1) Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames and discuss the role of the sender's IP and MAC address in these packets.

ARP stands for **Address Resolution Protocol**. It's a network protocol used to find the **physical address (MAC address)** associated with a given **IP address** on a local network.

ARP Request: If a device (say, the computer) wants to send data to another device on the same local network, it will first check its ARP cache (a list of recently mapped IP addresses to MAC addresses).
If the MAC address isn’t in the cache, it will broadcast an ARP request on the network. This request is essentially asking, "Who has this IP address? Please send me your MAC address!"
ARP Reply: The device with the matching IP address will send back an ARP reply with its MAC address. This reply is not broadcast but sent directly back to the device that made the request.

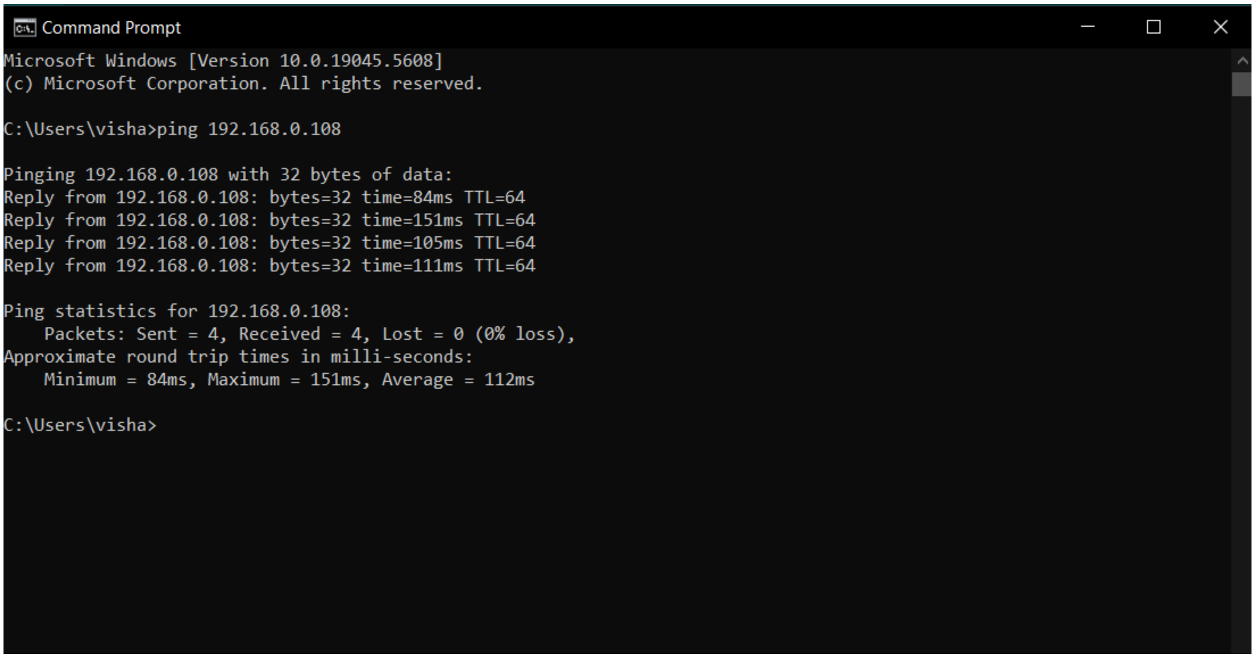
Now, the requesting device has the MAC address and can use it to send data directly to the other device.

An **ARP packet** is the data that is sent during this process. There are two main types:

- **ARP Request Packet** – Sent to ask "Who has this IP?"
- **ARP Reply Packet** – Sent in response with the MAC address.

