



CompTIA Security+® Lab Series

Lab 19: General Cryptography Concepts

CompTIA Security+® Domain 6 - Cryptography

Objective 6.1: Summarize General Cryptography Concepts

Document Version: **2013-08-02**

Organization: Moraine Valley Community College

Author: Jesse Varsalone

Copyright © Center for Systems Security and Information Assurance (CSSIA), National Information Security, Geospatial Technologies Consortium (NISGTC)

The original works of this document were funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community College (MVCC).



This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCT) Grant No. TC-22525-11-60-A-48. The National Information Security, Geospatial Technologies Consortium (NISGTC) is authorized to create derivatives of identified elements modified from the original works. These elements are licensed under the Creative Commons Attributions 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

The Network Development Group (NDG) is given a perpetual worldwide waiver to distribute per US Law this lab and future derivatives of these works.

Contents

Introduction	3
Objective: Summarize general cryptography concepts.....	4
Pod Topology	5
Lab Settings.....	6
1 Hiding a Picture within a Picture Using S-Tools.....	7
1.1 Hiding a Picture Using S-Tools.....	7
1.2 Conclusion	17
1.3 Discussion Questions.....	17
2 Hiding a Media File within a Picture Using S-Tools	18
2.1 Hiding a WAV file with S-Tools	18
2.2 Conclusion	27
2.3 Discussion Questions.....	27
3 Revealing Hidden Data Using S-Tools.....	28
3.1 Revealing Hidden Data	28
3.2 Conclusion	32
3.3 Discussion Questions.....	32
References	33

Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. This series of lab exercises is intended to support courseware for CompTIA Security+® certification

This lab includes the following tasks:

- 1 - Hiding a Picture within a Picture Using S-Tools
- 2 - Hiding a Media File within a Picture Using S-Tools
- 3 - Revealing Hidden Data Using S-Tools

Objective: Summarize general cryptography concepts

You may have read an article online about how some Russian spies used steganography to conceal information and send information to one another. The tools and techniques used in this lesson are very similar to those used in high profile cases within the media.

S-Tools – S-Tools is a steganography tool that can be utilized to hide pictures or WAV files. S-Tools can also be used to reveal hidden digital messages in pictures if the person has the correct password and encryption algorithm. Tools like this one and similar tools have been used to transmit files with hidden digital messages in them.

Encryption Algorithm – S-Tools allows the user to use various symmetric encryption algorithms to encrypt their hidden digital message, including:

- IDEA - International Data Encryption Algorithm
- DES – Digital Encryption Standard
- Triple DES - Triple Data Encryption Standard

BMP File – A BMP, Bitmap Image File, is a picture image format that can be utilized within the S-Tools program.

WAV File – A WAV, Waveform Audio File Format file, is a sound file format that can be utilized within the S-Tools program. WAV files can be hidden within or used to hide other files.

GIF File – A GIF, Graphics Interchange Format file, is a picture image format that can be utilized within the S-Tools program. Other files can be hidden within GIF files.

Pod Topology

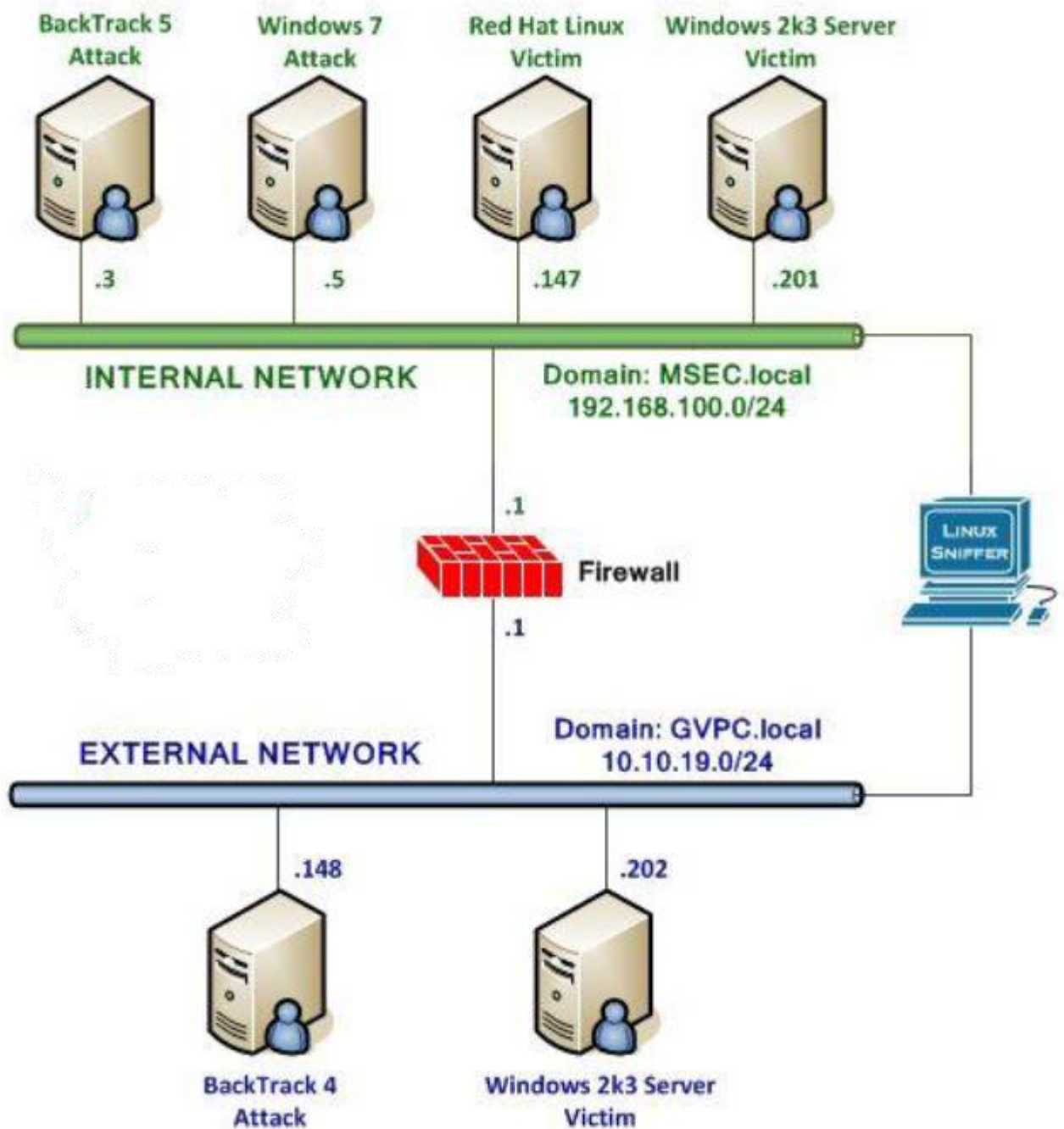


Figure 1: Topology

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

Log in to the following virtual machine before starting the tasks in this lab:

Windows 7 Internal Attack Machine	192.168.100.5
Windows 7 student password	password

Windows 7 Internal Attack Login:

1. Click on the Windows 7 Internal Attack icon on the topology.
2. Enter the username, **student** (verify the username with your instructor).
3. Type in the password, **password** and hit enter to log in (verify the password with your instructor).



Figure 2: Windows 7 login

1 Hiding a Picture within a Picture Using S-Tools

S-Tools is a steganography tool that can be used to hide bitmap, GIF, and WAV files from plain view. The files will be embedded in a picture file.

1.1 Hiding a Picture Using S-Tools

Open S-Tools

1. In the Windows 7 Internal Attack Machine, double-click on the **steg** folder on your desktop. Double-click to open **S-Tools.exe**.

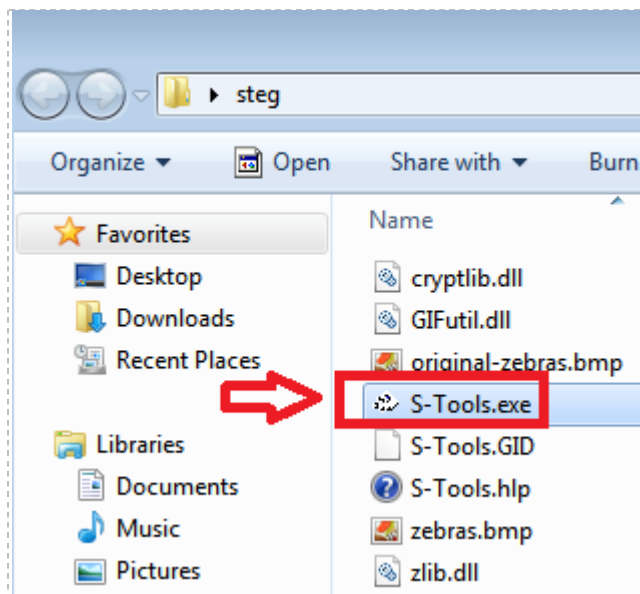


Figure 3: Double-Clicking on the S-Tools.exe file

2. Click **Continue** if you receive a warning. Click the single rectangle in the bottom left hand side of the screen to maximize the **Actions** window for S-Tools.

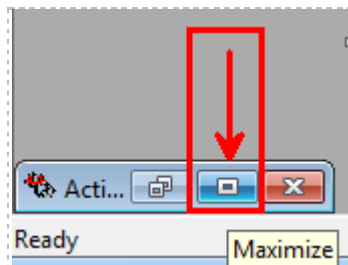


Figure 4: Maximize the Actions Window

3. Move the S-Tools window and the open **steg** folder side-by-side. Drag the **original-zebras.bmp** file from the **steg** folder into the S-Tools **Actions** window.

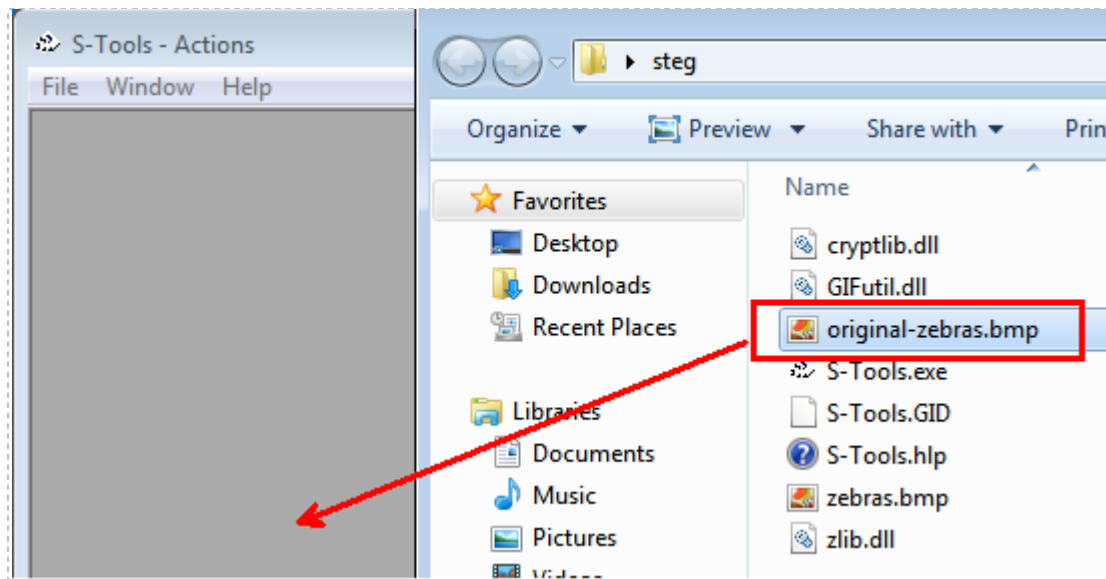


Figure 5: Dragging a File into the S-Tools Actions Windows

Notice in the bottom right hand corner, it states that this bitmap picture file can hold up to 294,896 bytes. This is the size limit for a file that can be hidden within this picture.



Figure 6: The original-zebra.bmp file can hold up to 294,896 bytes

4. Drag the **msec.bmp** file on to the **original-zebras.bmp** picture in the S-Tools Actions window. After the file is placed in the window, you will see a box appear. This box asks for a **passphrase**, **passphrase verification**, and the **encryption algorithm**.

