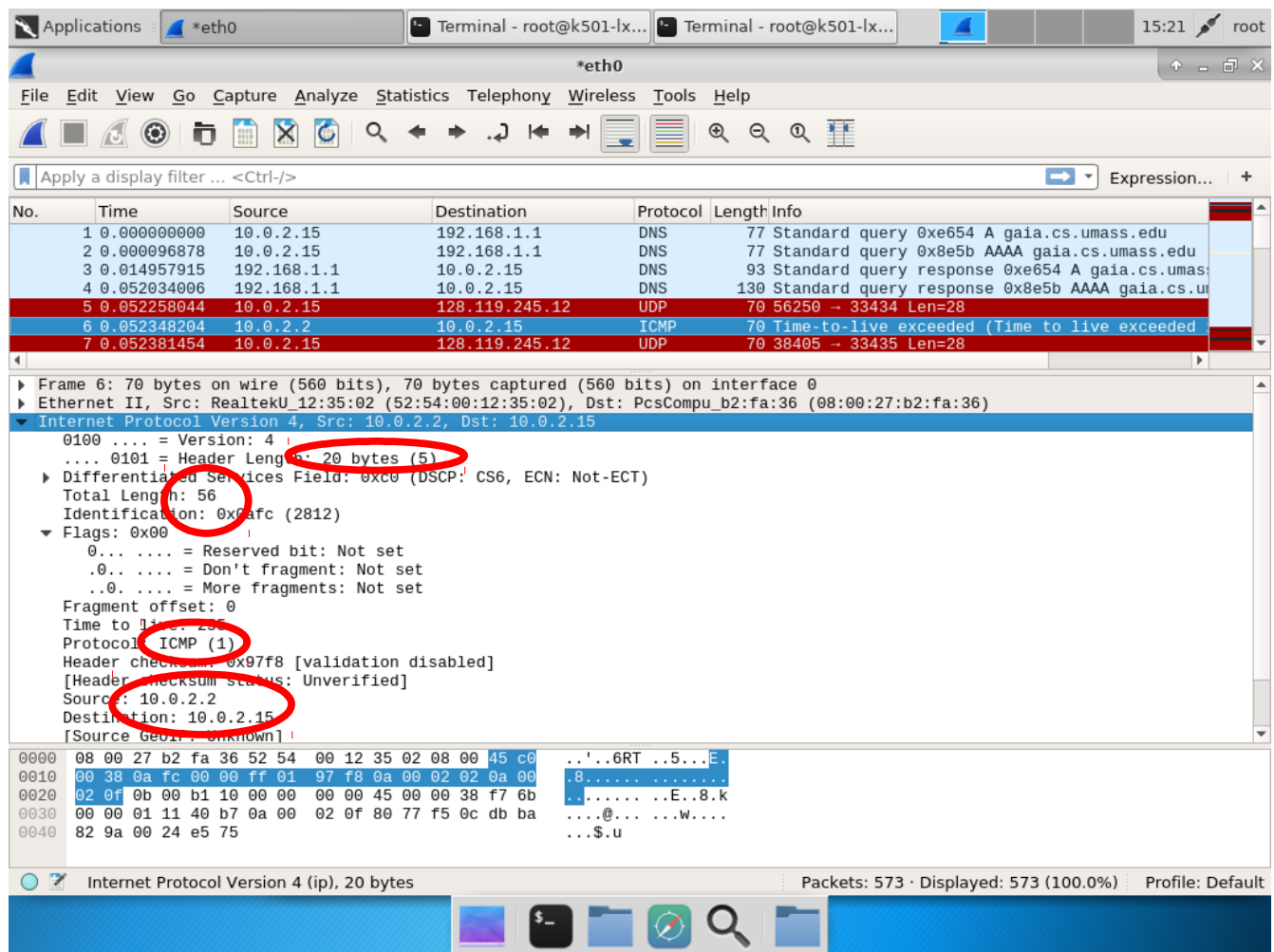


# Wireshark Lab: IP

## Questions:

- 10.0.2.15
- The value is ICMP 0x01 or (1)
- There are 20 bytes in the IP header, 36 bytes in the payload datagram for a total of 56 bytes.
- The More Fragments flag is not set, therefore, the data is not fragmented
- Frame, Identification Time to Live, and Header checksum always change



- The fields that are constant and must stay constant are the Version due to IPv4 use for all packets, Header length due to ICMP packet type, source and destination IP addresses because they are being sent and received by the same machines, Upper Layer Protocol due to ICMP packet type, and Differentiated Services because ICMP packets use the same Type of Service.

