Defeating Anti-forensics Techniques

Module 05

Defeating Anti-forensics Techniques

Anti-forensics techniques are the techniques the perpetrators use to avert detection through forensics investigation process. These techniques hinder proper forensics investigation process by reducing the quantity and quality of digital evidence.

ICON KEY

🗀 Valuable information

✎ Test your knowledge

💻 Web exercise

📖 Workbook review

Lab Scenario

In order to investigate web attacks, as a **forensic investigator**, you must be able to collect and analyze evidences from victims' or attackers' system. The attackers try to avert the forensics processes by applying some anti-forensics techniques that damage the evidence, hide the pathways used and delete the attacked data from the victims' systems. You must be aware of such techniques and their impact over the evidences and systems.

Lab Objectives

The objective of this lab is to provide expert knowledge about:

- How to find anti-forensics techniques
- Bypass the anti-forensics attacks to collect the evidence

🗀 **Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 05 Defeating Anti-forensics Techniques**

Lab Environment

To carry out the lab, you need:

- A computer running **Windows 10** virtual machine
- A computer running **Windows Server 2012** virtual machine
- A web browser with an **Internet** connection
- Administrative privileges to run tools

Lab Duration

Time: 55 Minutes

Overview of Anti-forensics

There are different types of anti-forensics techniques such as data/file deletion, wiping/overwriting data and metadata, corruption / degaussing, cryptographic file systems, password protection, etc.

TASK 1

Overview

Lab Tasks

Recommended labs to assist you in Defeating Anti-forensics Techniques:

- Cracking Application Password
- Detecting Steganography

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab

1

Cracking Application Password

Passware Kit Forensic is an electronic evidence discovery solution that reports all password-protected items on a computer and decrypts them.

ICON KEY

🗁 Valuable information

✎ Test your knowledge

💻 Web exercise

🕮 Workbook review

Lab Scenario

Applications are a package of programs developed to perform certain tasks. The developers use encryptions and authentication to protect the data. Attackers also create such encrypted applications, which are difficult to see through. To be an expert **forensic investigator**, you must have the skills to crack system passwords, application passwords and other security mechanisms, which can act as hindrance in solving the case.

Lab Objectives

The objective of this lab is to help investigators:

- Crack the application passwords

Lab Environment

🗁 **Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 05 Defeating Anti-forensics Techniques**

To carry out the lab, you need:

- The Passware Kit Forensic tool, located at **C:\CHFI-Tools\CHFIv9 Module 05 Defeating Anti-forensics Techniques\Password Cracking Tools\Passware Kit Forensic**.
- You can also download the latest version of **Passware Kit Forensic** from this link **https://www.passware.com/kit-forensic**.
- If you decide to download the latest version, screenshots shown in the lab might differ.
- A computer running **Windows 10**.
- Administrative privileges to install and run tools.
- A web browser with an **Internet** connection.

Lab Duration

Time: 25 Minutes

Overview of Passware Kit Forensic

Passware Kit Forensic is an electronic evidence discovery solution that reports all password-protected items on a computer and decrypts them. It reports all password-protected items on a computer and gains access to these items using the fastest decryption and password recovery algorithms.

Lab Tasks

TASK 1

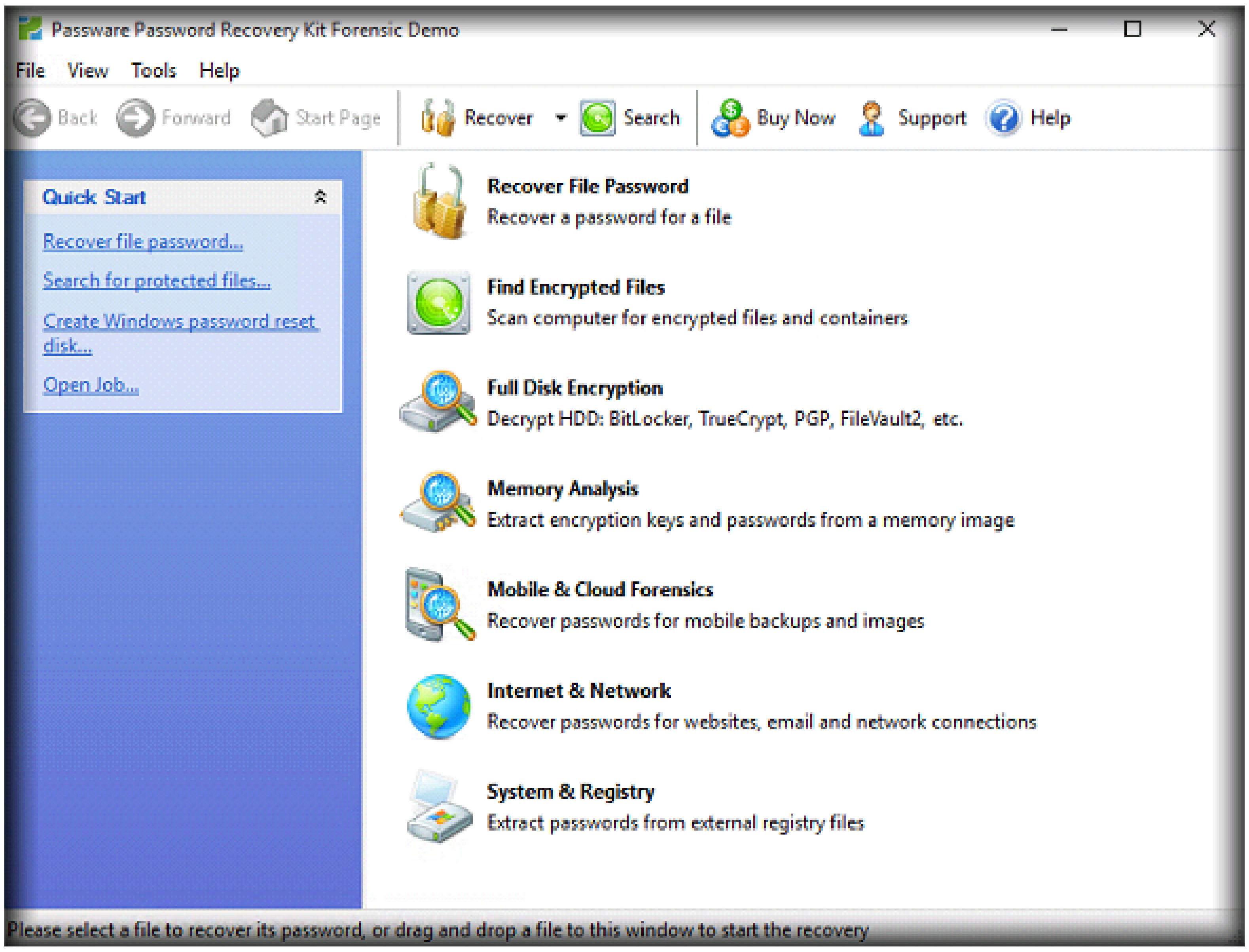
Launching and Updating Password Recovery Bundle

1. Navigate to **Z:\CHFIv9 Module 05 Defeating Anti-forensics Techniques\Password Cracking Tools\Passware Kit Forensic**.
2. Double-click **passware-kit-forensic-demo.msi** to launch the setup, and follow the wizard driven installation steps.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

If a **User Account Control** pop-up appears, enter the credentials of Windows Server 2012 virtual machine.

3. During the final step of installation, ensure that **Run Passware Kit Forensic Demo** option is checked, and click **Finish**.
4. Passware Password Recovery Kit Forensic Demo GUI appears as shown in the following screenshot:



Recover File Password
Recover a password for a file

Find Encrypted Files
Scan computer for encrypted files and containers

Full Disk Encryption
Decrypt HDD: BitLocker, TrueCrypt, PGP, FileVault2, etc.

Memory Analysis
Extract encryption keys and passwords from a memory image

Mobile & Cloud Forensics
Recover passwords for mobile backups and images

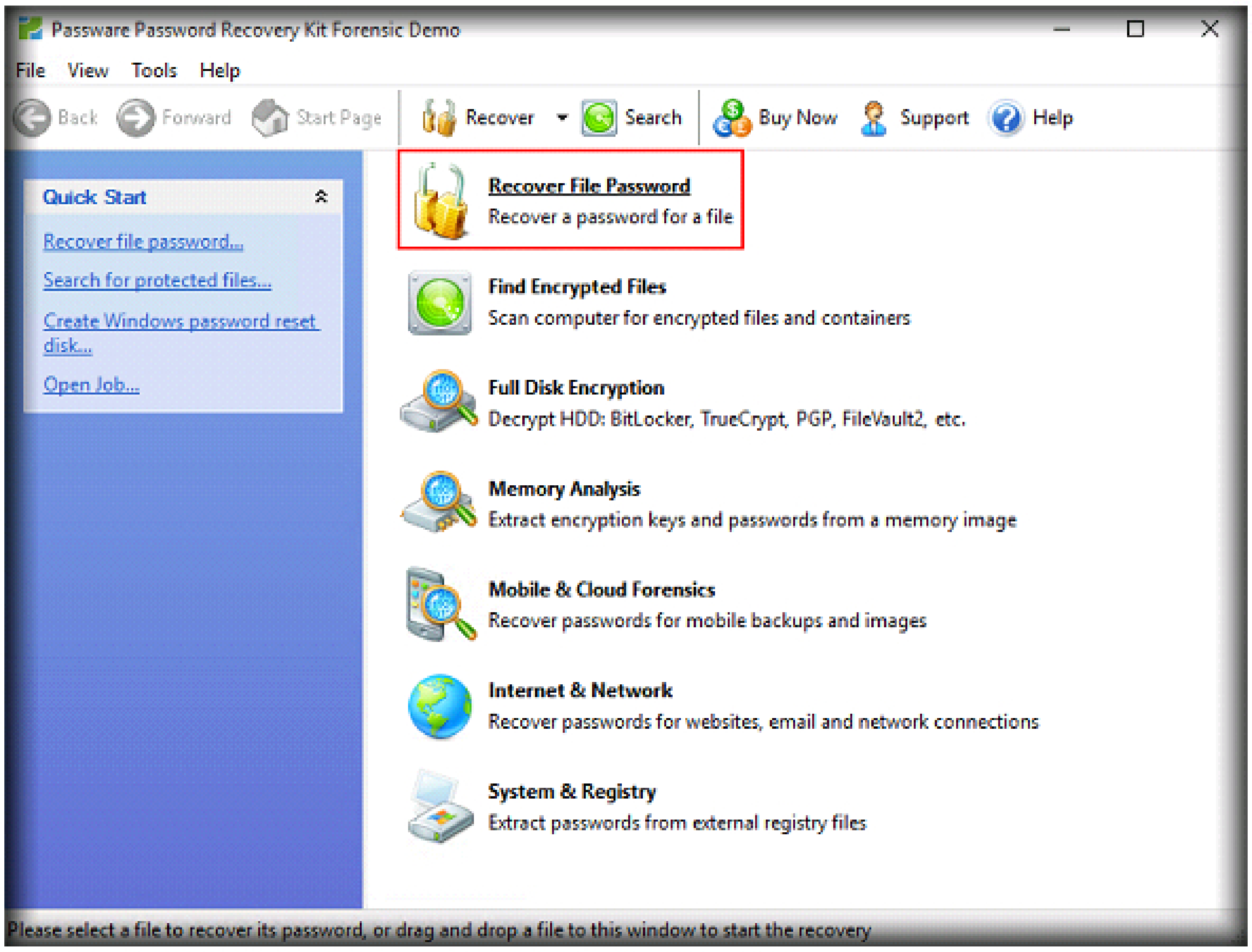
Internet & Network
Recover passwords for websites, email and network connections

System & Registry
Extract passwords from external registry files

Please select a file to recover its password, or drag and drop a file to this window to start the recovery

FIGURE 1.1: Passware Password Recovery Kit Forensic Demo GUI

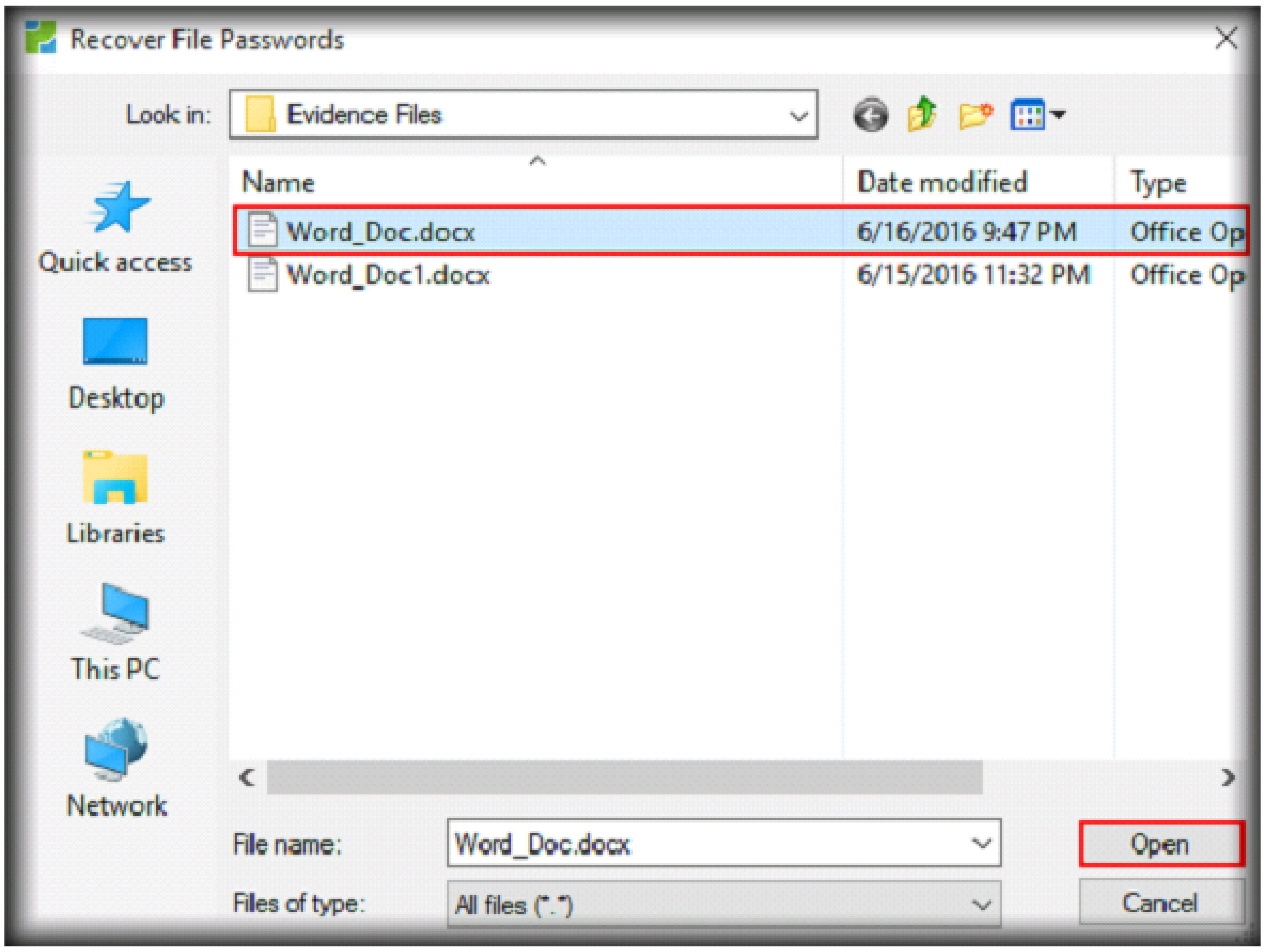
5. Click the **Recover File Password** option from the main window of the tool.


Passware Password Recovery Kit Forensic Demo
File
View
Tools
Help
Back
Forward
Start Page
Recover
Search
Buy Now
Support
Help
Quick Start
Recover file password...
Search for protected files...
Create Windows password reset disk...
Open Job...
Recover File Password
Recover a password for a file
Find Encrypted Files
Scan computer for encrypted files and containers
Full Disk Encryption
Decrypt HDD: BitLocker, TrueCrypt, PGP, FileVault2, etc.
Memory Analysis
Extract encryption keys and passwords from a memory image
Mobile & Cloud Forensics
Recover passwords for mobile backups and images
Internet & Network
Recover passwords for websites, email and network connections
System & Registry
Extract passwords from external registry files

Please select a file to recover its password, or drag and drop a file to this window to start the recovery

FIGURE 1.2: Recover File Password option

6. Navigate to the location **Z:\Evidence Files**, select the file **Word_Doc.docx** and click **Open**.



Look in: Evidence Files

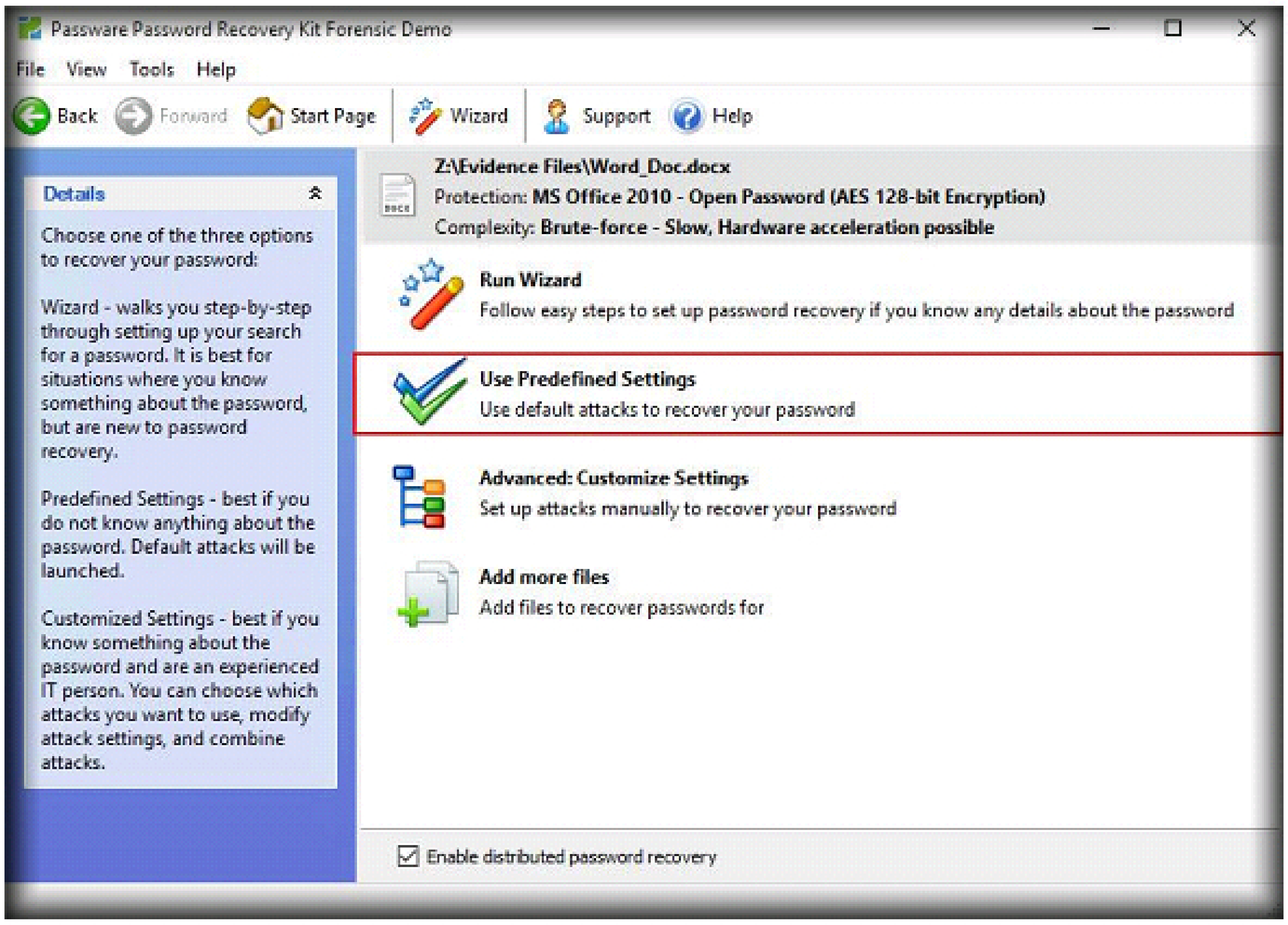
Name	Date modified	Type
Word_Doc.docx	6/16/2016 9:47 PM	Office Op
Word_Doc1.docx	6/15/2016 11:32 PM	Office Op

File name: Word_Doc.docx

Files of type: All files (*.*)

FIGURE 1.3: Open Word_Doc.docx

7. Upon selecting the file, a wizard appears where you need to select **Use Predefined Settings** option.


Passware Password Recovery Kit Forensic Demo
File View Tools Help
Back Forward Start Page Wizard Support Help
Details

Z:\Evidence Files\Word_Doc.docx
Protection: **MS Office 2010 - Open Password (AES 128-bit Encryption)**
Complexity: **Brute-force - Slow, Hardware acceleration possible**

Choose one of the three options to recover your password:

Wizard - walks you step-by-step through setting up your search for a password. It is best for situations where you know something about the password, but are new to password recovery.

Predefined Settings - best if you do not know anything about the password. Default attacks will be launched.

Customized Settings - best if you know something about the password and are an experienced IT person. You can choose which attacks you want to use, modify attack settings, and combine attacks.

