

Part 1. Capturing and analyzing Ethernet and IP headers

- first GET request and GET response packets, including IP address of the source and destination:

No.	Time	Source	Destination	Protocol	Length	Info
224	4.040518	192.168.1.213	93.184.216.34	HTTP	598	GET / HTTP/1.1
244	4.275400	93.184.216.34	192.168.1.213	HTTP	1076	HTTP/1.1 200 OK (text/html)

- GET request packet, number of bytes from the beginning of the Ethernet frame where the ASCII "G" in "GET" appears:

Frame 224: 598 bytes on wire (4784 bits), 598 bytes captured (4784 bits) on interface \Device\NPF_{D7AC33AD-268D-4D05-A96C-...}

Ethernet II, Src: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7), Dst: ZyxelCom_31:c5:70 (d4:1a:d1:31:c5:70)

Destination: ZyxelCom_31:c5:70 (d4:1a:d1:31:c5:70)

Source: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.1.213, Dst: 93.184.216.34

Transmission Control Protocol, Src Port: 9644, Dst Port: 80, Seq: 1, Ack: 1, Len: 544

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]

Request Method: GET

Request URI: /

Request Version: HTTP/1.1

Host: example.com\r\n

HTTP Request Method (http.request.method), 3 bytes

Packets: 567 · Displayed: 2 (0.4%)

- 48-bit Ethernet address and the gateway of the system:

Frame 224: 598 bytes on wire (4784 bits), 598 bytes captured (4784 bits) on interface \Device\NPF_{D7AC33AD-268D-4D05-A96C-...}

Ethernet II, Src: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7), Dst: ZyxelCom_31:c5:70 (d4:1a:d1:31:c5:70)

Destination: ZyxelCom_31:c5:70 (d4:1a:d1:31:c5:70)

Source: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.1.213, Dst: 93.184.216.34

Transmission Control Protocol, Src Port: 9644, Dst Port: 80, Seq: 1, Ack: 1, Len: 544

Hypertext Transfer Protocol

Ethernet (eth), 14 bytes

Packets: 567 · Displayed: 2 (0.4%)

Profile: Default

- Time to Live:

The image shows a Wireshark packet capture analysis of an HTTP GET request. The packet list at the top shows two packets: a GET request (No. 224) and its response (No. 244). The packet details pane on the left shows the structure of the selected packet (No. 224), which is an HTTP GET request. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
224	4.040518	192.168.1.213	93.184.216.34	HTTP	598	GET / HTTP/1.1
244	4.275400	93.184.216.34	192.168.1.213	HTTP	1076	HTTP/1.1 200 OK (text/html)

Packet Details (No. 224):

- Frame 224: 598 bytes on wire (4784 bits), 598 bytes captured (4784 bits) on interface \Device\NPF_{D7AC...}
- Ethernet II, Src: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7), Dst: ZyxelCom_31:c5:70 (d4:1a:d1:31:c5:70)
- Internet Protocol Version 4, Src: 192.168.1.213, Dst: 93.184.216.34
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 584
 - Identification: 0x262e (9774)
 - 010. = Flags: 0x2, Don't fragment
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 64
 - Protocol: TCP (6)
 - Header Checksum: 0x0000 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.1.213
 - Destination Address: 93.184.216.34
- Transmission Control Protocol, Src Port: 9644, Dst Port: 80, Seq: 1, Ack: 1, Len: 544
- Hypertext Transfer Protocol

