Data Representation

We’ve done some of the maths for you, and have a Binary and Hexadecimal Conversion sheet on the Student Portal with the conversions. You can start to see the patterns of how these various representations work!.

|  |
| --- |
| Problem 1 Your grandmother sent you a recipe, but it's all in binary! She says each 8-bit binary number represents a letter. You have what you think might be the recipe title - can you decode this, so that you can ask grandma for the recipe in a more legible format?  01000011 01001111 01001111 01001011 01001001 01000101 01010011 |

|  |
| --- |
| Problem 2 A message was intercepted, but it's using multiple representations! Each group is encoded differently. Decode them all to reveal the full message:  01001000 01000101 01011000  4C 4F 56 45 53  MDEwMA==  Note: we can only tell you that the last system has been encoded in Base64. You may need to use an online converter like <https://www.base64decode.org/> |

|  |
| --- |
| Problem 3 You've found three colored pixels in an image with these RGB values:  Pixel 1: rgb(72, 33, 69)  Pixel 2: rgb(44, 76, 33)  Pixel 3: rgb(80, 42, 33)  The artist left a note: "Each pixel holds a letter”, and you suspect there might be a secret message.   1. Each pixel contains exactly one letter. 2. For each pixel, each channel holds an ASCII value that maps to a capital letter in English. 3. Your task is to find the secret message. |

Extra fun:Want to play with hex colours? Here you are: <https://www.w3schools.com/colors/colors_picker.asp>

Encryption

**Decode each of the ciphers to find the flags**

## Caesar Cipher

Tjmlmk\_Osk\_Xjsewv

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Morse Code

..- -. ... .. -. -.- .- -... .-.. . ... .... .. .--. ...

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Pigpen Cipher



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## [Vigenère](https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher) Cipher

Jmmeurpk\_gvq\_s\_jssk\_hiel\_lvuwth

Key: Gems

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Atbash

Ivevihv\_Ivelofgrlm

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Base64

WW91X0NvdWxkbid0X0RvX1RoaXNfQnlfSGFuZA==

Hint: Can you find an online tool to do this for you?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

File Types

Ask your facilitator for access to the files! With the instructions given to you, look through each file to find the hidden flag.

|  |  |  |
| --- | --- | --- |
| **File Name** | **File Type** | **Flag** |
| Demofile |  |  |
| File1 |  |  |
| File2 |  |  |
| File3 |  |  |
| File4 |  |  |
| File5 |  |  |
| File6 |  |  |

# 

Digital Forensics

## Problem 1

You’re a digital forensics investigator in training, and you’ve been tasked with solving a curious case.

The student council at your school is organising a secret event, but they accidentally left a clue on the school's shared network drive. The principal suspects the event is being planned in violation of school rules because it might disrupt classes. Your job is to analyse the digital evidence and uncover the details of the secret meeting.

On the network drive, you find a single image file titled **"meeting.jpg"**. At first glance, it looks like a basic attempt from a student at drawing a school logo. However, the principal believes the file contains hidden details about the meeting—perhaps the time, date, or location.

Your goal is to uncover the hidden information. Here’s what you need to do:

1. **Access the file metadata**: Investigate the metadata of "***school\_logo.jpg***", found on the Student Portal. Metadata often contains information such as the creation date, modification date, camera settings, or GPS data.
2. **Analyse the details**: Look carefully at all the metadata fields.
3. **Solve the mystery**: Use the metadata to answer these questions:

|  |  |
| --- | --- |
| Meeting Date |  |
| Meeting Time |  |
| Meeting Location |  |

**How can you view EXIF data?**

On a Windows PC: right-click on the image file, select Properties and click the Details tab.

On a Mac: you can open the image in Preview, go to the Tools menu, select Show Inspector and click the Exif tab.

If you can’t find what you are after, use an online image metadata viewer like <https://raw.pics.io/photo-metadata-viewer>

## Problem 2: The Case of the Missing Pizza Recipe

You’ve been hired as a junior digital investigator by **Mama Jacqui’s Famous Pizzeria**, a popular local pizza shop. Disaster has struck—the secret recipe for their award-winning pizza sauce is missing! Without it, they can’t make their signature pizzas, and customers are getting upset.

Mama Jacqui suspects it might have been taken late last night. Luckily, their recipe storage room has a security system that logs every access to the door. Your job is to analyze the **access log file** and help Mama Jacqui figure out who might have taken the recipe.

The pizzeria’s security system recorded every time someone swiped their access card at the recipe room door. The log file is a spreadsheet with these columns:

* **Timestamp**: The date and time of the swipe.
* **ID Number**: A unique number assigned to each employee.
* **Name**: The name of the person who swiped their card.
* **Access Status**: Either "Granted" (door opened) or "Denied" (attempt failed).

Your task is to analyse the log file and identify the prime suspect. The log file can be found in the directory .

### **Questions to Solve**

1. **Who was the last person to access the recipe room?**
   * Sort the data by **Timestamp** to find the last successful access.
2. **How many employees tried to access the recipe room after closing hours (9 PM to 12 AM)?**
   * Use filters to narrow down the entries.
3. **Were there any suspicious patterns, and if so, what are they?**
4. **Who is the most likely culprit?**
   * Based on the data, identify someone who accessed the room close to the time the recipe went missing. Why do you think they are the most likely culprit?

|  |  |
| --- | --- |
| Potential culprit |  |
| Why? |  |
| Why can’t we say that the above person is definitely the culprit? |  |

### 

### **How likely is this scenario?**

There’s a lot of very valuable data that companies hold: movie scripts for the next mega-blockbuster; pharmaceutical formulations that promise revolutionary treatments for cancer etc. This data is protected fiercely.

Digital forensic techniques are used to investigate intellectual property thefts. But going beyond that, big movie studios use extensive logging and automated analysis to ensure that clips don’t get leaked! So while this pizza shop scenario may seem a bit far fetched, we can assure you that digital forensics investigators look into issues like this all the time!

## Problem 3: Eek!

There are rumours that one of the world’s hottest music stars is about to tour Australia, and there is a secret pre-sale only available to insiders. A friend of a friend who knows the musician’s third favourite personal assistant’s holistic healer has sent you a photo of their holiday, which you can access through the steganography tool available on the Student Portal. You suspect that there is more than meets the eye. Your facilitator should have shown you where the photo is.

### **Questions to Solve**

Use the steganography tool to discover:

|  |  |
| --- | --- |
| Name of the music star |  |
| Ticket presales code |  |

# 

Phishing

There are some messages on the student portal that look a little unusual. Outline the suspicious aspects of each of the messages that make you think they may be phishing attempts.

|  |  |
| --- | --- |
| Message 1 |  |
| Message 2 |  |
| Message 3 |  |