Network Forensics with Malcolm

CyberCrime and Forensics Course Project

Ahmed Nouralla

Content

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.

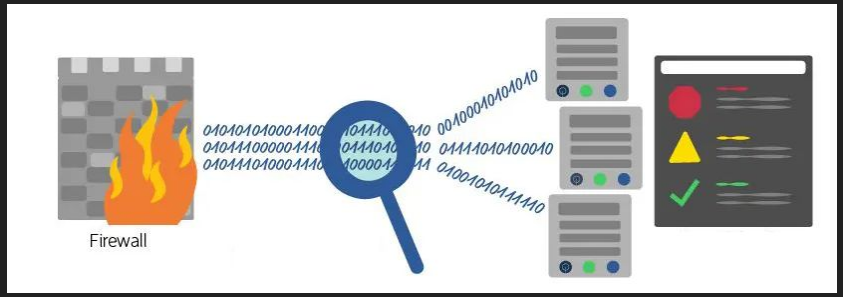
An advantage and a disadvantage:

+ 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

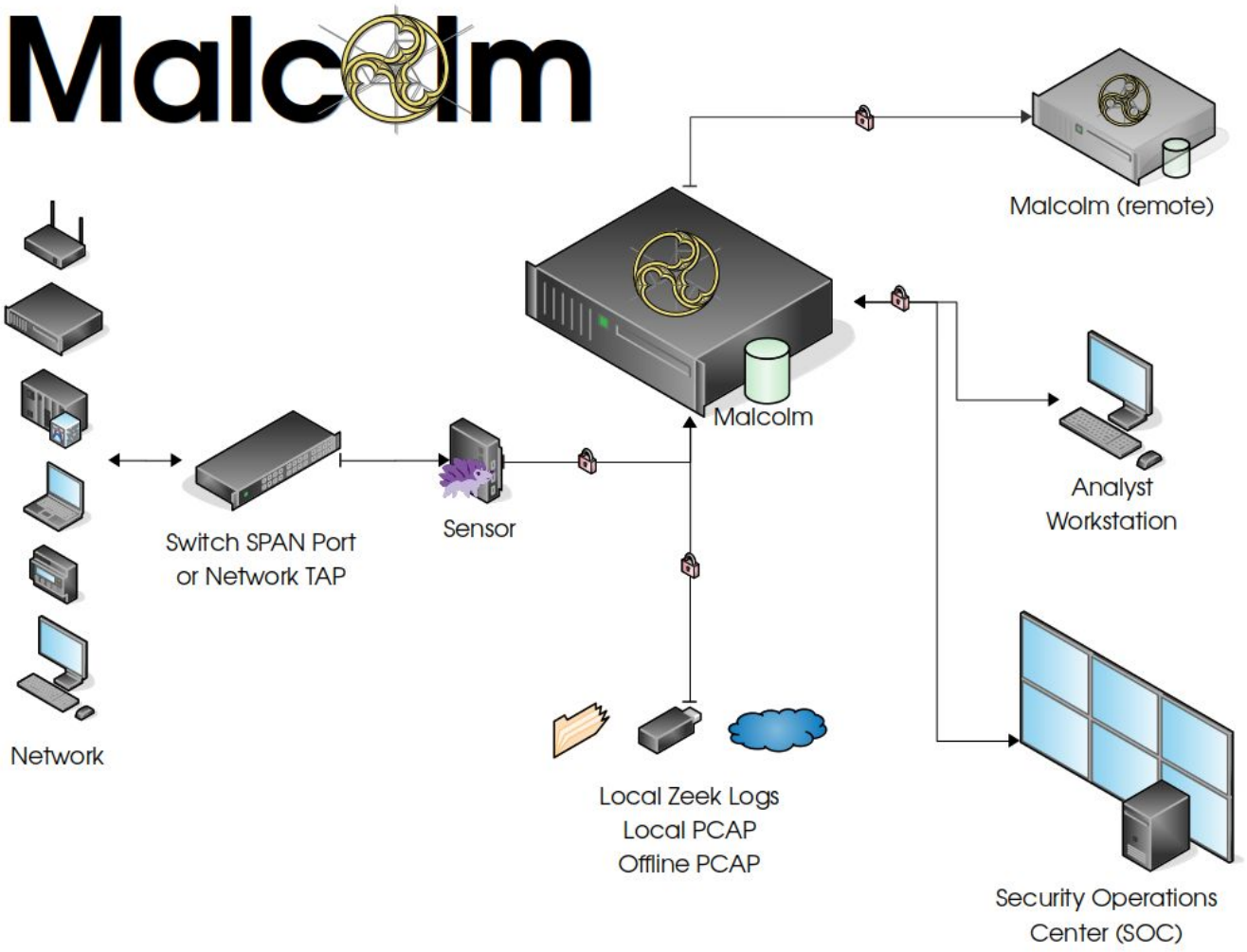
Steps taken:

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

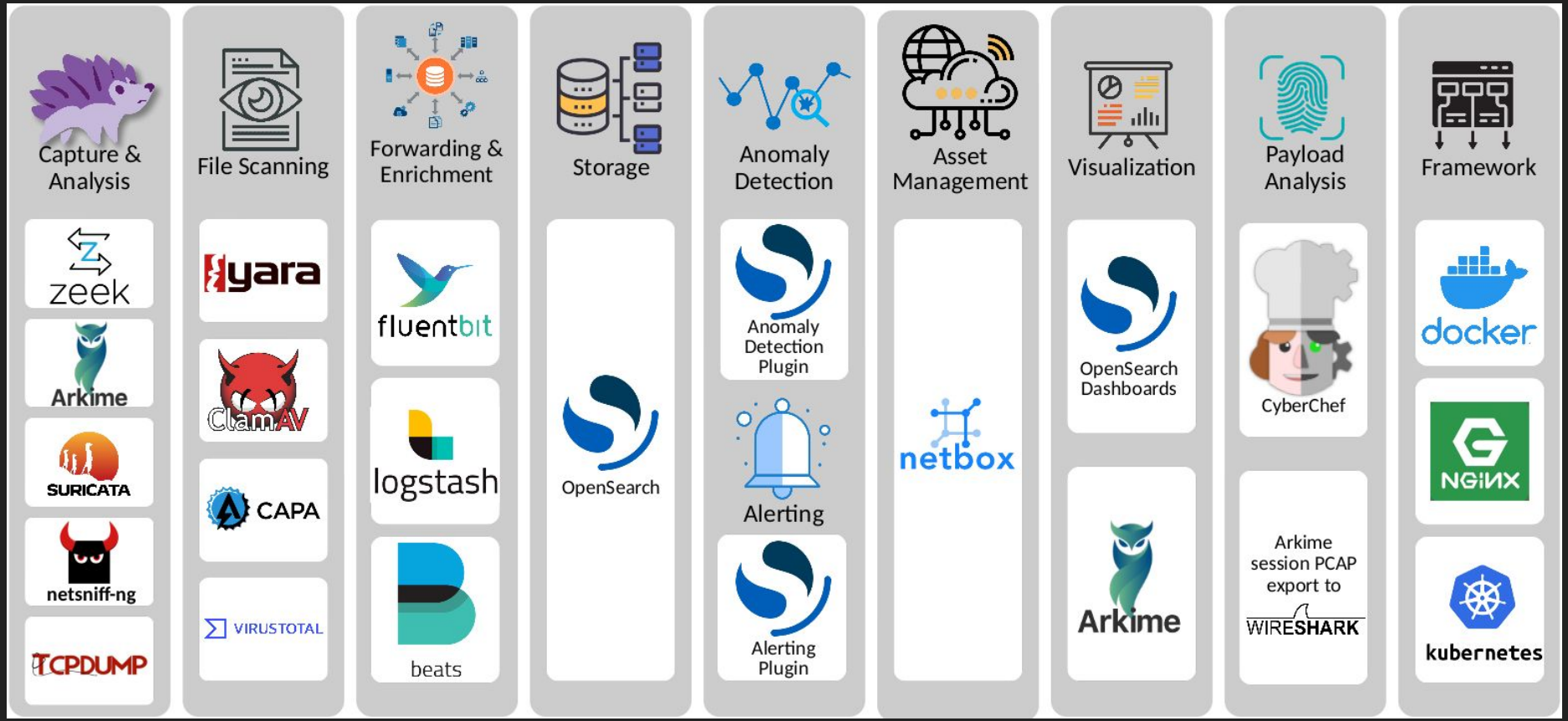
Overview & Architecture

Malcolm is a comprehensive tool suite for network security monitoring.

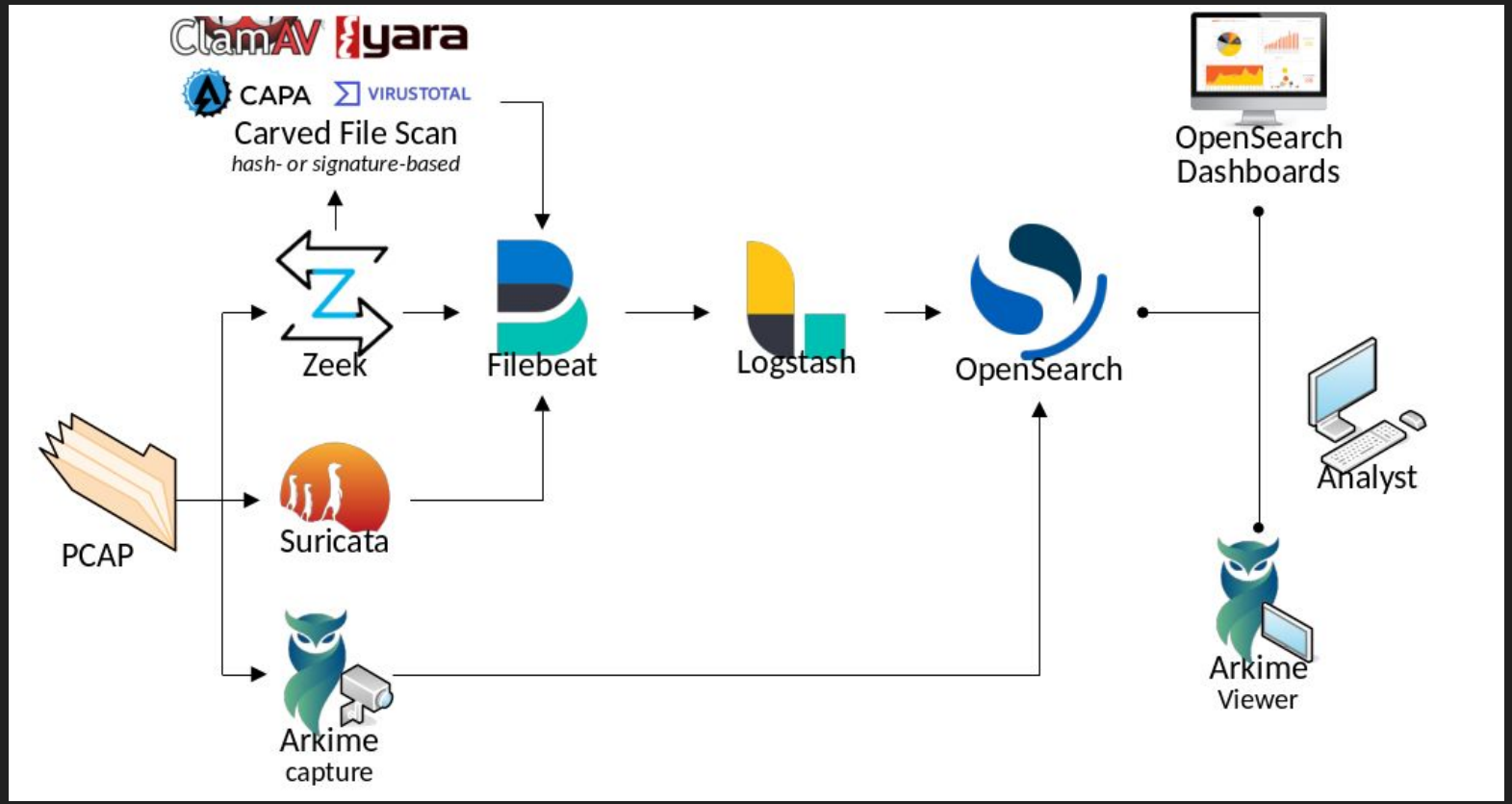
It leverages existing open-source tools to build a complete pipeline for collecting and analyzing network traffic.



