

User Guide

SYSInfo Tool

Disclaimer

The SYSInfo Tool's features depend on your system setup and may need specific hardware, software, or permissions to work properly. Check the user guide for more details.

This document and the tool cannot be used for legal cases or to make claims against the SYSInfo Tool or its creators. By using the tool, you agree not to claim any patent rights based on the tool's design or features.

The SYSInfo Tool does not come with any guarantees. We are not responsible for any problems, errors, or damages caused by using this tool. Use it carefully, especially when working with sensitive files or systems.

SYSInfo Tool belong to AAAM. Other names mentioned may belong to others.

Copyright © 2024 AAAM. All rights reserved.

Table of Contents

Disclaimer	1
Introduction	3
Installed OS information:	3
BIOS/UEFI details:	3
Hardware information:	3
Registry Entries:	3
System Requirements	3
Operating System:	3
RAM:	3
Disk Space:	3
Installation	4
Prerequisites	4
Python Installation:	4
SYSInfo Utility Installation	4
Troubleshooting	12
FAQs	12
Appendix	13

Introduction

Welcome to the SYSInfo Tool user guide. SYSInfo Tool is a powerful and user-friendly GUI-based application designed to provide detailed system information, either from a live system or a forensic analysis of exported registry files. This tool gives you the ability to examine a wide range of system data, making it an essential tool for IT professionals, system administrators, and forensic experts.

Whether you're working on an active system or analyzing a forensic analysis, SYSInfo Tool allows you to access critical system details directly from the Windows Registry. This includes:

Installed OS information: Version, installation dates, and time stamps.

BIOS/UEFI details: System firmware information, version, and configuration.

Hardware information:

1. Hard Drives (HDD/SSD)
2. Installed RAM
3. System model, manufacturer, and serial number

Registry Entries: Detailed registry values related to system configuration and more.

SYSInfo Tool provides as much information as possible, helping you gather essential system data for troubleshooting, system audits, and forensic analysis.

This user guide will walk you through the installation process, usage instructions, and troubleshooting tips, ensuring you can make the most of all the features SYSInfo Tool has to offer. Whether you're retrieving information from a live system or forensic analysis of exported registry files, this tool simplifies your task of gathering comprehensive system data.

System Requirements

The SYSInfo Tool is designed to work on all modern Windows operating systems. There are no specific hardware or software requirements. However, it is recommended to use a system with the following for optimal performance:

Operating System: Windows 10 or later

RAM: 4 GB or more (recommended)

Disk Space: 50 MB or more

The tool should work on both live systems and forensic analysis, with no special configuration required.

Installation

Prerequisites

Before proceeding with the installation, ensure you have the following:

Python Installation:

The SYSInfo Tool is written in Python, so you need Python installed on your system.

Download the latest version of Python from [Python](#).

FTK Imager (Required for forensic analysis only):

FTK Imager is needed to obtain protected or inaccessible files.

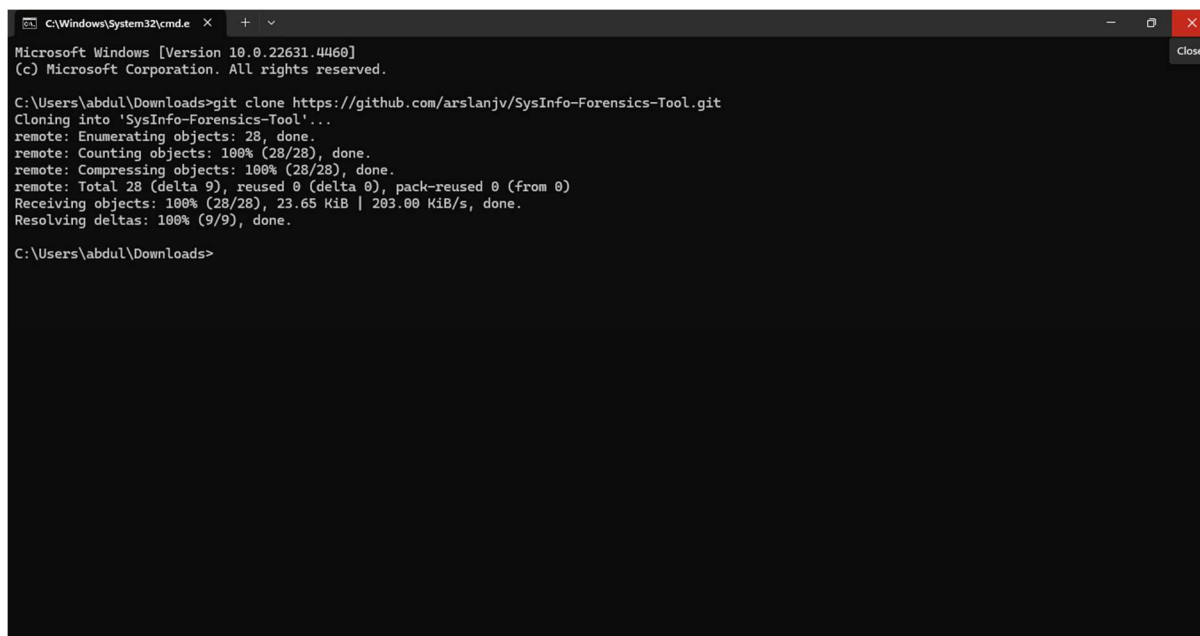
Download FTK Imager from [FTK-Imager](#).

