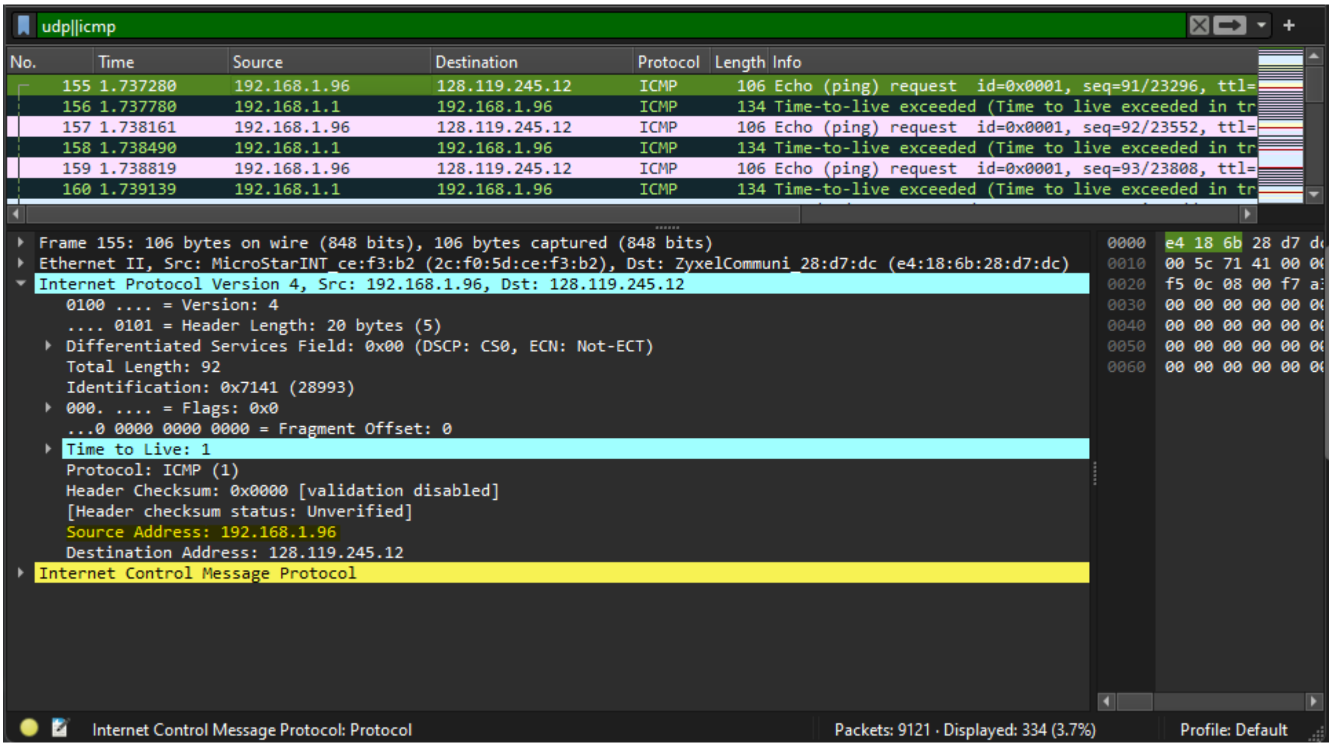
WSA5

2448025

1. Source Address: 192.168.1.96
2. Time to Live: 1
3. Upper Layer Protocol is ICMP (0x01)



udp||icmp

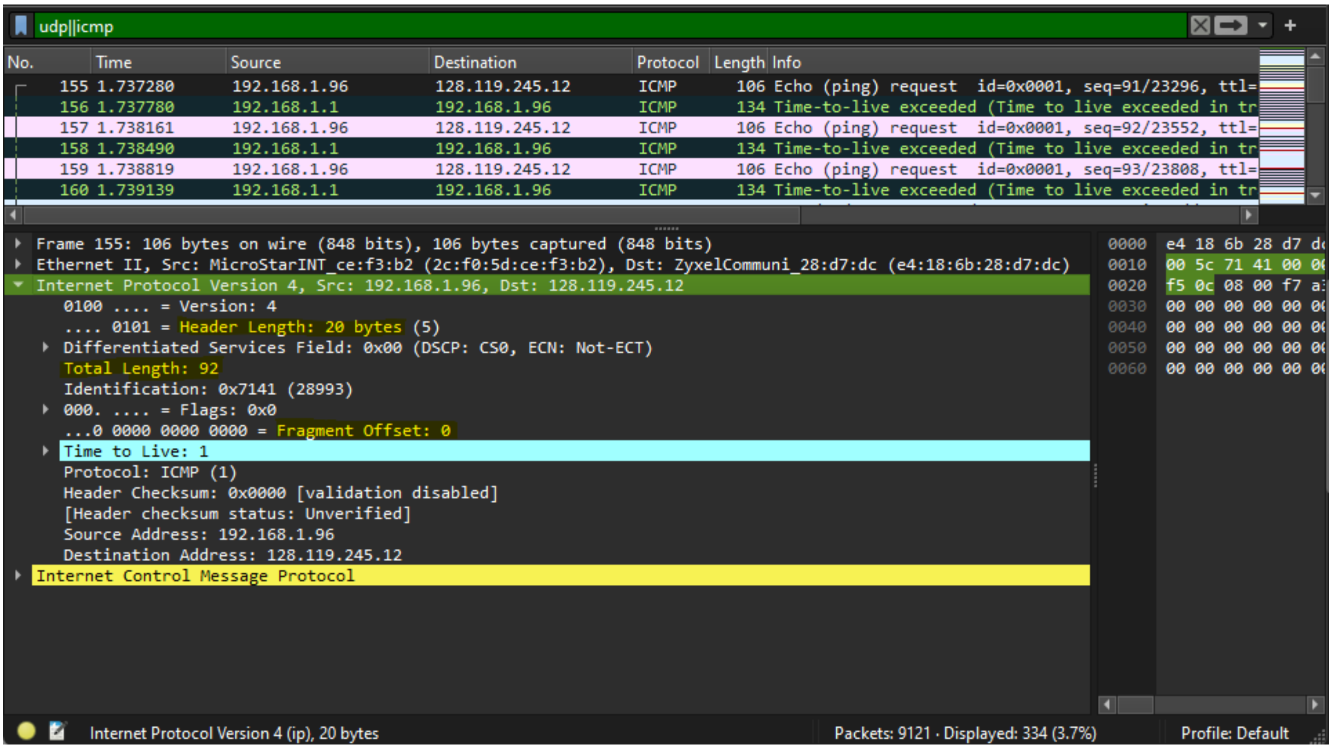
```
No.   Time       Source          Destination      Protocol Length Info
  155 1.737280   192.168.1.96    128.119.245.12   ICMP     106 Echo (ping) request  id=0x0001, seq=91/23296, ttl=
  156 1.737780   192.168.1.1     192.168.1.96     ICMP     134 Time-to-live exceeded (Time to live exceeded in tr
  157 1.738161   192.168.1.96    128.119.245.12   ICMP     106 Echo (ping) request  id=0x0001, seq=92/23552, ttl=
  158 1.738490   192.168.1.1     192.168.1.96     ICMP     134 Time-to-live exceeded (Time to live exceeded in tr
  159 1.738819   192.168.1.96    128.119.245.12   ICMP     106 Echo (ping) request  id=0x0001, seq=93/23808, ttl=
  160 1.739139   192.168.1.1     192.168.1.96     ICMP     134 Time-to-live exceeded (Time to live exceeded in tr
```

```
> Frame 155: 106 bytes on wire (848 bits), 106 bytes captured (848 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)
v Internet Protocol Version 4, Src: 192.168.1.96, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x7141 (28993)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.96
    Destination Address: 128.119.245.12
> Internet Control Message Protocol
```

```
0000  e4 18 6b 28 d7 d
0010  00 5c 71 41 00 0
0020  f5 0c 08 00 f7 a
0030  00 00 00 00 00 0
0040  00 00 00 00 00 0
0050  00 00 00 00 00 0
0060  00 00 00 00 00 0
```

