Lab – Using Steganography

**Additional Note:** Yellow highlighted text indicates all of my answers.

*(672021159)*

1. Objectives

Use steganography to hide a document within a JPEG file.

1. Background / Scenario

Steghide is an open source steganography program that hides data in various types of files such as audio and image files. You are going to hide a data file within an image file.

1. Required Resources

* PC with Ubuntu 16.04 Desktop LTS installed in a VirtualBox or VMware virtual machine
* 
  1. Open a terminal window in Ubuntu.
     1. Log in to Ubuntu using the following credentials:

User: **cisco**

Password: **password**

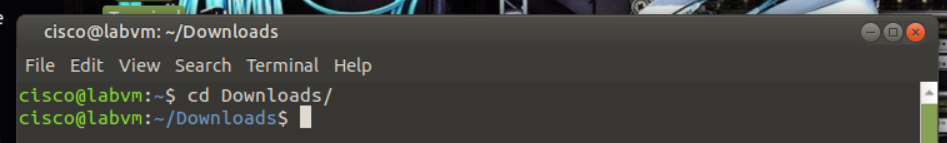


* + 1. Click on the terminal icon to open a terminal.



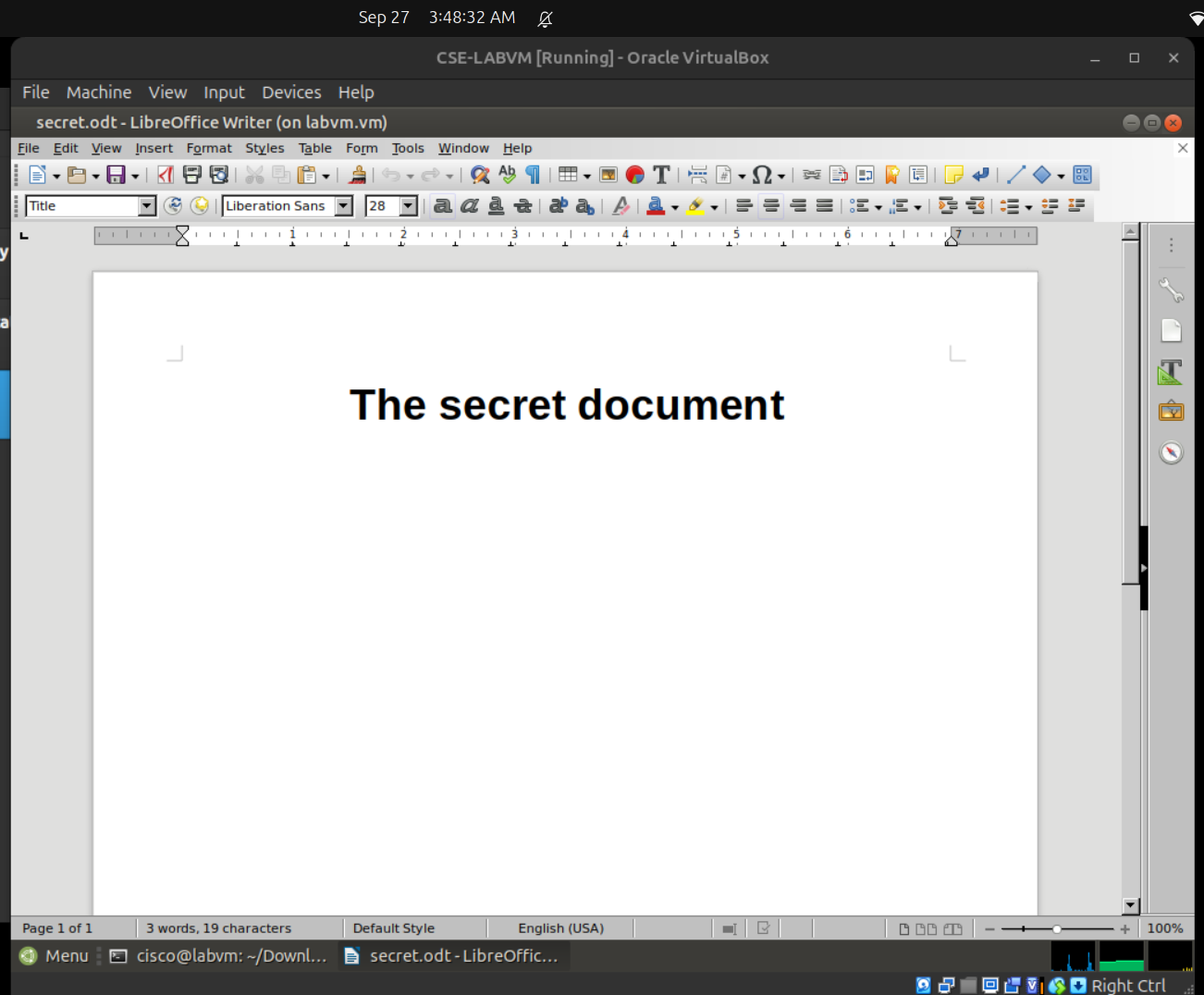
* 1. Run Steghide.
     1. At the command prompt, enter the following command to change to the **Downloads** directory:

