Practical Test 1: Incident Response Report

By

Buwaneka Hettiarachchi

SID 104376165

SPR600

Preface

This is the second phase of the Practical Test, in this report, we are updating all the necessary information through a given link by our professor. This lab has many information on the specific steps taken in the threat hunting process and give a more detailed in-depth feeling idea on the finding the necessary IP addresses related to the attack and the information of the Malware.

Table of Contents

Chapter 1: Executive Summary

The given pcap for this Practical test included a Wireshark pcap file, within the pcap file there are several information that the user will be able to extract from and get an idea of the type of malware that caused this breach and what IP addresses were affected from the breach. First, we need to look into the malware that cause the attack. By looking through the http request filter from Wireshark, we were able to identify a certain host that doesn't have a host name, but a simple IP address, the IP address gives information of a certain file known as the (coreupdater.exe), after exporting the file, and searching it through virus total, you'll be able to see that the file is indeed a Malware. There are two distinct IP addresses that were affected from the malware itself. These IP addresses are (10.42.85.10) and (10.42.85.115). The Hostnames of both the addresses are CITADEL-DC01 for 10.42.85.10 and DESKTOP-SDN1RPT for the IP address 10.42.85.115. while looking into the user accounts that were affected from the breach, I was able to find the user account that was affiliated to the IP address 10.42.85.115, the user account name is mortysmith. The attack took place at two distinct times, the attack was first affected to the IP address 10.42.85.10 at the time period of (22:19) on the 18th of September 2020. While the second attack took place at (12:23) on the 19th of September 2020, and it affected the IP address 10.42.85.115. The breach is a malware breach and while looking into the severity of the malware file, it was shown to be highly severe. The Malware Family is a Trojan Malware family, while the Malware took place on 2020 September 18. Details on how they were extracted are further enhanced in chapter 2 of this incident report.

Chapter 2: Details

To find the details of the victim machine, I mainly used tools such as Wireshark and snort to discover their IP addresses, using snort I started to check information on a specific range of IP addresses, since we do have an understanding that the machines range within 10.42 network, I used a command to get information on the machine affected.

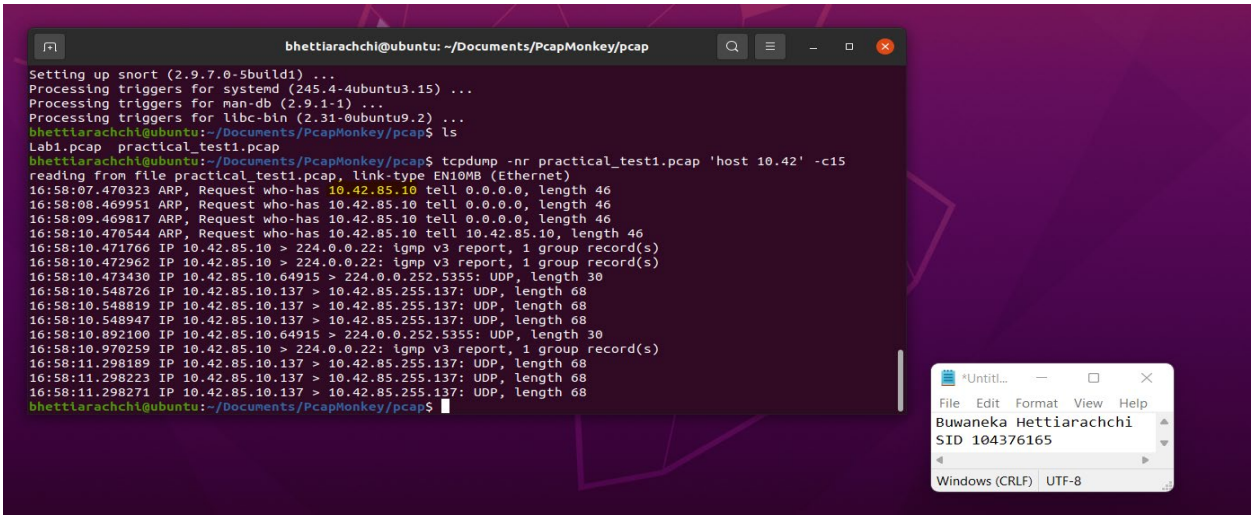

Figure 1: Possible information on the victim machine

The above screenshot gives us a hint that the possible IP address that may have been affected from the malware attack. Next, we will be using a command from snort to discover the time range of the whole activity.

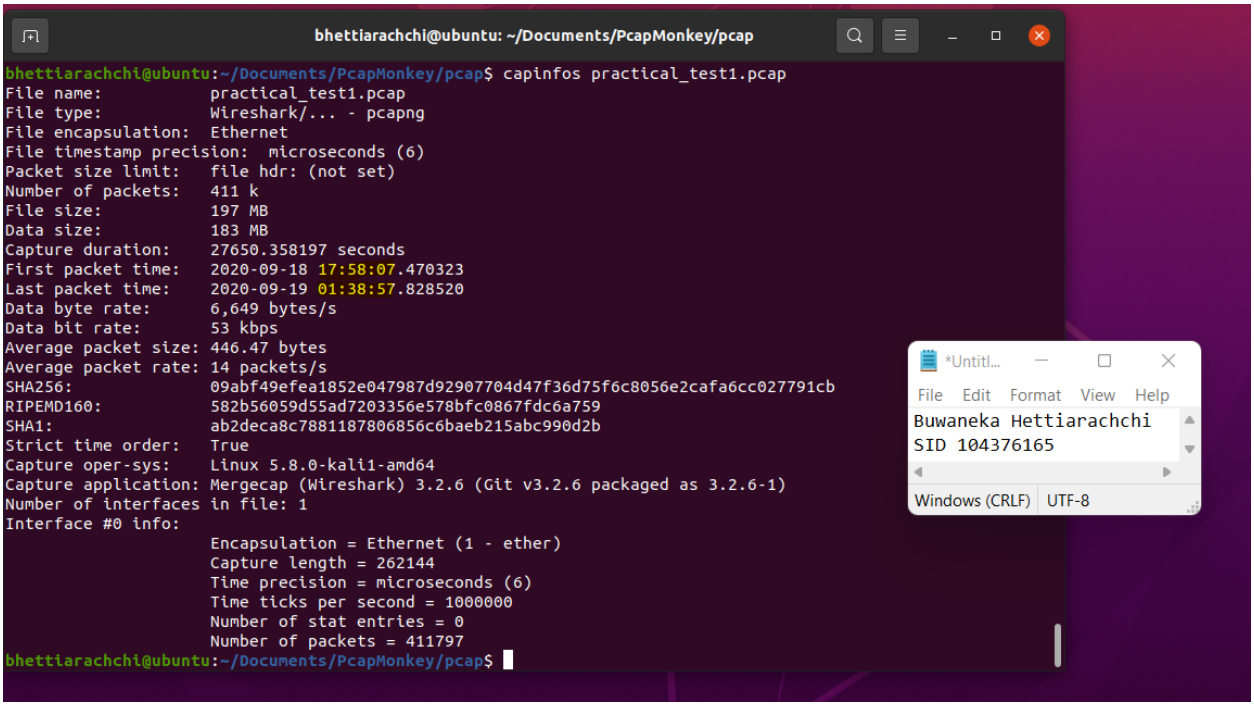

Figure 2: Figure showing information on the Time range of the packets

As you can see the time range of the packets indicate that the whole attack took place in a span of 7 hours where they started at 5:58 pm on the 18th of September 2020 and then it stretched till 1:38 am on 19th of September 2020. To understand and see if the above IP address is the actual Ip address related to the attack, I performed another command in snort which was (sudo snort -c /etc/snort/snort.conf -r practical_test1.pcap -q -K none -A console | tee snort.out). This command proved that it was indeed 10.42.85.10 is the vicim IP address

