Project 2 Lab: Detecting Malicious Attacks

Ifeanyi Uzoukwu

CST 620

University of Maryland Global Campus

29 January 2021

**Introduction**

This lab report was assigned to help students learn about malicious attacks and how to detect them. Using Snort and Wireshark, I was able to learn about network intrusion, and have put together an experimental results report documenting these findings.

**Task 1**: Using Snort: Snort is an open-source Network Intrusion program that runs mainly from the command prompt function in Windows. The following figures and captions document the work I conducted in this lab.

Figure 1: Opening Up Snort

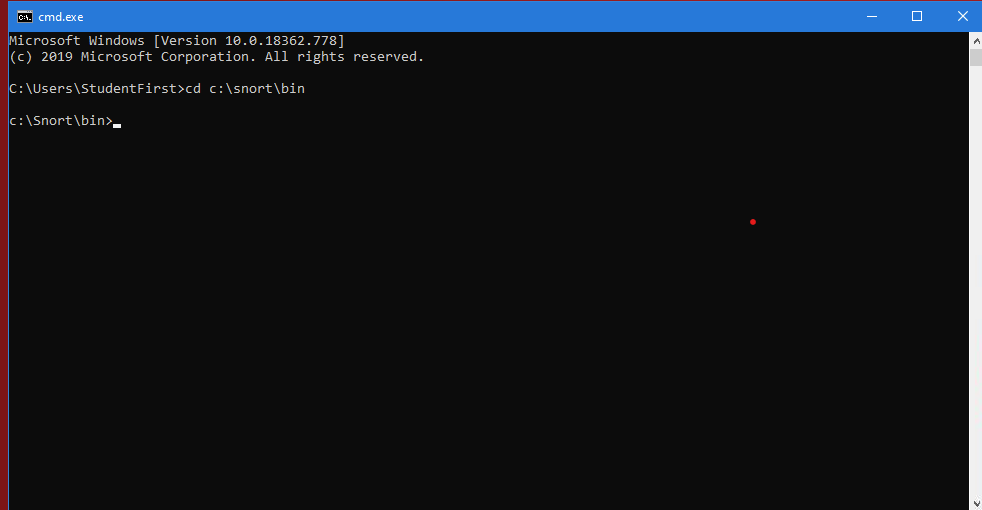


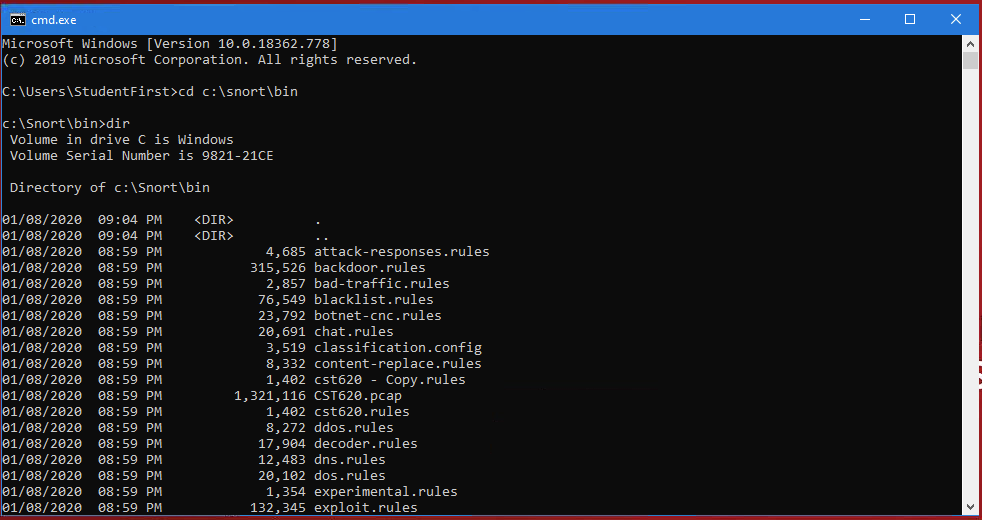
Figure 2: Snort Directory

Figure 3: Viewing Configuration Files

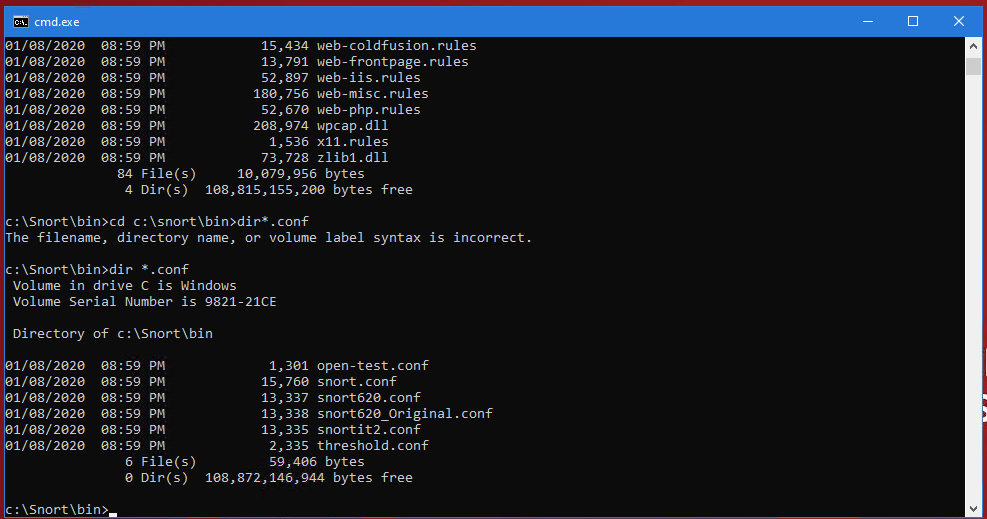


Figure 4: Viewing Rule Files

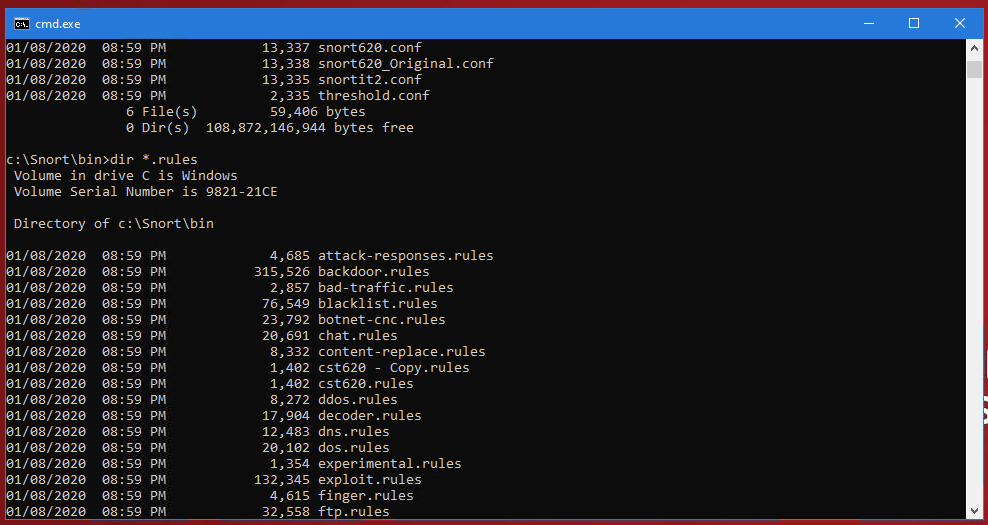


Figure 5: Viewing Packet Capture Files

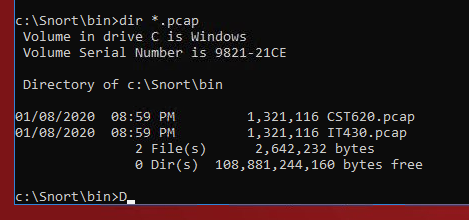


Figure 6: Viewing Log Directory

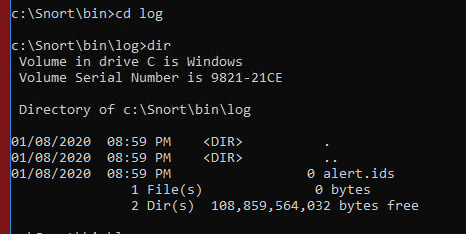


Figure 7: Directory Change and Test Run

