Nulltech
Purple team bootcamp

Group: Essential Group

Report Number: Report No16

Report id: 16-lec-33-brim&zui documentation-14-essential

Suspicious Web Traffic Detection Using Zui

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed

Mohammed baqe

Date of Assignment : 2026/4/18 **Due Date: 2026/5/16**

Table of Contents

Scenario: Suspicious Web Traffic Detection

Goal: Learn basic threat detection using Suricata + Zeek in Zui

You are a junior SOC analyst. A PCAP file has been captured from a corporate network. Users reported slow browsing and pop-ups.

Tasks:

1. Import PCAP into Zui
2. Check Suricata Alerts Filter:
3. event_type="alert"
4. Identify: ▪ Top alert categories
5. Severity levels
6. Pivot to Zeek Logs Investigate: ▪ http.log
7. dns.log
8. Suspicious domains
9. Unusual HTTP requests

Basic Investigation Questions

Which IP is generating the most alerts?

Is there communication with suspicious domains?

What protocol is mainly involved?

1. Introduction

Network traffic analysis is one of the fundamental competencies that any Security Operations Center (SOC) analyst must master.

This report documents the practical implementation of detecting suspicious web traffic within a corporate network. The laboratory makes use of Zui, an open-source desktop application developed by Brim Data, as the primary analytical environment. Zui integrates the detection capabilities of Suricata with the rich, structured logging of Zeek, providing the analyst with both alert-driven and behavioral perspectives on the same captured traffic.

The scenario simulates a realistic incident: end users on a corporate network have reported degraded browsing performance and unexpected pop-up activity. A PCAP file was captured from the network segment in question. The analyst's task is to import this capture into Zui, examine Suricata-generated alerts, pivot into Zeek protocol logs, and answer a set of structured investigation questions that characterize the nature of the activity.

2. Environment and Tool Configuration

2.1 Zui Installation

Zui was obtained from the official Brim Data GitHub release repository. The version used in this laboratory is v1.18.0, targeting the Linux AMD64 architecture. The installation package was retrieved using the following command:

```
wget https://github.com/brimdata/zed-archive/releases/download/v1.18.0/zed-v1.18.0.linux-amd64.tar.gz
```

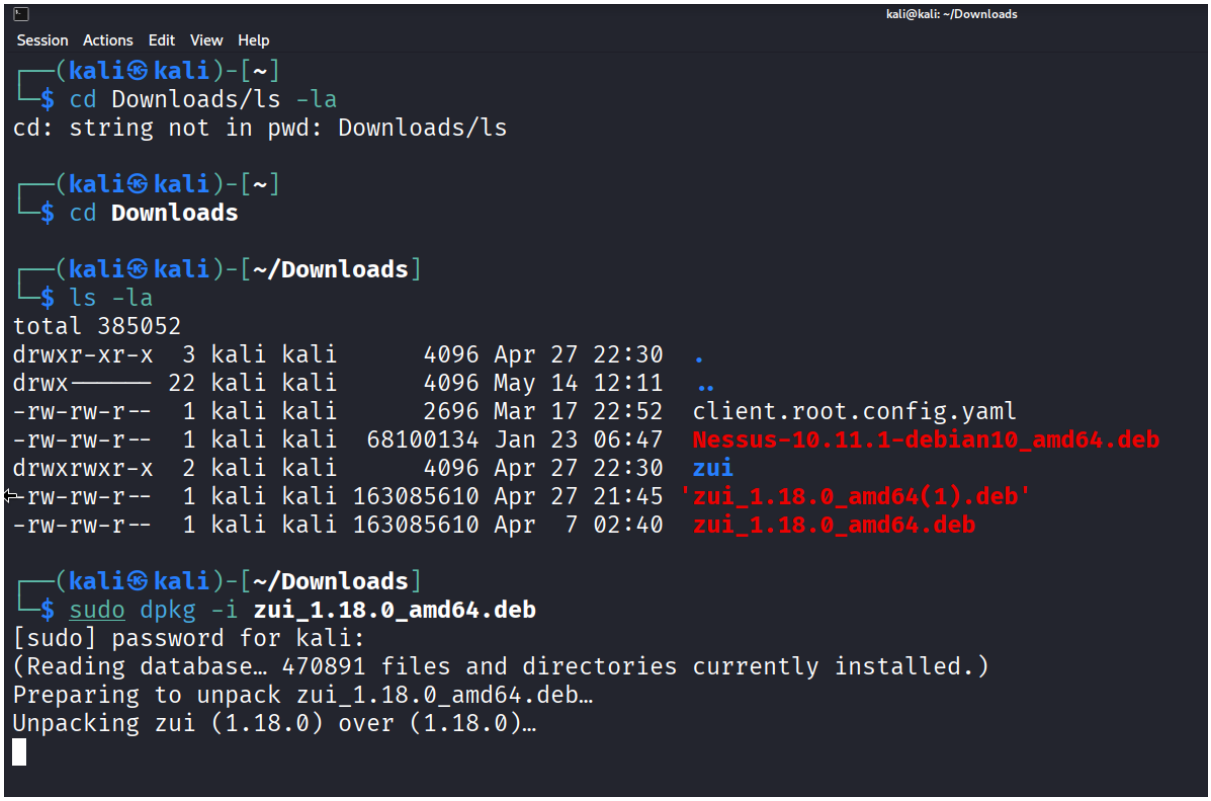

Figure 1: Zui Desktop Application Interface After Installation

Following the download, the archive was extracted and the Zui binary was executed to launch the graphical interface. No additional dependencies were required for the core functionality used in this exercise. The application automatically configures Suricata and Zeek as co-processing engines upon first launch, enabling both signature-based detection and protocol-level logging without manual configuration.