Run Wizard
Follow easy steps to set up password recovery if you know any details about the password

Use Predefined Settings
Use default attacks to recover your password

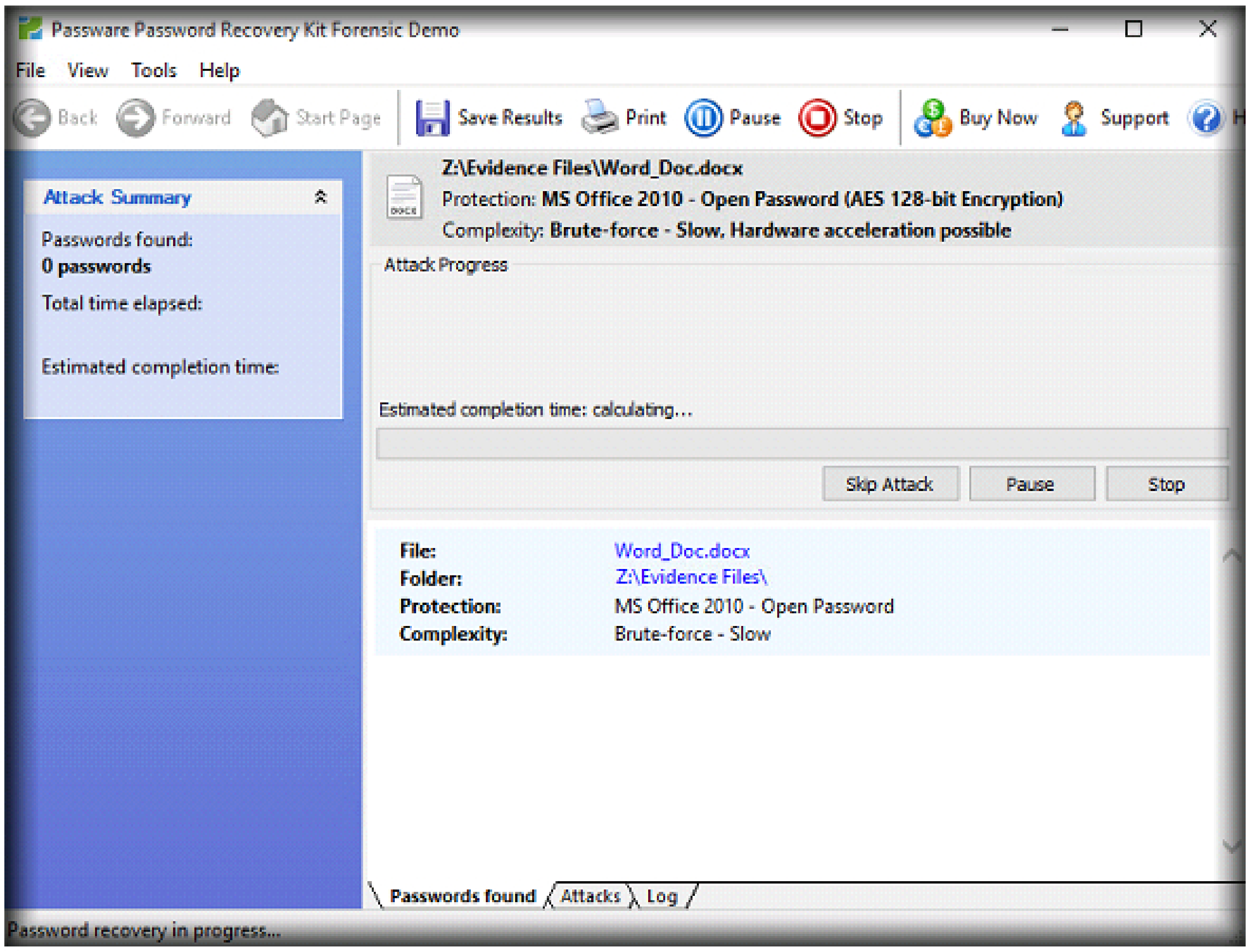
Advanced: Customize Settings
Set up attacks manually to recover your password

Add more files
Add files to recover passwords for

☑ Enable distributed password recovery

FIGURE 1.4: Use Predefined Settings option

8. The tool will take some time to crack the password. The time is proportionate to the number of characters the password has, as well as types of characters used.


Passware Password Recovery Kit Forensic Demo
File View Tools Help
Back Forward Start Page Save Results Print Pause Stop Buy Now Support H
Attack Summary
Attack Progress
Skip Attack
Pause
Stop
Passwords found
Attacks
Log

Z:\Evidence Files\Word_Doc.docx
Protection: **MS Office 2010 - Open Password (AES 128-bit Encryption)**
Complexity: **Brute-force - Slow, Hardware acceleration possible**

Passwords found:
0 passwords
Total time elapsed:
Estimated completion time:

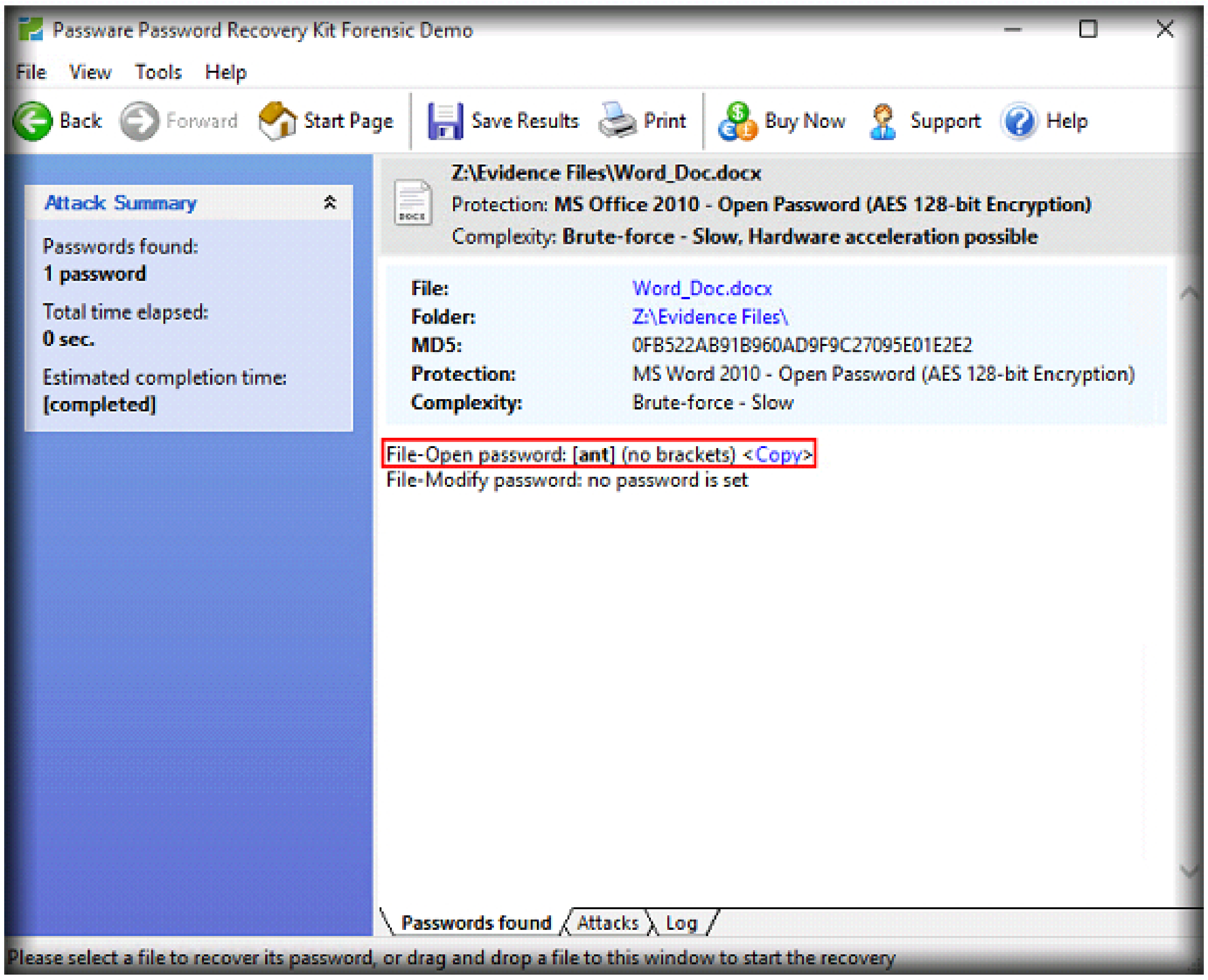
Estimated completion time: calculating...

File:	Word_Doc.docx
Folder:	Z:\Evidence Files\
Protection:	MS Office 2010 - Open Password
Complexity:	Brute-force - Slow

Password recovery in progress...

FIGURE 1.5: Password cracking screen

9. After analysis, the tool displays the password as shown in the screenshot:


Passware Password Recovery Kit Forensic Demo
File View Tools Help
Back Forward Start Page Save Results Print Buy Now Support Help
Attack Summary
Passwords found Attacks Log

Z:\Evidence Files\Word_Doc.docx
Protection: **MS Office 2010 - Open Password (AES 128-bit Encryption)**
Complexity: **Brute-force - Slow, Hardware acceleration possible**

Passwords found:
1 password
Total time elapsed:
0 sec.
Estimated completion time:
[completed]

File:	Word_Doc.docx
Folder:	Z:\Evidence Files\
MD5:	0FB522AB91B960AD9F9C27095E01E2E2
Protection:	MS Word 2010 - Open Password (AES 128-bit Encryption)
Complexity:	Brute-force - Slow

File-Open password: **[ant]** (no brackets) <Copy>
File-Modify password: no password is set

Please select a file to recover its password, or drag and drop a file to this window to start the recovery

FIGURE 1.6: Password display

10. To crack password of a compressed folder or winRAR file, navigate to the **Z:\CHFIv9 Module 05 Defeating Anti-forensics Techniques\Password Cracking Tools\Advanced Archive Password Recovery**, and double click the **archpr_setup_en.msi** setup file.

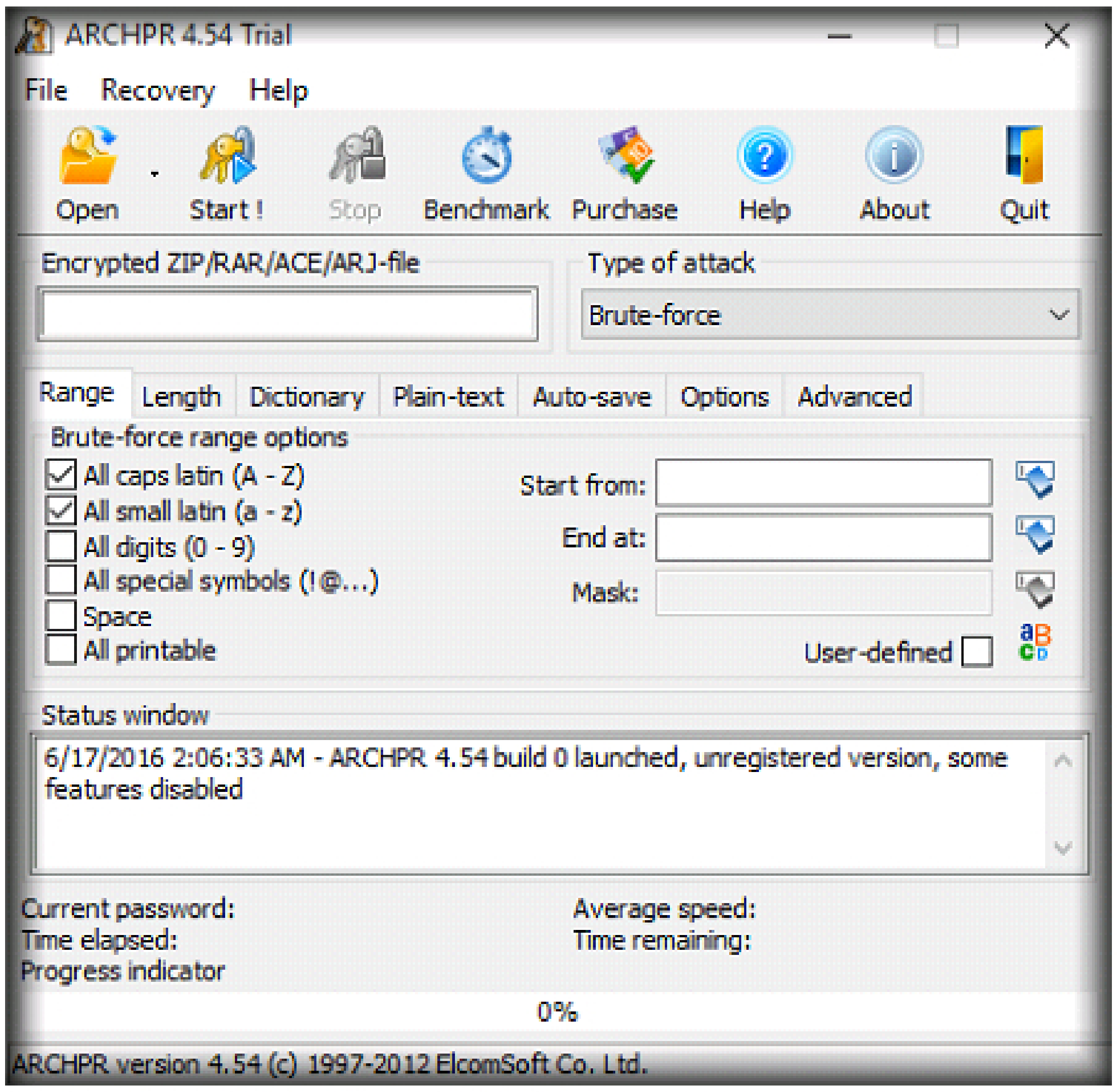
11. Follow the installation instructions to install the tool.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

If a **User Account Control** pop-up appears, enter the credentials of Windows Server 2012 virtual machine.

12. During the final step of installation, ensure that **Run Advanced Archive Password Recovery** is checked, and click **Finish**.

13. **Advanced Archive Password Recovery** GUI appears as shown in the following screenshot:



Encrypted ZIP/RAR/ACE/ARJ-file

Type of attack: Brute-force

Brute-force range options
☑ All caps latin (A - Z)
☑ All small latin (a - z)
☐ All digits (0 - 9)
☐ All special symbols (!@...)
☐ Space
☐ All printable

Start from:
End at:
Mask:
User-defined ☐

Status window

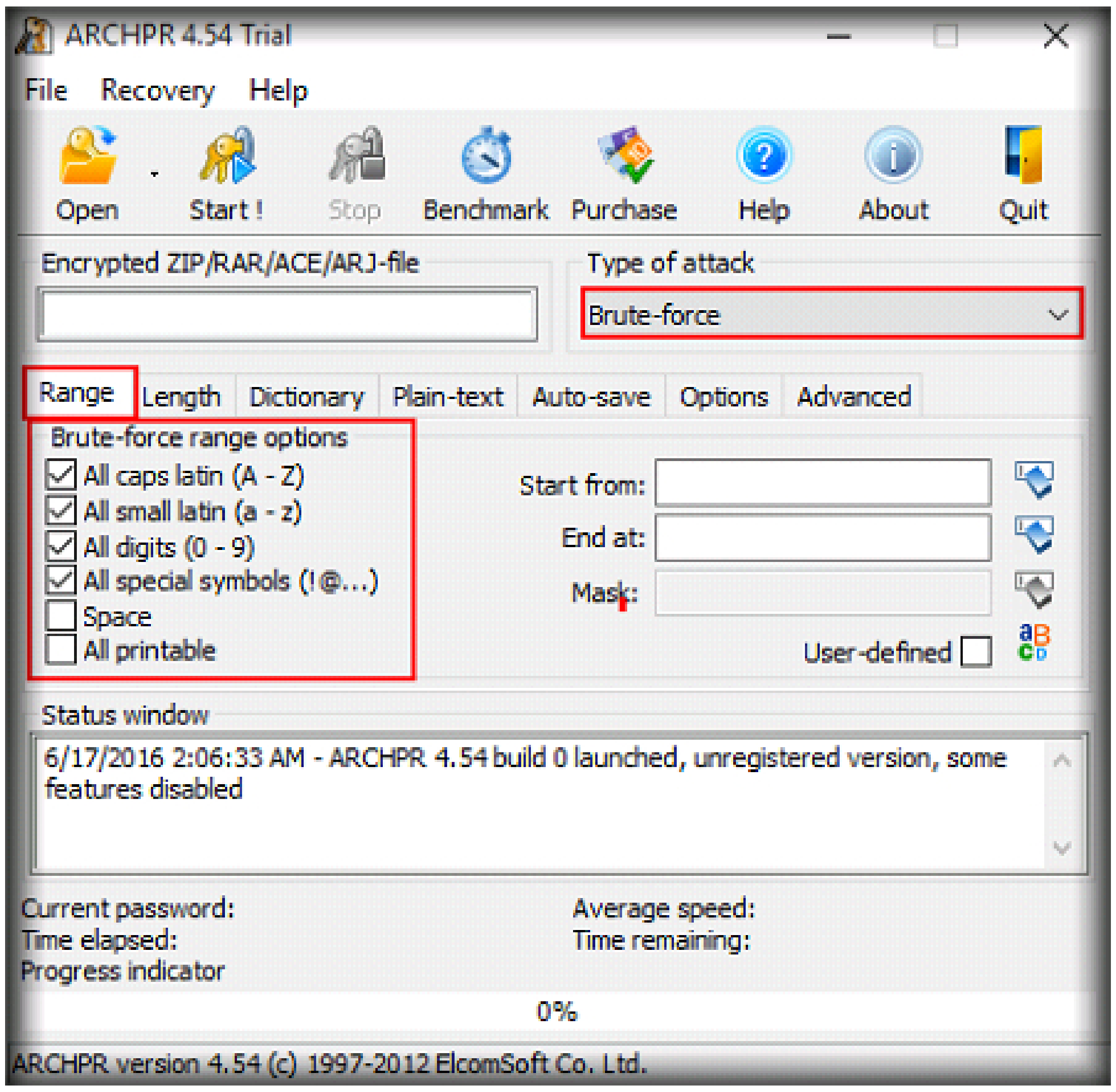
6/17/2016 2:06:33 AM - ARCHPR 4.54 build 0 launched, unregistered version, some features disabled

Current password:
Time elapsed:
Progress indicator
Average speed:
Time remaining:
0%

ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

FIGURE 1.7: Advanced Archive Password Recovery GUI

14. Provide the cracking factors by providing parameters such as the **Type of attack**, **Range**, **length**, **Dictionary**, etc., by clicking the respective tabs and giving in the required details.



Encrypted ZIP/RAR/ACE/ARJ-file

Type of attack: Brute-force

Brute-force range options
☑ All caps latin (A - Z)
☑ All small latin (a - z)
☑ All digits (0 - 9)
☑ All special symbols (!@...)
☐ Space
☐ All printable

Start from:
End at:
Mask:
User-defined ☐

Status window

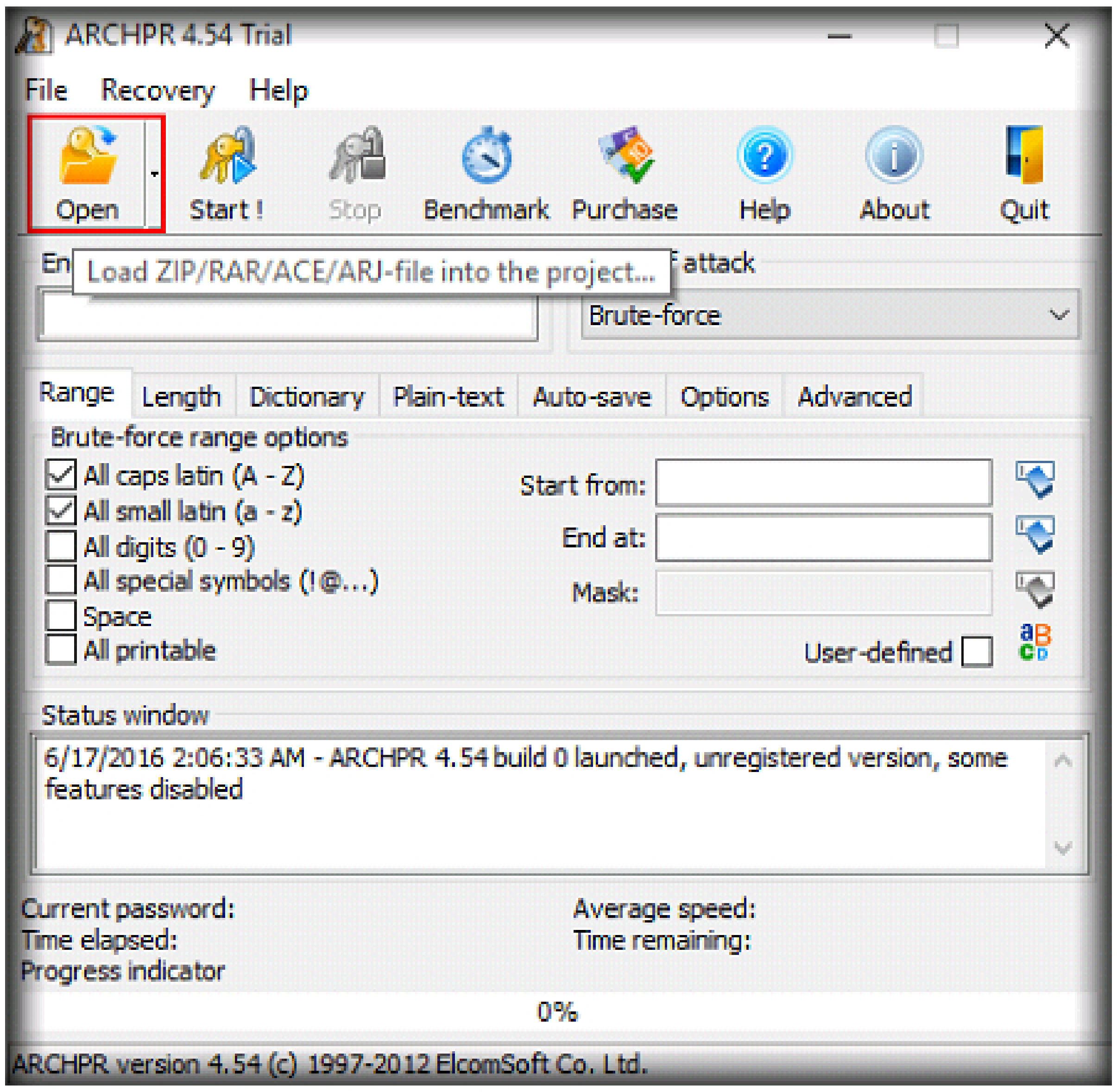
6/17/2016 2:06:33 AM - ARCHPR 4.54 build 0 launched, unregistered version, some features disabled

