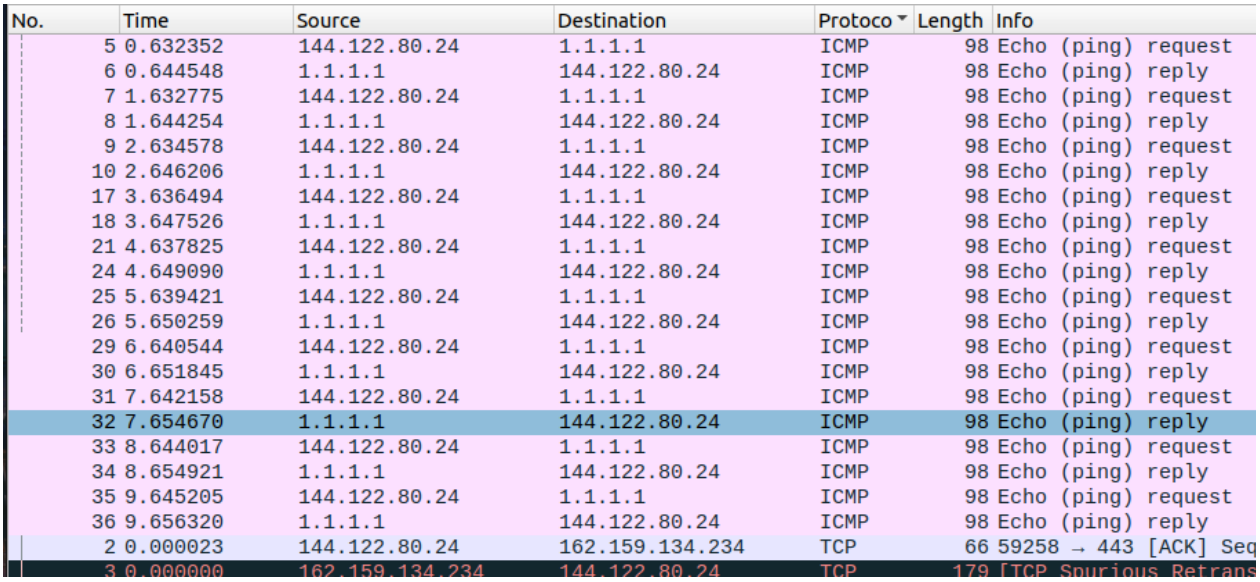
435

THE 4

Burak Bahar

2380137

1.