Install and configure FTK Imager on your system as per the instructions provided on their website.

SYSInfo Utility Installation

1. First, you need to get the file of the SYSInfo Tool from the GitHub.
2. Clone the repository:

```
git clone https://github.com/arslanjv/SysInfo-Forensics-Tool.git
cd SysInfo-Forensics-Tool/df_proj
```



```
C:\Windows\System32\cmd.exe X + -
Microsoft Windows [Version 10.0.22631.4460]
(c) Microsoft Corporation. All rights reserved.

C:\Users\abdul\Downloads>git clone https://github.com/arslanjv/SysInfo-Forensics-Tool.git
Cloning into 'SysInfo-Forensics-Tool'...
remote: Enumerating objects: 28, done.
remote: Counting objects: 100% (28/28), done.
remote: Compressing objects: 100% (28/28), done.
remote: Total 28 (delta 9), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (28/28), 23.65 KiB | 203.00 KiB/s, done.
Resolving deltas: 100% (9/9), done.

C:\Users\abdul\Downloads>
```

3. Open Command Prompt and verify the Python installation by typing: `python --version`.

```
C:\Windows\System32\cmd.exe X + -
Microsoft Windows [Version 10.0.22631.4460]
(c) Microsoft Corporation. All rights reserved.

C:\Users\abdul\Downloads\SysInfo-Forensics-Tool\df_proj>python --version
Python 3.13.0

C:\Users\abdul\Downloads\SysInfo-Forensics-Tool\df_proj>
```

4. Navigate to the SysInfo-Forensics-Tool/df_proj and install the required dependencies by running: **`pip install -r requirements.txt`**

```
C:\Windows\System32\cmd.exe X + -
(c) Microsoft Corporation. All rights reserved.

C:\Users\abdul\Downloads\SysInfo-Forensics-Tool\df_proj>pip install -r requirements.txt
Requirement already satisfied: Flask==3.0.3 in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from -r requirements.txt (line 1)) (3.0.3)
Requirement already satisfied: Jinja2==3.1.4 in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from -r requirements.txt (line 2)) (3.1.4)
Requirement already satisfied: psutil==6.1.0 in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from -r requirements.txt (line 3)) (6.1.0)
Requirement already satisfied: python-registry==1.3.1 in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from -r requirements.txt (line 4)) (1.3.1)
Requirement already satisfied: registry==0.4.2 in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from -r requirements.txt (line 5)) (0.4.2)
Requirement already satisfied: WMI==1.5.1 in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from -r requirements.txt (line 6)) (1.5.1)
Requirement already satisfied: Werkzeug==3.0.0 in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from Flask==3.0.3->-r requirements.txt (line 1)) (3.1.3)
Requirement already satisfied: itsdangerous==2.1.2 in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from Flask==3.0.3->-r requirements.txt (line 1)) (2.2.0)
Requirement already satisfied: click==8.1.3 in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from Flask==3.0.3->-r requirements.txt (line 1)) (8.1.7)
Requirement already satisfied: blinker==1.6.2 in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from Flask==3.0.3->-r requirements.txt (line 1)) (1.9.0)
Requirement already satisfied: MarkupSafe==2.0 in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from Jinja2==3.1.4->-r requirements.txt (line 2)) (3.0.2)
Requirement already satisfied: enum-compat in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from python-registry==1.3.1->-r requirements.txt (line 4)) (0.0.3)
Requirement already satisfied: unicodcsv in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from python-registry==1.3.1->-r requirements.txt (line 4)) (0.14.1)
Requirement already satisfied: pywin32 in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from WMI==1.5.1->-r requirements.txt (line 6)) (308)
Requirement already satisfied: colorama in c:\users\abdul\appdata\local\programs\python\python313\lib\site-packages (from click==8.1.3->Flask==3.0.3->-r requirements.txt (line 1)) (0.4.6)

C:\Users\abdul\Downloads\SysInfo-Forensics-Tool\df_proj>
```

5. Inside the tool's folder, run the command to start the SYSInfo Tool: **`python app.py`**. Note the output indicating the tool is running on a local server, such as: Running on **`http://127.0.0.1:5000``**