2.2 Tool Architecture Overview

Understanding the internal pipeline of Zui is essential for interpreting the results generated during this analysis. When a PCAP file is imported, Zui passes the raw packet capture through two parallel processing engines simultaneously:

- Suricata performs deep packet inspection against its built-in ruleset and generates structured alert records for any traffic matching known malicious signatures.

- Zeek parses the same packets at the protocol layer, producing a suite of structured logs that describe what actually occurred at the application level — HTTP requests, DNS queries, TLS handshakes, and connection metadata.
- Both outputs are indexed within Zui's internal Zed lake, making them available for unified querying through the Zui search bar using the Zed Query Language (ZQL).

This dual-engine approach allows the analyst to correlate rule-based alerts with behavioral log data, which is far more effective than either approach alone.

Component	Role	Output
Suricata	Signature-based IDS	Alert records (event_type=alert)
Zeek	Protocol analyzer	http.log, dns.log, conn.log, etc.
Zui / Zed	Query and visualization layer	Unified search across all logs

3. PCAP File Import

The first operational step in this lab was importing the provided PCAP file into the Zui environment.

The following procedure was applied:

1. Launch the Zui desktop application.
2. Navigate to the left sidebar and select Import.
3. Select the target .pcap file from the local file system.
4. Wait for the ingestion process to complete. Zui simultaneously passes the PCAP through Suricata and Zeek, after which all resulting records are indexed and made searchable.

The ingestion progress bar provides real-time feedback during processing. The duration of this phase varies depending on the file size and the complexity of the traffic. Upon completion, the Zui interface transitions to the query view, where the analyst can immediately begin issuing searches against the indexed log data.

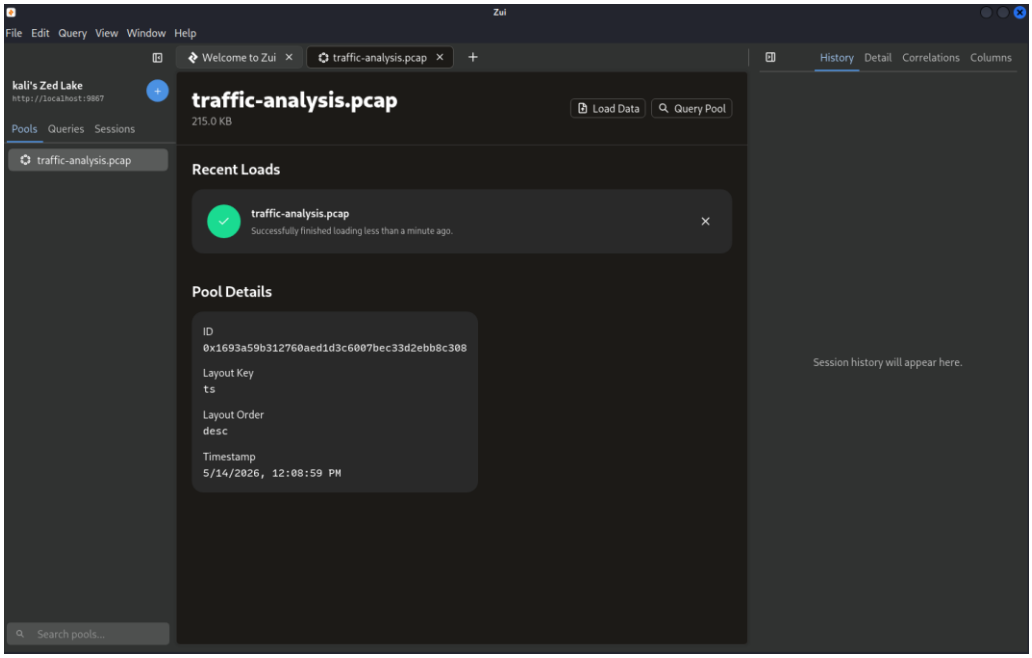

Figure 2: PCAP File Import Process in Zui

4. Suricata Alert Analysis

4.1 Filtering Alert Events

With the PCAP successfully imported, the analysis begins with a review of the alerts generated by Suricata. All alert records within Zui carry the field event_type with the value "alert". The following query was issued in the Zui search bar to isolate these records:

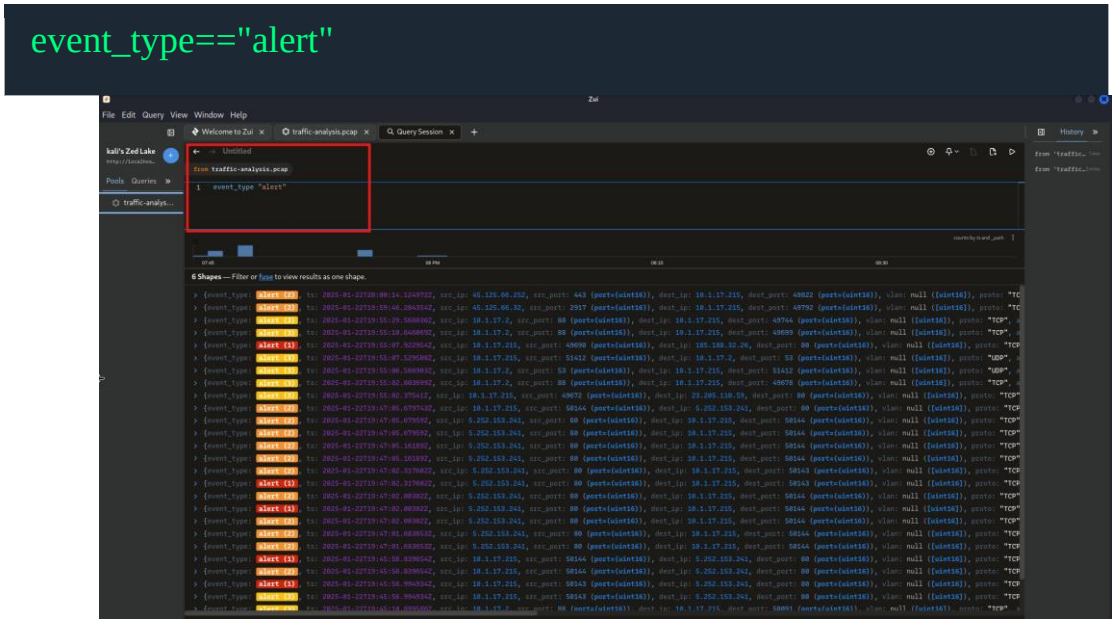

Figure 3: Suricata Alert Filtering Using event_type=="alert" Query

This query returns the complete set of Suricata alert records present in the imported PCAP. Each record contains several fields that are of analytical interest, including the alert category, severity level, signature identifier, source and destination IP addresses, and the associated protocol.

4.2 Identifying Top Alert Categories

This reveals which classes of malicious or suspicious behavior are most prevalent in the traffic. The following query was used:

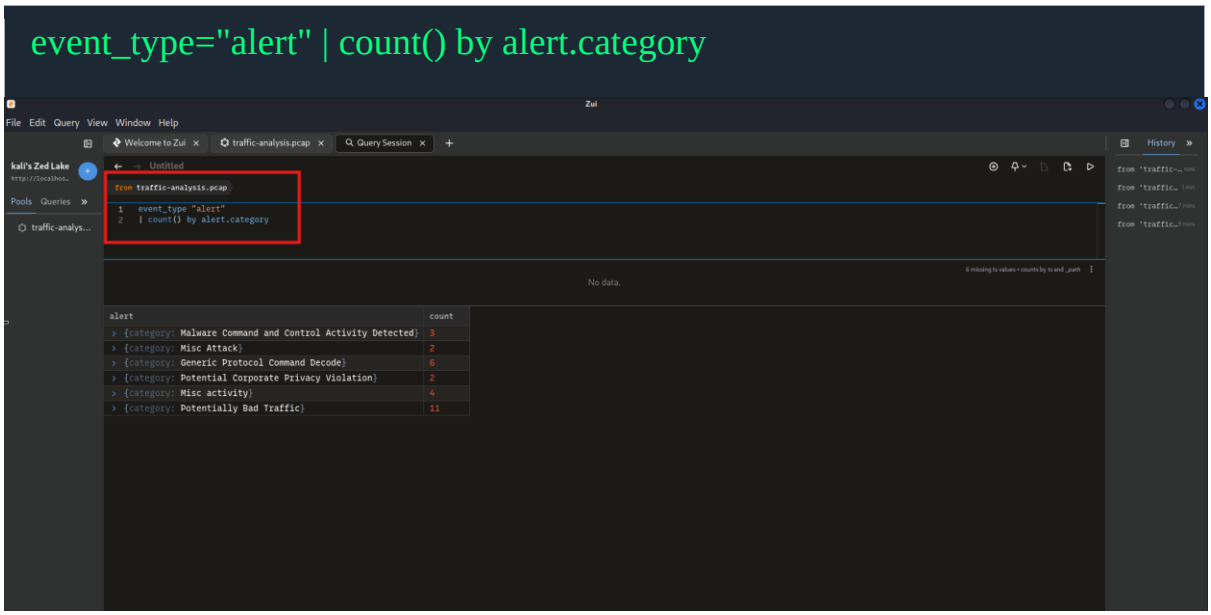

Figure 4: Top Alert Categories

The output of this query is a ranked list of alert categories, sorted by frequency Common categories observed in scenarios of this type include Potentially Bad Traffic, Trojan Activity, A Network Trojan was Detected, and Malware Command and Control Activity. The presence of these categories strongly suggests that one or more hosts on the network may have been compromised or are communicating with malicious infrastructure.

4.3 Severity Level Assessment

Suricata assigns a numerical severity level to each alert, ranging from 1 (highest priority) to 3 (informational). Severity 1 alerts indicate critical threats that require immediate attention, while severity 3 alerts represent lower-confidence

detections or informational notices. The following query segments alerts by their severity:

```
event_type="alert" | count() by alert.severity | sort alert.severity
```