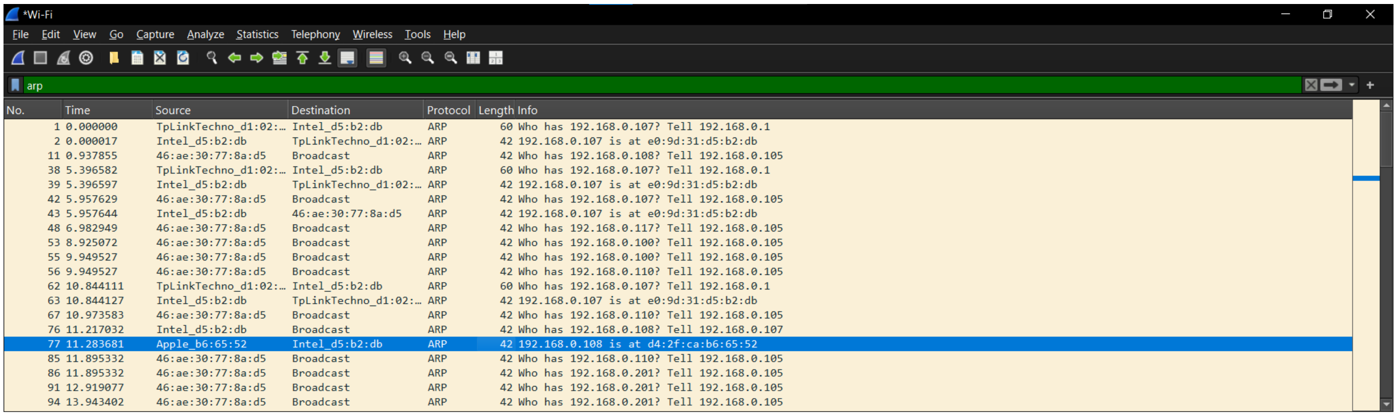
So, here,

Source Device: Laptop (192.168.0.107)
Target Device: Phone (192.168.0.108)



```
Microsoft Windows [Version 10.0.19045.5608]
(c) Microsoft Corporation. All rights reserved.

C:\Users\visha>ping 192.168.0.108

Pinging 192.168.0.108 with 32 bytes of data:
Reply from 192.168.0.108: bytes=32 time=84ms TTL=64
Reply from 192.168.0.108: bytes=32 time=151ms TTL=64
Reply from 192.168.0.108: bytes=32 time=105ms TTL=64
Reply from 192.168.0.108: bytes=32 time=111ms TTL=64

Ping statistics for 192.168.0.108:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 84ms, Maximum = 151ms, Average = 112ms

C:\Users\visha>
```

