# **MIST 400 – Advanced Information Security**

# Capture the Flag (CTF) Assignment #1 (team-based/ 100 points)

# Steganography Challenge I

**Target:** Binary1.txt

**Background:** Steganography is the practice of hiding or obfuscating data within other files. Try to find the hidden flag within this file. Download the file Binary1.txt from eCampus or use the data below. (The file is safe to download, don’t worry.)

**Deliverables**: Provide your answers in the template page named CTF1\_Answers\_Sheet.docx, maintain the same format please. In the first page, provide your group number and group members names. Your answer should be a minimum 1-page walkthrough report on how your team was able to find the “flag”. Include a detailed description of your methods (even failed ones) and some screenshots of your progress along the way. Make sure to cite any sources you used and include a proper bibliography.

**In this CTF, the flag will be an alphanumeric string inside a { }.**

**Requirements: You may need to access to the following software:**

1. **Web browser on a desktop computer or smartphone,**
2. **Steganography tools**
3. **Python or java development environment**
4. **Binary converter.**

**HINTS:**

**Here is some background on Steganography.**

* + [**https://www.comptia.org/blog/what-is-steganography**](https://www.comptia.org/blog/what-is-steganography)

**Binary can be converted into a variety of formats, not just text.**

**Dimensions matter.**

**Remember, all types of data eventually get converted into binary.**

**Data:**

1111111111111100111111001100110000001111111111111111111111111111001111110011001100000011111111111111110000000000110011111100000000001100110000000000111100000000001100111111000000000011001100000000001111001111110011001100111100110011000011001111110011110011111100110011001111001100110000110011111100111100111111001100111100110000110000001100111111001111001111110011001111001100001100000011001111110011110011111100110000000000001111111100110011111100111100111111001100000000000011111111001100111111001111000000000011001100001111111100000011000000000011110000000000110011000011111111000000110000000000111111111111111100110011001100110011001111111111111111111111111111001100110011001100110011111111111111000000000000000000110000110011110000000000000000000000000000000000001100001100111100000000000000000011110000111111000000001100111100000000110011111111111100001111110000000011001111000000001100111111110000000011000011111111001100001111000000110000001100000000110000111111110011000011110000001100000011000000001100110011000011111111111100111111110000000000000011001100110000111111111111001111111100000011111111000000110000111100110011001111000000111100111111110000001100001111001100110011110000001111001111110000001111000011001111000011111100001111111111111100000011110000110011110000111111000011111111110000001100000011110000001111110011000011001111111100000011000000111100000011111100110000110011111100000000000011001111110000000011000000110000000000000000000000110011111100000000110000001100000000000000001100000000110000001100110011110000000011110000000011000000001100000011001100111100000000111100111111111100111111110011001111001111111111110000001111111111001111111100110011110011111111111100000000000000000000001100000011000011110000001100000011000000000000000011000000110000111100000011000000111111111111111100001100111111110011001100110011000011111111111111000011001111111100110011001100110000110000000000110011000011001100111100000011001100001100000000001100110000110011001111000000110011000011001111110011001111110011110000111111111111000011110011111100110011111100111100001111111111110000111100111111001100000011000011110000111111000000111111001111110011000000110000111100001111110000001111110011111100110000001100000000001100000000110011001100111111001100000011000000000011000000001100110011000000000011001100000011001111000011111100111100110000000000110011000000110011110000111111001111001111111111111100110011110011111100110000001100111111111111111111001100111100111111001100000011001111