Tooling

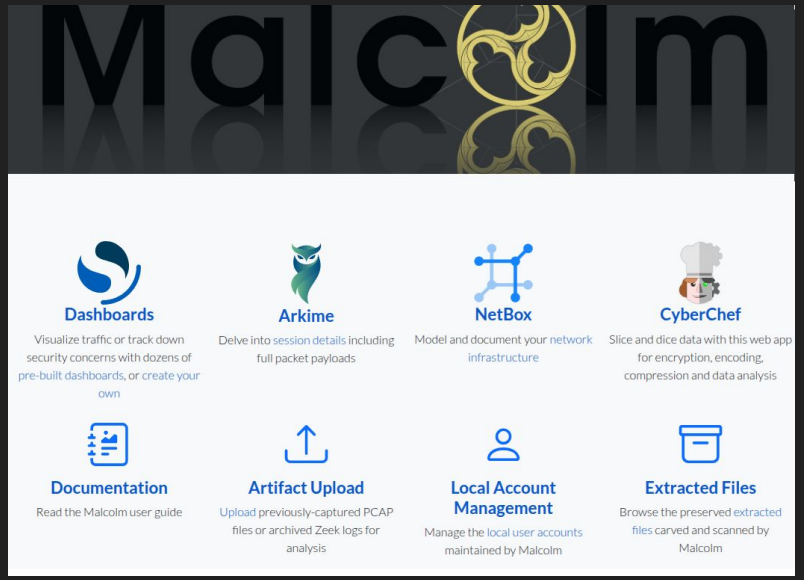

Capture & Analysis
zeek
Arkime
SURICATA
netsniff-ng
TCPDUMP
File Scanning
yara
ClamAV
CAPA
VIRUSTOTAL
Forwarding & Enrichment
fluentbit
logstash
beats
Storage
OpenSearch
Anomaly Detection
Anomaly Detection Plugin
Alerting
Alerting Plugin
Asset Management
netbox
Visualization
OpenSearch Dashboards
Arkime
Payload Analysis
CyberChef
Arkime session PCAP export to
WIRESHARK
Framework
docker
NGINX
kubernetes

Data Pipeline



Deployment

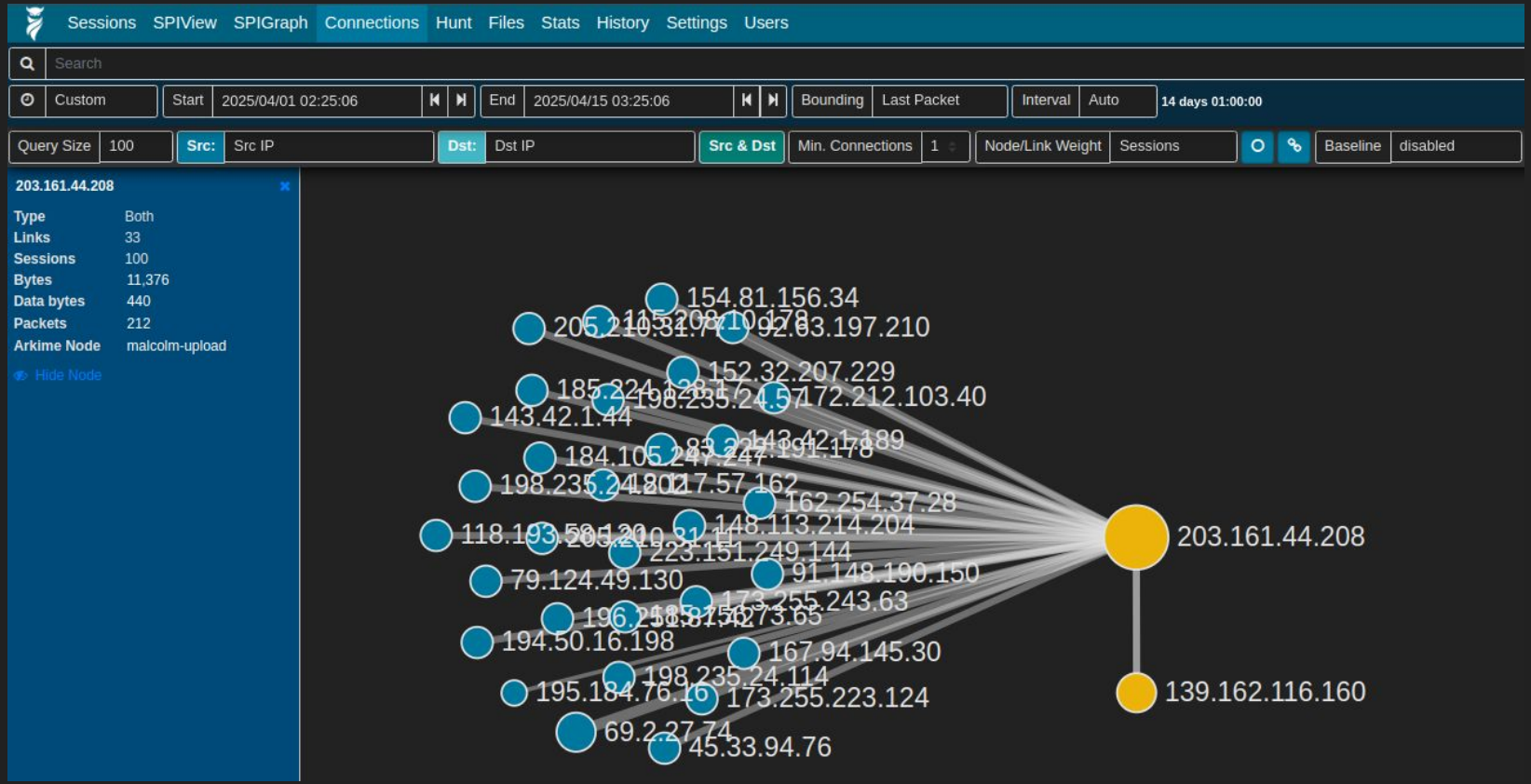
Malcolm is distributed as an ISO image (based on stable Debian) preconfigured with necessary docker images and helper scripts. Successful installation runs a web server.



