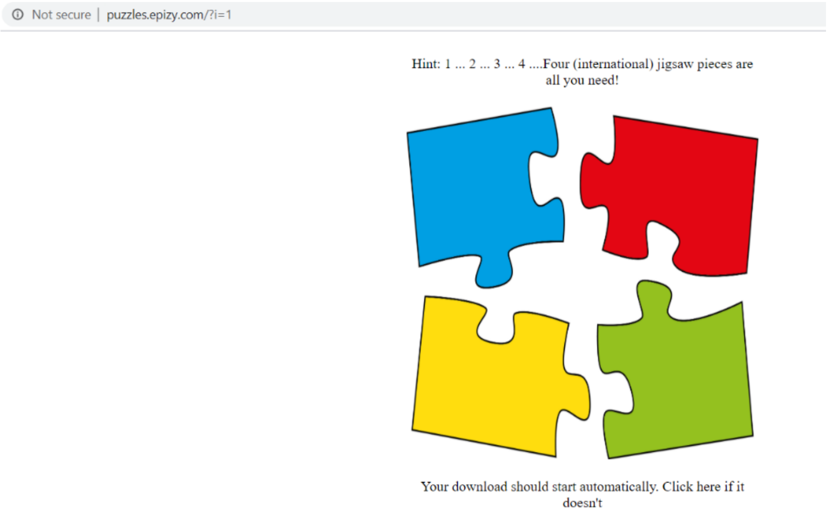
Challenge 08

FLAG: Ard_e_world@pm.me

Spent the longest time on this CTF as I feel that it really lacks a lot of hint. There's a wrong file downloaded every time the page is refreshed. So basically, we have to manipulate something to download a correct file.



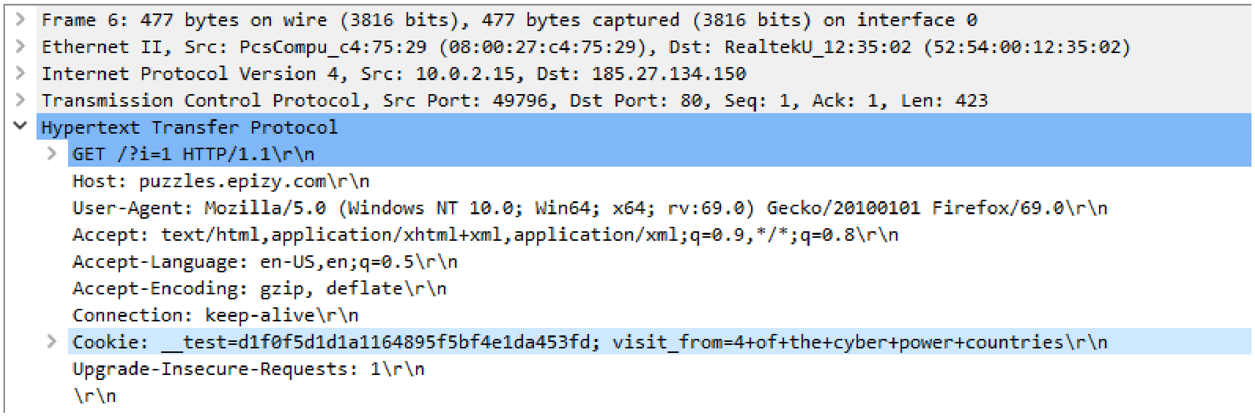
Hint: 1 ... 2 ... 3 ... 4 ....Four (international) jigsaw pieces are all you need!

Your download should start automatically. Click here if it doesn't

"International" was mentioned and the url contains "?i=1". So, I tried setting i = 1,2,3 and 4. Wrong file is still downloaded.

Noticed that there's two images, icon.jpg and puzzle.png. Tried various methods of steganography but no results. Quite lost at this point. Images were some random images file which can be reversed search in Google.

So, I decided to use Wireshark to monitor the traffic. Checking the http protocol, we noticed from the first packet there's some information in the cookie. "visit_from=4+of+the+cyber+power+countries"