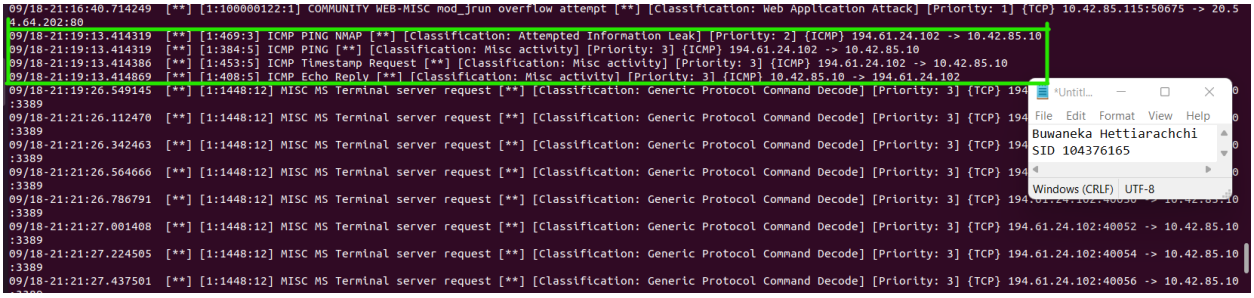

Figure 3: Figure showing, possible information leak happening between the Victim and the attacker

The above screenshot shows information that a possible data leak has occurred during 21:19 on September 18th, 2020. This further shows that the IP address of the victim is indeed 10.42.85.10.

But if we scroll down on the output file, we are able to witness that there has been another data leak and if we look into it, the IP address is 10.42.85.115.

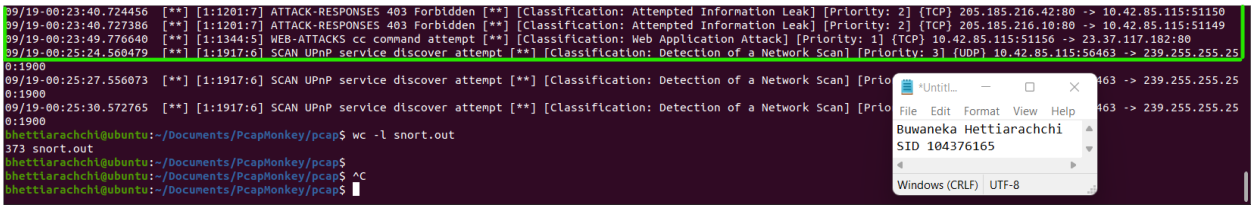

Figure 4: Showing another data leak on the second victim

So, to find additional information on both the machines, I opened Wireshark and started to look in the Information such as IP address Information, MAC addresses on both the victim machines.

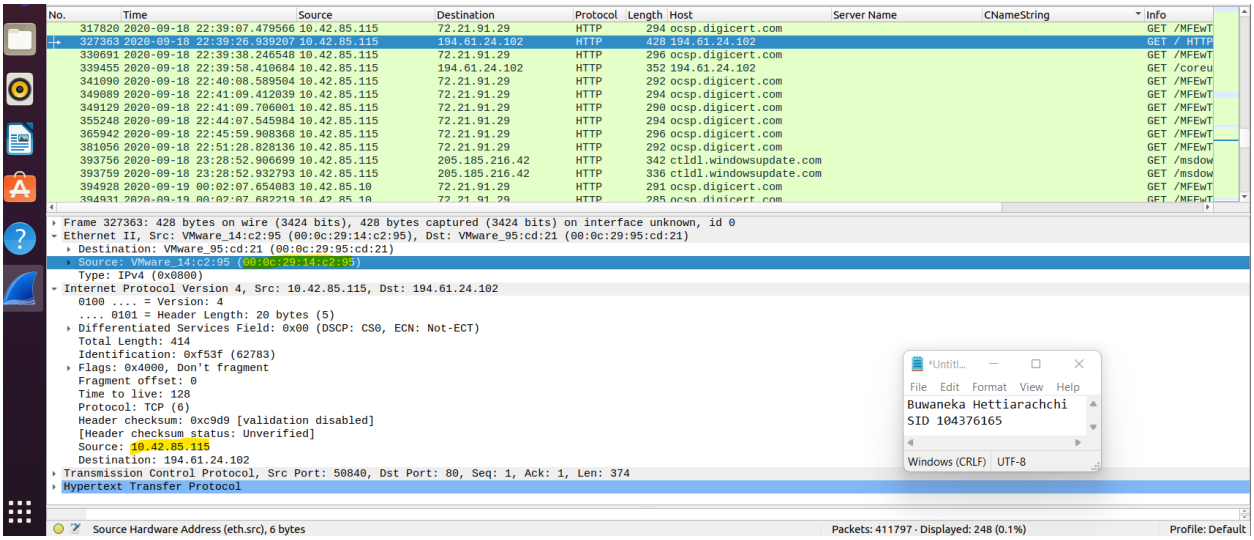

Figure 5: Indicates the IP address and the MAC address of the first victim machine

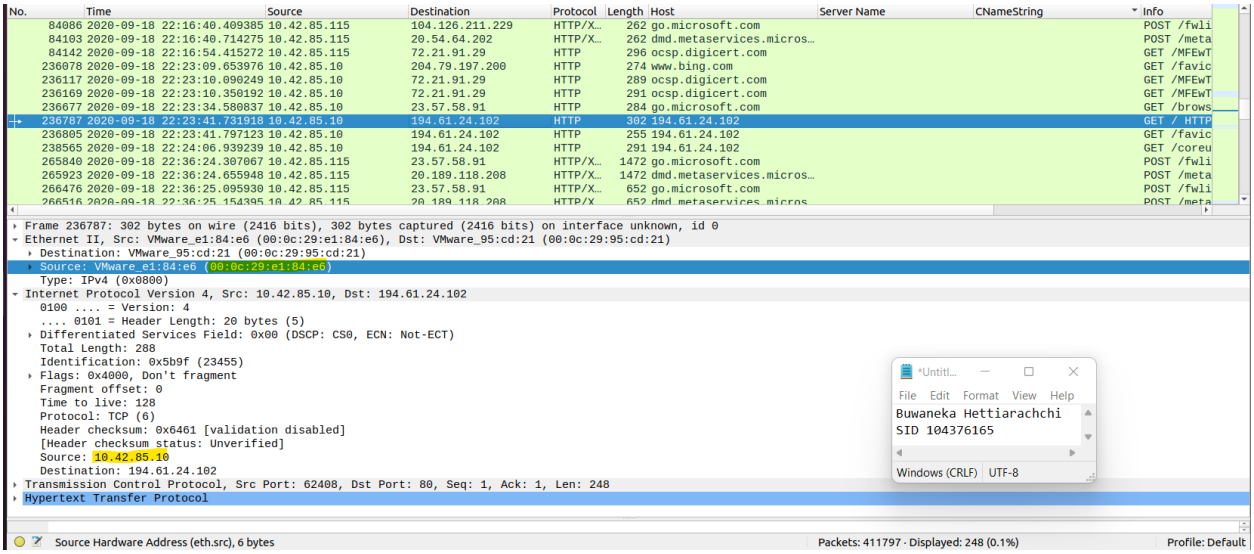

Figure 6: The Information of IP address and MAC addresses of the second victim

The IP address of the victim was 10.42.85.115 and the MAC address was 00:0c:29:14:c2:95. The IP address of the main second victim machine is 10.42.85.10 and the MAC address of it is 00:0c:29:e1:84:e6. Not much to describe about the two victim IP addresses, but the only commonality between them is that both these machines lie under the same network. To find the specified hostname, we need to look into two different areas of Wireshark, If we start looking into the nbns (the NetBIOS Name Service) filter, we would be able to see the information of the Hostnames of the Two machines.

