# Cyber Forensics Triage Tool - Documentation

## Project Overview

The Cyber Forensics Triage Tool is a software application designed to assist forensic investigators in scanning directories for file metadata, detecting potentially sensitive content, analyzing network logs, and generating both PDF and visual reports. The tool has a GUI that simplifies directory selection, displays file information, and allows for report generation.

Key Features:

1. Directory scanning and metadata acquisition.
2. File hashing for integrity checks.
3. Image content detection.
4. Network log analysis for suspicious IPs.
5. PDF report generation.
6. Visualization of file types.

## Requirements

Functional Requirements:

- Directory Analysis: Allow users to select a directory for analysis and display each file's metadata.
- Hash Calculation: Generate SHA-256 hashes for file integrity verification.
- Content Detection: Identify potentially sensitive images (e.g., JPG, PNG).
- Network Log Analysis: Detect suspicious IP addresses in log files.
- PDF Report Generation: Generate a PDF report with collected metadata and analysis results.

- Visual Report Generation: Generate a pie chart to visualize file types within the directory.

Non-Functional Requirements:

- Usability: Provide a user-friendly GUI with clear prompts, buttons, and feedback messages.

- Performance: Efficiently handle directories with a large number of files without crashing.

- Reliability: Ensure accurate hashing and error handling for file access issues.

- Scalability: Allow analysis of large directory structures without performance degradation.

- Security: Log all actions for auditing purposes and ensure data handling complies with legal standards.

## Software Design

Architecture:

The application follows a Modular Architecture with the following layers:

1. GUI Layer: Implements the interface with the user using Tkinter.

2. Processing Layer: Handles file analysis, hashing, and report generation.

3. Data Management Layer: Manages logging and maintains a report list.

Component Design:

GUI Layer (ForensicToolGUI Class): Manages user interaction.

Processing Layer (ForensicTool Class): Manages data acquisition, content analysis, and report generation.

Utility Functions: General-purpose functions for hashing and logging.

## Implementation

Development Tools:

- Programming Language: Python

- Libraries: os, hashlib, logging, PIL, matplotlib, reportlab

Code Structure:

Classes: ForensicTool and ForensicToolGUI for analysis logic and GUI, respectively.

Utility Functions: General-purpose functions for hashing and logging.

Main Execution Block: Initializes the GUI and starts the main event loop.

Error Handling:

File access errors are caught and logged. If hashing or image processing fails, the process logs the error and moves to the next file.

## Testing

Unit Testing:

- Hash Calculation: Verify correct SHA-256 values.

- Metadata Extraction: Test retrieval of file metadata.

- Content Detection: Confirm that image files are correctly flagged as sensitive.

Integration Testing:

- File Analysis Workflow: Validate the complete process from data acquisition to report generation.

User Interface Testing:

Verify GUI responsiveness, particularly file list loading and report generation buttons.

Test interactions with file dialogs and error handling for invalid inputs.

Performance Testing:

Test the application with large directories (1000+ files) to ensure stable performance.

## Maintenance

Logging and Monitoring:

Logs are maintained in forensic_tool_log.log. Review logs periodically to identify frequent issues or improvements.

Future Enhancements:

- Multi-threading: Speed up processing for large directories.

- Additional Analysis Features: Such as metadata comparison or duplicate file detection.

Bug Tracking and Updates:

- Use a version control system (e.g., Git) for tracking changes.

- Document updates and bug fixes in a changelog.

## Legal Disclaimer

This tool is for legal, ethical use only. Unauthorized access to files or systems without permission is illegal and may lead to legal consequences. Users should ensure compliance with all applicable laws and regulations.