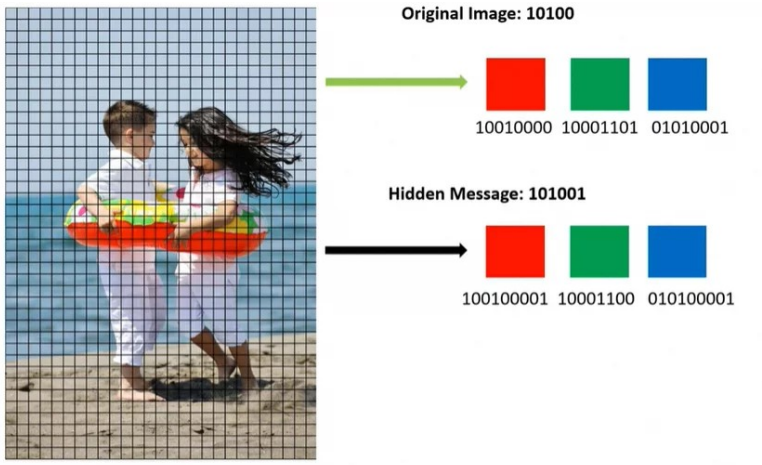
## Determine HIDDEN TEXT In the Image

Images have become an import part on the web, Other than the visual representation of an image, Images can be used to transfer information, this information can be used to attack another person or carry sensitive information.

An attacker goes through a multi-step process when creating an image technique. They must set their sights on a specific company, select a specific target at that company, research the access available to that target, and determine how exactly the hack should take place.

The payload must also be determined: what do they want technique to accomplish? Do they want to take control of the target's machine or quietly extract information?

As an example, take a standard, innocent-looking image, and alter a number of its pixels to embed hidden messages or files inside the image




To see how that can be done check.

**https://votiro.com/blog/image-steganography-example-how-i-created-an-attack/**

In this Lesson we will be extracting hidden text in an image and identify what information is hidden and how malicious it is. Pentesters, Cyber security experts can use Image Extraction tools to identify hidden malicious content hidden in images.

**Binwalk**

Binwalk is a fast, easy to use tool for analyzing, reverse engineering, and extracting firmware images.  Usually used in Forensics Study.

Binwalk is a tool that allows you to search binary images for embedded files and executable code. We can use binwalk to search images for embedded files such as flags or files that may contain clues to the flag.

You may need to download binwalk on your system. Run the following command to install binwalk.

```
mrkmety@kali:~ $ sudo apt install binwalk -y
```

**Example 1:**

You are provided an image named dog.jpg.

Run the following command to see if Binwalk finds any embedded files.

```
mrkmety@kali:~ $ binwalk dog.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION

--------------------------------------------------------------------
```

```
0           0x0           JPEG image data, JFIF standard 1.01

88221       0x1589D       Zip archive ... name: hidden_text.txt

88384       0x15940       End of Zip archive, footer length: 22
```

Binwalk detects a zip file embedded within dog.jpg. The file within the zip file is named hidden_text.txt.

You can extract hidden files by running the following command.

```
mrkmety@kali:~ $ binwalk -e dog.jpg

DECIMAL  HEXADECIMAL  DESCRIPTION

--------------------------------------------------------------------

0          0x0           JPEG image data, JFIF standard 1.01

88221      0x1589D       Zip archive data, ... hidden_text.txt

88384      0x15940       End of Zip archive, footer length: 22
```

A directory named ‘_dog.jpg.extracted’ has been created with the file automatically unzipped.

```
mrkmety@kali:~ $ cd _dog.jpg.extracted/

mrkmety@kali:~/_dog.jpg.extracted $ ls -l

total 8

-rw-r--r-- 1 pi pi 185 Jul  5 19:50 1589D.zip

-rw-r--r-- 1 pi pi  21 Jul  5 15:39 hidden_text.txt

mrkmety@kali:~/_dog.jpg.extracted $

mrkmety@kali~/_dog.jpg.extracted $ cat hidden_text.txt

THIS IS A HIDDEN FLAG
```

Running the cat command on the embedded text file reveals "**THIS IS A HIDDEN FLAG**."

Useful Links
https://manpages.ubuntu.com/manpages/trusty/en/man1/binwalk.1.html

https://subscription.packtpub.com/book/networking-and-servers/9781789952308/10/ch10lvl1sec11/using-binwalk

https://allabouttesting.org/short-tutorial-firmware-analysis-tool-binwalk/