Arsalan Favakeh

12/2/2024

Prof. Omprakash Gnawali

Project Documentation: NetAnalyzer Suite

Project Overview

The NetAnalyzer Suite is a Python-based tool designed for network traffic monitoring and analysis. It supports processing `.har` and `.pcap` files to extract detailed network metrics and enables real-time traffic monitoring using PyShark. The suite also provides interactive visualizations to present traffic data insights in an intuitive manner.

This tool is aimed at assisting users in understanding and analyzing network performance, including download rates, protocol distributions, and IP mappings, with applications in both academic and practical network studies.

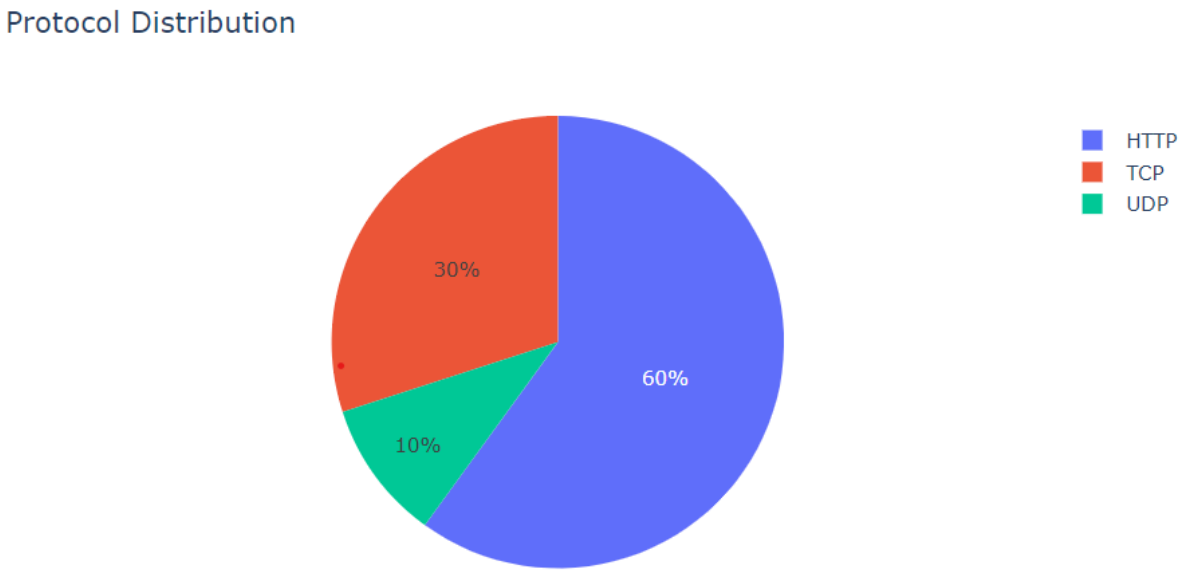
Key Features

1. **HAR File Processing**:
    - Computes total download size, average request latency, and resource type distributions from `.har` files.
2. **PCAP File Processing**:
    - Extracts total packet length, packet counts, time interval, download data rate, protocol distribution, and IP mappings from `.pcap` files.
3. **Real-Time Traffic Monitoring**:
    - Captures live network traffic on a selected interface, displaying source/destination IPs, protocols, and packet details.
4. **Visualization Dashboard**:
    - Provides interactive visualizations such as pie charts and time-series graphs for metrics derived from `.har` and `.pcap` files.

Results Achieved

1. **HAR File Processing**:
    - **Input**: `favakeh_2071132.har`
    - **Output**:
        - Total Size: `5,293,371 bytes`
        - Average Latency: `608.78 ms`
        - Resource Types Breakdown: Detailed breakdown of resource types such as `text/html` (full breakdown available in code results).
2. **PCAP File Processing**:
    - **Input**: `favakeh_2071132.pcap`
    - **Output**:
        - Total Packet Length: `9,743,976 bytes`
        - Total Packets: `18,591`
        - Time Interval: `1238.07 seconds`
        - Download Data Rate: `0.00787 Mbps`
        - Protocol Count:
            - `TCP: 12,946`
            - `UDP: 5,505`
            - `UNKNOWN: 140`
        - IP Mappings: Extensive mapping of source-to-destination IPs, demonstrating network communication patterns.
3. **Real-Time Monitoring**:
    - **Error Handling**: Resolved missing interface error by identifying correct interface names (e.g., `Wi-Fi`, `Ethernet`, etc.).
    - **Functionality**: Captured live traffic with accurate packet details, including IPs and protocols.
4. **Visualization Dashboard**:
    - Successfully ran the dashboard at `http://127.0.0.1:8050/`.
    - Visualized metrics with interactive pie charts, bar graphs, and time-series plots.

NetAnalyzer Dashboard



Challenges Encountered

1. **Real-Time Monitoring**:
   - Initial error with interface selection (`eth0` not available on Windows). Resolved by listing available interfaces and selecting the appropriate one (`Wi-Fi`).
2. **Data Consistency**:
   - Validated results against manual calculations using tools like Wireshark and HAR Viewer to ensure accuracy.

Packaging

- **Included Files**:

1. `HAR_Processor.py`: Script for `.har` file processing.
2. `PCAP_Processor.py`: Script for `.pcap` file processing.
3. `RealTimeMonitor.py`: Script for real-time traffic monitoring.
4. `VisualizationDashboard.py`: Script for launching the interactive visualization dashboard.
5. `favakeh_2071132.har`: Example `.har` file used for analysis.
6. `favakeh_2071132.pcap`: Example `.pcap` file used for analysis.
7. `env.txt`: List of dependencies required to run the project.

How to Use

1. **Install Dependencies**:
   - Run: `pip install -r env.txt`
2. **Run Scripts**:
   - **HAR Processing**: `python HAR_Processor.py favakeh_2071132.har`
   - **PCAP Processing**: `python PCAP_Processor.py favakeh_2071132.pcap`
   - **Real-Time Monitoring**: `python RealTimeMonitor.py` (select an available interface).
   - **Visualization Dashboard**: `python VisualizationDashboard.py` (open `http://127.0.0.1:8050` in a browser).
3. **Analyze Results**:
   - Review console outputs and interactive visualizations for insights.

Conclusion

The **NetAnalyzer Suite** successfully achieves its objectives, providing a powerful set of tools for network traffic analysis and visualization. By processing `.har` and `.pcap` files and enabling real-time traffic monitoring, the suite delivers comprehensive insights into network behavior, making it a valuable resource for both academic and professional use cases.