

# 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

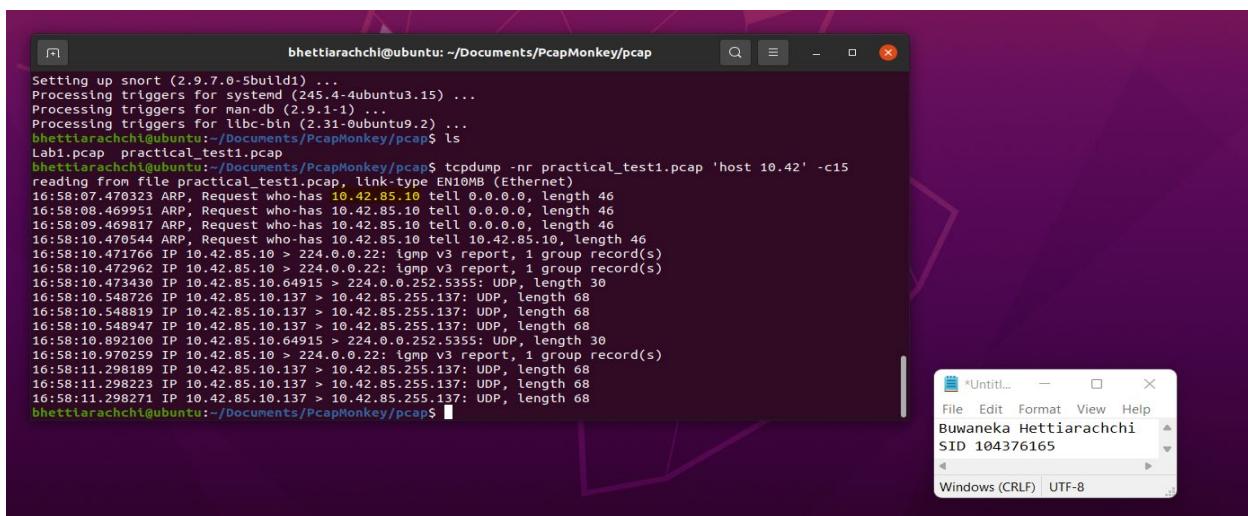
Chapter 1: Executive Summary .....	3
Chapter 2: Details.....	3
Chapter 3: IOC (Indicators Of Compromise) .....	10
Chapter 4: Threat Hunting .....	11
Methodologies .....	11
Threat Hunting Demonstration and Implementation.....	12
Limitations and considerations.....	15
Chapter 5: Comparison with the older Report .....	15
References .....	17
Figure 1: Possible information on the victim machine .....	3
Figure 2: Figure showing information on the Time range of the packets.....	4
Figure 3: Figure showing, possible information leak happening between the Victim and the attacker.....	4
Figure 4: Showing another data leak on the second victim.....	5
Figure 5: Indicates the IP address and the MAC address of the first victim machine .....	5
Figure 6: The Information of IP address and MAC addresses of the second victim .....	5
Figure 7: Hostname of IP 10.42.85.10 highlighted in yellow .....	6
Figure 8: The highlighted text shows the Hostname of the IP address 10.42.85.115 .....	6
Figure 9: User Account Name of the Infected machine.....	7
Figure 10: The changed User account.....	7
Figure 11: ICMP packet distribution between the Two Ips .....	8
Figure 12: Information on leading to the malware.....	8
Figure 13: HTTP Export of the Coreupdate.exe file .....	9
Figure 14: The output from virus total .....	9
Figure 15: Virus Total information on the Attacker IP address .....	10
Figure 16: Domains related to the IP address.....	10
Figure 17: URL associated with the malware.....	11
Figure 18: SHA256 hash of the malware file.....	11
Figure 19: Http requests used to detect evidences of the malware .....	12
Figure 20: Grab the communication between the victim and the attacker .....	12
Figure 21: Grab the communication between the second victim and the attacker.....	12
Figure 22: Command to filter the user account names .....	13
Figure 23: Used to filter the Hostnames of the IP addresses .....	13
Figure 24: Ingesting the Pcap into the Elasticsearch dashboards.....	13
Figure 25: Elasticsearch Visual dashboard, showing the IP's with the most source packets .....	14
Figure 26: Visualization for the Elasticsearch dashboard .....	15

## 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 (coreupdate.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 18<sup>th</sup> of September 2020. While the second attack took place at (12:23) on the 19<sup>th</sup> 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.



The screenshot shows a terminal window on a Linux system (Ubuntu 20.04 LTS) with a purple desktop background. The terminal window title is 'bhettiarachchi@ubuntu: ~/Documents/PcapMonkey/pcap'. The terminal output is as follows:

```
Setting up snort (2.9.7.0-5build1) ...
Processing triggers for systemd (245.4-4ubuntu3.15) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libcurl4-openssl-dev (7.61.1-1ubuntu1) ...
bhettiarachchi@ubuntu:~/Documents/PcapMonkey/pcap$ ls
Lab1.pcap  practical_test1.pcap
bhettiarachchi@ubuntu:~/Documents/PcapMonkey/pcap$ tcpdump -nr practical_test1.pcap 'host 10.42' -c15
reading from file 'practical_test1.pcap', link-type EN10MB (Ethernet)
16:58:07.470323 ARP, Request who-has 10.42.85.10 tell 0.0.0.0, length 46
16:58:08.469951 ARP, Request who-has 10.42.85.10 tell 0.0.0.0, length 46
16:58:09.469817 ARP, Request who-has 10.42.85.10 tell 0.0.0.0, length 46
16:58:10.470544 ARP, Request who-has 10.42.85.10 tell 10.42.85.10, length 46
16:58:10.471766 IP 10.42.85.10 > 224.0.0.22: igmp v3 report, 1 group record(s)
16:58:10.472962 IP 10.42.85.10 > 224.0.0.22: igmp v3 report, 1 group record(s)
16:58:10.473438 IP 10.42.85.10.64915 > 224.0.0.252.5355: UDP, length 30
16:58:10.548726 IP 10.42.85.10.137 > 10.42.85.255.137: UDP, length 68
16:58:10.548819 IP 10.42.85.10.137 > 10.42.85.255.137: UDP, length 68
16:58:10.548947 IP 10.42.85.10.137 > 10.42.85.255.137: UDP, length 68
16:58:10.892108 IP 10.42.85.10.64915 > 224.0.0.252.5355: UDP, length 30
16:58:10.979259 IP 10.42.85.10 > 224.0.0.22: igmp v3 report, 1 group record(s)
16:58:11.298189 IP 10.42.85.10.137 > 10.42.85.255.137: UDP, length 68
16:58:11.298223 IP 10.42.85.10.137 > 10.42.85.255.137: UDP, length 68
16:58:11.298271 IP 10.42.85.10.137 > 10.42.85.255.137: UDP, length 68
bhettiarachchi@ubuntu:~/Documents/PcapMonkey/pcap$
```

