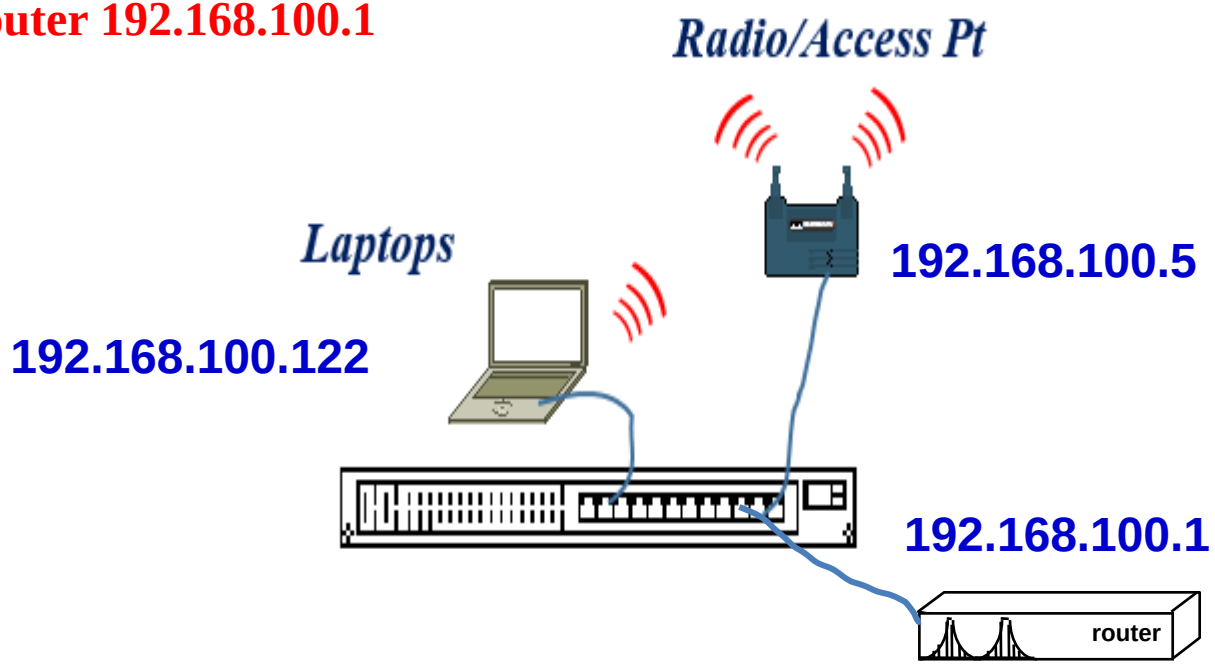
