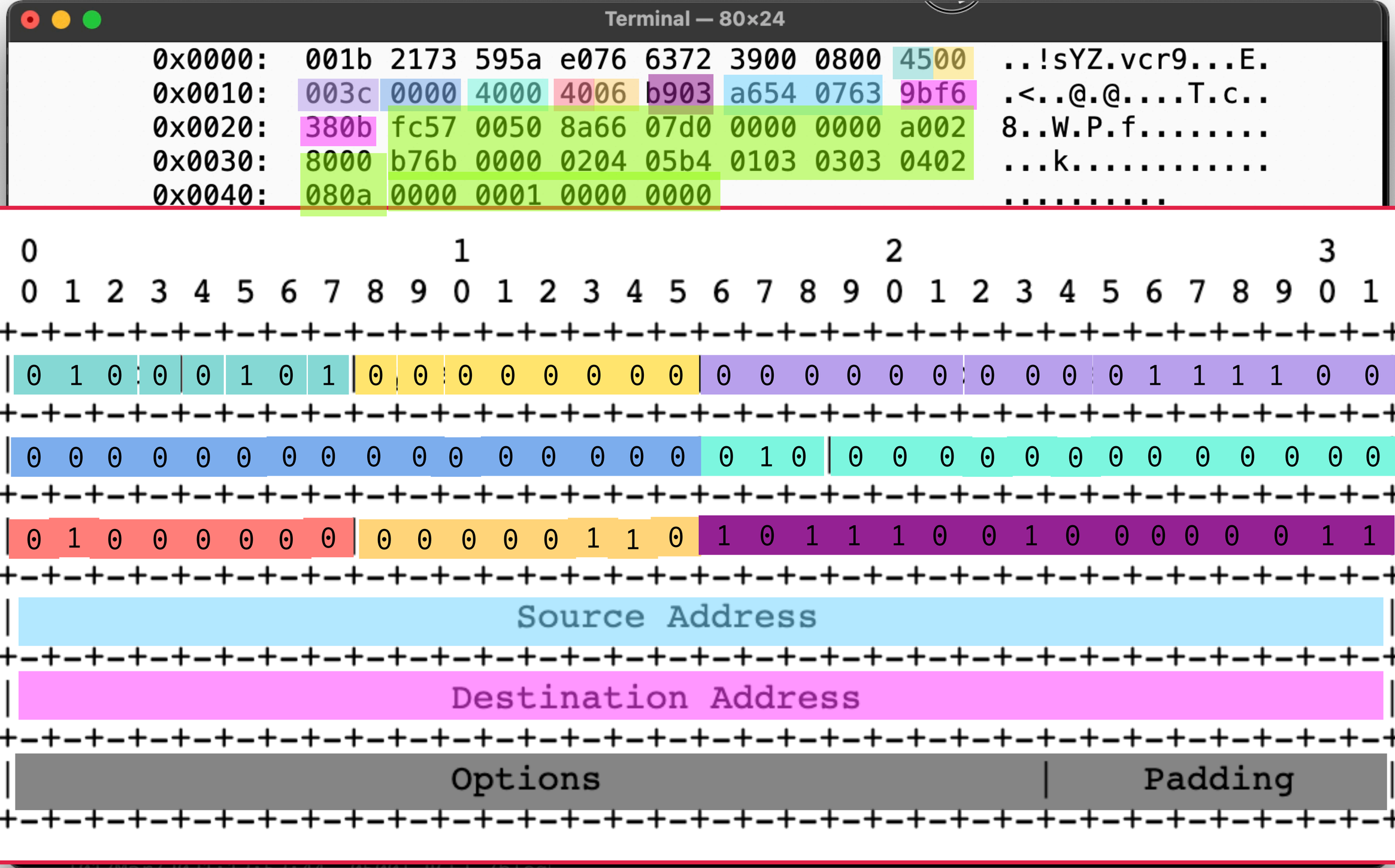
```
0x0000:  001b 2173 595a e076 6372 3900 0800 4500  ..!sYZ.vcr9...E.
0x0010:  003c 0000 4000 4006 b903 a654 0763 9bf6  .<..@.@....T.c..
0x0020:  380b fc57 0050 8a66 07d0 0000 0000 a002  8..W.P.f........
0x0030:  8000 b76b 0000 0204 05b4 0103 0303 0402  ...k............
0x0040:  080a 0000 0001 0000 0000                 ..........
```