Packet Bytes:

```

0010 02 48 26 2e 40 00 00 00 00 c0 a8 01 d5 5d b8 -H&.@.....]
0020 d8 22 25 ac 00 50 46 dc b0 6b 34 d3 9d 28 50 18 -"%-PF..-k4..(P
0030 02 04 fa 92 00 00 47 45 54 20 2f 20 48 54 54 50 -.....GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 65 78 61 6d /1.1..Ho st: exam
0050 70 6c 65 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 ple.com. -Connect
0060 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d ion: kee p-alive-
0070 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 -Cache-C ontrol:
0080 6d 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 max-age= 0 -Upgra
0090 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ
00a0 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 ests: 1- -User-Ag
00b0 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Moz illa/5.0
00c0 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e (Window s NT 10.
00d0 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 0; Win64 ; x64) A
00e0 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 ppleWebK it/537.3
00f0 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 6 (KHTML , like G
0100 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 31 33 ecko) Ch rome/113
0110 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 2f 35 33 .0.0.0 S afari/53
0120 37 2e 33 36 20 45 64 67 2f 31 31 33 2e 30 2e 31 7.36 Edg /113.0.1
0130 37 37 34 2e 33 35 0d 0a 41 63 63 65 70 74 3a 20 774.35 . Accept:
0140 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 text/htm l,applic
0150 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c ation/xh tml+xml;
0160 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b applicat ion/xml;
0170 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 77 65 62 70 q=0.9,im age/webp
0180 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b ,image/a png,*/*;
0190 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f q=0.8,ap plicatio
01a0 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 6e 67 n/signed -exchang
01b0 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a 41 63 e;v=b3;q =0.7 -Ac
  
```

Time to Live: 64

Protocol: TCP (6)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.213

Destination Address: 93.184.216.34

Transmission Control Protocol, Src Port: 9644, Dst Port: 80, Seq: 1, Ack: 1, Len: 544

Hypertext Transfer Protocol

Time to Live (ip.ttl), 1 byte

Packets: 567 · Displayed: 2 (0.4%) · Dropped: 0 (0.0%)

Profile: Default

- 48-bit destination and source address in the Ethernet frame:

The image shows a Wireshark packet capture analysis of an HTTP GET request. The packet list at the top shows two packets: packet 224 (HTTP GET) and packet 244 (HTTP OK). The packet details pane for packet 224 shows the Ethernet II frame with source and destination MAC addresses (4c:1d:96:5b:ed:f7) highlighted in blue. The packet bytes pane shows the raw data with the same MAC addresses highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
224	4.040518	192.168.1.213	93.184.216.34	HTTP	598	GET / HTTP/1.1
244	4.275400	93.184.216.34	192.168.1.213	HTTP	1076	HTTP/1.1 200 OK (text/html)

Frame 224: 598 bytes on wire (4784 bits), 598 bytes captured (4784 bits) on interface \Device\NPF_{D7AC...}

Ethernet II, Src: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7), Dst: ZyxelCom_31:c5:70 (d4:1a:d1:31:c5:70)

- Destination: ZyxelCom_31:c5:70 (d4:1a:d1:31:c5:70)
- Source: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.1.213, Dst: 93.184.216.34
- Transmission Control Protocol, Src Port: 9644, Dst Port: 80, Seq: 1, Ack: 1, Len: 544
- Hypertext Transfer Protocol

0000 d4 1a d1 31 c5 70 4c 1d 96 5b ed f7 08 00 45 00 ...1.pL...[...E-
0010 02 48 26 2e 40 00 40 06 00 00 c0 a8 01 d5 5d b8 .H&.@...-.....]
0020 d8 22 25 ac 00 50 46 dc b0 6b 34 d3 9d 28 50 18 ."%-PF..k4..(P.
0030 02 04 fa 92 00 00 47 45 54 20 2f 20 48 54 54 50GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 65 78 61 6d /1.1--Ho st: exam
0050 70 6c 65 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 ple.com..Connect
0060 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d ion: kee p-alive-
0070 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 -Cache-C ontrol:
0080 6d 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 max-age= 0--Upgra
0090 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ
00a0 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 ests: 1..-User-Ag
00b0 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Moz illa/5.0
00c0 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e (Window s NT 10.
00d0 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 0; Win64 ; x64) A
00e0 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 ppleWebK it/537.3
00f0 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 6 (KHTML , like G
0100 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 31 33 ecko) Ch rome/113
0110 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 2f 35 33 .0.0.0 S afari/53
0120 37 2e 33 36 20 45 64 67 2f 31 31 33 2e 30 2e 31 7.36 Edg /113.0.1
0130 37 37 34 2e 33 35 0d 0a 41 63 63 65 70 74 3a 20 774.35.. Accept:
0140 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 text/htm l,applic
0150 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c ation/xh tml+xml,
0160 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b applicat ion/xml;
0170 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 77 65 62 70 q=0.9,im age/webp
0180 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b ,image/a png,*/*;
0190 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f q=0.8,ap plicatio
01a0 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 6e 67 n/signed -exchang

