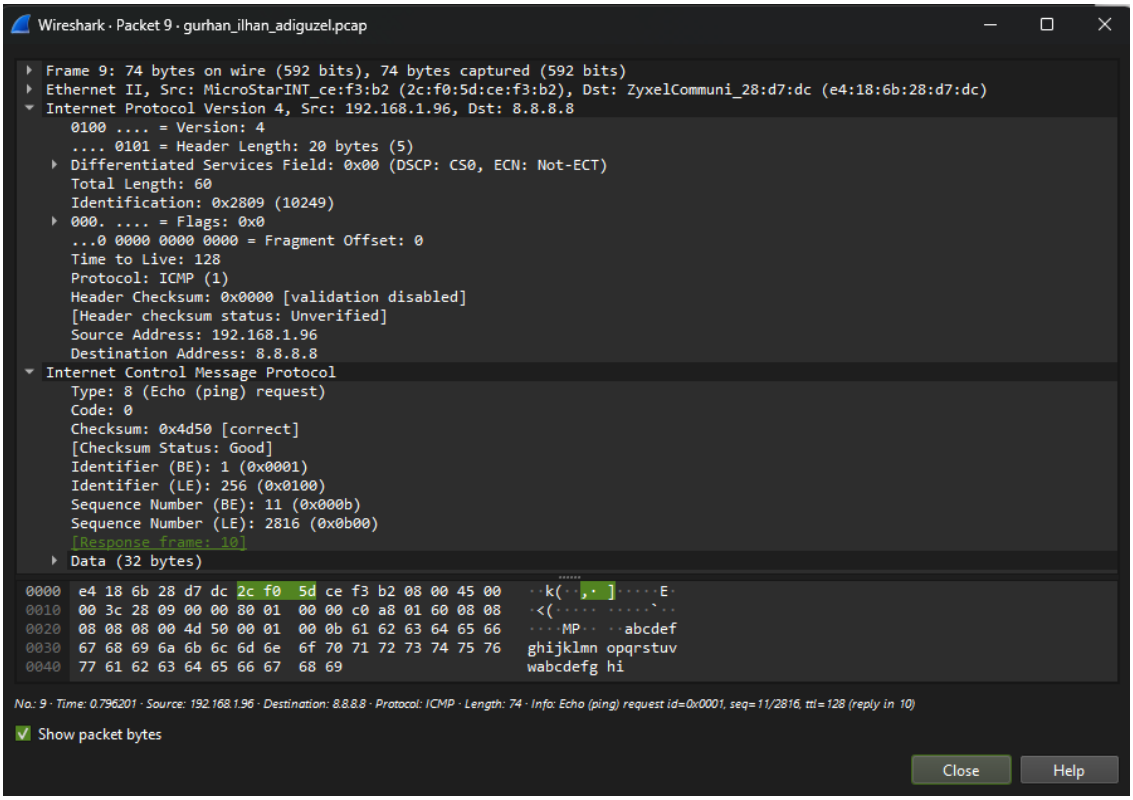
WSA6

2448025

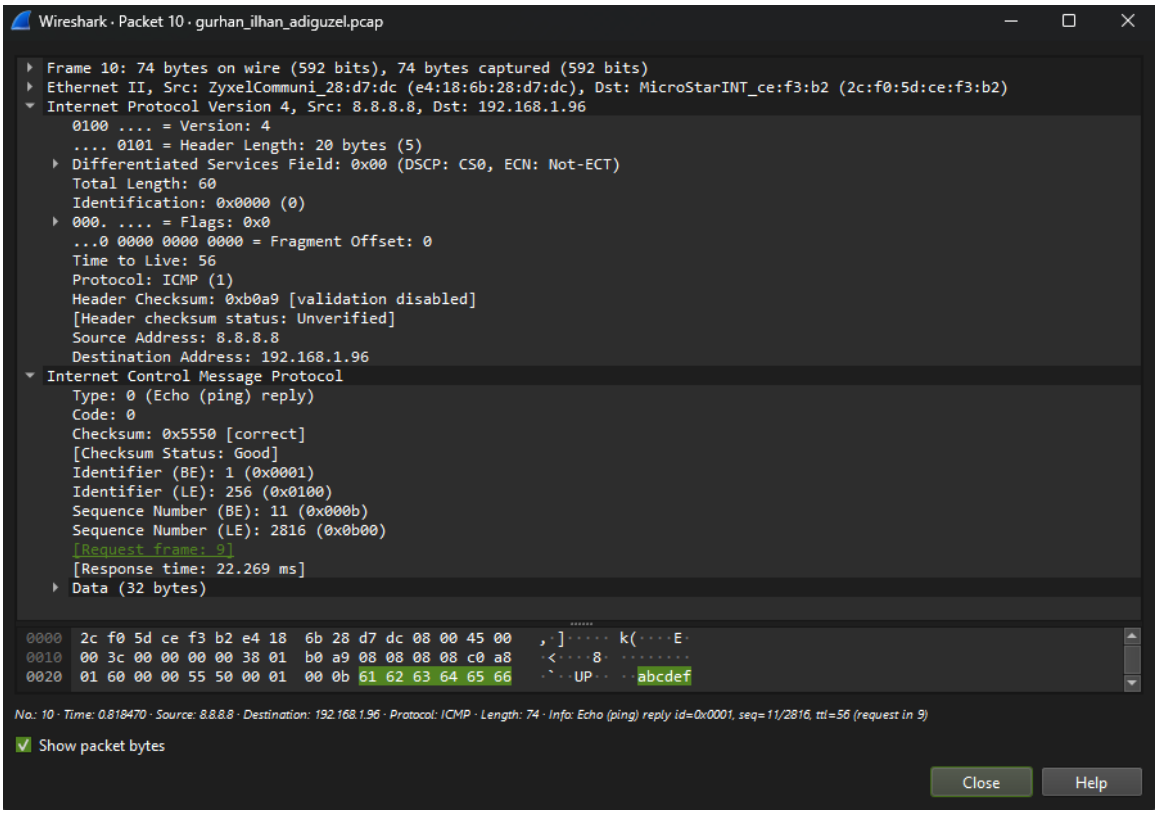
```
C:\Windows\System32>ping -n 10 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=22ms TTL=56
Reply from 8.8.8.8: bytes=32 time=22ms TTL=56
Reply from 8.8.8.8: bytes=32 time=22ms TTL=56
Reply from 8.8.8.8: bytes=32 time=22ms TTL=56
Reply from 8.8.8.8: bytes=32 time=22ms TTL=56
Reply from 8.8.8.8: bytes=32 time=22ms TTL=56
Reply from 8.8.8.8: bytes=32 time=22ms TTL=56
Reply from 8.8.8.8: bytes=32 time=22ms TTL=56
Reply from 8.8.8.8: bytes=32 time=22ms TTL=56
Reply from 8.8.8.8: bytes=32 time=22ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 22ms, Average = 22ms
```

```
C:\Windows\System32>route print
===========================================================================
Interface List
  2...0a 00 27 00 00 02 ......VirtualBox Host-Only Ethernet Adapter
 22...2c f0 5d ce f3 b2 ......Realtek PCIe GbE Family Controller #2
  8...00 1a 7d da 71 13 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
 25...00 15 5d 10 d6 dc ......Hyper-V Virtual Ethernet Adapter
 58...00 15 5d 6e da c3 ......Hyper-V Virtual Ethernet Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.96     35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     172.26.192.0    255.255.240.0         On-link      172.26.192.1   5256
     172.26.192.1  255.255.255.255         On-link      172.26.192.1   5256
   172.26.207.255  255.255.255.255         On-link      172.26.192.1   5256
      172.30.80.0    255.255.240.0         On-link       172.30.80.1   5256
      172.30.80.1  255.255.255.255         On-link       172.30.80.1   5256
    172.30.95.255  255.255.255.255         On-link       172.30.80.1   5256
      192.168.1.0    255.255.255.0         On-link      192.168.1.96    291
     192.168.1.96  255.255.255.255         On-link      192.168.1.96    291
    192.168.1.255  255.255.255.255         On-link      192.168.1.96    291
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link      192.168.1.96    291
        224.0.0.0        240.0.0.0         On-link       172.30.80.1   5256
        224.0.0.0        240.0.0.0         On-link      172.26.192.1   5256
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link      192.168.1.96    291
  255.255.255.255  255.255.255.255         On-link       172.30.80.1   5256
  255.255.255.255  255.255.255.255         On-link      172.26.192.1   5256
===========================================================================
Persistent Routes:
  None
```

