ObfuscateLogs.exe

# Table of Contents

[Table of Contents 1](#_Toc187831308)

[Overview 2](#_Toc187831309)

[Features 2](#_Toc187831310)

[Requirements 2](#_Toc187831311)

[Installation 2](#_Toc187831312)

[Usage 2](#_Toc187831313)

[Running the Program from Command Line 2](#_Toc187831314)

[Options 2](#_Toc187831315)

[Usage Examples 3](#_Toc187831316)

[Example 1: Obfuscate a Single Log File 3](#_Toc187831317)

[Example 2: Obfuscate All Files in a Directory 3](#_Toc187831318)

[Example 3: Use a Custom Output Folder 3](#_Toc187831319)

[Example 4: Enable Detailed Logging 3](#_Toc187831320)

[Example 5: Obfuscate IPv4 Addresses 4](#_Toc187831321)

[Example 6: Use a Custom Keyword Mapping File 4](#_Toc187831322)

[Example 7: Check the Program Version 4](#_Toc187831323)

[Creating a Windows Shortcut for Drag-and-Drop Analysis 4](#_Toc187831324)

[Steps to Create the Shortcut 4](#_Toc187831325)

[Configuration File (`.ini`) 5](#_Toc187831326)

[Example `keywords.ini` File: 5](#_Toc187831327)

[Sections 6](#_Toc187831328)

[Customization 6](#_Toc187831329)

[Notes 6](#_Toc187831330)

[Logging 6](#_Toc187831331)

[Functionality 7](#_Toc187831332)

[Getting Help 7](#_Toc187831333)

# Overview

`ObfuscateLogs.exe` is a Windows executable designed to process log files or directories of log files and obfuscate any personal or sensitive data based on predefined criteria. The program supports processing individual files or entire directories, and it allows for keyword-based obfuscation using a configuration file (`.ini` format).

This tool is particularly useful for sanitizing logs before sharing or analyzing them to ensure sensitive information is not exposed.

# Features

* Obfuscates sensitive data such as:
  + HTTP/HTTPS URLs
  + IPv4 addresses
  + User-defined keywords (from an `.ini` file)
* Supports both single-file and batch (folder) processing.
* Detailed logging of obfuscation operations.
* Supports custom keyword mappings through a configuration file.

# Requirements

* Windows 10 or later.
* No external dependencies are required.

# Installation

1. Download the `ObfuscateLogs.exe` file.
2. Place the `.exe` file in a directory of your choice.

# Usage

## Running the Program from Command Line

To use the program, open a Command Prompt (CMD) window and run the following command:

ObfuscateLogs.exe [options] <path>

## Options

* **path** (required): The path to the log file or folder containing log files to process. If a folder is specified, all log files in the folder (and its subdirectories) will be processed.
* **-o** or **--output** (optional): Specifies the path to the output folder where obfuscated files will be saved. If not specified, the program will use the same directory as the input file or folder.
* **-i** or **--ipv4** (optional): Enables obfuscation of IPv4 IP addresses. If this option is not specified, IPv4 obfuscation is disabled.
* **-k** or **--keywords** (optional): Specifies the path to a custom .ini file containing user-defined keyword mappings. If not specified, the program will look for a default .ini file in the same directory as the .exe file.
* **-d** or **--detailed** (optional): Enables detailed logging of individual obfuscations. If this option is not specified, detailed logging is disabled.
* **-v** or **--version** (optional): Displays the version of the program and exits.
* **-h** or **--help** (optional): Displays a help message with information about the program's usage and options, then exits.

# Usage Examples

## Example 1: Obfuscate a Single Log File

To obfuscate a single log file:

ObfuscateLogs.exe C:\path\to\logfile.log

This will process `logfile.log` and save the obfuscated file in the same directory with the suffix `\_obfuscated`.

## Example 2: Obfuscate All Files in a Directory

To obfuscate all log files in a directory:

ObfuscateLogs.exe C:\path\to\logs\

This will process all log files in the specified directory and its subdirectories, saving the obfuscated files in the same folder structure under the specified output directory.

## Example 3: Use a Custom Output Folder

To specify a custom output folder for the obfuscated files:

ObfuscateLogs.exe C:\path\to\logs\ -o C:\path\to\output\

This will save the obfuscated files in the `C:\path\to\output\` directory.

## Example 4: Enable Detailed Logging

To enable detailed logging of the obfuscation process:

ObfuscateLogs.exe C:\path\to\logfile.log -d

Detailed logs will be generated, showing before/after values for each obfuscation.

## Example 5: Obfuscate IPv4 Addresses

To enable obfuscation of IPv4 IP addresses:

ObfuscateLogs.exe C:\path\to\logfile.log -i

This will enable the obfuscation of IPv4 IP addresses.

