Nulltech
Purple team bootcamp

Network Forensics & Packet Analysis

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed

Mohammed baqer

Contents

`

1.1 Wireshark

Wireshark is the heavy great GUI, very powerful. It supports two main things we care about:

- Packet Analysis going deep inside individual packets
- Log Analysis working with network event logs

The problem with Wireshark? When the file gets large let's say more than 200 MB it starts getting really slow. It doesn't handle big files well.

1.2 Zeek

Zeek is interesting. You can use it for packet analysis, and you can also use it to see the logs things like HTTP logs, SSH logs

Zeek handles big files better. But here's its problem: it has no GUI. You're working in the command line the whole time. If you're comfortable doing everything without a graphical interface, great

1.3 Brim / Zui The Best of Both Worlds

This is where Brim comes in. Brim which now uses an interface called Zui was designed to fix the problems of the other tools:

- It HAS a GUI unlike Zeek alone
- It handles large files more than 200 MB, no problem
- It uses modern backend processing, so it opens files much faster
- It has two powerful modes: Ztools and Stream
- It has builtin visualization
- It supports ZQL (Zeek Query Language) a query system to search your data precisely

`

So in short: Brim gives you Zeek's power with a proper graphical interface that can handle large files. That's why it's our tool of choice today.

1.4 NetworkMiner

All the tools we mentioned work by capturing packets and storing them which requires a lot of storage. Think about it: if I'm capturing traffic all day, I could be storing hundreds of megabytes or gigabytes every single day.

NetworkMiner solves this differently. Instead of capturing and storing raw packets, it analyzes the traffic and gives you a summary it tells you what happened on the network without keeping all the raw data. This means:

- Much less storage required
- You get visibility across more locations
- Useful where full packet capture isn't practical

So NetworkMiner is great for when you need broad visibility without the storage cost of full packet captures.

