Incident handler's journal

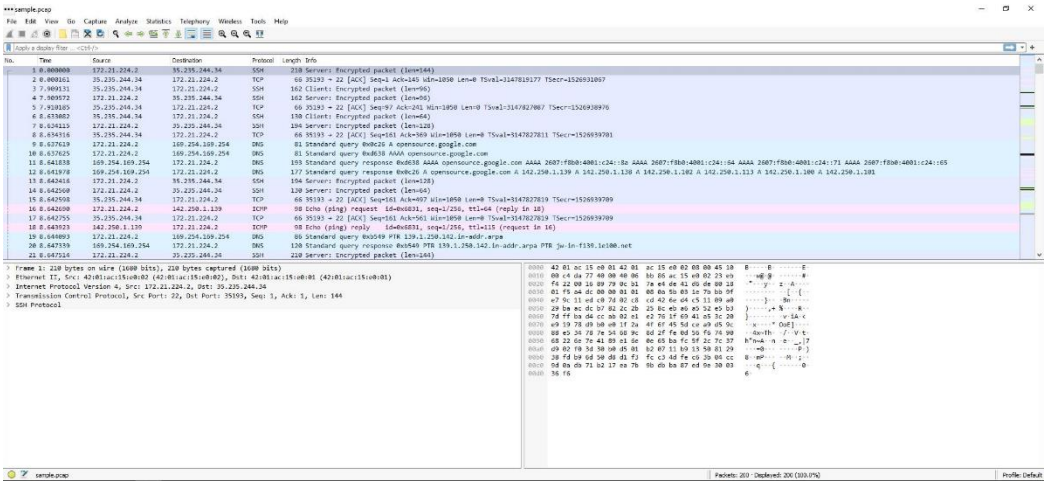
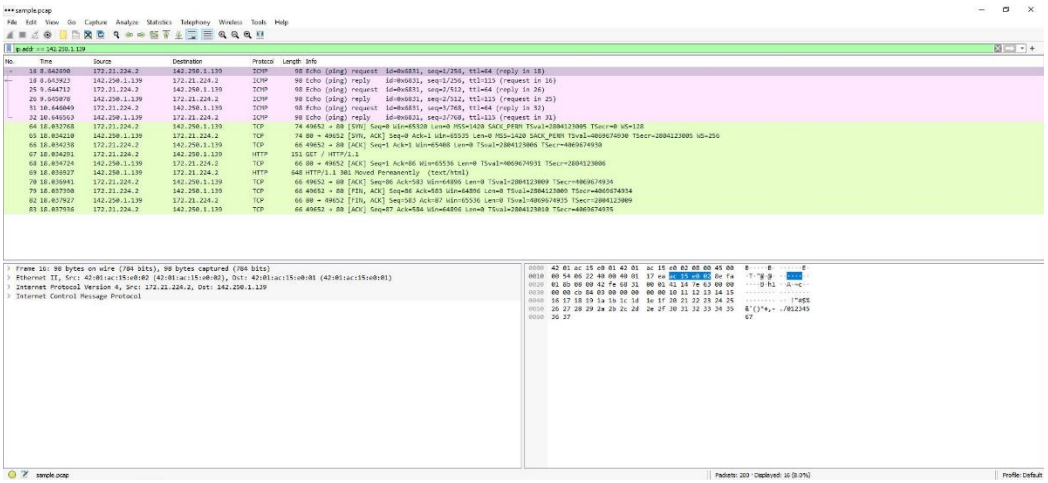
Instructions

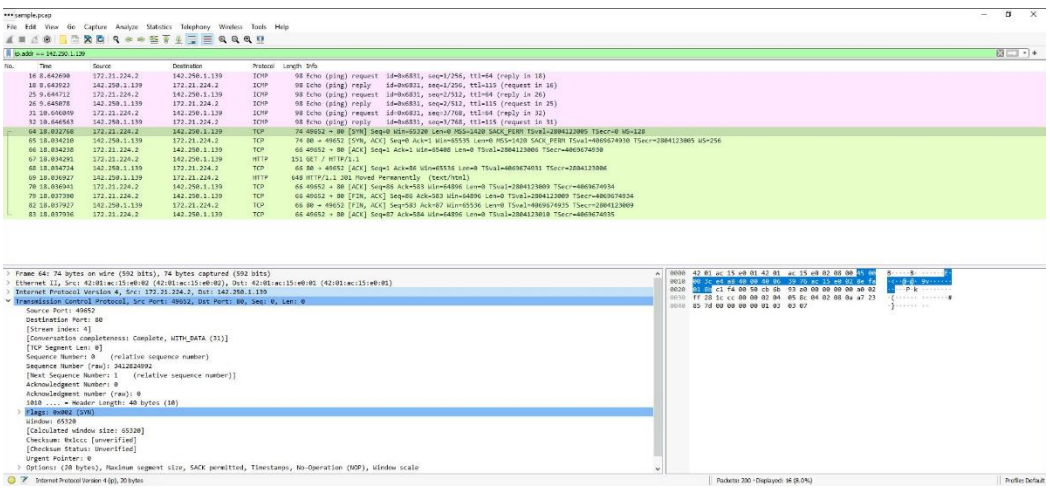
As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 7/24/2023	**Entry:** 1 *"Document an incident with an incident handler's journal"*
Description	**NIST Incident Response Lifecycle Phase:** Detection and Analysis, Containment, Eradication, and Recovery. Ransomware attack occurred on a small U.S. health care clinic. Targeted phishing emails were used to deploy malicious malware onto machines, escalate privilege, and encrypt critical patient files.
Tool(s) used	Not Applicable.
The 5 W's	• **Who**: An organized group of unethical hackers who target organizations in healthcare and transportation industries. • **What**: A ransomware attack was conducted on critical patient files, causing business operations to shut down. • **When**: Incident occurred on Tuesday at 9:00 a.m. • **Where**: Incident occurred at a small U.S. health clinic specializing in delivering primary-care services. • **Why**: The incident occurred because the organized group of unethical hackers were able to gain privileged access by conducting a campaign of targeting phishing emails on employees. Once the employees ran the malicious program in the email, the hackers were able to escalate their privileges to view and

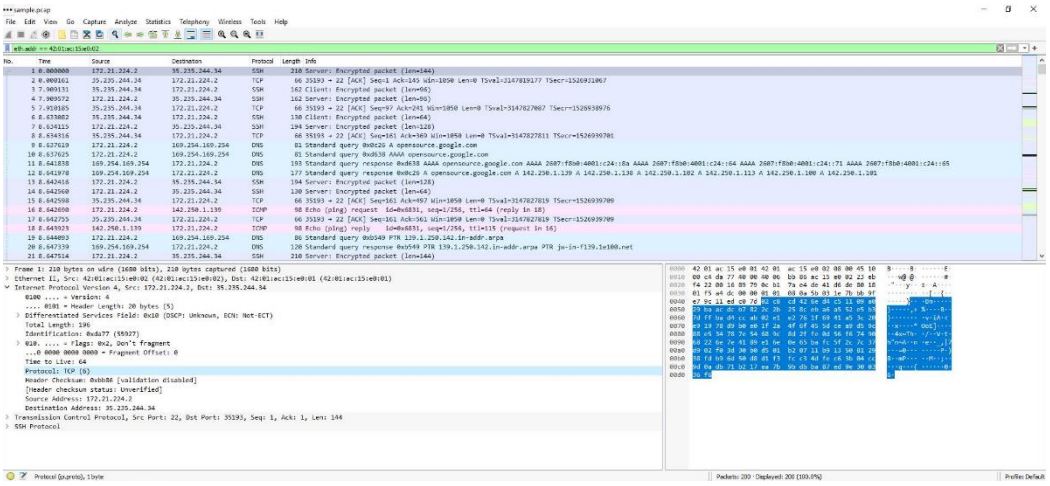
	encrypt patient files, rendering the business inoperable. The attacker's goal was to profit as the ransom note demanded a large sum of money and in return, they will provide the decryption key for the files.
Additional notes	1. **Note:** Deploy security awareness training for all emails. Email phishing campaigns can appear legitimate but often they can be flagged with common sense. 2. **Question:** Can some organizations reverse the encryption and decrypt themselves? Drawback of this would be time and money expended but maybe there are some scenarios (like a good tool or team) where this is feasible. 3. **Question:** They must pay the ransom or report it to law enforcement, correct? Then maybe law enforcement can expend their resources to help?

Date: 7/26/2023	**Entry:** 2 *"Analyze your first packet"*
Description	**NIST Incident Response Lifecycle Phase:** Detection and Analysis. As a security analyst, it is important that I analyze network traffic to better understand the type of traffic that is being sent to and from the systems on the networks. I will further develop my skills in packet analysis by leveraging Wireshark, a valuable tool in the cybersecurity arsenal. While I have experience in this area from previous cybersecurity courses and self-motivated pursuits, I find immense pleasure in refining this skill through this course.
Tool(s) used	• **Wireshark** – a network protocol analyzer that uses a graphical user interface.
The 5 W's	• **Who:** Not applicable. • **What:** Not applicable. • **When:** Not applicable. • **Where:** Not applicable.

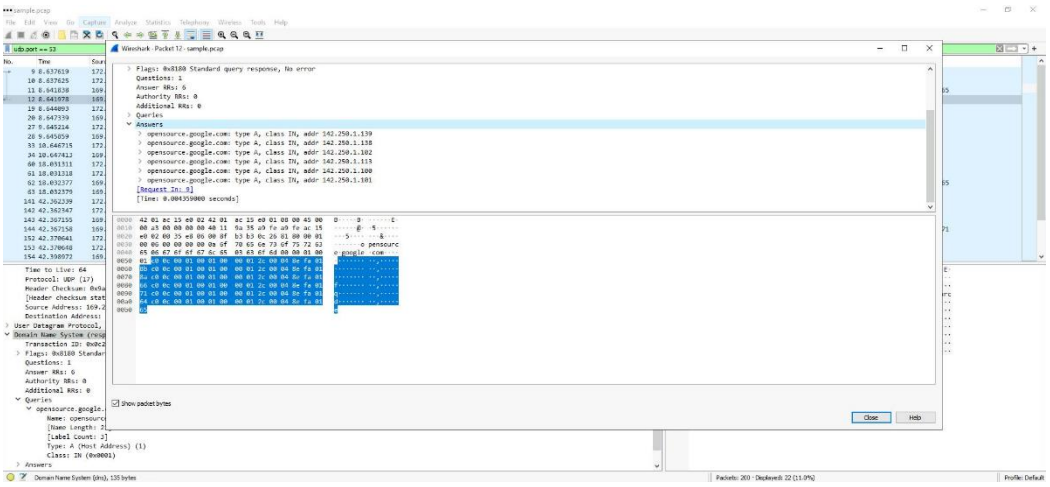
	• **Why:** Not applicable.
Additional notes	**Screenshots:**  *Wireshark – Analyze ICMP*  *Wireshark – Analyze Basic Filter*



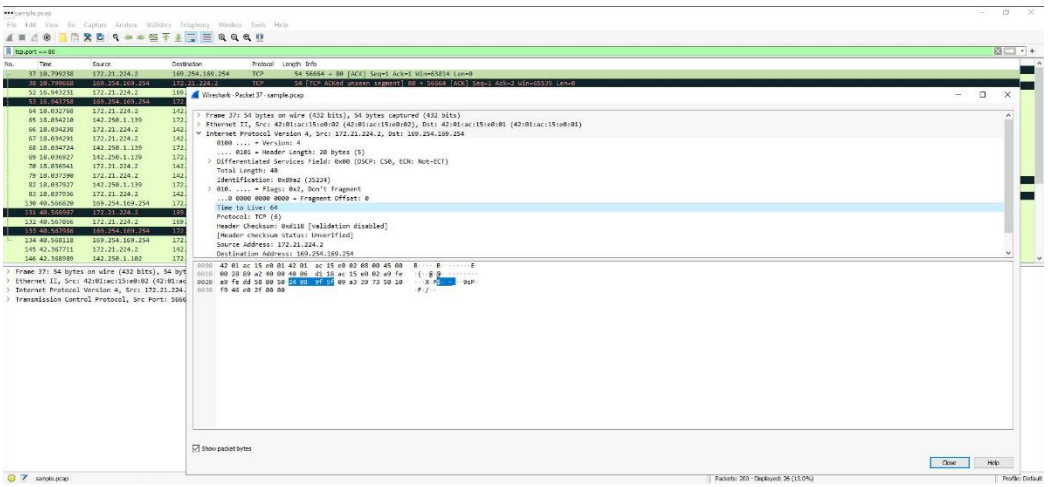
Wireshark – Analyze ip.addr Packets Dst Port 80