Current password:
Time elapsed:
Progress indicator
Average speed:
Time remaining:
0%

ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

FIGURE 1.8: Provide parameters

15. Click the **Open** button from the toolbar of the main page to add the WinRAR file you want to crack.



Type of attack: Brute-force

Brute-force range options

☑ All caps latin (A - Z)
☑ All small latin (a - z)
☐ All digits (0 - 9)
☐ All special symbols (!@...)
☐ Space
☐ All printable

Start from:
End at:
Mask:
User-defined ☐

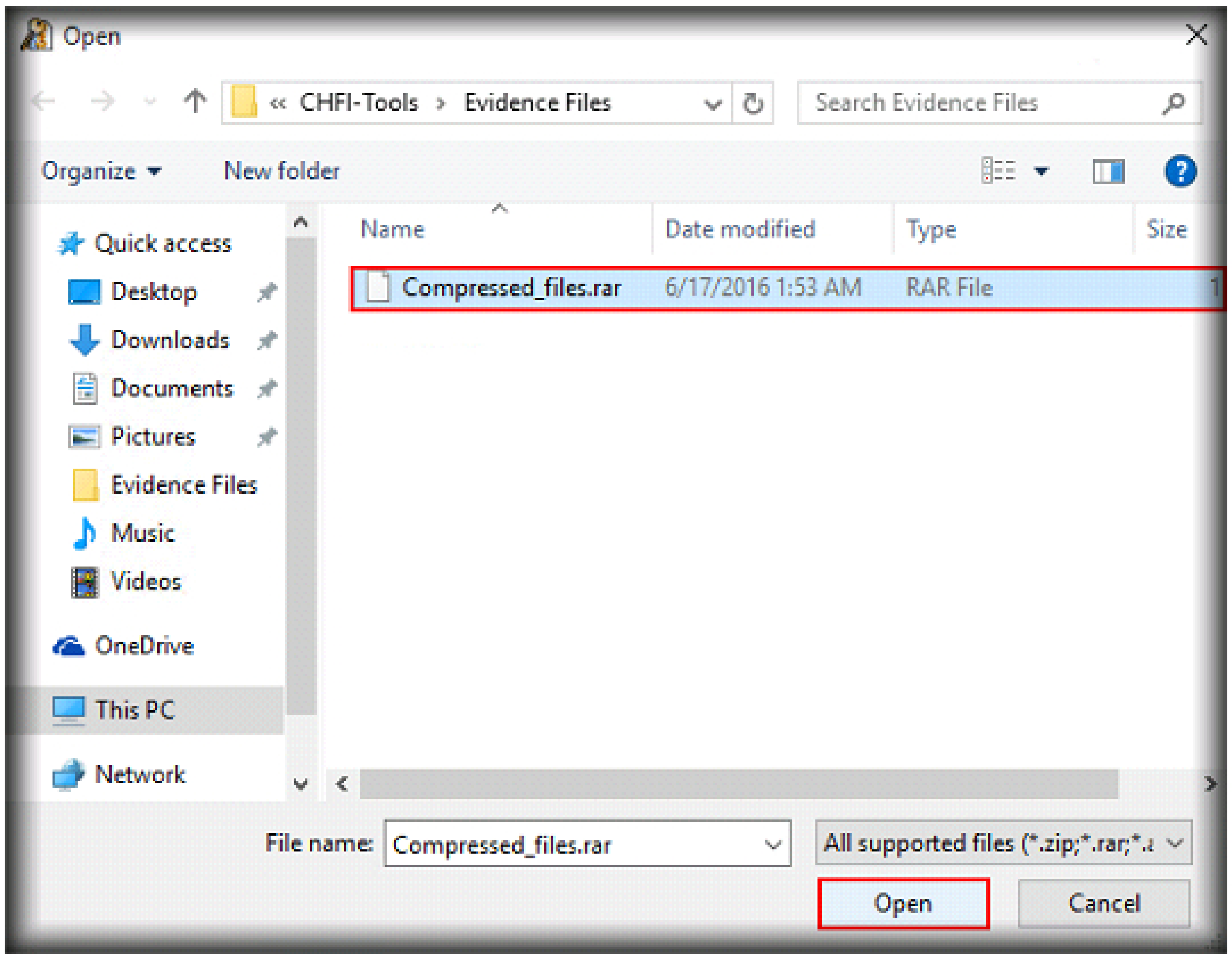
6/17/2016 2:06:33 AM - ARCHPR 4.54 build 0 launched, unregistered version, some features disabled

0%

ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

FIGURE 1.9: Click the Open button

16. Navigate to the file location **Z:\Evidence Files**, select the file **Compressed_files.rar** and click **Open**.



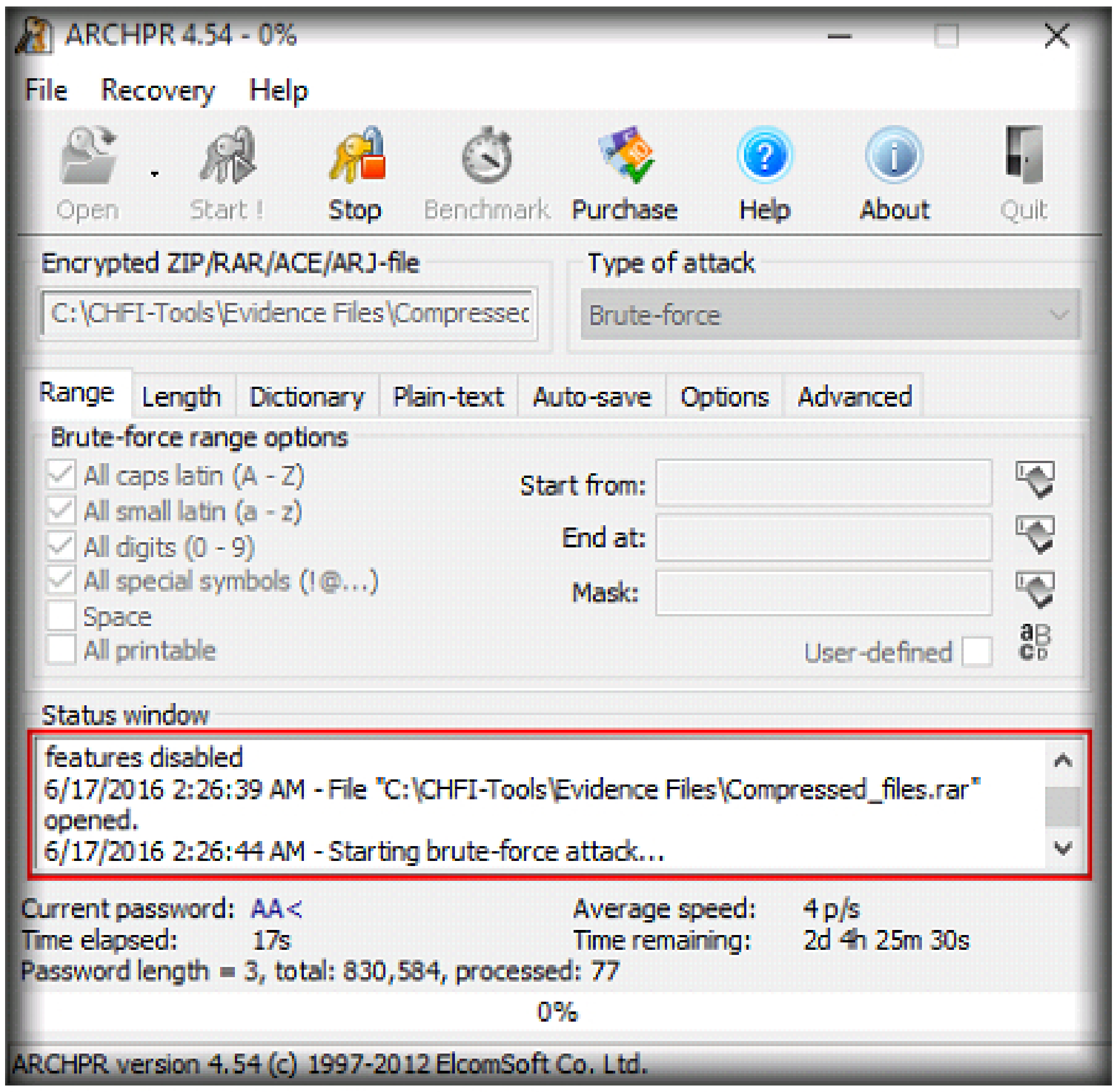
Name	Date modified	Type	Size
Compressed_files.rar	6/17/2016 1:53 AM	RAR File	

File name: Compressed_files.rar

All supported files (*.zip;*.rar;*.a

FIGURE 1.10: Select Compressed_files.rar

17. The tool will start cracking the password automatically and display the process status in the provided status window.



Encrypted ZIP/RAR/ACE/ARJ-file: C:\CHFI-Tools\Evidence Files\Compressec

Type of attack: Brute-force

Brute-force range options

☑ All caps latin (A - Z)
☑ All small latin (a - z)
☑ All digits (0 - 9)
☑ All special symbols (!@...)
□ Space
□ All printable

Start from:
End at:
Mask:
User-defined □

Status window

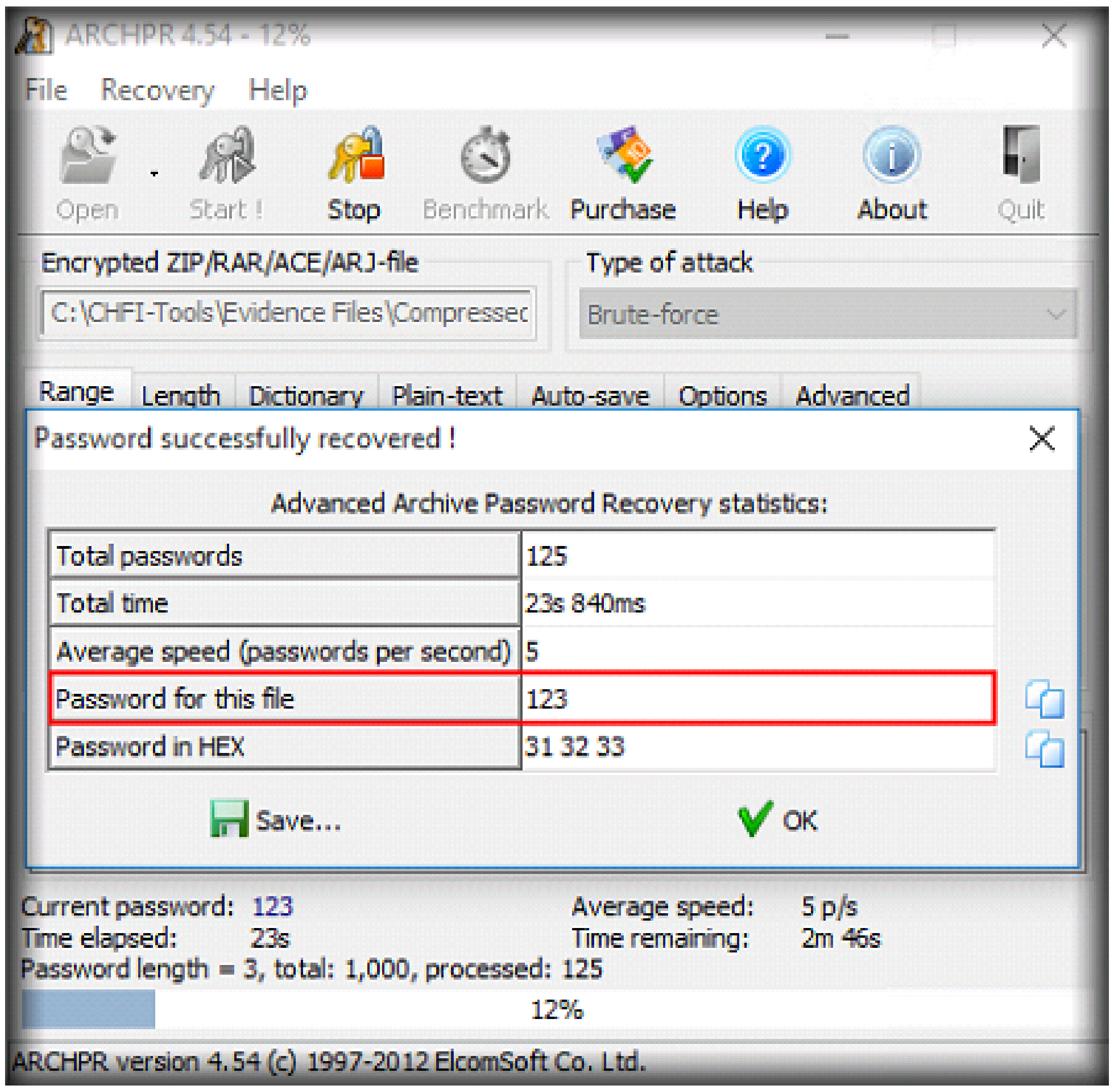
```
features disabled
6/17/2016 2:26:39 AM - File "C:\CHFI-Tools\Evidence Files\Compressed_files.rar"
opened.
6/17/2016 2:26:44 AM - Starting brute-force attack...
```

```
Current password:  AA<          Average speed:    4 p/s
Time elapsed:      17s          Time remaining:   2d 4h 25m 30s
Password length = 3, total: 830,584, processed: 77
0%
```

ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

FIGURE 1.11: Process status display

18. After completion of cracking, the tool will display the **password** with details regarding the scan as shown in the screenshot:



Encrypted ZIP/RAR/ACE/ARJ-file: C:\CHFI-Tools\Evidence Files\Compressec

Type of attack: Brute-force

Password successfully recovered !

Advanced Archive Password Recovery statistics:

Total passwords	125
Total time	23s 840ms
Average speed (passwords per second)	5
Password for this file	123
Password in HEX	31 32 33

```
Current password:  123          Average speed:    5 p/s
Time elapsed:      23s          Time remaining:   2m 46s
Password length = 3, total: 1,000, processed: 125
12%
```

ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

FIGURE 1.12: Password display

19. To crack password of a password-protected PDF file, navigate to the **Z:\CHFIv9 Module 05 Defeating Anti-forensics Techniques\Password Cracking Tools\Advanced PDF Password Recovery**.

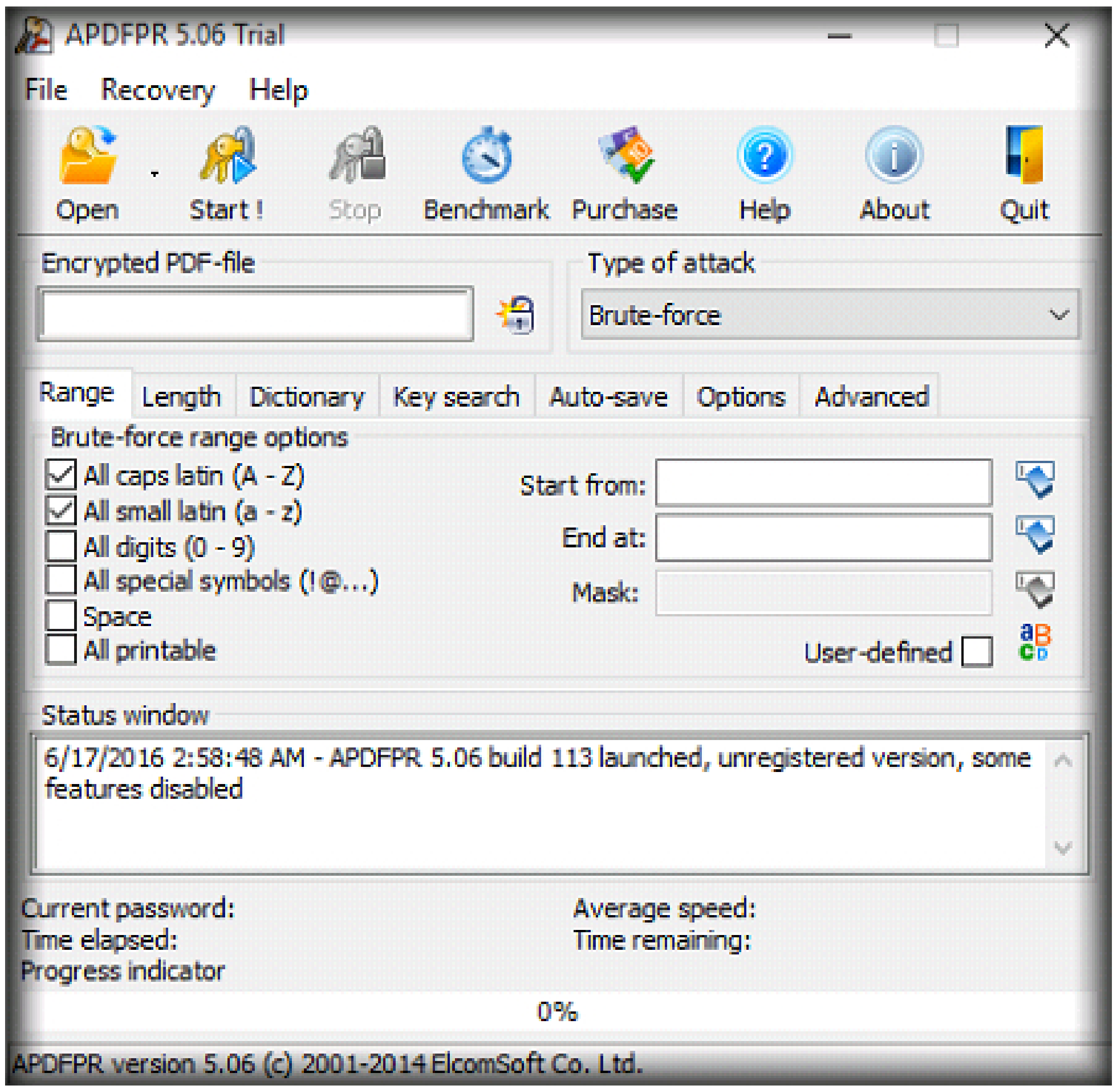
20. Double click the **apdfpr_setup_en.msi** setup file and follow the installation instructions to install the tool.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

If a **User Account Control** pop-up appears, enter the credentials of Windows Server 2012 virtual machine.

21. During the final step of installation, ensure that **Run Advanced PDF Password Recovery** is checked, and click **Finish**.

22. **Advanced PDF Password Recovery** GUI appears as shown in the following screenshot:



Encrypted PDF-file:

Type of attack: Brute-force

Brute-force range options

☑ All caps latin (A - Z)
☑ All small latin (a - z)
☐ All digits (0 - 9)
☐ All special symbols (!@...)
☐ Space
☐ All printable

Start from:
End at:
Mask:
User-defined ☐

Status window

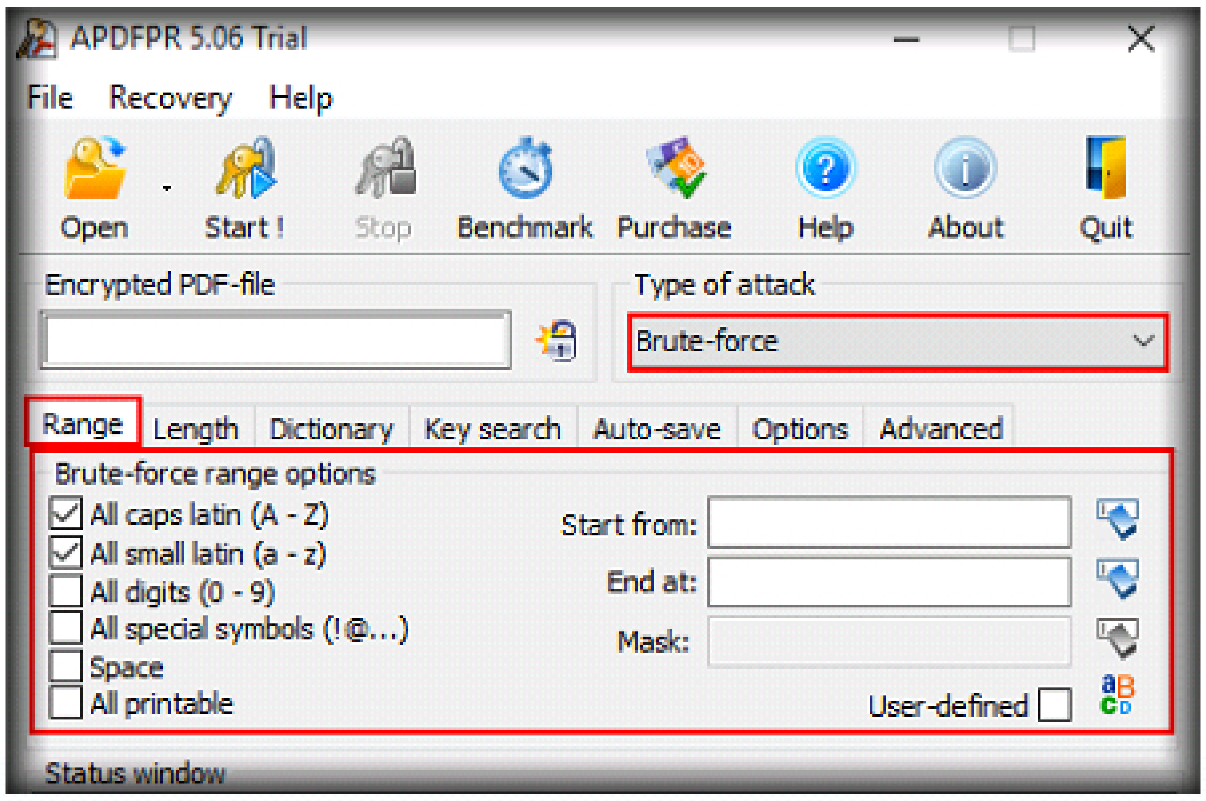
6/17/2016 2:58:48 AM - APDFPR 5.06 build 113 launched, unregistered version, some features disabled

Current password:
Time elapsed:
Progress indicator
Average speed:
Time remaining:
0%

APDFPR version 5.06 (c) 2001-2014 ElcomSoft Co. Ltd.

