Network THE 4 Report

Uygar Yaşar / 2310613

January 5, 2023

1 Answers

Since I could not take a nice .pcap on windows, my friend took a new pcap for me and my report is about that .pcap file.

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=1/256, ttl=64 (reply in 2)
2	0.015233	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=1/256, ttl=55 (request in 1)
3	1.001467	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=2/512, ttl=64 (reply in 4)
4	1.016971	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=2/512, ttl=55 (request in 3)
5	2.003190	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=3/768, ttl=64 (reply in 6)
6	2.018769	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=3/768, ttl=55 (request in 5)
7	3.004411	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=4/1024, ttl=64 (reply in 8)
8	3.019784	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=4/1024, ttl=55 (request in 7)
9	4.005934	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=5/1280, ttl=64 (reply in 10)
10	4.021212	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=5/1280, ttl=55 (request in 9)
11	5.007431	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=6/1536, ttl=64 (reply in 12)
12	5.021849	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=6/1536, ttl=55 (request in 11)
15	6.008938	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=7/1792, ttl=64 (reply in 16)
16	6.063668	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=7/1792, ttl=55 (request in 15)
17	7.010713	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=8/2048, ttl=64 (reply in 18)
18	7.033646	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=8/2048, ttl=55 (request in 17)
21	8.011853	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=9/2304, ttl=64 (reply in 22)
22	8.026041	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=9/2304, ttl=55 (request in 21)
23	9.013174	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=10/2560, ttl=64 (reply in 24)
24	9.026327	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=10/2560, ttl=55 (request in 23)

Figure 1: Capture filtered by icmp

1- As it can be seen from the figure, all the requests goes from 144.122.180.56 which is source IP address. And destination is 1.1.1.1.

2- No there is no port number, because ICMP works on network layer betwen hosts and layers and network software interprets ICMP messages, port numbers are not needed to direct message to an application level process. (figure 2 and 3 shows request and reply information there is no port number information.)

```
> Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
v Ethernet II, Src: IntelCor_bf:6a:80 (0c:54:15:bf:6a:80), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
  > Destination: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
  > Source: IntelCor_bf:6a:80 (0c:54:15:bf:6a:80)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 144.122.180.56, Dst: 1.1.1.1
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x60b0 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 2]
    Timestamp from icmp data: Jan  5, 2023 15:23:38.000000000 Türkiye Standart Saati
    [Timestamp from icmp data (relative): 0.873699000 seconds]
  v Data (48 bytes)
      Data: ca540d0000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b…
      [Length: 48]
```

Figure 2: Packet information of request

```
> Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
v Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_bf:6a:80 (0c:54:15:bf:6a:80)
  > Destination: IntelCor_bf:6a:80 (0c:54:15:bf:6a:80)
  > Source: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 1.1.1.1, Dst: 144.122.180.56
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x68b0 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Request frame: 1]
    [Response time: 15,233 ms]
    Timestamp from icmp data: Jan  5, 2023 15:23:38.000000000 Türkiye Standart Saati
    [Timestamp from icmp data (relative): 0.888932000 seconds]
  v Data (48 bytes)
      Data: ca540d0000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b…
      [Length: 48]
```

Figure 3: Packet information of reply

3- Type is the byte that specifies whether it is request, response, destination unreachable etc. (The types and meanings can be seen from figure 4)

Type	Name	Reference
0	Echo Reply	[RFC792]
1	Unassigned	[JBP]
2	Unassigned	[JBP]
3	Destination Unreachable	[RFC792]
4	Source Quench	[RFC792]
5	Redirect	[RFC792]
6	Alternate Host Address	[JBP]
7	Unassigned	[JBP]
8	Echo	[RFC792]
9	Router Advertisement	[RFC1256]
10	Router Selection	[RFC1256]
11	Time Exceeded	[RFC792]
12	Parameter Problem	[RFC792]
13	Timestamp	[RFC792]
14	Timestamp Reply	[RFC792]
15	Information Request	[RFC792]
16	Information Reply	[RFC792]
17	Address Mask Request	[RFC950]
18	Address Mask Reply	[RFC950]
19	Reserved (for Security)	[Solo]
20-29	Reserved (for Robustness Experiment)	[ZSu]
30	Traceroute	[RFC1393]
31	Datagram Conversion Error	[RFC1475]
32	Mobile Host Redirect	[David Johnson]
33	IPv6 Where-Are-You	[Bill Simpson]
34	IPv6 I-Am-Here	[Bill Simpson]
35	Mobile Registration Request	[Bill Simpson]
36	Mobile Registration Reply	[Bill Simpson]
37	Domain Name Request	[RFC1788]
38	Domain Name Reply	[RFC1788]
39	SKIP	[Markson]
40	Photuris	[RFC2521]
41-255	Reserved for future use	