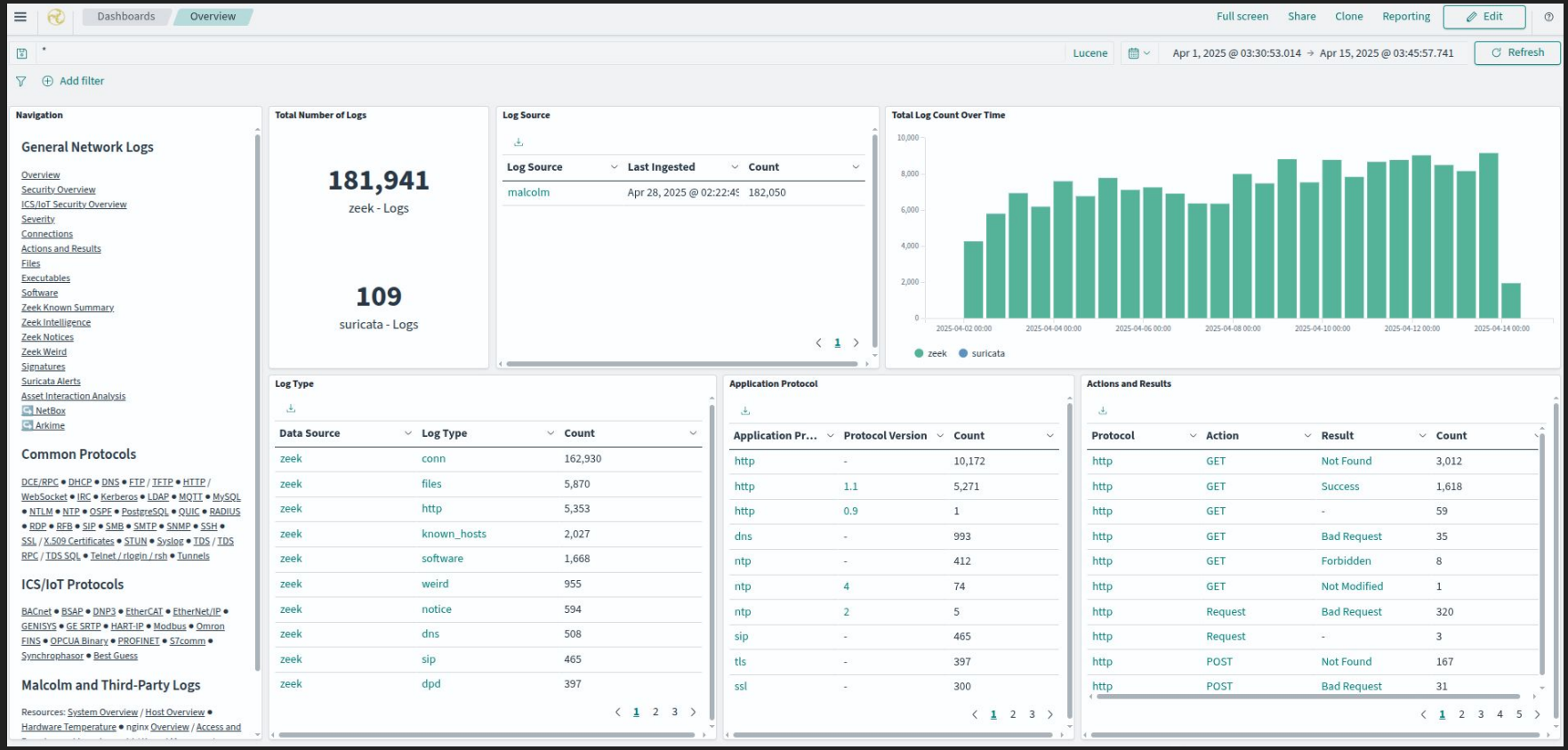
Arkime Sessions View

- **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

DNS - Queries

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

1 2 3 4 5 6

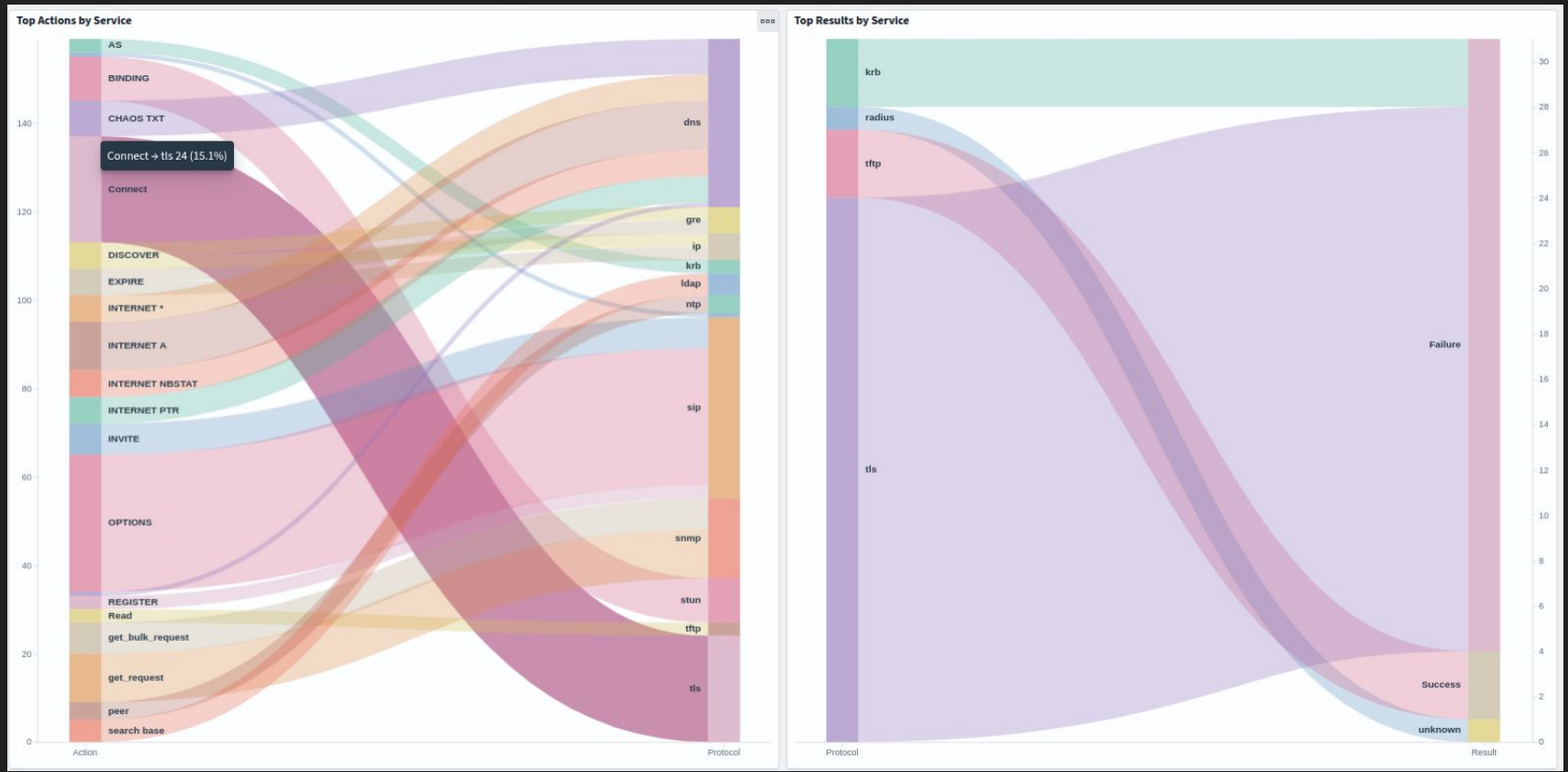
