

**I&M Inter University Cyber Security Contest - 20th November 2020**

**Flag4**

**Instructions:-**

1. Log in to <http://10.50.240.97/filemanager>
2. Go to Flag4 folder.
3. The “somewhat” challenge is to find the flag4.txt which is embedded inside the image. The file is also encrypted using AES 256 and is password protected. The password is 15 characters long. This is achieved from taking the last 5 characters from each flag contents and making them as one, from Flag1 to Flag3 respectively.

As an example if:-

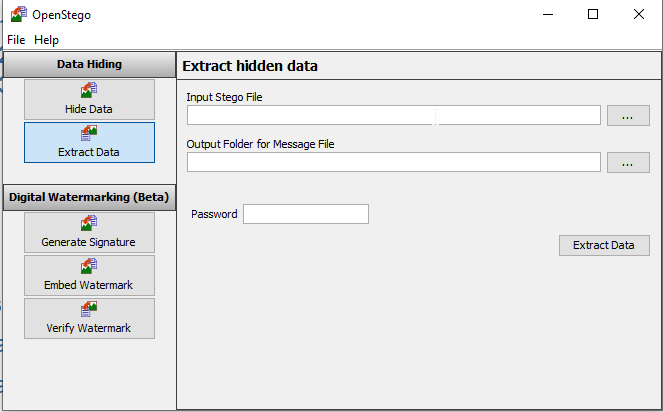
Flag1 is Flag1.1234567812345678

Flag2 is Flag2.abcdabcdabcdabcd

Flag3 is abcd123

Then the password is 45678dabcdcd123

1. The participant is expected to use openstego, an open source steganography application. This application will be hosted on the http://10.50.240.97/filemanager/Flag4/openstego. It has been tested on Windows 10 Enterprise Edition and Kali Linux 2019.4.amd64.
2. The application is very simple. All you need to do is to extract the data, insert the password and location to extract, then viola. Get the Flag4 contents, send to ……. well, you know the drill.



**Expected Solution:-**

The expected solution is in the format:-

Flag4.XXXXXXXXXXXXXXXX