What are the information that can be viewed? What do these mean? Here are some basic guidelines to assist you in understanding what the data means. Captured data from packet analysis can be used either directly or indirectly as evidence against a certain cybercrime based on information gathered from analysis.

Some sources of information that are forensic material are:

Source IP Address: Retrieves information of the user, cross checking this physically would allow the identification of which device is on this address.

Destination IP Address: Shows which target address that the person is searching/sending data to.

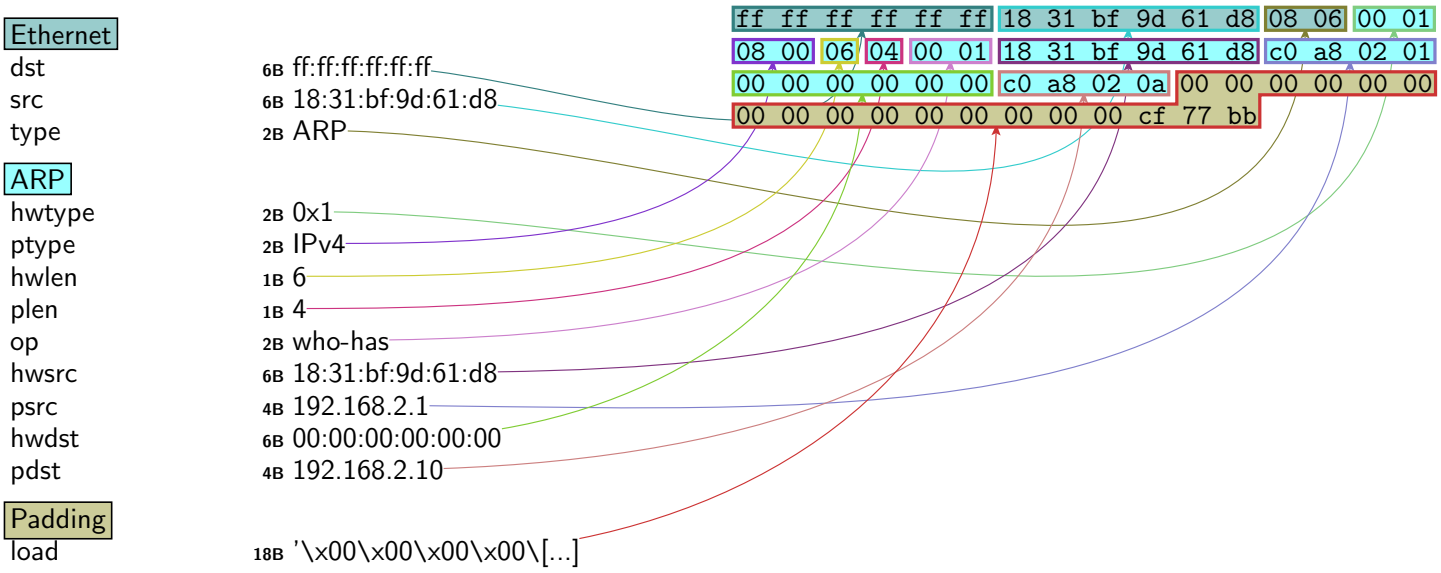
Port numbers: What kind of specific ports are being used and what type of malicious activity is done through open ports.

ICMP packets: Long ICMP packets shows that there might be some DoS(Denial of Service) attack.

