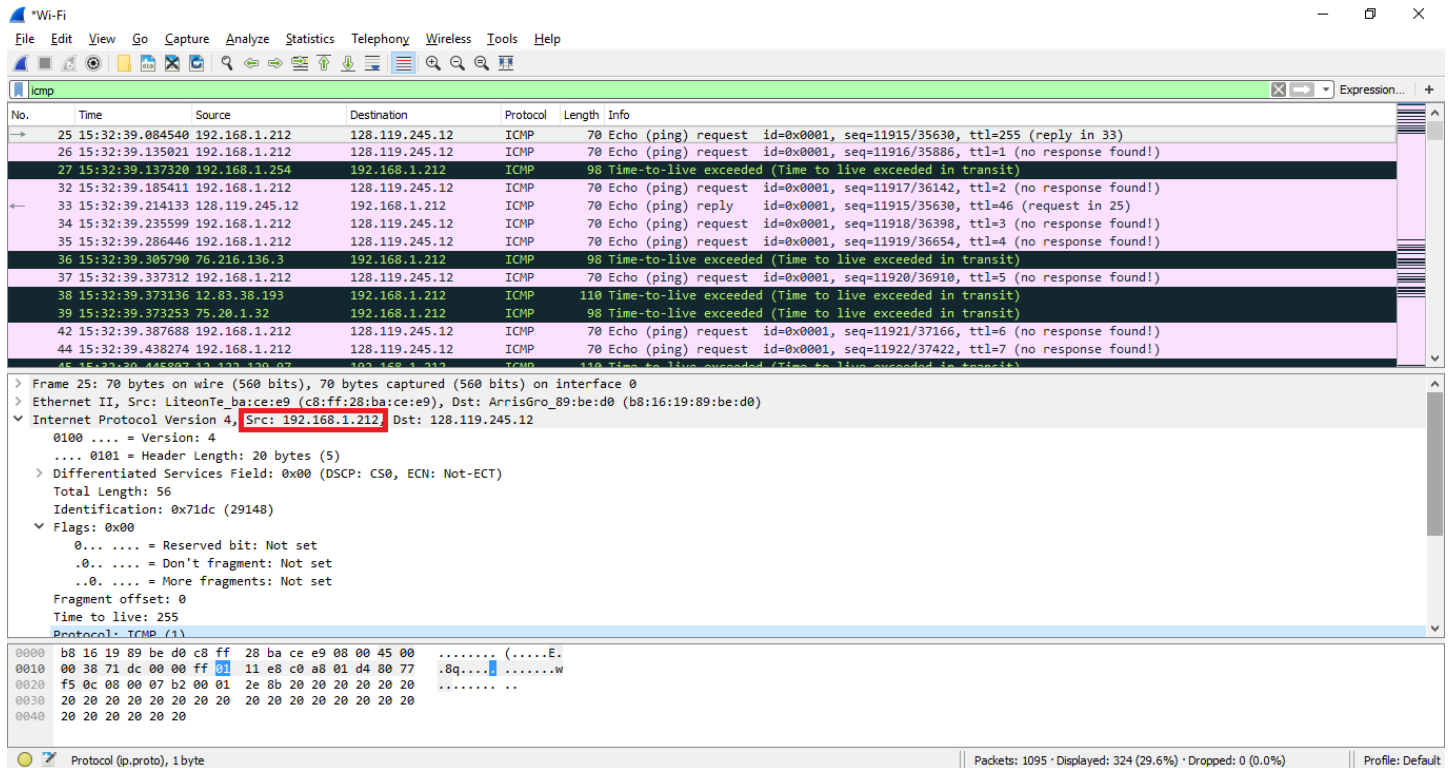


Lab 4

1. What is the IP address of your computer?

My computer's IP address is 192.168.1.212



Wireshark packet capture showing ICMP Echo (ping) requests and replies. The source IP is 192.168.1.212 and the destination is 128.119.245.12. The packet list shows multiple requests with 'Time to live exceeded' and replies with 'no response found!'.

No.	Time	Source	Destination	Protocol	Length	Info
25	15:32:39.084540	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11915/35630, ttl=255 (reply in 33)
26	15:32:39.135021	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11916/35886, ttl=1 (no response found!)
27	15:32:39.137320	192.168.1.254	192.168.1.212	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
32	15:32:39.185411	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11917/36142, ttl=2 (no response found!)
33	15:32:39.214133	128.119.245.12	192.168.1.212	ICMP	70	Echo (ping) reply id=0x0001, seq=11915/35630, ttl=46 (request in 25)
34	15:32:39.235599	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11918/36398, ttl=3 (no response found!)
35	15:32:39.286446	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11919/36654, ttl=4 (no response found!)
36	15:32:39.305790	76.216.136.3	192.168.1.212	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
37	15:32:39.337312	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11920/36910, ttl=5 (no response found!)
38	15:32:39.373136	12.83.38.193	192.168.1.212	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
39	15:32:39.373253	75.20.1.32	192.168.1.212	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
42	15:32:39.387688	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11921/37166, ttl=6 (no response found!)
44	15:32:39.438274	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11922/37422, ttl=7 (no response found!)
45	15:32:39.445807	12.132.130.02	192.168.1.212	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)

