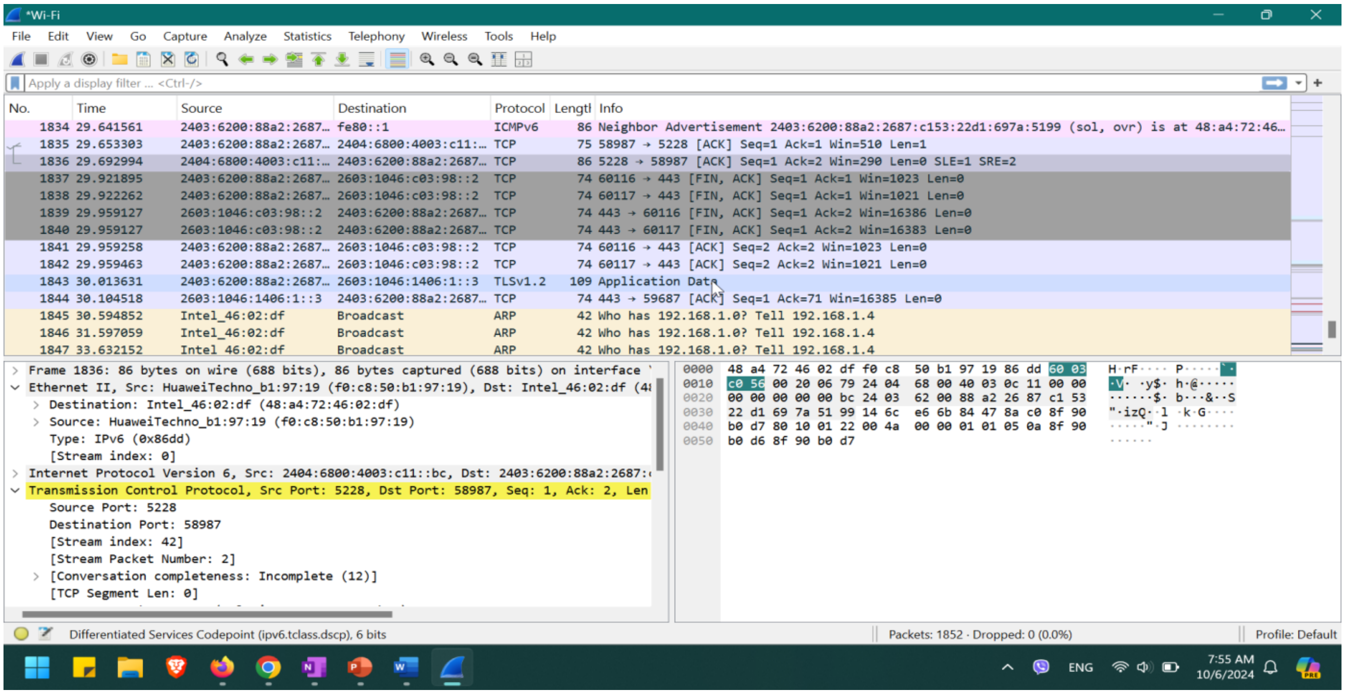
Incident handler's journal

Entry Logs

Date: July 23, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident This incident occurred in the two phases: 1. **Detection and Analysis**: The scenario outlines how the organization first detected the ransomware incident. For the analysis step, the organization contacted several organizations for technical assistance. 2. **Containment, Eradication, and Recovery**: The scenario details some steps that the organization took to contain the incident. For example, the company shut down their computer systems. However, since they could not work to eradicate and recover from the incident alone, they contacted several other organizations for assistance.
Tool(s) used	None
The 5 W's	● **Who**: An organized group of unethical hackers ● **What**: A ransomware security incident ● **Where**: At a health care company ● **When**: Tuesday 9:00 a.m. ● **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	1. How could the health care company prevent an incident like this from occurring again? Give security awareness training to internal employees to not click or open suspicious email or link and check with IT system administrator 2. Should the company pay the ransom to retrieve the decryption key? Company should never pay the ransom because what gone is gone, even paying will not guarantee that data will be retrieved. Additionally, it might happen again in future from same attacker.

Date: Oct 6 2024	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity.