A second terminal window titled 'Untitled...' is visible in the background, showing the user's name and session ID.

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.

```
bhettiarachchi@ubuntu:~/Documents/PcapMonkey/pcap$ capinfos practical_test1.pcap
File name: practical_test1.pcap
File type: Wireshark... - pcapng
File encapsulation: Ethernet
File timestamp precision: microseconds (6)
Packet size limit: file hdr: (not set)
Number of packets: 411 k
File size: 197 MB
Data size: 183 MB
Capture duration: 27650.358197 seconds
First packet time: 2020-09-18 17:58:07.470323
Last packet time: 2020-09-19 01:38:57.828520
Data byte rate: 6,649 bytes/s
Data bit rate: 53 kbps
Average packet size: 446.47 bytes
Average packet rate: 14 packets/s
SHA256: 09abf49efea1852e047987d92907704d47f36d75f6c8056e2cafa6cc027791cb
RIPEMD160: 582b56059d5ad7203356e578fc0867fdc6a759
SHA1: ab2deca8c7881187806856c6baeb215abc990d2b
Strict time order: True
Capture oper-sys: Linux 5.8.0-kali1-amd64
Capture application: Mergecap (Wireshark) 3.2.6 (Git v3.2.6 packaged as 3.2.6-1)
Number of interfaces in file: 1
Interface #0 info:
    Encapsulation = Ethernet (1 - ether)
    Capture length = 262144
    Time precision = microseconds (6)
    Time ticks per second = 1000000
    Number of stat entries = 0
    Number of packets = 411797
bhettiarachchi@ubuntu:~/Documents/PcapMonkey/pcap$
```

\*Untitled... File Edit Format View Help  
Buwaneka Hettiarachchi  
SID 104376165  
Windows (CRLF) UTF-8

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 18<sup>th</sup> of September 2020 and then it stretched till 1:38 am on 19<sup>th</sup> 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 victim IP address

```
09/18-21:16:40.714240 [**] [1:1000000122:1] COMMUNITY WEB-MISC Mod_jrun overflow attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 10.42.85.115:56675 -> 20.54.64.282:80
09/18-21:19:13.414319 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 194.61.24.102 -> 10.42.85.10
09/18-21:19:13.414319 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 194.61.24.102 -> 10.42.85.10
09/18-21:19:13.414386 [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP} 194.61.24.102 -> 10.42.85.10
09/18-21:19:13.414869 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.42.85.10 -> 194.61.24.102
09/18-21:19:26.549145 [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102 -> 10.42.85.10
:3389
09/18-21:21:26.112470 [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102 -> 10.42.85.10
:3389
09/18-21:21:26.342463 [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102 -> 10.42.85.10
:3389
09/18-21:21:26.564666 [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102 -> 10.42.85.10
:3389
09/18-21:21:26.786791 [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102 -> 10.42.85.10
:3389
09/18-21:21:27.001408 [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40052 -> 10.42.85.10
:3389
09/18-21:21:27.224505 [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40054 -> 10.42.85.10
:3389
09/18-21:21:27.437501 [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40056 -> 10.42.85.10
:3389
```

\*Untitled... File Edit Format View Help  
Buwaneka Hettiarachchi  
SID 104376165  
Windows (CRLF) UTF-8

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 18<sup>th</sup>, 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.

```
09/19-00:23:40.724456 [**] [1:1201:7] ATTACK-RESPONSES 403 Forbidden [**] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 205.185.216.42:80 -> 10.42.85.115:51150
09/19-00:23:40.727386 [**] [1:1201:7] ATTACK-RESPONSES 403 Forbidden [**] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 205.185.216.10:80 -> 10.42.85.115:51149
09/19-00:23:49.776640 [**] [1:1344:5] WEB-ATTACKS cc command attempt [**] [Classification: Web Application Attack] [Priority: 1] [TCP] 10.42.85.115:51150 -> 23.37.117.182:80
09/19-00:25:24.560479 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 10.42.85.115:56463 -> 239.255.255.25
0:1900
09/19-00:25:27.556073 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 10.42.85.115:56463 -> 239.255.255.25
0:1900
09/19-00:25:30.572765 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 10.42.85.115:56463 -> 239.255.255.25
0:1900
bhettiarachchi@ubuntu:~/Documents/PcapMonkey/pcap$ wc -l snort.out
373 snort.out
bhettiarachchi@ubuntu:~/Documents/PcapMonkey/pcap$ 
bhettiarachchi@ubuntu:~/Documents/PcapMonkey/pcap$ ^C
bhettiarachchi@ubuntu:~/Documents/PcapMonkey/pcap$ 
```

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.