Frame 25: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)
> Internet Protocol Version 4, Src: 192.168.1.212, 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: 56
Identification: 0x71dc (29148)
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)
b8 16 19 89 be d0 c8 ff 28 ba ce e9 08 00 45 00 (.....E..
0010 00 38 71 dc 00 00 ff 21 11 e8 c0 a8 01 d4 80 77 .8q.....W
0020 f5 0c 08 00 07 b2 00 01 2e 8b 20 20 20 20 20 20
0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

2. Within the IP packet header, what is the value in the upper layer protocol field?

The value in the upper layer protocol field is ICMP (1)

Wireshark packet capture showing ICMP Echo (ping) requests and replies. The selected packet is an ICMP Echo (ping) request from 192.168.1.212 to 128.119.245.12. The packet details show the IP header and ICMP payload.

No.	Time	Source	Destination	Protocol	Length	Info
25	15:32:39.084540	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11915/35630, ttl=255 (reply in 33)
26	15:32:39.135021	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11916/35886, ttl=1 (no response found!)
27	15:32:39.137320	192.168.1.254	192.168.1.212	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
32	15:32:39.185411	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11917/36142, ttl=2 (no response found!)
33	15:32:39.214133	128.119.245.12	192.168.1.212	ICMP	70	Echo (ping) reply id=0x0001, seq=11915/35630, ttl=46 (request in 25)
34	15:32:39.235599	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11918/36398, ttl=3 (no response found!)
35	15:32:39.286446	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11919/36654, ttl=4 (no response found!)
36	15:32:39.305790	76.216.136.3	192.168.1.212	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
37	15:32:39.337312	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11920/36910, ttl=5 (no response found!)

Frame 25: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)
 Internet Protocol Version 4, Src: 192.168.1.212, 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: 56
 Identification: 0x71dc (29148)
 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: 0x11e8 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.212
 Destination: 128.119.245.12

0000 b8 16 19 89 be d0 c8 ff 28 ba ce e9 08 00 45 00 (.....E.
 0010 00 38 71 dc 00 00 ff 11 e8 c0 a8 01 d4 80 77 .8q.....W
 0020 f5 0c 08 00 07 b2 00 01 2e 8b 20 20 20 20 20
 0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0040 20 20 20 20 20 20

Protocol (ip.proto), 1 byte

Packets: 1095 · Displayed: 324 (29.6%) · Dropped: 0 (0.0%) Profile: Default

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.

There are 20 bytes in the IP header, and total length is 56 bytes which leaves 36 bytes in the payload of the IP datagram

Wireshark packet capture showing ICMP Echo (ping) requests and replies. The selected packet is an ICMP Echo (ping) request from 192.168.1.212 to 128.119.245.12. The packet details show the IP header and ICMP payload.

No.	Time	Source	Destination	Protocol	Length	Info
25	15:32:39.084540	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11915/35630, ttl=255 (reply in 33)
26	15:32:39.135021	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11916/35886, ttl=1 (no response found!)
27	15:32:39.137320	192.168.1.254	192.168.1.212	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
32	15:32:39.185411	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11917/36142, ttl=2 (no response found!)
33	15:32:39.214133	128.119.245.12	192.168.1.212	ICMP	70	Echo (ping) reply id=0x0001, seq=11915/35630, ttl=46 (request in 25)
34	15:32:39.235599	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11918/36398, ttl=3 (no response found!)
35	15:32:39.286446	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11919/36654, ttl=4 (no response found!)
36	15:32:39.305790	76.216.136.3	192.168.1.212	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
37	15:32:39.337312	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11920/36910, ttl=5 (no response found!)

Frame 25: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)
 Internet Protocol Version 4, Src: 192.168.1.212, 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: 56
 Identification: 0x71dc (29148)
 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: 0x11e8 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.212
 Destination: 128.119.245.12

0000 b8 16 19 89 be d0 c8 ff 28 ba ce e9 08 00 45 00 (.....E.
 0010 00 38 71 dc 00 00 ff 11 e8 c0 a8 01 d4 80 77 .8q.....W
 0020 f5 0c 08 00 07 b2 00 01 2e 8b 20 20 20 20 20
 0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0040 20 20 20 20 20 20

Protocol (ip.proto), 1 byte

Packets: 1095 · Displayed: 324 (29.6%) · Dropped: 0 (0.0%) Profile: Default

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

No, this IP datagram has not been fragmented. We can see that the 'More fragments' flag as well as the 'fragment offset' are zero which indicate that it is not fragmented. (more fragments set to zero indicates that this is the last packet and fragment offset set to zero means that this packet contains the beginning of the datagram)

