42_MicroForensX

Forensic in windows !

Summary: Micro_ForensiX: Analyze recent file activity with a user-friendly desktop app.

Version: 1.00

Contents

I **Preamble** **2**

II **Objectives** **3**

III **General rules** **4**

IV **Mandatory Part** **5**

V **Submission and peer-evaluation** **7**

Chapter I

Preamble

This subject is the production of a partnership between 42 and Microsoft Corporation.

Microsoft Corporation is an American multinational technology corporation headquartered in Redmond, Washington.Microsoft's best-known software products are the Windows line of operating systems, the Microsoft Office suite, and the Internet Explorer and Edge web browsers.

Through this partnership, we aim to provide you with a unique opportunity to simplify your journey towards obtaining certifications offered by Microsoft. These certifications hold significant value and recognition in the industry, enabling you to enhance your professional profile and unlock exciting career prospects in the field of security.

To access the Microsoft certification programs and explore the wide range of certificates available, you can visit the following link: Microsoft Security Certification. This comprehensive platform offers extensive training resources and examinations covering various security-related topics.

By successfully completing the projects and earning Microsoft certifications, you will demonstrate your proficiency and expertise in security practices. These certifications serve as a testament to your skills and can open doors to exciting career opportunities.

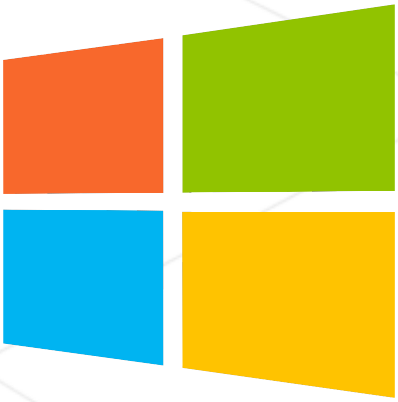

Figure I.1: https://www.microsoft.com/

Chapter II

Objectives

In partnership with Microsoft

> You're provided with a helper pdf, foundable inside the attachments of the subject.
> It will show you how to access the VMs created for you to complete this subject, how to lock your VMs, etc.

The objective of this project is to develop WindowsForensiX Lite, a desktop application for Windows that allows users to analyze recently accessed files.

The application should provide an intuitive user interface for specifying search parameters, display analysis results in a clear and organized manner, and offer the ability to export the results for further use.

The goal is to create a user-friendly and efficient tool for quick analysis of recent files on a Windows system.

Chapter III

General rules

- Only this page will serve as a reference: do not trust rumors.
- This project need to be done on a Virtual Machine.
- This project must use the C# programming language.
- This project must use the flags: /warn:4 /warnaserror.
- Your program must not leak.
- You have the option to use a batch script or directly utilize a build system such as MSBuild or Visual Studio to manage the project's construction.
- If your program doesn't compile, you'll get `0`.

> ℹ `You can use any libraries you want. However, it's important to be able to justify your choices.`

Chapter IV

Mandatory Part

ℹ You're provided with a helper pdf, foundable inside the attachments of the subject.

It will show you how to access the VMs created for you to complete this subject, how to lock your VMs, etc.

In this section, we will delve into the specific requirements for the development of the WindowsForensiX Lite application. The objective is to create a functional prototype that showcases essential features while maintaining a manageable scope.

- Application Overview and Naming: Develop the WindowsForensiX Lite desktop application with a focus on analyzing recently accessed files within a Windows system. The application name should be "WindowsForensiX Lite". Although a simplified version of the full application, ensure that the core functionalities are implemented effectively.

- Recent File Information Retrieval: Utilize the Windows API to retrieve crucial information from recently accessed files. This includes extracting and presenting attributes such as the file name, full path, access date, modification date, creation date, and file extension. Use appropriate Windows event logs or directly access file metadata to obtain this information. Ensure accuracy and data integrity during information retrieval.

- User Interface Design: Design an intuitive user interface that empowers users to specify search parameters seamlessly. Implement input mechanisms that allow users to define a date range for analysis and select specific file types for scrutiny. The interface should be user-friendly, providing a clear understanding of how to interact with the application.

- Results Presentation: Implement a visually organized presentation for the analysis results. Design a display that exhibits key information about each recently accessed file. This information includes the file name, full path, access date, modification date, creation date, and file extension. Arrange the information in a structured layout that facilitates easy comprehension.

- Result Export Functionality: Equip users with the capability to export analysis results for external utilization. Develop a feature that enables users to export the displayed results to a CSV (Comma-Separated Values) file format. This export functionality should enhance the usability of the application by enabling users to store, share, or conduct further analysis on the data.

- Customizable Settings: Integrate a settings section that grants users the flexibility to personalize their experience. Offer options to modify settings such as the maximum number of displayed results and additional filters, if applicable. These customizable features should enrich the user's ability to tailor the application according to their preferences.

By meticulously implementing these aspects, the WindowsForensiX Lite application will successfully achieve the outlined objectives within a manageable scope. Remember that the aim is to create a functional prototype that effectively demonstrates the core functionalities of the application.

Chapter V

Submission and peer-evaluation

You're provided with a helper pdf, foundable inside the attachments of the subject.

It will show you how to access the VMs created for you to complete this subject, how to lock your VMs, etc.

Turn in your assignment in your `Git` repository as usual. Only the work inside your repository will be evaluated during the defense. Don't hesitate to double-check the names of your files to ensure they are correct.