

# Deadface CTF 2023 writeup

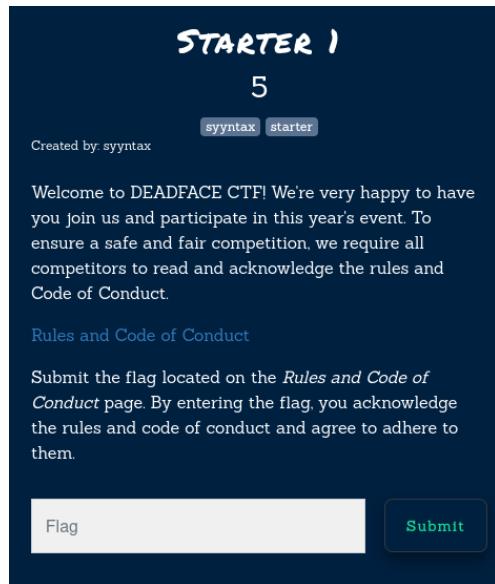
Chall Url -> <https://deadface.ctfd.io>

Cftime-url -> <https://ctftime.org/event/2031>

I will provide solutions with two categories (solved by me AND unsolved but should be solved)

First we have to solve Starter 1 then Starter 2 to access other challenges , if not challenges can't be seen!!!

## **Starter 1 (5 pts)**



This challenge is ez af , we only need to read the rules via link “Rules and Code of Conduct” and the flag is at the end.

```
flag{I_acknowledge_the_rules}
```

## **Starter 2 (5 pts)**

and enthusiasts to help out DEADFACE's victims.

While performing some basic reconnaissance, we found a public Discourse forum called Ghost Town that DEADFACE uses to communicate with each other. We managed to get an insider to open the forum up to non-authenticated users. Use Ghost Town as a resource to find out what DEADFACE is up to and how they managed to execute their attacks.

[Ghost Town](#)

There is a post titled "Where to even get started". Submit the flag as the username of the user that started the post and the date the post was made in this format: flag{username\_MMDD}.

Example: flag{hackyboi\_0615}



It's like OSINT category coz we have to find username and date from a website! They provide us a website that u can go via Ghost Town (<https://ghosttown.deadface.io>). And I try to search with post title "Where to even get started" in searchbar.

A screenshot of a Firefox browser window. The address bar shows 'https://ghosttown.deadface.io'. The page content is a Discourse forum. A search result for the post 'Where to even get started' by user '1337 hax' on May 18 is highlighted with a red box. The rest of the page shows other forum posts and navigation elements.

A screenshot of the 'Where to even get started' post on the GhostTown forum. The post was made by 'daem0n' on May 18. The content of the post is: "I'm trying to figure out what targets to hit for this year and I'm struggling to get started. How do you typically get information for planning operations? Do you engage in any physical surveillance? Or do you prefer more digital means of intelligence gathering, such as through hacking or data breaches? Do you have any favorite tools or techniques you've used in your operation? What's the craziest thing you've ever pulled off against a corporation or government?" Below the post, there is a reply: "Sorry for all the questions...I just love hearing about other people's work in this field, especially when they're so passionate about it." There are also like and unlike buttons at the bottom.

Username is daem0n AND posted date is May 18. So I put it in flag format .  
flag{daem0n-0518}

## OSINT (Open-source intelligence)

### Mama y Papa (10 pts) (unsolved)

The screenshot shows a challenge card with the following details:

- Challenge**: 254 Solves
- Title**: MAMA Y PAPA
- Score**: 10
- Tags**: Shamel, osint
- Created by**: Shamel
- Description**: Alejandro has been seen as an easy mark for DEADFACE. Do a sweep of his social media to see what information DEADFACE was able to gather on Alejandro. Scroll through Alejandros Social media to find out the name of his father and mother.
- Instructions**: Submit the flag as: `flag{father<3mother}`. Example: `flag{John<3Susan}`.
- Attempts**: 0/100 attempts
- Buttons**: Flag, Submit

This challenge is not ez for me, it took me like a day to solve although it's only 10pts.. First I tried to search "Alejandro" on their ghost town site <https://ghosttown.deadface.io>. I found a useful info!

gh0st404 posted 1 edit 8d ago

I think I found a guy who is getting an admin job or something at their HQ? he mentioned on his Facebook that he is getting a job there.

[facebook.com](#) Alejandro Rodriguez 401 Alejandro Rodriguez está en Facebook. Únete a Facebook para conectar con Alejandro Rodriguez y otras personas que quizás conocas. Facebook da a la gente el poder de compartir y hacer del mundo un...

@sunstalker can you confirm this? I know you work there but do you know where the HQ is?