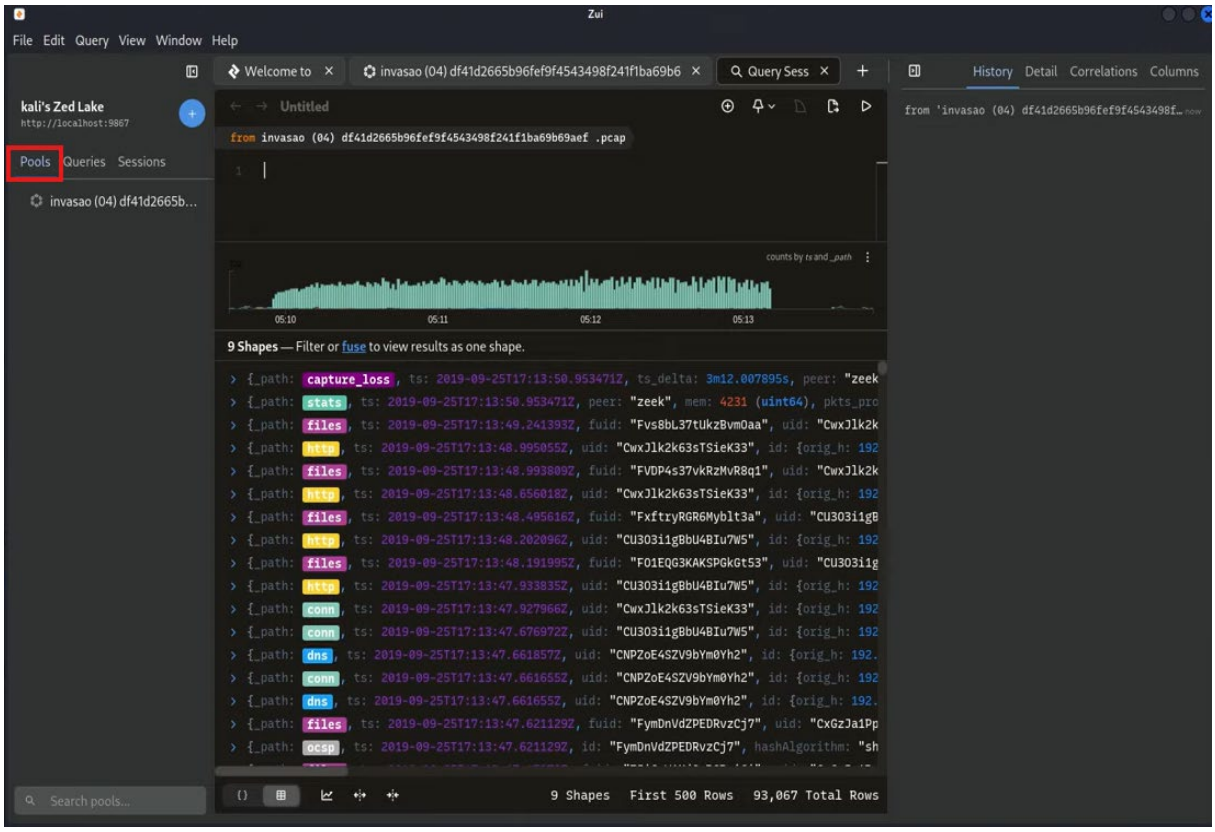
2. The Zui Interface

When you open Zui and load a PCAP file, you'll see several panels. Let me explain each one:

2.1 Left Panel Pools and Queries

This is your data source panel. It lists your loaded PCAPs and saved queries. You'll see something like 'Sample1.pcap' listed here. You can also use the + button to add new PCAPs or create new queries.

