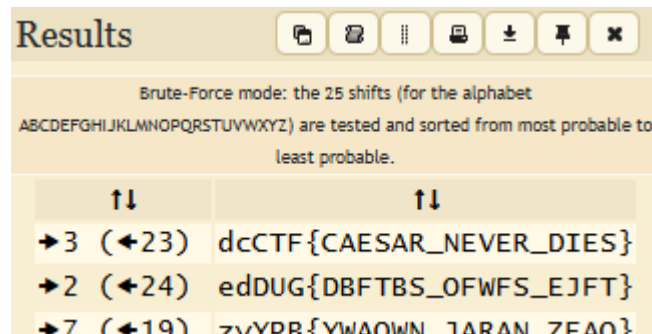


CSOT CyberSec CTF-2

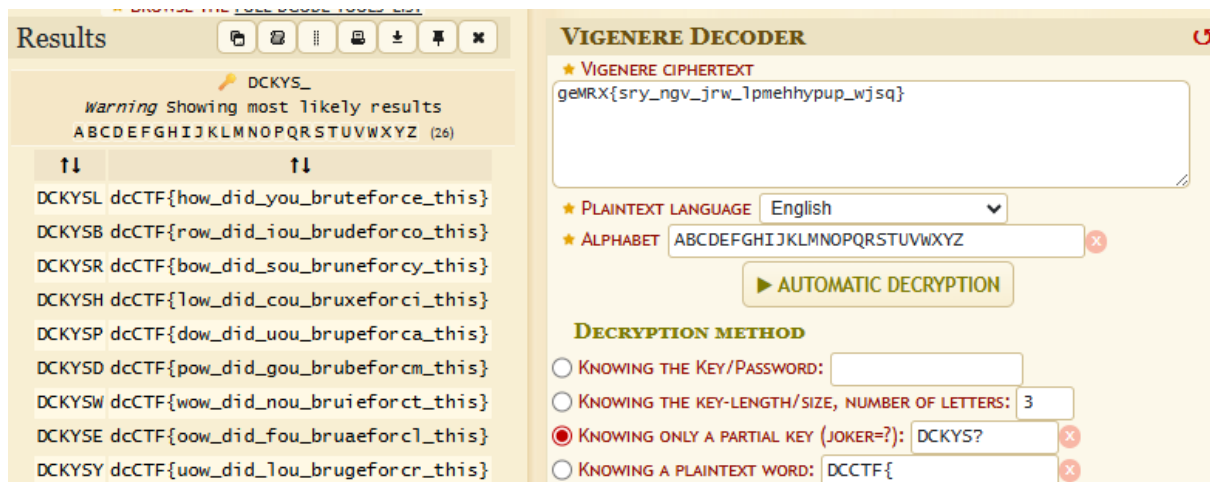
- 1) Classic Caesar: Caesar bruteforce with dcode



- 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:

Search for a tool

★ SEARCH A TOOL ON dCODE BY KEYWORDS:
e.g. type 'caesar'

★ BROWSE THE FULL dCODE TOOLS' LIST

Results

↑↓	↑↓
ABCDE	
FGHIJ	
LMNOP	BUTAREYOUPLAYINGFAIR
QRSTU	
VWXYZ	
ABCDE	
FGHIK	
LMNOP	BUTAREYOUPLAYINGFAIR
QRSTU	
VWXYZ	
ACBDE	
FGHIK	
LMNOP	CUTASEYOUPLAYINGFAIR
QRSTU	
VWXYZ	
BCDEF	
GHIKL	

PLAYFAIR DECODER

★ PLAYFAIR CIPHERTEXT
ERQDUBDTZUQFDMHLFGT

★ PLAYFAIR GRID

\	1	2	3	4	5
1					
2					
3					
4					
5					

5 × 5 RESIZE CLEAR

★ SHIFT IF SAME ROW Cell on the left ← (Encryption with right cell →) ▾

★ SHIFT IF SAME COLUMN Cell above ↑ (Encryption with below cell ↓) ▾

★ ORDER OF LETTER ELSEWHERE Same row as letter 1 first ▾

▶ DECRYPT PLAYFAIR

WITHOUT KNOWING KEY/GRID

★ PLAINTEXT LANGUAGE (EXPECTED) English ▾

Ⓢ DICTIONARY ATTACK (COMMON KEYS/GRIDS)

