Lab – Che giấu thông tin

1. Mục tiêu

Sử dụng kỹ thuật steganography để ẩn tài liệu trong file ảnh JPEG.

1. Kịch bản

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.

Steghide là một chương trình ẩn dữ liệu mã nguồn mở, ẩn dữ liệu trong nhiều loại file khác nhau như: audio và hình ảnh. Bạn sẽ ẩn một file dữ liệu trong file hình ảnh.

1. Yêu cầu

* PC với hệ điều hành Ubuntu 16.04 Desktop LTS được cài trong VirtualBox hoặc VMware
  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.



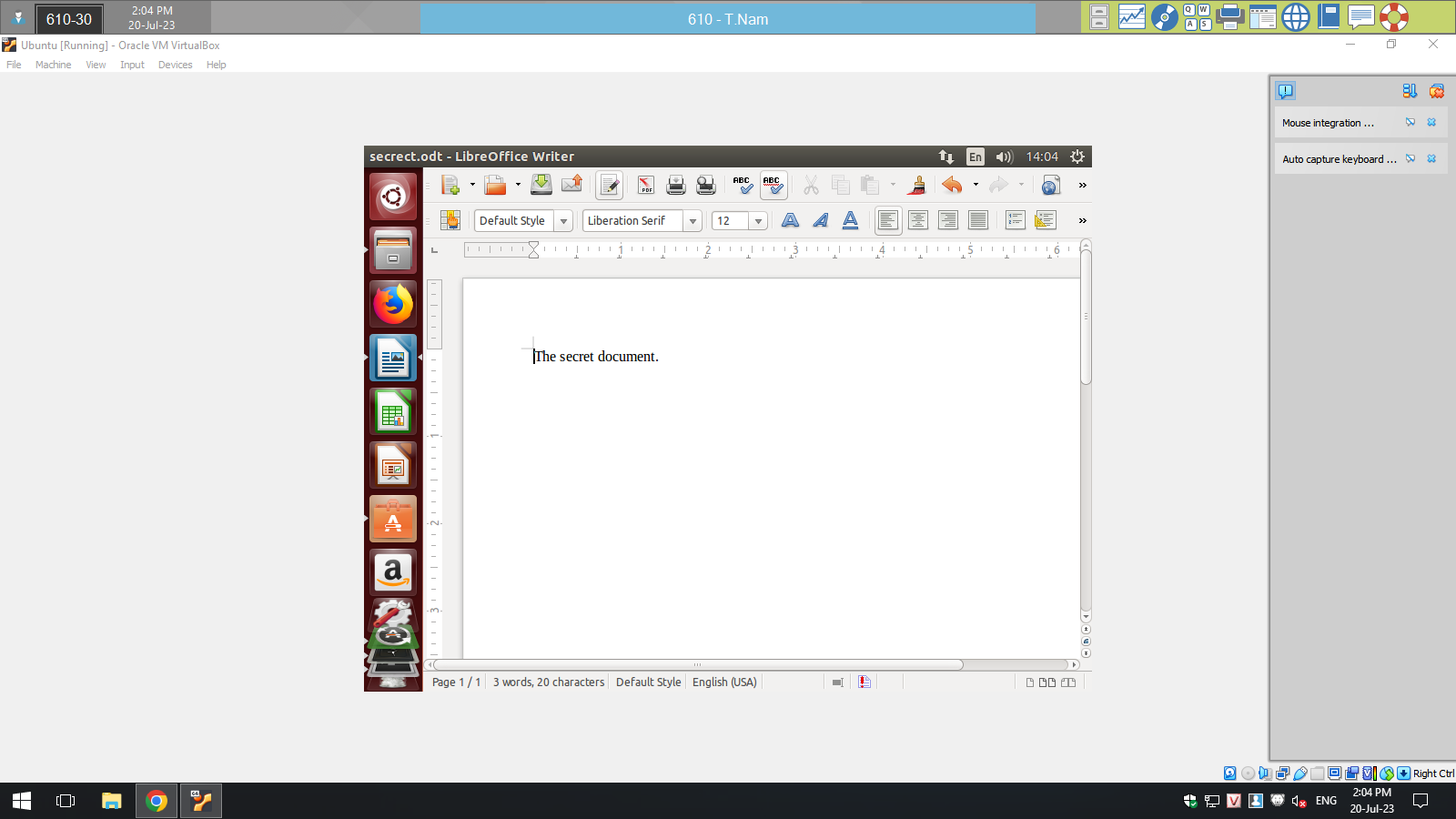
* 1. Run Steghide.
     1. At the command prompt, enter the following command to change to the **Downloads** directory:

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**?