Internet Control Message Protocol: Protocol   Packets: 9121 · Displayed: 334 (3.7%)   Profile: Default

4. Header Length: 20 bytes
5. Payload Length is 72 bytes because Payload Length = Total Length - Header Length = (92 -20 = 72)
6. The packet has not been fragmented because Fragment Offset is 0.



udp||icmp

```
No.   Time       Source          Destination      Protocol Length Info
  155 1.737280   192.168.1.96    128.119.245.12   ICMP     106 Echo (ping) request  id=0x0001, seq=91/23296, ttl=
  156 1.737780   192.168.1.1     192.168.1.96     ICMP     134 Time-to-live exceeded (Time to live exceeded in tr
  157 1.738161   192.168.1.96    128.119.245.12   ICMP     106 Echo (ping) request  id=0x0001, seq=92/23552, ttl=
  158 1.738490   192.168.1.1     192.168.1.96     ICMP     134 Time-to-live exceeded (Time to live exceeded in tr
  159 1.738819   192.168.1.96    128.119.245.12   ICMP     106 Echo (ping) request  id=0x0001, seq=93/23808, ttl=
  160 1.739139   192.168.1.1     192.168.1.96     ICMP     134 Time-to-live exceeded (Time to live exceeded in tr
```

```
> Frame 155: 106 bytes on wire (848 bits), 106 bytes captured (848 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)
v Internet Protocol Version 4, Src: 192.168.1.96, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x7141 (28993)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.96
    Destination Address: 128.119.245.12
> Internet Control Message Protocol
```

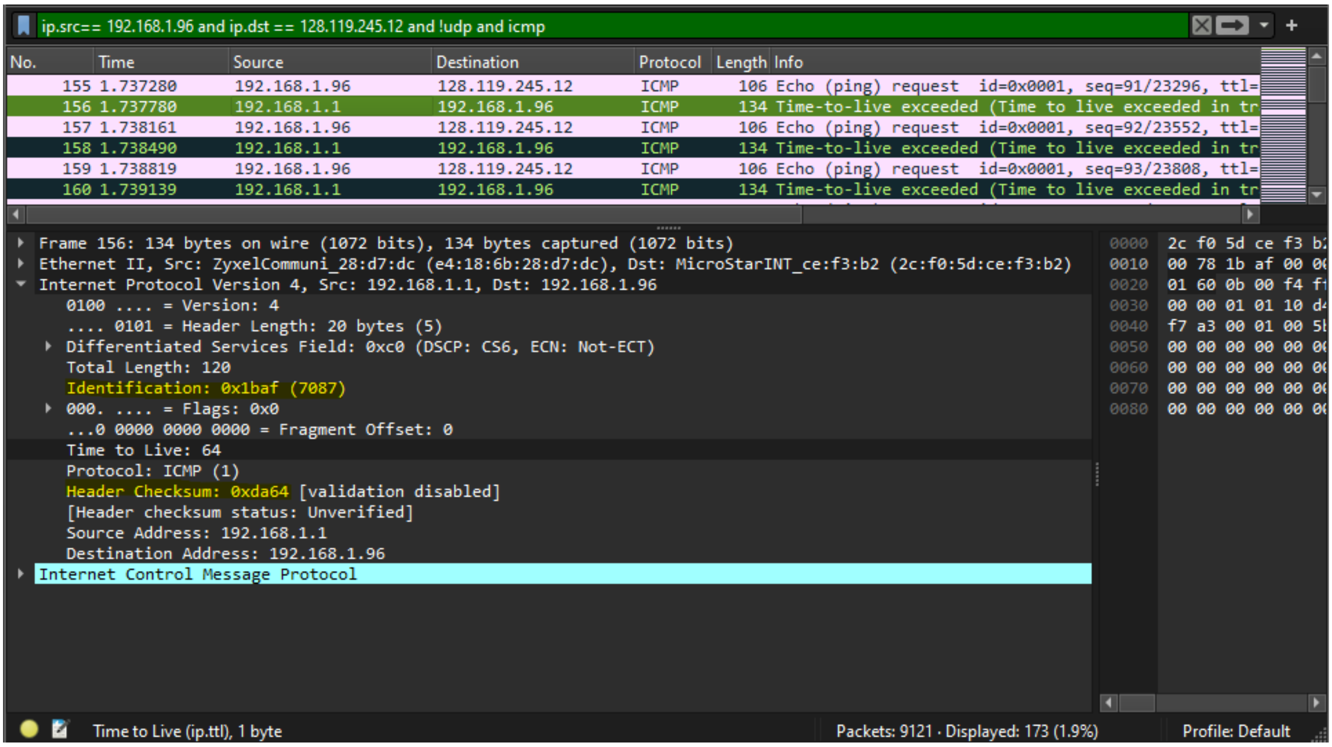
```
0000  e4 18 6b 28 d7 d
0010  00 5c 71 41 00 0
0020  f5 0c 08 00 f7 a
0030  00 00 00 00 00 0
0040  00 00 00 00 00 0
0050  00 00 00 00 00 0
0060  00 00 00 00 00 0
```