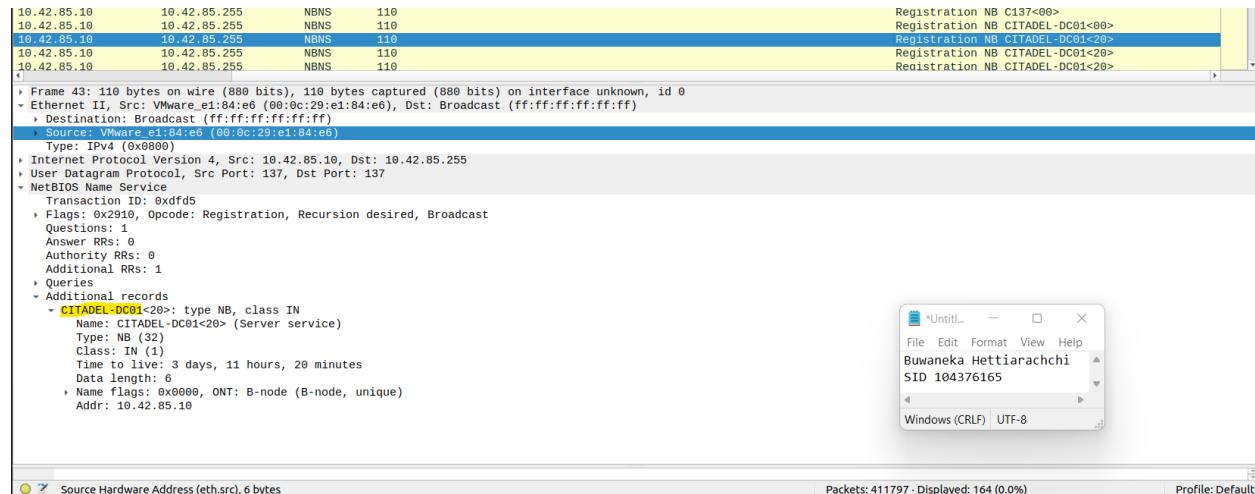


Figure 7: Hostname of IP 10.42.85.10 highlighted in yellow

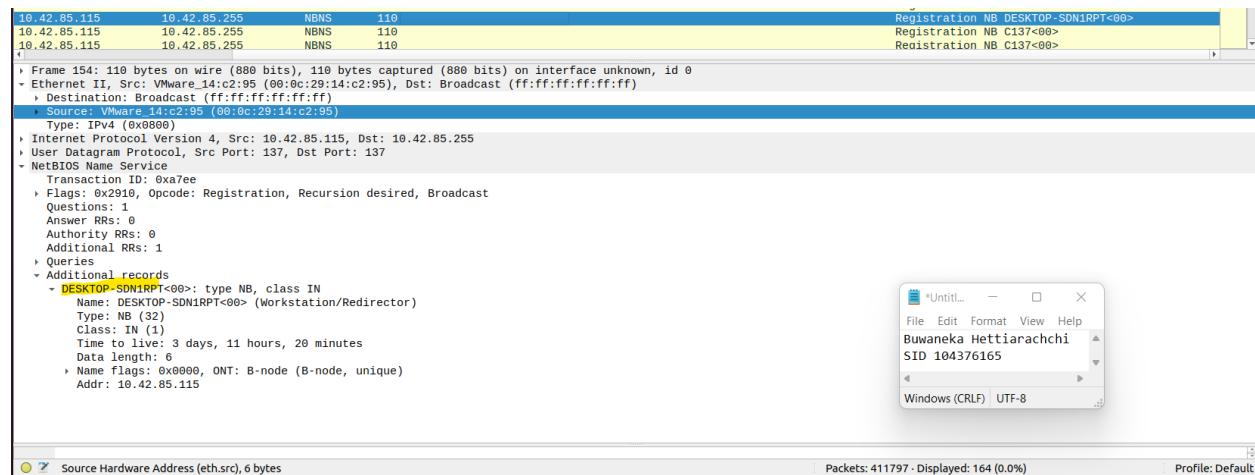


Figure 8: The highlighted text shows the Hostname of the IP address 10.42.85.115

Figure 3 shows the hostname that was associated with the IP address 10.42.85.10, the hostname is CITADEL-DC01. 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.

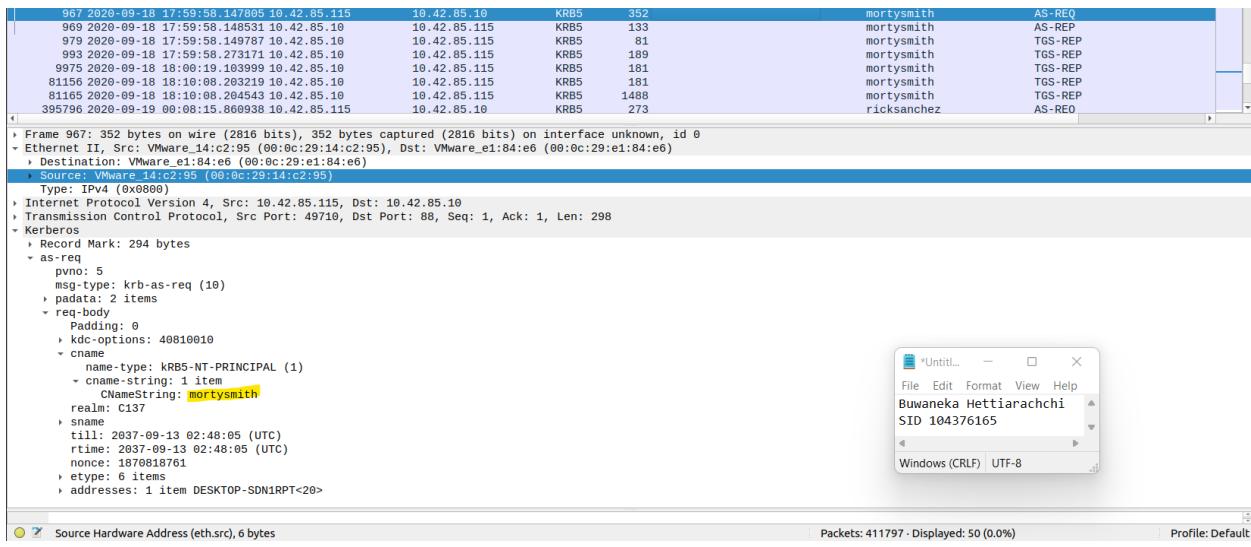


Figure 9: User Account Name of the Infected machine

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.