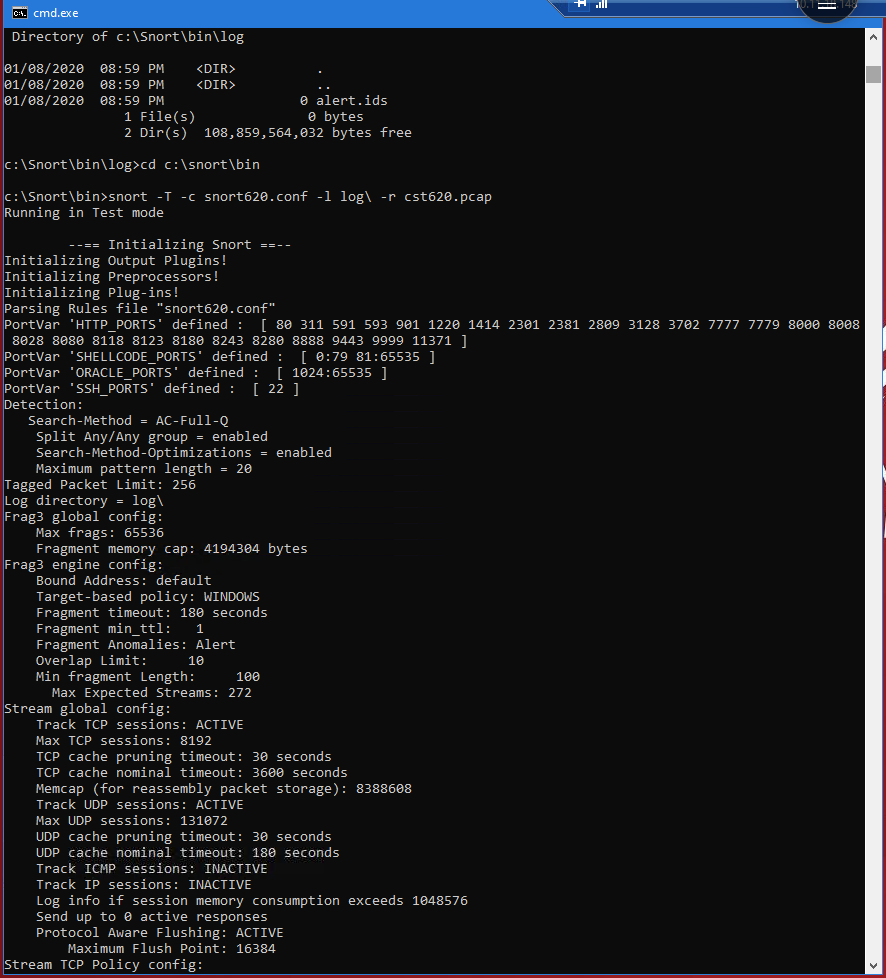


Figure 8: Empty Log after Alert was deleted

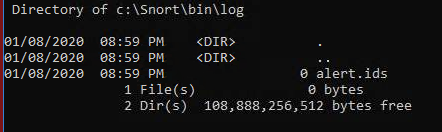


Figure 9: Log After initial ruleset run

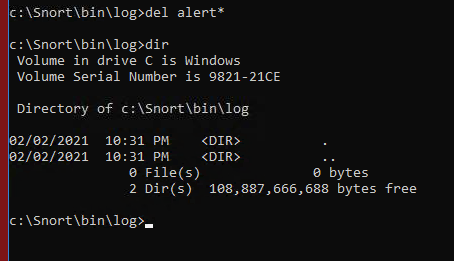


Figure 10: Running .pcap file through ruleset

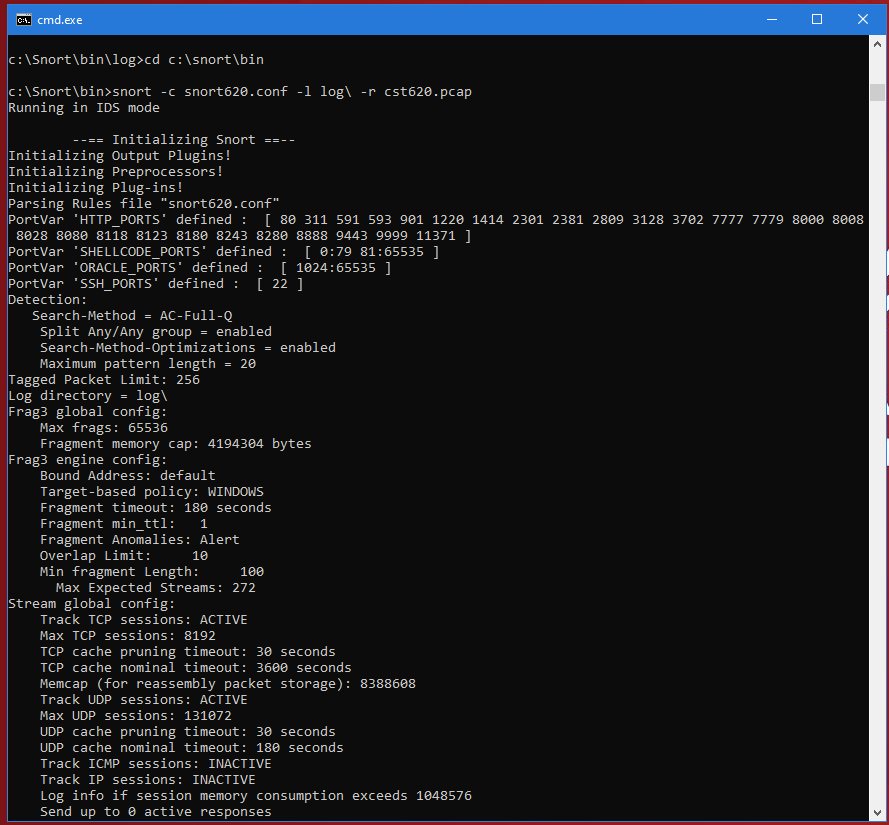


Figure 11: Directory after ruleset run

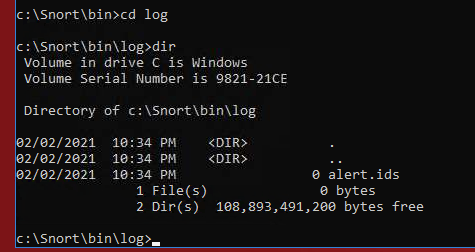


Figure 12: Created Alert.ids file in Windows Explorer

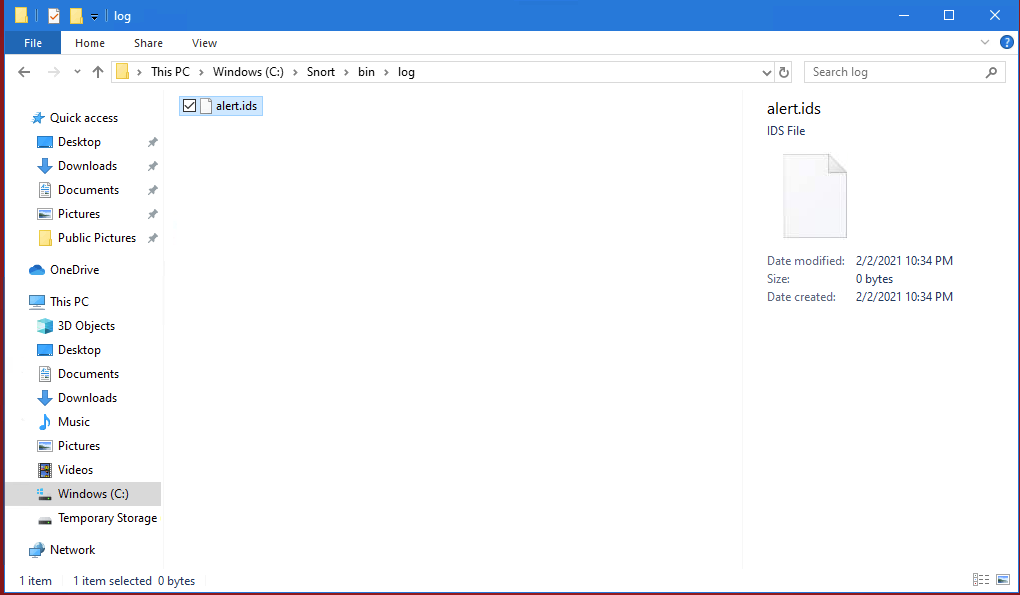


Figure 13: Alert.ids file opened up in WordPad (Empty File)