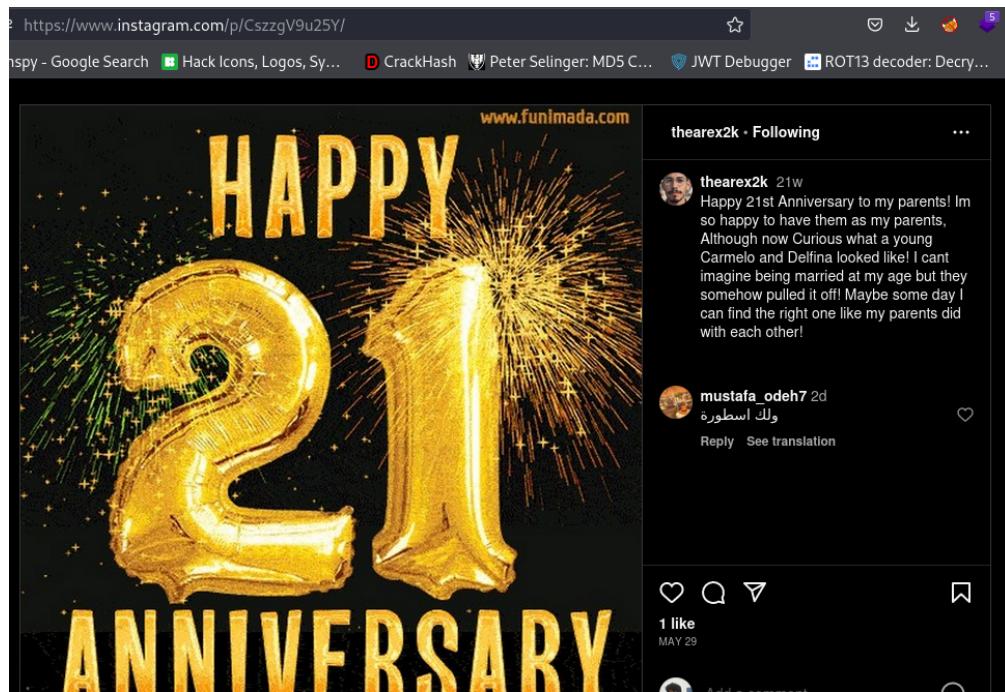
gh0st404 posted 2 edits 8d ago

Seems like he is taking a trip "cross country" ? what the heck? is TGIR not on the east coast? I also did some snooping and found out he has an Instagram and LinkedIn profile too. It was easy enough seeing as he used the same photo for each one .

Ghost town post -> <https://ghosttown.deadface.io/t/tgri-and-lytton-labs/96/9>

We got facebook account name and we know he has Instagram and LinkedIn accs with same pfp. So I searched for his ig acc and on his account , I found his Mama and Papa names.

IG post -> <https://www.instagram.com/p/CszzgV9u25Y>



flag{Carmelo<3Delfina}

### Nice Vacation (20 pts) (solved)

**NICE VACATION**  
20

Created by: Shamel

Shamel osint

Alejandro has been on a road trip to get to his new job working for Techno Global industries. This one one of the first paces he stopped at according to his Instagram.

Submit the flag as `flag{City. state abbreviation}`.  
Example: `flag{Denver, CO}`.

[Download Image](#)  
SHA1: `b5656528384d4556af025507981a80520609ca26`

0/100 attempts

Flag

Submit

This chall gave us the following image to download.



If u zoom in the pic ,there are words on the board “Mobile Onsite Oil” , So I dont think too much. Just Google it “Mobile Onsite Oil location” .. Boom! Got the location and put it in flag format.

mobile onsite oil location

All Images Videos Maps More Tools

About 13,000,000 results (0.51 seconds)

Results for Mingaladon Township, Yangon Use precise location :

1402 E 2nd St, Casper, WY 82601, USA  
Mobile Onsite Oil, address

flag{Casper, WY}

## Steganography

**You've Been Ransomware (10 pts) (solved)**

This chall was solved by my teammate but I'll write it up!!!!

# RANSOMWARED

## 10

RP-01? steg crypto

Created by: RP-01?

DEADFACE is taunting GlitterCo with their latest ransomware attack. According to our intel, the attackers like to leave a calling card in their attacks. If we can figure out which DEADFACE actor executed this attack, we might be able to figure out a way around paying. Can you find anything in this screenshot that might point to which attacker ran this ransomware attack?

Submit the flag as `flag{attacker_name}`.

[Download Image](#)  
SHA1: `6e653b2efc61cb6c9df39c45ccc0f73549e07910`

0/100 attempts

[Flag](#) [Submit](#)

So downloaded the given image!! I tried useful tools like exiftool,steghide,zsteg but didn't okay.So I have stegsolve tool to try.

### [Here u can install Stegsolve](#)

So I opened the image with this tool and I saw some binary words at the end of image.So I changed Blue Plane 5 to see more clearly



```
01010100 01101000 01101001 01110011 00100000 01110010 01100001 01101110  
01110011 01101111 0110001 01110010 01100101 00100000 01100010 01110010 01101111  
01110101 01100111 01101000 01110100 00100000 01110100 01101111 00100000 01111001  
01101111 01110101 00100000 01100010 01111001 00100000 01101101 01101001  
01110010 01110110 01100101 01100001 01101100 00101110
```

Got them so translate it into plain text [here](#) . “This ranso1re brought to you by mirveal “  
flag{mirveal}

**Fetching Secrets (20 pts) (Solved)**

**FETCHING SECRETS**  
**20**

[syyntax](#) [steg](#)



Created by: syyntax

This image was found on Ghost Town. Looks like one of DEADFACE's newest members is new to steganography. See if you can find any hidden information in this image. Knowing information about the image may help to reveal the flag.

Submit the flag as: flag{flag\_text}.

[Download Image](#)  
SHA1: [378f0b4e793aac93d5333d854d552e56aae08ede](#)

[Unlock Hint for 3 points](#)

Hint -> image was found on Ghost Town

 luciafer  
Creative 

1  May 18

My dog's name is Kira (means "killer" in Japanese) even though she's a big softy.