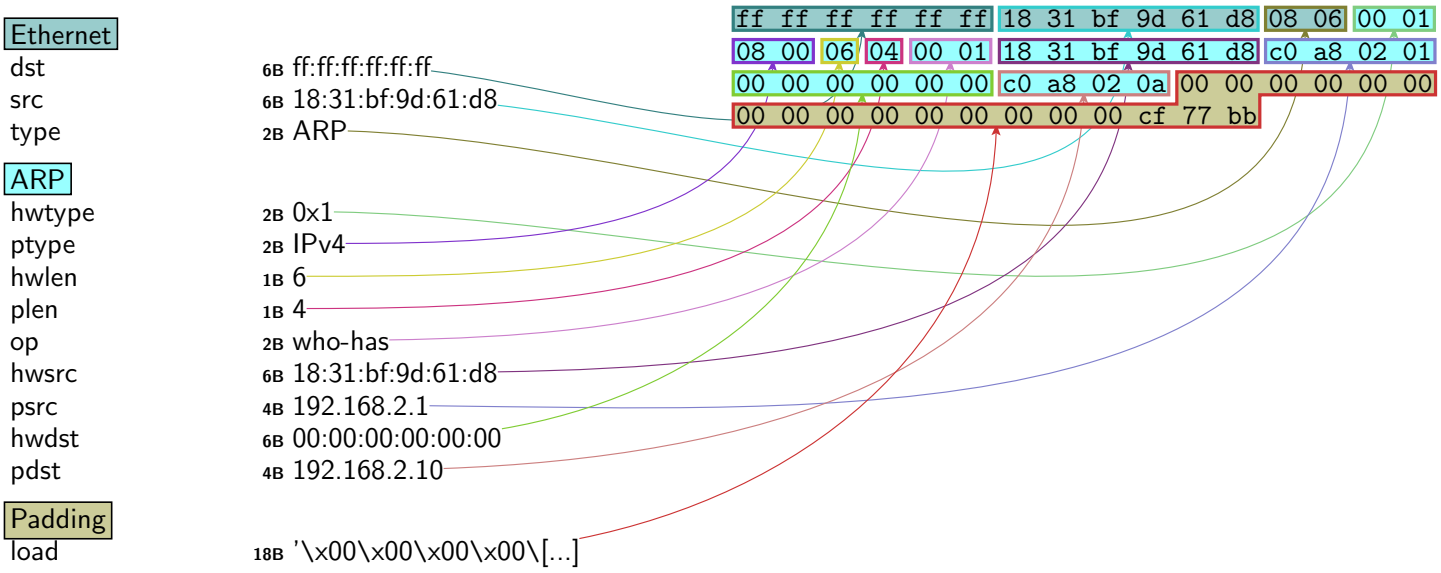
---

tbc

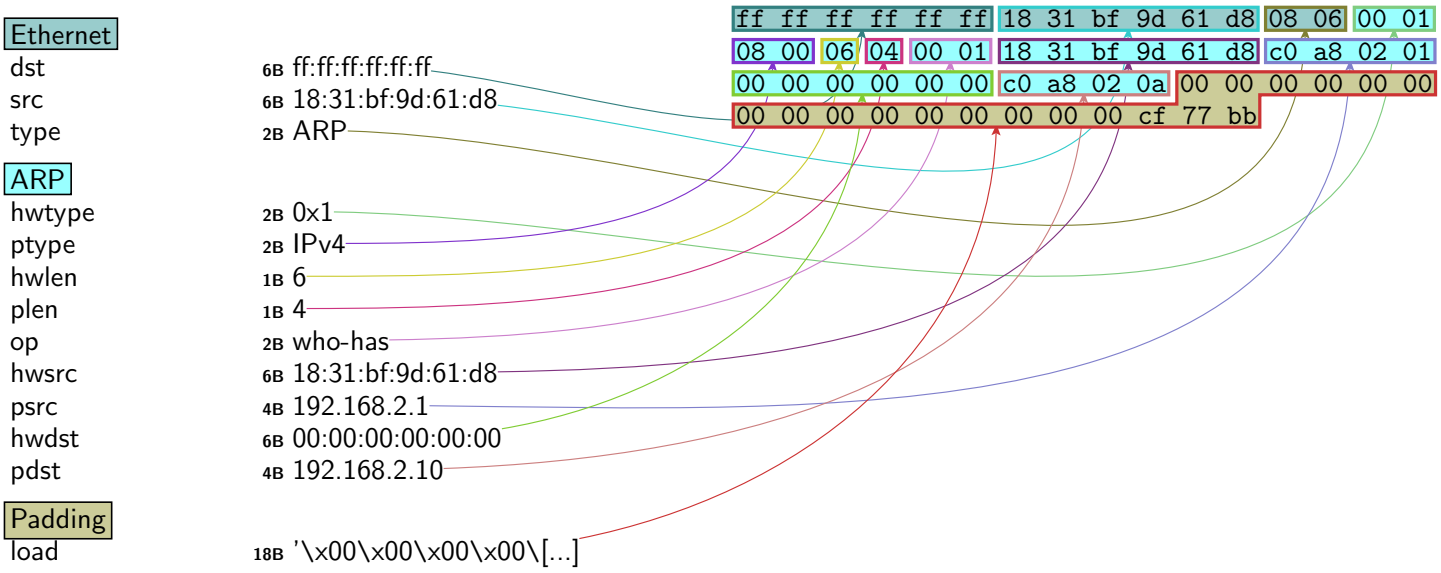
Frame 0/10


Ethernet
dst
src
type
ARP
hwtype
ptype
hwlen
plen
op
hwsrc
psrc
hwdst
pdst
Padding
load
6B ff:ff:ff:ff:ff:ff
6B 18:31:bf:9d:61:d8
2B ARP
2B 0x1
2B IPv4
1B 6
1B 4
2B who-has
6B 18:31:bf:9d:61:d8
4B 192.168.2.1
6B 00:00:00:00:00:00
4B 192.168.2.10
18B '\x00\x00\x00\x00\[...]
ff ff ff ff ff ff 18 31 bf 9d 61 d8 08 06 00 01
08 00 06 04 00 01 18 31 bf 9d 61 d8 c0 a8 02 01
00 00 00 00 00 00 c0 a8 02 0a 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 cf 77 bb

