**IP Lab**

Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

192.168.86.31

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

ICMP

How many bytes are in the IP header? 20 How many bytes are in the payload of the IP datagram? 3480 Explain how you determined the number of payload bytes.

Has this IP datagram been fragmented? Yes Explain how you determined whether or not the datagram has been fragmented. I typed in 3500 and it gave back 3480 witch is 20 less and the other 20 is in the header

Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer? Looks like Identification, Time to Live, Header Checksum

Which fields stay constant? Total Length, Flags, Protocol, source Address, destination Address Which of the fields must stay constant? source Address, destination Address Which fields must change? Identification Why? Each call should have their own Identification but the same addresses

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

Always +1 as we go down on the source.

What is the value in the Identification field and the TTL field? The Identification fields are all 0x0000, and the Time to Live is all 245 witch is different from request. It is only the same for all the same source numbers. Each different source numbers has a different ID and TTL but within the source it all the same

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

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? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the ipethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.3 ]

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?

**DNS Lab**

Locate the DNS query and response messages. Are then sent over UDP or TCP?

UDP

What is the destination port for the DNS query message? What is the source port of DNS response message?

58364

53

To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

104.16.45.99

No

Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

A

Yes, two

Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Only three

Cloud

Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

no

This web page contains images. Before retrieving each image, does your host issue new DNS queries?

11. What is the destination port for the DNS query message? What is the source port

of DNS response message?

3740

53

12. To what IP address is the DNS query message sent? Is this the IP address of your

default local DNS server?

128.238.38.160

128.238.29.22

13. Examine the DNS query message. What “Type” of DNS query is it? Does the

query message contain any “answers”?

A

no

14. Examine the DNS response message. How many “answers” are provided? What

do each of these answers contain?

One

Name Type Class TTL DataLength DomainName

15. Provide a screenshot

16. To what IP address is the DNS query message sent? Is this the IP address of your

default local DNS server?

128.238.38.160

No

17. Examine the DNS query message. What “Type” of DNS query is it? Does the

query message contain any “answers”?

PTR or Ns

no

18. Examine the DNS response message. What MIT nameservers does the response

message provide? Does this response message also provide the IP addresses of the

MIT namesers?

19. Provide a screenshot.

20. To what IP address is the DNS query message sent? Is this the IP address of your

default local DNS server? If not, what does the IP address correspond to?

21. Examine the DNS query message. What “Type” of DNS query is it? Does the

query message contain any “answers”?

22. Examine the DNS response message. How many “answers” are provided? What

does each of these answers contain?

23. Provide a screenshot.

**HTP Lab**

Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

1.1

2.4.6

What languages (if any) does your browser indicate that it can accept to the server?

En-US

What is the IP address of your computer? Of the gaia.cs.umass.edu server?

192.168.86.31

128.119.245.12

What is the status code returned from the server to your browser?

200

When was the HTML file that you are retrieving last modified at the server?

Sat 30 jan 2021 06:59:02GMT

How many bytes of content are being returned to your browser?

128

By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Yes, Cache-control, If-Modified since, if none match, upgrade-insecure-requests

**TCP Lab**

3. What is the IP address and TCP port number used by your client computer

(source) to transfer the file to gaia.cs.umass.edu?

192.168.86.31

61715

4. What is the sequence number of the TCP SYN segment that is used to initiate the

TCP connection between the client computer and gaia.cs.umass.edu? What is it

in the segment that identifies the segment as a SYN segment?

5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu

to the client computer in reply to the SYN? What is the value of the

Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu

determine that value? What is it in the segment that identifies the segment as a

SYNACK segment?

6. What is the sequence number of the TCP segment containing the HTTP POST

command? Note that in order to find the POST command, you’ll need to dig into

the packet content field at the bottom of the Wireshark window, looking for a

segment with a “POST” within its DATA field.

7. Consider the TCP segment containing the HTTP POST as the first segment in the

TCP connection. What are the sequence numbers of the first six segments in the

**Intro Lab:**

I ran into a little difficulty with the intro lab. The example shown in the pdf in figure 4 was not what I was seeing on my screen. I have about 11 different capture interfaces that were available on my Wireshark. Whereas the example only had two capture interfaces. The example also said to select Gigabit Network Connection, and I did not have that option on my wireshark. Thus, It took me a little bit to figure out what one I needed to use for the intro lab and to follow the examples. I eventually found out it was Microsoft: Wi-fi that I wanted to use. I figured this out because it was the only one out of my eleven choices that outputted the intro-wireshark-file1.html.

Another issue I ran into while doing the intro lab was again in figure 4. In figure 4 it showed a start button right next to the options. Mine did not have any start buttons at all. I was just randomly clicking and saw that I could just double click on the selection I wanted, and it ran.

**IP Lab:**

For this lab I downloaded ping plotter to capture my pockets. I then recorded the pockets with Wireshark. I captured pockets from www.pingplotter.com on ping plotter. I captured 3 different packet sizes at 56, 2000, and 3500. I then analyzed all the information on Wireshark and ran though the questions in the lab. Showed me how ICMP Request has all different identifications and Time to Live, whereas the ICMP Time to Live all have the same identifications and Time to Live for the same sources. I found this interesting because I would have thought identifications should be different for all but it’s not the case for ICMP Time to Live.

**DNS Lab**

For this lab I ran nslookup in my windows command prompt. I ran the code suggested in the lab as nslookup www.mit.edu I also ran nslookup www.studentaid.gov. In the example they showed the command had a server name. However, when I ran both of the commands my server name came up as unknow. Same thing happened when I ran the second command. However, when I ran the third command it gave me a server name but the DNS timed out. I decided I would continue with the lab and further investigate the issue later.

I looked into trying to get the issue resolved however, I was not able to. I tried to edit my firewall but could not find a workaround. Thus. I continued with the rest of the lab hoping I could still complete it.

I then used Wireshark to capture the DNS from the given website. I found out that my DNS pockets were being sent over UDP

At this point I stopped the lab because my nslookup was not working. I am going to see if I can get it to work on my mac or other windows.

**HTTP Lab**

For this lab I captured a http pocket in Wireshark with the given 1-line html document. This one already looked different then the other labs I have done because it only produced 2 http pockets. All the other pockets I captured so had a lot more even with the filters on. I then ran thought the questions on the lab answering everything they asked. Then, I compared those answers with the raw data in the inspect on the html document. I found most the information was the same as the information in Wireshark. However, I did notice there were a few fields that were not in Wireshark. Cache-control, If-Modified since, if none match, and upgrade-insecure-requests were all listed in the raw data but not in the data in Wireshark.

I then ran the second html file and captured the pockets in Wireshark. This time I noticed that it had If-Modified since, if none match, Cache-control, and upgrade-insecure-requests listed in the Wireshark Get. As noted before those were not listed there in the first file. However, It did not give the line based text like the first file and third file did. I also noticed that the Status code and phrase for files one and three were the same but for this second file the status code and phrase were changed.

I ran though and looked at the data for the fourth file as well. I noticed that it was similar to the second file. Lastly, I ran the fifth file twice. I ran it two times because The first time I did not read far enough in the lab to see they gave you a user name and password.