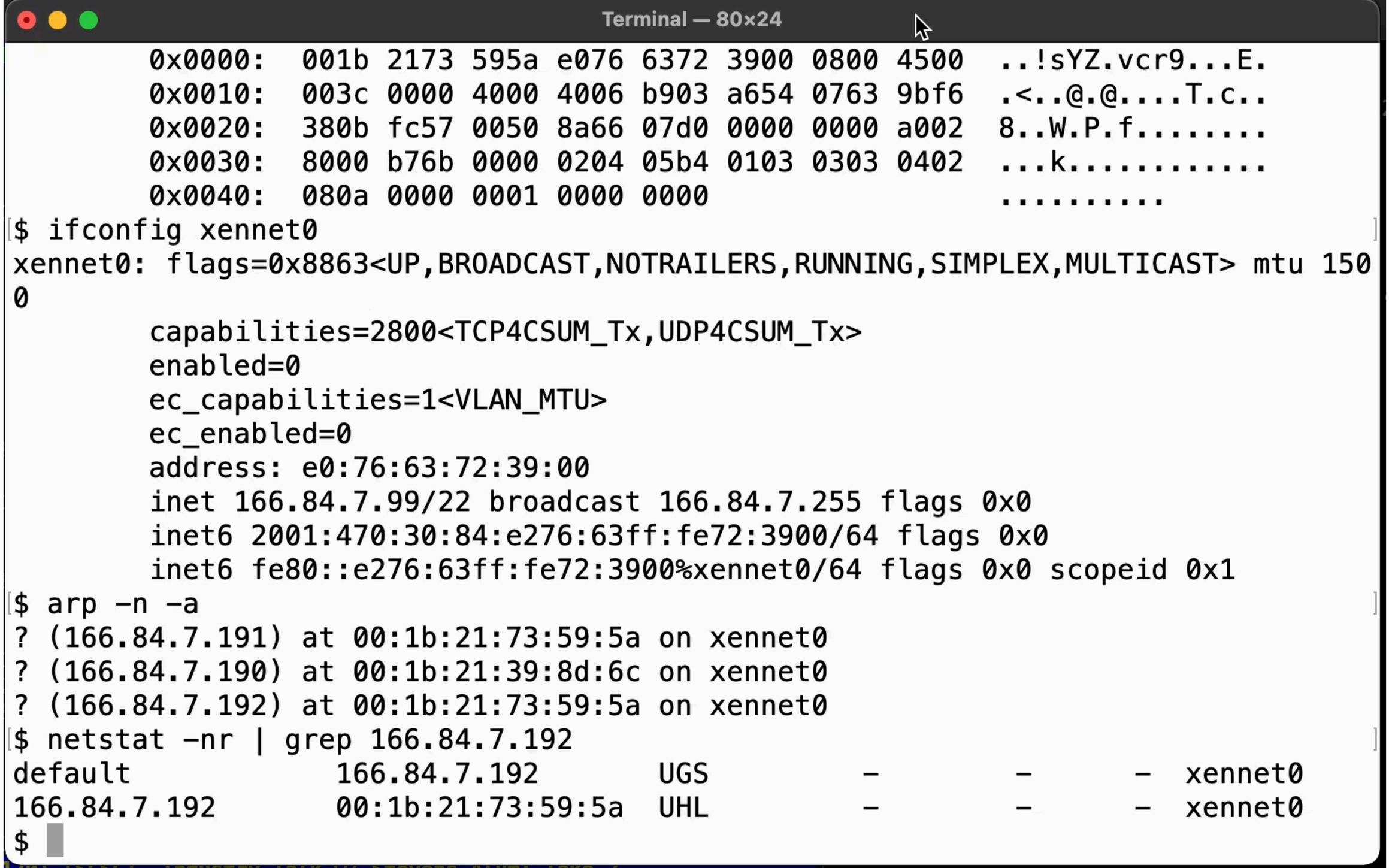
**Time To Live: 64 = 0x40**

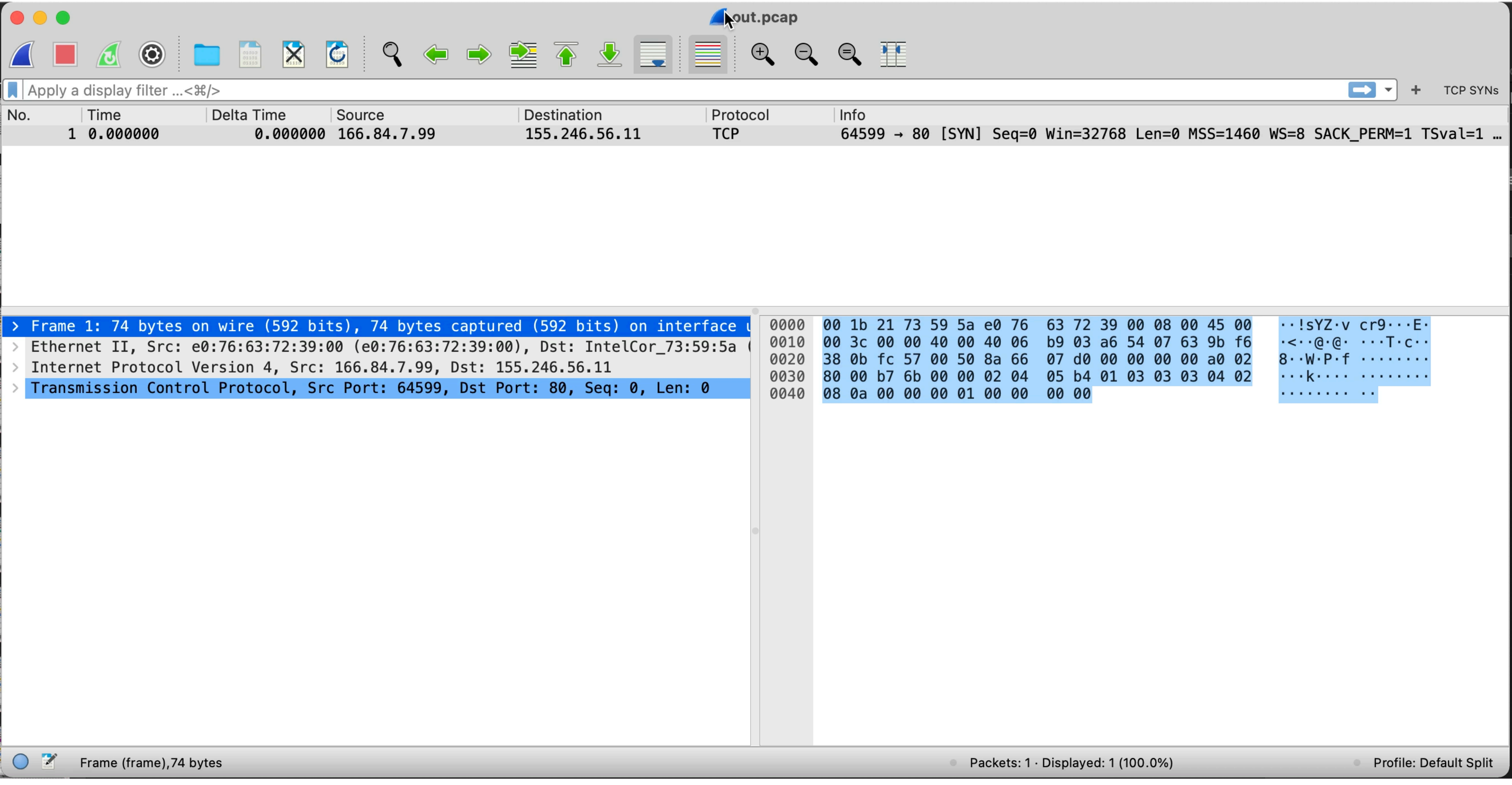



Terminal — 80×24
0x0000: 001b 2173 595a e076 6372 3900 0800 4500 ..!sYZ.vcr9...E.
0x0010: 003c 0000 4000 4006 b903 a654 0763 9bf6 .<..@.@....T.c..
0x0020: 380b fc57 0050 8a66 07d0 0000 0000 a002 8..W.P.f........
0x0030: 8000 b76b 0000 0204 05b4 0103 0303 0402 ...k............
0x0040: 080a 0000 0001 0000 0000 ..........
Protocol: TCP = 0x06
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 1 0 0 0 0 0 0
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding


Terminal — 80×24
0x0000: 001b 2173 595a e076 6372 3900 0800 4500 ..!sYZ.vcr9...E.
0x0010: 003c 0000 4000 4006 b903 a654 0763 9bf6 .<..@.@....T.c..
0x0020: 380b fc57 0050 8a66 07d0 0000 0000 a002 8..W.P.f........
0x0030: 8000 b76b 0000 0204 05b4 0103 0303 0402 ...k............
0x0040: 080a 0000 0001 0000 0000 ..........
Header Checksum: 0xb903
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0
0 1 0 0 0 0 0 0 0 0 0 0 0 1 1 0 Header Checksum
Source Address
Destination Address
Options Padding