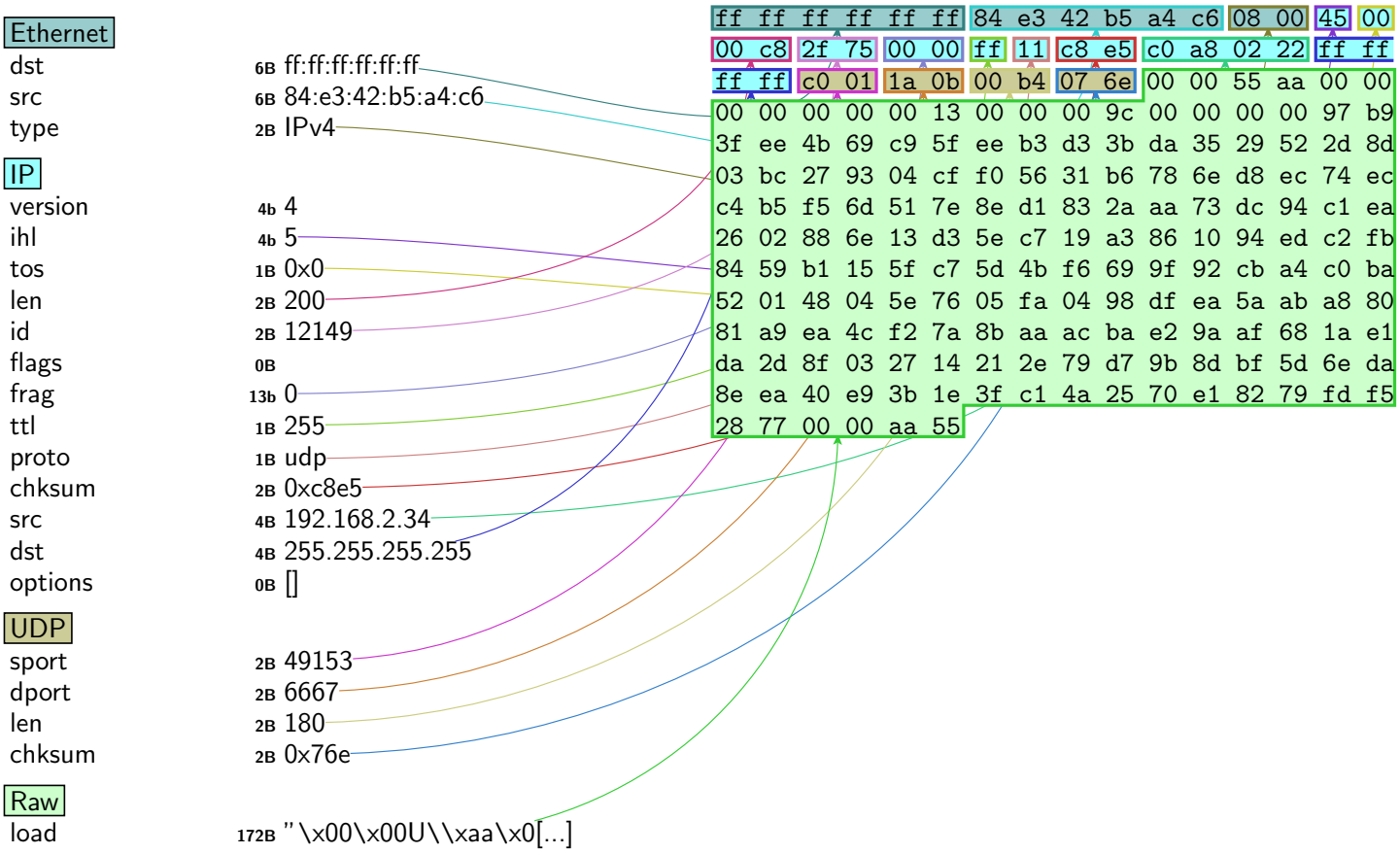
Frame 1/10


Ethernet
dst
src
type
ARP
hwtype
ptype
hwlen
plen
op
hwsrc
psrc
hwdst
pdst
Padding
load
6B ff:ff:ff:ff:ff:ff
6B 18:31:bf:9d:61:d8
2B ARP
2B 0x1
2B IPv4
1B 6
1B 4
2B who-has
6B 18:31:bf:9d:61:d8
4B 192.168.2.1
6B 00:00:00:00:00:00
4B 192.168.2.10
18B '\x00\x00\x00\x00\[...]
ff ff ff ff ff ff 18 31 bf 9d 61 d8 08 06 00 01
08 00 06 04 00 01 18 31 bf 9d 61 d8 c0 a8 02 01
00 00 00 00 00 00 c0 a8 02 0a 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 cf 77 bb

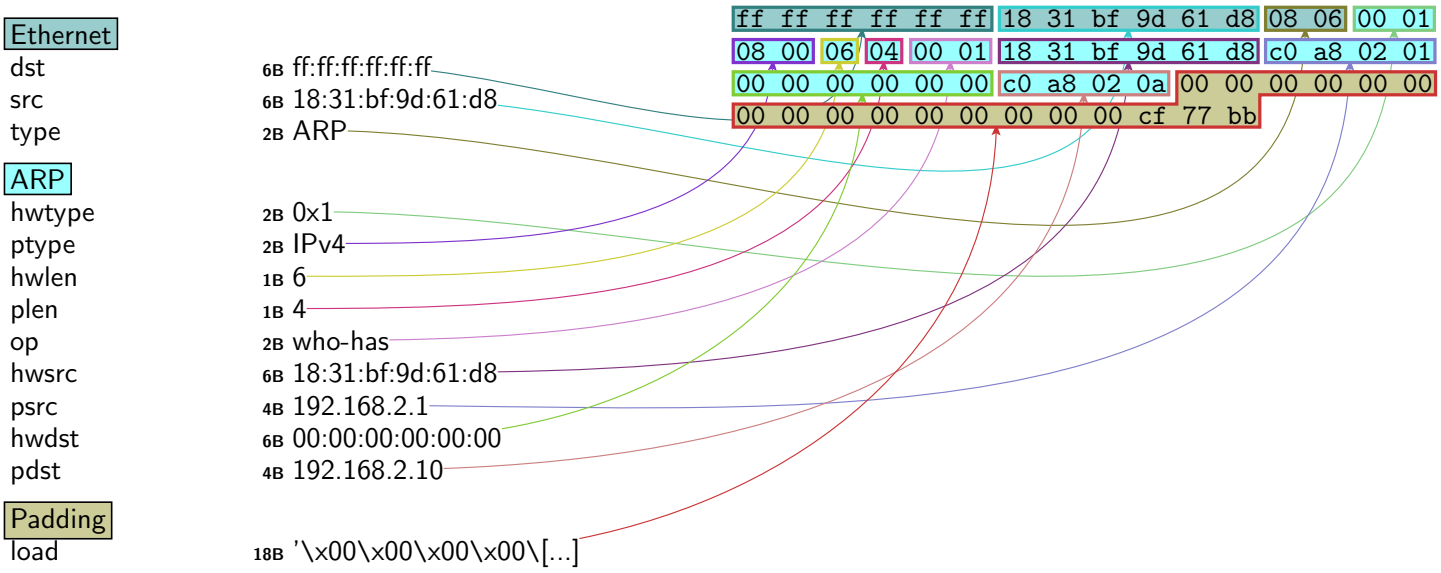
Frame 2/10


Ethernet
dst
src
type
ARP
hwtype
ptype
hwlen
plen
op
hwsrc
psrc
hwdst
pdst
Padding
load
6B ff:ff:ff:ff:ff:ff
6B 18:31:bf:9d:61:d8
2B ARP
2B 0x1
2B IPv4
1B 6
1B 4
2B who-has
6B 18:31:bf:9d:61:d8
4B 192.168.2.1
6B 00:00:00:00:00:00
4B 192.168.2.10
18B '\x00\x00\x00\x00\[...]
ff ff ff ff ff ff 18 31 bf 9d 61 d8 08 06 00 01
08 00 06 04 00 01 18 31 bf 9d 61 d8 c0 a8 02 01
00 00 00 00 00 00 c0 a8 02 0a 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 cf 77 bb