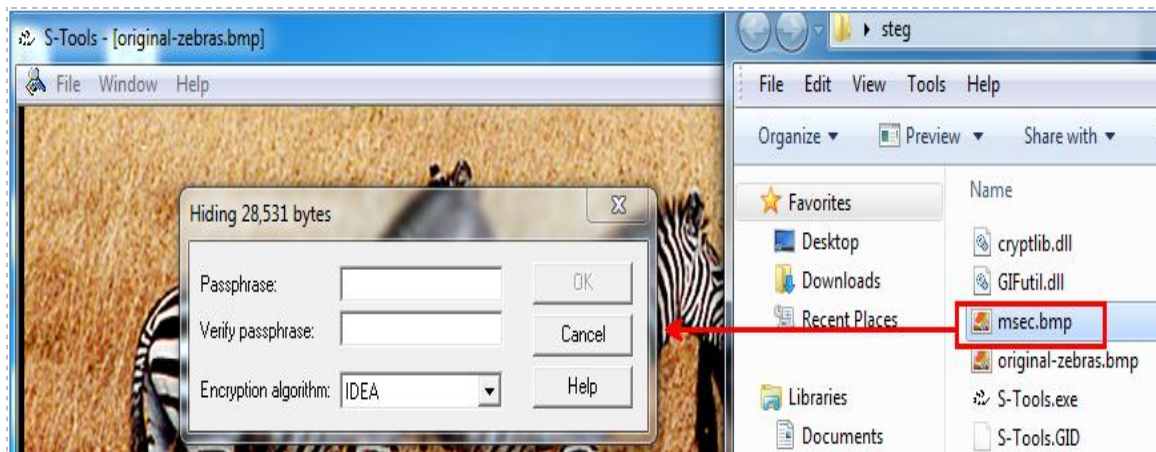


Figure 7: Hiding the msec.bmp file within the original-zebras file.

5. For the **Passphrase**, type **password**. For the **Verify passphrase**, type **password**. Leave **IDEA** for the Encryption algorithm. Click the **OK** button to hide the **msec.bmp** file. NOTE:

The passphrase will be displayed as asterisks (*) when you type.

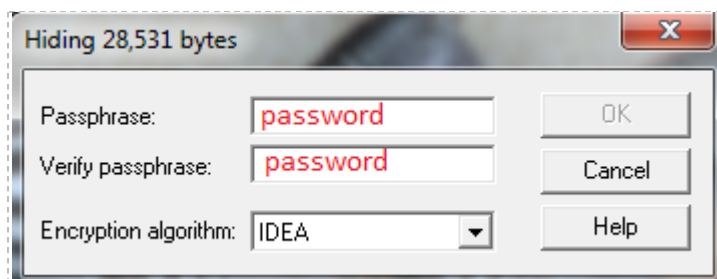


Figure 8: Typing the Password

Even though the IDEA Encryption was used, other encryption algorithms can be used. If an encryption algorithm other than the default is chosen, that information needs to be provided, along with the password, to the person who is revealing the hidden picture.

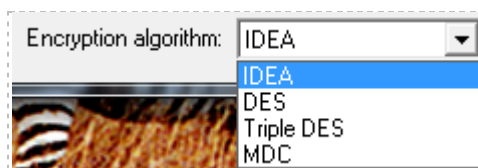


Figure 9: Selecting the Encryption Algorithm

Now, in the top left hand corner of the picture, the phrase **[hidden data]** will appear, indicating that digital information has been hidden in the **original-zebras.bmp** file.

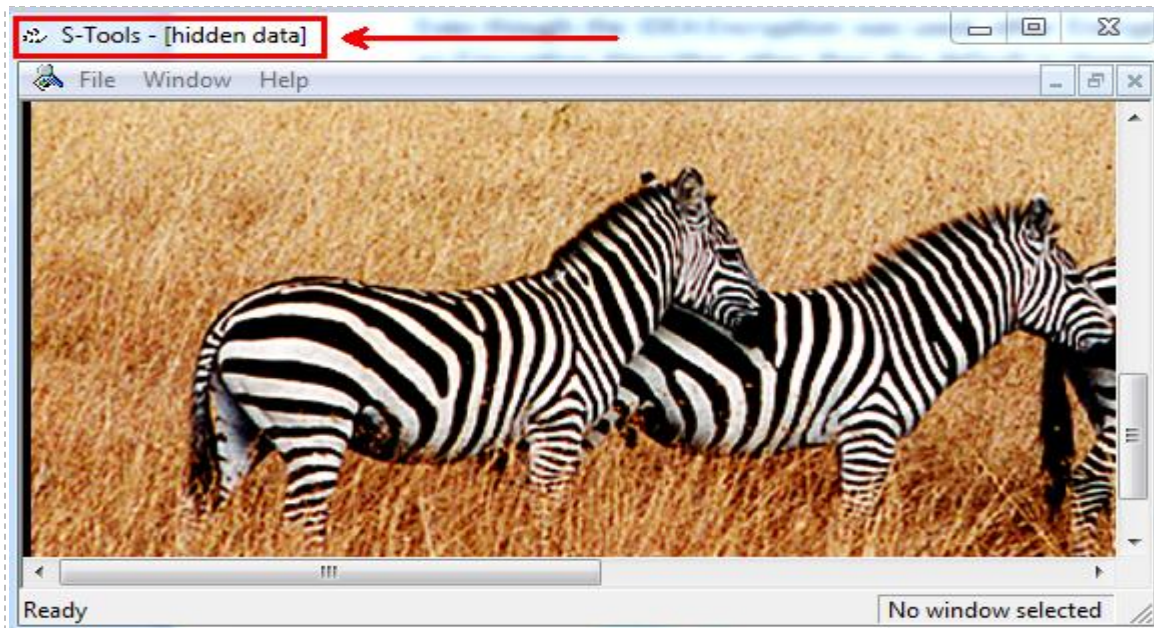


Figure 10: The msec.bmp file is hidden data within the original-zebras.bmp picture

6. To save the **original-zebras.bmp** file with the hidden **msec.bmp** file, right-click anywhere within the picture, and select **Save as...** from the menu list.

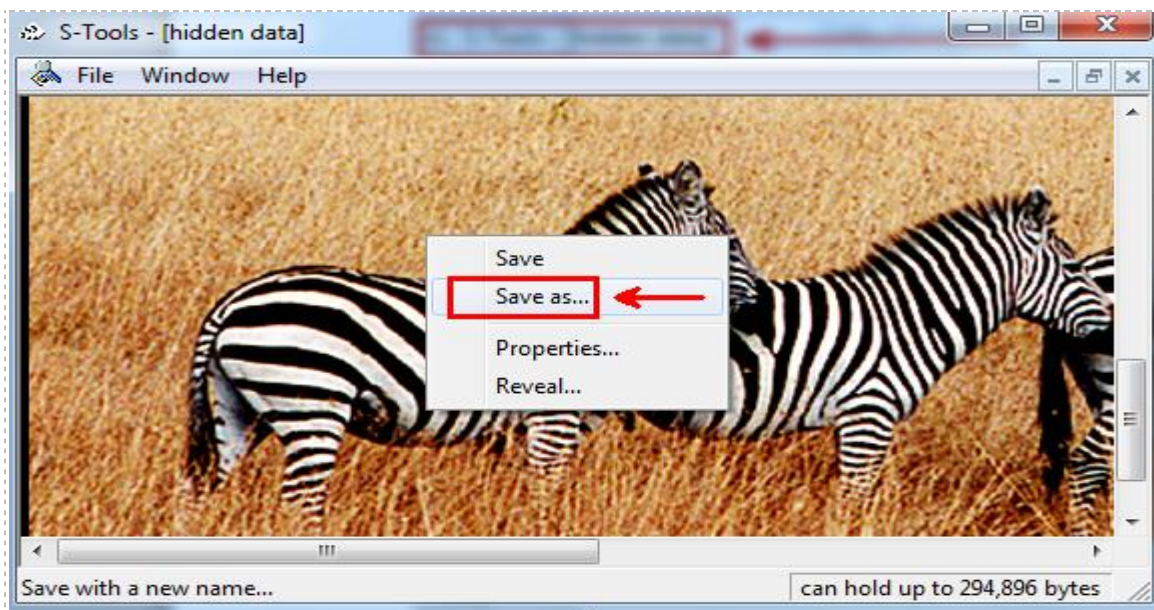


Figure 11: Saving the original-zebras.bmp picture with the embedded hidden msec.bmp picture

7. In the **Save As** Pop-up box:

- Verify the **Save in** location is the **steg** folder
- For the filename, type **zebras_with_hidden_msec.bmp**

Make sure you include the .bmp file extension.

- Verify the **Save as type** is **All Files (*.*)**
- Click the **Save** Button

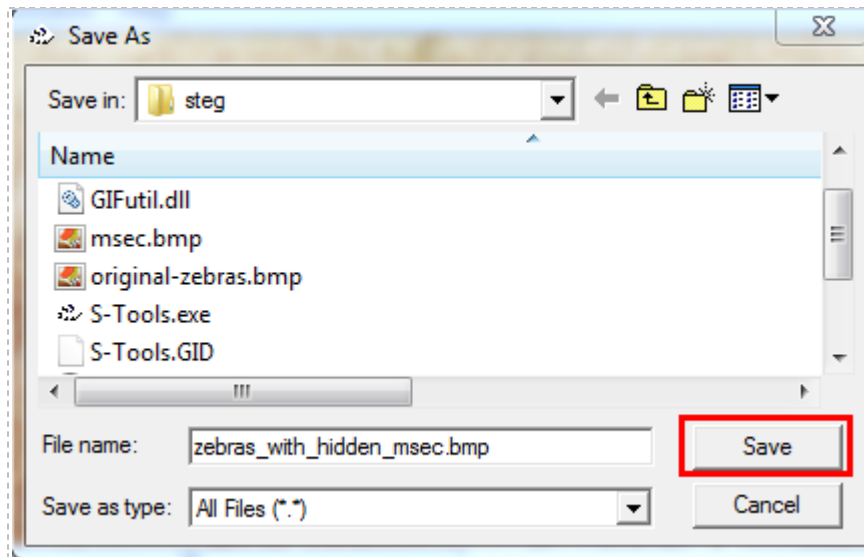


Figure 12: The Save as Dialog Box of S-Tools

Typically, the user would not indicate the name of the hidden picture file within the name of their picture. In this case, it is done to help you understand how S-Tools works.

