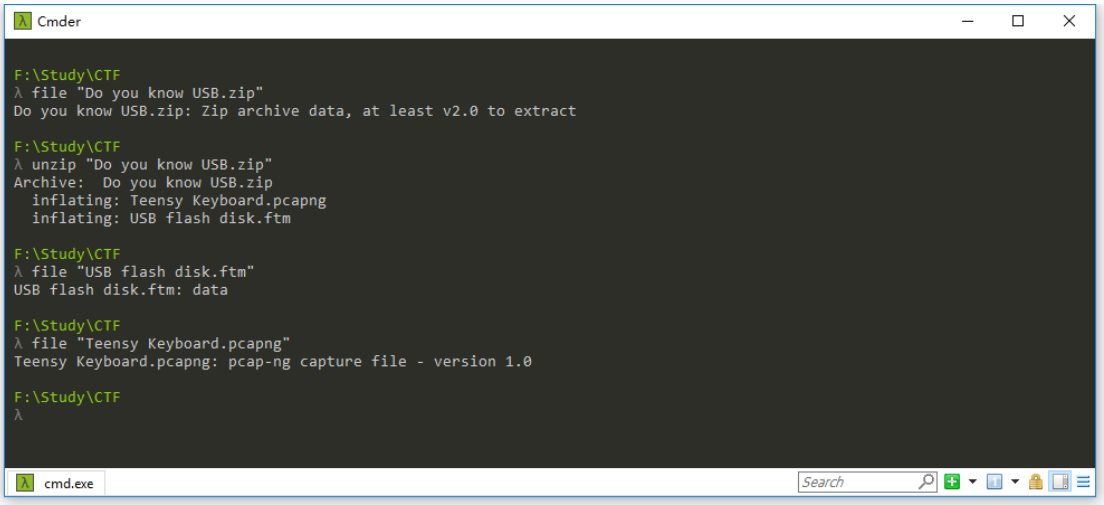
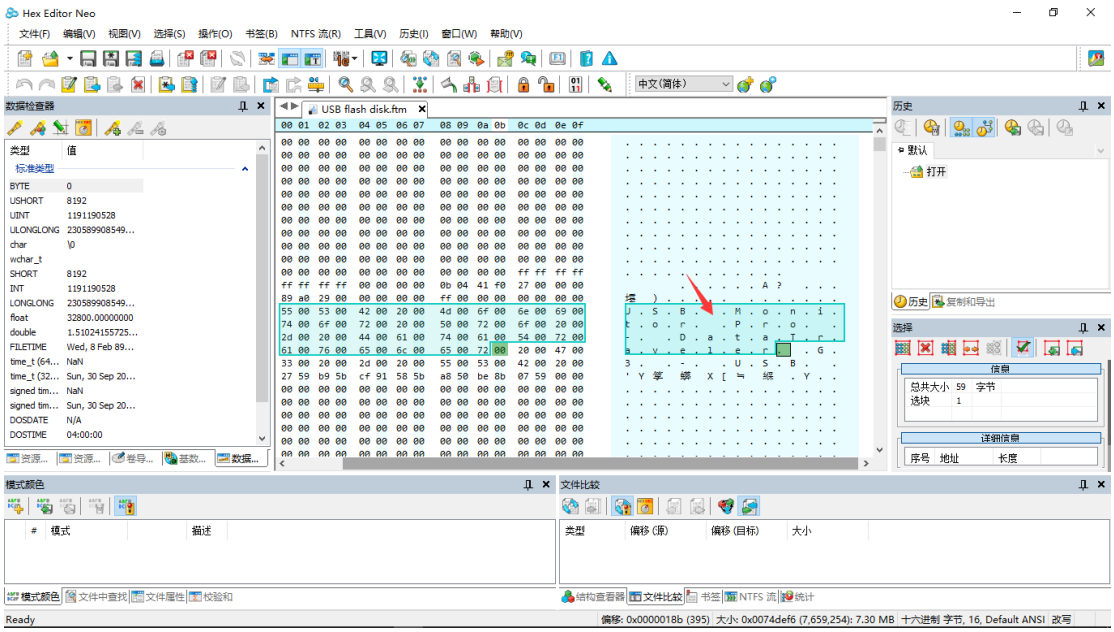
do you know USB write up