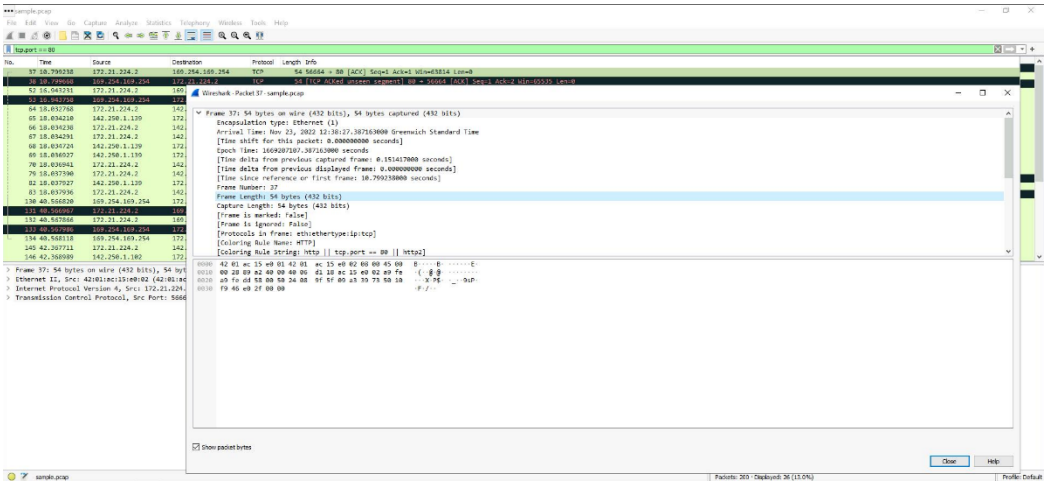
Wireshark – Analyze eth.addr Packets Protocol TCP



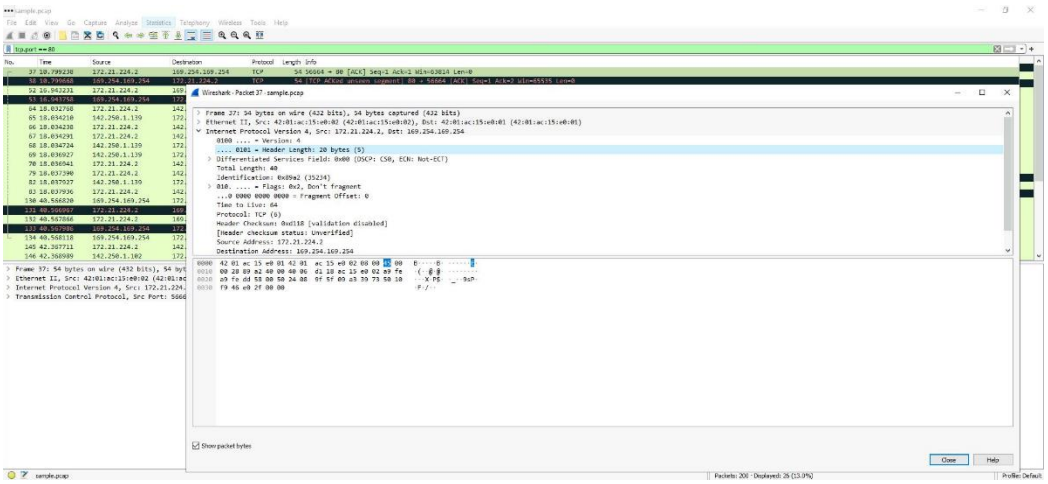
Wireshark – Analyze DNS Packets



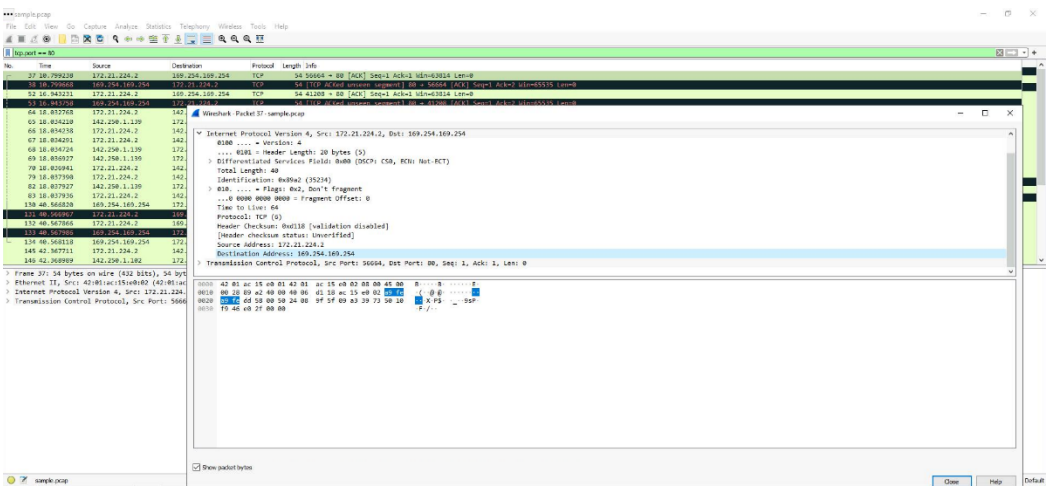
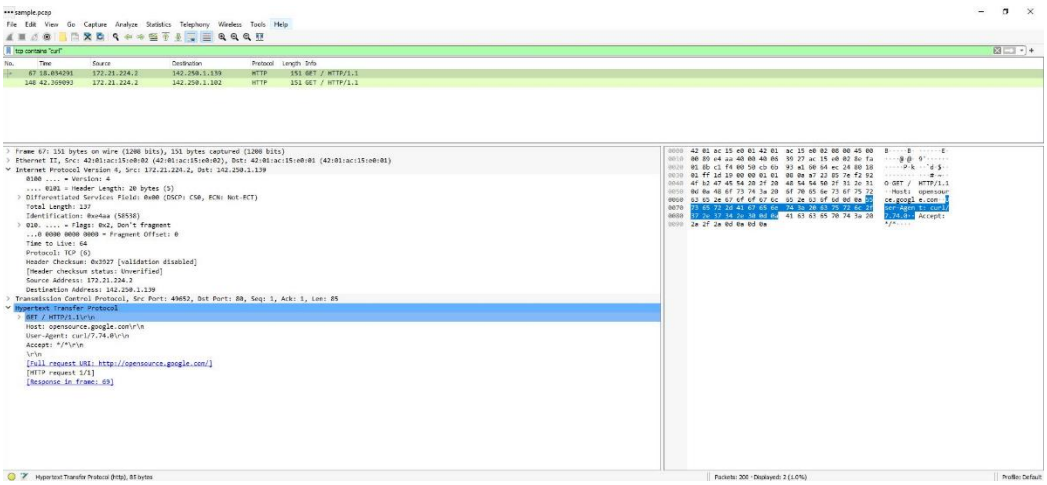
Wireshark – Analyze tcp.port Packets TTL



Wireshark – Analyze tcp.port Packets Frame Length



Wireshark – Analyze tcp.port Packets Header Length

	 *Wireshark – Analyze tcp.port Packets Destination Address*  *Wireshark – Analyze tcp contains "curl"*

Date: 7/26/2023	**Entry:** 3 *"Capture your first packet"*
Description	**NIST Incident Response Lifecycle Phase:** Detection and Analysis. As a security analyst, I must understand how to capture and analyze network traffic using `tcpdump` from a Linux virtual machine. In this activity, I have identified the network interfaces to capture network packet data, used `tcpdump` to filter live network traffic, captured network traffic using `tcpdump`, and filtered the captured

	packet data. Although I am familiar with using the command-line interface for Linux commands, using it to capture and filter network traffic was new to me. I encountered a few obstacles, but after some time I was able to complete this activity and add `tcpdump` to my tool belt.
Tool(s) used	• **`tcpdump`** – a network protocol analyzer that's accessed using the command-line interface.
The 5 W's	• **Who:** Not applicable. • **What:** Not applicable. • **When:** Not applicable. • **Where:** Not applicable. • **Why:** Not applicable.

Additional notes	**Screenshots:**
	`analyst@3843705cfb5f:~$ 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 618  bytes 13658595 (13.0 MiB)`
	`RX errors 0  dropped 0  overruns 0  frame 0`
	`TX packets 450  bytes 38975 (38.0 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 57  bytes 8381 (8.1 KiB)`
	`RX errors 0  dropped 0  overruns 0  frame 0`
	`TX packets 57  bytes 8381 (8.1 KiB)`
	`TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0`
	tcpdump – ifconfig
	`analyst@3843705cfb5f:~$ 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)`
	tcpdump – Interface Options

```
analyst@3843705cfb5f:~$ sudo tcpdump -i eth0 -v -c5
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:53:08.148139 IP (tos 0x0, ttl 64, id 23195, offset 0, flags [DF], proto TCP (6), length 113)
    3843705cfb5f.5000 > nginx-us-east1-c.c.qwiklabs-terminal-vms-prod-00.internal.35656: Flags [P.], cksum 0x588e (incorrect -> 0x02dd), seq 270396947:27
0397008, ack 750879717, win 501, options [nop,nop,TS val 1299370470 ecr 2796834067], length 61
19:53:08.148456 IP (tos 0x0, ttl 63, id 26117, offset 0, flags [DF], proto TCP (6), length 52)
    nginx-us-east1-c.c.qwiklabs-terminal-vms-prod-00.internal.35656 > 3843705cfb5f.5000: Flags [.], cksum 0xbb13 (correct), ack 61, win 507, options [nop
,nop,TS val 2796834193 ecr 1299370470], length 0
19:53:08.158882 IP (tos 0x0, ttl 64, id 23196, offset 0, flags [DF], proto TCP (6), length 146)
    3843705cfb5f.5000 > nginx-us-east1-c.c.qwiklabs-terminal-vms-prod-00.internal.35656: Flags [P.], cksum 0x58af (incorrect -> 0x3b46), seq 61:155, ack
1, win 501, options [nop,nop,TS val 1299370481 ecr 2796834193], length 94
19:53:08.159232 IP (tos 0x0, ttl 63, id 26118, offset 0, flags [DF], proto TCP (6), length 52)
    nginx-us-east1-c.c.qwiklabs-terminal-vms-prod-00.internal.35656 > 3843705cfb5f.5000: Flags [.], cksum 0xba9f (correct), ack 155, win 507, options [no
p,nop,TS val 2796834204 ecr 1299370481], length 0
19:53:08.180552 IP (tos 0x0, ttl 64, id 32375, offset 0, flags [DF], proto UDP (17), length 69)
    3843705cfb5f.49582 > metadata.google.internal.domain: 19030+ PTR? 2.0.21.172.in-addr.arpa. (41)
5 packets captured
8 packets received by filter
0 packets dropped by kernel
```