I checked if there was embedded data or not with steghide tool.

```
steghide --info cyberdog.jpg
```

Yes there was ! But we need passphrase to extract! But we knew dog's name is Kira. So the most possible password is kira . So I extracted data with

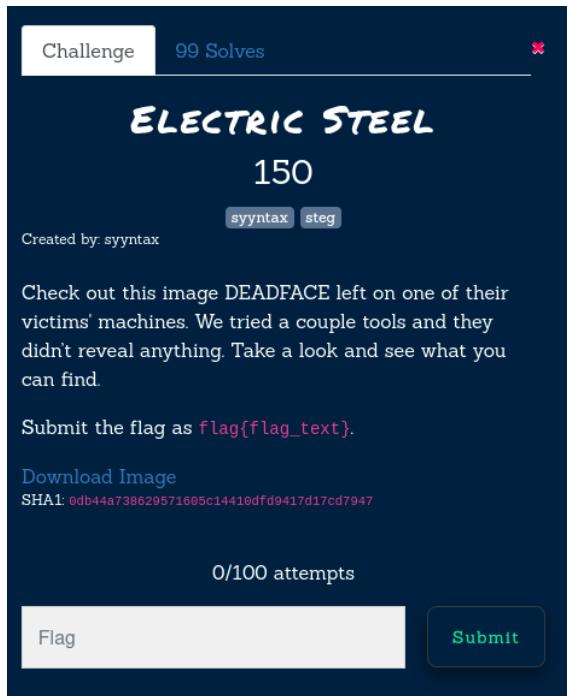
```
steghide extract --sf cyberdog.jpg -xf flagisout.jpg
```

The screenshot shows a terminal session on a Mac OS X system. The user is in their home directory (~) and has navigated to a folder named 'stegno/fetcng\_secrets'. They run 'ls' to see the contents of the folder, which include 'cyberdog.jpg' and 'flag.jpg'. Then, they run 'steghide --extract -sf cyberdog.jpg -xf flag.jpg' and are prompted for a passphrase. After entering 'kira', they are told that the extracted data has been written to 'flag.jpg'. Finally, they open 'flag.jpg' in a Preview application, which displays the text 'flag{g00d\_dawg\_woofw00f}' in red.

```
fluffy@ben: ~/milestone/deadface23/stegno/fetcng_secrets
└── (fluffy@ben)-[~/milestone/deadface23/stegno/fetcng_secrets]
    $ ls
    cyberdog.jpg
    └── (fluffy@ben)-[~/milestone/deadface23/stegno/fetcng_secrets]
        $ steghide --extract -sf cyberdog.jpg -xf flag.jpg
        Enter passphrase:
        wrote extracted data to "flag.jpg".
        └── (fluffy@ben)-[~/milestone/deadface23/stegno/fetcng_secrets]
            $ ls
            cyberdog.jpg  flag.jpg
            └── (fluffy@ben)-[~/milestone/deadface23/stegno/fetcng_secrets]
                $ open flag.jpg
```

flag{g00d\_dawg\_woofw00f}

## Electric Steel (150 pts) (unsolved)



This chall should be solved :(

I tested the given image with steghide,exiftool,stegsolve,zsteg.strings but didn't work  
So I extracted data with binwalk tool. In the extracted folder, there are 3 file (one with tar file , one empty and another zlib file) I didn't checked these files :3 so I didn't solved.  
We can check what file type is with "file" command. Then I extracted again tar file and fking flag is out .

```
fluffy@ben: ~/milestone/deadface23/stegno/electric_steel/... × fluffy@ben: ~
└── (fluffy@ben)-[~/milestone/deadface23/stegno/electric_steel]
    └── $ binwalk -e electric-steel.png

DECIMAL      HEXADECIMAL      DESCRIPTION
---          ---
0            0x0              PNG image, 1232 x 928, 8-bit/color RGB, non-interlaced
2767          0xACF            Zlib compressed data, default compression
1435378       0x15E6F2         TIFF image data, big-endian, offset of first image directory: 8
1435914       0x15E90A         Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"
1467642       0x1664FA         gzip compressed data, from Unix, last modified: 2023-06-04 01:14:27

└── (fluffy@ben)-[~/milestone/deadface23/stegno/electric_steel]
    └── $ ls -l
        electric-steel.png  _electric-steel.png.extracted

└── (fluffy@ben)-[~/milestone/deadface23/stegno/electric_steel]
    └── $ cd _electric-steel.png.extracted
        aseed0
```

```
fluffy@ben: ~/milestone/deadface23/stegno/electric_steel/_... x          fluffy@ben: ~
└─(fluffy@ben)-[~/.../deadface23/stegno/electric_steel/_electric-steel.png.extracted]
    └─$ ls
    1664FA  ACF  ACF.zlib

└─(fluffy@ben)-[~/.../deadface23/stegno/electric_steel/_electric-steel.png.extracted]
    └─$ file *
    1664FA:  POSIX tar archive (GNU)
    ACF:      empty
    ACF.zlib: zlib compressed data

└─(fluffy@ben)-[~/.../deadface23/stegno/electric_steel/_electric-steel.png.extracted]
    └─$ tar -xvf 1664FA
    flag.txt

└─(fluffy@ben)-[~/.../deadface23/stegno/electric_steel/_electric-steel.png.extracted]
    └─$ cat flag.txt
    flag{3L3ctr1c_5t33L_b1G_H41R}

└─(fluffy@ben)-[~/.../deadface23/stegno/electric_steel/_electric-steel.png.extracted]
    └─$ 
```

flag{3L3ctr1c\_5t33L\_b1G\_H41R}

### ***Syncopated Beat (300 pts) (unsolved)***

300

TheZeal0t steg

Created by: TheZeal0t

We know there's a hidden message somewhere here, but none of our steg tools are able to reveal it. Maybe we need to think outside the box?

It is a well-known fact that rock musicians are all Non-Incarnate Conscious Entities (NICEs) influenced. NICEs speak lyrics to them and insinuate their evil messages into the song.

Find the flag and enter it like this :

flag{Syncopated\_Beats\_Are\_EVIL!!!}

[Download ZIP](#)

SHA1: d453507c6be731fcagbefdca96c8ac8ca979d656

0/100 attempts

[Flag](#) [Submit](#)

I think I could solve it butttttttt .. I wont add screenshots coz if I start up my window on virtualbox , it will crash lmao!!

A zip file is given in description. Unzip it and two wav files are out.

Syncopated-Beat-2023.wav

Mysterious\_music.wav

If u listen “Syncopated-Beat-2023.wav” carefully, u’ll notice like evil sound but I know it’s reversed. So we need to reverse it again using [Audacity](#) tool.