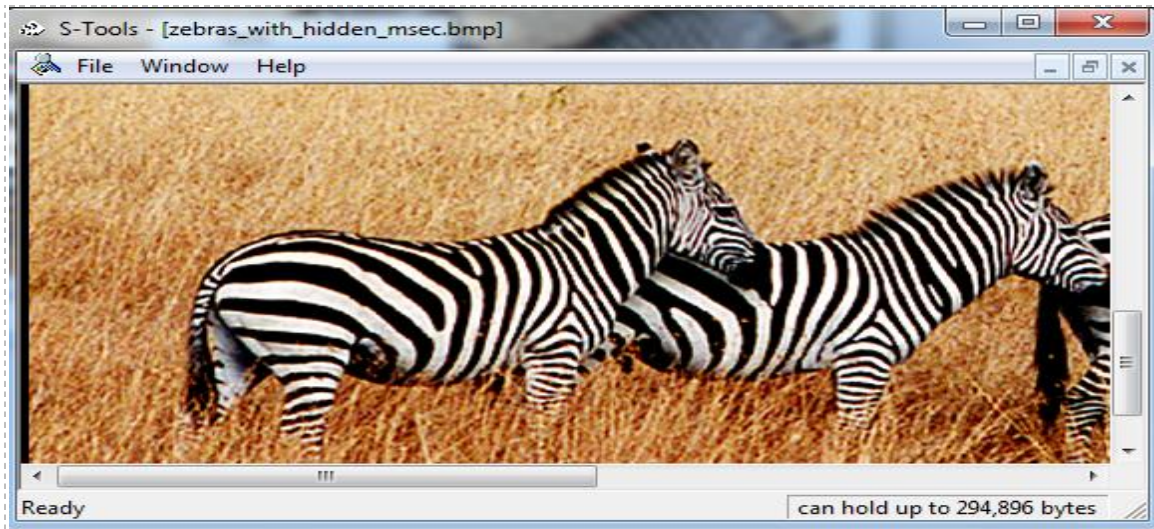


Figure 13: The Name of the New File that contains the Hidden MSEC bmp file

8. Close the S-Tools program by selecting **File** from the menu bar and selecting **Exit**.

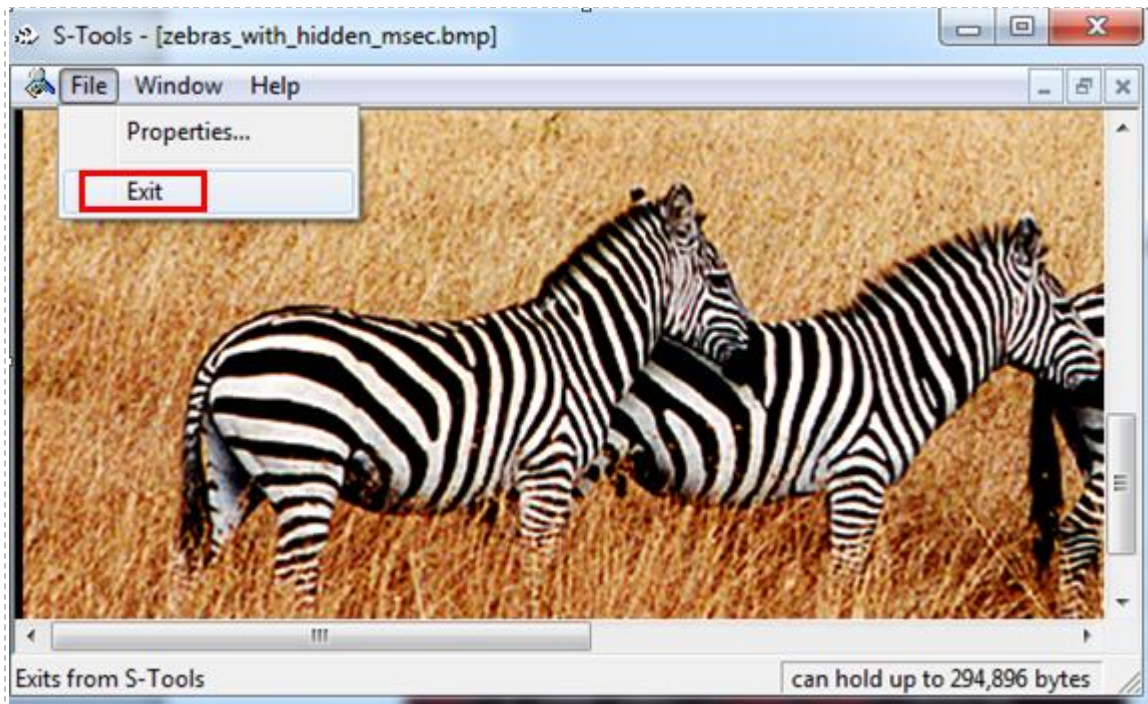


Figure 14: Closing S-Tools

9. Open the S-Tools program again, by double-clicking on the **S-Tools.exe** file.

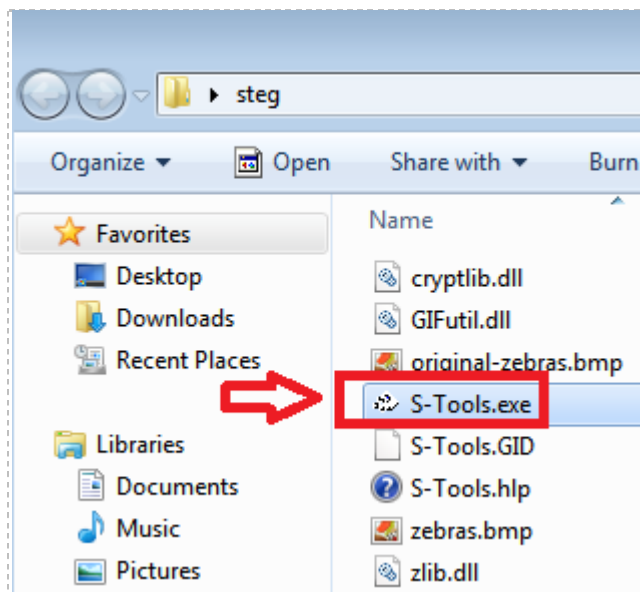


Figure 15: Double-Clicking on the S-Tools.exe file

- Click the single rectangle in the bottom left hand side of the screen to maximize the **Actions** window if needed. The **Actions** window should be maximized.

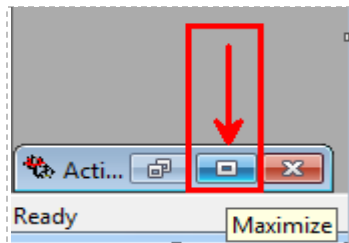


Figure 16: Maximize the Actions Window

- Drag the **zebras_with_hidden_msec.bmp** file from the **steg** folder located on the desktop into the S-Tools Actions window.

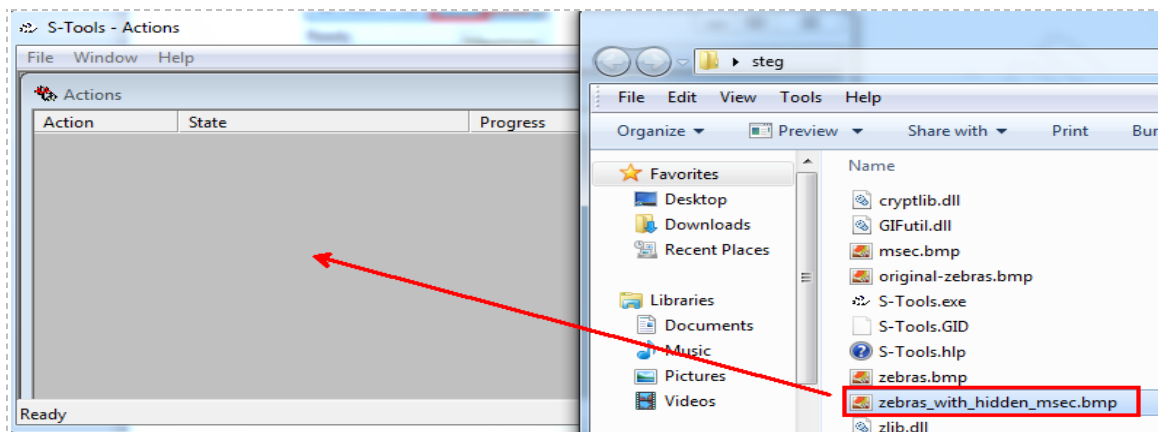


Figure 17: Dragging a File into the S-Tools Actions Windows

Verify that the file name **zebras_with_hidden_msec.bmp** is next to the word S-Tools.

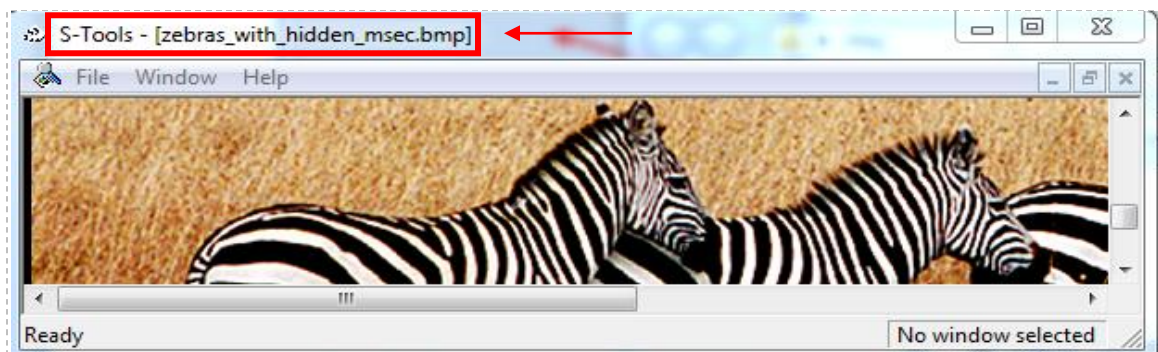


Figure 18: The zebras_with_hidden_msec.bmp file in the S-Tools Actions Window

12. To reveal the hidden picture, right-click on the zebra picture and select **Reveal**.

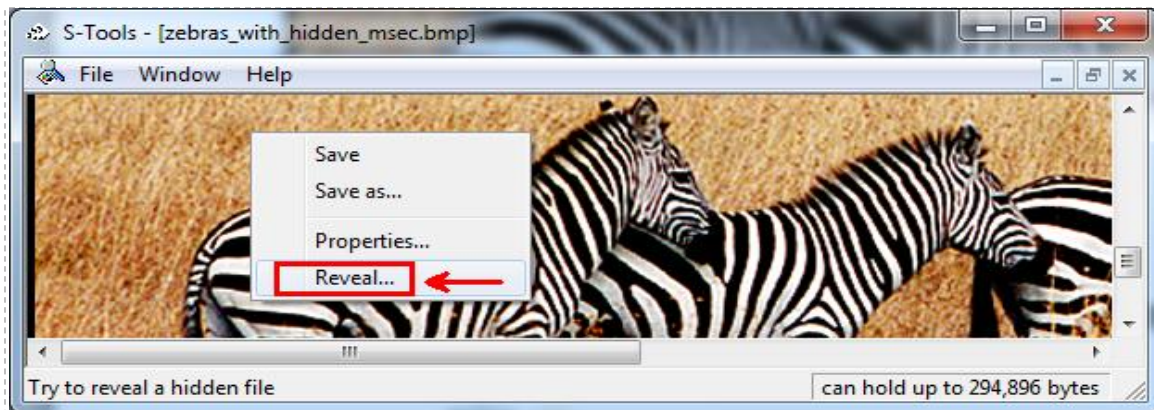


Figure 19: Revealing the Hidden Picture File

13. Type **password** in the **Passphrase** and **Verify passphrase** boxes. Leave **IDEA** for the **Encryption algorithm**. Click OK to reveal the hidden **msec.bmp** file.

The passphrase will be displayed as asterisks (*) when you type.

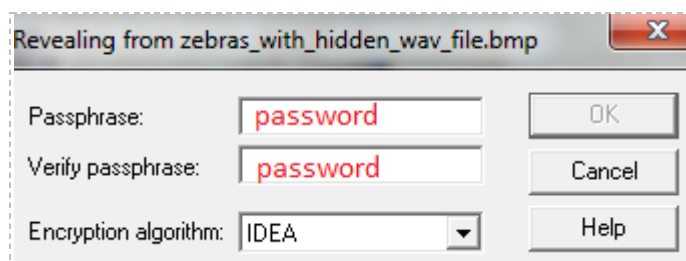


Figure 20: Typing the Password

The words, **S-Tools – [Revealed Archive]** should appear, along with a **Revealed files** window pane in which the name and size of the hidden file **msec.bmp** are displayed.

