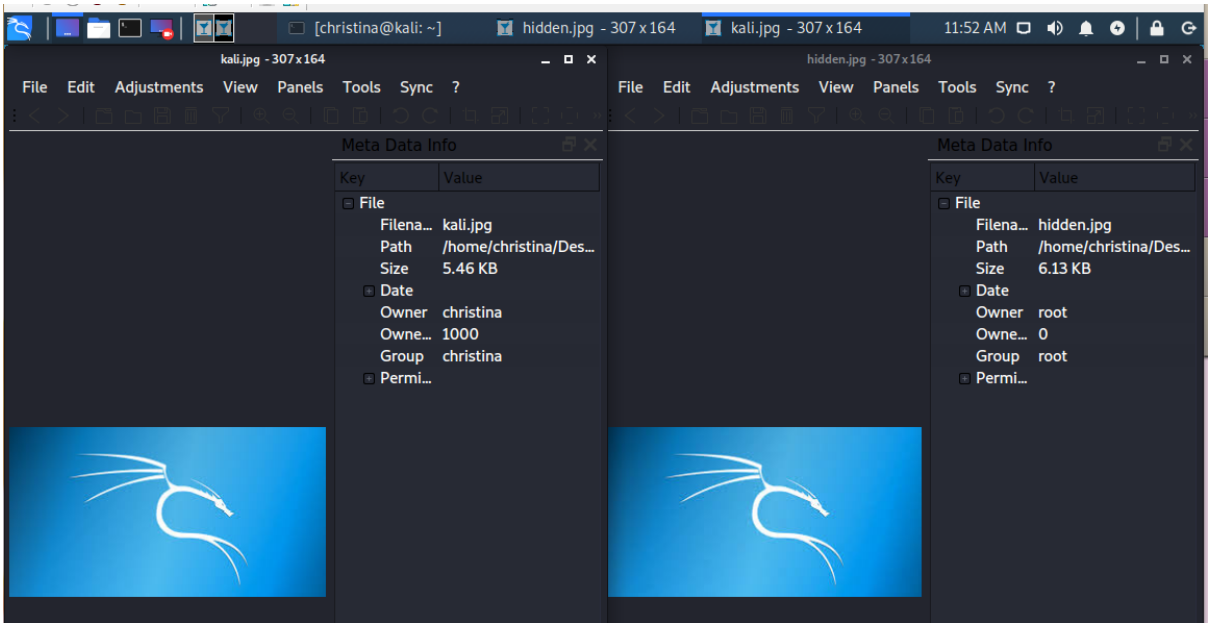
Christina Restauri
Computer Forensics
Indian River State College
April 1, 2020

Steghide

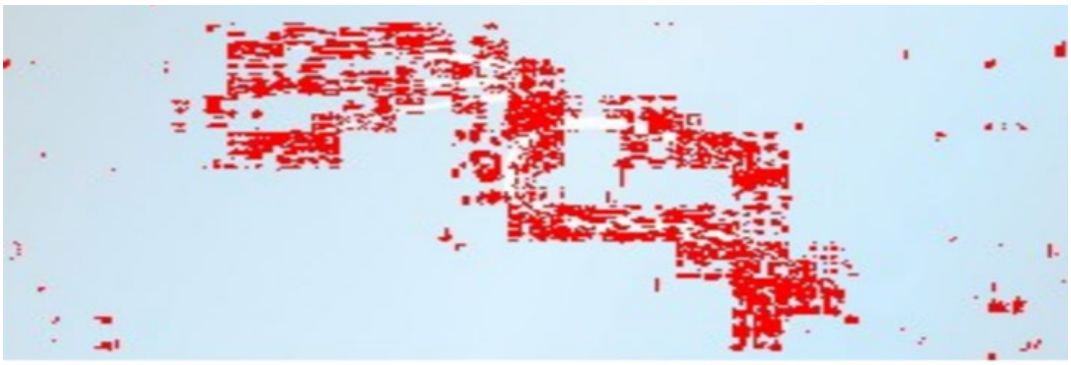
Steghide is a steganography tool in Kali Linux that can hide data behind images, audio files, documents, programs, and more. It takes a normal cover-media and hides a message without much notice. Below is my example of a normal Kali image and a newly created Kali image with a hidden message inside. A simple Steghide command hides a message file inside an image file. Extraction is also very easy using password protection and you can display which algorithm is used to encrypt the data or message in the file. As you can see below, I compared the original image and the new image with the hidden message that Steghide created called “hidden.jpg.” Notice the new image is slightly bigger in size (see metadata); because the hidden message is within.

It’s also relevant that when I tried to hide a larger message file, it would not let me because the cover image was too short to embed the larger message. There is a compression mode, but I haven’t tried that yet. There are online tools that let you compare the before and after images, pixel by pixel, and will show you exactly, in color, where the image changed due to the hidden message. See my example of the two images also below.



Online Comparison Tool showing, in color, the pixels that were changed due to the hidden message.

Before After



Chandel, R. (26 Jul. 2019). Comprehensive Guide to Steghide Tool. Retrieved from https://bit.ly/2IKtjDC.

WaKi Software GmbH. (2020). A Simple tool For Online Image Comparison. Retrieved from https://online-image-comparison.com/.