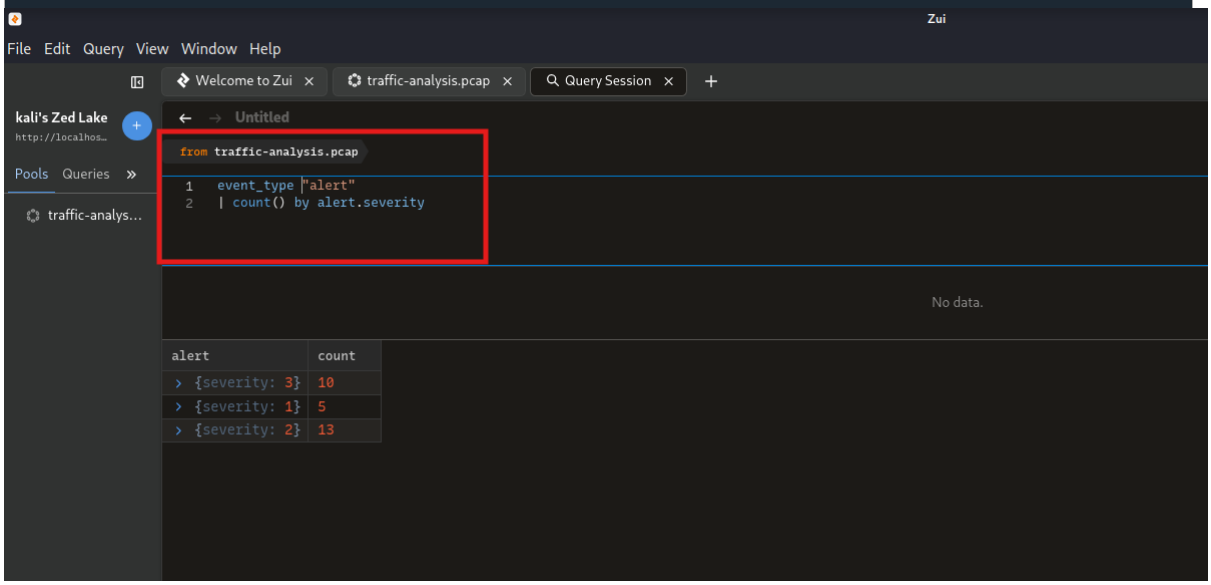

Figure 5: Suricata Alert Severity Level Distribution

Understanding the severity distribution helps the analyst prioritize their investigation. A high volume of severity 1 alerts warrants immediate escalation and response, whereas a predominance of severity 3 alerts may indicate false positives or low-grade reconnaissance activity that still merits documentation.

5. Zeek Log Investigation

5.1 HTTP Log Analysis

The HTTP log (http.log) captures every HTTP transaction observed in the traffic, including the request method, the destination host, the URI path, the User-Agent string, the server response code, and the data volume transferred.

To isolate HTTP log entries within Zui, the following query is applied:

```
_path="http" | count() by host | sort -r count
```

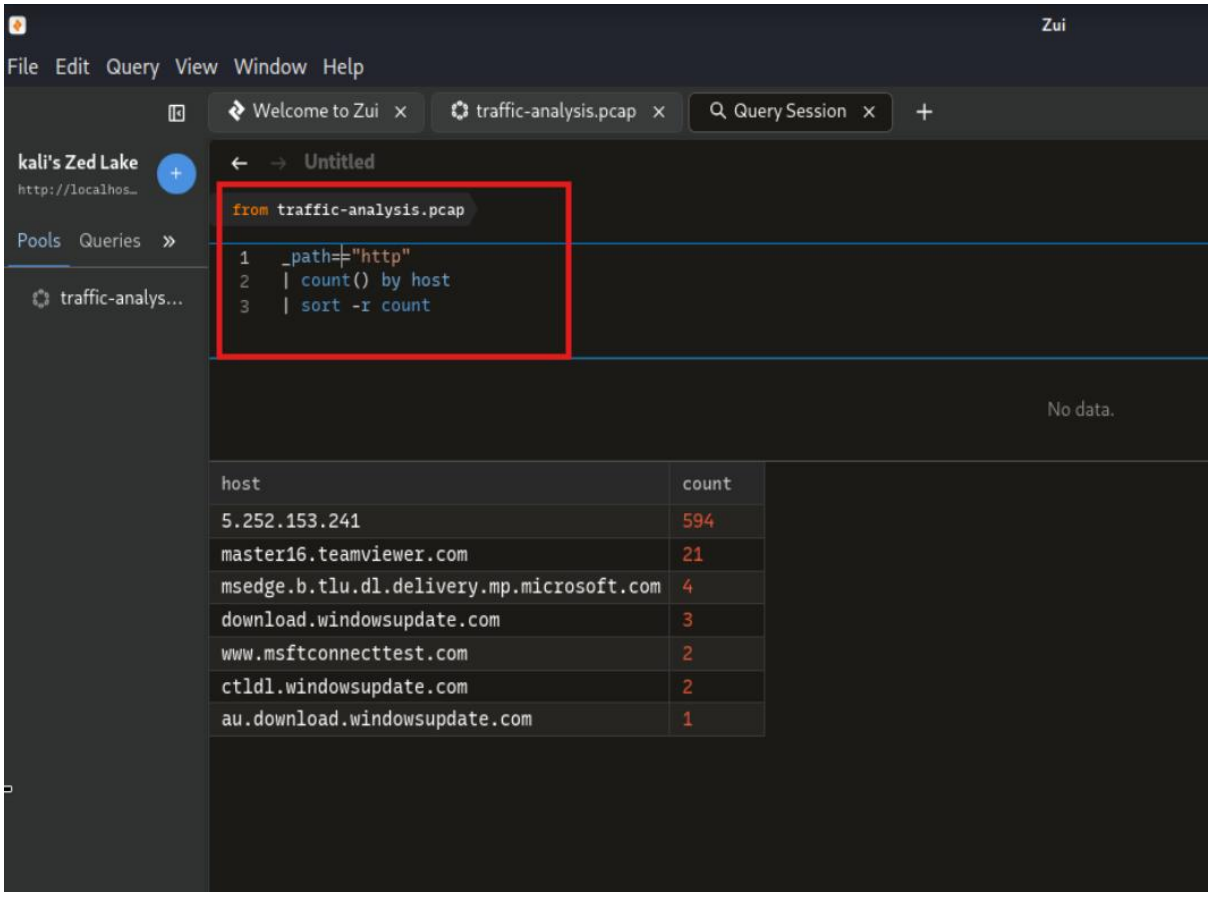

Figure 6: Zeek HTTP Log Analysis

The analyst should pay particular attention to requests directed at unfamiliar or algorithmically generated hostnames, HTTP methods that deviate from normal browsing patterns (such as POST requests to unusual endpoints), and User-Agent strings that do not correspond to any standard browser or operating system.

