PCAP Analyzer for Threat Hunting

FYP ID
2422

Supervisor:
Mr. Khwaja Mansoor

Industrial Supervisor:
Wing Commander Salman Ahmed (PAF)

Batch
Fall-2021

OUR TEAM

Hamza Haroon
211064

Noman Masood Khan
211042

Mazhar ul Hassan
211961

Table of Contents

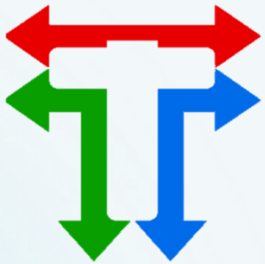
Problem Statement

Growing Need for Forensic Analysis

Specific Tools for Specific Tasks

Maintaining Malicious Database

Existing Software



Our Solution

One word..... **Swiss Army Knife!**

Project Overview

Goal

Platform & Interface

Malicious Traffic Discovery

Visualize Network Traffic

Objectives

Analyze

Develop capabilities to parse and analyze PCAP files, focusing on stream data.

Detect

Implement algorithms to identify and flag malicious domains, IPs, and files in network traffic.

Build

Develop an interactive map displaying network topology and node communications.

Extract

Develop tools to detect and extract all files (including malicious files) transferred over the network.

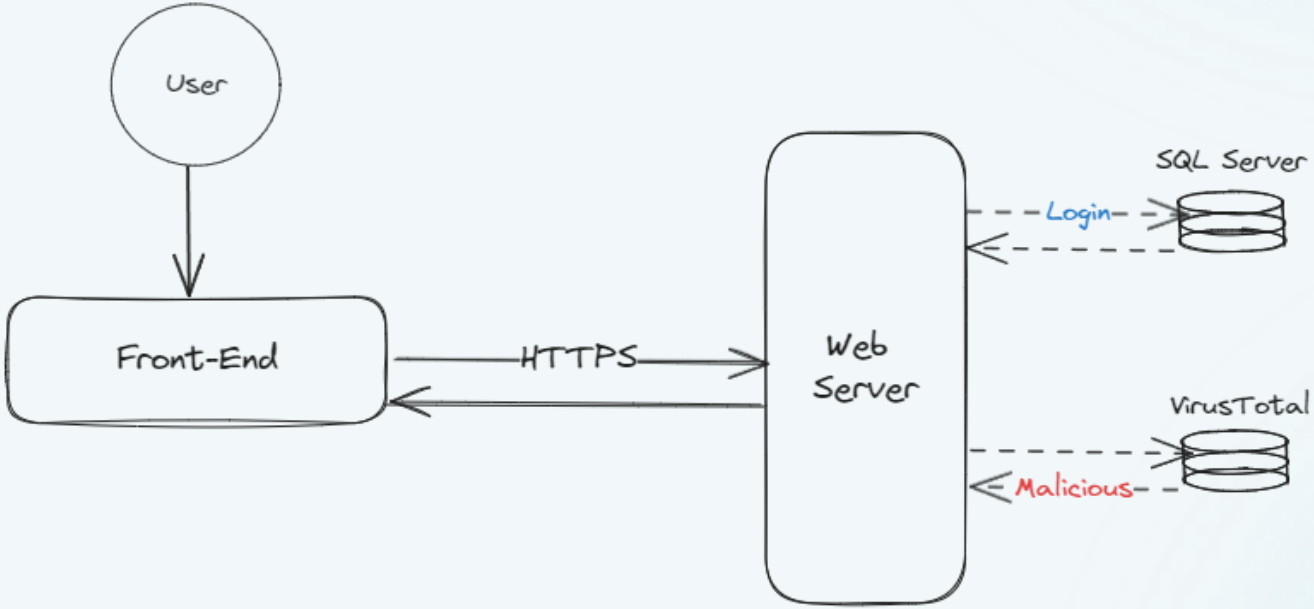
DFIR

Enhance network forensics capabilities to enable detailed analysis and reconstruction of network events for investigative purposes.