1、提取 flag.zip

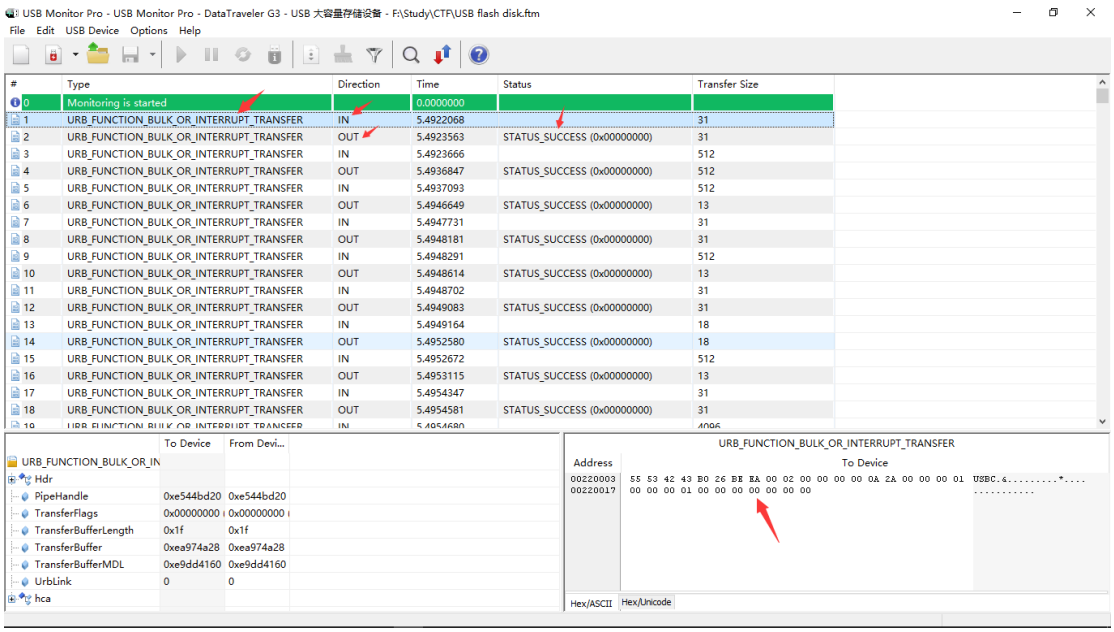
得到题目 Do you know USB.zip 解压得到 USB flash disk.ftm 和 Teensy Keyboard.pcapng 两个文件。