tcpdump – Inspect Network Traffic

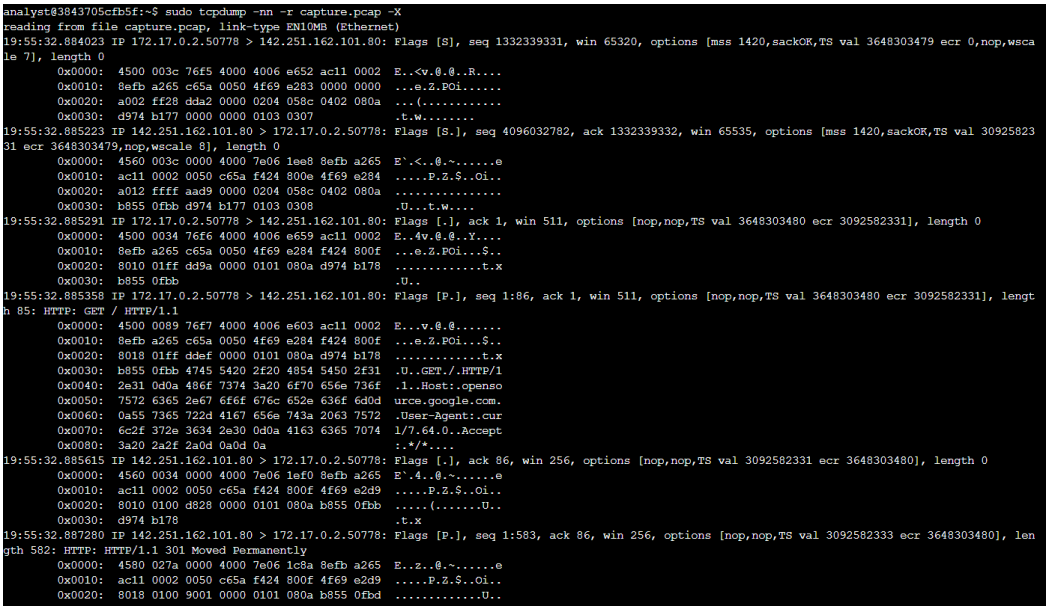
```
analyst@3843705cfb5f:~$ sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &
[1] 12757
analyst@3843705cfb5f:~$ tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
curl opensource.google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://opensource.google/">here</A>.
</BODY></HTML>
analyst@3843705cfb5f:~$ 9 packets captured
10 packets received by filter
0 packets dropped by kernel
ls -l capture.pcap
-rw-r--r-- 1 root root 1445 Jul 26 19:55 capture.pcap
[1]+  Done                    sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap
```

tcpdump – Capture Network Traffic

```
analyst@3843705cfb5f:~$ sudo tcpdump -nn -r capture.pcap -v
reading from file capture.pcap, link-type EN10MB (Ethernet)
19:55:32.884023 IP (tos 0x0, ttl 64, id 30453, offset 0, flags [DF], proto TCP (6), length 60)
    172.17.0.2.50778 > 142.251.162.101.80: Flags [S], cksum 0xdda2 (incorrect -> 0xe806), seq 1332339331, win 65320, options [mss 1420,sackOK,TS val 3648
303479 ecr 0,nop,wscale 7], length 0
19:55:32.885223 IP (tos 0x60, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    142.251.162.101.80 > 172.17.0.2.50778: Flags [S.], cksum 0xaad9 (correct), seq 4096032782, ack 1332339332, win 65535, options [mss 1420,sackOK,TS val
 3092582331 ecr 3648303479,nop,wscale 8], length 0
19:55:32.885291 IP (tos 0x0, ttl 64, id 30454, offset 0, flags [DF], proto TCP (6), length 52)
    172.17.0.2.50778 > 142.251.162.101.80: Flags [.], cksum 0xdd9a (incorrect -> 0xd77e), ack 1, win 511, options [nop,nop,TS val 3648303480 ecr 30925823
31], length 0
19:55:32.885358 IP (tos 0x0, ttl 64, id 30455, offset 0, flags [DF], proto TCP (6), length 137)
    172.17.0.2.50778 > 142.251.162.101.80: Flags [P.], cksum 0xddef (incorrect -> 0x4632), seq 1:86, ack 1, win 511, options [nop,nop,TS val 3648303480 e
cr 3092582331], length 85: HTTP, length: 85
        GET / HTTP/1.1
        Host: opensource.google.com
        User-Agent: curl/7.64.0
        Accept: */*

19:55:32.885615 IP (tos 0x60, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    142.251.162.101.80 > 172.17.0.2.50778: Flags [.], cksum 0xd828 (correct), ack 86, win 256, options [nop,nop,TS val 3092582331 ecr 3648303480], length
 0
19:55:32.887280 IP (tos 0x80, ttl 126, id 0, offset 0, flags [DF], proto TCP (6), length 634)
    142.251.162.101.80 > 172.17.0.2.50778: Flags [P.], cksum 0x9001 (correct), seq 1:583, ack 86, win 256, options [nop,nop,TS val 3092582333 ecr 3648303
480], length 582: HTTP, length: 582
        HTTP/1.1 301 Moved Permanently
        Location: https://opensource.google/
        Cross-Origin-Resource-Policy: cross-origin
        Content-Type: text/html; charset=UTF-8
        X-Content-Type-Options: nosniff
        Date: Wed, 26 Jul 2023 19:55:32 GMT
        Expires: Wed, 26 Jul 2023 20:25:32 GMT
        Cache-Control: public, max-age=1800
```

tcpdump – Filter the Captured Packet Data, Verbose



```
analyst@3843705cfb5f:~$ sudo tcpdump -nn -r capture.pcap -X
reading from file capture.pcap, link-type EN10MB (Ethernet)
19:55:32.884023 IP 172.17.0.2.50778 > 142.251.162.101.80: Flags [S], seq 1332339331, win 65320, options [mss 1420,sackOK,TS val 3648303479 ecr 0,nop,wsca
le 7], length 0
        0x0000:  4500 003c 76f5 4000 4006 e652 ac11 0002  E..<v.@.@..R....
        0x0010:  8efb a265 c65a 0050 4f69 e283 0000 0000  ...e.Z.POi......
        0x0020:  a002 ff28 dda2 0000 0204 058c 0402 080a  ...(............
        0x0030:  d974 b177 0000 0000 0103 0307            .t.w........
19:55:32.885223 IP 142.251.162.101.80 > 172.17.0.2.50778: Flags [S.], seq 4096032782, ack 1332339332, win 65535, options [mss 1420,sackOK,TS val 30925823
31 ecr 3648303479,nop,wscale 8], length 0
        0x0000:  4560 003c 0000 4000 7e06 1ee8 8efb a265  E`.<..@.~......e
        0x0010:  ac11 0002 0050 c65a f424 800e 4f69 e284  .....P.Z.$..Oi..
        0x0020:  a012 ffff aad9 0000 0204 058c 0402 080a  ................
        0x0030:  b855 0fbb d974 b177 0103 0308            .U...t.w....
19:55:32.885291 IP 172.17.0.2.50778 > 142.251.162.101.80: Flags [.], ack 1, win 511, options [nop,nop,TS val 3648303480 ecr 3092582331], length 0
        0x0000:  4500 0034 76f6 4000 4006 e659 ac11 0002  E..4v.@.@..Y....
        0x0010:  8efb a265 c65a 0050 4f69 e284 f424 800f  ...e.Z.POi...$..
        0x0020:  8010 01ff dd9a 0000 0101 080a d974 b178  .............t.x
        0x0030:  b855 0fbb                                .U..
19:55:32.885358 IP 172.17.0.2.50778 > 142.251.162.101.80: Flags [P.], seq 1:86, ack 1, win 511, options [nop,nop,TS val 3648303480 ecr 3092582331], lengt
h 85: HTTP: GET / HTTP/1.1
        0x0000:  4500 0089 76f7 4000 4006 e603 ac11 0002  E...v.@.@.......
        0x0010:  8efb a265 c65a 0050 4f69 e284 f424 800f  ...e.Z.POi...$..
        0x0020:  8018 01ff ddef 0000 0101 080a d974 b178  .............t.x
        0x0030:  b855 0fbb 4745 5420 2f20 4854 5450 2f31  .U..GET./.HTTP/1
        0x0040:  2e31 0d0a 486f 7374 3a20 6f70 656e 736f  .1..Host:.openso
        0x0050:  7572 6365 2e67 6f6f 676c 652e 636f 6d0d  urce.google.com.
        0x0060:  0a55 7365 722d 4167 656e 743a 2063 7572  .User-Agent:.cur
        0x0070:  6c2f 372e 3634 2e30 0d0a 4163 6365 7074  l/7.64.0..Accept
        0x0080:  3a20 2a2f 2a0d 0a0d 0a                   :.*/*....
19:55:32.885615 IP 142.251.162.101.80 > 172.17.0.2.50778: Flags [.], ack 86, win 256, options [nop,nop,TS val 3092582331 ecr 3648303480], length 0
        0x0000:  4560 0034 0000 4000 7e06 1ef0 8efb a265  E`.4..@.~......e
        0x0010:  ac11 0002 0050 c65a f424 800f 4f69 e2d9  .....P.Z.$..Oi..
        0x0020:  8010 0100 d828 0000 0101 080a b855 0fbb  .....(.......U..
        0x0030:  d974 b178                                .t.x
19:55:32.887280 IP 142.251.162.101.80 > 172.17.0.2.50778: Flags [P.], seq 1:583, ack 86, win 256, options [nop,nop,TS val 3092582333 ecr 3648303480], len
gth 582: HTTP: HTTP/1.1 301 Moved Permanently
        0x0000:  4580 027a 0000 4000 7e06 1c8a 8efb a265  E..z..@.~......e
        0x0010:  ac11 0002 0050 c65a f424 800f 4f69 e2d9  .....P.Z.$..Oi..
        0x0020:  8018 0100 9001 0000 0101 080a b855 0fbd  ............U..
```

tcpdump – Filter the Captured Packet Data, Hexadecimal and ASCII

Date: 7/25/2023	**Entry:** 4 *"Investigate a suspicious file hash"*
Description	**NIST Incident Response Lifecycle Phase:** Detection and Analysis. An employee opened a malicious spreadsheet sent to them via email. The spreadsheet was locked, and the password was provided in the email. The employee downloaded the spreadsheet and opened the file with the password. Then a malicious payload was executed. Upon further investigation using VirusTotal, this is a trojan virus called Flagpro.
Tool(s) used	• **SHA256 file hash** – used to verify file integrity. • **VirusTotal** – used to investigate the file hash and analyze the malicious file.
The 5 W's	• **Who:** The incident is caused by unknown threat actors. The employee initiated the attack unwittingly.

	• **What:** A malicious payload was sent to an employee in an email. The employee executed the file. The SHA256 file hash is: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. • **When:** 1:11 p.m. the employee received the email. By 1:20 p.m. the IDS detects the payload and sends out an alert to the SOC. • **Where:** The incident happened at a financial services company. The employee's computer was compromised via a malicious file download from an email. • **Why:** The incident occurred to deploy a malicious payload. Upon further investigation, the payload was determined to be "trojan.flagpro/jaik". The file is flagged by 56 security vendors and 2 sandboxes as malicious. The intent of this trojan is to gain access to install a backdoor into the system for an unknown malicious objective in the future.
Additional notes	1. **Note:** Deploy security awareness training for all emails. Email phishing campaigns can appear legitimate, but often times they can be flagged with common sense. 2. **Question:** Are there certain tools that can reside on to scan email servers for files sent and block those files from being delivered to the employee? This can help in case the employee training does not prevent the incident. 3. **Question:** What goals can occur after the backdoor is created? Endless possibilities? What is the likelihood that the backdoor could be stumbled upon by an employee?

Date: 7/25/2023	**Entry:** 5 *"Use a playbook to respond to an attack"*
Description	**NIST Incident Response Lifecycle Phase:** Detection and Analysis.

