Computer Networks Lab 9

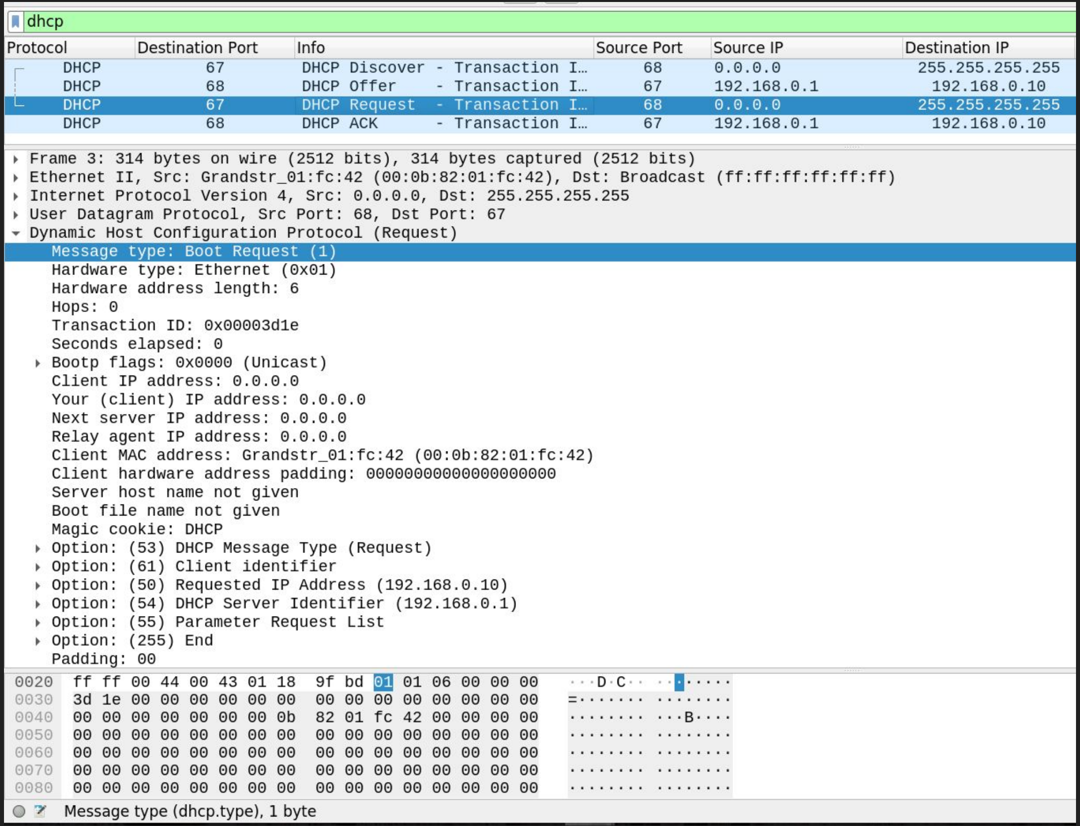
Wireshark --- ARP, DHCP and ICMP

Arun Ganti

2019A7PS0021G

1) Show a round of execution of DHCP

A. Show DHCP Request message



dhcp

Protocol	Destination Port	Info	Source Port	Source IP	Destination IP
DHCP	67	DHCP Discover - Transaction I…	68	0.0.0.0	255.255.255.255
DHCP	68	DHCP Offer - Transaction I…	67	192.168.0.1	192.168.0.10
DHCP	67	DHCP Request - Transaction I…	68	0.0.0.0	255.255.255.255
DHCP	68	DHCP ACK - Transaction I…	67	192.168.0.1	192.168.0.10

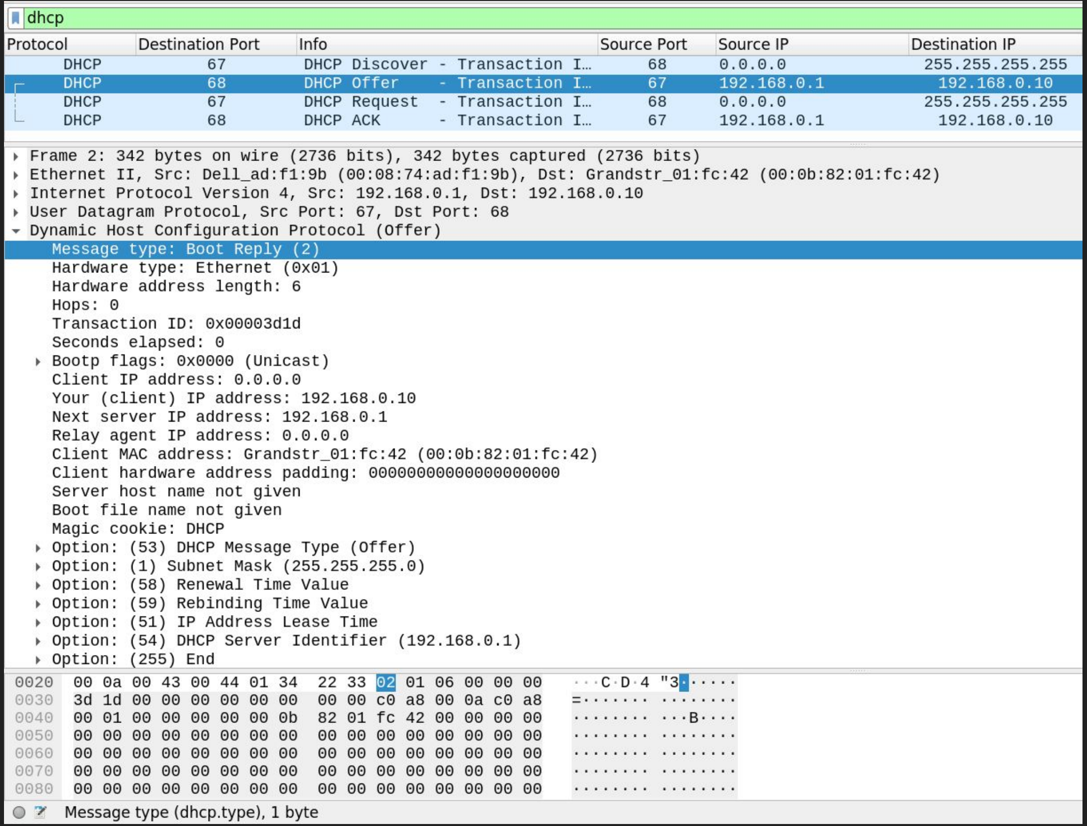
```
▸ Frame 3: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
▸ Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▾ Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1e
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Request)
  ▸ Option: (61) Client identifier
  ▸ Option: (50) Requested IP Address (192.168.0.10)
  ▸ Option: (54) DHCP Server Identifier (192.168.0.1)
  ▸ Option: (55) Parameter Request List
  ▸ Option: (255) End
    Padding: 00
```

```
0020  ff ff 00 44 00 43 01 18  9f bd 01 01 06 00 00 00   ···D·C·· ········
0030  3d 1e 00 00 00 00 00 00  00 00 00 00 00 00 00 00   =······· ········
0040  00 00 00 00 00 00 00 0b  82 01 fc 42 00 00 00 00   ········ ···B····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Message type (dhcp.type), 1 byte

1) Show a round of execution of DHCP

A. Show DHCP Reply message



dhcp

Protocol	Destination Port	Info	Source Port	Source IP	Destination IP
DHCP	67	DHCP Discover - Transaction I…	68	0.0.0.0	255.255.255.255
DHCP	68	DHCP Offer - Transaction I…	67	192.168.0.1	192.168.0.10
DHCP	67	DHCP Request - Transaction I…	68	0.0.0.0	255.255.255.255
DHCP	68	DHCP ACK - Transaction I…	67	192.168.0.1	192.168.0.10

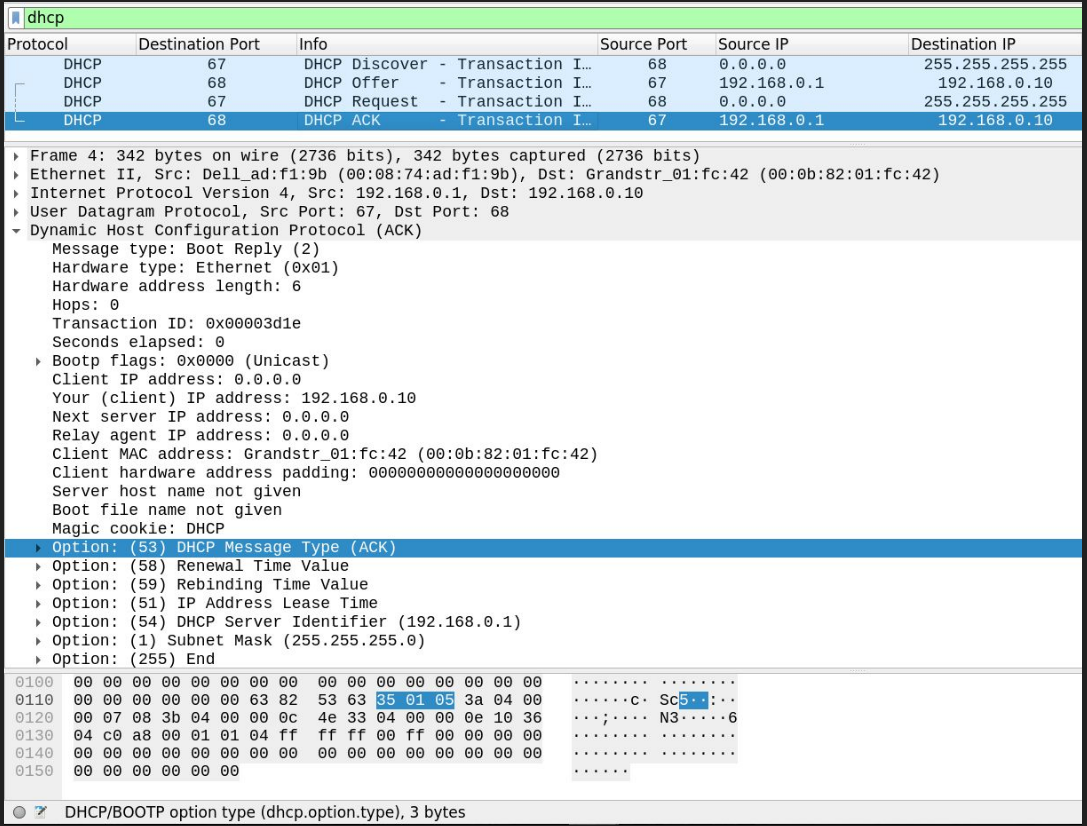
```
▸ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▸ Ethernet II, Src: Dell_ad:f1:9b (00:08:74:ad:f1:9b), Dst: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
▸ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.10
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▾ Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1d
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.0.10
    Next server IP address: 192.168.0.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Offer)
  ▸ Option: (1) Subnet Mask (255.255.255.0)
  ▸ Option: (58) Renewal Time Value
  ▸ Option: (59) Rebinding Time Value
  ▸ Option: (51) IP Address Lease Time
  ▸ Option: (54) DHCP Server Identifier (192.168.0.1)
  ▸ Option: (255) End
```