Import Syncopated-Beat-2023.wav file and select evil sound waves part

Then in tab menu, click effect > special > reverse

So we can hear human listenable voice. This is a hint and in this, they want me to use [Deepsound tool](#) that works on Windows. And the password is new cto of Evil Corp(e corp) and all caps ,no spaces.

So the password be TYRELLWELLICK . Open deepsound tool and import “Mysterious\_music.wav” , type password and click on extract files. Then a jpg is out. The flag is in there!!!!

## Cryptography

**Coin Code (10 pts) (solved)**

**COIN CODE**

10

syntax crypto



Created By: syntax

We found this image of a coin that belongs to a member of DEADFACE. The image has something to do with the encoded message. We believe the message indicates who this DEADFACE actor wants to target next. Figure out who the target is.

Submit the flag as `flag{Target Name}` (e.g., `flag{Bob's Auto}`)

The encoded message reads: `Fwpl lsjywl xgj ew oadd tw Smjgjs Hzsjes.`

[Download Image](#)

SHA1: `03e101c4c177ecc477e024366958f25ae595b124`

So I copied the given cipher text and analysed it to know what cipher is.

The screenshot shows the dCode Cipher Identifier interface. At the top, there's a search bar and a browse tools link. Below that, a message says "dCode's analyzer suggests to investigate: Warning The text has a short length, this can affect the quantity and reliability of the results (see FAQ)". The results section lists two possibilities: "ROT Cipher" and "Caesar Cipher", both with small icons next to them.

**Cryptography > Cipher Identifier**

**ENCRYPTED MESSAGE IDENTIFIER**

★ CIPHERTEXT TO RECOGNIZE ?

Fwpl lsjywl xgj ew oadd tw Smjgjs Hzsjes

★ CLUES/KEYWORDS (IF ANY)

► ANALYZE

See also: Frequency Analysis — Index of Coincidence

SYMBOLS IDENTIFIER

► Go to: Symbols Cipher List

So ROT and Caesar are possible ,I decipher with [Rot13](#) and flag is out

The screenshot shows the dCode ROT Cipher Decoder interface. It displays the cipher text "Fwpl lsjywl xgj ew oadd tw Smjgjs Hzsjes" and offers an "AUTOMATIC DECRYPTION (BRUTE-FORCE)" button. Below the text, several decryption results are listed:

Shift	Decrypted Text
A-Z]+18	Next target for me will be Aurora Pharma
A-Z]+5	Arkg gnetrg sbe zr jvyy or Nheben Cunezn
A-Z]+11	Ulea ahynla mvy tl dpss il Hbyvh Wohyth
A-Z]+5	Arkg gnetrg sbe 9r j588 or

flag{Aurora Pharma}

### Letter Soup (10 pts) (unsolved)

We believe we have ran into one of the newest members of DEADFACE while they were waiting for the train. The member seemed to have gotten spooked and stood up suddenly to jump on the train right before the doors shut. They seemed to have gotten away, but dropped this innocent looking word search. I believe this member might be actually a courier for DEADFACE. Let's solve the word search to decode the mystery message. We believe the message might tell us their next move.

Submit the flag as `flag{TARGETNAME}` (e.g. `flag{THISISTHEANSWER}`)

Download Image  
SHA1: `ec82f7bae41b800ef1d1ef5f00e97ffb43c737a5`

1/100 attempts

Flag  Submit

This is only 10 pts but didn't solve lmao!!

A halloween word search image is given and we have to find and circle the words



Then write down the remaining words and they became a cipher

mshnhzishjrmlhaolyzzopulpuaolzbu

Analyze with [Cipher Identifier](#) and it shows Caesar cipher , So decode with [Caesar decoder](#)

Enter Ciphertext here

mshnhzishjrmlhaolyzzopulpuaolzbu

Analyze Text Copy Paste Text Options...

Note: To get accurate results, your ciphertext should be at least 25 characters long.

CAESAR CIPHER DECODER

★ CAESAR SHIFTED CIPHERTEXT ?

mshnhzishjrmlhaolyzzopulpuaolzbu

Test all possible shifts (26-letter alphabet A-Z)

► DECRYPT (BRUTEFORCE)

flag{asblackfeatherssshineinthesun}

**B1Tz and B0tZ (25 pts) (solved by teammate)**

# BITZ AND BOTZ

25

Shamel crypto

Created by: Shamel

Yet another message was left at the scene. Perhaps they think they are giving us a lesson...either way report back to us what this says but dont give us guesses! Make sure you check your work!

Submit Flag as flag{hiddenmessage}

[Download File](#)

SHA1: f0e98796759c37cd47c4d91cce6e1675fb596583

0/100 attempts

Flag

Submit

In the given file, binary texts are included.

I solved the whole chall using [cyberchef](#).

I copied and translated binary text.

And I got the following

dont forget the basics! but you didnt think it would be that easy did you? HAHAHAHAHA  
Silly Turbos! More Like Turbo TACKY!!!! Go ahead and ROT  
73 79 6E 74 7B 73 79 76 63 76 67 6E 61 71 65 72 69 72 65 66 72 76 67 7D

I know hex are given and must convert it .After , I got a cipher ,ROT is got above and decoded with ROT13 and flag is out.