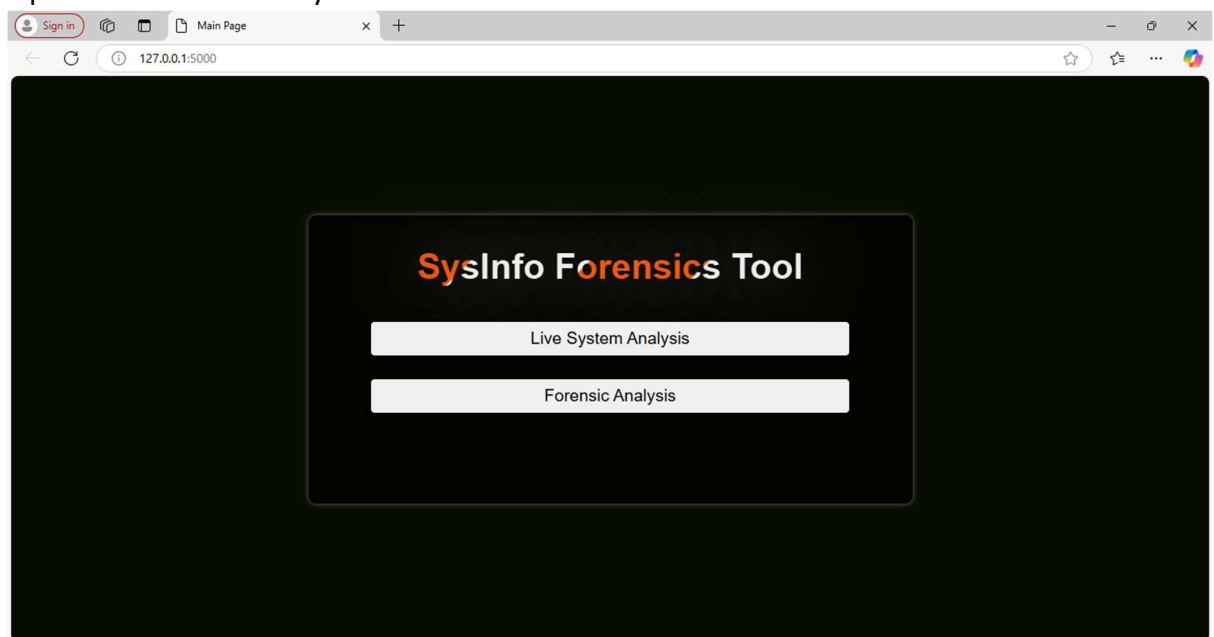
```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22631.4460]
(c) Microsoft Corporation. All rights reserved.

C:\Users\abdul\Downloads\SysInfo-Forensics-Tool\df_proj>python app.py
* Serving Flask app 'app'
* Debug mode: off
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
```

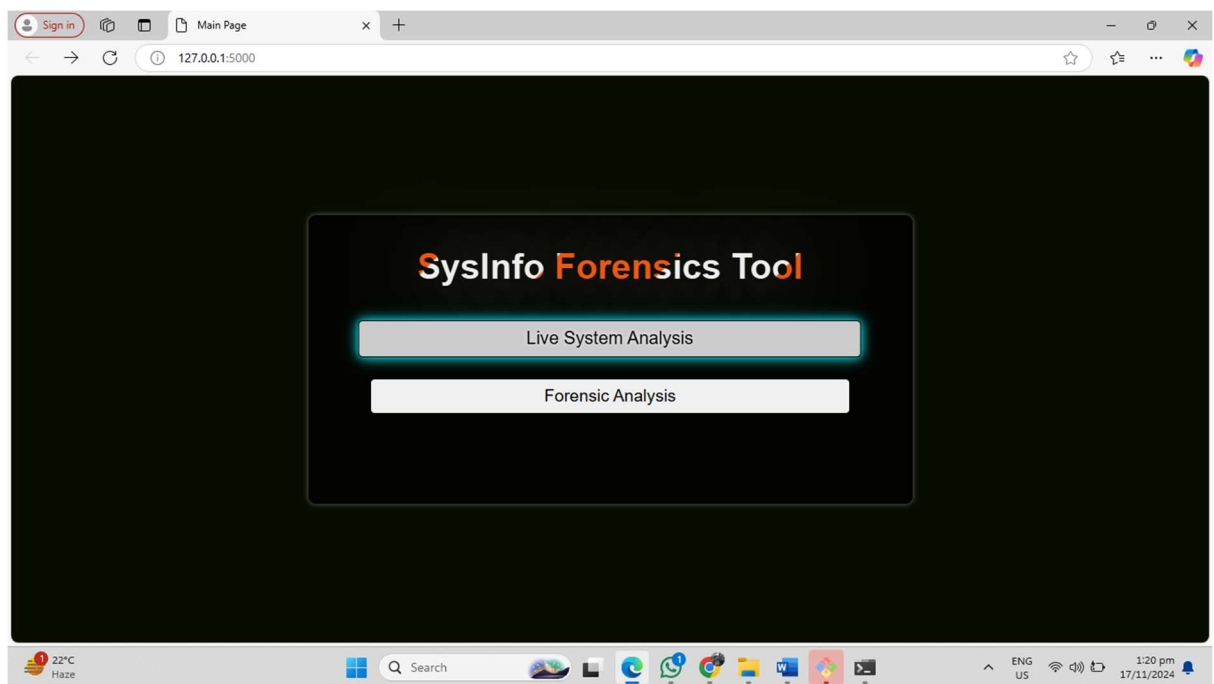
6. Open a web browser and go to the provided URL (e.g., `http://127.0.0.1:5000`). The homepage presents two options:

Option 1: Live System Analysis

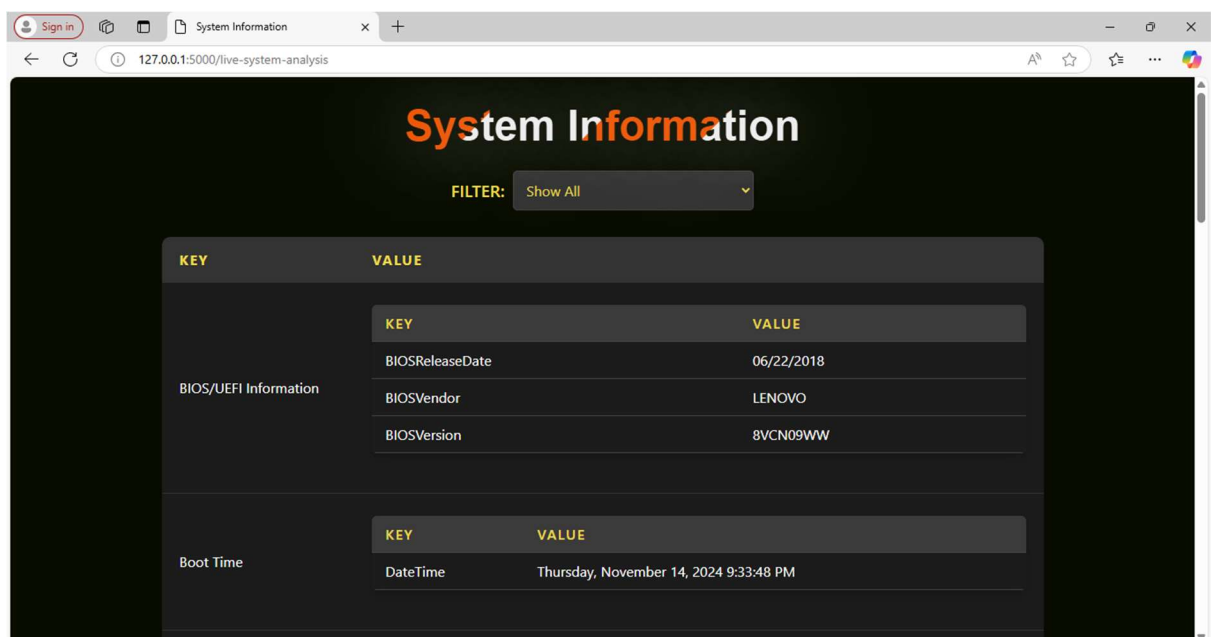
Option 2: Forensic Analysis

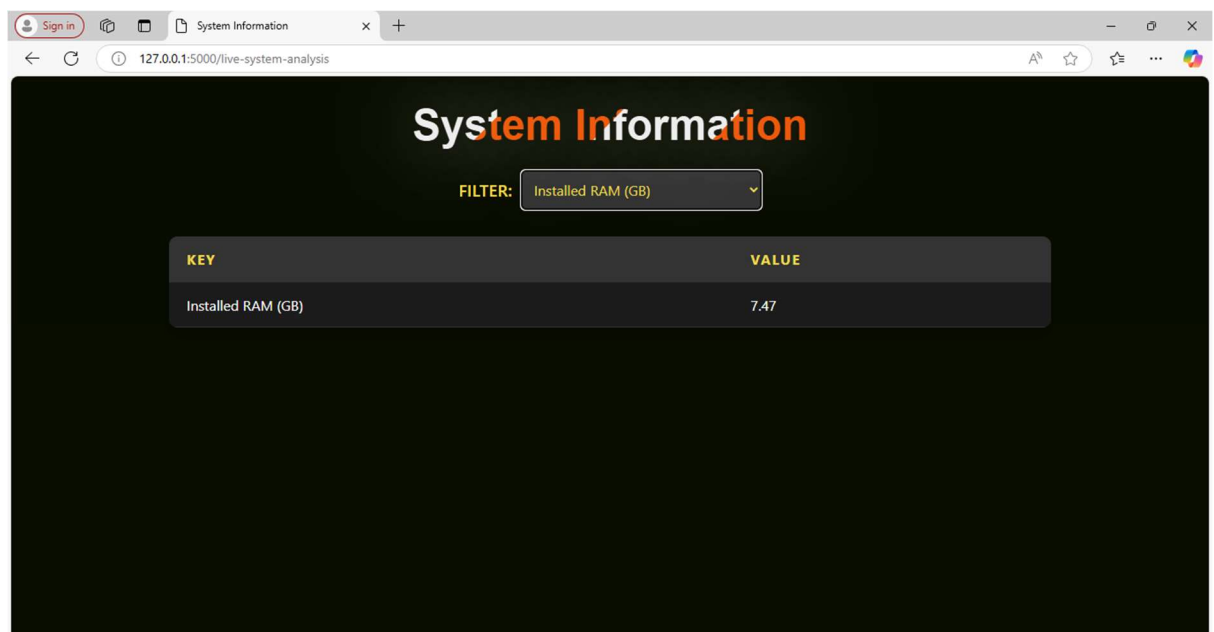
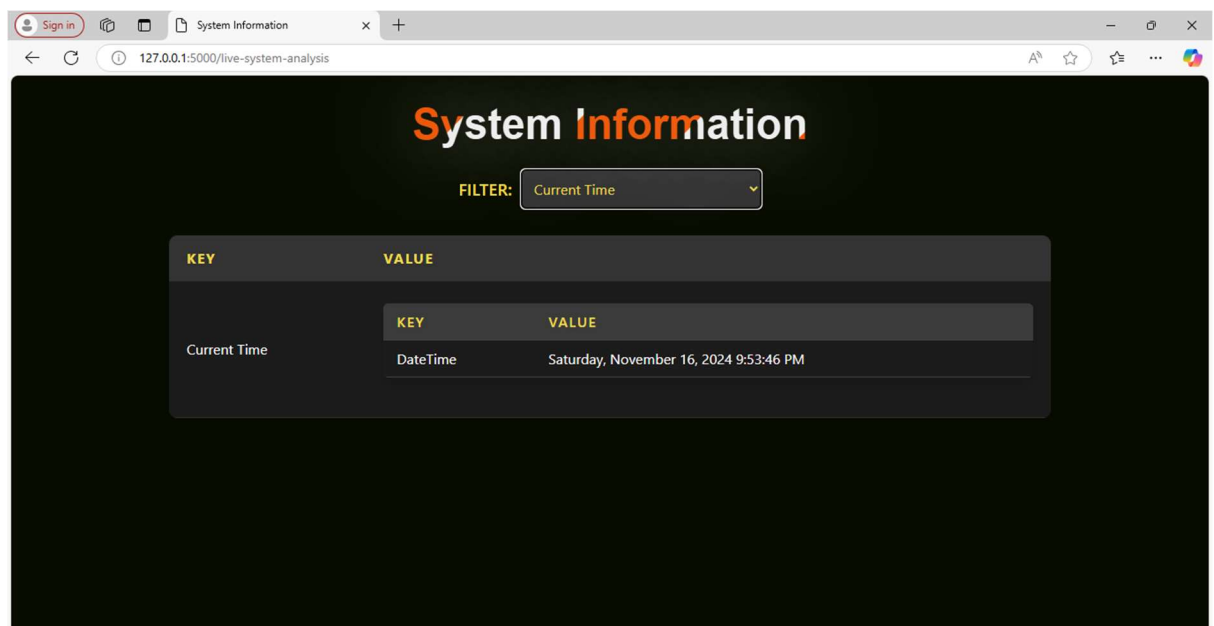