`

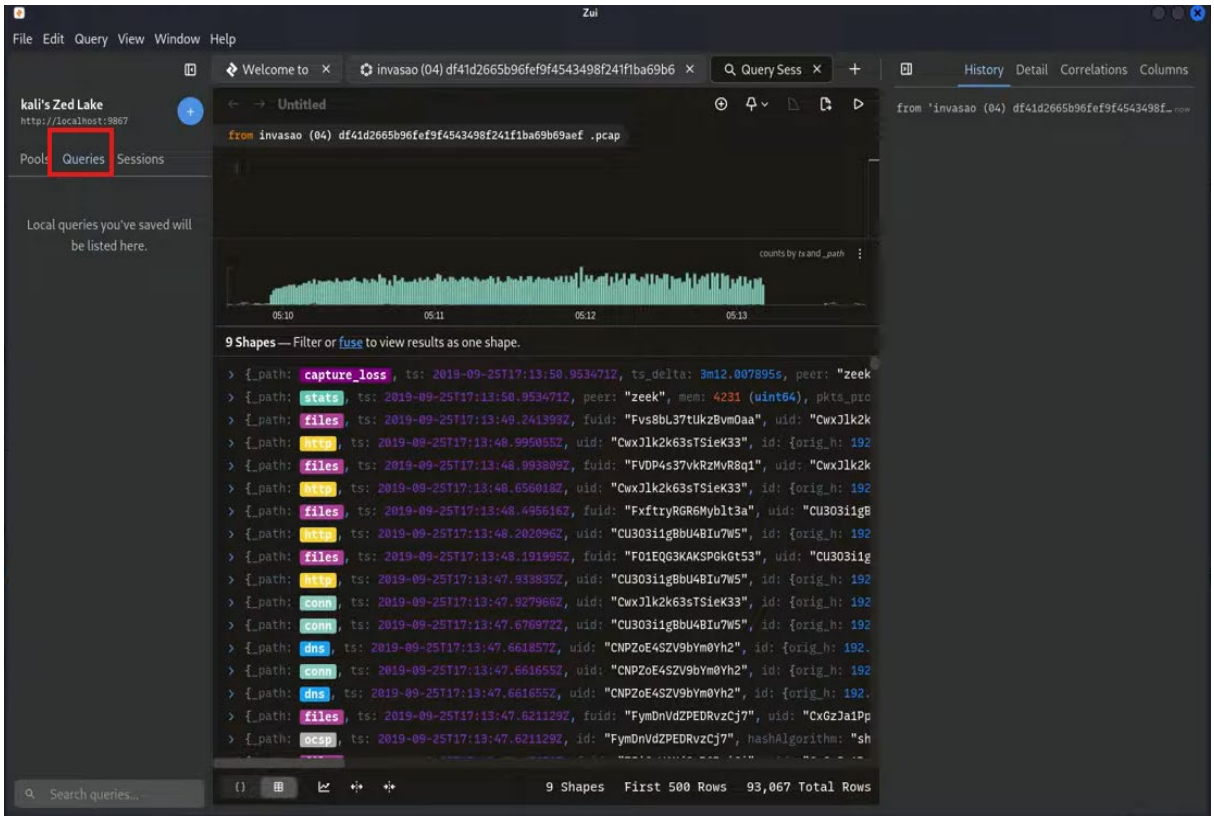


2.2 Query Editor

This is where you write ZQL Zeek Query Language. Think of it as the command prompt of Zui. You type what you're looking for, press Enter, and Zui filters the data accordingly.

> **Example query:** *event_type == "alert" This pulls only Suricata alert events from your PCAP.*

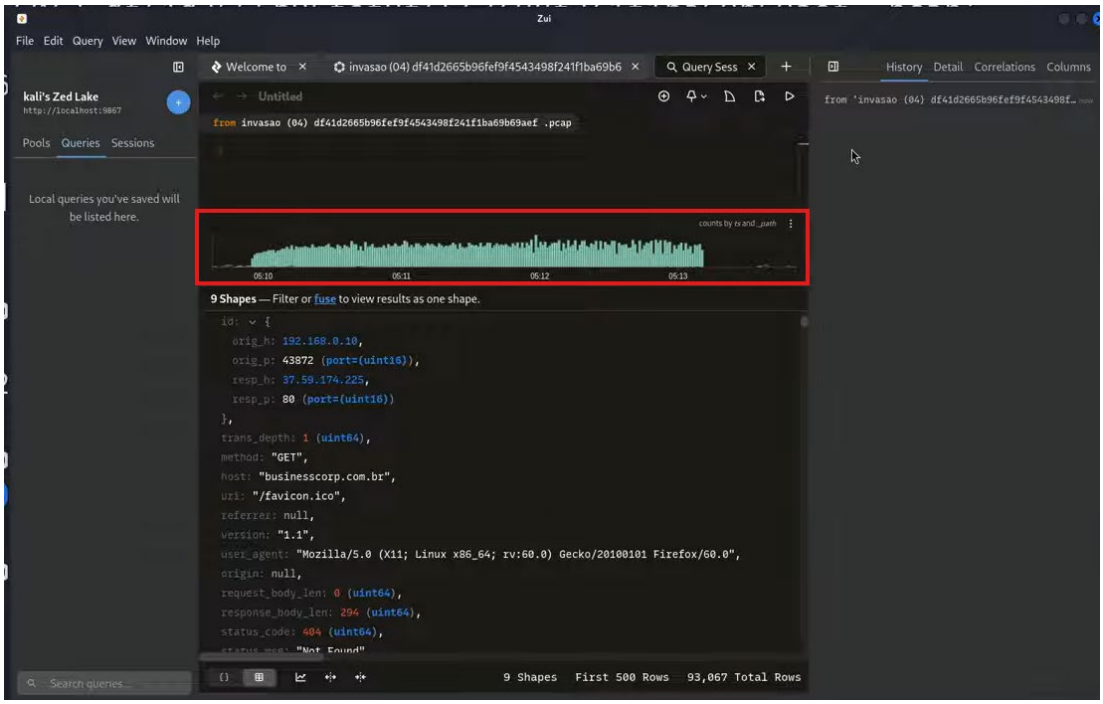
`



2.3 Visualization Panel The Time Series Graph

This panel draws a graph of network traffic over time for example, from 10 AM to 5 PM, it shows you how many connections happened at each point. This is extremely useful because you can immediately see traffic patterns and spikes. If there's a sudden spike at 2 AM, that's suspicious and worth investigating.