Internet Protocol Version 4 (ip), 20 bytes   Packets: 9121 · Displayed: 334 (3.7%)   Profile: Default

7. The following fields are always change each datagram to the next:
    - Identification (as it is used for uniquely identify fragments, it changes when fragmentation occurs),
    - Header Checksum (as it is used for Error-Checking, it should recalculated when IP header changes)

8. The following fields are consistent throughout IP datagrams:
    - Source Address (as we are sending from same source) ,
    - Destination Address (as we are sending to same),
    - Version (as we are using IPv4 for all packets) ,
    - Header Length (as header length is same for all ICMP packets),
    - Differentiated Services Field (as all ICMP packets use the same Type of Service),
    - Upper Layer Protocol (as they are all ICMP packets)

9. With every ICMP Echo (ping) request, there is a pattern where the IP header Identification fields increase.

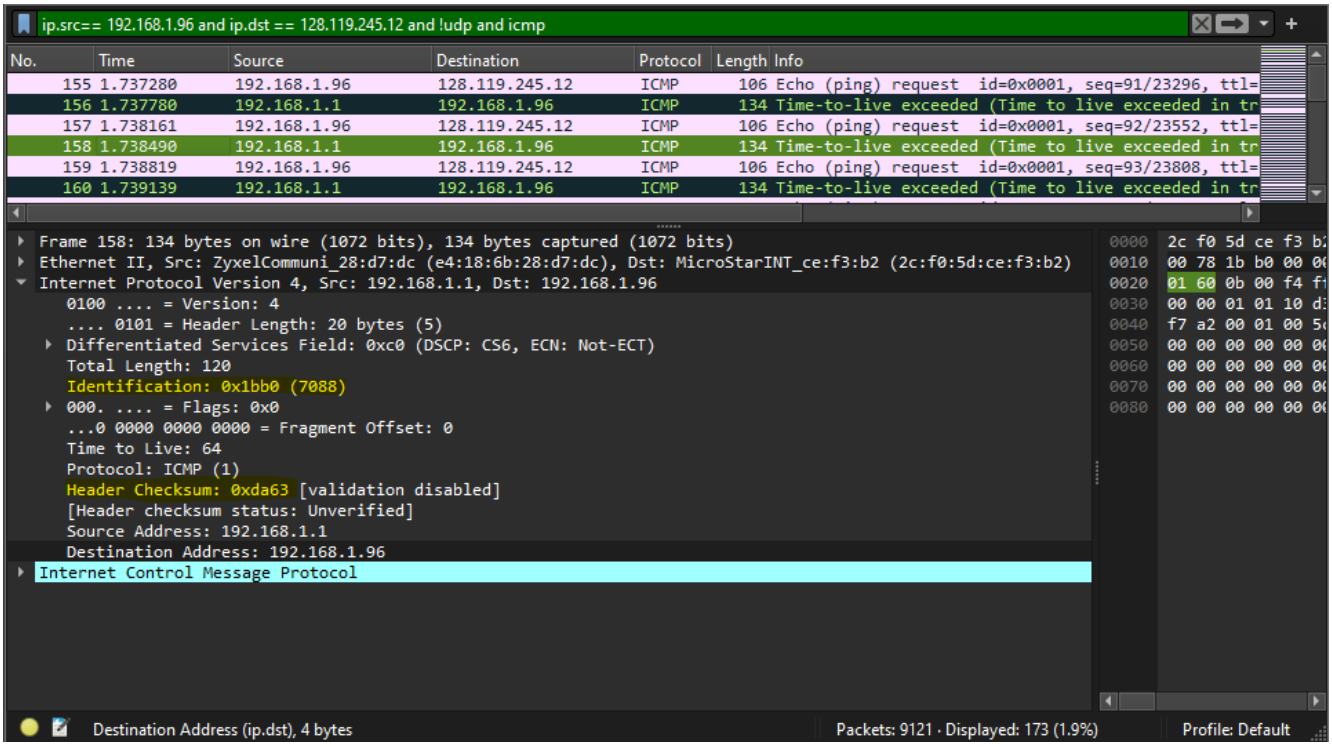


```
ip.src== 192.168.1.96 and ip.dst == 128.119.245.12 and !udp and icmp

No.   Time         Source          Destination       Protocol  Length Info
  155 1.737280     192.168.1.96    128.119.245.12    ICMP      106 Echo (ping) request  id=0x0001, seq=91/23296, ttl=
  156 1.737780     192.168.1.1     192.168.1.96      ICMP      134 Time-to-live exceeded (Time to live exceeded in tr
  157 1.738161     192.168.1.96    128.119.245.12    ICMP      106 Echo (ping) request  id=0x0001, seq=92/23552, ttl=
