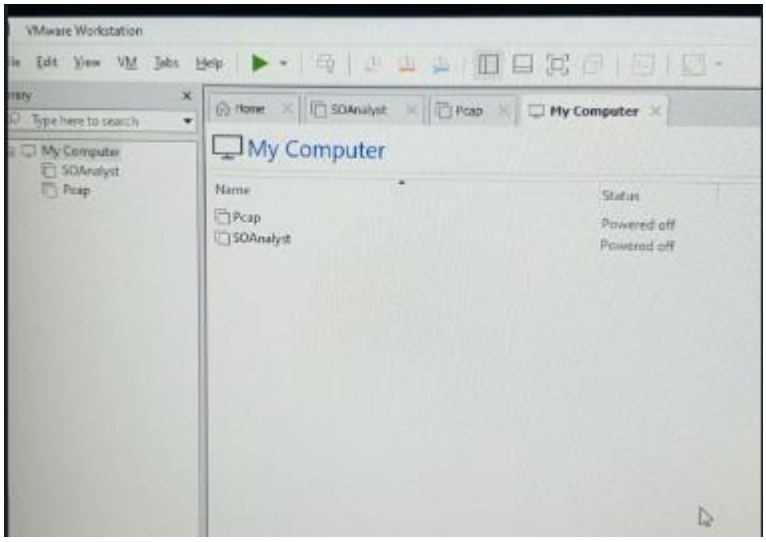
PCAP Analysis by Osman Hamza

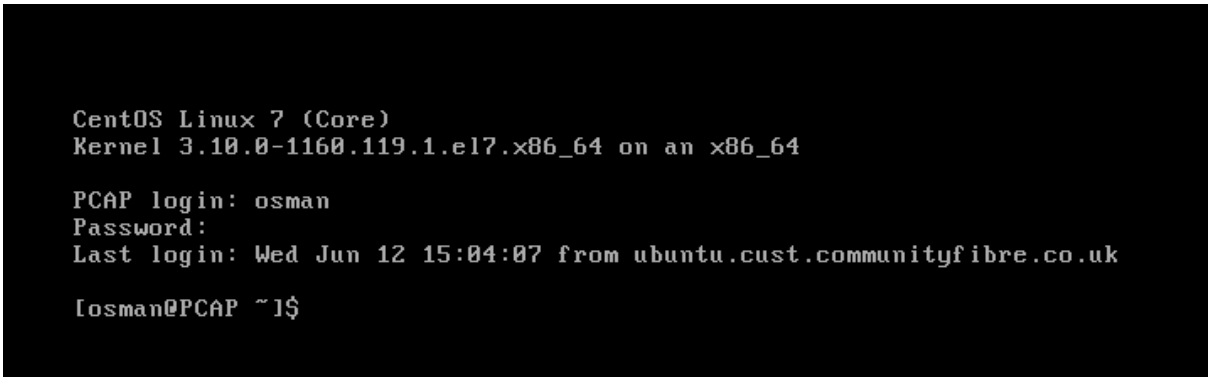
PCAP (Packet capture) analysis is the process of examining network traffic data captured in a Pcap file.

Below is an overview of what I have used, how I used it and what I have gained from this.

For this project, I have used a virtual machine called VMware workstation pro 16. With this virtual machine, I have installed 2 VMs which are Ubuntu and CentOS 7. - I have integrated CentOS7 with Security onion. You can use this link to install it https://lnkd.in/ez2ERsyi



CentOS 7 integrated with security onion.



Establishing connection

```
osman@PCAP:~
ubuntu@ubuntu:~$ sudo ssh osman@192.168.1.37
The authenticity of host '192.168.1.37 (192.168.1.37)' can't be established.
ED25519 key fingerprint is SHA256:3Gqy8wPgLN/VAl77FTCdopTCrpLmPqMzUZ8nTYIP+b8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.37' (ED25519) to the list of known hosts.
##############################################
##############################################
###                                        ###
###   UNAUTHORIZED ACCESS PROHIBITED       ###
###                                        ###
##############################################
##############################################
osman@192.168.1.37's password:
Last login: Wed Jun 12 15:02:26 2024

[osman@PCAP ~]$ wget https://www.malware-traffic-analysis.net/2024/05/14/2024-05-14-DarkGate-i
nfection-traffic.pcap.zip
```

