

Assignment 4: CHFIv9 Labs Module 05

Defeating Anti-forensics Techniques

Karthikeyan G

Roll Number: CB.SC.P2CYS24008

January 7, 2025

TASK 1: Launching and Updating Password Recovery Bundle

Recover File Password:

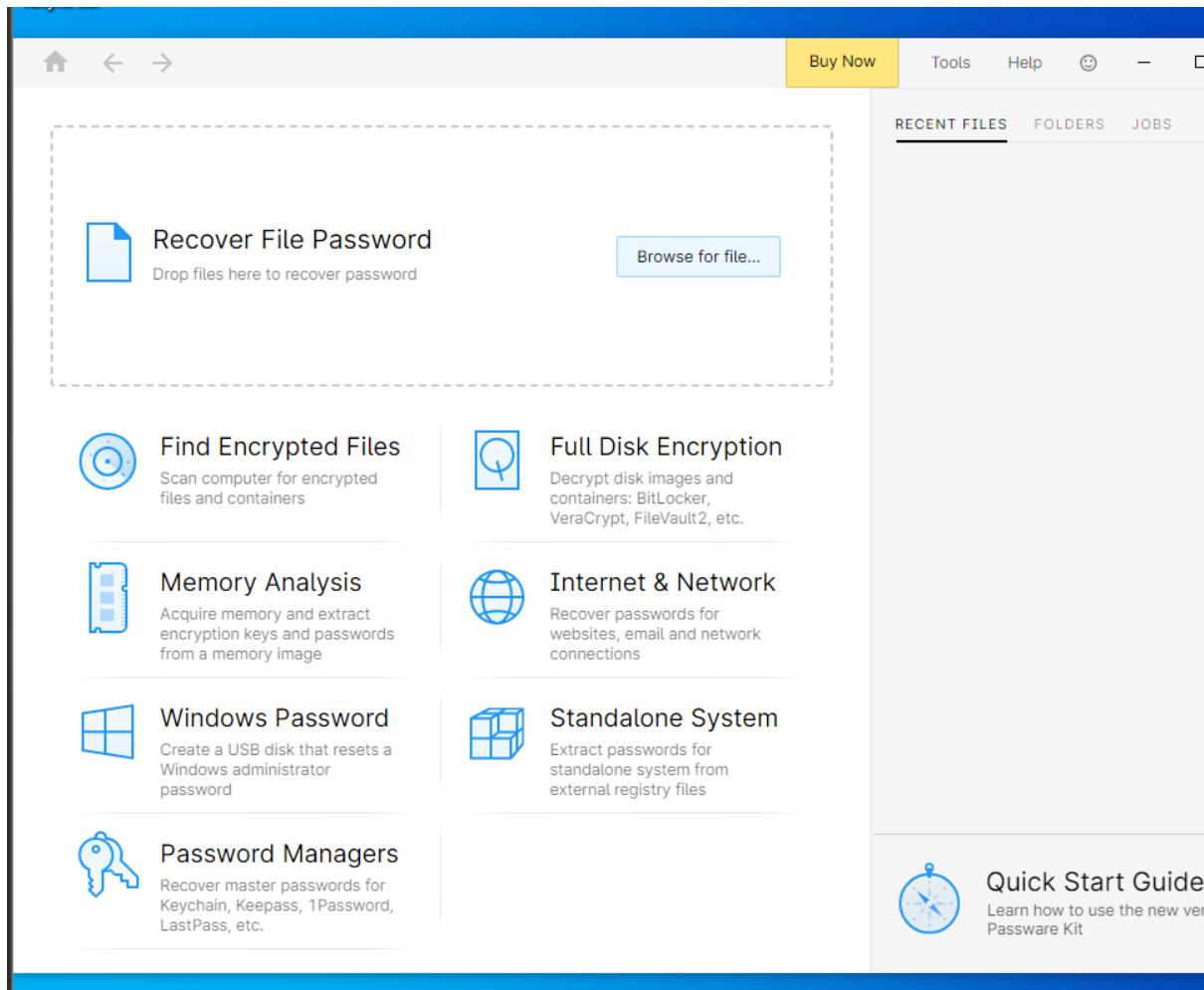


Figure 1: Open Passware Password Recovery Kit Forensic and select the option to "Recover File Password."

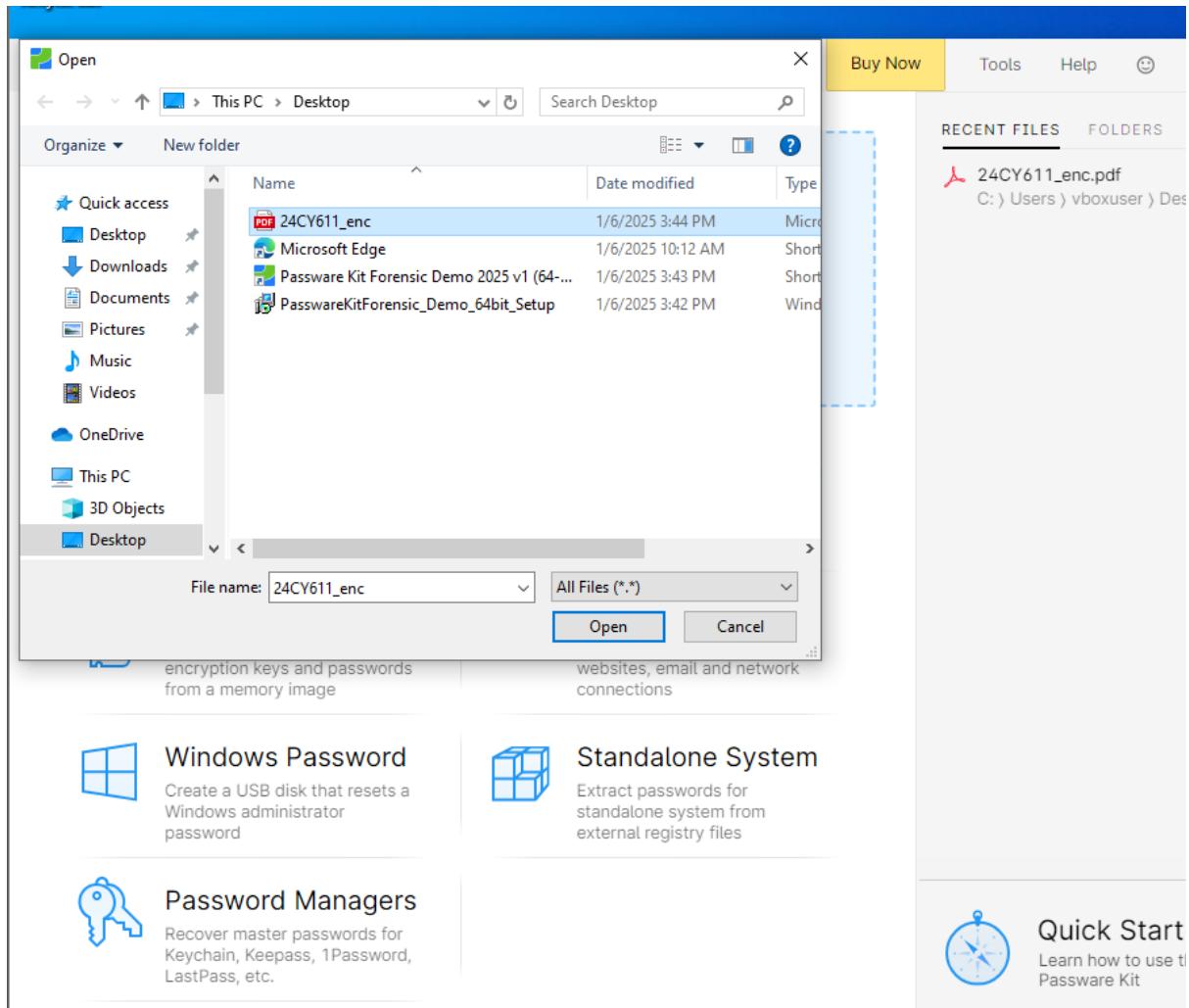


Figure 2: Select the encrypted file you wish to recover the password for and click "Open."

The screenshot shows the 'Recover Password' interface for a PDF file named '24CY611_enc.pdf'. The file is located at 'C:\Users\vboxuser\Desktop' and is an Acrobat 10.0-11.0 document. It requires a User Password, Open Password, Encrypted Metadata, Permissions Password, and AES Encryption. The complexity is listed as 'Brute-force - Slow'. Three recovery methods are presented:

- Use Predefined Settings**: Use default attacks to recover your password.
- Run Wizard**: Follow easy steps to set up password recovery if you know any details about the password.
- Customize Settings**: Set up attacks manually to recover your password.

At the bottom, there is a 'RECOVER' button and an 'Add Files' button.