`



2.4 Data Table The Event List

This is the main area where your events appear. Every row is a network event. Each event has attributes like:

- ts the timestamp (when it happened)
- id.orig_h source IP (where it came from)
- id.resp_h destination IP (where it went)
- Ports, protocols, and event types

2.5 Right Panel History, Details, Columns

The right panel has three useful sections:

- History shows your previously run queries, so you can go back and reuse them
- Details when you click on an event, this shows you its full details (every field of that specific connection)
- Columns shows you all available data fields in the current dataset

`

3. Working with Suricata Alerts in Zui

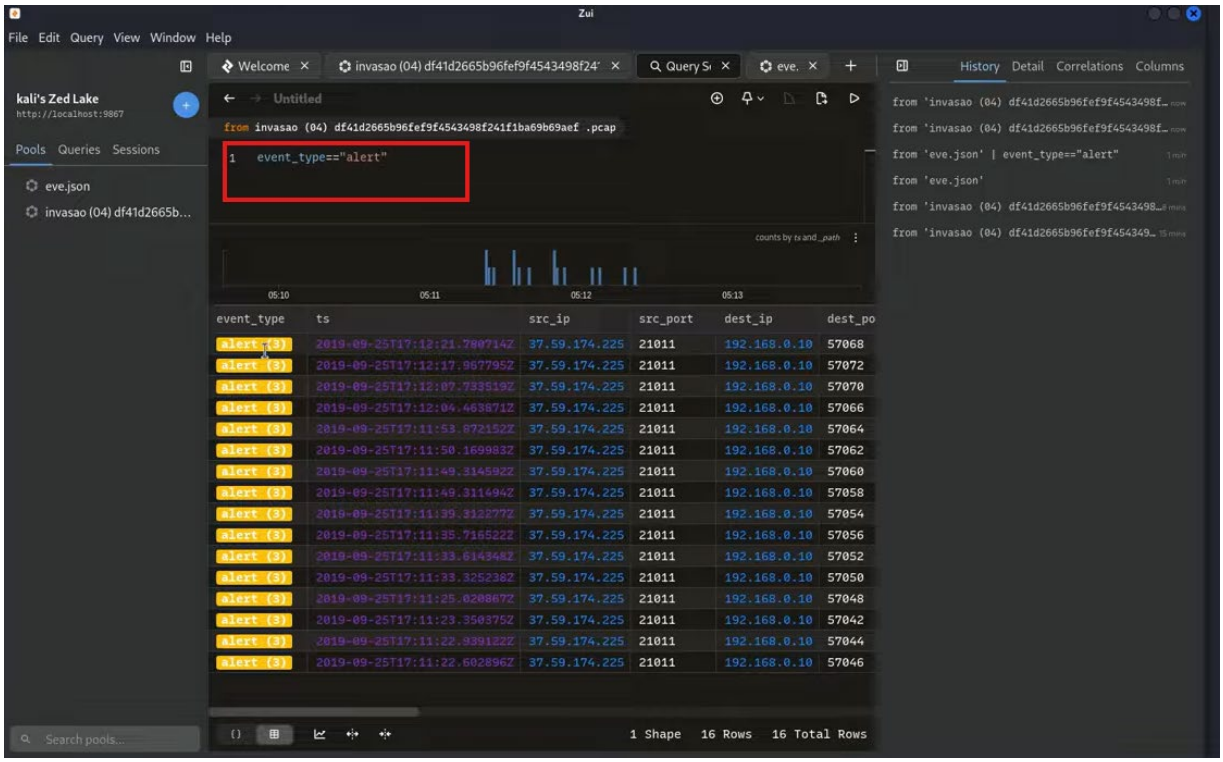
Suricata is our IDS Intrusion Detection System (and also IPS Prevention). It's what generates alerts when suspicious activity is detected. Remember, companies always care about their alerts that's their main interface with threats.