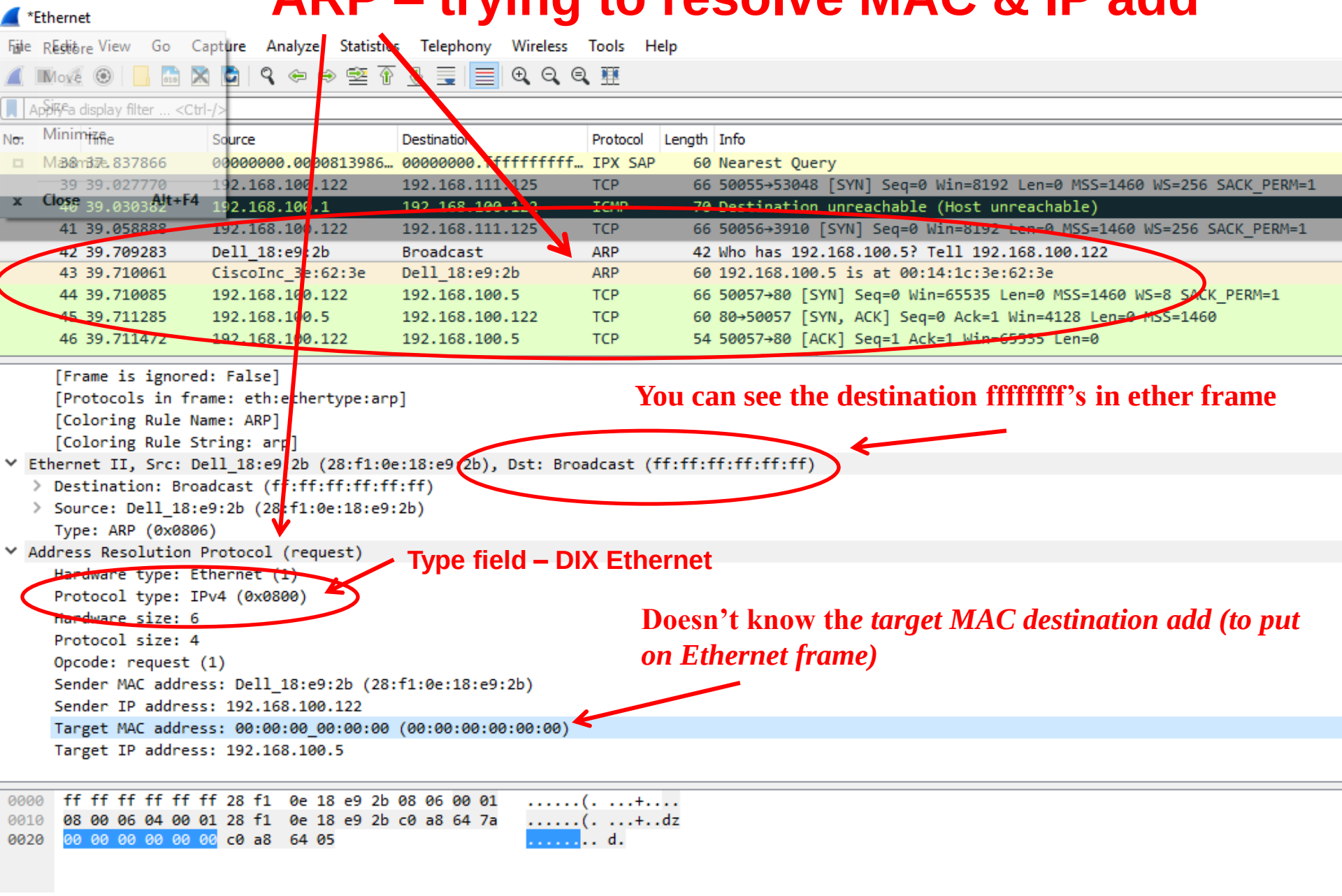
HTTP trace *(over Ethernet)*