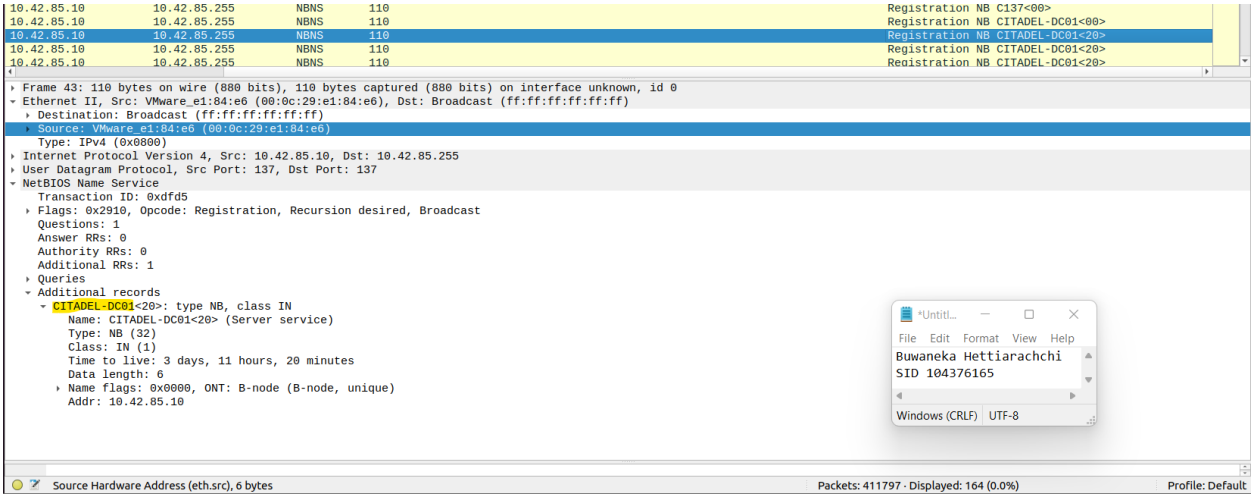

Figure 7: Hostname of IP 10.42.85.10 highlighted in yellow

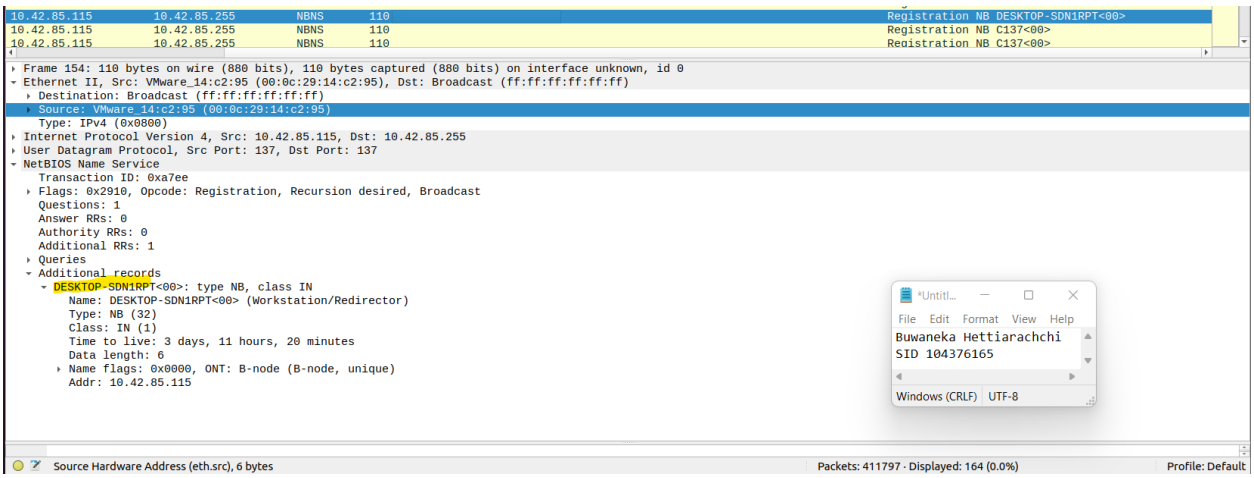

Figure 8: The highlighted text shows the Hostname of the IP address 10.42.85.115

Figure 3 shows the hostname that was associated with the IP address 10.42.85.10, the hostname is CITADEL-DCO1. Figure 4 shows the hostname of the IP address 10.42.85.115 with the hostname DESKTOP-SDN1RPT. To find the User account names, you are supposed to look into the Kerberos names string filter from the Wireshark, this filter would give the results of the User Account Name.

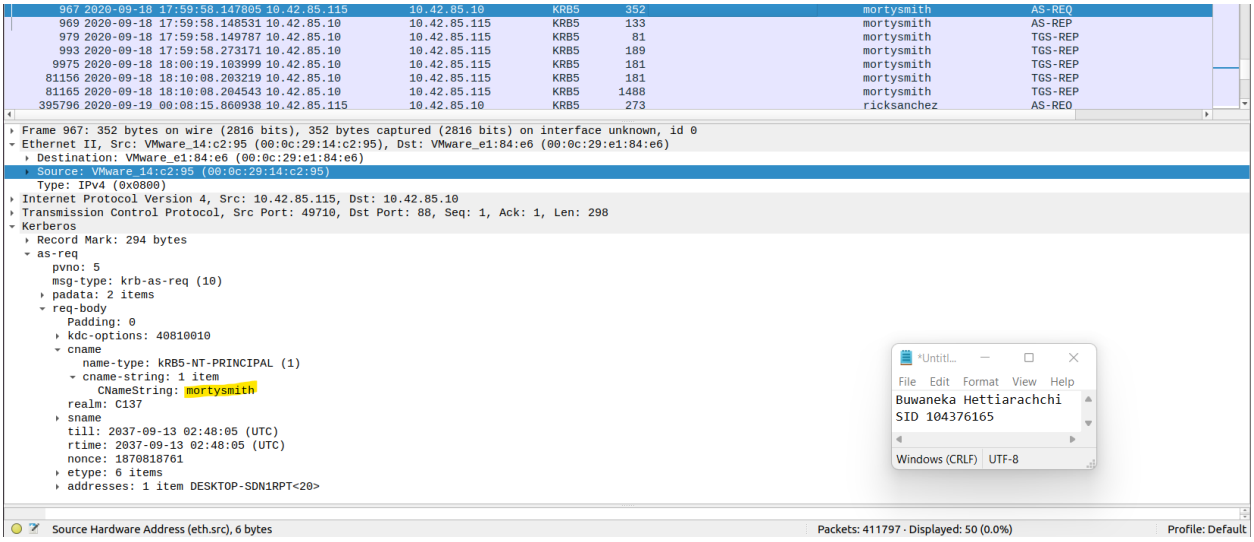

Figure 9: User Account Name of the Infected machine

The Victim machine's user account is called mortysmith and this user account is affiliated with the Machine (10.42.85.115), We were able to understand it using the hostname shown in the packet details. The most important detail from the user account information is that the user account changes from mortysmith to ricksanchez, which is shown in the packet information below.