Destination Hardware Address (eth.dst), 6 bytes

Packets: 567 · Displayed: 2 (0.4%) · Dropped: 0 (0.0%)

Profile: Default

- the header size:

The image shows a Wireshark packet capture window titled '*Wi-Fi'. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main display area is divided into three panes:

- Packet List:** Shows two captured packets. Packet 224 is an HTTP GET request from 192.168.1.213 to 93.184.216.34. Packet 244 is the corresponding HTTP 200 OK response from 93.184.216.34 to 192.168.1.213.
- Packet Details:** Expands packet 224, showing the following layers:
 - Frame 224: 598 bytes on wire (4784 bits), 598 bytes captured (4784 bits) on interface \Device\NPF_{D7AC}...
 - Ethernet II, Src: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7), Dst: ZyxelCom_31:c5:70 (d4:1a:d1:31:c5:70)
 - Destination: ZyxelCom_31:c5:70 (d4:1a:d1:31:c5:70)
 - Source: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7)
 - Type: IPv4 (0x0800)
 - Internet Protocol Version 4, Src: 192.168.1.213, Dst: 93.184.216.34
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 584
 - Identification: 0x262e (9774)
 - 010. = Flags: 0x2, Don't fragment
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 64
 - Protocol: TCP (6)
 - Header Checksum: 0x0000 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.1.213
 - Destination Address: 93.184.216.34
 - Transmission Control Protocol, Src Port: 9644, Dst Port: 80, Seq: 1, Ack: 1, Len: 544
 - Hypertext Transfer Protocol
- Packet Bytes:** Displays the raw packet data in hexadecimal and ASCII. The first few bytes are: d4 1a d1 31 c5 70 4c 1d 96 5b ed f7 08 00 45 00. The ASCII representation shows the start of an HTTP GET request: "...1 pL...[...].H&.@...].%-.PF..k4..(P.....GE T / HTTP /1.1...Host: exam ple.com...Connect ion: kee p-alive...Cache-C ontrol: max-age= 0...Upgra de-Insec ure-Requ ests: 1...User-Ag ent: Moz illa/5.0 (Window s NT 10.0; Win64 ; x64) A ppleWebK it/537.3 6 (KHTML , like G ecko) Ch rome/113 .0.0.0 S afari/53 7.36 Edg e/113.0.1 774.35... Accept: text/htm l,applic ation/xh tml+xml, applicat ion/xml; q=0.9,im age/webp ,image/a png,*/*; q=0.8,ap plicatio n/sign ed-exchang

At the bottom, a status bar indicates: Packets: 567 · Displayed: 2 (0.4%) · Dropped: 0 (0.0%) Profile: Default.

Part 2. The Address Resolution Protocol

- computer's ARP cache:

```

C:\Users\lenovo>arp -a

Interface: 192.168.122.1 --- 0x12
Internet Address      Physical Address      Type
192.168.122.255       ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.1.213 --- 0x13
Internet Address      Physical Address      Type
192.168.1.1           d4-1a-d1-31-c5-70     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.130.1 --- 0x14
Internet Address      Physical Address      Type
192.168.130.255       ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static
    
```

- the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message:

Wireshark packet capture showing ARP requests. The packet list shows four ARP requests. The packet details for the first request (Frame 411) are expanded, showing the Ethernet II header with Source: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7) and Destination: Broadcast (ff:ff:ff:ff:ff:ff). The packet bytes pane shows the hexadecimal representation of the frame.

No.	Time	Source	Destination	Protocol	Length	Info
411	5.181111	IntelCor_5b:ed:f7	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.213
412	5.182021	ZyxeCom_31:c5:70	IntelCor_5b:ed:f7	ARP	42	192.168.1.1 is at d4:1a:d1:31:c5:70
3822	21.833327	ZyxeCom_31:c5:70	IntelCor_5b:ed:f7	ARP	42	Who has 192.168.1.213? Tell 192.168.1.1
3823	21.833341	IntelCor_5b:ed:f7	ZyxeCom_31:c5:70	ARP	42	192.168.1.213 is at 4c:1d:96:5b:ed:f7