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

* + 1. Close the **secret.odt** file when done.
    2. 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. At the command prompt, enter the following command :

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

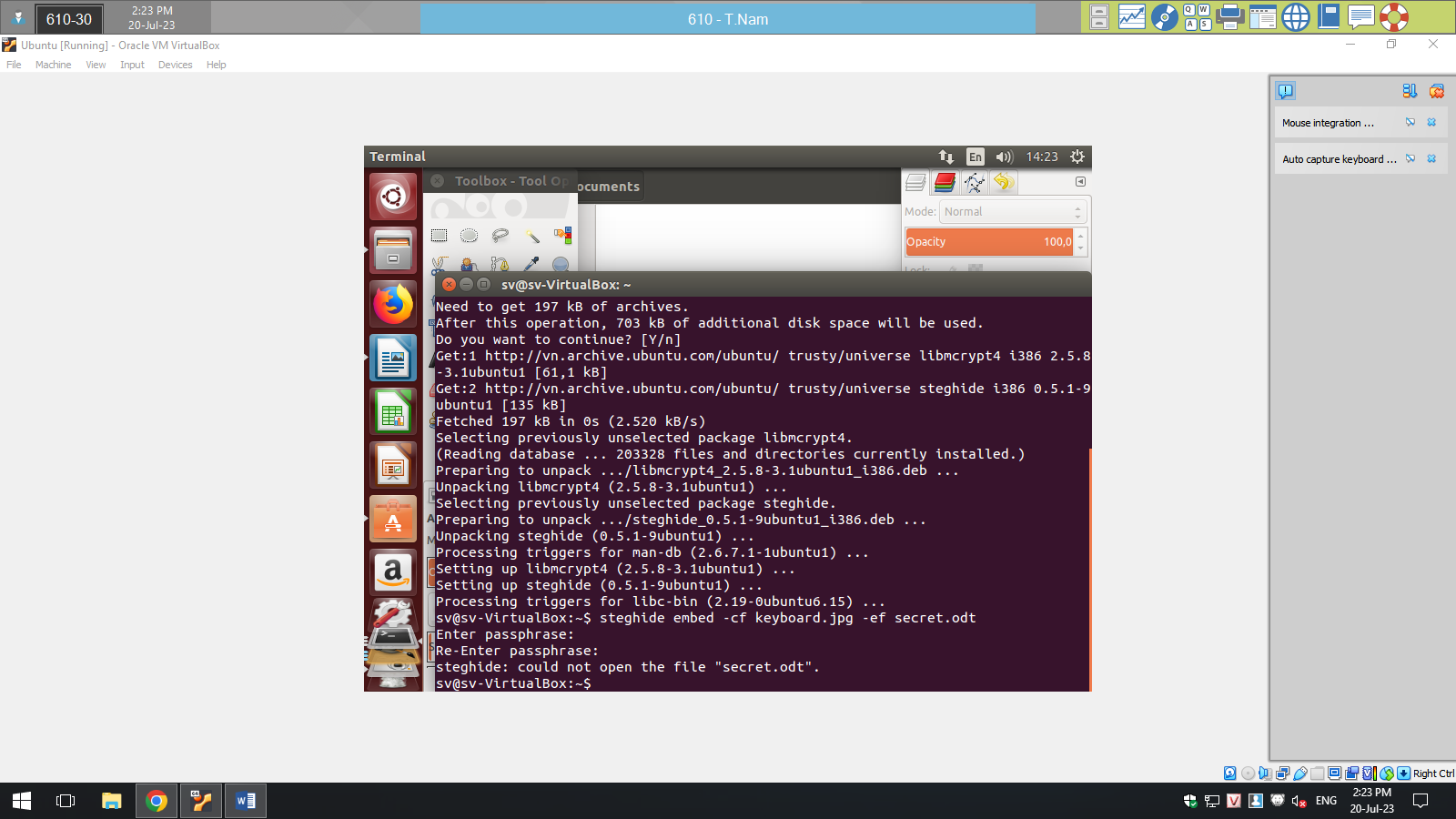
This command takes the jpeg file called “keyboard.jpg” and uses it as a carrier to embed the document, **secret.odt**, into it.