```
0020  00 0a 00 43 00 44 01 34  22 33 02 01 06 00 00 00   ···C·D·4 "3······
0030  3d 1d 00 00 00 00 00 00  00 00 c0 a8 00 0a c0 a8   =······· ········
0040  00 01 00 00 00 00 00 0b  82 01 fc 42 00 00 00 00   ········ ···B····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Message type (dhcp.type), 1 byte

1) Show a round of execution of DHCP

A. Show DHCP ACK message



dhcp

Protocol	Destination Port	Info	Source Port	Source IP	Destination IP
DHCP	67	DHCP Discover - Transaction I…	68	0.0.0.0	255.255.255.255
DHCP	68	DHCP Offer - Transaction I…	67	192.168.0.1	192.168.0.10
DHCP	67	DHCP Request - Transaction I…	68	0.0.0.0	255.255.255.255
DHCP	68	DHCP ACK - Transaction I…	67	192.168.0.1	192.168.0.10

```
▸ Frame 4: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▸ Ethernet II, Src: Dell_ad:f1:9b (00:08:74:ad:f1:9b), Dst: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
▸ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.10
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▾ Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1e
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.0.10
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (ACK)
  ▸ Option: (58) Renewal Time Value
  ▸ Option: (59) Rebinding Time Value
  ▸ Option: (51) IP Address Lease Time
  ▸ Option: (54) DHCP Server Identifier (192.168.0.1)
  ▸ Option: (1) Subnet Mask (255.255.255.0)
  ▸ Option: (255) End
```

```
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 05 3a 04 00   ······c· Sc5··:··
0120  00 07 08 3b 04 00 00 0c  4e 33 04 00 00 0e 10 36   ···;···· N3·····6
0130  04 c0 a8 00 01 01 04 ff  ff ff 00 ff 00 00 00 00   ········ ········
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0150  00 00 00 00 00 00                                  ······
```

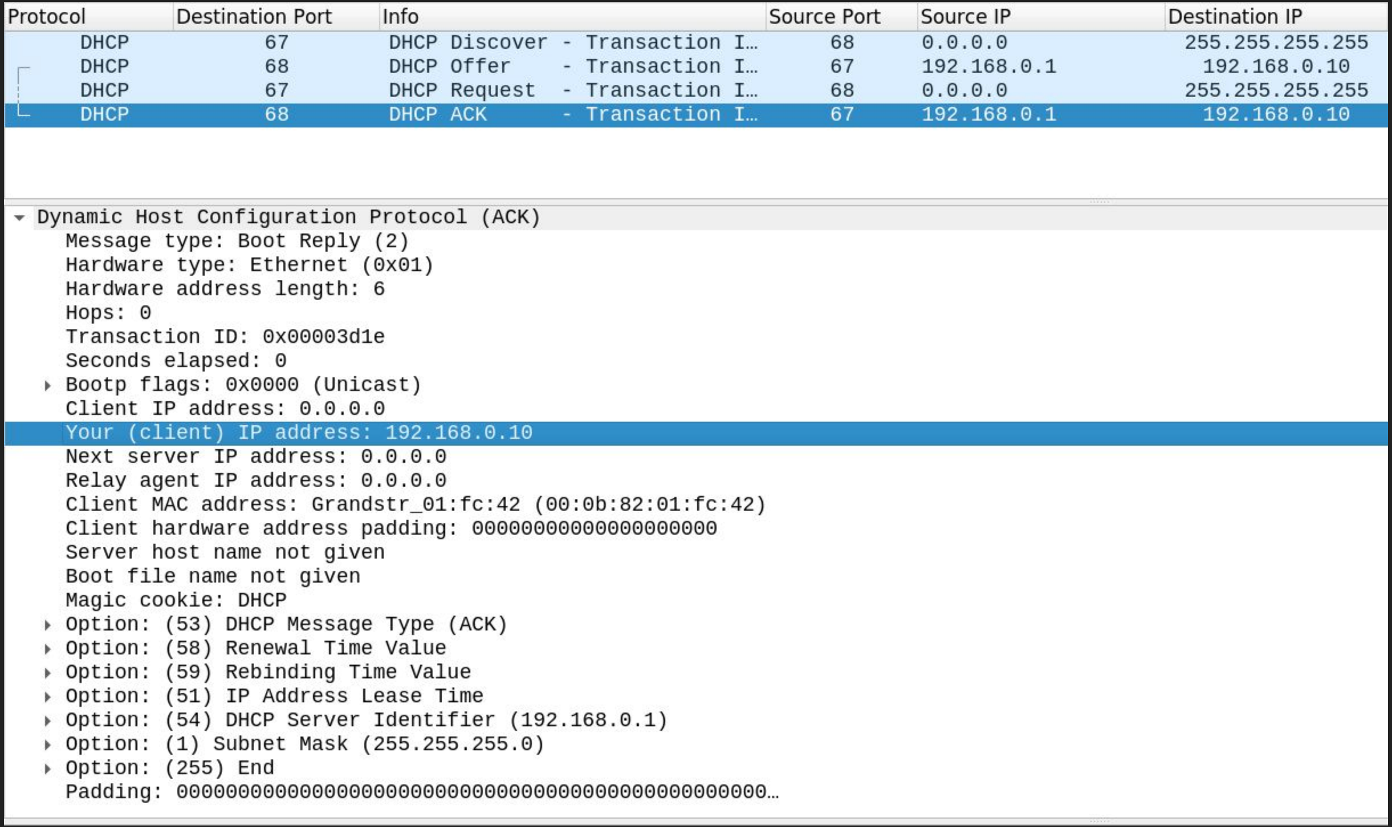
DHCP/BOOTP option type (dhcp.option.type), 3 bytes