Frame 411: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D7AC33AD...}

Ethernet II, Src: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

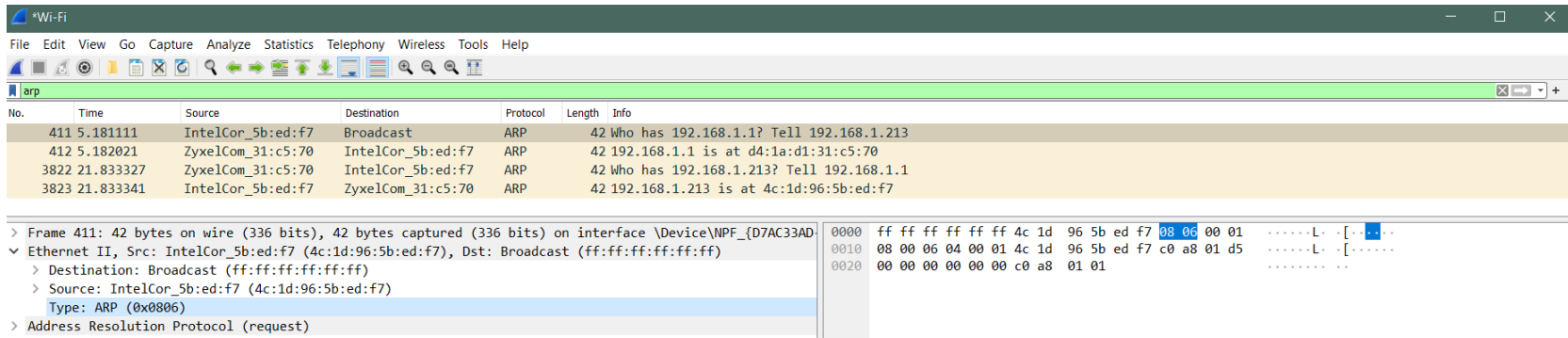
- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7)
- Type: ARP (0x0806)
- Address Resolution Protocol (request)

Packet bytes (hex):

```

0000 ff ff ff ff ff ff 4c 1d 96 5b ed f7 08 06 00 01 .....L.[-.-.-.-
0010 08 00 06 04 00 01 4c 1d 96 5b ed f7 c0 a8 01 d5 .....L.[-.-.-.-
0020 00 00 00 00 00 00 c0 a8 01 01 .....
    
```

- the hexadecimal value for the two-byte Ethernet Frame type field:



Wireshark capture of ARP requests. The packet list shows four packets. Packet 411 is selected, showing details for Ethernet II and ARP. The ARP section shows 'Type: ARP (0x0806)'.

No.	Time	Source	Destination	Protocol	Length	Info
411	5.181111	IntelCor_5b:ed:f7	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.213
412	5.182021	ZyxelCom_31:c5:70	IntelCor_5b:ed:f7	ARP	42	192.168.1.1 is at d4:1a:d1:31:c5:70
3822	21.833327	ZyxelCom_31:c5:70	IntelCor_5b:ed:f7	ARP	42	Who has 192.168.1.213? Tell 192.168.1.1
3823	21.833341	IntelCor_5b:ed:f7	ZyxelCom_31:c5:70	ARP	42	192.168.1.213 is at 4c:1d:96:5b:ed:f7