( binary => hex => Rot13 => plain text)

Last build: 3 months ago - Version 10 is here! Read about the new features here

Options About / Support

Recipe	Input
From Binary Delimiter: Space, Byte Length: 8	synt{syvcvgnaqerirefrvg}
From Hex Delimiter: Auto	
<b>ROT13</b> <input checked="" type="checkbox"/> Rotate lower case chars <input checked="" type="checkbox"/> Rotate upper case chars <input type="checkbox"/> Rotate numbers Amount: 13	<b>Output</b> flag{flipitandreverseit}
STEP <input checked="" type="checkbox"/> Auto Bake	Raw Bytes LF 19ms Raw Bytes LF

flag{flipitandreverseit}

### Refill On Soup (75 pts) (unsolved)



Created by: twilight\_sparkle

How could we have missed this?? There were TWO word searches stuck together that the DEADFACE courier dropped. We've already solved the first one, but maybe solving this second word search will help us uncover the secret message they're trying to covertly relay to the other members of DEADFACE. Hopefully, THIS will tell us how they plan to execute their next move.

Submit the flag as `flag{TARGETNAME}` (e.g.,  
`flag{THISISTHEANSWER}`)

Download Image

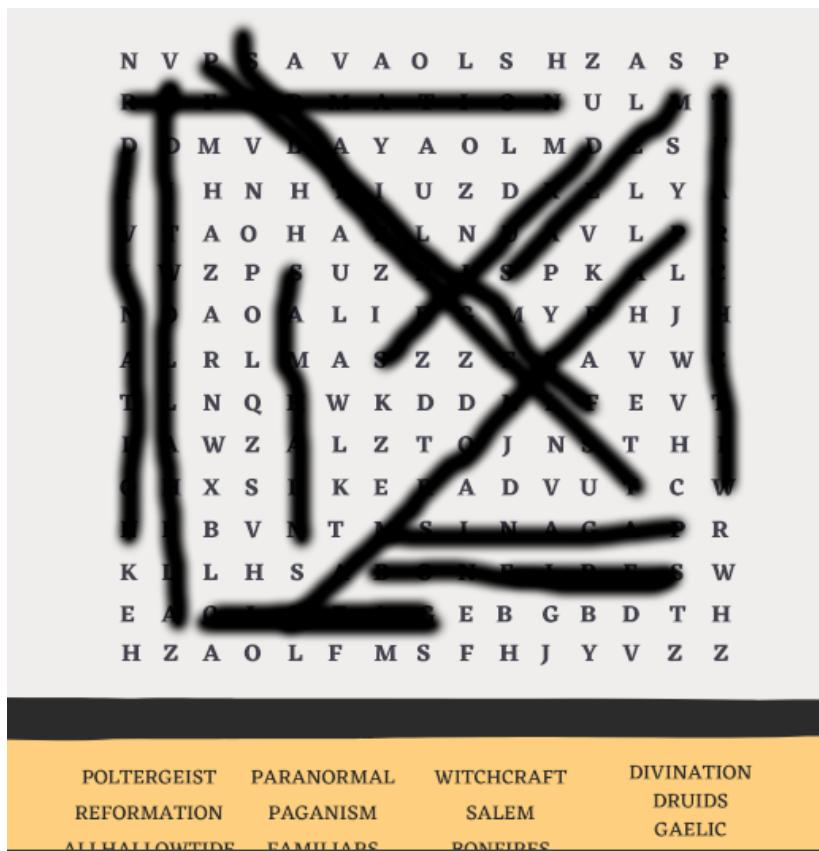
SHA1: `ec82f7bae41b800ef1d1ef5f00e97ffb43c737a5`

6/100 attempts

Flag

Submit

I do the same way like Letter Soup and write down the remained alphabets. But I space if one row is completed.



nvavaolshzasp ul mvyaolms hnhuzdly aohanvl zpuzpkl aoliyhjrlazzavw nqwkddew wzlztjnht  
xskeadvuc bvtr khsw eebcgbdt hzaolfmsfhjyvzz

Analyze cipher and decode with [MonoAlphabetic Substitution](#)

The screenshot shows the CryptTool-Online website interface. The URL is https://www.cryptool.org/en/cto/monoalpha. The page title is "CrypTool-Online" with the subtitle "Cryptography for everybody". The main input field contains the cipher text: "nvavaolshzasp ul mvyaolms hnhuzdly aohanvl zpuzpkl aoliyhjrlazzavw nqwkddew wzlztjnht eebcgbdt hzaolfmsfhjyvzz". Below the input field, there are two radio buttons: "Encipher" (selected) and "Decipher". Under the "Decipher" tab, there are two tabs: "Options" (selected) and "Alpha". Under "Options", there are two checkboxes: "Blocks of five" (unchecked) and "Keep non-alphabet characters" (checked). Below these checkboxes, there is a "Key" input field with the value "7" and a "+" button. To the right of the key input is a "Show / modify code" button. At the bottom of the page, under the heading "Output", the decrypted text is displayed: "goToTheLastLine forTheFinalAnswer ThatGoesInsideTheBracketsTop gjpdWWXo psesmcgma qldXTWonV Uomk dealp XXUVZUWma asTheyFlyAcross".

Flag is the last line So,  
flag{astheyflyacross}

### HAM JAM (75 pts) (unsolved)



Created by: Shamel

It seems as if there is an upcoming hack that the rest of DEADFACE is planning, but someone didn't seem to get the memo. So, instead of risking meeting up to share the date, one of them has used a ham radio to send a message we managed to intercept.

We also identified some chatter associated with the coded message, but we have not been able to figure it out. It's possible there might be clues left on their message board?

Submit the flag as `flag{Month-Day#}`. Example:  
`flag{DECEMBER-10}`.

[Download File](#)

SHA1: `f368acd851a93872f52607330adc0a9cdc69deb8`

0/100 attempts

Morse Wav file is given, I decoded with [Morse Audio Decoder](#)

Decoded message => THE KEY IS HACKTHEPLANET

So we got a key but dont know what to do with it. Trick is that we have to research on ghost town associated with ham radio . I found a post and got barcode image

lawncat 2

Nah I'm not dumb here i'll encode it all and just send the key over HAM. This is the actual date:

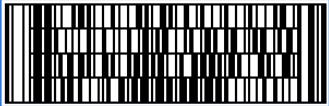
So scanned it using [Barcode Reader](#)

# Barcode Reader Online

Upload your image, choose the barcode type or leave "All types" and click the "Read Barcode" button.

