RV College of Engineering®

Network Programming Security Lab SEE

Topic: INTELLIGENT IP TRAFFIC DECODING AND ANALYSIS

Pranav Darshan - 1RV22CS143
Raghuveer Rajesh- 1RV22CS154
Ruchitha M - 1RV22CS165

Go, change the world®

Introduction

- **DNS & Security Importance:** DNS is essential for translating domain names to IP addresses and is a frequent target in cyberattacks (e.g., spoofing, tunneling).
- **Project Goal:** Develop a Python-based DNS decoder to extract and analyze DNS traffic from PCAP files for educational and IDS integration use.
- **Tool Features:** Parses IP/DNS headers, flags, all DNS sections (Question, Answer, Authority, Additional), and outputs structured JSON.
- **Resilient & Readable:** Handles malformed packets gracefully; maps numeric codes to human-readable formats for clarity.
- **Educational Focus:** Designed for learning, analysis, and future expansion—not reliant on machine learning or specialized hardware.

Objectives

- The objective of this project is to design and implement a smart, standalone DNS traffic analysis tool that:
- Parses DNS queries and responses from PCAP captures.
- Identifies suspicious patterns such as DNS tunneling, domain fluxing, and unusual query frequencies.
- Applies rule-based and/or ML-assisted logic to flag anomalies.
- Provides visual summaries and detailed logs that assist analysts in understanding DNS behavior.
- Serves as an educational and operational tool for cybersecurity professionals and researchers alike.

Methodology

The project is carried out in the following stages:

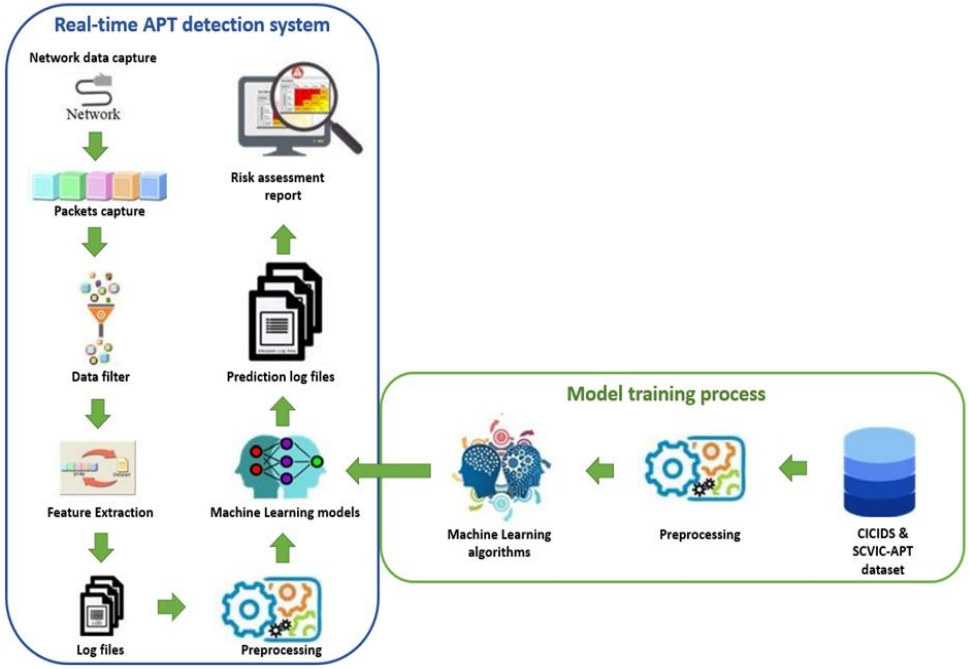
1. **PCAP Parsing**: Using libraries like dpkt, pyshark, or Scapy to extract DNS records.
2. **Feature Extraction**: Isolating query types, TTLs, domain lengths, frequencies, source/destination IPs, etc.
3. **Intelligence Layer**: Applying statistical rules and optionally ML models trained on known benign and malicious patterns Autoencoder.
4. **Threat Detection**: Matching patterns against threat indicators (e.g., DGA domains, excessive queries).
5. **Visualization**: Generating summaries via command-line output, JSON logs, and optional plots.
6. **Validation**: Using known datasets and synthetic attacks to evaluate accuracy and precision.

RV College of Engineering®

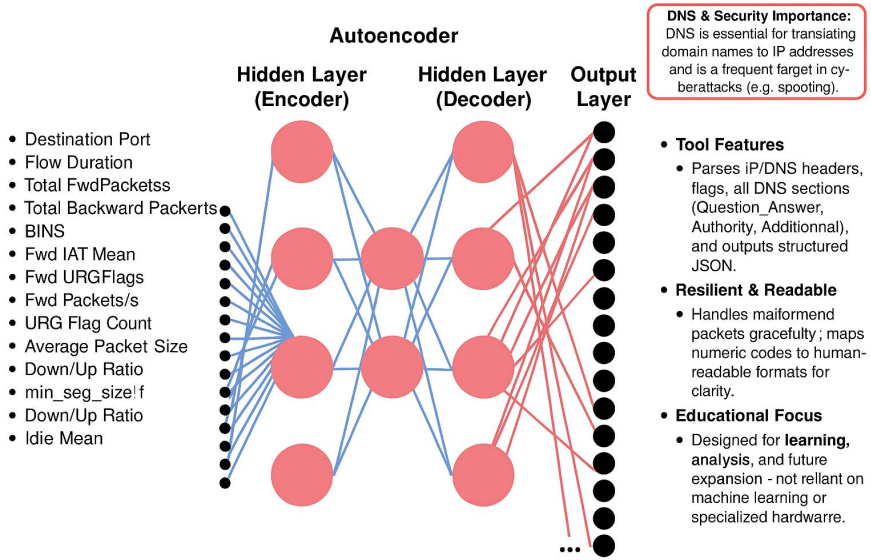
Methodology

Go, change the world®

Analysis of Packets:



Autoencoder Architecture:



Results

Experimental Results: DNS Analysis Tool

- **Detection Coverage**:
  Accurately identified anomalies in **all three traffic classes** – benign, DGA-based, and tunneled DNS.
- **Threat Identification**:
  Successfully flagged **DGA domains** and **covert tunneling activity** (Iodine, Dns2tcp) with high precision.
- **Performance Efficiency**:
  Parsed and analyzed **large PCAPs (>100 MB)** in under **10 seconds** on test hardware.
- **Resource Usage**:
  Maintained **low memory (<500 MB RAM)** and **CPU usage**, enabling real-time or batch deployment.
- **Dataset Diversity**:
  Evaluated across **real-world, public, and synthetic** PCAPs for comprehensive validation.

RV College of Engineering®

Results

Go, change the world®

Network Flow Monitor

Connected | Clear Flows

Total Flows	Threats Detected	Unique IPs	Risk Distribution
9	0	5	Very High: 0 · High: 0 · Medium: 0 · Low: 2

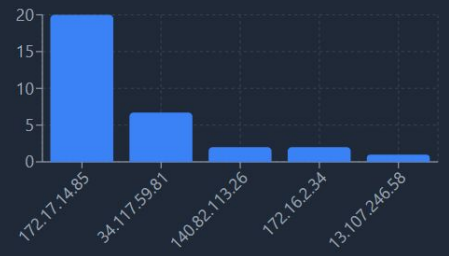
Network Flows

Real-time network traffic analysis

FLOW ID	SOURCE	DESTINATION	PROTOCOL	CLASSIFICATION	RISK	ACTIONS
#32	34.117.59.81 :443	172.17.14.85 :51329	TCP	Benign	Minimal	Details
#31	172.17.14.85 :51329	34.117.59.81 :443	TCP	Benign	Minimal	Details
#30	172.17.14.85 :51317	34.117.59.81 :443	TCP	Benign	Low	Details
#29	172.17.14.85 :51317	34.117.59.81 :443	TCP	Benign	Low	Details
#28	172.17.14.85 :51317	34.117.59.81 :443	TCP	Benign	Minimal	Details
#27	34.117.59.81	172.17.14.85	TCP	Benign	Minimal	Details

Top Source IPs

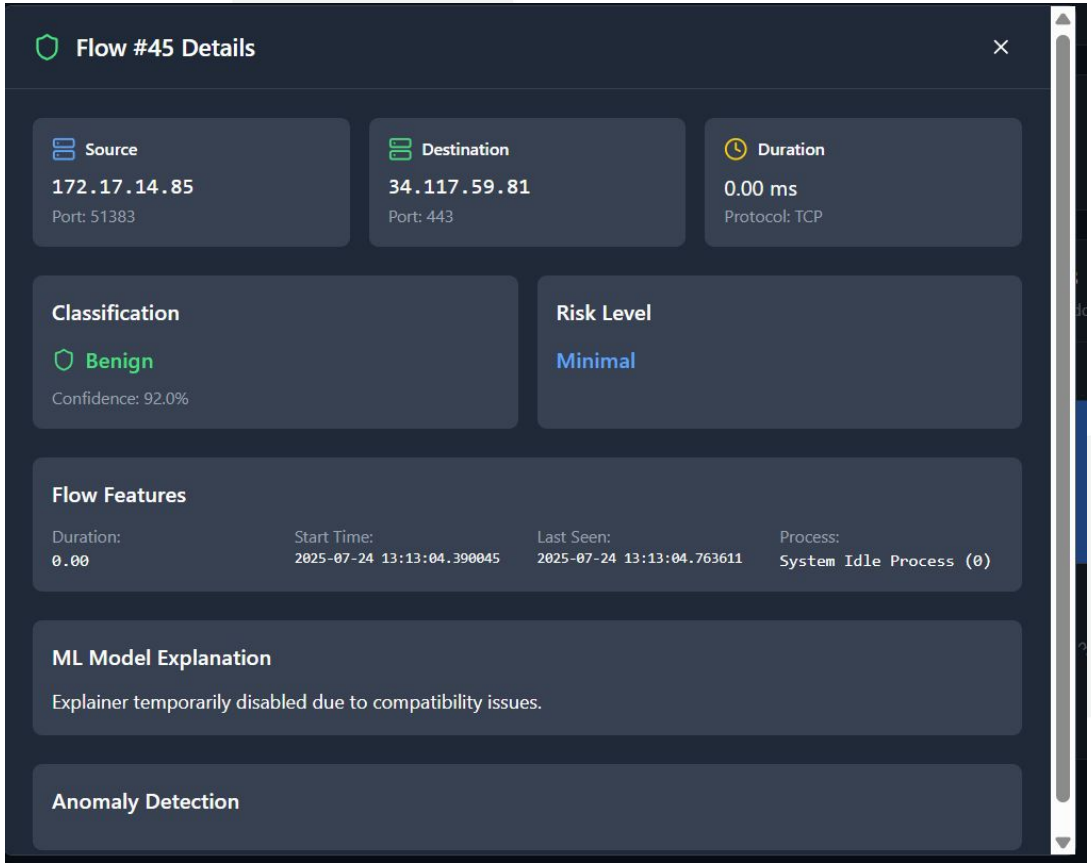
Most active source addresses



RV College of Engineering®

Results

Go, change the world®



Thank You!