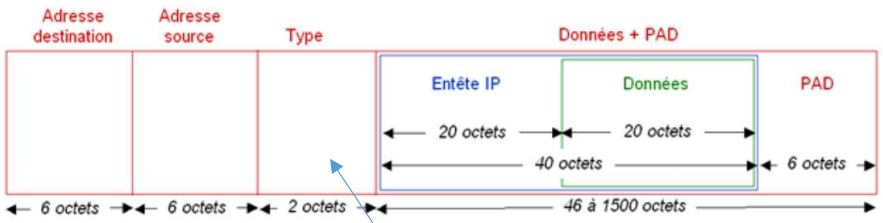
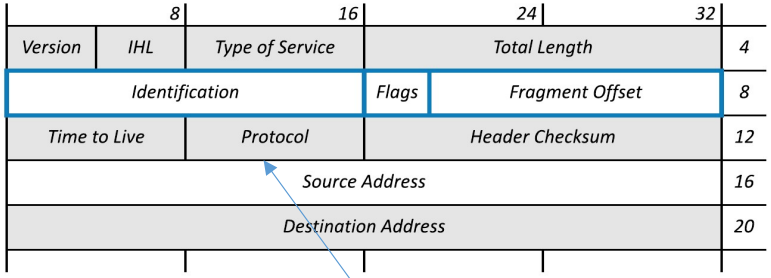
Network Traffic Analysis