1. I already started Wireshark session live capturing in background which will "see" all frames on Ethernet.
2. I am at browser of laptop (.122) entering IP add of 100.5 to HTTP into cisco router 192.168.100.1



*** The following pages are screen captures of Wireshark Traces of these devices**

ARP – trying to resolve MAC & IP add



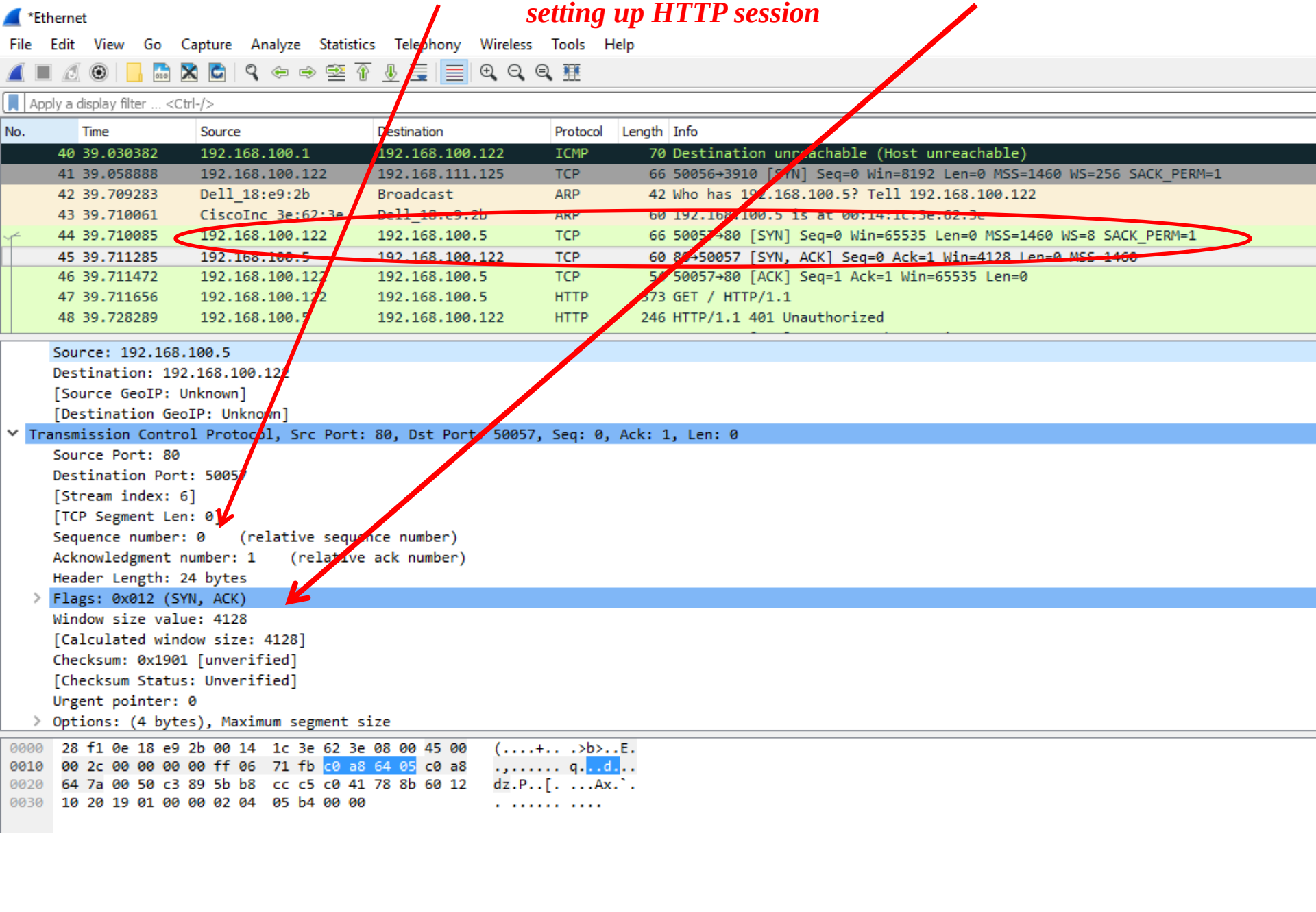
You can see the destination ffffffff's in ether frame

