

**HO CHI MINH UNIVERSITY OF TECHNOLOGY**  
Faculty of Computer Science and Engineering

---



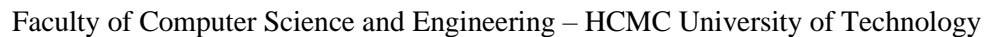
# Computer Networks

---

## Report for lab 4a

Lecture: Nguyễn Mạnh Thìn  
Student name: Đặng Trần Khánh-1852037



[illegible]

**3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.**

Answer: There are 20 bytes in the IP header (image below). Because the total length of the IP datagram is 56 bytes, the payload consists of  $56 - 20$  (header bytes) = 36 bytes.

```
> Frame 465: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{3219B7F4}
> Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HewlettP_4d:44:ac (00:26:55:4d:44:ac)
√ Internet Protocol Version 4, Src: 10.127.14.142, Dst: 172.217.25.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x2ecd (11981)
> Flags: 0x0000
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0xae0d [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.127.14.142
    Destination: 172.217.25.4
> Internet Control Message Protocol
```

**4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.**

Answer: The fragment offset field is 0 and the more fragments field is not set, therefore this IP datagram has not been fragmented.

```
> Frame 465: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{3219B7F4}
> Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HewlettP_4d:44:ac (00:26:55:4d:44:ac)
√ Internet Protocol Version 4, Src: 10.127.14.142, Dst: 172.217.25.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x2ecd (11981)
√ Flags: 0x0000
    0... .. = Reserved bit: Not set
    .0.. .. = Don't fragment: Not set
    ..0. .. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0xae0d [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.127.14.142
    Destination: 172.217.25.4
> Internet Control Message Protocol
```

**5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?**

Answer: Identification, Time to live and Header checksum always change from one datagram to the next within this series of ICMP messages sent by my computer.

**6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?**

Answer:

Fields stay constant:

- 1/ Version (IPv4 for all packets)
- 2/ Header length (doesn't change since we are always using IPv4)
- 3/ Source IP (my computer's IP address doesn't change)
- 4/ Destination IP (the site IP address doesn't change)
- 5/ Differentiated Services (since all packets are ICMP they use the same Type of Service class)
- 6/ Upper Layer Protocol (always using ICMP)

Fields must stay constant:

Same as fields stay constant: version, header length, source IP, destination IP, differentiated services, upper layer protocol.

```
> Frame 465: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{3219B7F...}
> Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HewlettP_4d:44:ac (00:26:55:4d:44:ac)
< Internet Protocol Version 4, Src: 10.127.14.142, Dst: 172.217.25.4
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x2ecd (11981)
  < Flags: 0x0000
    0... .. = Reserved bit: Not set
    .0.. .. = Don't fragment: Not set
    ..0. .. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0xae0d [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.127.14.142
    Destination: 172.217.25.4
  > Internet Control Message Protocol
```

Fields must change:

- 1/ Identification (Each IP packet must have different id to distinguish)
- 2/ Time to live (traceroute increments each subsequent packet as described in the lab specification)
- 3/ Header checksum (Header changes every time, therefore checksum also has to change)

```

> Frame 465: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{3219B7F4-C797-4F0F-9E1A-7D5DFE741F02}
> Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HewlettP_4d:44:ac (00:26:55:4d:44:ac)
v Internet Protocol Version 4, Src: 10.127.14.142, Dst: 172.217.25.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 56
        Identification: 0x2ecd (11981)
    v Flags: 0x0000
        0... .. = Reserved bit: Not set
        .0.. .. = Don't fragment: Not set
        ..0. .... = More fragments: Not set
        Fragment offset: 0
        Time to live: 255
        Protocol: ICMP (1)
        Header checksum: 0xae0d [validation disabled]
        [Header checksum status: Unverified]
        Source: 10.127.14.142
        Destination: 172.217.25.4
    > Internet Control Message Protocol

```

### 7. Describe the pattern you see in the values in the Identification field of the IP datagram

Answer: The pattern in the Identification field of IP datagram is that IP header Identification fields increment with each ICMP Echo (ping) request.