Type Field

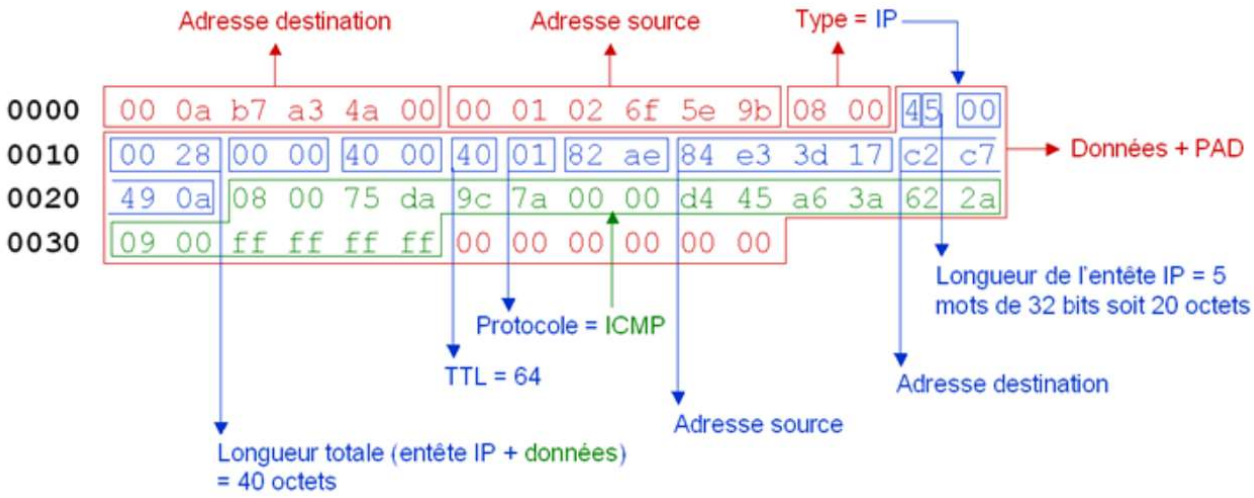
0x800 = IP

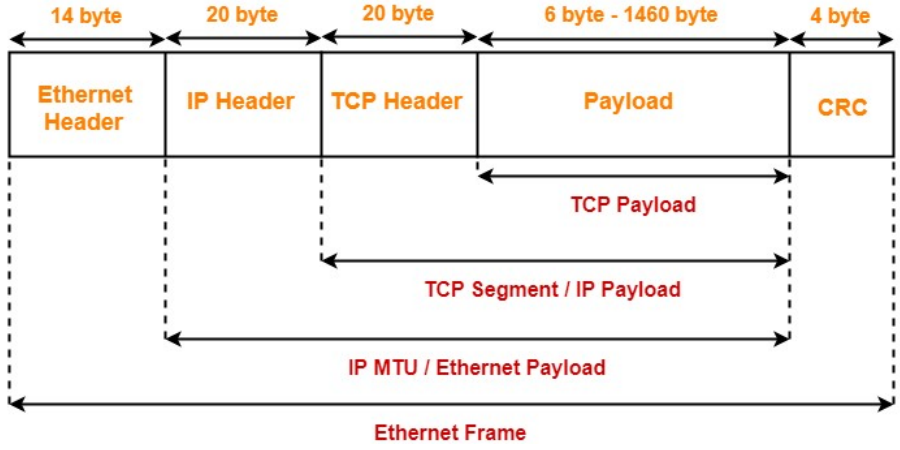
0x806= ARP

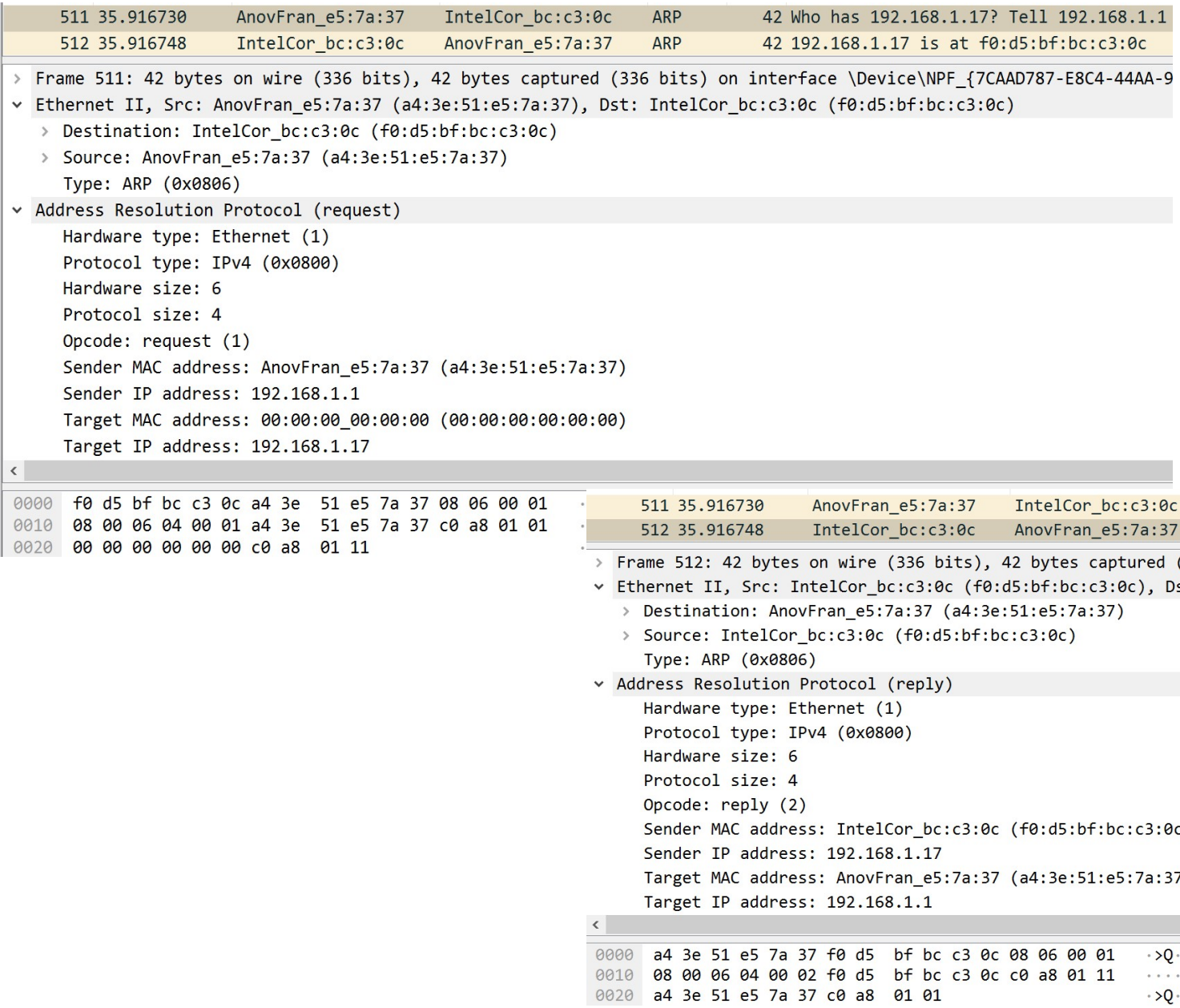


Protocol Field

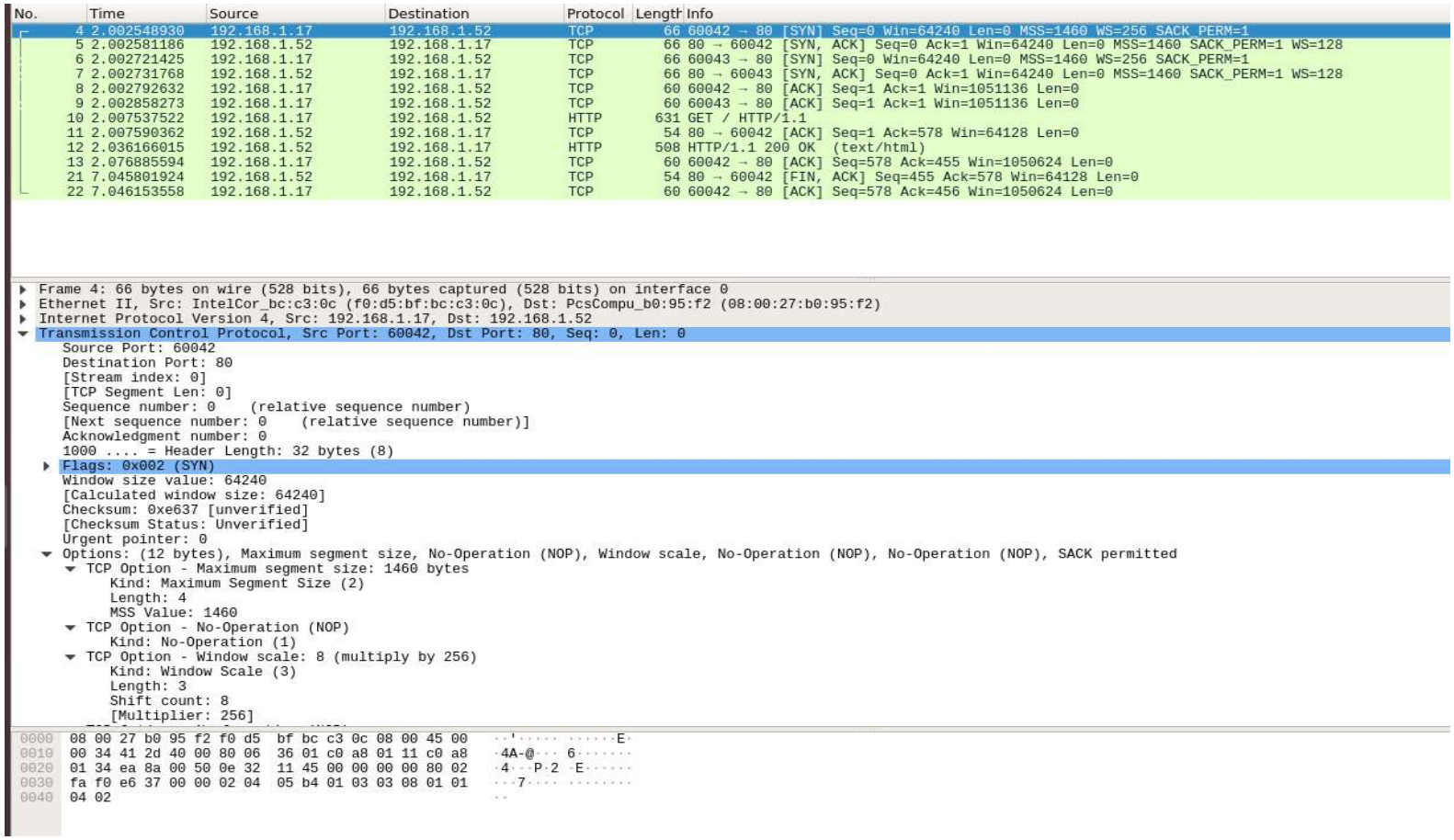
- 1 = ICMP
- 6 = TCP
- 17 =UDP






511 35.916730 AnovFran_e5:7a:37 IntelCor_bc:c3:0c ARP 42 Who has 192.168.1.17? Tell 192.168.1.1
512 35.916748 IntelCor_bc:c3:0c AnovFran_e5:7a:37 ARP 42 192.168.1.17 is at f0:d5:bf:bc:c3:0c
Frame 511: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{7CAAD787-E8C4-44AA-9
Ethernet II, Src: AnovFran_e5:7a:37 (a4:3e:51:e5:7a:37), Dst: IntelCor_bc:c3:0c (f0:d5:bf:bc:c3:0c)