Wireshark packet capture showing ICMP Echo (ping) requests and replies. The packet list shows several requests and replies. The packet details pane for packet 25 shows the IP header fields, including the 'More fragments' flag and 'Fragment offset' both set to 0, indicating no fragmentation. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
25	15:32:39.084540	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11915/35630, ttl=255 (reply in 33)
26	15:32:39.135021	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11916/35886, ttl=1 (no response found!)
27	15:32:39.137320	192.168.1.254	192.168.1.212	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
32	15:32:39.185411	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11917/36142, ttl=2 (no response found!)
33	15:32:39.214133	128.119.245.12	192.168.1.212	ICMP	70	Echo (ping) reply id=0x0001, seq=11915/35630, ttl=46 (request in 25)
34	15:32:39.235599	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11918/36398, ttl=3 (no response found!)
35	15:32:39.286446	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11919/36654, ttl=4 (no response found!)
36	15:32:39.305790	76.216.136.3	192.168.1.212	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
37	15:32:39.337312	192.168.1.212	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=11920/36910, ttl=5 (no response found!)

Frame 25: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)
 Internet Protocol Version 4, Src: 192.168.1.212, 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: 56
 Identification: 0x71dc (29148)
 > 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: 0x11e8 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.212
 Destination: 128.119.245.12

0000 b8 16 19 89 be d0 c8 ff 28 ba ce e9 08 00 45 00 (.....E.
 0010 00 38 71 dc 00 00 ff 21 11 e8 c0 a8 01 d4 80 77 .8q.....W
 0020 f5 0c 08 00 07 b2 00 01 2e 8b 20 20 20 20 20
 0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

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?

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

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1046	15:33:56.343587	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12143/28463, ttl=2 (no response found!)
1042	15:33:56.293497	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12142/28207, ttl=1 (no response found!)
1038	15:33:56.242366	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12141/27951, ttl=255 (no response found!)
1020	15:33:49.415618	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12140/27695, ttl=63 (no response found!)
1017	15:33:49.365453	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12139/27439, ttl=62 (no response found!)
1014	15:33:49.314881	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12138/27183, ttl=61 (no response found!)
1011	15:33:49.264763	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12137/26927, ttl=60 (no response found!)
1008	15:33:49.214584	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12136/26671, ttl=59 (no response found!)
1005	15:33:49.163922	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12135/26415, ttl=58 (no response found!)

Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)

Internet Protocol Version 4, Src: 192.168.1.212, 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: 0x72c2 (29378)
 > Flags: 0x00
 Fragment offset: 2960
 > Time to live: 1
 Protocol: ICMP (1)
 Header checksum: 0x0bad [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.212
 Destination: 128.119.245.12
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]
 > [3 IPv4 Fragments (3480 bytes): #1040(1480), #1041(1480), #1042(520)]

Internet Control Message Protocol

0010 02 1c 72 c2 01 72 01 01 0b ad c0 a8 01 d4 80 77 ..r...r.....W
 0020 f5 0c 20 20 20 20 20 20 20 20 20 20 20 20 20 ..
 0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Frame (554 bytes) Reassembled IPv4 (3480 bytes)

Protocol (p.proto), 1 byte

Packets: 1095 · Displayed: 324 (29.6%) · Dropped: 0 (0.0%) Profile: Default

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1046	15:33:56.343587	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12143/28463, ttl=2 (no response found!)
1042	15:33:56.293497	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12142/28207, ttl=1 (no response found!)
1038	15:33:56.242366	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12141/27951, ttl=255 (no response found!)
1020	15:33:49.415618	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12140/27695, ttl=63 (no response found!)
1017	15:33:49.365453	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12139/27439, ttl=62 (no response found!)
1014	15:33:49.314881	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12138/27183, ttl=61 (no response found!)
1011	15:33:49.264763	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12137/26927, ttl=60 (no response found!)
1008	15:33:49.214584	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12136/26671, ttl=59 (no response found!)
1005	15:33:49.163922	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12135/26415, ttl=58 (no response found!)

Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)

Internet Protocol Version 4, Src: 192.168.1.212, 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: 0x72c3 (29379)
 > Flags: 0x00
 Fragment offset: 2960
 > Time to live: 2
 Protocol: ICMP (1)
 Header checksum: 0x0aac [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.212
 Destination: 128.119.245.12
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]
 > [3 IPv4 Fragments (3480 bytes): #1044(1480), #1045(1480), #1046(520)]

Internet Control Message Protocol

0010 02 1c 72 c3 01 72 02 01 0a ac c0 a8 01 d4 80 77 ..r...r.....W
 0020 f5 0c 20 20 20 20 20 20 20 20 20 20 20 20 20 ..
 0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Frame (554 bytes) Reassembled IPv4 (3480 bytes)

Protocol (p.proto), 1 byte

Packets: 1095 · Displayed: 324 (29.6%) · Dropped: 0 (0.0%) Profile: Default

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

The fields that stay constant are Version, Header Length, Source, Destination, Differentiated Services Field, and Protocol

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1046	15:33:56.343587	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12143/28463, ttl=2 (no response found!)
1042	15:33:56.293497	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12142/28207, ttl=1 (no response found!)
1038	15:33:56.242366	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12141/27951, ttl=255 (no response found!)
1020	15:33:49.415618	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12140/27695, ttl=63 (no response found!)
1017	15:33:49.365453	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12139/27439, ttl=62 (no response found!)
1014	15:33:49.314881	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12138/27183, ttl=61 (no response found!)
1011	15:33:49.264763	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12137/26927, ttl=60 (no response found!)
1008	15:33:49.214584	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12136/26671, ttl=59 (no response found!)
1005	15:33:49.163922	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12135/26415, ttl=58 (no response found!)

