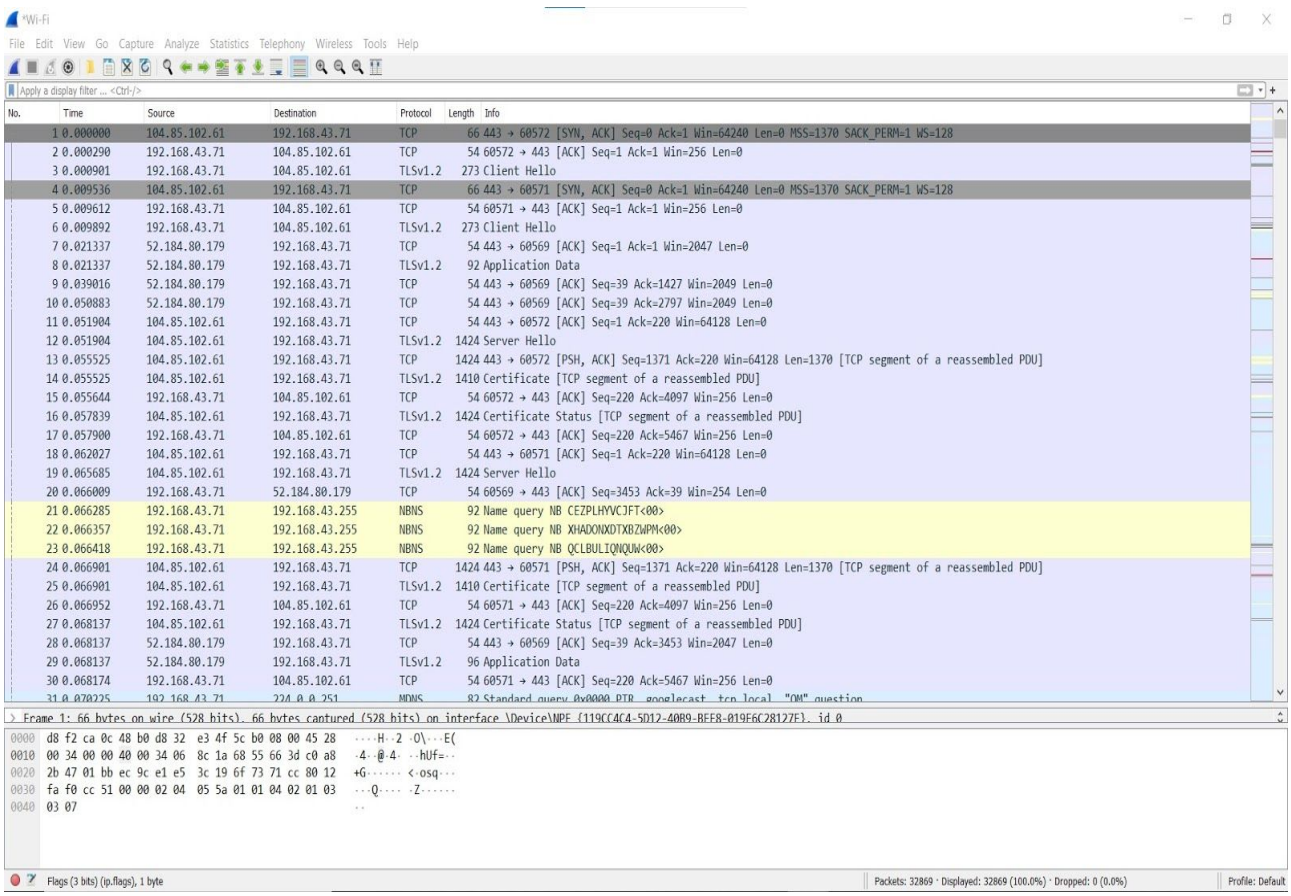
Networks Lab Experiment-2

Singam Sai Bala Subrahmanyam
B180522CS



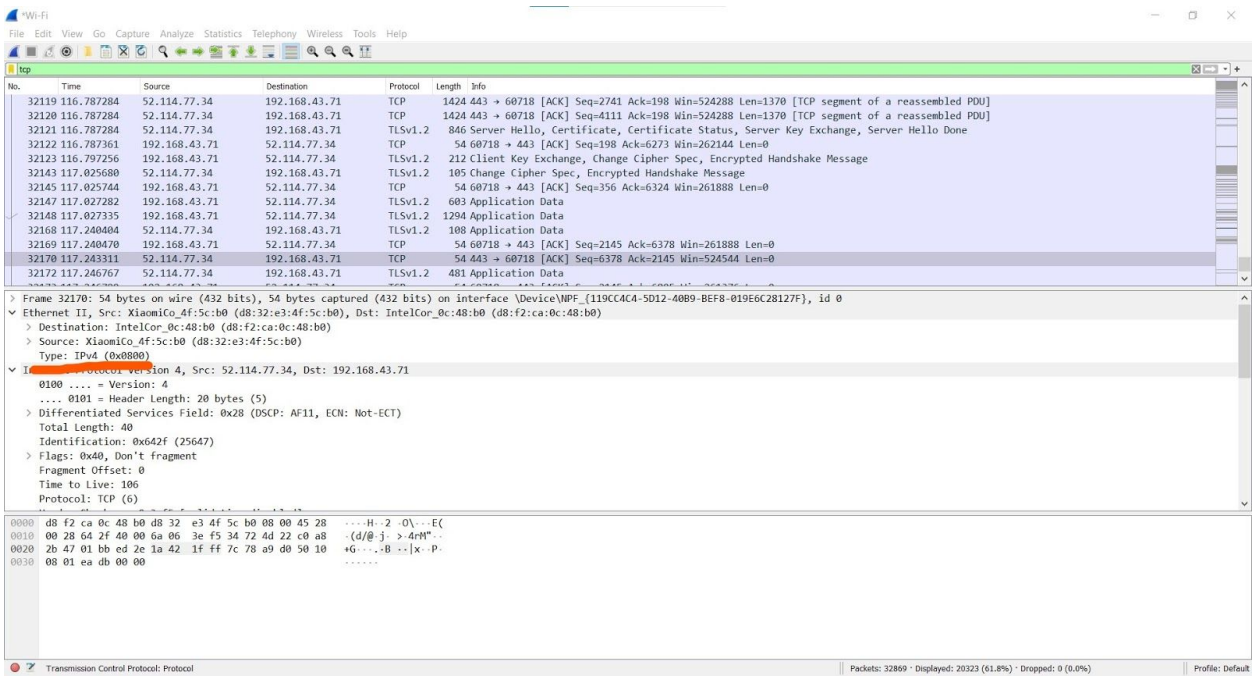
Capturing packets using wireshark for 5 seconds.

a. **For an IP and ARP packet, compare the MAC header of these two packets and find the protocol ID for ARP and IP, if exists.**

Each Ethernet frame starts with an Ethernet header or MAC header. The header features destination and source MAC addresses (each six octets in length), the EtherType field. A MAC address is a hardware identification number that uniquely identifies each device on a network. MAC addresses function at the data link layer (layer 2 in the OSI model).