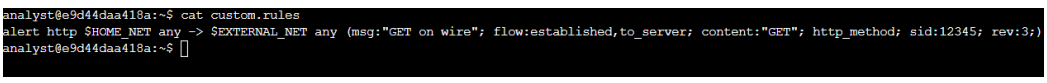
	An alert ticket, A-2703, has been generated with the message, “SERVER-MAIL Phishing attempt possible download of malware” and an alert severity of medium. The HR department received an email with the subject “Re: Infrastructure Egnieer Role” from an email account by the name of “Def Communications”, email address “76tguyhh6tgftrt7tg.su”, and IP address “114.114.114.114”. The contents of the email express interest in the engineer role posted online signed by “Clyde West”. The attachment provided in the email is said to be a resume and cover letter and to be password protected. The password is provided in the email and the filename is “bfsvc.exe”. In the email subject, there is a grammatical error, the name of sender does not match email address, and the email address is unusual. The filetype is also an executable with uncommon naming conventions. Having previously investigated the hash file for the downloaded file (see Entry #2), I have confirmed this is a malicious file. I have changed the status of this ticket to “Escalated” for further action by SOC analyst level II.
Tool(s) used	• **Alert ticket** – used to track ticket details and change ticket status. • **Phishing Playbook** – used to determine if file is malicious and if escalation is needed. • **Phishing Flowchart** – used to determine if file is malicious and if escalation is needed. • **SHA256 file hash** – used to verify file integrity. • **VirusTotal** – used to investigate the file hash and analyze the malicious file.
The 5 W's	• **Who:** The incident is caused by threat actors Misecure and BlackTech. The HR employee initiated the attack unknowingly. The email address used was “76tguyhh6tgftrt7tg.su”. • **What:** A malicious file was sent to an HR employee in a phishing email. The employee executed the file. • **When:** At 9:30 a.m. the phishing attempt was sent to the HR department. At 1:11 p.m. an HR employee opened the email. By 1:20 p.m. the IDS detects the payload and sends out an alert to the SOC.

	• **Where:** The incident happened at a financial services company. The employee's computer was compromised via a malicious file download from an email. • **Why:** The incident occurred to deploy a malicious payload. Upon further investigation, the payload was determined to be "trojan.flagpro/jaik". The file is flagged by 56 security vendors and 2 sandboxes as malicious. The intent of this trojan is to gain access to install a backdoor into the system for an unknown malicious objective in the future.
Additional notes	• **Note:** Deploy security awareness training for all emails. Email phishing campaigns can appear legitimate, but often times they can be flagged with common sense. • **Question:** Are there certain tools that can reside on to scan email servers for files sent and block those files from being delivered to the employee? This can help in case the employee training does not prevent the incident. • **Question:** What goals can occur after the backdoor is created? Endless possibilities? What is the likelihood that the backdoor could be stumbled upon by an employee?

Date: 7/25/2023	**Entry:** 6 *"Review a final report"*
Description	**NIST Incident Response Lifecycle Phase:** Post Incident Activity. An employee received an email from an outside source. The sender provided evidence of collected customer PII and financial data and presented a ransom note in cryptocurrency payment of $50,000. After investigating, the attacker used a forced browsing attack on the e-commerce web application to obtain order information for approximately 50,000 customers.

Tool(s) used	• **Incident Final Report** – used to review the full incident as part of the lessons learned & post incident review.
The 5 W's	● **Who:** An attacker who conducted a forced browsing attack on the e-commerce web application. ● **What:** An employee received an email from an outside source. The sender claimed they stole customer data, then requested a payment of $25,000 in cryptocurrency. The sender claimed they stole customer data, then requested a payment of $25,000 in cryptocurrency. On December 28, 2022, the same sender provided evidence of the collected data and increased the ransom to $50,000. From a vulnerability in the e-commerce web application, the attacked conducted a forced browsing attack, a form of injection attack, to view customer transaction data. The attacker modified the order number within the URL string of a purchase confirmation page. The incident was so severe, the Public Relations department was brought in to help disclose the data theft to its customers. Free identity protection was offered to affected customers. This individual gained unauthorized access to customer PII and financial information. Approximately 50,000 customer records were affected. ● **When:** At 3:13 p.m. PST, on December 22, 2022, an employee received an email from an outside source. On December 28, 2022, the same sender provided evidence of the collected data and increased the ransom to $50,000. On that same day, at 7:20 p.m., the incident was sent to the security team to begin their investigation. The investigation occurred between December 28, 2022, through December 31, 2022. ● **Where:** At a mid-sized retail company that conducts 80% of its business online. ● **Why:** The incident occurred due to a vulnerability in the e-commerce web application. The web application was vulnerable to forced browsing attacks. The incentive of the attacker was strictly monetary, as a ransom note for $50,000 in cryptocurrency was sent to an employee.
Additional notes	• **Note:** Implement secure coding practices. Dynamic and static code analysis of the e-commerce website can help identify vulnerabilities.

	• **Question:** Is the company forced to pay this amount in this scenario? Or is the data released, and the company performs damage control? Perhaps it is which is less expensive, damage control of leaking data vs paying the $50,000 of cryptocurrency.

Date: 7/26/2023	**Entry:** 7 *"Explore signatures and logs with Suricata"*
Description	**NIST Incident Response Lifecycle Phase:** Detection and Analysis, and Post Incident Activity. As a security analyst, I reviewed custom rules in Suricata, ran them, and examined the output logs in the `fast.log` file. Additionally, I examined the additional output that Suricata generated in the standard `eve.json` log file. With Suricata, I was able to gain new technical skills and knowledge required to be effective in monitoring and analyzing network traffic for potential security threats.
Tool(s) used	• **Suricata** – an open-source intrusion detection system (IDS), intrusion prevention system (IPS), and network analysis tool.
The 5 W's	• **Who:** Not Applicable. • **What:** Not Applicable. • **When:** Not Applicable. • **Where:** Not Applicable. • **Why:** Not Applicable.
Additional notes	**Screenshots:**  *Suricata – Review Custom Rule*

```
analyst@e9d44daa418a:~$ ls -l /var/log/suricata
total 0
analyst@e9d44daa418a:~$ sudo suricata -r sample.pcap -S custom.rules -k none
26/7/2023 -- 17:59:58 - <Notice> - This is Suricata version 6.0.1 RELEASE running in USER mode
26/7/2023 -- 17:59:59 - <Notice> - all 2 packet processing threads, 4 management threads initialized, engine started.
26/7/2023 -- 17:59:59 - <Notice> - Signal Received.  Stopping engine.
26/7/2023 -- 17:59:59 - <Notice> - Pcap-file module read 1 files, 200 packets, 54238 bytes
analyst@e9d44daa418a:~$ ls -l /var/log/suricata
total 16
-rw-r--r-- 1 root root 1418 Jul 26 17:59 eve.json
-rw-r--r-- 1 root root  292 Jul 26 17:59 fast.log
-rw-r--r-- 1 root root 3239 Jul 26 17:59 stats.log
-rw-r--r-- 1 root root 1512 Jul 26 17:59 suricata.log
analyst@e9d44daa418a:~$
```

Suricata – Run Custom Rule

```
analyst@e9d44daa418a:~$ cat /var/log/suricata/fast.log
11/23/2022-12:38:34.624866  [**] [1:12345:3] GET on wire [**] [Classification: (null)] [Priority: 3] {TCP} 172.21.224.2:49652 -> 142.250.1.139:80
11/23/2022-12:38:58.958203  [**] [1:12345:3] GET on wire [**] [Classification: (null)] [Priority: 3] {TCP} 172.21.224.2:58494 -> 142.250.1.102:80
analyst@e9d44daa418a:~$
```

Suricata – Examine fast.log

```
analyst@e9d44daa418a:~$ cat /var/log/suricata/eve.json
{"timestamp":"2022-11-23T12:38:34.624866+0000","flow_id":1083659243911317,"pcap_cnt":70,"event_type":"alert","src_ip":"172.21.224.2","src_port":49652,"de
st_ip":"142.250.1.139","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":12345,"rev":3,"signature":"GET on wire",
"category":"","severity":3},"http":{"hostname":"opensource.google.com","url":"/","http_user_agent":"curl/7.74.0","http_content_type":"text/html","http_me
thod":"GET","protocol":"HTTP/1.1","status":301,"redirect":"https://opensource.google/","length":223},"app_proto":"http","flow":{"pkts_toserver":4,"pkts_t
oclient":3,"bytes_toserver":357,"bytes_toclient":788,"start":"2022-11-23T12:38:34.620693+0000"}}
{"timestamp":"2022-11-23T12:38:58.958203+0000","flow_id":310000344012020,"pcap_cnt":151,"event_type":"alert","src_ip":"172.21.224.2","src_port":58494,"de
st_ip":"142.250.1.102","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":12345,"rev":3,"signature":"GET on wire",
"category":"","severity":3},"http":{"hostname":"opensource.google.com","url":"/","http_user_agent":"curl/7.74.0","http_content_type":"text/html","http_me
thod":"GET","protocol":"HTTP/1.1","status":301,"redirect":"https://opensource.google/","length":223},"app_proto":"http","flow":{"pkts_toserver":4,"pkts_t
oclient":3,"bytes_toserver":357,"bytes_toclient":797,"start":"2022-11-23T12:38:58.955636+0000"}}
```

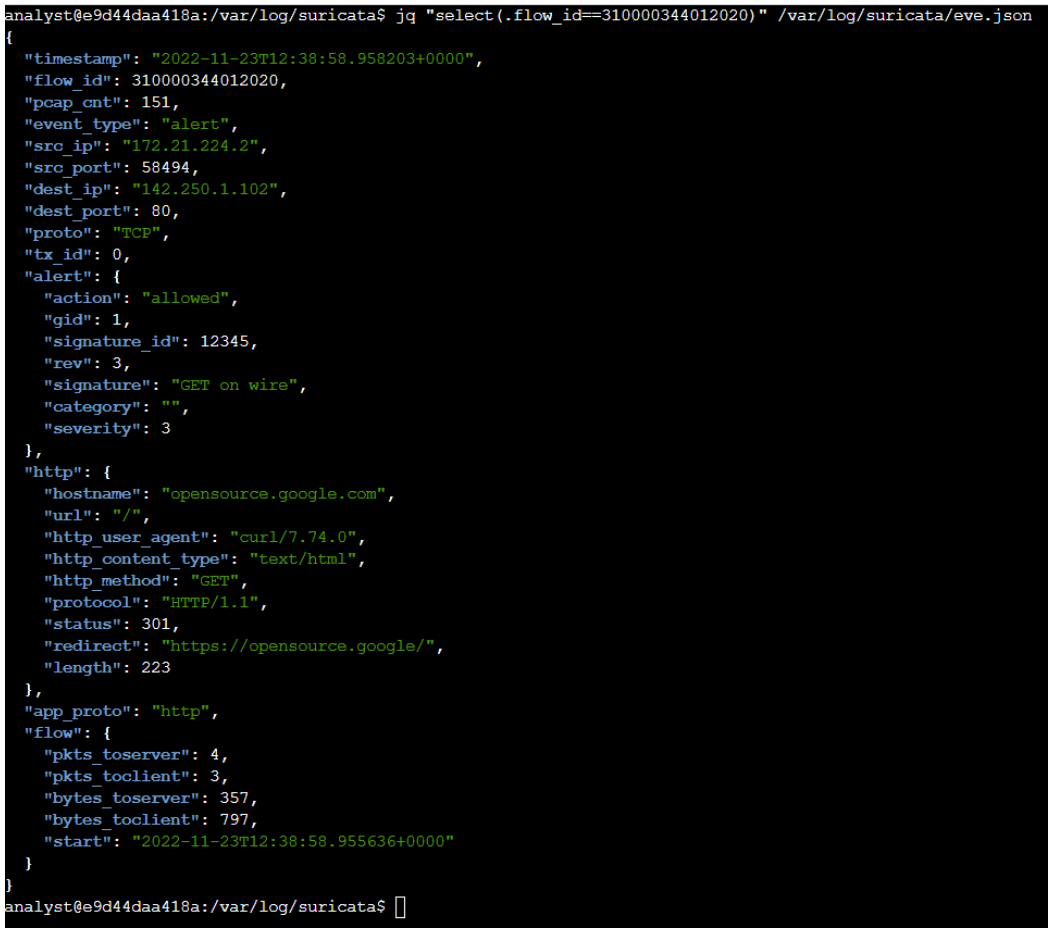
Suricata – Examine eve.json Raw Content

```
analyst@e9d44daa418a:~$ jq . /var/log/suricata/eve.json | less
{
  "timestamp": "2022-11-23T12:38:34.624866+0000",
  "flow_id": 1083659243911317,
  "pcap_cnt": 70,
  "event_type": "alert",
  "src_ip": "172.21.224.2",
  "src_port": 49652,
  "dest_ip": "142.250.1.139",
  "dest_port": 80,
  "proto": "TCP",
  "tx_id": 0,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 12345,
    "rev": 3,
    "signature": "GET on wire",
    "category": "",
    "severity": 3
  },
  "http": {
    "hostname": "opensource.google.com",
    "url": "/",
    "http_user_agent": "curl/7.74.0",
    "http_content_type": "text/html",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 301,
    "redirect": "https://opensource.google/",
    "length": 223
  },
  "app_proto": "http",
  "flow": {
    "pkts_toserver": 4,
    "pkts_toclient": 3,
    "bytes_toserver": 357,
    "bytes_toclient": 788,
    "start": "2022-11-23T12:38:34.620693+0000"
  }
```

