

Hgame-week1 Wp

Hgame-week1 Wp

Misc

Sign In

神秘的海报

e99p1ant_wan

Reverse

test your IDA

Crypto

神秘的电话（未解出）

纯纯小白之路

Misc


Sign In

base 64解码

Decode from Base64 format


Simply enter your data then push the decode button.

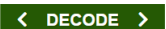

```
aGdhbWV7V2VsY29tZW9Ub19IR0FNRTlwMjMhQ==
```

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8  Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

 Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

 **DECODE**  Decodes your data into the area below.

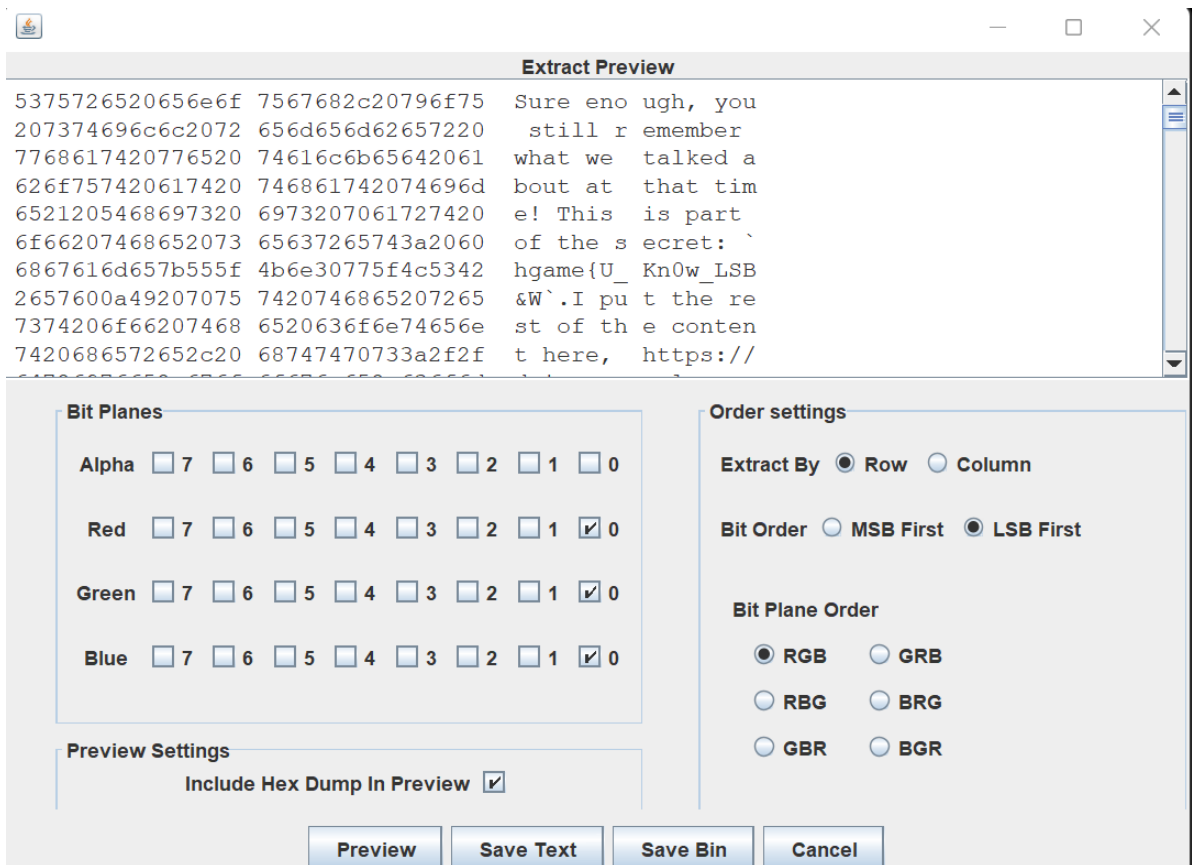
```
hgame{Welcome_To_HGAME2023!}
```

神秘的海报

首先根据题干描述可以知道这是图片隐写。然后回顾了一下misc培训的ppt，得知stegsolve这个软件。

1.下载stegsolve（使用需配置java环境）

2.使用stegsolve对海报进行data extract，得下图



从图中我们可以得到以下信息：

一半flag；一个网址（内容是ek1ng学长喜欢的音乐）；steghide加密；6位公认的数字密码。

3.访问网址，并下载得文件：Bossanova.wav

4.通过steghide解密

（一开始找到的使用方式都是在linux中，奈何还对linux一窍不通，最后在youtube上找到了在windows下的使用方式，，）

steghide使用时本身就会跳出常用参数

加密：steghide embed -cf (文件) -ef (文件)

解密：strghide extract -sf (文件) (-p密码)