Notes:

* Intelligent Filtering: The tool incorporates logic to minimize the risk of mistakenly obfuscating unrelated data, such as software version numbers. However, some software version numbers may closely resemble IPv4 dotted-decimal notation and could still be obfuscated inadvertently.
* Custom Keyword Mapping: If maintaining software version numbers is critical while obfuscating IPv4 addresses, use the custom keyword mapping feature. This approach allows you to explicitly list the IPv4 addresses that need to be obfuscated, ensuring other data remains intact.

## Example 6: Use a Custom Keyword Mapping File

To use a custom `.ini` file for keyword replacements:

ObfuscateLogs.exe C:\path\to\logfile.log -k C:\path\to\keywords.ini

This will load the keyword mappings from `keywords.ini` for obfuscation.

## Example 7: Check the Program Version

To check the version of the program:

ObfuscateLogs.exe -v

This will display the version of the executable and exit.

## Creating a Windows Shortcut for Drag-and-Drop Analysis

To simplify the process of analyzing files or folders, you can create a Windows shortcut that allows you to drag and drop a file or folder onto the shortcut. The shortcut can also be configured to use a specific keywords file located on a shared network UNC path.

### Steps to Create the Shortcut

1. Locate the Executable File
   * Ensure the `.exe` file is located in a folder that is easily accessible. For example, `C:\Tools\ObfuscateLogs.exe`.
2. Create a Shortcut
   * Right-click on the `.exe` file and select Create shortcut.
   * Rename the shortcut to something meaningful, such as `AnalyzeLogs`.
3. Edit the Shortcut Properties
   * Right-click the shortcut and select Properties.
   * In the Target field, append the following command-line arguments:

"C:\Tools\ObfuscateLogs.exe" "%1" --keywords "\\NetworkShare\Path\keywords.ini"

Replace:

`C:\Tools\ObfuscateLogs.exe` with the full path to your executable.

`\\NetworkShare\Path\keywords.ini` with the full UNC path to your shared keywords file.

Example:

"C:\Tools\ObfuscateLogs.exe" "%1" --keywords "\\SharedDrive\Obfuscation\keywords.ini"

1. Enable Drag-and-Drop Support
   * The `%1` in the target ensures that the dropped file or folder path is passed to the executable as an argument.
2. Save Changes
   * Click `OK` to save the changes.
3. Test the Shortcut
   * Drag and drop a file or folder onto the shortcut to verify it works as expected.

Notes:

* The `%1` placeholder automatically captures the path of the dragged-and-dropped file or folder.
* Ensure the network location (UNC path) for the keywords file is accessible to the system running the shortcut.

# Configuration File (`.ini`)

The program supports a configuration file in `.ini` format to define keyword/replacement pairs for obfuscation. If no custom file is provided, the program will default to using a file named `ObfuscateLogs.ini` in the same directory as the `.exe` file.

## Example `keywords.ini` File:

[servers]

server1=generic\_server1

server2=generic\_server2

[users]

admin=generic\_admin

guest=generic\_guest

[general]

password=obfuscated\_password

email=obfuscated\_email

## Sections

* [servers]: Replace server names with generic placeholders.
* [users]: Replace user names with generic placeholders.
* [general]: Replace general sensitive keywords (e.g., passwords, emails) with obfuscated values.

### Customization

* Adding Sections: You can add additional section headers as desired to organize your keywords. For example, you might include sections such as [databases], [applications], or [network].
* Informational Headers: The section headers (e.g., [servers], [users]) are purely informational and do not affect the program's functionality. They are provided as a way for the end user to group and organize keywords for clarity and convenience.

## Notes

* Keywords and their replacements must be provided in key=value pairs within each section.
* All keyword matches are case-insensitive. For example, the keyword Admin will match admin, ADMIN, or any variation of case.
* Duplicate keywords across different sections will result in the last defined value being used.
* If the .ini file does not exist, the program will create one with a default template.

# Logging

The program generates a log file in the output directory, which records the obfuscation operations performed, including the file names, line numbers, and types of obfuscation (e.g., HTTP URL, IPv4 address, keyword replacement).

Log files are named using the format `\_\_obfuscation\_log\_YYYYMMDD\_HHMMSS.log`.

# Functionality

Obfuscation of URLs: HTTP/HTTPS URLs are obfuscated by replacing the domain with a generic placeholder (e.g., generic-domain-1.com).

Obfuscation of IP Addresses: IPv4 addresses are obfuscated using a reserved IP range (e.g., 192.0.2.1).

Keyword-based Obfuscation: Keywords defined in the .ini file are replaced with corresponding obfuscated values.

# Getting Help

This program is released under the GNU General Public License, Version 3 (GPL-3.0). See the LICENSE file for more details.

This program comes with ABSOLUTELY NO WARRANTY and is unsupported.