cisco@ubuntu:~$ **cd Downloads/**



* + 1. Enter **libreoffice secret.odt &** at the prompt.

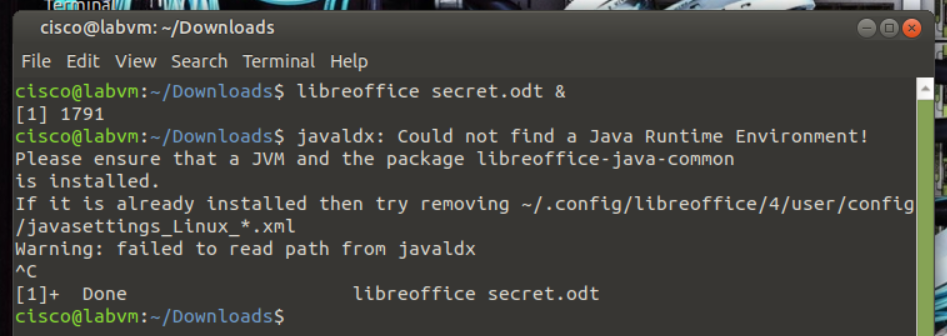
cisco@ubuntu:~/Downloads$ **libreoffice secret.odt &**



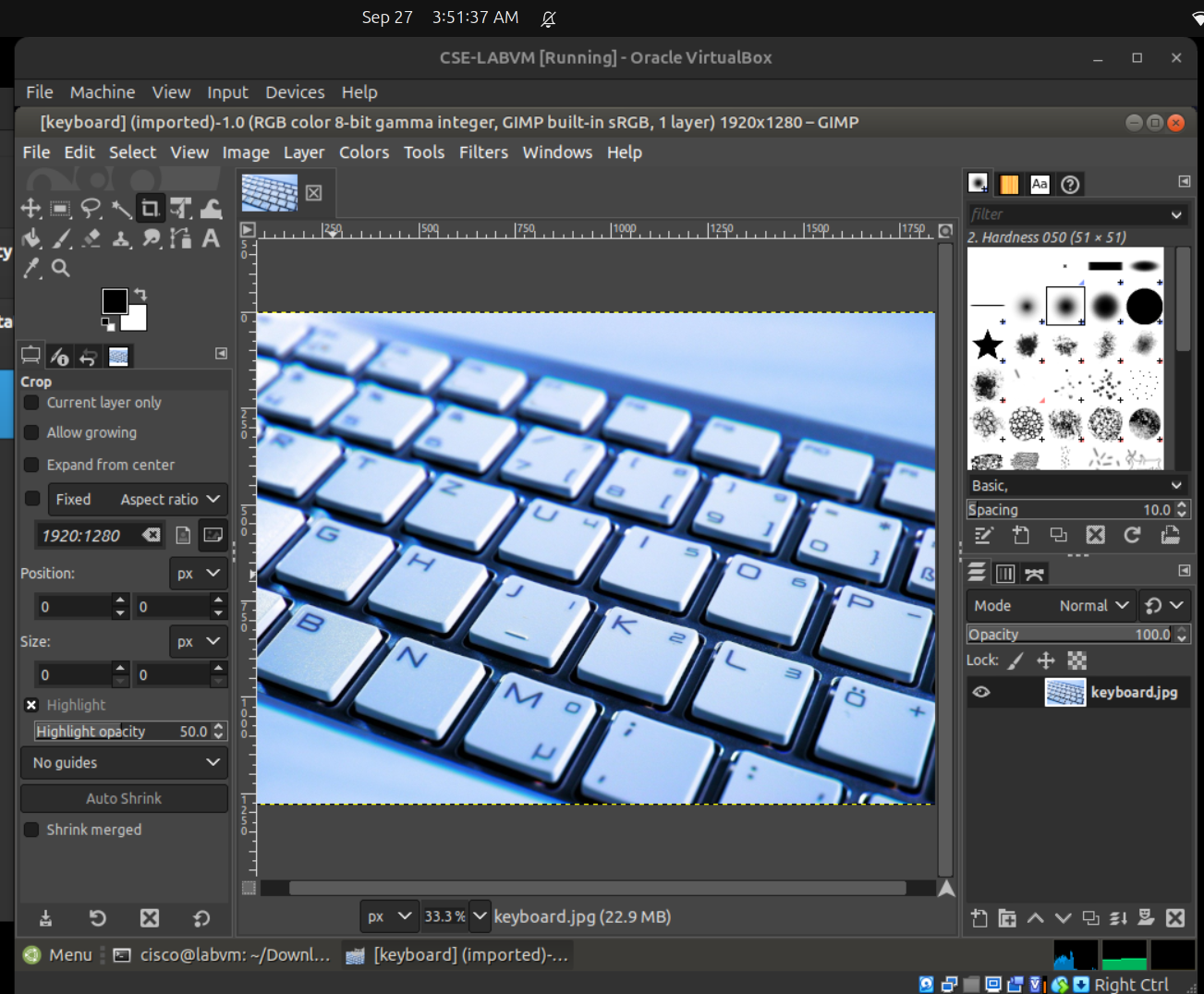
What is the message in the **secret.odt**?