  158 1.738490     192.168.1.1     192.168.1.96      ICMP      134 Time-to-live exceeded (Time to live exceeded in tr
  159 1.738819     192.168.1.96    128.119.245.12    ICMP      106 Echo (ping) request  id=0x0001, seq=93/23808, ttl=
  160 1.739139     192.168.1.1     192.168.1.96      ICMP      134 Time-to-live exceeded (Time to live exceeded in tr

Frame 156: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)          0000  2c f0 5d ce f3 b
Ethernet II, Src: ZyxelCommuni_28:d7:dc (e4:18:6b:28:d7:dc), Dst: MicroStarINT_ce:f3:b2 (2c:f0:5d:ce:f3:b2)   0010  00 78 1b af 00 0
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.96                   0020  01 60 0b 00 f4 f
    0100 .... = Version: 4                                                         0030  00 00 01 01 10 d
    .... 0101 = Header Length: 20 bytes (5)                                        0040  f7 a3 00 01 00 5
    Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)                  0050  00 00 00 00 00 0
    Total Length: 120                                                              0060  00 00 00 00 00 0
    Identification: 0x1baf (7087)                                                  0070  00 00 00 00 00 0
    000. .... = Flags: 0x0                                                         0080  00 00 00 00 00 0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xda64 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.1
    Destination Address: 192.168.1.96
Internet Control Message Protocol

Time to Live (ip.ttl), 1 byte          Packets: 9121 · Displayed: 173 (1.9%)          Profile: Default
```