Figure 3: In the wizard, choose the option to "Use Predefined Settings" for the recovery process.

The screenshot shows a software interface for recovering passwords. At the top, there are navigation icons (Home, Back, Forward) and a yellow "Buy Now" button. To the right are links for "Tools", "Help", and user settings. Below the header is a menu bar with tabs: "Files", "Passwords Found" (which is selected), "Resource Manager", "Performance", "Attacks", "Log", and "Network Log".

The main content area displays a file named "24CY611_enc.pdf". It includes the following details:

- File Type:** Acrobat 10.0-11.0 — User Password, Open Password, Encrypted Metadata, Permissions Password, AES Encryption, File p required
- Complexity:** ●●●● Brute-force - Slow
- MD5:** C61CFADB70973C2A226E5CB0FB01819B

Below these details, under the "Passwords" section, the found password is listed as "cat". The "Permissions" field shows "<disabled in demo>".

At the bottom left, status information is displayed: "PASSWORDS FOUND 1" and "TIME ELAPSED 2 seconds". At the bottom right are three buttons: "Print", "Save Job", "RESUME ATTACKS", "SAVE REPORT", and "DO".

Figure 4: Wait for the tool to complete the password cracking process.

Crack Compressed Folder or WinRAR File Password:

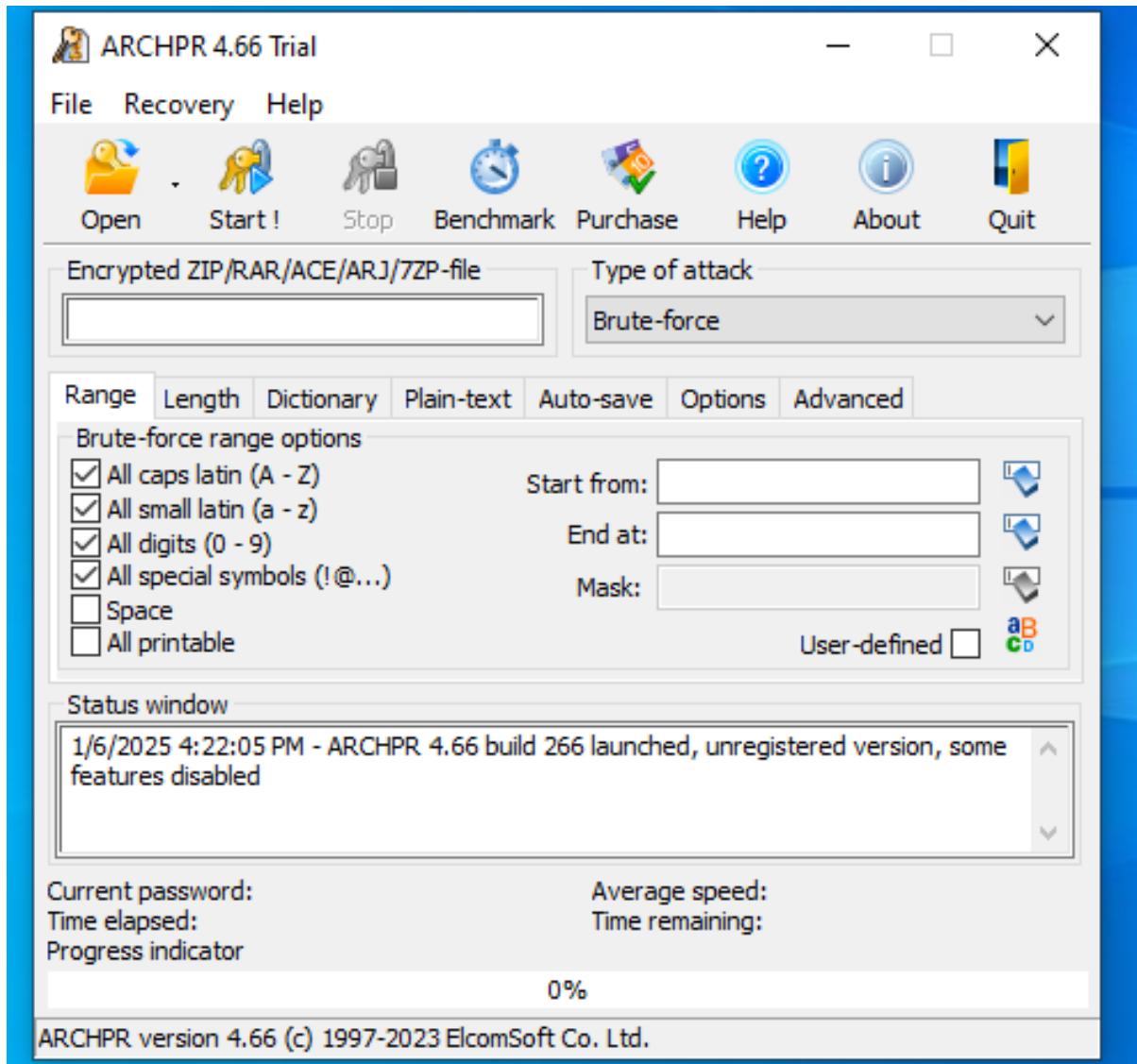


Figure 5: Install the Advanced Archive Password Recovery tool to begin the process.

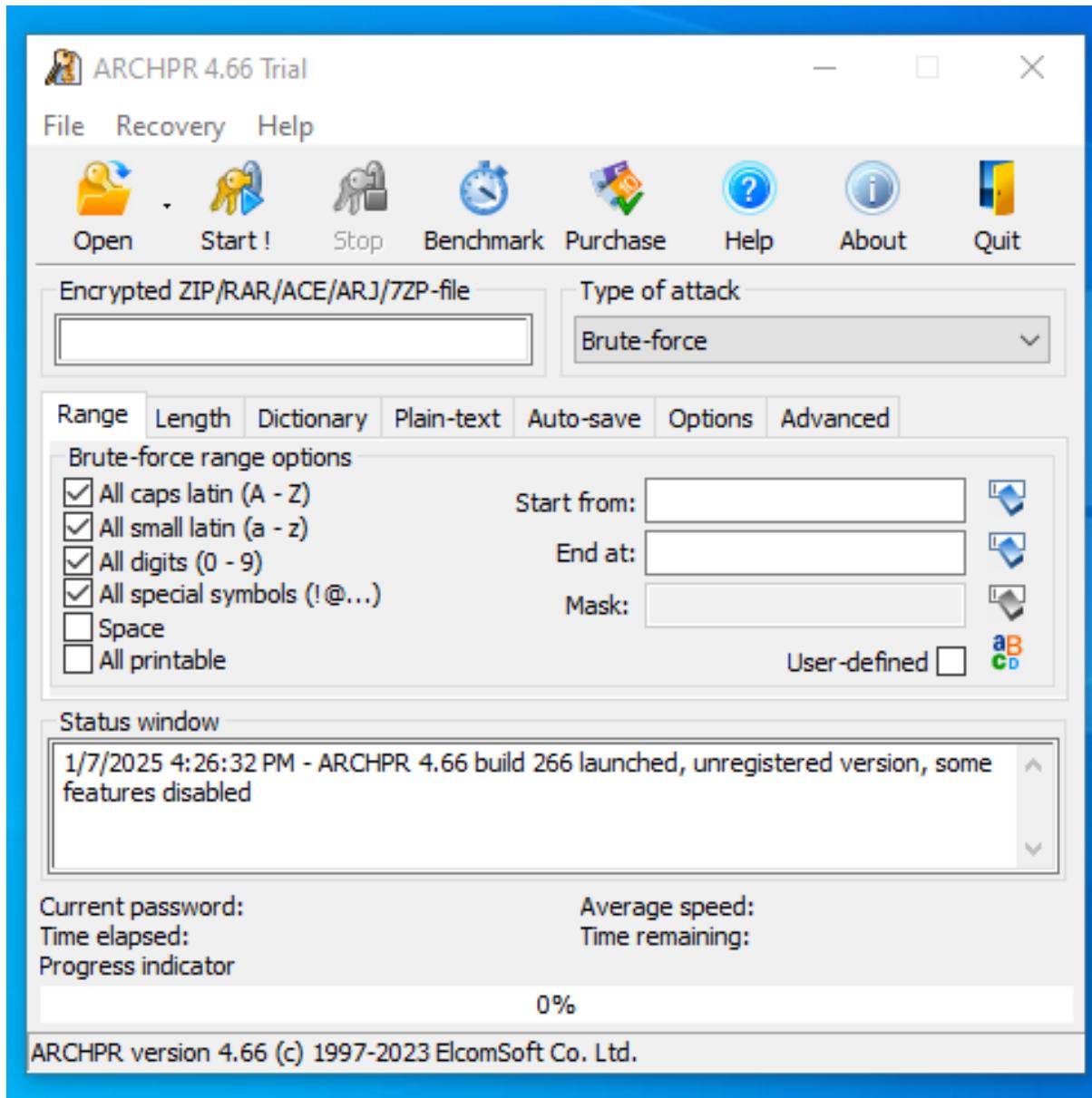


Figure 6: Provide the necessary cracking parameters such as the type of attack, range, length, and dictionary to be used.

