**TCP Session Analyzer with State Tracking**

**Project Overview**

This project is a Python-based analyzer for parsing and interpreting TCP sessions from a .pcapng file using the pyshark library. It focuses on:

* Identifying unique TCP sessions based on IP and port pairs
* Tracking packet count and TCP flag values per session
* Translating flags into meaningful TCP states (e.g., SYN, ACK, FIN)

This tool is helpful for understanding how TCP sessions are established and terminated, as well as detecting anomalies such as resets or incomplete handshakes.

**Features**

* 🔍 Extracts all TCP sessions from a .pcapng capture file
* 📑 Displays packet counts and TCP flag values for each direction
* 🧠 Maps TCP flags to readable states (e.g., SYN, FIN, RST)
* ✅ Confirms handshake or detects abnormal session terminations

**How It Works**

1. **Input File**: tcp\_session\_capture.pcapng
2. **Library Used**: pyshark (wrapper around tshark)
3. **Steps**:
   * Load the capture using pyshark.FileCapture
   * Group packets by (source IP, source port, destination IP, destination port)
   * For each group, collect:
     + Total packet count
     + TCP flags
     + Interpreted states
   * Print session summary with source-destination pair, packet count, flags, and states

**Example Output**

**TCP Packets filtered in Wireshark**

**A screenshot of a computer

AI-generated content may be incorrect.**

**The Output Captured**

**A computer screen shot of a black screen

AI-generated content may be incorrect.**

**Requirements**

* Python 3.7+
* Wireshark/tshark (required by pyshark)
* pyshark: Install using pip install pyshark

**Usage**

1. Place your .pcapng file (e.g., tcp\_session\_capture.pcapng) in the working directory.
2. Update the script path if your file has a different name.
3. Run the script:

python tcp\_session\_analyzer.py