The 5 W's	● **Who**: N/A ● **What**: N/A ● **Where**: N/A ● **When**: N/A ● **Why**: N/A
Additional notes	I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface was very overwhelming. I can see why it's such a powerful tool for understanding network traffic.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source                Destination           Protocol Lengtl Info
 1834 29.641561  2403:6200:88a2:2687…  fe80::1               ICMPv6     86 Neighbor Advertisement 2403:6200:88a2:2687:c153:22d1:697a:5199 (sol, ovr) is at 48:a4:72:46…
 1835 29.653303  2403:6200:88a2:2687…  2404:6800:4003:c11:…  TCP        75 58987 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1
 1836 29.692994  2404:6800:4003:c11:…  2403:6200:88a2:2687…  TCP        86 5228 → 58987 [ACK] Seq=1 Ack=2 Win=290 Len=0 SLE=1 SRE=2
 1837 29.921895  2403:6200:88a2:2687…  2603:1046:c03:98::2   TCP        74 60116 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
 1838 29.922262  2403:6200:88a2:2687…  2603:1046:c03:98::2   TCP        74 60117 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1021 Len=0
 1839 29.959127  2603:1046:c03:98::2   2403:6200:88a2:2687…  TCP        74 443 → 60116 [FIN, ACK] Seq=1 Ack=2 Win=16386 Len=0
 1840 29.959127  2603:1046:c03:98::2   2403:6200:88a2:2687…  TCP        74 443 → 60117 [FIN, ACK] Seq=1 Ack=2 Win=16383 Len=0
 1841 29.959258  2403:6200:88a2:2687…  2603:1046:c03:98::2   TCP        74 60116 → 443 [ACK] Seq=2 Ack=2 Win=1023 Len=0
 1842 29.959463  2403:6200:88a2:2687…  2603:1046:c03:98::2   TCP        74 60117 → 443 [ACK] Seq=2 Ack=2 Win=1021 Len=0
 1843 30.013631  2403:6200:88a2:2687…  2603:1046:1406:1::3   TLSv1.2   109 Application Data
 1844 30.104518  2603:1046:1406:1::3   2403:6200:88a2:2687…  TCP        74 443 → 59687 [ACK] Seq=1 Ack=71 Win=16385 Len=0
 1845 30.594852  Intel_46:02:df        Broadcast             ARP        42 Who has 192.168.1.0? Tell 192.168.1.4
 1846 31.597059  Intel_46:02:df        Broadcast             ARP        42 Who has 192.168.1.0? Tell 192.168.1.4
 1847 33.632152  Intel_46:02:df        Broadcast             ARP        42 Who has 192.168.1.0? Tell 192.168.1.4
```

```
> Frame 1836: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface '
v Ethernet II, Src: HuaweiTechno_b1:97:19 (f0:c8:50:b1:97:19), Dst: Intel_46:02:df (48
