NETWORK SECURITY LAB PROJECT

# NAME: ADITYA VIKRAM SINGH

# REGISTRATION NUMBER: 22BCE8635

# TOPIC: DNS ANALYSER WITH GEOIP MAPPING

# SUBMITTED TO: MOHINDER SINGH B.

# 

ABSTRACT

DNS (Domain Name System) is a critical component of the internet, translating domain names into IP addresses. However, DNS traffic can be exploited for malicious activities such as DNS tunneling, data ex-filtration, and command-and-control (C2) communications. This project presents a DNS Analyzer with Anomaly Detection and Geo-IP Mapping, designed to process PCAP (Packet Capture) files and identify suspicious patterns in DNS traffic.

The tool leverages Scapy for packet analysis, GeoIP2 for mapping IPs to geographical locations, and Matplotlib & Folium for visualization. Key features include anomaly detection for excessive NXDOMAIN responses, unusual query types, high traffic sources, and long subdomain queries—indicators of potential DNS abuse. Additionally, it inspects TXT records in DNS responses for signs of data ex-filtration. The output includes a detailed textual report summarizing findings and an interactive geographical map highlighting the origin of DNS requests.

This tool aids cyber-security professionals, network administrators, and researchers in analyzing DNS traffic, detecting anomalies, and improving network security.

INTRODUCTION

The DNS Analyzer with Anomaly Detection and Geo-IP Mapping is a cybersecurity tool designed to analyze DNS (Domain Name System) traffic from PCAP (Packet Capture) files. DNS plays a crucial role in internet communication by resolving domain names into IP addresses. However, it is also a common target for cyber threats such as DNS tunneling, cache poisoning, data ex-filtration, and command-and-control (C2) attacks.

This tool provides detailed analysis and anomaly detection in DNS queries and responses, allowing network administrators and security analysts to identify suspicious activities that may indicate cyber threats. Additionally, the tool incorporates Geo-IP mapping, which helps in locating the geographical origin of DNS queries, aiding in further threat assessment.

* **Purpose**

The main objectives of this tool are:

* Detecting Anomalies in DNS Traffic: Identifies unusual DNS patterns, excessive NXDOMAIN responses, long subdomains, and high-frequency queries.
* Monitoring Suspicious DNS Requests: Analyzes TXT records for potential data ex-filtration or unauthorized communication.
* Geo-location of DNS Requests: Maps source IP addresses to their geographical locations using GeoIP2 to provide insights into request origins.
* Providing Comprehensive Reports: Generates text-based reports summarizing detected anomalies and an interactive world map visualization of DNS traffic.
* **Significance**
* Cybersecurity Enhancement: Helps in detecting and mitigating DNS-based cyber attacks.
* Network Traffic Analysis: Provides valuable insights into DNS request patterns for better network monitoring.
* Incident Response: Assists security teams in investigating DNS-related incidents by pinpointing potential attack sources.
* This tool is useful for cybersecurity professionals, network administrators, and researchers to enhance DNS traffic visibility and detect malicious activities effectively.

Drawbacks of The Existing Tools?

Several existing **DNS analysis and anomaly detection tools** are available, but they have certain limitations that our **DNS Analyzer with Anomaly Detection and Geo-IP Mapping** aims to address. Below are some common drawbacks of current solutions:

### ****1. Limited Anomaly Detection Capabilities****

Many tools **only focus on basic DNS logging** and lack advanced anomaly detection for identifying patterns like **excessive NXDOMAIN responses, unusually long subdomains, or high-frequency queries**.

Some solutions do not analyze **TXT records**, which can be used for **data ex-filtration and covert communications**.

### ****2. Lack of Geo location Analysis****

Traditional DNS analyzers **do not provide Geo-IP mapping**, making it difficult to trace the geographical origin of suspicious DNS queries.

Without Geo-IP data, identifying whether requests are coming from **malicious foreign networks or known attack sources** becomes harder.

### ****3. Dependency on Continuous Network Monitoring****

Some existing solutions rely on **real-time packet sniffing**, which requires continuous monitoring and **cannot process historical PCAP files** effectively.

Our tool allows for **offline analysis of PCAP files**, making it more flexible for forensic investigations.

### ****4. High Resource Consumption****

Enterprise-grade solutions like **SIEM (Security Information and Event Management) tools** can perform DNS analysis, but they are often **resource-intensive and expensive**.

Open-source alternatives may not be optimized for **efficient performance**, leading to **high memory and CPU usage** when analyzing large PCAP files.

Proposed tool: DNS Analyzer with Anomaly Detection and GeoIP Mapping

## ****Purpose of the Tool****

The proposed **DNS Analyzer with Anomaly Detection and Geo-IP Mapping** is designed for **analyzing DNS traffic from PCAP files** to detect anomalies and visualize geographical locations of DNS queries. This tool serves as a **cybersecurity forensic analysis utility**, helping security analysts and network administrators to:

1. **Identify suspicious DNS activity** (e.g., malware communication, data exfiltration, DNS tunneling).
2. **Detect anomalies** like excessive NXDOMAIN responses, long subdomains, and high request rates.
3. **Map IPs to real-world locations** using Geo-IP data to trace the origin of DNS requests.
4. **Provide a structured report** summarizing anomalies, statistics, and geographical information.