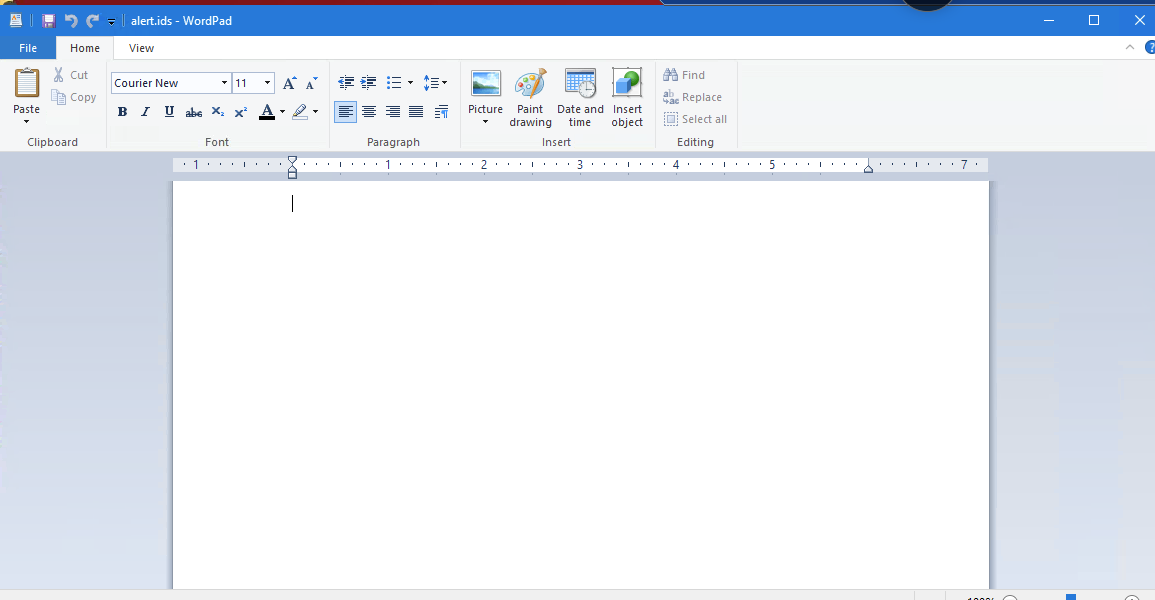


Figure 14: cst620.rules file copied

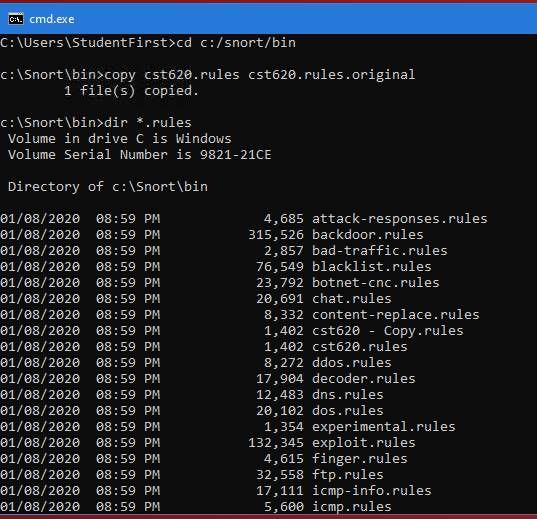


Figure 15: Opening cst620.rules in WordPad

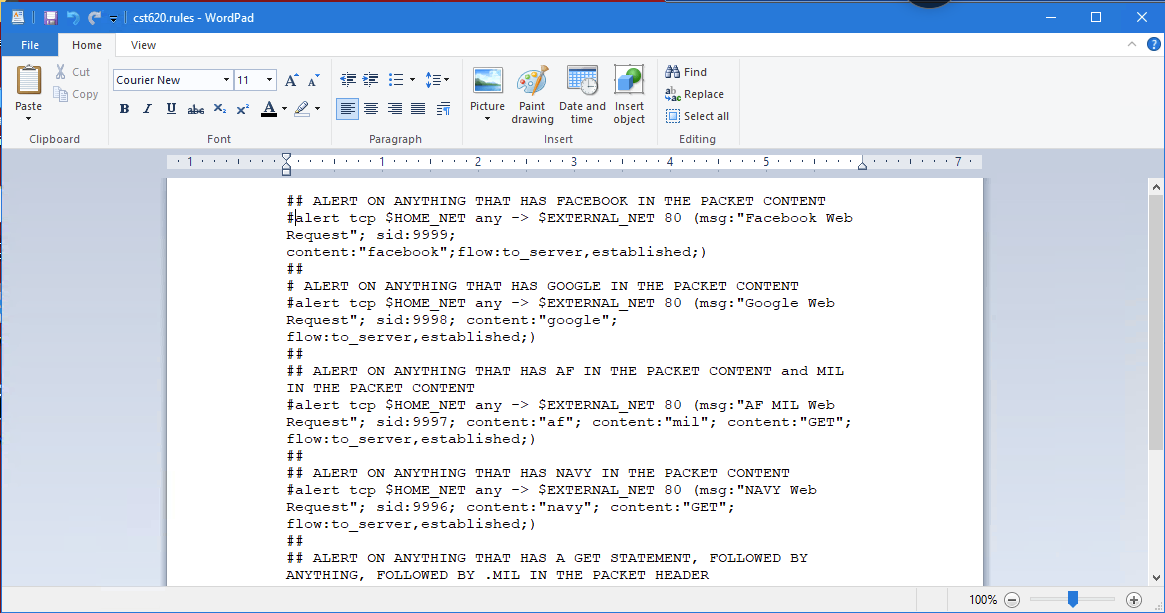


Figure 16: Uncommenting first rule of ruleset

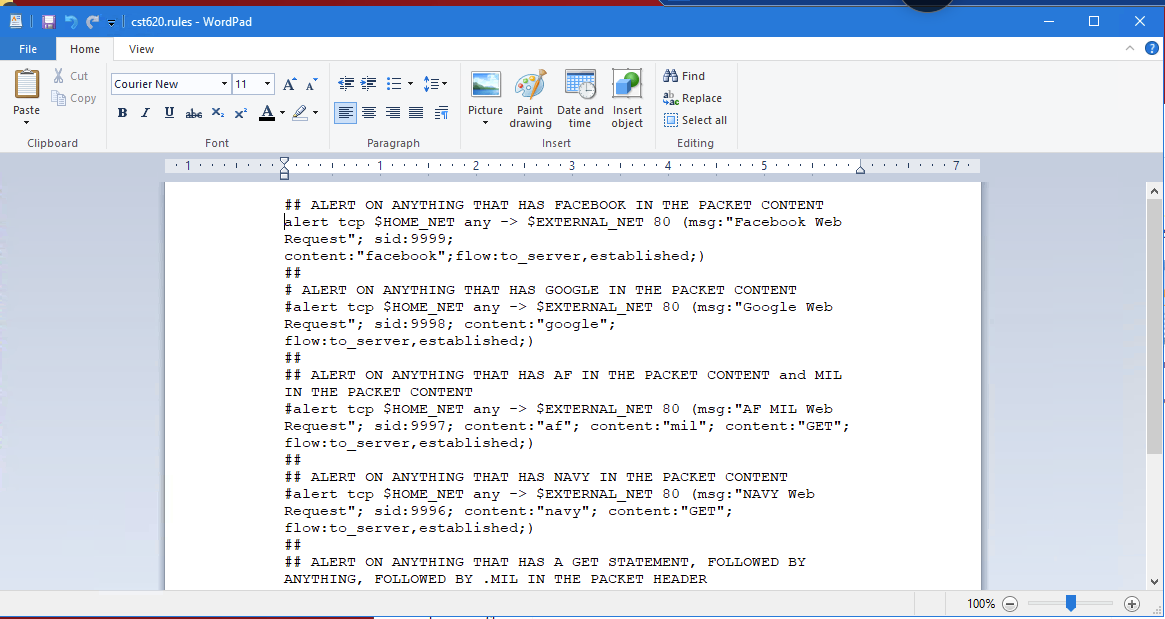


Figure 17: Log after rule 1 is ran through Snort

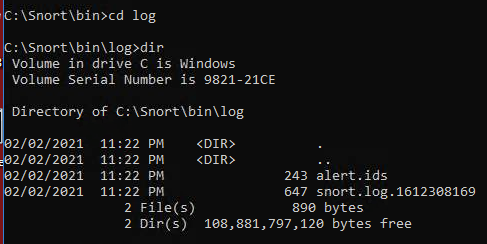


Figure 19: Open new alert.ids file in Wordpad