FIGURE 1.13: Advanced PDF Password Recovery GUI

23. Provide the cracking factors by providing parameters such as the **Type of attack**, **Range**, **length**, **Dictionary**, etc., by clicking the respective tabs and giving in the required details.



Encrypted PDF-file:

Type of attack: Brute-force

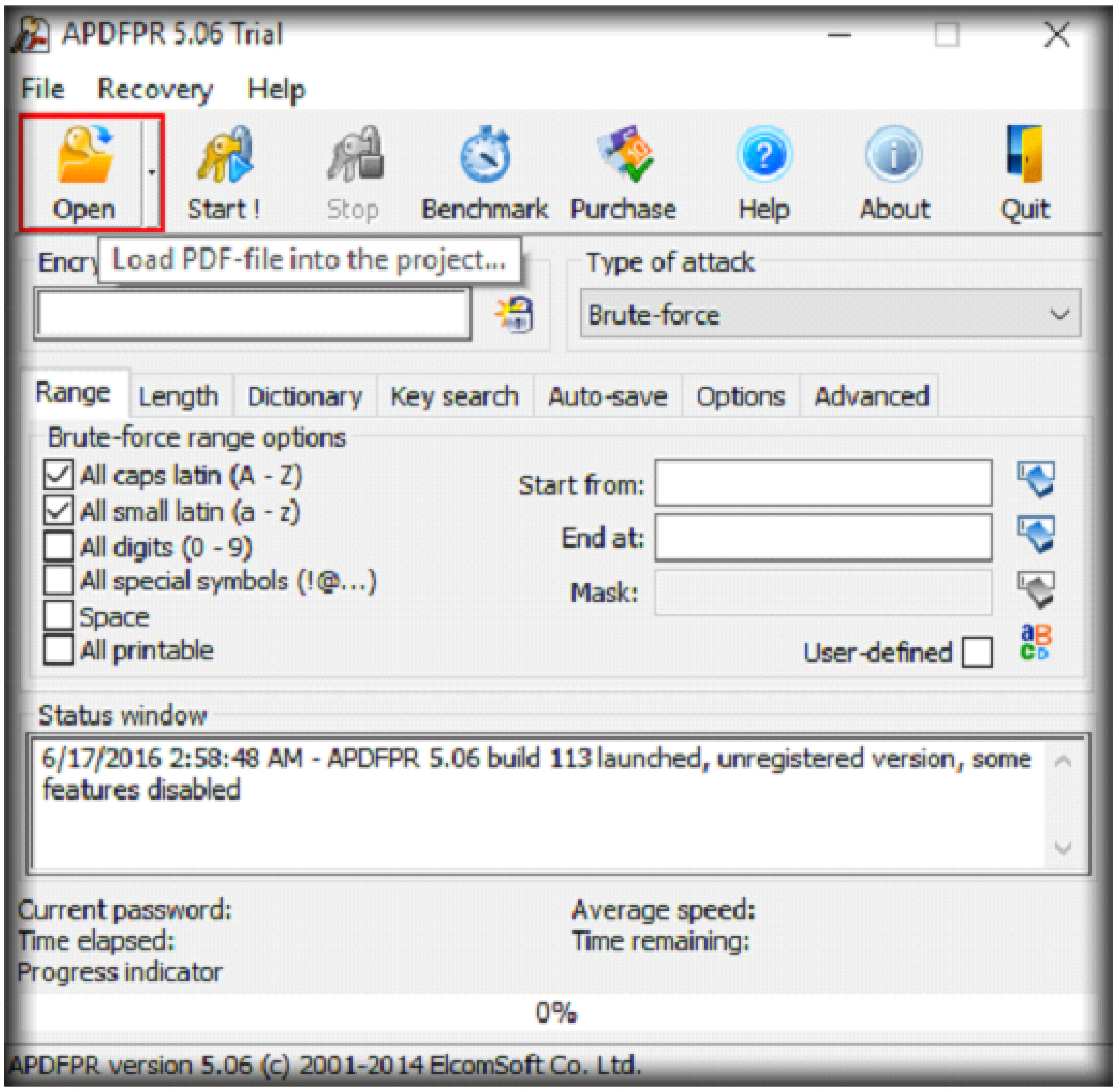
Brute-force range options

☑ All caps latin (A - Z)
☑ All small latin (a - z)
☐ All digits (0 - 9)
☐ All special symbols (!@...)
☐ Space
☐ All printable

Start from:
End at:
Mask:
User-defined ☐

FIGURE 1.14: Provide parameters

24. Click the **Open** button from the toolbar of the main page to add the PDF file you want to crack.



Type of attack: Brute-force

☑ All caps latin (A - Z)
☑ All small latin (a - z)
□ All digits (0 - 9)
□ All special symbols (!@...)
□ Space
□ All printable

Start from:
End at:
Mask:
User-defined □

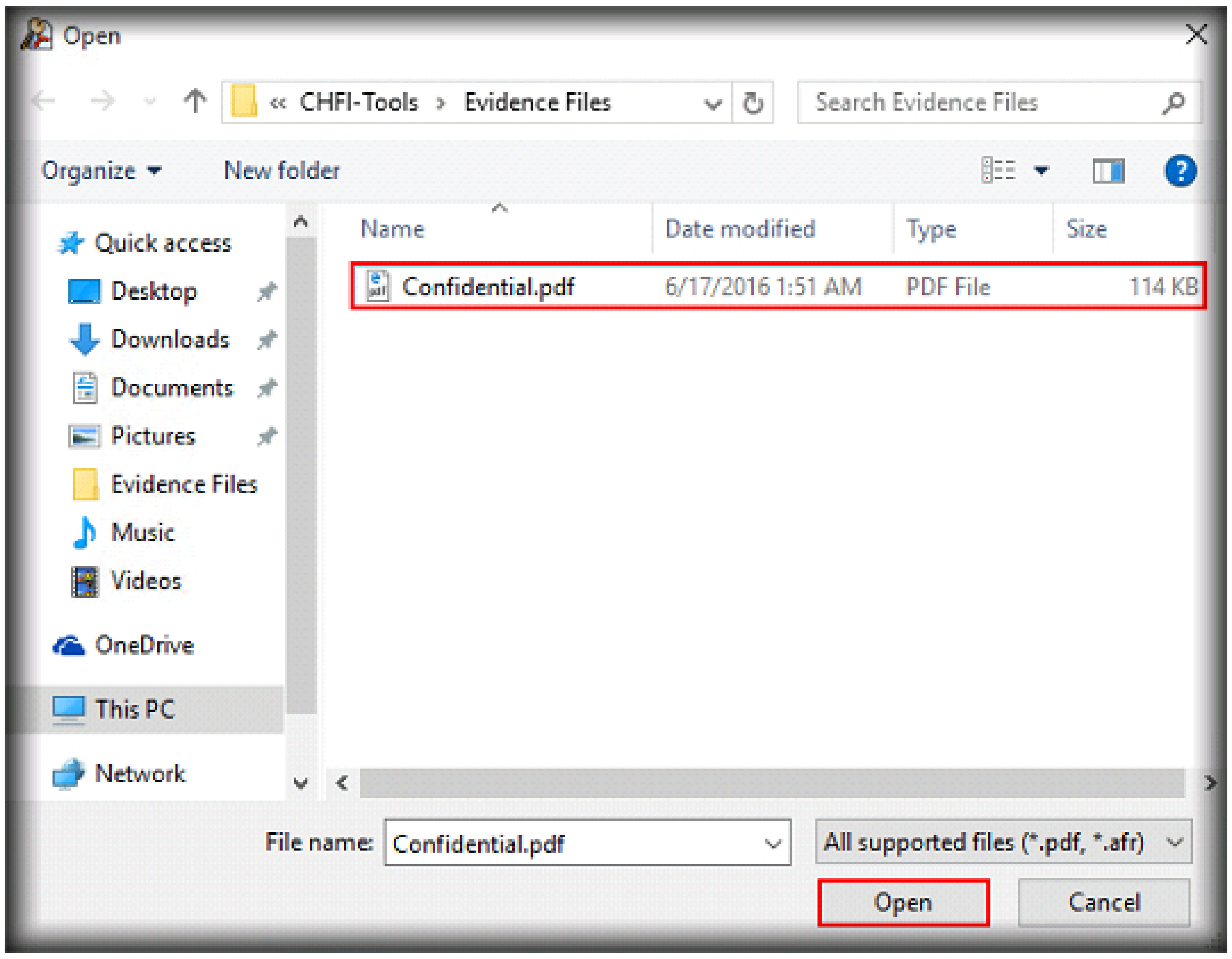
6/17/2016 2:58:48 AM - APDFPR 5.06 build 113 launched, unregistered version, some features disabled

Current password:
Time elapsed:
Progress indicator
Average speed:
Time remaining:
0%

APDFPR version 5.06 (c) 2001-2014 ElcomSoft Co. Ltd.

FIGURE 1.15: Click the Open button

25. Navigate to the file location **Z:\Evidence Files**, select the file **Confidential.pdf** and click **Open**.



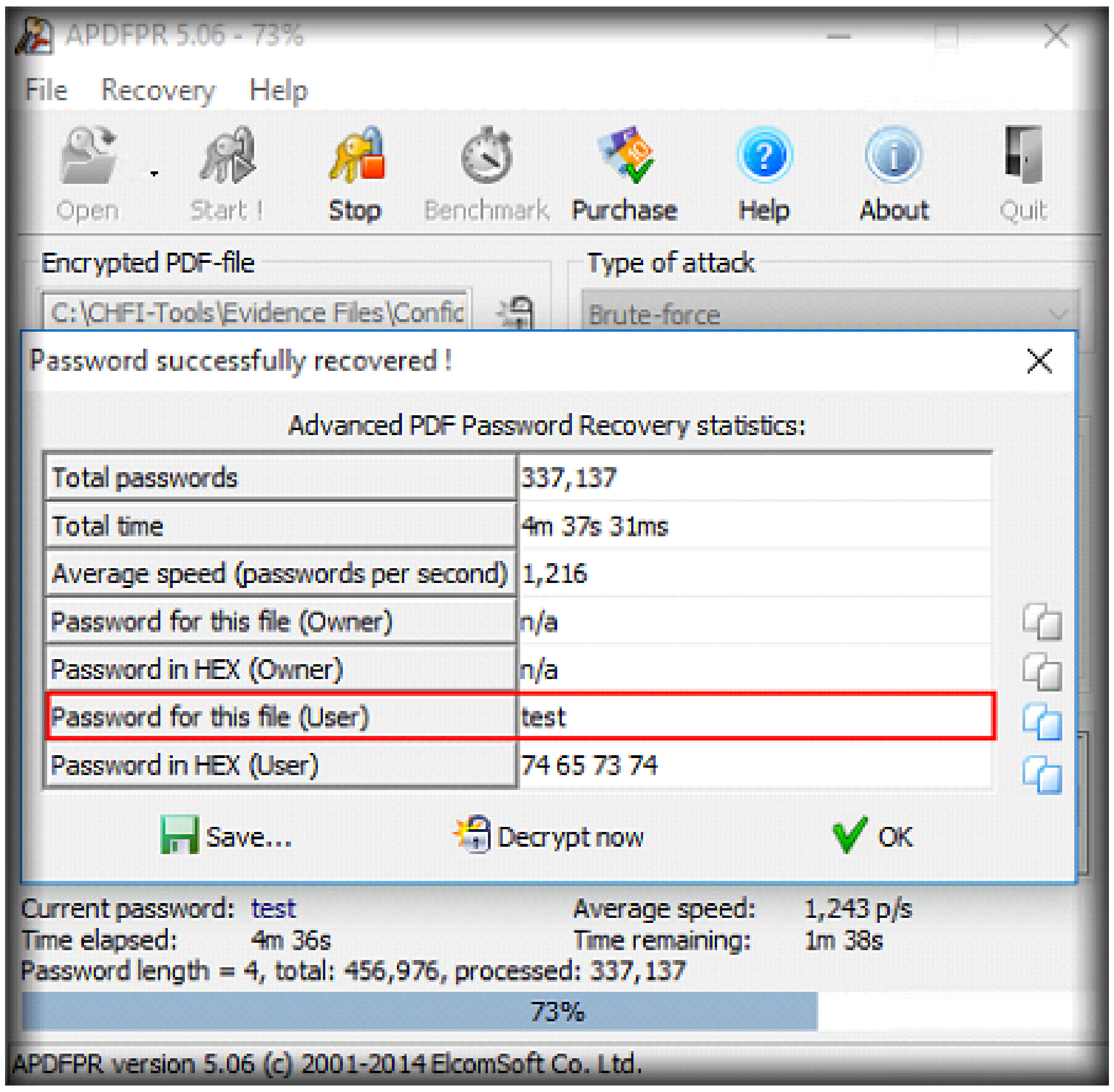
Name	Date modified	Type	Size
Confidential.pdf	6/17/2016 1:51 AM	PDF File	114 KB

File name: Confidential.pdf
All supported files (*.pdf, *.afr)

FIGURE 1.16: Select Confidential.pdf

26. The tool will start cracking the file password automatically.

27. **Note**: If the tool displays a message to enter the password, click the **Cancel** button and click **Start** on the tool page.



Encrypted PDF-file: C:\CHFI-Tools\Evidence Files\Confic

Type of attack: Brute-force

Password successfully recovered !

Advanced PDF Password Recovery statistics:

Total passwords	337,137
Total time	4m 37s 31ms
Average speed (passwords per second)	1,216
Password for this file (Owner)	n/a
Password in HEX (Owner)	n/a
Password for this file (User)	test
Password in HEX (User)	74 65 73 74

```
Current password:  test              Average speed:     1,243 p/s
Time elapsed:      4m 36s            Time remaining:    1m 38s
Password length = 4, total: 456,976, processed: 337,137
73%
APDFPR version 5.06 (c) 2001-2014 ElcomSoft Co. Ltd.
```

FIGURE 1.17: Crack file password

28. After analysis the tool will display a window with the password of the **Confidential.pdf** file.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
□ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

2

Detecting Steganography

Steganography is the process of hiding information or file with another file. In other words, it is the process of disguising a harmful file as a safe file.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

The attackers sometime try to deceive the users and the system security by hiding the malicious program with an apparently useful image or file. By doing this they can avert the security check and lure the victims to download and run the malware as well as escape from forensic identification. As an expert **forensic investigator**, you must be able to detect the steganography files and analyze them.

Lab Objectives

The objective of this lab is to help investigators analyze files hidden using steganography and find their impact on the system or network.

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 05 Defeating Anti-forensics Techniques

Lab Environment

To carry out the lab, you need:

- Stegspy, located at **C:\CHFI-Tools\CHFIv9 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\StegSpy**.
- OpenStego, located at **C:\CHFI-Tools\CHFIv9 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\OpenStego**.
- A computer running **Windows Server 2012**.
- Administrative privileges to run the tools.

Lab Duration

Time: 30 Minutes

Overview of StegSpy

StegSpy allows identification of hidden file and the program used to hide the message as well as the location of the hidden content. **StegSpy** currently identifies the use of steganography techniques such as:

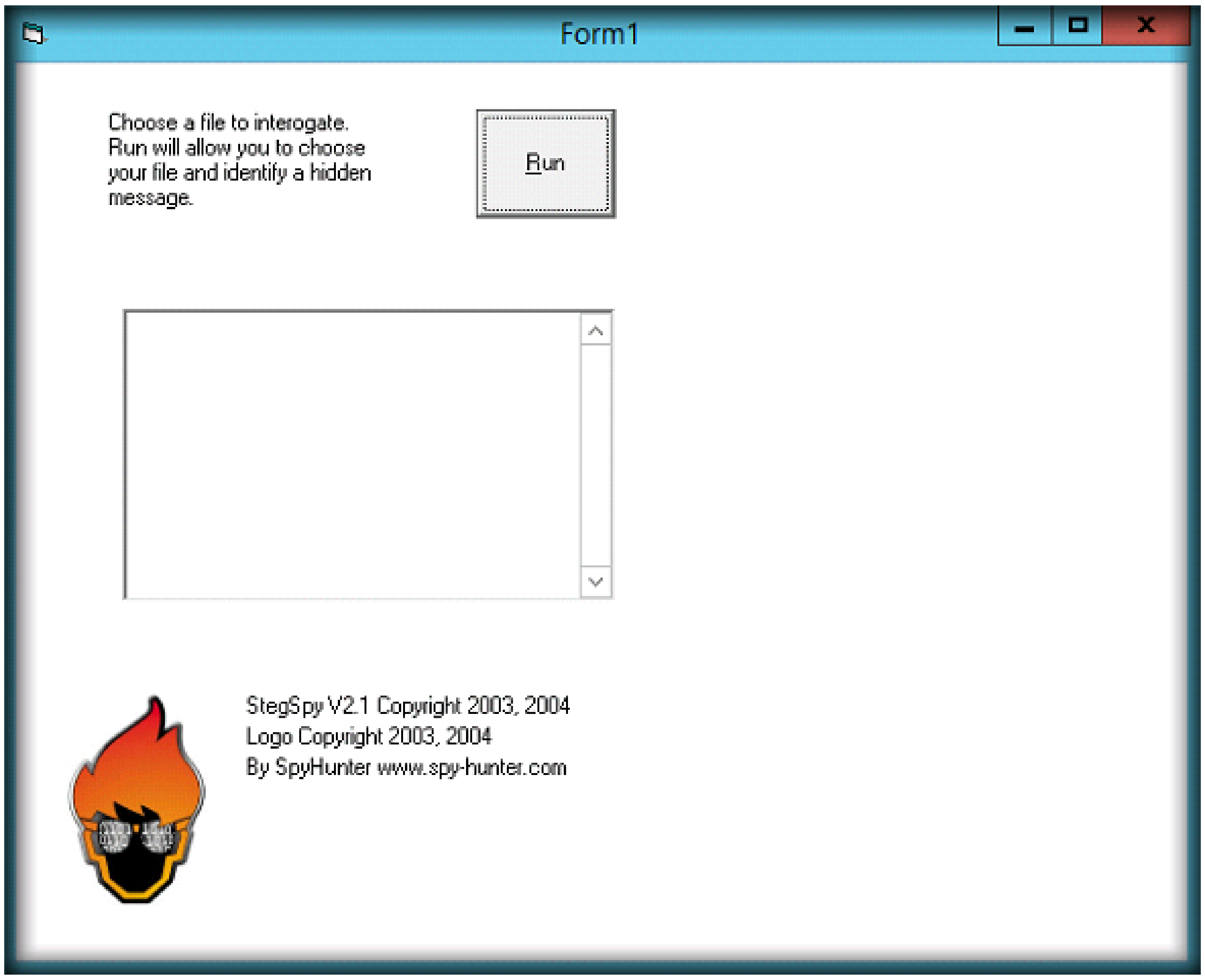
- Hiderman
- JPHideandSeek
- Masker
- JPegX
- Invisible Secrets

Lab Tasks

TASK 1

Launching SmartWhois

1. Navigate to **C:\CHFI-Tools\CHFIv9 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\StegSpy**.
2. Double-click **StegSpy2.1.exe** to launch the tool.



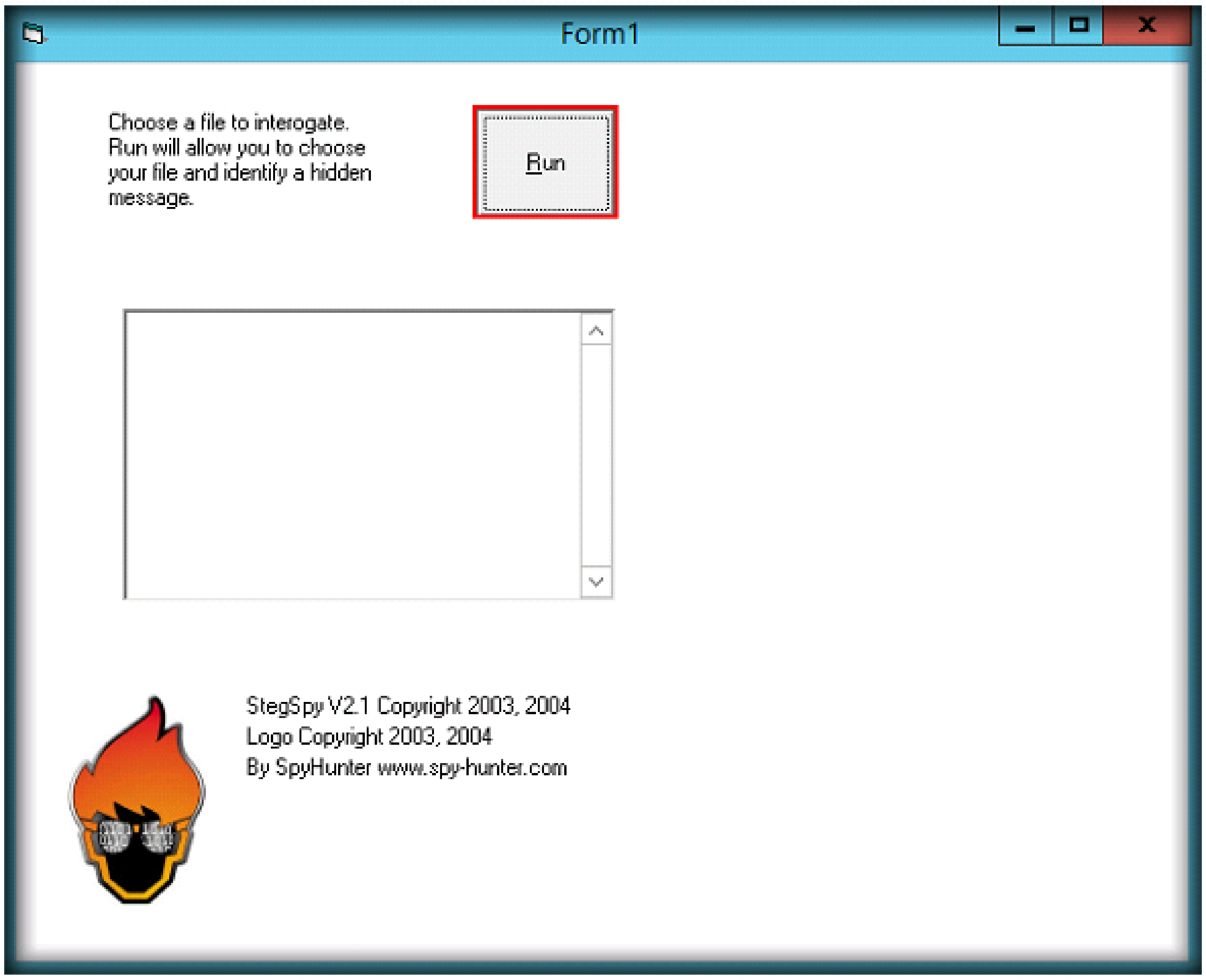
Form1

Choose a file to interogate. Run will allow you to choose your file and identify a hidden message.