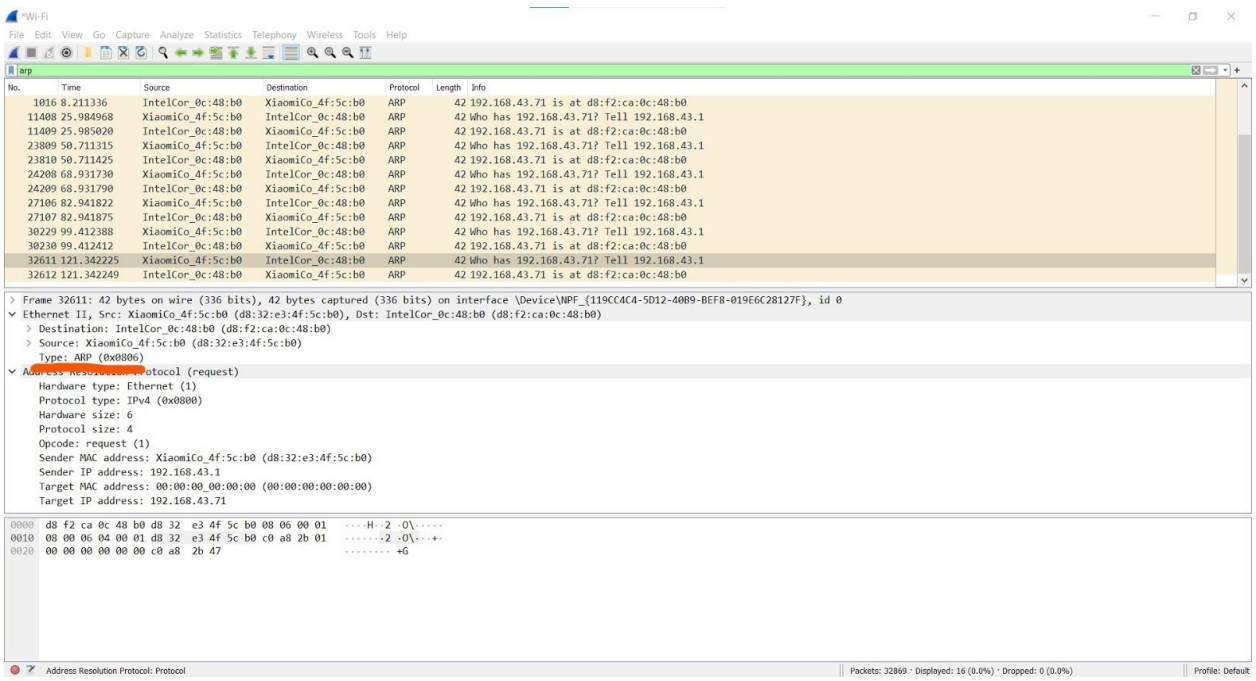
Both IP and ARP packet's MAC header contains

a. Source MAC address
b. Destination MAC address
c. Ether type



IP packet mac header contains:

1. Source MAC address: IntelCor_0c:48:b0 (d8:f2:ca:0c:48:b0)
2. Destination MAC address: XiaomiCo_4f:5c:b0 (d8:32:e3:4f:5c:b0)
3. Type: IPv4 (***Protocol ID: 0x0800***)



ARP packet mac header contains:

4. Source MAC address: IntelCor_0c:48:b0 (d8:f2:ca:0c:48:b0)
1. Destination MAC address: XiaomiCo_4f:5c:b0 (d8:32:e3:4f:5c:b0)
2. Type: ARP (***Protocol ID: 0x0806***)

b. Is the destination address of the ARP packet a broadcast address or a unicast address?

Address Resolution Protocol (ARP) is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area network (LAN). The physical machine address is also known as a Media Access Control or MAC address.

The job of the ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice-versa. This is necessary because an IP address is 32-bits long, but MAC addresses are 48-bits long.

ARP works between network layers 2 and 3 of OSI model. The MAC address exists on layer 2 of the OSI model, the data link layer, while the IP address exists on layer 3, the network layer.