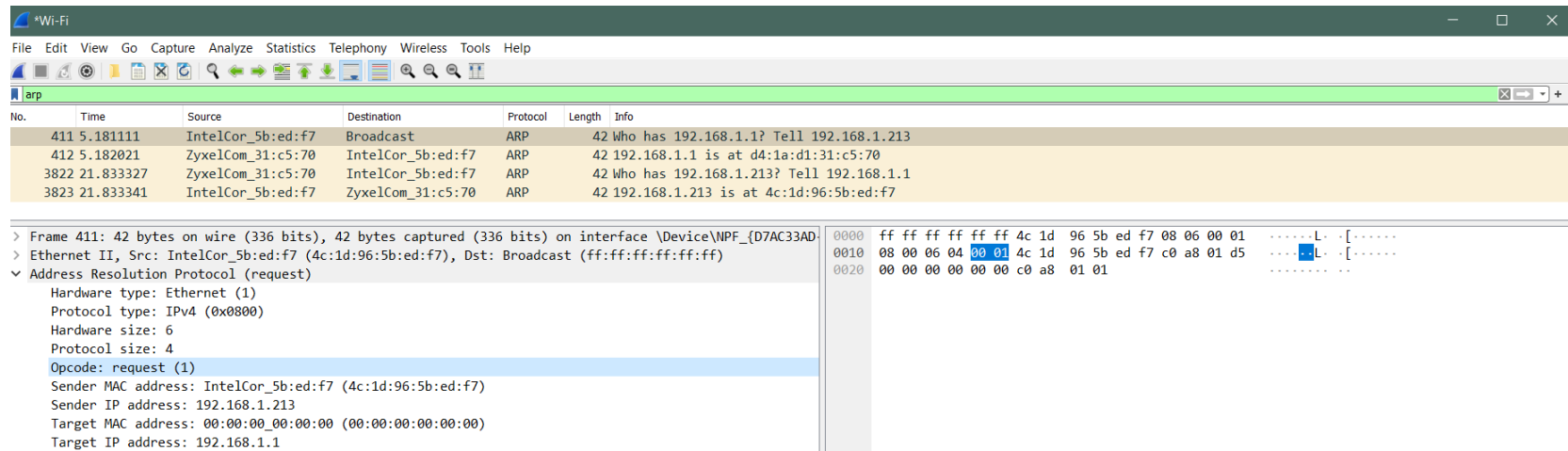
Frame 411: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D7AC33AD...}

Ethernet II, Src: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7)
- Type: ARP (0x0806)

Address Resolution Protocol (request)

- the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made:



Wireshark capture of ARP requests. The packet list shows four packets. Packet 411 is selected, showing details for Ethernet II, Address Resolution Protocol (request), and Opcode: request (1). The Opcode field is highlighted.

No.	Time	Source	Destination	Protocol	Length	Info
411	5.181111	IntelCor_5b:ed:f7	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.213
412	5.182021	ZyxelCom_31:c5:70	IntelCor_5b:ed:f7	ARP	42	192.168.1.1 is at d4:1a:d1:31:c5:70
3822	21.833327	ZyxelCom_31:c5:70	IntelCor_5b:ed:f7	ARP	42	Who has 192.168.1.213? Tell 192.168.1.1
3823	21.833341	IntelCor_5b:ed:f7	ZyxelCom_31:c5:70	ARP	42	192.168.1.213 is at 4c:1d:96:5b:ed:f7

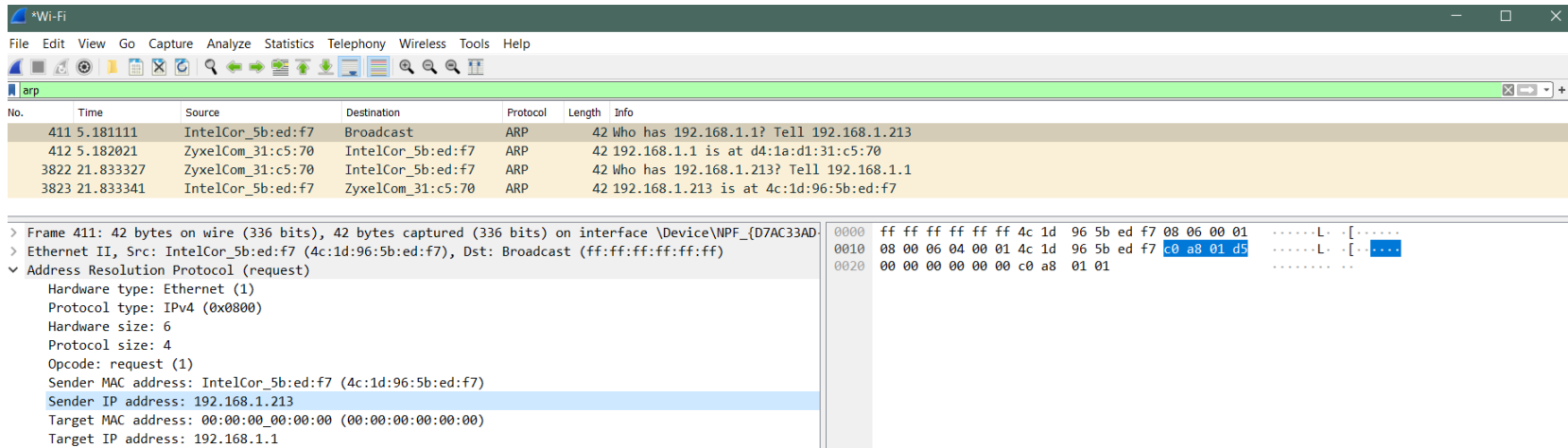
Frame 411: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D7AC33AD...}