The idea is this: when there's a high volume event, you want to be able to centralize and see all the Suricata alerts quickly. That's where Brim/Zui shines it centralizes and visualizes those alerts for you.

3.1 Querying for Alerts

To filter down to only Suricata alerts, use this query in the Query Editor:

```
event_type == "alert"
```



When you run this, the Data Table will show you every alert with all its metadata:

`

- ts timestamp
- src_ip and src_port source address
- dest_ip and dest_port destination address
- proto protocol used
- alert.signature what signature triggered it
- alert.severity how serious it is
- alert.category what category of attack it is

3.2 Color Coding by Severity

Zui uses color coding to help you quickly spot critical alerts:

- Yellow Severity 3 (lower priority)
- Orange Severity 2
- Red Severity 1 (critical investigate immediately)

3.3 Count by Field

A very useful technique is 'Count by Field'. For example, if I want to see how many alerts triggered per category or per signature, I can group by that field. This immediately tells me which threats are most frequent so I know where to focus my investigation.

4. Exploring Zeek Logs in Zui

Zeek takes raw PCAP traffic and converts it into structured, organized log files. Each log type represents a different protocol or behavior.

The types of Zeek logs you'll commonly work with:

- conn.log all connections in the capture
- http.log all HTTP requests and responses

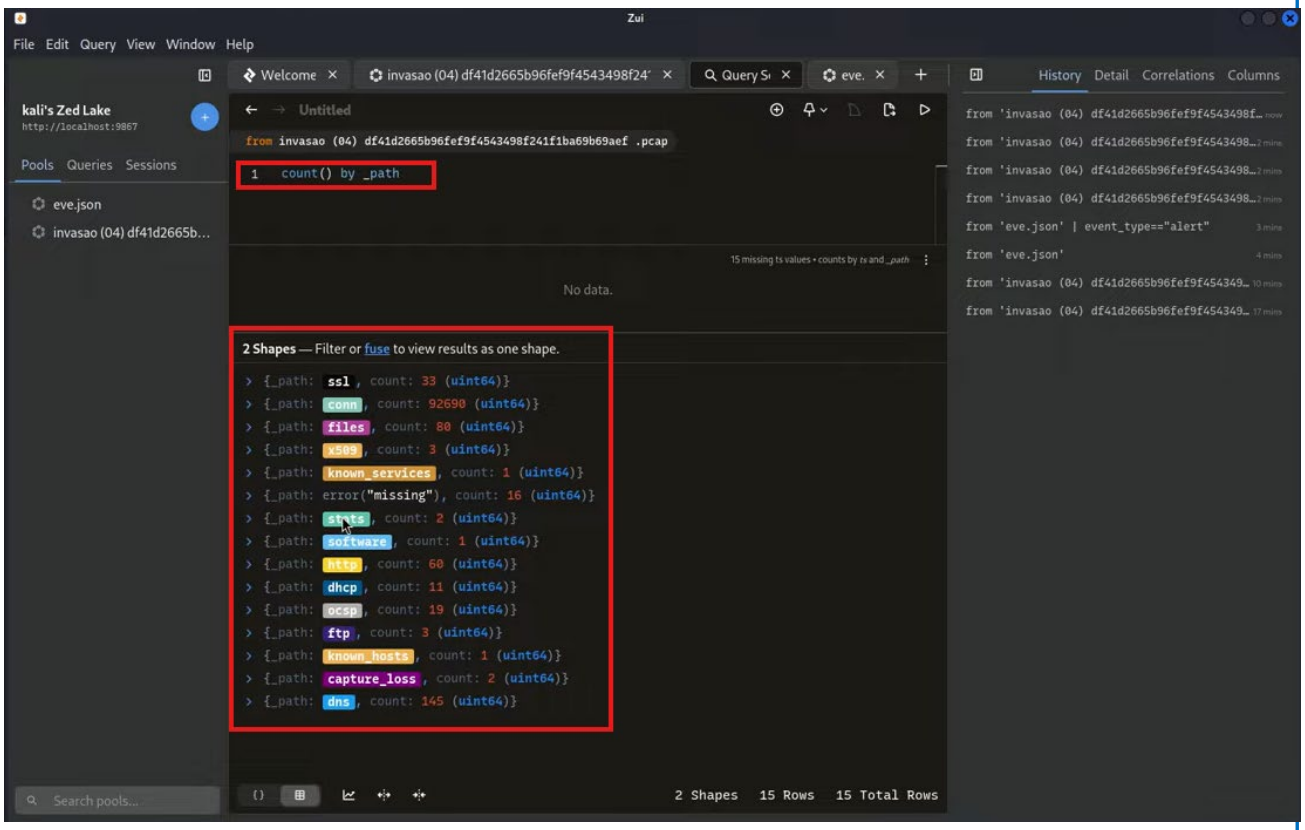
`

- dns.log all DNS queries
- ssl.log TLS handshake and certificate information
- And many others depending on the traffic

4.1 Listing All Log Types

One of the first things you do when you open a PCAP in Zui is list what Zeek logs are available. You do this with the following query:

```
count() by _path
```



This tells you: from this PCAP, here are all the Zeek log types and how many entries each one has. So if I see conn: 5000, http: 200, dns: 800 I now know the shape of my traffic before I even start digging.

`

4.2 Zeek Working Like a Log Analyzer

Here's something cool about Zui when you click on a path (like the http path from your results), it automatically groups and correlates those logs for you. Instead of seeing 60 individual HTTP events one by one, it organizes them into a meaningful view just like what Zeek does when you analyze it directly from the command line.

