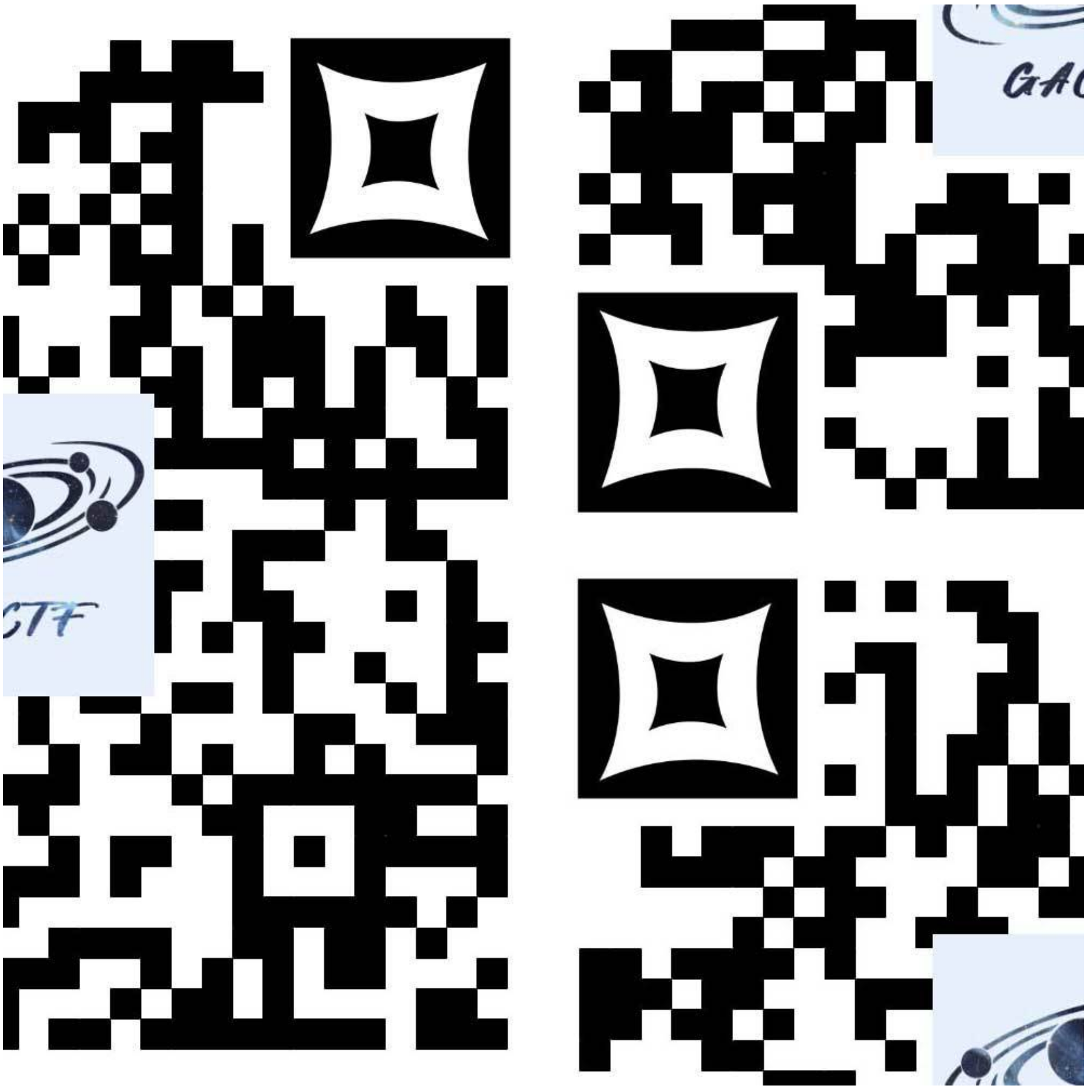
2020GACTF misc复现

国际赛的题真的好懵啊,还找不到太多wp复现学习,孩子傻了

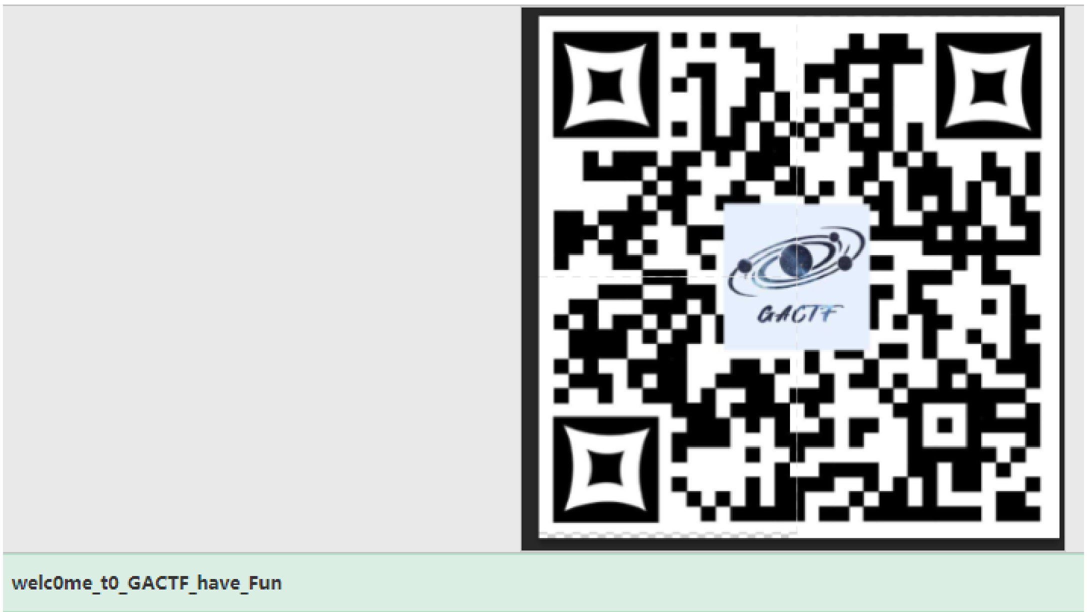
SignIN

题目描述:内容裹上GACTF{}后提交
submit with GACTF{}
交流群：QQ：282546 TG：https://t.me/GACTF
解题步骤:



ps修复一下二维码

在线网址识别一下tools.jb51.net/transcoding/trans_qrcode

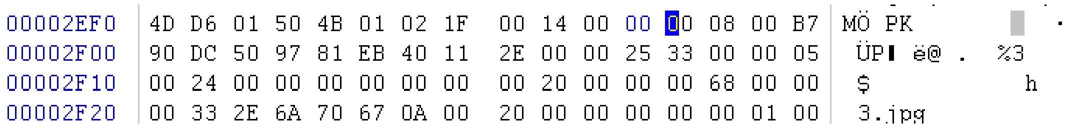


welc0me_t0_GACTF_have_Fun

welc0me_t0_GACTF_have_Fun

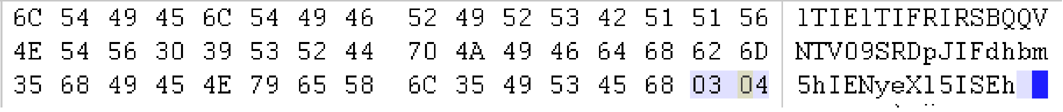
crymisc

题目描述:8.25 is Chinese Valentine's Day.Yesterday my brother told me he was refused by a beautiful girl.He was sooooooooooooo sad and bursted into tears.
链接：https://pan.baidu.com/s/1EZzhnAa5Q4OD8y-YEAcjzQ
提取码：866h
https://drive.google.com/drive/folders/1gDfMBrtqwvi7f9BaB1ixjogeLDascjED?usp=sharing
解题步骤:
下载是个docx文档,打开错误,于是把包解压拆开,得到一个1.txt和加密的图片
I'm going to tell her how i feel.DO YOU WANT TO KNOW WHAT I TOLD HER?
图片解伪加密可得