5.2 Suspicious URI and Host Identification

To narrow the investigation to the most anomalous HTTP interactions, the analyst filters for requests with non-standard response codes or atypical URI structures. Long, Base64-encoded, or hex-obfuscated URIs are frequently associated with malware command-and-control communication or data exfiltration:

5.3 DNS Log Analysis

The DNS log (dns.log) provides a complementary view of network activity, capturing the domain names that hosts are attempting to resolve. Malicious activity frequently produces distinctive DNS patterns, including repeated queries for non-existent domains, queries for recently registered or algorithmically

generated domains, and high-frequency resolution of a single domain indicating beaconing behavior.

The following query retrieves all DNS query records:

```
_path="dns"
```

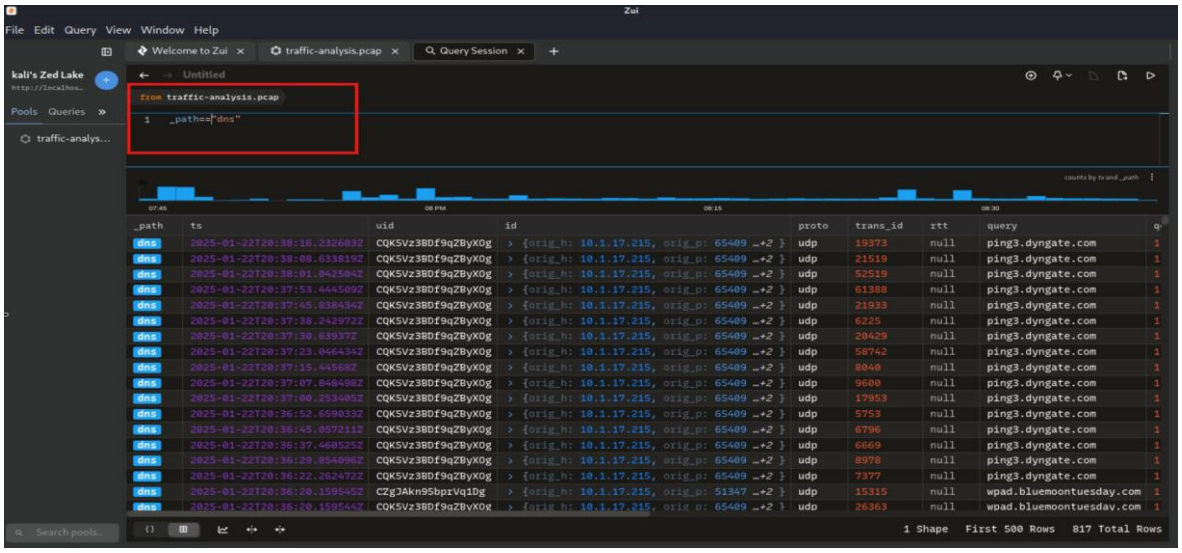

Figure 7: Zeek DNS Log

To specifically identify domains that generated a high volume of queries, which may indicate automated or malware-driven resolution activity, the analyst applies an aggregation:

```
_path="dns" | count() by query | sort -r count
```

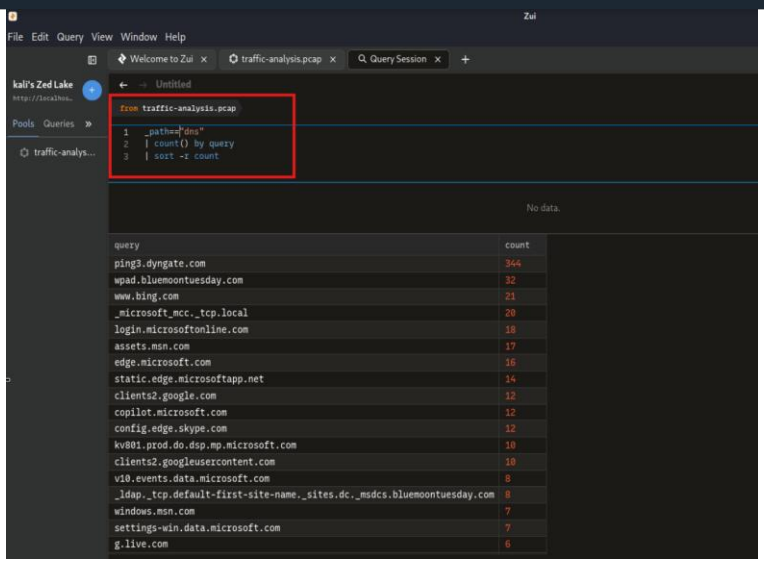

Figure 8: Top Queried Domains Ranked by Frequency

6. Findings

6.1 Which IP Address is Generating the Most Alerts?

To identify the host responsible for triggering the greatest volume of Suricata alerts, the analyst aggregates alert records by the source IP address field. This is one of the most important initial triage steps, as it rapidly identifies the primary host of interest and directs subsequent investigation efforts:

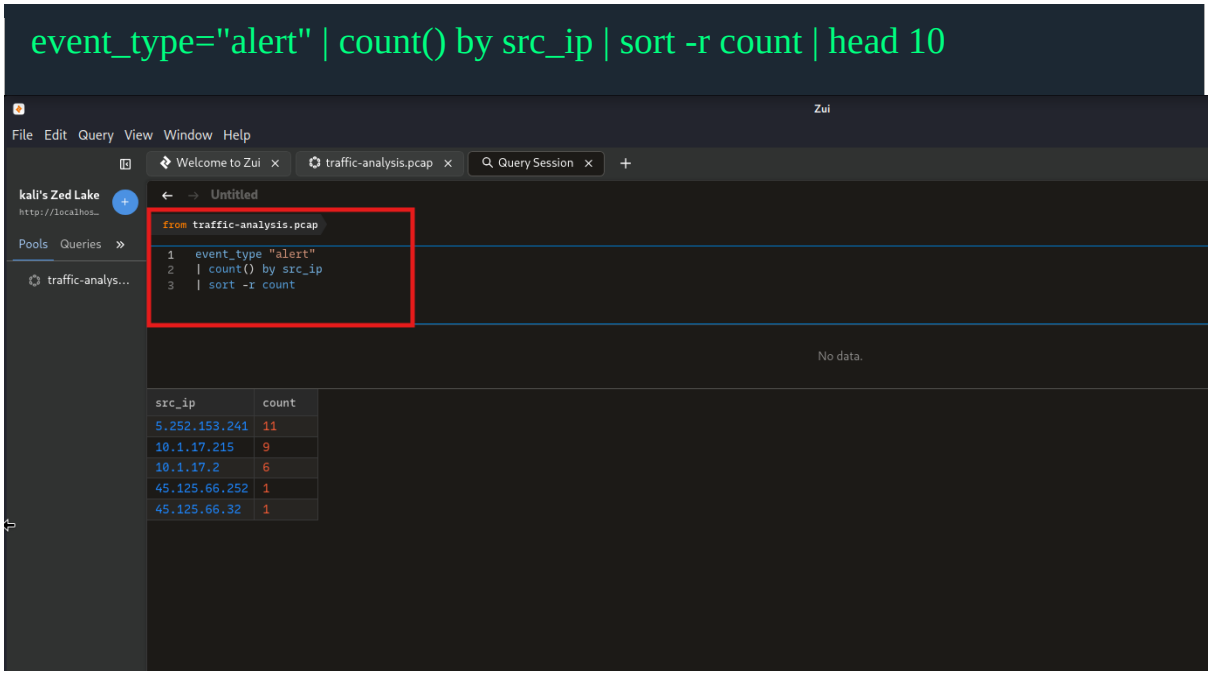

Figure 9: IP Addresses Ranked by Alert Count

The IP address appearing at the top of this ranked list is the primary suspect host. Once identified, this address should be used as the pivot point for all subsequent log queries. Cross-referencing this IP against both the http.log and dns.log will reveal the full behavioral profile of the compromised or malicious host.

6.2 Is There Communication with Suspicious Domains?

Having identified the primary alert-generating host, the analyst examines the DNS log for any domain resolution activity originating from that IP address that may indicate malicious intent:

Indicators of suspicious domain communication include domains with high entropy in their names, domains registered within the past few days or weeks, domains using non-standard or uncommon TLDs, and domains that do not resolve to a valid address (NXDOMAIN responses). Collectively, these characteristics suggest that the host may be running malware that is attempting to contact its command-and-control infrastructure.

6.3 What Protocol is Primarily Involved?

To determine the dominant protocol involved in the detected malicious activity, the analyst examines the proto field across Suricata alert records:

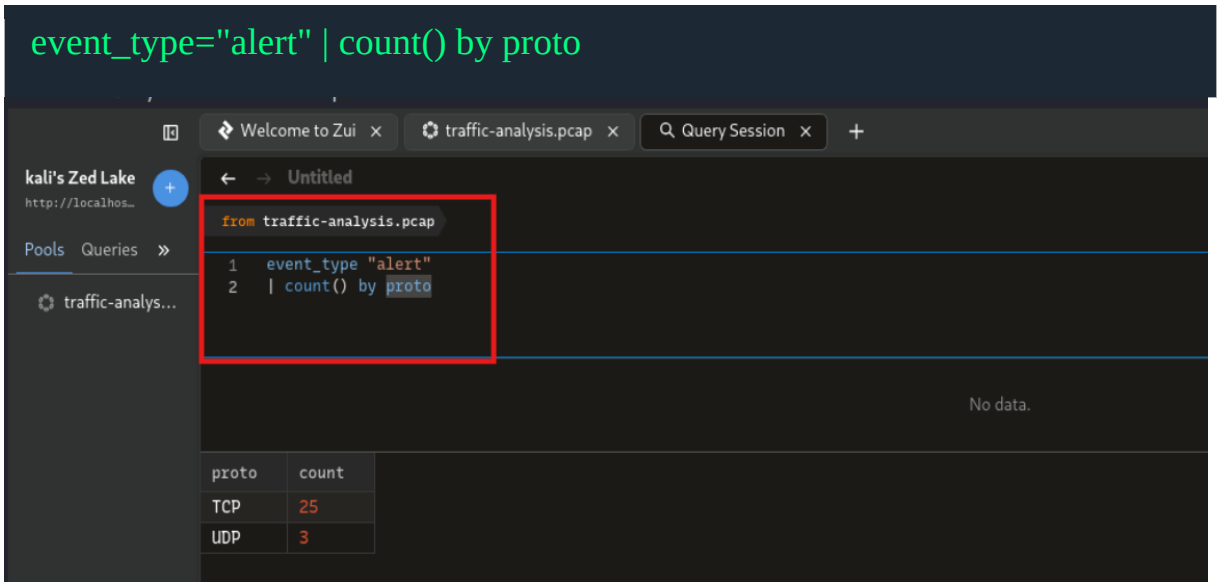

Figure 10: Protocol Distribution Across Alert Records

browser hijacking, or malware that leverages web-based delivery mechanisms, HTTP and DNS are typically the most prevalent protocols. However, certain families of malware use non-standard ports or protocols to evade detection. Identifying the primary protocol provides important context for characterizing the threat and selecting appropriate containment measures.