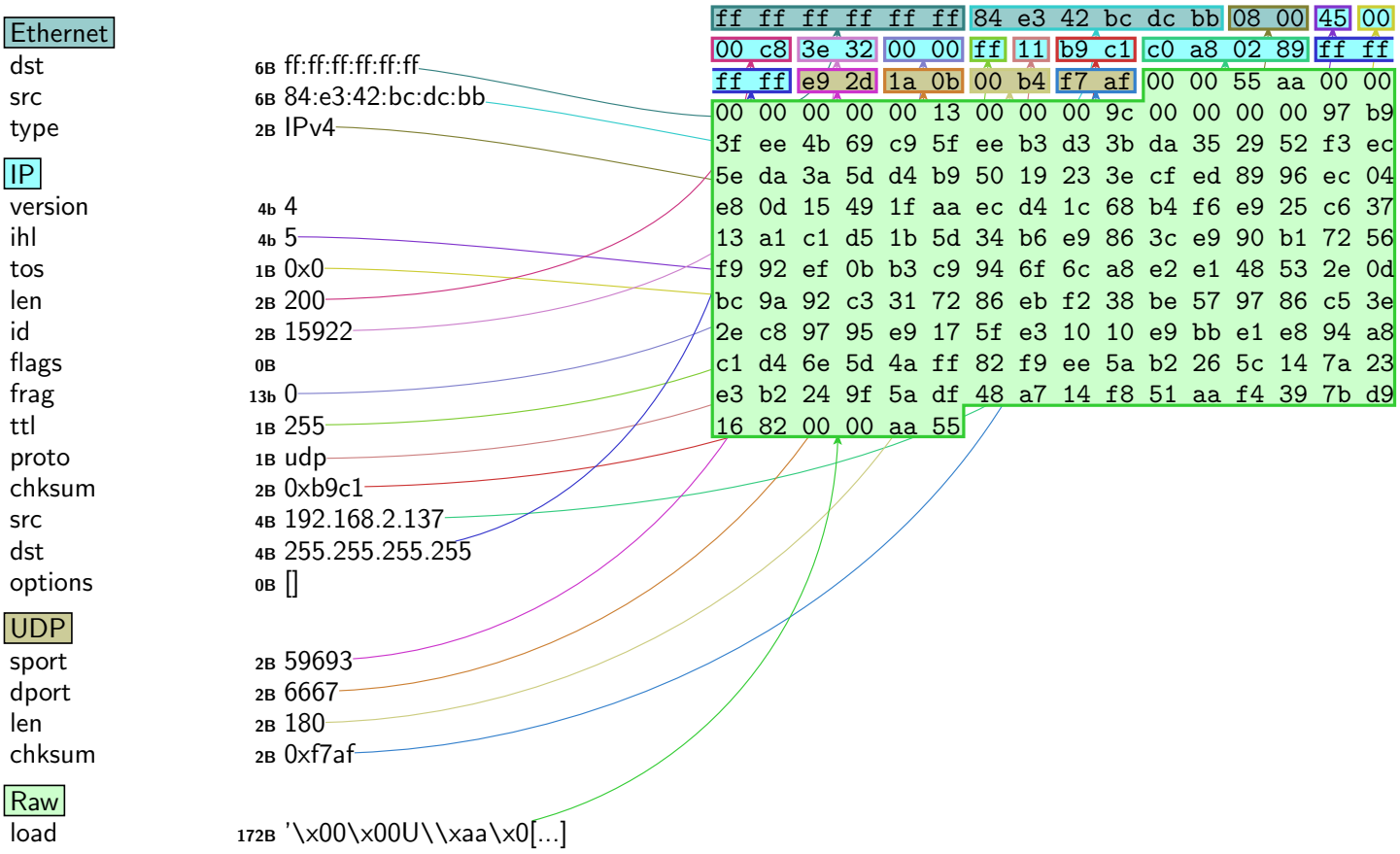
Frame 3/10


Ethernet
dst 6B ff:ff:ff:ff:ff:ff
src 6B 84:e3:42:b5:a4:c6
type 2B IPv4
IP
version 4b 4
ihl 4b 5
tos 1B 0x0
len 2B 200
id 2B 12149
flags 0B
frag 13b 0
ttl 1B 255
proto 1B udp
chksum 2B 0xc8e5
src 4B 192.168.2.34
dst 4B 255.255.255.255
options 0B []
UDP
sport 2B 49153
dport 2B 6667
len 2B 180
chksum 2B 0x76e
Raw
load 172B "\x00\x00U\\xaa\x0[...]
ff ff ff ff ff ff 84 e3 42 b5 a4 c6 08 00 45 00
00 c8 2f 75 00 00 ff 11 c8 e5 c0 a8 02 22 ff ff
ff ff c0 01 1a 0b 00 b4 07 6e 00 00 55 aa 00 00
00 00 00 00 00 13 00 00 00 9c 00 00 00 00 97 b9
3f ee 4b 69 c9 5f ee b3 d3 3b da 35 29 52 2d 8d
03 bc 27 93 04 cf f0 56 31 b6 78 6e d8 ec 74 ec
c4 b5 f5 6d 51 7e 8e d1 83 2a aa 73 dc 94 c1 ea
26 02 88 6e 13 d3 5e c7 19 a3 86 10 94 ed c2 fb
84 59 b1 15 5f c7 5d 4b f6 69 9f 92 cb a4 c0 ba
52 01 48 04 5e 76 05 fa 04 98 df ea 5a ab a8 80
81 a9 ea 4c f2 7a 8b aa ac ba e2 9a af 68 1a e1
da 2d 8f 03 27 14 21 2e 79 d7 9b 8d bf 5d 6e da
8e ea 40 e9 3b 1e 3f c1 4a 25 70 e1 82 79 fd f5
28 77 00 00 aa 55