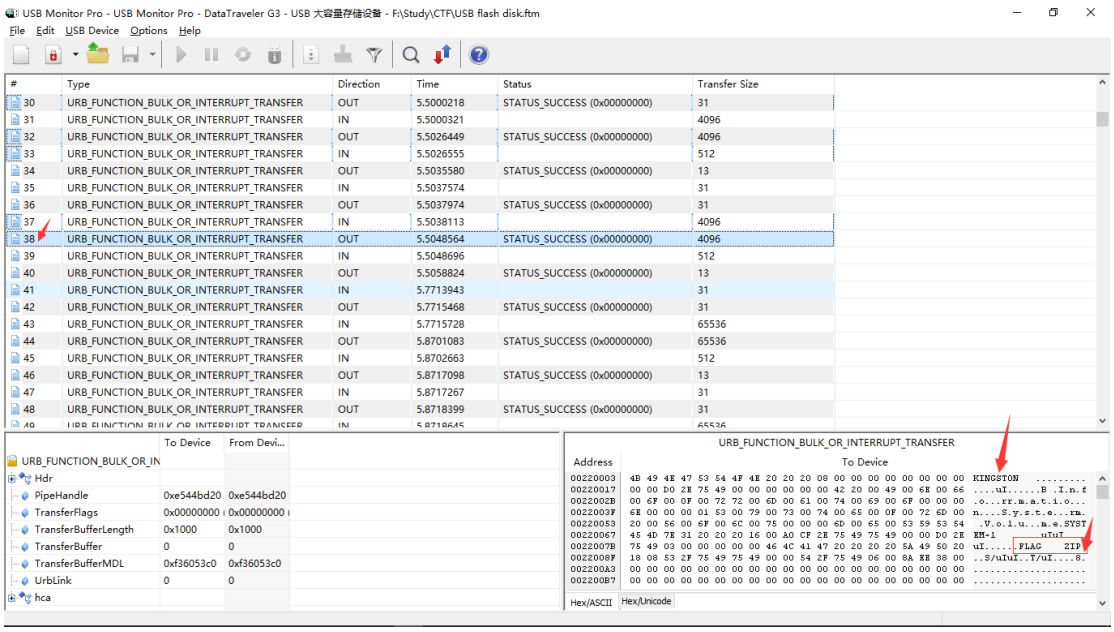
使用 Hex Editor Neo 分析 USB flash disk.ftm，网上查询关于 ftm 格式和 USB Monitor Pro 资料发现，这是 USB 流量抓取和分析工具 USB Monitor Pro 抓取 USB 流量生成的文件。

