

435
THE 4
Burak Bahar
2380137

1.

No.	Time	Source	Destination	Protocol	Length	Info
5	0.632352	144.122.80.24	1.1.1.1	ICMP	98	Echo (ping) request
6	0.644548	1.1.1.1	144.122.80.24	ICMP	98	Echo (ping) reply
7	1.632775	144.122.80.24	1.1.1.1	ICMP	98	Echo (ping) request
8	1.644254	1.1.1.1	144.122.80.24	ICMP	98	Echo (ping) reply
9	2.634578	144.122.80.24	1.1.1.1	ICMP	98	Echo (ping) request
10	2.646206	1.1.1.1	144.122.80.24	ICMP	98	Echo (ping) reply
17	3.636494	144.122.80.24	1.1.1.1	ICMP	98	Echo (ping) request
18	3.647526	1.1.1.1	144.122.80.24	ICMP	98	Echo (ping) reply
21	4.637825	144.122.80.24	1.1.1.1	ICMP	98	Echo (ping) request
24	4.649090	1.1.1.1	144.122.80.24	ICMP	98	Echo (ping) reply
25	5.639421	144.122.80.24	1.1.1.1	ICMP	98	Echo (ping) request
26	5.650259	1.1.1.1	144.122.80.24	ICMP	98	Echo (ping) reply
29	6.640544	144.122.80.24	1.1.1.1	ICMP	98	Echo (ping) request
30	6.651845	1.1.1.1	144.122.80.24	ICMP	98	Echo (ping) reply
31	7.642158	144.122.80.24	1.1.1.1	ICMP	98	Echo (ping) request
32	7.654670	1.1.1.1	144.122.80.24	ICMP	98	Echo (ping) reply
33	8.644017	144.122.80.24	1.1.1.1	ICMP	98	Echo (ping) request
34	8.654921	1.1.1.1	144.122.80.24	ICMP	98	Echo (ping) reply
35	9.645205	144.122.80.24	1.1.1.1	ICMP	98	Echo (ping) request
36	9.656320	1.1.1.1	144.122.80.24	ICMP	98	Echo (ping) reply
2	0.000023	144.122.80.24	162.159.134.234	TCP	66	59258 → 443 [ACK] Seq
3	0.000000	162.159.134.234	144.122.80.24	TCP	179	[TCP Spurious Retrans