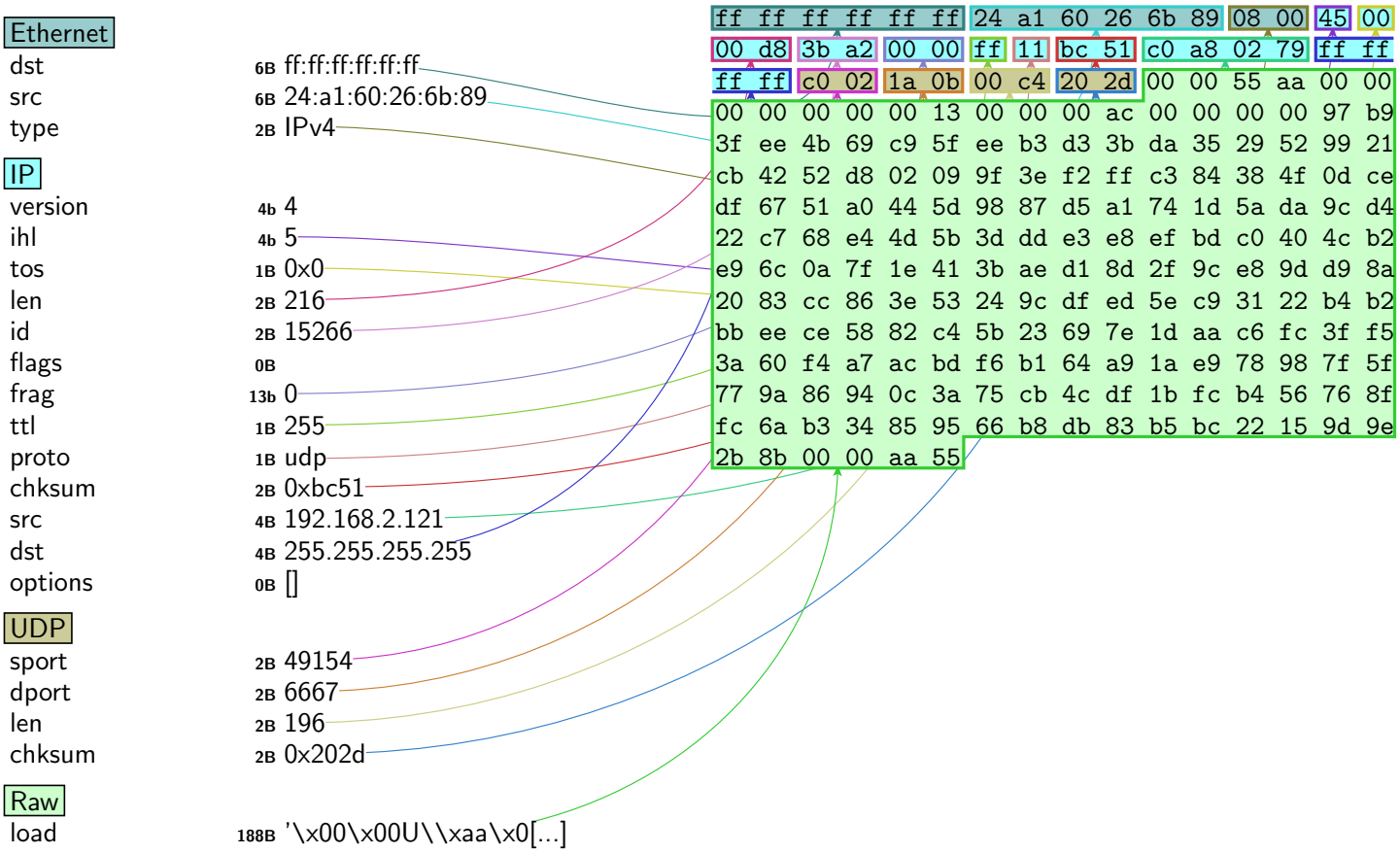
Frame 4/10


Ethernet
dst
src
type
ARP
hwtype
ptype
hwlen
plen
op
hwsrc
psrc
hwdst
pdst
Padding
load
6B ff:ff:ff:ff:ff:ff
6B 18:31:bf:9d:61:d8
2B ARP
2B 0x1
2B IPv4
1B 6
1B 4
2B who-has
6B 18:31:bf:9d:61:d8
4B 192.168.2.1
6B 00:00:00:00:00:00
4B 192.168.2.10
18B '\x00\x00\x00\x00\[...]
ff ff ff ff ff ff 18 31 bf 9d 61 d8 08 06 00 01
08 00 06 04 00 01 18 31 bf 9d 61 d8 c0 a8 02 01
00 00 00 00 00 00 c0 a8 02 0a 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 cf 77 bb