StegSpy V2.1 Copyright 2003, 2004
Logo Copyright 2003, 2004
By SpyHunter www.spy-hunter.com

FIGURE 2.1: The StegSpy main window

3. Click the **Run** button from the tool main page to add the suspicious file.

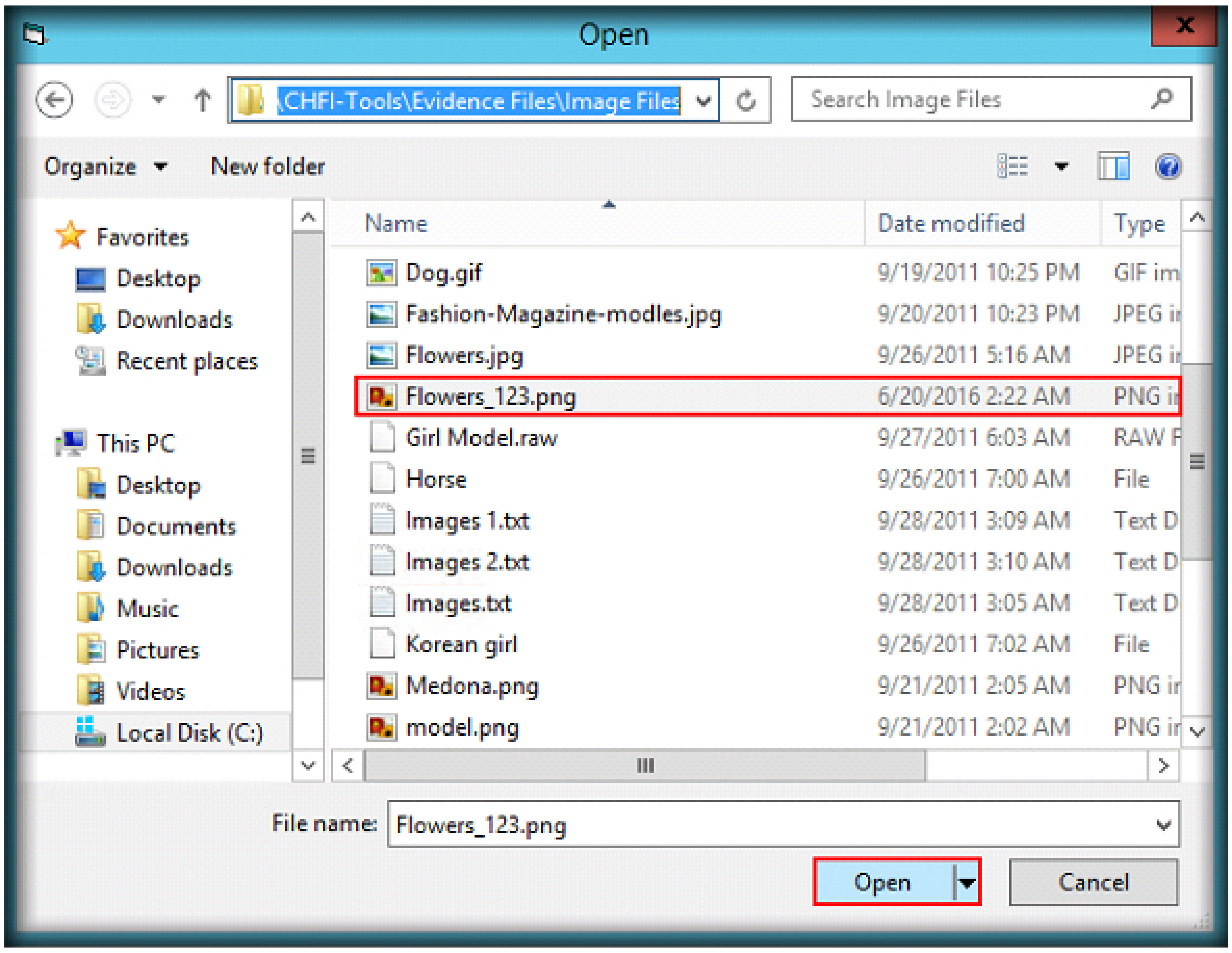


Choose a file to interogate. Run will allow you to choose your file and identify a hidden message.

StegSpy V2.1 Copyright 2003, 2004
Logo Copyright 2003, 2004
By SpyHunter www.spy-hunter.com

FIGURE 2.2: Click the Run button

4. Navigate to the location of the suspicious file, **C:\CHFI-Tools\Evidence Files\Image Files**, select the file **Flowers_123.png** and click the **Open** button.

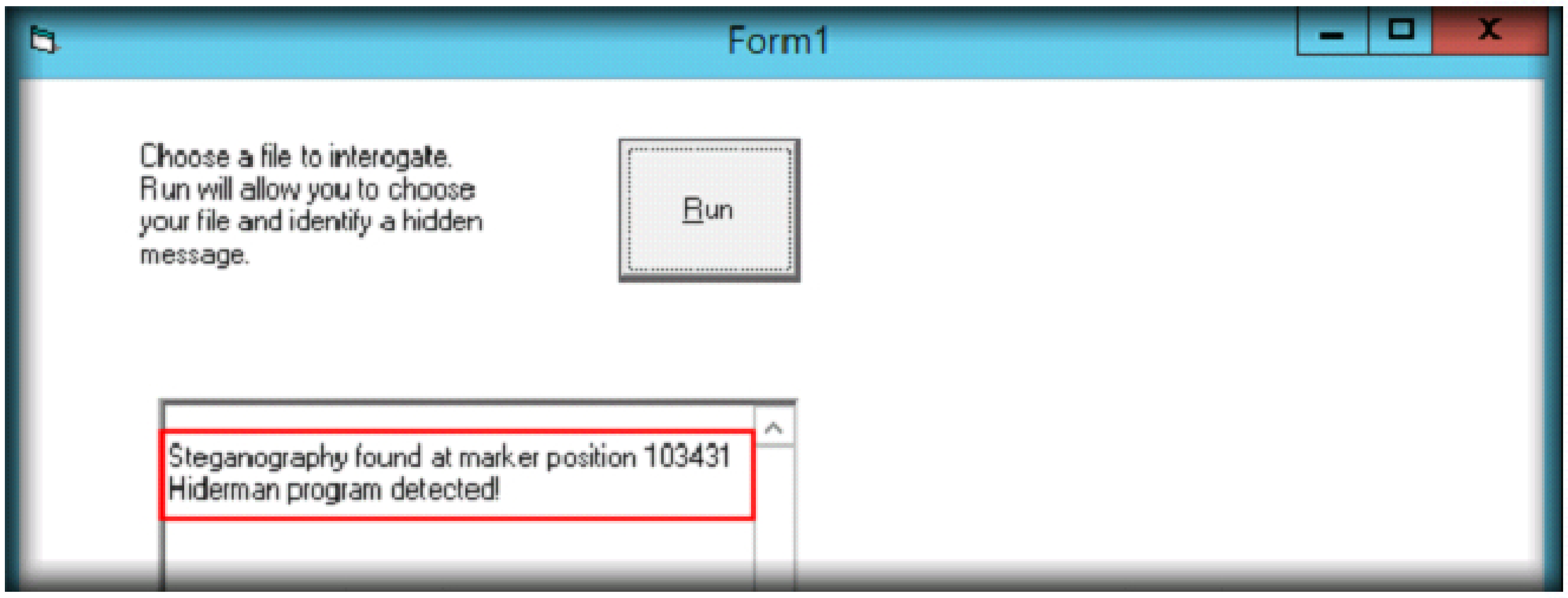


Name	Date modified	Type
Dog.gif	9/19/2011 10:25 PM	GIF im
Fashion-Magazine-modles.jpg	9/20/2011 10:23 PM	JPEG i
Flowers.jpg	9/26/2011 5:16 AM	JPEG i
Flowers_123.png	6/20/2016 2:22 AM	PNG i
Girl Model.raw	9/27/2011 6:03 AM	RAW F
Horse	9/26/2011 7:00 AM	File
Images 1.txt	9/28/2011 3:09 AM	Text D
Images 2.txt	9/28/2011 3:10 AM	Text D
Images.txt	9/28/2011 3:05 AM	Text D
Korean girl	9/26/2011 7:02 AM	File
Medona.png	9/21/2011 2:05 AM	PNG i
model.png	9/21/2011 2:02 AM	PNG i

File name: Flowers_123.png

FIGURE 2.3: Select Flowers_123.png

5. The tool will scan the file and display the type of steganography technique used to hide another file in it.



Form1
Choose a file to interrogate. Run will allow you to choose your file and identify a hidden message.
Run

Steganography found at marker position 103431
Hiderman program detected!

FIGURE 2.4: Display steganography type

6. Navigate to the location of Image Steganography tool, **C:\CHFI-Tools\CHFIv9 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\Image Steganography**.

7. Double click the **Image Steganography Setup.exe** file, to launch the setup and follow the instructions to install the **Image Steganography** tool.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

8. The tool will launch automatically after installation as shown in the following screenshot:

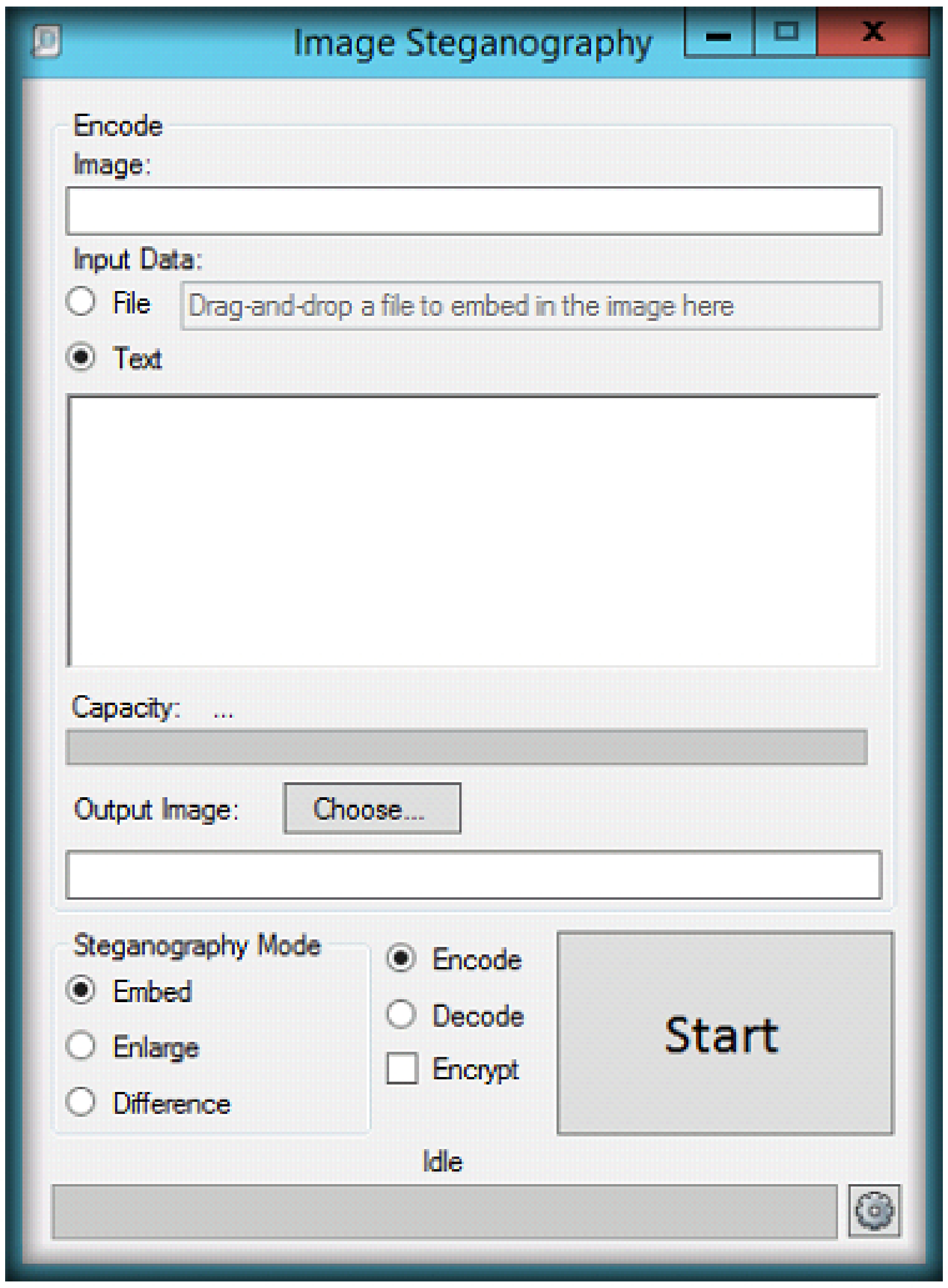


FIGURE 2.5: Tool launch screen

9. Check the **Decode** button to extract the hidden file from a steganography file.

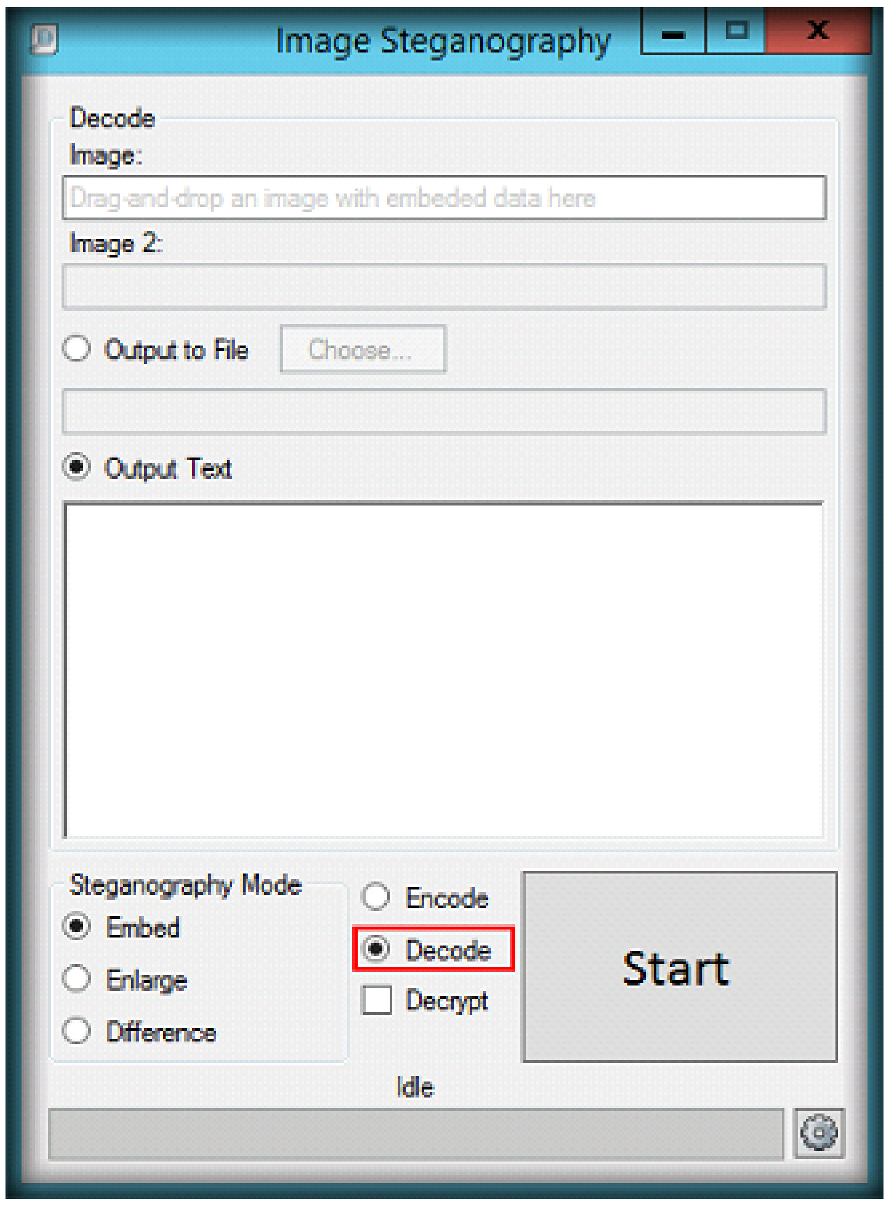


Image Steganography

Decode

Image:

Drag-and-drop an image with embeded data here

Image 2:

○ Output to File Choose...

● Output Text

Steganography Mode

● Embed

○ Enlarge

○ Difference

○ Encode

● Decode

□ Decrypt

Start

Idle

FIGURE 2.6: Check Decode button

10. Navigate to the location of the suspicious file, **C:\CHFI-Tools\Evidence Files\Image Files**, select the file **Flowers_123.png** and drop it in the **Image** section of the **Image Steganography** tool.

11. Click the **Start** button to start extracting the file.

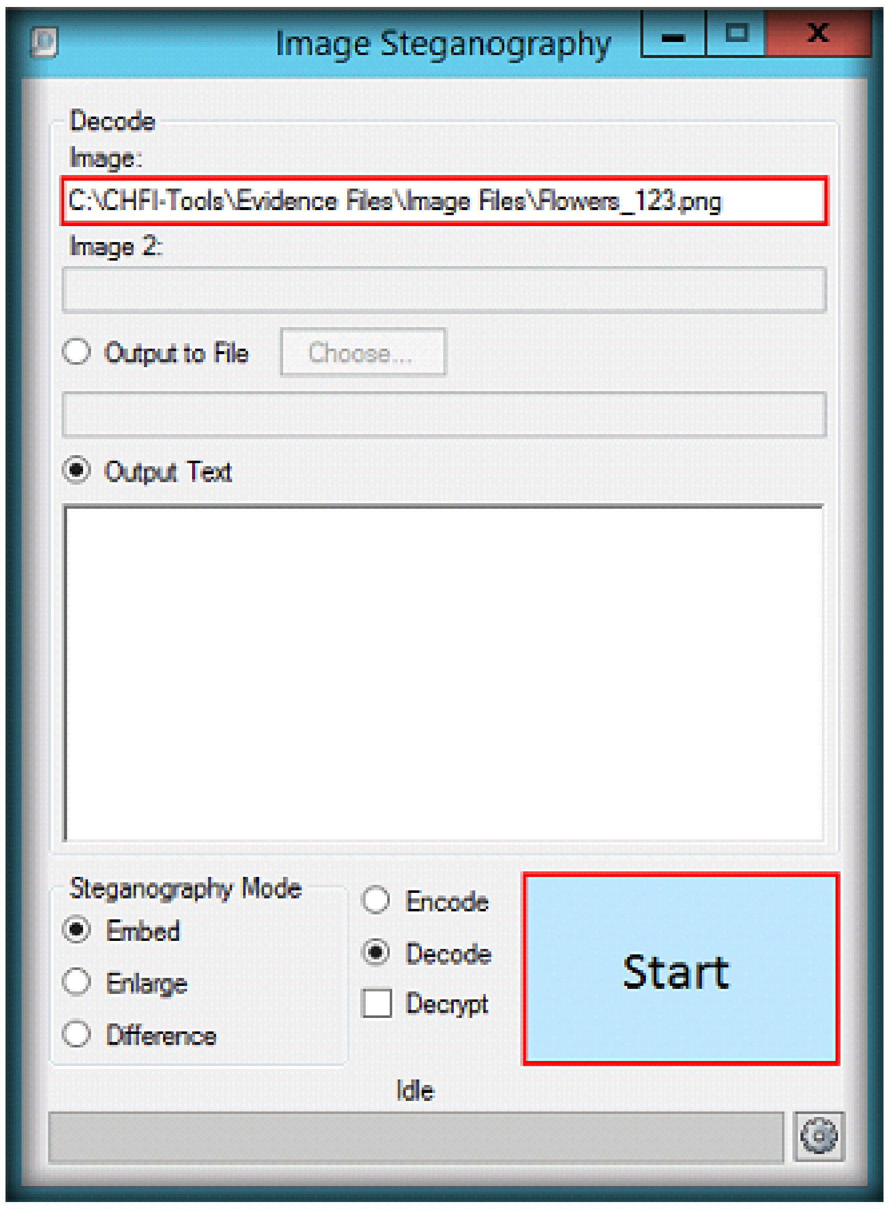


Image Steganography

Decode

Image:

C:\CHFI-Tools\Evidence Files\Image Files\Flowers_123.png

Image 2:

○ Output to File Choose...