1) Show a round of execution of DHCP

B. Find out IP Addresses of DHCP server and client

Server IP address:
192.168.0.1

Client IP address:
192.168.0.10

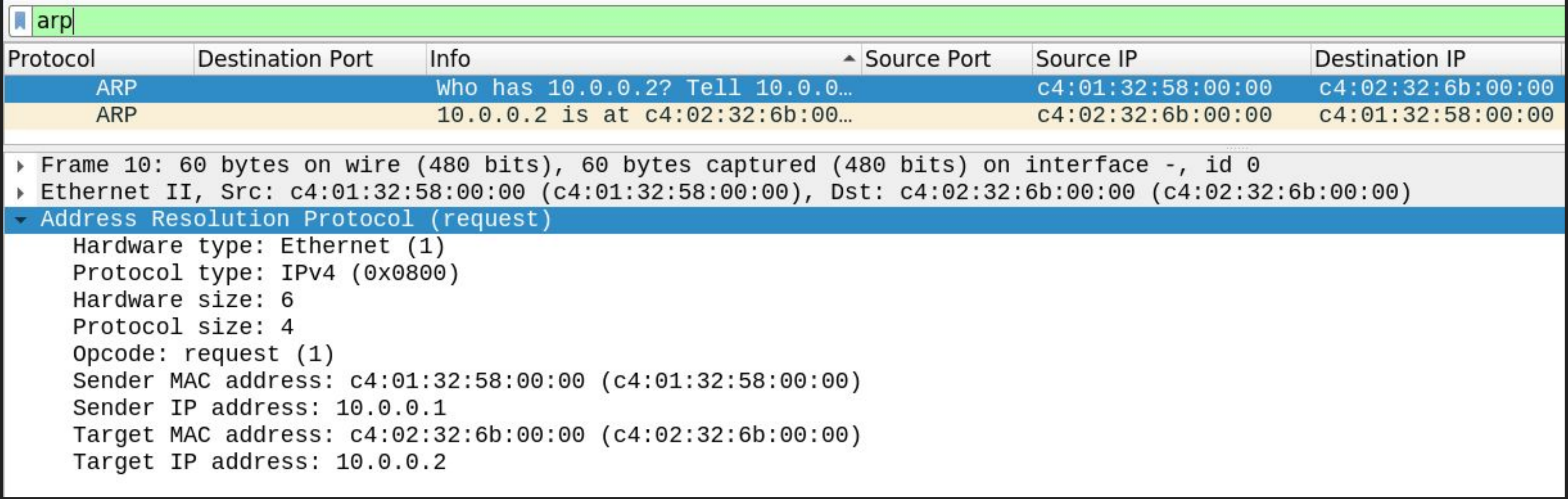


Protocol	Destination Port	Info	Source Port	Source IP	Destination IP
DHCP	67	DHCP Discover - Transaction I…	68	0.0.0.0	255.255.255.255
DHCP	68	DHCP Offer - Transaction I…	67	192.168.0.1	192.168.0.10
DHCP	67	DHCP Request - Transaction I…	68	0.0.0.0	255.255.255.255
DHCP	68	DHCP ACK - Transaction I…	67	192.168.0.1	192.168.0.10

```
▾ Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1e
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.0.10
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (ACK)
  ▸ Option: (58) Renewal Time Value
  ▸ Option: (59) Rebinding Time Value
  ▸ Option: (51) IP Address Lease Time
  ▸ Option: (54) DHCP Server Identifier (192.168.0.1)
  ▸ Option: (1) Subnet Mask (255.255.255.0)
  ▸ Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000…
```

2) Show a round of execution of ARP

A. Show ARP Request



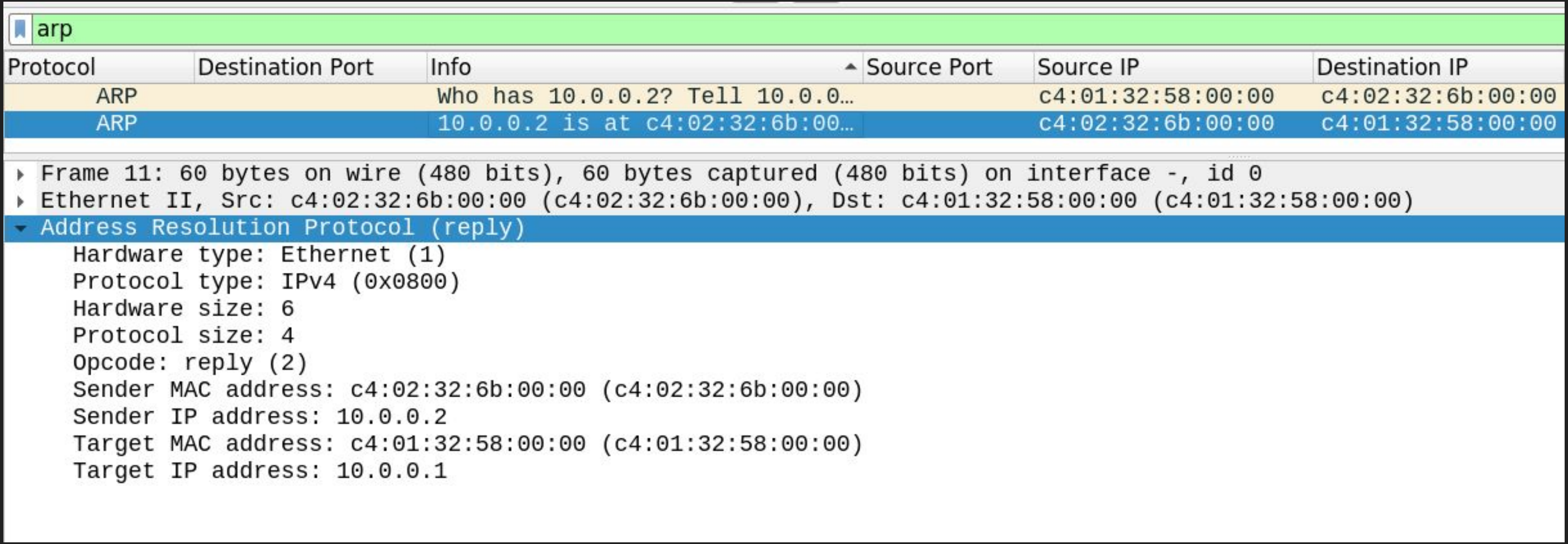
arp

Protocol	Destination Port	Info	Source Port	Source IP	Destination IP
ARP		Who has 10.0.0.2? Tell 10.0.0…		c4:01:32:58:00:00	c4:02:32:6b:00:00
ARP		10.0.0.2 is at c4:02:32:6b:00…		c4:02:32:6b:00:00	c4:01:32:58:00:00

```
▸ Frame 10: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 0
▸ Ethernet II, Src: c4:01:32:58:00:00 (c4:01:32:58:00:00), Dst: c4:02:32:6b:00:00 (c4:02:32:6b:00:00)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: c4:01:32:58:00:00 (c4:01:32:58:00:00)
    Sender IP address: 10.0.0.1
    Target MAC address: c4:02:32:6b:00:00 (c4:02:32:6b:00:00)
    Target IP address: 10.0.0.2
```