Request:



Response:



1. Request:
    - Source Adress : 192.168.1.96
    - Destination Adress : 8.8.8.8

   Reply:

    - Source Adress : 8.8.8.8
    - Destination Adress : 192.168.1.96

2. The ICMP packet was created to transfer network-layer data between hosts and routers, not between application layer processes, so it does not contain source or destination port numbers.

3. a) Purpose of the "type" field:
   - The "type" field is an 8-bit field that specifies the purpose or function of the ICMP message. It indicates whether the packet is an ICMP request or reply.

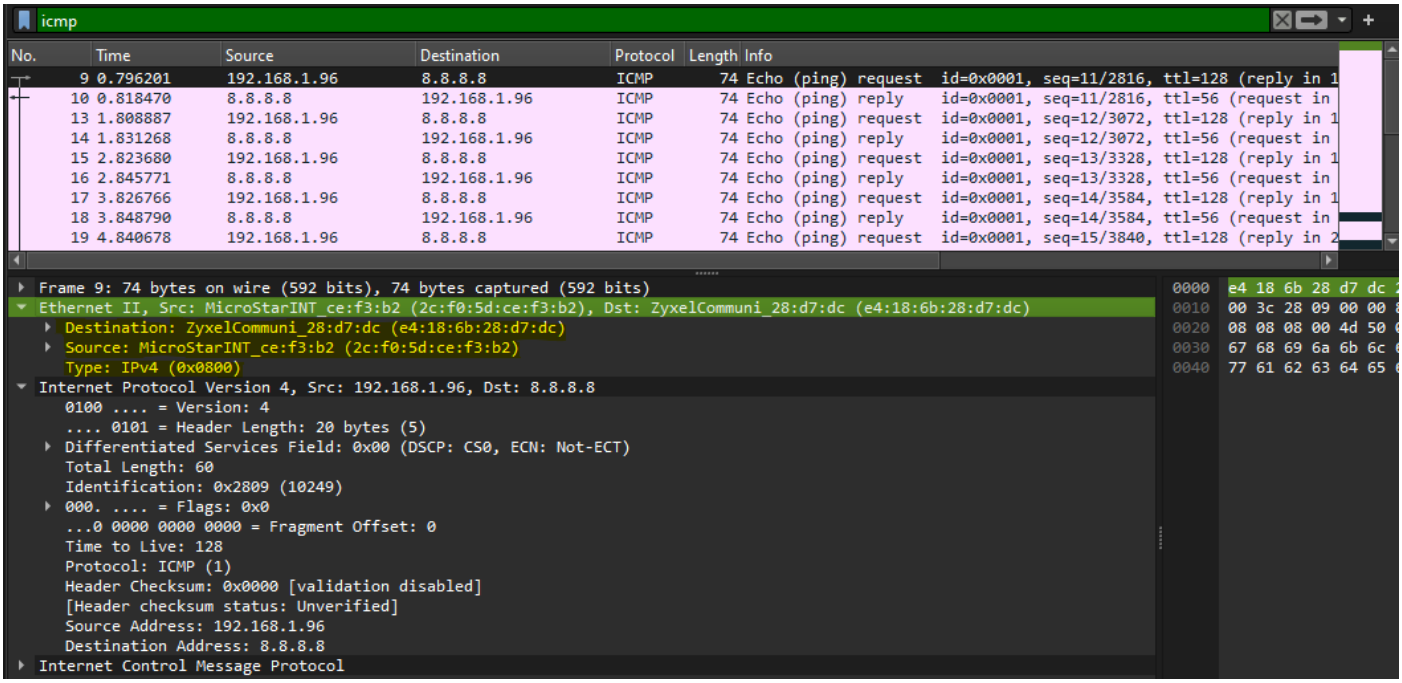
   b) Purpose of the "code" field:
   - The "code" field is also an 8-bit field, and it provides additional information or details related to the "type." It enhances the data that the "type" field conveys.

