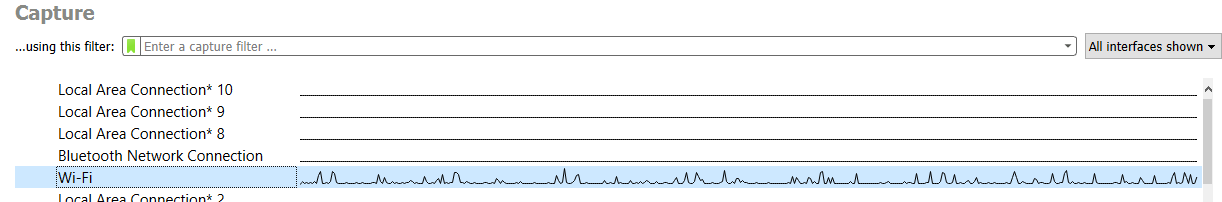
**Question 1: what did you do?**

For this assignment, we were instructed to download and install a network analysis tool called Wireshark and use it to capture packets in real time. This tool includes a variety of settings and filters which enables one to dig deep into network traffic and inspect individual packets. Once skilled, you could use Wireshark to inspect a suspicious program’s network traffic, analyze your own network’s traffic flow or even troubleshoot network problems.

After launching the Wireshark program, I captured packets specifically on the Wifi network interface and left the promiscuous mode enabled which allowed me to see all packets on the network aside from just those addressed to my network adapter.



First, I scanned my home network which is password protected. I was surprised to see our network stretched a good distance past our back fence meaning anyone could park on the public road behind the fence and connect to our network if we left it open. I added network range extenders in our home so we could more seamlessly add wireless cameras but the added range could also be our downfall if we didn’t secure it. Second, I then scanned my general neighborhood areas looking to find an unsecured option to connect to and test but amazingly, all of my neighbors intelligently have secured their networks. I know back when I was in college this was not the case as friends would surf for free internet connections all the time. How little we understood what that free YouTube video could have cost us. As I could not find any open networks to capture from, I took a little bit of time and was able to drive to a shopping center area. I found one open network to connect to and use Wireshark to capture packets. From all the packets I captured, home and the open network I found, I was able to inspect and apply filters by type such as “dns” as well as use Wireshark to follow a TCP stream. This allows me to see the entire TCP conversation which occurred between the client and server.

For the second part of the assignment, I completed two phishing exercises which displayed examples of both phish and legitimate email or websites and I had to determined if the example was a phish or not. A quick definition – phishing is a type of social engineering attack used to steal data. It occurs when the attacker is masquerading as a trusted source and tricks someone into opening an email, an attachment, downloading a file or responding to a text message. Doing any of these seemingly simple things can lead to the installation of malware and ultimately a breach of your sensitive information.

Phishing attack training is something many workplaces utilize these days to help employees improve their cyber awareness thus protecting the company from fraud. There are many dangers to social engineering and building a system and behaviors able to detect potential phishing attacks allows you to take the appropriate actions to protect yourself.