7. To perform a live system analysis, click **Live System Analysis**.

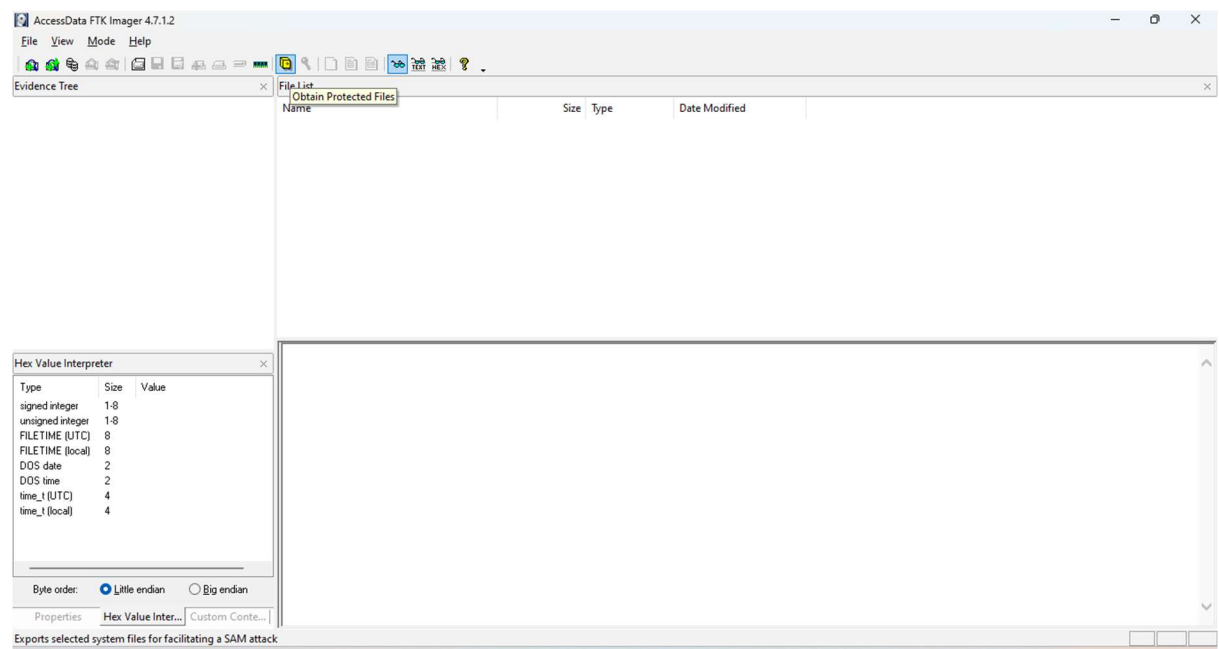


8. The tool retrieve data from the system registry and performs calculations. After completion, you will see detailed system information. Use the filter option to view specific information, such as registry values, OS version, hardware details, etc.