得到flag2.txt

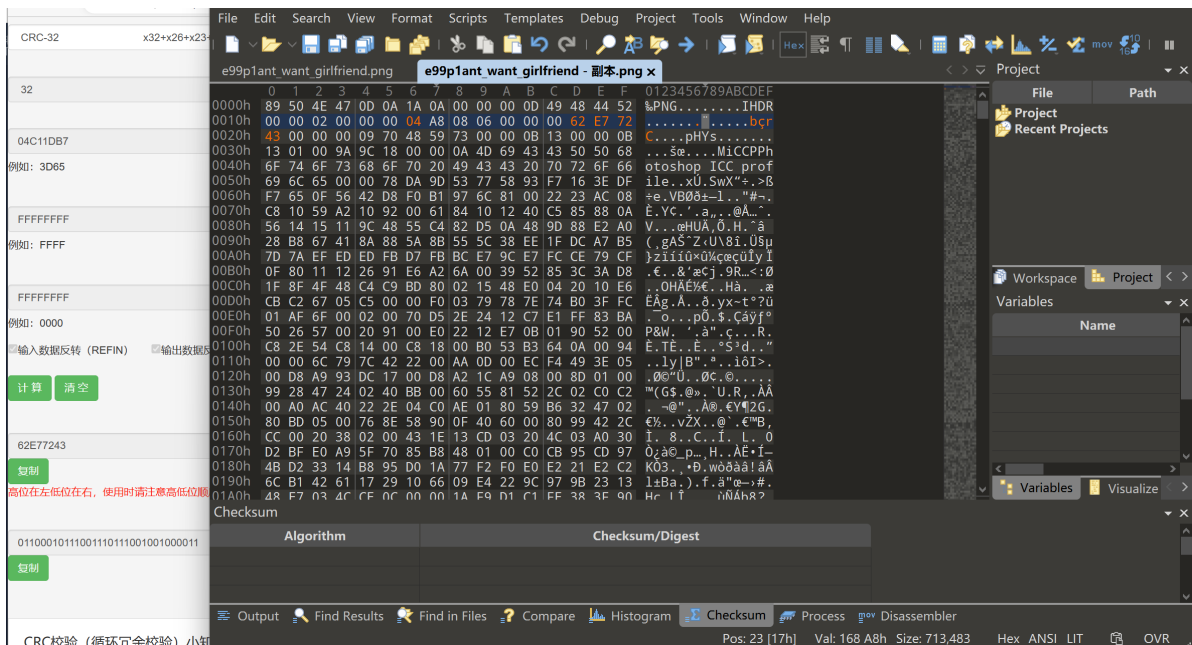
拼接得flag:hgame{U_Kn0w_LSB&Wav^Mp3_Stego}

finish!

（图片隐写，两个工具的使用）

e99p1ant_wan

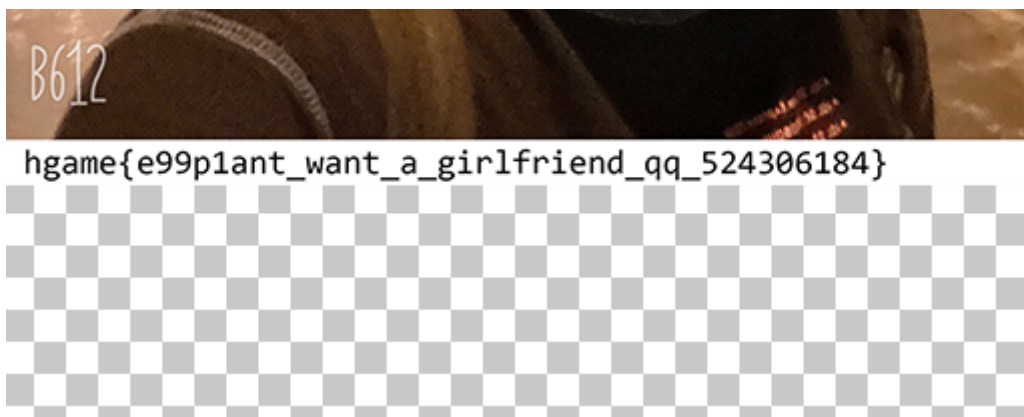
题干提示crc校验不正确，于是在010 Editor修改了一下高并用一个在线网站计算出此时的crc，然后再修改。



相关介绍：

- (1). png的文件头： 8个字节 89 50 4E 47 0D 0A 1A 0A 为 png的文件头(固定);
- (2). 4个字节 00 00 00 0D (即为十进制的13)代表头部数据块的长度为13(固定);
- (3). 4个字节 49 48 44 52 (即为ASCII码的IHDR)是文件头数据块的标示(IDCH)(固定);
- (4). 13位数据块(IHDR)
前四个字节代表该图片的宽 00 00 02 00
后四个字节代表该图片的高 00 00 04 A8
后五个字节依次为: Bit depth、ColorType、 Compression method、 Filter method、 Interlace method
(可变)
- (5). 剩余四字节为该png的CRC检验码， 由从IDCH到THDR的十七位字节进行crc计算得到。(可变)