Ethernet II, Src: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7)
- Sender IP address: 192.168.1.213
- Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.1.1

- ARP message contains the IP address of the sender:



Wireshark capture of ARP messages. The packet list shows four ARP packets. Packet 411 is an ARP request from IntelCor_5b:ed:f7 to Broadcast. The packet details pane shows the 'Sender IP address: 192.168.1.213' highlighted in blue. The packet bytes pane shows the raw data with the sender IP address (08 06 00 01) highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
411	5.181111	IntelCor_5b:ed:f7	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.213
412	5.182021	ZyxeCom_31:c5:70	IntelCor_5b:ed:f7	ARP	42	192.168.1.1 is at d4:1a:d1:31:c5:70
3822	21.833327	ZyxeCom_31:c5:70	IntelCor_5b:ed:f7	ARP	42	Who has 192.168.1.213? Tell 192.168.1.1
3823	21.833341	IntelCor_5b:ed:f7	ZyxeCom_31:c5:70	ARP	42	192.168.1.213 is at 4c:1d:96:5b:ed:f7

Frame 411: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D7AC33AD...}

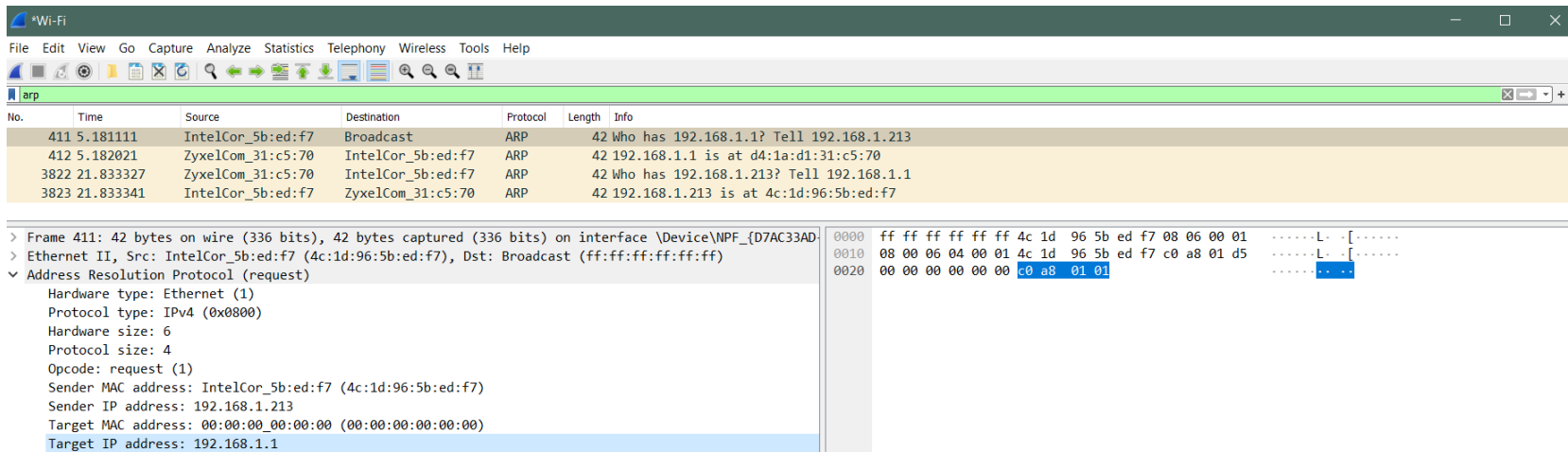
Ethernet II, Src: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7)
 Sender IP address: 192.168.1.213
 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Target IP address: 192.168.1.1

0000 ff ff ff ff ff ff 4c 1d 96 5b ed f7 08 06 00 01L..[.....
 0010 08 00 06 04 00 01 4c 1d 96 5b ed f7 c0 a8 01 d5L..[.....
 0020 00 00 00 00 00 00 c0 a8 01 01L..[.....