For requests, source is 144.122.80.24 and destination is 1.1.1.1

For replies, source is 1.1.1.1 and destination is 144.122.80.24

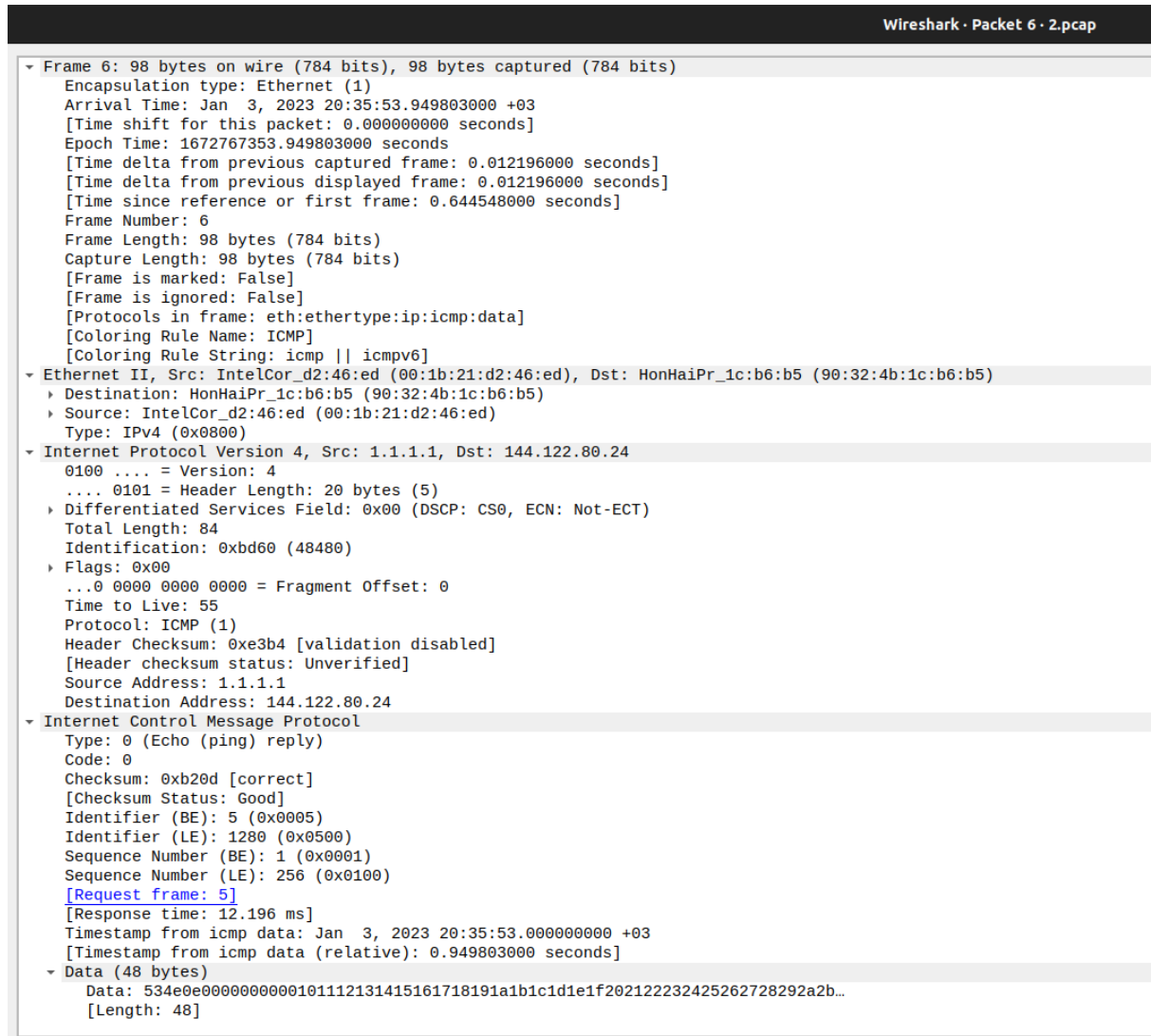
2. For request

Wireshark · Packet 5 · 2.pcap

▼ Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Jan 3, 2023 20:35:53.937607000 +03
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1672767353.937607000 seconds
[Time delta from previous captured frame: 0.632312000 seconds]
[Time delta from previous displayed frame: 0.632312000 seconds]
[Time since reference or first frame: 0.632352000 seconds]
Frame Number: 5
Frame Length: 98 bytes (784 bits)
Capture Length: 98 bytes (784 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
▼ Ethernet II, Src: HonHaiPr_1c:b6:b5 (90:32:4b:1c:b6:b5), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
 Destination: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
 Source: HonHaiPr_1c:b6:b5 (90:32:4b:1c:b6:b5)
 Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 144.122.80.24, Dst: 1.1.1.1
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 84
 Identification: 0x9255 (37461)
 ► Flags: 0x40, Don't fragment
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 64
 Protocol: ICMP (1)
 Header Checksum: 0xc5bf [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 144.122.80.24
 Destination Address: 1.1.1.1
▼ Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0xaa0d [correct]
 [Checksum Status: Good]
 Identifier (BE): 5 (0x0005)
 Identifier (LE): 1280 (0x0500)
 Sequence Number (BE): 1 (0x0001)
 Sequence Number (LE): 256 (0x0100)
 [Response frame: 6]
 Timestamp from icmp data: Jan 3, 2023 20:35:53.000000000 +03
 [Timestamp from icmp data (relative): 0.937607000 seconds]
▼ Data (48 bytes)
 Data: 534e0e0000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b...
 [Length: 48]

0000 00 1b 21 d2 46 ed 90 32 4b 1c b6 b5 08 00 45 00 ...!F..2K...E.

