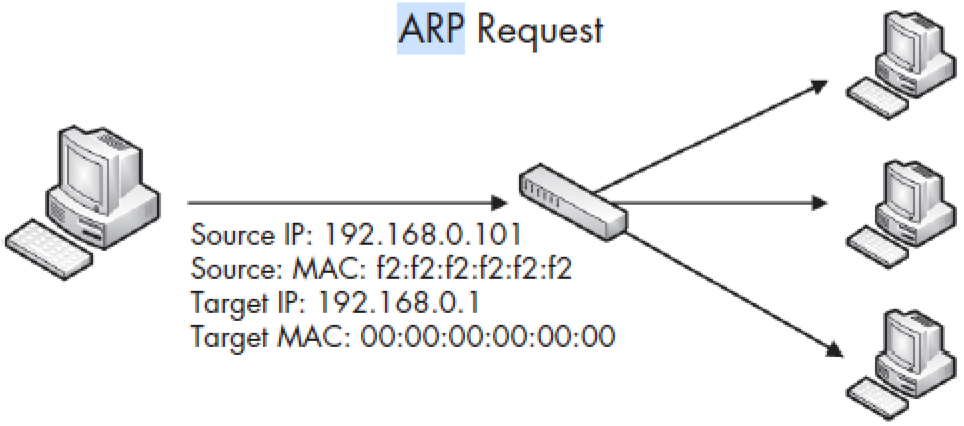
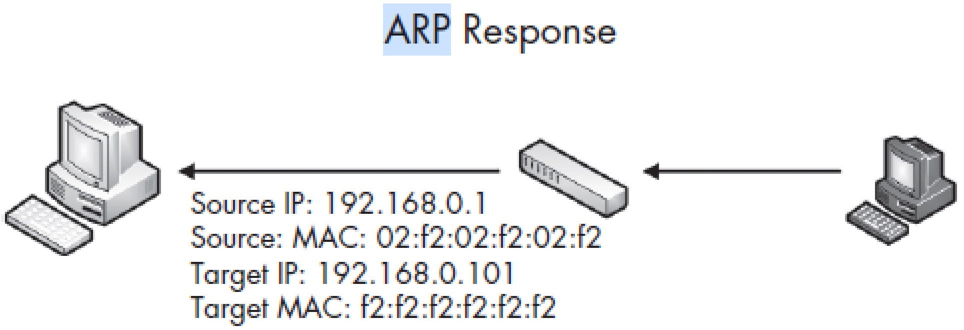
How it work Address Resolution Protocol

The resolution process that TCP/IP networking (with IPv4) uses to resolve an IP address to a MAC address is called the *Address Resolution Protocol (ARP)*, which is defined in RFC 826. The ARP resolution process uses only two packets



Source IP: 192.168.0.101
Source: MAC: f2:f2:f2:f2:f2:f2
Target IP: 192.168.0.1
Target MAC: 00:00:00:00:00:00

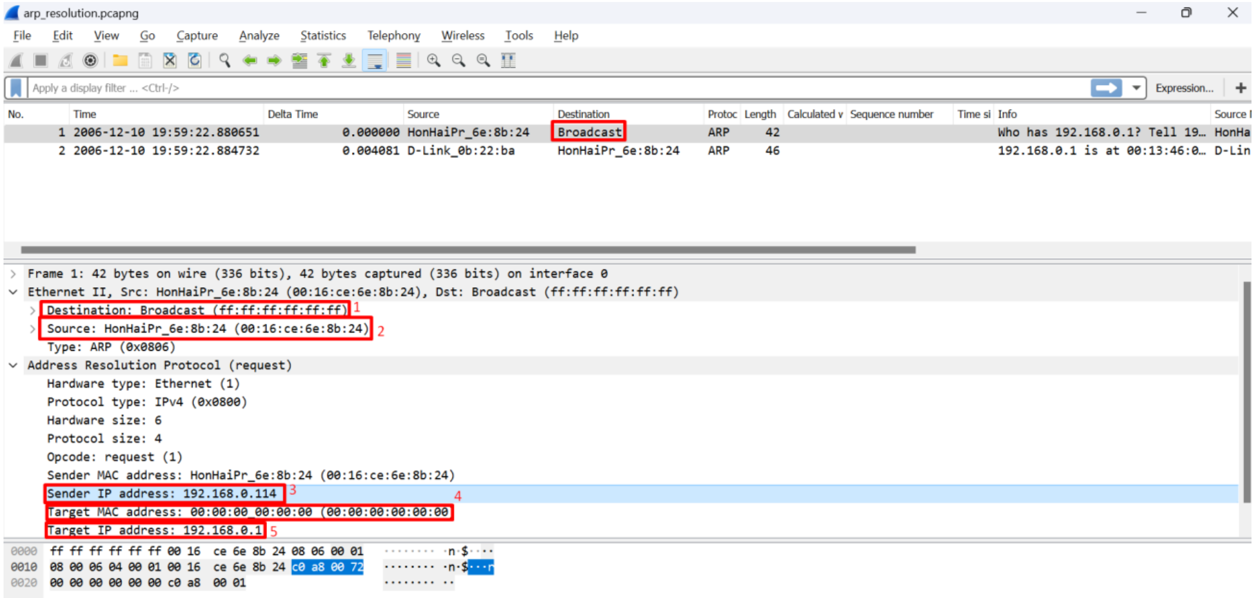


Source IP: 192.168.0.1
Source: MAC: 02:f2:02:f2:02:f2
Target IP: 192.168.0.101
Target MAC: f2:f2:f2:f2:f2:f2