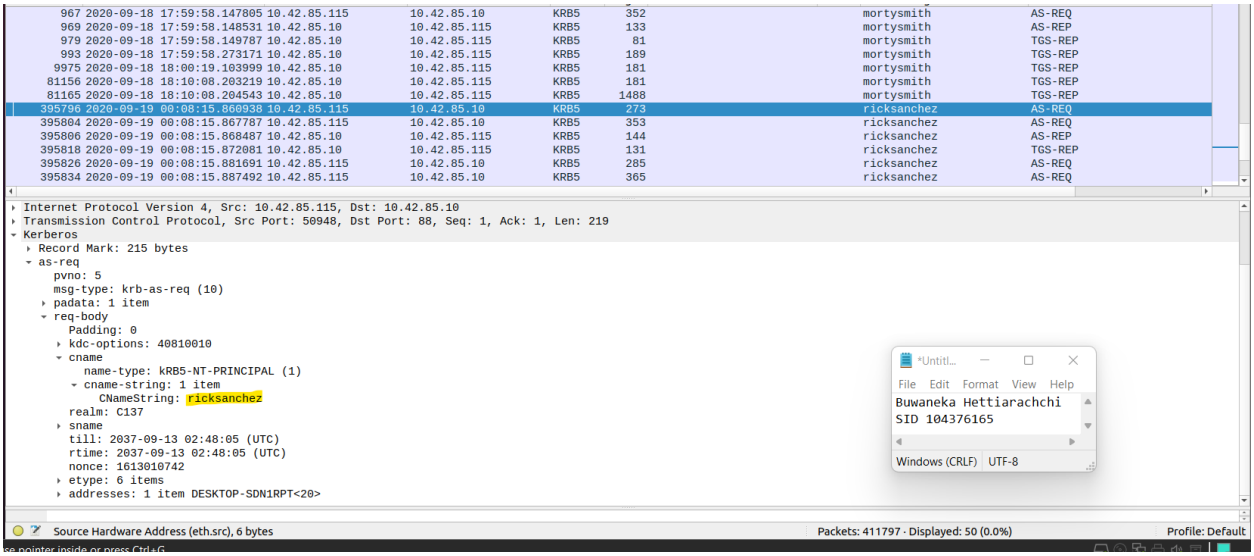

Figure 10: The changed User account

Again, we can conclude that the machine is (10.42.85.115), the information we can see is that it has been changed from mortysmith to ricksanchez in a span of hours, because if you see the date, the user account has been changed to ricksanchez on the 19th of September 2020, this means that the attacker may have gain access into the system and changed the information.

More details on the communication between the Victim and the suspicious machine have been shown when the both the machines performed and ICMP packet exchange shown in the Figure Below.

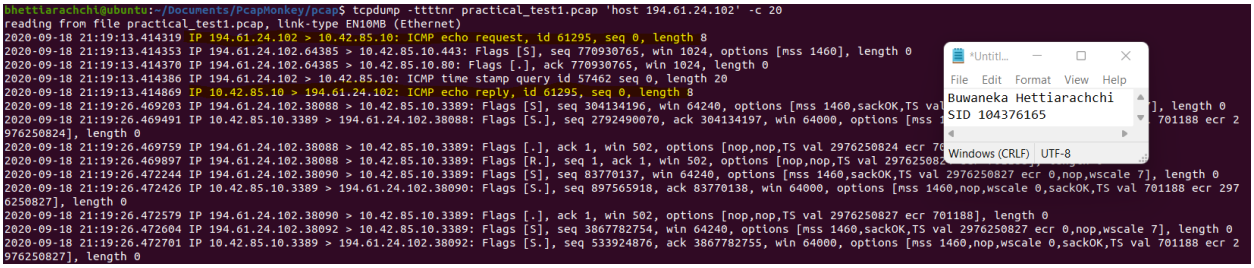

Figure 11: ICMP packet distribution between the Two Ips

More details on the 192.61.24.102 address will be enhanced in the next chapter when I will describe about the Indicators of Compromise.

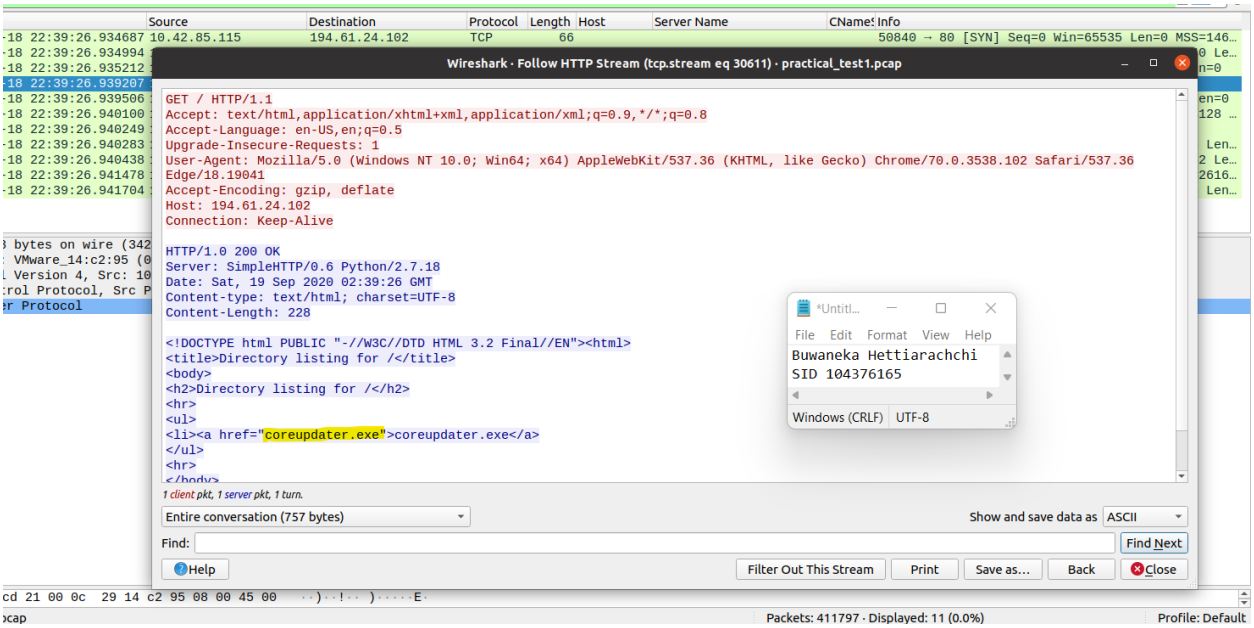

Figure 12: Information on leading to the malware

When we look into the Export file, we were able to witness that the coreupdate.exe file had affected two IP addresses, these IP addresses are the victim addresses we discussed earlier.