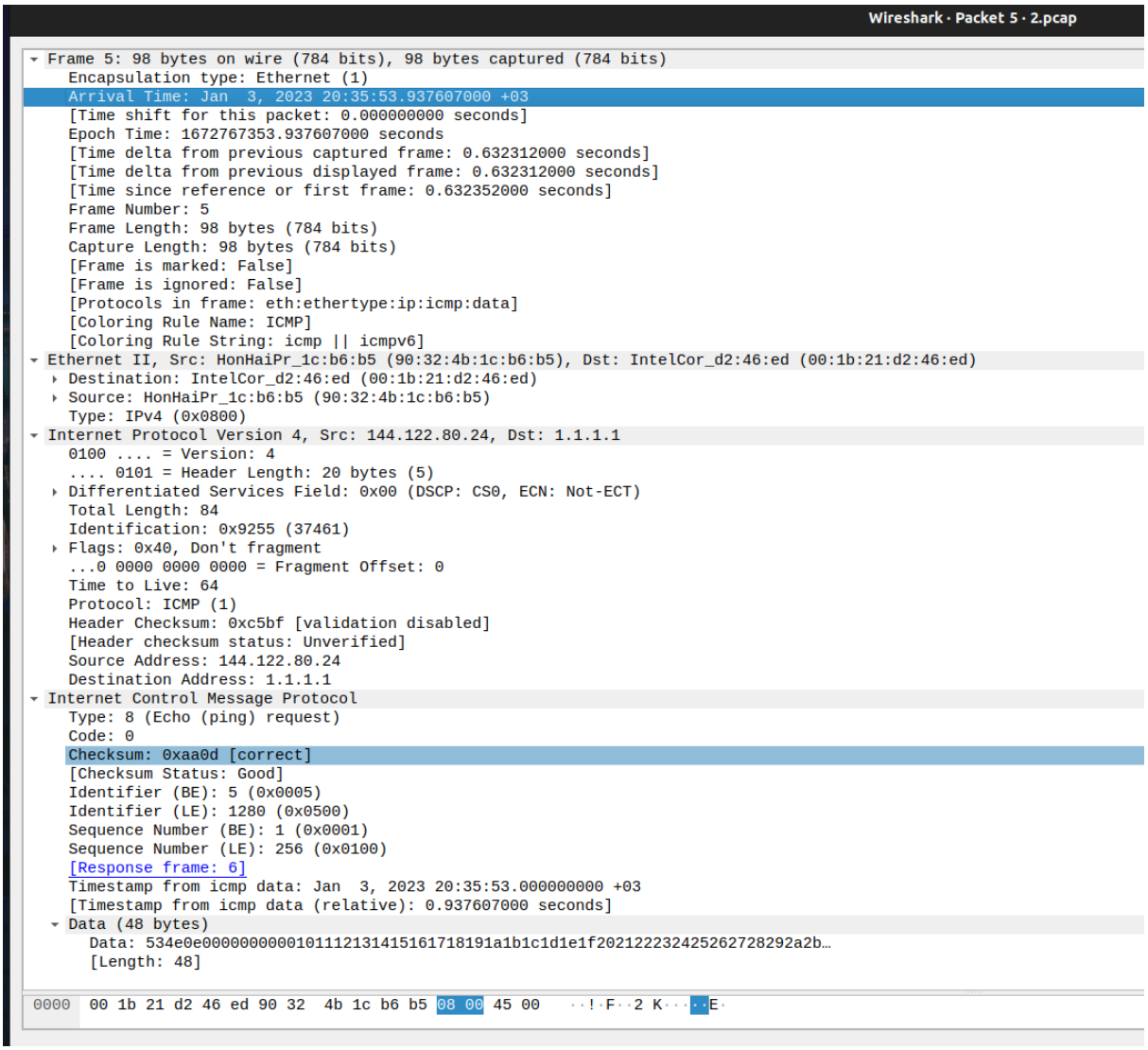


No.	Time	Source	Destination	Protoco	Length	Info
5	0.632352	144.122.80.24	1.1.1.1	ICMP	98	Echo (ping) request
6	0.644548	1.1.1.1	144.122.80.24	ICMP	98	Echo (ping) reply
7	1.632775	144.122.80.24	1.1.1.1	ICMP	98	Echo (ping) request
8	1.644254	1.1.1.1	144.122.80.24	ICMP	98	Echo (ping) reply
9	2.634578	144.122.80.24	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

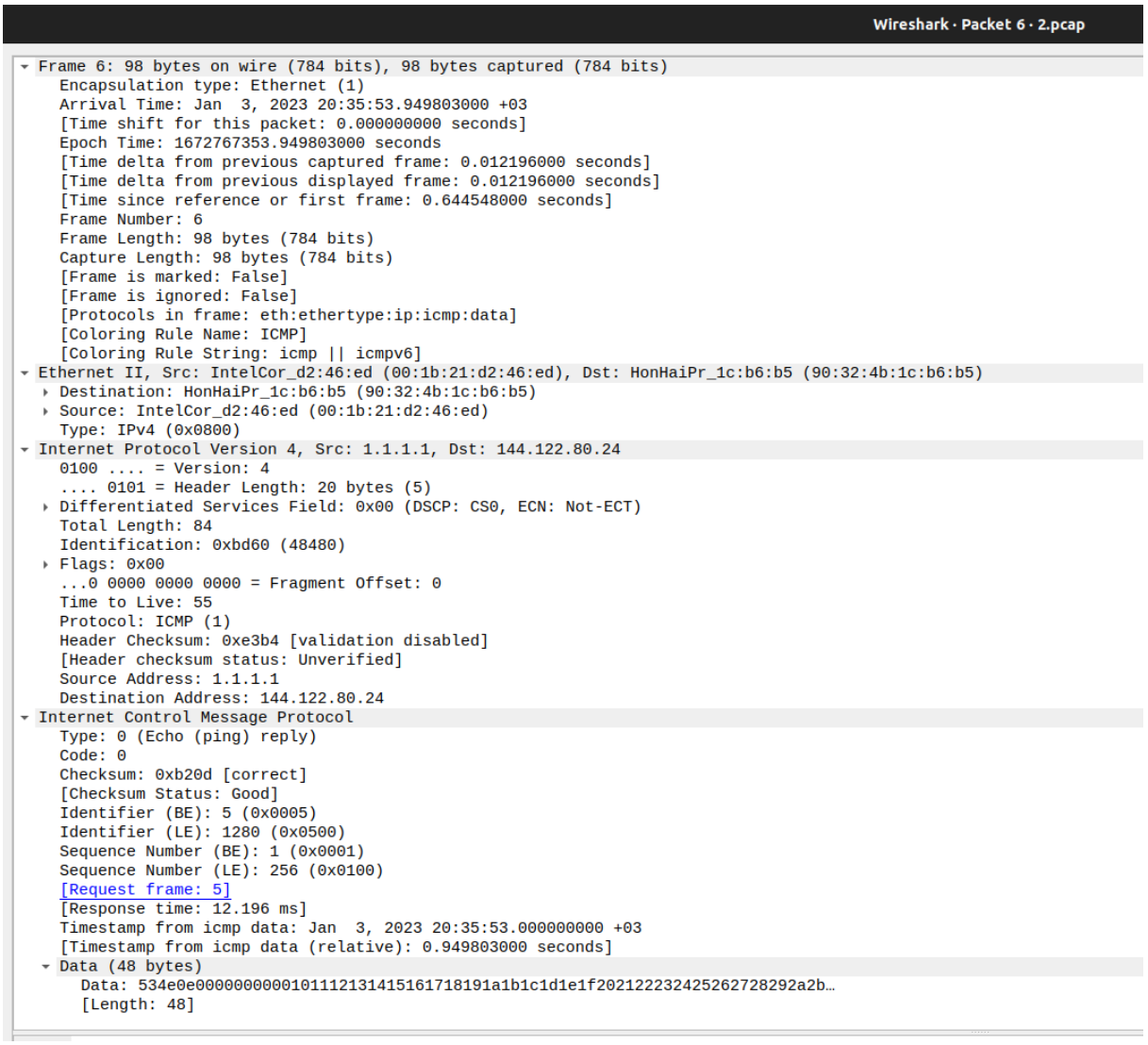
For requests, source is 144.122.80.24 and destination is 1.1.1.1

