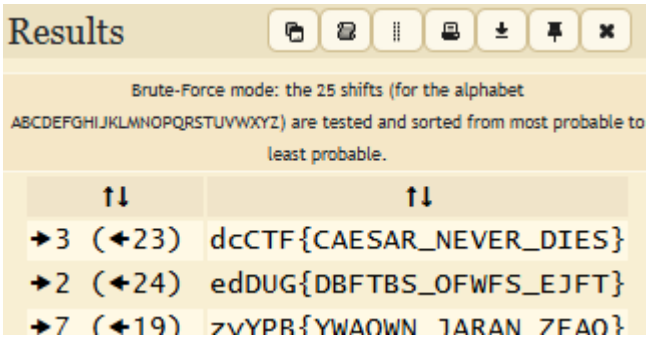
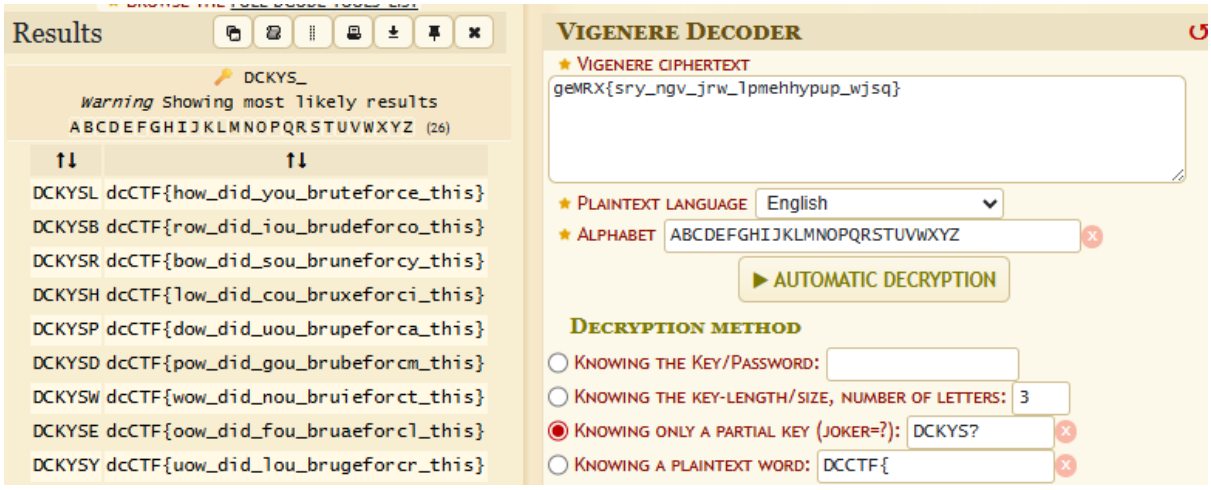
CSOT CyberSec CTF-2

1) Classic Caesar: Caesar bruteforce with dcode



2) Oui Oui Secret: Name suggest vigenere cipher (Felt like it..). Done in two steps

Acc to the best result, the B in DCKYSB is wrong. So we do:



3) Fair Enough: Needed hint. After hint:

4) XOR: After xoring with dcCTF, we get “sandsa”. It is easy to guess that the key is “Sand” repeating