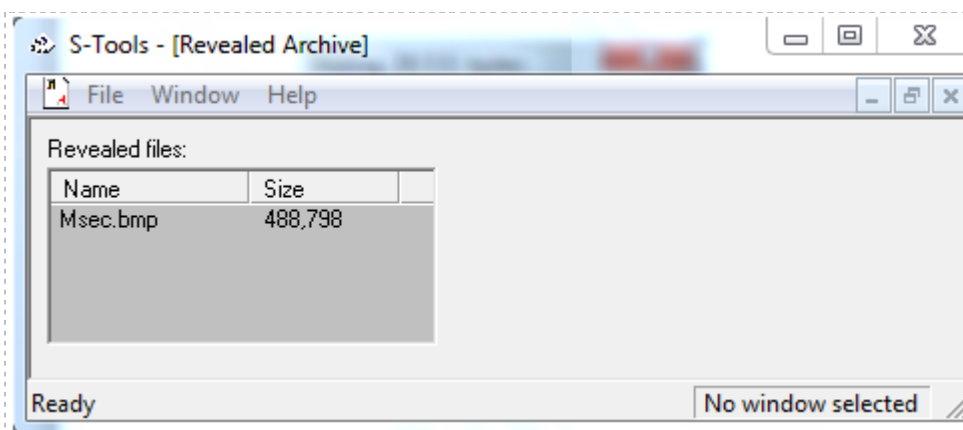


Figure 21: S-Tools – [Revealed Archive] Window

14. Right-click on the **Msec.bmp** file, and select **Save as...**

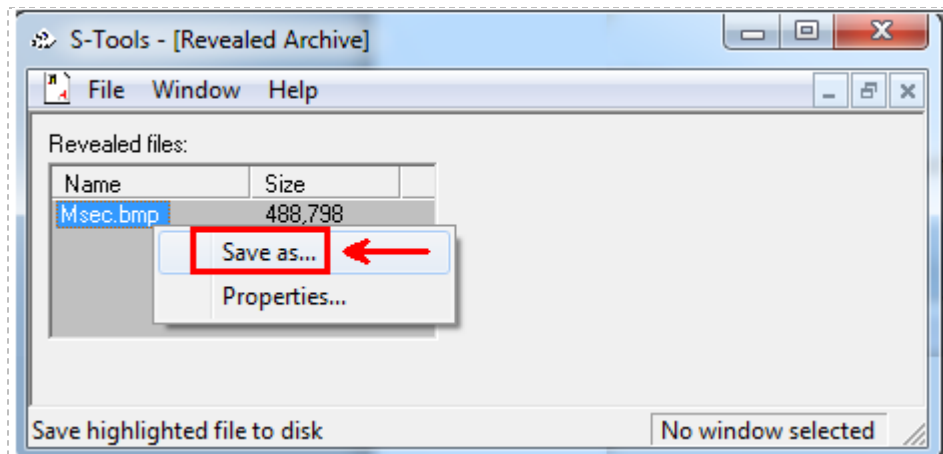


Figure 22: Saving the Hidden File within the Zebras Picture File

15. Type the following in the file name box: **my_hidden_file.bmp**. Verify that the **Save in** location is the **steg** folder and click **Save**.

Make sure you include the .bmp file extension.

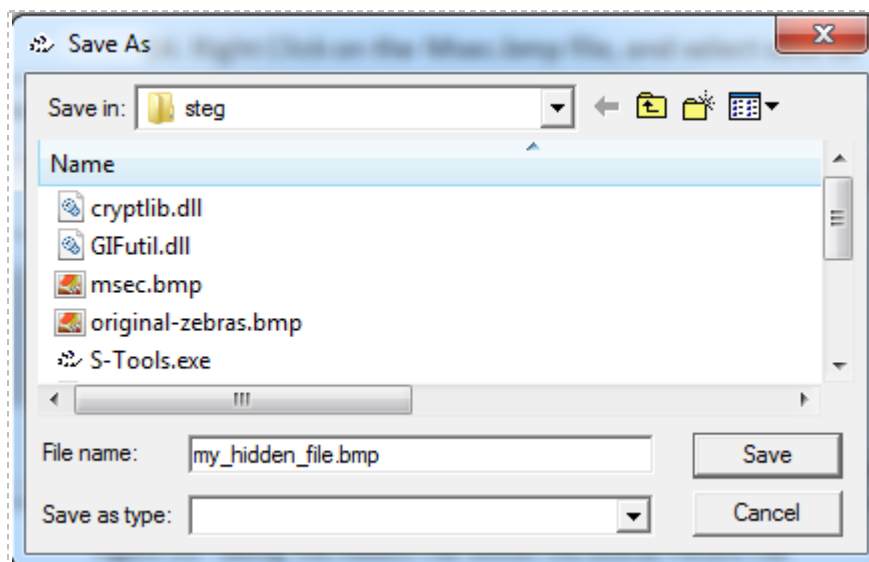


Figure 23: Saving the Hidden File

16. Double-click on the **my_hidden_file.bmp** in the **steg** folder on your desktop.

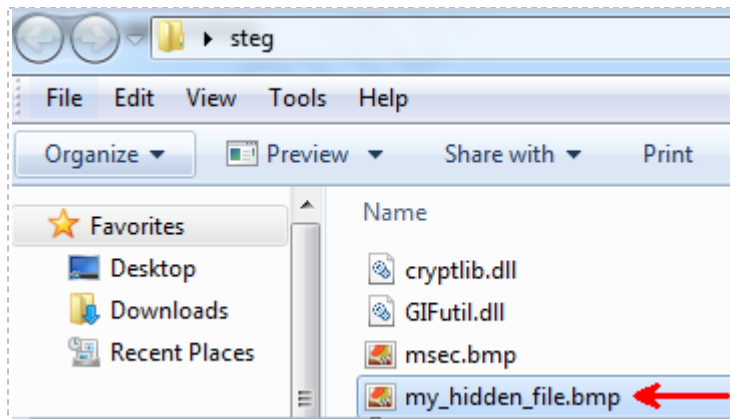


Figure 24: Opening the Revealed File

The picture that you hid within the original-zebras.bmp file should now be revealed.

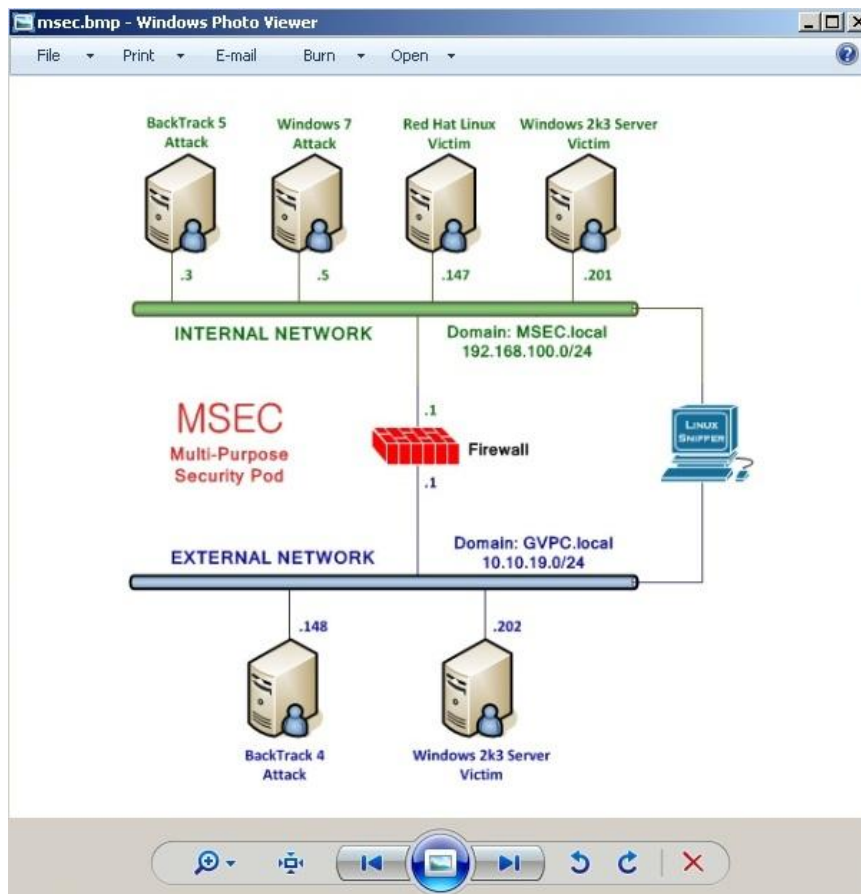


Figure 25: My-hidden_file.bmp is the msec.bmp file that was hidden within the original-zebras.bmp picture

17. Close the S-Tools program by selecting **File** from the menu bar and selecting **Exit**.

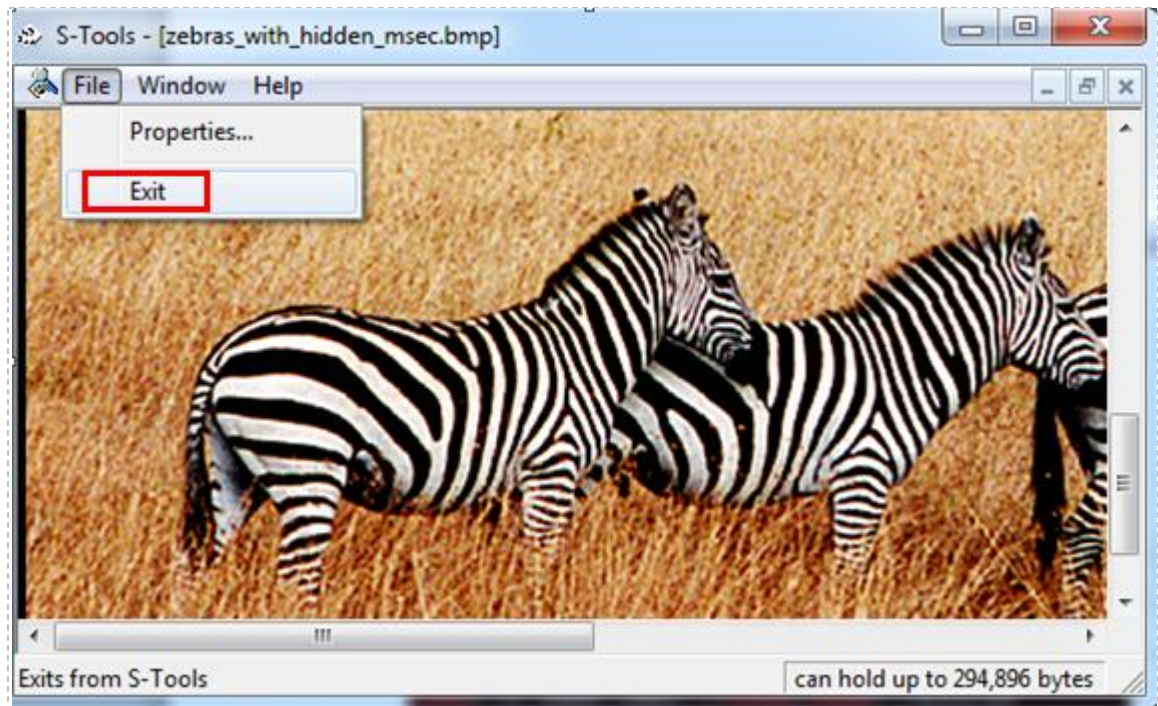


Figure 26: Closing S-Tools

1.2 Conclusion

S-Tools is a steganography tool that can be used to hide bitmap, GIF, and WAV files from plain view. The files will be embedded in a picture file. During the lab, we hid a picture named msec.bmp within another picture of zebras called original-zebras.bmp. Only users who know the password and encryption algorithm used will be able to reveal the hidden msec.bmp picture file.

1.3 Discussion Questions

1. What kind of files can be hidden with the S-Tools Steganography tool?
2. How is a hidden file revealed within the S-Tools program?
3. What is needed to reveal a hidden file in the S-Tools program?
4. What are some of the available encryption algorithms within S-Tools?

2 Hiding a Media File within a Picture Using S-Tools

S-Tools is a steganography tool that can be used to hide bitmap, GIF, and wave files from plain view. The files will be embedded in a picture file. There is a popular saying that “a picture can say a thousand words.” In this task, we will accomplish just that, by hiding a WAV file, which is a sound file, in a picture. That WAV file could be a message of someone speaking a thousand words, a secret message from one person to another, or it could be even be a music file.

2.1 Hiding a WAV file with S-Tools

Open S-Tools

1. If necessary, double-click on the **steg** folder on your desktop. Open the **S-Tools.exe** file.

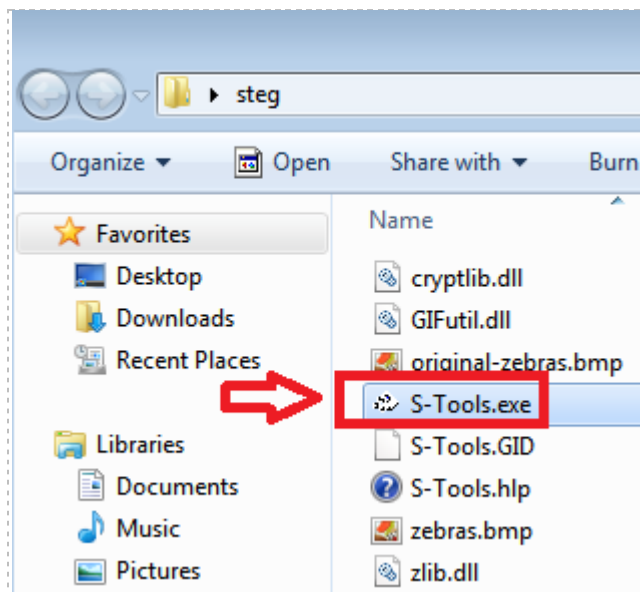


Figure 27: Double Clicking on the S-Tools.exe file

2. Click the single rectangle in the bottom left hand side of the screen to maximize the **Actions** window, if needed. The **Actions** window should be maximized.

