ISCC 2017 writeup(部分)

原创

PrayerYa 于 2017-05-25 12:07:02 发布 3936 收藏
分类专栏： ctf 文章标签： ISCC ctf wav波形隐写

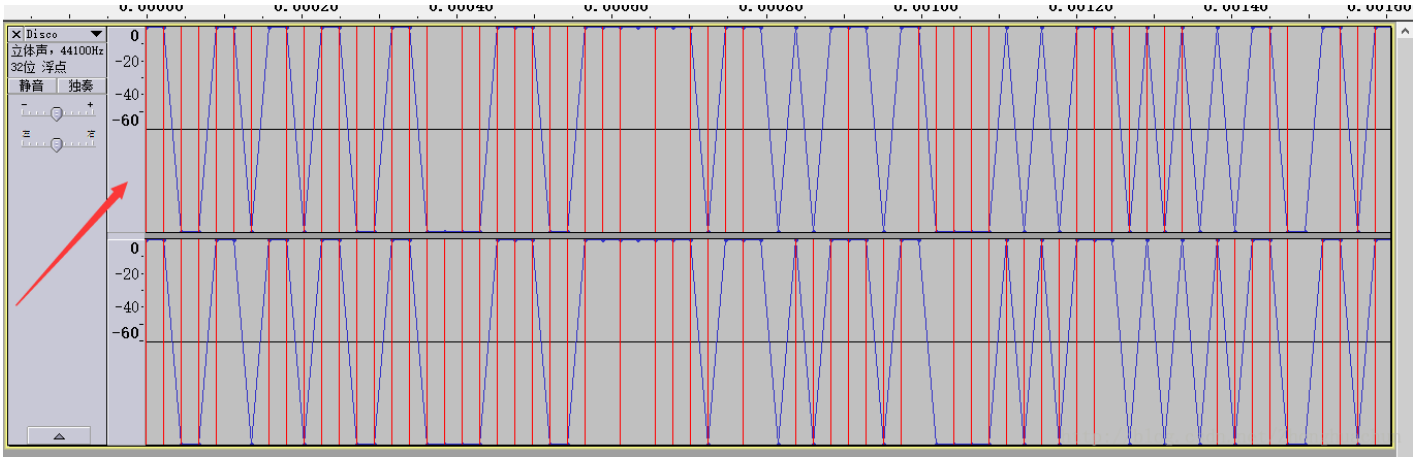
问题描述：普通的DISCO我们普通的摇~~~~

附件是一个wav的音频

开始以为是音频隐写，结果好像错了，然后百度：wav ctf 还真让我找到了另外一种思路：波形谱转换为二进制

这里就要用到一样工具了：Audacity

用工具打开文件后，放大波形谱，果不其然，有东西，23333



开始我以为上面一小横岗代表1，下面则代表0，然后解出来是乱码（ORZ,我也很绝望呀）

后来我发现很多只有一点的太多了

按照上面的思路，这是被忽略的，发现不对劲了，好吧，上面一小点是1，下面一小点是0

得到：

```
1100110110110011000011100111111101110101110110000010101110101010110011011101011011101101
```

一共105位，额，不符合8位一个字符，符合7位，于是在每个7位之前加个0，得到

01100110,01101100,01100001,01100111,01111011,01010111,00110000
01010111,00101010,01100110,01110101,01101110,01101110,01111001,
01111101

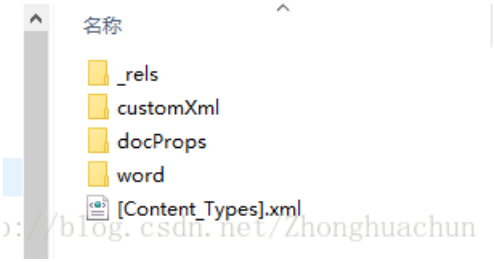
最后二进制转十进制，转ASCII得到：flag{W0W*funny}

眼见非实

给出的附件是一个打不开的word文档，根据题目提示肯定是其他文件类型，用file命令判断一下

```
Misc-02.doc  _mail2LiHua (2).zip.extracted
[root@VM_104_206_centos text]# file Misc-02.doc
Misc-02.doc: Zip archive data, at least v2.0 to extract
[root@VM_104_206_centos text]#
```