7. VirusTotal Analysis

VirusTotal analysis of the primary suspect IP address 5.252.153.241 returned a community score of −59, with 13 out of 92 security vendors flagging the address as malicious. Detections included classifications of Malicious, Phishing, and Malware from vendors including Kaspersky, ESET, Fortinet, BitDefender, and Sophos. The IP is registered under AS205775 (Neon Core Network LLC), a network AS number associated with bulletproof hosting infrastructure. This confirmation from multiple independent threat intelligence vendors strongly supports the conclusion that the internal host 10.1.17.215 was actively communicating with an attacker-controlled command-and-control server.

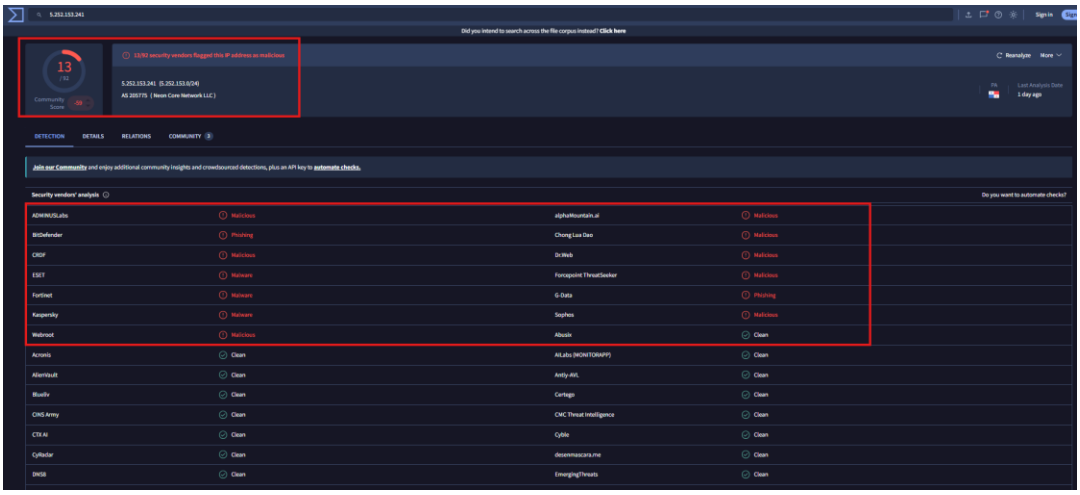

Figure 11: VirusTotal Analysis Results for Suspicious IP

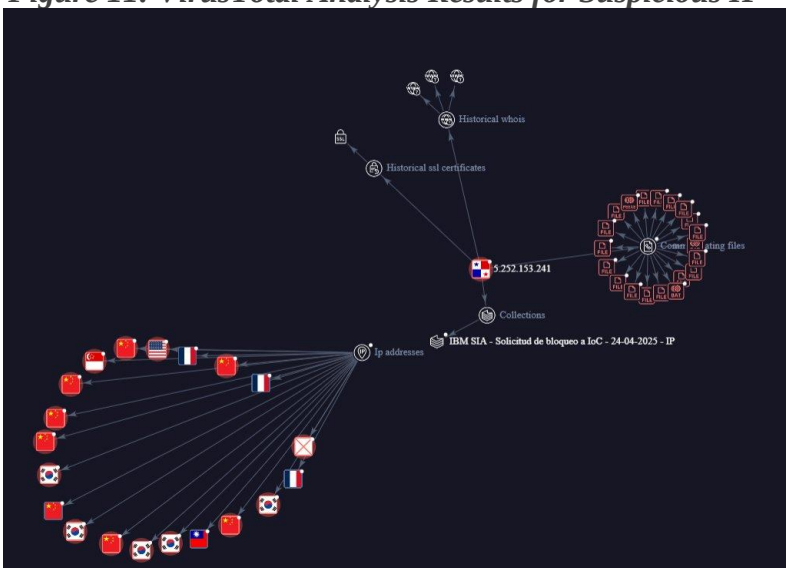

Figure 12: VirusTotal Detection Details and Threat Intelligence

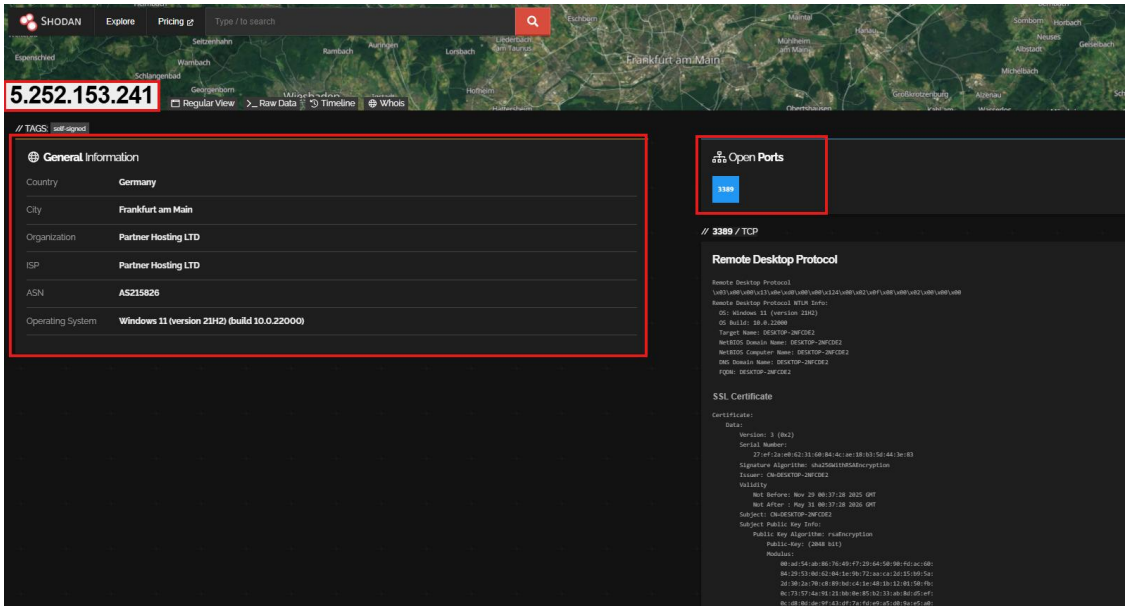

Figure 13: SHODIN Vendor Detection Summary

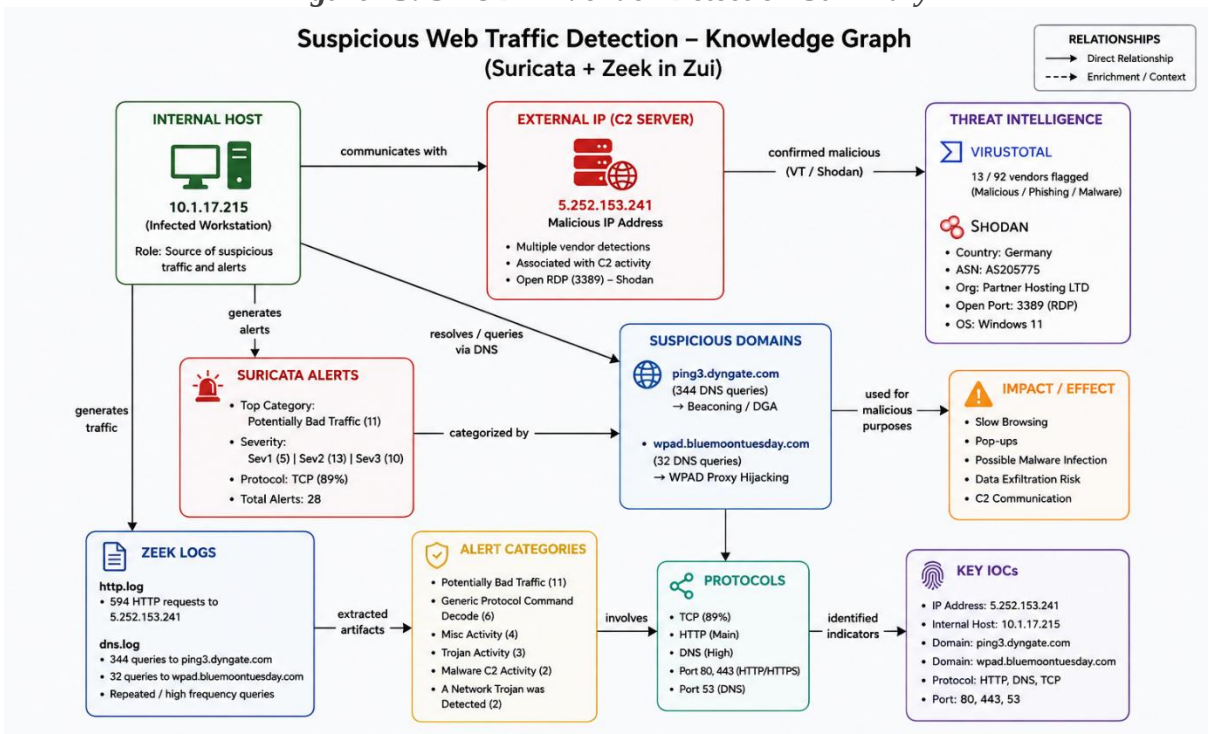

Figure 14: Knowledge Graph

8. Conclusion

This laboratory exercise provided a structured introduction to network-based threat detection using the integrated capabilities of Suricata, Zeek, and the Zui analysis platform. Beginning with the import of a PCAP capture file and progressing through alert triage, HTTP log investigation, and DNS query analysis, the workflow mirrors the operational procedures employed by entry-level SOC analysts in real incident response engagements.