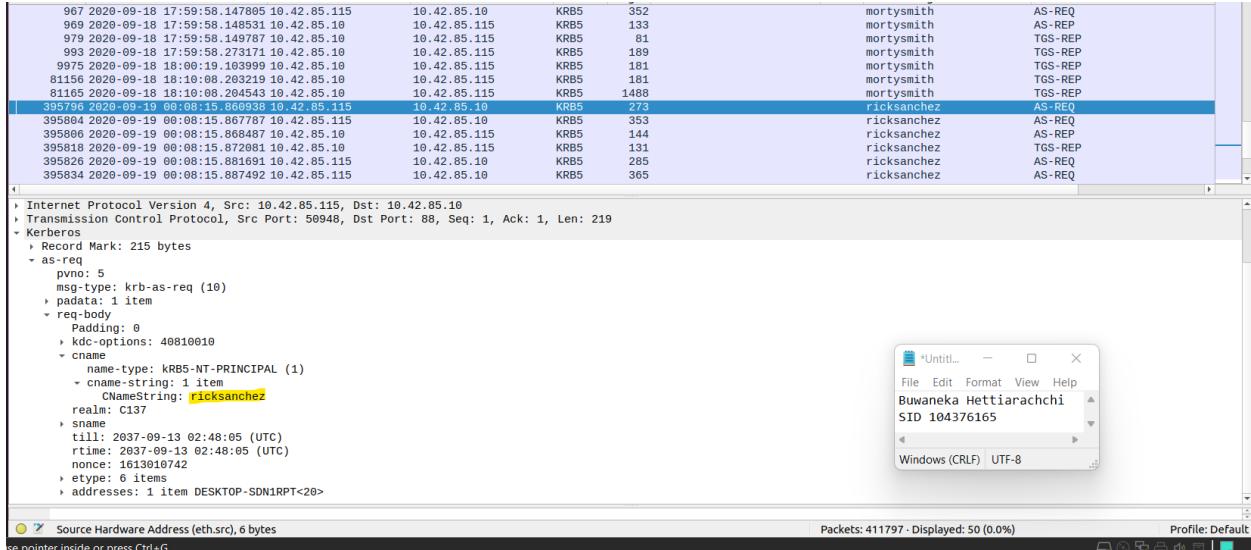


Figure 10: The changed User account

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 19<sup>th</sup> 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.

```
hettiarachchi@ubuntu:/Documents/PcapMonkey/pcap$ tcpdump -tttttt practical_test1.pcap 'host 194.61.24.102' -c 20
reading from file practical_test1.pcap, link-type EN10MB (Ethernet)
2020-09-18 21:19:13.414319 IP 194.61.24.102 > 10.42.85.10: ICMP echo request, id 61295, seq 0, length 8
2020-09-18 21:19:13.414353 IP 194.61.24.102.64385 > 10.42.85.10.443: Flags [S], seq 770930765, win 1024, options [mss 1460], length 0
2020-09-18 21:19:13.414378 IP 194.61.24.102.64385 > 10.42.85.10.80: Flags [.], ack 770930765, win 1024, length 0
2020-09-18 21:19:13.414384 IP 194.61.24.102 > 10.42.85.10: ICMP time stamp query id 57462 seq 0, length 20
2020-09-18 21:19:26.469203 IP 194.61.24.102.38081 > 10.42.85.10.3389: Flags [S], seq 304134196, win 64240, options [mss 1460,sackOK,TS val 2972490670,ack 304134197], length 8
2020-09-18 21:19:26.469491 IP 10.42.85.10.3389 > 194.61.24.102.38088: Flags [S], seq 2792490670, ack 304134197, win 64000, options [mss 1460,sackOK,TS val 701188 ecr 2972490670], length 8
2020-09-18 21:19:26.469897 IP 194.61.24.102.38088 > 10.42.85.10.3389: Flags [R.], ack 1, win 502, options [nop,nop,TS val 2976250824 ecr 701188]
2020-09-18 21:19:26.469902 IP 194.61.24.102.38088 > 10.42.85.10.3389: Flags [R.], seq 1, ack 1, win 502, options [nop,nop,TS val 2976250824 ecr 701188]
2020-09-18 21:19:26.472244 IP 194.61.24.102.38089 > 10.42.85.10.3389: Flags [S], seq 83770137, win 64240, options [mss 1460,sackOK,TS val 2976250827 ecr 0,nop,wscale 7], length 0
2020-09-18 21:19:26.472426 IP 10.42.85.10.3389 > 194.61.24.102.38090: Flags [S.], seq 83770138, win 64000, options [mss 1460,nop,wscale 0,sackOK,TS val 701188 ecr 2976250827], length 0
2020-09-18 21:19:26.472579 IP 194.61.24.102.38090 > 10.42.85.10.3389: Flags [.], ack 1, win 502, options [nop,nop,TS val 2976250827 ecr 701188], length 0
2020-09-18 21:19:26.472604 IP 194.61.24.102.38092 > 10.42.85.10.3389: Flags [S.], seq 3867782754, win 64240, options [mss 1460,sackOK,TS val 2976250827 ecr 0,nop,wscale 7], length 0
2020-09-18 21:19:26.472701 IP 10.42.85.10.3389 > 194.61.24.102.38092: Flags [S.], seq 533924876, ack 3867782755, win 64000, options [mss 1460,nop,wscale 0,sackOK,TS val 701188 ecr 2976250827], length 0
```

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.

