## Objective:

The objective of this class activity was to explore the concept of steganography, specifically how text can be hidden within an image and subsequently retrieved, and to check if common email systems can detect such hidden messages.

### Tools Used:

1. Steganography Online Tool: Steganography Online Tool
2. Email Client: Email Service
3. Image Forensic Tool: ImageForensic.org

### Steps and Observations:

1. Downloading an Image:

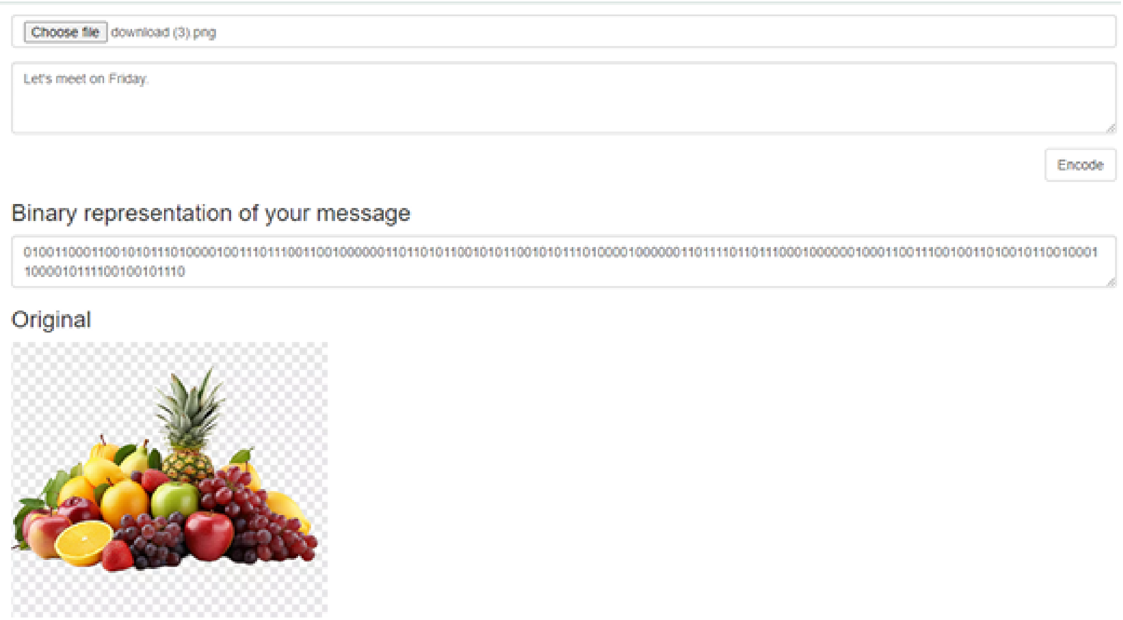
    - I downloaded an image of fruits and saved it as download(3).png.

2. **Encoding the Message:**
    - I uploaded the image download(3).png to the online steganography tool.
    - I wrote the message Let's meet on Friday in the text field provided.
    - I encoded the message into the image and saved the encoded image as download(4).png.

3. **Decoding the Message:**
    - To verify the encoding, I uploaded the encoded image download(4).png back to the online steganography tool.
    - I clicked on the 'Decode' button, which revealed the hidden message as shown in the attached image. The message Let's meet on Friday was successfully retrieved.

4. **Email Testing:**
    - I sent the encoded image download(4).png as an attachment to my email.
    - Upon checking my email, there was no notification or security warning indicating the presence of hidden steganographic data.

## Before Encoding



Choose file download (3).png

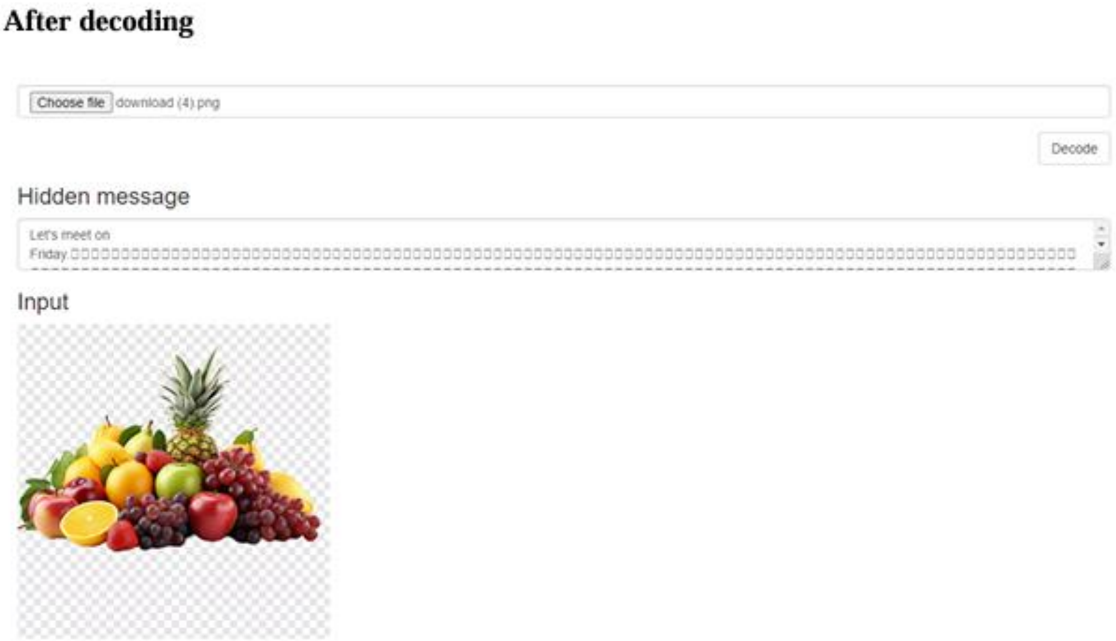
Let's meet on Friday.

Binary representation of your message

```
0100110001100101011101000010011101110011001000000110110101100101011001010111010000100000011011110110111000100000010001100111001001101001011001000
1
1000010111100100101110
```

Original

## After Decoding



After decoding

Choose file download (4).png

Hidden message

Let's meet on Friday.□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

Input

## Image Analysis

I used ImageForensic.org to analyze the encoded image.

1. **Image Details**

- File Name: Downloaded(4).png
- File Size:121.8 KB

2. **Analysis Result**

- Static Analysis: Static data
- EXIF Metadata Extraction: No EXIF metadata
- IPTC Metadata Extraction: No IPTC metadata
- XMP Metadata Extraction: No XMP metadata
- Preview Extraction from Metadata: No Preview
- Localization: No GPS data
- Error Level Analysis (ELA): Applicable
- Signature Check: No signature match

3. **Interpretation of Results:**

- The static analysis indicates the image contains some static data.
- There is no EXIF, IPTC, or XMP metadata present in the image, suggesting the image does not contain standard metadata information often embedded by cameras or editing software.
- No preview image is extracted, and no GPS data is embedded.
- Error Level Analysis (ELA) is applicable, which means that the image can be analyzed for any alterations or hidden data.
- No signature match found, indicating the image does not match any known unaltered image signatures.

4. **Conclusion:**

- The lack of standard metadata suggests that the image may have been processed to remove identifying information.
- The presence of applicable ELA suggests that further analysis can be performed to detect hidden data or manipulations.
- The analysis indicates that the image could potentially contain hidden steganographic data.