2) Show a round of execution of ARP

A. Show ARP Reply



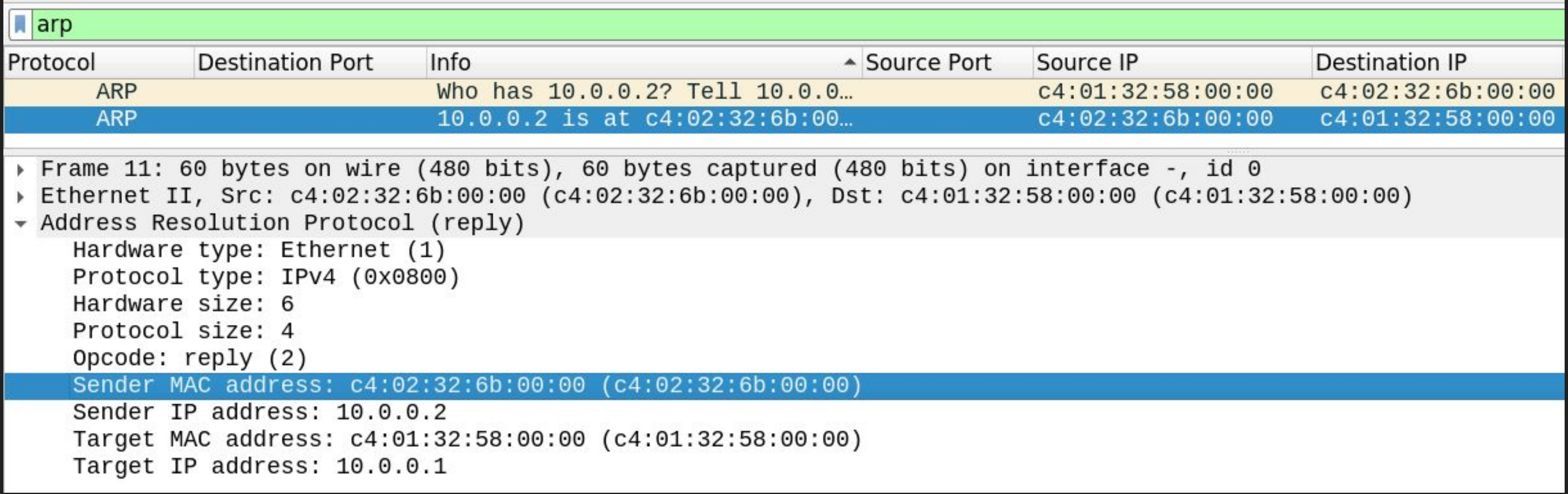
arp

Protocol	Destination Port	Info	Source Port	Source IP	Destination IP
ARP		Who has 10.0.0.2? Tell 10.0.0…		c4:01:32:58:00:00	c4:02:32:6b:00:00
ARP		10.0.0.2 is at c4:02:32:6b:00…		c4:02:32:6b:00:00	c4:01:32:58:00:00

```
▸ Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 0
▸ Ethernet II, Src: c4:02:32:6b:00:00 (c4:02:32:6b:00:00), Dst: c4:01:32:58:00:00 (c4:01:32:58:00:00)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: c4:02:32:6b:00:00 (c4:02:32:6b:00:00)
    Sender IP address: 10.0.0.2
    Target MAC address: c4:01:32:58:00:00 (c4:01:32:58:00:00)
    Target IP address: 10.0.0.1
```

2) Show a round of execution of ARP

B. Find the MAC Address of the Replier



arp

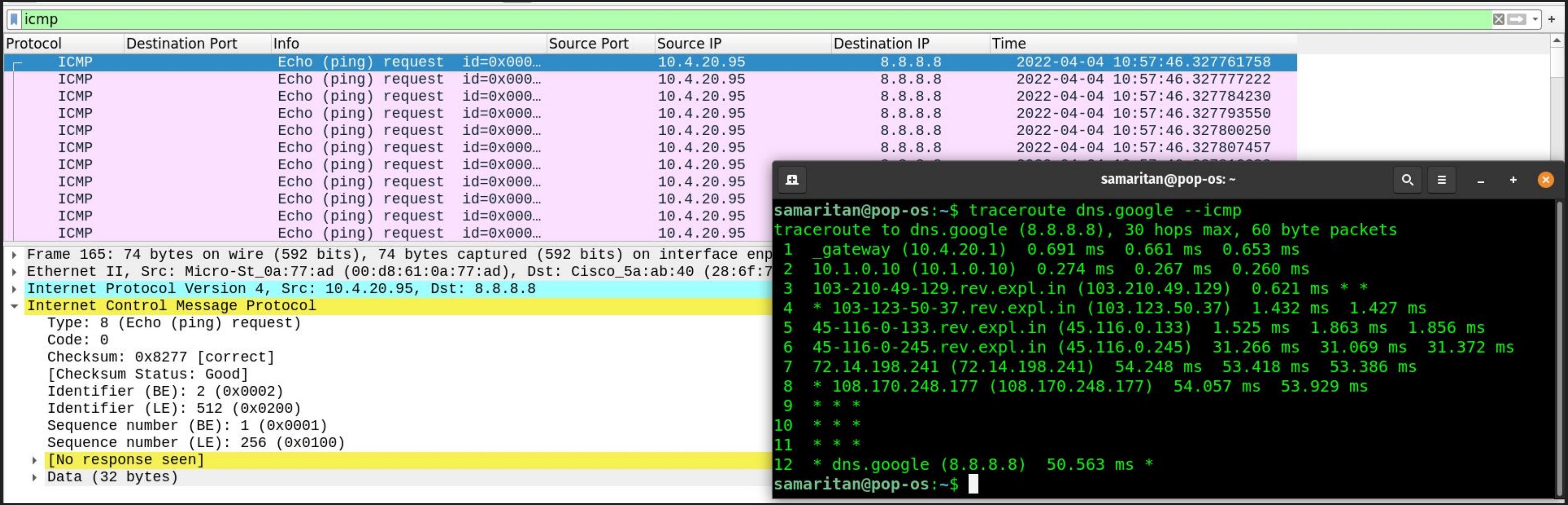
Protocol	Destination Port	Info	Source Port	Source IP	Destination IP
ARP		Who has 10.0.0.2? Tell 10.0.0…		c4:01:32:58:00:00	c4:02:32:6b:00:00
ARP		10.0.0.2 is at c4:02:32:6b:00…		c4:02:32:6b:00:00	c4:01:32:58:00:00

```
▸ Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 0
▸ Ethernet II, Src: c4:02:32:6b:00:00 (c4:02:32:6b:00:00), Dst: c4:01:32:58:00:00 (c4:01:32:58:00:00)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: c4:02:32:6b:00:00 (c4:02:32:6b:00:00)
    Sender IP address: 10.0.0.2
    Target MAC address: c4:01:32:58:00:00 (c4:01:32:58:00:00)
    Target IP address: 10.0.0.1
```

