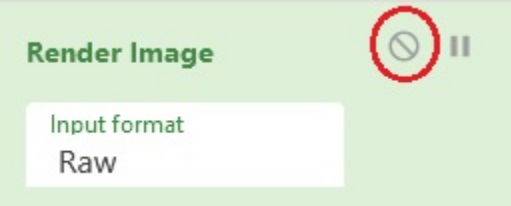
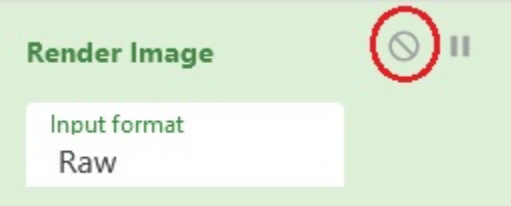
Step 0: Set up
In this step, we'll download the folder of images we'll use in Cyberchef.

Download this folder of images: Lab_6_Images.zip
Open Cyberchef in your web browser (on your host machine is fine, no need to use Azure Labs)
🎯 Checkpoint 0: Cyberchef should be open and ready.

Step 1: Investigate The Data In An Image
In this step, you will open the image called "simpleImage" and investigate it's data in Cyberchef.



Open the simpleImage in the "Input" area of Cyberchef
You will see a "magic wand" appear next to the "Output" title. Go ahead and click on the magic wand to render the image.
magicWand



Now let's actually look at the binary and hex data behind the image.

Turn off (or pause) the "Render Image" Recipe.
stopRecipe

Find the "To Binary" recipe and drop it into the Recipe area.
What Am I Looking At?

All of these 1s and 0s make up the image! There is actually two different pieces of information held within all of the 1s and 0s: metadata and pixel data. Metadata, simply put, is data about data.

Some of those 1s and 0s tell the computer information about your image such as the dimensions the image should be as well as the date, time, and location that the

image was taken or created, and even information about the type of camera that took the picture!

Most of the 1s and 0s is pixel data. This tells the computer what color each individual pixel should be. For example, a pure red pixel would have the following data: 11111111 00000000 00000000. That's just for ONE pixel!

Another way to look at all of this image data is through hexadecimal values. The data doesn't change, just how each piece of data is represented will change. Hex is easier for non-computers, people, to read and understand - all of those 1s and 0s start to blur together!

Let's switch from looking at the image data in binary to hex.

Turn off (or pause) the "To Binary" Recipe.
Drop a "To Hex" recipe into the Recipe area.
Again, this is the same data but just in hexadecimal format.

Let's find where some of that metadata is in the actual data in the Output area.

Look through this information to find the hex value bytes for the "Start of Frame" of a JPEG image.
Click for help with the Start of Frame task
Hold ctrl+F in the output field and search for the Marker Identifier of the Start of Frame.
Once you locate the Start of Frame values, take a look at the next sets of hex values to find more metadata such as the image height and image width.
jpg Hex Values

Optional: Use an online Hex to Decimal Converter to find out what the image height and image width are in decimal values.
Upload a few of your own images and find their Start of Frame, height, and width.
But who wants to try to figure out all of the metadata by looking for it within the image data! That's what we have computers and tools like Cyberchef for!

Step 2: Extract The Metadata
In this step, you will extract the metadata of images.

Delete all Recipes and delete any images from the Input field.
Upload the City landscape image for the input.
The "Magic Wand" icon should appear again next to "Output". Go ahead and click it in order to render the image.

Find the “Get Time” Recipe.
The “Magic Wand” icon should appear again! Go ahead and click it.
Ta da! You found the date and time metadata that this image was downloaded!

But wait … when was the image created?

Now let’s find the “EXIF” data which is metadata that’s more than just the date and time the image was downloaded. Let’s see what other kind of information we can find this time!