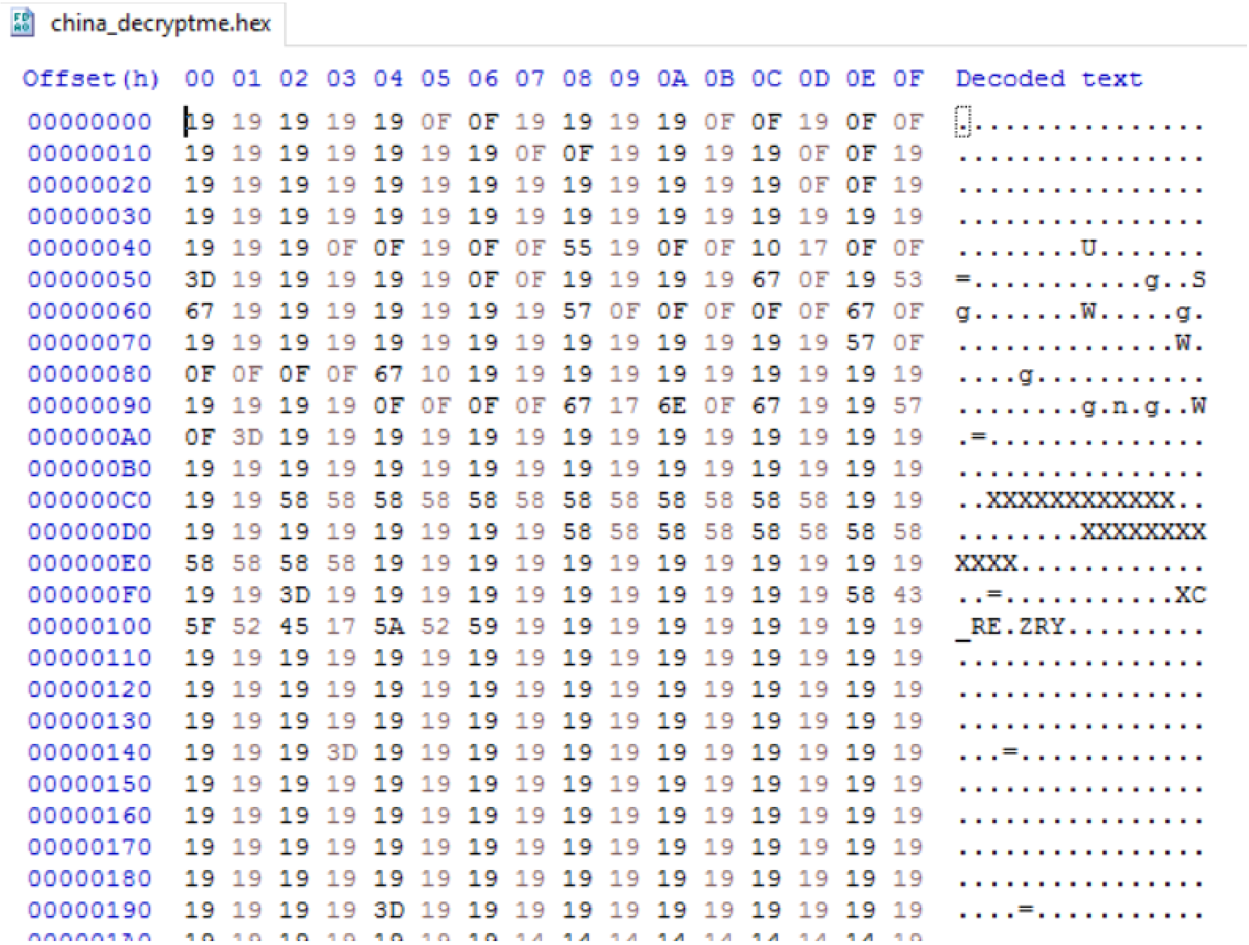


```
> Frame 6: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface 0
> Ethernet II, Src: PcsCompu_c4:75:29 (08:00:27:c4:75:29), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 185.27.134.150
> Transmission Control Protocol, Src Port: 49796, Dst Port: 80, Seq: 1, Ack: 1, Len: 423
v Hypertext Transfer Protocol
  > GET /?i=1 HTTP/1.1\r\n
    Host: puzzles.epizy.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
  > Cookie: __test=d1f0f5d1d1a1164895f5bf4e1da453fd; visit_from=4+of+the+cyber+power+countries\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
```

Went to Googled on this and few countries came up. US, UK, Russia, China, Israel, Iran and North Korea. Still have no idea what to do at this point so I tried modifying cookies using burp suite, both __test and visit_from. Modifying __test gave me information that it's just a cookie with AES encryption, while visit_from gave us nothing.

Suddenly remember that our IP address is displayed in the title and "international" is a hint. Might be doing something related to my IP address and the countries that came up. Used different proxy and VPN to spoof the location of the said countries. Suddenly the downloaded files are different! The new files end with "_decryptme" this time. I managed to get 4 files by spoofing from China, Israel, US and Russia.