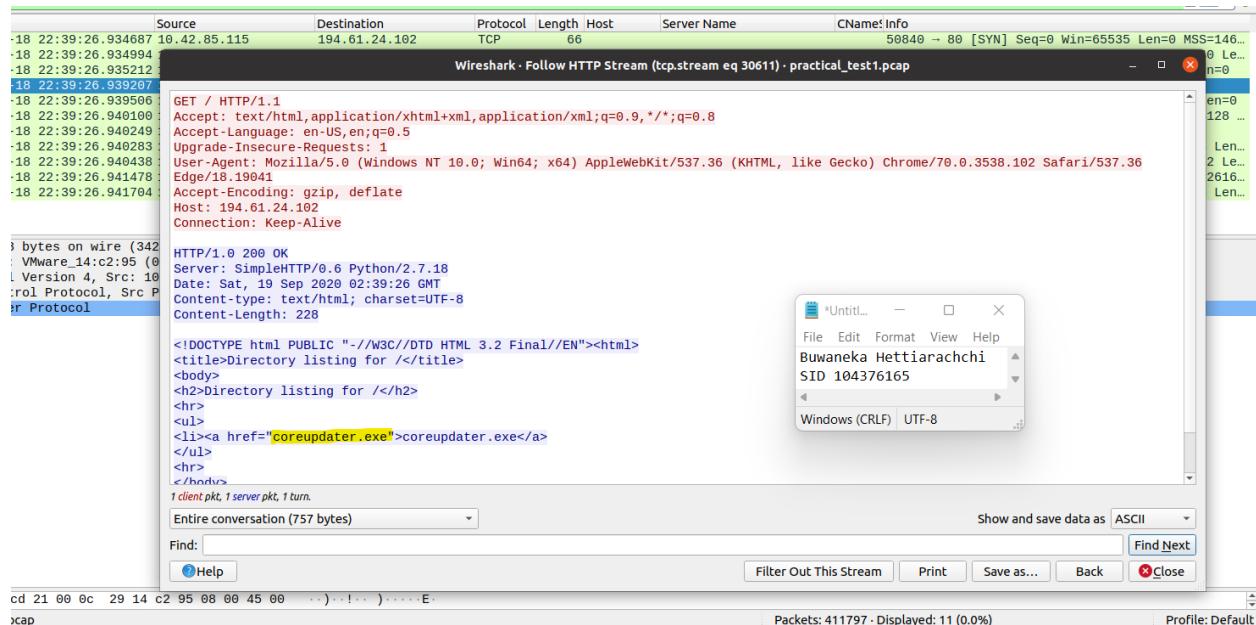


Figure 12: Information on leading to the malware

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.

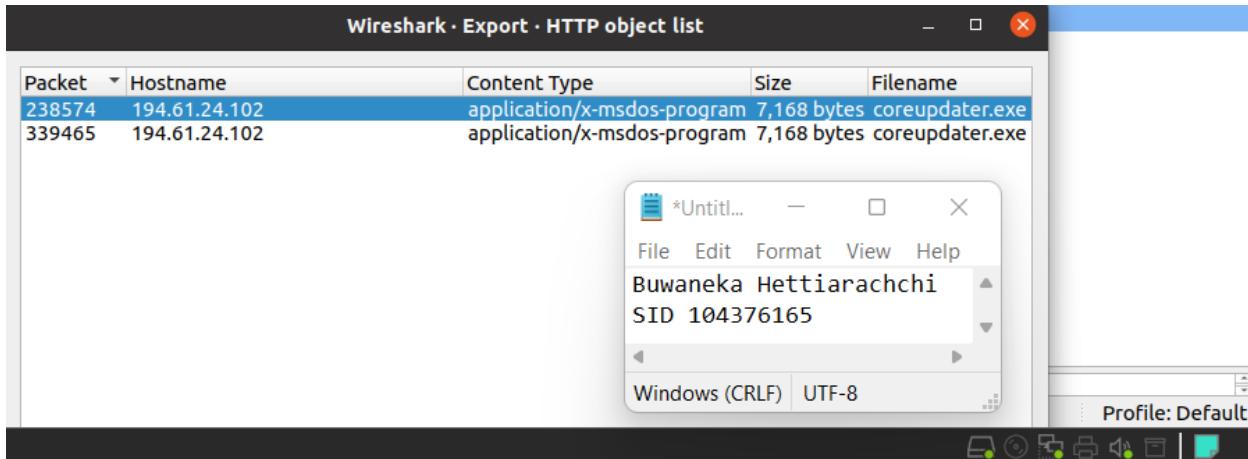


Figure 13: HTTP Export of the Coreupdate.exe file

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.

Engine	Result	Notes
Acronis (Static ML)	Suspicious	Ad-Aware
AhnLab-V3	Trojan/Win64_RL_Shelma.R298109	Alibaba
AIYac	Trojan.Metasploit.A	Antiy-AVL
Arcabit	Trojan.Metasploit.A	Avast
AVG	Win64:MetasploitEncod-A [Tr]	Avira (no cloud)
BitDefender	Trojan.Metasploit.A	CAT-QuickHeal
Comodo	Malware#@3k99pse66s6bl	CrowdStrike Falcon
Cybereason	Malicious.500e47	Cylance
Cynet	Malicious (score: 100)	Cyren
DrWeb	BackDoor.Shell.244	Elastic

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.

The screenshot shows the Virus Total interface for the IP address 194.61.24.102. At the top, a circular icon indicates 1 out of 90 security vendors flagged the address as malicious. The main panel displays the IP address (194.61.24.102, AS 38994, ERA LLC) and a note about one vendor flagging it as malicious. Below this, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. The DETECTION tab is selected, showing a table of vendor detections:

Vendor	Status	Notes
CRDF	Malicious	
Acronis	Clean	
AICC (MONITORAPP)	Clean	
alphaMountain.ai	Clean	
Armis	Clean	
BADWARE.INFO	Clean	
benkow.cc	Clean	

To the right, a separate window shows the Windows command-line interface (cmd) with the following text:

```
*Until... File Edit Format View Help
Buwaneka Hettiarachchi
SID 104376165
Windows (CRLF) UTF-8
```

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.