Suricata – Examine eve.json Improved Format

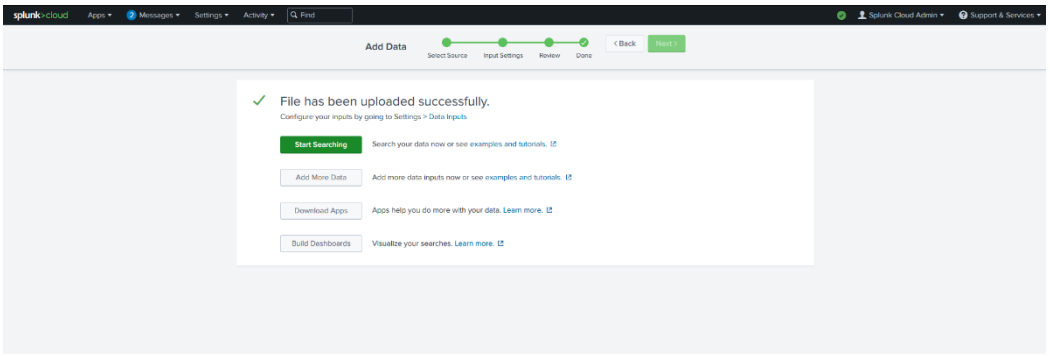
```
analyst@e9d44daa418a:~$ jq -c "[.timestamp,.flow_id,.alert.signature,.proto,.dest_ip]" /var/log/suricata/eve.json
["2022-11-23T12:38:34.624866+0000",1083659243911317,"GET on wire","TCP","142.250.1.139"]
["2022-11-23T12:38:58.958203+0000",310000344012020,"GET on wire","TCP","142.250.1.102"]
```

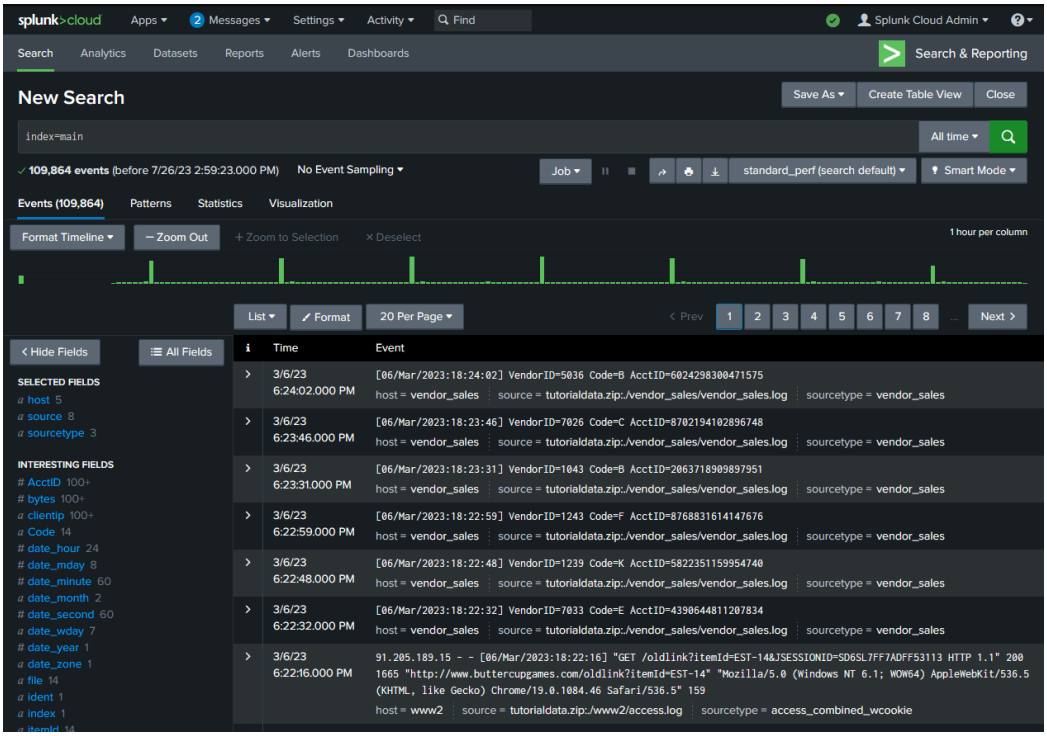
Suricata – Examine eve.json Extract Specific Event Data



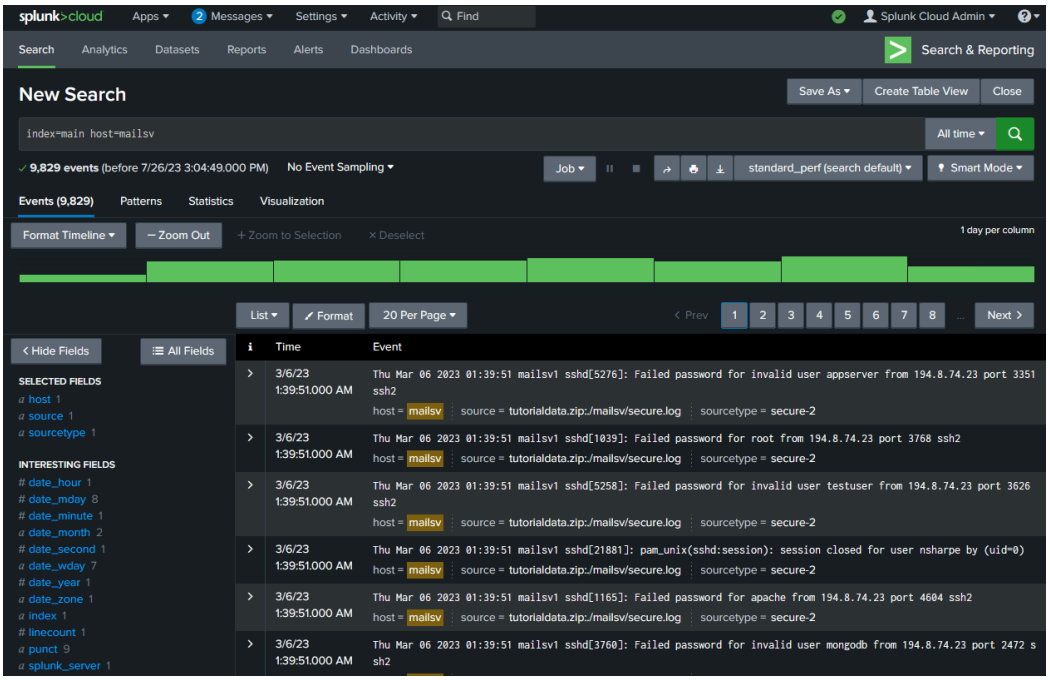
Suricata – Examine eve.json flow_id

Date: 7/26/2023	**Entry:** 8 *"Perform a query with Splunk"*
Description	**NIST Incident Response Lifecycle Phase:** Detection and Analysis. As a security analyst at the e-commerce store Buttercup Games, I have explored failed SSH logins for the root account on the mail server. I have determined that failed SSH login attempts to the root account on the mail server occurred. The incident followed a

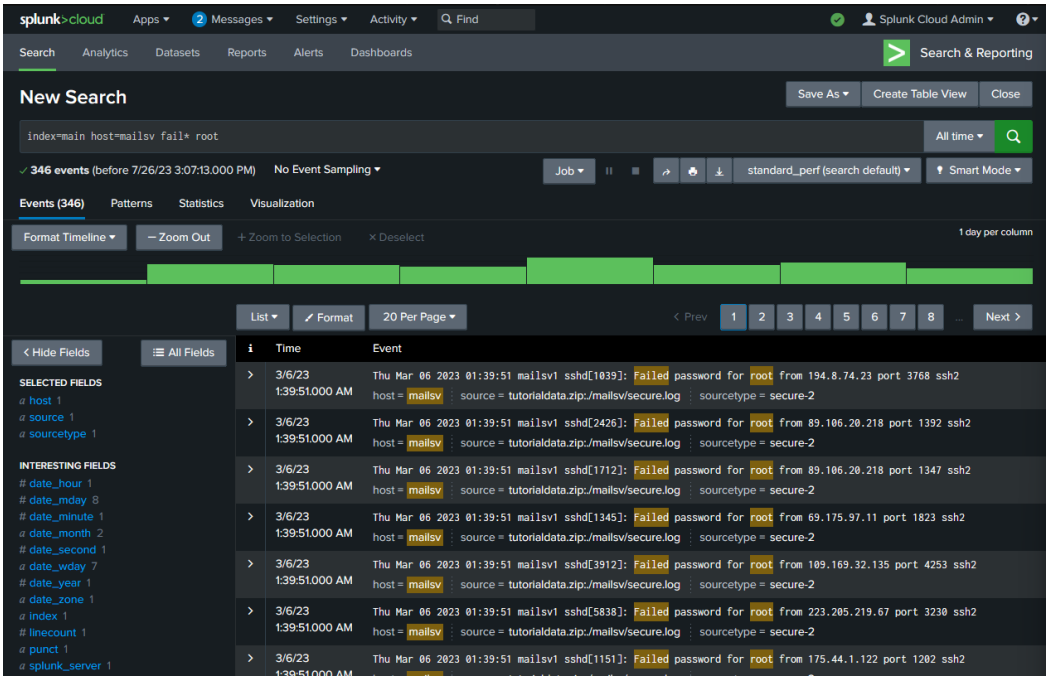
	recurring pattern, happening daily over the course of a week at the same time. Over 100 failed SSH login attempts occurred (346 in total).
Tool(s) used	• **Splunk Cloud** – upload data, perform searches on the data.
The 5 W's	• **Who:** Unknown attacker targeting the root account on the mail server. • **What:** Failed SSH login attempts to the root account on the mail server occurred. The incident followed a recurring pattern, happening daily over the course of a week at the same time. Over 100 failed SSH login attempts occurred (346 in total). • **When:** Daily, from 2/27/2023 and 3/6/2023 failed SSH login attempts occurred at 1:39 a.m. exactly. • **Where:** The incident occurred on the mail server of an e-commerce store, Buttercup Games. • **Why:** The incident occurred as an attempt to gain privileged access on the mail server via SSH. The intents behind this are unclear but we can safely assume the intentions of this was malicious as a large amount of failed SSH logins can be an indicator that someone is attempting a password attack (e.g., brute force, rainbow table, dictionary, etc.).
Additional notes	**Screenshots:**  *Splunk Cloud - Upload Data*



index=main (all times)