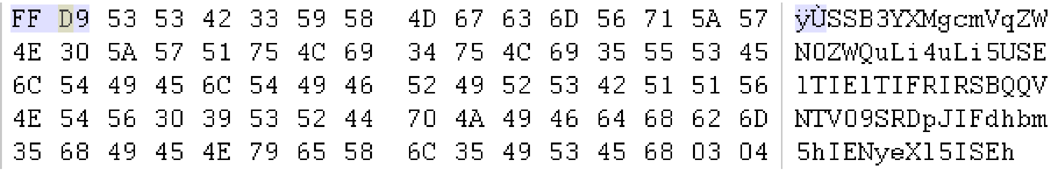
```
00002EF0  4D D6 01 50 4B 01 02 1F  00 14 00 00 00 08 00 B7  MÖ PK
00002F00  90 DC 50 97 81 EB 40 11  2E 00 00 25 33 00 00 05   ÜP▌ ë@ .  %3
00002F10  00 24 00 00 00 00 00 00  00 20 00 00 00 68 00 00   $          h
00002F20  00 33 2E 6A 70 67 0A 00  20 00 00 00 00 00 01 00   3.jpg
```

分析图片结尾有带有pk标志头的crymisc.txt,观察明显信息后有0304,手动补头504B并提取得到加密压缩包



```
6C 54 49 45 6C 54 49 46  52 49 52 53 42 51 51 56  lTIElTIFRIRSBQQV
4E 54 56 30 39 53 52 44  70 4A 49 46 64 68 62 6D  NTV09SRDpJIFdhbm
35 68 49 45 4E 79 65 58  6C 35 49 53 45 68 03 04  5hIENyeXl5ISEh
```

因为FFD9后接的数据不影响整体,这一串应该是密码

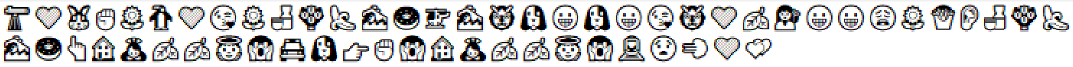


```
FF D9 53 53 42 33 59 58  4D 67 63 6D 56 71 5A 57  ÿÙSSB3YXMgcmVqZW
4E 30 5A 57 51 75 4C 69  34 75 4C 69 35 55 53 45  N0ZWQuLi4uLi5USE
6C 54 49 45 6C 54 49 46  52 49 52 53 42 51 51 56  lTIElTIFRIRSBQQV
4E 54 56 30 39 53 52 44  70 4A 49 46 64 68 62 6D  NTV09SRDpJIFdhbm
35 68 49 45 4E 79 65 58  6C 35 49 53 45 68 03 04  5hIENyeXl5ISEh
```

SSB3YXMgcmVqZWN0ZWQuLi4uLi5USElTIElTIFRIRSBQQVNTV09SRDpJIFdhbm5hIENyeXl5ISEh

解个base64得 I was rejected......THIS IS THE PASSWORD:I Wanna Cryyy!!!