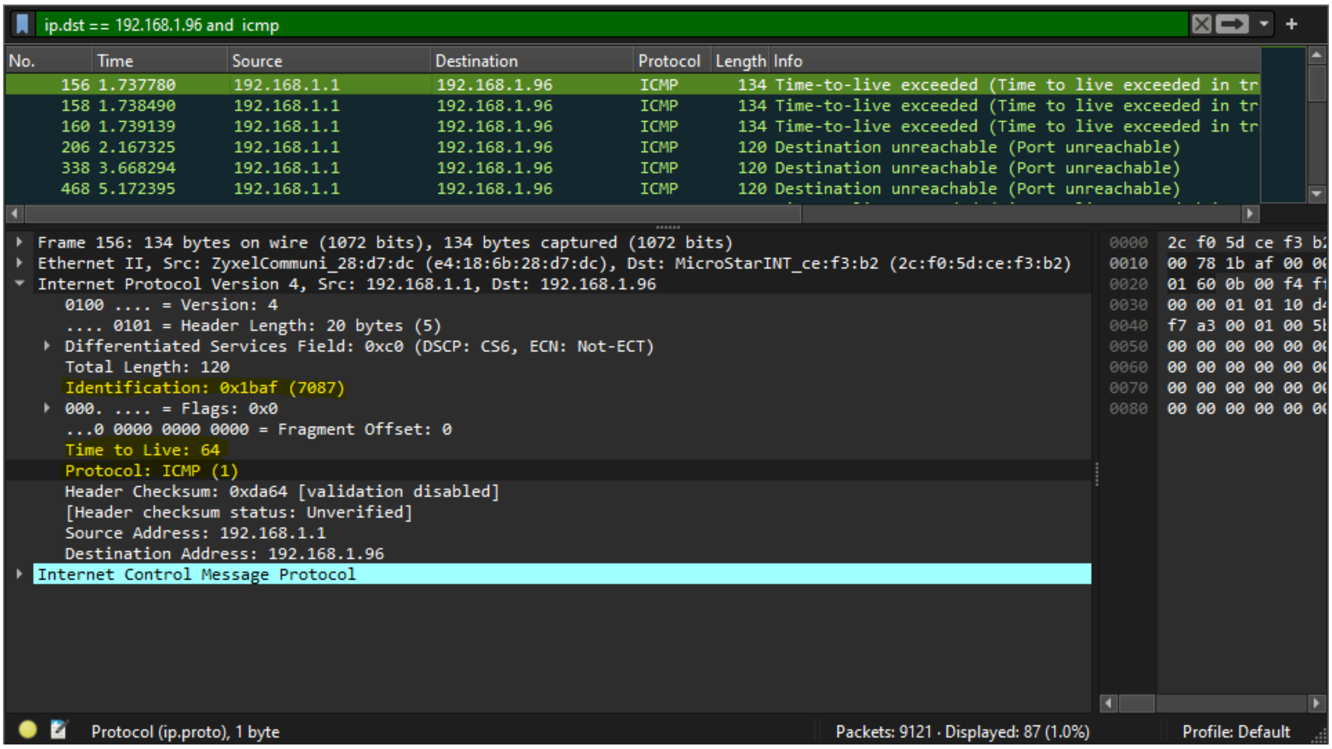
```
ip.src== 192.168.1.96 and ip.dst == 128.119.245.12 and !udp and icmp

No.   Time         Source          Destination       Protocol  Length Info
  155 1.737280     192.168.1.96    128.119.245.12    ICMP      106 Echo (ping) request  id=0x0001, seq=91/23296, ttl=
  156 1.737780     192.168.1.1     192.168.1.96      ICMP      134 Time-to-live exceeded (Time to live exceeded in tr
  157 1.738161     192.168.1.96    128.119.245.12    ICMP      106 Echo (ping) request  id=0x0001, seq=92/23552, ttl=
  158 1.738490     192.168.1.1     192.168.1.96      ICMP      134 Time-to-live exceeded (Time to live exceeded in tr
  159 1.738819     192.168.1.96    128.119.245.12    ICMP      106 Echo (ping) request  id=0x0001, seq=93/23808, ttl=
  160 1.739139     192.168.1.1     192.168.1.96      ICMP      134 Time-to-live exceeded (Time to live exceeded in tr

Frame 158: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)          0000  2c f0 5d ce f3 b
Ethernet II, Src: ZyxelCommuni_28:d7:dc (e4:18:6b:28:d7:dc), Dst: MicroStarINT_ce:f3:b2 (2c:f0:5d:ce:f3:b2)   0010  00 78 1b b0 00 0
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.96                   0020  01 60 0b 00 f4 f
    0100 .... = Version: 4                                                         0030  00 00 01 01 10 d
    .... 0101 = Header Length: 20 bytes (5)                                        0040  f7 a2 00 01 00 5
    Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)                  0050  00 00 00 00 00 0
    Total Length: 120                                                              0060  00 00 00 00 00 0
    Identification: 0x1bb0 (7088)                                                  0070  00 00 00 00 00 0
    000. .... = Flags: 0x0                                                         0080  00 00 00 00 00 0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xda63 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.1
    Destination Address: 192.168.1.96
Internet Control Message Protocol

Destination Address (ip.dst), 4 bytes          Packets: 9121 · Displayed: 173 (1.9%)          Profile: Default
```