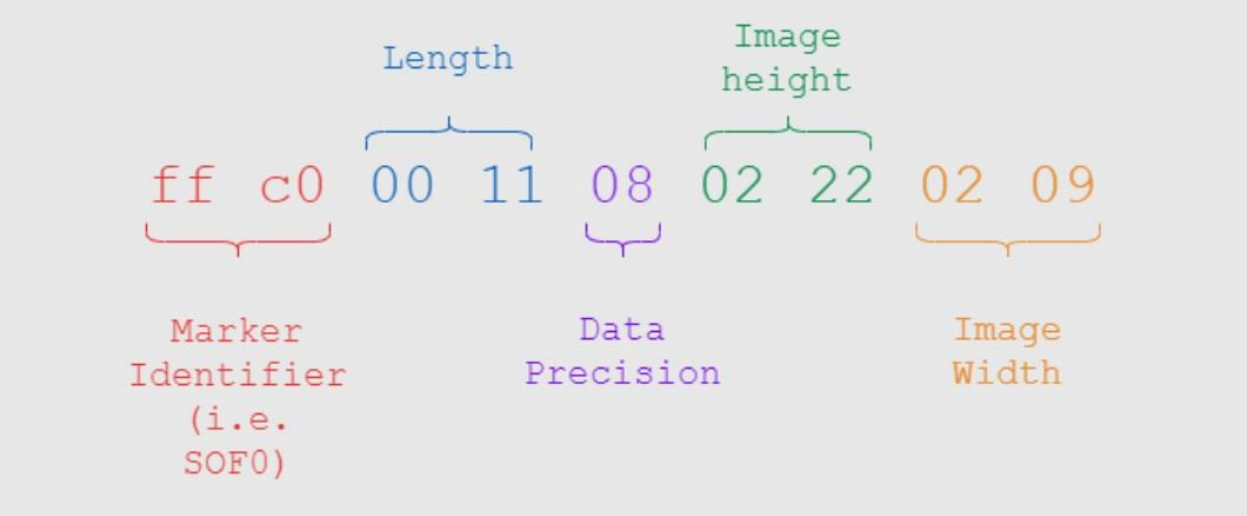
Delete all recipes but keep the same “City” image from above.
Open the Forensics tab, find and drag the “Extract EXIF” recipe to the Recipe panel.
Look through the long list of information!
Can you figure out the actual creation date of the image?
Click me for help with figuring out the image creation date.
Upload a few of your own pictures taken by a digital camera or your phone.
Find the EXIF data!
Step 3: Hidden Files In Images
In this step, you will learn how to find files hidden within the image itself!

Steganography is the practice of concealing or hiding a file, message, or other data within another file. It can enable individuals to covertly communicate data and can be used to bypass content filters or Data Loss Prevention.

With the use of tools, such as Cyberchef, it isn’t that hard to find hidden files … that is if you know you should be looking for them in the first place! That being said, let’s use Cyberchef to find us some hidden files!

Delete all recipes and images from the Input field.
Open the image called ohNo in the Input field.
Click the “Magic Wand” icon to render the image and see what it looks like.
Open the Extractors tab, find and pull out the “Extract Files” Recipe.
Click on the different files that Cyberchef found embedded within the image.
Click the “download” icon for the largest embedded file.

downloadZip



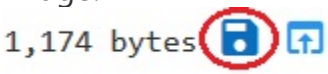
Navigate to where the file was downloaded and double-click the zip folder to open it up and see what is inside.
Continue opening folders until you come across hidden text files.
Can you figure out what secret message they were trying to hide in the image?
Click me for help with extracting the files and finding the secret message.
🎉 Congratulations, you've completed your sixth lab! 🎉
If you have time left over, continue on to the stretch features to learn how to hide information in images!

Stretch Features
Step 4: Reveal A Hidden Message That's Just Out Of Sight
In this step, we'll learn how to perform steganography and hide data within an image's height metadata.

Clear Cyberchef of any recipes and any input.

Upload the imaged called Hidden into the Input Field.

Go ahead and click the Magic Wand that appears in the Output field and render the image.



Repeat your previous lab steps in order to find the Start of Frame hex values as well as the image height and image width.

Note the image height and convert the value to decimal.

You will need to increase the metadata value that the computer reads for the image height by 50.

Once you have increased the value, convert the decimal number back to hex values.

Copy all of the output hex values and click the trash icons to clear the Input and Recipe panels.

Find the “From Hex” recipe and drag it into the Recipe panel.

Paste your copied hex values into the Input panel.

Click on the Magic Wand icon to render the image.

In the Input field, locate the Start of Frame, height and width data.

Change the hex values for the image’s height to the new, increased value.

Scroll down in your Output field and you should see something that wasn’t visible before!

Note: the actual image has not changed - only the metadata for the dimensions that the computer uses to determine what to display!

Click me for help with revealing this hidden message.
Your turn! Reverse the above process to create a hidden message!

Create a simple image with text outside the image “frame”. You can do this using a simple image editor such as MS Paint, Adobe Photoshop, etc. ❗ Be sure to save it as a JPG or JPEG file!
Upload the image to Cyberchef and find the Start of Frame, image height and image width hex values.
Locate the hex values for the image height (or width depending on where you put your text that you want to hide).
Use a hex to decimal converter to get the decimal value for the height (or width).
Decrease the value and convert the new value back to hexadecimal.
Copy all of the Output hex data.
Clear out all Recipes and Input fields.
Drag out the “From Hex” recipe into the Recipe panel.
Paste your copied hex values into the Input field.
Click the “Magic Wand” in the Output field.
Locate the required metadata for the image height (or width).
Change the image height values to the new, decreased hex values.

Scroll down in your Output panel and you'll see that your secret text is gone!
Save the output by clicking on the Save icon in the Output panel!

Select a repo

Edit Note Details

Change note title, set tags, cover photos, and other metadata here.