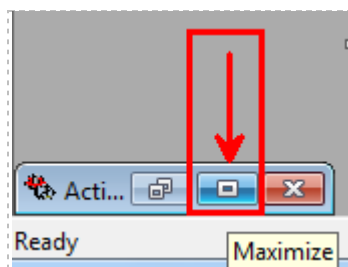


Figure 28: Maximize the Actions Window

3. Drag the **original-zebras.bmp** file from the **steg** folder into the S-Tools **Actions** window.

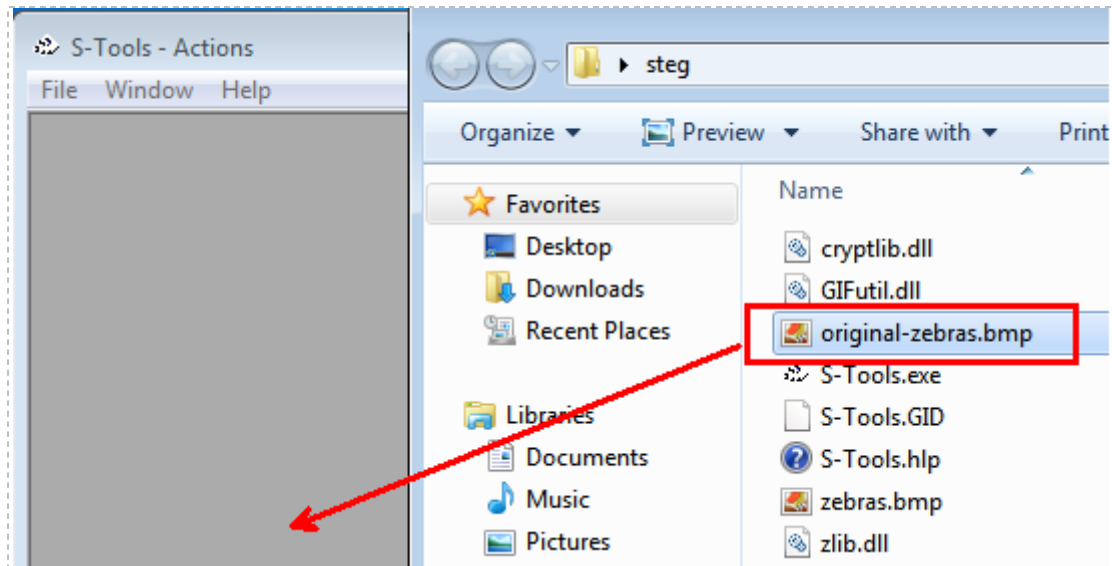


Figure 29: Dragging a File into the S-Tools Actions Windows

4. Drag the **Windows_Ding.wav** file on to the **original-zebras.bmp** picture in the S-Tools Actions window. After the file is in the window, you will see a box appear. This box asks for a **passphrase**, **passphrase verification**, and the **Encryption algorithm**.

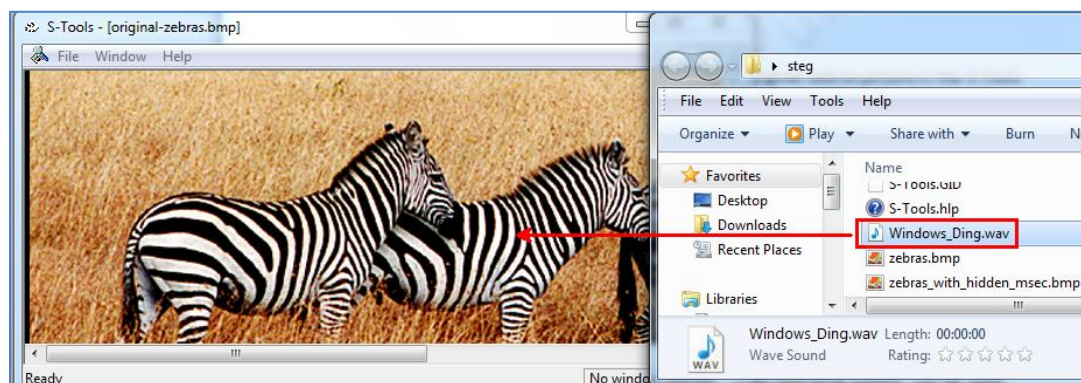


Figure 30: Hiding the Windows_Ding.wav file within the original-zebras.bmp file.

5. Type **password** in the **Passphrase** and **Verify passphrase** boxes. Leave **IDEA** for the **Encryption** algorithm. Click the OK button to hide **Windows_Ding.wav**.

The passphrase will be displayed as asterisks (*) when you type.

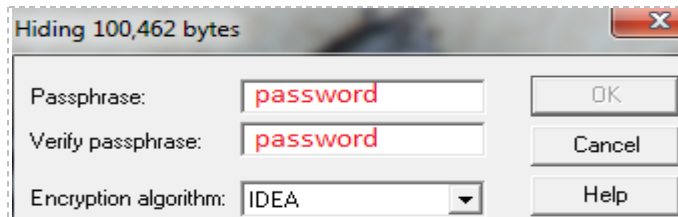


Figure 31: Typing the Password

Now, in the top left hand corner of the picture, the phrase **[hidden data]** will appear, indicating that digital information has been hidden in the original-zebras.bmp file.

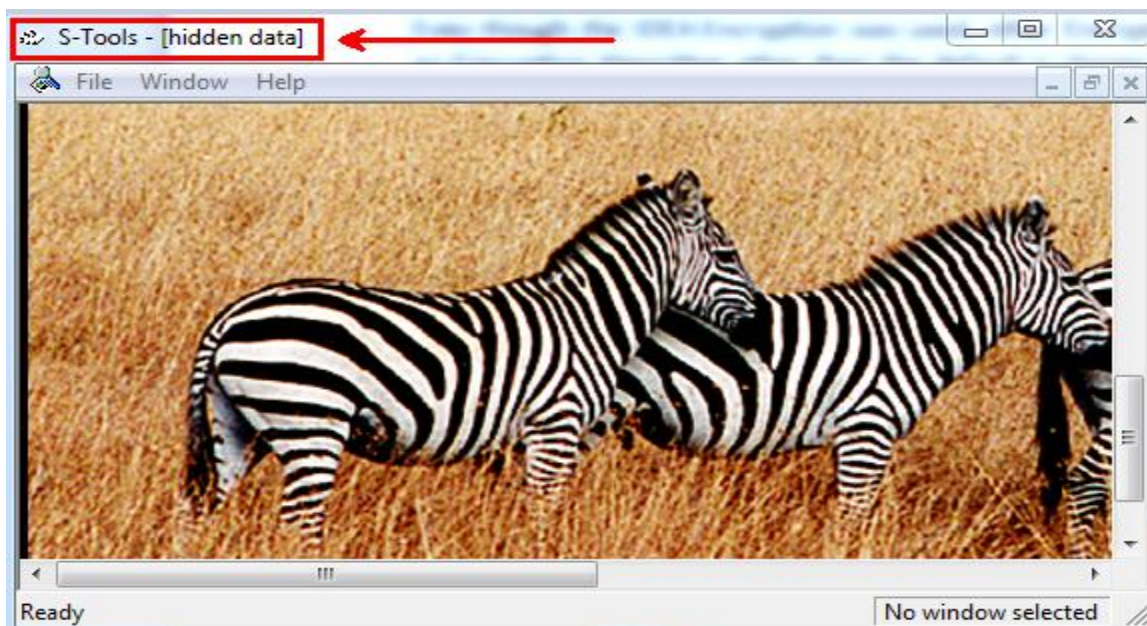


Figure 32: The Windows_Ding.wav file is hidden data within the original-zebras.bmp picture

6. To save the **original-zebras.bmp** file with the hidden **Windows_Ding.wav** file, right-click anywhere within the picture, and select **Save as...** from the menu list.

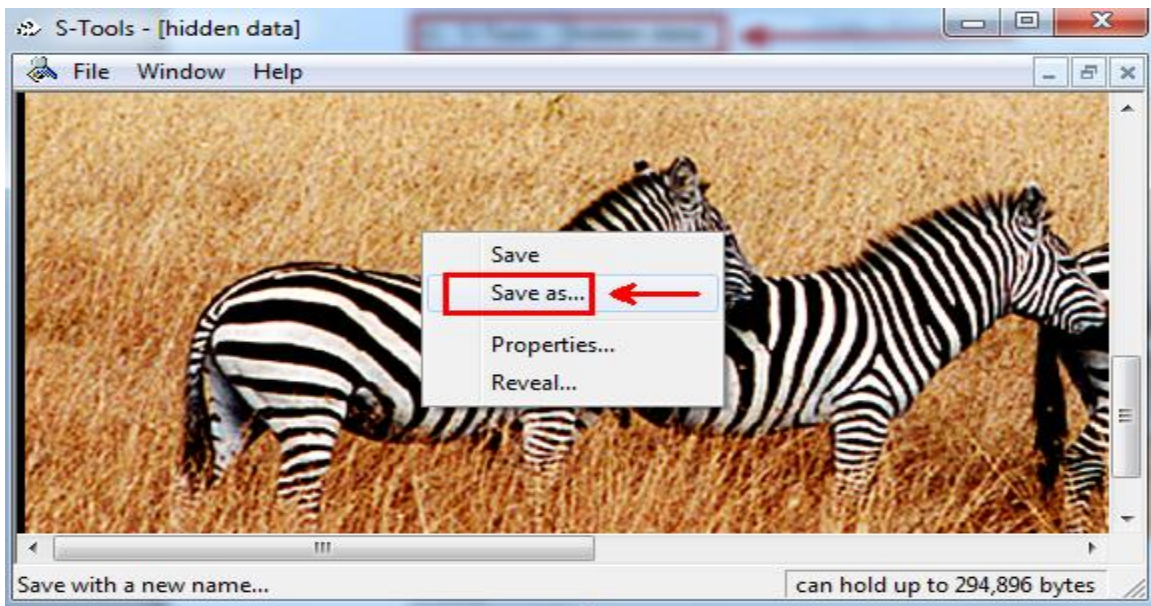


Figure 33: Saving the original-zebras.bmp picture with the embedded hidden Windows_Ding.wav file

7. In the **Save As Pop-up** box:

- Verify the **Save in** location is the **steg** folder
- For the filename, type **zebras_with_hidden_wav_file.bmp**

Make sure you include the .bmp file extension.

- Verify the **Save as type** says **All Files (*.*)**
- Click the **Save** Button

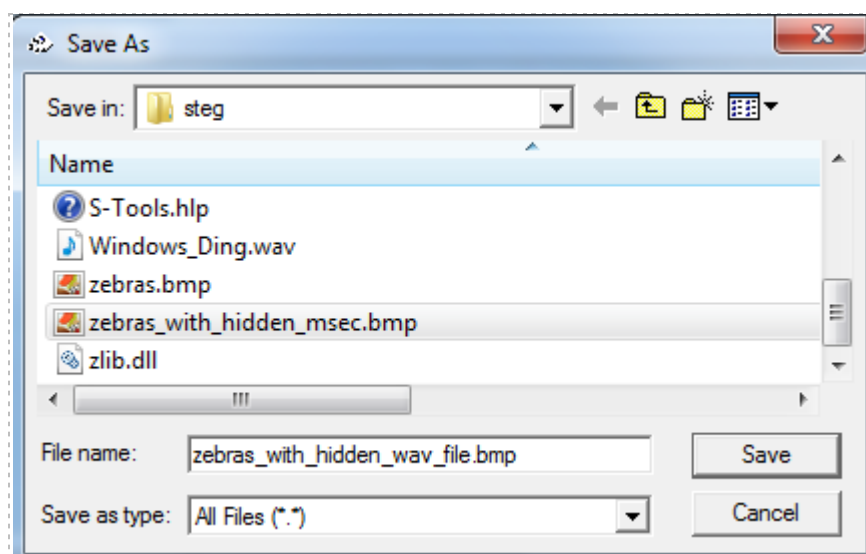


Figure 34: The Save As Dialog Box of S-Tools

Normally, the user would not indicate the name of the hidden picture file within the name of their picture. In this case, it is done to help you understand how S-Tools works.