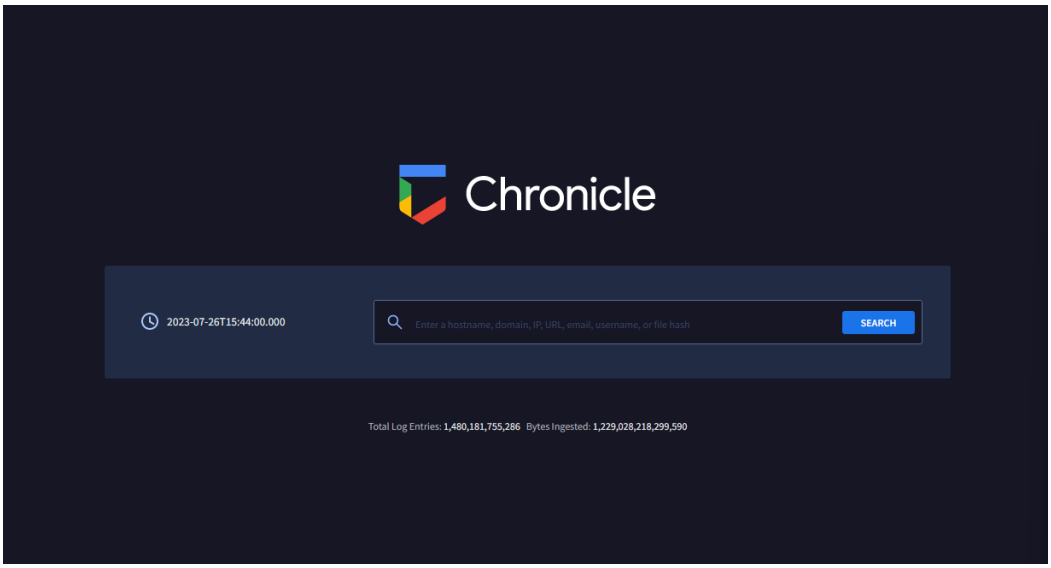
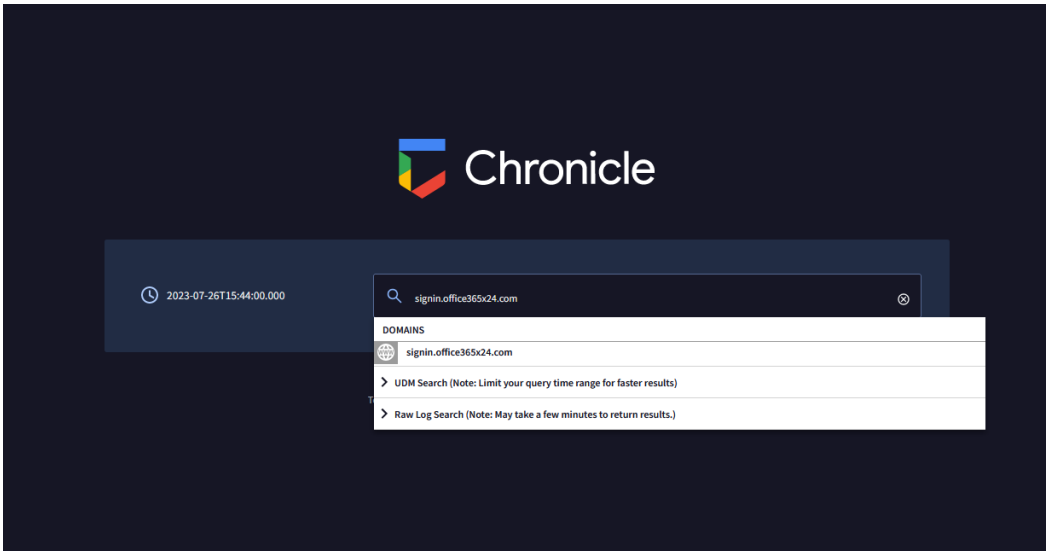


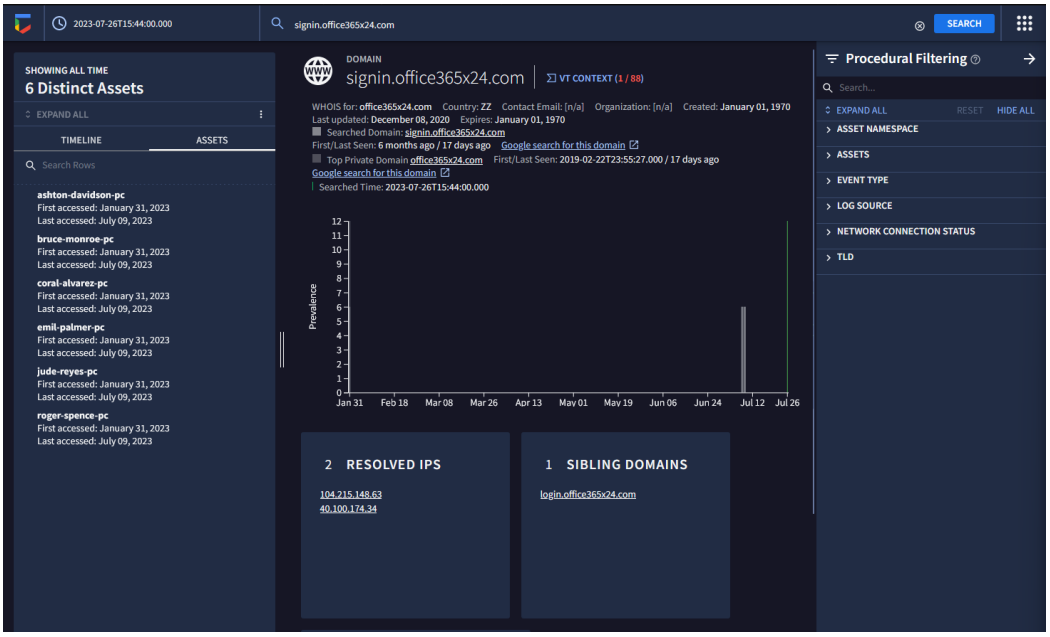
Index=main host=mailsv (all times)

	 *index=main host=mailsv fail* root (all times) - Failed SSH Logins*

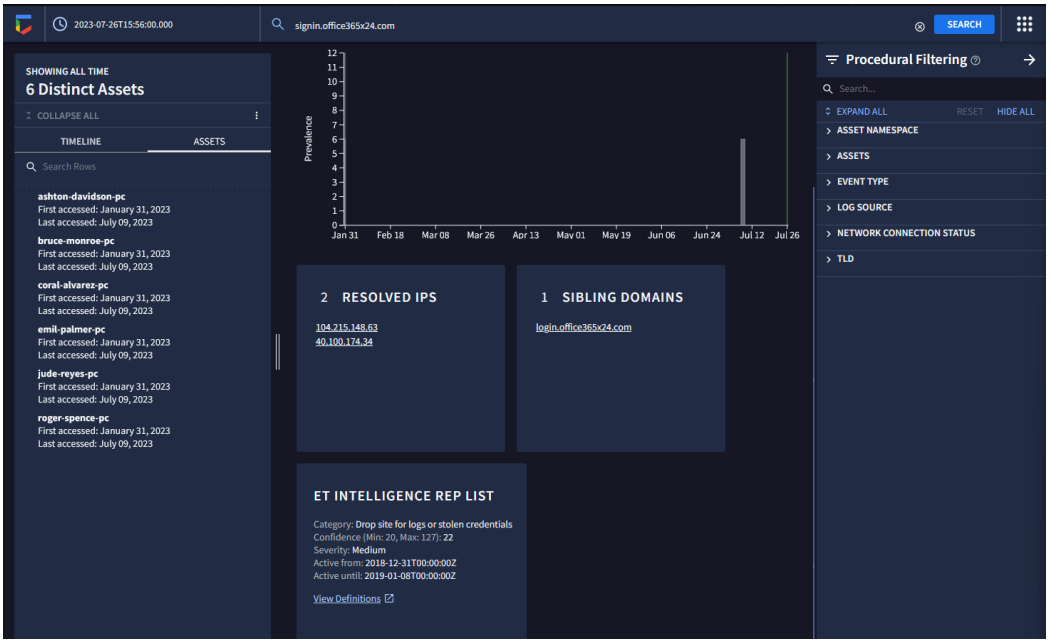
Date: 7/26/2023	**Entry:** 9 *"Perform a query with Chronicle"*
Description	**NIST Incident Response Lifecycle Phase:** Detection and Analysis. As a security analyst at a financial services company, I have received an alert that an employee received a phishing email in their inbox. I have identified a suspicious domain name contained in the email's body: `signin.office365x24.com`. After performing log analysis, I have determined that the suspicious domain has been involved in phishing campaigns. As evidenced in the logs, I have also determined that multiple assets might have been impacted by the phishing campaign. Login information was submitted to the suspicious domain via POST requests by two assets. Lastly, after examining the resolved IP address, I have identified two additional domains related to the suspicious domain.
Tool(s) used	• **Chronicle** – cloud native tool used to investigate security incidents involving

	phishing.
The 5 W's	● **Who:** The **WHOIS** for `signin.office365x24.com`: ○ **Country**: ZZ ○ **Organization**: [n/a] ○ **Contact Email**: [n/a] However, the VirusTotal Context provided more information: ○ **City**: New Delhi ○ **Country**: IN ○ **Email**: 9a6229aeb54b0cc2s@kamtrononline ○ **Organization**: Kamtron Systems Pvt. Ltd. The sibling domain is `login.office365x24.com`, and the resolved IP addresses are 40.100.174.34 and 104.215.148.63. ● **What:** A phishing campaign was successful, as evidenced by POST log data in the "Timeline" section of Chronicle. POST information tells us that data was sent to the domain that is being investigated, suggesting a successful phishing attack. There were two occurrences of the successful phishing attack on asset identifiers `emil-palmer-pc` and `ashton-davidson-pc`. Under the Resolved IPS, 40.100.174.34, for the `signin.office365x24.com` domain, there are three occurrences of the POST request to asset identifiers `ashton-davidson-pc`, `emil-palmer-pc`, and `warren-morris-pc`). Additional affected assets are: `amir-david-pc`, `ashton-davidson-pc`, `bruce-monroe-pc`, `coral-alvarez-pc`, `emil-palmer-pc`, `jude-reyes-pc`, `roger-spence-pc`, and `warren-morris-pc`. The additional domains associated with this IP address are: `signin.office365x24.com` and `signin.accounts-gooqle.com`. The severity of this phishing campaign is medium, and the category is "Drop site for logs or stolen credentials". ● **When:** The ET Intelligence Rep List indicates that the domain was active from 12/18/2018 through 1/8/2019. The timeline for the domain shows that the POST incidents occurred between 1/31/2023 and 7/9/2023.