> Frame 1046: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0

> Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)

> Internet Protocol Version 4, Src: 192.168.1.212, 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: 0x72c3 (29379)

Flags: 0x00

Fragment offset: 2960

> Time to live: 2

Protocol: ICMP (1)

Header checksum: 0x0aac [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.212

Destination: 128.119.245.12

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

> [3 IPv4 Fragments (3480 bytes): #1044(1480), #1045(1480), #1046(520)]

0000 b8 16 19 89 be d0 c8 ff 28 ba ce e9 08 00 45 00 (.....E

0010 02 1c 72 c3 01 72 02 01 0a ac c0 a8 01 d4 80 77 ..r..r.....W

0020 f5 0c 20 20 20 20 20 20 20 20 20 20 20 20 20 ..

0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Frame (554 bytes) Reassembled IPv4 (3480 bytes)

Differentiated Services Field (p.dsfld), 1 byte

Packets: 1095 · Displayed: 324 (29.6%) · Dropped: 0 (0.0%) Profile: Default

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1046	15:33:56.343587	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12143/28463, ttl=2 (no response found!)
1042	15:33:56.293497	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12142/28207, ttl=1 (no response found!)
1038	15:33:56.242366	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12141/27951, ttl=255 (no response found!)
1020	15:33:49.415618	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12140/27695, ttl=63 (no response found!)
1017	15:33:49.365453	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12139/27439, ttl=62 (no response found!)
1014	15:33:49.314881	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12138/27183, ttl=61 (no response found!)
1011	15:33:49.264763	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12137/26927, ttl=60 (no response found!)
1008	15:33:49.214584	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12136/26671, ttl=59 (no response found!)
1005	15:33:49.163922	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12135/26415, ttl=58 (no response found!)

> Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)

> Internet Protocol Version 4, Src: 192.168.1.212, 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: 0x72c3 (29379)

Flags: 0x00

Fragment offset: 2960

> Time to live: 2

Protocol: ICMP (1)

Header checksum: 0x0aac [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.212

Destination: 128.119.245.12

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

> [3 IPv4 Fragments (3480 bytes): #1044(1480), #1045(1480), #1046(520)]

> Internet Control Message Protocol

0010 02 1c 72 c3 01 72 02 01 0a ac c0 a8 01 d4 80 77 ..r..r.....W

0020 f5 0c 20 20 20 20 20 20 20 20 20 20 20 20 20 ..

0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Frame (554 bytes) Reassembled IPv4 (3480 bytes)

Protocol (p.proto), 1 byte

Packets: 1095 · Displayed: 324 (29.6%) · Dropped: 0 (0.0%) Profile: Default

The fields that *must* stay constant are:

- Version: all packets use IPv4
- Header Length: all ICMP packets have the same header length
- Source: all packets are being sent from the same source
- Destination: all packets are being sent to the same destination
- Differentiated Services Field: all ICMP packets use the same type of service class
- Protocol: all ICMP packets use the same protocol

The fields that *must* change are:

- Identification: each packet must have a unique id
- Time to live: ttl is incremented with every packet
- Header checksum: the header changes so the checksum must as well

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

The Identification field of the IP datagram increments each time an ICMP Echo Request message is sent.

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1046	15:33:56.343587	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12143/28463, ttl=2 (no response found!)
1042	15:33:56.293497	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12142/28207, ttl=1 (no response found!)
1038	15:33:56.242366	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12141/27951, ttl=255 (no response found!)
1020	15:33:49.415618	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12140/27695, ttl=63 (no response found!)
1017	15:33:49.365453	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12139/27439, ttl=62 (no response found!)
1014	15:33:49.314881	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12138/27183, ttl=61 (no response found!)
1011	15:33:49.264763	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12137/26927, ttl=60 (no response found!)
1008	15:33:49.214584	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12136/26671, ttl=59 (no response found!)
1005	15:33:49.163922	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12135/26415, ttl=58 (no response found!)

> Frame 1042: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0

> Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)

> Internet Protocol Version 4, Src: 192.168.1.212, 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: 0x72c2 (29378)

> Flags: 0x00

Fragment offset: 2960

> Time to live: 1

Protocol: ICMP (1)

Header checksum: 0x0bad [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.212

Destination: 128.119.245.12

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

> [3 IPv4 Fragments (3480 bytes): #1040(1480), #1041(1480), #1042(520)]

0010 02 1c 72 c2 01 72 01 01 0b ad c0 a8 01 d4 80 77 ..P..P.....W

0020 f5 0c 20 20 20 20 20 20 20 20 20 20 20 20 20 ..