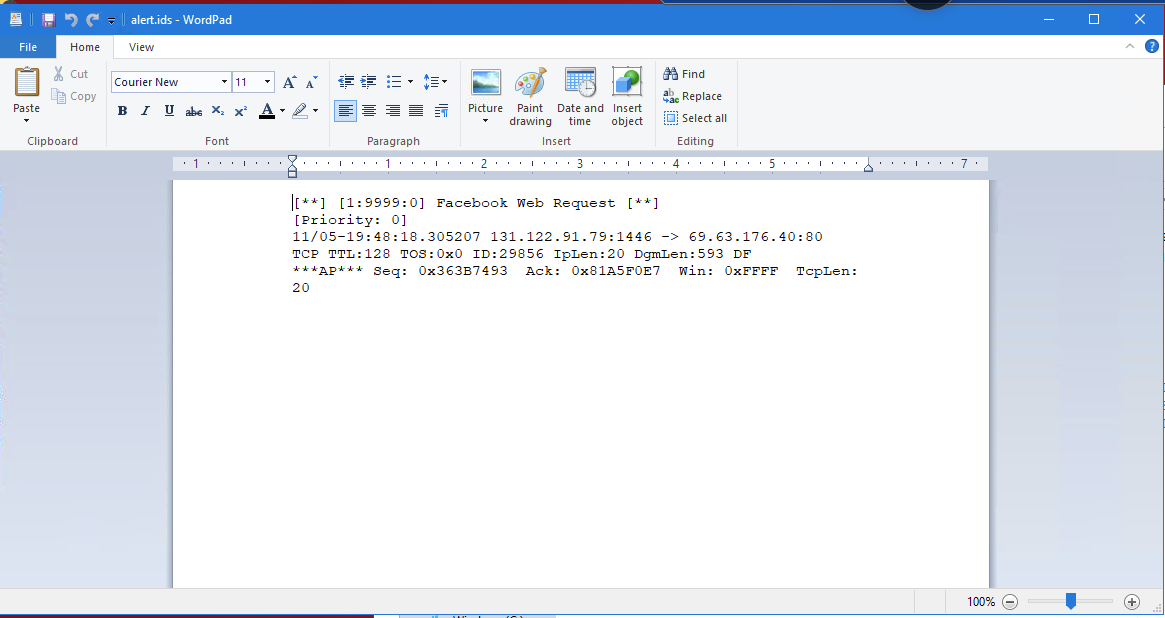


Figure 20: Renaming alert.ids file “Alert 1”

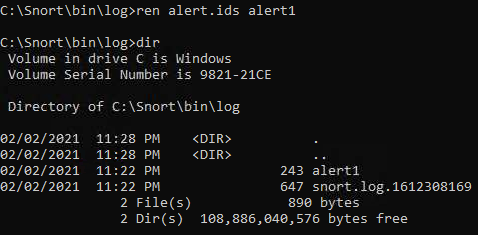


Figure 21: Turning Off Rule 1 and activating rule 2

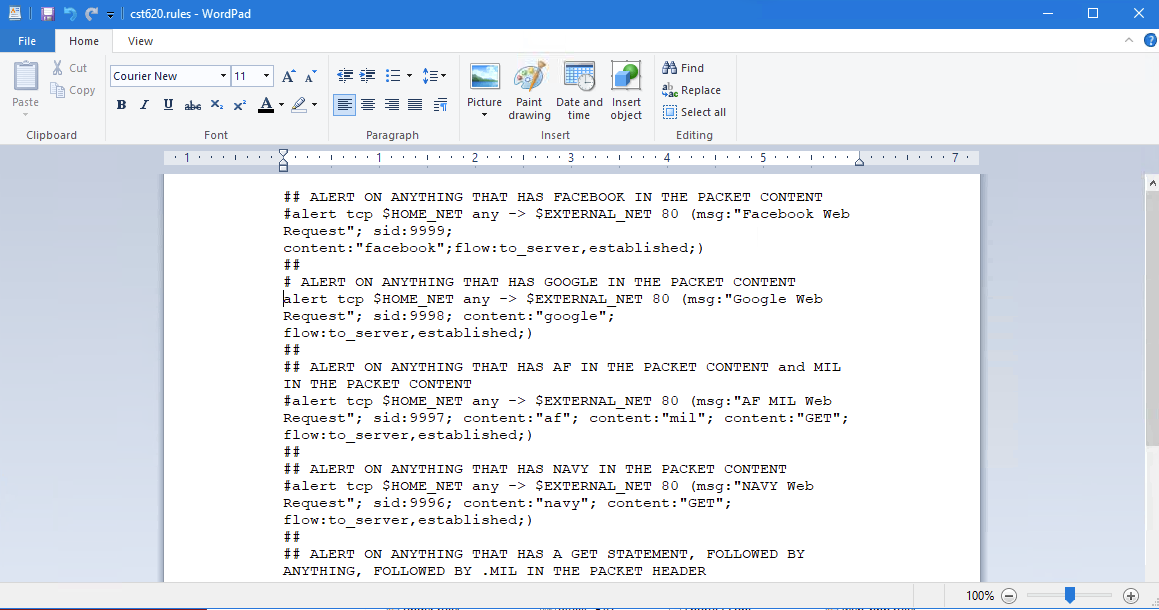
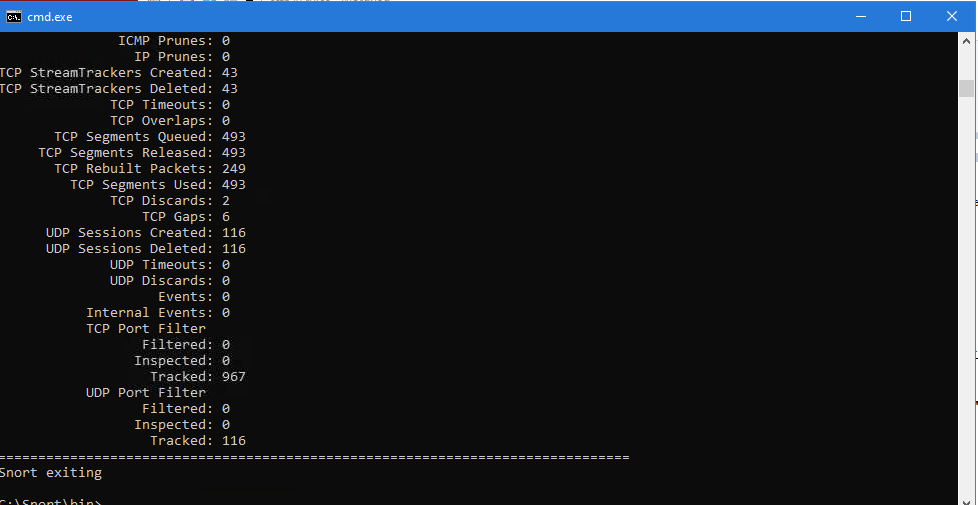


Figure 22: Rule 2 ran through Snort



I ran the same process thru all six rules in the cst620.rules file, and then I was ready to attempt the Combined Snort Run.