491	07:29:56.911006	10.127.14.142	172.217.25.4	ICMP	70 Echo (ping) request	id=0x0003, seq=16976/20546, ttl=3
492	07:29:56.950759	10.127.14.142	172.217.25.4	ICMP	70 Echo (ping) request	id=0x0003, seq=16977/20802, ttl=4
493	07:29:56.952229	10.127.128.69	224.0.0.251	MDNS	70 Standard query 0x0000 A wpad.local, "QM" question	

```

> Frame 491: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{3219B7F4-C797-4F0F-9E1A-7D5DFE741F02},
> Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HewlettP_4d:44:ac (00:26:55:4d:44:ac)
v Internet Protocol Version 4, Src: 10.127.14.142, Dst: 172.217.25.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 56
        Identification: 0x2ed0 (11984)
    v Flags: 0x0000
        0... .. = Reserved bit: Not set
        .0.. .. = Don't fragment: Not set
        ..0. .... = More fragments: Not set
        Fragment offset: 0
    > Time to live: 3
        Protocol: ICMP (1)
        Header checksum: 0xaa0b [validation disabled]
        [Header checksum status: Unverified]
        Source: 10.127.14.142
        Destination: 172.217.25.4
    v Internet Control Message Protocol

```



491	07:29:56.911006	10.127.14.142	172.217.25.4	ICMP	70 Echo (ping) request id=0x0003, seq=16976/20546, ttl=3
492	07:29:56.950759	10.127.14.142	172.217.25.4	ICMP	70 Echo (ping) request id=0x0003, seq=16977/20802, ttl=4
493	07:29:56.952229	10.127.128.69	224.0.0.251	MDNS	70 Standard query 0x0000 A wpad.local, "QM" question

>	Frame 492: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{3219B7F4-C797-4F0F-9E1A-7D5DFE741F02},
>	Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HewlettP_4d:44:ac (00:26:55:4d:44:ac)
✓	Internet Protocol Version 4, Src: 10.127.14.142, Dst: 172.217.25.4
0100	.... = Version: 4
.... 0101	= Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length:	56
Identification:	0x2ed1 (11985)
✓	Flags: 0x0000
0... ..	= Reserved bit: Not set
.0.. ..	= Don't fragment: Not set
..0. ..	= More fragments: Not set
Fragment offset:	0
>	Time to live: 4
Protocol:	ICMP (1)
Header checksum:	0xa90a [validation disabled]
[Header checksum status:	Unverified]
Source:	10.127.14.142
Destination:	172.217.25.4
✓	Internet Control Message Protocol

The value increments from 11984 (the first image) to 11985 (second request).

### 8. What is the value in the Identification field and the TTL field?

Answer: The identification field is 0x0000 (0), the TTL field is 254.

4844	08:07:45.583124	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
4434	08:07:43.080261	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
4079	08:07:40.713773	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
3676	08:07:38.125986	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
3443	08:07:35.572458	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
3260	08:07:33.134172	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2849	08:07:30.637906	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2408	08:07:28.081203	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2077	08:07:25.577666	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1766	08:07:23.085593	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1511	08:07:20.559168	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1305	08:07:18.025536	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1084	08:07:15.546029	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
895	08:07:13.017702	14.169.128.1	10.127.14.142	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)

>	Ethernet II, Src: HewlettP_4d:44:ac (00:26:55:4d:44:ac), Dst: AzureWav_5b:72:7f (70:66:55:5b:72:7f)
✓	Internet Protocol Version 4, Src: 14.169.128.1, Dst: 10.127.14.142
0100	.... = Version: 4
.... 0101	= Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length:	56
Identification:	0x0000 (0)
✓	Flags: 0x0000
0... ..	= Reserved bit: Not set
.0.. ..	= Don't fragment: Not set
..0. ..	= More fragments: Not set
Fragment offset:	0
Time to live:	254
Protocol:	ICMP (1)
Header checksum:	0x150e [validation disabled]
[Header checksum status:	Unverified]
Source:	14.169.128.1
Destination:	10.127.14.142
✓	Internet Control Message Protocol
Type:	11 (Time-to-live exceeded)
Code:	0 (Time to live exceeded in transit)
Checksum:	0x28c9 [correct]

### 9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

Answer:

The TTL will remain unchanged because the first hop router is always the same. Identification field for all ICMP TTL-exceeded replies will change because it is assigned a unique value. When two or more IP datagrams have the same identification value that means that these IP datagrams are fragments of a single large IP datagram.