10. The upper layer protocol of IP datagrams returned from the routers is ICMP (0x01).
11. Yes, all the routers' ICMP packets have Identification fields that behave similarly to the datagrams I send from my PC.
12. No, TTL values in ICMP packets from different routers are not necessarily the same. Routers decrement the TTL values by 1 for each hop.



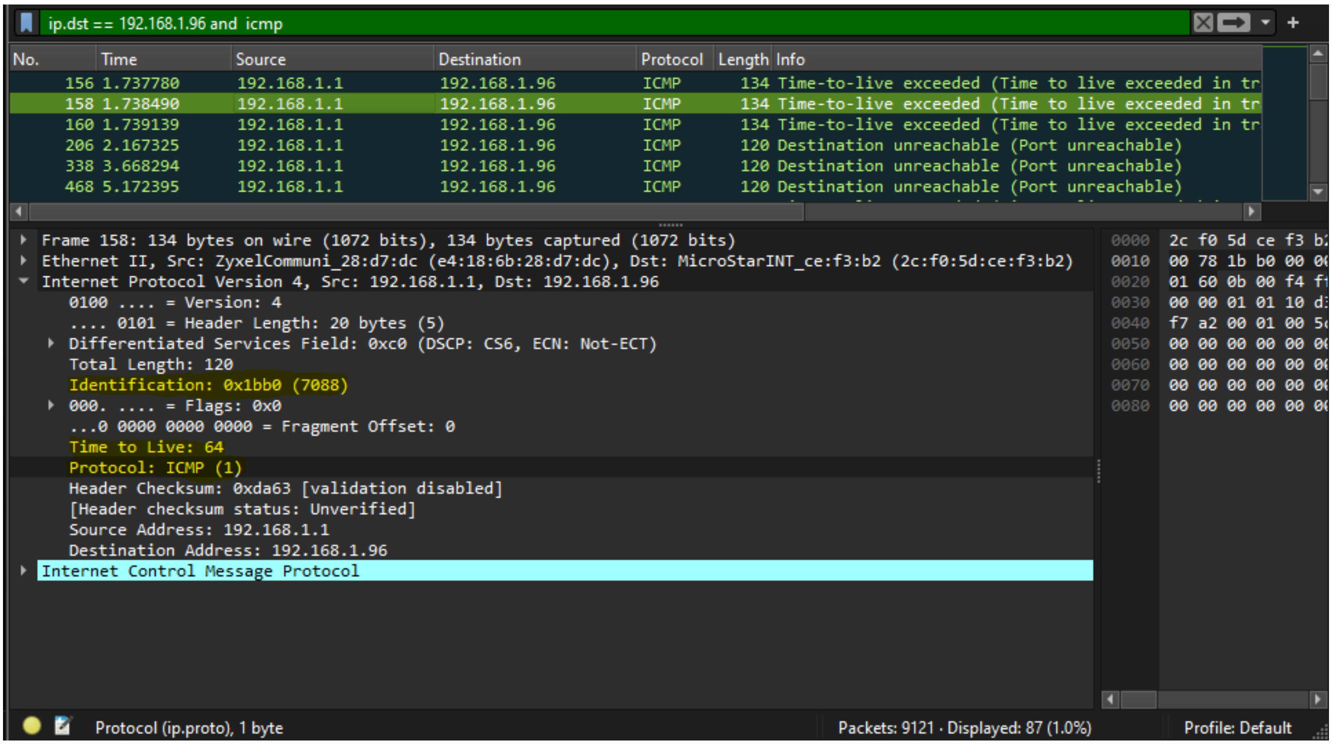
ip.dst == 192.168.1.96 and icmp

```
No.   Time       Source        Destination   Protocol Length Info
  156 1.737780   192.168.1.1   192.168.1.96  ICMP     134 Time-to-live exceeded (Time to live exceeded in tr
  158 1.738490   192.168.1.1   192.168.1.96  ICMP     134 Time-to-live exceeded (Time to live exceeded in tr
  160 1.739139   192.168.1.1   192.168.1.96  ICMP     134 Time-to-live exceeded (Time to live exceeded in tr
  206 2.167325   192.168.1.1   192.168.1.96  ICMP     120 Destination unreachable (Port unreachable)
  338 3.668294   192.168.1.1   192.168.1.96  ICMP     120 Destination unreachable (Port unreachable)
  468 5.172395   192.168.1.1   192.168.1.96  ICMP     120 Destination unreachable (Port unreachable)
```

```
> Frame 156: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)
> Ethernet II, Src: ZyxelCommuni_28:d7:dc (e4:18:6b:28:d7:dc), Dst: MicroStarINT_ce:f3:b2 (2c:f0:5d:ce:f3:b2)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.96
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 120
    Identification: 0x1baf (7087)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xda64 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.1
    Destination Address: 192.168.1.96
> Internet Control Message Protocol
```

```
0000  2c f0 5d ce f3 b
0010  00 78 1b af 00 0
0020  01 60 0b 00 f4 f
0030  00 00 01 01 10 d
0040  f7 a3 00 01 00 5
0050  00 00 00 00 00 0
0060  00 00 00 00 00 0
0070  00 00 00 00 00 0
0080  00 00 00 00 00 0
```