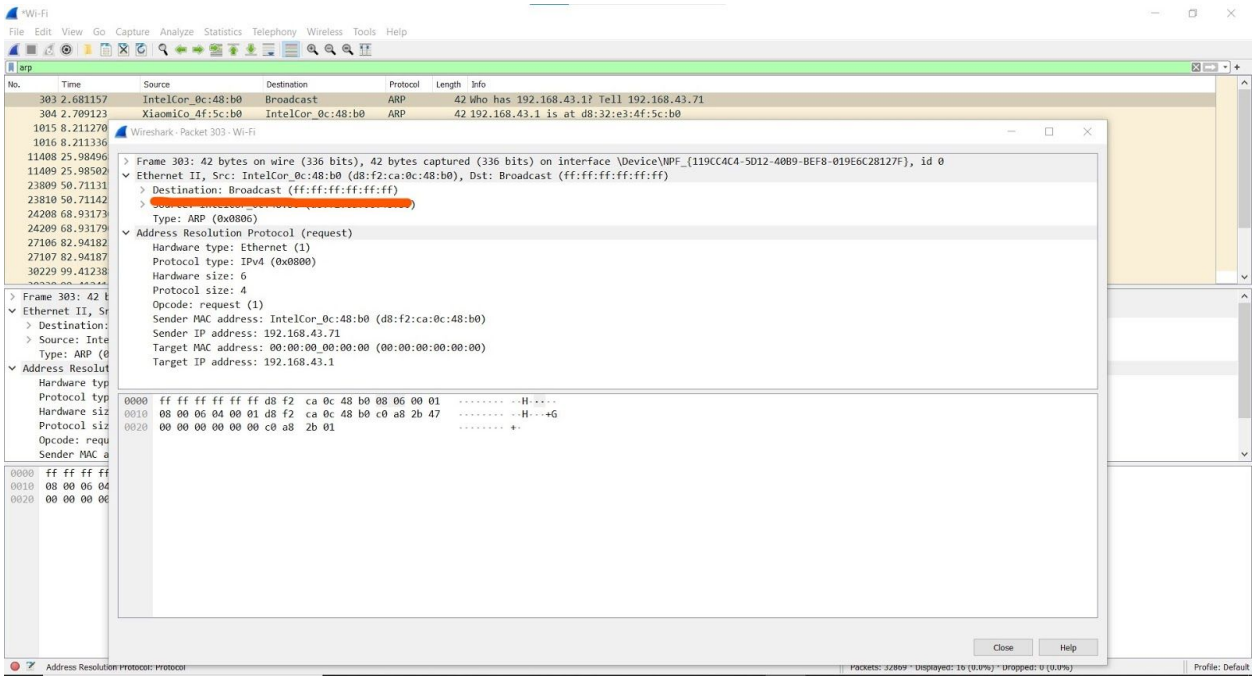
All operating systems in an IPv4 Ethernet network keep an ARP cache. Every time a host requests a MAC address in order to send a packet to another host in the LAN, it checks its ARP cache to see if the IP to MAC address translation already exists. If it does, then a new ARP request is unnecessary. If the translation does not already exist, then the request for network addresses is sent and ARP is performed.

ARP broadcasts a request packet to all the machines on the LAN and asks if any of the machines know they are using that particular IP address. When a machine recognizes the IP address as its own, it sends a reply so ARP can update the cache for future reference and proceed with the communication.

Types of ARP packets:

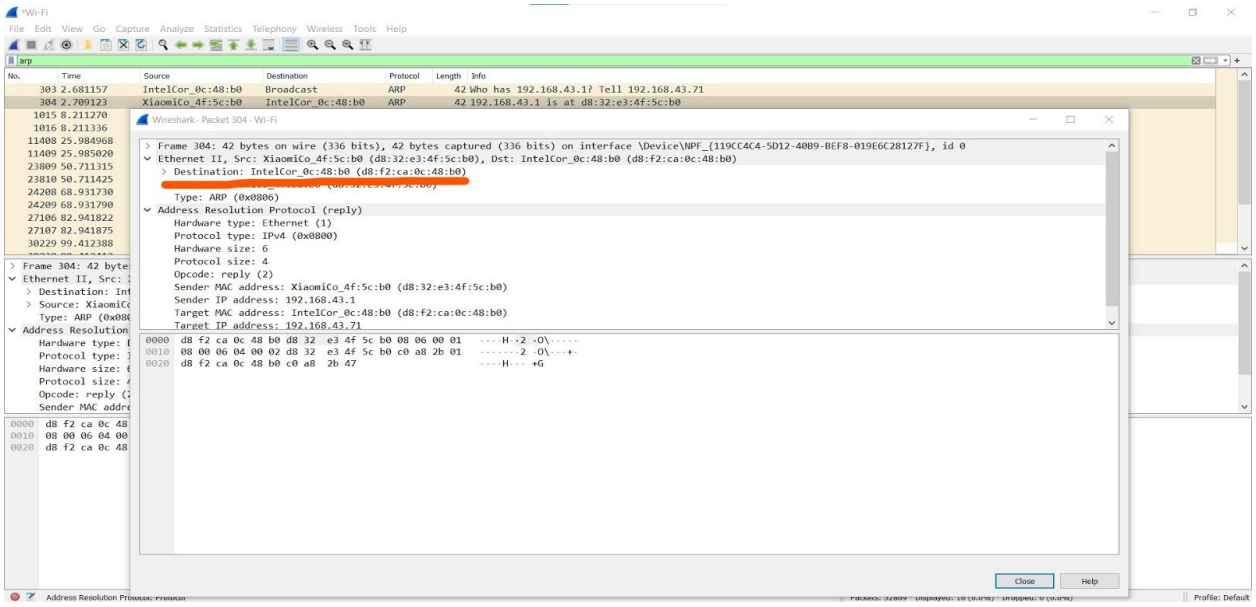
a. ARP Request packets
b. ARP Reply packets