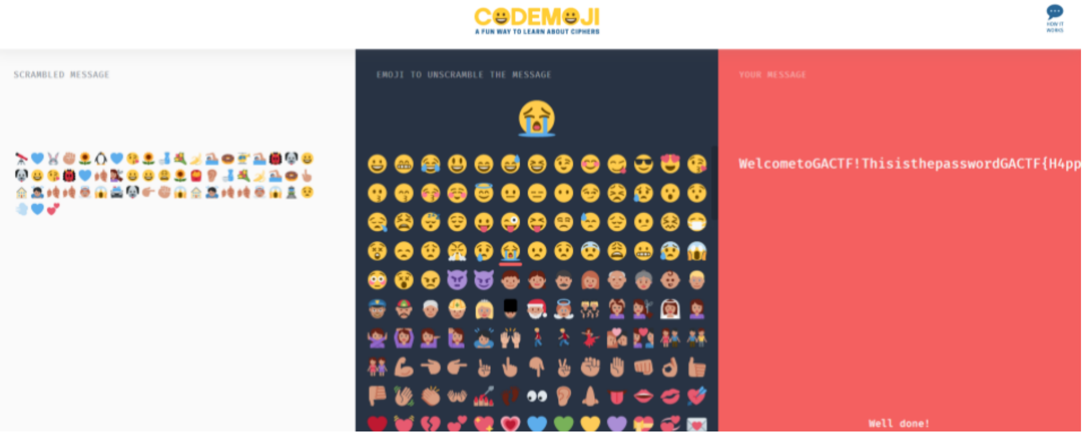
得到一串emoji密码



That is what i told her↑↑↑

在线网址解密 https://codemoji.miaotony.xyz/#/landing

根据cry!!!!!选择大哭的密钥



CODEMOJI
A FUN WAY TO LEARN ABOUT CIPHERS
HOW IT WORKS
SCRAMBLED MESSAGE
EMOJI TO UNSCRAMBLE THE MESSAGE
YOUR MESSAGE

WelcometoGACTF!ThisisthepasswordGACTF{H4pp

Well done!

这个网站后面好像炸了,可以用某个脚本解密

https://github.com/pavelvodrazka/ctf-writeups/tree/master/hackyeaster2018/challenges/egg17/files/cracker

WelcometoGACTF!ThisisthepasswordGACTF{H4ppy_Mi5c_H4ppy_L1fe}

oldmodem

题目描述:old modem (bell 202)

China:

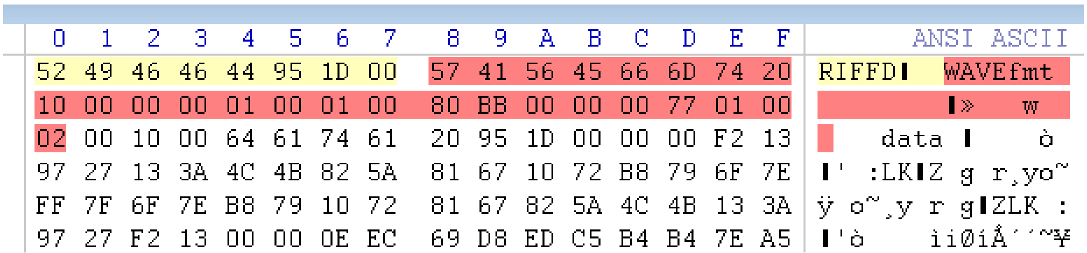
https://pan.baidu.com/s/184Trg9M94uVSekGycaAR_w (密码:5mp2)

Overseas:

https://drive.google.com/drive/folders/1T94OrcveHAZTmTCwaVCojLXYIJc3lL3f?usp=sharing

解题步骤:

oldmodem文件带PK头,解压得到encoded文件,看到有wav文件头



```
     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F    ANSI ASCII
    52 49 46 46 44 95 1D 00  57 41 56 45 66 6D 74 20  RIFFD▌  WAVEfmt 
    10 00 00 00 01 00 01 00  80 BB 00 00 00 77 01 00          ▌»   w 
    02 00 10 00 64 61 74 61  20 95 1D 00 00 00 F2 13      data ▌    ò
    97 27 13 3A 4C 4B 82 5A  81 67 10 72 B8 79 6F 7E  ▌'  :LK▌Z g r¸yo~
    FF 7F 6F 7E B8 79 10 72  81 67 82 5A 4C 4B 13 3A  ÿ o~¸y r g▌ZLK :
    97 27 F2 13 00 00 0E EC  69 D8 ED C5 B4 B4 7E A5  ▌'ò     iíØíÅ´´~¥
```