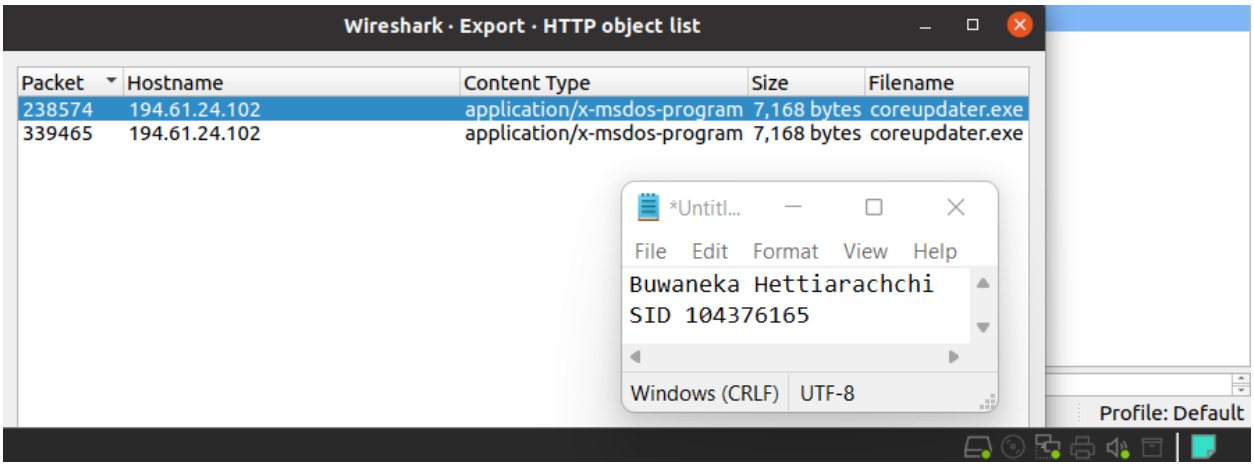

Figure 13: HTTP Export of the Coreupdate.exe file

Then, I proceed to take the md5 hash of the coreupdate.exe file and, proceed to look into the virus total website and the information below is the output I got.

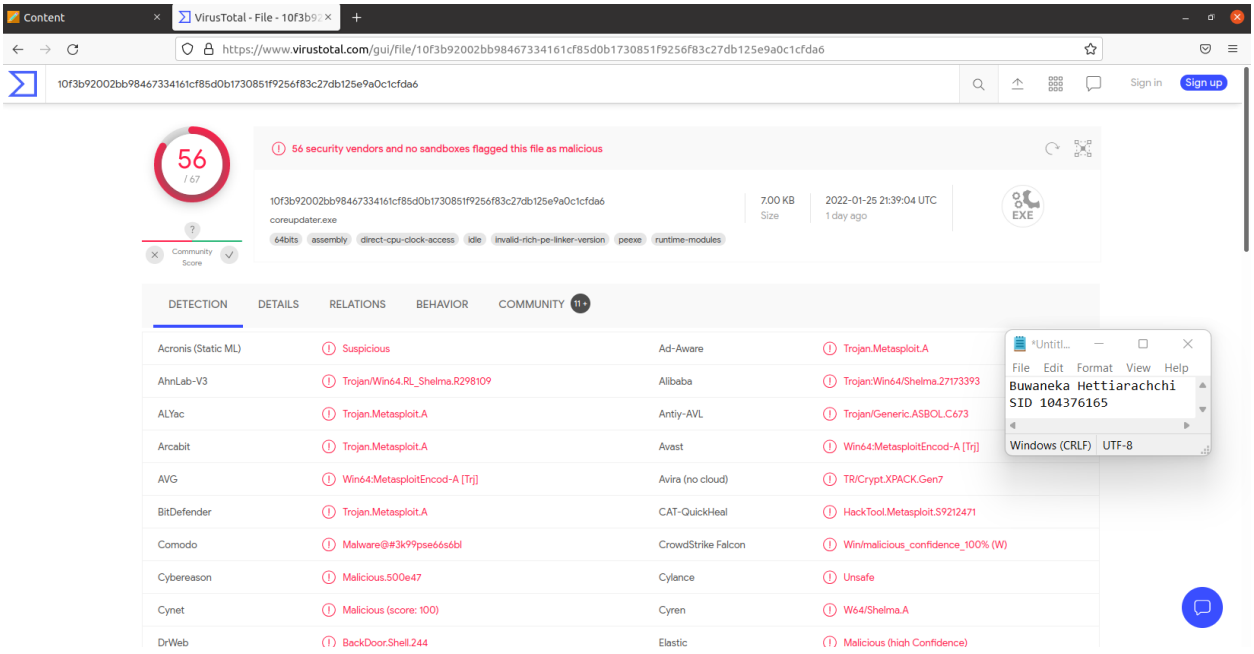

Figure 14: The output from virus total

As you can see from the output from virus total, we can come to a conclusion that the file is a malware and as shown in the above figure, the malware itself has gotten flagged 56 times by different security vendors. By doing some research on the file, we were able to extract information such as, that the file itself is an executable file and in some cases this executable file can damage Windows machines here it can be executed by putting in arbitrary codes in it. The file is normally 7168 bytes in size.

Chapter 3: IOC (Indicators Of Compromise)

The IP addresses that are related throughout the whole breach are 10.42.85.10, 10.42.85.115, and 194.61.24.102. When we look into the details of the Attacker IP (194.61.24.102) using Virus Total, we are able to get information such as the type of Attack related to it and how malicious is the IP address.

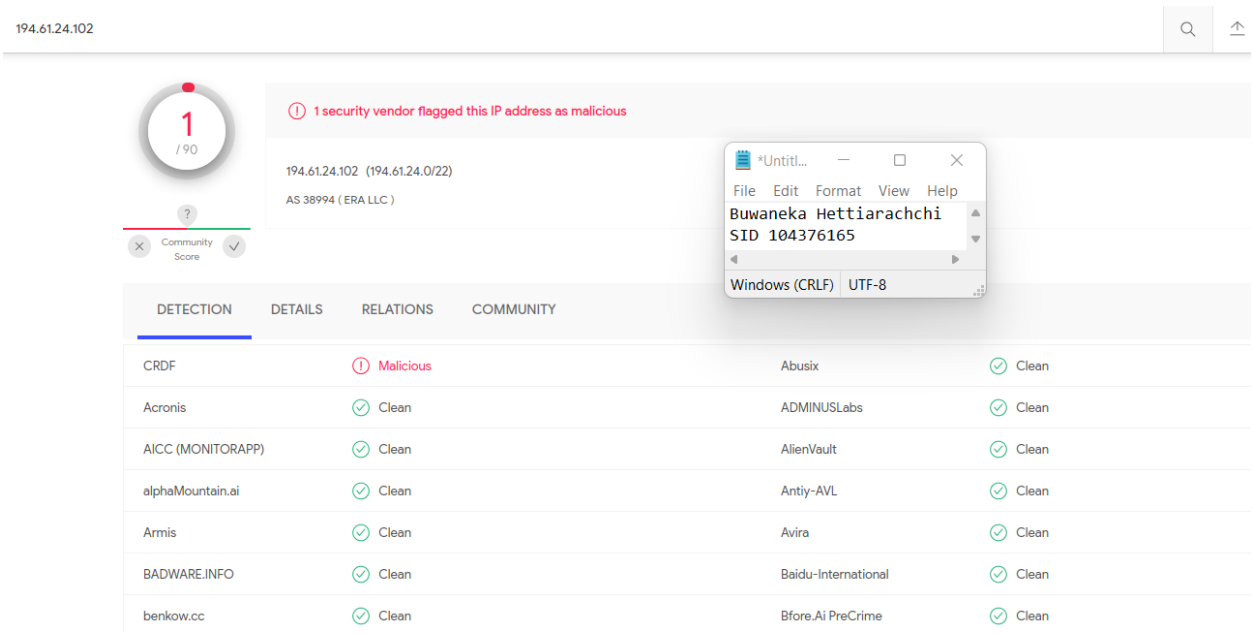

Figure 15: Virus Total information on the Attacker IP address

These were the biggest IP addresses that were involved in the whole breach, where the first two IP addresses were resulted to becoming the victim machines while the third machine acted more as the attacker machine.