Filtering ARP in Wireshark

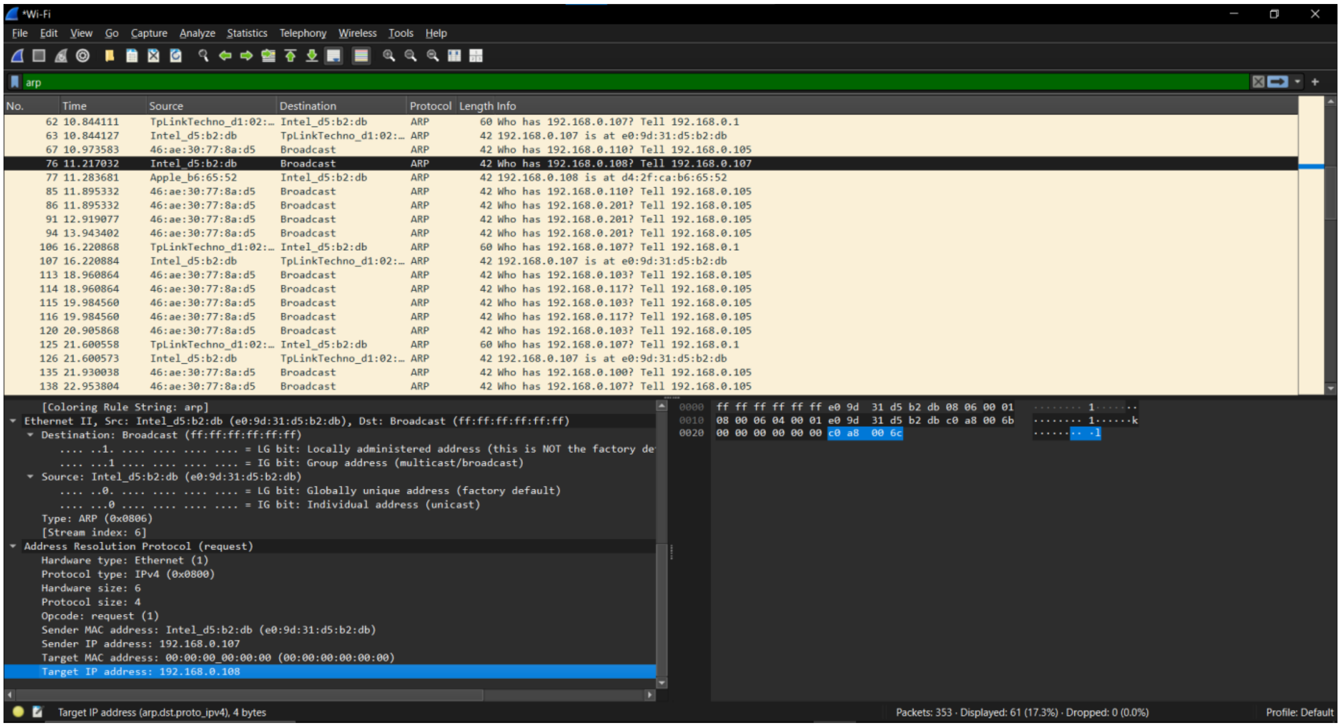


arp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	TpLinkTechno_d1:02:…	Intel_d5:b2:db	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
2	0.000017	Intel_d5:b2:db	TpLinkTechno_d1:02:…	ARP	42	192.168.0.107 is at e0:9d:31:d5:b2:db
11	0.937855	46:ae:30:77:8a:d5	Broadcast	ARP	42	Who has 192.168.0.108? Tell 192.168.0.105
38	5.396582	TpLinkTechno_d1:02:…	Intel_d5:b2:db	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
39	5.396597	Intel_d5:b2:db	TpLinkTechno_d1:02:…	ARP	42	192.168.0.107 is at e0:9d:31:d5:b2:db
42	5.957629	46:ae:30:77:8a:d5	Broadcast	ARP	42	Who has 192.168.0.107? Tell 192.168.0.105
43	5.957644	Intel_d5:b2:db	46:ae:30:77:8a:d5	ARP	42	192.168.0.107 is at e0:9d:31:d5:b2:db
48	6.982949	46:ae:30:77:8a:d5	Broadcast	ARP	42	Who has 192.168.0.117? Tell 192.168.0.105
53	8.925072	46:ae:30:77:8a:d5	Broadcast	ARP	42	Who has 192.168.0.100? Tell 192.168.0.105
55	9.949527	46:ae:30:77:8a:d5	Broadcast	ARP	42	Who has 192.168.0.100? Tell 192.168.0.105
56	9.949527	46:ae:30:77:8a:d5	Broadcast	ARP	42	Who has 192.168.0.110? Tell 192.168.0.105
62	10.844111	TpLinkTechno_d1:02:…	Intel_d5:b2:db	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
63	10.844127	Intel_d5:b2:db	TpLinkTechno_d1:02:…	ARP	42	192.168.0.107 is at e0:9d:31:d5:b2:db
67	10.973583	46:ae:30:77:8a:d5	Broadcast	ARP	42	Who has 192.168.0.110? Tell 192.168.0.105
76	11.217032	Intel_d5:b2:db	Broadcast	ARP	42	Who has 192.168.0.108? Tell 192.168.0.107
77	11.283681	Apple_b6:65:52	Intel_d5:b2:db	ARP	42	192.168.0.108 is at d4:2f:ca:b6:65:52
85	11.895332	46:ae:30:77:8a:d5	Broadcast	ARP	42	Who has 192.168.0.110? Tell 192.168.0.105
86	11.895332	46:ae:30:77:8a:d5	Broadcast	ARP	42	Who has 192.168.0.201? Tell 192.168.0.105
91	12.919077	46:ae:30:77:8a:d5	Broadcast	ARP	42	Who has 192.168.0.201? Tell 192.168.0.105
94	13.943402	46:ae:30:77:8a:d5	Broadcast	ARP	42	Who has 192.168.0.201? Tell 192.168.0.105

ARP Request:

The **target MAC is unknown** (`00:00:00:00:00:00`) because the sender doesn’t know it.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
No.   Time       Source                Destination           Protocol Length Info
   62 10.844111  TpLinkTechno_d1:02:…  Intel_d5:b2:db        ARP      60 Who has 192.168.0.107? Tell 192.168.0.1
   63 10.844127  Intel_d5:b2:db        TpLinkTechno_d1:02:…  ARP      42 192.168.0.107 is at e0:9d:31:d5:b2:db
   67 10.973583  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.110? Tell 192.168.0.105
   76 11.217032  Intel_d5:b2:db        Broadcast             ARP      42 Who has 192.168.0.108? Tell 192.168.0.107
   77 11.283681  Apple_b6:65:52        Intel_d5:b2:db        ARP      42 192.168.0.108 is at d4:2f:ca:b6:65:52
   85 11.895332  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.110? Tell 192.168.0.105
   86 11.895332  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.201? Tell 192.168.0.105
   91 12.919077  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.201? Tell 192.168.0.105
   94 13.943402  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.201? Tell 192.168.0.105
  106 16.220868  TpLinkTechno_d1:02:…  Intel_d5:b2:db        ARP      60 Who has 192.168.0.107? Tell 192.168.0.1
  107 16.220884  Intel_d5:b2:db        TpLinkTechno_d1:02:…  ARP      42 192.168.0.107 is at e0:9d:31:d5:b2:db
  113 18.960864  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.103? Tell 192.168.0.105
  114 18.960864  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.117? Tell 192.168.0.105
  115 19.984560  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.103? Tell 192.168.0.105
  116 19.984560  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.117? Tell 192.168.0.105
  120 20.905868  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.103? Tell 192.168.0.105
  125 21.600558  TpLinkTechno_d1:02:…  Intel_d5:b2:db        ARP      60 Who has 192.168.0.107? Tell 192.168.0.1
  126 21.600573  Intel_d5:b2:db        TpLinkTechno_d1:02:…  ARP      42 192.168.0.107 is at e0:9d:31:d5:b2:db
  135 21.930038  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.100? Tell 192.168.0.105
  138 22.953804  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.107? Tell 192.168.0.105
```