The screenshot shows the Virus Total interface for the IP address 194.61.24.102. At the top, a circular icon indicates 1 out of 90 security vendors flagged the address as malicious. The main panel displays the IP address (194.61.24.102, AS 38994, ERA LLC) and a note about one vendor flagging it as malicious. Below this, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. The DETAILS tab is selected, showing a table of passive DNS replication data:

Date resolved	Detections	Resolver	Domain
2020-05-07	0 / 90	VirusTotal	blacklist-in.rbl.ipline.eu
2019-11-06	0 / 89	VirusTotal	klient055.online
2019-11-05	0 / 91	VirusTotal	klient-293.xyz

To the right, a separate window shows the Windows command-line interface (cmd) with the following text:

```
*Until... File Edit Format View Help
Buwaneka Hettiarachchi
SID 104376165
Windows (CRLF) UTF-8
```

Figure 16: Domains related to the IP address

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

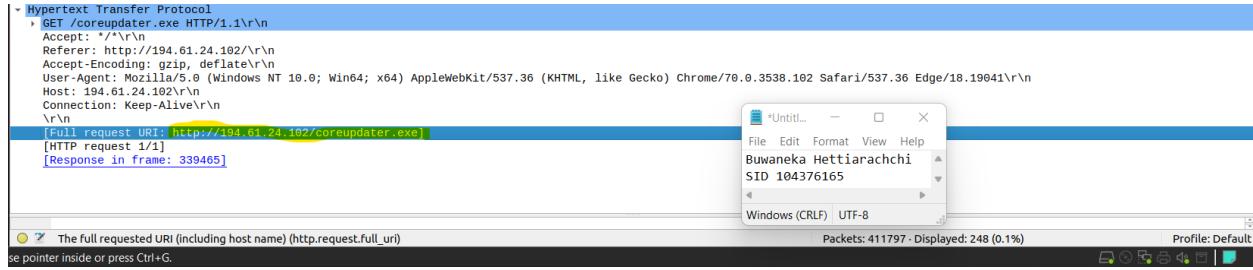


Figure 17: URL associated with the malware

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.

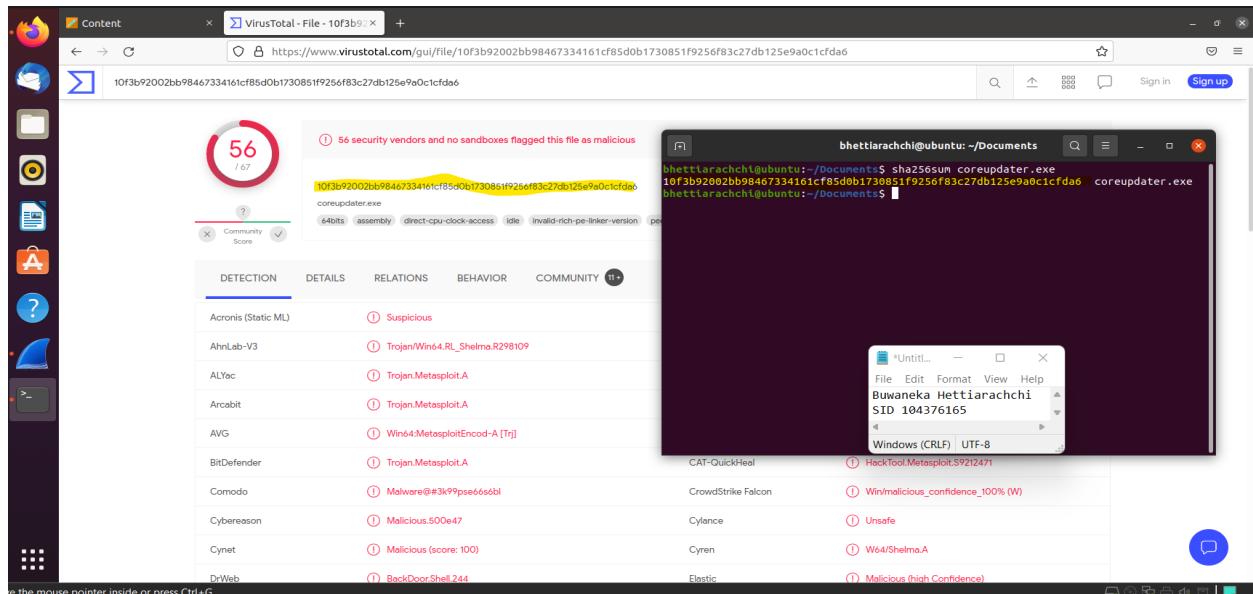


Figure 18: SHA256 hash of the malware file

## 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.

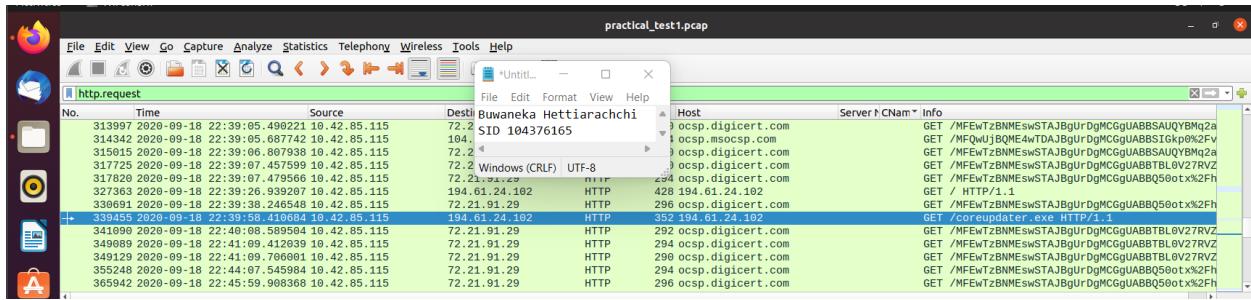


Figure 19: Http requests used to detect evidences of the malware

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.