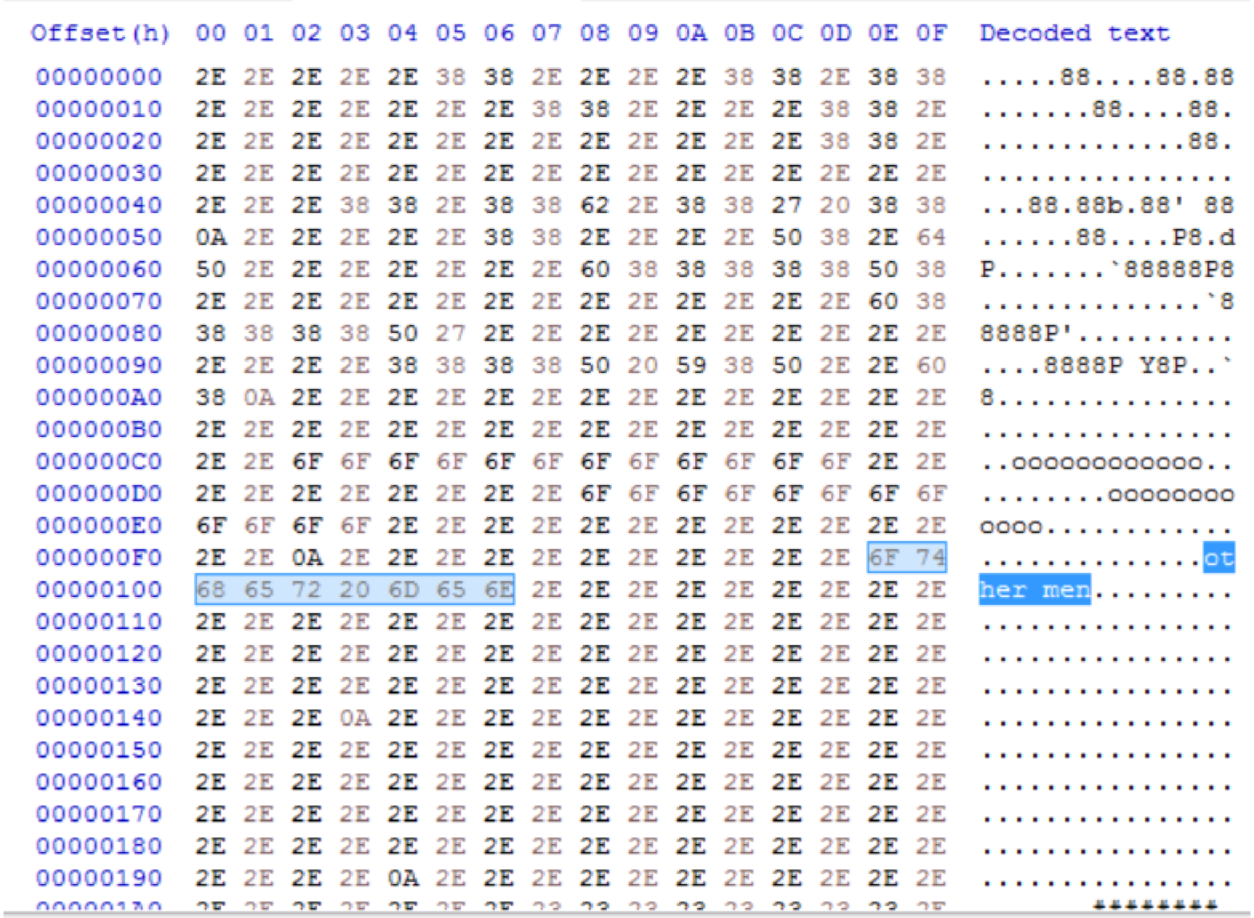
I open the file in HxD and the first thing I noticed is the consecutive bytes. This mean that it's most likely a XOR decryption. Using Sublime Text 3 SMRT tools, I tried XOR-ing the encrypted bytes with consecutive bytes like 0x19 and 0x14. However, I am still unable to decipher anything. Most of the bytes are also common bytes which means that the flag is not as simple as a string in ASCII...