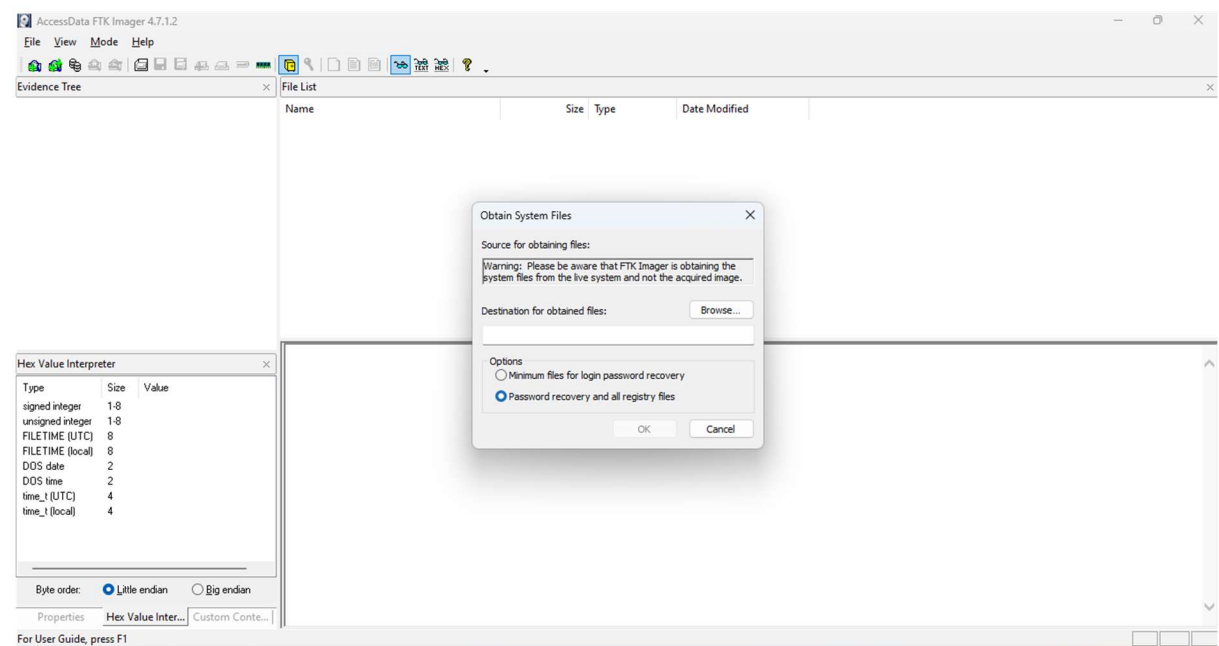




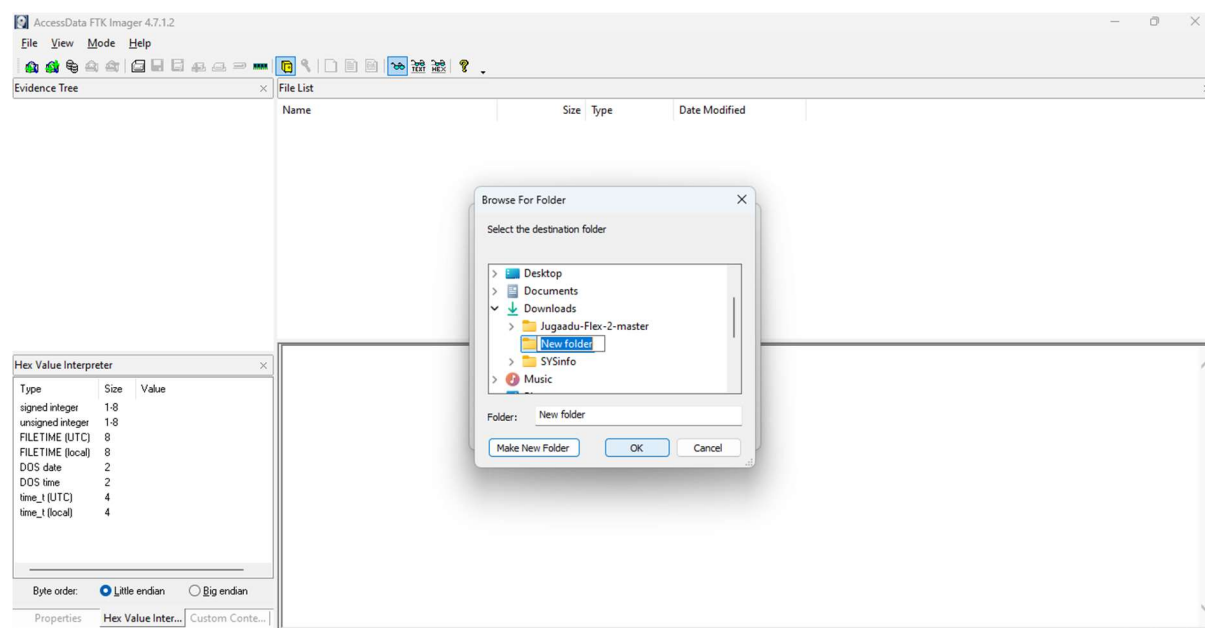
9. For forensic analysis, first use FTK Imager to extract protected files:
Open FTK Imager and click on **Obtain Protected File** in the menu.



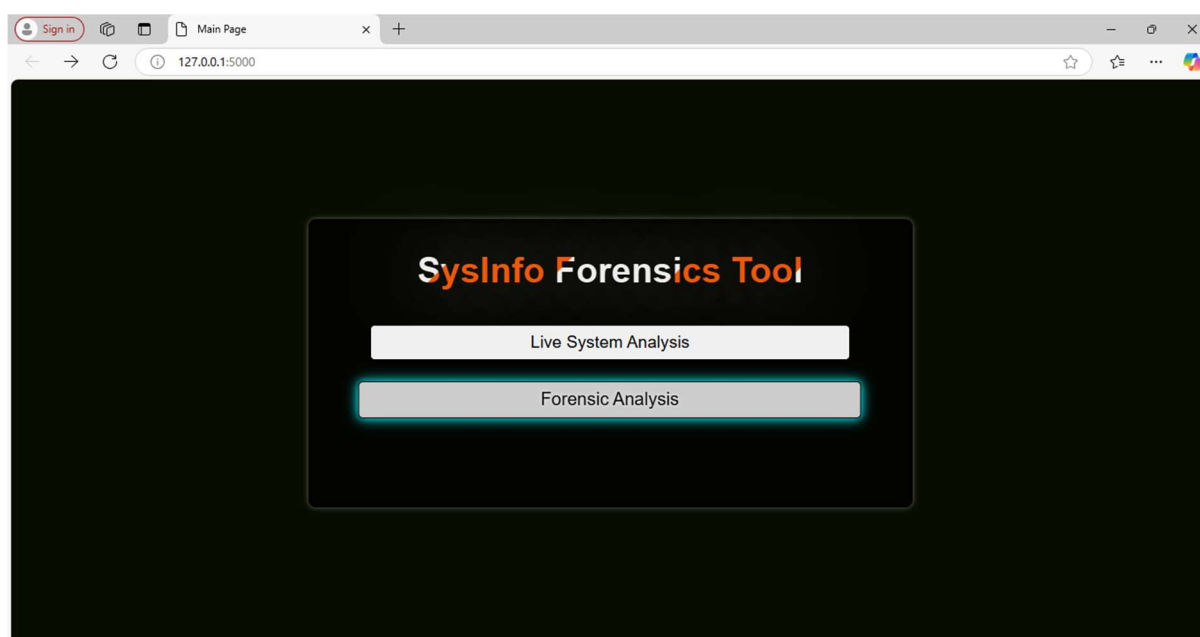
10. Select options for Password Recovery and Registry Files.