Figure 23: This is the log after the combined Snort run

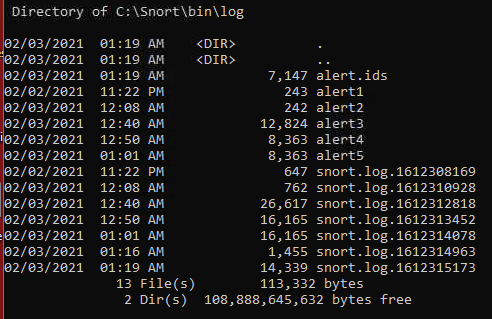
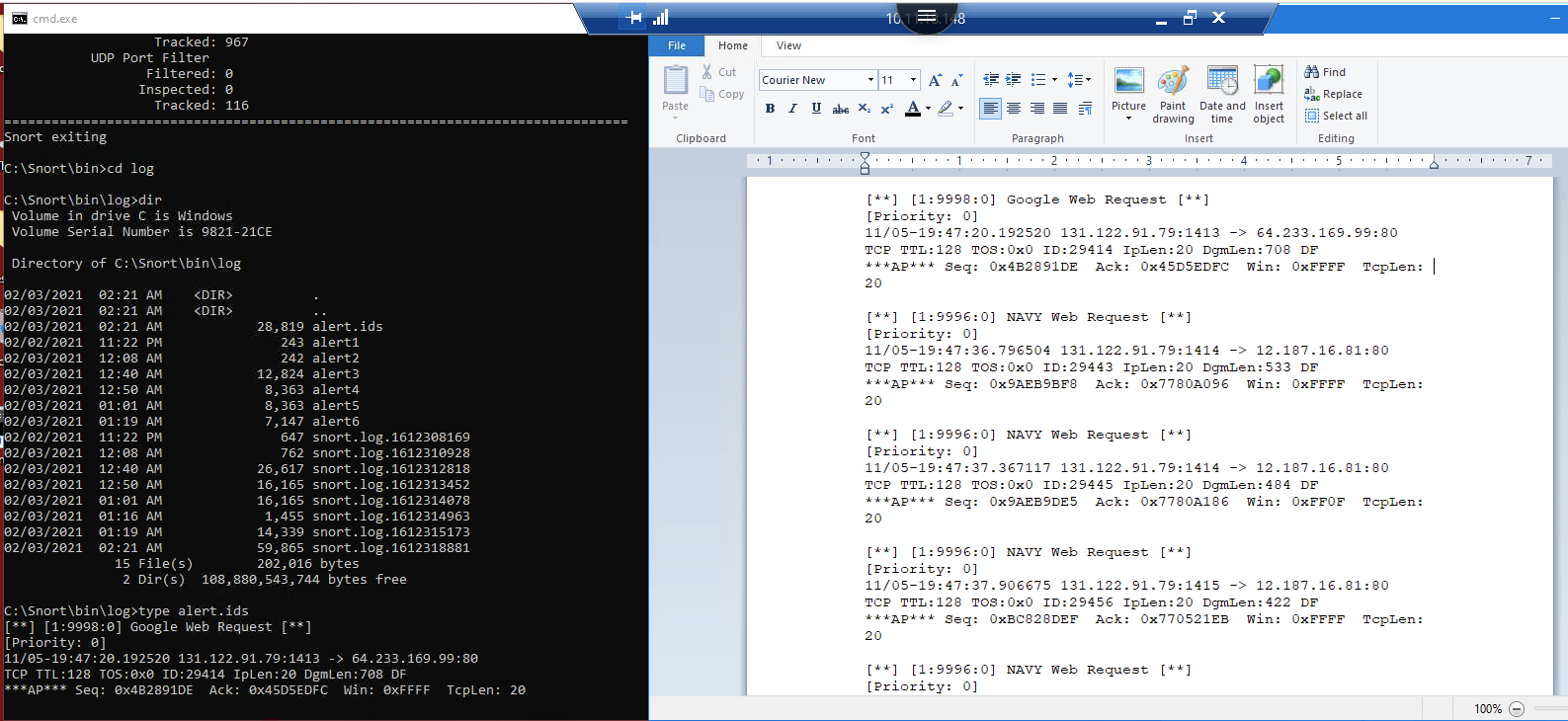


Figure 24: This is the side-by-side of my Combined Snort test run result with the alert.ids file opened in Wordpad.



**Task 2:** Using WireShark, we examined network packets from previously captured traffic.

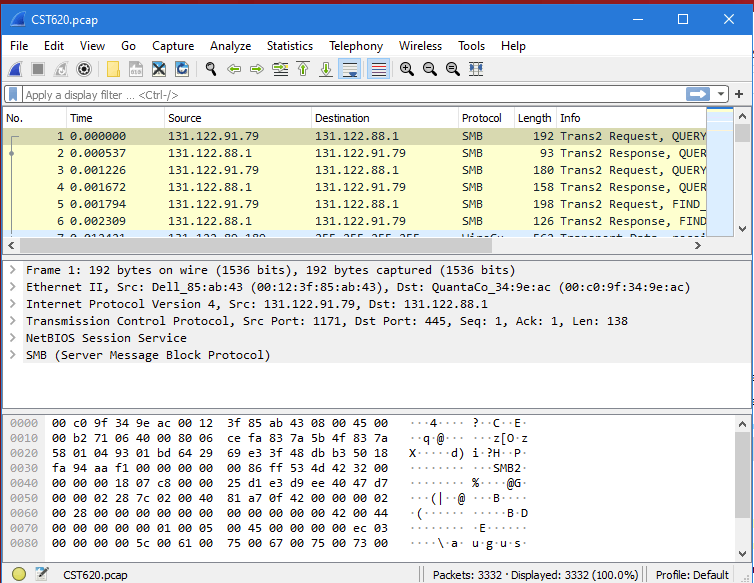
Figure 25: Opened cst620.pcap in wireshark. 

