Writeup: Susnography

### Title: --INSERT NAME HERE--

**Date made: 6/04/2020**

**Used in what CSEC CTF: Autumn**

**Writeup:**

**Flag**: CSEC{57up1d\_5u5p1c10u5\_fl4nd3r5} (Stupid Suspicious Flanders)

**Difficulty**: Easy? / **Medium**

**Category**: **Steganography** / some Cryptography(Rot13)

**Description**:

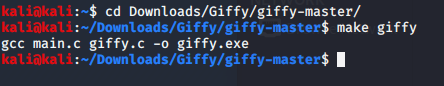
* Don’t mind flanders he has nothing to hide… nothing at all, nothing at all

**Write up**:

1. Download “suspicious.gif”
2. Upon viewing **suspicious.gif** in a browser/software it becomes apparent there is a URL at the end of the GIF.



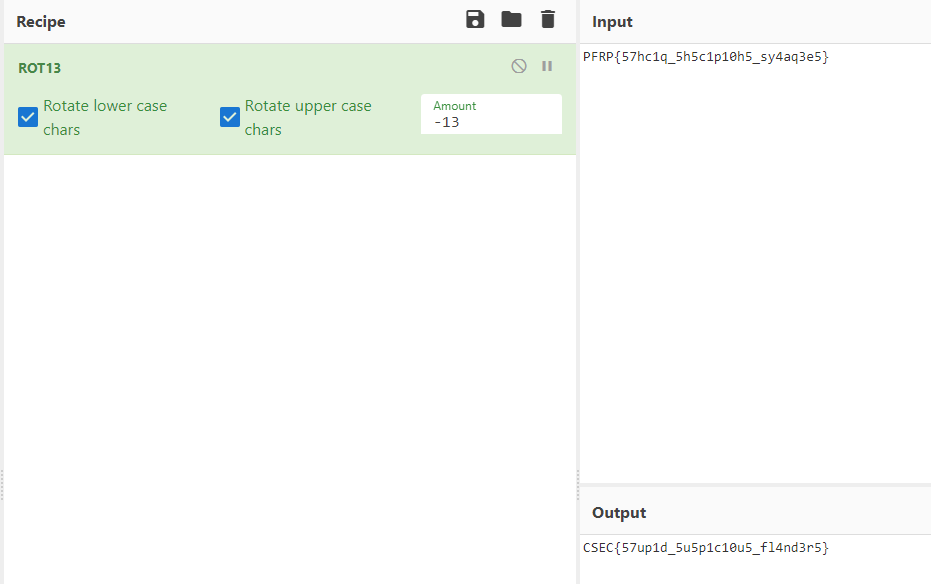
* <https://github.com/vipyne/giffy>

1. Visit <https://github.com/vipyne/giffy>
   1. Download the master branch as .zip and extract it
      1. Compile in Kali via console / Terminal
         1. cd to directory of extracted .zip
         2. Type: ‘make giffy’ as directed by <https://github.com/vipyne/giffy> (To compile)
2. Follow the instructions for decoding on the github
   1. **In terminal**
      1. **./giffy.exe d suspicious.gif**
      2. Or if the suspicious.gif is in the downloads folder still
         1. ./giffy.exe ~/Downloads/suspicious.gif
      3. Or
         1. ./giffy.exe [directory of whereever else you put the GIF]



* 1. User is shown: PFRP{57hc1q\_5h5c1p10h5\_sy4aq3e5} Hint:The flag has ROTen
     1. Simple Rot 13 Cipher: Use a website to reverse the ROT13
        1. <http://decode.org/> or <https://gchq.github.io/CyberChef/>





1. Receive Flag “CSEC{57up1d\_5u5p1c10u5\_fl4nd3r5}”