● Output Text

Steganography Mode

● Embed

○ Enlarge

○ Difference

○ Encode

● Decode

□ Decrypt

Start

Idle

FIGURE 2.7: Click the Start button

12. The tool will analyze the file and display result if it could decipher it, else it will display a result box with message.

13. In this case, the tool failed to detect or extract the hidden content or file. It has displayed a message. Click **OK**.

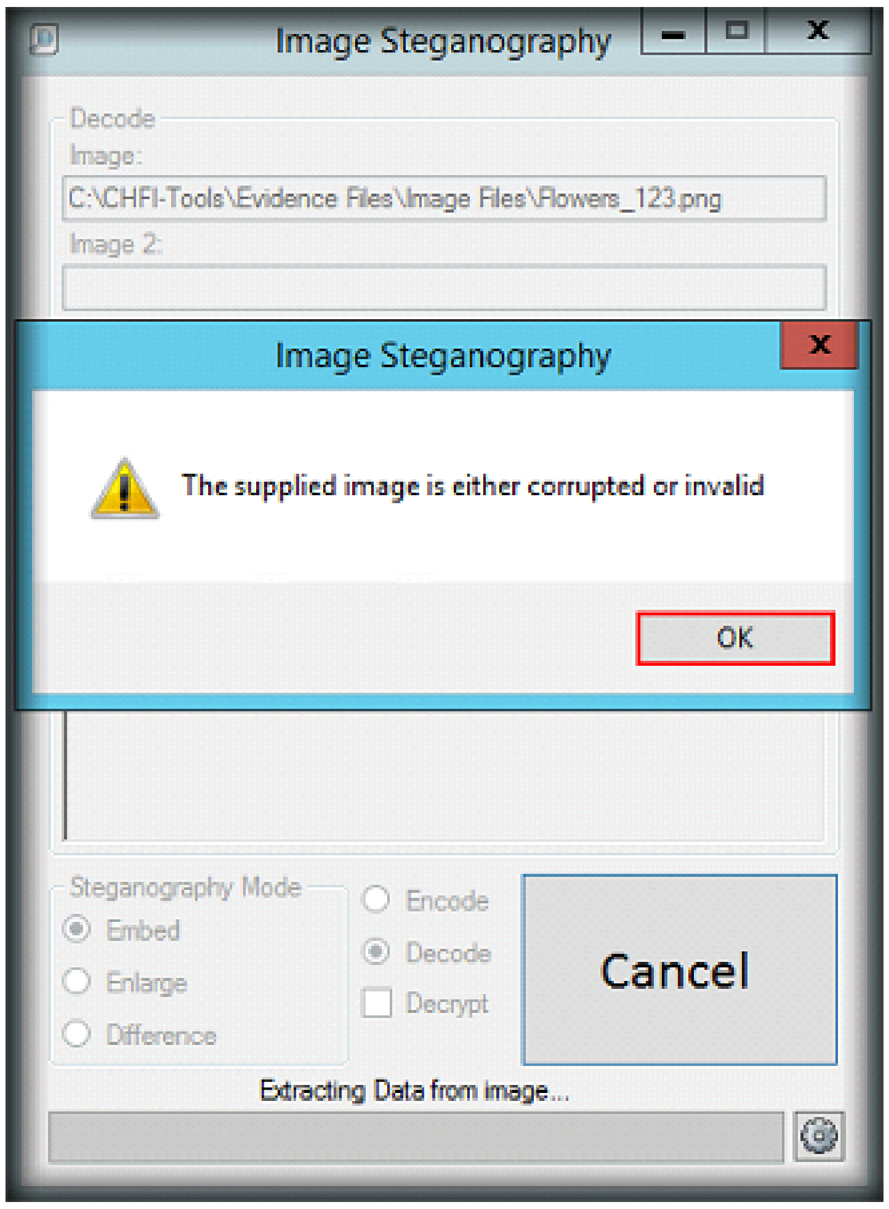


Image: C:\CHFI-Tools\Evidence Files\Image Files\Flowers_123.png

The supplied image is either corrupted or invalid

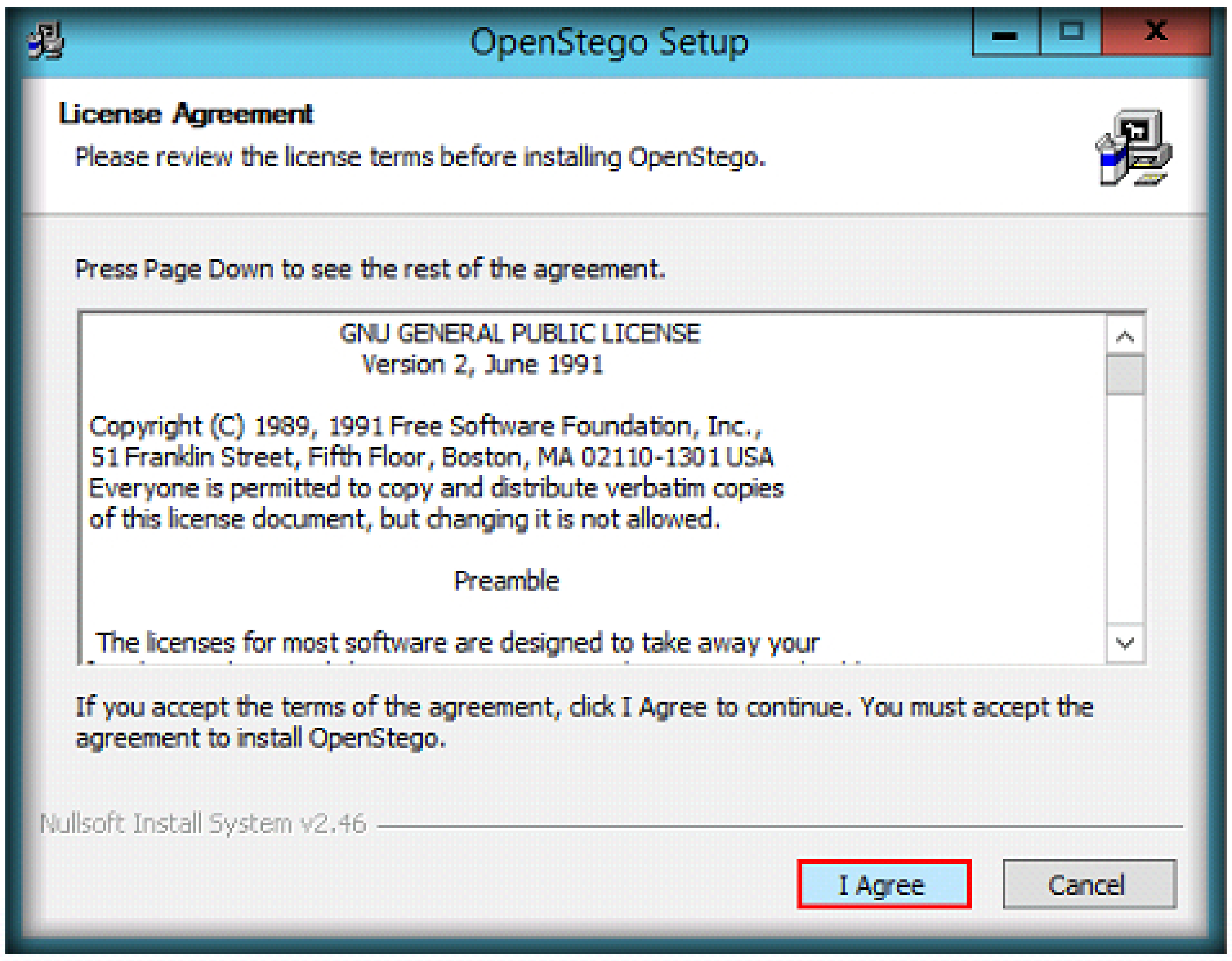
Extracting Data from image...

FIGURE 2.8: Image Steganography popup

14. You can try with other tools.

15. Navigate to the location **C:\CHFI-Tools\CHFIv9 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\OpenStego**, and double-click the **Setup-OpenStego-0.6.1.exe** file.

16. The **OpenStego** setup wizard appears, click **I Agree** button.



License Agreement

Please review the license terms before installing OpenStego.

Press Page Down to see the rest of the agreement.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

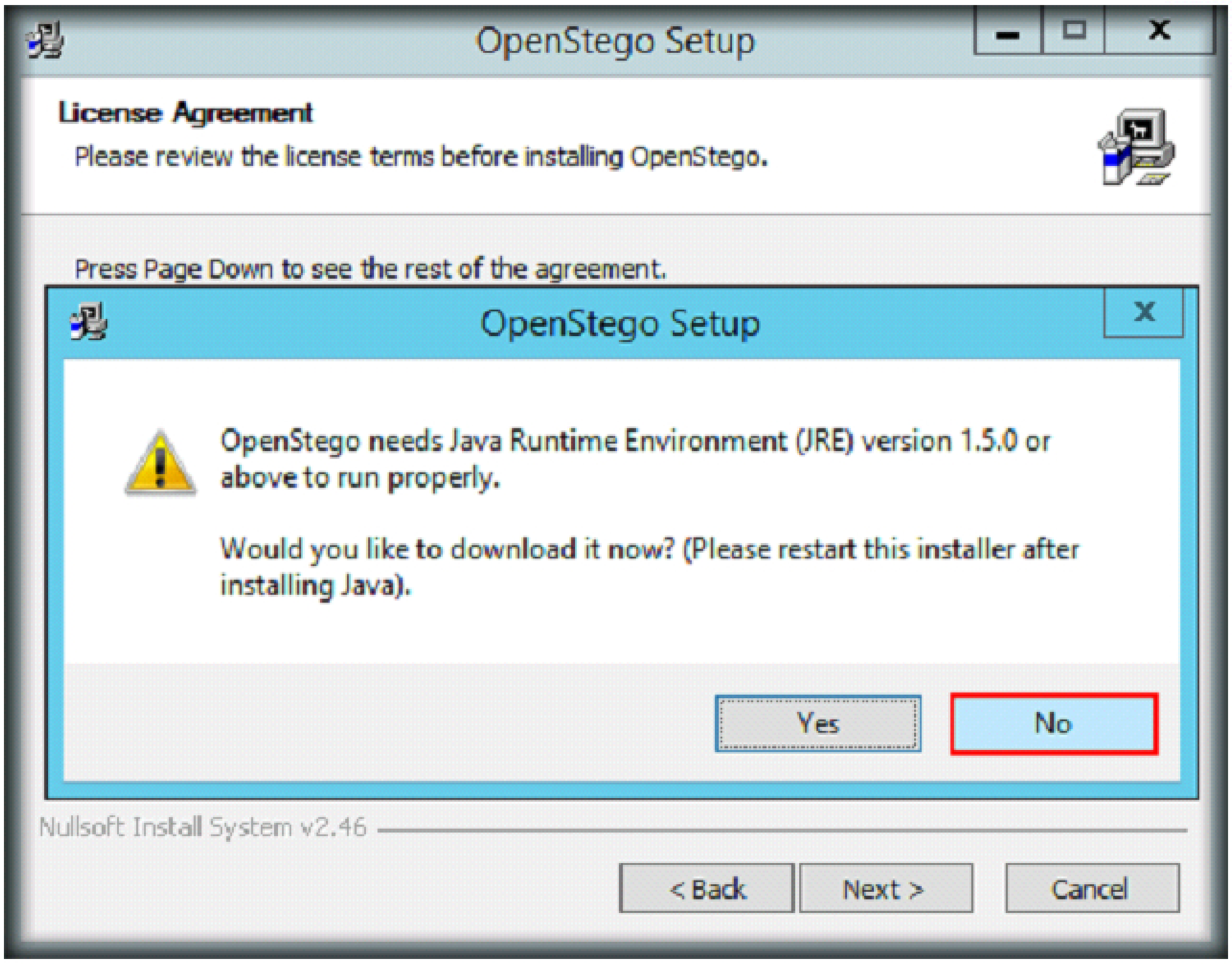
The licenses for most software are designed to take away your

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenStego.

Nullsoft Install System v2.46

FIGURE 2.9: OpenStego setup wizard

17. In the next step of the wizard, if you are asked to download java runtime environment, click **No**.



OpenStego Setup

License Agreement

Please review the license terms before installing OpenStego.

Press Page Down to see the rest of the agreement.

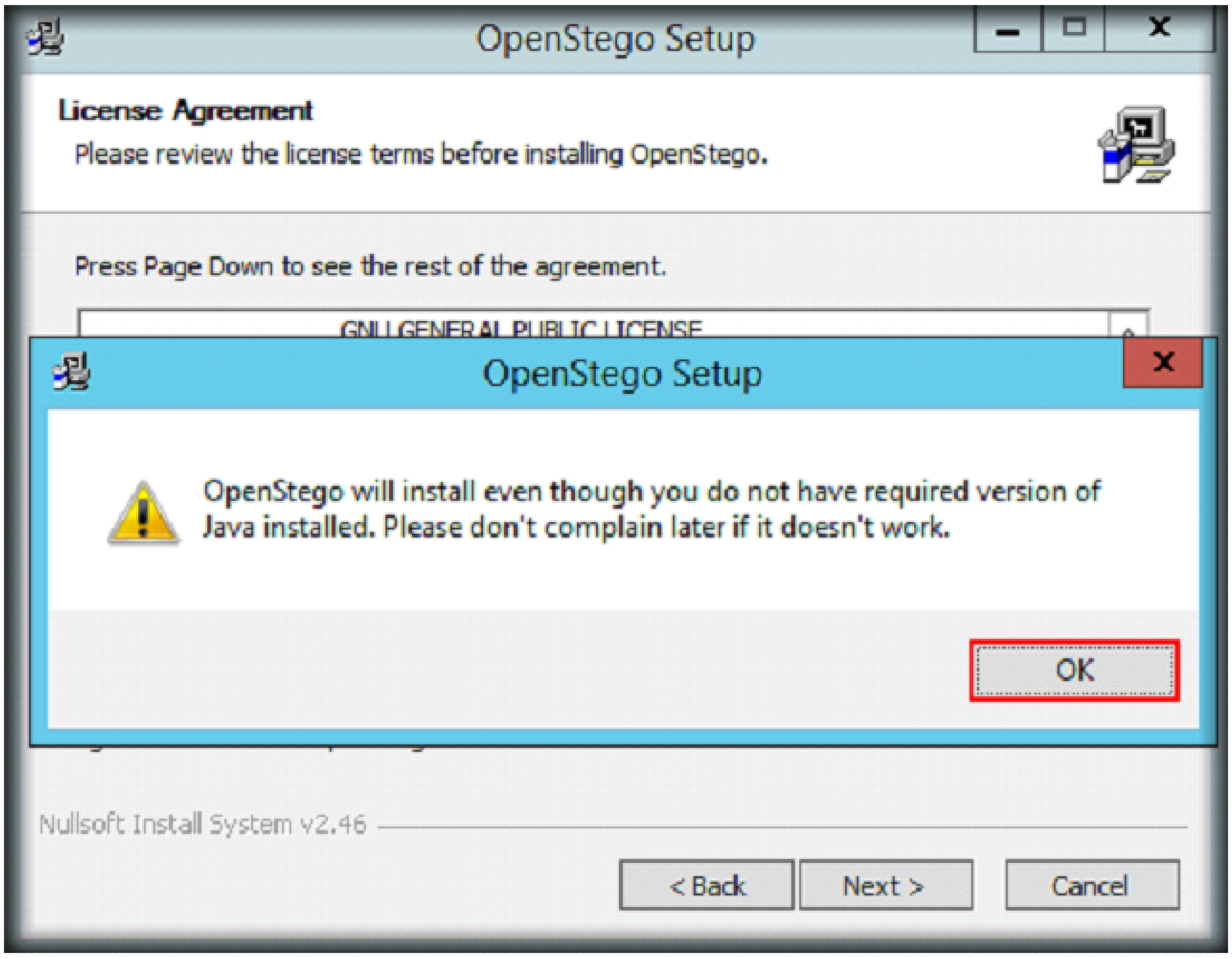
OpenStego Setup

OpenStego needs Java Runtime Environment (JRE) version 1.5.0 or above to run properly.

Would you like to download it now? (Please restart this installer after installing Java).

FIGURE 2.10: Download java runtime environment popup

18. After you click **No**, an **OpenStego** pop-up appears; click **OK**.



OpenStego Setup

License Agreement

Please review the license terms before installing OpenStego.

Press Page Down to see the rest of the agreement.

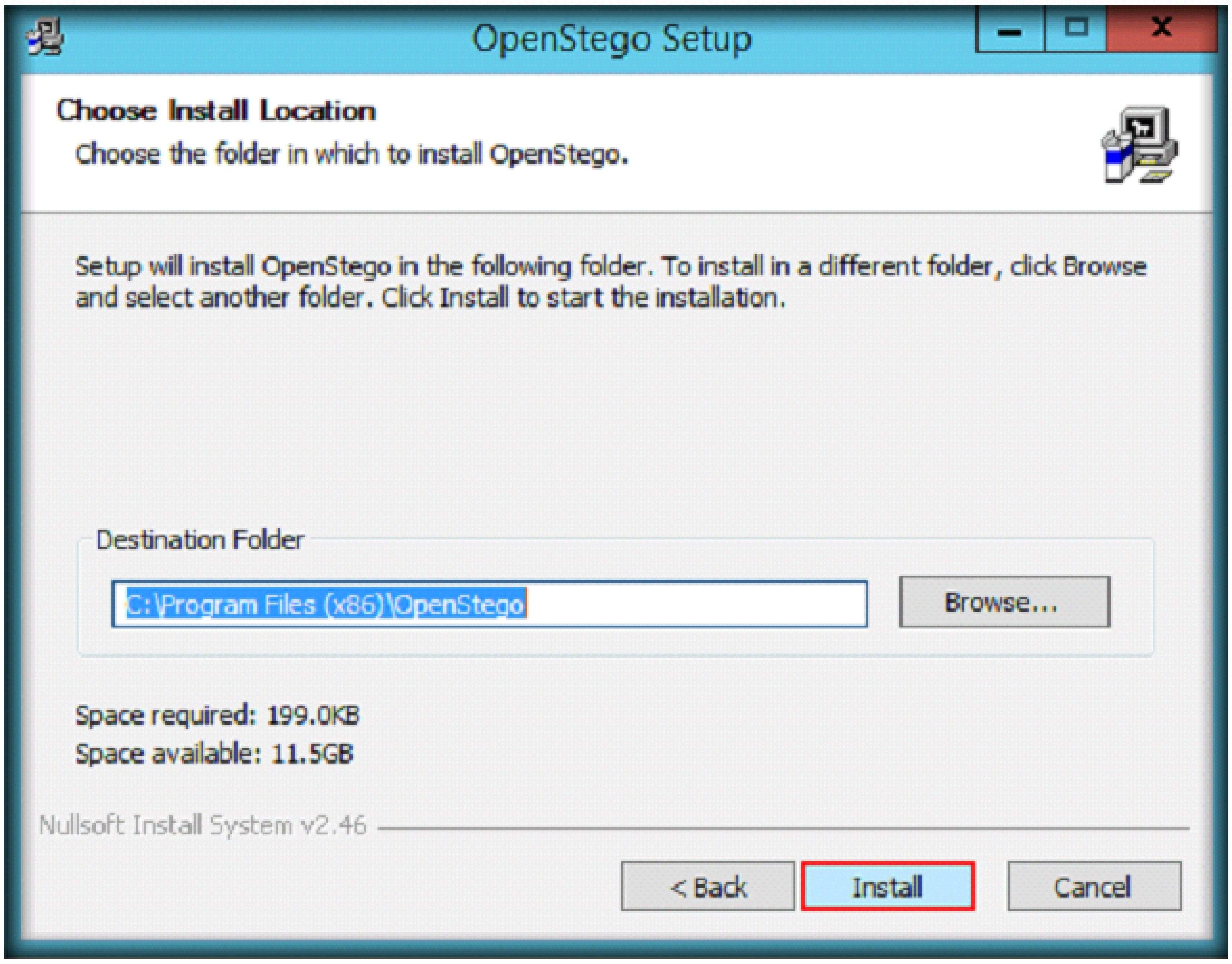
GNU GENERAL PUBLIC LICENSE

OpenStego Setup

OpenStego will install even though you do not have required version of Java installed. Please don't complain later if it doesn't work.

FIGURE 2.11: OpenStego Setup pop-up

19. In the next step of the wizard, click **Install**.



OpenStego Setup

Choose Install Location

Choose the folder in which to install OpenStego.