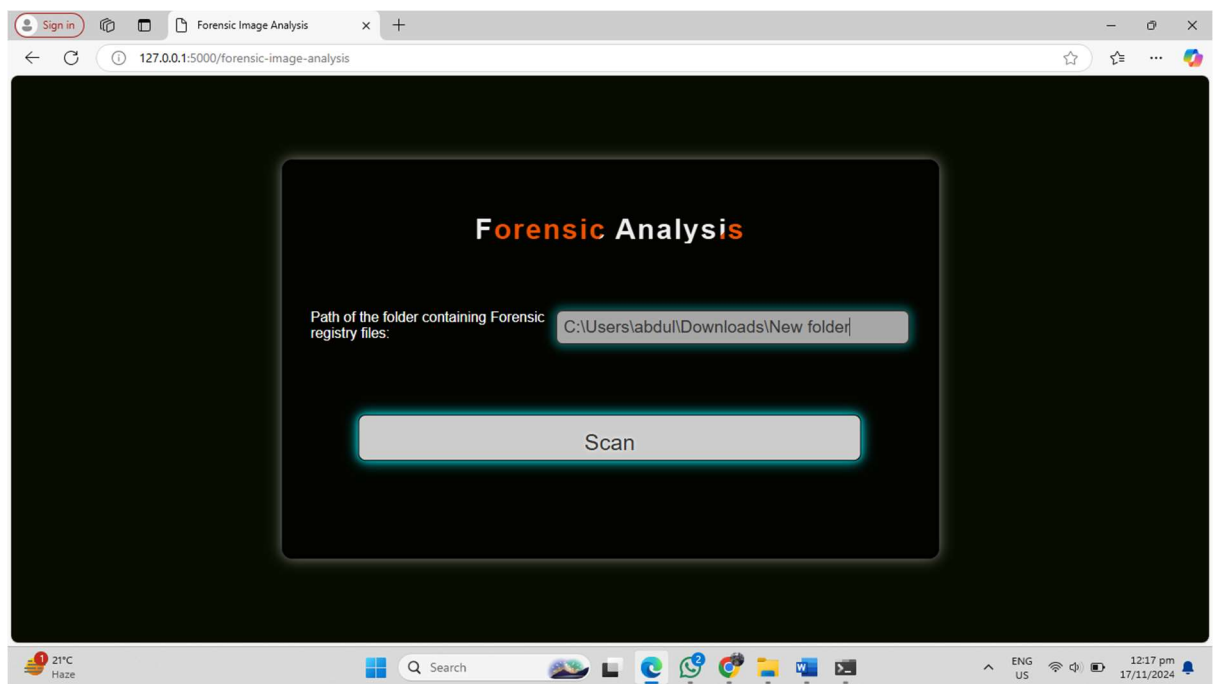
11. Save the extracted files to a new folder and remember the folder path.



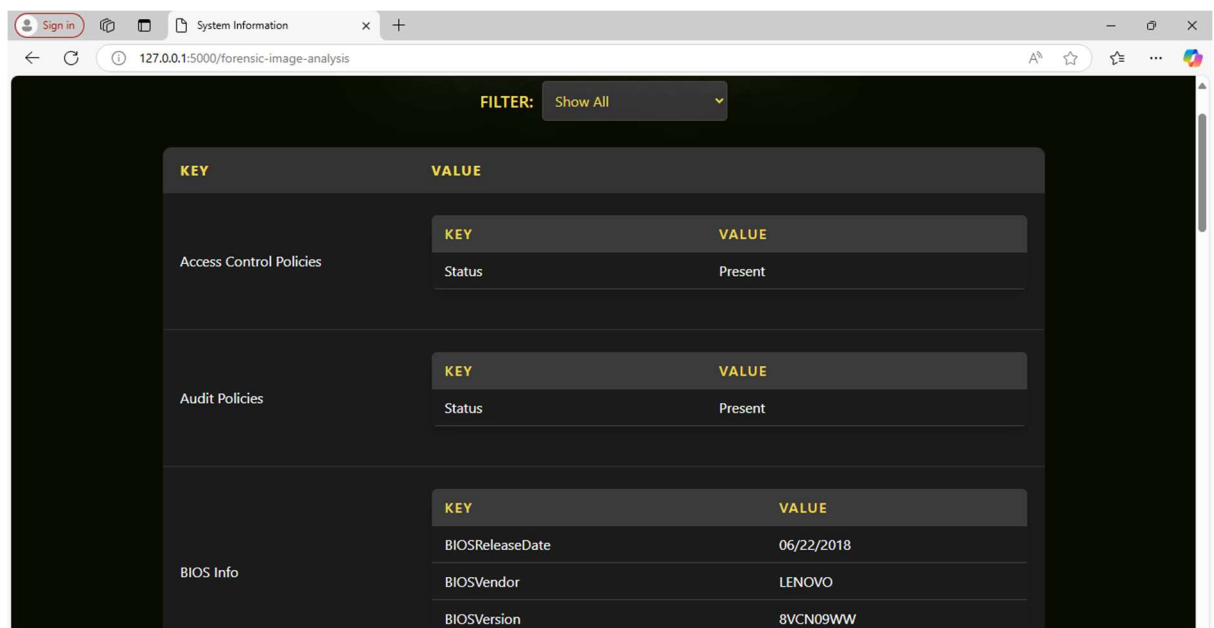
12. Return to the SYSInfo Tool webpage and select Forensic Analysis.