0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Frame (554 bytes) Reassembled IPv4 (3480 bytes)

Identification (p.id), 2 bytes

Packets: 1095 · Displayed: 324 (29.6%) · Dropped: 0 (0.0%) Profile: Default

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1046	15:33:56.343587	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12143/28463, ttl=2 (no response found!)
1042	15:33:56.293497	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12142/28207, ttl=1 (no response found!)
1038	15:33:56.242366	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12141/27951, ttl=255 (no response found!)
1020	15:33:49.415618	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12140/27695, ttl=63 (no response found!)
1017	15:33:49.365453	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12139/27439, ttl=62 (no response found!)
1014	15:33:49.314881	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12138/27183, ttl=61 (no response found!)
1011	15:33:49.264763	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12137/26927, ttl=60 (no response found!)
1008	15:33:49.214584	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12136/26671, ttl=59 (no response found!)
1005	15:33:49.163922	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12135/26415, ttl=58 (no response found!)

> Frame 1046: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0

> Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)

> Internet Protocol Version 4, Src: 192.168.1.212, 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: 0x72c3 (29379)

> Flags: 0x00

Fragment offset: 2960

> Time to live: 2

Protocol: ICMP (1)

Header checksum: 0x0aac [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.212

Destination: 128.119.245.12

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

> [3 IPv4 Fragments (3480 bytes): #1044(1480), #1045(1480), #1046(520)]

0000 b8 16 19 89 be d0 c8 ff 28 ba ce e9 08 00 45

0010 02 1c 72 c3 01 72 02 01 0a ac c0 a8 01 d4 80 77 ..P..P.....W

0020 f5 0c 20 20 20 20 20 20 20 20 20 20 20 20 20 ..

0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Frame (554 bytes) Reassembled IPv4 (3480 bytes)

Differentiated Services Field (p.dsfield), 1 byte

Packets: 1095 · Displayed: 324 (29.6%) · Dropped: 0 (0.0%) Profile: Default

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

Identification: 0x76fe 30462

TTL: 250

The image shows a Wireshark packet capture window titled 'lab 4.pcapng'. The main pane displays a list of ICMP packets. The first packet (No. 45) is highlighted, and its details pane is expanded. The details pane shows the following information:

- Total Length: 96
- Identification: 0x76fe (30462)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 250
- Protocol: ICMP (1)
- Header checksum: 0xf946 [validation disabled]
- [Header checksum status: Unverified]
- Source: 12.122.129.97
- Destination: 192.168.1.212
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]
- Internet Control Message Protocol
 - Type: 11 (Time-to-live exceeded)
 - Code: 0 (Time to live exceeded in transit)
 - Checksum: 0xf6a8 [correct]
 - [Checksum Status: Good]
 - Length: 1
 - [Length of original datagram: 4]

The packet list pane shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
45	15:32:39.445807	12.122.129.97	192.168.1.212	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
216	15:32:49.423470	12.122.129.97	192.168.1.212	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
261	15:32:59.461618	12.122.129.97	192.168.1.212	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
38	15:32:39.373136	12.83.38.193	192.168.1.212	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
215	15:32:49.420810	12.83.38.193	192.168.1.212	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
260	15:32:59.459546	12.83.38.193	192.168.1.212	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
66	15:32:39.863615	128.119.0.109	192.168.1.212	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
228	15:32:49.798672	128.119.0.109	192.168.1.212	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
271	15:32:59.818482	128.119.0.109	192.168.1.212	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