根据bell 202标准提示,使用minimodem工具分析

可直接安装或clone

https://github.com/kamalmostafa/minimodem.git

> apt-get install minimodem
> # ubuntu安装minimodem
> sudo add-apt-repository ppa:kamalmostafa/minimodem
> sudo apt-get update
> sudo apt-get install minimodem

-r 指定读取模式

-f 选择读取的文件

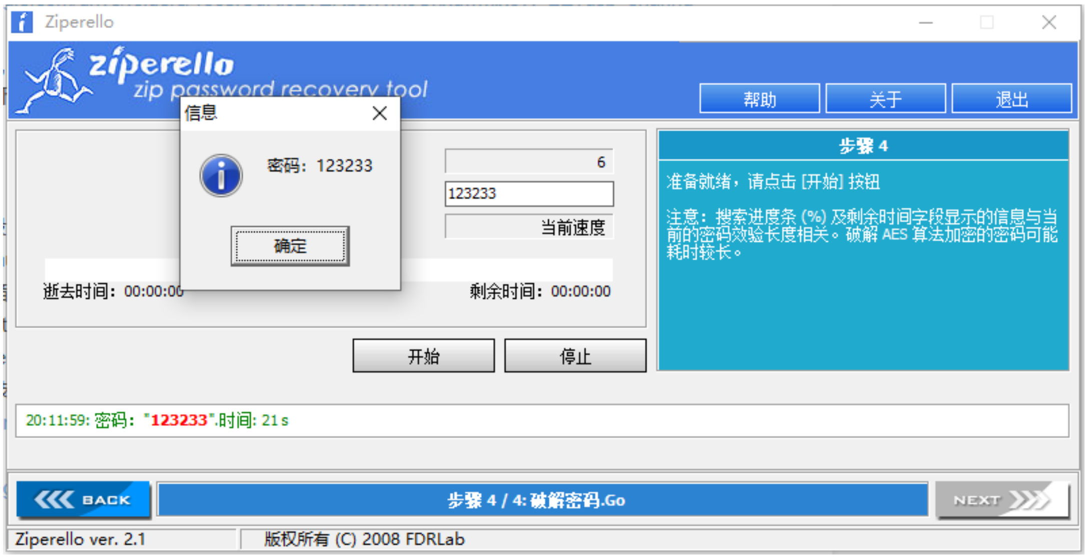
1200 指定Bell202 1200 bps

> minimodem -r -f encoded 1200
> ### CARRIER 1200 @ 1200.0 Hz ###
> The Bell 202 modem was an early (1976) modem standard developed by the Bell System. It specifies audio frequency-shift keying (AFSK) to encode and transfer data at a rate of 1200 bits per second, half-duplex (i.e. transmission only in one direction at a time). These signalling protocols, also used in third-party modems, are referred to generically as Bell 202 modulation, and any device employing it as Bell-202-compatible.
>
> Bell 202 AFSK uses a 1200 Hz tone for mark (typically a binary 1) and 2200 Hz for space (typically a binary 0).
> In North America, Bell 202 AFSK modulation is used to transmit Caller ID information over POTS lines in the public telephone network. It is also employed in some commercial settings.
>
> In addition, Bell 202 is the basis for the most commonly used physical layer for the HART Communication Protocol - a communication protocol widely used in the process industries.
>
> Surplus Bell 202 modems were used by amateur radio operators to construct the first packet radio stations, despite its low signalling speed. A modified Bell 202 AFSK modulation, a common physical layer for AX.25, remains the standard for amateur VHF operation in most areas. Notably, Automatic Packet Reporting System (APRS) transmissions are encoded this way on VHF. On HF, APRS uses Bell 103 modulation.
>
> The Bell 202 standard was adopted around 1980 as the communications standard for subsea oil and gas production control systems, pioneered by the then FSSL (Ferranti Subsea Systems Ltd.) Controls, a spin-out company from the former TRW - Ferranti joint venture in the UK. This modulation standard was retained until around 2000, when it was superseded by faster FSK and PSK modulation methods,