Figure 26: Opening Protocol Hierarchy

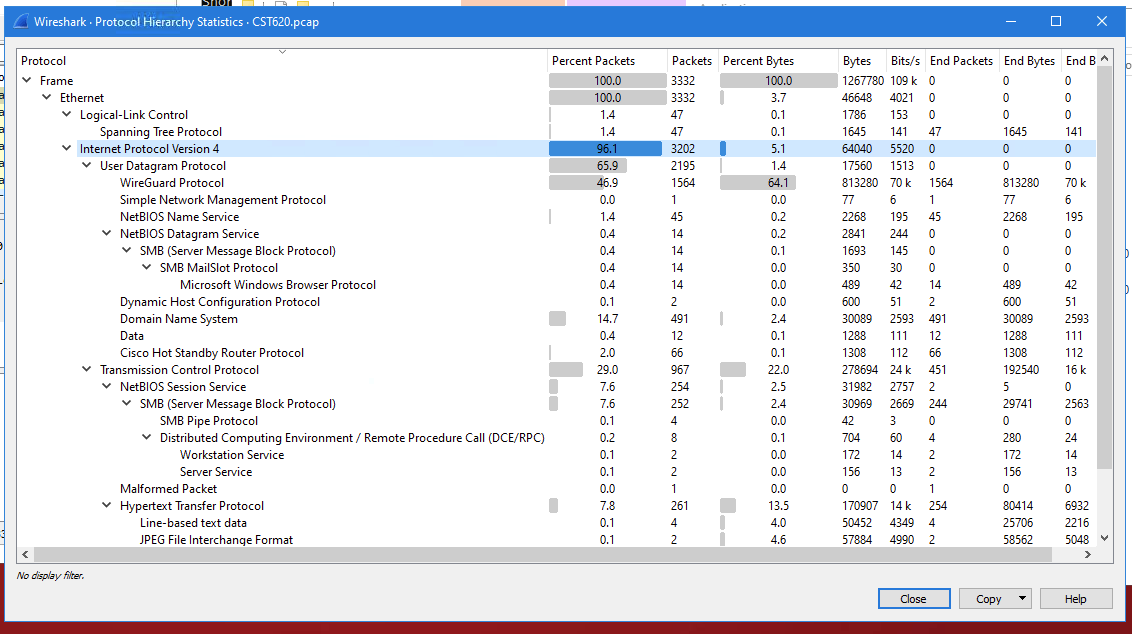
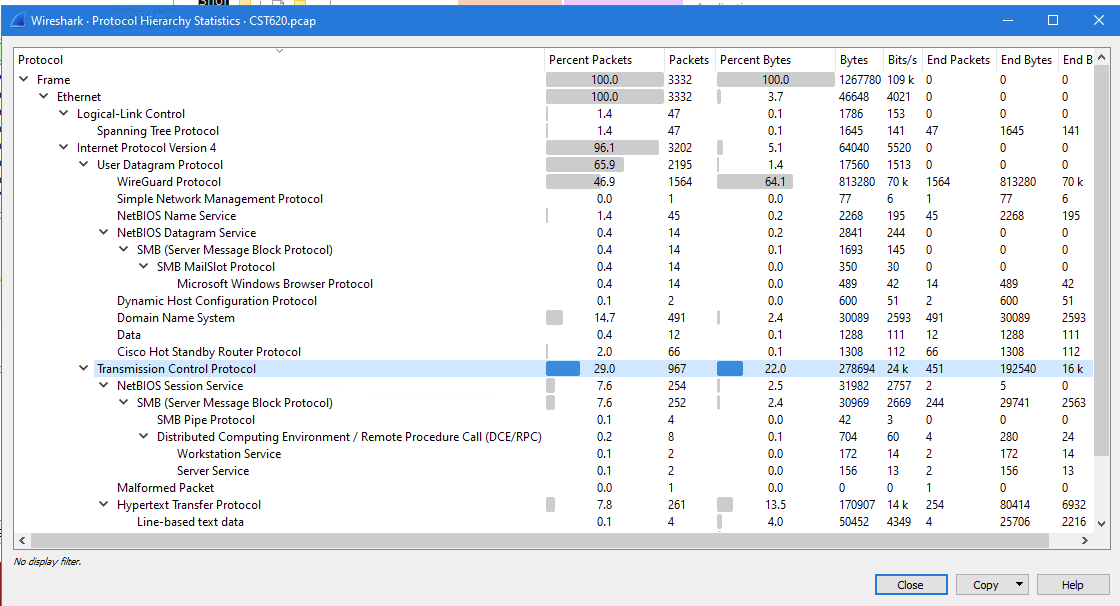


Figure 27: Filtering Viewing Panel to see TCP captured packets



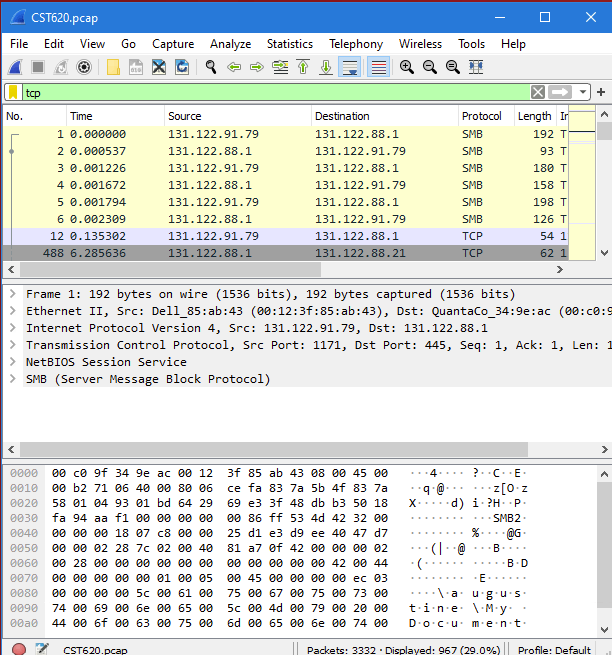
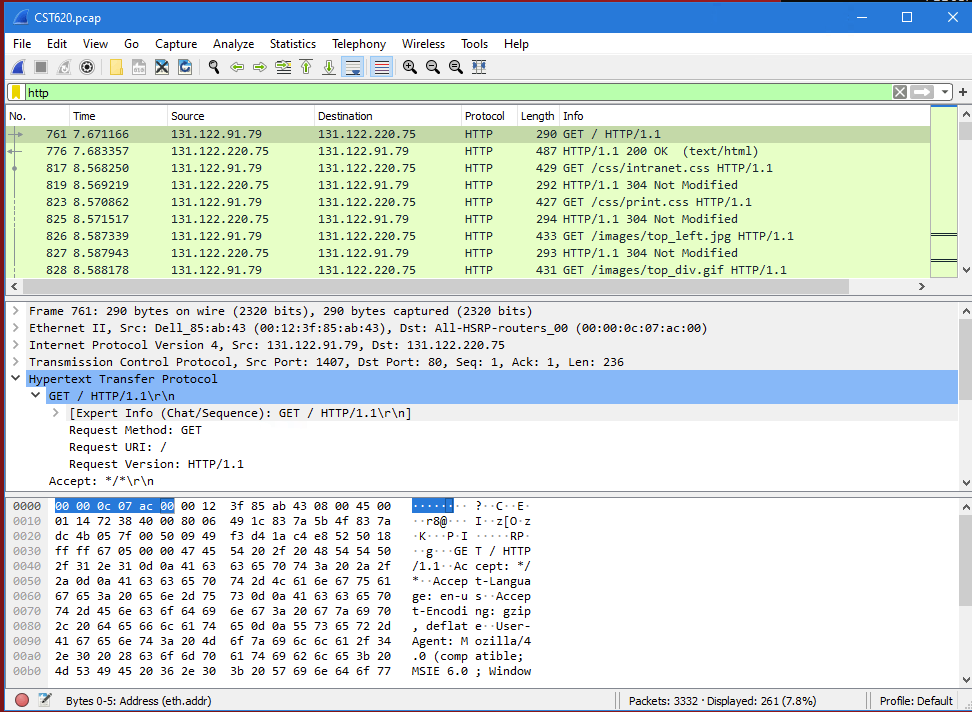