Figure 4: Type informations and meanings

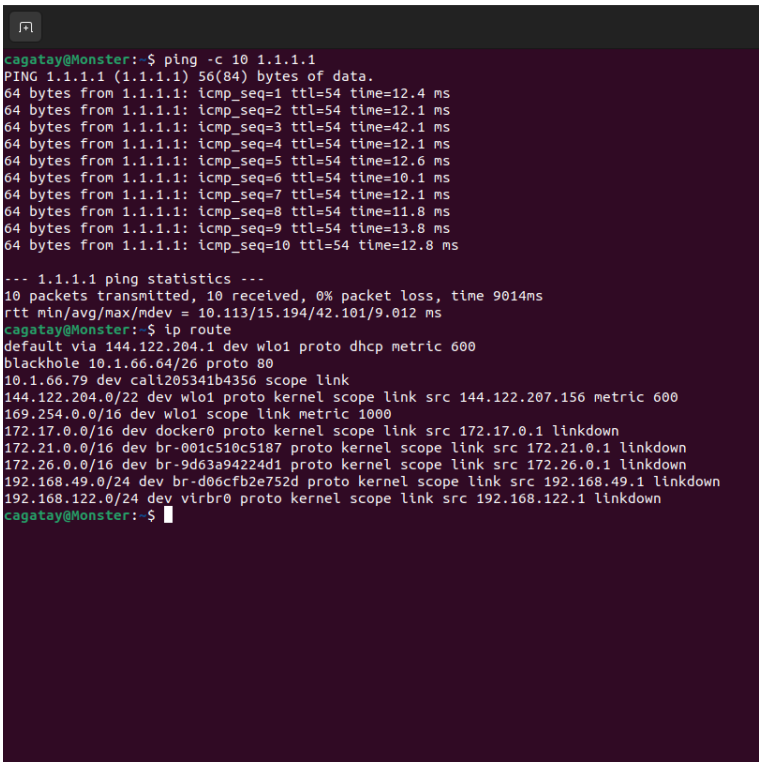
Code is the second byte which specifies what kind of ICMP message it is according to its type. If type is 0 or 8 code code can be 0 which implies no code error. Otherwise, code can be different values (For example, if type is 3 then the 0 code means network error, 1 means means host unreachable.) (All the codes can be seen from figure 5.)

```
0     Echo Reply                          (used by "ping")
            Codes
        0  No Code
1     Unassigned
2     Unassigned
3     Destination Unreachable
      Codes
        0  Net Unreachable
        1  Host Unreachable
        2  Protocol Unreachable
        3  Port Unreachable
        4  Fragmentation Needed and Don't Fragment was Set
        5  Source Route Failed
        6  Destination Network Unknown
        7  Destination Host Unknown
        8  Source Host Isolated
        9  Communication with Destination Network is
           Administratively Prohibited
       10  Communication with Destination Host is
           Administratively Prohibited
       11  Destination Network Unreachable for Type of Service
       12  Destination Host Unreachable for Type of Service
       13  Communication Administratively Prohibited

                                14  Host Precedence Violation

                                15  Precedence cutoff in effect


4     Source Quench
      Codes
        0  No Code
5     Redirect
      Codes
        0  Redirect Datagram for the Network (or subnet)
        1  Redirect Datagram for the Host
        2  Redirect Datagram for the Type of Service and Network
        3  Redirect Datagram for the Type of Service and Host
6     Alternate Host Address
      Codes
        0  Alternate Address for Host
7     Unassigned
8     Echo                                                    (used by "ping")
      Codes
        0  No Code
9     Router Advertisement
      Codes
        0  Normal router advertisement

                                16  Does not route common traffic
10    Router Selection
      Codes
        0  No Code
```

```
11    Time Exceeded
      Codes
        0  Time to Live exceeded in Transit
        1  Fragment Reassembly Time Exceeded
12    Parameter Problem
      Codes
        0  Pointer indicates the error
        1  Missing a Required Option
        2  Bad Length
13    Timestamp
      Codes
        0  No Code
14    Timestamp Reply
      Codes
        0  No Code
15    Information Request
      Codes
        0  No Code
16    Information Reply
      Codes
        0  No Code
17    Address Mask Request
      Codes
        0  No Code
18    Address Mask Reply
      Codes
        0  No Code
19    Reserved (for Security)
20-29 Reserved (for Robustness Experiment)
30    Traceroute
31    Datagram Conversion Error
32    Mobile Host Redirect
33    IPv6 Where-Are-You
34    IPv6 I-Am-Here
35    Mobile Registration Request
36    Mobile Registration Reply
37    Domain Name Request
38    Domain Name Reply
39    SKIP

                        40     Photuris
      Codes
        0 = Bad SPI

                                  1 = Authentication Failed

                                  2 = Decompression Failed

                                  3 = Decryption Failed

                                  4 = Need Authentication

                                  5 = Need Authorization
```

Figure 5: Code informations and meanings
erg.abdn.ac.uk/users/gorry/course/inet-pages/icmp-code.html