Terminal — 80×24
0x0000: 001b 2173 595a e076 6372 3900 0800 4500 ..!sYZ.vcr9...E.
0x0010: 003c 0000 4000 4006 b903 a654 0763 9bf6 .<..@.@....T.c..
0x0020: 380b fc57 0050 8a66 07d0 0000 0000 a002 8..W.P.f........
0x0030: 8000 b76b 0000 0204 05b4 0103 0303 0402 ...k............
0x0040: 080a 0000 0001 0000 0000 ..........
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 1 1 0 0 1 0 0 0 0 0 0 1 1
Source Address
Destination Address
Options
Padding


Terminal — 80×24
0x0000: 001b 2173 595a e076 6372 3900 0800 4500 ..!sYZ.vcr9...E.
0x0010: 003c 0000 4000 4006 b903 a654 0763 9bf6 .<..@.@....T.c..
0x0020: 380b fc57 0050 8a66 07d0 0000 0000 a002 8..W.P.f........
0x0030: 8000 b76b 0000 0204 05b4 0103 0303 0402 ...k............
0x0040: 080a 0000 0001 0000 0000 ..........
$ ifconfig xennet0
xennet0: flags=0x8863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST> mtu 150
0
capabilities=2800<TCP4CSUM_Tx,UDP4CSUM_Tx>
enabled=0
ec_capabilities=1<VLAN_MTU>
ec_enabled=0
address: e0:76:63:72:39:00
inet 166.84.7.99/22 broadcast 166.84.7.255 flags 0x0
inet6 2001:470:30:84:e276:63ff:fe72:3900/64 flags 0x0
inet6 fe80::e276:63ff:fe72:3900%xennet0/64 flags 0x0 scopeid 0x1
$ arp -n -a
? (166.84.7.191) at 00:1b:21:73:59:5a on xennet0
? (166.84.7.190) at 00:1b:21:39:8d:6c on xennet0
? (166.84.7.192) at 00:1b:21:73:59:5a on xennet0
$ netstat -nr | grep 166.84.7.192
default 166.84.7.192 UGS - - - xennet0
166.84.7.192 00:1b:21:73:59:5a UHL - - - xennet0
$


out.pcap
Apply a display filter ...<⌘/>
TCP SYNs
No. Time Delta Time Source Destination Protocol Info
1 0.000000 0.000000 166.84.7.99 155.246.56.11 TCP 64599 → 80 [SYN] Seq=0 Win=32768 Len=0 MSS=1460 WS=8 SACK_PERM=1 TSval=1 …
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface
Ethernet II, Src: e0:76:63:72:39:00 (e0:76:63:72:39:00), Dst: IntelCor_73:59:5a
Internet Protocol Version 4, Src: 166.84.7.99, Dst: 155.246.56.11
Transmission Control Protocol, Src Port: 64599, Dst Port: 80, Seq: 0, Len: 0
0000 00 1b 21 73 59 5a e0 76 63 72 39 00 08 00 45 00 ··!sYZ·v cr9···E·
0010 00 3c 00 00 40 00 40 06 b9 03 a6 54 07 63 9b f6 ·<··@·@· ···T·c··
0020 38 0b fc 57 00 50 8a 66 07 d0 00 00 00 00 a0 02 8··W·P·f ····
0030 80 00 b7 6b 00 00 02 04 05 b4 01 03 03 03 04 02 ···k···· ····
0040 08 0a 00 00 00 01 00 00 00 00 ···· ··
Frame (frame),74 bytes
Packets: 1 · Displayed: 1 (100.0%)
Profile: Default Split

## Summary

- TCP/IP and OSI Layers: ✅
- RFCs and `tcpdump(8)` appear to align: ✅
- Wireshark does not appear to be magic: ✅

What's next?

- IPv4 subnetting
- IPv6
- Global Internet Administration (Part I)
- The Physical Internet

# Links

- Shell functions to convert IP addresses:

  https://www.netmeister.org/ip.sh

- OSI Model:

  https://en.wikipedia.org/wiki/OSI_model

  See also:

  https://twitter.com/jschauma/status/1231623662937223169

- IPv4 RFC791

  https://tools.ietf.org/html/rfc791