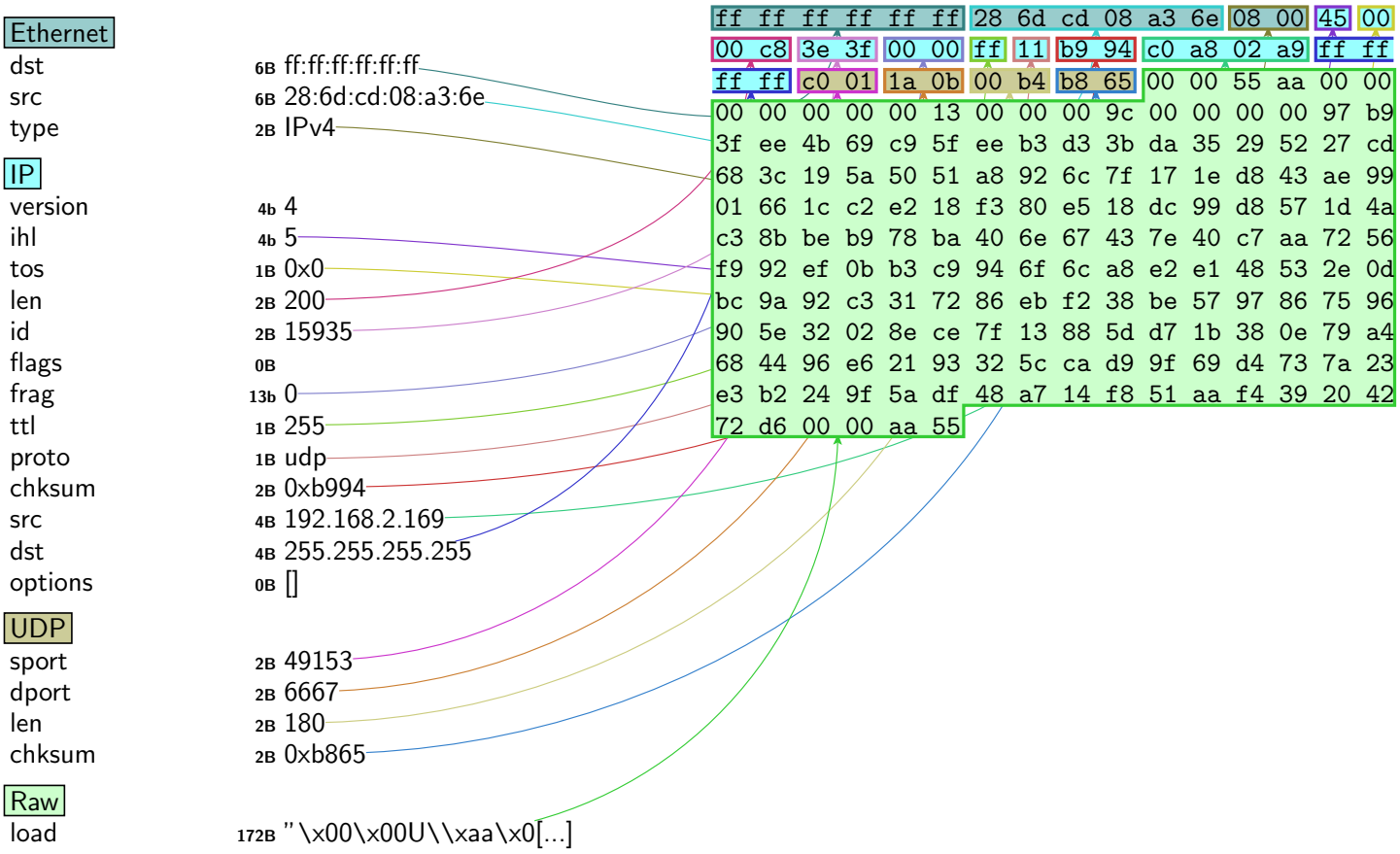
Frame 5/10


Ethernet
dst 6B ff:ff:ff:ff:ff:ff
src 6B 84:e3:42:bc:dc:bb
type 2B IPv4
IP
version 4b 4
ihl 4b 5
tos 1B 0x0
len 2B 200
id 2B 15922
flags 0B
frag 13b 0
ttl 1B 255
proto 1B udp
chksum 2B 0xb9c1
src 4B 192.168.2.137
dst 4B 255.255.255.255
options 0B []
UDP
sport 2B 59693
dport 2B 6667
len 2B 180
chksum 2B 0xf7af
Raw
load 172B '\x00\x00U\\xaa\x0[...]
ff ff ff ff ff ff 84 e3 42 bc dc bb 08 00 45 00
00 c8 3e 32 00 00 ff 11 b9 c1 c0 a8 02 89 ff ff
ff ff e9 2d 1a 0b 00 b4 f7 af 00 00 55 aa 00 00
00 00 00 00 00 13 00 00 00 9c 00 00 00 00 97 b9
3f ee 4b 69 c9 5f ee b3 d3 3b da 35 29 52 f3 ec
5e da 3a 5d d4 b9 50 19 23 3e cf ed 89 96 ec 04
e8 0d 15 49 1f aa ec d4 1c 68 b4 f6 e9 25 c6 37
13 a1 c1 d5 1b 5d 34 b6 e9 86 3c e9 90 b1 72 56
f9 92 ef 0b b3 c9 94 6f 6c a8 e2 e1 48 53 2e 0d
bc 9a 92 c3 31 72 86 eb f2 38 be 57 97 86 c5 3e
2e c8 97 95 e9 17 5f e3 10 10 e9 bb e1 e8 94 a8
c1 d4 6e 5d 4a ff 82 f9 ee 5a b2 26 5c 14 7a 23
e3 b2 24 9f 5a df 48 a7 14 f8 51 aa f4 39 7b d9
16 82 00 00 aa 55