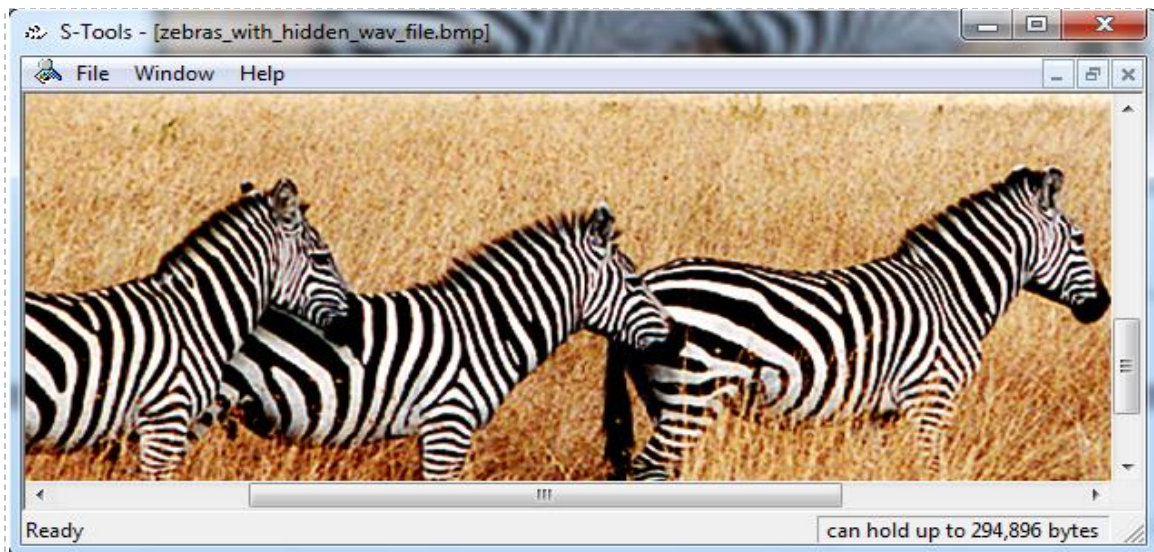


Figure 35: The Name of the New File that contains the Hidden Windows_Ding.wav file

8. Close the S-Tools program by selecting **File** from the menu bar and selecting **Exit**.

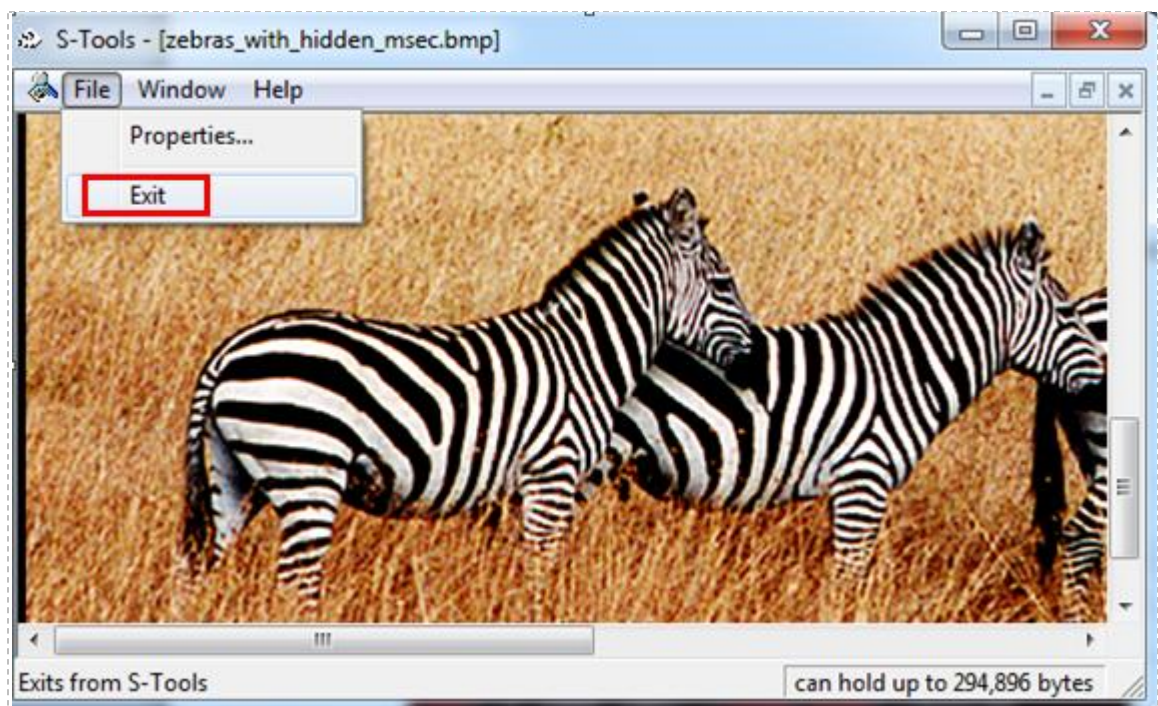


Figure 36: Closing S-Tools

9. Open the S-Tools program again by double-clicking on the **S-Tools.exe** file.

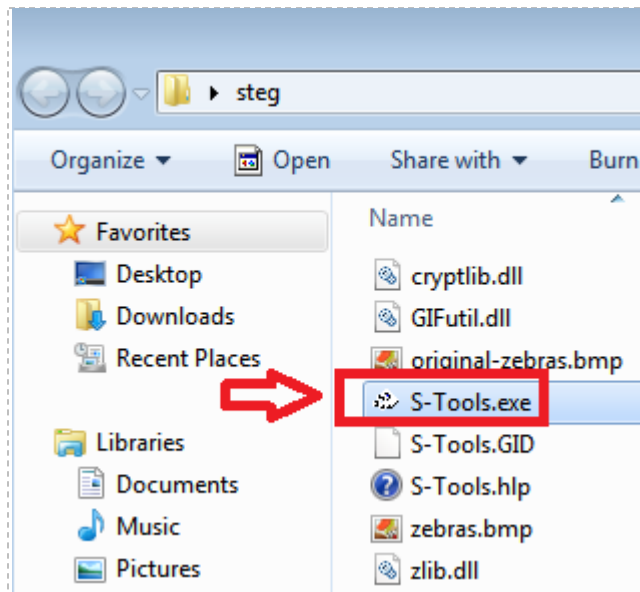


Figure 37: Double Clicking on the S-Tools.exe file

10. Click the single rectangle in the bottom left hand side of the screen to maximize the **Actions** window if needed. The **Actions** window should be maximized.

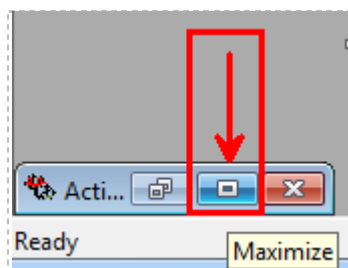


Figure 38: Maximize the Actions Window

11. Drag the **zebras_with_hidden_wav_file.bmp** file from the **steg** folder located on the desktop into the S-Tools Actions window.

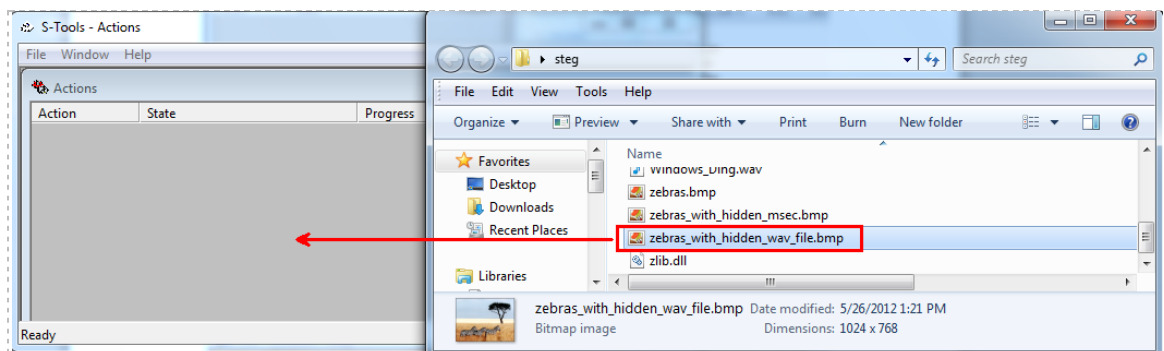


Figure 39: Dragging a File into the S-Tools Actions Windows

Verify that the file name **zebras_with_hidden_wav_file.bmp** is next to the word S-Tools.

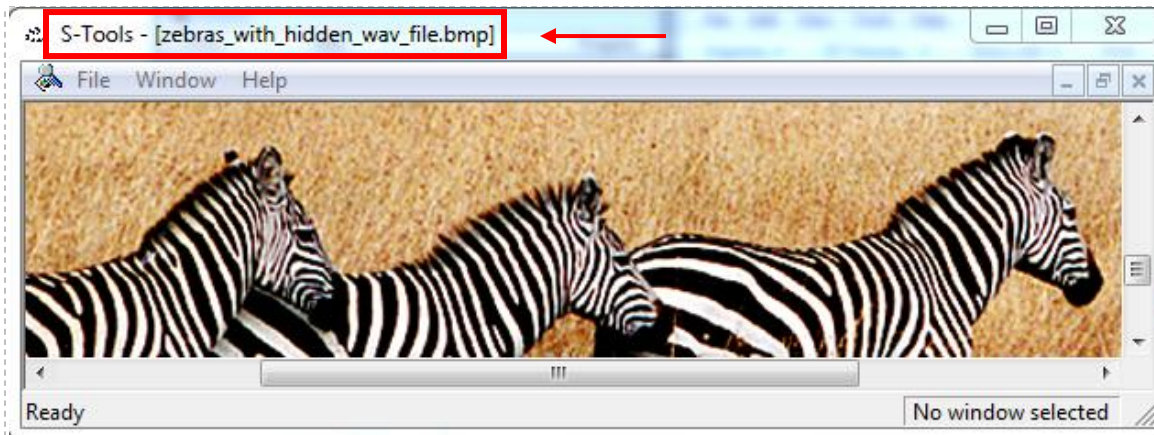


Figure 40: The zebras_with_hidden_wav_file in the S-Tools Actions Window

12. To reveal the hidden wav file, right-click on the zebra picture and select **Reveal**.

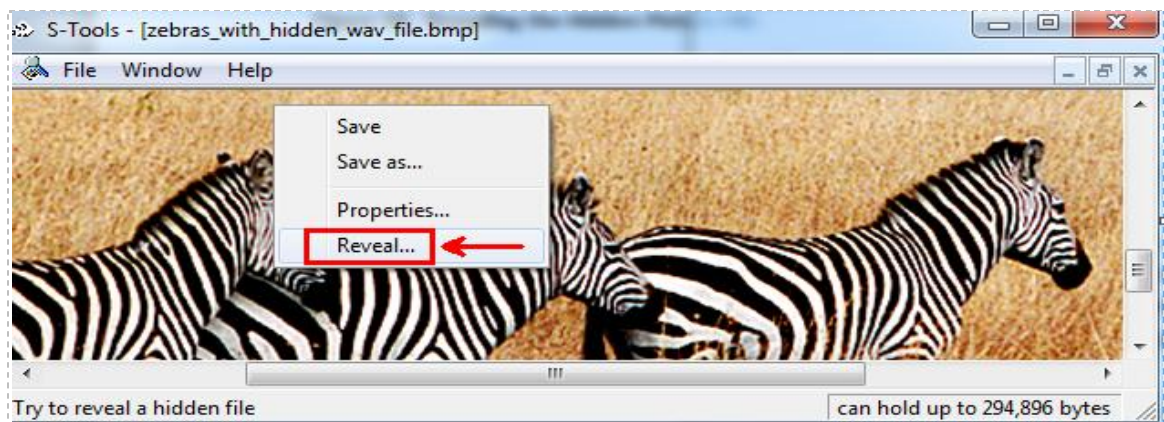


Figure 41: Revealing the Hidden Picture File

13. Type **password** in the **Passphrase** and **Verify passphrase** boxes. Leave **IDEA** for the **Encryption algorithm**. Click the OK button to reveal the hidden WAV file.