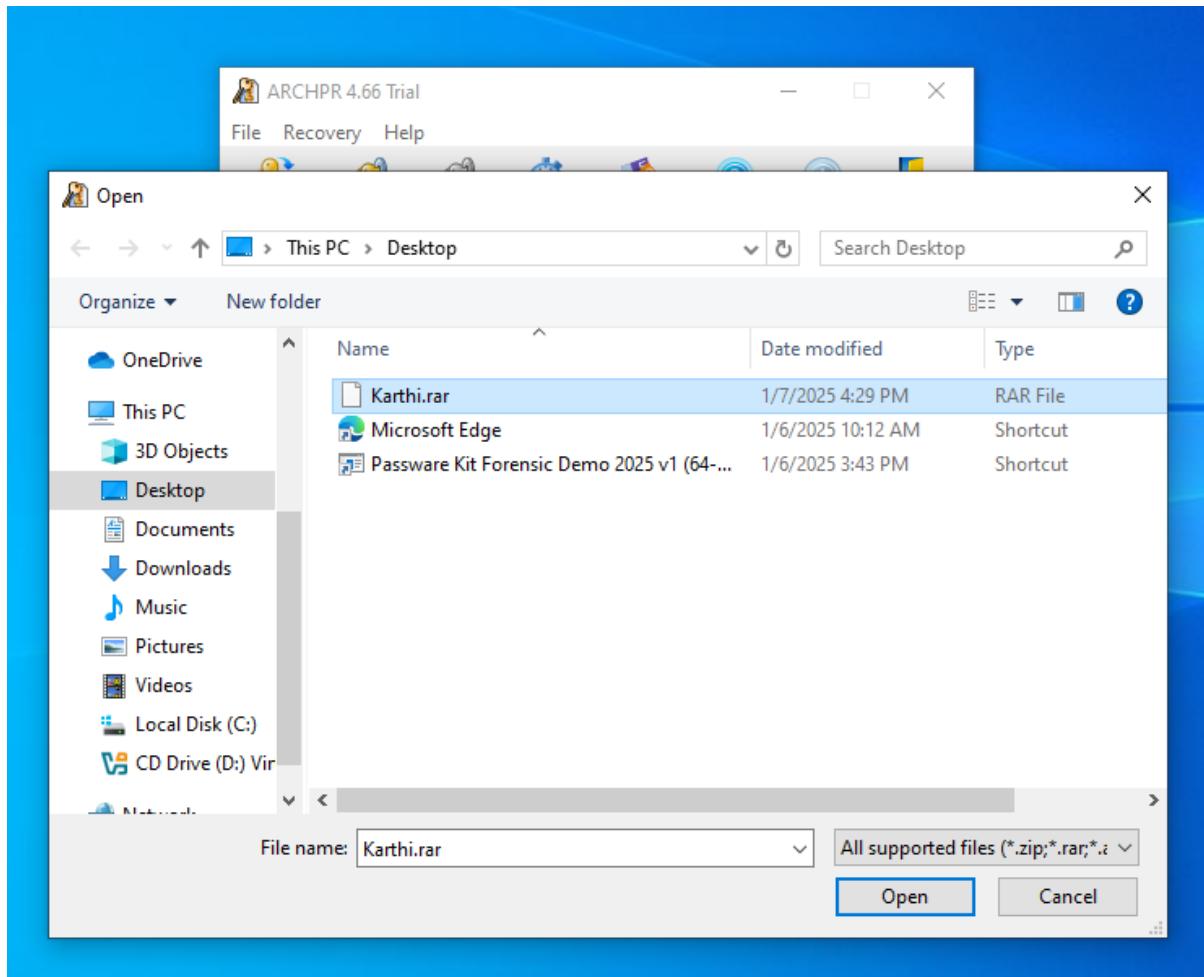


Figure 7: Click "Open" to add the WinRAR file whose password you wish to crack.

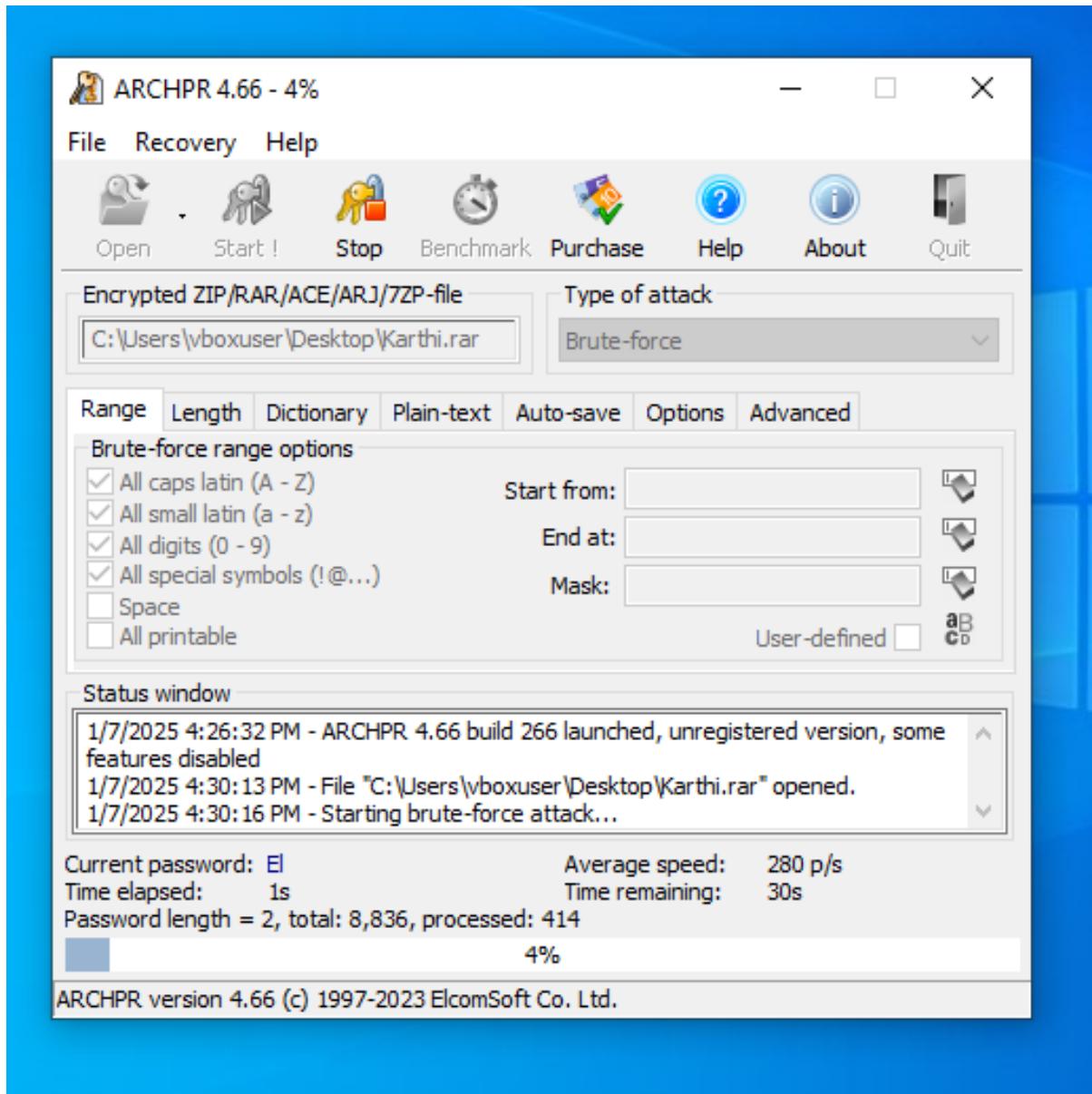


Figure 8: The tool will automatically start the process of cracking the password.