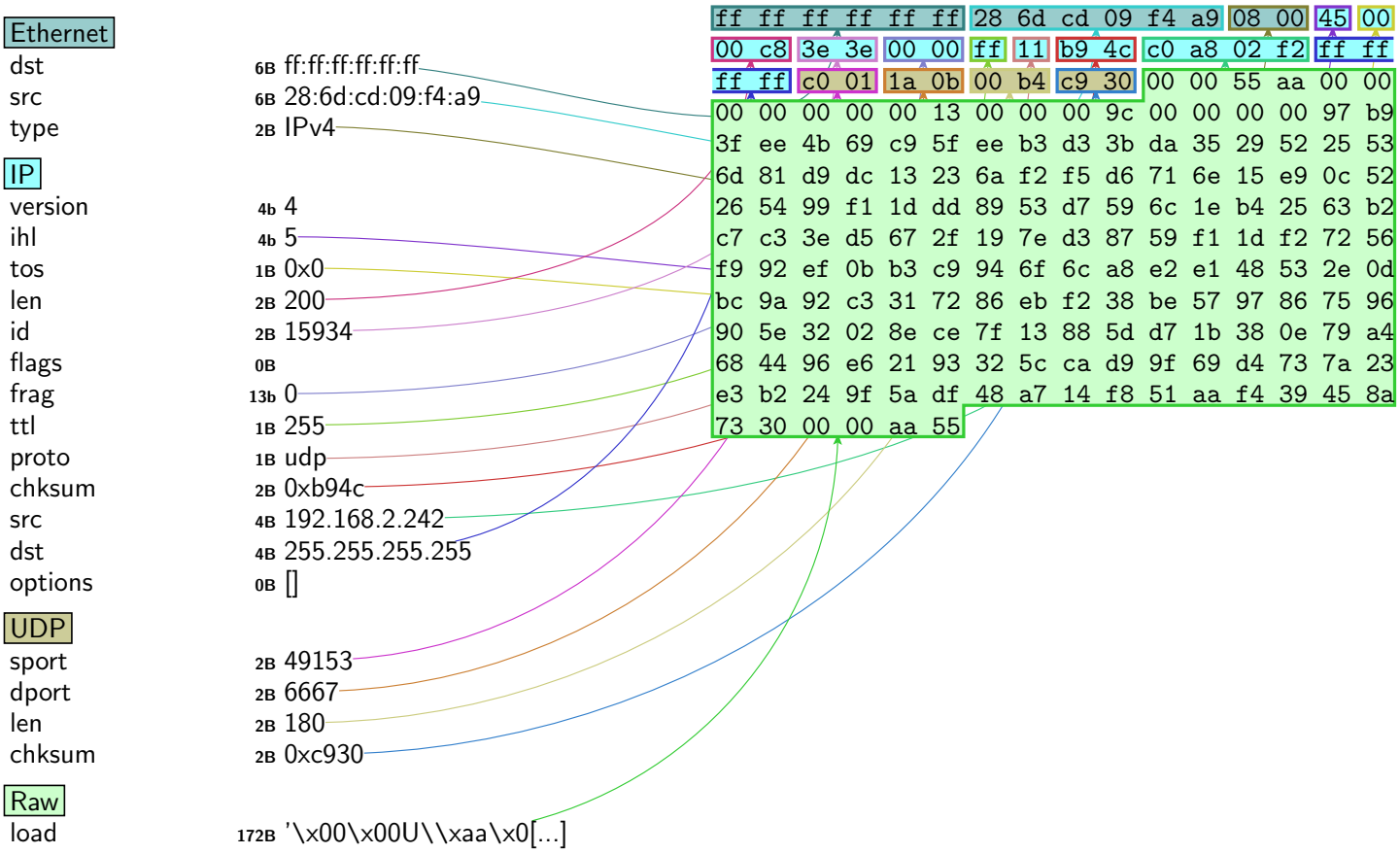
Frame 6/10


Ethernet
dst 6B ff:ff:ff:ff:ff:ff
src 6B 24:a1:60:26:6b:89
type 2B IPv4
IP
version 4b 4
ihl 4b 5
tos 1B 0x0
len 2B 216
id 2B 15266
flags 0B
frag 13b 0
ttl 1B 255
proto 1B udp
chksum 2B 0xbc51
src 4B 192.168.2.121
dst 4B 255.255.255.255
options 0B []
UDP
sport 2B 49154
dport 2B 6667
len 2B 196
chksum 2B 0x202d
Raw
load 188B '\x00\x00U\\xaa\x0[...]
ff ff ff ff ff ff 24 a1 60 26 6b 89 08 00 45 00
00 d8 3b a2 00 00 ff 11 bc 51 c0 a8 02 79 ff ff
ff ff c0 02 1a 0b 00 c4 20 2d 00 00 55 aa 00 00
00 00 00 00 00 13 00 00 00 ac 00 00 00 00 97 b9
3f ee 4b 69 c9 5f ee b3 d3 3b da 35 29 52 99 21
cb 42 52 d8 02 09 9f 3e f2 ff c3 84 38 4f 0d ce
df 67 51 a0 44 5d 98 87 d5 a1 74 1d 5a da 9c d4
22 c7 68 e4 4d 5b 3d dd e3 e8 ef bd c0 40 4c b2
e9 6c 0a 7f 1e 41 3b ae d1 8d 2f 9c e8 9d d9 8a
20 83 cc 86 3e 53 24 9c df ed 5e c9 31 22 b4 b2
bb ee ce 58 82 c4 5b 23 69 7e 1d aa c6 fc 3f f5
3a 60 f4 a7 ac bd f6 b1 64 a9 1a e9 78 98 7f 5f
77 9a 86 94 0c 3a 75 cb 4c df 1b fc b4 56 76 8f
fc 6a b3 34 85 95 66 b8 db 83 b5 bc 22 15 9d 9e
2b 8b 00 00 aa 55