a. ARP Request packet



Destination address of ARP Request packet is a broadcast address since the packet is broadcasted to all machines in local area network asking if any of them has the particular IP address.

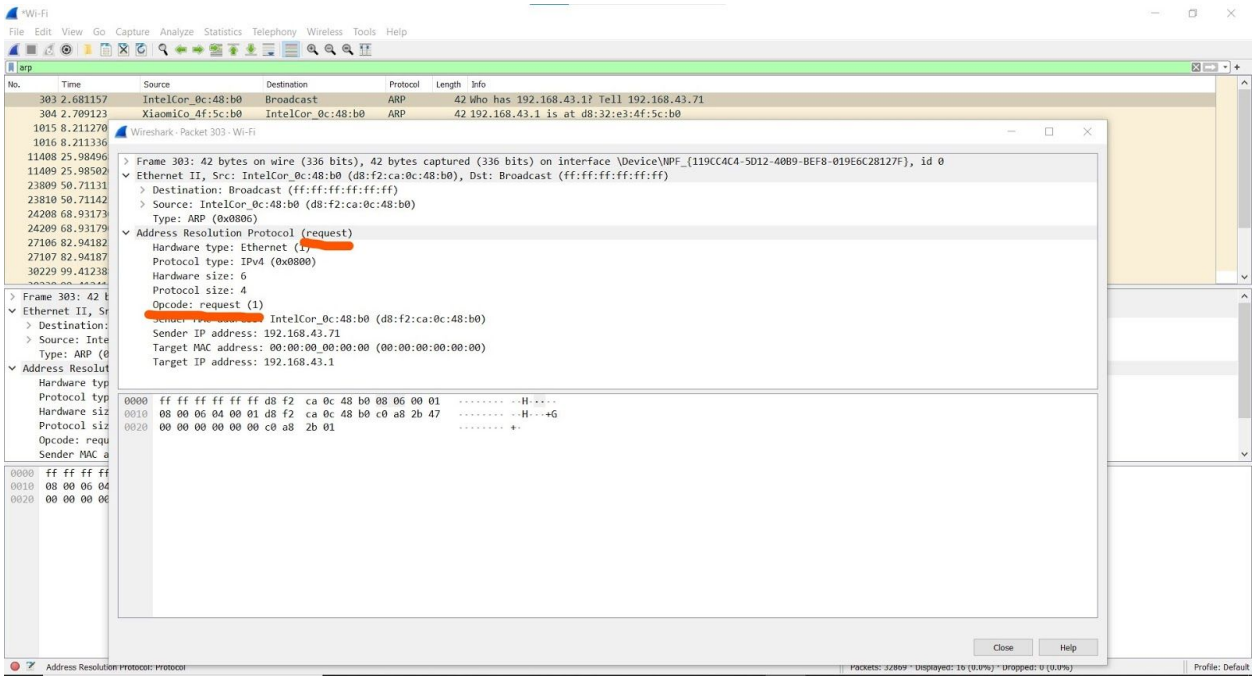
b. ARP Reply packet



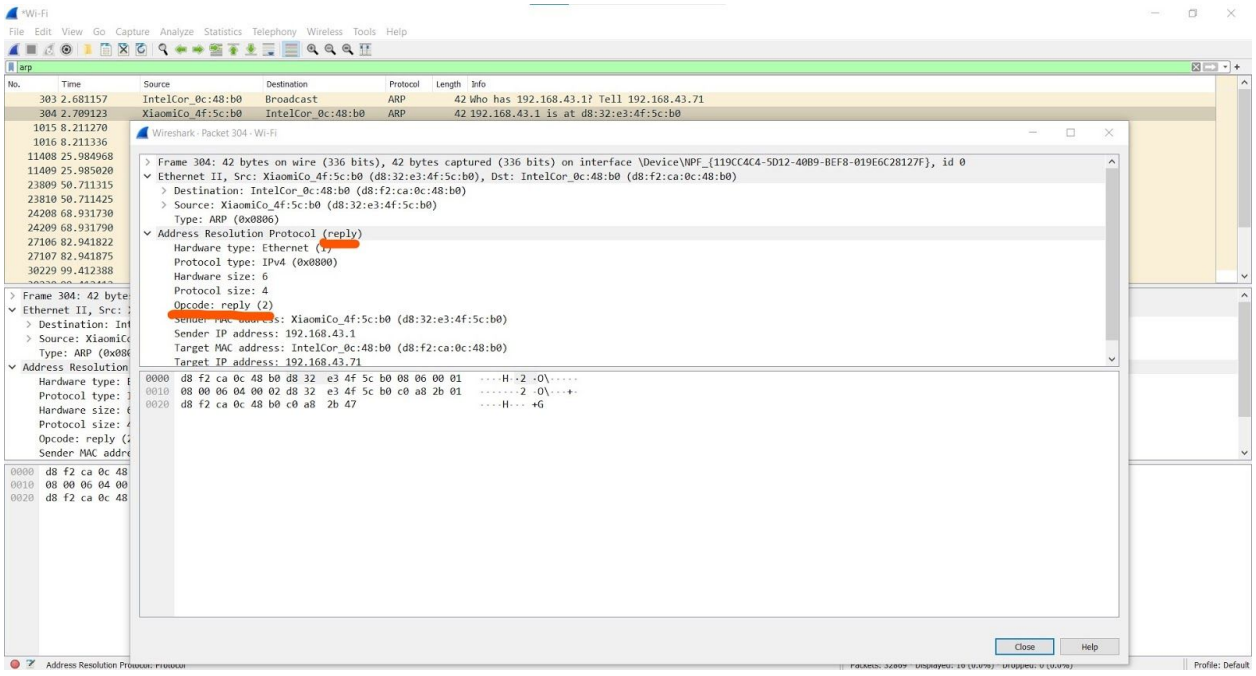
Destination address of ARP Reply packet is a unicast address as the destination will be the broadcasted source of ARP request.

c. Is the ARP packet a request or reply packet? Justify

ARP packets are of two types i.e ARP Request packets and ARP Reply packets. The opcode in the ARP field specifies the type of packet.



