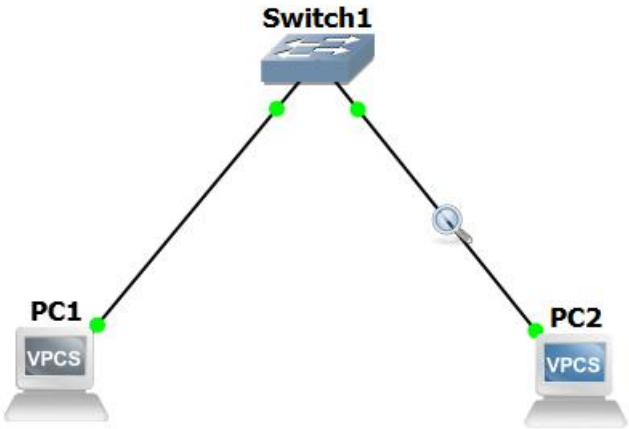
Q2. Capture and analyze Ethernet frames using Wireshark. Inspect the structure of the frame, including destination and source MAC addresses, Ethertype, payload, and FCS Use GNS3 or Packet Tracer to simulate network traffic.

Using GNS3



PC1 PC2

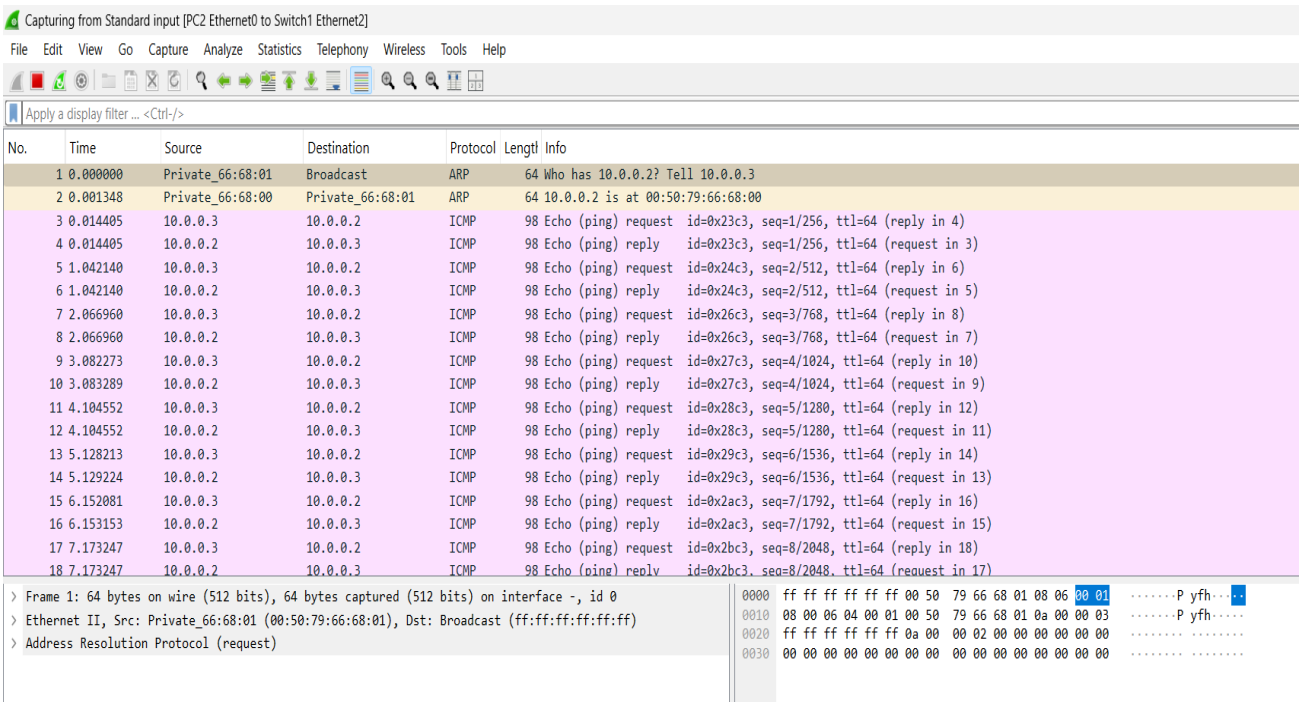
```
PC2>
PC2> ip 10.0.0.2 255.0.0.0 10.0.0.1
Checking for duplicate address...
10.0.0.2 is being used by MAC 00:50:79:66:68:00
Address not changed

PC2> ip 10.0.0.3 255.0.0.0 10.0.0.1
Checking for duplicate address...
PC1 : 10.0.0.3 255.0.0.0 gateway 10.0.0.1

PC2> ping 10.0.0.2
84 bytes from 10.0.0.2 icmp_seq=1 ttl=64 time=1.816 ms
84 bytes from 10.0.0.2 icmp_seq=2 ttl=64 time=1.156 ms
84 bytes from 10.0.0.2 icmp_seq=3 ttl=64 time=1.018 ms
84 bytes from 10.0.0.2 icmp_seq=4 ttl=64 time=1.162 ms
84 bytes from 10.0.0.2 icmp_seq=5 ttl=64 time=7.038 ms

PC2> ping 10.0.0.2 -t
84 bytes from 10.0.0.2 icmp_seq=1 ttl=64 time=1.182 ms
84 bytes from 10.0.0.2 icmp_seq=2 ttl=64 time=1.074 ms
84 bytes from 10.0.0.2 icmp_seq=3 ttl=64 time=1.231 ms
84 bytes from 10.0.0.2 icmp_seq=4 ttl=64 time=1.210 ms
84 bytes from 10.0.0.2 icmp_seq=5 ttl=64 time=1.115 ms
84 bytes from 10.0.0.2 icmp_seq=6 ttl=64 time=1.086 ms
```