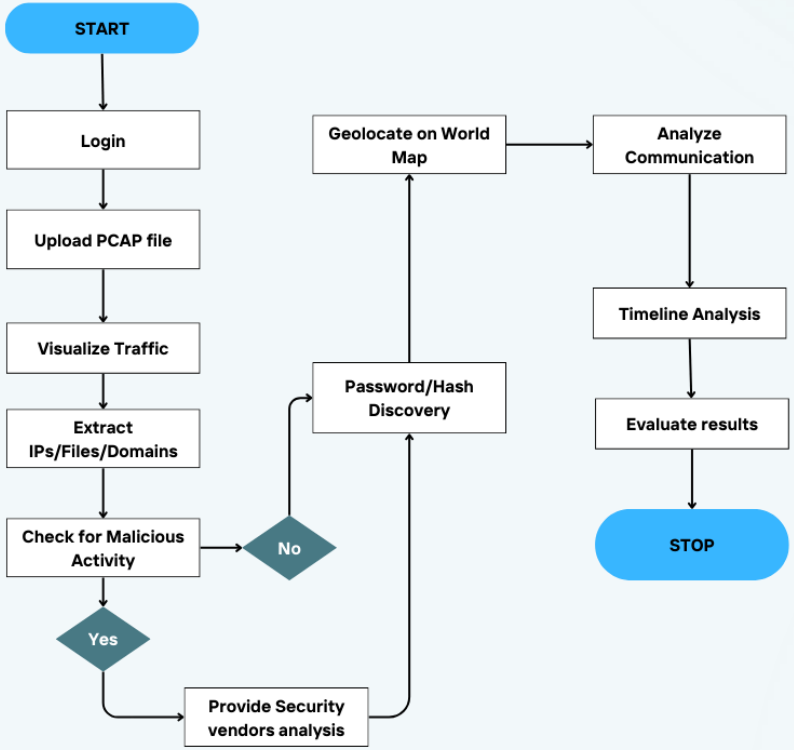
Gap Analysis

Features/Tools	Wireshark	PacketTotal	APackets	Nethor	Arkime	CAPAnalysis	HawkEye
Deep Packet Analysis	✓	✓	✓	✓	✓	✓	✓
SSL/HTTPS Inspection	✓	✓	✓	✓	✓	✓	✓
Network Traffic Viewing	✓	✓	✓	✓	✓	✓	✓
Automated File Extraction	✓	✓	✓		✓		✓
Geolocate IPs			✓	✓		✓	✓
Network Visualization		✓	✓	✓	✓	✓	✓
User Friendly Interface	✓	✓	✓	✓	✓	✓	✓
Automated Malicious Traffic		✓					✓
Automated Attack Detection		✓					✓
Uploads remain Private	✓			✓	✓		✓
Free	✓	✓	✓	✓	✓	✓	✓

Application Architecture



High Level System Component



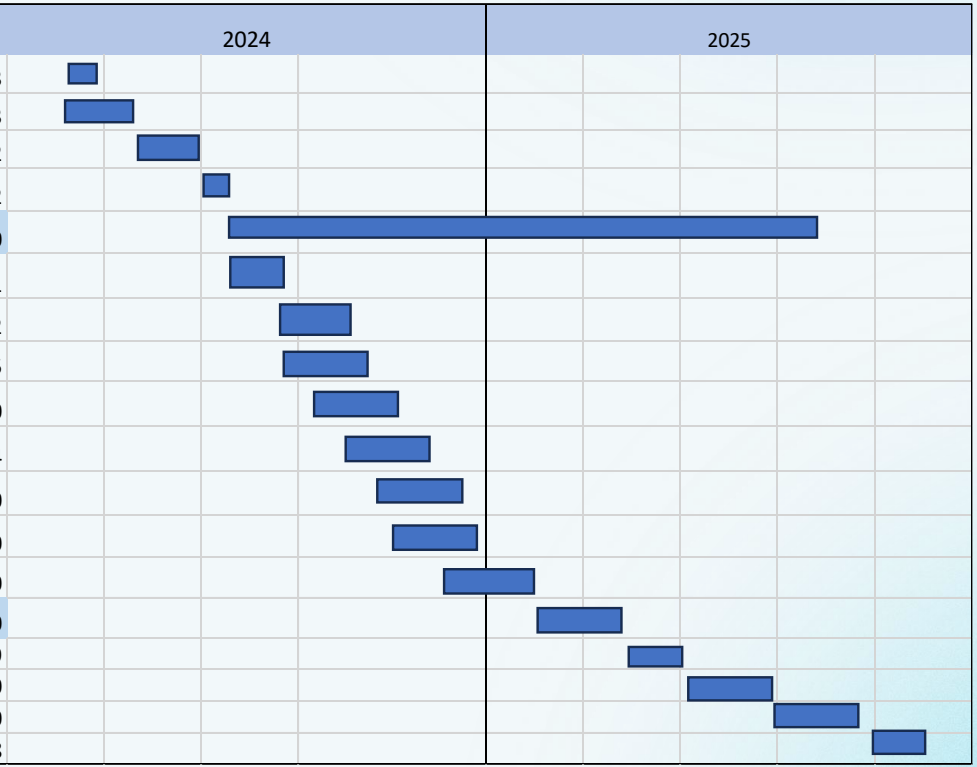
Tools and Technologies

Front-End Development

Back-End Technologies

Timeline

Task Name	Start date	End Date	Duration
Project Selection	15-Mar	18-Mar	3
Research	18-Mar	20-Apr	33
FYP-I Proposal Writing	11-Apr	23-Apr	12
FYP-I Defence	23-Apr	25-Apr	2
Backend Development	01-May	06-Jun-25	300
Deep Packet Analysis	01-May-24	30-May-24	31
SSL/HTTPS Inspection	01-Jun	30-Jun-24	42
Automated Files Extraction	01-Jul-24	30-Jul-24	25
Geolocate IPs	01-Aug-24	30-Aug-24	20
Automated Attack Detection	01-Sep-24	30-Sep-24	14
WIFI Handshake Analysis	01-Oct-24	30-Oct-24	30
Automated Malicious Traffic Detection	01-Nov-24	30-Nov-24	30
Database Intergration	01-Dec-24	30-Dec-24	30
Front-end Development	01-Jan-25	30-Jan-25	30
FYP-II Defence	02-Feb	21-Feb-25	19
FYP III	01-Mar-25	30-Mar-25	30
Testing and Improvements	01-Apr-25	01-Jun-25	30
FYP-III Defence	01-May-25	08-May-25	8



Thank You

Any Questions