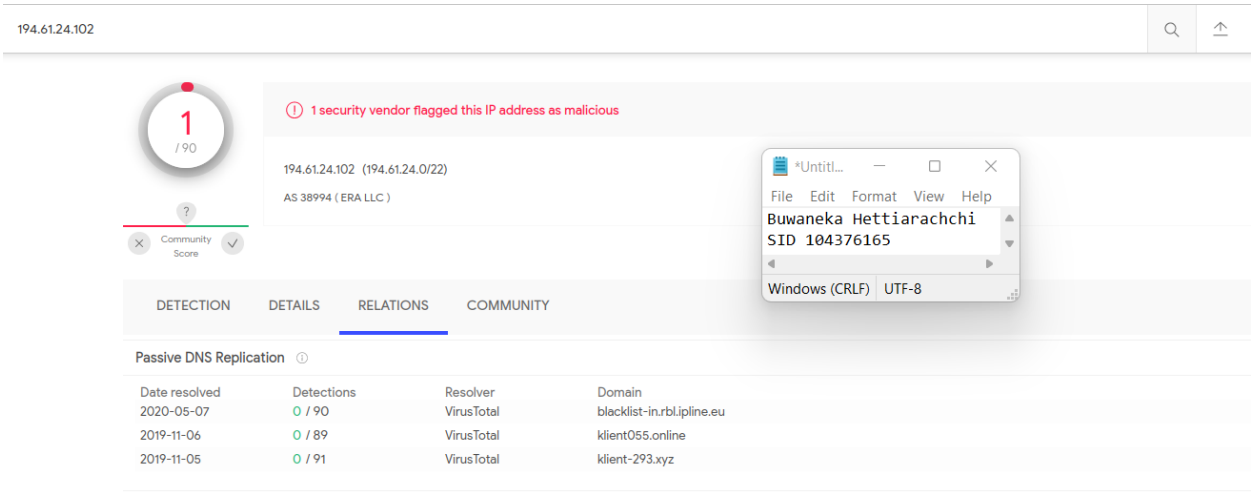

Figure 16: Domains related to the IP address

The URL associated with this malware type is http://194.61.24.102/coreupdater.exe. The figure below shows an examples of the URL.

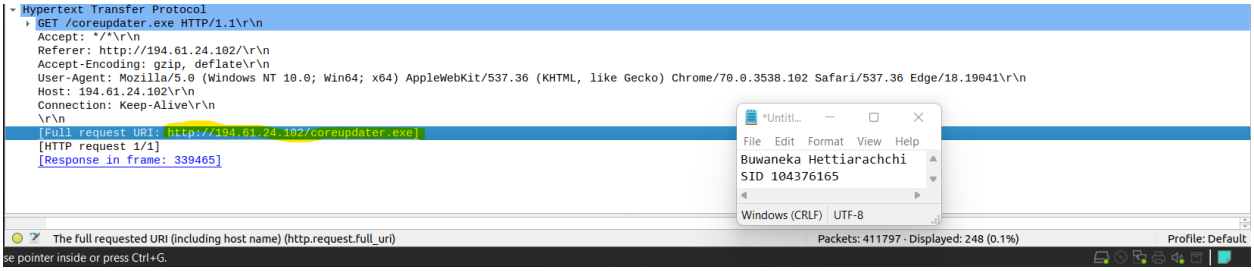

Figure 17: URL associated with the malware

To find the SHA256 hashes of the associated files, you have to save the coreupdate.exe file and then you need to get the sha256 command through the use of the terminal command, if the output is correct, it needs to be exactly the same as the Virus total output of the malware.

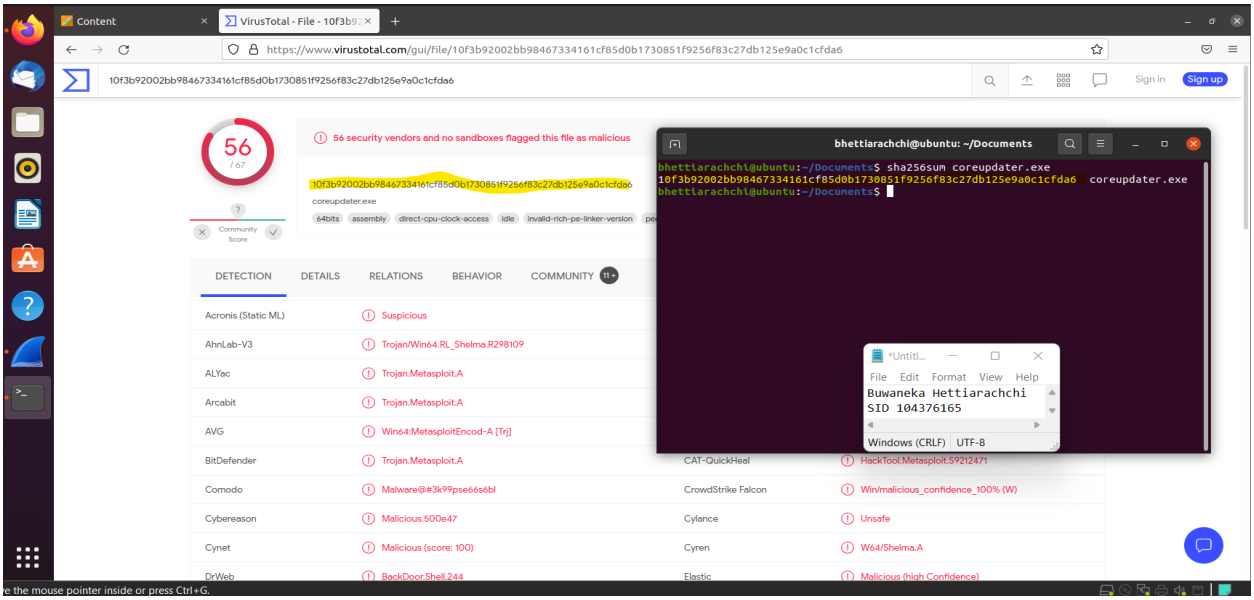

Figure 18: SHA256 hash of the malware file

Chapter 4: Threat Hunting

Methodologies

In the threat hunting process, one of the most important places we should be supposed to hunting is the specific communications between the IP addresses because attacks mainly happen between two IP addresses and normally, If we can look into some uncommon traffic in between two different machines, then that is one of the places we need to be threat hunting because, we can get an idea on what type of attack led into it. In this certain exercise, the biggest clue on performing a threat hunting process was at the location of the packet requesting the coreupdate.exe file. The tell-tale of a problem is when, we would have issues like the attacker gaining administrative privileges on the victim machine, which would then give him access to

change specific information such as User account information, this would cause damages to the system itself. To automate, threat hunting, we need to develop an advanced firewall system that is capable of detecting any unwanted activities in network environment, or we need to create a specific security device that needs to script through coding software such as Python or Java, and script to automate threat hunting and then create a log of all the events that has been taken in place. To explain the Problem, we would need to make adequate research on the problem itself and try to find certain methods of mitigating the problems, then to report the results, it is best if we perform visualizations.

Threat Hunting Demonstration and Implementation

Some of the Wireshark displays used in this exercise are shown below.