ARP Request packet



ARP Reply packet

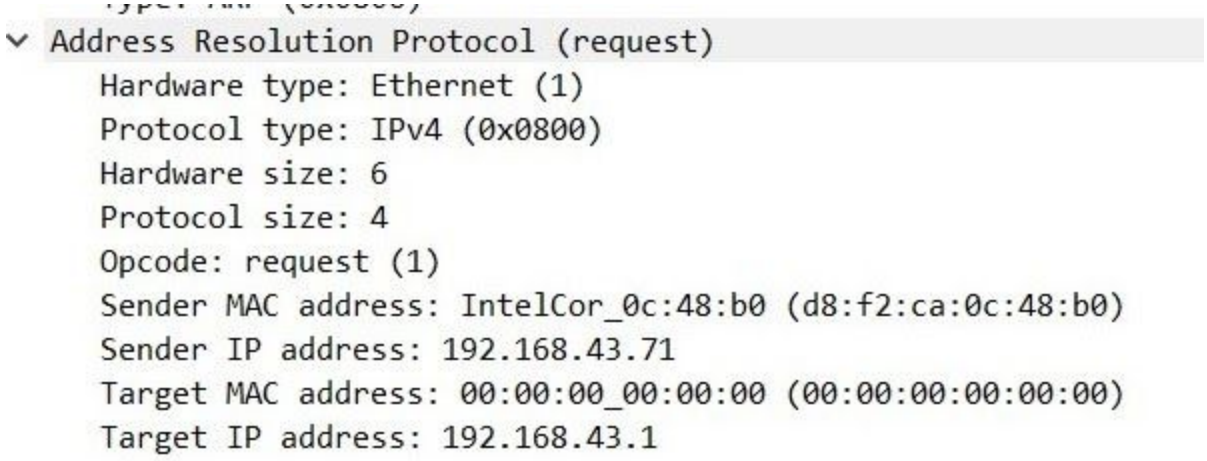
ARP request packets are broadcasted from the source to all the machines in a local area network in search of a machine with a particular IP address.

Whereas ARP reply packets are sent by the machine with particular IP sending its MAC address to the requested source address.

d. Examine the payload of the packet.

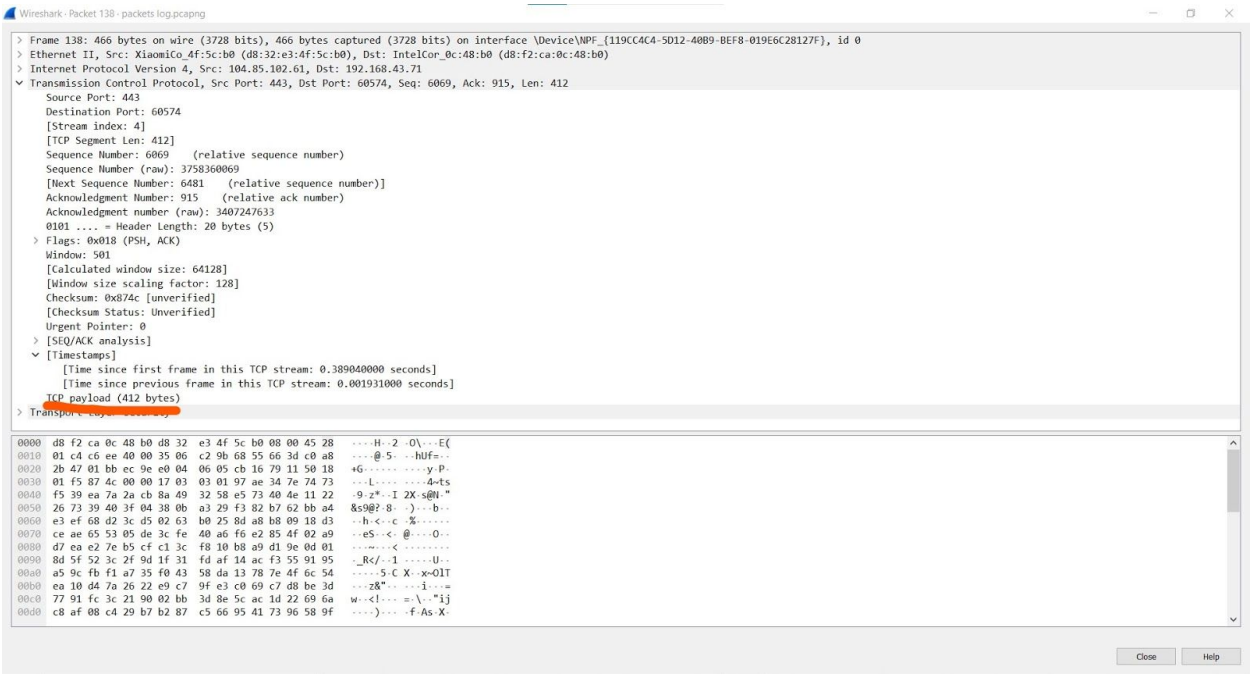
ARP header consists of

a. Hardware type
b. Hardware size
c. Protocol type
d. Protocol size
e. Opcode
f. Sender MAC address
g. Sender IP address
h. Target MAC address
i. Target IP address