For reply

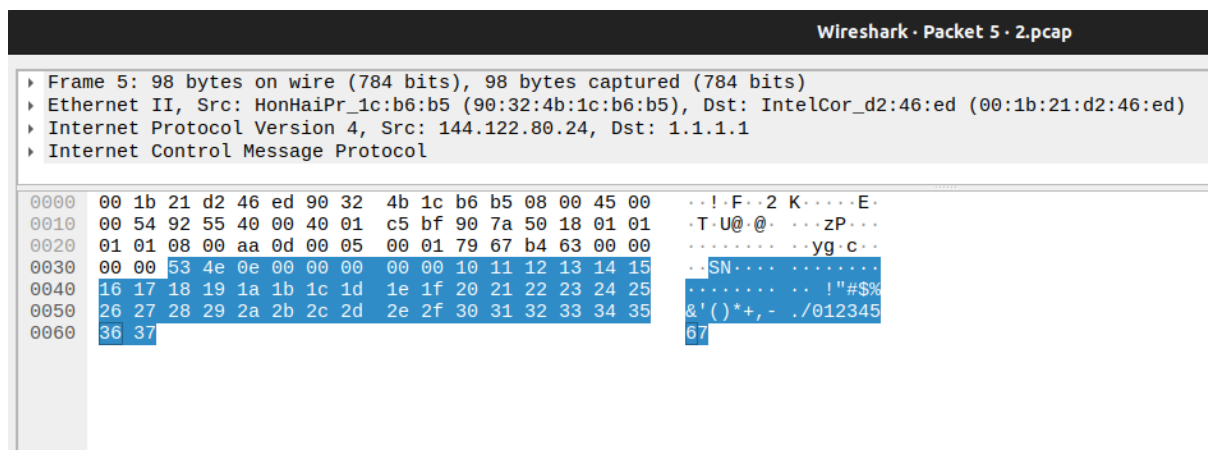


There is no port information given to us. Port is necessary to understand what to do with the given information. Ping is mainly used for checking connection issues. It functions like feedback. So there is no port information.

3. You can see the information about type and code of reply and requests in the second question's screenshots.

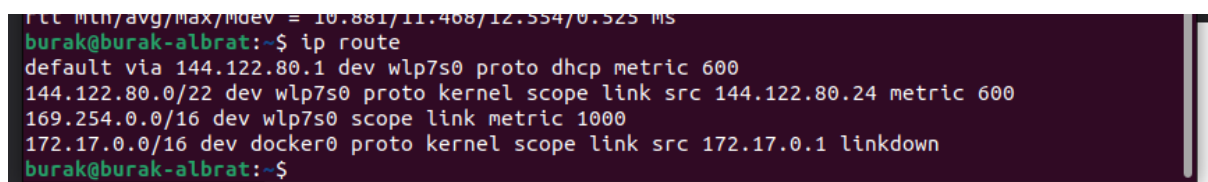
- Type gives information about the ICMP to the user. They represent error types.
- Code field gives more detailed information about type.
- For request type 8 and code 0 represents Echo request. For reply type 0 and code 0 represents echo reply.

4.



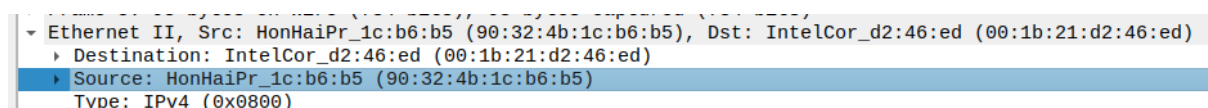
There are 98 bytes. 6 bytes for source and destination 12 bytes in total. 2 bytes for type which is ipv4. 1 for version and header length. 1 for differentiated service fields. 2 for total length. 2 for identification. 2 for flags. 1 for TTL. 1 for protocol. 2 for header checksum. Total of 8 for source and destination addresses. 2 for type and code. 2 for checksum. 2 for identifier. 2 for sequence number. 8 for timestamp. 48 for data.

5.



Second rule should be removed so that my machine will drop the outgoing packages and will not be able to send any ping requests.

6.



- From the screenshot of request from above my computer's ethernet address is 90:32:4b:1c:b6:b5
- From the screenshot of request from above destination address in the Ethernet frame is 00:1b:21:d2:46:ed
- There is only one type which is IPv4. IP version 4. It defines and enables connection between devices in networks or between networks. It gives devices their IP addresses, performs routing and defines packet structures for data.