Huynh (Dan) Doan  
3/9/2021

Cis2337-18348

Tuesday & Thursday 5:50-7:00

Wireshark Lab

1. First, open the trace file dns-walk.pcap and examine Line #1.
2. What type of DNS query is this (full title)?

According to Wireshark, if you open up the Domain Name System (query) and then open up the queries, it will show you that the type is SOA, also known as Start Of a zone of Authority (6).

1. What byte offset in this packet marks the beginning of the IP protocol?

If you counts the bytes at the bottom of the screen, it will tells you that there are 14 bytes before the first beginning bytes from the IP protocol. With the IP starting at/from 15.

1. What are the similarities of the DNS protocols of these two packets?

Their similarities are that they both have the same Transaction ID, they are both standard query, they both require recursion, and then their type and class is the same, being type A and class IN.

1. What is the answer to the query?

The answer to the query seems to be like a website, ns11a.verui-web.com, with type A and class In with the website IP address being 161.58.148.38.

1. Close this file and open ipv6-mcasts.pcap. Examine packet 10.
2. What do you notice about the way the IPv6 destination address is written in the Packet Details Pane and the packet bytes window?

From the look of the destination of packet 6, it seems shorter/can be reduced and maybe easier to understand. If you look at the bytes section it starts off with 60, classification for ipv6, followed by the ipv6 address of the source, and followed by the ipv6 address of the destination.

1. Close this file and open icmp-lotsostuff.pcap.
2. What is the source and destination address of the original request? What type of traffic was the original request?

The source and destination address of the original request is 192.168.1.105, being the source address, and 192.168.1.100 being the destination address. According to Wireshark they were trying to send an efi-mg (2224) over to snmp (161), with the 2224 port being a game of some sort trying to reach a server I assume.

1. To how many different servers and to what addresses did the client in question 3(a) attempt the same request?

They tried to sent it to about 6 different servers, changing the last number in the IPv4 every time doing it.

1. What type of Operating System is each of these computers (Windows or Linux)? How do you know?

According to some googling, you can find out which operating system by using ping/tracert command through the TTL, or time to live, and find out. With TTL values being 64 = Unix/Linux, 128 = Windows, and 254 = Solaris/AIX. And with our packets being TTL 128, our machine is running Windows Operating System.

1. Open http-browse-ok.pcap.
2. Beginning with the first line, how many packets are involved with this initial conversation?

It took about 8 total packets to finish the initial conversation.

1. What happened?

It look like they were both sending and receiving status codes and information regarding the initial request which they both went back and forth until they finished.

1. Openhttp-microsoft.pcap.
2. What is the title (text in between the two “<title>” tags in the line-based text data) of the first text/html document found after applying the filter? (Hint: you may have to look in the Packet Byte Pane to see the whole title.)

The title inside of the first text/html document is “Microsoft Corporation”.

1. How can you create a filter to show only the client's HTTP GET requests? After applying that filter, how many packets are left? (Hint: look for the number of packets “Marked” in the Status Bar at the bottom of the window.)

You can filter it out to only contain “GET” packages by using “http.request.method == "GET"” in the filter.

1. Openhttps-justlaunchpage.pcap.
2. What handshake messages take place in order to establish encryption between these two computers?

There were 4 (2 if you don’t count responses) of them being hello from client and server hello back, server showing certificate and then hello done. Next both of them exchanged key in order to encrypt handshake messages to each other.

1. What kind of data is this? What are the first five bytes of the data? (Remember, this is hexadecimal, so each letter/number represents half of a byte. Thus, you need to find five pairs.)

It is a transport layer security containing http-over-tls, meaning it is a secured/encrypted transfer of html over the transport layer security. The first five bytes contain the content type, the version, and then the length of the data. In this case it is Application for the content, TLS 1.0 for the version and the length is 708.

1. Open smtp-normal.pcap and consider the entire trace file.
2. How would a client or mail server handle an email with multiple recipients in the To, CC, or BCC fields?

They would have to connect to each and everyone of the To, CC, and BCC emails destination and then be able to send them to each and everyone of them.

1. How many times has the body (the message) of the email been included in this packet?

It seems like it has included the body of the email two times in this packet.

1. What are the different formats the body has been encapsulated into?

It has been encapsulated into a text/plain part and a text/html part

1. Why has the mail client done this?

It has done this because it used MIME to be able to format the body of the message into two separate section and then sent it over email for the client to decode each section separately with different rules.