**Question 2: what were the results?**

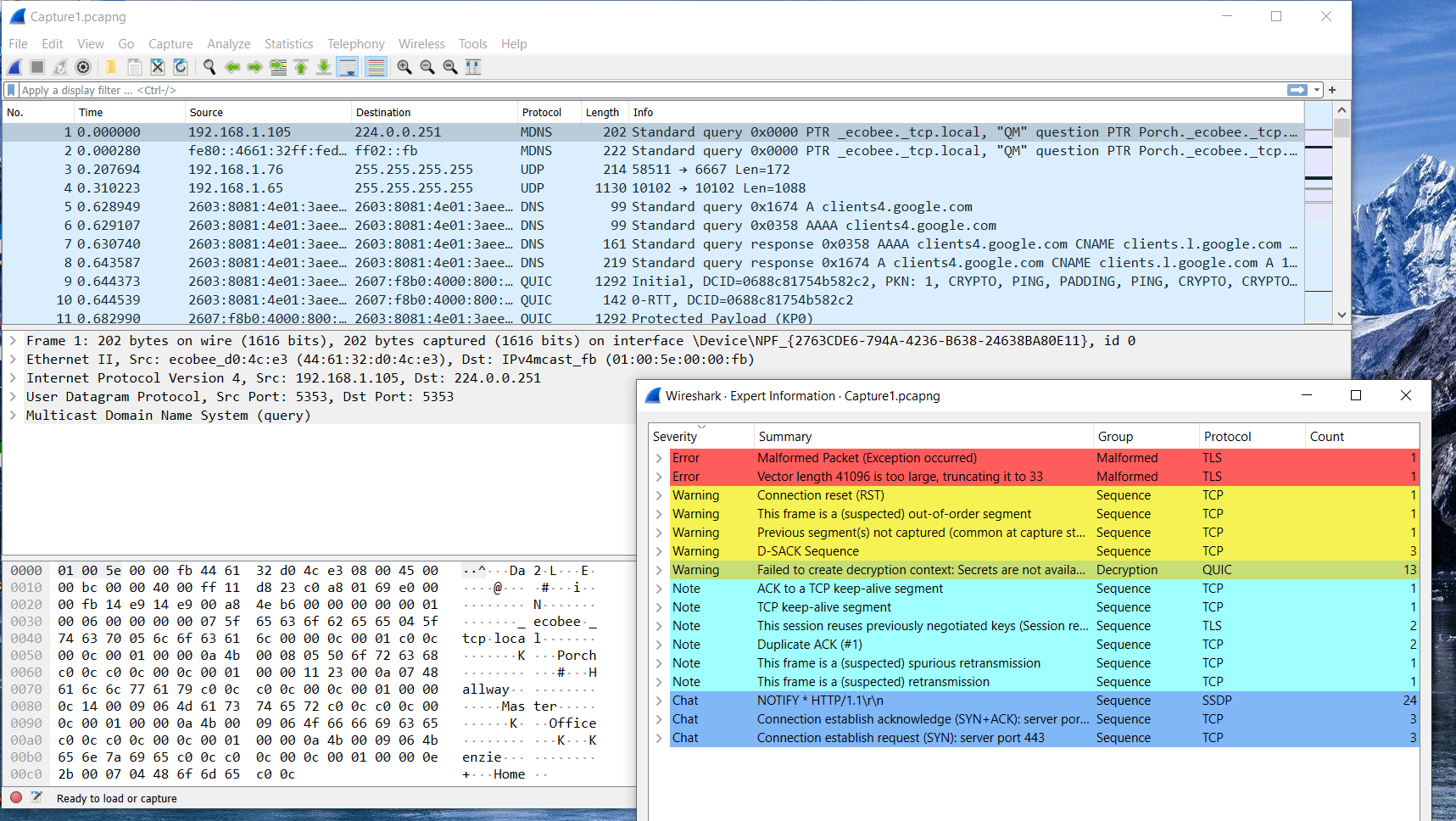
My captures were grouped by severity level seen color coded in each screenshot below. Wireshark color codes and ranks the items. Blue indicates information of usual workflows which were a great deal of my captures. Cyan blue were indicative of when an application returned a simple or common error code. Warnings were highlighted in yellow and represent error codes such as connection issues. Then finally red which can be a more serious error and the grouping I had for those noted malformed packets. The malformed packets indicate there’s a bug of sorts and due to this, the packet is aborted.

Almost all of my captures were grouped by sequence, which represents when a protocol sequence number is potentially suspicious meaning the sequence was not continuous or a retransmission was detected. I did find it interesting the high severity capture actually occurred on my home network which is secured compared to the open network I briefly captured from.