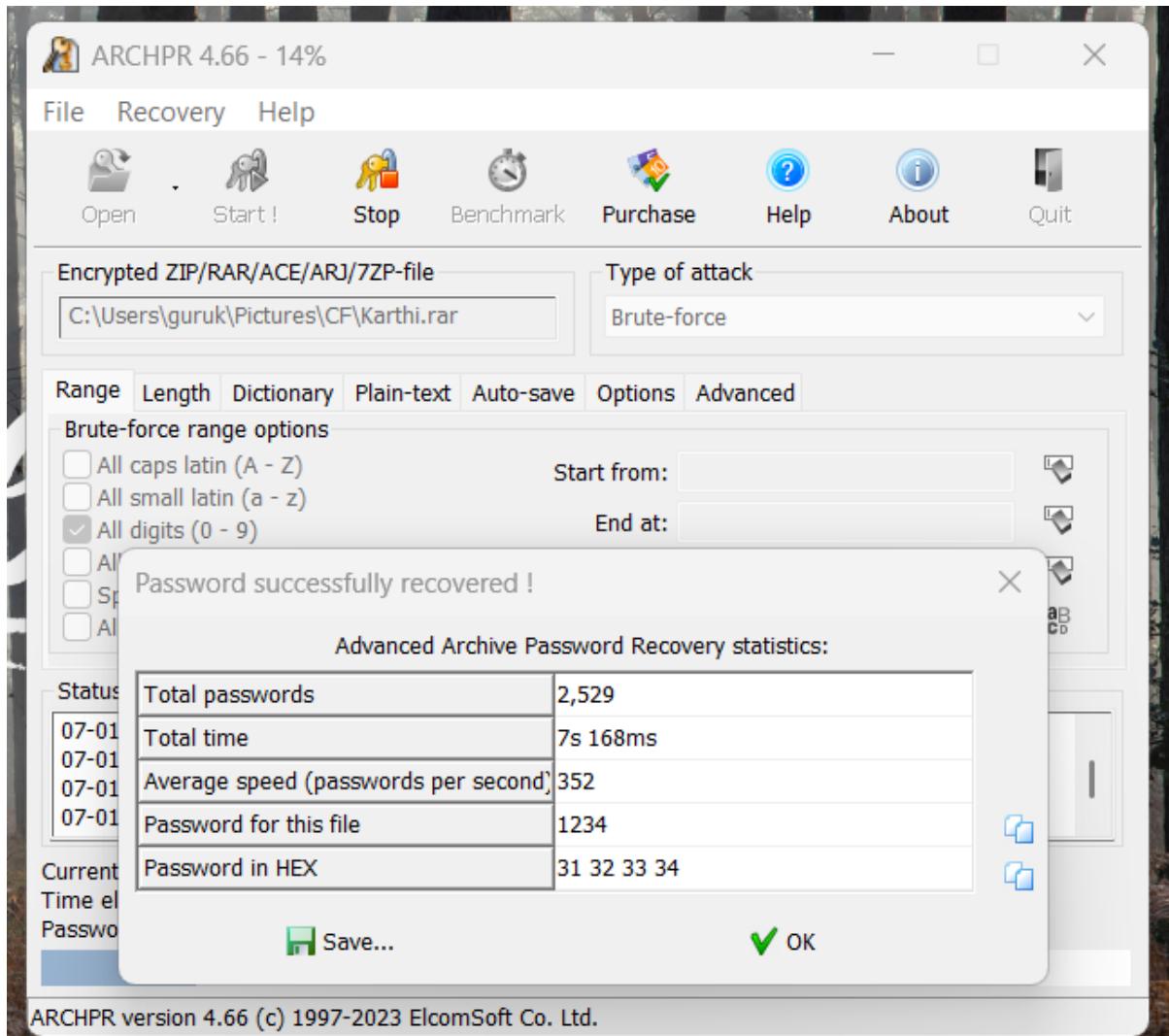


Figure 9: Result of the password cracking process.

Crack PDF File Password:

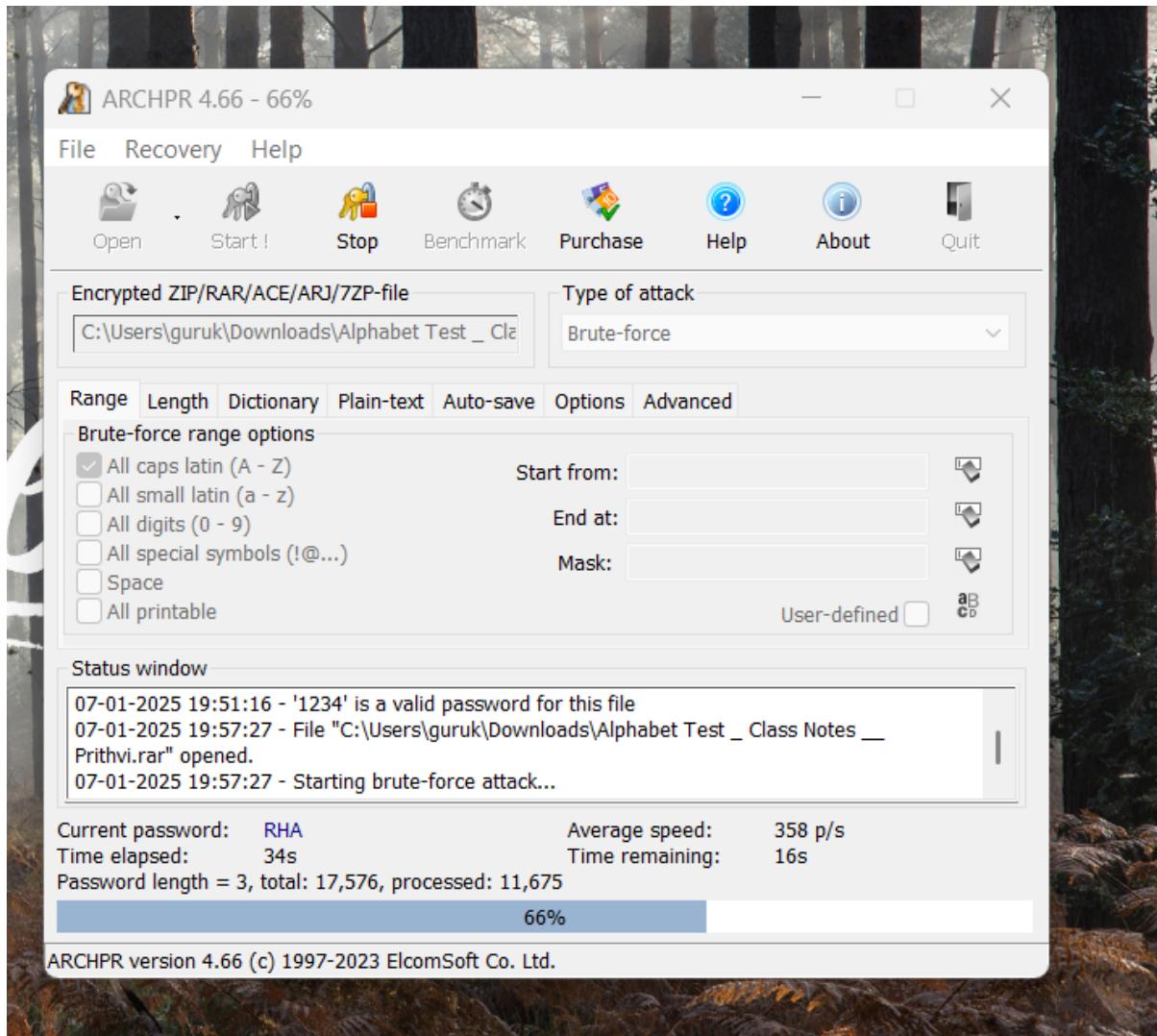


Figure 10: Install the Advanced PDF Password Recovery tool to begin the process.

