

1. Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames when your device attempts to find the router's MAC address. Discuss the importance of ARP in packet forwarding.

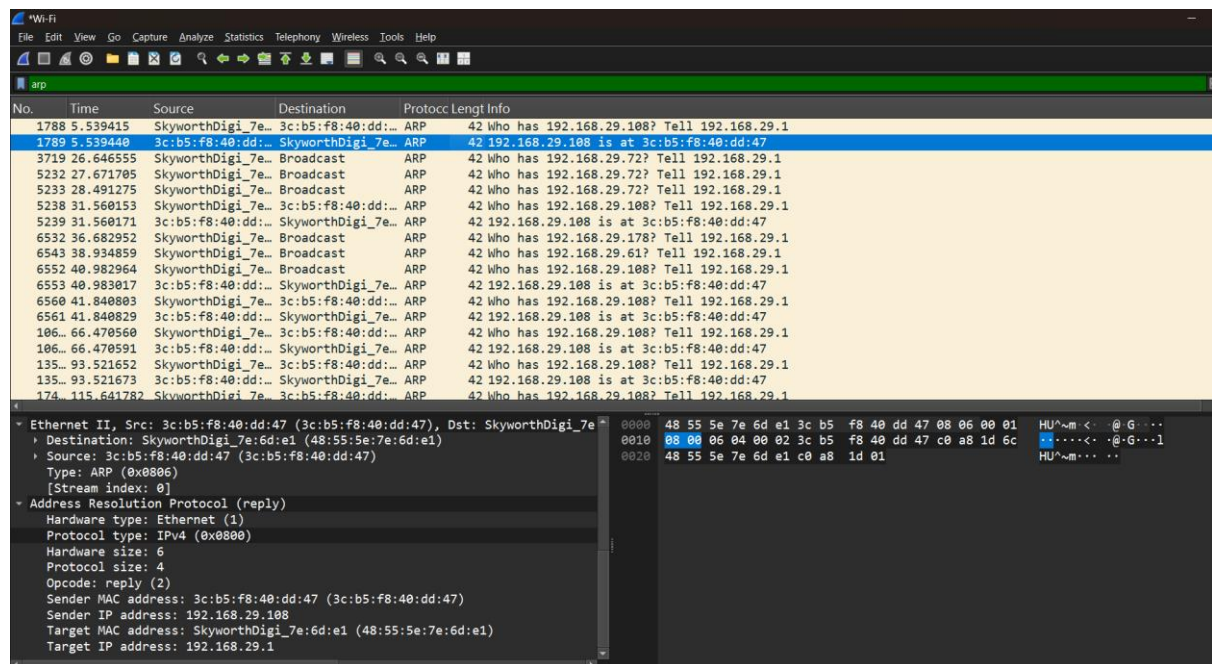
Step 1: sending packets to the router using ping command

```
PS C:\WINDOWS\system32> ping 192.168.29.1

Pinging 192.168.29.1 with 32 bytes of data:
Reply from 192.168.29.1: bytes=32 time=1ms TTL=64
Reply from 192.168.29.1: bytes=32 time=1ms TTL=64
Reply from 192.168.29.1: bytes=32 time=1ms TTL=64
Reply from 192.168.29.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.29.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Step 2: Capturing the Arp packets



The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets, with ARP packets highlighted. The middle pane shows the details of the selected ARP packet (No. 1789), including the Ethernet II header, Internet Protocol (IPv4) header, and Address Resolution Protocol (ARP) details. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1788	5.539415	SkyworthDigi_7e...	3c:b5:f8:40:dd:...	ARP	42	Who has 192.168.29.108? Tell 192.168.29.1
1789	5.539440	3c:b5:f8:40:dd:...	SkyworthDigi_7e...	ARP	42	192.168.29.108 is at 3c:b5:f8:40:dd:47
3719	26.646555	SkyworthDigi_7e...	Broadcast	ARP	42	Who has 192.168.29.72? Tell 192.168.29.1
5232	27.671705	SkyworthDigi_7e...	Broadcast	ARP	42	Who has 192.168.29.72? Tell 192.168.29.1
5233	28.491275	SkyworthDigi_7e...	Broadcast	ARP	42	Who has 192.168.29.72? Tell 192.168.29.1
5238	31.560153	SkyworthDigi_7e...	3c:b5:f8:40:dd:...	ARP	42	Who has 192.168.29.108? Tell 192.168.29.1
5239	31.560171	3c:b5:f8:40:dd:...	SkyworthDigi_7e...	ARP	42	192.168.29.108 is at 3c:b5:f8:40:dd:47
6532	36.682952	SkyworthDigi_7e...	Broadcast	ARP	42	Who has 192.168.29.178? Tell 192.168.29.1
6543	38.934859	SkyworthDigi_7e...	Broadcast	ARP	42	Who has 192.168.29.61? Tell 192.168.29.1
6552	40.982964	SkyworthDigi_7e...	Broadcast	ARP	42	Who has 192.168.29.108? Tell 192.168.29.1
6553	40.983017	3c:b5:f8:40:dd:...	SkyworthDigi_7e...	ARP	42	192.168.29.108 is at 3c:b5:f8:40:dd:47
6560	41.840803	SkyworthDigi_7e...	3c:b5:f8:40:dd:...	ARP	42	Who has 192.168.29.108? Tell 192.168.29.1
6561	41.840829	3c:b5:f8:40:dd:...	SkyworthDigi_7e...	ARP	42	192.168.29.108 is at 3c:b5:f8:40:dd:47
106...	66.470560	SkyworthDigi_7e...	3c:b5:f8:40:dd:...	ARP	42	Who has 192.168.29.108? Tell 192.168.29.1
106...	66.470591	3c:b5:f8:40:dd:...	SkyworthDigi_7e...	ARP	42	192.168.29.108 is at 3c:b5:f8:40:dd:47
135...	93.521652	SkyworthDigi_7e...	3c:b5:f8:40:dd:...	ARP	42	Who has 192.168.29.108? Tell 192.168.29.1
135...	93.521673	3c:b5:f8:40:dd:...	SkyworthDigi_7e...	ARP	42	192.168.29.108 is at 3c:b5:f8:40:dd:47
174	115.641782	SkyworthDigi_7e...	3c:b5:f8:40:dd:...	ARP	42	Who has 192.168.29.108? Tell 192.168.29.1

Ethernet II, Src: 3c:b5:f8:40:dd:47 (3c:b5:f8:40:dd:47), Dst: SkyworthDigi_7e...
Destination: SkyworthDigi_7e:6d:e1 (48:55:5e:7e:6d:e1)
Source: 3c:b5:f8:40:dd:47 (3c:b5:f8:40:dd:47)
Type: ARP (0x0806)
[Stream index: 0]
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: 3c:b5:f8:40:dd:47 (3c:b5:f8:40:dd:47)
Sender IP address: 192.168.29.108
Target MAC address: SkyworthDigi_7e:6d:e1 (48:55:5e:7e:6d:e1)
Target IP address: 192.168.29.1

Step 3: Analyzing the arp reply packets from the router which contains mac address of router