Powered by [aspose.com](#) and [aspose.cloud](#)

[Another image](#)

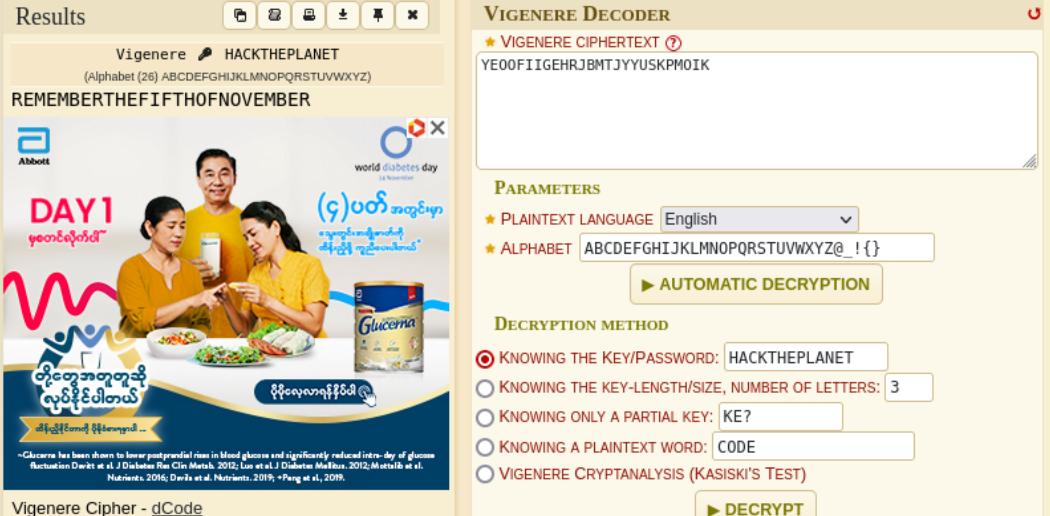


Type: Codablock-F

YE00FIIGEHRJBMTJYYUSKPOMIK

[Generate new](#)

A cipher text is appeared. I know we got a key so, that must be Vigenere cipher. I decoded using [Vigenere Decoder](#) with key ' HACKTHEPLANET ' and got the plain text.



The screenshot shows the Vigenere Decoder interface. On the left, there's a small image of a diabetes awareness campaign featuring a family and a can of Glucerna. The main area displays the decrypted text: "REMEMBERTHEFIFTHOFNOVEMBER". Below this, the parameters are set to "PLAINTEXT LANGUAGE: English" and "ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ@\_!{}". Under "DECRIPTION METHOD", the option "KNOWING THE KEY/PASSWORD: HACKTHEPLANET" is selected. To the right, a sidebar lists various topics related to the Vigenere cipher.

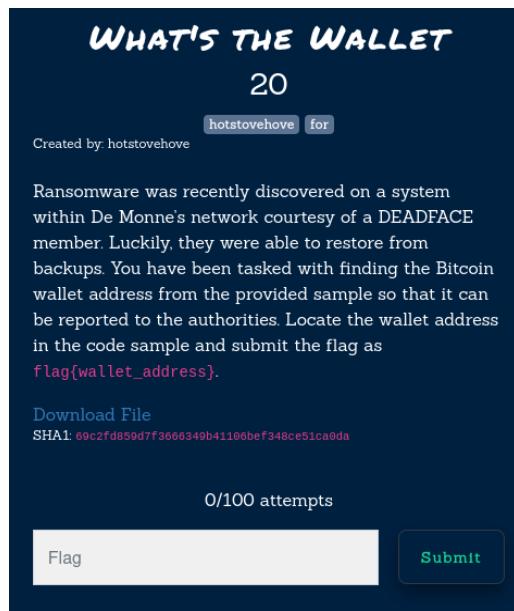
- \* How to encrypt using Vigenere cipher?
- \* How to decrypt Vigenere cipher?
- \* How to recognize ciphertext?
- \* How to decipher ciphertext without knowing the key?
- \* How to find the key having both cipher and plaintext?
- \* What are the variants of Vigenere cipher?
- \* How to choose the encryption key?
- \* What is the running key in vigenere cipher?
- \* What is the keyencyption cipher?
- \* What is a Saint-Cesaire cipher?
- \* Why the name Vigenere?
- \* What are the advantages of Vigenere cipher?

But we have to fix in flag format.