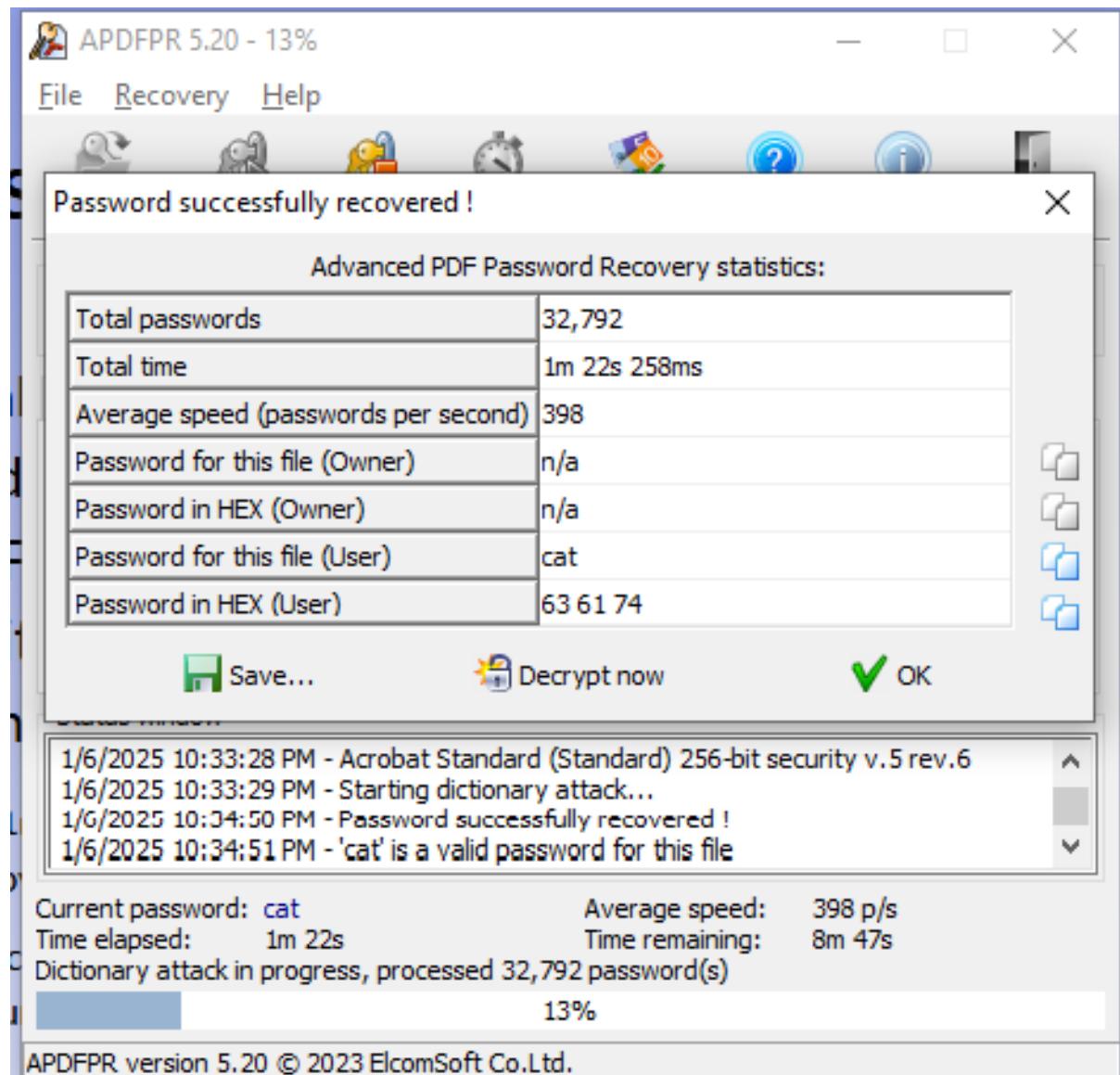


Figure 11: The tool will automatically start the process of cracking the PDF file password.

TASK 2: Detecting Steganography



Figure 12: image used for upcoming analysis.

Using StegSpy:

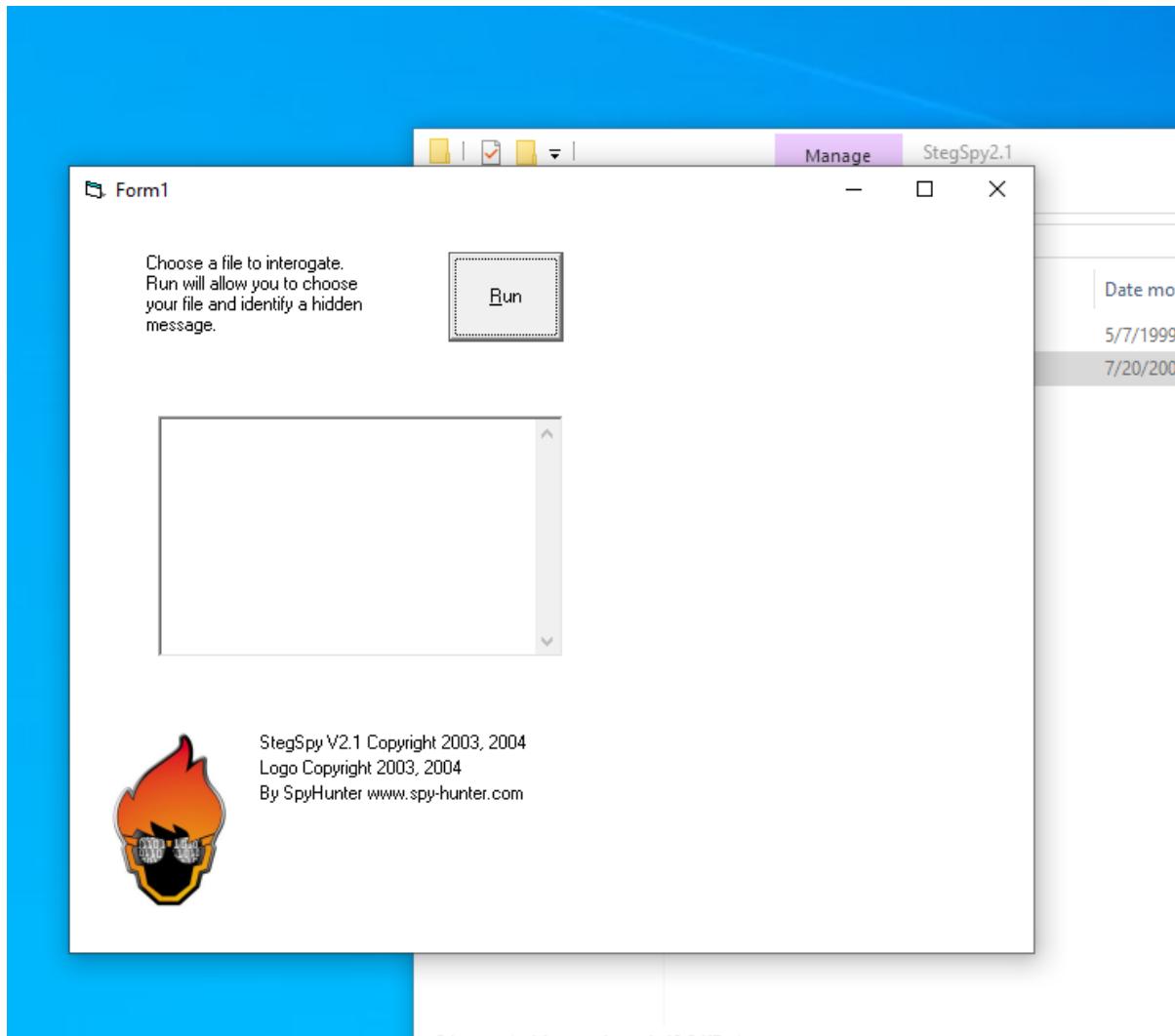


Figure 13: Open the StegSpy tool to begin the steganography detection process.

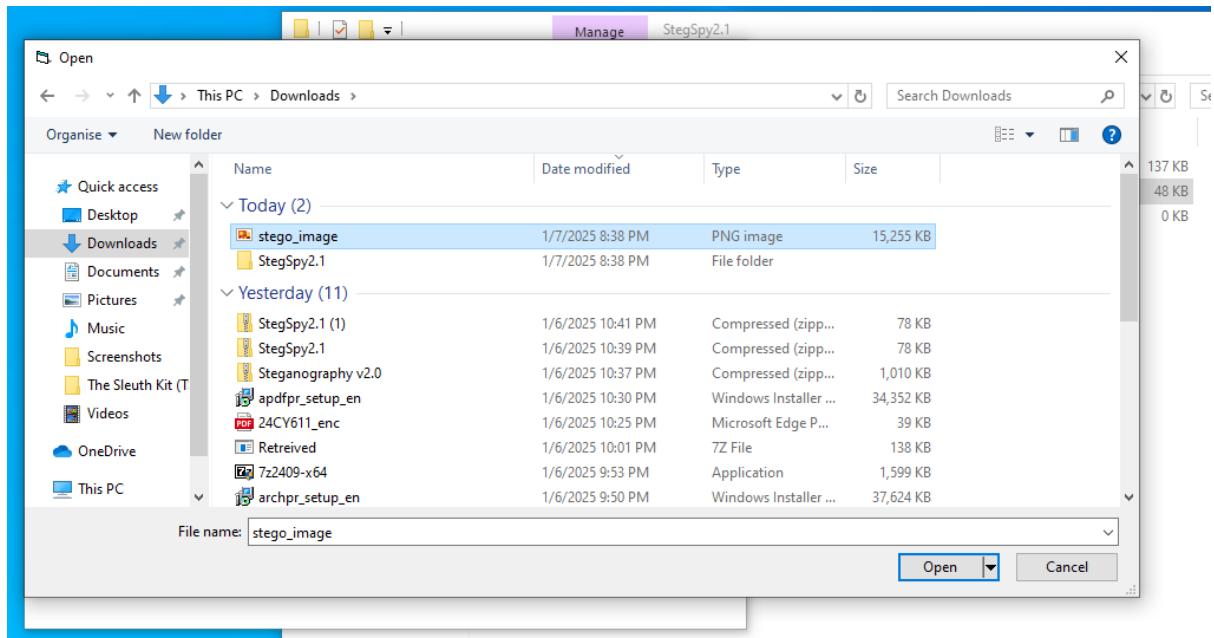


Figure 14: Click "Run" to add the suspicious file you wish to analyze.

