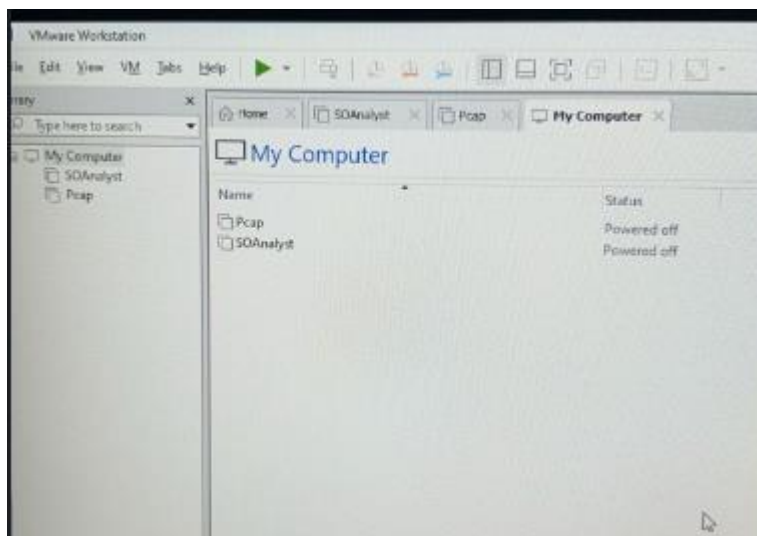


# PCAP Analysis by Osman Hamza

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.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.119.1.el7.x86_64 on an x86_64

PCAP login: osman
Password:
Last login: Wed Jun 12 15:04:07 from ubuntu.cust.communityfibre.co.uk

[osman@PCAP ~]$
```

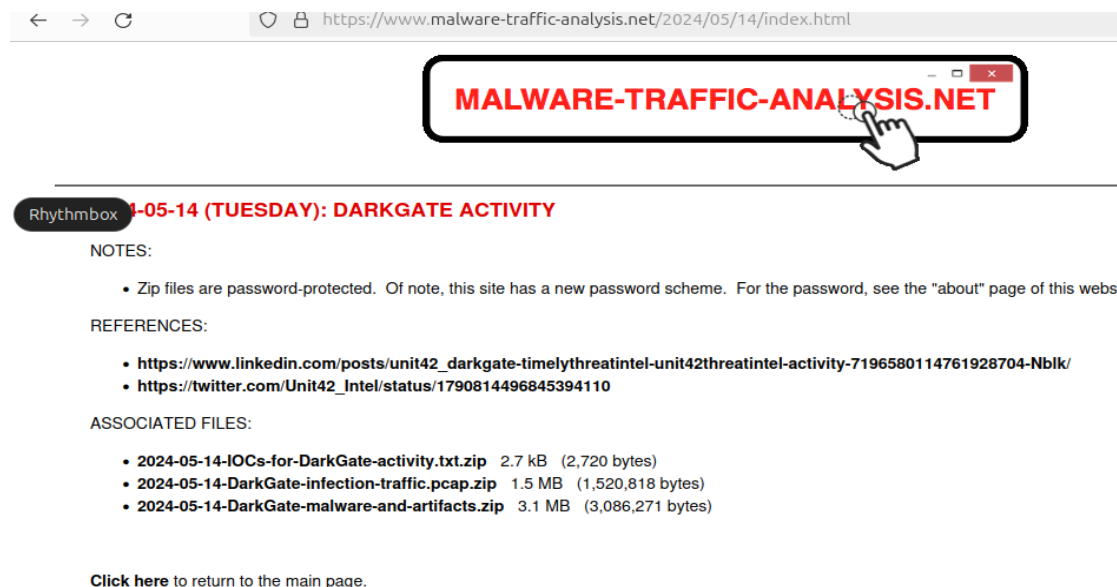
## Establishing connection