In the image below (the next ICMP of the question 8), identification field remains at 0, the time to live also remains at 254.

```

4844 08:07:45.583124 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4434 08:07:43.080261 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4079 08:07:40.713773 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
3676 08:07:38.125986 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
3443 08:07:35.572458 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
3260 08:07:33.134172 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
2849 08:07:30.637906 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
2408 08:07:28.081203 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
2077 08:07:25.577666 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
1766 08:07:23.085593 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
1511 08:07:20.559168 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
1305 08:07:18.025536 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
1084 08:07:15.546029 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
895 08:07:13.017702 14.169.128.1 10.127.14.142 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)

```

```

> Ethernet II, Src: HewlettP_4d:44:ac (00:26:55:4d:44:ac), Dst: AzureWav_5b:72:7f (70:66:55:5b:72:7f)
< Internet Protocol Version 4, Src: 14.169.128.1, Dst: 10.127.14.142
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x0000 (0)
  < Flags: 0x0000
    0... .. = Reserved bit: Not set
    .0.. .. = Don't fragment: Not set
    ..0. .. = More fragments: Not set
    Fragment offset: 0
    Time to live: 254
    Protocol: ICMP (1)
    Header checksum: 0x150e [validation disabled]
    [Header checksum status: Unverified]
    Source: 14.169.128.1
    Destination: 10.127.14.142
  < Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x0aab [correct]

```

**10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?**

Answer: Yes, this packet has been fragmented across more than one IP datagram. The flags field shows that there are more fragments of this IP datagram.

2092	08:07:25.620109	10.127.14.142	216.58.200.14	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=cfa9) [Reassembled in #209]
2093	08:07:25.620109	10.127.14.142	216.58.200.14	ICMP	534	Echo (ping) request id=0x0003, seq=18696/2121, ttl=3 (no response found!)
2094	08:07:25.652051	172.17.5.33	10.127.14.142	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2095	08:07:25.652051	113.171.17.121	10.127.14.142	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2096	08:07:25.670365	10.127.14.142	216.58.200.14	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=cfaa) [Reassembled in #209]
2097	08:07:25.670365	10.127.14.142	216.58.200.14	ICMP	534	Echo (ping) request id=0x0003, seq=18697/2377, ttl=4 (no response found!)
2098	08:07:25.696086	fe80::e2dc:ffff:fed::ff02::2		ICMPv6	70	Router Solicitation from e0:dc:ff:d6:40:f1
2099	08:07:25.696454	Cisco_11:e0:b8	Broadcast	0x8899	60	Realtek Layer 2 Protocols
2100	08:07:25.697151	10.127.4.110	10.127.255.255	NBNS	92	Name query NB ASNXALWTO<00>
2101	08:07:25.697862	10.127.4.110	224.0.0.251	MDNS	75	Standard query 0x0000 A asnxalwto.local, "QM" question
2102	08:07:25.698638	fe80::3414:34ec:fa5::ff02::fb		MDNS	95	Standard query 0x0000 A asnxalwto.local, "QM" question
2103	08:07:25.699363	fe80::3414:34ec:fa5::ff02::1:3		LLMNR	89	Standard query 0x3231 A asnxalwto
2104	08:07:25.699862	9a:5f:9d:2c:05:df	Broadcast	ARP	60	ARP Announcement for 10.127.121.249

```

> Frame 2092: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{3219B7F4-C797-4F0F-9E1A-7D5DFE741F02}, id 0
> Ethernet II, Src: AzureWav_Sb:72:7f (70:66:55:5b:72:7f), Dst: HewlettP_Ad:44:ac (08:26:55:4d:44:ac)
> Internet Protocol Version 4, Src: 10.127.14.142, Dst: 216.58.200.14
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xcfa9 (53161)
  > Flags: 0x2000, More fragments
    0... .. = Reserved bit: Not set
    .0.. .. = Don't fragment: Not set
    ..1. .... = More fragments: Set
    Fragment offset: 0
  > Time to live: 3
  Protocol: ICMP (1)
  Header checksum: 0x0922 [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.127.14.142
  Destination: 216.58.200.14
  [Reassembled IPv4 in frame: 2093]
  > Data (1480 bytes)

```

**11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?**

Answer: The more fragments field is set, which indicates the datagram has been fragmented. The fragment offset (0) points out that this is the first fragment. The length of this fragment is 1500.



