Documentation for USB Sanitizer

# Overview

The USB Sanitizer is a Python-based tool designed to monitor and clean USB drives by detecting and quarantining suspicious files. The tool uses the Watchdog library to monitor file changes on the USB drive and logs activities for audit and review purposes.

# Features

* Monitors a specified USB drive for new files.
* Detects and quarantines suspicious files based on file extensions and filenames.
* Logs detected suspicious files and quarantine actions.
* Ensures files with the same name are uniquely quarantined by appending a timestamp.

# Prerequisites

* Python 3.x
* watchdog library
* logging library (part of Python's standard library)
* shutil library (part of Python's standard library)
* datetime library (part of Python's standard library)
* os library (part of Python's standard library)

# Installation

1. Install the watchdog library:

pip install watchdog

1. Ensure you have the other required libraries (which are part of Python's standard library).

# Usage

1. Update the USB\_PATH variable in the script to point to your USB drive.
2. Run the script
3. The script will perform an initial scan and then start monitoring the USB drive for new files.
4. Detected suspicious files will be moved to a quarantine folder within the USB drive.
5. Check the log file (USB-Sanitization/usb\_sanitizer.log) for details about detected and quarantined files.

# Code Explanation

* **Logging Configuration:** Sets up logging to record activities to a log file.
* **Path Configuration:** Specifies the USB drive path and quarantine folder.
* **Suspicious File Criteria:** Defines file extensions and filenames to be considered suspicious.
* **Scanning Function:** Recursively scans the USB drive for suspicious files and quarantines them.
* **Quarantine Function:** Moves suspicious files to the quarantine folder, ensuring unique filenames.
* **Event Handler:** Watches for new files on the USB drive and triggers the scan and clean process.
* **Main Execution:** Performs an initial scan and sets up the observer to monitor the USB drive.