Figure 28: Viewing HTTP captured packets through filter



**Questions and Answers**

1. When Running Snort IDS, why might there be no alerts?

*The ruleset being used was not producing any alerts because each rule had been turned off.*

1. If you only went to a few websites, why are there so many alerts?

*This could be due to the website creating an alert each time you visit or revisiting the same website over and over.*

1. What are the advantages of logging more information into the alerts file?

*This creates a stronger security tool and allows Snort to learn from the mistakes it makes. Going into great detail describing the mistakes makes it easier for Snort to not make those mistakes again.*

1. What are the disadvantages of logging more information into the alerts file?

*A potential drawback of logging more information would be potentially overloading the system, and this is akin to leaving a blueprint of our strategy on the file. If an attacker were to see these files, there is a grave risk of exposure.*

1. What are the advantages of using rulesets from the Snort Website?

*The rulesets from Snort’s website are premade and have been ran through a battery of tests. Using these rulesets provides a lesser risk of attack versus creating your own rulesets that have not been tested.*

1. Describe at least one type of rule set you would want to add to a high-level security network and why.

*I would like to add the back-door rule to a high-level network. The Back-door rule send alerts whenever someone is trying to bypass authentication.*

1. If malicious actors got into your network with read/write access to your IDS log or rule set, how could they use that information to their advantage?

*Malicious actors could remove traces of their activity from the log of the IDS, they could also modify the IDS to allow malicious activity to pass.*

1. An intrusion prevention system can either wait until it has all the information it needs or can allow packets through based on statistics (guessed or previously known facts). What are the advantages and disadvantages of each approach?

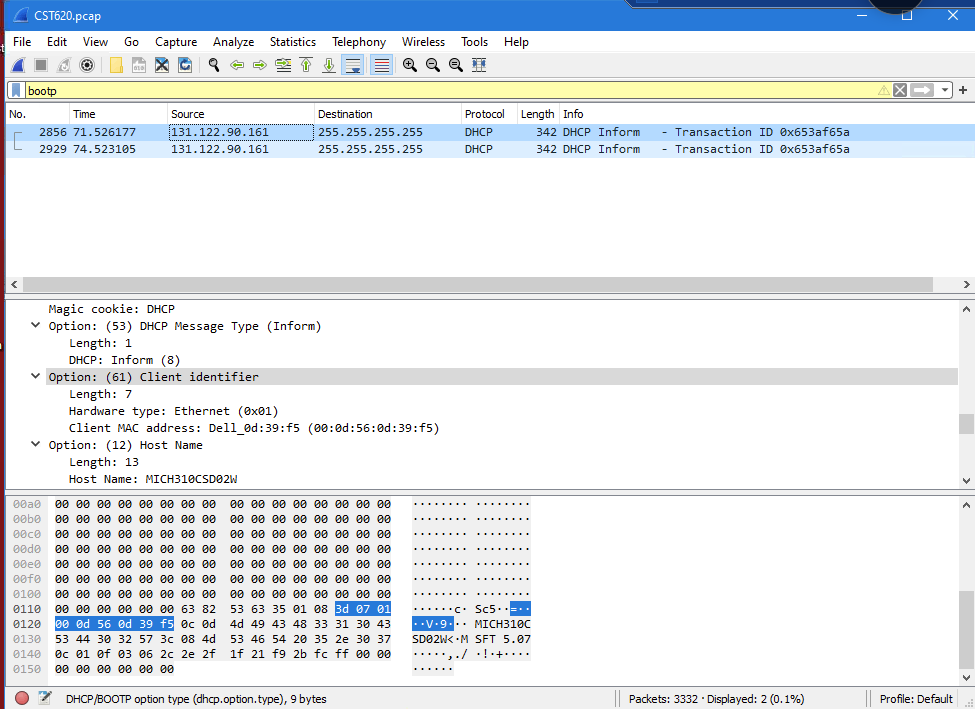
*If the user waits until the IPS has all the information that it needs, the chance of preventing future threats is diminished, but there is also a risk of decreasing the speed at which the IPS moves.*

*If the IPS runs on the minimal amount of information, the IPS moves quickly, but there is a lower chance of the IPS actually detecting the threats.*

1. Provide examples of IP addresses, hostnames, and mac addresses based on your analysis of the .pcap files in Wireshark.

IP Addresses, Hostnames, and MAC Addresses can be found using the Boot Parameter Filter “Bootp” in Wireshark. By viewing the Host name and Client Identifier options, the information is available as seen in Figure 29.

Figure 29:



1. What did you find particularly useful about this lab (please be specific)? What if anything was difficult to follow? What would you change to make it better?

*Learning how to work within IDS systems like Snort and Wireshark provided me with invaluable experience I can use later on. I thought that the end of the Snort exercise it was a little challenging to keep up with as I thought the examples and the process I was using would be exactly the same. In spite of that, I would not change the exercise as this will be useful to learn and hopefully master one day.*