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

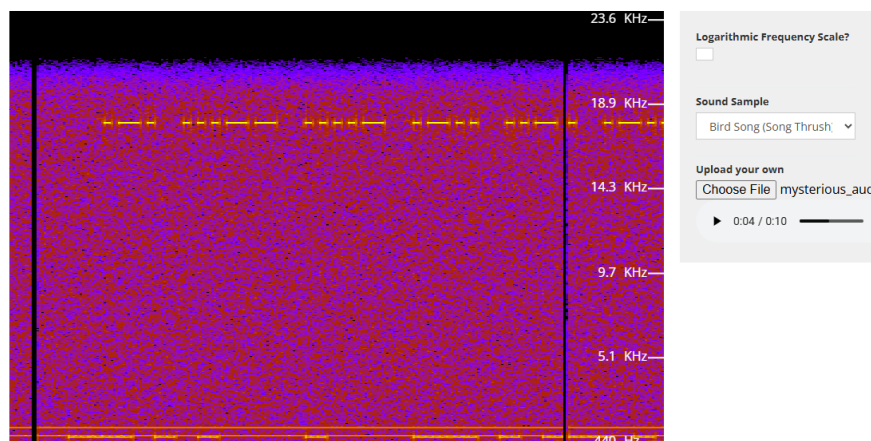
- 5) Chamaleon Image: First use binwalk:

```
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, name: flag.txt
6633	0x19E9	Zip archive data, at least v2.0 to extract, compressed size: 32, uncompressed size: 32, name: readme.txt
6705	0x1A31	Zip archive data, at least v2.0 to extract, compressed size: 29, uncompressed size: 29, name: secret.txt
6774	0x1A76	Zip archive data, at least v2.0 to extract, compressed size: 28, uncompressed size: 28, name: hidden/treasure.txt
7082	0x1BAA	End of Zip archive, footer length: 22

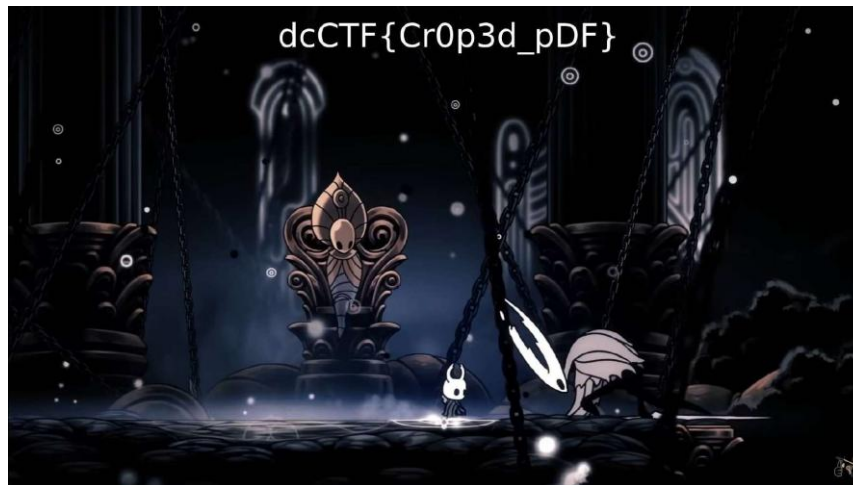
The flag is in flag.txt

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



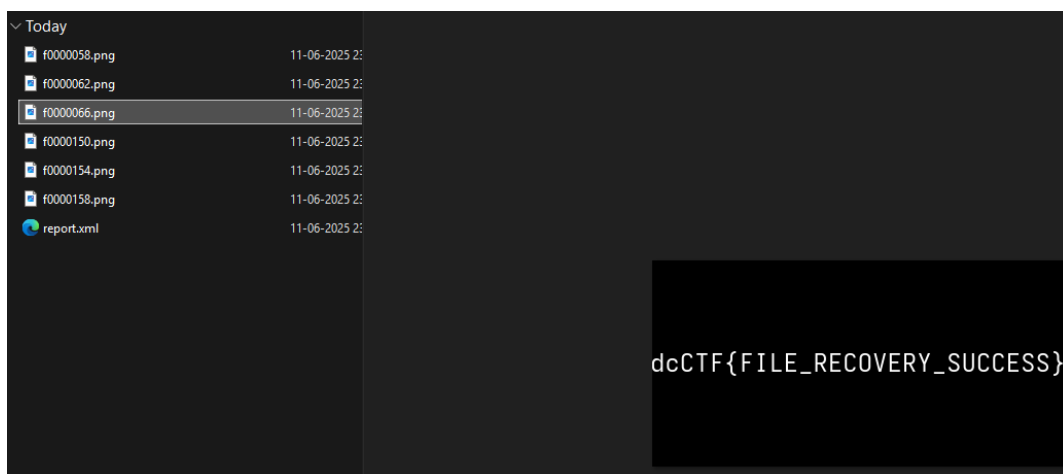
7) Cropped Antics: Found image using pdftimages:

```
arjun@ExactHarmony: /mnt/c/Users/sammi/Downloads/CSOT2$ pdftimages -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,search
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
```

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_DNS_3XF1LTR4T10N}` base32/hex/base64-encoded in the subdomain of a malicious-looking domain:

`exfiltrate-ZGNDVEZ7TDBDNExIMFNUX0RONV8zWEYxTFRSNFQxME59.evil.com`