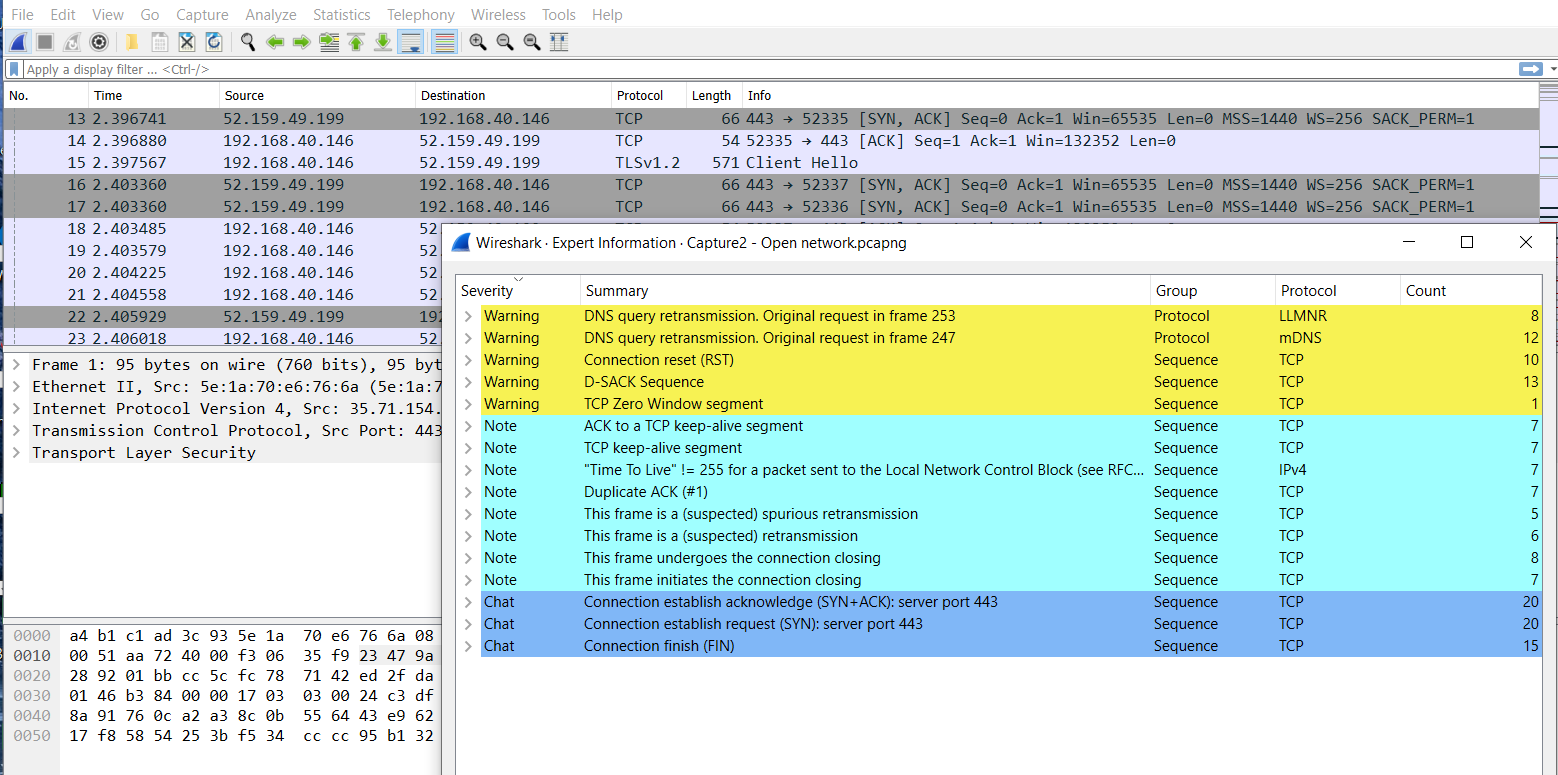
Digging into the capture I did on my home network using the filtering, I found many of the yellow sequencing items to actually be stemming from our house-wide Ring camera system and what I believe to be is the cameras and Ring Wi-Fi range extenders retransmitting the signal. This brings me a bit of relief and I was somewhat worried initially seeing all the severity issues highlighted from the capture.

For the open network capture, I received a high number of DNS query retransmission items. I looked into this and it simply means the DNS query has no corresponding response received by the host and so it sends the query again. Often retransmission like this occurs due to the Windows client timing out too quickly so the server response and the client’s retransmission basically pass each other in the network.