Analysing Ethernet frames using Wireshark



Destination MAC Address

- Value: ff:ff:ff:ff:ff:ff

Source MAC Address

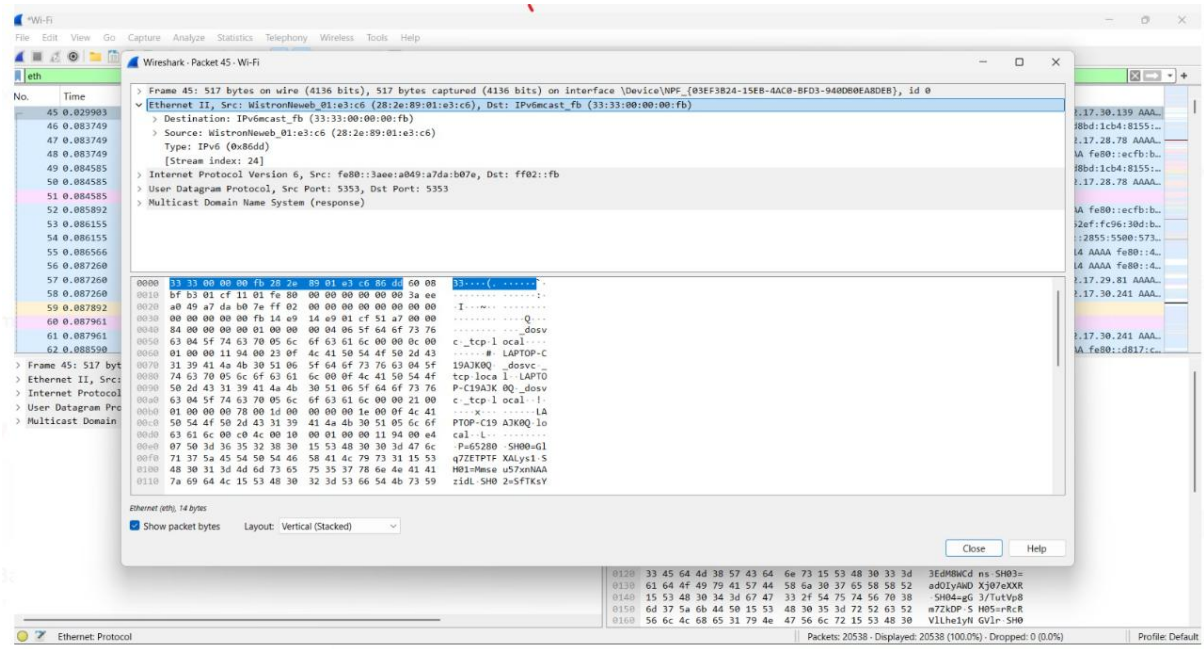
- Value: 00:50:79:66:68:01

Ethertype

- Value: 0x0806

Payload (Data Inside the Frame)

- This contains the ARP request:
    - Sender IP: 10.0.0.3
    - Sender MAC: 00:50:79:66:68:01



Ethernet frame details:

1. Destination MAC Address

MAC Address: 33:33:00:00:00:fb

2. Source MAC Address

MAC Address: 28:2e:89:01:e3:c6

3. Ethertype

Value: 0x86dd (payload contains an IPv6 packet)

4. Payload

Source IP: fe80::3aee

Destination IP: ff02::fb

Protocol: UDP

Source Port: 5353

Destination Port: 5353