The packet bytes pane shows the raw data of the selected packet, with the first few bytes highlighted in red:

```
0010 00 60 76 fe 00 00 fa 01 f9 46 0c 7a 81 61 c0 a8 .F.z.a...
0020 01 d4 0b 00 f6 a8 01 01 fd 55 45 00 00 38 71 e1 .....UE..8q.
0030 00 00 01 01 0f e4 c0 a8 01 d4 80 77 f5 0c 08 00 .....W....
0040 07 ad 00 01 2e 90 20 20 20 20 20 20 20 20 20 20 .....
0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .....
0060 20 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

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?

Each of the ICMP TTL-exceeded replies has a unique identification number. (if the identification numbers were the same it would suggest that the datagrams are actually fragments of the same datagram). The TTL field stays constant because the time to live for the first hop router is always the same.

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?

Because the 'More fragments' flag is set, we know that the datagram has been fragmented. The Fragment offset = 0 which indicates that this is the first fragment. This IP datagram is 1500 bytes long.

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
334	15:33:12.464432	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=723b) [Reassembled in #335]
335	15:33:12.464448	192.168.1.212	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=12007/59182, ttl=255 (no response found!)
336	15:33:12.515333	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=723c) [Reassembled in #337]
337	15:33:12.515349	192.168.1.212	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=12008/59438, ttl=1 (no response found!)
338	15:33:12.518632	192.168.1.254	192.168.1.212	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
339	15:33:12.529749	192.168.1.212	192.168.1.254	DNS	86	Standard query 0x4877 PTR 254.1.168.192.in-addr.arpa
340	15:33:12.531351	192.168.1.254	192.168.1.212	DNS	117	Standard query response 0x4877 PTR 254.1.168.192.in-addr.arpa PTR dsldevice.att.net
341	15:33:12.532167	192.168.1.212	192.168.1.254	DNS	77	Standard query 0x50 A dsldevice.att.net
342	15:33:12.533692	192.168.1.254	192.168.1.212	DNS	93	Standard query response 0x50 A dsldevice.att.net A 192.168.1.254
343	15:33:12.559312	192.168.1.212	64.233.171.188	TCP	55	33733→5228 [ACK] Seq=0 Ack=1 Win=63 Len=1

> Frame 334: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

> Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)

> Internet Protocol Version 4, Src: 192.168.1.212, 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: 0x723b (29243)

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: 255

Protocol: ICMP (1)

Header checksum: 0xebe4 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.212

0010 05 dc f2 3b 20 00 ff 01 eb e4 c0 a8 01 d4 80 77W

0020 f5 0c 08 00 0d 5c 00 01 2e e7 20 20 20 20 20 20W

0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20W

0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20W

0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20W

0060 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20W

Identification (p.id), 2 bytes

Packets: 1095 · Displayed: 1095 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.17 | Profile: Default

4:59 PM 11/8/2016

12. Screenshot the second fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?

The Fragment offset = 1480 which indicates that this is not the first datagram fragment. The 'More fragments' flag is not set which indicated that there aren't any more fragments.

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
334	15:33:12.464432	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=723b) [Reassembled in #335]
335	15:33:12.464448	192.168.1.212	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=12007/59182, ttl=255 (no response found!)
336	15:33:12.515333	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=723c) [Reassembled in #337]
337	15:33:12.515349	192.168.1.212	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=12008/59438, ttl=1 (no response found!)
338	15:33:12.518632	192.168.1.254	192.168.1.212	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
339	15:33:12.529749	192.168.1.212	192.168.1.254	DNS	86	Standard query 0x4877 PTR 254.1.168.192.in-addr.arpa
340	15:33:12.531351	192.168.1.254	192.168.1.212	DNS	117	Standard query response 0x4877 PTR 254.1.168.192.in-addr.arpa PTR dsldevice.att.net
341	15:33:12.532167	192.168.1.212	192.168.1.254	DNS	77	Standard query 0xbc50 A dsldevice.att.net
342	15:33:12.533692	192.168.1.254	192.168.1.212	DNS	93	Standard query response 0xbc50 A dsldevice.att.net A 192.168.1.254
343	15:33:12.559312	192.168.1.212	64.233.171.188	TCP	55	33733→5228 [ACK] Seq=0 Ack=1 Win=63 Len=1

> Frame 335: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0

> Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)

> Internet Protocol Version 4, Src: 192.168.1.212, 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: 0x723b (29243)

Flags: 0x00

0... = Reserved bit: Not set

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

.0... = More fragments: Not set

Fragment offset: 1480

Time to live: 255

Protocol: ICMP (1)

Header checksum: 0x0f00 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.212

0010 02 08 72 3b 00 b9 ff 01 0f 00 c0 a8 01 d4 80 77 ..:.....W

0020 f5 0c 08 20 20 20 20 20 20 20 20 20 20 20 20 ..

0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Frame (534 bytes) Reassembled IPv4 (1980 bytes)

Identification (p.id), 2 bytes

Packets: 1095 · Displayed: 1095 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.17 | Profile: Default

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

The fields that change in the IP header between the first and second fragments are: total length, flags, fragment offset, and checksum.

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
334	15:33:12.464432	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=723b) [Reassembled in #335]
335	15:33:12.464448	192.168.1.212	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=12007/59182, ttl=255 (no response found!)
336	15:33:12.515333	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=723c) [Reassembled in #337]