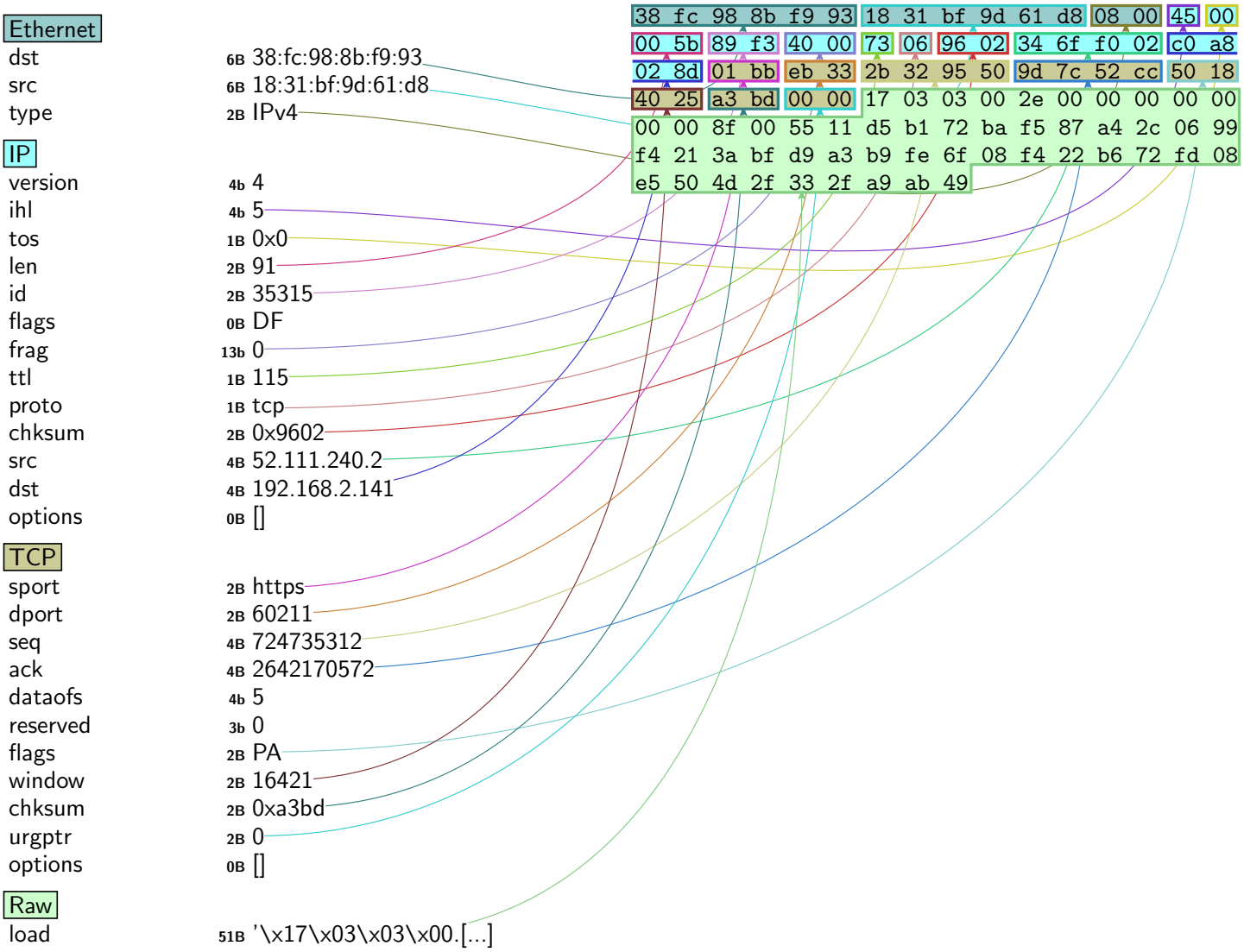
Frame 7/10


Ethernet
dst 6B ff:ff:ff:ff:ff:ff
src 6B 28:6d:cd:08:a3:6e
type 2B IPv4
IP
version 4b 4
ihl 4b 5
tos 1B 0x0
len 2B 200
id 2B 15935
flags 0B
frag 13b 0
ttl 1B 255
proto 1B udp
chksum 2B 0xb994
src 4B 192.168.2.169
dst 4B 255.255.255.255
options 0B []
UDP
sport 2B 49153
dport 2B 6667
len 2B 180
chksum 2B 0xb865
Raw
load 172B b"\x00\x00U\\xaa\x0[...]
ff ff ff ff ff ff 28 6d cd 08 a3 6e 08 00 45 00
00 c8 3e 3f 00 00 ff 11 b9 94 c0 a8 02 a9 ff ff
ff ff c0 01 1a 0b 00 b4 b8 65 00 00 55 aa 00 00
00 00 00 00 00 13 00 00 00 9c 00 00 00 00 97 b9
3f ee 4b 69 c9 5f ee b3 d3 3b da 35 29 52 27 cd
68 3c 19 5a 50 51 a8 92 6c 7f 17 1e d8 43 ae 99
01 66 1c c2 e2 18 f3 80 e5 18 dc 99 d8 57 1d 4a
c3 8b be b9 78 ba 40 6e 67 43 7e 40 c7 aa 72 56
f9 92 ef 0b b3 c9 94 6f 6c a8 e2 e1 48 53 2e 0d
bc 9a 92 c3 31 72 86 eb f2 38 be 57 97 86 75 96
90 5e 32 02 8e ce 7f 13 88 5d d7 1b 38 0e 79 a4
68 44 96 e6 21 93 32 5c ca d9 9f 69 d4 73 7a 23
e3 b2 24 9f 5a df 48 a7 14 f8 51 aa f4 39 20 42
72 d6 00 00 aa 55

Frame 8/10


Ethernet
dst 6B ff:ff:ff:ff:ff:ff
src 6B 28:6d:cd:09:f4:a9
type 2B IPv4
IP
version 4b 4
ihl 4b 5
tos 1B 0x0
len 2B 200
id 2B 15934
flags 0B
frag 13b 0
ttl 1B 255
proto 1B udp
chksum 2B 0xb94c
src 4B 192.168.2.242
dst 4B 255.255.255.255
options 0B []
UDP
sport 2B 49153
dport 2B 6667
len 2B 180
chksum 2B 0xc930
Raw
load 172B '\x00\x00U\\xaa\x0[...]
ff ff ff ff ff ff 28 6d cd 09 f4 a9 08 00 45 00
00 c8 3e 3e 00 00 ff 11 b9 4c c0 a8 02 f2 ff ff
ff ff c0 01 1a 0b 00 b4 c9 30 00 00 55 aa 00 00
00 00 00 00 00 13 00 00 00 9c 00 00 00 00 97 b9
3f ee 4b 69 c9 5f ee b3 d3 3b da 35 29 52 25 53
6d 81 d9 dc 13 23 6a f2 f5 d6 71 6e 15 e9 0c 52
26 54 99 f1 1d dd 89 53 d7 59 6c 1e b4 25 63 b2
c7 c3 3e d5 67 2f 19 7e d3 87 59 f1 1d f2 72 56
f9 92 ef 0b b3 c9 94 6f 6c a8 e2 e1 48 53 2e 0d
bc 9a 92 c3 31 72 86 eb f2 38 be 57 97 86 75 96
90 5e 32 02 8e ce 7f 13 88 5d d7 1b 38 0e 79 a4
68 44 96 e6 21 93 32 5c ca d9 9f 69 d4 73 7a 23
e3 b2 24 9f 5a df 48 a7 14 f8 51 aa f4 39 45 8a
73 30 00 00 aa 55

Frame 9/10


Ethernet
dst 6B 38:fc:98:8b:f9:93
src 6B 18:31:bf:9d:61:d8
type 2B IPv4
IP
version 4b 4
ihl 4b 5
tos 1B 0x0
len 2B 91
id 2B 35315
flags 0B DF
frag 13b 0
ttl 1B 115
proto 1B tcp
chksum 2B 0x9602
src 4B 52.111.240.2
dst 4B 192.168.2.141
options 0B []
TCP
sport 2B https
dport 2B 60211
seq 4B 724735312
ack 4B 2642170572
dataofs 4b 5
reserved 3b 0
flags 2B PA
window 2B 16421
chksum 2B 0xa3bd
urgptr 2B 0
options 0B []
Raw
load 51B '\x17\x03\x03\x00.[...]
38 fc 98 8b f9 93 18 31 bf 9d 61 d8 08 00 45 00
00 5b 89 f3 40 00 73 06 96 02 34 6f f0 02 c0 a8
02 8d 01 bb eb 33 2b 32 95 50 9d 7c 52 cc 50 18
40 25 a3 bd 00 00 17 03 03 00 2e 00 00 00 00 00
00 00 8f 00 55 11 d5 b1 72 ba f5 87 a4 2c 06 99
f4 21 3a bf d9 a3 b9 fe 6f 08 f4 22 b6 72 fd 08
e5 50 4d 2f 33 2f a9 ab 49