Connections - Source MAC Address

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

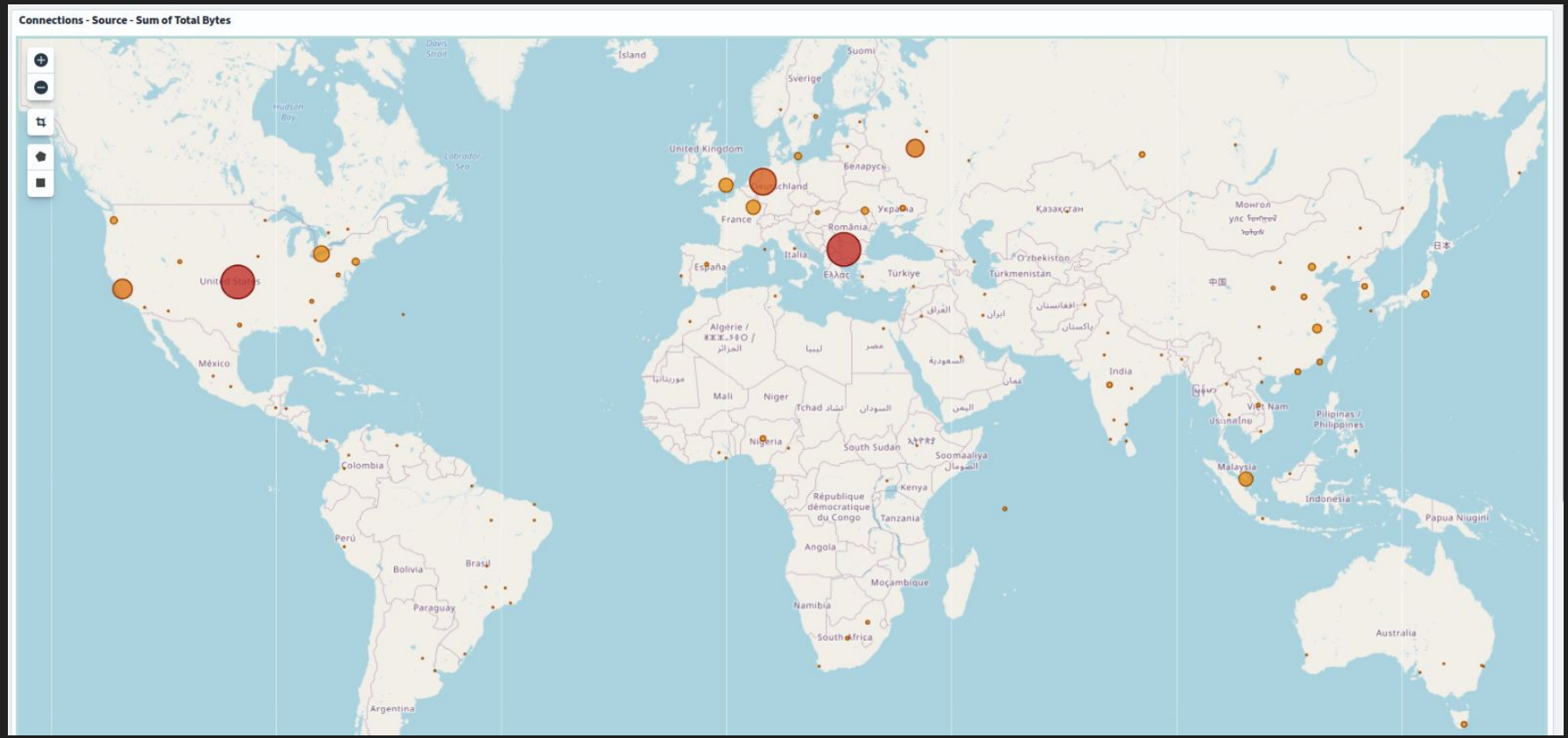
Connections - Destination MAC Address

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)