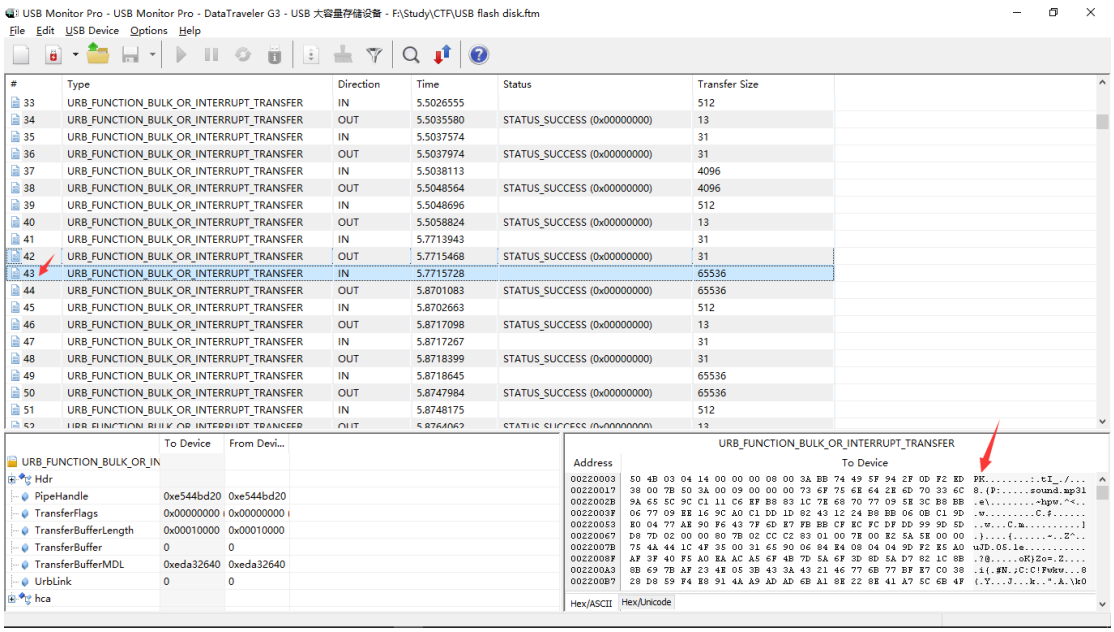


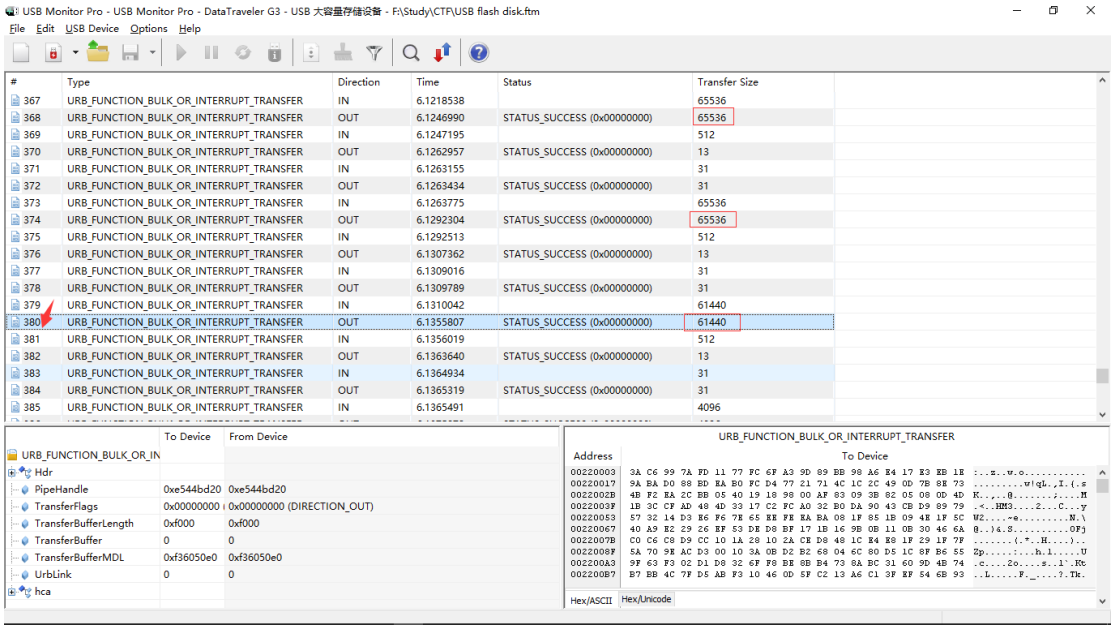
下载使用 USB Monitor Pro，打开 USB flash disk.ftm 分析



网上查阅有关 USB 协议和 URB（USB Request Block）资料，发现 URB_FUNCTION_BULK_OR_INTERRUPT_TRANSFER 这个 URB 功能函数就是 USB 接口的四种数据传输方式中中断传输和批量传输的合并。数据先从（IN）磁盘复制到缓存区，然后从缓存区提取（OUT）到 U 盘。上图右下角的便是传输的数据。