- the Ethernet address of the machine whose corresponding IP address is being queried:



Wireshark capture of ARP messages. The packet list shows four ARP packets. Packet 411 is an ARP request from IntelCor_5b:ed:f7 to Broadcast. The packet details pane shows the 'Target IP address: 192.168.1.1' highlighted in blue. The packet bytes pane shows the raw data with the target IP address (c0 a8 01 01) highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
411	5.181111	IntelCor_5b:ed:f7	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.213
412	5.182021	ZyxeCom_31:c5:70	IntelCor_5b:ed:f7	ARP	42	192.168.1.1 is at d4:1a:d1:31:c5:70
3822	21.833327	ZyxeCom_31:c5:70	IntelCor_5b:ed:f7	ARP	42	Who has 192.168.1.213? Tell 192.168.1.1
3823	21.833341	IntelCor_5b:ed:f7	ZyxeCom_31:c5:70	ARP	42	192.168.1.213 is at 4c:1d:96:5b:ed:f7

Frame 411: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D7AC33AD...}

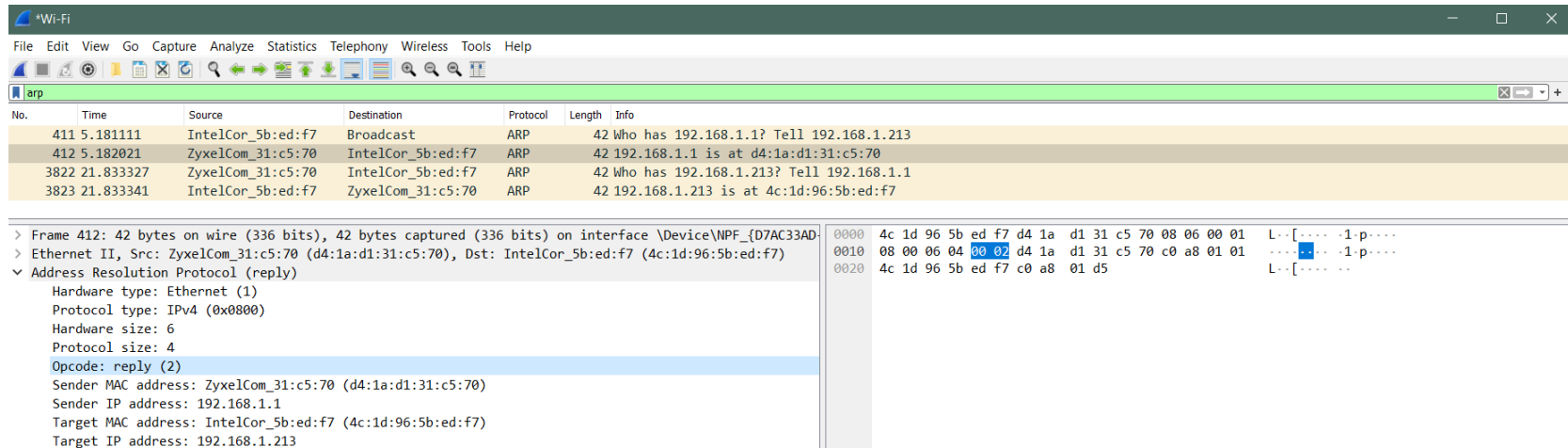
Ethernet II, Src: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