The passphrase will be displayed as asterisks (*) when you type.

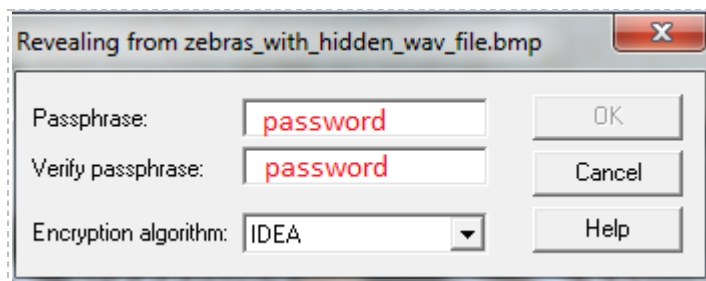


Figure 42: Typing the Password

The words, **S-Tools – [Revealed Archive]** should appear, along with a **Revealed files** window pane in which the name and size of the hidden **Windows_ding.wav** file are displayed.

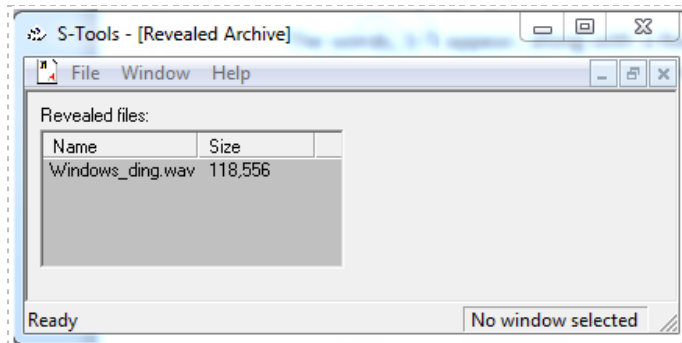


Figure 43: S-Tools – [Revealed Archive] Window

14. Right-click on the **Windows_ding.wav** file, and select **Save as...**

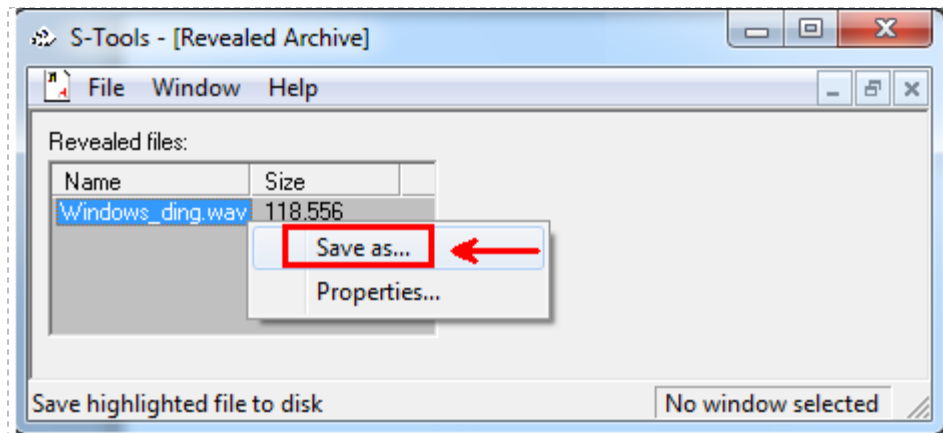


Figure 44: Saving the Hidden File within the Zebras Picture File

15. Type the following in the file name box: **my_hidden_wav_file.wav**. Verify that the **Save in** location is the **steg** folder and click **Save**.

Make sure you include the .wav file extension.

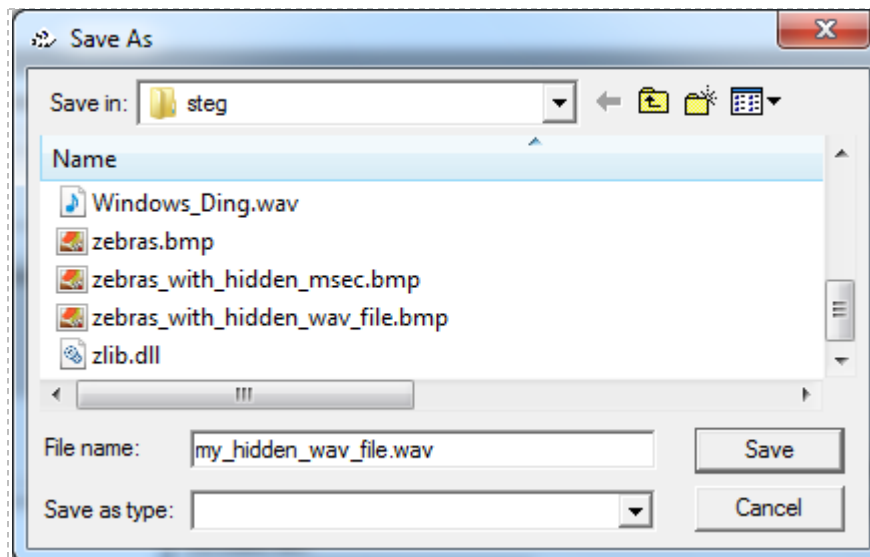


Figure 45: Saving the Hidden WAV File

16. Close the **S-Tools.exe** by selecting **File**, then **exit**.
17. View the **my_hidden_wav_file.wav** folder on your desktop.

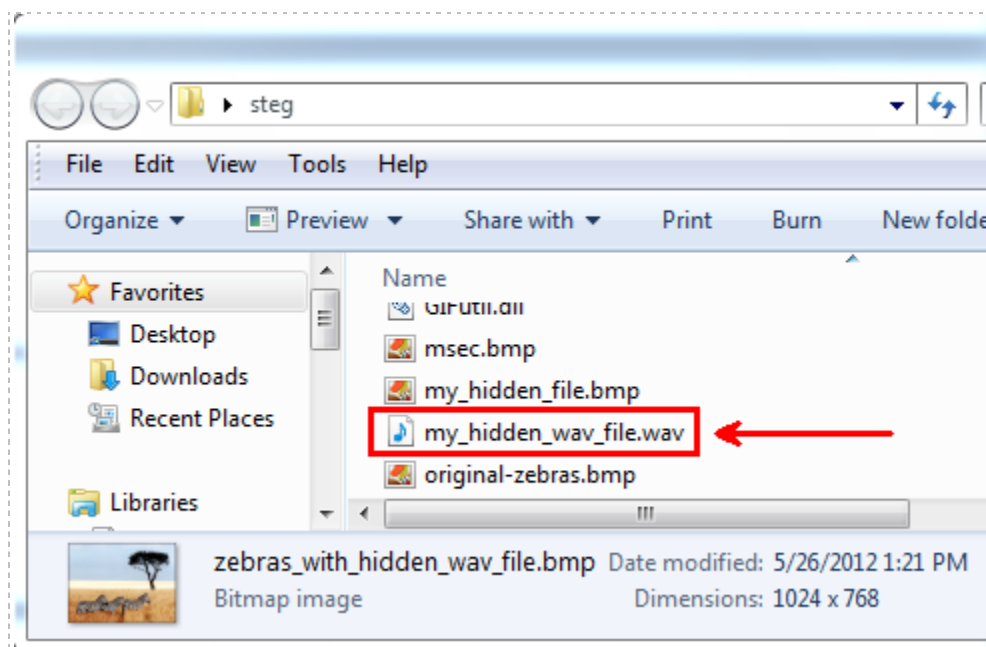


Figure 46: Viewing the Revealed File

If we have an audio device installed on our system, we can listen to the messages and sounds within the WAV file. This WAV file is from the Windows operating system.

2.2 Conclusion

S-Tools is a stenography tool that can be used to hide bitmap, GIF, and wave files from plain view. The files will be embedded in a picture file. During the lab, we hid a sound file called Windows_Ding.wav within a picture of zebras. Only users who know the password and encryption algorithm used will be able to reveal the hidden Windows_Ding.wav sound file. This is a great way to transmit secret messages.

2.3 Discussion Questions

1. What kind of sound files can be hidden with the S-Tools Stenography tool?
2. What kind of picture files can be hidden with the S-Tools Stenography tool?
3. How do you hide a sound file in the S-Tools program?
4. How do you reveal a hidden sound file in the S-Tools program?

3 Revealing Hidden Data Using S-Tools

In Task 1, we hid a bitmap MSEC picture within the original-zebras picture. Then, in Task 2, we hid a Windows_Ding WAV file within the original-zebras picture. In this task, we will reveal hidden BMP, WAV, and GIF files within various pictures. These techniques can be used to send secret messages to another person. Anyone who receives the original-zebras.bmp picture and does not have S-Tools, the password, or the encryption algorithm will not be able to view the hidden content in the picture.

3.1 Revealing Hidden Data

Open S-Tools

1. If necessary, double-click on the **steg** folder on your desktop. Open the **S-Tools.exe** file.

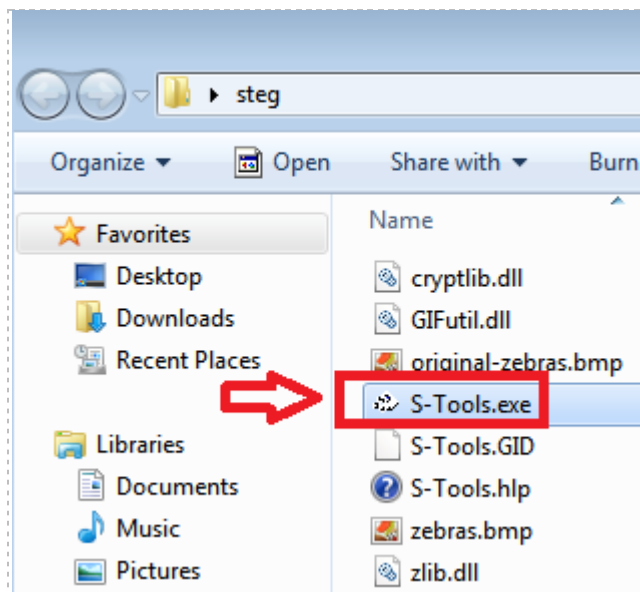


Figure 47: Double Clicking on the S-Tools.exe file

2. Click the single rectangle in the bottom left hand side of the screen to maximize the **Actions** window, if needed. The **Actions** window should be maximized.