> although it is still utilised for extension of existing control systems that are already configured for this technique.
>
> The 202 standard permitted useful techniques such as multi-dropping of slave modems to allow multiple nodes to be connected to the host via a single modem channel. Other techniques have included superposition of signal on power conductors, and distances in excess of 80 km were achieved in subsea applications using these techniques. This has been enhanced through the use of Manchester encoding over the FSK link, to provide simple Modulo-2 RZ (return to Zero) bit error detection and suppression improvement over these long distances.
>
> Here is the flag: GACTF{9621827f-a41b-4f27-8d72-9e0b77415a4f}
> ### NOCARRIER ndata=2423 confidence=4.397 ampl=0.997 bps=1200.00 (rate perfect) ###

v for Vendetta

题目描述:v is the hero in my mind
hint1:注意每一帧图片的不同之处(Pay attention to the difference in each frame)
hint2:尝试找出藏在GIF图片内的二维码(Try to find the QR code hidden in the GIF picture)
China：
链接: https://pan.baidu.com/s/13kf30SUo4V2RDSp6tT77fA
提取码：xnio
Overseas:
https://drive.google.com/drive/folders/185sICdRI9zVERbsiWMJChxdwmIx6W-QE?usp=sharing
解题步骤:
是个加密压缩包,readme.txt里提示 the password is pure six digit numbers.纯六位数字
ziperello爆破一下,密码是123233



密码：123233

6

123233

当前速度

逝去时间：00:00:00

剩余时间：00:00:00

步骤 4

准备就绪，请点击 [开始] 按钮

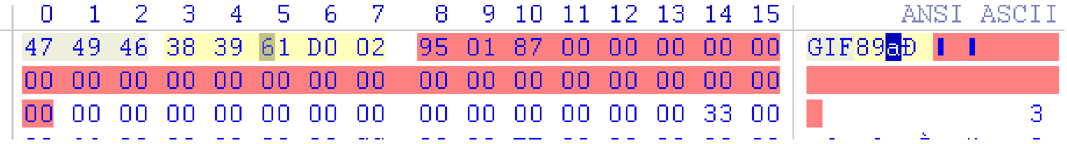
注意：搜索进度条 (%) 及剩余时间字段显示的信息与当前的密码效验长度相关。破解 AES 算法加密的密码可能耗时较长。

20:11:59: 密码："123233".时间: 21 s

步骤 4 / 4: 破解密码.Go

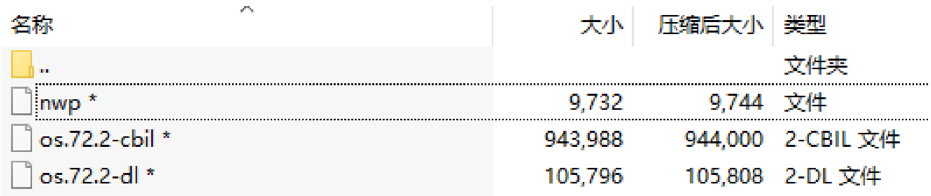
Ziperello ver. 2.1 版权所有 (C) 2008 FDRLab

解出来一个两百多m的文件,拖进winhex分析,头部有89a标识,尾部有一些pk头
头部补上474946,改后缀gif,得到一张超大的图片



```
  0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15        ANSI ASCII
 47 49 46 38 39 61 D0 02  95 01 87 00 00 00 00 00   GIF89aÐ
 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00  00 00 00 00 00 00 33 00                 3
```

没办法,先foremost一下,分离出三个文件



名称	大小	压缩后大小	类型
..			文件夹
nwp *	9,732	9,744	文件
os.72.2-cbil *	943,988	944,000	2-CBIL 文件
os.72.2-dl *	105,796	105,808	2-DL 文件

好像是macos自带的一些东西,还是根据hint逐帧分析吧

Frame : 1 of 3583

在第847帧有一张贼小贼小的图片,ps放大看就是个小像素块,人傻了