1. Select the first UDP segment sent by your computer via the traceroute command to gaia.cs.umass.edu. (Hint: this is 44th packet in the trace file in the *ip-wireshark-trace1-1.pcapng* file in footnote 2). Expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?  
   It is 192.168.86.61
2. What is the value in the time-to-live (TTL) field in this IPv4 datagram’s header?

It is 1.



1. What is the value in the upper layer protocol field in this IPv4 datagram’s header? [Note: the answers for Linux/MacOS differ from Windows here.

17(UDP) for Linux/MacOS and 1(ICMP) for Windows.



1. How many bytes are in the IP header?

There are 20 bytes in the IP header.



1. How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.  
   There are 28 bytes in the payload of the IP datagram.



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

This IP datagram has not been fragmented. Because Fragment offset is 0.



1. Which fields in the IP datagram *always* change from one datagram to the next within this series of UDP segments sent by your computer destined to 128.119.245.12, via traceroute? Why?

The identification field has a different value because it uniquely identifies each IP datagram. The TTL field is also set to a different value for router discovery in the traceroute. The header checksum is also a value that verifies the arguments of the IP header, and its value changes when the header changes.

1. Which fields in this sequence of IP datagrams (containing UDP segments) ﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿stay constant? Why?

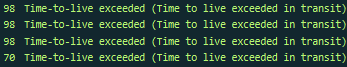
The Source IP Address remains the same as the sender's unique address. The Destination IP Address is fixed as the destination address of the traceroute command. The Protocol is fixed as UDP at the upper layer and is applied equally to all datagrams.

1. Describe the pattern you see in the values in the Identification field of the IP datagrams being sent by your computer.

The identification value increases sequentially by 1 for each datagram.

1. What is the upper layer protocol specified in the IP datagrams returned from the routers? [Note: the answers for Linux/MacOS differ from Windows here].

The upper layer protocol specified in the IP datagrams returned from the routers is ICMP. Because ICMP sends “time exceeded”.



1. Are the values in the Identification fields (across the sequence of all of ICMP packets from all of the routers) similar in behavior to your answer to question 9 above?

The Identification field of an ICMP packet returned from a router has a different rule than the Identification field of a UDP packet. This is because the Identification field of an ICMP packet returned from a router is generated individually.

1. Are the values of the TTL fields similar, across all of ICMP packets from all of the routers?   
   No. The values ​​of the TTL fields are irregular.

1. Find the first IP datagram containing the first part of the segment sent to 128.119.245.12 sent by your computer via the traceroute command to gaia.cs.umass.edu, *after* you specified that the traceroute packet length should be 3000. (Hint: This is packet 179 in the *ip-wireshark-trace1-1.pcapng* trace file in footnote 2. Packets 179, 180, and 181 are three IP datagrams created by fragmenting the first single 3000-byte UDP segment sent to 128.119.145.12). Has that segment been fragmented across more than one IP datagram? (Hint: the answer is yes[[1]](#footnote-1)!)

Yes. segment been fragmented across more than one IP datagram.



1. What information in the IP header indicates that this datagram been fragmented?

MF flag indicate that this datagram has been fragmented.

텍스트, 폰트, 스크린샷, 화이트이(가) 표시된 사진

자동 생성된 설명

1. What information in the IP header for this packet indicates whether this is the first fragment versus a latter fragment?

Fragment offset can indicates whether this is the first fragment versus a latter fragment. If Fragment Offset = 0, it is the first fragment.  


1. How many bytes are there in is this IP datagram (header plus payload)?

IP header = 20 bytes, Data = 1480 bytes. So there are 1500 bytes in this IP datagram.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

1. Now inspect the datagram containing the second fragment of the fragmented UDP segment. What information in the IP header indicates that this is *not* the first datagram fragment?

MF flags = 1 & Fragment Offset = not zero indicates that this in not the first datagram fragment.

텍스트, 폰트, 스크린샷, 영수증이(가) 표시된 사진

자동 생성된 설명

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

Identification field and Fragment Offset are changed.

1. Now find the IP datagram containing the third fragment of the original UDP segment. What information in the IP header indicates that this is the last fragment of that segment?

MF flag is set 0.



1. What is the IPv6 address of the computer making the DNS AAAA request? This is the source address of the 20th packet in the trace. Give the IPv6 source address for this datagram in the exact same form as displayed in the Wireshark window[[2]](#footnote-2).

78:4f:43:98:d9:27



1. What is the IPv6 destination address for this datagram? Give this IPv6 address in the exact same form as displayed in the Wireshark window.

44:1c:12:81:74:5a



1. What is the value of the flow label for this datagram?

0x63ed0



1. How much payload data is carried in this datagram?

29 bytes is carried in this datagram.



1. What is the upper layer protocol to which this datagram’s payload will be delivered at the destination?

The upper layer protocol is UDP



1. How many IPv6 addresses are returned in the response to this AAAA request?

There are 4 IPv6 addresses.

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

1. What is the first of the IPv6 addresses returned by the DNS for youtube.com (in the ip-wireshark-trace2-1.pcapng trace file, this is also the address that is numerically the smallest)? Give this IPv6 address in the exact same shorthand form as displayed in the Wireshark window.

2607:f8b0:4006:806::200e

1. Note: if you find your packet has not been fragmented, you should download the zip file in footnote 2 and extract the trace file *ip-wireshark-trace1-1.pcapng* . If your computer has an Ethernet or WiFi interface, a packet size of 3000 *should* cause fragmentation. [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)