Sender MAC address: c4:02:32:6b:00:00 (c4:02:32:6b:00:00)

3) Show a round of execution of traceroute command for dns.google

A. Find the IP Address of your host and the destination.



icmp

Protocol	Destination Port	Info	Source Port	Source IP	Destination IP	Time
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327761758
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327777222
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327784230
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327793550
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327800250
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327807457
ICMP		Echo (ping) request id=0x000…		10.4.20.95		
ICMP		Echo (ping) request id=0x000…		10.4.20.95		
ICMP		Echo (ping) request id=0x000…		10.4.20.95		
ICMP		Echo (ping) request id=0x000…		10.4.20.95		
ICMP		Echo (ping) request id=0x000…		10.4.20.95		

```
Frame 165: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp
Ethernet II, Src: Micro-St_0a:77:ad (00:d8:61:0a:77:ad), Dst: Cisco_5a:ab:40 (28:6f:7
Internet Protocol Version 4, Src: 10.4.20.95, Dst: 8.8.8.8
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x8277 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
  [No response seen]
  Data (32 bytes)
```

samaritan@pop-os: ~

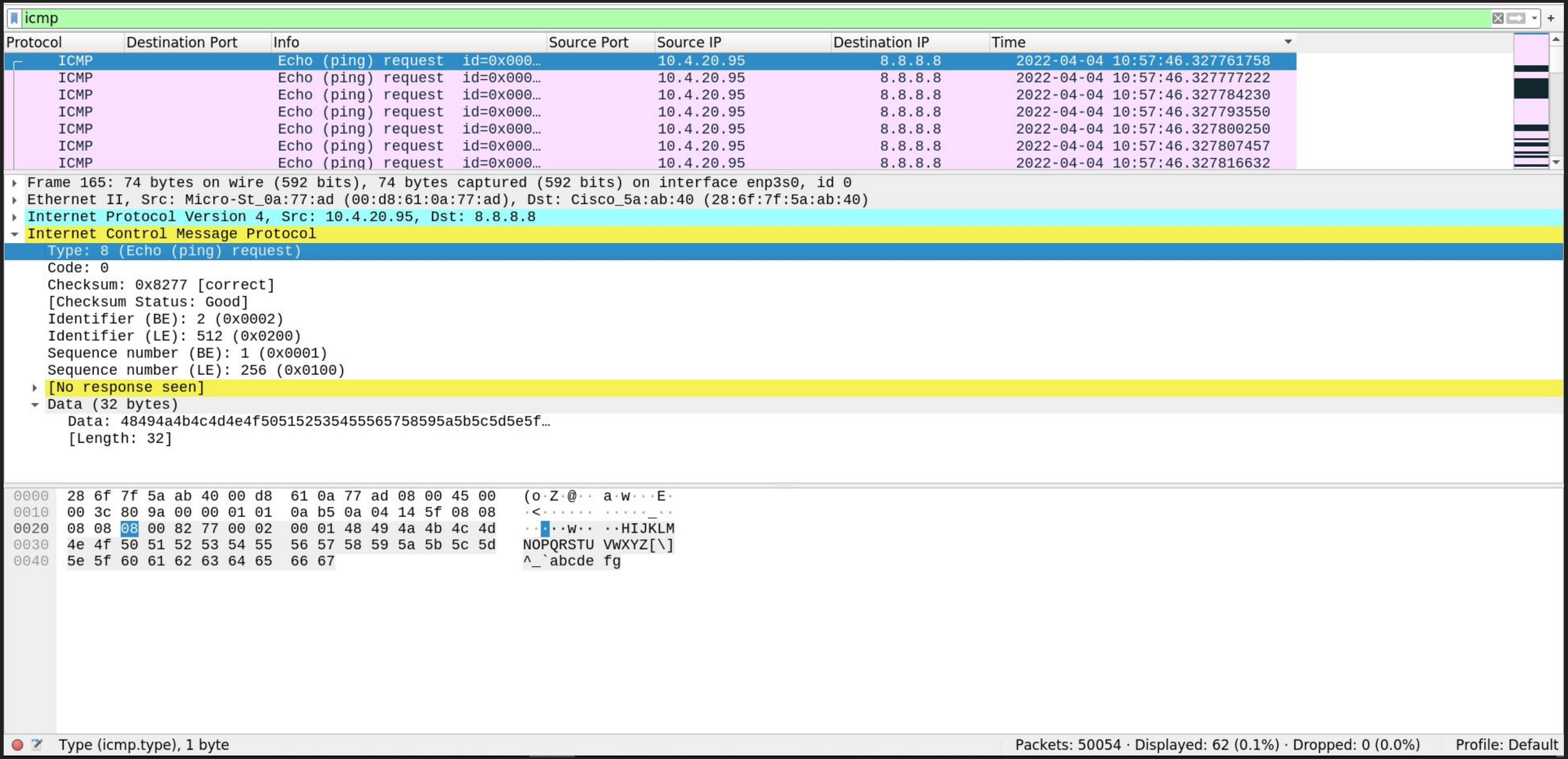
```
samaritan@pop-os:~$ traceroute dns.google --icmp
traceroute to dns.google (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (10.4.20.1)  0.691 ms  0.661 ms  0.653 ms
 2  10.1.0.10 (10.1.0.10)  0.274 ms  0.267 ms  0.260 ms
 3  103-210-49-129.rev.expl.in (103.210.49.129)  0.621 ms * *
 4  * 103-123-50-37.rev.expl.in (103.123.50.37)  1.432 ms  1.427 ms
 5  45-116-0-133.rev.expl.in (45.116.0.133)  1.525 ms  1.863 ms  1.856 ms
 6  45-116-0-245.rev.expl.in (45.116.0.245)  31.266 ms  31.069 ms  31.372 ms
 7  72.14.198.241 (72.14.198.241)  54.248 ms  53.418 ms  53.386 ms
 8  * 108.170.248.177 (108.170.248.177)  54.057 ms  53.929 ms
 9  * * *
10  * * *
11  * * *
12  * dns.google (8.8.8.8)  50.563 ms *
samaritan@pop-os:~$ 
```

IP Address of host = 10.4.28.95

Destination IP Address = 8.8.8.8

3) Show a round of execution of traceroute command for dns.google

B. Identify bytes that represent type and code.



icmp

```
Protocol  Destination Port  Info                                Source Port  Source IP     Destination IP  Time
  ICMP                      Echo (ping) request  id=0x000…                   10.4.20.95    8.8.8.8         2022-04-04 10:57:46.327761758
  ICMP                      Echo (ping) request  id=0x000…                   10.4.20.95    8.8.8.8         2022-04-04 10:57:46.327777222
  ICMP                      Echo (ping) request  id=0x000…                   10.4.20.95    8.8.8.8         2022-04-04 10:57:46.327784230
  ICMP                      Echo (ping) request  id=0x000…                   10.4.20.95    8.8.8.8         2022-04-04 10:57:46.327793550
  ICMP                      Echo (ping) request  id=0x000…                   10.4.20.95    8.8.8.8         2022-04-04 10:57:46.327800250
  ICMP                      Echo (ping) request  id=0x000…                   10.4.20.95    8.8.8.8         2022-04-04 10:57:46.327807457
  ICMP                      Echo (ping) request  id=0x000…                   10.4.20.95    8.8.8.8         2022-04-04 10:57:46.327816632
```

```
▸ Frame 165: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp3s0, id 0
▸ Ethernet II, Src: Micro-St_0a:77:ad (00:d8:61:0a:77:ad), Dst: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40)
▸ Internet Protocol Version 4, Src: 10.4.20.95, Dst: 8.8.8.8
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x8277 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
  ▸ [No response seen]
  ▾ Data (32 bytes)
      Data: 48494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f…
      [Length: 32]
```