```
[Coloring Rule String: arp]
Ethernet II, Src: 3c:b5:f8:40:dd:47 (3c:b5:f8:40:dd:47), Dst: SkyworthDigi_7e
  Destination: SkyworthDigi_7e:6d:e1 (48:55:5e:7e:6d:e1)
  Source: 3c:b5:f8:40:dd:47 (3c:b5:f8:40:dd:47)
  Type: ARP (0x0806)
[Stream index: 0]
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: 3c:b5:f8:40:dd:47 (3c:b5:f8:40:dd:47)
  Sender IP address: 192.168.29.108
  Target MAC address: SkyworthDigi_7e:6d:e1 (48:55:5e:7e:6d:e1)
  Target IP address: 192.168.29.1
```



```
Frame 1789: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
  Section number: 1
  Interface id: 0 (\Device\NPF_{9CEA6653-53CB-431F-8BEC-C93FB4F81BAF})
  Encapsulation type: Ethernet (1)
  Arrival Time: Mar 12, 2025 13:32:43.370837000 India Standard Time
  UTC Arrival Time: Mar 12, 2025 08:02:43.370837000 UTC
  Epoch Arrival Time: 1741766563.370837000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000025000 seconds]
  [Time delta from previous displayed frame: 0.000025000 seconds]
  [Time since reference or first frame: 5.539440000 seconds]
  Frame Number: 1789
  Frame Length: 42 bytes (336 bits)
  Capture Length: 42 bytes (336 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:arp]
  [Coloring Rule Name: ARP]
  [Coloring Rule String: arp]
Ethernet II, Src: 3c:b5:f8:40:dd:47 (3c:b5:f8:40:dd:47), Dst: SkyworthDigi_7e
  Destination: SkyworthDigi_7e:6d:e1 (48:55:5e:7e:6d:e1)
  Source: 3c:b5:f8:40:dd:47 (3c:b5:f8:40:dd:47)
  Type: ARP (0x0806)
[Stream index: 0]
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: 3c:b5:f8:40:dd:47 (3c:b5:f8:40:dd:47)
  Sender IP address: 192.168.29.108
```

0000	48 55 5e 7e 6d e1 3c b5 f8 40 dd 47 08 06 00 01	HU^~m < @ G ...
0010	08 00 06 04 00 02 3c b5 f8 40 dd 47 c0 a8 1d 6c< @ G ...1
0020	48 55 5e 7e 6d e1 c0 a8 1d 01	HU^~m! ..

Step 3: Importance of ARP in Packet Forwarding

- **Address Resolution:** Maps IP addresses to MAC addresses for network communication.
- **Local Network Communication:** Essential for devices to send packets within a LAN.
- **Packet Forwarding:** Ensures that packets reach the correct MAC address before being transmitted over Ethernet.
- **Security Concerns:** ARP spoofing can lead to **Man-in-the-Middle (MITM) attack**