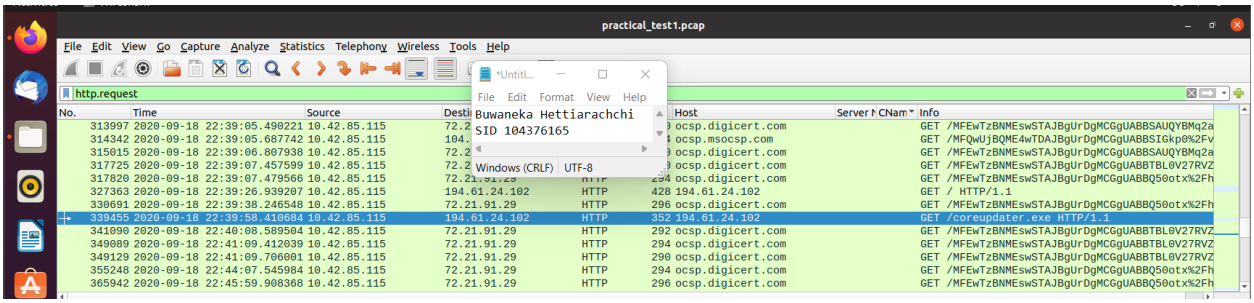

Figure 19: Http requests used to detect evidences of the malware

We used the http.request filter to get information such as evidences to the malware file, and we then use that evidence to go ahead on finding the packets related to the malware.

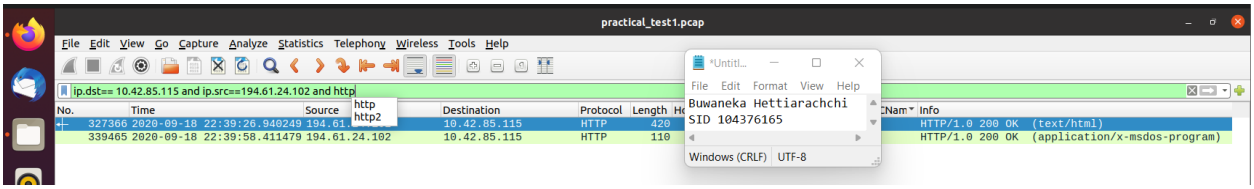

Figure 20: Grab the communication between the victim and the attacker

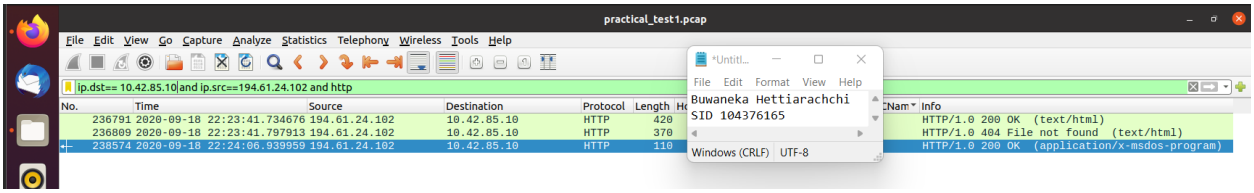

Figure 21: Grab the communication between the second victim and the attacker

The above two figures represent a filter that is used to gain an idea on when then the Ip addresses had contact with the IP address containing the malware. This filter gives an idea when the malware was first put into action.

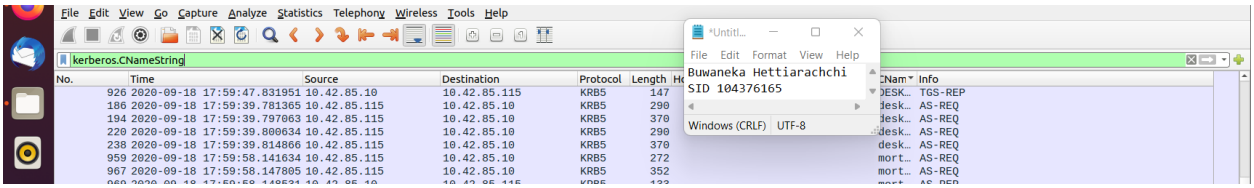

Figure 22: Command to filter the user account names

The above figure represents the filter that is used to filter out the user account names of the machines within the network.

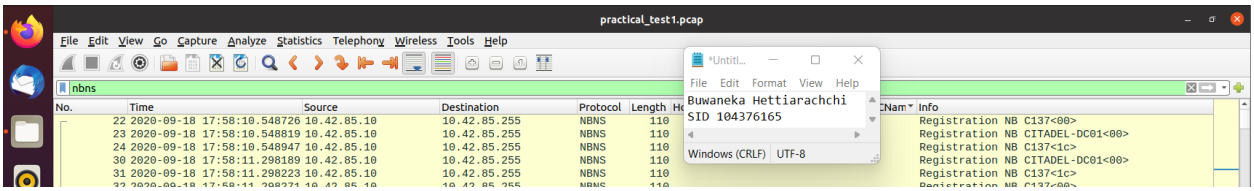

Figure 23: Used to filter the Hostnames of the IP addresses

The above command is used to filter the hostname of the IP addresses. The filter name is nbns or NetBIOS Name Service. The above filters are some of the filters used in this practical test and most of these filters were used to minimize and make it easier for people to look into what they want to look into.

After looking into the Filters, I put my focus into creating Dashboards using Elasticsearch module. To send in the pcap into the Elasticsearch dashboard, I had to use Pcapmonkey to ingest the Pcap into the Elasticsearch module.