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  19 19 19 19 19 0F 0F 19 19 19 19 0F 0F 19 0F 0F  ................
00000010  19 19 19 19 19 19 19 0F 0F 19 19 19 19 0F 0F 19  ................
00000020  19 19 19 19 19 19 19 19 19 19 19 19 19 0F 0F 19  ................
00000030  19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19  ................
00000040  19 19 19 0F 0F 19 0F 0F 55 19 0F 0F 10 17 0F 0F  ........U.......
00000050  3D 19 19 19 19 19 0F 0F 19 19 19 19 67 0F 19 53  =...........g..S
00000060  67 19 19 19 19 19 19 19 57 0F 0F 0F 0F 0F 67 0F  g.......W.....g.
00000070  19 19 19 19 19 19 19 19 19 19 19 19 19 19 57 0F  ..............W.
00000080  0F 0F 0F 0F 67 10 19 19 19 19 19 19 19 19 19 19  ....g...........
00000090  19 19 19 19 0F 0F 0F 0F 67 17 6E 0F 67 19 19 57  ........g.n.g..W
000000A0  0F 3D 19 19 19 19 19 19 19 19 19 19 19 19 19 19  .=..............
000000B0  19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19  ................
000000C0  19 19 58 58 58 58 58 58 58 58 58 58 58 58 19 19  ..XXXXXXXXXXXX..
000000D0  19 19 19 19 19 19 19 19 58 58 58 58 58 58 58 58  ........XXXXXXXX
000000E0  58 58 58 58 19 19 19 19 19 19 19 19 19 19 19 19  XXXX............
000000F0  19 19 3D 19 19 19 19 19 19 19 19 19 19 19 58 43  ..=...........XC
00000100  5F 52 45 17 5A 52 59 19 19 19 19 19 19 19 19 19  _RE.ZRY.........
00000110  19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19  ................
00000120  19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19  ................
00000130  19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19  ................
00000140  19 19 19 3D 19 19 19 19 19 19 19 19 19 19 19 19  ...=............
00000150  19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19  ................
00000160  19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19  ................
00000170  19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19  ................
00000180  19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19  ................
00000190  19 19 19 19 3D 19 19 19 19 19 19 19 19 19 19 19  ....=...........
```

I was stuck on this for quite some time, until I came across something called the ASCII art. The repeating bytes are patterns suggesting that it can be an ASCII art. I also noticed that every 80 bytes there is an "=" ASCII character. The "=" must be some kind of delimiter. In order to create a puzzle piece sort of delimiter, it's most probably a new line character. A new line character is 0x0A. In order to obtain it, it must be XOR-ed with 0x37. After I XOR-ed it, I noticed some legible English words within. Below is an example from china_decrypted.hex.

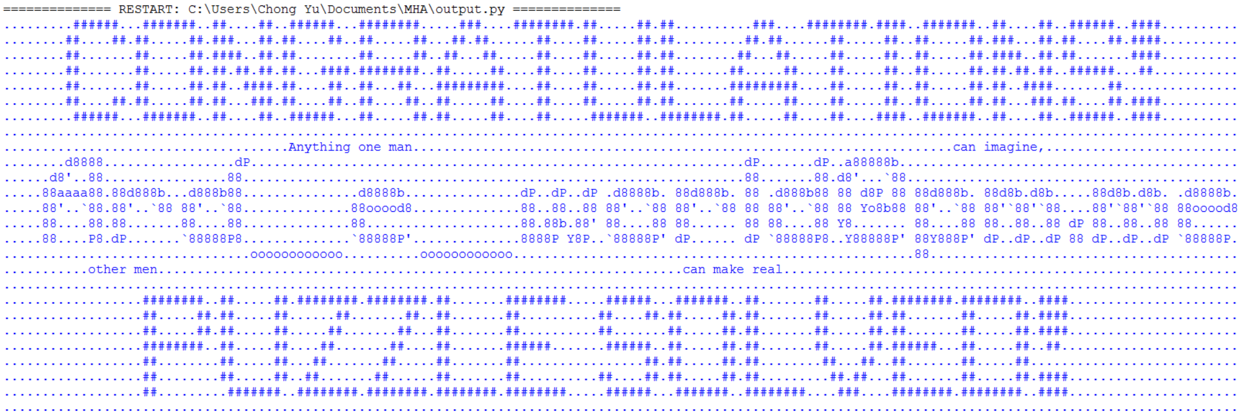


