**Project Overview Anvar Suleyman, Ridvan Suleymanov**

**Title:** Network Traffic Analysis Tool

**Description:**  
This Python project aims to examine PCAP files for network traffic data. It offers insights into network communications by extracting packet information, finding frequent communication pairings, seeing possible security risks like port monitoring and suspicious activities, and visualizing different aspects of the network traffic.

**Key Features:** Reads PCAP files to capture packet data. Analyzes packet data to determine top talkers/listeners, protocol usage, and packet size distribution. Identifies possible security risks like port scanning and unusually high traffic volumes coming from certain IP addresses. Provides data visualization to make it easier to understand network activities.

**Input:**

* + **PCAP File:** A file that contains packet capture data. This file is passed as a command-line argument.

**Output:**

* + **Console Logs:** Informative logs about the process and results.
  + **Data Visualizations:** Graphs displaying protocol distribution, packet size distribution, top talkers and listeners, and traffic flow rate.
  + **Data Export:** Optionally, filtered data can be exported to CSV or Excel format based on user input.

**How to Run the Code**

* + “Python 3.x” needs to be installed.
  + Install required packages: **scapy**, **pandas**, **matplotlib**, **tqdm**.
  + Line of bash to be put in terminal: pip install scapy pandas matplotlib tqdm

**Run the Script:**

* + Navigate to the directory containing the script.
  + Execute the script with the PCAP file path as the first argument and optionally, the port scan threshold as the second argument.
  + Line of bash: python network\_traffic\_analysis.py path\_to\_pcap\_file.pcap 100

**Follow the outputs given:**

* + Enter an IP address to filter the data (optional).
  + Enter a protocol to filter the data (optional) further.
  + Choose whether to export the filtered data and in which format.

**Example Execution**

* + python network\_traffic\_analysis.py /path/to/network\_data.pcap
  + This command starts the analysis process, logs the steps being performed, displays plots directly, and asks for user input to refine data handling and export.