```
osman@PCAP:~$ 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



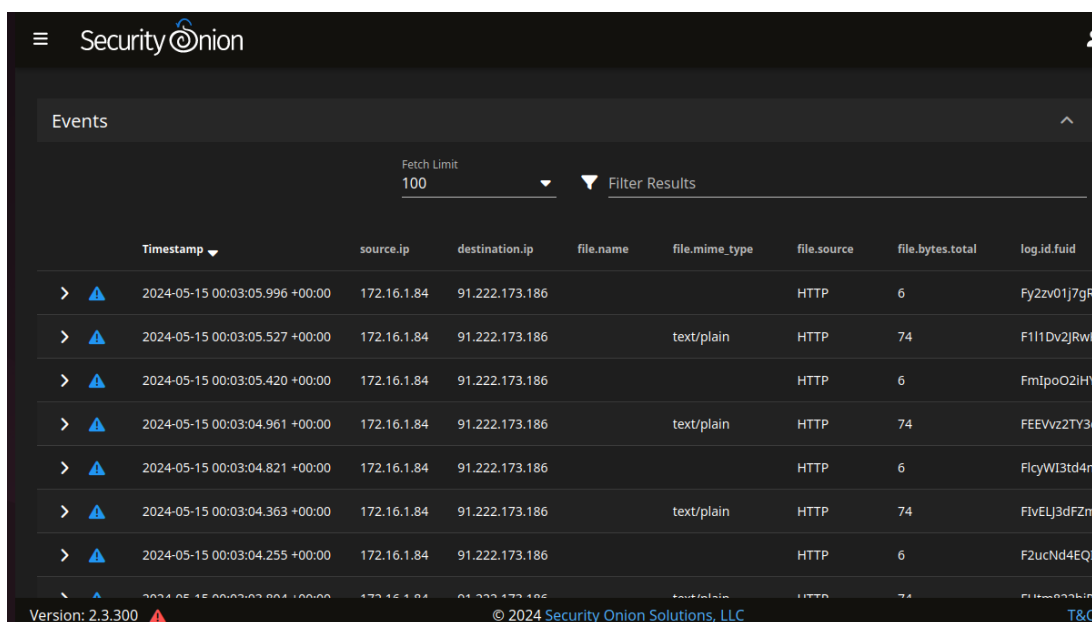
Once established connection, I then went ahead and started my malware analysis from there. I have used “malware traffic analysis” site to get a malicious file and downloaded the zip file on my Ubuntu VM from the Associated files. This file was used for my experiment.

## 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



The screenshot shows the Security Onion web interface. At the top, there's a header with the Security Onion logo and a hamburger menu. Below the header, there's a section titled "Events". Under "Events", there's a "Fetch Limit" dropdown set to "100" and a "Filter Results" button. Below this, there's a table with columns: "Timestamp", "source.ip", "destination.ip", "file.name", "file.mime\_type", "file.source", "file.bytes.total", and "log.id.fuid". The table contains several rows of data, each representing a network event. The first row shows a timestamp of "2024-05-15 00:03:05.996 +00:00", source IP "172.16.1.84", destination IP "91.222.173.186", file source "HTTP", and file bytes total "6". The second row shows a timestamp of "2024-05-15 00:03:05.527 +00:00", source IP "172.16.1.84", destination IP "91.222.173.186", file mime type "text/plain", file source "HTTP", and file bytes total "74". The third row shows a timestamp of "2024-05-15 00:03:05.420 +00:00", source IP "172.16.1.84", destination IP "91.222.173.186", file source "HTTP", and file bytes total "6". The fourth row shows a timestamp of "2024-05-15 00:03:04.961 +00:00", source IP "172.16.1.84", destination IP "91.222.173.186", file mime type "text/plain", file source "HTTP", and file bytes total "74". The fifth row shows a timestamp of "2024-05-15 00:03:04.821 +00:00", source IP "172.16.1.84", destination IP "91.222.173.186", file source "HTTP", and file bytes total "6". The sixth row shows a timestamp of "2024-05-15 00:03:04.363 +00:00", source IP "172.16.1.84", destination IP "91.222.173.186", file mime type "text/plain", file source "HTTP", and file bytes total "74". The seventh row shows a timestamp of "2024-05-15 00:03:04.255 +00:00", source IP "172.16.1.84", destination IP "91.222.173.186", file source "HTTP", and file bytes total "6". The eighth row shows a timestamp of "2024-05-15 00:03:03.994 +00:00", source IP "172.16.1.84", destination IP "91.222.173.186", file mime type "text/plain", file source "HTTP", and file bytes total "74". At the bottom of the table, there's a footer that says "Version: 2.3.300" and "© 2024 Security Onion Solutions, LLC".