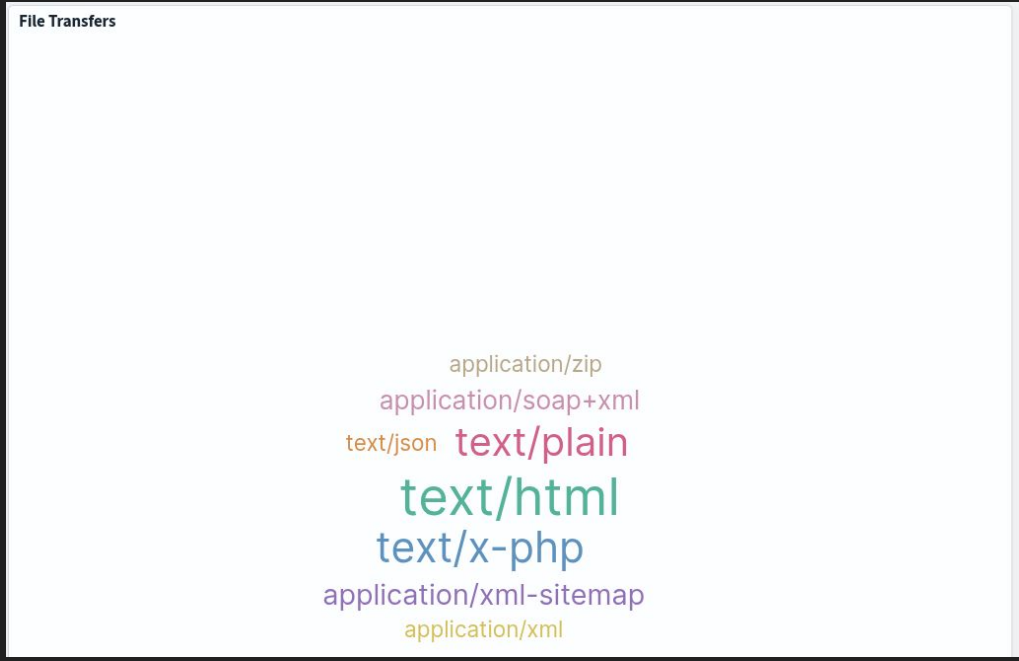


Connections - Source by Total Bytes



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

File Transfers

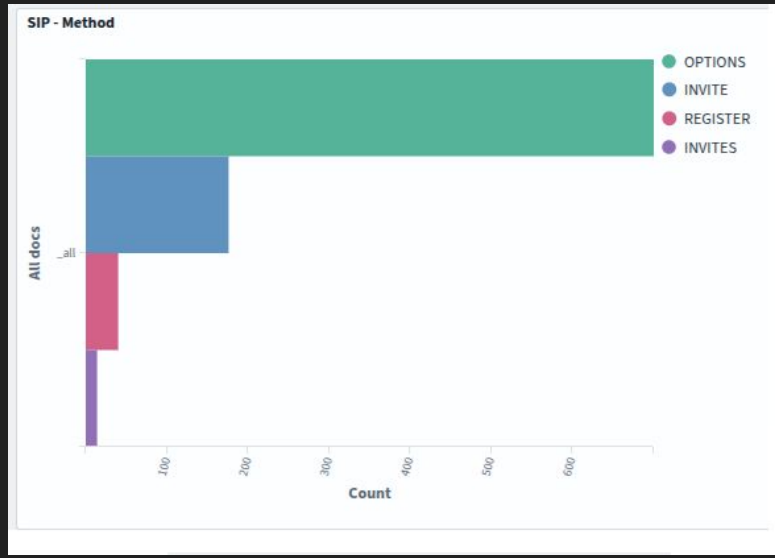


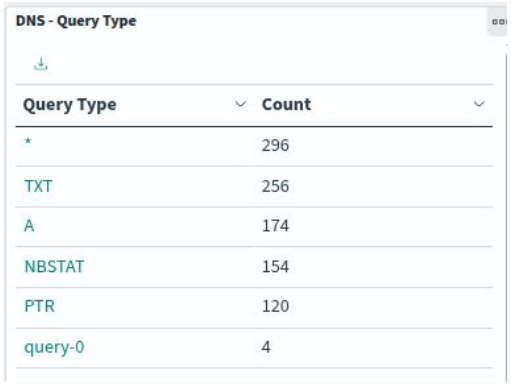
DNS Queries by Randomness

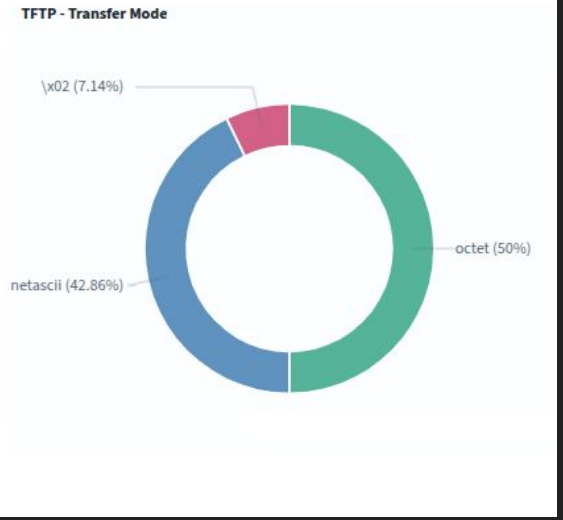
DNS Query	Randomness Score (method 1)	Rando...	Count
wzb.eu	0.08730000257492065	0.150099992	3
kdl.xyzdns.xyz	0.7200999855995178	1.488700032	1
mz.gov.pl	2.6259000301361084	2.868000030	2
u7f1x4.cba12cd0.n24951	2.805000066757202	3.158600091	2
tool.lu	3.3610999584198	4.827000141	1
0-cba12cd0-202504081-g	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-	4.3769001960754395	6.479400157	1
_services._dns-sd._udp.	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.