  > Destination: Intel_46:02:df (48:a4:72:46:02:df)
  > Source: HuaweiTechno_b1:97:19 (f0:c8:50:b1:97:19)
    Type: IPv6 (0x86dd)
    [Stream index: 0]
> Internet Protocol Version 6, Src: 2404:6800:4003:c11::bc, Dst: 2403:6200:88a2:2687:
v Transmission Control Protocol, Src Port: 5228, Dst Port: 58987, Seq: 1, Ack: 2, Len
    Source Port: 5228
    Destination Port: 58987
    [Stream index: 42]
    [Stream Packet Number: 2]
  > [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 0]
```

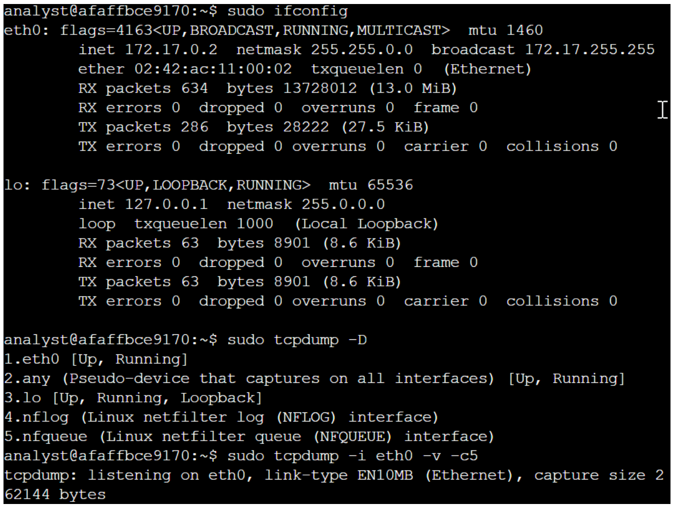
```
0000  48 a4 72 46 02 df f0 c8  50 b1 97 19 86 dd 60 03   H·rF···· P·····`·
0010  c0 56 00 20 06 79 24 04  68 00 40 03 0c 11 00 00   ·V· ·y$· h·@·····
0020  00 00 00 00 00 bc 24 03  62 00 88 a2 26 87 c1 53   ······$· b···&··S
0030  22 d1 69 7a 51 99 14 6c  e6 6b 84 47 8a c0 8f 90   "·izQ··l ·k·G····
0040  b0 d7 80 10 01 22 00 4a  00 00 01 01 05 0a 8f 90   ·····"·J ········
0050  b0 d6 8f 90 b0 d7                                   ······
```

Differentiated Services Codepoint (ipv6.tclass.dscp), 6 bits

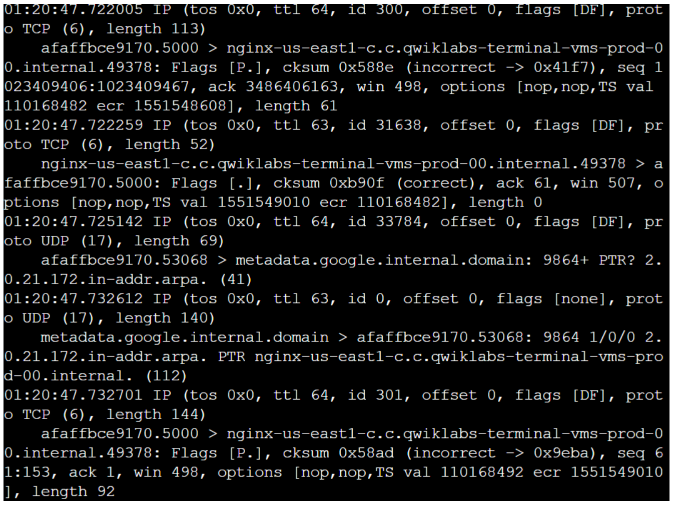
Packets: 1852 · Dropped: 0 (0.0%)

Profile: Default

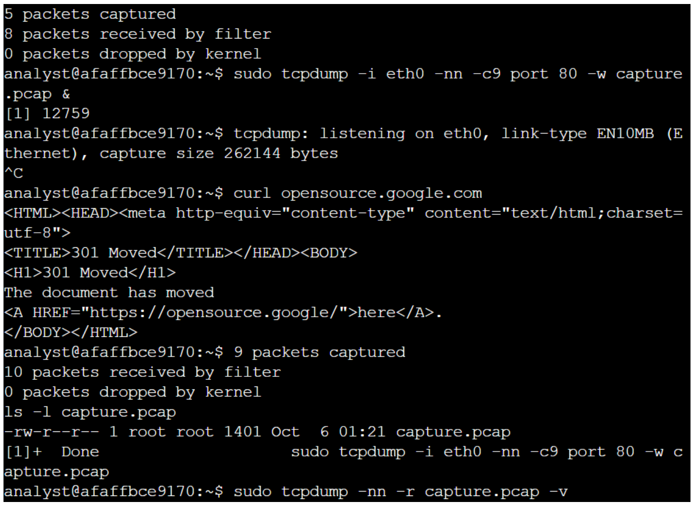
Date: Oct 6 2024	**Entry:** #3
Description	Capturing my first network packet
Tool(s) used	For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the command-line interface. Similar to Wireshark, the value of tcpdump in cybersecurity is that it allows security analysts to capture, filter, and analyze network traffic.
The 5 W's	- **Who**: N/A - **What**: N/A - **Where**: N/A - **When**: N/A - **Why**: N/A
Additional notes	I'm still new to using the command-line interface, so using it to capture and filter network traffic was a challenge. I got stuck a couple of times because I used the wrong commands. But after carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic.



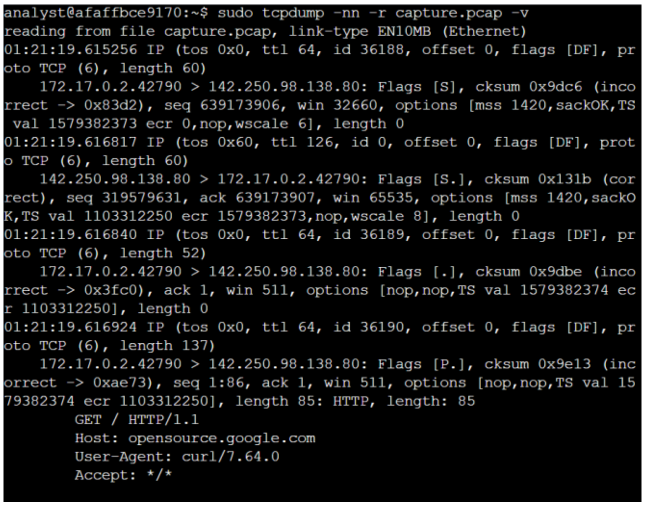
```
analyst@afaffbce9170:~$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1460
        inet 172.17.0.2  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ac:11:00:02  txqueuelen 0  (Ethernet)
        RX packets 634  bytes 13728012 (13.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 286  bytes 28222 (27.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 63  bytes 8901 (8.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 63  bytes 8901 (8.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