Destination: IntelCor_bc:c3:0c (f0:d5:bf:bc:c3:0c)
Source: AnovFran_e5:7a:37 (a4:3e:51:e5:7a:37)
Type: ARP (0x0806)
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: AnovFran_e5:7a:37 (a4:3e:51:e5:7a:37)
Sender IP address: 192.168.1.1
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.17
0000 f0 d5 bf bc c3 0c a4 3e 51 e5 7a 37 08 06 00 01
0010 08 00 06 04 00 01 a4 3e 51 e5 7a 37 c0 a8 01 01
0020 00 00 00 00 00 00 c0 a8 01 11
511 35.916730 AnovFran_e5:7a:37 IntelCor_bc:c3:0c ARP 42 Who has 192.168.1.17? Tell 192.168.1.1
512 35.916748 IntelCor_bc:c3:0c AnovFran_e5:7a:37 ARP 42 192.168.1.17 is at f0:d5:bf:bc:c3:0c
Frame 512: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{7CAAD787-E8C4-44AA-9
Ethernet II, Src: IntelCor_bc:c3:0c (f0:d5:bf:bc:c3:0c), Dst: AnovFran_e5:7a:37 (a4:3e:51:e5:7a:37)
Destination: AnovFran_e5:7a:37 (a4:3e:51:e5:7a:37)
Source: IntelCor_bc:c3:0c (f0:d5:bf:bc:c3:0c)
Type: ARP (0x0806)
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: IntelCor_bc:c3:0c (f0:d5:bf:bc:c3:0c)
Sender IP address: 192.168.1.17
Target MAC address: AnovFran_e5:7a:37 (a4:3e:51:e5:7a:37)
Target IP address: 192.168.1.1
0000 a4 3e 51 e5 7a 37 f0 d5 bf bc c3 0c 08 06 00 01
0010 08 00 06 04 00 02 f0 d5 bf bc c3 0c c0 a8 01 11
0020 a4 3e 51 e5 7a 37 c0 a8 01 01

