XCTF高校战“疫”网络安全分享赛（隐藏的信息）

原创

Warning 于 2020-03-14 10:15:24 发布 760 收藏 2
分类专栏： 杂项
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/destiny1507/article/details/104855068
版权


杂项 专栏收录该内容
15 篇文章 1 订阅
订阅专栏

知识点：

- 双音多频（拨号音隐写）
- 二维码相关知识

解压完是一个残缺的二维码和一个压缩包。压缩包是加密的，所以我们先看二维码。

二维码很容易看出来需要反色+补上三个小黑块（用于位置探测）（讲真，我以前一直觉得二维码是个很特殊的东西，每一个二维码都是独一无二的，毕竟你看扫出来的东西都不一样嘛……）

这张图片缺少的是位置探测区，这三个小黑块用来确定二维码的大小和位置，帮助我们正确定位二维码里的数据。所以，先用stegsolve对原图进行反色，然后可以在其它二维码上截下来小黑块，再把它贴上去就可以了。

**********更多关于二维码的知识详见：https://www.cnblogs.com/magicsoar/p/4483032.html

（好像广告是怎么回事……我不认识这个博主，但是这篇文章讲的很详细）

贴好的图片：

扫完之后：

```
已解码数据 1:
------------------------------------------------------------------------
位置:(9.9,12.9)-(290.9,11.0)-(10.6,291.5)-(291.6,289.6)
颜色正常, 正像
版本: 4
纠错等级:L, 掩码:0
内容:
flag{this_is_also_not_flag}解压密码不在这里0.0!
------------------------------------------------------------------------
```

（微笑）

看来主要信息在那个压缩包里了。压缩包的名字是纯数字，嗐，这不是明明白白的提示我爆破嘛，连字典都给了。

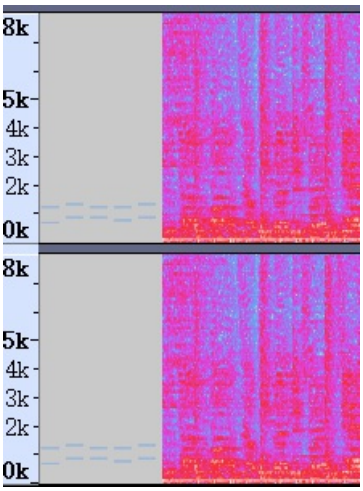
然后我爆了快十分钟……越来越强烈的直觉告诉我：不！不是这样的！

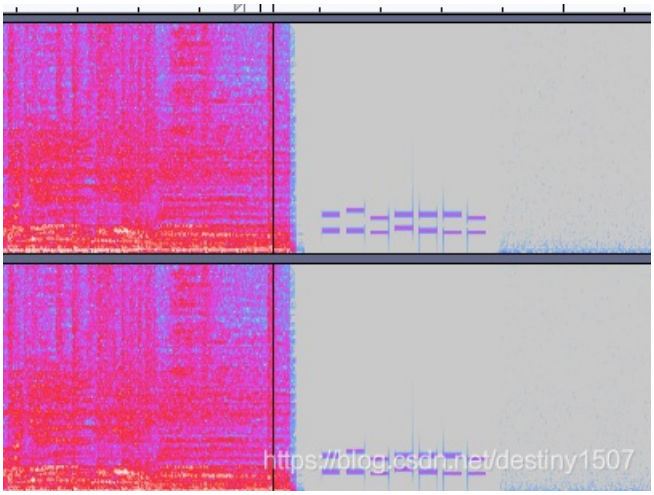
到处都没有提示密码的，那去看看是不是伪加密。果然……

用winhex修改了压缩包之后，顺利解压。里面是个音频文件。

说起来，那这个“纯数字”既然不是密码的提示，提示的可能就是压缩包里面的内容了吧。

使用Audacity打开，听了一遍（虽然对我来说听一遍永远没啥用吧……但架不住好奇）。然后仔细观察频谱图，发现在最前面和最后的部分有一串可疑的东西：





不知道是什么……后来看了wp才知道，这是赤裸裸的双音多频，拨号音隐写。

双音多频，简称DTMF。产生的最初原因是为了完成自动长途呼叫，它由高频群和低频群组成，一个高频信号和一个低频信号叠加组成的信号代表一个数字，利用DTMF信号可选择呼叫相应的对讲机。

双音多频键盘

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

https://blog.csdn.net/destiny1507

在Audacity中读出每一个信号的频率，然后对照这个频率表就可以读出来啦。

或者也可以使用脚本，更快一点：https://github.com/hfeeki/dtmf/blob/master/dtmf-decoder.py