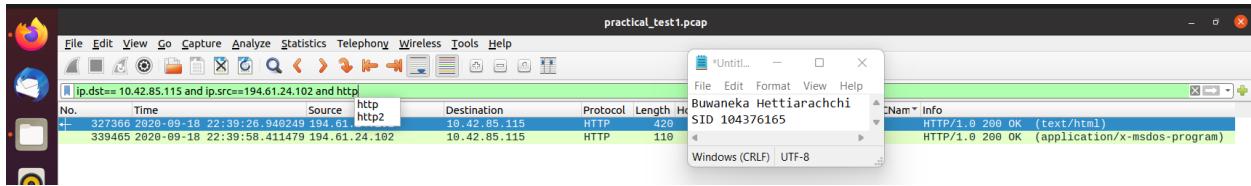


Figure 20: Grab the communication between the victim and the attacker

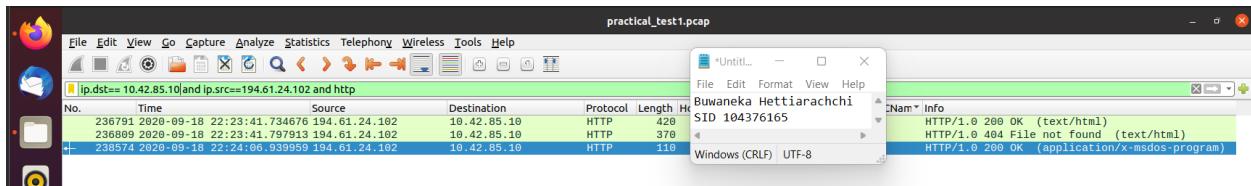


Figure 21: Grab the communication between the second victim and the attacker

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.

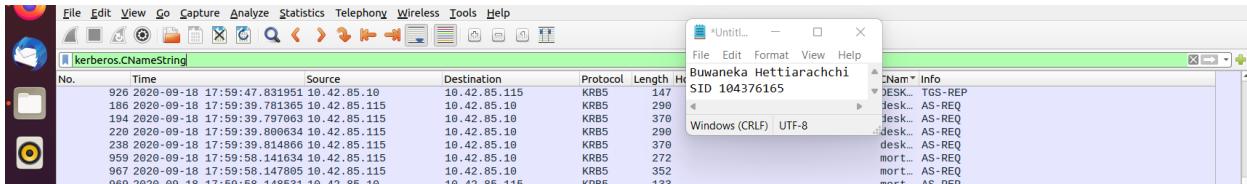


Figure 22: Command to filter the user account names

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

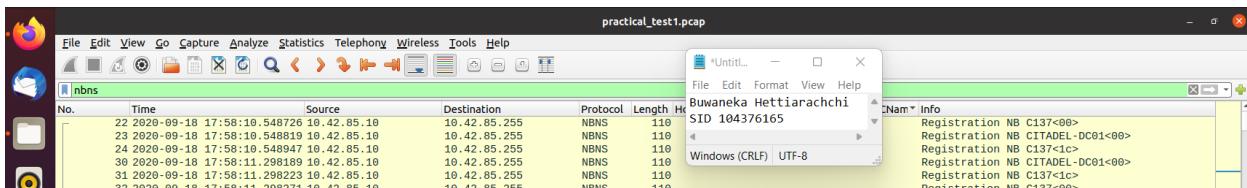


Figure 23: Used to filter the Hostnames of the IP addresses

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.