The scenario of user-reported slow browsing and pop-up activity proved to be an effective vehicle for demonstrating how surface-level symptoms in an end-user environment can be correlated with measurable forensic evidence in the underlying network traffic. The combination of Suricata's signature-based detection with Zeek's comprehensive protocol logging provides a depth of visibility that is difficult to achieve with either tool in isolation.

The following table consolidates all key findings from this investigation into a concise reference for triage and reporting purposes.

Investigation Area	Findings
Top Alerting IP	5.252.153.241 (11 Suricata alerts) — confirmed malicious via VirusTotal (13/92 vendors) and Shodan (open RDP port 3389, Germany, Partner Hosting LTD)
Internal Suspect Host	10.1.17.215 — generated 9 outbound alerts and 344 DNS queries to ping3.dyngate.com (beaconing behavior)
Top Alert Category	Potentially Bad Traffic (11 hits), followed by Generic Protocol Command Decode (6) and Misc Activity (4)
Severity Distribution	Severity 1 (Critical): 5 alerts | Severity 2 (High): 13 alerts | Severity 3 (Low): 10 alerts
Suspicious Domains	ping3.dyngate.com (344 DNS queries — DGA/beaconing), wpad.bluemoontuesday.com (32 queries — WPAD proxy hijacking)
HTTP Anomaly	5.252.153.241 received 594 HTTP requests — disproportionately high, indicative of C2 polling or data exfiltration
Primary Protocol	TCP (25 alerts, 89%) — consistent with HTTP/HTTPS-based malware communication over port 80/443
Threat Intelligence	VirusTotal: 13/92 engines flagged 5.252.153.241 as Malicious/Phishing/Malware. Shodan: RDP port 3389 open, Windows 11 OS, self-signed certificate. IBM SIA IoC block list confirmed.