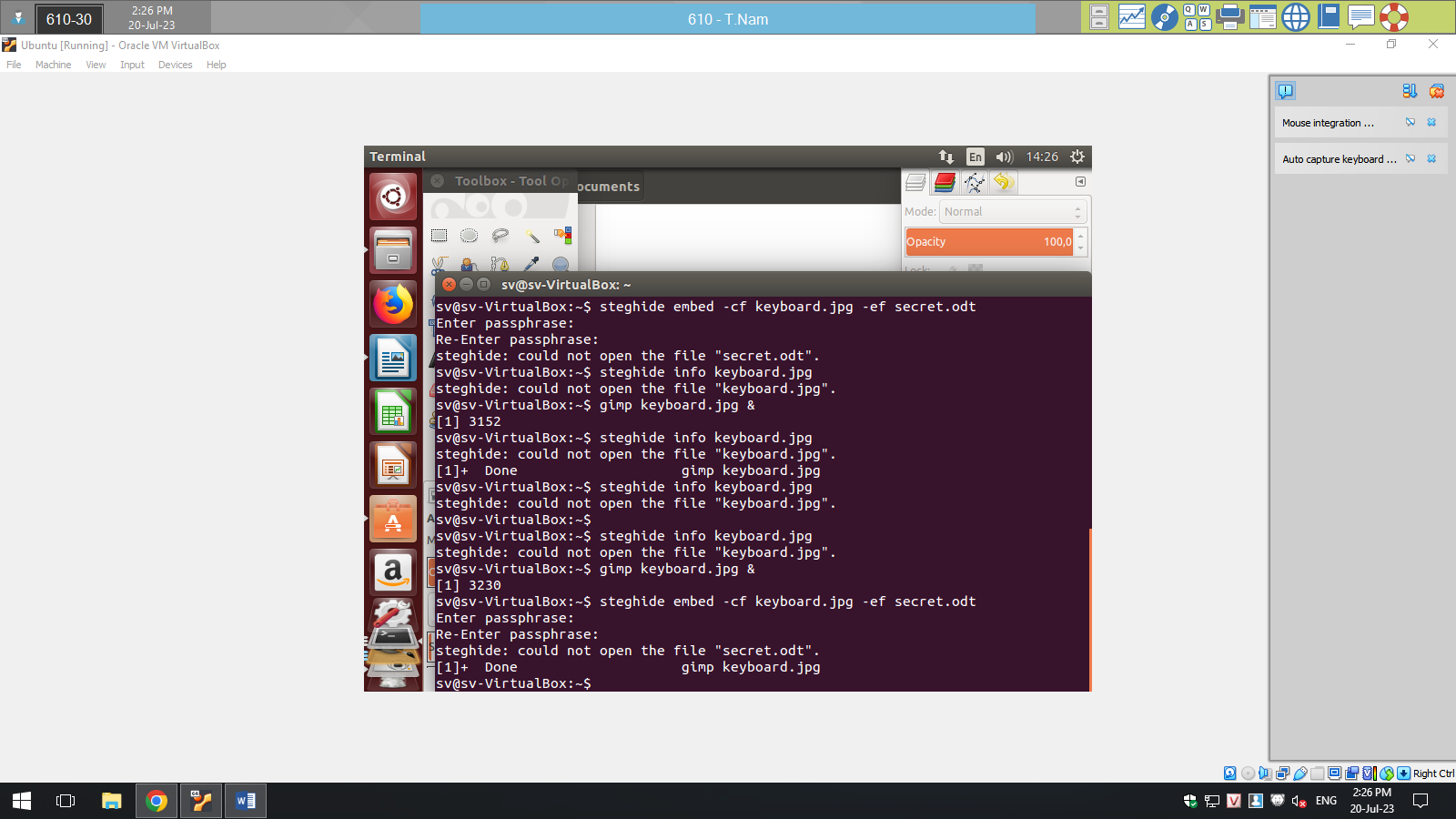
* + 1. When prompted for a passphrase, use **Cisco**. Re-enter the passphrase when prompted.



* + 1. You have embedded the document, **secret.odt**, into the image file, keyboard.jpg.
    2. Open the files, **secret.odt** and **keyboard.jpg**. Did these files change?

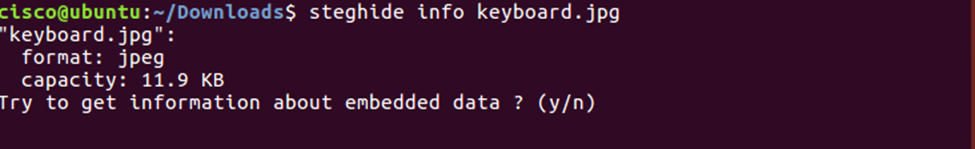
No the files did not change.