Setup will install OpenStego in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder

C:\Program Files (x86)\OpenStego

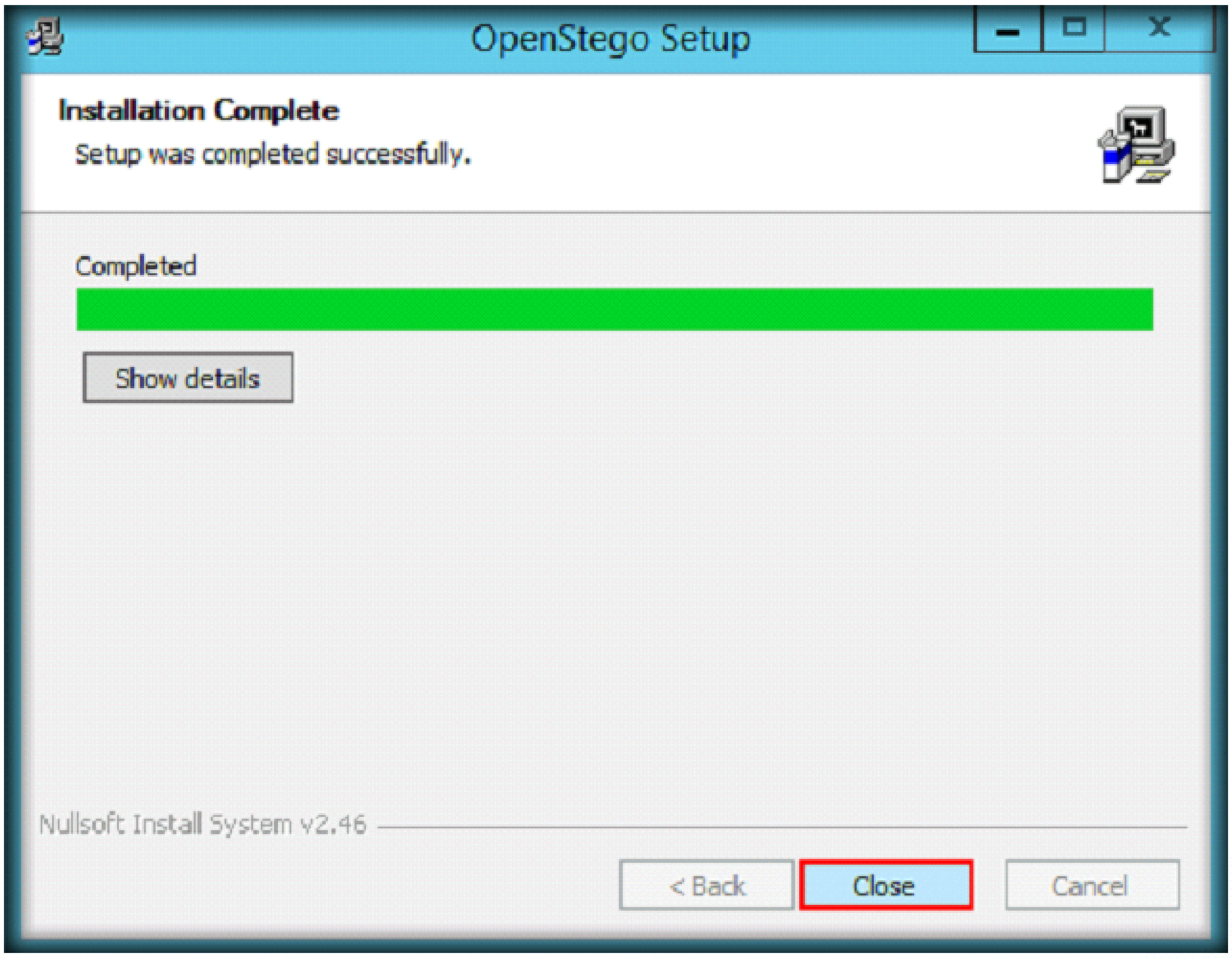
Space required: 199.0KB

Space available: 11.5GB

Nullsoft Install System v2.46

FIGURE 2.12: OpenStego Setup wizard

20. On completing the installation, click **Close**.



OpenStego Setup

Installation Complete

Setup was completed successfully.

Completed

Nullsoft Install System v2.46

FIGURE 2.13: OpenStego Setup wizard

21. Navigate to the **Apps** screen, and click **Run OpenStego** icon to launch the application.

22. OpenStego GUI appears as shown in the following screenshot:

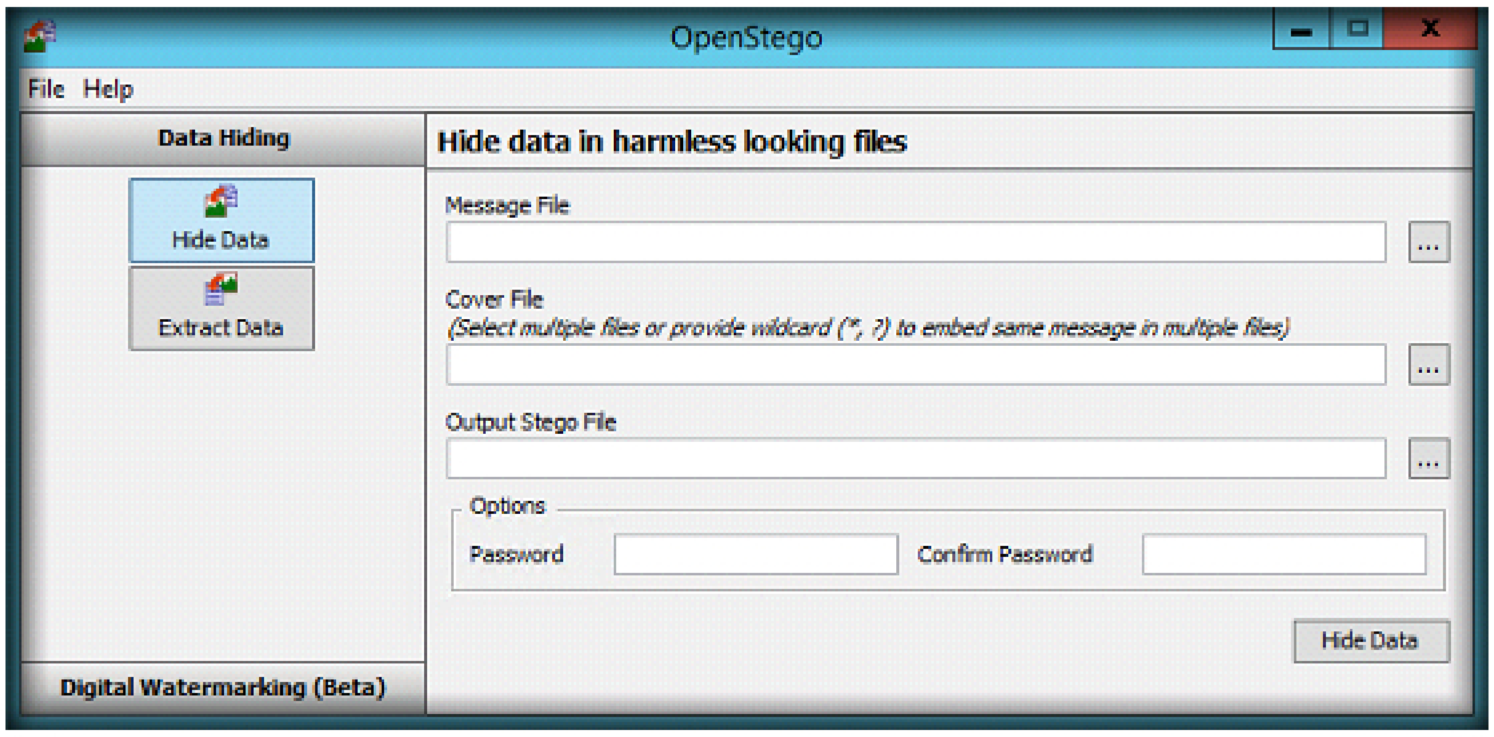

OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Hide data in harmless looking files
Message File
Cover File
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
Output Stego File
Options
Password
Confirm Password
Hide Data

FIGURE 2.14: OpenStego GUI

23. Click the **Extract Data** button on the tool main page to give the steganography file as input in order to extract the hidden data.

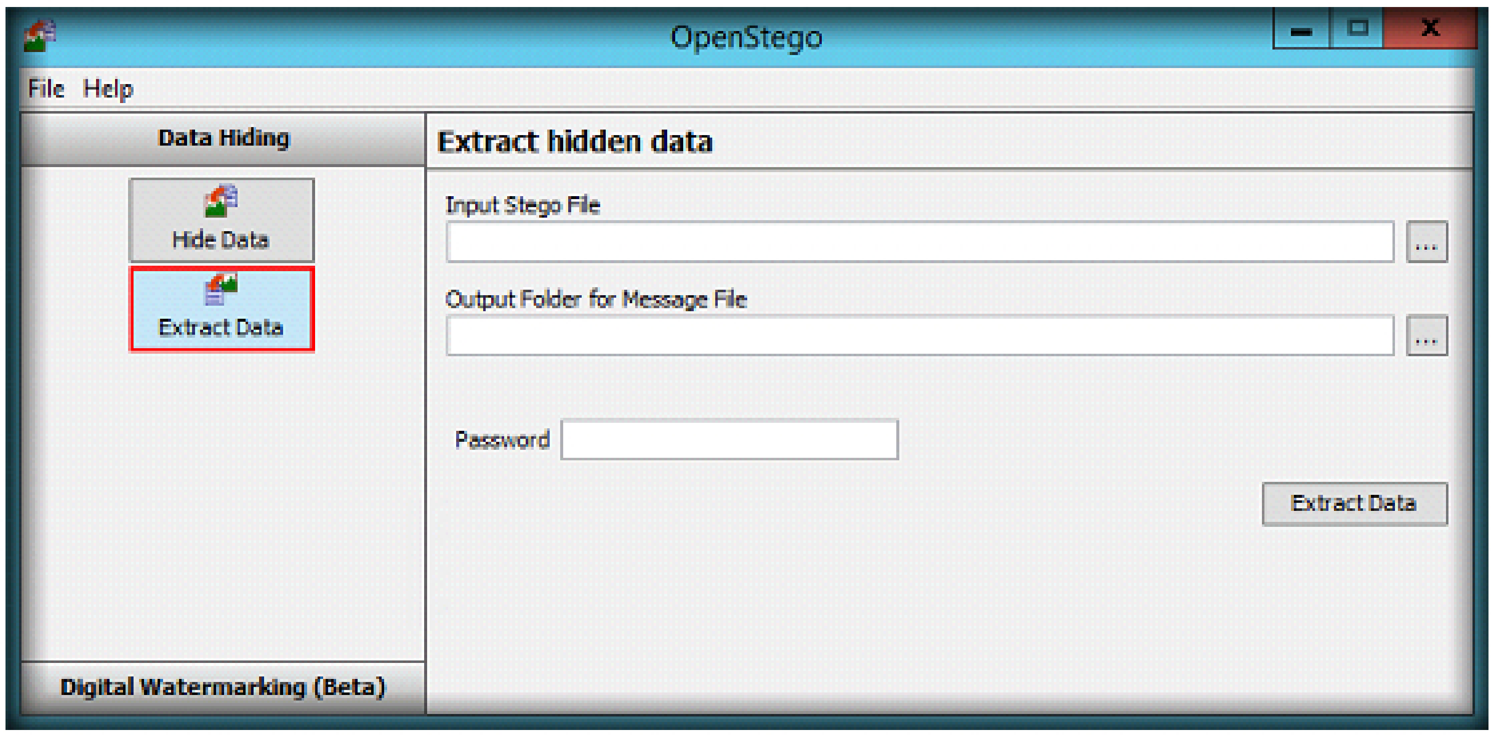
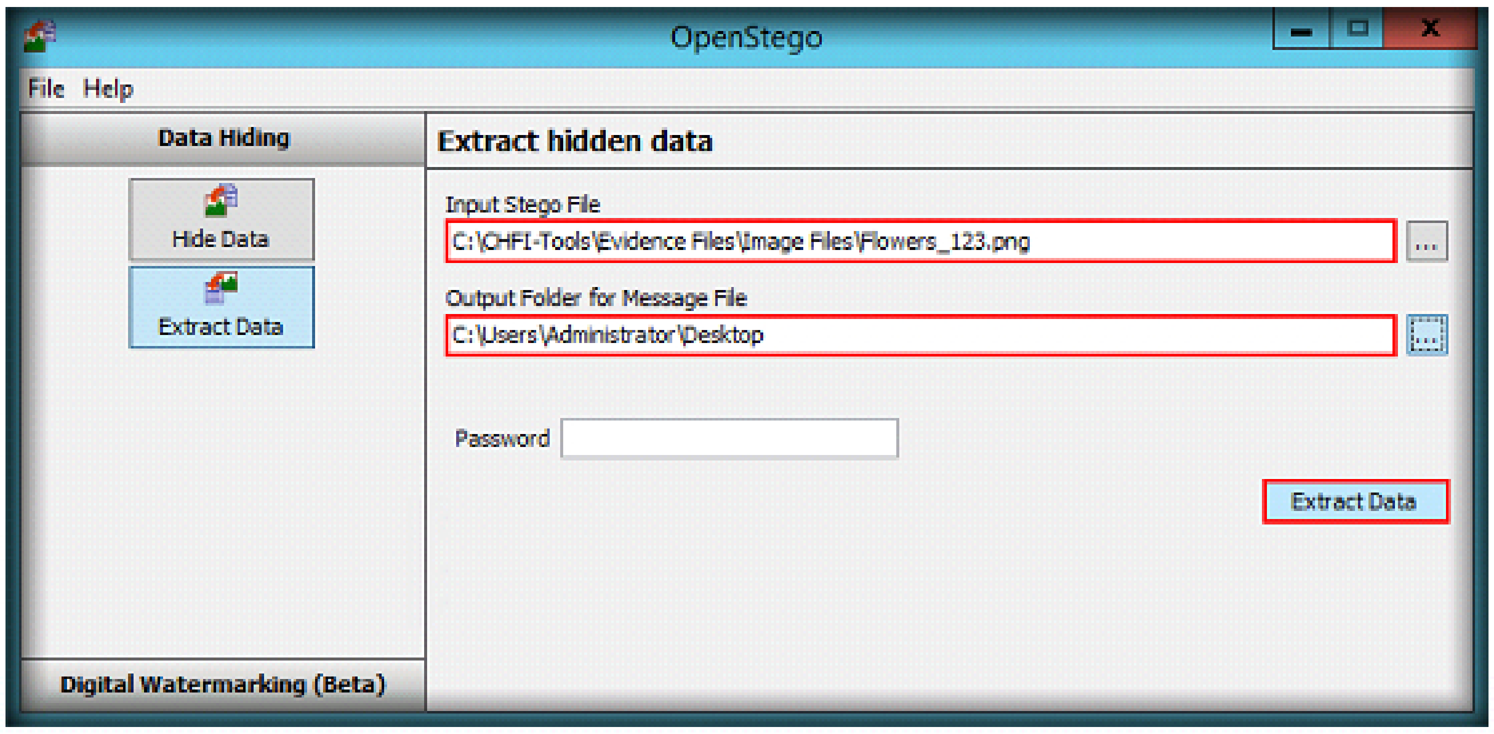


FIGURE 2.15: Extract Data button

24. Provide the location of the steganography file in the **Input Stego File** and specify a folder (here, **Desktop**) to provide output in the **Output Folder for Message File**. Click **Extract Data** button.

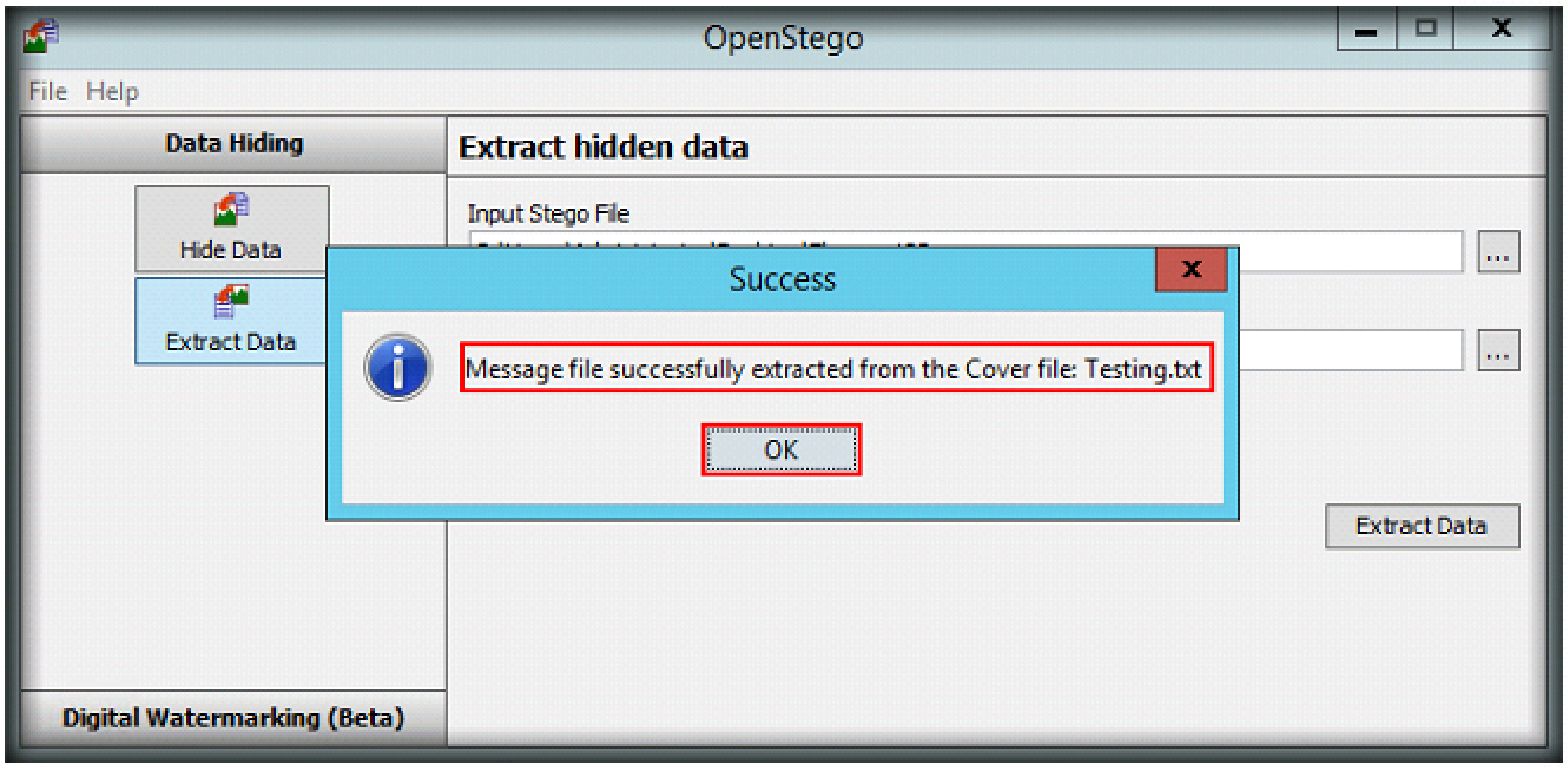


Input Stego File: C:\CHFI-Tools\Evidence Files\Image Files\Flowers_123.png

Output Folder for Message File: C:\Users\Administrator\Desktop

FIGURE 2.16: Input Stego File

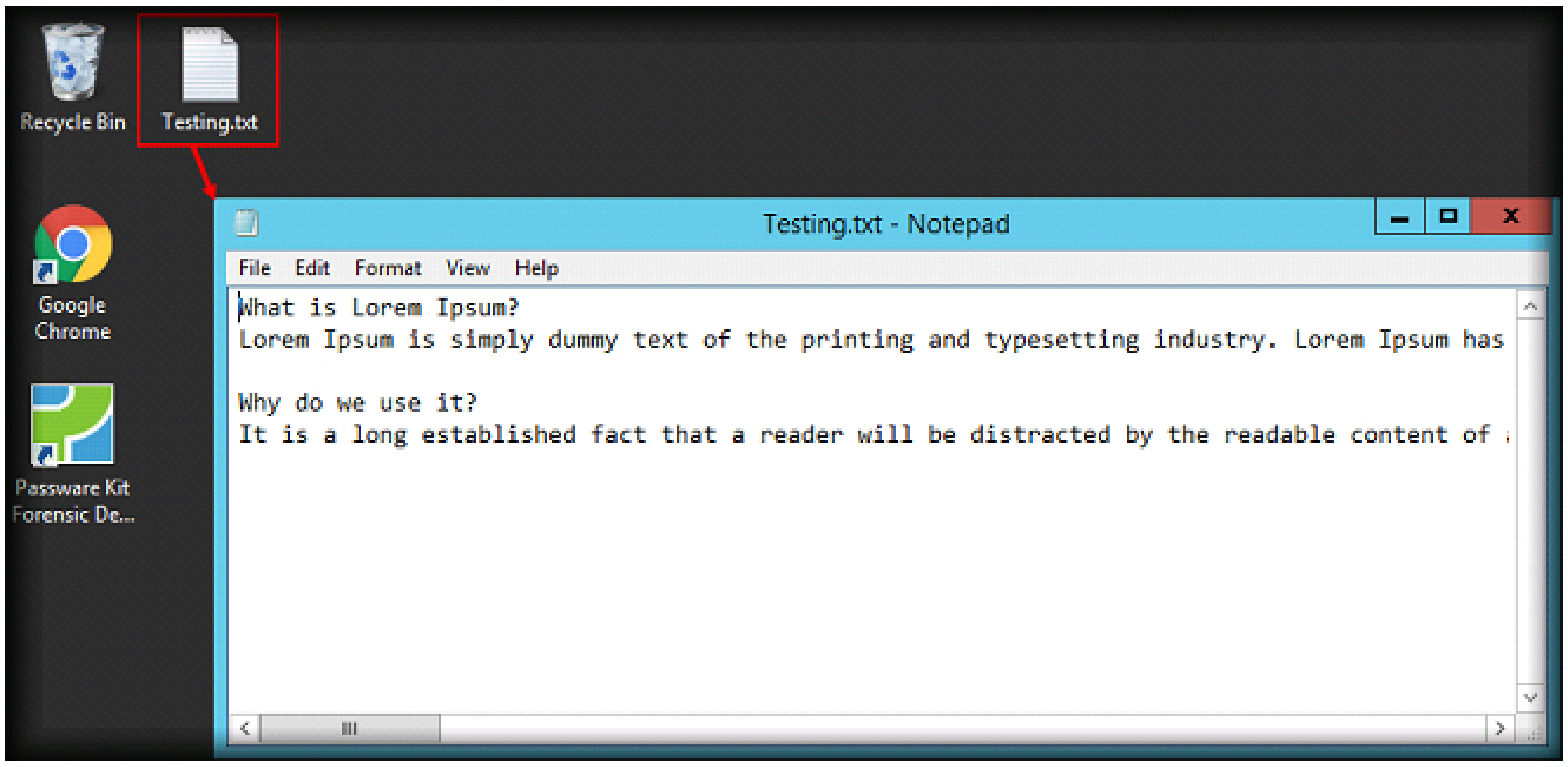
25. The tool will analyze and extract the hidden file and store it in the provided output folder. Click **OK**.