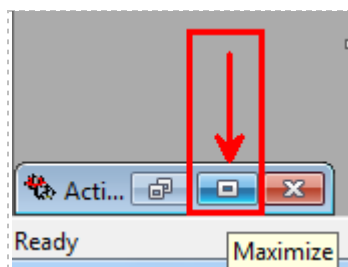


Figure 48: Maximize the Actions Window

3. Drag the **picture1.bmp** file from the **steg** folder into the S-Tools **Actions** window.

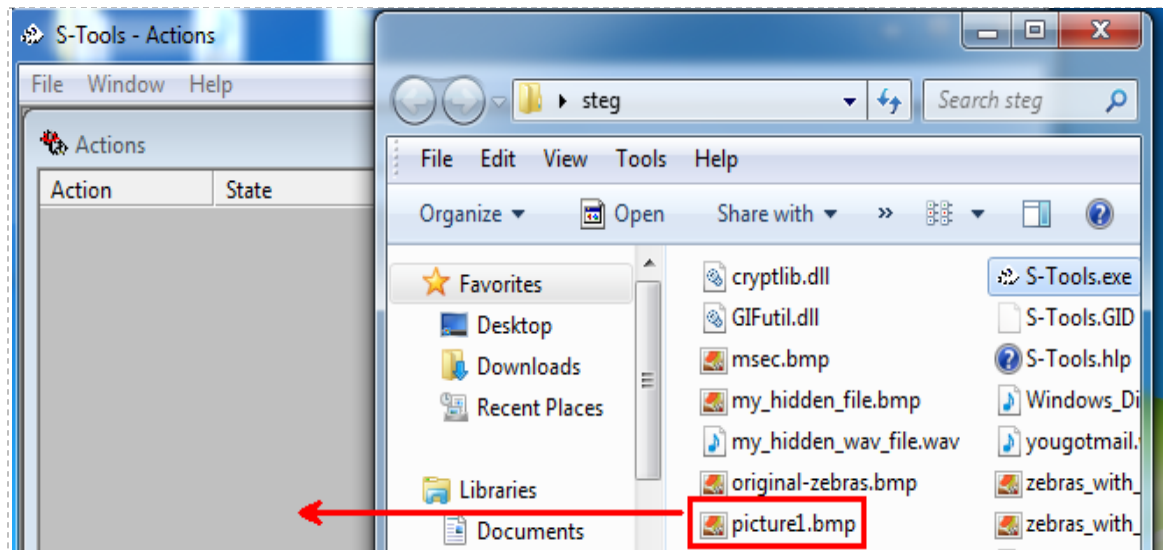


Figure 49: Dragging a File into the S-Tools Actions Windows

4. To reveal the hidden **WAV** file, right-click on **picture1.bmp** picture and select **Reveal**.

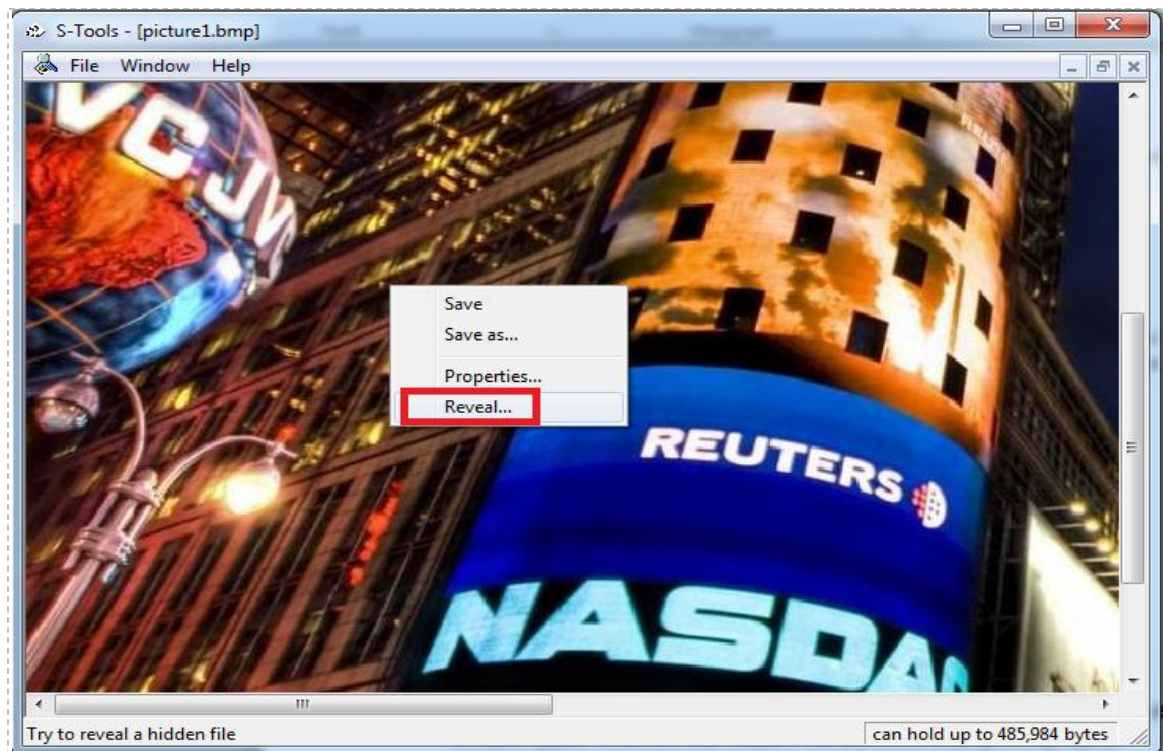


Figure 50: Revealing the Hidden Picture File

5. Type **password** in the **Passphrase** and **Verify passphrase** boxes Leave **IDEA** for the **Encryption algorithm**. Click the OK button to reveal the hidden BMP file.

The passphrase will be displayed as asterisks (*) when you type.

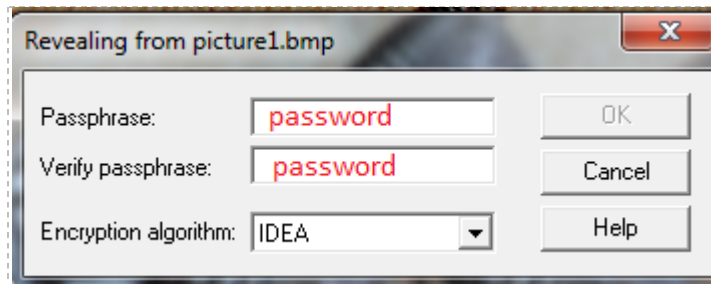


Figure 51: Typing the Password

The words, **S-Tools – [Revealed Archive]** should appear, along with a **Revealed files** windowpane in which the hidden file **Black_arts.bmp** is displayed.

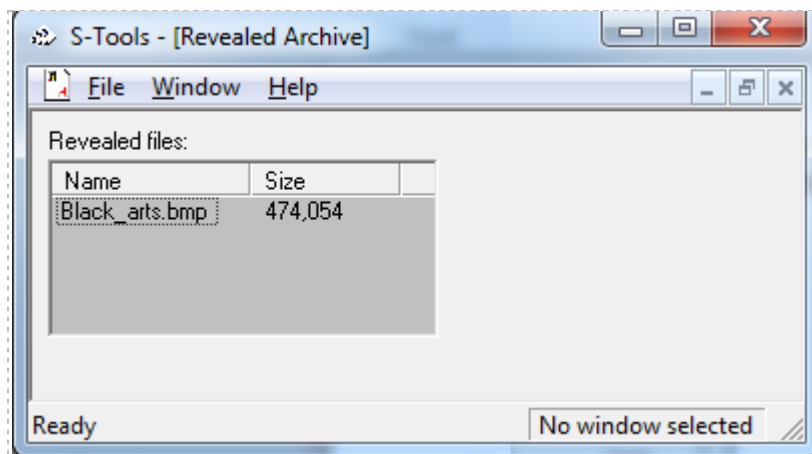


Figure 52: S-Tools – [Revealed Archive] Window

6. Right-click on the **Black_arts.bmp**, and select **Save as...**

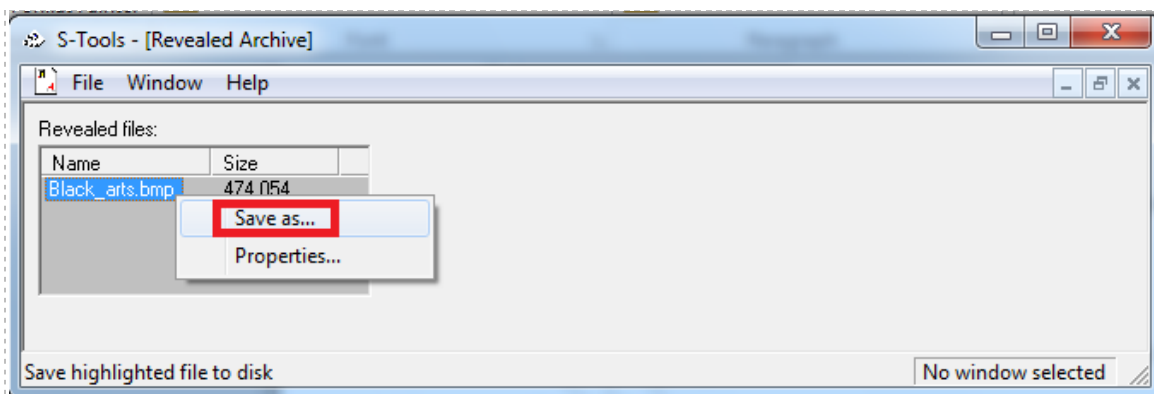


Figure 53: Saving the Hidden File within the Picture File

7. Change the **Save in** location to **Desktop** and click **Save**.

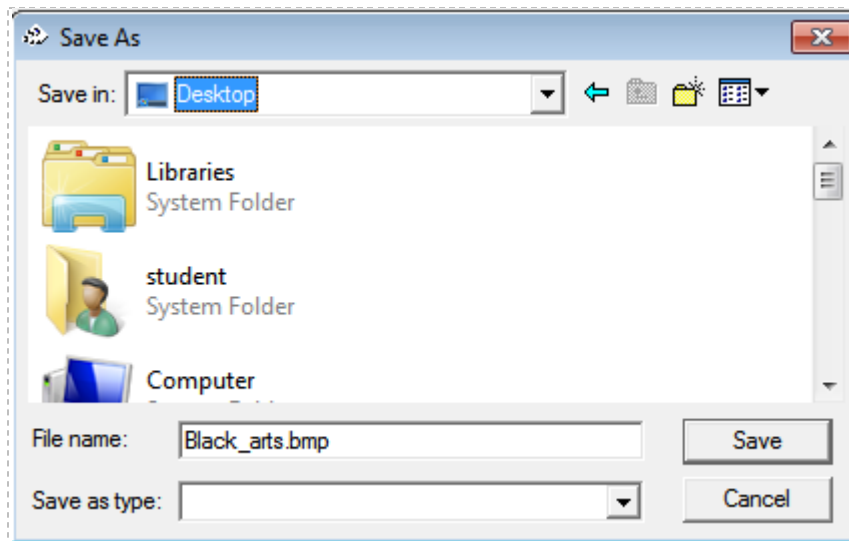


Figure 54: Saving the Hidden File to the Desktop

8. View the picture on your desktop by double-clicking on the **Black_arts.bmp** file.

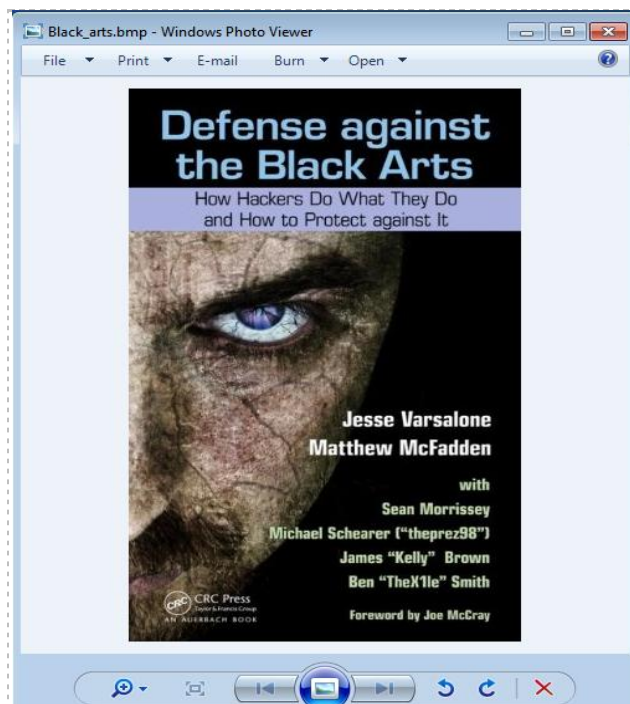


Figure 55: Viewing the Hidden Picture File

9. Close S-Tools by clicking **File**, then **exit**. Close the **steg** window.

3.2 Conclusion

S-Tools is a stenography tool that can be used to hide bitmap, GIF, and WAV files from plain view. Bitmap, GIF, and WAV file formats can be embedded in a GIF or BMP picture file, or a WAV file. When someone receives a file with one of these format types, it is very difficult to detect the presence of Stenography. Only users with the Stenography tool who know the password and Encryption algorithm will be able to open the file.

3.3 Discussion Questions

1. Use the same procedure in steps 1-9 to identify the name of the hidden file in picture2.bmp.
2. Use the same procedure in steps 1-9 to identify the name of the hidden file in picture3.bmp.
3. Use the same procedure in steps 1-9 to identify the name of the hidden file in picture4.bmp.
4. Use the same procedure in steps 1-9 to identify the name of the hidden file in picture5.bmp.

References

1. S-Tools Download:
<http://www.cs.vu.nl/~ast/books/mos2/steg.zip>
2. Steganography Explained:
<http://www.garykessler.net/library/steganography.html>
3. MP3Stego:
<http://www.petitcolas.net/fabien/steganography/mp3stego/>
4. Hide4PGP:
<http://www.heinz-repp.onlinehome.de/Hide4PGP.htm>
5. List of Steganography Tools:
<http://www.jitc.com/Steganography/toolmatrix.htm>