```
    [Coloring Rule String: arp]
▾ Ethernet II, Src: Intel_d5:b2:db (e0:9d:31:d5:b2:db), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▾ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
       .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory de
       .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▾ Source: Intel_d5:b2:db (e0:9d:31:d5:b2:db)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    [Stream index: 6]
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Intel_d5:b2:db (e0:9d:31:d5:b2:db)
    Sender IP address: 192.168.0.107
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.108
```

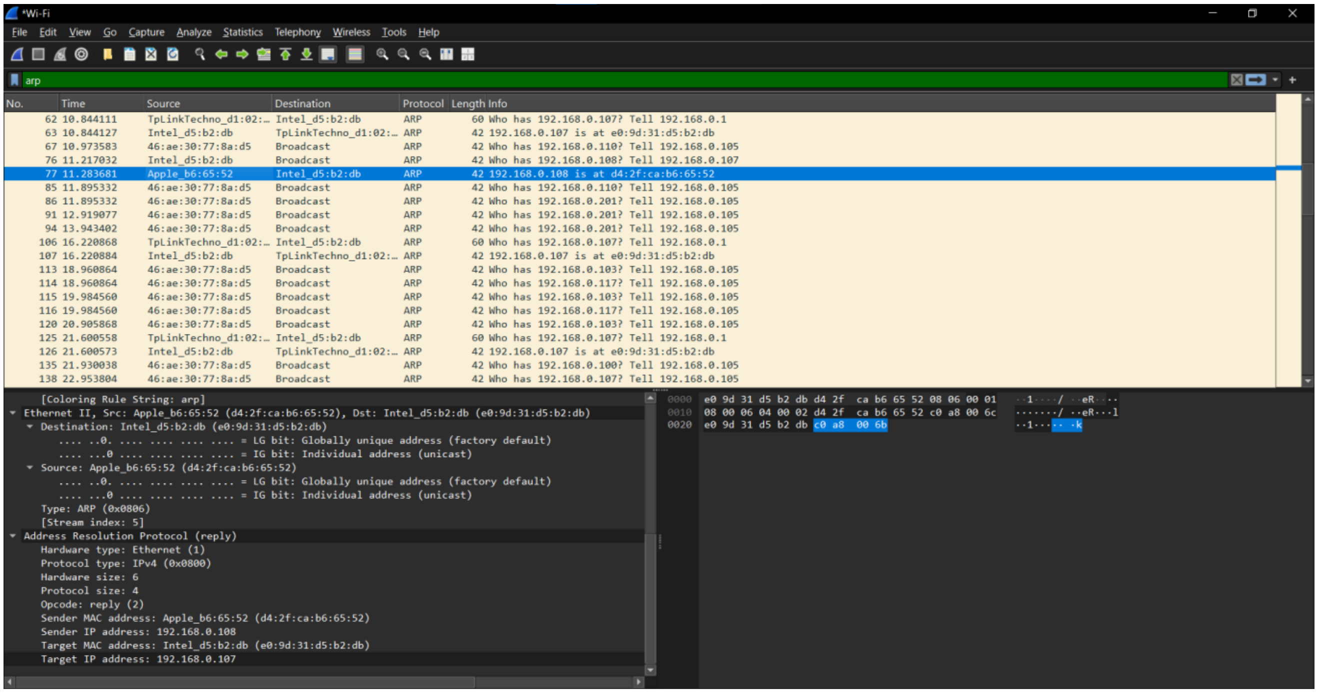
```
0000  ff ff ff ff ff ff e0 9d  31 d5 b2 db 08 06 00 01   ········ 1·······
0010  08 00 06 04 00 01 e0 9d  31 d5 b2 db c0 a8 00 6b   ········ 1······k
0020  00 00 00 00 00 00 c0 a8  00 6c                     ········ ·l
```

Target IP address (arp.dst.proto_ipv4), 4 bytes

Packets: 353 · Displayed: 61 (17.3%) · Dropped: 0 (0.0%)

Profile: Default

ARP Reply:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
No.   Time       Source                Destination           Protocol Length Info
   62 10.844111  TpLinkTechno_d1:02:…  Intel_d5:b2:db        ARP      60 Who has 192.168.0.107? Tell 192.168.0.1
   63 10.844127  Intel_d5:b2:db        TpLinkTechno_d1:02:…  ARP      42 192.168.0.107 is at e0:9d:31:d5:b2:db
   67 10.973583  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.110? Tell 192.168.0.105
   76 11.217032  Intel_d5:b2:db        Broadcast             ARP      42 Who has 192.168.0.108? Tell 192.168.0.107
   77 11.283681  Apple_b6:65:52        Intel_d5:b2:db        ARP      42 192.168.0.108 is at d4:2f:ca:b6:65:52
   85 11.895332  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.110? Tell 192.168.0.105
   86 11.895332  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.201? Tell 192.168.0.105
   91 12.919077  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.201? Tell 192.168.0.105
   94 13.943402  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.201? Tell 192.168.0.105
  106 16.220868  TpLinkTechno_d1:02:…  Intel_d5:b2:db        ARP      60 Who has 192.168.0.107? Tell 192.168.0.1
  107 16.220884  Intel_d5:b2:db        TpLinkTechno_d1:02:…  ARP      42 192.168.0.107 is at e0:9d:31:d5:b2:db
  113 18.960864  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.103? Tell 192.168.0.105
  114 18.960864  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.117? Tell 192.168.0.105
  115 19.984560  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.103? Tell 192.168.0.105
  116 19.984560  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.117? Tell 192.168.0.105
  120 20.905868  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.103? Tell 192.168.0.105
  125 21.600558  TpLinkTechno_d1:02:…  Intel_d5:b2:db        ARP      60 Who has 192.168.0.107? Tell 192.168.0.1
  126 21.600573  Intel_d5:b2:db        TpLinkTechno_d1:02:…  ARP      42 192.168.0.107 is at e0:9d:31:d5:b2:db
  135 21.930038  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.100? Tell 192.168.0.105
  138 22.953804  46:ae:30:77:8a:d5     Broadcast             ARP      42 Who has 192.168.0.107? Tell 192.168.0.105
```

```
    [Coloring Rule String: arp]
▾ Ethernet II, Src: Apple_b6:65:52 (d4:2f:ca:b6:65:52), Dst: Intel_d5:b2:db (e0:9d:31:d5:b2:db)
  ▾ Destination: Intel_d5:b2:db (e0:9d:31:d5:b2:db)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Apple_b6:65:52 (d4:2f:ca:b6:65:52)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    [Stream index: 5]
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Apple_b6:65:52 (d4:2f:ca:b6:65:52)
    Sender IP address: 192.168.0.108
    Target MAC address: Intel_d5:b2:db (e0:9d:31:d5:b2:db)
    Target IP address: 192.168.0.107
```

```
0000  e0 9d 31 d5 b2 db d4 2f  ca b6 65 52 08 06 00 01   ··1····/ ··eR····
0010  08 00 06 04 00 02 d4 2f  ca b6 65 52 c0 a8 00 6c   ·······/ ··eR···l
0020  e0 9d 31 d5 b2 db c0 a8  00 6b                     ··1····· ·k
```

ARP helps devices on a local network find each other’s physical addresses, enabling them to communicate directly and efficiently. Without ARP, devices would have no way to convert IP addresses into MAC addresses, and communication wouldn't be possible.