Type field – DIX Ethernet

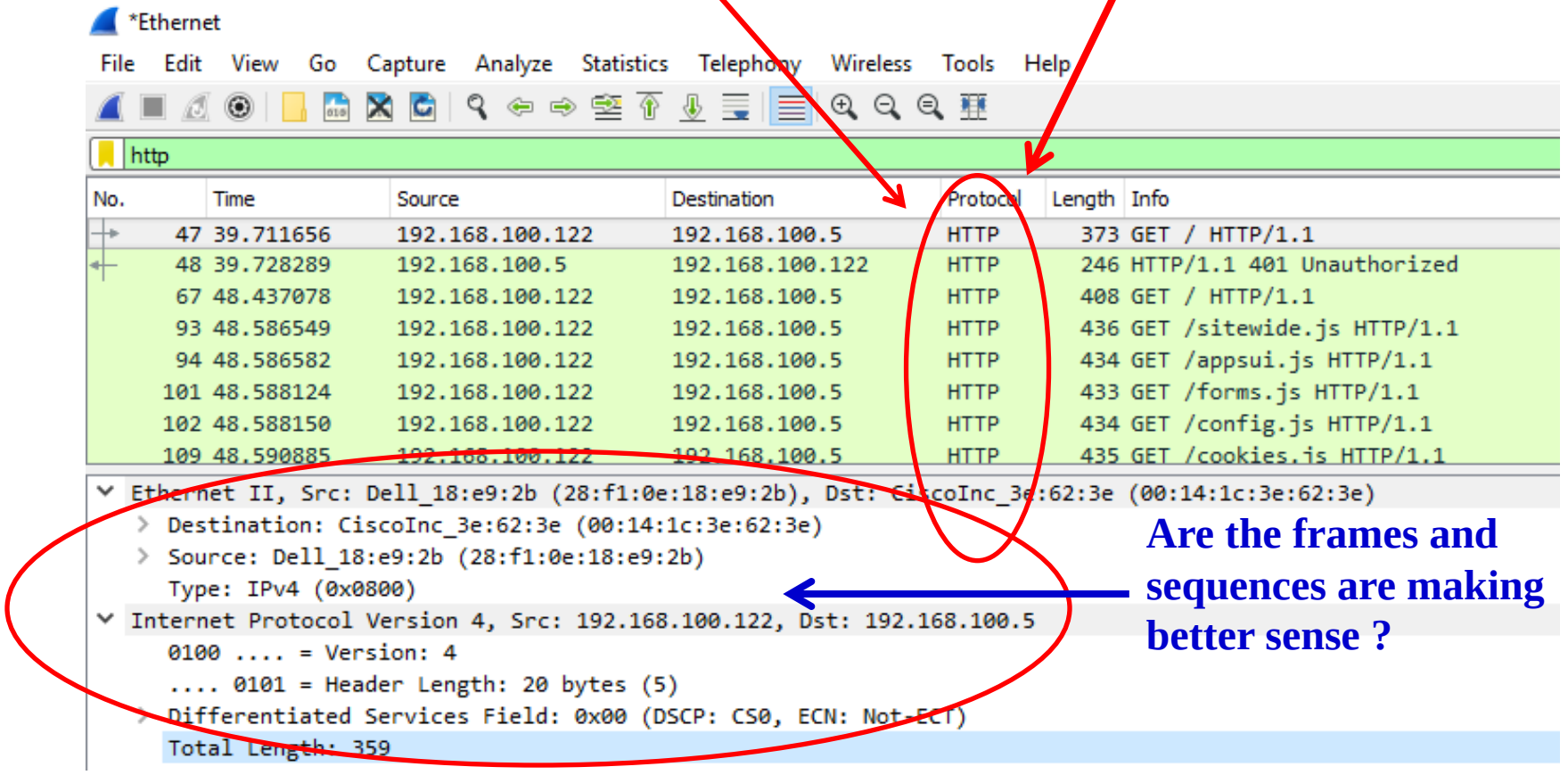
Doesn't know the *target MAC destination add (to put on Ethernet frame)*

TCP (initial sequence # - syn, ack)