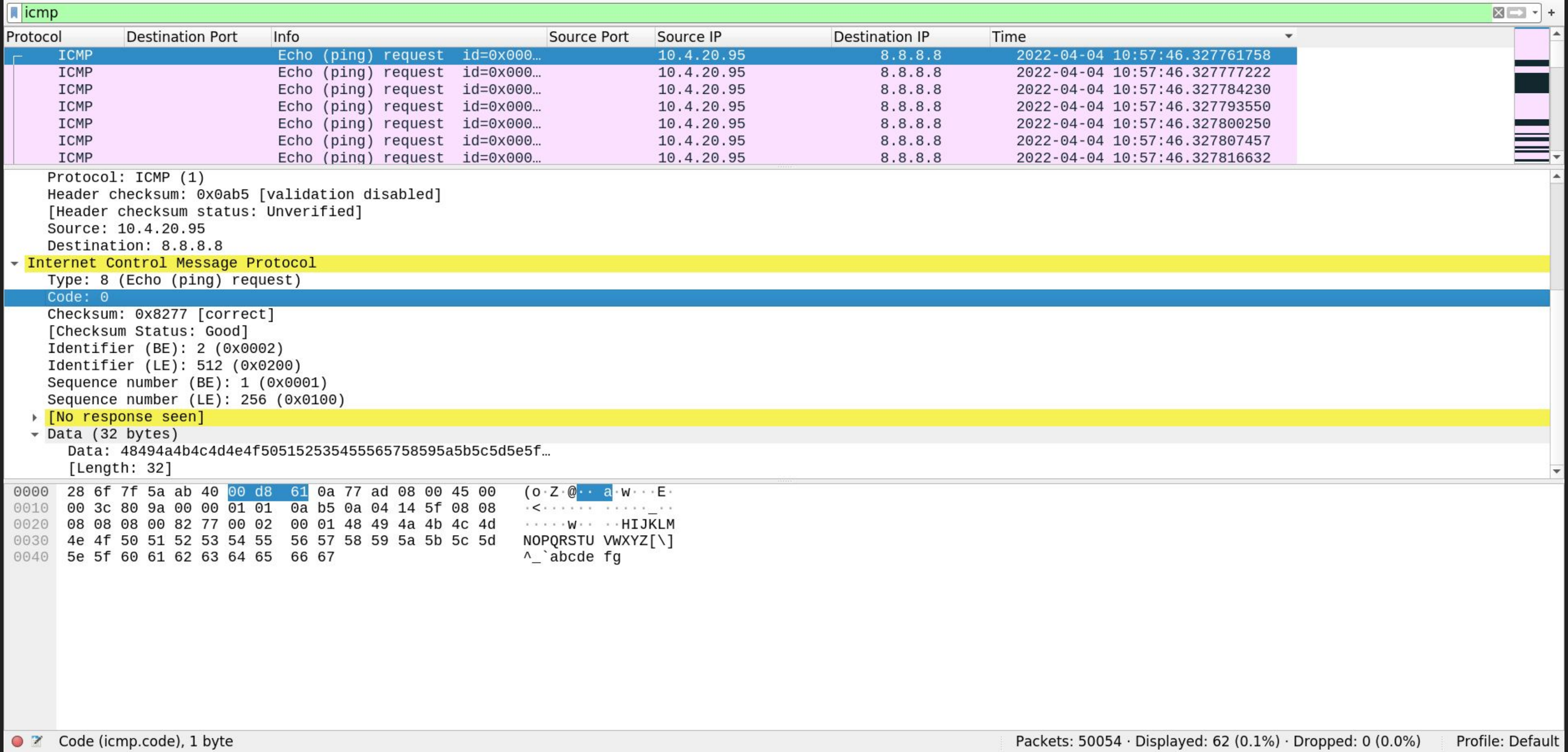
```
0000  28 6f 7f 5a ab 40 00 d8  61 0a 77 ad 08 00 45 00   (o·Z·@·· a·w···E·
0010  00 3c 80 9a 00 00 01 01  0a b5 0a 04 14 5f 08 08   ·<······ ·····_··
0020  08 08 08 00 82 77 00 02  00 01 48 49 4a 4b 4c 4d   ·····w·· ··HIJKLM
0030  4e 4f 50 51 52 53 54 55  56 57 58 59 5a 5b 5c 5d   NOPQRSTU VWXYZ[\]
0040  5e 5f 60 61 62 63 64 65  66 67                     ^_`abcde fg
```

Type (icmp.type), 1 byte   Packets: 50054 · Displayed: 62 (0.1%) · Dropped: 0 (0.0%)   Profile: Default

Highlighted byte is Type byte

3) Show a round of execution of traceroute command for dns.google

B. Identify bytes that represent type and code in Echo packet.



icmp

Protocol	Destination Port	Info	Source Port	Source IP	Destination IP	Time
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327761758
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327777222
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327784230
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327793550
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327800250
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327807457
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327816632

```
    Protocol: ICMP (1)
    Header checksum: 0x0ab5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.4.20.95
    Destination: 8.8.8.8
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x8277 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
  ▸ [No response seen]
  ▾ Data (32 bytes)
      Data: 48494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f…
      [Length: 32]
```

```
0000   28 6f 7f 5a ab 40 00 d8  61 0a 77 ad 08 00 45 00   (o·Z·@·· a·w···E·
0010   00 3c 80 9a 00 00 01 01  0a b5 0a 04 14 5f 08 08   ·<······ ·····_··
0020   08 08 08 00 82 77 00 02  00 01 48 49 4a 4b 4c 4d   ·····w·· ··HIJKLM
0030   4e 4f 50 51 52 53 54 55  56 57 58 59 5a 5b 5c 5d   NOPQRSTU VWXYZ[\]
0040   5e 5f 60 61 62 63 64 65  66 67                     ^_`abcde fg
```

Code (icmp.code), 1 byte

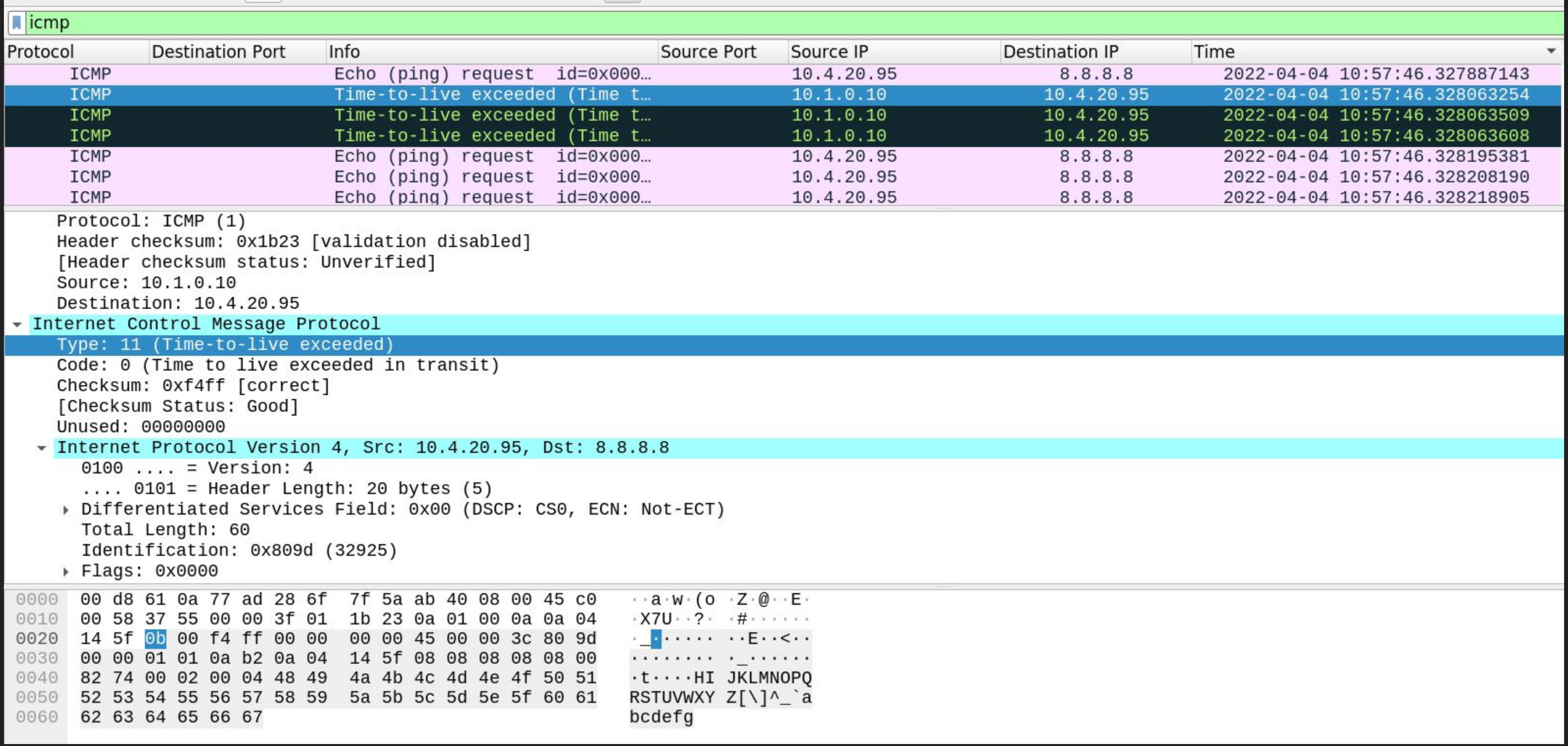
Packets: 50054 · Displayed: 62 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