2092	08:07:25.620109	10.127.14.142	216.58.200.14	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=cfa9) [Reassembled in #209]
2093	08:07:25.620109	10.127.14.142	216.58.200.14	ICMP	534	Echo (ping) request id=0x0003, seq=18696/2121, ttl=3 (no response found!)
2094	08:07:25.652051	172.17.5.33	10.127.14.142	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2095	08:07:25.652051	113.171.17.121	10.127.14.142	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2096	08:07:25.670365	10.127.14.142	216.58.200.14	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=cfaa) [Reassembled in #209]
2097	08:07:25.670365	10.127.14.142	216.58.200.14	ICMP	534	Echo (ping) request id=0x0003, seq=18697/2377, ttl=4 (no response found!)
2098	08:07:25.696086	fe80::e2dc:ffff:fed...	ff02::2	ICMPv6	70	Router Solicitation from e0:dc:ff:d6:40:f1
2099	08:07:25.696454	Cisco_11:a0:b8	Broadcast	0x8899	60	Realtek Layer 2 Protocols
2100	08:07:25.697151	10.127.4.110	10.127.255.255	NBNS	92	Name query NB ASNXALWTO<00>
2101	08:07:25.697862	10.127.4.110	224.0.0.251	MDNS	75	Standard query 0x0000 A asnxalwto.local, "QM" question
2102	08:07:25.698638	fe80::3414:34ec:fa5...	ff02::fb	MDNS	95	Standard query 0x0000 A asnxalwto.local, "QM" question
2103	08:07:25.699363	fe80::3414:34ec:fa5...	ff02::1:3	LLMNR	89	Standard query 0x3231 A asnxalwto
2104	08:07:25.699862	9a:5f:9d:2c:05:df	Broadcast	ARP	60	ARP Announcement for 10.127.121.249

>	Frame 2092: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{3219B7F4-C797-4F0F-9E1A-7D5DFE741F02}, id 0
>	Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HewlettP_4d:44:ac (00:26:55:4d:44:ac)
>	Internet Protocol Version 4, Src: 10.127.14.142, Dst: 216.58.200.14
>	0100 .... = Version: 4
>	.... 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
>	Total Length: 1500
>	Identification: 0xcfa9 (53161)
>	Flags: 0x2000, More fragments
>	0... .. = Reserved bit: Not set
>	.0... .. = Don't fragment: Not set
>	..1... .. = More fragments: Set
>	Fragment offset: 0
>	Time to live: 3
>	Protocol: ICMP (1)
>	Header checksum: 0x0922 [validation disabled]
>	[Header checksum status: Unverified]
>	Source: 10.127.14.142
>	Destination: 216.58.200.14
>	[Reassembled IPv4 in frame: 2093]
>	Data (1480 bytes)

**12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?**

Answer: The fragment offset (1480) indicates that this is not the first datagram fragment. There are no more fragments as the More fragments field is not set.

2092	08:07:25.620109	10.127.14.142	216.58.200.14	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=cfa9) [Reassembled in #2093]
2093	08:07:25.620109	10.127.14.142	216.58.200.14	ICMP	534	Echo (ping) request id=0x0003, seq=18696/2121, ttl=3 (no response found!)
2094	08:07:25.652051	172.17.5.33	10.127.14.142	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2095	08:07:25.652051	113.171.17.121	10.127.14.142	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2096	08:07:25.670365	10.127.14.142	216.58.200.14	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=cfaa) [Reassembled in #2097]
2097	08:07:25.670365	10.127.14.142	216.58.200.14	ICMP	534	Echo (ping) request id=0x0003, seq=18697/2377, ttl=4 (no response found!)
2098	08:07:25.696086	fe80::e2dc:ffff:fed...	ff02::2	ICMPv6	70	Router Solicitation from e0:dc:ff:d6:40:f1
2099	08:07:25.696454	Cisco_11:a0:b8	Broadcast	0x8899	60	Realtek Layer 2 Protocols
2100	08:07:25.697151	10.127.4.110	10.127.255.255	NBNS	92	Name query NB ASNXALWTO<00>
2101	08:07:25.697862	10.127.4.110	224.0.0.251	MDNS	75	Standard query 0x0000 A asnxalwto.local, "QM" question
2102	08:07:25.698638	fe80::3414:34ec:fa5...	ff02::fb	MDNS	95	Standard query 0x0000 A asnxalwto.local, "QM" question
2103	08:07:25.699363	fe80::3414:34ec:fa5...	ff02::1:3	LLMNR	89	Standard query 0x3231 A asnxalwto
2104	08:07:25.699862	9a:5f:9d:2c:05:df	Broadcast	ARP	60	ARP Announcement for 10.127.121.249

