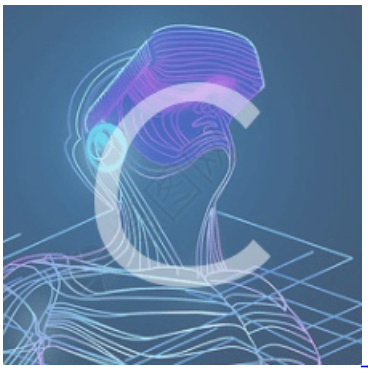
i春秋 misc code_in_morse、套娃

原创

H4ppyD0g 于 2020-03-01 09:32:54 发布 459 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_42172261/article/details/104573497



code_in_morse

wireshark打开pcapng，看到有image/jpeg图片，追踪流看到莫尔斯电码。
在线转换，得到一大堆英文字母串。

观察一下大写字母A-Z，数字2-7，base32编码，解码一下，看到了png头。

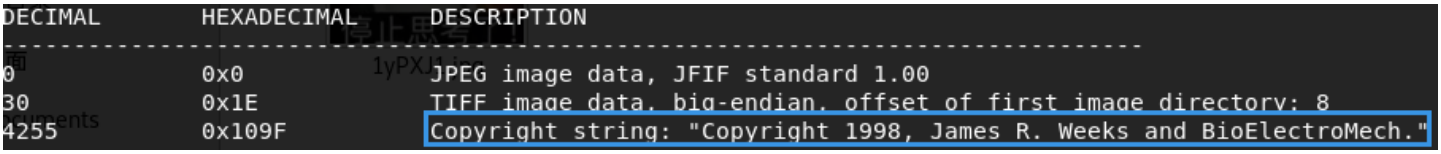
解码写到文件中，其实这个base32编码好像不完整，python解码出错，我就各种加等号直到成功。

```
import base64
ls = ""
with open("C:\\Users\\dell\\Desktop\\1.txt", "r") as fp:
 ls = fp.read()
ls += '='
ls += '='
ls += '='
ls += '='
res = base64.b32decode(ls)
with open("C:\\Users\\dell\\Desktop\\1.png", "wb") as fp:
 fp.write(res)
```

出现一张码，看wp说是条形码。
管他什么，不知道就找在线解密**https://www.sojson.com/qr/deqr.html**

解密出一个url，https://s2.ax1x.com/2020/02/06/1yPXJ1.jpg，访问一下，下载这张图片。

binwalk查看一下图片信息



说是根据蓝框框起来的部分看出是**F5隐写，**

早期F5算法总插入"JPEG Encoder Copyright 1998,James R. Weeks and BioElectroMech"
自己查了一下这个F5隐写，奈何本菜鸡太弱，看不懂，放弃。

命令`java Extract 图片名称 (-p password)`会生成output.txt，flag就在里面。

套娃
题目链接：链接：https://pan.baidu.com/s/1LQHcWVo_e2WeaBaB9NXekA
提取码：rdp5

1
看剧情，发现Ook编码，在线解密一下https://www.splitbrain.org/services/ook
解码出来`dcaf03aa88d038686c5e8067a7a45ff8`,32位十六进制，猜测是md5值。
在线破解了一下是`XYJ`.

多次提到佛啥东西的，应该还有佛语编码吧。

2.zip用`XYJ`解压不行，在用刚才的md5值解压一下就可以了。

2
小黄车上有个二维码，扫一下，显示NOFLAG

直接爆破第二关的zip吧，密码是3302

3
提示虚张声势，应该是zip伪加密了。
使用ZipCenOp.jar解密一下就可以

4
wp说是看到5.zip里面看到4.jpg，所以判定应该是**明文攻击**
一看时间好长啊，问问别人，说是等一会就可以取消了，把文件保存下来就可以。

5
很明显猪圈密码，`FOJIAJIELV`
小写打开6.zip

6
终于出来佛语了，http://www.keyfc.net/bbs/tools/tudoucode.aspx，解密结果`amtf12345`
不知道为啥google解不出来，换成火狐就好了

7
银河密码，解密结果`yinhezm`

8
提示要32位密码，看wp说是1-7关每一关都会有几位，重新来。

part1, winhex

藏在1.连环画.png的末尾，用winhex打开最后就能看见。`part1:068c`

part2， 文件属性

在2.连环画.jpeg文件属性里。`part2：555b`

part3，LSB隐写

Stegsolve打开3.连环画.png，Analyse->Data Extract
`part3:578b`

part4, 修改文件高度

`part4:0eae`

part5, 拼图

`part5:9d4b`

part6, 莫尔斯电码

记事本打开，最后看到莫尔斯电码，解码得到`PART6:e52bd67`

part7, gif隐写

看wp，说是**gif隐写一般两种方式，一种是插帧，另一种就是时间隐写。**

查看时间

`identify -verbose 7连环画.gif |grep Delay`

导出时间

`identify -format “%T” 7连环画.gif`

导出时间得到字符序列
102020201010101010202010101010201020202010102010102020201020101010102020102020201010202020102010101
02020102020101010202010101020101020201020102010102020102020101010202010102010
然后把10转化为0,20转为1，之后得到01串，ascii码转字符后得到`part7:61562`

回到8

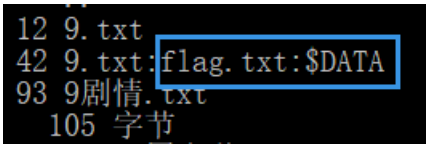
用拿到的32位密码`068c555b578b0eae9d4be52bd6761562`解密9.zip，

知识盲区

在NTFS文件系统中存在着NTFS交换数据流（Alternate Data Streams，简称ADS），这是NTFS磁盘格式的特性之一。每一个文件，都有着主文件流和非主文件流，主文件流能够直接看到；而非主文件流寄宿于主文件流中，无法直接读取，这个非主文件流就是NTFS交换数据流。
ADS的作用在于，它允许一个文件携带着附加的信息。例如，IE浏览器下载文件时，会向文件添加一个数据流，标记该文件来源于外部，即带有风险，那么，在用户打开文件时，就会弹出文件警告提示。再如，在网址收藏中，也会附加一个favicon数据流以存放网站图标。
ADS也被用于一些恶意文件隐藏自身,作为后门。

9， NTFS流隐写

windows下可以使用`dir /r`的方式来查看



发现flag信息，notepad查看flag.txt`notepad 9.txt:flag.txt`，最后终于爆出了flag。