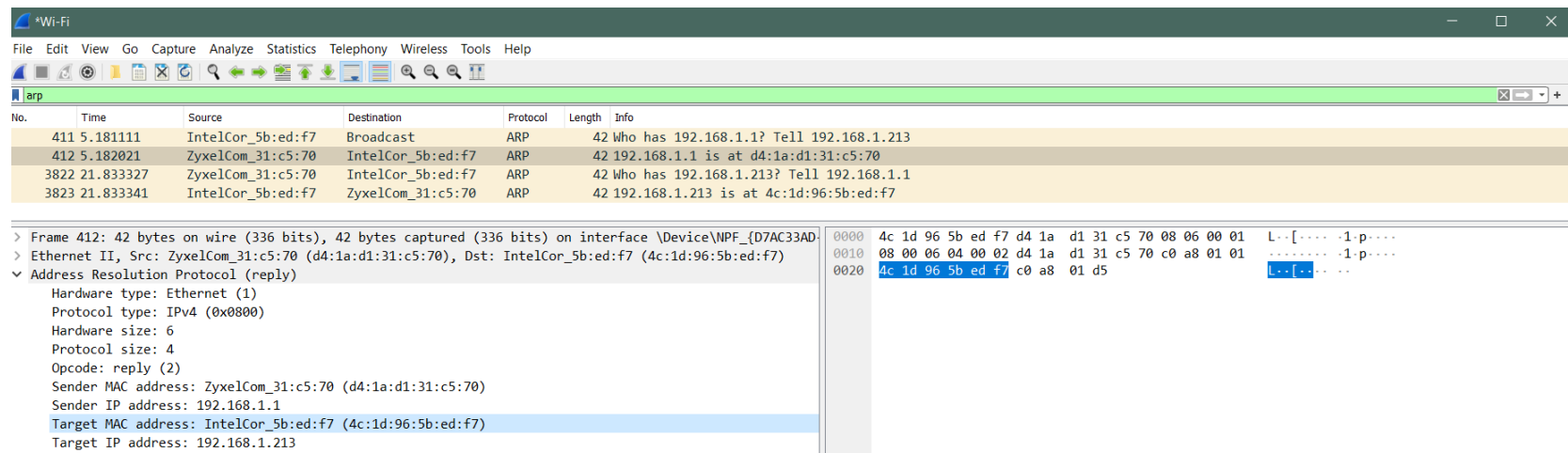
Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7)
 Sender IP address: 192.168.1.213
 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Target IP address: 192.168.1.1

0000 ff ff ff ff ff ff 4c 1d 96 5b ed f7 08 06 00 01L..[.....
 0010 08 00 06 04 00 01 4c 1d 96 5b ed f7 c0 a8 01 d5L..[.....
 0020 00 00 00 00 00 00 c0 a8 01 01L..[.....

- in the ARP reply that was sent in response to the ARP request, the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made:



- the IP address of the machine having the Ethernet address whose corresponding IP address is being queried:



- the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message:

The top screenshot shows the Wireshark interface with the packet list pane displaying four ARP entries. The bottom screenshot shows the packet details pane for frame 412, highlighting the source and destination MAC addresses in the Ethernet II section.

Packet List (Top Screenshot):

No.	Time	Source	Destination	Protocol	Length	Info
411	5.181111	IntelCor_5b:ed:f7	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.213
412	5.182021	ZyxeCom_31:c5:70	IntelCor_5b:ed:f7	ARP	42	192.168.1.1 is at d4:1a:d1:31:c5:70
3822	21.833327	ZyxeCom_31:c5:70	IntelCor_5b:ed:f7	ARP	42	Who has 192.168.1.213? Tell 192.168.1.1
3823	21.833341	IntelCor_5b:ed:f7	ZyxeCom_31:c5:70	ARP	42	192.168.1.213 is at 4c:1d:96:5b:ed:f7

Packet Details (Bottom Screenshot):

Frame 412: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D7AC33AD...}

Ethernet II, Src: ZyxeCom_31:c5:70 (d4:1a:d1:31:c5:70), Dst: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7)

Destination: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7)

Address: IntelCor_5b:ed:f7 (4c:1d:96:5b:ed:f7)

.....0. = LG bit: Globally unique address (factory default)

.....0. = IG bit: Individual address (unicast)

Source: ZyxeCom_31:c5:70 (d4:1a:d1:31:c5:70)

Address: ZyxeCom_31:c5:70 (d4:1a:d1:31:c5:70)

.....0. = LG bit: Globally unique address (factory default)

.....0. = IG bit: Individual address (unicast)

Type: ARP (0x0806)

Address Resolution Protocol (reply)

Hex Dump (Bottom Screenshot):

```

0000  4c 1d 96 5b ed f7 d4 1a d1 31 c5 70 08 06 00 01  L...-1-p...
0010  08 00 06 04 00 02 d4 1a d1 31 c5 70 c0 a8 01 01  .....-1-p...
0020  4c 1d 96 5b ed f7 c0 a8 01 d5  L...-1-p...
    
```