# ProtectWare Documentation

## Overview

ProtectWare is a Windows desktop application designed to detect and log malware threats in files and folders. It offers a graphical user interface built with C++ and Windows APIs with a Python-based malware detection backend, and provides efficient protection for Windows systems.

## Key Features

1. User-Friendly GUI:

- A Windows desktop application with an interface for selecting files and folders.  
- Options to scan individual files or entire directories.  
- Real-time display of scan results.

2. Malware Detection:

- Employs a Python script that integrates with a machine learning model to predict the likelihood of malware in files.  
- Detailed logging for each scan operation.

3. Comprehensive Logging:

- Logs scan activities and results to a file for later review by system administrators.

## Technical Stack

- Programming Languages:  
 - C++ for GUI and application logic.  
 - Python for backend malware detection.

- Libraries and Tools:  
 - C++: Windows API for GUI development.  
 - Python: pefile, joblib, logging, and other standard libraries.  
 - Visual Studio: Development environment for compiling the C++ application.

- Machine Learning:  
 - A pre-trained machine learning model predicts whether files are malicious.  
 - Features extracted from PE and OLE file headers and sections.

## System Architecture

1. Frontend (C++):

- Built using the Windows API to create a desktop application with buttons, dialogs, and file/folder selection options.  
- Communicates with the backend Python script by invoking it via command-line execution.

2. Backend (Python):

- Processes files or directories using the pefile library to extract features such as entropy and section sizes.  
- Runs a machine learning model to classify files as legitimate or malware.  
- Logs results and returns output to the frontend.

3. Flow of Operation:

- The user interacts with the GUI to select files or folders.  
 - The application invokes the Python script with the selected path.  
 - The script processes the input and returns the result (malware or legitimate).  
 - Results are displayed in the GUI and logged for administrative review.

## Usage Instructions

### Running the Application

1. Open the compiled ProtectWare executable on your Windows system.  
2. Follow the splash screen to access the main application interface.

### Scanning Files/Folders

1. Click the SCAN button to select a single file or the SCAN ALL button to select a folder.  
2. Browse to the desired file or folder and confirm your selection.  
3. The application will display the scan results in the output section.

### Updating the Application

Click the UPDATE VERSION button to refresh the application with the latest features or model updates.

### Exiting the Application

Use the EXIT button to close the application.

## Python Script Details

File: virusChecker.py

The script performs the following tasks:  
1. Feature Extraction:  
 - Extracts characteristics from PE files, such as entropy, section sizes, and imported functions.  
  
2. Machine Learning:  
 - Loads a pre-trained model to classify files based on extracted features.  
  
3. Logging:  
 - Logs the scan results, including file paths and classification outcomes (legitimate or malware), to a designated log file.  
  
4. Command-Line Interface:  
 - Accepts a file or folder path as input.  
 - Scans files recursively in directories.

Example Usage:

python virusChecker.py <path\_to\_file\_or\_folder>