analyst@afaffbce9170:~$ sudo tcpdump -D
1.eth0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
analyst@afaffbce9170:~$ sudo tcpdump -i eth0 -v -c5
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 2
62144 bytes
```



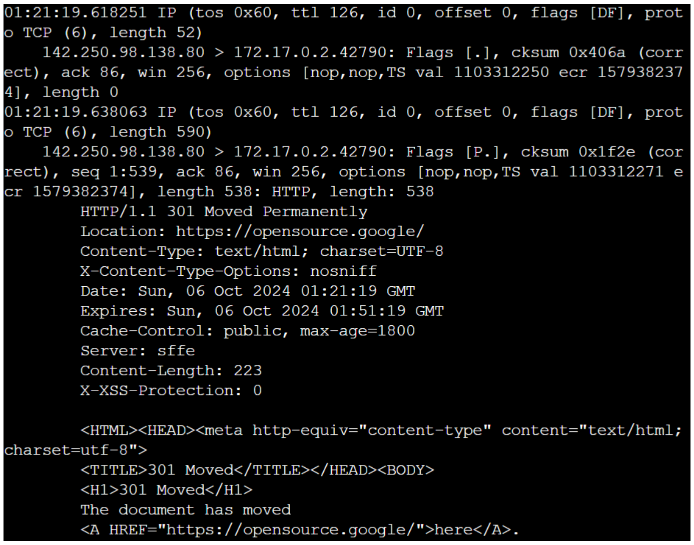
```
01:20:47.722005 IP (tos 0x0, ttl 64, id 300, offset 0, flags [DF], prot
o TCP (6), length 113)
    afaffbce9170.5000 > nginx-us-east1-c.c.qwiklabs-terminal-vms-prod-0
0.internal.49378: Flags [P.], cksum 0x588e (incorrect -> 0x41f7), seq 1
023409406:1023409467, ack 3486406163, win 498, options [nop,nop,TS val
110168482 ecr 1551548608], length 61
01:20:47.722259 IP (tos 0x0, ttl 63, id 31638, offset 0, flags [DF], pr
oto TCP (6), length 52)
    nginx-us-east1-c.c.qwiklabs-terminal-vms-prod-00.internal.49378 > a
faffbce9170.5000: Flags [.], cksum 0xb90f (correct), ack 61, win 507, o
ptions [nop,nop,TS val 1551549010 ecr 110168482], length 0
01:20:47.725142 IP (tos 0x0, ttl 64, id 33784, offset 0, flags [DF], pr
oto UDP (17), length 69)
    afaffbce9170.53068 > metadata.google.internal.domain: 9864+ PTR? 2.
0.21.172.in-addr.arpa. (41)
01:20:47.732612 IP (tos 0x0, ttl 63, id 0, offset 0, flags [none], prot
o UDP (17), length 140)
    metadata.google.internal.domain > afaffbce9170.53068: 9864 1/0/0 2.
0.21.172.in-addr.arpa. PTR nginx-us-east1-c.c.qwiklabs-terminal-vms-pro
d-00.internal. (112)
01:20:47.732701 IP (tos 0x0, ttl 64, id 301, offset 0, flags [DF], prot
o TCP (6), length 144)
    afaffbce9170.5000 > nginx-us-east1-c.c.qwiklabs-terminal-vms-prod-0
0.internal.49378: Flags [P.], cksum 0x58ad (incorrect -> 0x9eba), seq 6
1:153, ack 1, win 498, options [nop,nop,TS val 110168492 ecr 1551549010
], length 92
```



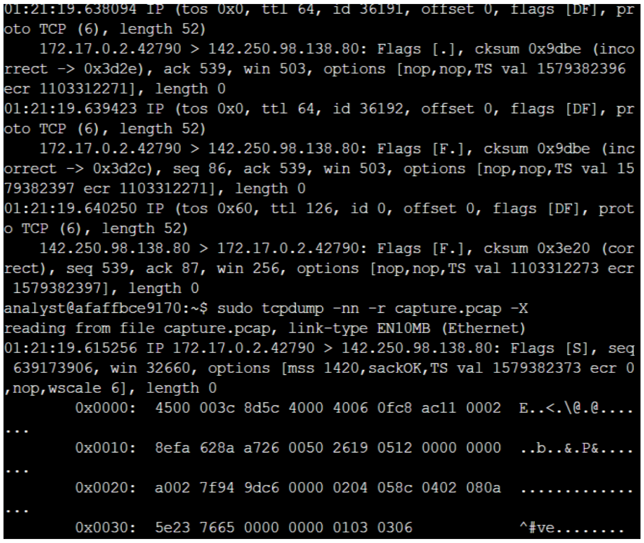
```
5 packets captured
8 packets received by filter
0 packets dropped by kernel
analyst@afaffbce9170:~$ sudo tcpdump -i eth0 -nn -c9 port 80 -w capture
.pcap &
[1] 12759
analyst@afaffbce9170:~$ tcpdump: listening on eth0, link-type EN10MB (E
thernet), capture size 262144 bytes
^C
analyst@afaffbce9170:~$ curl opensource.google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=
utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://opensource.google/">here</A>.