I have used SSH protocol to establish the connection between the 2 virtual machines which were Ubuntu and CentOS 7

Malware Traffic Analysis site

https://www.malware-traffic-analysis.net/2024/05/14/index.html

MALWARE-TRAFFIC-ANALYSIS.NET

Rhythmbox

4-05-14 (TUESDAY): DARKGATE ACTIVITY

NOTES:

- Zip files are password-protected. Of note, this site has a new password scheme. For the password, see the "about" page of this websit

REFERENCES:

- **https://www.linkedin.com/posts/unit42_darkgate-timelythreatintel-unit42threatintel-activity-7196580114761928704-Nblk/**
- **https://twitter.com/Unit42_Intel/status/1790814496845394110**

ASSOCIATED FILES:

- **2024-05-14-IOCs-for-DarkGate-activity.txt.zip** 2.7 kB (2,720 bytes)
- **2024-05-14-DarkGate-infection-traffic.pcap.zip** 1.5 MB (1,520,818 bytes)
- **2024-05-14-DarkGate-malware-and-artifacts.zip** 3.1 MB (3,086,271 bytes)

Click here to return to the main page.

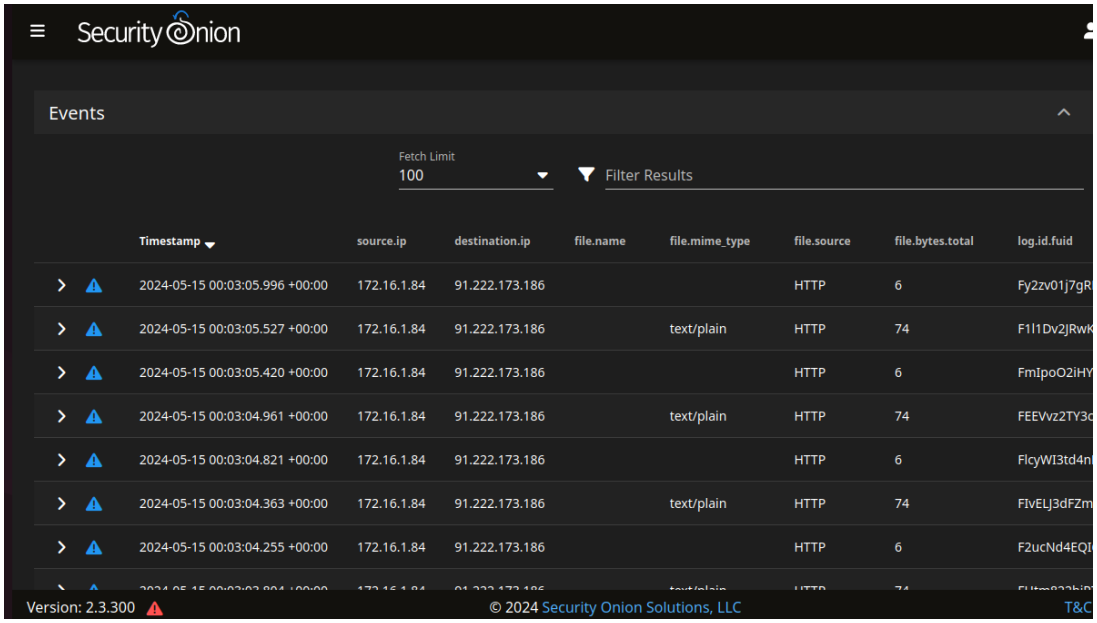
Once established connection, I then went ahead and started my malware analysis from there. I have used “malware traffic analysis” site to get a malicious file and downloaded the zip file on my Ubuntu VM from the Associated files. This file was used for my experiment.