* 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. The results below shows that the file, secret.odt, is encrypted and compressed.

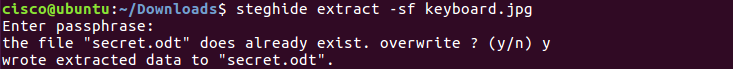


* 1. Extract the hidden file.
     1. Type the following command in terminal.

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

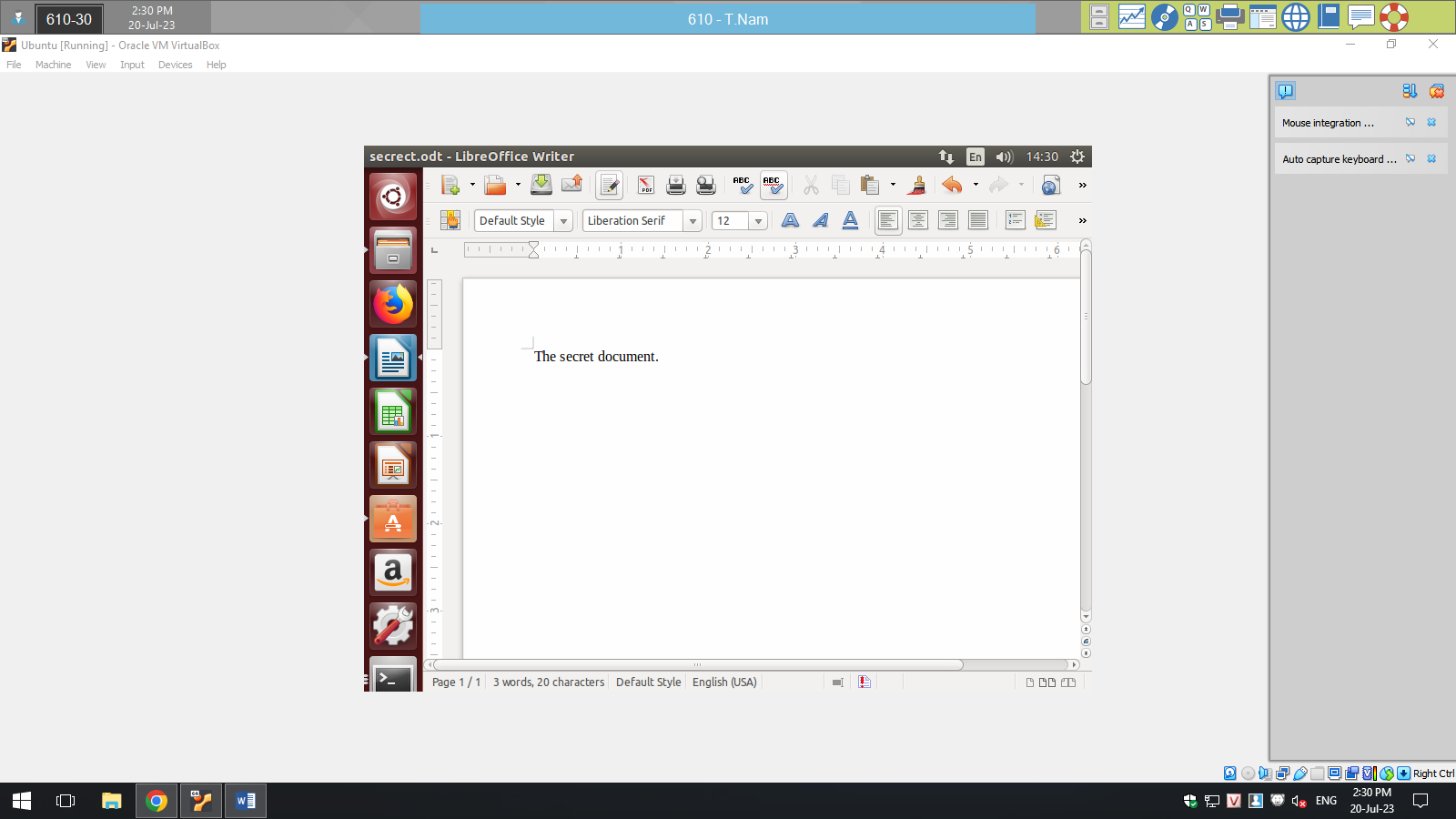


* + 1. Enter the passphrase, **Cisco**, and press **Enter**.
    2. Enter **y** when prompted to overwrite the existing **secret.odt** file with the new extracted **secret.odt** file.



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

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



1. The file can be opened and the message is the same as before.
2. References

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