再以zip文件解压出来



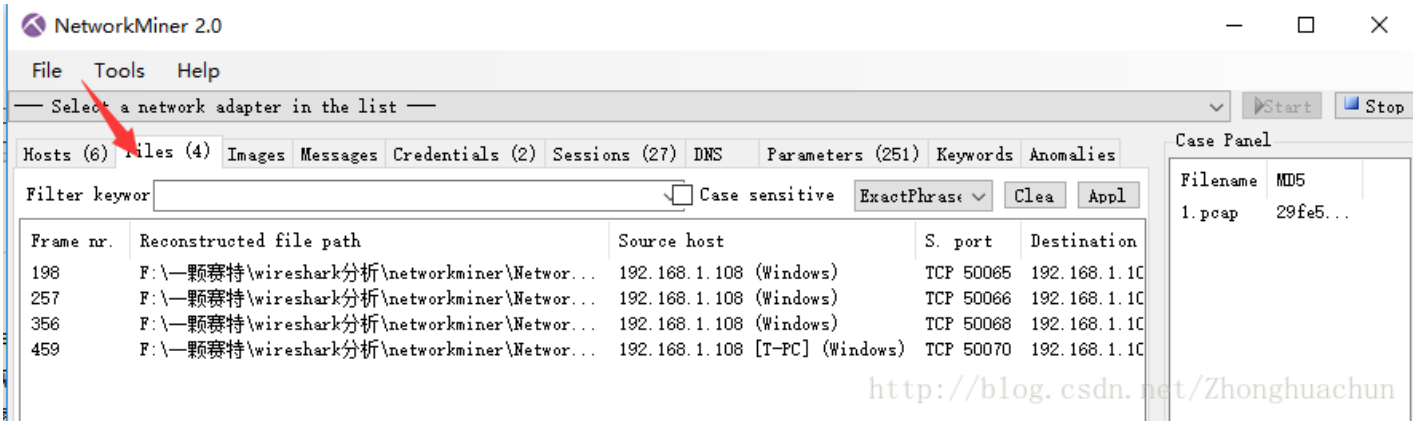
以前见过类似的题，没猜错的话flag就在word/document.xml里面

```
- <w:r>
    <w:t>Flag</w:t>
  </w:r>
- <w:r>
    <w:t>在这里呦！</w:t>
  </w:r>
</w:p>
- <w:p w:rsidRDefault="002B3D8D" w:rsidR="002B3D8I
  - <w:pPr>
    - <w:rPr>
        <w:rFonts w:hint="eastAsia"/>
        <w:vanish/>
      </w:rPr>
    </w:pPr>
  - <w:r w:rsidRPr="002B3D8D">
    - <w:rPr>
        <w:vanish/>
      </w:rPr>
      <w:t>flag{F1@g}</w:t>
    </w:r>
```

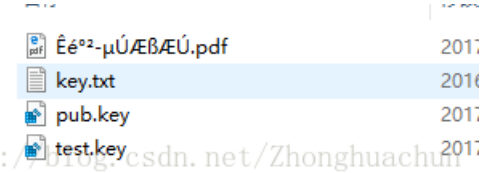

找到了

捕捉到了什么

附件是一个pcapng文件，按照一般套路就是提取文件，这里用到一个工具NetworkMiner，（ps:这个工具只能分析pcap文件，不过可以同wireshark转换格式），打开文件



最后得到以下文件



竟然是openssl,更有趣的是有test.key(该文件保函公钥和私钥)，linux执行命令：openssl rsautl -decrypt -in key.txt -inkey test.key -out flag.txt （解密）

得到flag.txt ,内容：hi, boys and girls! flag is {haPPy_Use_0penSsl}