337	15:33:12.515349	192.168.1.212	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=12008/59438, ttl=1 (no response found!)
338	15:33:12.518632	192.168.1.254	192.168.1.212	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
339	15:33:12.529749	192.168.1.212	192.168.1.254	DNS	86	Standard query 0x4877 PTR 254.1.168.192.in-addr.arpa
340	15:33:12.531351	192.168.1.254	192.168.1.212	DNS	117	Standard query response 0x4877 PTR 254.1.168.192.in-addr.arpa PTR dsldevice.att.net
341	15:33:12.532167	192.168.1.212	192.168.1.254	DNS	77	Standard query 0xbc50 A dsldevice.att.net
342	15:33:12.533692	192.168.1.254	192.168.1.212	DNS	93	Standard query response 0xbc50 A dsldevice.att.net A 192.168.1.254
343	15:33:12.559312	192.168.1.212	64.233.171.188	TCP	55	33733→5228 [ACK] Seq=0 Ack=1 Win=63 Len=1

> Frame 335: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0

> Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)

> Internet Protocol Version 4, Src: 192.168.1.212, 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: 0x723b (29243)

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: 255

Protocol: ICMP (1)

Header checksum: 0xeb4 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.212

Destination: 128.119.245.12

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

0010 05 dc 72 3b 20 00 ff 01 eb e4 c0 a8 01 d4 80 77 ..:.....W

0020 f5 0c 08 0d 5c 00 01 2e e7 20 20 20 20 20 20

0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0060 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Identification (p.id), 2 bytes

Packets: 1095 · Displayed: 1095 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.17 | Profile: Default

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
334	15:33:12.464432	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=723b) [Reassembled in #335]
335	15:33:12.464448	192.168.1.212	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=12007/59182, ttl=255 (no response found!)
336	15:33:12.515333	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=723c) [Reassembled in #337]
337	15:33:12.515349	192.168.1.212	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=12008/59438, ttl=1 (no response found!)
338	15:33:12.518632	192.168.1.254	192.168.1.212	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
339	15:33:12.529749	192.168.1.212	192.168.1.254	DNS	86	Standard query 0x4877 PTR 254.1.168.192.in-addr.arpa PTR dsldevice.att.net
340	15:33:12.531351	192.168.1.254	192.168.1.212	DNS	117	Standard query response 0x4877 PTR 254.1.168.192.in-addr.arpa PTR dsldevice.att.net
341	15:33:12.532167	192.168.1.212	192.168.1.254	DNS	77	Standard query 0xbcc50 A dsldevice.att.net
342	15:33:12.533692	192.168.1.254	192.168.1.212	DNS	93	Standard query response 0xbcc50 A dsldevice.att.net A 192.168.1.254
343	15:33:12.559312	192.168.1.212	64.233.171.188	TCP	55	33733→5228 [ACK] Seq=0 Ack=1 Win=63 Len=1

Frame 335: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0

Ethernet II, Src: LiteonTe_ba:ce:e9 (c8:ff:28:ba:ce:e9), Dst: ArrisGro_89:be:d0 (b8:16:19:89:be:d0)

Internet Protocol Version 4, Src: 192.168.1.212, 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: 0x723b (29243)

Flags: 0x00

0... = Reserved bit: Not set

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

.0... = More fragments: Not set

Fragment offset: 1480

Time to live: 255

Protocol: ICMP (1)

Header checksum: 0x0f00 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.212

0010 02 08 72 3b 00 b9 ff 01 0f 00 c0 a8 01 d4 80 77 ..:.....W

0020 f5 0c 20 20 20 20 20 20 20 20 20 20 20 20 20 ..

0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Frame (534 bytes) Reassembled IPv4 (1980 bytes)

Identification (p.id), 2 bytes

Packets: 1095 · Displayed: 1095 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.17 | Profile: Default

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

There were three fragments created from the original datagram

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
821	15:33:46.241285	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7281) [Reassembled in #823]
822	15:33:46.241342	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7281) [Reassembled in #823]
823	15:33:46.241385	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12077/11567, ttl=255 (no response found!)
824	15:33:46.253709	192.168.1.212	216.92.151.75	TCP	54	[TCP ZeroWindow] [TCP ACKED unseen segment] 52241→80 [ACK] Seq=1 Ack=17 Win=0 Len=0
825	15:33:46.292063	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7282) [Reassembled in #827]
826	15:33:46.292097	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7282) [Reassembled in #827]
827	15:33:46.292121	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12078/11823, ttl=1 (no response found!)
828	15:33:46.294261	192.168.1.254	192.168.1.212	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
829	15:33:46.308836	192.168.1.212	192.168.1.254	DNS	86	Standard query 0x0022 PTR 254.1.168.192.in-addr.arpa
830	15:33:46.311156	192.168.1.254	192.168.1.212	DNS	117	Standard query response 0x0022 PTR 254.1.168.192.in-addr.arpa PTR dsldevice.att.net
831	15:33:46.312638	192.168.1.212	192.168.1.254	DNS	77	Standard query 0xd2a5 A dsldevice.att.net

0100 = Version: 4

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

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

Total Length: 1500

Identification: 0x7281 (29313)

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: 255

Protocol: ICMP (1)

Header checksum: 0xeb9e [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.212

Destination: 128.119.245.12

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

0010 05 dc 72 81 20 00 ff 01 eb 9e c0 a8 01 d4 80 77 ..:.....W

0020 f5 0c 00 00 ee f7 00 01 2f 2d 20 20 20 20 20 20 ..:...../-

0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

0060 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Identification (p.id), 2 bytes

Packets: 1095 · Displayed: 1095 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.17 | Profile: Default

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