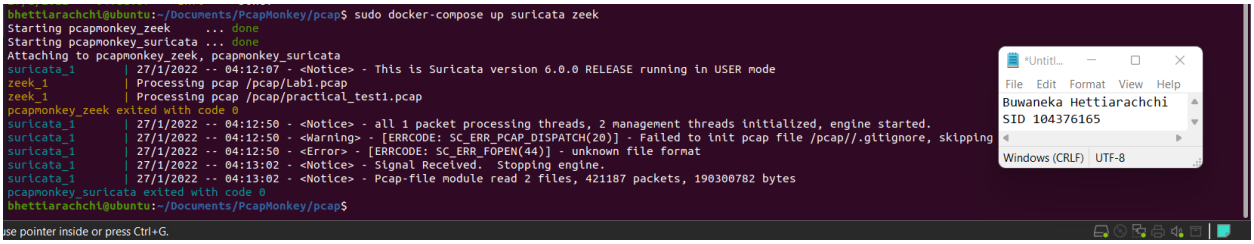

Figure 24: Ingesting the Pcap into the Elasticsearch dashboards

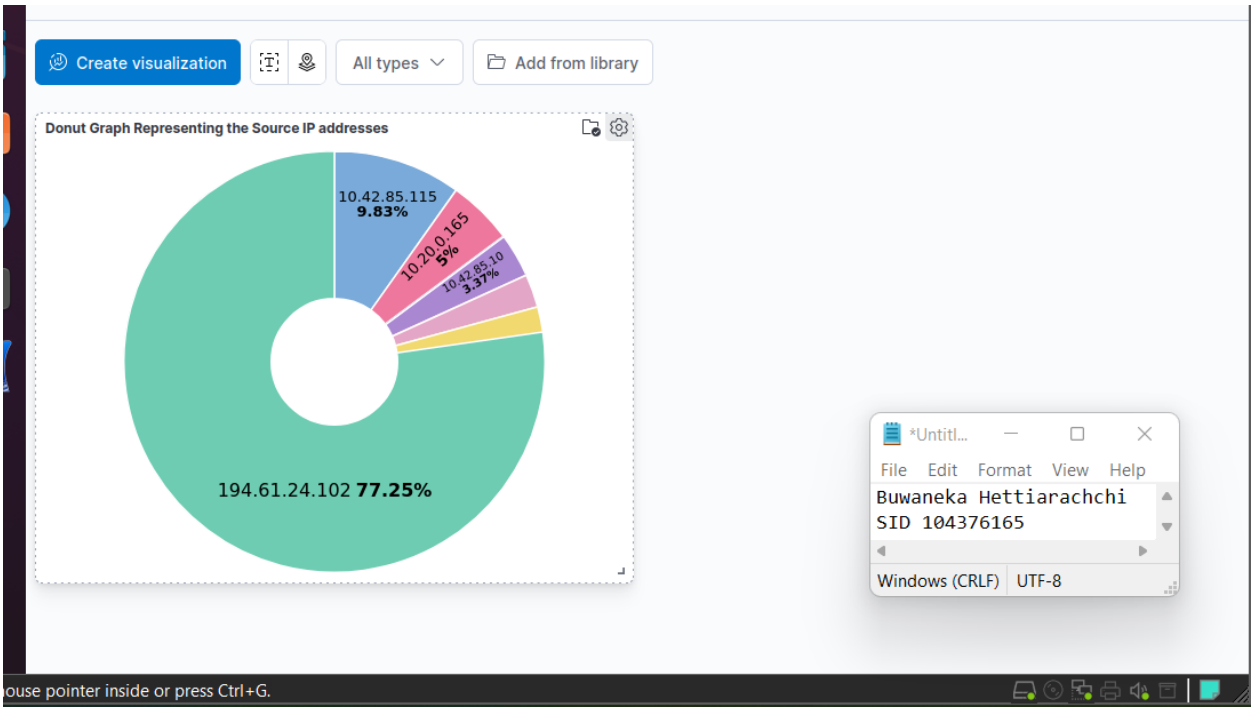

Figure 25: Elasticsearch Visual dashboard, showing the IP's with the most source packets

The above figure shows the donut graph of the IP addresses with the most source packets, and as we can see, the highest percentage of packets are coming from the IP address 194.62.24.102, which was the packet that was involved with the distribution of Malware.

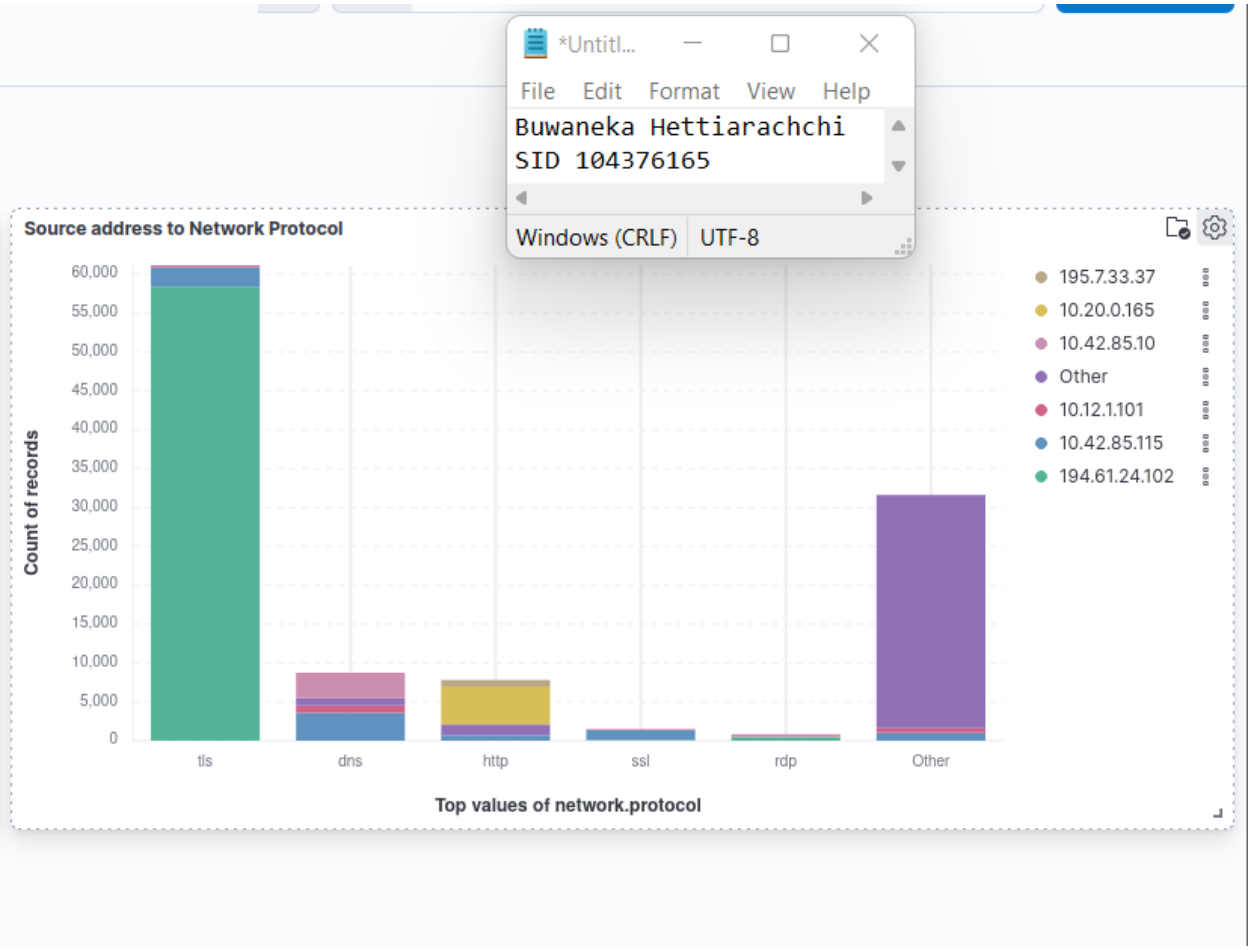

Figure 26: Visualization for the Elasticsearch dashboard

The above dashboard shows information such as the network protocols used throughout the pcap and what address used it the most. Again, as you can see the address 194.61.24.102 uses the mostly the TLS network protocol, which is also called the Transport Layer Protocol.

Limitations and considerations

One of the biggest limitations in this assignment is the fact that we are unable to see the severity of the malware, because we do not have a safe environment to run it, hence we have to look into research to identify the severity of it.

Chapter 5: Comparison with the older Report

In comparison to the Older report, there was no sense of understanding the IP addresses and how severe the IP addresses are. In this report, we were able to understand that the IP address 194.61.24.102 is a malicious IP address and we were able to identify some of its domains which are associated with the IP. Further, we were also able to explain how the victim IP addresses were able to communicate with the certain Attacking IP addresses and we were able to come to a conclusion that there were specific data leaks within their packet distribution, which did prove our point on whether the IP addresses were the victims or not. Furthermore, we used additional

tools such as snort, which was able to identify the certain clues within the Ip range and we were also able to briefly give an explanation on finding the specific file containing the Malware.

References

- "What Is Coreupdate.exe? Is It Safe or a Virus? How to Remove or Fix It." Windows Bulletin Tutorials, 25 Feb. 2019, windowsbulletin.com/files/exe/perfect-world-entertainment-inc/coreupdate/coreupdate-exe.
- LLC, Joe Security. "Analysis Report Coreupdater.exe." Automated Malware Analysis Report for Coreupdater.exe - Generated by Joe Sandbox, www.joesandbox.com/analysis/292908/0/html.
- "Case 001 PCAP Analysis." DFIR Madness, 1 Feb. 2021, dfirmadness.com/case-001-pcap-analysis/.