Here's a step-by-step guide on how to use OpenPuff to embed a secret message payload into a JPG file in Windows 10:

### Requirements:

* OpenPuff software
* JPG file (carrier file)
* ZIP file (message.zip) containing the secret message (message.txt)

### Steps:

1. **Download and Install OpenPuff:**
   * If you haven't already, download OpenPuff from its official website or a trusted source. I went to [emdeddedsw](http://embeddedsw.net/OpenPuff_Steganography_Home.html).
   * Install it on your Windows 10 system.
2. **Prepare Your Files:**
   * Ensure you have the JPG file that you want to use as a carrier.
   * Create a message.zip file that contains the secret message (message.txt file). This is the payload you will hide.
   * I found that there was a ratio of what I wanted to hide to the filesize of the jpg file. So, I downloaded a Blizzard jpeg that was a bit larger than my message.
   * I made a message.txt file with the, "This is a secret message" payload.
   * My first tries were not successful because my "screenshot" was too small and the text message-payload was too large for that file size.
3. **Launch OpenPuff:**
   * Open OpenPuff by double-clicking the application icon.
4. **Embedding the Payload:**
   * In the OpenPuff interface, select the "Hide" option to begin the embedding process.
5. **Set Security Passwords:**
   * You will be prompted to enter up to three passwords. These can be different or the same, depending on the level of security you want. Make sure to write these down if you want to extract the payload later.
   * After entering the passwords, click **OK**.
   * See my [password-file](lab-6-1/OpenPuffPasses.txt).
6. **Select the Payload (Secret File):**
   * Click the **Payload** button to browse and select your message.zip file that contains message.txt.
7. **Select Carrier File (JPG):**
   * Click the **Carrier** button and choose the JPG file that will carry the secret message.
   * You can use multiple carriers (files) if needed. If using multiple carriers, OpenPuff will split the payload among them.
8. **Adjust Hiding Options (Optional):**
   * You can adjust some of the hiding parameters, such as hiding strength and redundancy, but the default settings are generally sufficient for most uses.
   * Click **OK** once everything is configured.
9. **Save the New Carrier File:**
   * Click the **Hide Data** button to embed the message.zip file into the JPG.
   * OpenPuff will prompt you to save the modified carrier file. Choose a location and name the file appropriately (e.g., op\_loaded.jpg). [Jpeg File](lab-6-1/op_loaded.JPG)
10. **Test the Process (Optional):**
    * To ensure that the message has been hidden successfully, try opening the JPG file in an image viewer. It should display normally without any signs of modification.

### Extracting the Hidden Message:

If you or someone else wants to extract the secret message later, follow these steps:

1. **Open OpenPuff:**
   * Open the software and select the "Unhide" option.
2. **Enter the Security Passwords:**
   * Enter the same passwords used when embedding the message.
3. **Select the Carrier File:**
   * Click the **Carrier** button and select the hidden\_message.jpg file (the modified carrier).
4. **Extract the Payload:**
   * Click **Unhide Data** to extract the payload (message.zip).
   * You will be prompted to choose a destination folder for the extracted message.zip file.
5. **Access the Secret Message:**
   * Navigate to the folder where the message.zip file was saved, extract it, and open the message.txt file to view the hidden content.

This process allows you to hide and extract secret messages using OpenPuff with JPG files on Windows 10. I had a lot of fun with this lab. It felt N.C.I.S. like. Heh, "two idiots one keyboard" comes to mind when McGee and Sciuto get hacked and they are both typing on one keyboard. I rolled my eyes and did a face palm when I saw that.