flag{NOVEMBER-5}

## Forensics

**What's the Wallet (20 pts) (solved by teammate)**



It's really ez . Bitcoin.txt file is given. Download and read with 'cat' command  
A useful function that store BTC address but encoded with base64 so. Decode it and flag is out.

```
Write-Host "Hyper-V is installed and enabled on this system."
} else {
    Write-Host "Hyper-V is not installed or enabled on this system."
}
$encodedScript = @"
function Store-BtcWalletAddress {
    $global:BtcWalletAddress = [System.Convert]::FromBase64String([System.Text.Encoding]::UTF8.GetBytes('bjMzaGE1bm96aXhlNnJyZzctxa2d3eWlubWt1c3gy'))
}
# Call the function to store the encoded Bitcoin wallet address
Store-BtcWalletAddress

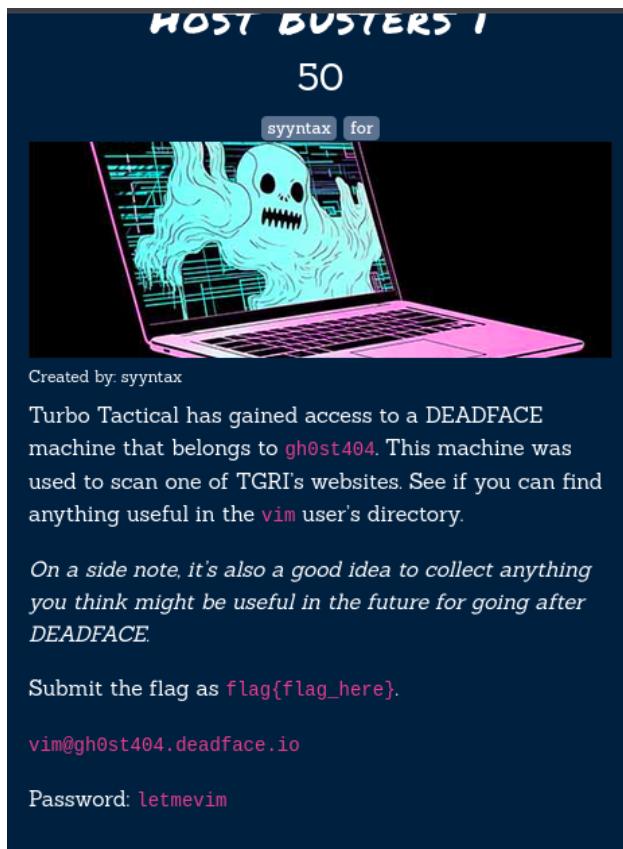
# Access the stored encoded Bitcoin wallet address
Write-Host "Encoded Bitcoin Wallet Address: '$BtcWalletAddress"
"@

Clear-Host
```

```
(fluffy*ben)@[~/milestone/deadface23/forensics/whatsthewallet]
$ echo "bjMzaGE1bm96aXhlNnJyZzctxa2d3eWlubWt1c3gy" | base64 -d
n33ha5nozixe6rrg71kgwyinmkusx2
in the code sample and submit the flag as
[flag{n33ha5nozixe6rrg71kgwyinmkusx2}]
```

flag{n33ha5nozixe6rrg71kgwyinmkusx2}

**Host Busters 1 (50 pts) (solved)**



ssh credentials are given !

So connect ssh with password letmevim

```
(fluffy*ben)@[~/milestone/deadface23/forensics/whatsthewallet] $ ssh vim@gh0st404.deadface.io
vim@gh0st404.deadface.io's password: 50
```

Then vim editor is automatically opened ! I know I should try to get shell access via vim.

Here u can explore [VimToShell](#) . I used “ :shell ” to gain shell .

Then used ‘ ls ’ command to list dirs and found a txt file that can has flag text.

So opened this txt file using ‘ cat ‘ command and flag is outtt.

```
(fluffy*ben)@[~/milestone/deadface23/forensics/whatsthewallet] $ ssh vim@gh0st404.deadface.io
vim@gh0st404.deadface.io's password: 150
$ ls
$ cat hostbusters1.txt
Tin Balloons
$ Turbo Tactical has gained access to a DEADFACE
$ flag{esc4P3_fr0m_th3_V1M} to gh0st404. This machine was
$ used to scan one of TGRI's websites. See if you can find
anything useful in the vim user's directory
```

flag{Hunt\_4\_UDP\_s3rv3r}

**Tin Balloon (150 pts) (solved)**

**TIN BALLOON**  
150  
Shamel for



Created by: Shamel

We've discovered that DEADFACE was somehow able to extract a fair amount of data from Techno Global Research Industries. We are still working out the details, but we believe they crafted custom malware to gain access to one of TGR's systems. We intercepted a Word document that we believe mentions the name of the malware, in addition to an audio file that was part of the same conversation. We're not sure what the link is between the two files, but I'm sure you can figure it out!

Submit the flag as: `flag{executable_name}`. Example:  
`flag{malware.exe}`.

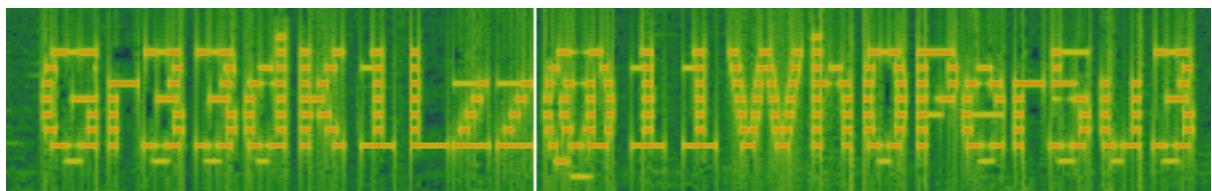
[Download ZIP](#)  
SHA1: 10d87e2d614b242c3a2bd1a5781274ab921475e4

Unzipped the given file and the followings are out.

Sequence 01.mp3

Untitlednosubject.docx

When I open the docx file , it requires password to be opened. So I know the password is in mp3 file. I used [Sonic Visuliser](#) and add spectrogram to this mp3 file and got the password



Gr33dK1Lzz@11Wh0Per5u3

I used it to open docx file and boom , i got name of malware.exe

`flag{Wh1t3_N01Z3.exe}`

## Host Busters 2 (200 pts) (unsolved)



This series of host busters 1 and we have to find the flag not switching other users . So we checked the network status with ‘ netstat ‘ command.