Highlighted byte is Code byte

3) Show a round of execution of traceroute command for dns.google

C. Identify bytes that represent type and code in Error packet.



```
icmp
```

```
Protocol   Destination Port   Info                                  Source Port   Source IP      Destination IP   Time
  ICMP                         Echo (ping) request  id=0x000…                      10.4.20.95        8.8.8.8        2022-04-04 10:57:46.327887143
  ICMP                         Time-to-live exceeded (Time t…                      10.1.0.10      10.4.20.95        2022-04-04 10:57:46.328063254
  ICMP                         Time-to-live exceeded (Time t…                      10.1.0.10      10.4.20.95        2022-04-04 10:57:46.328063509
  ICMP                         Time-to-live exceeded (Time t…                      10.1.0.10      10.4.20.95        2022-04-04 10:57:46.328063608
  ICMP                         Echo (ping) request  id=0x000…                      10.4.20.95        8.8.8.8        2022-04-04 10:57:46.328195381
  ICMP                         Echo (ping) request  id=0x000…                      10.4.20.95        8.8.8.8        2022-04-04 10:57:46.328208190
  ICMP                         Echo (ping) request  id=0x000…                      10.4.20.95        8.8.8.8        2022-04-04 10:57:46.328218905
```

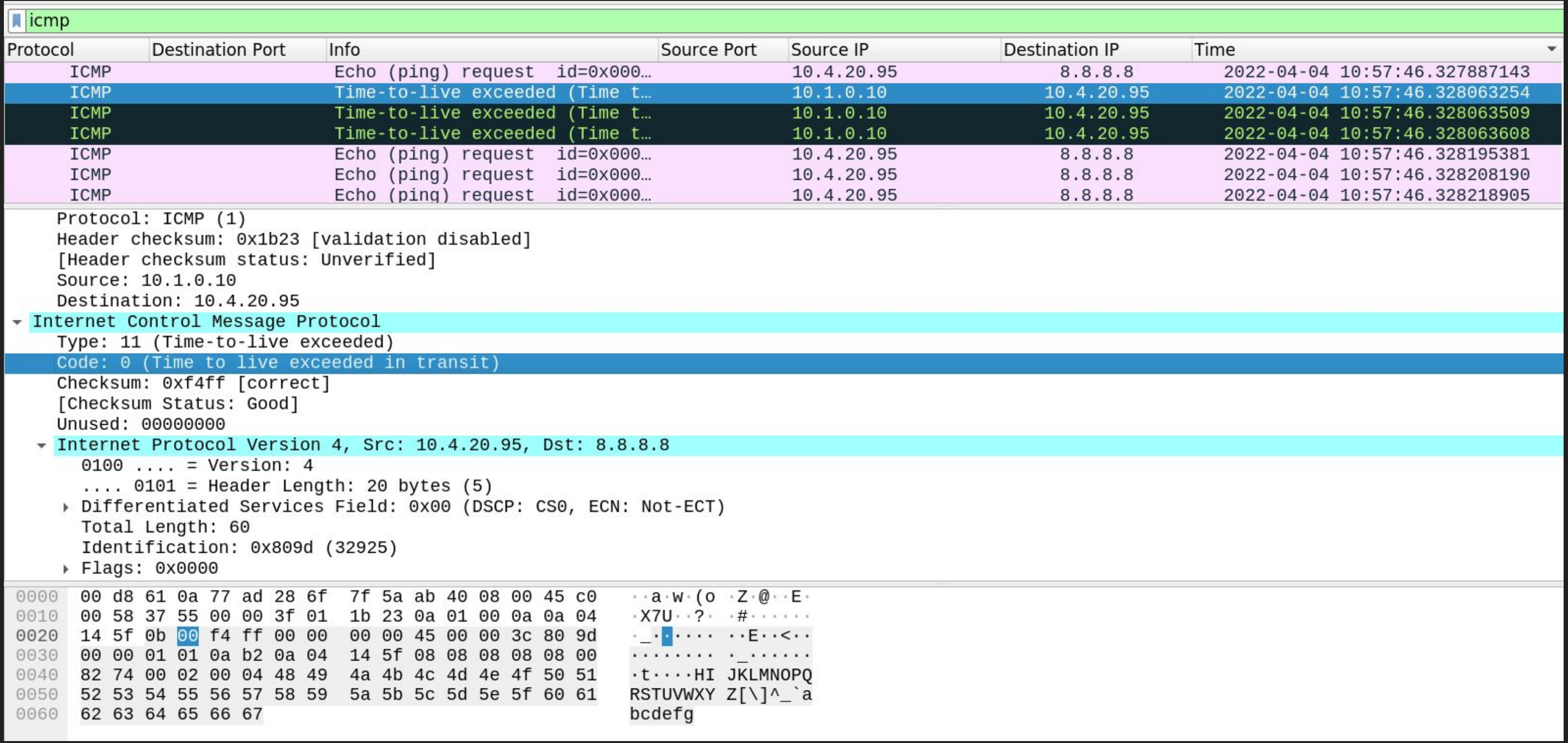
```
    Protocol: ICMP (1)
    Header checksum: 0x1b23 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.1.0.10
    Destination: 10.4.20.95
▾ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ▾ Internet Protocol Version 4, Src: 10.4.20.95, 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: 0x809d (32925)
    ▸ Flags: 0x0000
```

```
0000   00 d8 61 0a 77 ad 28 6f  7f 5a ab 40 08 00 45 c0   ··a·w·(o ·Z·@··E·
0010   00 58 37 55 00 00 3f 01  1b 23 0a 01 00 0a 0a 04   ·X7U··?· ·#······
0020   14 5f 0b 00 f4 ff 00 00  00 00 45 00 00 3c 80 9d   ·_······ ··E··<··
0030   00 00 01 01 0a b2 0a 04  14 5f 08 08 08 08 08 00   ········ ·_······
0040   82 74 00 02 00 04 48 49  4a 4b 4c 4d 4e 4f 50 51   ·t····HI JKLMNOPQ
0050   52 53 54 55 56 57 58 59  5a 5b 5c 5d 5e 5f 60 61   RSTUVWXY Z[\]^_`a
0060   62 63 64 65 66 67                                  bcdefg
```