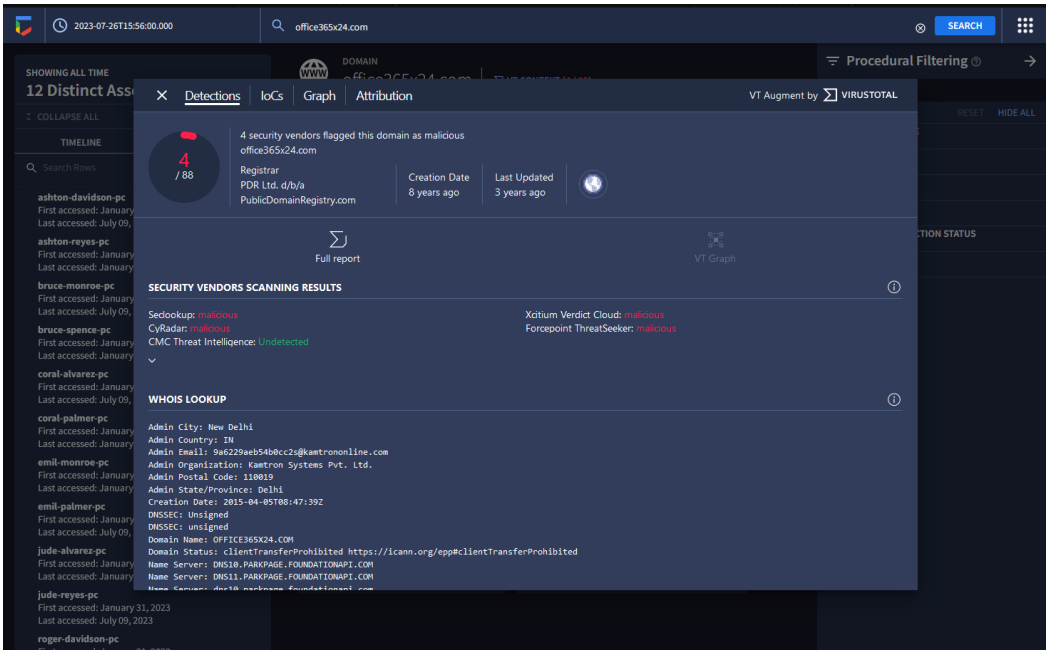
	• **Where:** The phishing campaign occurred at a financial services company. • **Why:** This incident occurred to obtain logs or stolen credentials. The intent behind this is malicious. The attacker likely wanted to gain an understanding of the logs to gain a better understanding of our security posture and any attack vectors to take. Additionally, stealing credentials would allow the attacker to facilitate another educated attack in tandem with the log data obtained.
Additional notes	**Screenshots:**  *Chronicle – Home Page*  *Chronicle – Search for Domain*



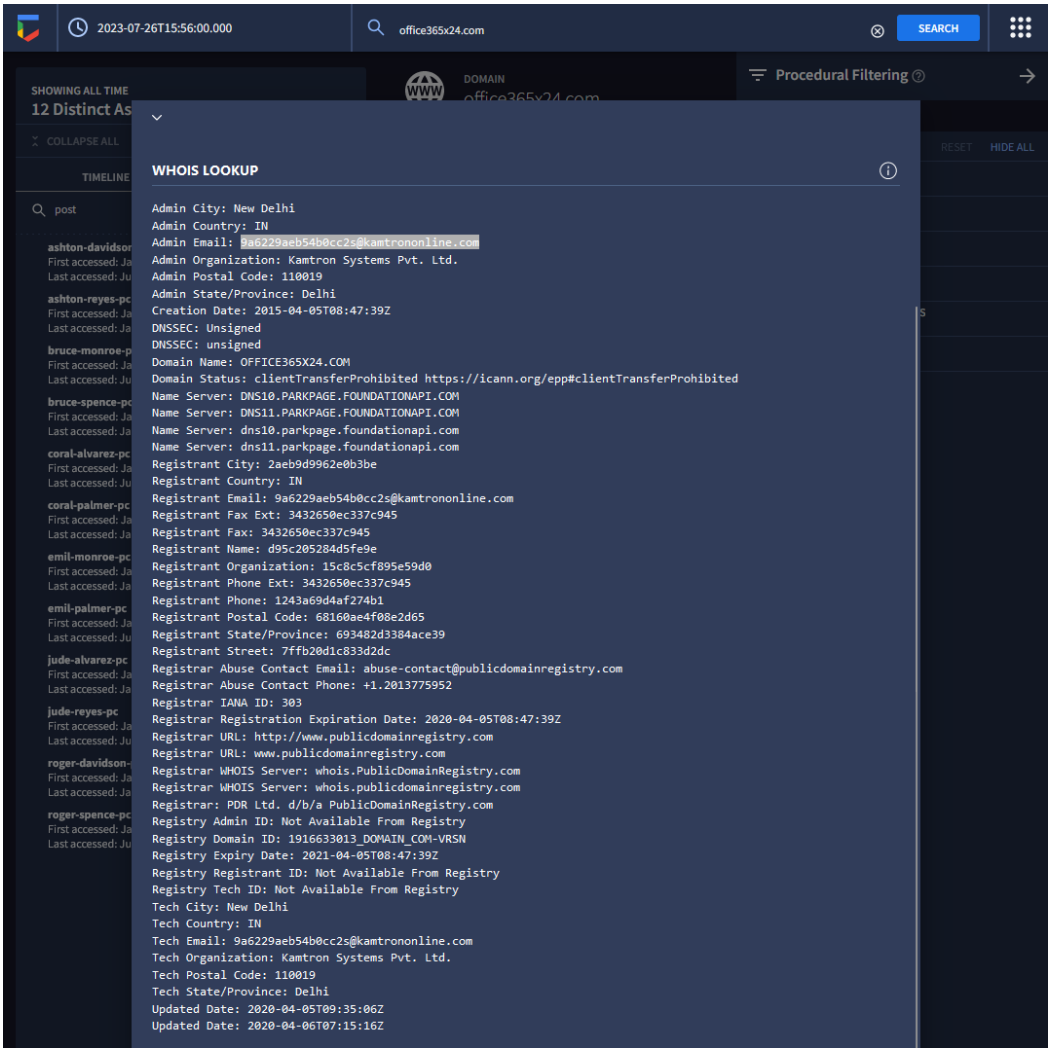
Chronicle – Search Results



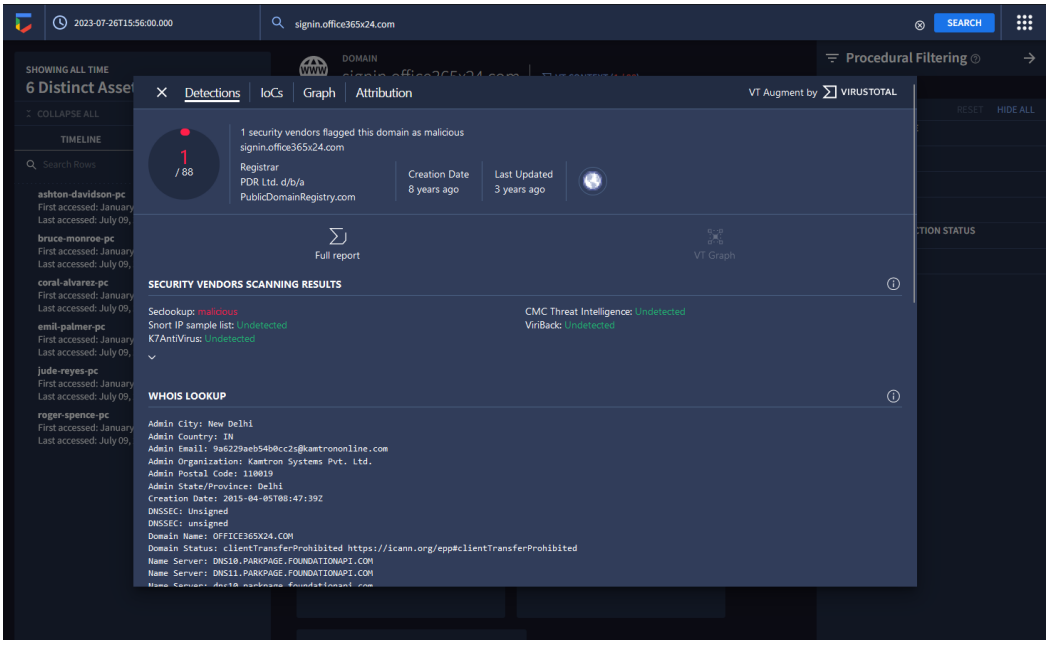
Chronicle – Resolved IPS, Sibling Domains, ET Intelligence Rep List



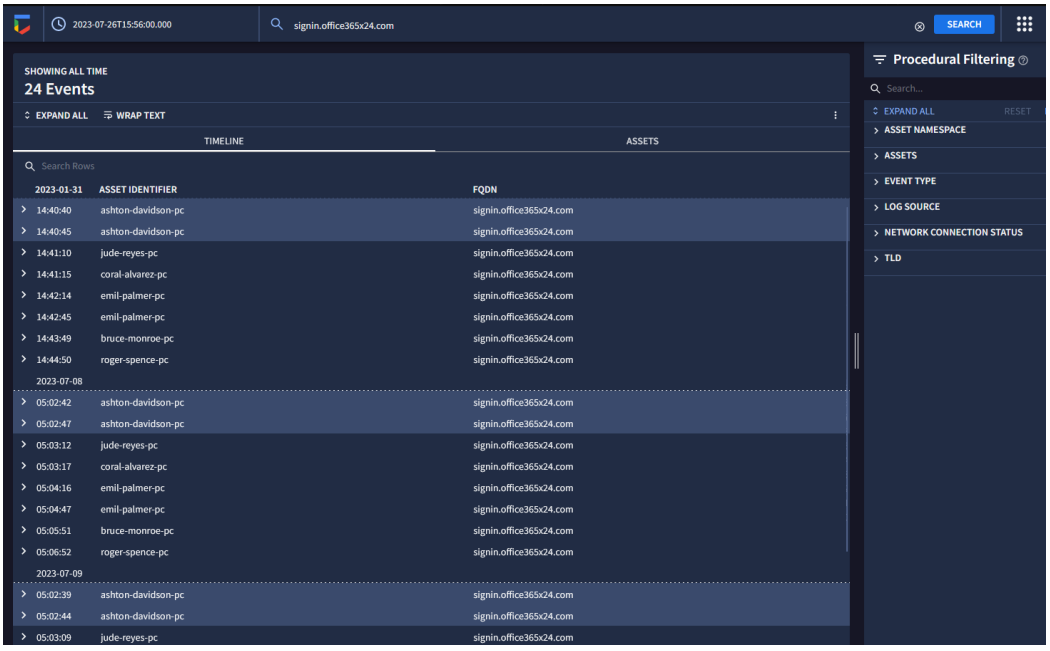
Chronicle – Top Domain VirusTotal Context



Chronicle – Top Domain WHOIS



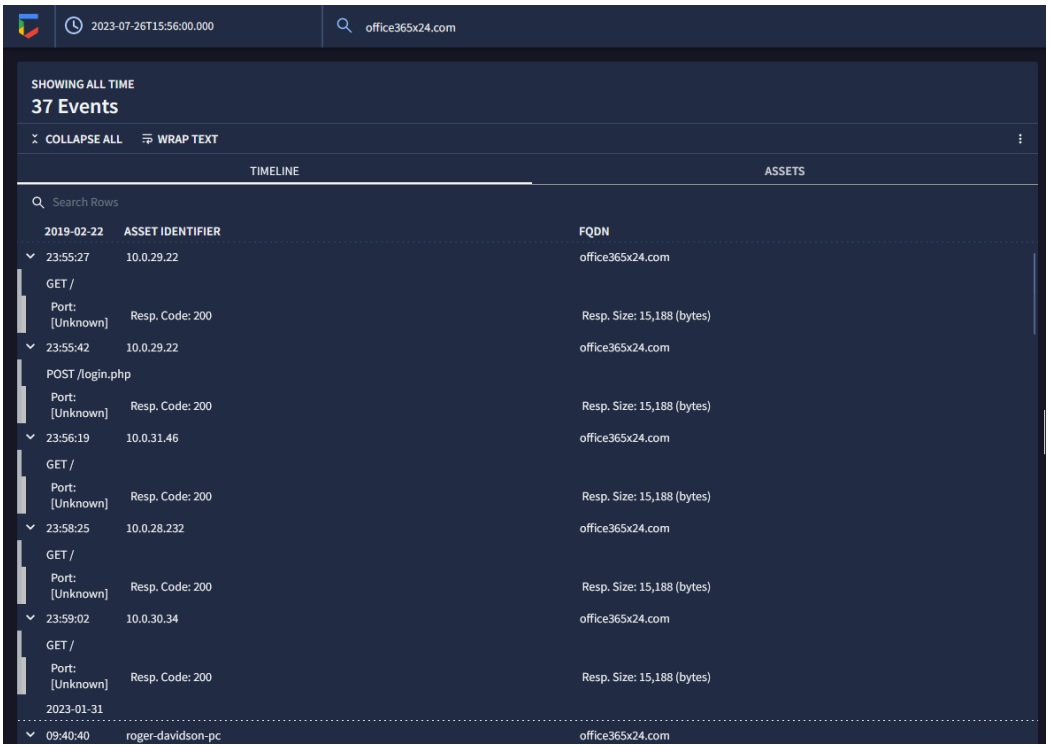
Chronicle – Sibling Domain VirusTotal Context