   c) Request:
   The ICMP message has a "Type" value of 8, indicating an echo request (ping). The "Code" field is 0, suggesting that this is a standard echo request without any specific code details.
   Response:
   The ICMP message has a "Type" value of 0, signaling an echo reply in response to the previous echo request. Like the request, the "Code" field is 0, indicating a standard echo reply without additional code details.

4. The IP datagram Total Length = 60 bytes.
   The IP header Length = 20 bytes.
   The type field = 1 byte,
   Code = 1 byte,
   Checksum = 2 bytes,
   Identifier = 2 bytes,
   Sequence number = 2 bytes
   The remaining 32 bytes are Data.

5. The routing table suggests that the default route directs traffic to the gateway, enabling communication with external networks. If we wish to stop our machine from sending ICMP echo requests, we can modify or remove this default route.

6. a) Source: MicroStarINT_ce:f3:b2 (2c:f0:5d:ce:f3:b2)
   b) Destination: ZyxelCommuni_28:d7:dc (e4:18:6b:28:d7:dc)
   c) All the packets I have sniffed has Type: IPv4 (0x0800). The type of protocol contained in a data link layer frame is indicated in Wireshark's Layer 2 Type field. The next layer's protocol is identified by the Type field, which is a component of the Ethernet frame header. In Wireshark, the value "Type: IPv4 (0x0800)" indicates that an IPv4 packet is encapsulated in an Ethernet frame..


icmp
No. Time Source Destination Protocol Length Info
9 0.796201 192.168.1.96 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 1
10 0.818470 8.8.8.8 192.168.1.96 ICMP 74 Echo (ping) reply id=0x0001, seq=11/2816, ttl=56 (request in
13 1.808887 192.168.1.96 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 1
14 1.831268 8.8.8.8 192.168.1.96 ICMP 74 Echo (ping) reply id=0x0001, seq=12/3072, ttl=56 (request in
15 2.823680 192.168.1.96 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 1
16 2.845771 8.8.8.8 192.168.1.96 ICMP 74 Echo (ping) reply id=0x0001, seq=13/3328, ttl=56 (request in
17 3.826766 192.168.1.96 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 1
18 3.848790 8.8.8.8 192.168.1.96 ICMP 74 Echo (ping) reply id=0x0001, seq=14/3584, ttl=56 (request in
19 4.840678 192.168.1.96 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 2
Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: MicroStarINT_ce:f3:b2 (2c:f0:5d:ce:f3:b2), Dst: ZyxelCommuni_28:d7:dc (e4:18:6b:28:d7:dc)
Destination: ZyxelCommuni_28:d7:dc (e4:18:6b:28:d7:dc)
Source: MicroStarINT_ce:f3:b2 (2c:f0:5d:ce:f3:b2)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.96, Dst: 8.8.8.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x2809 (10249)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.96
Destination Address: 8.8.8.8
Internet Control Message Protocol
0000 e4 18 6b 28 d7 dc
0010 00 3c 28 09 00 00
0020 08 08 08 00 4d 50
0030 67 68 69 6a 6b 6c
0040 77 61 62 63 64 65