```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  2E 2E 2E 2E 2E 38 38 2E 2E 2E 2E 38 38 2E 38 38  .....88....88.88
00000010  2E 2E 2E 2E 2E 2E 2E 38 38 2E 2E 2E 2E 38 38 2E  .......88....88.
00000020  2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 38 38 2E  .............88.
00000030  2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  ................
00000040  2E 2E 2E 38 38 2E 38 38 62 2E 38 38 27 20 38 38  ...88.88b.88' 88
00000050  0A 2E 2E 2E 2E 2E 38 38 2E 2E 2E 2E 50 38 2E 64  ......88....P8.d
00000060  50 2E 2E 2E 2E 2E 2E 2E 60 38 38 38 38 38 50 38  P.......`88888P8
00000070  2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 60 38  ..............`8
00000080  38 38 38 38 50 27 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  8888P'..........
00000090  2E 2E 2E 2E 38 38 38 38 50 20 59 38 50 2E 2E 60  ....8888P Y8P..`
000000A0  38 0A 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  8...............
000000B0  2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  ................
000000C0  2E 2E 6F 6F 6F 6F 6F 6F 6F 6F 6F 6F 6F 6F 2E 2E  ..oooooooooooo..
000000D0  2E 2E 2E 2E 2E 2E 2E 2E 6F 6F 6F 6F 6F 6F 6F 6F  ........oooooooo
000000E0  6F 6F 6F 6F 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  oooo............
000000F0  2E 2E 0A 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 6F 74  ..............ot
00000100  68 65 72 20 6D 65 6E 2E 2E 2E 2E 2E 2E 2E 2E 2E  her men.........
00000110  2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  ................
00000120  2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  ................
00000130  2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  ................
00000140  2E 2E 2E 0A 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  ................
00000150  2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  ................
00000160  2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  ................
00000170  2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  ................
00000180  2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  ................
00000190  2E 2E 2E 2E 0A 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E  ................
000001A0  2E 2E 2E 2E 2E 2E 2E 23 23 23 23 23 23 23 23 2E  .......########.
```

XOR-ed the remaining 3 files, I decrypted the rest of the puzzle pieces.

Writing a simple python script, piecing them together gives the flag.



```
============== RESTART: C:\Users\Chong Yu\Documents\MHA\output.py ==============
.........######...#######..##....##..######...########.....###....########.##.....##.##..........###....########.####..#######..##....##..######..####..........
........##....##.##.....##.###...##.##....##..##.....##...##.##......##....##.....##.##.........##.##......##.....##..##.....##.###...##.##....##.####..........
........##.........##.....##.####..##.##........##.....##..##...##.....##....##.....##.##........##...##.....##.....##..##.....##.####..##.##.......####..........
........##.........##.....##.##.##.##.##...####.########..##.....##....##....##.....##.##.......##.....##....##.....##..##.....##.##.##.##..######...##...........
........##.........##.....##.##..####.##....##..##...##....#########....##....##.....##.##.......#########....##.....##..##.....##.##..####.......##...............
........##....##.##.....##.##...###.##....##..##....##..##.....##....##....##.....##.##.......##.....##....##.....##..##.....##.##...###.##....##.####..........
.........######...#######..##....##..######...##.....##.##.....##....##.....#######..########.##.....##....##....####..#######..##....##..######..####..........
................................................................................................................................................................
.....................................Anything one man......................................................................can imagine,.........................
........d8888................dP.................................................................dP.......dP..a88888b............................................
......d8'..88................88.................................................................88.......88.d8'...`88...........................................
.....88aaaa88.88d888b...d888b88...............d8888b..............dP..dP..dP .d8888b. 88d888b. 88 .d888b88 88 d8P 88 88d888b. 88d8b.d8b....88d8b.d8b. .d8888b.
.....88'..`88.88'..`88 88'..`88..............88ooood8..............88..88..88 88'..`88 88'..`88 88 88'..`88 88 Yo8b88 88'..`88 88'`88'`88....88'`88'`88 88ooood8
.....88....88.88.......88....88..............88....................88.88b.88' 88....88 88...... 88 88....88 Y8....... 88....88 88..88..88 dP 88..88..88 88......
.....88....P8.dP.......`88888P8..............`88888P'..............8888P Y8P..`88888P' dP...... dP `88888P8..Y88888P' 88Y888P' dP..dP..dP 88 dP..dP..dP `88888P.
................................oooooooooooo..........oooooooooooo....................................................88........................................
...........other men....................................................................can make real...........................................................
................................................................................................................................................................
..................########..##.....##.########.########.##.......########.....######...#######..##.......##.....##.########.########..####......................
..................##.....##.##.....##.......##.......##.##.......##..........##....##.##.....##.##.......##.....##.##.......##.....##.####......................
..................##.....##.##.....##......##.......##..##.......##..........##.......##.....##.##.......##.....##.##.......##.....##.####......................
..................########..##.....##.....##.......##...##.......######.......######..##.....##.##.......##.....##.######...##.....##..##.......................
..................##........##.....##....##.......##....##.......##................##.##.....##.##........##...##..##.......##.....##...........................
..................##........##.....##...##.......##.....##.......##..........##....##.##.....##.##.........##.##...##.......##.....##.####......................
..................##.........#######..########.########.########.########.....######...#######..########....###....########.########..####......................
................................................................................................................................................................
```