Importing the zip file

```
osman@PCAP:~
- assigning unique identifier to import: 8dfdb1eefc91f684e66d13c210602550
- analyzing traffic with Suricata
- analyzing traffic with Zeek
- saving PCAP data spanning dates 2024-05-15 through 2024-05-15

Cleaning up:

Import complete!

You can use the following hyperlink to view data in the time range of your import.  You can t
iple-click to quickly highlight the entire hyperlink and you can then copy it into your brows
r:
https://192.168.1.37/#/dashboards?q=import.id:8dfdb1eefc91f684e66d13c210602550%20%7C%20groupb
%20-sankey%20event.dataset%20event.category%2a%20%7C%20groupby%20-pie%20event.category%20%7C%
0groupby%20-bar%20event.module%20%7C%20groupby%20event.dataset%20%7C%20groupby%20event.module
20%7C%20groupby%20event.category%20%7C%20groupby%20observer.name%20%7C%20groupby%20source.ip%
0%7C%20groupby%20destination.ip%20%7C%20groupby%20destination.port&t=2024%2F05%2F15%2000%3A00
3A00%20AM%20-%202024%2F05%2F16%2000%3A00%3A00%20AM&z=UTC

or you can manually set your Time Range to be (in UTC):
From: 2024-05-15    To: 2024-05-16
Disk
Please note that it may take 30 seconds or more for events to appear in Security Onion Consol
.
[osman@PCAP ~]$
```

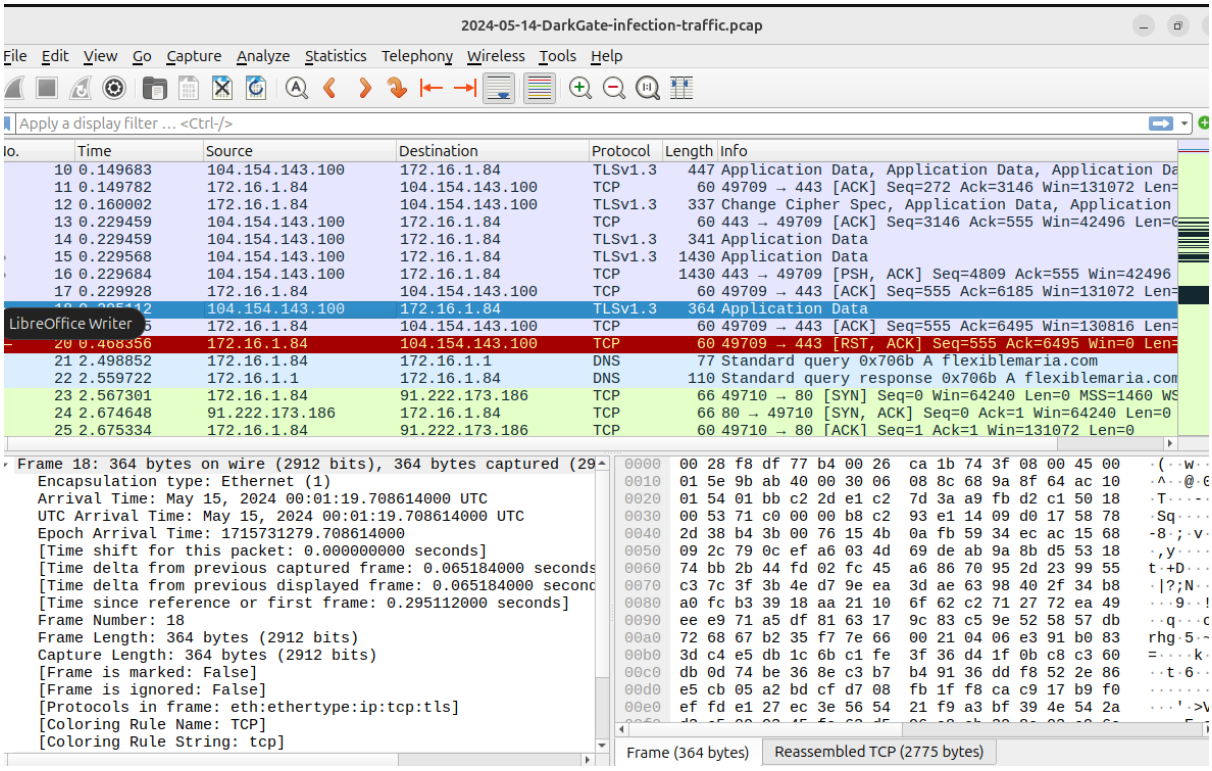
After downloading the zip file, I have used the so-import-pcap command to import the pcap file into security onion for the analysis. From there, I have received the link to view my onion security dashboard