</BODY></HTML>
analyst@afaffbce9170:~$ 9 packets captured
10 packets received by filter
0 packets dropped by kernel
ls -l capture.pcap
-rw-r--r-- 1 root root 1401 Oct  6 01:21 capture.pcap
[1]+  Done                    sudo tcpdump -i eth0 -nn -c9 port 80 -w c
apture.pcap
analyst@afaffbce9170:~$ sudo tcpdump -nn -r capture.pcap -v
```



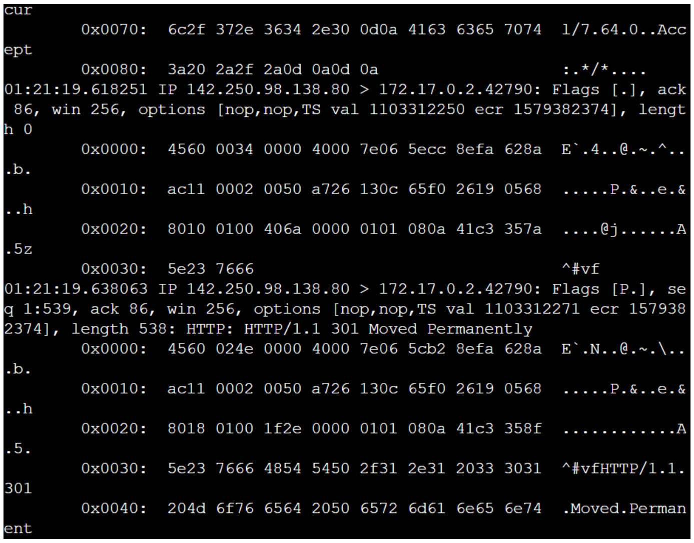
```
analyst@afaffbce9170:~$ sudo tcpdump -nn -r capture.pcap -v
reading from file capture.pcap, link-type EN10MB (Ethernet)
01:21:19.615256 IP (tos 0x0, ttl 64, id 36188, offset 0, flags [DF], pr
oto TCP (6), length 60)
    172.17.0.2.42790 > 142.250.98.138.80: Flags [S], cksum 0x9dc6 (inco
rrect -> 0x83d2), seq 639173906, win 32660, options [mss 1420,sackOK,TS
 val 1579382373 ecr 0,nop,wscale 6], length 0
01:21:19.616817 IP (tos 0x60, ttl 126, id 0, offset 0, flags [DF], prot
o TCP (6), length 60)
    142.250.98.138.80 > 172.17.0.2.42790: Flags [S.], cksum 0x131b (cor
rect), seq 319579631, ack 639173907, win 65535, options [mss 1420,sackO
K,TS val 1103312250 ecr 1579382373,nop,wscale 8], length 0
01:21:19.616840 IP (tos 0x0, ttl 64, id 36189, offset 0, flags [DF], pr
oto TCP (6), length 52)
    172.17.0.2.42790 > 142.250.98.138.80: Flags [.], cksum 0x9dbe (inco
rrect -> 0x3fc0), ack 1, win 511, options [nop,nop,TS val 1579382374 ec
r 1103312250], length 0
01:21:19.616924 IP (tos 0x0, ttl 64, id 36190, offset 0, flags [DF], pr
oto TCP (6), length 137)
    172.17.0.2.42790 > 142.250.98.138.80: Flags [P.], cksum 0x9e13 (inc
orrect -> 0xae73), seq 1:86, ack 1, win 511, options [nop,nop,TS val 15
79382374 ecr 1103312250], length 85: HTTP, length: 85
        GET / HTTP/1.1
        Host: opensource.google.com
        User-Agent: curl/7.64.0
        Accept: */*
```



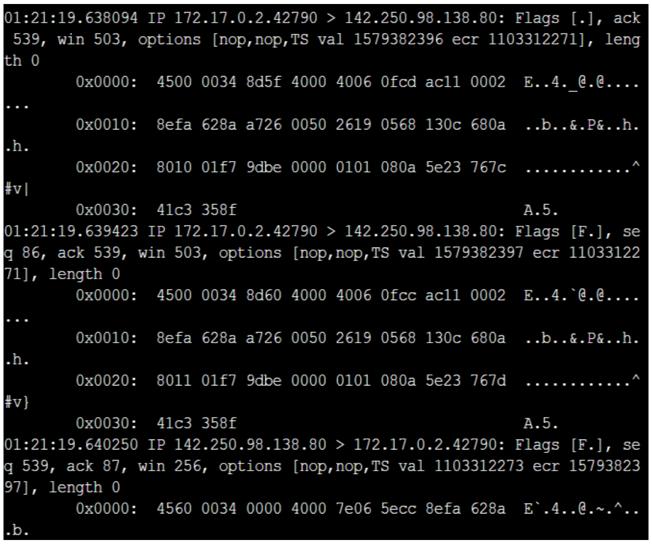
```
01:21:19.618251 IP (tos 0x60, ttl 126, id 0, offset 0, flags [DF], prot
o TCP (6), length 52)
    142.250.98.138.80 > 172.17.0.2.42790: Flags [.], cksum 0x406a (corr
ect), ack 86, win 256, options [nop,nop,TS val 1103312250 ecr 157938237
4], length 0
01:21:19.638063 IP (tos 0x60, ttl 126, id 0, offset 0, flags [DF], prot
o TCP (6), length 590)