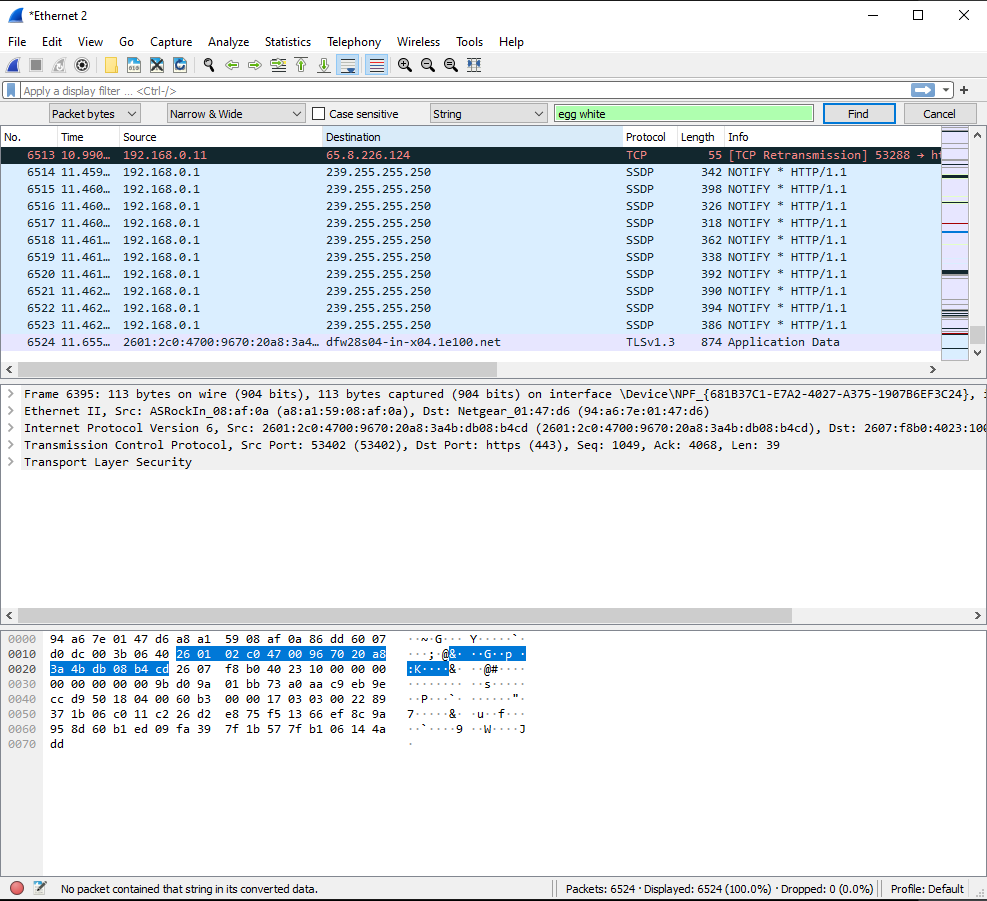


Figure 1.

## Live Traffic Capture

1. Open Firefox and let the browser connect to its default home page. How many packets were created?

Just from opening the browser alone, it created 80 packets just to connect to the home page. But it was also loading a few packets before I opened up Firefox into its default page so I am not sure where it is coming from. It shows that the source is from me and destination is from my internet provider, but I do not have any other applications open beside a word document, Wireshark, and google chrome of a PDF open.

1. Search for something unique but appropriate (i.e. nothing obscene, pornographic, etc.), then find the first packet that contains your search string (use Edit → Find Packet …, then search by string and search in the Packet bytes). Where in your packet did the string appear? What kind of packet is this?

I tried doing this step with two different browser, one being Firefox and the other one being chrome and with both of them I was unable to find any packet containing my searched value. I have included a screen shot of searching (Figure 1.)from Firefox, where I searched “egg white” and then at the bottom of the screenshot you can see Wireshark could not find any packet contained that string in its searched data with the string being “egg white”. I also tried using just “egg” and “white”, but nothing also came out of that. I believe that this might be because google uses something that won’t allow the sniffer to find out what the user might be searching for privacy reasons. Some other reason I could think of is that google is HTTPS and Wireshark isn’t great at sniffing details of https websites.

1. Go to a web site for which you have a username and password and log in. Is the log in page encrypted (connect so https://instead of http://)? Can you find your username unencrypted in the packets? What about your password? Try a few different sites. (Note: in the lab writeup, do not reveal your username or password.)

I went ahead and reached our blackboard website, which Wireshark’s said it is connected using https(443) and I could not find any packets containing my username or password data. I tried logging into both the blackboard website and YouTube, nothing from Wireshark regarding my username or passwords.

## Questionnaires from the Turn-in

One page Description of Wireshark and components – what does it do and how?

Wireshark uses your network flow of information, all the packets that are sent by you and received by the destination of your choice into a nice UI that you can check and see all types of information that was captured by Wireshark.

How can Wireshark help system administrators?

Wireshark can help system admin by allowing them to see what is going in and out of the router, allowing them to check which machine/ip address is sending what information and receiving what information. It could also allow them to pin point the person/machine doing so by using such IP address given by Wireshark and what type of information that was exchanged by using the information given.

Describe the various network protocols discussed in this laboratory, what role they play in making the Internet work or in our daily lives, and how they relate to each other.

Some of the most important ones that were discussed in this lab were HTTPS, HTTP, MIME, IMF, SMTP, IPv4, IPv6 and DNS. All of them helps our computer connect to every website that we want with ease and encrypt them so that no one outside of our network can see what we are doing. Protocols such as HTTPS help us by encrypting our webpage visit and then our username and password for logins, MINE and SMTP help us by decoding and sending emails to each other, while IPv4 and IPv6 identifies who we are.

Answer the questions and describe what you learned from the live capture portion of this laboratory

From the live capture portion, I learned that there are many packets that will be exchanged even if you do such a simple task, for example opening a browser to its default page could take up to 50 or 200 packets to do so. While searching for a simple string on google can net up to hundreds and thousands of packet just from one simple google search. This knowledge was unknown to me prior to this lab since I thought that only one or two packets would be exchanged every time I do something, not a hundred or thousands of them. I also learned that HTTPS protect all login information’s in the packet exchanges from anyone that would be sniffing for such information. The searching for my string that I searched for went a little bad since I could not find what I was looking up. I am not sure if this was supposed to happen or not since apparently google uses SSL whenever you searches. Meaning that SSL encrypts the information to prevent people from sniffing (aka me in this example) my information that I am searching up. But their website also said that they don’t always hide the search term that I typed so could also mean I did something wrong.