For example: HTTP had 60 log entries. When you open them in Zui, they're organized you can see the connections, see what went where, filter by SSL, filter out specific protocols, and navigate the entire flow of traffic visually.

4.3 Filtering by Protocol

Once you're looking at Zeek logs, you can further filter. For example, if I want to see only SSL traffic:

```
_path = "ssl"
```

Or if I want everything EXCEPT SSL:

```
_path != "ssl"
```

Each filtered view then shows you the UID (unique ID for that session), the full logs, and the connection details source, destination, port, protocol, everything. You get complete visibility.

5. Correlation Connecting the Dots

Here's where Zui becomes truly powerful for an analyst. After you find something suspicious say a Suricata alert you don't stop there. You want to understand the full picture.

Zui's correlation feature lets you pivot from a Suricata alert directly to the related Zeek logs. For example:

`

- You see a Suricata alert about suspicious HTTP activity
- You click on it, and Zui shows you the Related Connections the Zeek conn.log entries for the same traffic flow
- Then you can jump to the http.log to see exactly what URL was requested, what headers were sent
- And if needed, you can go even deeper with Wireshark

This is the workflow: Suricata alerts give you the what. Zeek logs give you the context. Wireshark gives you the deepest detail if you need it.

6. Wireshark Integration When You Need to Go Deeper

There's a button in Zui the little Wireshark icon. When you click it on a specific log or filtered result, it exports those specific packets and opens them directly in Wireshark.

Why is this powerful? Because you're not opening the entire PCAP in Wireshark you're only opening the specific packets you care about. This means:

- Faster Wireshark only loads a small subset of packets
- Focused you go straight to the suspicious traffic
- Detailed you can inspect headers, payloads, flags, everything at the byte level

> **Workflow Summary:** *Brim/Zui → identifies what to investigate → Wireshark → deep packet inspection of only the relevant packets.*

For example: if I filter for SSL logs in Zui and then click the Wireshark button, it exports only the SSL traffic and opens it in Wireshark with the SSL filter already applied. I didn't have to manually filter anything in Wireshark Zui did the work for me.