The fields that change are flags, fragment offset, checksum, and total length. Each of the three packets has a unique fragment offset and checksum. The first two packets have the same total length and flags but the third has different values in those fields.

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
821	15:33:46.241285	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7281) [Reassembled in #823]
822	15:33:46.241342	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7281) [Reassembled in #823]
823	15:33:46.241385	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12077/11567, ttl=255 (no response found!)
824	15:33:46.253709	192.168.1.212	216.92.151.75	TCP	54	[TCP ZeroWindow] [TCP ACKed unseen segment] 52241-80 [ACK] Seq=1 Ack=17 Win=0 Len=0
825	15:33:46.292063	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7282) [Reassembled in #827]
826	15:33:46.292097	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7282) [Reassembled in #827]
827	15:33:46.292121	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12078/11823, ttl=1 (no response found!)
828	15:33:46.294261	192.168.1.254	192.168.1.212	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
829	15:33:46.308836	192.168.1.212	192.168.1.254	DNS	86	Standard query 0x0022 PTR 254.1.168.192.in-addr.arpa
830	15:33:46.311156	192.168.1.254	192.168.1.212	DNS	117	Standard query response 0x0022 PTR 254.1.168.192.in-addr.arpa PTR dsldevice.att.net

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 1500
 Identification: 0x7281 (29313)
 > 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: 255
 Protocol: ICMP (1)
 Header checksum: 0xeb9e [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.212
 Destination: 128.119.245.12
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]

0010 05 dc 72 81 20 00 ff 01 eb 9e c0 a8 01 d4 80 77 ..
 0020 f5 0c 08 00 ee f7 00 01 2f 2d 20 20 20 20 20 20
 0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0060 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Identification (p.id), 2 bytes

Packets: 1095 · Displayed: 1095 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.17 · Profile: Default

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
821	15:33:46.241285	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7281) [Reassembled in #823]
822	15:33:46.241342	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7281) [Reassembled in #823]
823	15:33:46.241385	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12077/11567, ttl=255 (no response found!)
824	15:33:46.253709	192.168.1.212	216.92.151.75	TCP	54	[TCP ZeroWindow] [TCP ACKed unseen segment] 52241-80 [ACK] Seq=1 Ack=17 Win=0 Len=0
825	15:33:46.292063	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7282) [Reassembled in #827]
826	15:33:46.292097	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7282) [Reassembled in #827]
827	15:33:46.292121	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12078/11823, ttl=1 (no response found!)
828	15:33:46.294261	192.168.1.254	192.168.1.212	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
829	15:33:46.308836	192.168.1.212	192.168.1.254	DNS	86	Standard query 0x0022 PTR 254.1.168.192.in-addr.arpa
830	15:33:46.311156	192.168.1.254	192.168.1.212	DNS	117	Standard query response 0x0022 PTR 254.1.168.192.in-addr.arpa PTR dsldevice.att.net

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 1500
 Identification: 0x7281 (29313)
 > 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: 255
 Protocol: ICMP (1)
 Header checksum: 0xaea5 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.212
 Destination: 128.119.245.12
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]

0010 05 dc 72 81 20 00 b9 ff 01 ea e5 c0 a8 01 d4 80 77 ..
 0020 f5 0c 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0060 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Identification (p.id), 2 bytes

Packets: 1095 · Displayed: 1095 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.17 · Profile: Default

lab 4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
821	15:33:46.241285	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7281) [Reassembled in #823]
822	15:33:46.241342	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7281) [Reassembled in #823]
823	15:33:46.241385	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12077/11567, ttl=255 (no response found!)
824	15:33:46.253709	192.168.1.212	216.92.151.75	TCP	54	[TCP ZeroWindow] [TCP ACKed unseen segment] 52241->80 [ACK] Seq=1 Ack=17 Win=0 Len=0
825	15:33:46.292063	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7282) [Reassembled in #827]
826	15:33:46.292097	192.168.1.212	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=7282) [Reassembled in #827]
827	15:33:46.292121	192.168.1.212	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=12078/11823, ttl=1 (no response found!)
828	15:33:46.294261	192.168.1.254	192.168.1.212	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
829	15:33:46.308836	192.168.1.212	192.168.1.254	DNS	86	Standard query 0x0022 PTR 254.1.168.192.in-addr.arpa
830	15:33:46.311156	192.168.1.254	192.168.1.212	DNS	117	Standard query response 0x0022 PTR 254.1.168.192.in-addr.arpa PTR dsldevice.att.net
831	15:33:46.312538	192.168.1.212	192.168.1.254	DNS	77	Standard query 0x026f A dsldevice.att.net

0100 ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 540
Identification: 0x7281 (29313)
Flags: 0x00
0... .. = Reserved bit: Not set
.0... .. = Don't fragment: Not set
..0... .. = More fragments: Not set
Fragment offset: 2960
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0x0ded [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.212
Destination: 128.119.245.12
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]

0010 02 1c 72 81 01 72 ff 01 0d ed c0 a8 01 d4 80 77 .. .P.W
0020 f5 0c 20 20 20 20 20 20 20 20 20 20 20 20 20 ..
0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Frame (554 bytes) Reassembled IPv4 (3480 bytes)
Identification (p.id), 2 bytes

Packets: 1095 · Displayed: 1095 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.17 | Profile: Default