Protocol (ip.proto), 1 byte   Packets: 9121 · Displayed: 87 (1.0%)   Profile: Default



ip.dst == 192.168.1.96 and icmp

```
No.   Time       Source        Destination   Protocol Length Info
  156 1.737780   192.168.1.1   192.168.1.96  ICMP     134 Time-to-live exceeded (Time to live exceeded in tr
  158 1.738490   192.168.1.1   192.168.1.96  ICMP     134 Time-to-live exceeded (Time to live exceeded in tr
  160 1.739139   192.168.1.1   192.168.1.96  ICMP     134 Time-to-live exceeded (Time to live exceeded in tr
  206 2.167325   192.168.1.1   192.168.1.96  ICMP     120 Destination unreachable (Port unreachable)
  338 3.668294   192.168.1.1   192.168.1.96  ICMP     120 Destination unreachable (Port unreachable)
  468 5.172395   192.168.1.1   192.168.1.96  ICMP     120 Destination unreachable (Port unreachable)
```

```
> Frame 158: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)
> Ethernet II, Src: ZyxelCommuni_28:d7:dc (e4:18:6b:28:d7:dc), Dst: MicroStarINT_ce:f3:b2 (2c:f0:5d:ce:f3:b2)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.96
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 120
    Identification: 0x1bb0 (7088)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xda63 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.1
    Destination Address: 192.168.1.96
> Internet Control Message Protocol
```

```
0000  2c f0 5d ce f3 b
0010  00 78 1b b0 00 0
0020  01 60 0b 00 f4 f
0030  00 00 01 01 10 d
0040  f7 a2 00 01 00 5
0050  00 00 00 00 00 0
0060  00 00 00 00 00 0
0070  00 00 00 00 00 0
0080  00 00 00 00 00 0
```

Protocol (ip.proto), 1 byte   Packets: 9121 · Displayed: 87 (1.0%)   Profile: Default