    142.250.98.138.80 > 172.17.0.2.42790: Flags [P.], cksum 0x1f2e (cor
rect), seq 1:539, ack 86, win 256, options [nop,nop,TS val 1103312271 e
cr 1579382374], length 538: HTTP, length: 538
        HTTP/1.1 301 Moved Permanently
        Location: https://opensource.google/
        Content-Type: text/html; charset=UTF-8
        X-Content-Type-Options: nosniff
        Date: Sun, 06 Oct 2024 01:21:19 GMT
        Expires: Sun, 06 Oct 2024 01:51:19 GMT
        Cache-Control: public, max-age=1800
        Server: sffe
        Content-Length: 223
        X-XSS-Protection: 0

        <HTML><HEAD><meta http-equiv="content-type" content="text/html;
charset=utf-8">
        <TITLE>301 Moved</TITLE></HEAD><BODY>
        <H1>301 Moved</H1>
        The document has moved
        <A HREF="https://opensource.google/">here</A>.
```



```
01:21:19.638094 IP (tos 0x0, ttl 64, id 36191, offset 0, flags [DF], pr
oto TCP (6), length 52)
    172.17.0.2.42790 > 142.250.98.138.80: Flags [.], cksum 0x9dbe (inco
rrect -> 0x3d2e), ack 539, win 503, options [nop,nop,TS val 1579382396
ecr 1103312271], length 0
01:21:19.639423 IP (tos 0x0, ttl 64, id 36192, offset 0, flags [DF], pr
oto TCP (6), length 52)
    172.17.0.2.42790 > 142.250.98.138.80: Flags [F.], cksum 0x9dbe (inc
orrect -> 0x3d2c), seq 86, ack 539, win 503, options [nop,nop,TS val 15
79382397 ecr 1103312271], length 0
01:21:19.640250 IP (tos 0x60, ttl 126, id 0, offset 0, flags [DF], prot
o TCP (6), length 52)
    142.250.98.138.80 > 172.17.0.2.42790: Flags [F.], cksum 0x3e20 (cor
rect), seq 539, ack 87, win 256, options [nop,nop,TS val 1103312273 ecr
 1579382397], length 0
analyst@afaffbce9170:~$ sudo tcpdump -nn -r capture.pcap -X
reading from file capture.pcap, link-type EN10MB (Ethernet)
01:21:19.615256 IP 172.17.0.2.42790 > 142.250.98.138.80: Flags [S], seq
 639173906, win 32660, options [mss 1420,sackOK,TS val 1579382373 ecr 0
,nop,wscale 6], length 0
        0x0000:  4500 003c 8d5c 4000 4006 0fc8 ac11 0002  E..<.\@.@....
...
        0x0010:  8efa 628a a726 0050 2619 0512 0000 0000  ..b..&.P&....
...
        0x0020:  a002 7f94 9dc6 0000 0204 058c 0402 080a  ............
...
        0x0030:  5e23 7665 0000 0000 0103 0306            ^#ve........