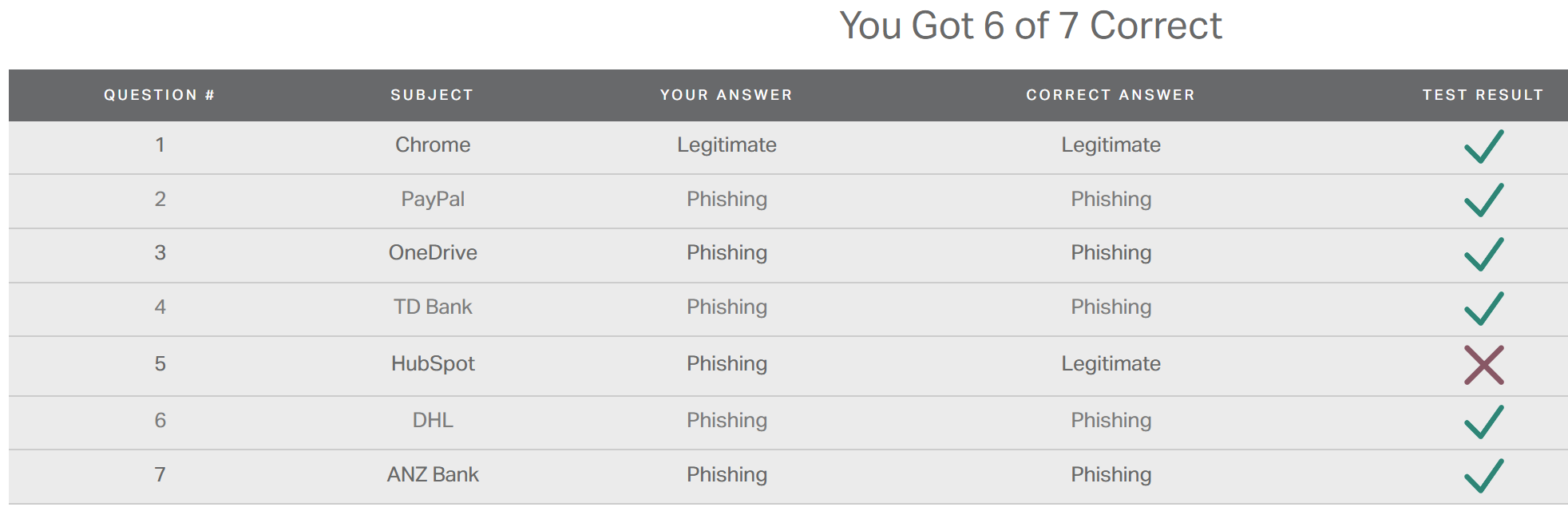
**Home Network Capture results**



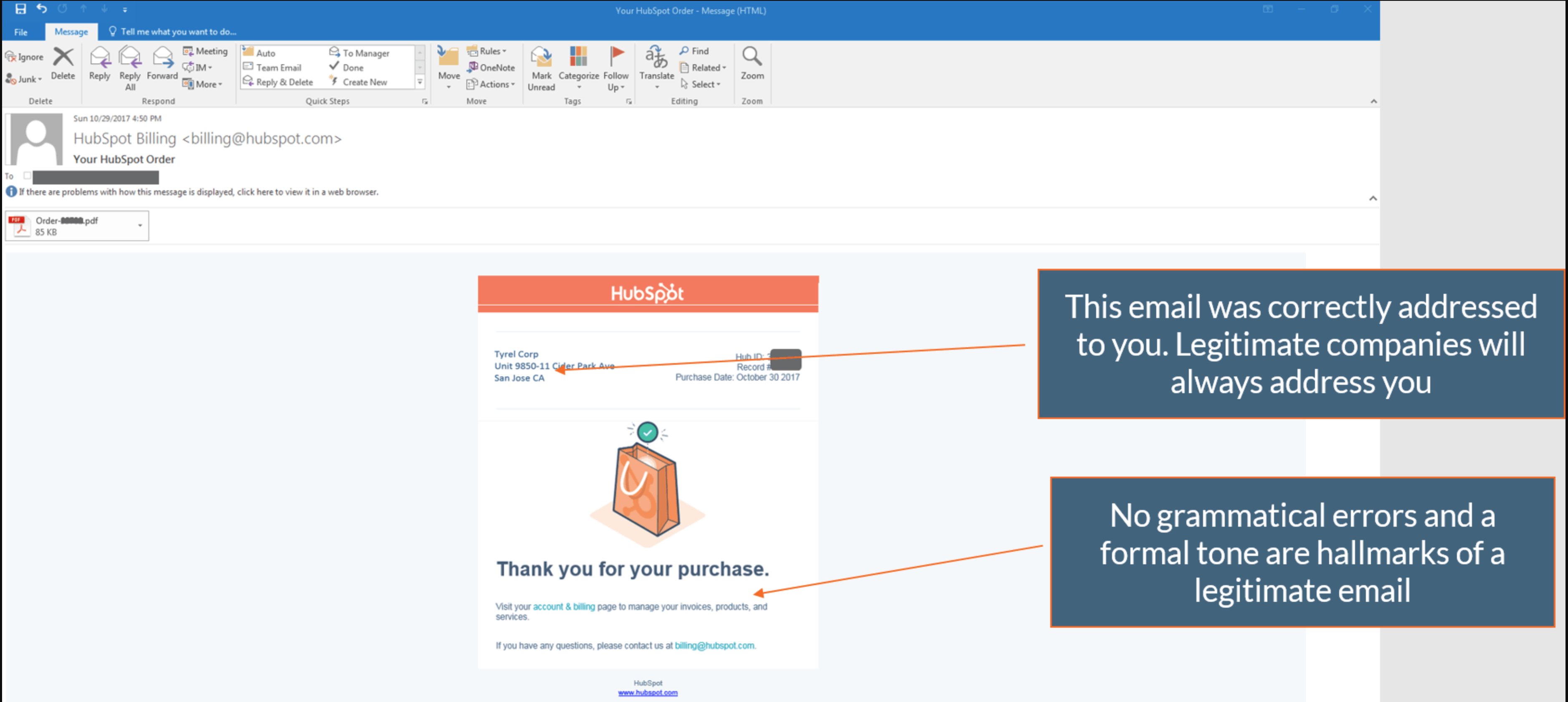
**Open Network Capture results**



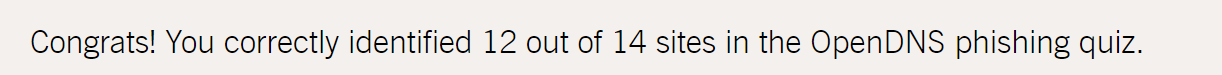
For the second part of the assignment which tested phishing, below are my results from the two quizzes. On the Sonicwall quiz, I correctly guessed 6 of the 7 examples. Each example I was presented with was one of the typical methods used by malicious individuals in phishing attacks.



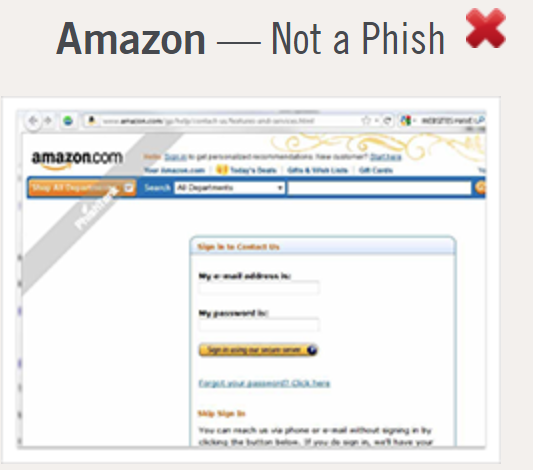
I missed the below example. This did look possibly real to me but I actually selected phish only because of the different dates listed in the email. The date of the bill was for the date after the email was sent. My reasoning was how could I receive a bill from the future and thus it was suspect in my mind. I suppose it is a good thing to be more wary than not in these instances.



For the Open DNS quiz, I completed it with only missing two test examples. Again, I was presented with usual instances of phishing attacks and had to determine whether the item was legitimate or not.



For the items I missed, I jumped immediately to feeling the example was suspect due to the very long website address. I have been used to being warned of long addresses as they can be long when rerouting you to another destination you were not aiming to visit. One example is shown below and you can see how long the website address is. Again, it is probably for the best that I do not trust easily when reviewing things I receive in the cyber universe.



**Question 3: what did you learn?**

This assignment opened my eyes to the truth behind what I have always heard of “Never connect to an open Wi-Fi network”. I learned my entire connection is essentially broadcasted, and when on an open network it’s unencrypted, so all that someone needs to watch what I do is a wireless interface capture tool in monitoring mode. While the initial capture looks like garbled amounts of characters and information, using a tool to filter it organizes it very easily. Without any encryption, it would be comparable to me writing my passwords down on the back of a postcard and sending that through the public mail system. Anyone could see it plain as day.