	Timestamp ▼	source.ip	destination.ip	file.name	file.mime_type	file.source	file.bytes.total	log.id.fuid
> ⚠	2024-05-15 00:03:05.996 +00:00	172.16.1.84	91.222.173.186			HTTP	6	Fy2zv01J7gR
> ⚠	2024-05-15 00:03:05.527 +00:00	172.16.1.84	91.222.173.186		text/plain	HTTP	74	F111Dv2JRwK
> ⚠	2024-05-15 00:03:05.420 +00:00	172.16.1.84	91.222.173.186			HTTP	6	FmIpoO2iHY
> ⚠	2024-05-15 00:03:04.961 +00:00	172.16.1.84	91.222.173.186		text/plain	HTTP	74	FEEVvz2TY3d
> ⚠	2024-05-15 00:03:04.821 +00:00	172.16.1.84	91.222.173.186			HTTP	6	FicYWI3td4n
> ⚠	2024-05-15 00:03:04.363 +00:00	172.16.1.84	91.222.173.186		text/plain	HTTP	74	FivELJ3dFZm
> ⚠	2024-05-15 00:03:04.255 +00:00	172.16.1.84	91.222.173.186			HTTP	6	F2ucNd4EQI
> ⚠	2024-05-15 00:03:03.994 +00:00	172.16.1.84	91.222.173.186		text/plain	HTTP	74	F1w033k1R