```

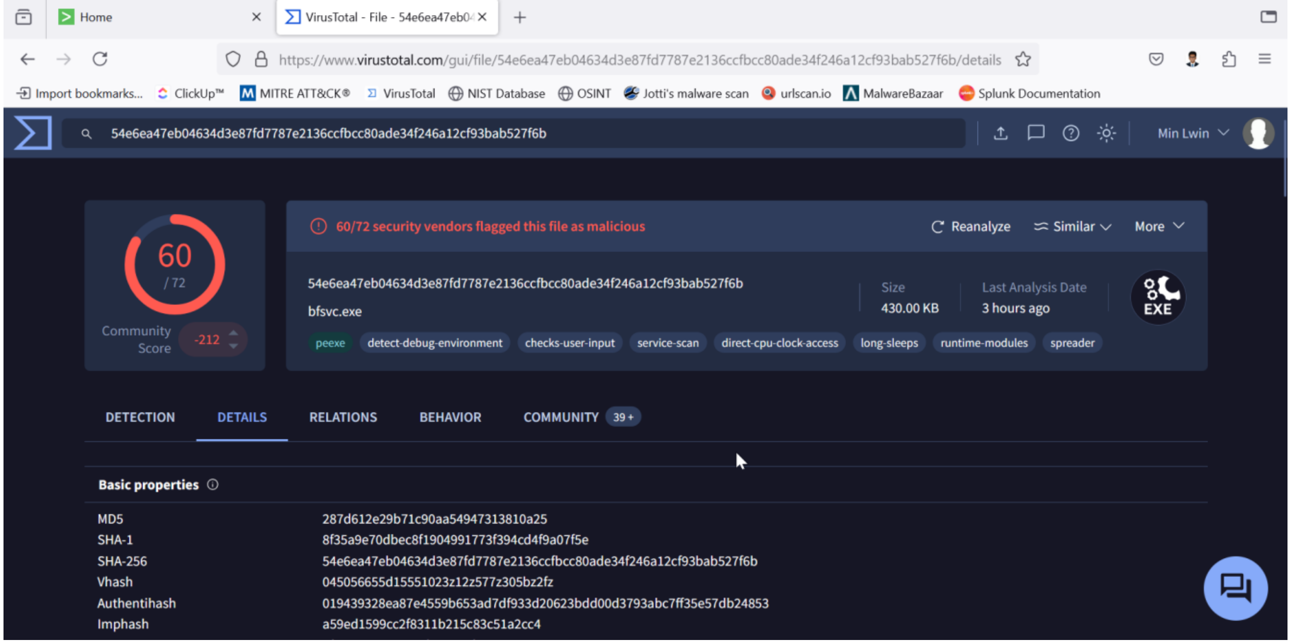


```
cur
        0x0070:  6c2f 372e 3634 2e30 0d0a 4163 6365 7074  l/7.64.0..Acc
ept
        0x0080:  3a20 2a2f 2a0d 0a0d 0a                   :.*/*....
01:21:19.618251 IP 142.250.98.138.80 > 172.17.0.2.42790: Flags [.], ack
 86, win 256, options [nop,nop,TS val 1103312250 ecr 1579382374], lengt
h 0
        0x0000:  4560 0034 0000 4000 7e06 5ecc 8efa 628a  E`.4..@.~.^..
.b.
        0x0010:  ac11 0002 0050 a726 130c 65f0 2619 0568  .....P.&..e.&
..h
        0x0020:  8010 0100 406a 0000 0101 080a 41c3 357a  ....@j......A
.5z
        0x0030:  5e23 7666                                ^#vf
01:21:19.638063 IP 142.250.98.138.80 > 172.17.0.2.42790: Flags [P.], se
q 1:539, ack 86, win 256, options [nop,nop,TS val 1103312271 ecr 157938
2374], length 538: HTTP: HTTP/1.1 301 Moved Permanently
        0x0000:  4560 024e 0000 4000 7e06 5cb2 8efa 628a  E`.N..@.~.\..
.b.
        0x0010:  ac11 0002 0050 a726 130c 65f0 2619 0568  .....P.&..e.&
..h
        0x0020:  8018 0100 1f2e 0000 0101 080a 41c3 358f  ...........A
.5.
        0x0030:  5e23 7666 4854 5450 2f31 2e31 2033 3031  ^#vfHTTP/1.1.
301
        0x0040:  204d 6f76 6564 2050 6572 6d61 6e65 6e74  .Moved.Perman
ent
```



```
01:21:19.638094 IP 172.17.0.2.42790 > 142.250.98.138.80: Flags [.], ack
 539, win 503, options [nop,nop,TS val 1579382396 ecr 1103312271], leng
th 0
        0x0000:  4500 0034 8d5f 4000 4006 0fcd ac11 0002  E..4._@.@....
...
        0x0010:  8efa 628a a726 0050 2619 0568 130c 680a  ..b..&.P&..h.
.h.
        0x0020:  8010 01f7 9dbe 0000 0101 080a 5e23 767c  ...........^
#v|
        0x0030:  41c3 358f                                A.5.
01:21:19.639423 IP 172.17.0.2.42790 > 142.250.98.138.80: Flags [F.], se
q 86, ack 539, win 503, options [nop,nop,TS val 1579382397 ecr 11033122
71], length 0
        0x0000:  4500 0034 8d60 4000 4006 0fcc ac11 0002  E..4.`@.@....
...
        0x0010:  8efa 628a a726 0050 2619 0568 130c 680a  ..b..&.P&..h.
.h.
        0x0020:  8011 01f7 9dbe 0000 0101 080a 5e23 767d  ...........^
#v}
        0x0030:  41c3 358f                                A.5.