Also, I had no idea how simple it is for black hat hackers to intentionally broadcast their own signal pretending to be a McDonalds or Starbucks open network and then capture all of the traffic automatically. This is how important information like passwords, banking logins or work security features can be stolen. And that individual doesn’t have to sort out your information that moment. They can save the capture and dig through it at a later time. In short, I learned if I need to use a connection and there are only public open options available, I should never trust it and use VPN. A VPN tunnel adds a layer of safety.

For the second half of the assignment, I learned that email offers hackers a vehicle to deliver a variety of vulnerabilities to your system as well as organization, by using ransomware or other malicious tools. Cyber criminals are cleverer than ever at creating sites that fool even the most experienced phishing security layers. Phishing is used to gain a tooth or foothold into not just personal networks, but corporations and governments. Employees can unknowingly compromise all security perimeters that have been established by doing something as simple as clicking a link in an email. This gesture however small, can cause an organization to succumb to an attack and sustain all kinds of financial losses in addition to reputation or brand damage, loss of consumer trust and a reduced market share. A business can have a hard time recovering from such an attack.

For an individual, this could equate to unauthorized purchases made using their accounts or identity theft. In general, email phishing is a simple statistics numbers game. Mass amounts of emails are sent out and even if only a tiny percentage fall for the scam, the attacker can net significant information and maybe even sums of money. The most common attack used is one that drives a sense of urgency with a deadline, such as, if you do not reset your password immediately to ABC account it will be deactivated or something along those lines. This catches people attention quickly and applying such a level of pressure causes the person to be less diligent and more prone to making a rash and ultimately, bad, decision.