After that we can see a connection is alive and connect it with netcat ‘ nc ‘ .

```
$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:9023              0.0.0.0:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State          I-Node      Path
$ nc -u 0.0.0.0 9023
^C
$ nc -u 0.0.0.0 9023
flag{Hunt_4_UDP_s3rv3r}
flag{Hunt_4_UDP_s3rv3r}
flag{Hunt_4_UDP_s3rv3r}

Turbo Tactical has gained access to a DEADFACE machine that belongs to ghost404. This machine was used to scan one of TGRI's websites. See if you can find anything useful in the vim user's directory.

On a side note, it's also a good idea to collect anything you think might be useful in the future for going after DEADFACE

Submit the flag as flag{flag_here}.
```

Enter twice and flag is out  
flag{Hunt\_4\_UDP\_s3rv3r}

# SQL

## Aurora Compromise (10 pts) (solved)

**AURORA COMPROMISE**

10

[syntax](#) [sql](#)

Created by: syyntax

DEADFACE has taken responsibility for a partial database hack on a pharmacy tied to Aurora Pharmaceuticals. The hacked data consists of patient data, staff data, and information on drugs and prescriptions.

We've managed to get a hold of the hacked data. Provide the first and last name of the patient that lives on a street called Hansons Terrace.

Submit the flag as: flag{First Last}.

[Download Database Dump](#)  
SHA1: [35717ca5c498d90458478ba9f72557c62042373f](#)

[Download System Design Specification](#)  
SHA1: [d6627aa2099a5707d34e26fc82bb532af6398575](#)

1/100 attempts

[Flag](#) [Submit](#)

Query -> select first\_name ,last\_name from patients where street like "%Hansons Terrace%";

```
Empty set (0.013 sec) Transaction Approved
MariaDB [aurl]> select first_name ,last_name from patients where street like "%Hansons Terrace%" 100
; DEADFACE has taken responsibility for a partial
+---+---+---+---+---+
| first_name | last_name |
+---+---+---+---+---+
| Sandor    | Beyer      |
+---+---+---+---+---+
| data, staff, let and iformation on drugs and
+---+---+---+---+
| prescriptions |
+---+---+---+---+
1 row in set (0.013 sec)
```

flag{Sandor Beyer}

**Foreign keys (10 pts) (solved)**

Challenge    254 Solves    \*

## FOREIGN KEYS

10

Created by: syyntax    syntax sql

How many foreign keys are described in the design of the inventory table?

Submit the flag as `flag{#}`.

Use the database dump from *Aurora Compromise*.

0/10 attempts

Flag    Submit

Open the pdf file given in Aurora Compromise and search for foreign  
There are 2 foreign keys in Inventory table  
flag{2}

**Credit Compromise (15 marks) (solved by teammate)**

## CREDIT COMPROMISE

15

Created by: syyntax    syntax sql

How many credit cards were exposed in the Aurora database hack?

Submit the flag as `flag{#}`.

Use the database dump from *Aurora Compromise*.

0/100 attempts

Flag    Submit

Query -> select count(card\_num) from billing;

```
Created by: syntax
MariaDB [aurl]> select count(card_num) from billing;
+-----+
| count(card_num) |
+-----+
|          10391 |
+-----+
Submit the flag as flag{#}.
1 row in set (0.010 sec)
```

flag{10391}

**Transaction Approved (100 pts) (solved)**

**TRANSACTION APPROVED**

100

Created by: syntax

Turbo Tactical wants you to determine how many credit cards are still potentially at risk of being used by DEADFACE. How many credit cards in the Aurora database are NOT expired as of Oct 2023?

Submit the flag as flag{#}.

Use the database dump from *Aurora Compromise*.

3/50 attempts

Flag      Submit

Query -> select count(card\_num) from billing where exp > '2023-10';

```
MariaDB [aurl]> select count(card_num) from billing where exp > '2023-10';      0/50 attempts
+-----+
| count(card_num) |
+-----+
|          8785 |
+-----+
1 row in set (0.007 sec)
```

flag{8785}

### Order Up (125 pts) (unsolved)

I got the flag and the challenge is over ! So sad :(

**ORDER UP**  
**125**

[syntax](#) [sql](#)

Created by: syyntax

Dr. Flegg prescribed Automeda to a patient in June 2023. What is the order number for this prescription?

Submit the flag as `flag{order_num}`.

Use the database dump from *Aurora Compromise*.

0/100 attempts

[Flag](#) [Submit](#)

```
Query -> SELECT o.order_num
FROM prescriptions AS p
JOIN orders AS o ON p.prescription_id = o.prescription_id
JOIN drugs AS d ON p.drug_id = d.drug_id
JOIN staff AS s ON p.doctor_id = s.staff_id
WHERE s.last_name = 'Flegg'
AND d.drug_name = 'Automeda'
AND p.date_prescribed >= '2023-06-01'
AND p.date_prescribed < '2023-07-01';
```

```
MariaDB [aurl]> SELECT o.order_num
-> FROM prescriptions AS p
-> JOIN orders AS o ON p.prescription_id = o.prescription_id
-> JOIN drugs AS d ON p.drug_id = d.drug_id
-> JOIN staff AS s ON p.doctor_id = s.staff_id
-> WHERE s.last_name = 'Flegg'
-> AND d.drug_name = 'Automeda'
-> AND p.date_prescribed >= '2023-06-01'
-> AND p.date_prescribed < '2023-07-01';
+-----+
| order_num |
+-----+
| DYP8AXK3QG9OTPWB |
+-----+
1 row in set (0.004 sec)
```

This query:

- We start by selecting the 'order\_num' column.
- We use 'JOIN' statements to connect the 'prescriptions', 'orders', 'drugs', and 'staff' (for the doctor) tables based on their respective IDs.
- We use the 'WHERE' clause to filter the results.
- 's.last\_name = 'Flegg'' ensures we're looking at Dr. Flegg's prescriptions.
- 'd.drug\_name = 'Automeda'' ensures we're looking for Automeda prescriptions.
- 'p.date\_prescribed >= '2023-06-01' AND p.date\_prescribed < '2023-07-01'' filters the prescriptions to those issued in June 2023.

Send a message

flag{DYP8AXK3QG9OTPWB}

Author : M1n Y3ll S1 T8u

Oct 25 , 23

Hope we can explore new new things together

Have fun guyss