最后打开图片得flag。

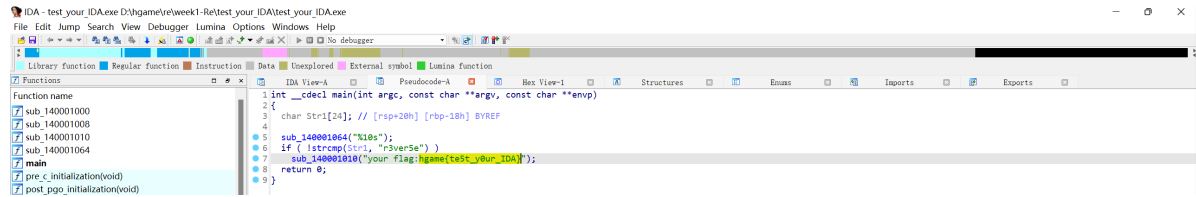


finish!

Reverse

test your IDA

先按空格键切换成文本结构的反汇编，然后按F5进行反编译跳转至伪代码界面。（IDA快速入门手册）



Crypto

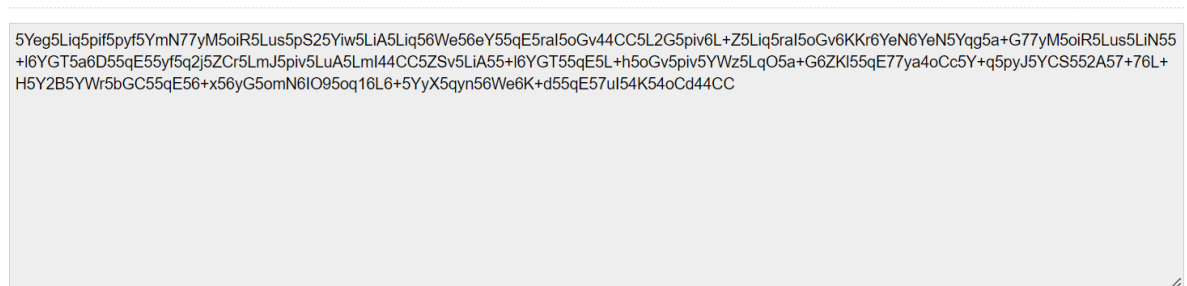
神秘的电话（未解出）


附件是一个加密文件和一段莫斯密码

首先base64解密:

Decode from Base64 format

Simply enter your data then push the decode button.



 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8

Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF

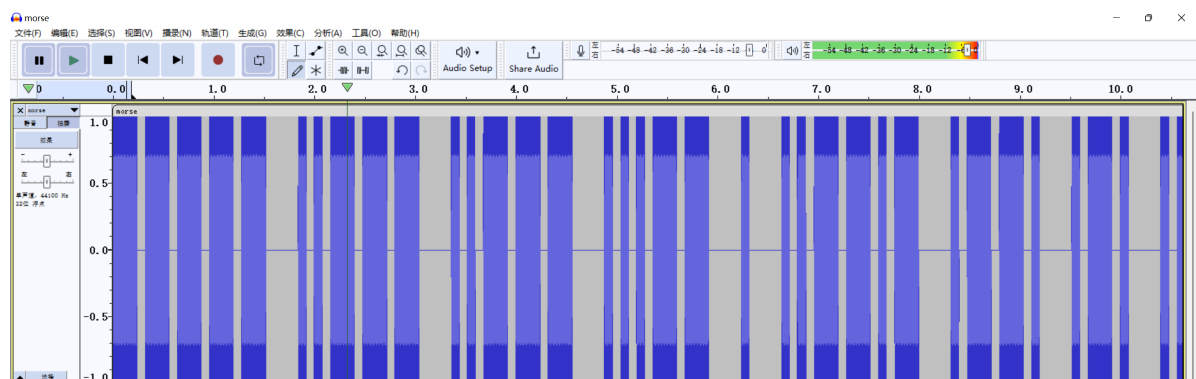
Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE >

Decodes your data into the area below.

几个星期前，我们收到一个神秘的消息。但是这个消息被重重加密，我们不知道它的真正含义是什么。唯一知道的信息是关于密钥的：“只有倒着翻过十八层的篱笆才能抵达北欧神话的终点”。

然后打开morse的音频



得到摩斯密码：----/.--/.---/..././.-/-./-././..../.-/-/-/--./..-/.....---/./-/-/./.-/-/---/-/-./..../-
-/-./.-/-/-/-/-/---/./-/-/-/-/-/..:/.

摩斯密码解密得: 0223epriibly_hona_jmghfgkcqaotmfr

通过“倒着翻过十八层的篱笆”这句话我觉得要用栅栏密码解密，然后得到：

023piby_oaigfkqomrftacghm_nh_lire2

(然后就知道了，感觉应该是哪里出了大问题)