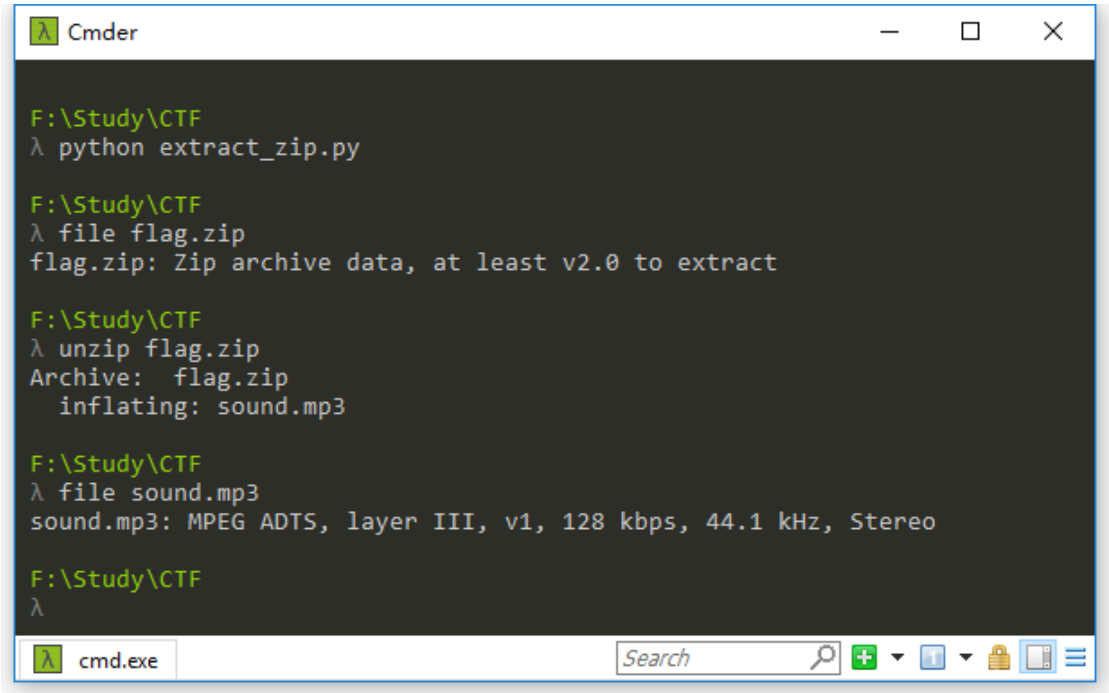




综合分析可知这是主机拷贝 flag.zip 到 KINGSTON U 盘的过程。结合包的大小规律分析可知，而传输 flag.zip 的数据从 43 号包到第 380 号结束。所以编写脚本提取出 flag.zip：

```
#-*- coding:utf-8 -*-
#!/usr/bin/python
# extract_zip.py

ftm_file = open('USB flash disk.ftm', 'rb')
zip_file = open('flag.zip', 'wb')
read_pointer = 46495
```

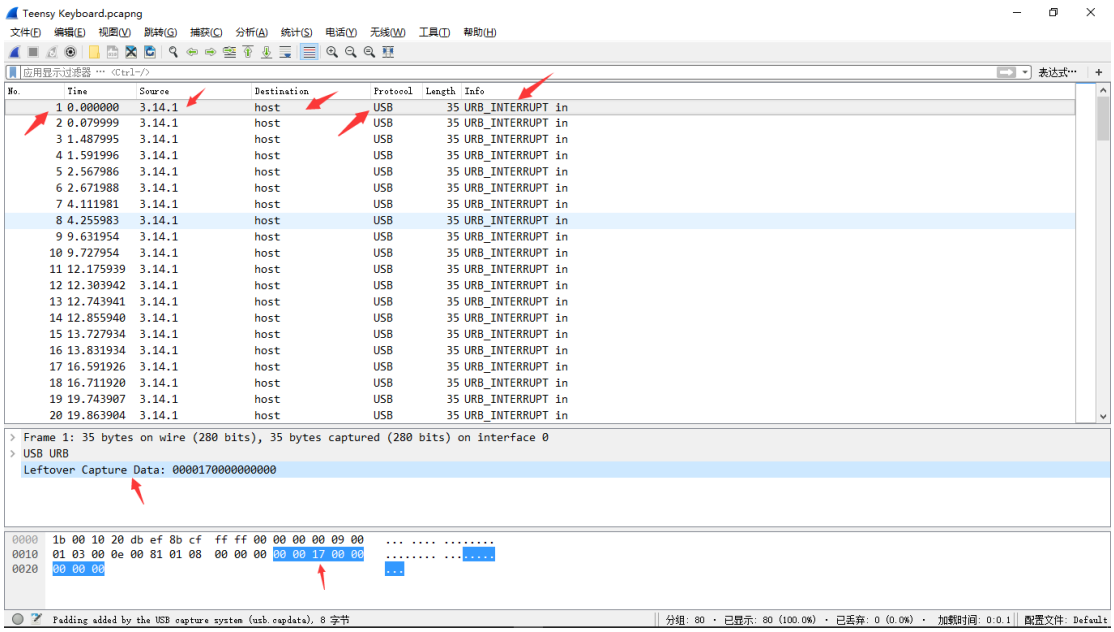
```
offset = 132715
zip_data = ''

#循环读取 56 个大小为 65526 的包
for x in xrange(1, 57):
    ftm_file.seek(read_pointer)
    zip_data += ftm_file.read(65536)
    read_pointer += offset

#读取最后一个大小为 61440 的包
last_read_pointer = 7478535
ftm_file.seek(last_read_pointer)
zip_data += ftm_file.read(61440)

zip_data = zip_data[:-374]#除去尾部填充的无用字节

zip_file.write(zip_data)
```