Using Image Steganography Tool:

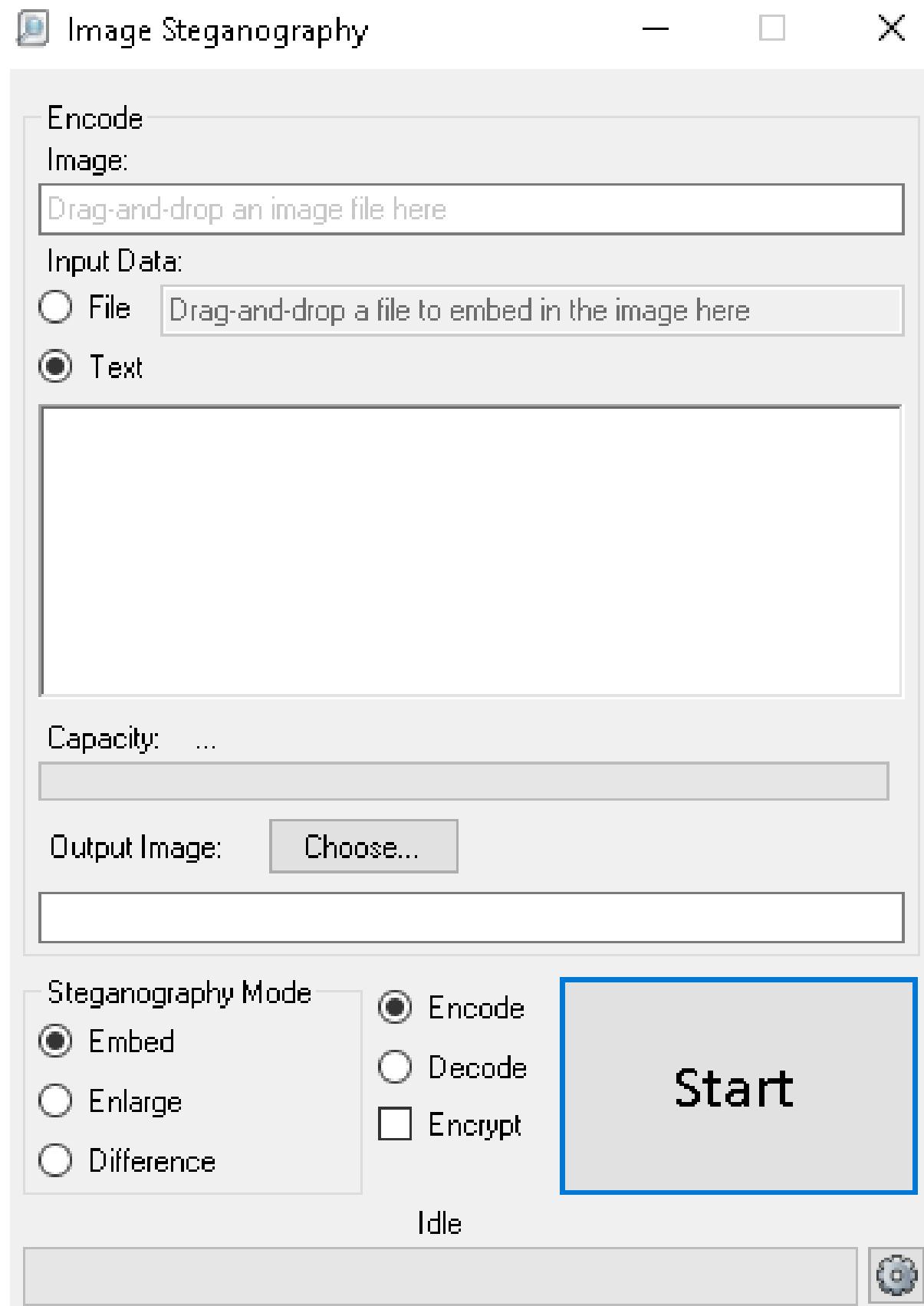


Figure 15: Install and launch the Image Steganography tool for analysis.

Image Steganography



The supplied image is either corrupted or invalid

OK

Figure 16: No further output was generated from the tool.

Using OpenStego:

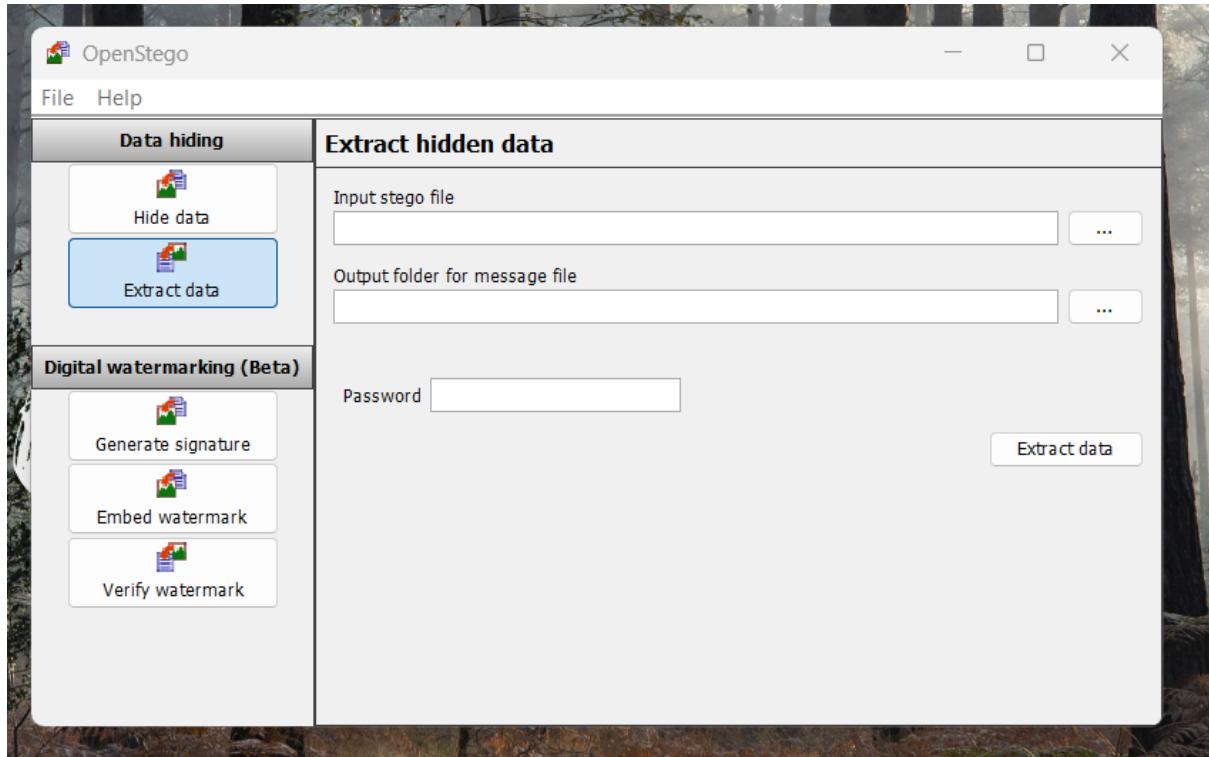


Figure 17: Install and launch the OpenStego tool to begin the steganography detection process.