Dynamic fields include the Identification header because the ids are unique, the Time to live as this value is incremented with every packet as well as the checksum because of the header change.

7. The identification header is incremented by one with each request.

8. 2812 is in the identification field, 255 is the total time to live value

The image shows a Wireshark packet capture analysis of ICMP Echo (ping) requests. The packet list shows multiple ICMP Echo requests from 10.0.2.2 to 10.0.2.15. The packet details pane for Frame 6 shows the IP header and ICMP Echo request details. The Identification field is circled in red, showing 0x0afc (2812). The Time to live field is also circled in red, showing 255. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.052348204	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded)
11	0.052606273	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded)
12	0.052610193	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded)
108	52.689367891	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded)
115	52.692411228	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded)
116	52.692417926	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded)
299	107.024501878	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded)

Frame 6: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0  
Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_b2:fa:36 (08:00:27:b2:fa:36)  
Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.15  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)  
Total Length: 80  
Identification: 0x0afc (2812)  
Flags: 0x00  
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: 0x97f8 [validation disabled]  
[Header checksum status: Unverified]  
Source: 10.0.2.2  
Destination: 10.0.2.15  
[Source GeoIP: Unknown]

0000 08 00 27 b2 fa 36 52 54 00 12 35 02 08 00 45 c0 ..6RT ..5..E.  
0010 00 38 0a fc 00 00 ff 01 97 f8 0a 00 02 02 0a 00 .8.....  
0020 02 0f 0b 00 b1 10 00 00 00 00 45 00 00 38 f7 6b .....E..8.k  
0030 00 00 01 11 40 b7 0a 00 02 0f 80 77 f5 0c db ba ...@...w....  
0040 82 9a 00 24 e5 75 ...\$.u

Ethernet (eth), 14 bytes      Packets: 573 · Displayed: 9 (1.6%) · Dropped: 0 (0.0%)      Profile: Default

9. The identification field contains a unique value, therefore it must change for all exceeded replies. The same identification number would indicate a fragmented IP datagram. The total time to live does not change because it remains constant for the first hop router.

10. Yes, the packet is fragmented across multiple datagrams.

11. The more fragments bit is set, indicating fragmentation and the fragment offset is 0, indicating the first fragment of the set. This IP datagram has a length of 1500.

The image shows a Wireshark packet capture interface for the interface \*eth0. The packet list at the top shows several packets, with packet 106 highlighted in red. A red arrow points to packet 106. The packet details pane for packet 106 shows the following information:

- Frame 106: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
- Ethernet II, Src: PcsCompu\_b2:fa:36 (08:00:27:b2:fa:36), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)
- Internet Protocol Version 4, Src: 10.0.2.15, 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: 1500
  - Identification: 6383
  - Flags: 0x01 (More Fragments)
    - 0... .... = Reserved bit: Not set
    - .0... .... = Don't fragment: Not set
    - 1... .... = More fragments: Set
  - Fragment offset: 0
  - Time to live: 64
  - Protocol: UDP (17)
  - Header checksum: 0xf98f [validation disabled]
  - [Header checksum status: Unverified]
  - Source: 10.0.2.15
  - Destination: 128.119.245.12
  - [Source GeoIP: Unknown]

The packet bytes pane at the bottom shows the raw data of the packet, with the first 1500 bytes highlighted in blue. The status bar at the bottom indicates: Frame (frame), 1514 bytes; Packets: 573 · Displayed: 573 (100.0%) · Dropped: 0 (0.0%) · Profile: Default.

12. The more fragments flag is not set, therefore we know this is the last in the set. This is also not the first fragment in the set, the total length is 1480 for the segment in question.