01:21:19.640250 IP 142.250.98.138.80 > 172.17.0.2.42790: Flags [F.], se
q 539, ack 87, win 256, options [nop,nop,TS val 1103312273 ecr 15793823
97], length 0
        0x0000:  4560 0034 0000 4000 7e06 5ecc 8efa 628a  E`.4..@.~.^..
.b.
```

Date: July 27 2024	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	For this activity, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious. The file hash has been reported as malicious by over 60 vendors. Upon further investigation, this file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor BlackTech. This incident occurred in the **Detection and Analysis** phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat.
The 5 W's	● **Who**: An unknown malicious actor ● **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ● **Where**: An employee's computer at a financial services company ● **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file ● **Why**: An employee was able to download and execute a malicious file attachment via e-mail.
Additional notes	How can this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on?



60/72 security vendors flagged this file as malicious

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

Size 430.00 KB

Last Analysis Date 3 hours ago

peexe · detect-debug-environment · checks-user-input · service-scan · direct-cpu-clock-access · long-sleeps · runtime-modules · spreader

Basic properties

MD5	287d612e29b71c90aa54947313810a25
SHA-1	8f35a9e70dbec8f1904991773f394cd4f9a07f5e
SHA-256	54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
Vhash	045056655d15551023z12z577z305bz2fz
Authentihash	019439328ea87e4559b653ad7df933d20623bdd00d3793abc7ff35e57db24853
Imphash	a59ed1599cc2f8311b215c83c51a2cc4

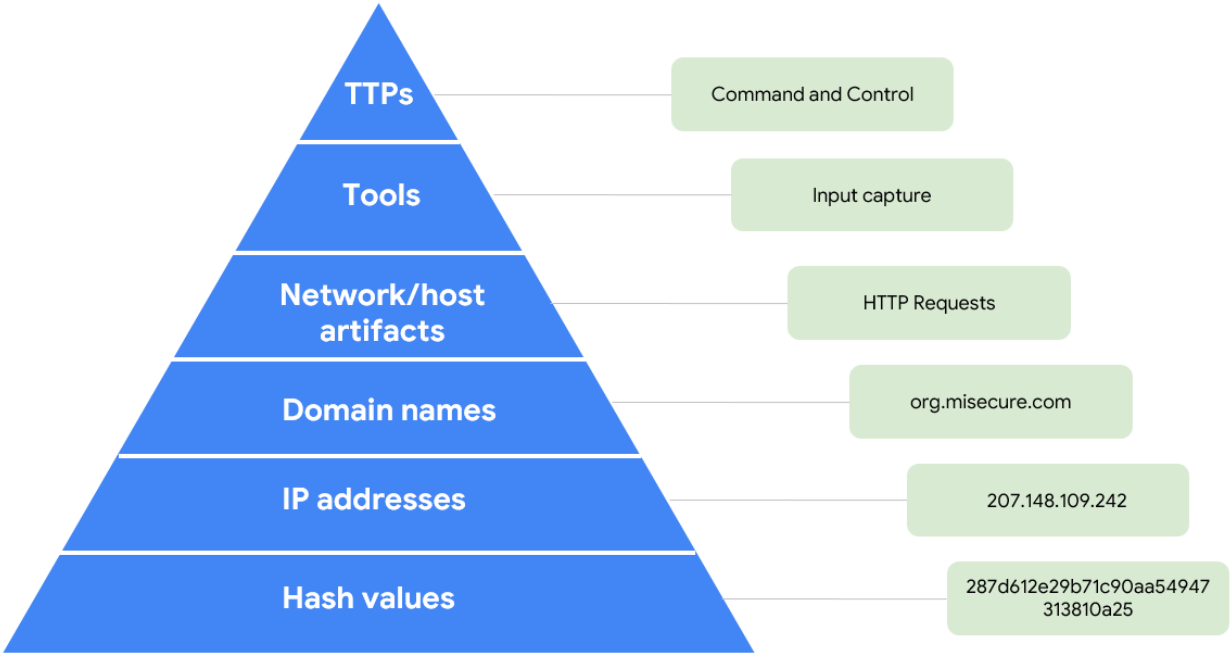


Diagram: Pyramid of Pain

Reflections/Notes:

I really found the activity using tcpdump challenging. I am new to using the command line, and learning the syntax for a tool like tcpdump was a big learning curve. At first, I felt very frustrated because I wasn't getting the right output. I redid the activity and figured out where I went wrong. What I learned from this was to carefully read the instructions and work through the process slowly.

After taking this course, my understanding of incident detection and response has definitely evolved. At the beginning of the course, I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and people; and tools used. Overall, I feel that my understanding has changed, and I am equipped with more knowledge and understanding about incident detection and response.