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

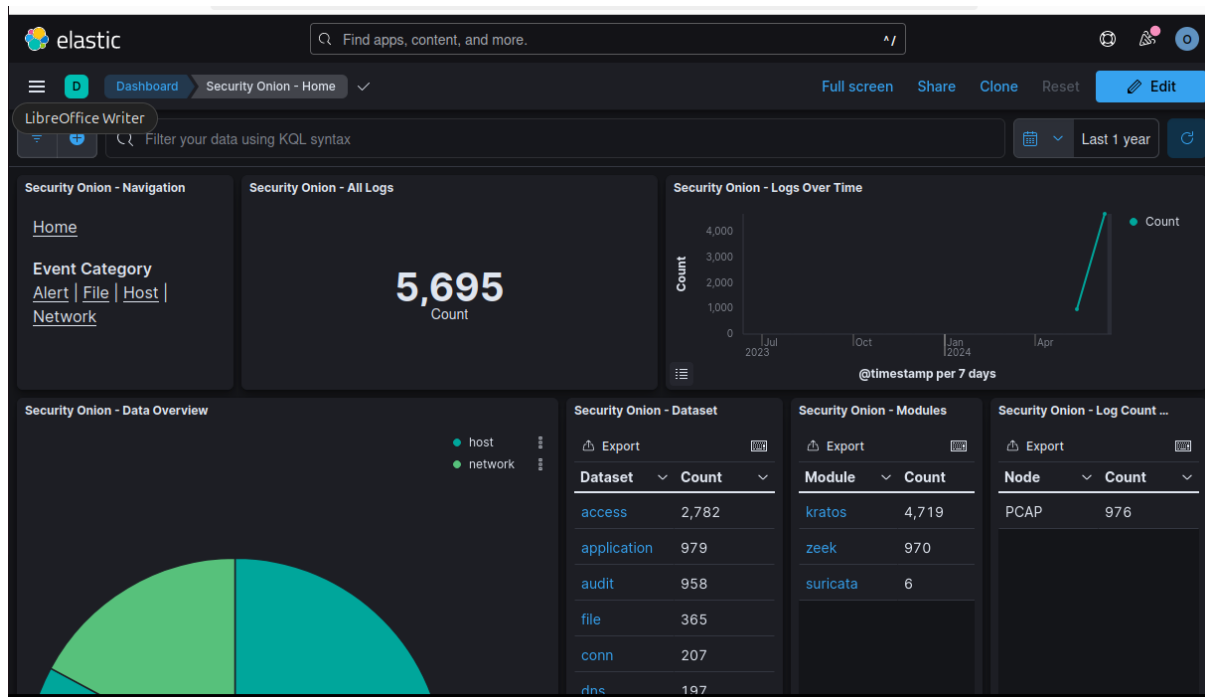
The image shows the Wireshark interface with a packet capture file named "2024-05-14-DarkGate-infection-traffic.pcap". The packet list on the left shows a series of TCP and TLSv1.3 packets. The selected packet (Frame 18) is a 364-byte application data packet. The packet details pane on the right shows the packet structure, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
10	0.149683	104.154.143.100	172.16.1.84	TLSv1.3	447	Application Data, Application Data, Application Data
11	0.149782	172.16.1.84	104.154.143.100	TCP	60	49709 → 443 [ACK] Seq=272 Ack=3146 Win=131072 Len=0
12	0.160002	172.16.1.84	104.154.143.100	TLSv1.3	337	Change Cipher Spec, Application Data, Application Data
13	0.229459	104.154.143.100	172.16.1.84	TCP	60	443 → 49709 [ACK] Seq=3146 Ack=555 Win=42496 Len=0
14	0.229459	104.154.143.100	172.16.1.84	TLSv1.3	341	Application Data
15	0.229568	104.154.143.100	172.16.1.84	TLSv1.3	1430	Application Data
16	0.229684	104.154.143.100	172.16.1.84	TCP	1430	443 → 49709 [PSH, ACK] Seq=4809 Ack=555 Win=42496 Len=0
17	0.229928	172.16.1.84	104.154.143.100	TCP	60	49709 → 443 [ACK] Seq=555 Ack=6185 Win=131072 Len=0
18	0.205412	104.154.143.100	172.16.1.84	TLSv1.3	364	Application Data
19	0.408356	172.16.1.84	104.154.143.100	TCP	60	49709 → 443 [ACK] Seq=555 Ack=6495 Win=130816 Len=0
20	0.408356	172.16.1.84	104.154.143.100	TCP	60	49709 → 443 [RST, ACK] Seq=555 Ack=6495 Win=0 Len=0
21	2.498852	172.16.1.84	172.16.1.1	DNS	77	Standard query 0x706b A flexiblemaria.com
22	2.559722	172.16.1.1	172.16.1.84	DNS	110	Standard query response 0x706b A flexiblemaria.com
23	2.567301	172.16.1.84	91.222.173.186	TCP	66	49710 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=0
24	2.674648	91.222.173.186	172.16.1.84	TCP	66	80 → 49710 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
25	2.675334	172.16.1.84	91.222.173.186	TCP	60	49710 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0

Frame 18: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface eth0  
Encapsulation type: Ethernet (1)  
Arrival Time: May 15, 2024 00:01:19.708614000 UTC  
UTC Arrival Time: May 15, 2024 00:01:19.708614000 UTC  
Epoch Arrival Time: 1715731279.708614000  
[Time shift for this packet: 0.000000000 seconds]  
[Time delta from previous captured frame: 0.065184000 seconds]  
[Time delta from previous displayed frame: 0.065184000 seconds]  
[Time since reference or first frame: 0.295112000 seconds]  
Frame Number: 18  
Frame Length: 364 bytes (2912 bits)  
Capture Length: 364 bytes (2912 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp:tls]  
[Coloring Rule Name: TCP]  
[Coloring Rule String: tcp]

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.