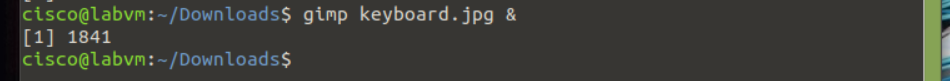
*The secret document*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

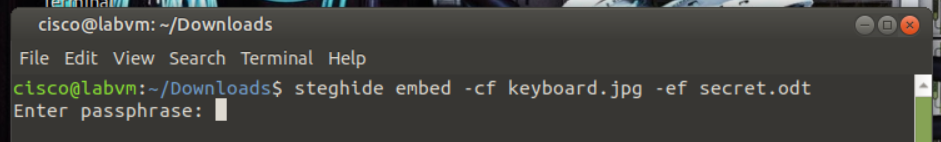
* + 1. Close the **secret.odt** file when done.
    2. 
    3. Enter **gimp keyboard.jpg &** at the prompt to view the image file

cisco@ubuntu:~/Downloads$ **gimp keyboard.jpg &**

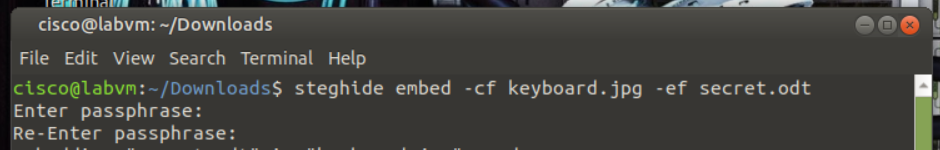


* + 1. Close the **keyboard.jpg** file when done.
    2. 
    3. At the command prompt, enter the following command :