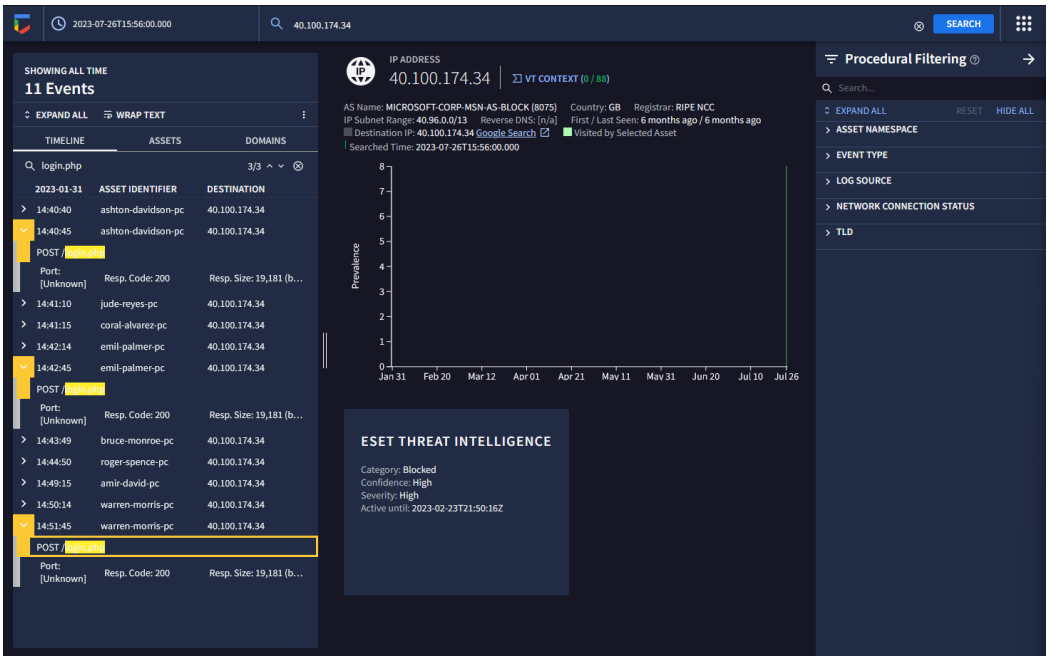
Chronicle – Timeline


2023-07-26T15:56:00.000
SHOWING ALL TIME
12 Distinct Assets
EXPAND ALL
TIMELINE
ASSETS
Search Rows
ashton-davidson-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023
ashton-reyes-pc
First accessed: January 31, 2023
Last accessed: January 31, 2023
bruce-monroe-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023
bruce-spence-pc
First accessed: January 31, 2023
Last accessed: January 31, 2023
coral-alvarez-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023
coral-palmer-pc
First accessed: January 31, 2023
Last accessed: January 31, 2023
emil-monroe-pc
First accessed: January 31, 2023
Last accessed: January 31, 2023
emil-palmer-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023
jude-alvarez-pc
First accessed: January 31, 2023
Last accessed: January 31, 2023
jude-reyes-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023
roger-davidson-pc

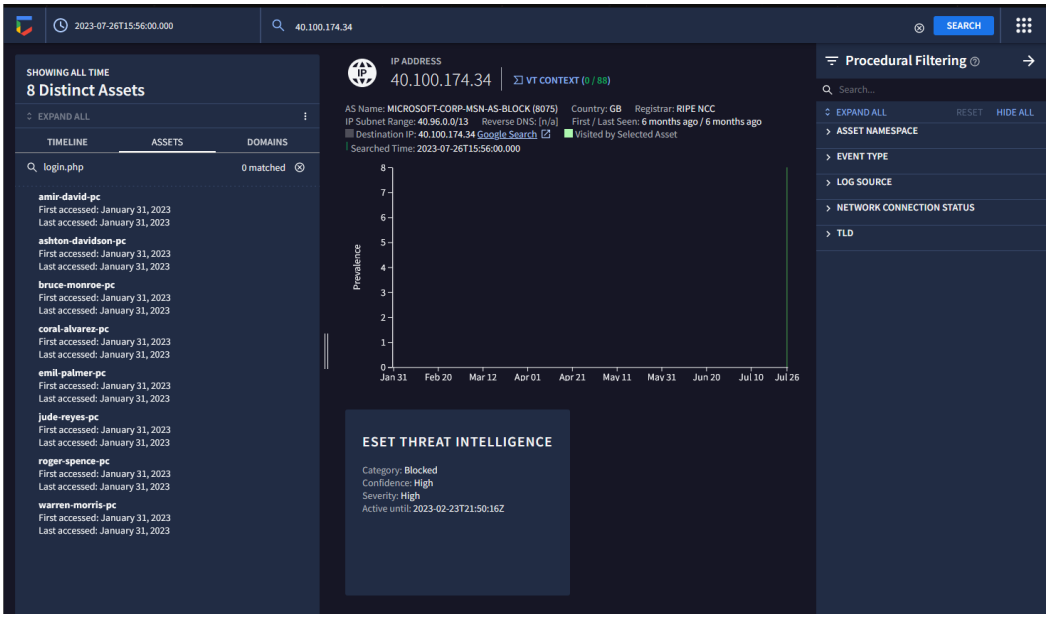
Chronicle – Assets



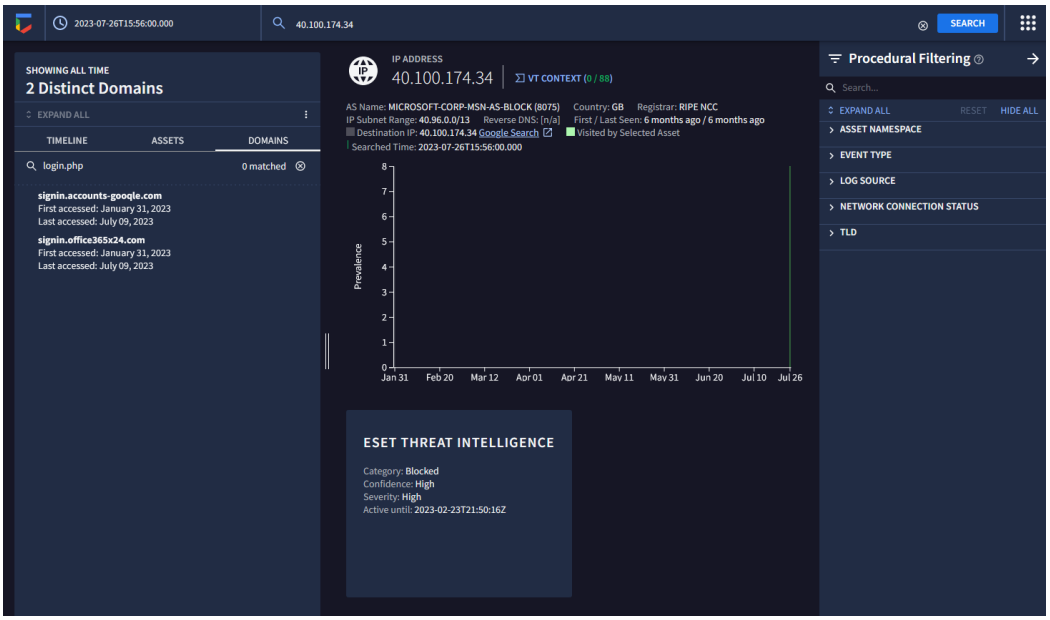
Chronicle – Timeline Expanded



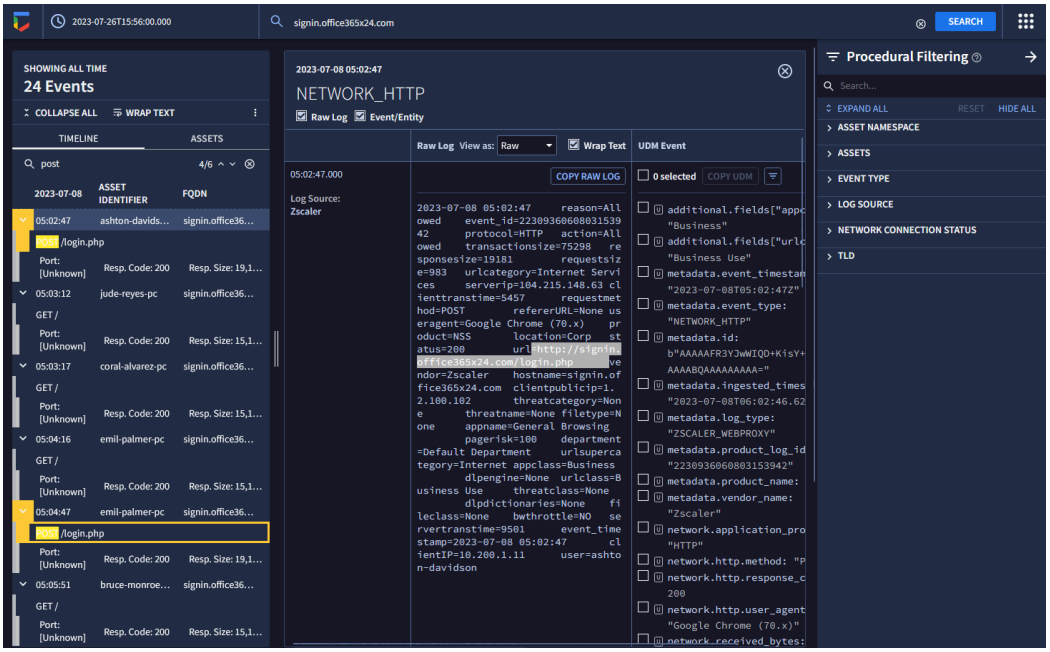
Chronicle – Resolved IP Timeline POST Query



Chronicle – Resolved IP Assets



Chronicle – Resolved IP Domains



Chronicle – Timeline POST Query, Assets, URL

Reflections/Notes

- **Were there any specific activities that were challenging for you? Why or why not?**

One specific activity that I found challenging was understanding Suricata. As a newcomer to IDS/IPS tools like Suricata, I initially followed the provided instructions, but I also attempted to explore and troubleshoot on my own. This independent exploration led to moments of confusion, but I persevered and eventually returned to the assignment's guidelines. Eventually, I successfully completed the assignment and later restarted the activity in the exemplar section, solidifying my understanding of Suricata's functionalities. I found that using `jq` to process JSON output can be a bit tricky, as I am not familiar with JSON formatting. However, with practice and more exposure to Suricata and other tools, it will become easier to use.

Another activity I found challenging was learning the differences and applications of Splunk and Chronicle. Splunk and Chronicle are both simple to use SIEM solutions, but they have their own unique ways of managing and querying data. Learning this took some time, but I know that being able to fully understand their capabilities is a valuable skill for a security analyst.

Lastly, `tcpdump` was a tool that I was not experienced using. Although I am familiar with using the command-line interface for Linux commands, using it to capture and filter network traffic was new to me. I encountered obstacles, but after some time I was able to complete this activity and add `tcpdump` to my tool belt.

- **Has your understanding of incident detection and response changed after taking this course?**

My understanding of incident detection and response has improved. With my CompTIA Security+ and CASP+ certificates, as well as my experience in performing IT audits, Segregation of Duties audits, Access Control audits, and SOC audits, my foundational understanding of incident detection and response has absolutely been improved upon. Taking this course provided me with more in-depth knowledge and practical experience, reinforcing what I already knew, and helping me to see how these concepts apply in real-world scenarios.

- **Was there a specific tool or concept that you enjoyed the most? Why?**

It's clear to me that I enjoyed investigating the hash, as it's a practical and relevant skill in cybersecurity. In addition, I love learning new tools, so learning how to effectively use Suricata, Splunk, and Chronicle, was a highlight. In addition to learning something new, having the opportunity to gain hands-on experience with these tools was extremely valuable for me.