Onion security dashboard



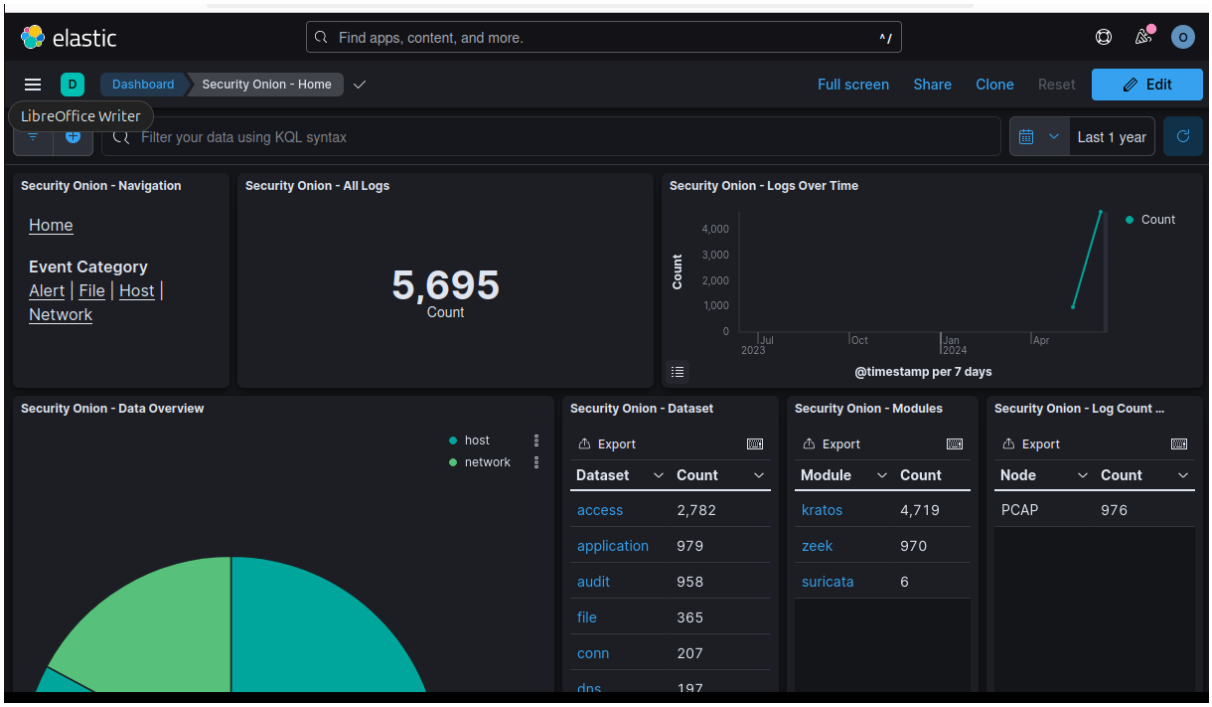
From here, I was able to visualise and analyse the generated logs and alerts of network activity, HTTP protocols, sources, DNS queries, SSL/TLS handshakes and many more. I was also able to view timestamp, dates and IP sources for events. I was also able to access Elastic from security onion web interface to visualise and investigate traffic volume over time.

Wireshark



I then installed Wireshark on my Ubuntu machine and accessed it using my malicious pcap file. I have used Wireshark to investigate the file thoroughly using the statistics and analyse menu to generate summaries, reports, and conversations between endpoints.

Elastic



Conclusion

This lab marked my first time into the practical world of malware analysis and provided an invaluable experience that enriched my understanding of cybersecurity. By engaging in hands-on activities, I gained a thorough grasp of Intrusion Detection Systems (IDS), Wireshark, and digital forensic investigations.

The process involved using these powerful tools to analyse a malicious PCAP (Packet Capture) file, which presented a comprehensive and immersive approach to learning. This experience significantly deepened my knowledge of core cybersecurity principles, advanced threat detection methodologies, and effective incident response techniques.

Working with IDS allowed me to understand how these systems identify and respond to potential threats in real-time, enhancing network security. Utilizing Wireshark, I learned how to capture and analyse network traffic, a crucial skill for identifying suspicious activities and understanding network behaviours. The digital forensic investigation aspect of the lab equipped me with the skills needed to meticulously examine digital evidence, an essential practice for uncovering malicious activities and preserving the integrity of the investigation.

Overall, this lab experience has not only broadened my technical skills but also instilled a comprehensive understanding of the multifaceted nature of cybersecurity. It underscored the importance of practical, hands-on learning in mastering the complex and dynamic field of cybersecurity.