>	Frame 2093: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{3219B7F4-C797-4F0F-9E1A-7D5DFE741F02}, id 0
>	Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HewlettP_4d:44:ac (00:26:55:4d:44:ac)
>	Internet Protocol Version 4, Src: 10.127.14.142, Dst: 216.58.200.14
>	0100 .... = Version: 4
>	.... 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
>	Total Length: 520
>	Identification: 0xcfa9 (53161)
>	Flags: 0x00b9
>	0... .. = Reserved bit: Not set
>	.0... .. = Don't fragment: Not set
>	..0... .. = More fragments: Not set
>	Fragment offset: 1480
>	Time to live: 3
>	Protocol: ICMP (1)
>	Header checksum: 0x2c3d [validation disabled]
>	[Header checksum status: Unverified]
>	Source: 10.127.14.142
>	Destination: 216.58.200.14
>	[2 IPv4 Fragments (1980 bytes): #2092(1480), #2093(500)]

### 13. What fields change in the IP header between the first and second fragment?

Answer: The IP header fields that changed between the fragments are: total length, flags, fragment offset and checksum.

### 14. How many fragments were created from the original datagram?

Answer: According to the screenshot, there were 3 fragments created from the original datagram.

3434 08:07:35.519652	10.127.14.142	216.58.200.14	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=cfd3) [Reassembled in #3436]
3435 08:07:35.519652	10.127.14.142	216.58.200.14	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=cfd3) [Reassembled in #3436]
3436 08:07:35.519652	10.127.14.142	216.58.200.14	ICMP	554	Echo (ping) request id=0x0003, seq=18738/12873, ttl=1 (no response found!)
3437 08:07:35.524276	10.127.133.55	224.0.0.251	MDNS	255	Standard query response 0x0000 PTR, cache flush Quoc-Duy.local PTR, cache flush Q
3438 08:07:35.525015	fe80::1c79:e456:45c...	ff02::fb	MDNS	275	Standard query response 0x0000 PTR, cache flush Quoc-Duy.local PTR, cache flush Q
3439 08:07:35.570517	10.127.14.142	216.58.200.14	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=cfd4) [Reassembled in #3441]
3440 08:07:35.570517	10.127.14.142	216.58.200.14	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=cfd4) [Reassembled in #3441]
3441 08:07:35.570517	10.127.14.142	216.58.200.14	ICMP	554	Echo (ping) request id=0x0003, seq=18739/13129, ttl=2 (no response found!)
3442 08:07:35.572458	10.127.16.199	224.0.0.252	LLMNR	75	Standard query 0x3334 A BRW485F99CA2B7C
3443 08:07:35.572458	14.169.128.1	10.127.14.142	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3444 08:07:35.620522	10.127.14.142	216.58.200.14	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=cfd5) [Reassembled in #3446]
3445 08:07:35.620522	10.127.14.142	216.58.200.14	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=cfd5) [Reassembled in #3446]

> Frame 3434: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF\_{3219B7F4-C797-4F0F-9E1A-7D5DFE741F02}, id 0

> Ethernet II, Src: AzureWav\_5b:72:7f (70:66:55:5b:72:7f), Dst: HewlettP\_4d:44:ac (08:26:55:4d:44:ac)

> Internet Protocol Version 4, Src: 10.127.14.142, Dst: 216.58.200.14

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 1500

Identification: 0xcfd3 (53203)

> Flags: 0x2000, More fragments

0... .. = Reserved bit: Not set

.0... .. = Don't fragment: Not set

..1... .. = More fragments: Set

Fragment offset: 0

> Time to live: 1

Protocol: ICMP (1)

Header checksum: 0x0af8 [validation disabled]

[Header checksum status: Unverified]

Source: 10.127.14.142

Destination: 216.58.200.14

[Reassembled IPv4 in frame: 3436]

> Data (1480 bytes)

### 15. What fields change in the IP header among the fragments?

Answer: The fields changing in the IP header among the fragments are the fragment offset, 0 for the first, 1480 for the second and 2960 for the third. The checksum was also different among the fragments. The first 2 packets also have lengths of 1500 and more fragments flags set, while the last fragment is shorter (540) and does not have a flag set.