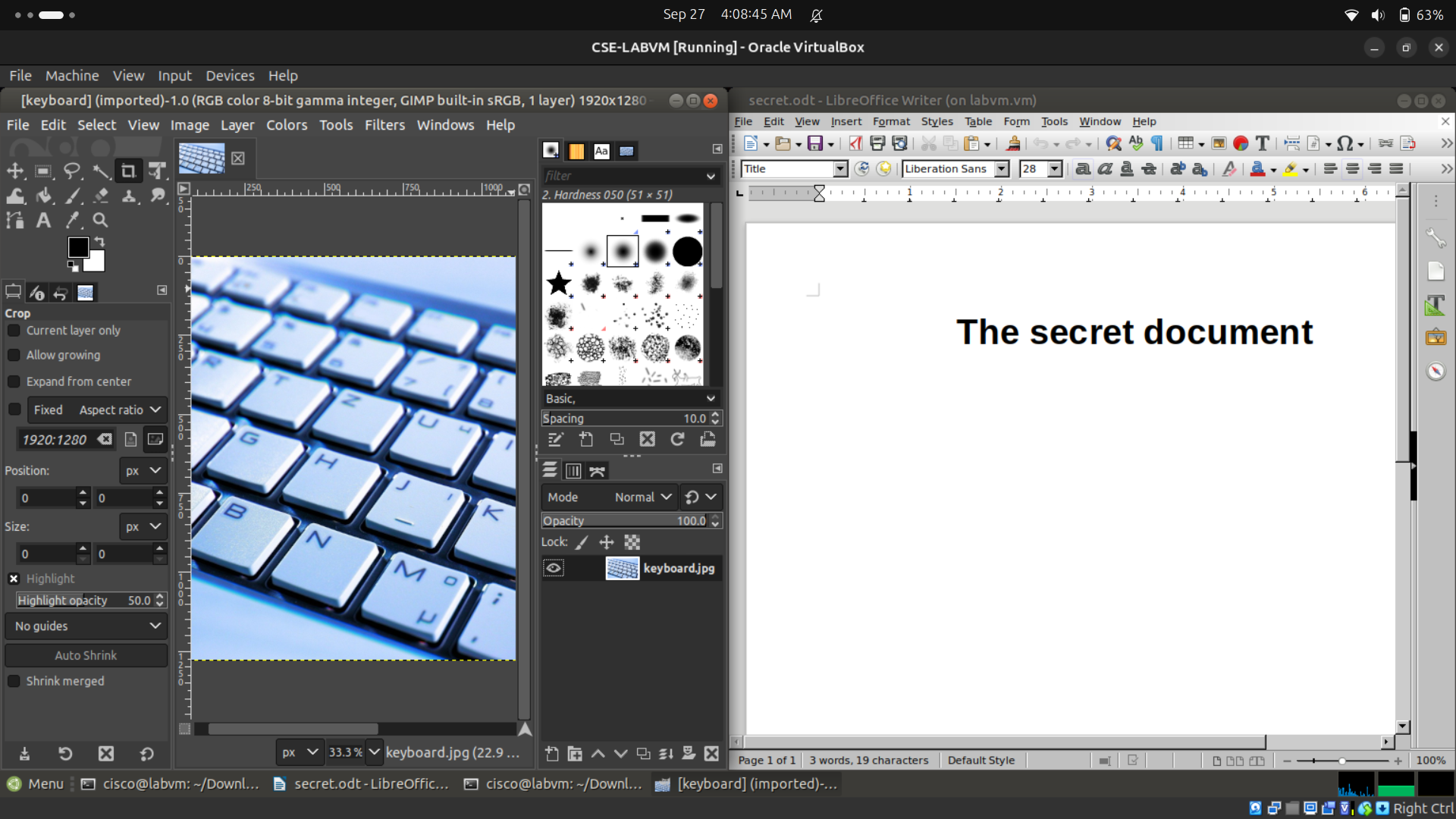
cisco@ubuntu:~/Downloads$ **steghide embed -cf keyboard.jpg -ef secret.odt**



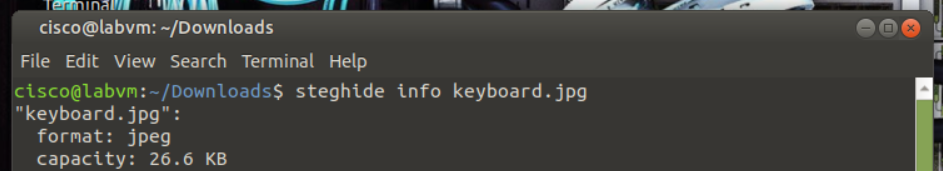
This command takes the jpeg file called “keyboard.jpg” and uses it as a carrier to embed the document, **secret.odt**, into it.