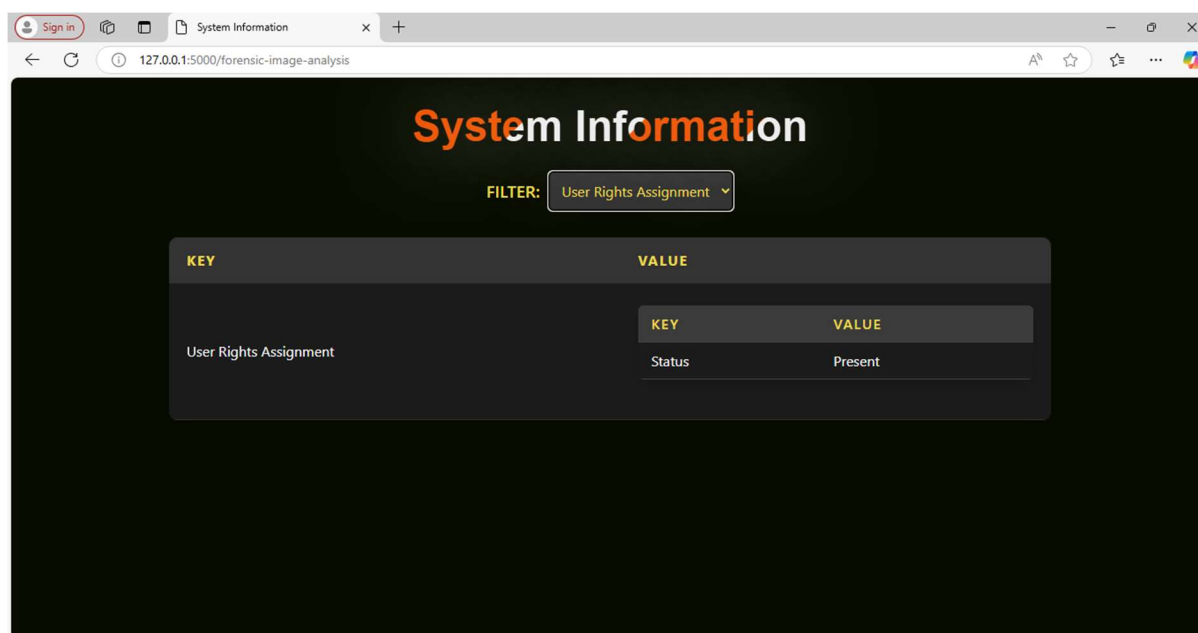


13. Enter the path to the extracted folder containing the registry files and click **Scan**.



14. The tool will analyze and display system information similar to the live system analysis.





Troubleshooting

Issue: Unable to load the hive.

Solution: Ensure the hive file is not in use by another application. Make sure you have proper access permissions to the file.

Issue: Incorrect data displayed.

Solution: Verify that the hive is not corrupted. Re-extract the hive or use a backup copy.

Issue: The tool fails to start.

Solution: Ensure that Python and all dependencies are correctly installed. Check if the correct version of Python is being used by running `python --version`.

Issue: Issue: The webpage is not loading.

Solution: Check if the Flask server is running correctly. Ensure no firewall or antivirus software is blocking the local server (`http://127.0.0.1:5000`).

Issue: The Forensic Analysis doesn't process the files.

Solution: Confirm that the correct path to the extracted registry files is entered. Ensure the registry files are not encrypted or password protected.

FAQs

Q: Can I use the tool on a live system?

A: Yes, but Administrator privileges are required for full access to system data.

Q: Is the tool compatible with older Windows versions?

A: No, it supports only Windows 10/11 and may not function correctly on earlier versions.

Q: Can I use the tool to analyse remote systems?

A: No, the tool is designed for use on local systems or forensic analysis only.

Q: Does the tool require an internet connection?

A: No, the tool works offline as it only needs local system data or forensic analysis of protected files.

Q: How do I stop the Flask server once it's running?

A: You can stop the server by pressing Ctrl + C in the Command Prompt window where it is running.

Appendix

Registry Hive File Paths:

System Registry Path: C:\Windows\System32\config\system

Security Registry Path: C:\Windows\System32\config\security

Software Registry Path: C:\Windows\System32\config\software

SAM Registry Path: C:\Windows\System32\config\sam

Commands:

To install dependencies:

```
pip install -r requirements.txt
```

To run the tool:

```
python app.py
```

----- The End -----