For replies, source is 1.1.1.1 and destination is 144.122.80.24

2. For request



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.

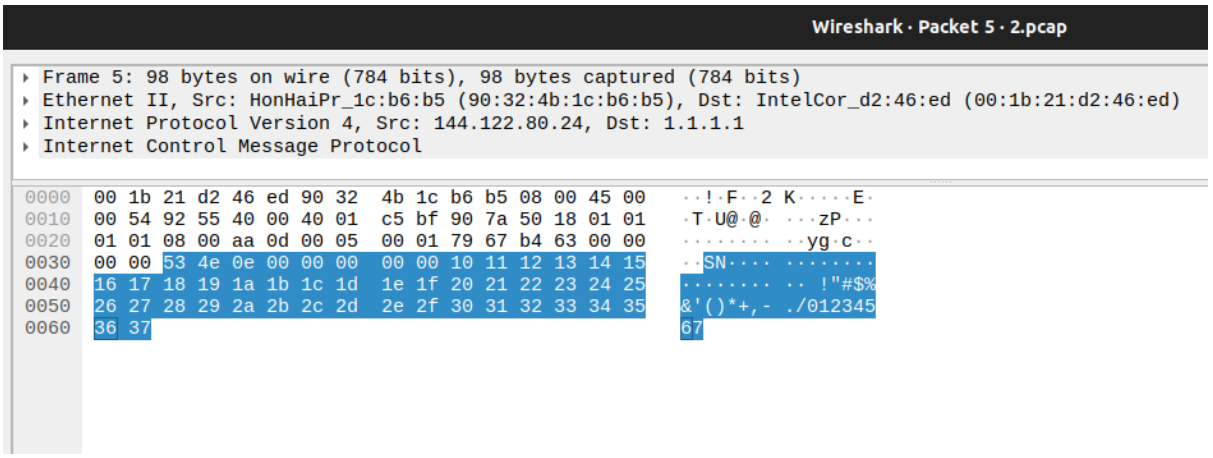
3. You can see the information about type and code of reply and requests in the second question's screenshots.

a) Type gives information about the ICMP to the user. They represent error types.

b) Code field gives more detailed information about type.

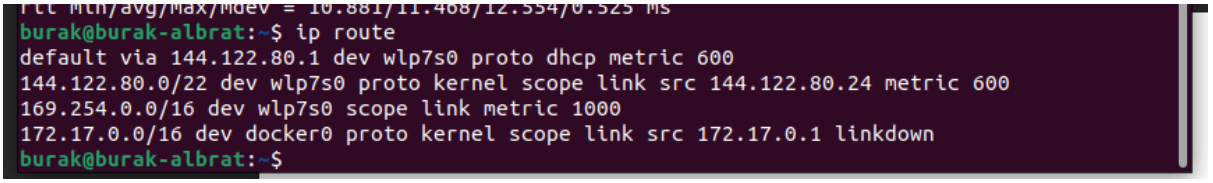
c) For request type 8 and code 0 represents Echo request. For reply type 0 and code 0 represents echo reply.

4.



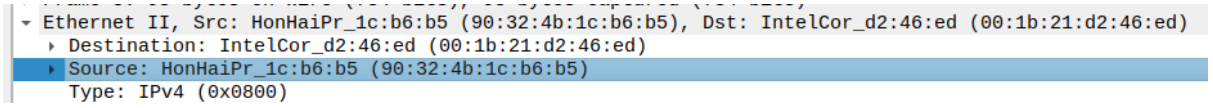
There are 98 bytes. 6 bytes for source and destination 12 bytes in total. 2 bytes for type which is ipv4. 1 for version and header length. 1 for differentiated service fields. 2 for total length. 2 for identification. 2 for flags.1 for TTL. 1 for protocol. 2 for header checksum. Total of 8 for source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



a) From the screenshot of request from above my computer's ethernet address is 90:32:4b:1c:b6:b5

b) From the screenshot of request from above destination address in the Ethernet frame is 00:1b:21:d2:46:ed

c) 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.