Core Pseudocode:

1. Load the PCAP file.

2. Extract DNS queries and responses from packets.

3. Initialize counters and data structures for anomaly detection.

4. For each DNS query in the PCAP file:

a. Extract the queried domain, source IP, and response type.

b. Check for anomalies:

- Excessive NXDOMAIN responses.

- Long subdomain names.

- High frequency of queries from a single IP.

- Suspicious TXT records.

c. If an anomaly is detected, log the details.

d. Perform Geo-IP lookup for the source IP.

5. Generate a detailed report:

a. Summary of total queries and anomalies detected.

b. List of flagged anomalies with timestamps and IP addresses.

c. Generate a Geo-IP map highlighting the locations of DNS queries.

6. Save the report and visualization output.

# Explanation of the Algorithm

The algorithm follows these key steps:

### ****1. PCAP File Processing****

The tool **reads and parses DNS packets** from the provided **PCAP file** using Scapy.

Extracts relevant information such as **domain names, response codes, and source IP addresses**.

### ****2. Anomaly Detection Mechanisms****

**Excessive NXDOMAIN responses**: If an IP generates too many failed DNS queries, it may indicate **reconnaissance or DGA (Domain Generation Algorithm) activity**.

**Long subdomains**: Domains with excessively long subdomains could be an indicator of **DNS tunneling or malware communication**.

**High query frequency from a single IP**: Identifies potential **botnet activity or DDoS attacks**.

**Suspicious TXT records**: Checks for DNS TXT records that might be used for **data ex-filtration or command & control communication**.

### ****3. Geo-IP Mapping****

Uses **MaxMind’s GeoLite2 database** to **resolve IP addresses to their geographical locations**.

Stores **latitude, longitude, and country information** for visualization.

### ****4. Report Generation****

**Text Report**: Summarizes detected anomalies, statistics, and flagged DNS queries.

**Geo-IP Map**: Generates an interactive map (using Folium) showing the **geographical origin of DNS queries**.

System Requirement Specification

## ****1. Hardware Requirements****

* **Processor**: Intel Core i3 (or equivalent) with at least **2.0 GHz**
* **RAM**: Minimum **4 GB** (8 GB recommended for large PCAP files)
* **Storage**: At least **500 MB free space** (for PCAP storage, reports, and Geo-IP database)
* **Display**: Standard **HD display (1366x768)** or higher
* **Network**: Internet connection required for downloading GeoIP database (optional)

## ****2. Software Requirements****

* + **Operating System**:

Windows 10 / 11

Ubuntu 18.04+ / Debian-based Linux

macOS 10.15+

* + **Programming Environment**:

**Python 3.7+** (Ensure it's installed and configured)

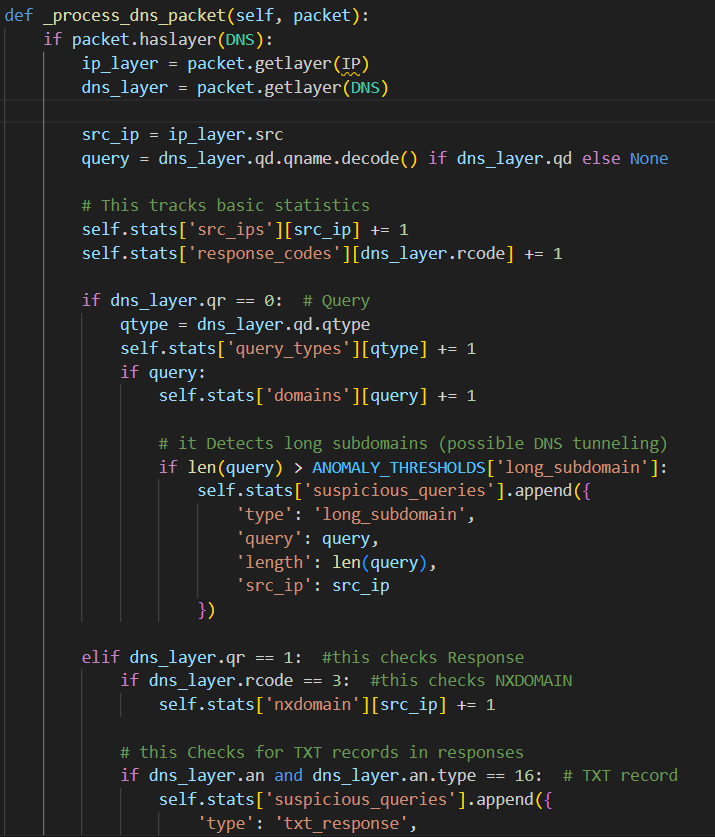
## ****Software Requirements****

**Wireshark** - optional, for PCAP capture and visualization)

**GeoLite2-City.mmdb** - For Geo-IP lookup

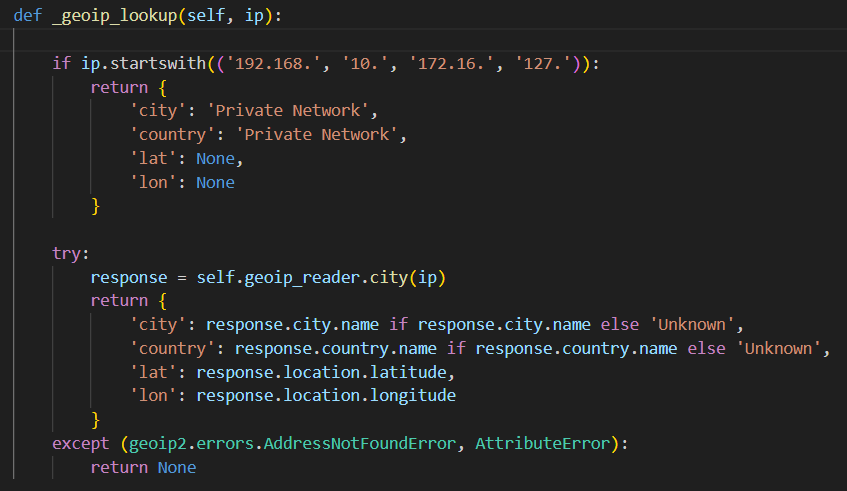
Result And Discussion

The DNS Analyser tool is implemented in Python and consists of several key components. The first is packet parsing, which involves reading .pcapng files and extracting information such as source IP addresses, query types, and domain names. This is done using the scapy library, which provides powerful tools for network packet analysis. The tool skips non-IP packets to ensure accurate analysis.

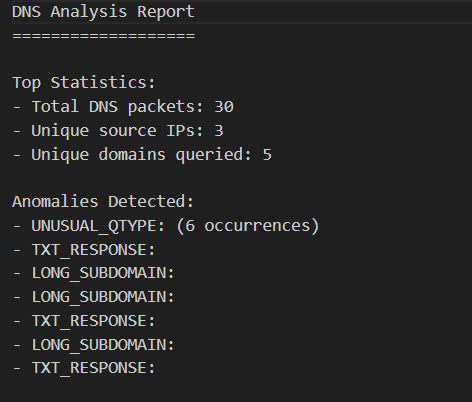


Anomaly detection is another critical component of the tool. It flags excessive NXDOMAIN responses, unusual query types, long subdomains, and high traffic from single sources. These anomalies are often indicators of malicious activity, and the tool tracks them using dictionaries and counters. For example, the tool increments a counter for each NXDOMAIN response from a specific IP address and flags the IP if the count exceeds a predefined threshold.

The Geo-IP lookup feature uses the MaxMind Geo-IP database to map source IPs to geographic locations. This is done using the geoip2 library, which provides an interface to the Geo-IP database. The tool handles private IPs by assigning them dummy locations, ensuring that all IPs are included in the analysis. The interactive map is generated using the folium library, which provides tools for creating interactive maps in Python. The tool adds markers for each Geo-IP entry, displaying the IP address, city, and country in a popup.



Finally, the tool generates a detailed text report summarizing the analysis results. The report includes statistics such as the total number of DNS packets, unique source IPs, and unique domains queried. It also lists any anomalies detected, such as excessive NXDOMAIN responses or unusual query types. This report provides a comprehensive overview of the DNS traffic and helps administrators identify potential threats.

Conclusion

The DNS Analyzer tool is a powerful solution for analyzing DNS traffic, detecting anomalies, and visualizing the geographic origin of DNS queries. It automates the process of DNS traffic analysis, saving time and reducing the risk of human error. By detecting anomalies such as excessive NXDOMAIN responses and unusual query types, the tool helps identify potential threats, such as DNS tunneling, phishing, and malware communication. The Geo-IP mapping feature provides insights into the geographic origin of DNS queries, which is useful for identifying the source of attacks and ensuring compliance with data protection regulations. Overall, the DNS Analyzer tool is an essential tool for network security, troubleshooting, and compliance.

References

**Scapy Documentation** – Used for DNS packet parsing and analysis.

[https://scapy.readthedocs.io/en/latest/](https://scapy.readthedocs.io/en/latest/" \t "_new)

**MaxMind GeoIP2 Database** – Used for mapping IP addresses to geographical locations.

https://dev.maxmind.com/geoip/geoip2/geolite2/

**Wireshark and PCAP File Analysis** – Understanding PCAP file structures and DNS traffic patterns.

[https://www.wireshark.org/](https://www.wireshark.org/" \t "_new)

**Matplotlib & Folium Documentation** – Used for data visualization and geographical mapping.

https://matplotlib.org/stable/contents.html

https://python-visualization.github.io/folium/

**RFC 1035 - Domain Names: Implementation and Specification** – Understanding DNS query and response structures.

https://datatracker.ietf.org/doc/html/rfc1035

**Network Security Textbooks & Research Papers** – Used for anomaly detection techniques and DNS-based attacks.

"DNS Security: Defening the Domain Name System" by Allan Liska

Various cybersecurity whitepapers on DNS-based attacks and anomaly detection.

**Python Official Documentation** – For handling networking, file operations, and threading.

[https://docs.python.org/3/](https://docs.python.org/3/" \t "_new)