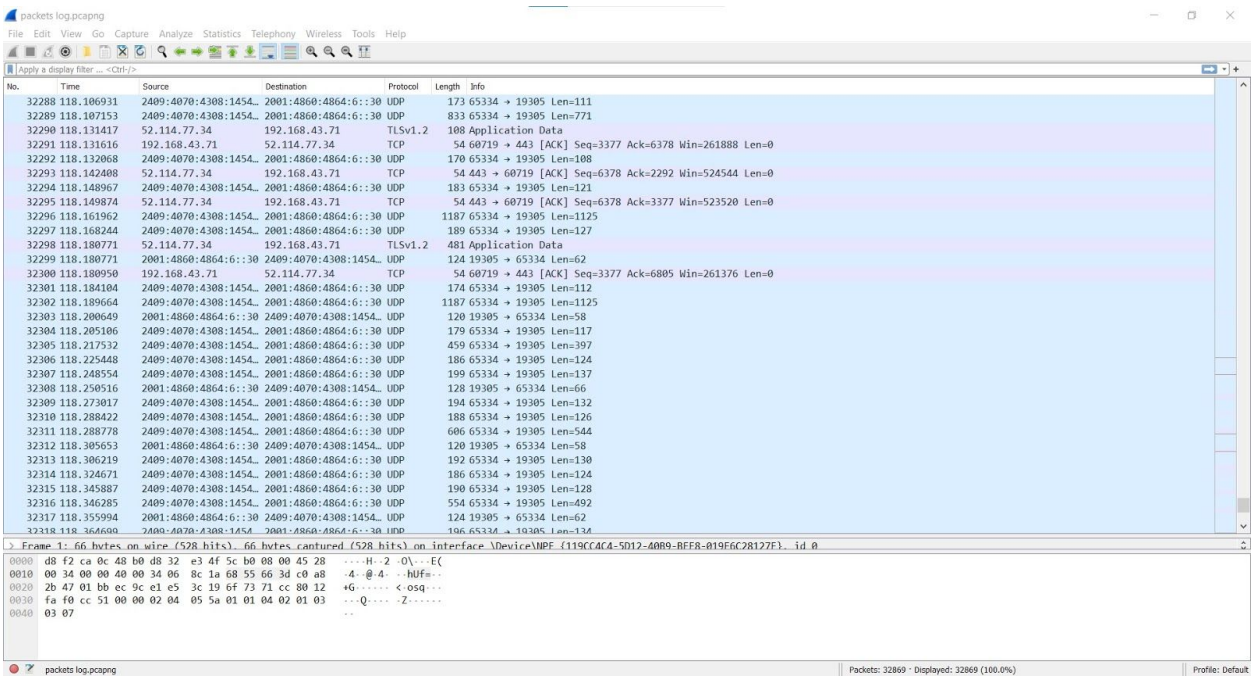


The payload of the packet consists of four addresses, the hardware and protocol address of the sender and receiver hosts which are Sender MAC, IP addresses and Target MAC, IP addresses as shown above.

Internet protocol (IP) is network layer protocol. Data segments from the transport layer are divided into packets and this encapsulated segment is IP payload.



e. What transport layer protocols are used in Skype and Zoom.



As seen from the wireshark capture, TCP and UDP packets are present during a video call.

Skype and zoom use both transport layer protocols UDP and TCP.

They send Audio and video over UDP then use TCP to initiate connection or to bypass some firewalls that block UDP packets. TCP is also used for any text communications during video calls.

UDP connections are fast and efficient but do not provide any error checking. So they are preferred for video conferencing and calls.

Whereas TCP connections are more reliable so they are used for text communications etc