The image shows a Wireshark packet capture interface. The top pane displays a list of captured packets. Packet 107 is selected, showing details of an Ethernet II frame, an Internet Protocol Version 4 (IPv4) packet, and a User Datagram Protocol (UDP) packet. The IPv4 packet details show the 'Flags' field with 'More fragments: Not set' circled in red. The UDP packet details show the 'Length' field as 1972. The bottom pane displays the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
102	52.669341845	10.0.2.15	192.168.1.1	DNS	77	Standard query 0x94c6 A gaia.cs.umass.edu
103	52.669436444	10.0.2.15	192.168.1.1	DNS	77	Standard query 0xdbcd AAAA gaia.cs.umass.edu
106	52.688923056	10.0.2.15	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, len=1480)
107	52.688991859	10.0.2.15	128.119.245.12	UDP	534	39261 - 33434 Len=1972
109	52.692106770	10.0.2.15	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, len=1480)
110	52.692188412	10.0.2.15	128.119.245.12	UDP	534	41575 - 33435 Len=1972
111	52.692239545	10.0.2.15	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, len=1480)

Frame 107: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0

Ethernet II, Src: PcsCompu\_b2:fa:36 (08:00:27:b2:fa:36), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, 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: 520
- Identification: 0x18ef (6383)
- Flags: 0x00
  - 0... .... = Reserved bit: Not set
  - ..0. .... = Don't fragment: Not set
  - ..0. .... = More fragments: Not set
- Fragment Offset: 0
- Time to live: 1
- Protocol: UDP (17)
- Header checksum: 0x1cab [validation disabled]
- [Header checksum status: Unverified]
- Source: 10.0.2.15
- Destination: 128.119.245.12
- [Source GeoIP: Unknown]

0000 52 54 00 12 35 02 08 00 27 b2 fa 36 08 00 45 00 RT..5... '..6..E.

0010 02 08 18 ef 00 b9 01 11 1c ab 0a 00 02 0f 80 77 .....w

0020 f5 0c 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d ..@ABCDE FGHIJKLM

0030 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d NOPQRSTU VWXYZ[\]

Frame (534 bytes) Reassembled IPv4 (1980 bytes)

Packets: 573 · Displayed: 573 (100.0%) · Dropped: 0 (0.0%) Profile: Default

13. The IP header fields that change are total length, flags, checksum and fragment offsets.

14. Three fragments are created from the original datagram.

15. Fragment offset changes from 0 to 1480 to 2960. The checksums, total length varies between the first two fragments and the 3<sup>rd</sup>. The more fragments flag is 0 in the last segment.

The image shows a Wireshark packet capture analysis of IP fragmentation. A red arrow points to the first fragment (packet 297). The packet list shows three fragments of a 1514-byte datagram. The packet details pane shows the structure of the first fragment with fields like Version, Header Length, Differentiated Services Field, Total Length, Identification, Flags (More Fragments), and Fragment offset.

Source	Destination	Protocol	Length	Info
0030 10.0.2.15	128.119.245.12	UDP	534	46482 → 33523 Len=1972
30469 10.0.2.15	192.168.1.1	DNS	77	Standard query 0xf497 A gaia.cs.umass.edu
20645 10.0.2.15	192.168.1.1	DNS	77	Standard query 0x7b9e AAAA gaia.cs.umass.edu
00366 10.0.2.15	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=3311) [Reasse...
61059 10.0.2.15	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=3311) [Rea...
25520 10.0.2.15	128.119.245.12	UDP	554	34288 → 33434 Len=3472
96901 10.0.2.15	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=3312) [Reasse...

Frame 297: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

Ethernet II, Src: PcsCompu\_b2:fa:36 (08:00:27:b2:fa:36), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, 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: 1500
- Identification: 0x0011 (15073)
- Flags: 0x01 (More Fragments)
  - 0... .. = Reserved bit: Not set
  - .0... .. = Don't fragment: Not set
  - ..1. .... = More fragments: Set
- Fragment offset: 0

Protocol: UDP (17)

Header checksum: 0xdf6d [validation disabled]  
[Header checksum status: Unverified]  
Source: 10.0.2.15  
Destination: 128.119.245.12  
[Source GeoIP: Unknown]

0000 52 54 00 12 35 02 08 00 27 b2 fa 36 08 00 45 00 RT..5... '..6..E.  
0010 05 dc 33 11 20 00 01 11 df 6d 0a 00 02 0f 80 77 ..3. ... .m.....w  
0020 f5 0c 85 f0 82 9a 0d 98 55 da 40 41 42 43 44 45 ..... U.@ABCDE  
0030 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 FGHIJKLM NOPQRSTU  
0040 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 VWXYZ[\] ^\_abcde  
0050 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 fghijklm nopqrstu