Directory Listing of Captured files

Directory listing for /

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

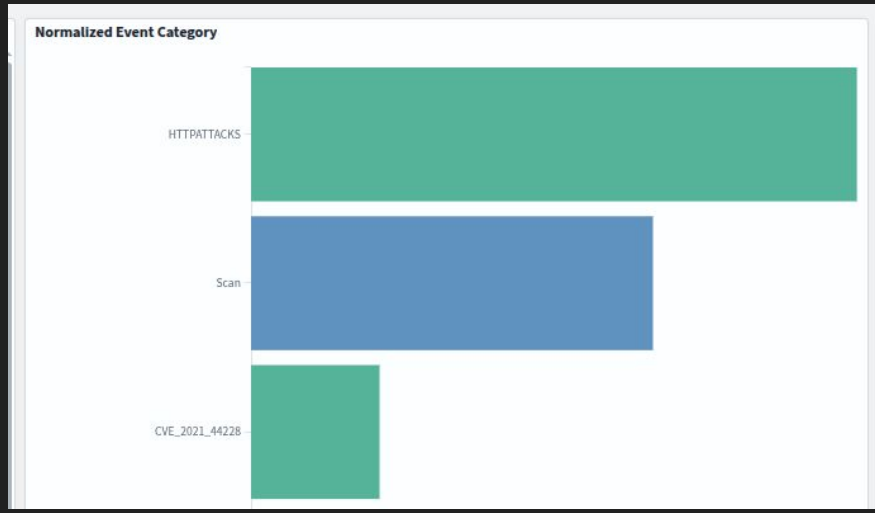
/extracted-files/HTTP-FC8yQS1u7LgrjRdZRh-C2HW4j1pcC3QfMg44i-20250402030252.html

Welcome to www.wiresharkworkshop.online!

Email: info@wiresharkworkshop.online

Security Overview Dashboard

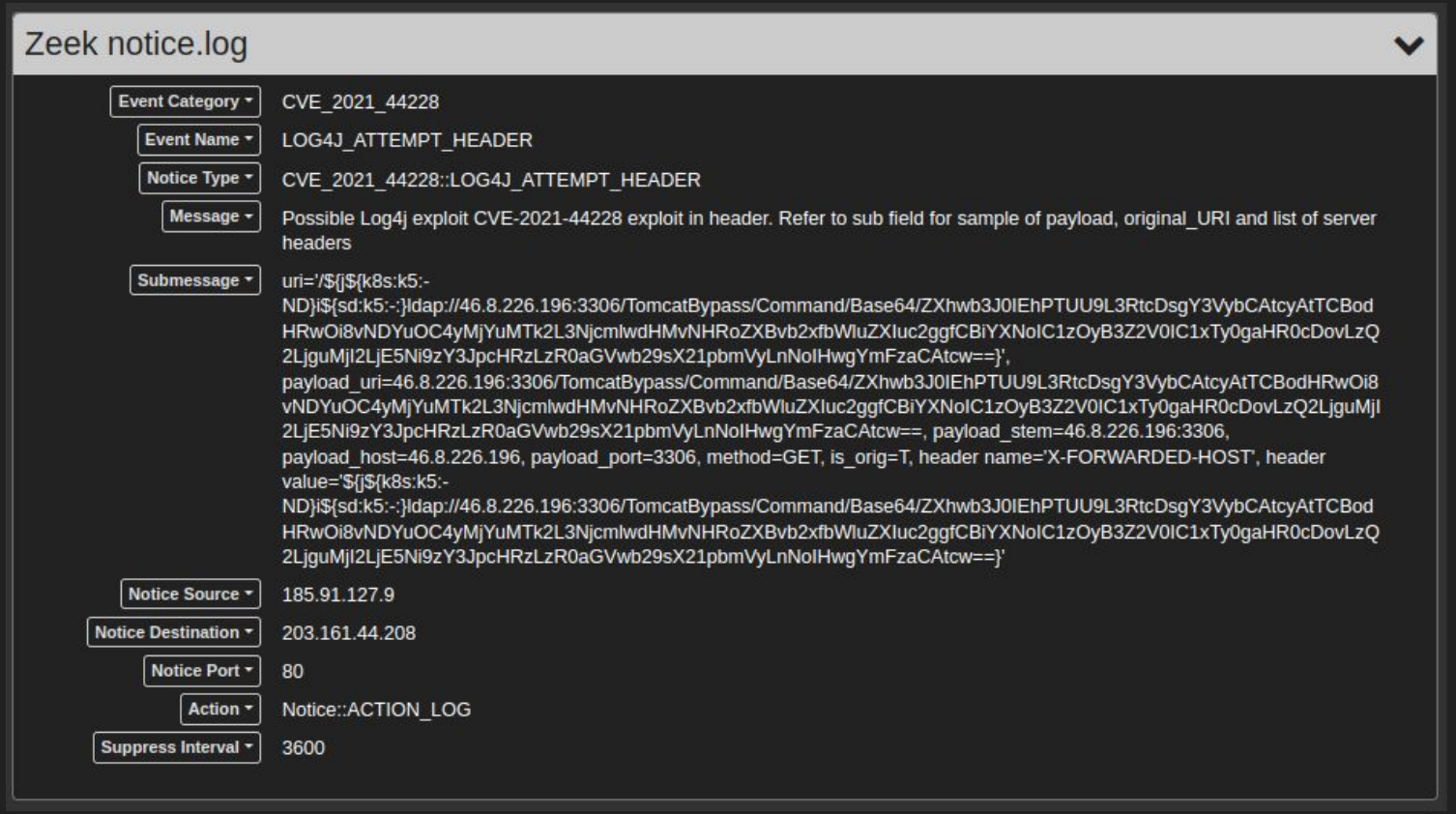
Show top notices and alerts from Zeek and Suricata: multiple port scan attempts, HTTP smuggling payloads, and a payload for a known Log4j header injection exploit