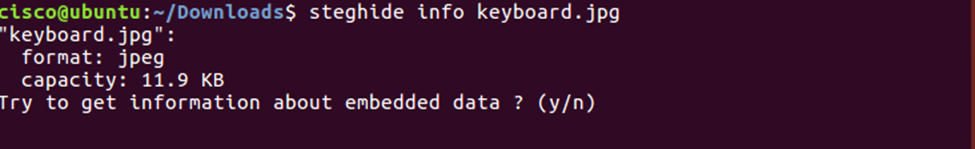
* + 1. When prompted for a passphrase, use **Cisco**. Re-enter the passphrase when prompted.
    2. 



* + 1. You have embedded the document, **secret.odt**, into the image file, keyboard.jpg.
    2. 
    3. Open the files, **secret.odt** and **keyboard.jpg**.
    4. 
    5. Did these files change?
    6. **secret.odt** → No change
    7. **keyboard.jpg** → Changed (because it now carries the hidden file)
  1. Verify the hidden file.
     1. Type the following command in terminal.

cisco@ubuntu:~/Downloads$ **steghide info keyboard.jpg**





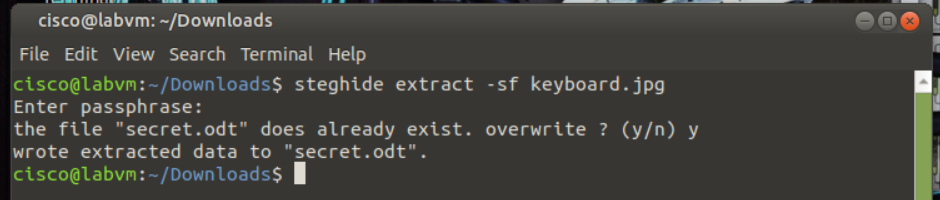
* + 1. Type **y** at the prompt. (Do not press **Enter**).
    2. Enter the passphrase **Cisco** and press **Enter**.
    3. 
    4. The results below shows that the file, secret.odt, is encrypted and compressed.
    5. 

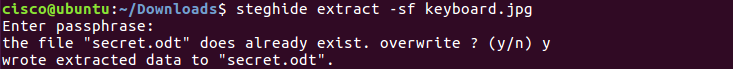


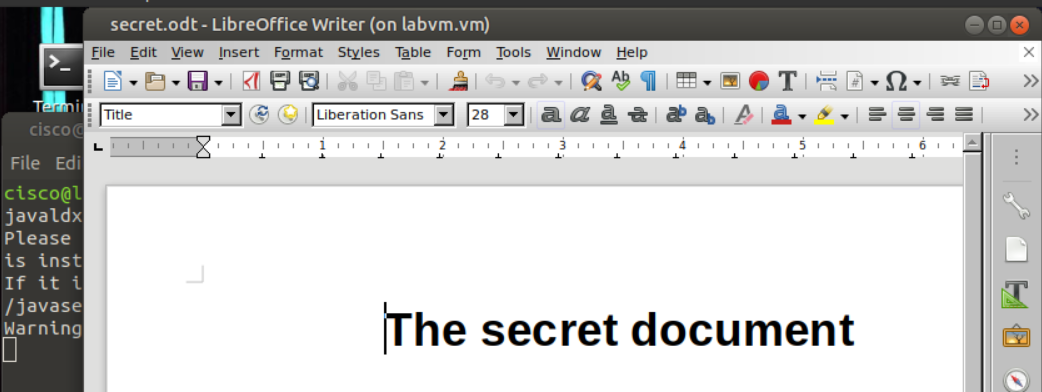
* 1. Extract the hidden file.
     1. Type the following command in terminal.

cisco@ubuntu:~/Downloads$ **steghide extract -sf keyboard.jpg**



* + 1. Enter the passphrase, **Cisco**, and press **Enter**.
    2. 
    3. Enter **y** when prompted to overwrite the existing **secret.odt** file with the new extracted **secret.odt** file.



* + 1. You have extracted the file. Open the extracted **secret.odt** file with LibreOffice.
    2. 

Could you open the file? Is the secret message the same as before?

***Yes, the extracted secret.odt can be opened with LibreOffice as before.***

***Yes, the message is exactly the same as the original secret.odt.***

*steghide does not modify the content of the hidden file, it only hides it inside the carrier image and then restores it unchanged.*

***In conclusion:*** *after extraction, secret.odt can be opened, and the secret message is the same as before.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. References

Steghide: <http://steghide.sourceforge.net/>