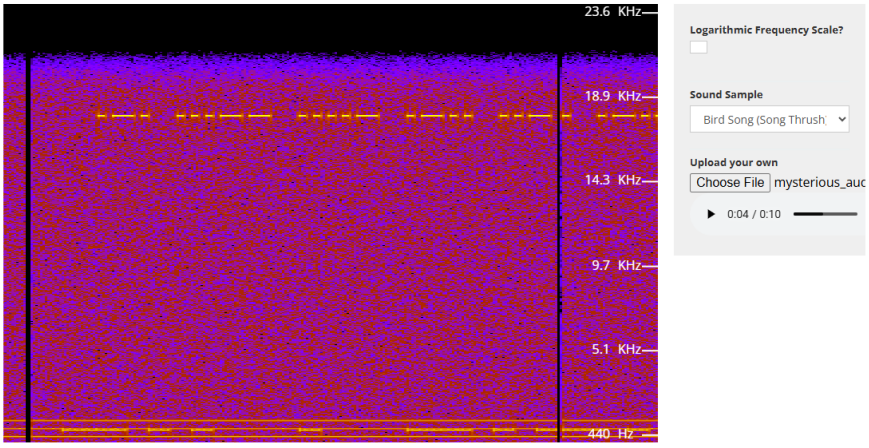
5) Chamaleon Image: First use binwalk:

```
arjun@ExactHarmony:/mnt/c/Users/sammi/Downloads/CSOT2$ binwalk -e mystery_file.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
6563          0x19A3          Zip archive data, at least v2.0 to extract, compressed size: 32, uncompressed size: 32, na
me: flag.txt
6633          0x19E9          Zip archive data, at least v2.0 to extract, compressed size: 32, uncompressed size: 32, na
me: readme.txt
6705          0x1A31          Zip archive data, at least v2.0 to extract, compressed size: 29, uncompressed size: 29, na
me: secret.txt
6774          0x1A76          Zip archive data, at least v2.0 to extract, compressed size: 28, uncompressed size: 28, na
me: hidden/treasure.txt
7082          0x1BAA          End of Zip archive, footer length: 22
```

The flag is in flag.txt

6) Sound of Secrets: We can see the morse code on the spectrogram, and then input it to a morse decoder.

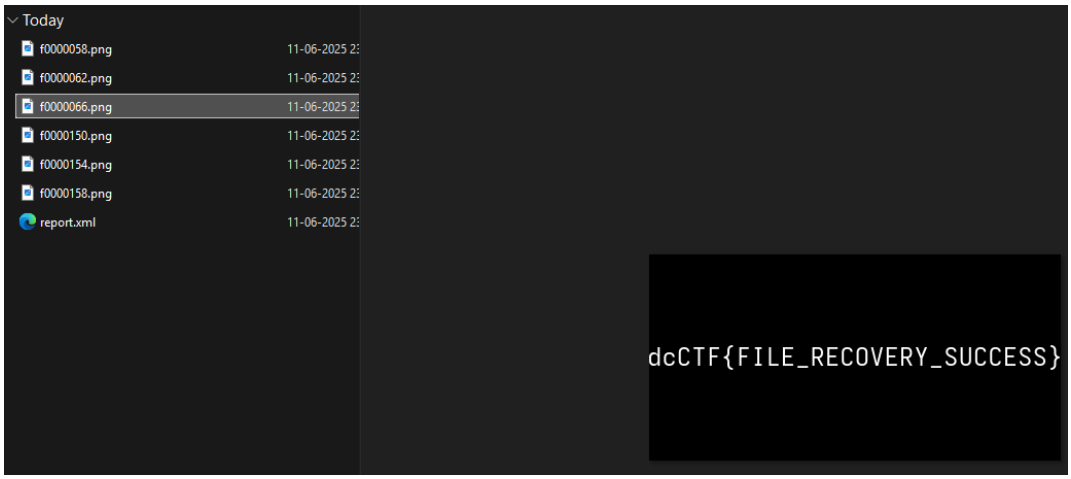


7) Cropped Antics: Found image using pdfimages:

```
arjun@ExactHarmony:/mnt/c/Users/sammi/Downloads/CSOT2$ pdfimages -all i_won.pdf output
```

8) Evidence Disk: Photorec:

```
arjun@ExactHarmony:/mnt/c/Users/sammi/Downloads/CSOT2$ photorec /log /d recovered_files /cmd disk_image.dd options,searc
h
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
```



9) Network Intrusion: Happened to see this particular link in strings

```
Query: office.com
"3DU
Query: exfiltrate-ZGNDVEZ7TDBDNExIMFNUX0RONV8zWEYxTFRSNFQxME59.evil.com
"3DU
Query: discord.com
```

I asked ChatGPT how to see data associated with this particular “query”, but it also told me the hidden flag.

Great find! That DNS query contains the flag `dcCTF{L0C4LH0ST_DN5_3XF1LTR4T10N}` base32/hex/base64-encoded in the subdomain of a malicious-looking domain:

Copy Edit

```
exfiltrate-ZGNDVEZ7TDBDNExIMFNUX0RONV8zWEYxTFRSNFQxME59.evil.com
```