Highlighted byte is Type byte

3) Show a round of execution of traceroute command for dns.google

C. Identify bytes that represent type and code in Error packet.



icmp

Protocol	Destination Port	Info	Source Port	Source IP	Destination IP	Time
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.327887143
ICMP		Time-to-live exceeded (Time t…		10.1.0.10	10.4.20.95	2022-04-04 10:57:46.328063254
ICMP		Time-to-live exceeded (Time t…		10.1.0.10	10.4.20.95	2022-04-04 10:57:46.328063509
ICMP		Time-to-live exceeded (Time t…		10.1.0.10	10.4.20.95	2022-04-04 10:57:46.328063608
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.328195381
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.328208190
ICMP		Echo (ping) request id=0x000…		10.4.20.95	8.8.8.8	2022-04-04 10:57:46.328218905

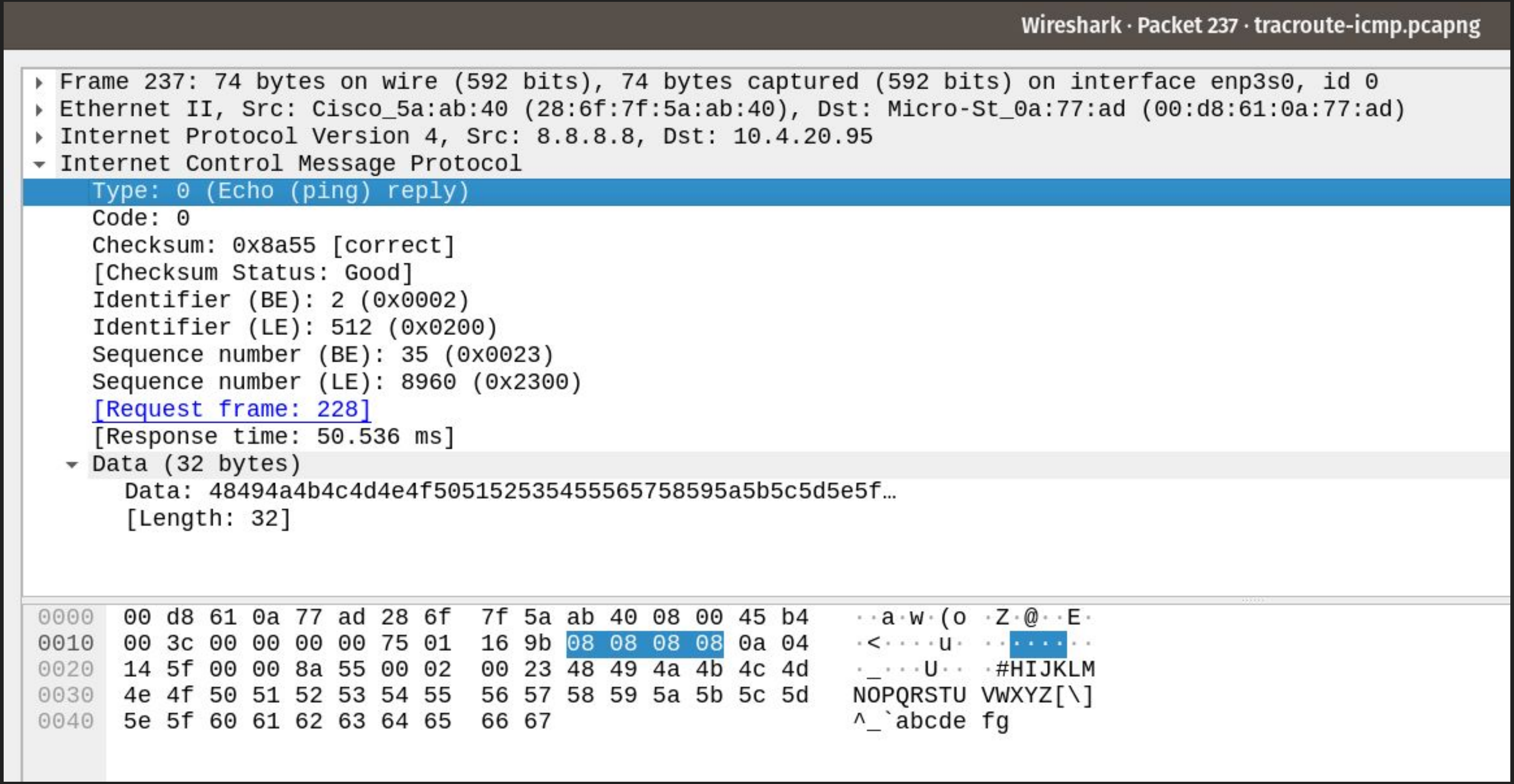
```
    Protocol: ICMP (1)
    Header checksum: 0x1b23 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.1.0.10
    Destination: 10.4.20.95
▾ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ▾ Internet Protocol Version 4, Src: 10.4.20.95, 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: 0x809d (32925)
    ▸ Flags: 0x0000
```

```
0000  00 d8 61 0a 77 ad 28 6f  7f 5a ab 40 08 00 45 c0   ··a·w·(o ·Z·@··E·
0010  00 58 37 55 00 00 3f 01  1b 23 0a 01 00 0a 0a 04   ·X7U··?· ·#······
0020  14 5f 0b 00 f4 ff 00 00  00 00 45 00 00 3c 80 9d   ·_······ ··E··<··
0030  00 00 01 01 0a b2 0a 04  14 5f 08 08 08 08 08 00   ········ ·_······
0040  82 74 00 02 00 04 48 49  4a 4b 4c 4d 4e 4f 50 51   ·t····HI JKLMNOPQ
0050  52 53 54 55 56 57 58 59  5a 5b 5c 5d 5e 5f 60 61   RSTUVWXY Z[\]^_`a
0060  62 63 64 65 66 67                                  bcdefg
```

Highlighted byte is Code byte

3) Show a round of execution of traceroute command for dns.google

D. Examine the last 3 ICMP packets



Wireshark · Packet 237 · tracroute-icmp.pcapng

```
▸ Frame 237: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp3s0, id 0
▸ Ethernet II, Src: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40), Dst: Micro-St_0a:77:ad (00:d8:61:0a:77:ad)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.4.20.95
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x8a55 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence number (BE): 35 (0x0023)
    Sequence number (LE): 8960 (0x2300)
    [Request frame: 228]
    [Response time: 50.536 ms]
  ▾ Data (32 bytes)
      Data: 48494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f…
      [Length: 32]
```

```
0000  00 d8 61 0a 77 ad 28 6f  7f 5a ab 40 08 00 45 b4   ··a·w·(o ·Z·@··E·
0010  00 3c 00 00 00 00 75 01  16 9b 08 08 08 08 0a 04   ·<····u· ········
0020  14 5f 00 00 8a 55 00 02  00 23 48 49 4a 4b 4c 4d   ·_···U·· ·#HIJKLM
0030  4e 4f 50 51 52 53 54 55  56 57 58 59 5a 5b 5c 5d   NOPQRSTU VWXYZ[\]
0040  5e 5f 60 61 62 63 64 65  66 67                     ^_`abcde fg
```

3) Show a round of execution of traceroute command for dns.google

D. Examine the last 3 ICMP packets

The screenshot in the previous page shows one of the last 3 ICMP packets received by the host.

How are they different?

1. Source IP is 8.8.8.8
2. Type is 0
3. Response Time is seen

Why are they different?

They are different because these packets are replies from the destination server. These are not error packets that are sent by intermediate hops.