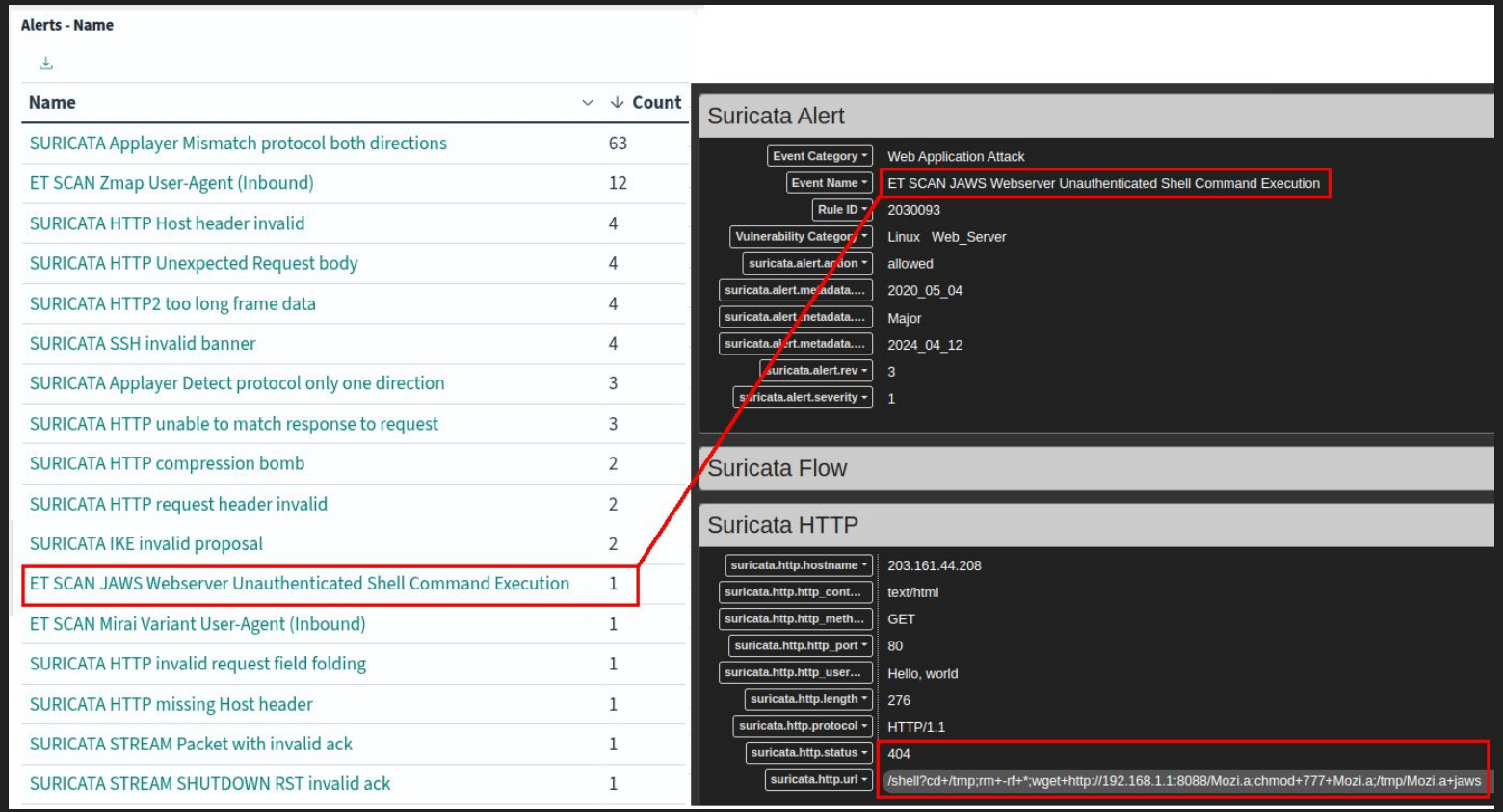
Notice, Alert and Signature - Summary

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 Sca	ET SCAN Zmap User-Agent (	12
suricata	alert	Attempted Administrator Pr	ET SCAN Mirai Variant User-A	1
suricata	alert	Web Application Attack	ET SCAN JAWS Webserver U	1

Interesting Zeek Log

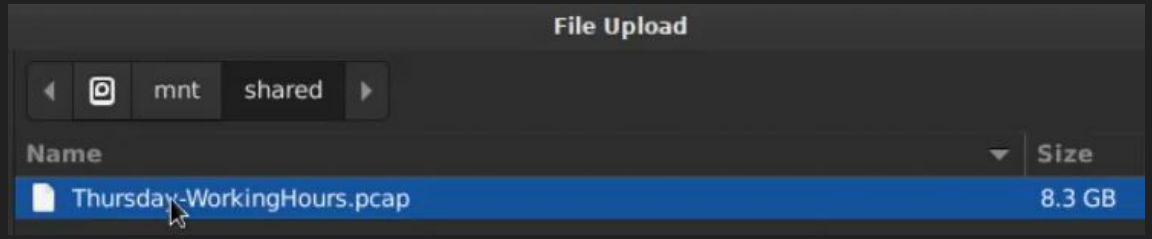


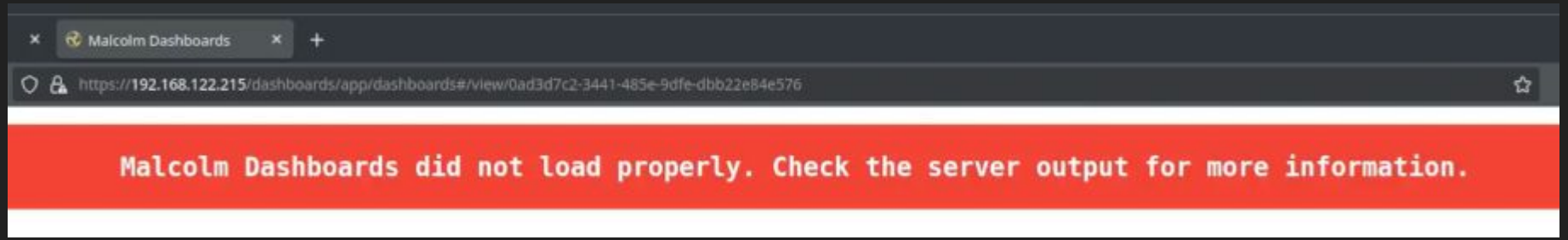
Interesting Suricata Alert



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://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