You can verify the ARP table of a Windows host by typing ***arp –a*** *from a command prompt.*

Packet 1: ARP Request

We can see first packet is broadcast type of ARP.



```
No.   Time                         Delta Time  Source              Destination         Protoc Length Calculated v Sequence number Time si Info                              Source I
    1 2006-12-10 19:59:22.880651   0.000000 HonHaiPr_6e:8b:24   Broadcast           ARP      42                                     Who has 192.168.0.1? Tell 19…     HonHa
    2 2006-12-10 19:59:22.884732   0.004081 D-Link_0b:22:ba     HonHaiPr_6e:8b:24   ARP      46                                     192.168.0.1 is at 00:13:46:0…     D-Lin
```

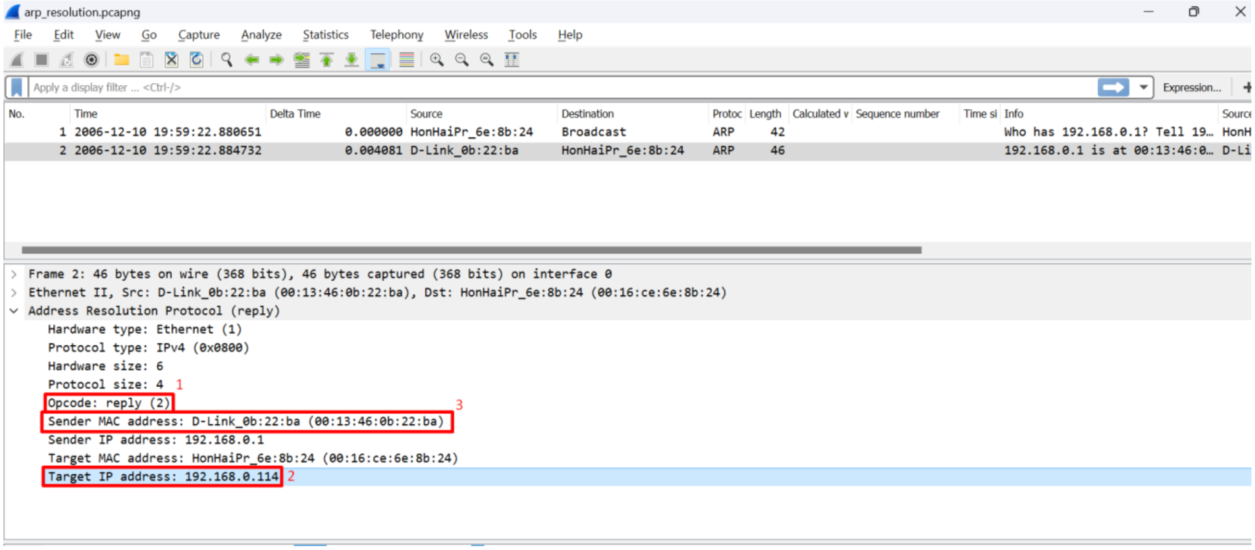
```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
v Ethernet II, Src: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24)
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24)
    Sender IP address: 192.168.0.114
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.1
```

```
0000  ff ff ff ff ff ff 00 16  ce 6e 8b 24 08 06 00 01   ········ ·n·$····
0010  08 00 06 04 00 01 00 16  ce 6e 8b 24 c0 a8 00 72   ········ ·n·$···r
0020  00 00 00 00 00 00 c0 a8  00 01                     ········ ··
```

1. The packet’s destination address is ff:ff:ff:ff:ff:ff .
2. Source address mac 00:16:ce:6e:8b:24
3. Sender ip is source pc ip address (192.168.0.114)
4. Target Mac address (00:00:00:00:00:00)
5. Targe ip address is gate way ip address (192.168.0.1)

Packet 2: ARP Response

Arp response packet will few changes as per below packet analysis



```
No.   Time                        Delta Time  Source             Destination        Protoc Length Calculated v Sequence number Time si Info                              Source
    1 2006-12-10 19:59:22.880651    0.000000  HonHaiPr_6e:8b:24  Broadcast          ARP       42                                   Who has 192.168.0.1? Tell 19…     HonH
    2 2006-12-10 19:59:22.884732    0.004081  D-Link_0b:22:ba    HonHaiPr_6e:8b:24  ARP       46                                   192.168.0.1 is at 00:13:46:0…     D-Li
```

```
> Frame 2: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface 0
> Ethernet II, Src: D-Link_0b:22:ba (00:13:46:0b:22:ba), Dst: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: D-Link_0b:22:ba (00:13:46:0b:22:ba)
    Sender IP address: 192.168.0.1
    Target MAC address: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24)
    Target IP address: 192.168.0.114
```

1. Opcode reply (2)
2. Target back to Source user pc (192.168.0.114)
3. Sender mac address ((00:13:46:0b:22:ba)

Reference Guide book : PRACTICAL PACKET ANALYSIS by CHRIS SANDERS