Frame (frame), 1514 bytes      Packets: 573 · Displayed: 573 (100.0%) · Dropped: 0 (0.0%)      Profile: Default

Applications \*eth0 Terminal - root@k501-lx... Terminal - root@k501-lx... 17:18 root

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

Source	Destination	Protocol	Length	Info
0030 10.0.2.15	128.119.245.12	UDP	534	46482 → 33523 Len=1972
30469 10.0.2.15	192.168.1.1	DNS	77	Standard query 0xf497 A gaia.cs.umass.edu
20645 10.0.2.15	192.168.1.1	DNS	77	Standard query 0x7b9e AAAA gaia.cs.umass.edu
00366 10.0.2.15	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=3311) [Reasse...
61059 10.0.2.15	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=3311) [Rea...
25520 10.0.2.15	128.119.245.12	UDP	554	34288 → 33434 Len=3472
96901 10.0.2.15	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=3312) [Reasse...

▶ Frame 298: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

▶ Ethernet II, Src: PcsCompu\_b2:fa:36 (08:00:27:b2:fa:36), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

▼ Internet Protocol Version 4, Src: 10.0.2.15, 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: 1500
- Identification: 0x3311 (13073)
- ▼ Flags: 0x01 (More Fragments)
- 0... .... = Reserved bit: Not set
- .0... .... = Don't fragment: Not set
- ..1. .... = More fragments: Set
- Fragment offset: 1480
- ▶ Time to live: 1
- Protocol: UDP (17)
- Header checksum: 0xdeb4 [validation disabled]
- [Header checksum status: Unverified]
- Source: 10.0.2.15
- Destination: 128.119.245.12
- [Source GeoIP: Unknown]

0000	52 54 00 12 35 02 08 00	27 b2 fa 36 08 00 45 00	RT...5... '..6..E..
0010	05 dc 33 11 20 b9 01 11	de b4 0a 00 02 0f 80 77	..3. ... ..w
0020	f5 0c 40 41 42 43 44 45	46 47 48 49 4a 4b 4c 4d	..@ABCDE FGHIJKLM
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 68 69 6a 6b 6c 6d	^_`abcde fghijkLm
0050	6e 6f 70 71 72 73 74 75	76 77 78 79 7a 7b 7c 7d	nopqrstu vwxyz{}}

Frame (frame), 1514 bytes Packets: 573 · Displayed: 573 (100.0%) · Dropped: 0 (0.0%) Profile: Default



Applications \*eth0 Terminal - root@k501-lx... Terminal - root@k501-lx... 17:18 root

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

Source	Destination	Protocol	Length	Info
0030 10.0.2.15	128.119.245.12	UDP	534	46482 → 33523 Len=1972
30469 10.0.2.15	192.168.1.1	DNS	77	Standard query 0xf497 A gaia.cs.umass.edu
20645 10.0.2.15	192.168.1.1	DNS	77	Standard query 0x7b9e AAAA gaia.cs.umass.edu
00366 10.0.2.15	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=3311) [Reasse...
61059 10.0.2.15	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=3311) [Rea...
25520 10.0.2.15	128.119.245.12	UDP	554	34288 → 33434 Len=3472
96901 10.0.2.15	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=3312) [Reasse...

▶ Frame 300: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0

▶ Ethernet II, Src: PcsCompu\_b2:fa:36 (08:00:27:b2:fa:36), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

▼ Internet Protocol Version 4, Src: 10.0.2.15, 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: 540

Identification: 0x0011 (4097)

▼ Flags: 0x00

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

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

..0. .... = More fragments: Not set

Fragment offset: 2960

Protocol: UDP (17)

Header checksum: 0x01bc [validation disabled]

[Header checksum status: Unverified]

Source: 10.0.2.15

Destination: 128.119.245.12

[Source GeoIP: Unknown]

0000	52 54 00 12 35 02 08 00 27 b2 fa 36 08 00 45 00	RT...5... '..6..E..
0010	02 1c 33 11 01 72 01 11 01 bc 0a 00 02 0f 80 77	..3..r... ..w
0020	f5 0c 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55	..HIJKLM NOPQRSTU
0030	56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65	VWXYZ[\] ^_abcde

Frame (554 bytes) Reassembled IPv4 (3480 bytes)

Frame (frame), 554 bytes

Packets: 573 · Displayed: 573 (100.0%) · Dropped: 0 (0.0%) Profile: Default