Exercise 1



No.	Time	Source	Destination	Protocol	Length	Info
4	2.002548930	192.168.1.17	192.168.1.52	TCP	66	60042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	2.002581186	192.168.1.52	192.168.1.17	TCP	66	80 → 60042 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
6	2.002721425	192.168.1.17	192.168.1.52	TCP	66	60043 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	2.002731768	192.168.1.52	192.168.1.17	TCP	66	80 → 60043 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
8	2.002792632	192.168.1.17	192.168.1.52	TCP	60	60042 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
9	2.002858273	192.168.1.17	192.168.1.52	TCP	60	60043 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
10	2.007537522	192.168.1.17	192.168.1.52	HTTP	631	GET / HTTP/1.1
11	2.007590362	192.168.1.52	192.168.1.17	TCP	54	80 → 60042 [ACK] Seq=1 Ack=578 Win=64128 Len=0
12	2.036166015	192.168.1.52	192.168.1.17	HTTP	508	HTTP/1.1 200 OK (text/html)
13	2.076885594	192.168.1.17	192.168.1.52	TCP	60	60042 → 80 [ACK] Seq=578 Ack=455 Win=1050624 Len=0
21	7.045801924	192.168.1.52	192.168.1.17	TCP	54	80 → 60042 [FIN, ACK] Seq=455 Ack=578 Win=64128 Len=0
22	7.046153558	192.168.1.17	192.168.1.52	TCP	60	60042 → 80 [ACK] Seq=578 Ack=456 Win=1050624 Len=0

```
▸ Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▸ Ethernet II, Src: IntelCor_bc:c3:0c (f0:d5:bf:bc:c3:0c), Dst: PcsCompu_b0:95:f2 (08:00:27:b0:95:f2)
▸ Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.52
▾ Transmission Control Protocol, Src Port: 60042, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 60042
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x002 (SYN)
    Window size value: 64240
    [Calculated window size: 64240]
    Checksum: 0xe637 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▾ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    ▾ TCP Option - Maximum segment size: 1460 bytes
        Kind: Maximum Segment Size (2)
        Length: 4
        MSS Value: 1460
    ▾ TCP Option - No-Operation (NOP)
        Kind: No-Operation (1)
    ▾ TCP Option - Window scale: 8 (multiply by 256)
        Kind: Window Scale (3)
        Length: 3
        Shift count: 8
        [Multiplier: 256]
```

```
0000  08 00 27 b0 95 f2 f0 d5  bf bc c3 0c 08 00 45 00   ··'····· ······E·
0010  00 34 41 2d 40 00 80 06  36 01 c0 a8 01 11 c0 a8   ·4A-@··· 6·······
0020  01 34 ea 8a 00 50 0e 32  11 45 00 00 00 00 80 02   ·4···P·2 ·E······
0030  fa f0 e6 37 00 00 02 04  05 b4 01 03 03 08 01 01   ···7···· ········
0040  04 02                                             ··
```

- Analyse the traffic : @IP source and destination, the Type of traffic,
- Connection analysis : Seq Number, ACK number and the flags

Exercise 2

FR-1

```
08 00 27 b0 95 f2 08 00  27 4b 35 58 08 00 45 00
00 3c f2 00 40 00 40 06  c4 3b c0 a8 01 fb c0 a8
01 34 aa 18 00 16 d5 41  e4 31 00 00 00 00 a0 02
fa f0 de 9c 00 00 02 04  05 b4 04 02 08 0a c7 33
bf 1c 00 00 00 00 01 03  03 07
```

FR-2

```
08 00 27 4b 35 58 08 00  27 b0 95 f2 08 00 45 00
00 3c 00 00 40 00 40 06  b6 3c c0 a8 01 34 c0 a8
01 fb 00 16 aa 18 d2 63  5e 14 d5 41 e4 32 a0 12
fe 88 84 ae 00 00 02 04  05 b4 04 02 08 0a 61 b0
21 2a c7 33 bf 1c 01 03  03 07
```

FR-3

```
08 00 27 b0 95 f2 08 00  27 4b 35 58 08 00 45 00
00 34 f2 01 40 00 40 06  c4 42 c0 a8 01 fb c0 a8
01 34 aa 18 00 16 d5 41  e4 32 d2 63 5e 15 80 10
01 f6 52 ff 00 00 01 01  08 0a c7 33 bf 1d 61 b0
21 2a
```

- Analyse this traffic :
  - @MAC src and dest, @IPsrc and dst
  - Protocol used on transport layer
  - Port source and destination : identify the network service
  - The flags : identify the connection type