Network Analyzer Tool - User Manual

Overview

The **Network Analyzer** is a Python application that reads network log files (tcpdump format), automatically extracts statistics (top source/destination IPs, TCP flags, errors), detects security anomalies, and exports the results as interactive Excel spreadsheets or Markdown reports.

System Requirements

- **Python 3.7+**
- **Operating System**: Windows, macOS, or Linux
- **Required Python Libraries**:
  - `tkinter` (usually included with Python)
  - `matplotlib` (optional, for graphs)
  - `openpyxl` (for Excel export)

Installation

Step 1: Install Python

Download from python.org and ensure "Add Python to PATH" is checked during installation.

Step 2: Install Dependencies

Open a terminal/command prompt and run:
pip install matplotlib openpyxl

Step 3: Run the Application

Navigate to the script folder and run:
python Analyseur_réseau.py

A window titled "🛡️ SAE 1.05 - Analyseur Réseau avec Graphiques" should open.

Using the Program

Step-by-Step Guide

1. Select a File

- Click the "📂 **Sélectionner un fichier**" (Select File) button
- Choose a network log file with one of these formats:
    - `.txt` (text files)
    - `.log` (log files)
    - `.csv` (CSV files)
    - `.dump` (tcpdump dumps)

2. View Analysis Results

Once a file is selected, the application automatically:

- **Parses** the log file line-by-line
- **Extracts** source IPs, destination IPs, TCP flags, and errors
- **Detects** security alerts (DOS, SYN floods, unbalanced traffic)
- **Displays** results in the main window with:
    - **Text summary**: Statistics and top IPs
    - **Graphs** (if matplotlib is installed):
        - Pie chart of top 5 source IPs
        - Pie chart of top 5 destination IPs
        - Bar chart of TCP flags
        - Pie chart of error types

3. Export Results

Option A: Export to Excel

1. Click "📊 **Export Excel (avec graphiques)**" (Export Excel with graphs)
2. Choose a save location and filename
3. The generated `.xlsx` file contains:
    - **Summary sheet**: Key metrics (file name, analysis date, line count, IP counts, error count)
    - **Sources sheet**: Top 10 source IPs with pie chart
    - **Destinations sheet**: Top 10 destination IPs with pie chart
    - **Flags TCP sheet**: TCP flag distribution with bar chart
    - **Error Types sheet** (if errors detected): Error breakdown with pie chart
    - **Error Details sheet**: Line-by-line error listings

- **Alerts sheet** (if alerts detected): Security anomalies detected

Option B: Export to Markdown

1. Click "📝 **Export Markdown**" (Export Markdown)
2. Choose a save location and filename
3. The generated `.md` file contains:
   - Analysis date and source file name
   - Global statistics
   - Top 10 source IPs with percentages
   - Top 10 destination IPs with percentages
   - Security alerts (if any)

Understanding the Analysis

What the Program Extracts

Source & Destination IPs

The tool identifies IP addresses using the `>` symbol in log lines:

- **Source**: IP address before `>`
- **Destination**: IP address after `>`

Example: `192.168.1.10 > 10.0.0.5` means traffic from 192.168.1.10 to 10.0.0.5

TCP Flags

TCP flags indicate connection state and intent:

- **[S]** = SYN (connection initiation)
- **[S.]** = SYN-ACK (server acknowledgment)
- **[.]** = ACK (acknowledgment)
- **[F]** = FIN (connection close)
- **[R]** = RST (connection reset)
- **[P.]** = PSH-ACK (data push with acknowledgment)

Error Detection

The tool searches for error keywords:

- ERROR, ERR, Exception, CRITICAL, FATAL, failed, failure, denied
- Each error is logged with line number, type, and message excerpt

Security Alerts

The program automatically generates warnings based on:

- **DOS Alert**: 🔴 More than 50 connections to a single destination IP
- **SYN Flood Alert**: 🟠 More than 50 SYN packets ([S] flags) detected
- **Traffic Imbalance Alert**: 🟡 An IP sends significantly more data than receives (ratio > 5:1)
- **Error Alert**: ❌ Total error count summary

Excel Export Details

Sheet Structure

Sheet Name	Content	Visualization
Summary	Global metrics: file name, date, line count, distinct IPs	-
Sources	Top 10 source IPs with packet count and percentage	Pie chart (top 5)
Destinations	Top 10 destination IPs with connection count and percentage	Pie chart (top 5)
Flags TCP	All TCP flags with occurrence count and percentage	Horizontal bar chart
Error Types	(If errors exist) Error classification with count	Pie chart
Error Details	(If errors exist) Line-by-line error information: line number, type, message	-
Alerts	(If alerts exist) Security alerts with descriptions	-

Customizing the Excel File

After export, you can:

- Modify colors and fonts in Excel
- Adjust chart sizes and positions
- Add filters and sorting
- Insert additional analysis columns

Markdown Export Details

The markdown file includes:

- **Header**: Analysis metadata (date, source file)
- **Statistics Section**: Line count, distinct IP counts, error counts
- **Top 10 Sources Table**: Ranked list with packet counts and percentages
- **Top 10 Destinations Table**: Ranked list with connection counts and percentages
- **Alerts Section** (if applicable): Security anomalies flagged

Technical Details

File Processing

- **Encoding**: UTF-8 with error tolerance (invalid characters ignored)
- **Line Filtering**: Skips empty lines and lines starting with `0x`
- **Parsing Strategy**: Word-by-word tokenization using whitespace delimiter

Statistics Calculation

- **Source/Destination Counting**: Counter objects for O(1) lookup
- **Percentage Calculation**: `(count / total) × 100`
- **Top N Extraction**: `Counter.most_common(n)` for efficiency

Alert Thresholds

- DOS detection: > 50 connections to single destination
- SYN flood: > 50 total SYN packets
- Imbalance ratio: > 5:1 (sent to received)

Version Information

- **Program Name**: SAE 1.05 - Analyseur Réseau avec Graphiques
- **Language**: Python 3.7+
- **GUI Framework**: Tkinter
- **Visualization**: Matplotlib
- **Export Formats**: Excel (XLSX), Markdown (MD)
- **Last Updated**: January 2026

Document Version: 1.0
Language: English
Date: January 13, 2026

This manual provides complete guidance for analyzing network logs and generating professional reports using the Network Analyzer tool.