setting up HTTP session

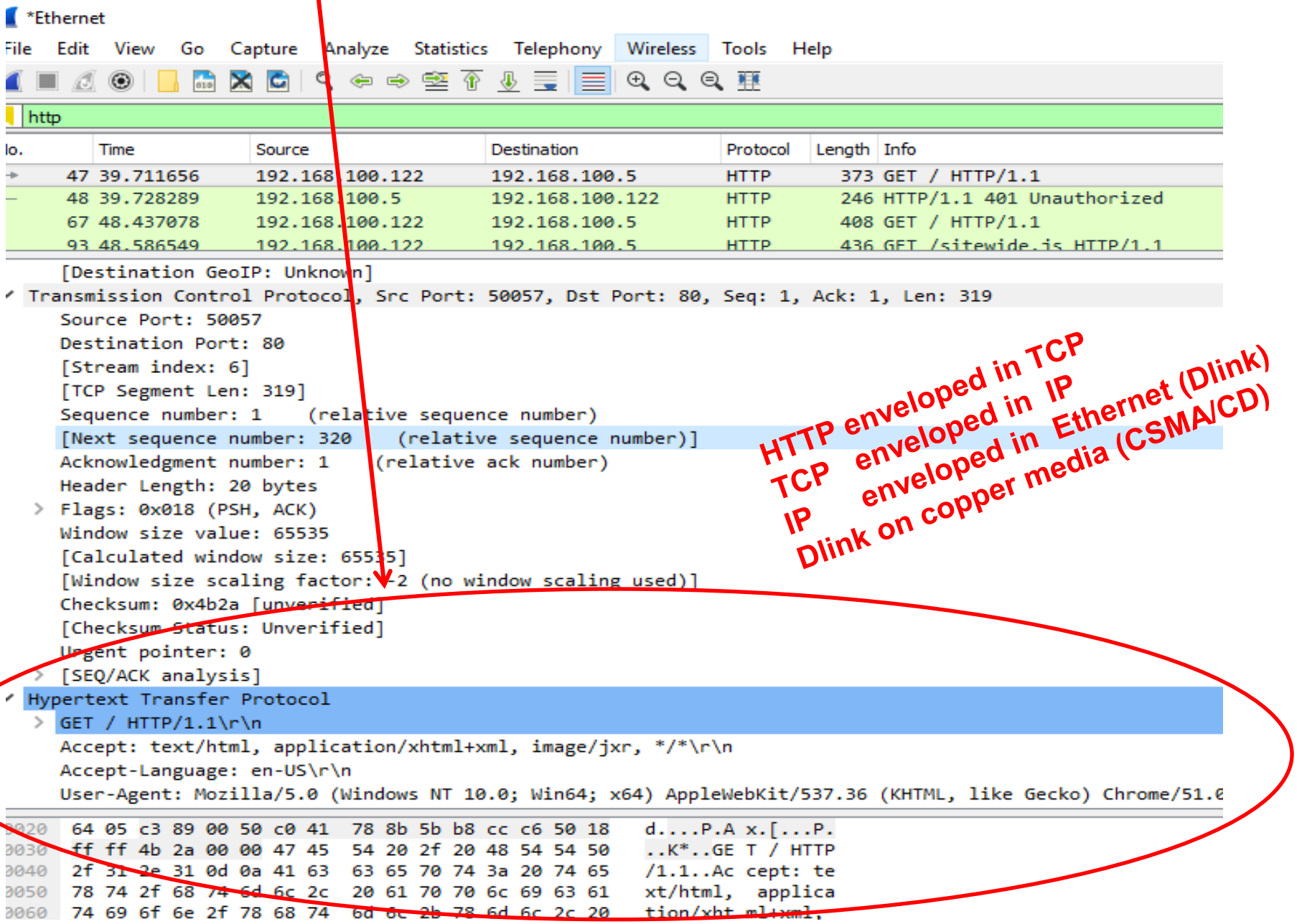


HTTP Protocol – Application Layer

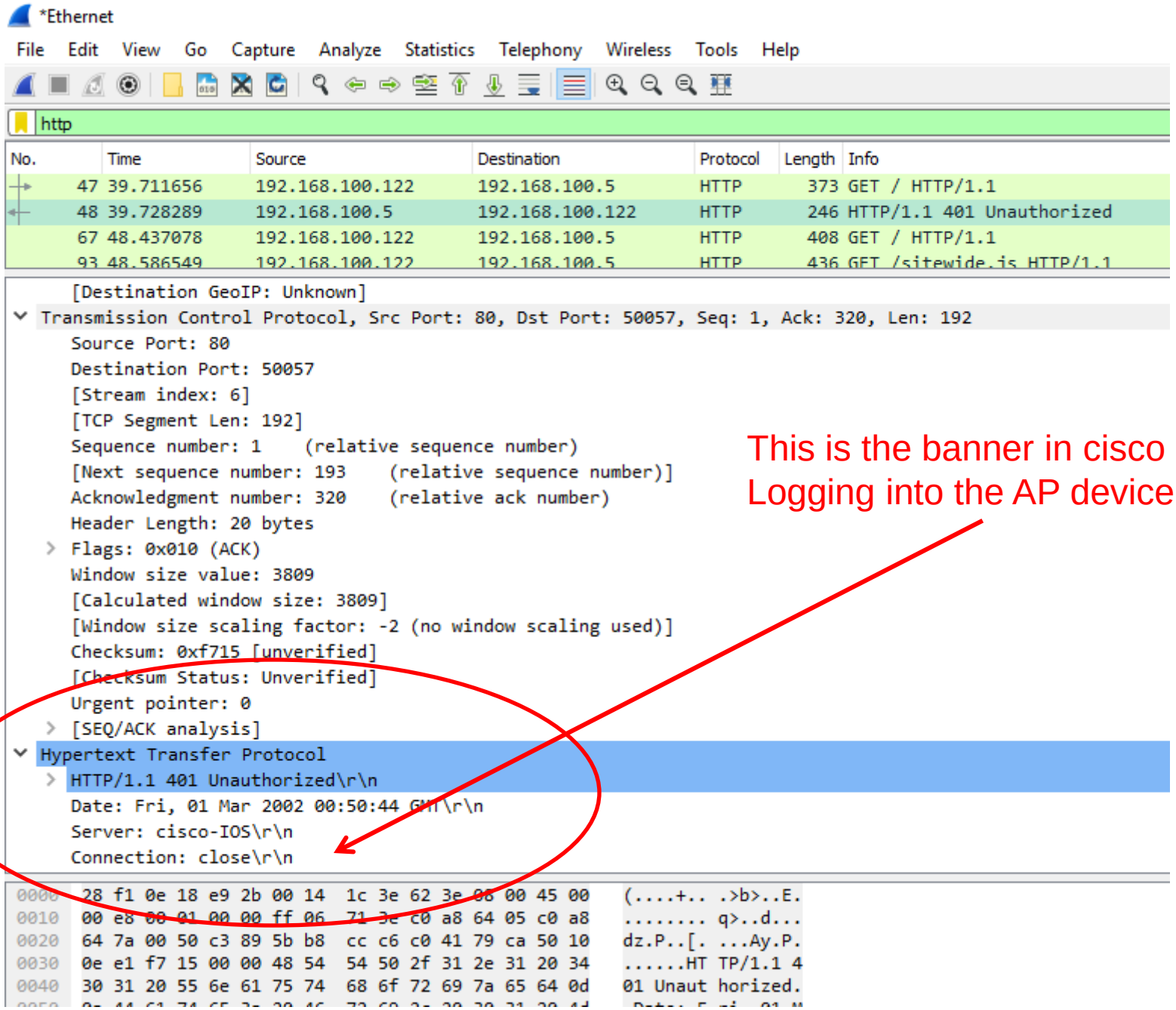


Are the frames and sequences are making better sense ?

HTTP Protocol – Application Layer



HTTP enveloped in TCP
TCP enveloped in IP
IP enveloped in Ethernet (Dlink)
Dlink on copper media (CSMA/CD)


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
47 39.711656 192.168.100.122 192.168.100.5 HTTP 373 GET / HTTP/1.1
48 39.728289 192.168.100.5 192.168.100.122 HTTP 246 HTTP/1.1 401 Unauthorized
67 48.437078 192.168.100.122 192.168.100.5 HTTP 408 GET / HTTP/1.1
93 48.586549 192.168.100.122 192.168.100.5 HTTP 436 GET /sitewide.js HTTP/1.1
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 80, Dst Port: 50057, Seq: 1, Ack: 320, Len: 192
Source Port: 80
Destination Port: 50057
[Stream index: 6]
[TCP Segment Len: 192]
Sequence number: 1 (relative sequence number)
[Next sequence number: 193 (relative sequence number)]
Acknowledgment number: 320 (relative ack number)
Header Length: 20 bytes
Flags: 0x010 (ACK)
Window size value: 3809
[Calculated window size: 3809]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0xf715 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
Hypertext Transfer Protocol
HTTP/1.1 401 Unauthorized\r\n
Date: Fri, 01 Mar 2002 00:50:44 GMT\r\n
Server: cisco-IOS\r\n
Connection: close\r\n
0000 28 f1 0e 18 e9 2b 00 14 1c 3e 62 3e 08 00 45 00 (....+.. .>b>..E.
0010 00 e8 00 01 00 00 ff 06 71 3e c0 a8 64 05 c0 a8 .... q>..d...
0020 64 7a 00 50 c3 89 5b b8 cc c6 c0 41 79 ca 50 10 dz.P..[. ...Ay.P.
0030 0e e1 f7 15 00 00 48 54 54 50 2f 31 2e 31 20 34 ......HT TP/1.1 4
0040 30 31 20 55 6e 61 75 74 68 6f 72 69 7a 65 64 0d 01 Unaut horized.
This is the banner in cisco as
Logging into the AP device