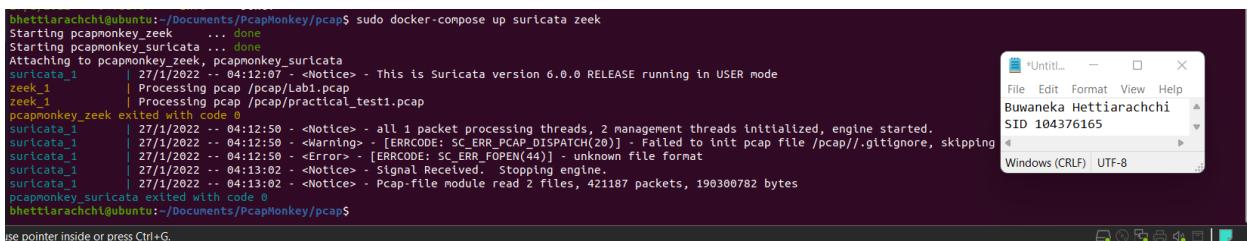


Figure 24: Ingesting the Pcap into the Elasticsearch dashboards

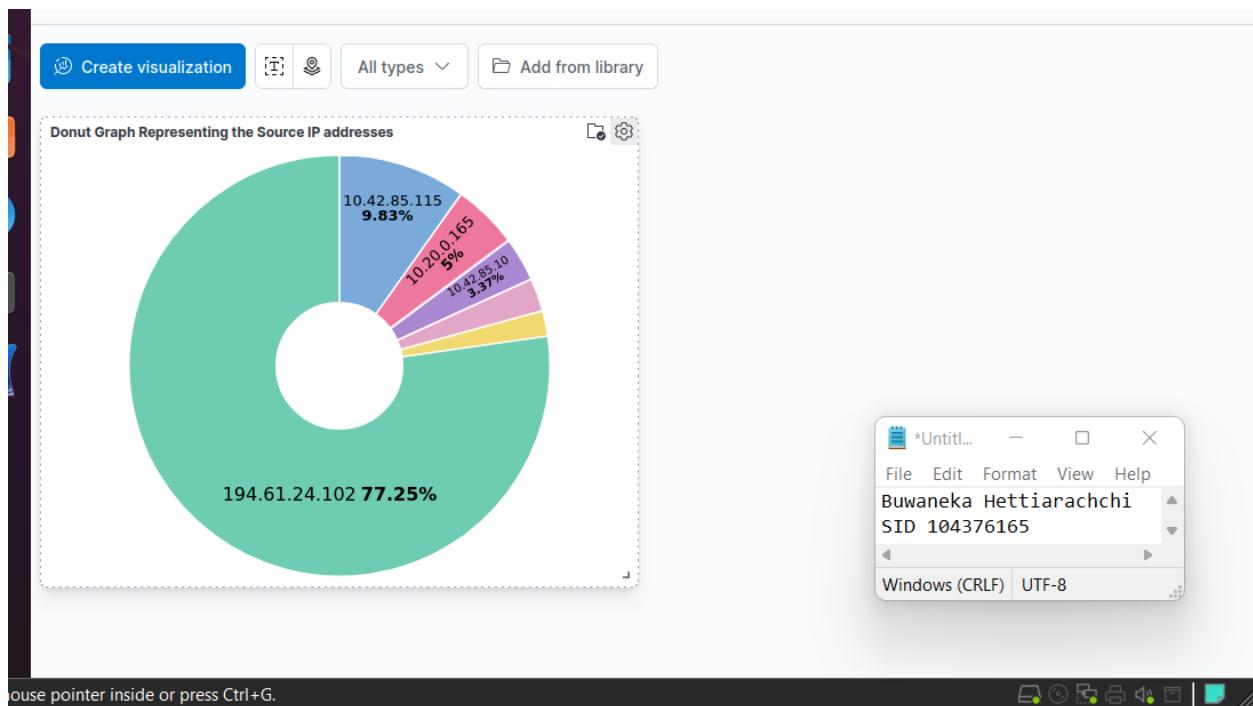


Figure 25: Elasticsearch Visual dashboard, showing the IP's with the most source packets

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.

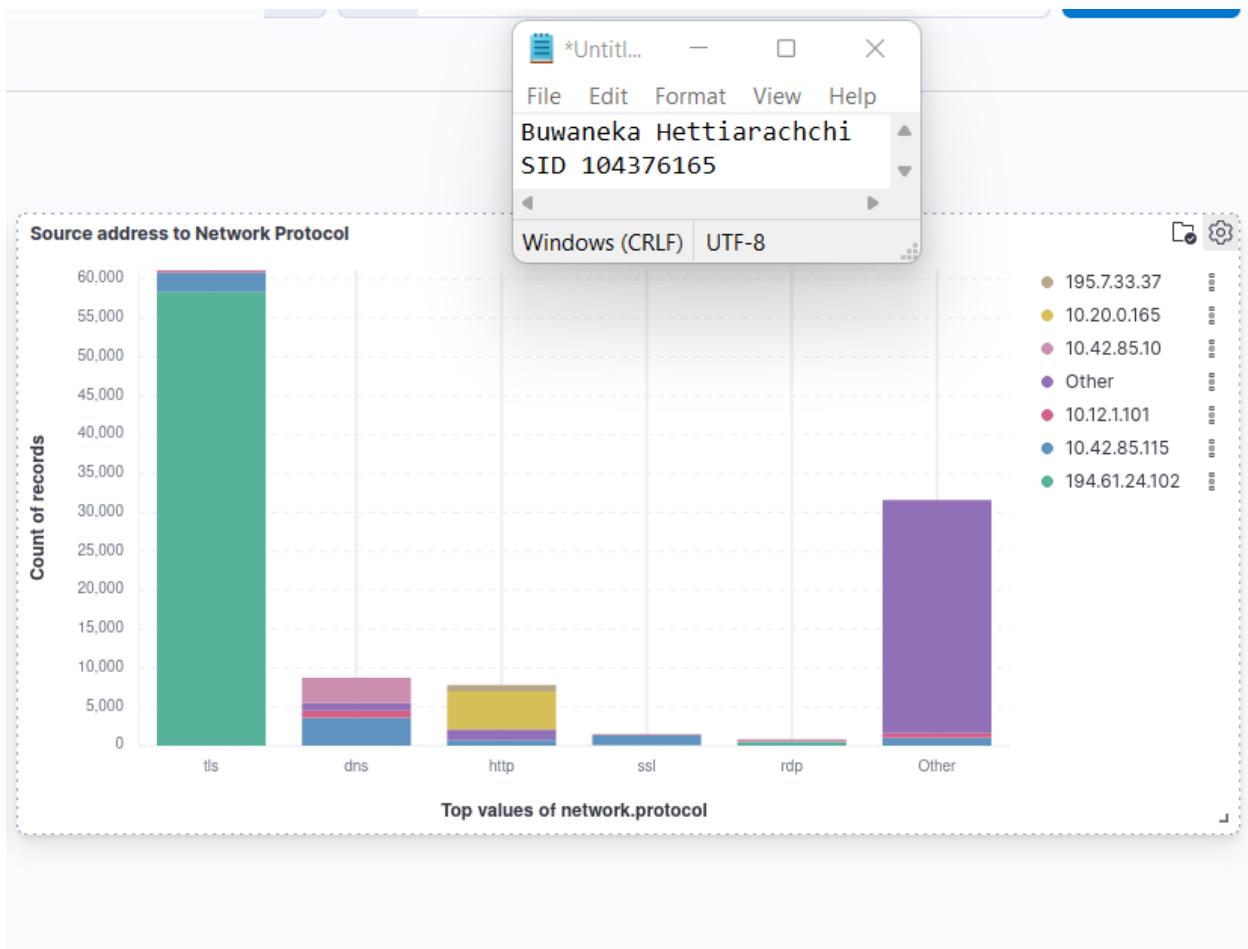


Figure 26: Visualization for the Elasticsearch dashboard

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 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](http://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](http://www.joesandbox.com/analysis/292908/0/html).
- “Case 001 PCAP Analysis.” DFIR Madness, 1 Feb. 2021, [dfirmadness.com/case-001-pcap-analysis/](http://dfirmadness.com/case-001-pcap-analysis/).