4- 20 bytes for IP header, 16 bytes for ICMP header (type(1), code(1), sequence number(2) identifier(2), checksum(2), timestamp(8)), 48 bytes data There is also 14 byte ethernet header so we see that 20+14+16+48= 98 on capture as length of frame.



```
cagatay@Monster:~$ ping -c 10 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=54 time=12.4 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=54 time=12.1 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=54 time=42.1 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=54 time=12.1 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=54 time=12.6 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=54 time=10.1 ms
64 bytes from 1.1.1.1: icmp_seq=7 ttl=54 time=12.1 ms
64 bytes from 1.1.1.1: icmp_seq=8 ttl=54 time=11.8 ms
64 bytes from 1.1.1.1: icmp_seq=9 ttl=54 time=13.8 ms
64 bytes from 1.1.1.1: icmp_seq=10 ttl=54 time=12.8 ms

--- 1.1.1.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 10.113/15.194/42.101/9.012 ms
cagatay@Monster:~$ ip route
default via 144.122.204.1 dev wlo1 proto dhcp metric 600
blackhole 10.1.66.64/26 proto 80
10.1.66.79 dev cali205341b4356 scope link
144.122.204.0/22 dev wlo1 proto kernel scope link src 144.122.207.156 metric 600
169.254.0.0/16 dev wlo1 scope link metric 1000
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
172.21.0.0/16 dev br-001c510c5187 proto kernel scope link src 172.21.0.1 linkdown
172.26.0.0/16 dev br-9d63a94224d1 proto kernel scope link src 172.26.0.1 linkdown
192.168.49.0/24 dev br-d06cfb2e752d proto kernel scope link src 192.168.49.1 linkdown
192.168.122.0/24 dev virbr0 proto kernel scope link src 192.168.122.1 linkdown
cagatay@Monster:~$
```

Figure 6: Terminal

5- The routing table displays how outgoing packets are sent through the gateway at 144.122.204.1. If the root is removed, the machine will be unable to send ping requests (network will be unreachable) and the packets will not reach their intended destination.

6-

a) The ethernet address of my computer is 0c:54:15:bf:6a:80 and its name is "IntelCor_bf" (can be seen from figure 2 and 3)

b) The destination address is 00:1b:21:d2:46:ed (its name is "IntelCor_d2") Since destination is reachable in my pcap, it belongs to the server. (If it was not, the address would belongs to a router.) (can be seen from figure 2 and 3)

c) I encountered three types which are (0x0800 means IPv4 packets, 0x86dd IPv6 packets, and 0x0806 ARP packets)

Address Resolution Protocol (ARP) is a networking protocol used to find the media access control (MAC) address of a device from its Internet Protocol (IP) address. It is used to map IP addresses to the hardware addresses used by a data link protocol, such as Ethernet.

IPv6 is the latest version of the Internet Protocol (IP), the communication protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

Internet Protocol version 4 (IPv4) is a widely-used networking protocol that provides an identification and location system for computers on networks. It is used to route data across the Internet and other networks.

1	0.000000	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=1/256, ttl=64 (reply in 2)
2	0.015233	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=1/256, ttl=55 (request in 1)
3	1.001467	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=2/512, ttl=64 (reply in 4)
4	1.016971	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=2/512, ttl=55 (request in 3)
5	2.003190	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=3/768, ttl=64 (reply in 6)
6	2.018769	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=3/768, ttl=55 (request in 5)
7	3.004411	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=4/1024, ttl=64 (reply in 8)
8	3.019784	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=4/1024, ttl=55 (request in 7)
9	4.005934	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=5/1280, ttl=64 (reply in 10)
10	4.021212	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=5/1280, ttl=55 (request in 9)
11	5.007431	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=6/1536, ttl=64 (reply in 12)
12	5.021849	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=6/1536, ttl=55 (request in 11)
13	5.038924	IntelCor_d2:46:ed	IntelCor_bf:6a:80	ARP	56	Who has 144.122.180.56? Tell 144.122.180.1
14	5.038929	IntelCor_bf:6a:80	IntelCor_d2:46:ed	ARP	42	144.122.180.56 is at 0c:54:15:bf:6a:80
15	6.008938	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=7/1792, ttl=64 (reply in 16)
16	6.063668	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=7/1792, ttl=55 (request in 15)
17	7.010713	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=8/2048, ttl=64 (reply in 18)
18	7.033646	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=8/2048, ttl=55 (request in 17)
19	7.695198	fe80::1040:e868:bda…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
20	7.695229	144.122.180.56	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM" question
21	8.011853	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=9/2304, ttl=64 (reply in 22)
22	8.026041	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=9/2304, ttl=55 (request in 21)
23	9.013174	144.122.180.56	1.1.1.1	ICMP	98	Echo (ping) request id=0x0002, seq=10/2560, ttl=64 (reply in 24)
24	9.026327	1.1.1.1	144.122.180.56	ICMP	98	Echo (ping) reply id=0x0002, seq=10/2560, ttl=55 (request in 23)

Figure 7: My capture without icmp filter