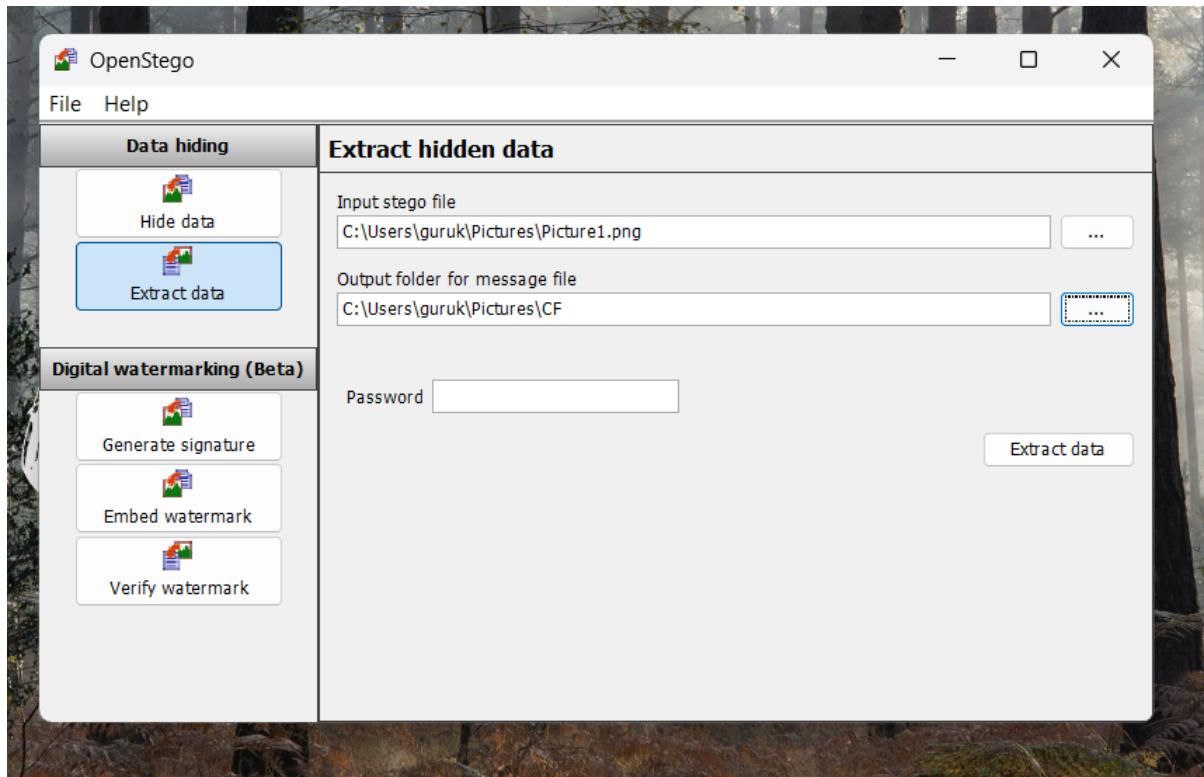


Figure 18: Click "Extract Data" and provide the location of the steganography file to be analyzed.

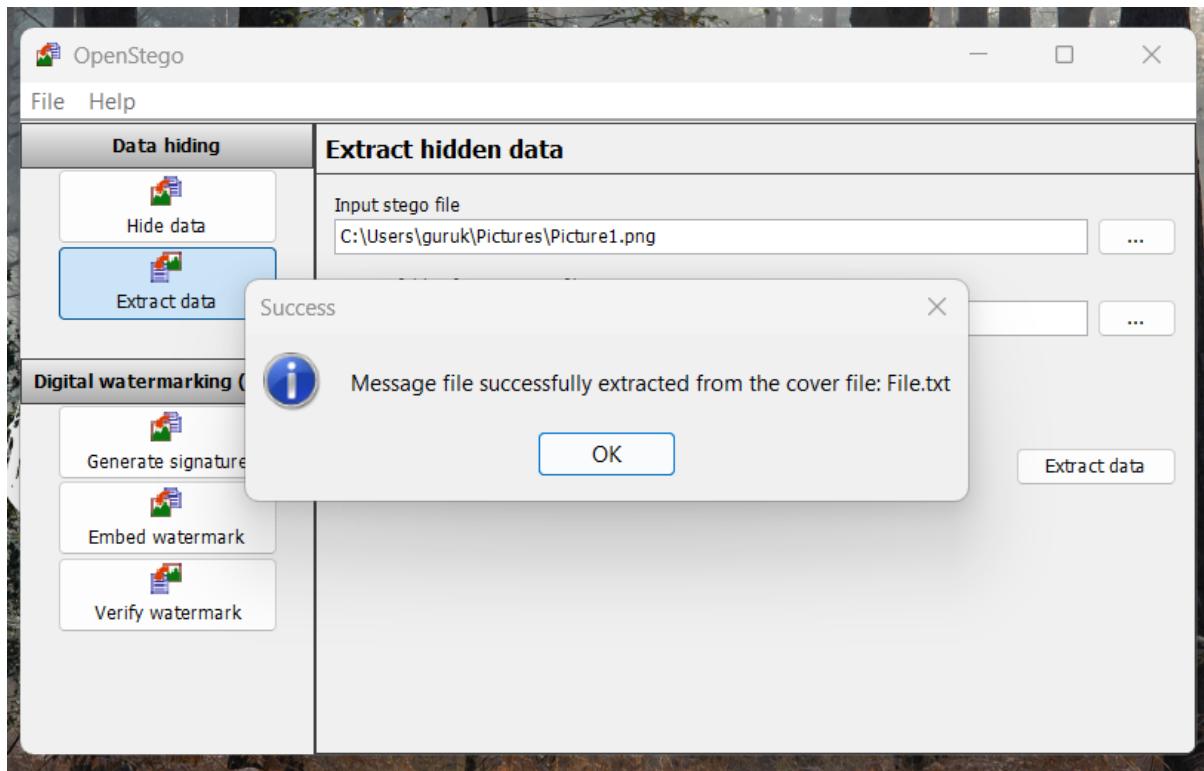


Figure 19: Successfully extracted the hidden data from the steganography file.

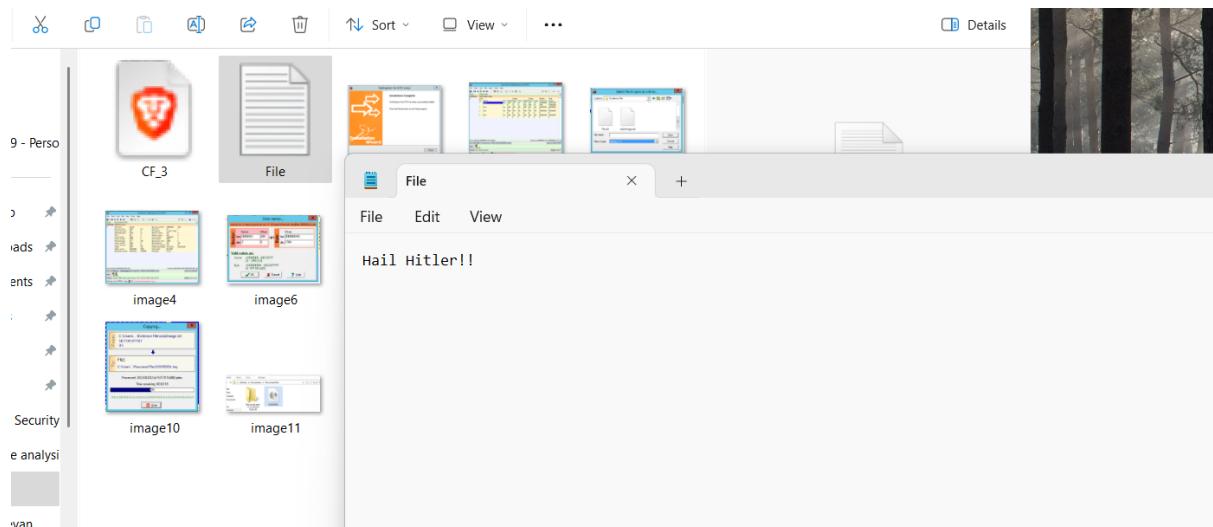


Figure 20: Extracted output displaying the hidden data.

Using DeepSound:

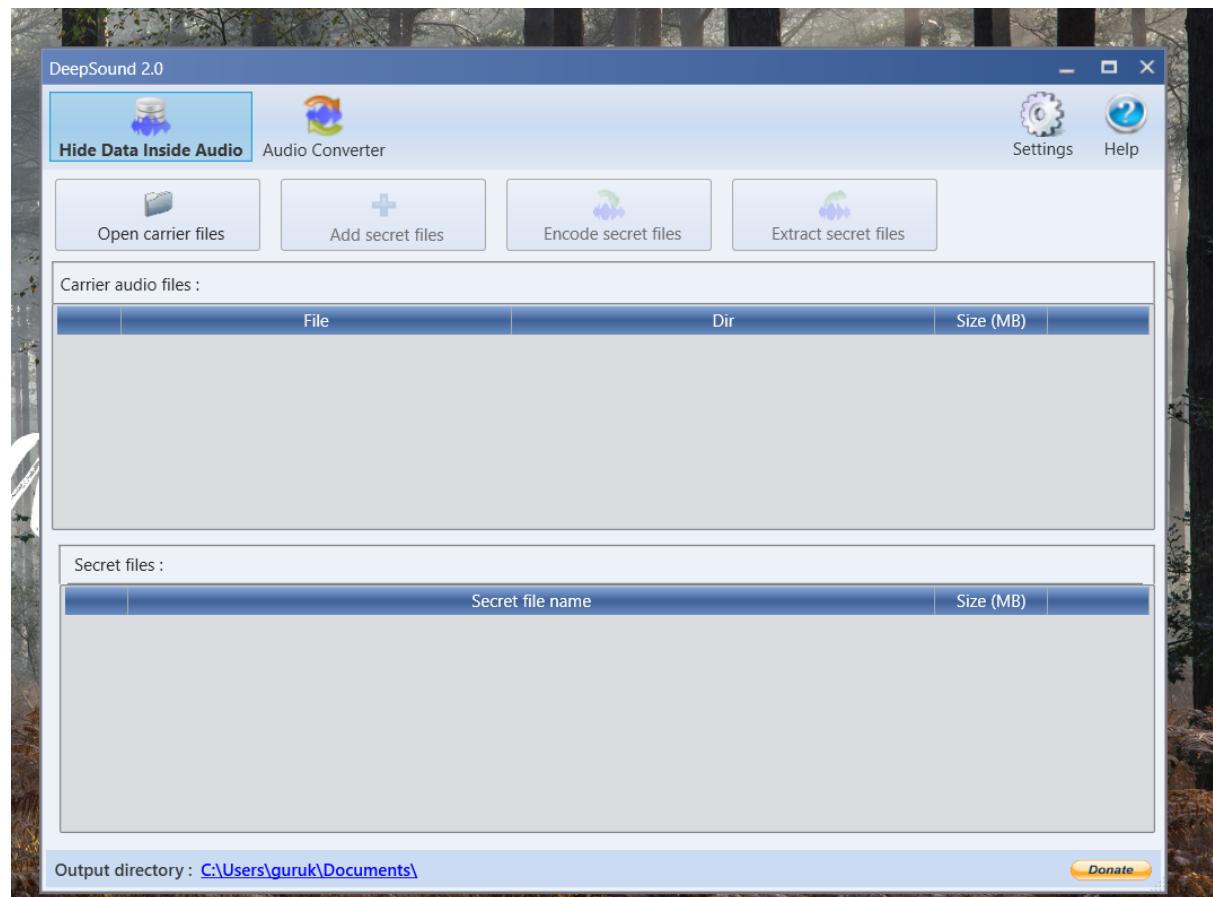


Figure 21: Install and launch the DeepSound tool to begin the steganography detection process.

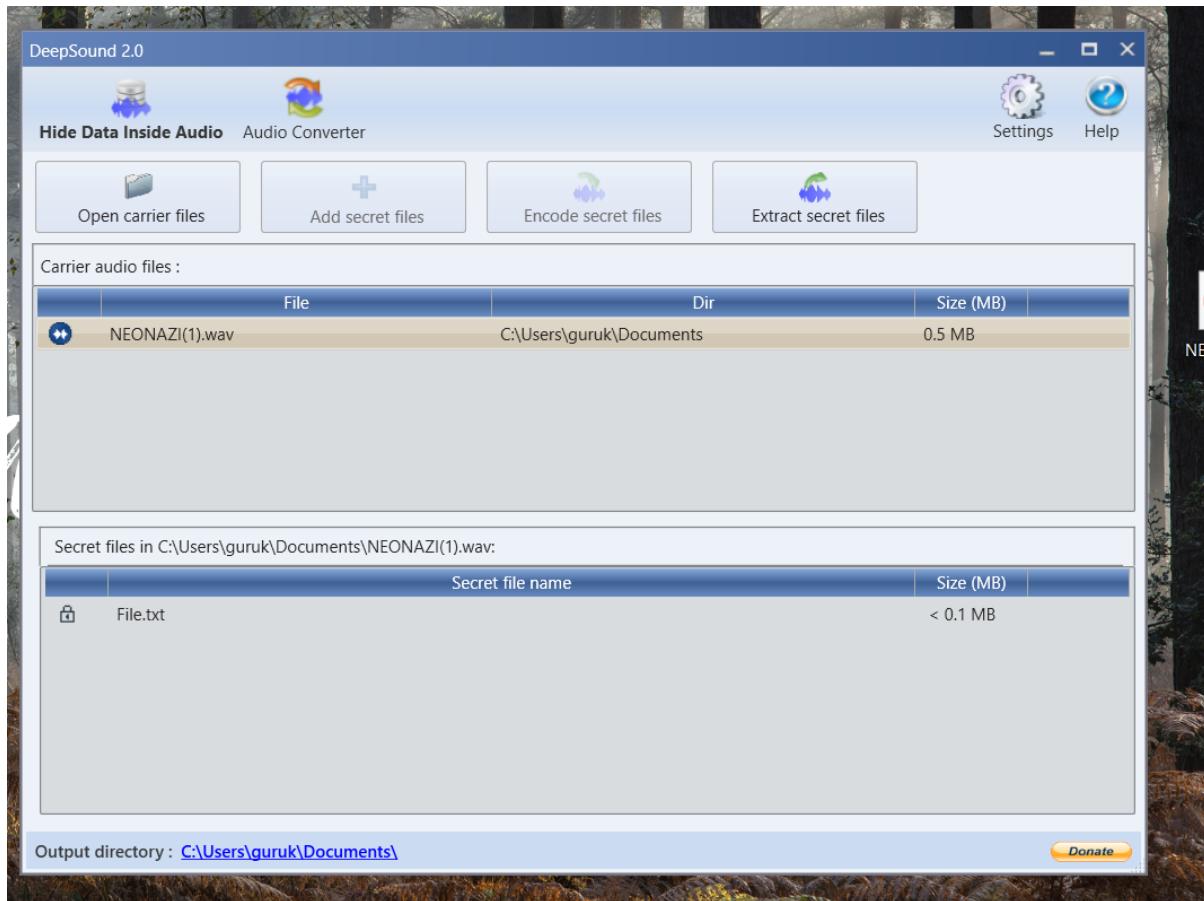


Figure 22: Click "Open carrier files" to add the steganography audio file for analysis.

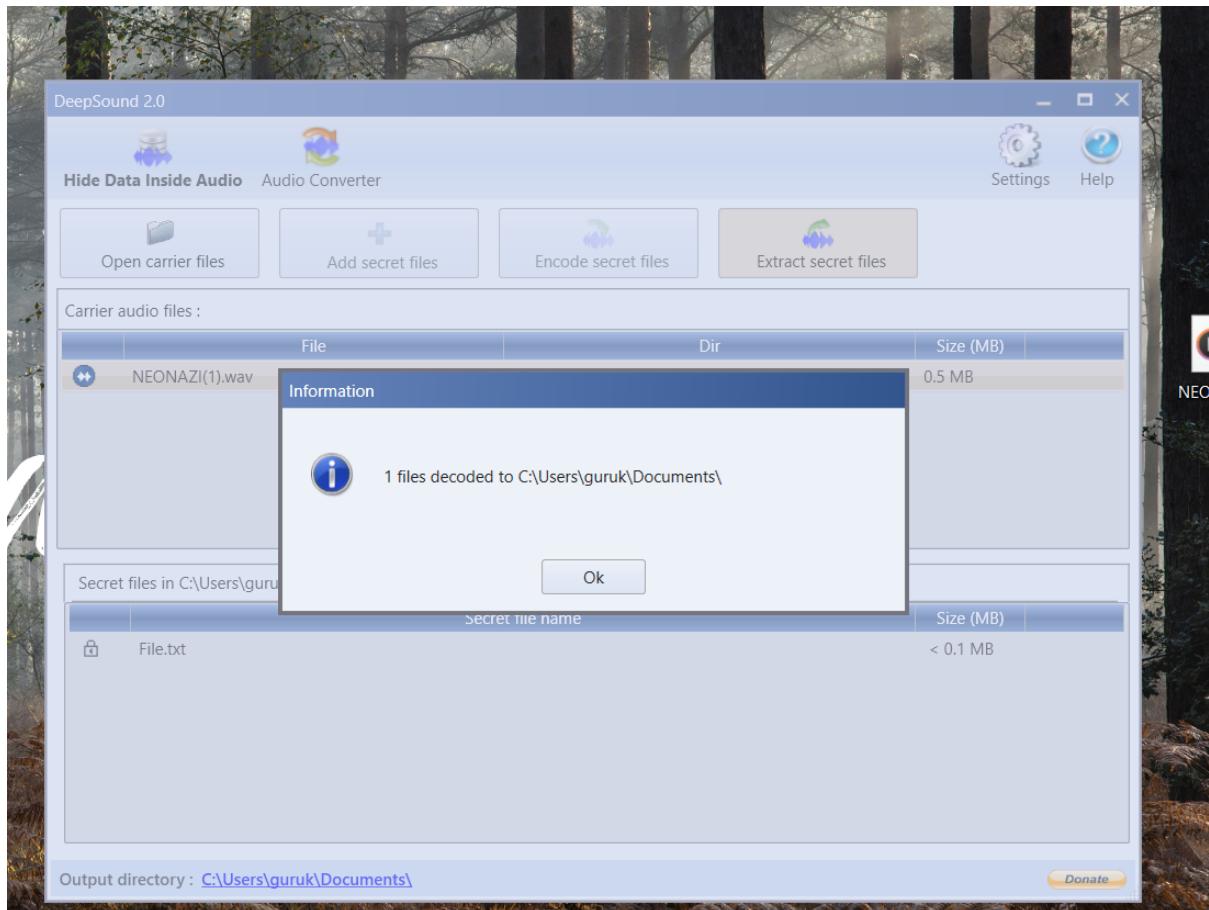


Figure 23: Successfully extracted the hidden data from the steganography audio file.