The first fragment:

2098	10:12:39.554732	192.168.100.7	23.2.16.27	TCP	54 62400 → 443 [RST, ACK] Seq=564 Ack=6105 Win=0 Len=0
2099	10:12:39.559482	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b310) [Reassembled in #2101]
2100	10:12:39.559482	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b310) [Reassembled in #2101]
2101	10:12:39.559482	192.168.100.7	172.217.25.4	ICMP	554 Echo (ping) request id=0x0001, seq=4292/50192, ttl=2 (no response found!)
2102	10:12:39.567345	108.177.97.188	192.168.100.7	TCP	66 [TCP Keep-Alive ACK] 5228 → 61984 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
2103	10:12:39.567445	203.210.144.219	192.168.100.7	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2104	10:12:39.609700	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b311) [Reassembled in #2106]
2105	10:12:39.609700	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b311) [Reassembled in #2106]
2106	10:12:39.609700	192.168.100.7	172.217.25.4	ICMP	554 Echo (ping) request id=0x0001, seq=4293/50448, ttl=3 (no response found!)
2107	10:12:39.613748	172.17.5.73	192.168.100.7	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2108	10:12:39.615310	192.168.100.7	74.125.200.189	UDP	75 54310 → 443 Len=33
2109	10:12:39.660057	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b312) [Reassembled in #2111]
2110	10:12:39.660057	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b312) [Reassembled in #2111]
2111	10:12:39.660057	192.168.100.7	172.217.25.4	ICMP	554 Echo (ping) request id=0x0001, seq=4294/50704, ttl=4 (no response found!)
2112	10:12:39.665552	112.171.40.31	192.168.100.7	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
> Frame 2099: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{3219B7F4-C797-4F0F-9E1A-7D5DFE741F02}, id 0					
> Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HuaweiTe_86:4d:dc (68:89:c1:86:4d:dc)					
Internet Protocol Version 4, Src: 192.168.100.7, Dst: 172.217.25.4					
0100 .... = Version: 4					
.... 0101 = Header Length: 20 bytes (5)					
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
0000 00.. = Differentiated Services Codepoint: Default (0)					
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)					
Total Length: 1500					
Identification: 0xb310 (45840)					
Flags: 0x2000, More fragments					
0... .... = Reserved bit: Not set					
.0. .... = Don't fragment: Not set					
..1. .... = More fragments: Set					
Fragment offset: 0					
Time to live: 2					
> [Expert Info (Note/Sequence): "Time To Live" only 2]					
Protocol: ICMP (1)					
Header checksum: 0xf583 [validation disabled]					
[Header checksum status: Unverified]					
Source: 192.168.100.7					
Destination: 172.217.25.4					

The second fragment:

2098	10:12:39.554732	192.168.100.7	23.2.16.27	TCP	54 62400 → 443 [RST, ACK] Seq=564 Ack=6105 Win=0 Len=0
2099	10:12:39.559482	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b310) [Reassembled in #2101]
2100	10:12:39.559482	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b310) [Reassembled in #2101]
2101	10:12:39.559482	192.168.100.7	172.217.25.4	ICMP	554 Echo (ping) request id=0x0001, seq=4292/50192, ttl=2 (no response found!)
2102	10:12:39.567345	108.177.97.188	192.168.100.7	TCP	66 [TCP Keep-Alive ACK] 5228 → 61984 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
2103	10:12:39.567445	203.210.144.219	192.168.100.7	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2104	10:12:39.609700	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b311) [Reassembled in #2106]
2105	10:12:39.609700	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b311) [Reassembled in #2106]
2106	10:12:39.609700	192.168.100.7	172.217.25.4	ICMP	554 Echo (ping) request id=0x0001, seq=4293/50448, ttl=3 (no response found!)
2107	10:12:39.613748	172.17.5.73	192.168.100.7	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2108	10:12:39.615310	192.168.100.7	74.125.200.189	UDP	75 54310 → 443 Len=33
2109	10:12:39.660057	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b312) [Reassembled in #2111]
2110	10:12:39.660057	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b312) [Reassembled in #2111]
2111	10:12:39.660057	192.168.100.7	172.217.25.4	ICMP	554 Echo (ping) request id=0x0001, seq=4294/50704, ttl=4 (no response found!)
2112	10:12:39.665552	112.171.40.31	192.168.100.7	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
> Frame 2100: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{3219B7F4-C797-4F0F-9E1A-7D5DFE741F02}, id 0					
> Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HuaweiTe_86:4d:dc (68:89:c1:86:4d:dc)					
Internet Protocol Version 4, Src: 192.168.100.7, Dst: 172.217.25.4					
0100 .... = Version: 4					
.... 0101 = Header Length: 20 bytes (5)					
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
0000 00.. = Differentiated Services Codepoint: Default (0)					
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)					
Total Length: 1500					
Identification: 0xb310 (45840)					
Flags: 0x2009, More fragments					
0... .... = Reserved bit: Not set					
.0. .... = Don't fragment: Not set					
..1. .... = More fragments: Set					
Fragment offset: 1480					
Time to live: 2					
> [Expert Info (Note/Sequence): "Time To Live" only 2]					
Protocol: ICMP (1)					
Header checksum: 0xf4ca [validation disabled]					
[Header checksum status: Unverified]					
Source: 192.168.100.7					
Destination: 172.217.25.4					

The third fragment:



2098	10:12:39.554732	192.168.100.7	23.2.16.27	TCP	54 62400 → 443 [RST, ACK] Seq=564 Ack=6105 Win=0 Len=0
2099	10:12:39.559482	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b310) [Reassembled in #2101]
2100	10:12:39.559482	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b310) [Reassembled in #2101]
2101	10:12:39.559482	192.168.100.7	172.217.25.4	ICMP	554 Echo (ping) request id=0x0001, seq=4292/50192, ttl=2 (no response found!)
2102	10:12:39.567345	108.177.97.188	192.168.100.7	TCP	66 [TCP Keep-Alive ACK] 5228 → 61984 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
2103	10:12:39.567445	203.210.144.219	192.168.100.7	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2104	10:12:39.609700	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b311) [Reassembled in #2106]
2105	10:12:39.609700	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b311) [Reassembled in #2106]
2106	10:12:39.609700	192.168.100.7	172.217.25.4	ICMP	554 Echo (ping) request id=0x0001, seq=4293/50448, ttl=3 (no response found!)
2107	10:12:39.613748	172.17.5.73	192.168.100.7	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
2108	10:12:39.615310	192.168.100.7	74.125.200.189	UDP	75 54310 → 443 Len=33
2109	10:12:39.660057	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b312) [Reassembled in #2111]
2110	10:12:39.660057	192.168.100.7	172.217.25.4	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b312) [Reassembled in #2111]
2111	10:12:39.660057	192.168.100.7	172.217.25.4	ICMP	554 Echo (ping) request id=0x0001, seq=4294/50704, ttl=4 (no response found!)
2112	10:12:39.665562	112.121.48.31	192.168.100.7	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
> Frame 2101: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \Device\NPF_{3219B7F4-C797-4F0F-9E1A-7D5DFE741F02}, id 0					
> Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HuaweiTe_86:4d:dc (68:89:c1:86:4d:dc)					
Internet Protocol Version 4, Src: 192.168.100.7, Dst: 172.217.25.4					
0100 .... = Version: 4					
.... 0101 = Header Length: 20 bytes (5)					
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
0000 00.. = Differentiated Services Codepoint: Default (0)					
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)					
Total Length: 540					
Identification: 0xb310 (45840)					
Flags: 0x0172					
0... .. = Reserved bit: Not set					
.0... .. = Don't fragment: Not set					
..0... .. = More fragments: Not set					
Fragment offset: 2960					
Time to live: 2					
> [Expert Info (Note/Sequence): "Time To Live" only 2]					
Protocol: ICMP (1)					
Header checksum: 0x17d2 [validation disabled]					
[Header checksum status: Unverified]					
Source: 192.168.100.7					