Message file successfully extracted from the Cover file: Testing.txt

FIGURE 2.17: Success popup

26. The hidden file has been extracted to the Desktop, which contains the following text in it:



```
What is Lorem Ipsum?
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has

Why do we use it?
It is a long established fact that a reader will be distracted by the readable content of
```

FIGURE 2.18: Extracted hidden file

27. You might also come across audio files that the attackers use to hide data, other files or malware in order to fool the user into clicking it. In this section, you will learn the process of extracting hidden data from an audio file.

28. Navigate to the location of the file DeepSound.msi, **C:\CHFI-Tools\CHFIv9 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools**.

TASK 2

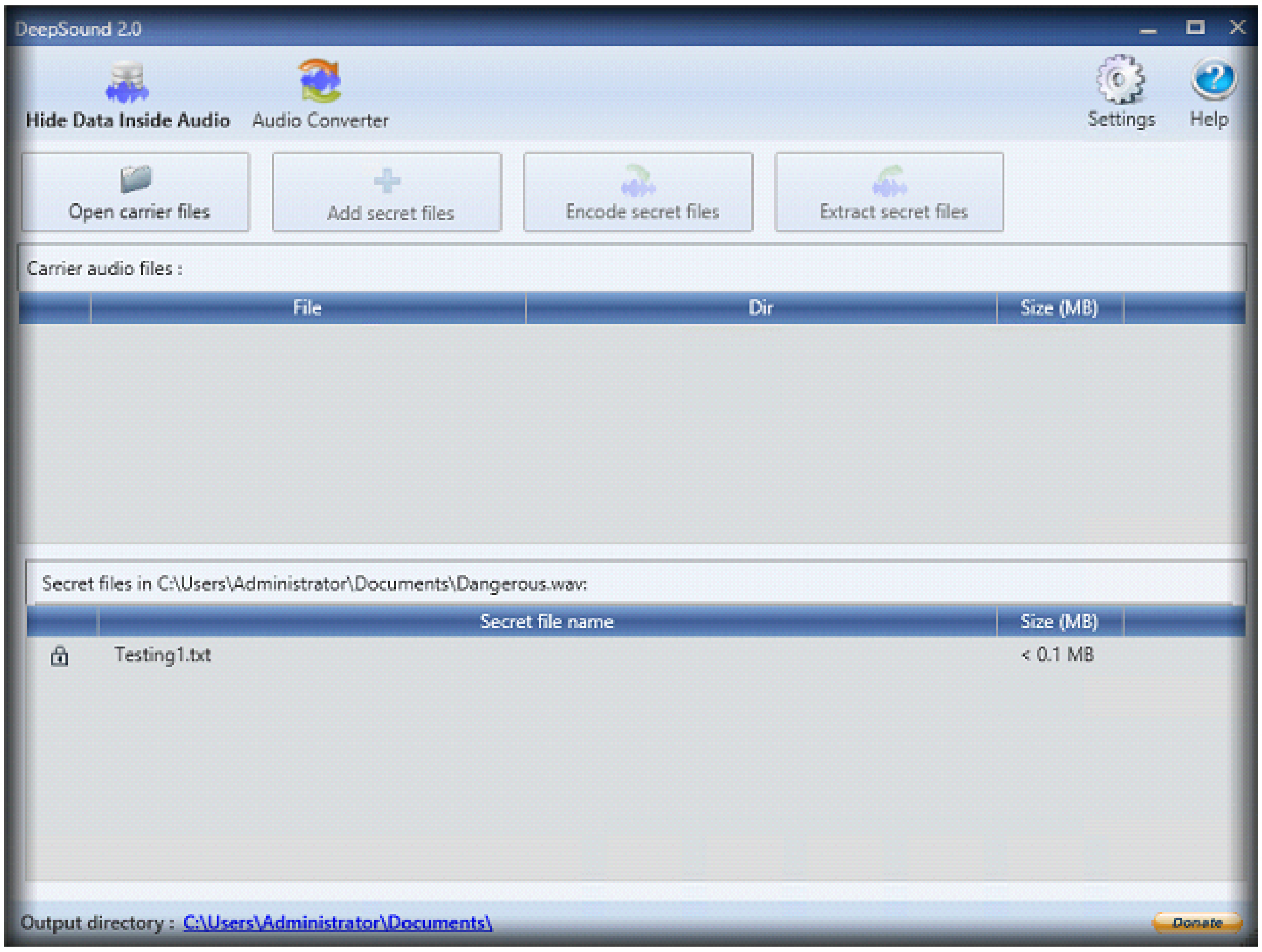
Analyzing an Audio File

29. Double click the **DeepSoundSetup.msi** file, and follow the instructions to install the tool.

30. On completing the installation, a webpage associated with DeepSound application appears. Close it.

31. Double-click **DeepSound** icon located on the Deskop, to launch the application.

32. DeepSound GUI appears as shown in the following screenshot:



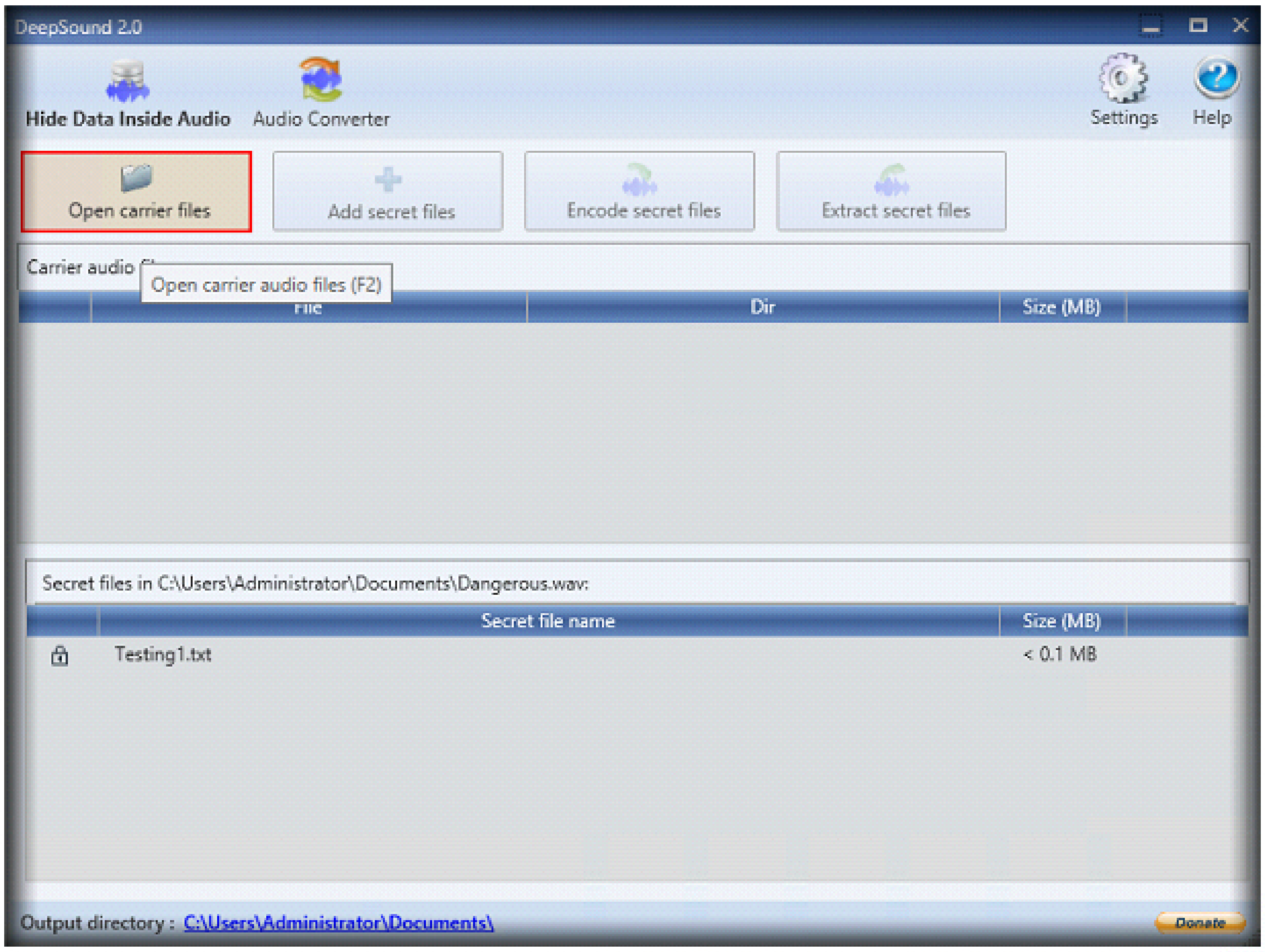
Secret files in C:\Users\Administrator\Documents\Dangerous.wav:

Secret file name	Size (MB)
Testing1.txt	< 0.1 MB

Output directory : C:\Users\Administrator\Documents\

FIGURE 2.19: DeepSound GUI

33. Click the **Open carrier files** button to add the steganography file.



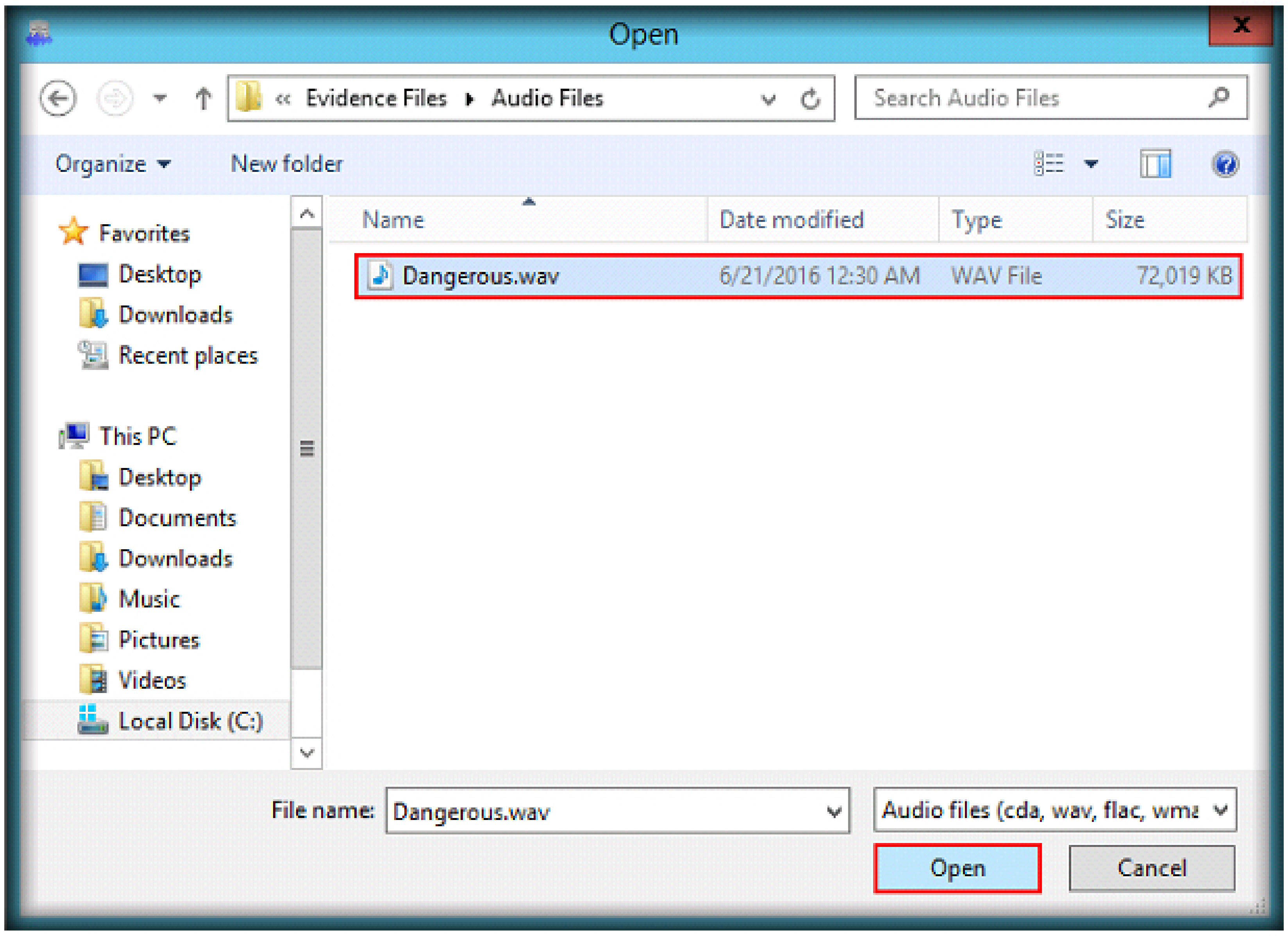
Secret files in C:\Users\Administrator\Documents\Dangerous.wav:

Secret file name	Size (MB)
Testing1.txt	< 0.1 MB

Output directory : C:\Users\Administrator\Documents\

FIGURE 2.20: Open carrier files button

34. Navigate to the location **C:\CHFI-Tools\Evidence Files\Audio Files**, select the steganography file **Dangerous.wav** and click the **Open** button.



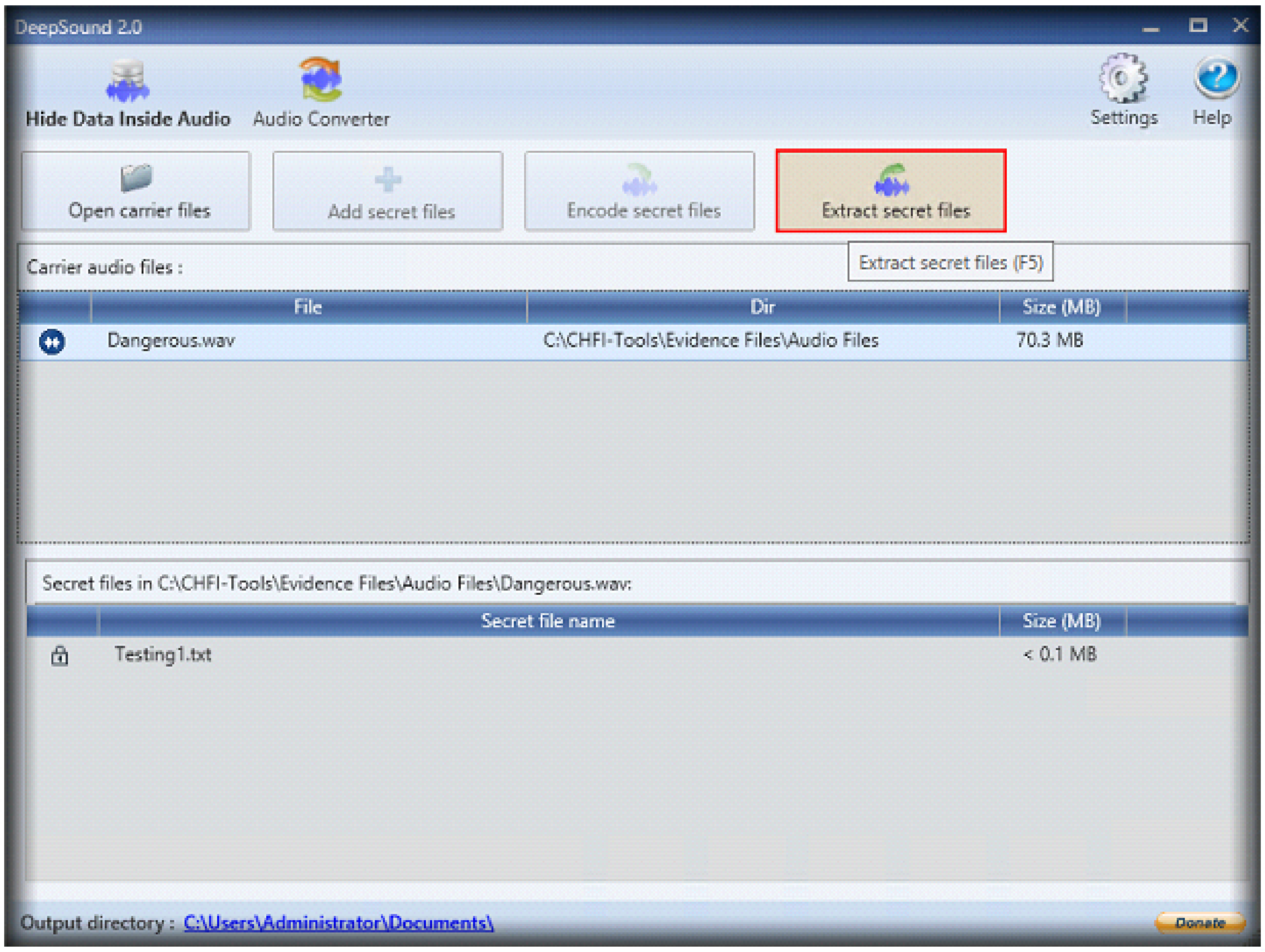
Name	Date modified	Type	Size
Dangerous.wav	6/21/2016 12:30 AM	WAV File	72,019 KB

File name: Dangerous.wav

Audio files (cda, wav, flac, wma

FIGURE 2.21: Open Dangerous.wav

35. Click the **Extract secret files** button to start extracting the hidden files or data.



Carrier audio files :

File	Dir	Size (MB)
Dangerous.wav	C:\CHFI-Tools\Evidence Files\Audio Files	70.3 MB

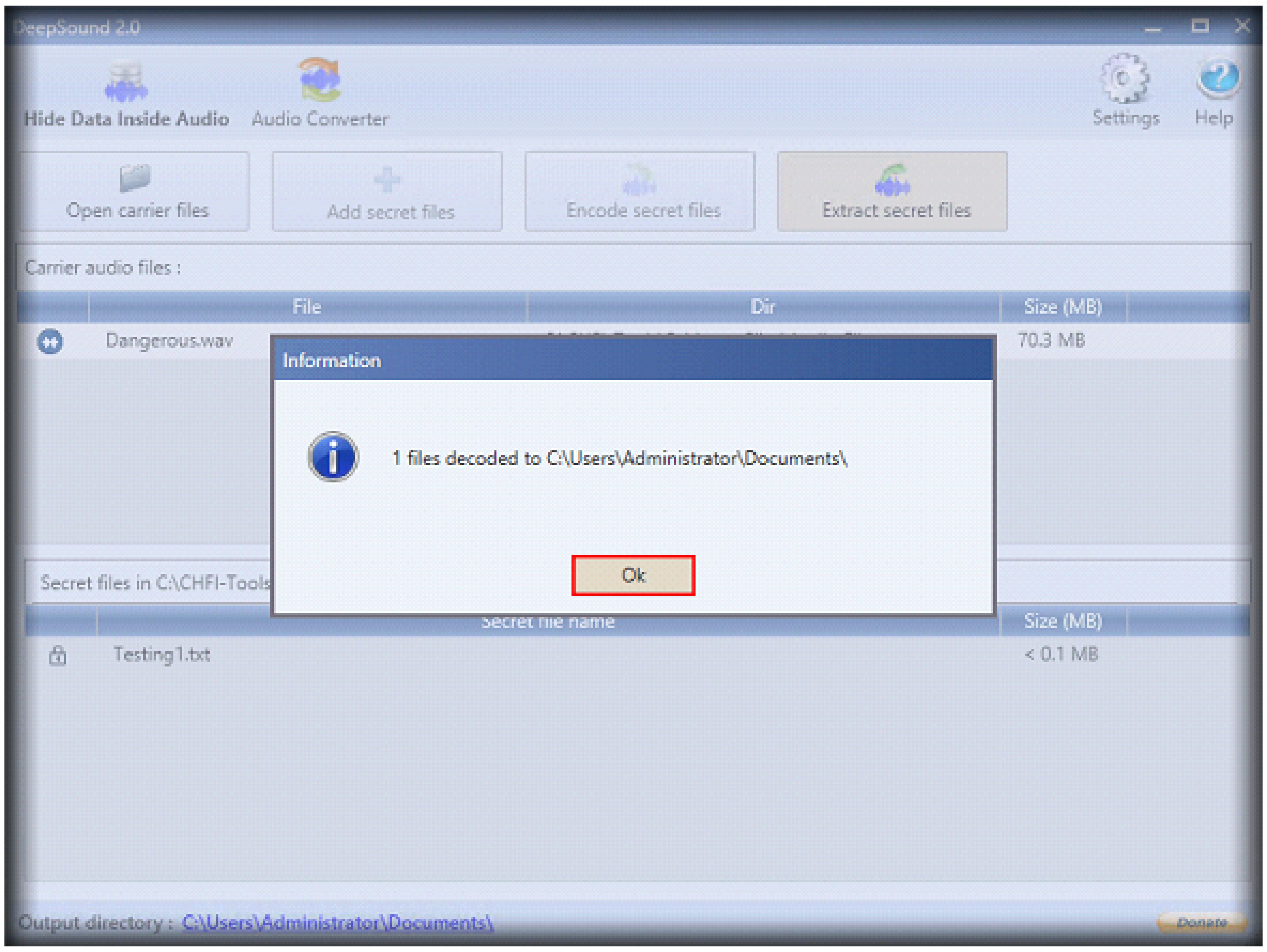
Secret files in C:\CHFI-Tools\Evidence Files\Audio Files\Dangerous.wav:

Secret file name	Size (MB)
Testing1.txt	< 0.1 MB

Output directory : C:\Users\Administrator\Documents\

FIGURE 2.22: Extract secret files button

36. Post extraction, the tool will display a message box containing the location of extracted file. Click **OK**.



Information

1 files decoded to C:\Users\Administrator\Documents\

Ok

FIGURE 2.23: Message box

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	□ No
Platform Supported	
☑ Classroom	☑ iLabs