得到一个 sound.mp3 文件，推测 flag 可能是通过 mp3stego 加密隐藏在 sound.mp3，而还有一个 Teensy Keyboard.pcapng 可能会有一些关于密码的提示，所以着手分析 Teensy Keyboard.pcapng。

2、得到有关密码的提示

用 Wireshark 打开 Teensy Keyboard.pcapng 分析：



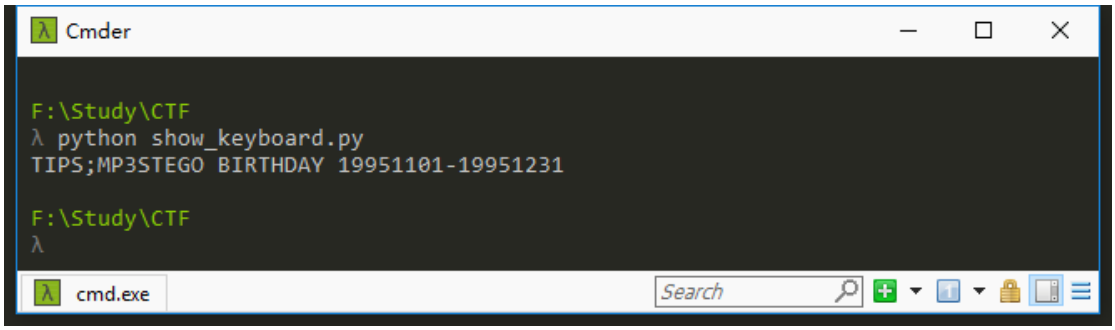
根据文件名 Teensy Keyboard 的提示，在网上查阅关于 Teensy Keyboard 键盘输入映射和 USB 协议结合分析得出这是一个编号 3.23.1 的接口（Teensy Keyboard 键盘）向主机 host 输入的过程。URB_INTERRUPT 是 USB 接口的数据传输方式中的中断传输，而在 USB 协议中 usb.capdata（在 Wireshark 的描述符：Leftover Capture Data）负责储存通过 USB 的传输数据。其中 8 个字节大小的 Leftover Capture Data 中的第三个字节为可显字符，于是将考虑使用 python 的 scapy 模块编写脚本自动提取，先将 pcapng 转换为 scapy 能解析的 pcap 格式：

```
root@kali:~/Desktop# editcap -F libpcap -T ether "Teensy Keyboard.pcapng" "Teensy Keyboard.pcap"
```

```
#!/usr/bin/python
#show_keyboard.py
from scapy.all import *

VISIBLE_KEY_CODES = {
    4: "A",
    5: "B",
    6: "C",
    7: "D",
    8: "E",
    9: "F",
    10: "G",
    11: "H",
    12: "I",
    13: "J",
```

```
    14: "K",
    15: "L",
    16: "M",
    17: "N",
    18: "O",
    19: "P",
    20: "Q",
    21: "R",
    22: "S",
    23: "T",
    24: "U",
    25: "V",
    26: "W",
    27: "X",
    28: "Y",
    29: "Z",
    30: "1",
    31: "2",
    32: "3",
    33: "4",
    34: "5",
    35: "6",
    36: "7",
    37: "8",
    38: "9",
    39: "0",
    40: "\n",
    44: " ",
    45: "-",
    46: "=",
    47: "{",
    48: "}",
    49: "\\",
    51: ";",
    52: "'",
    53: "~",
    54: ",",
    55: ".",
    56: "/",
}

pkts = rdpcap("Teensy Keyboard.pcap")
msg = ""
for packet in pkts:
```

```
    keybord_data = packet.load[-8:]
    key_code = ord(keybord_data[2])
    ch = VISIBLE_KEY_CODES.get(key_code, False)
    if ch:
        msg += ch
print msg
```

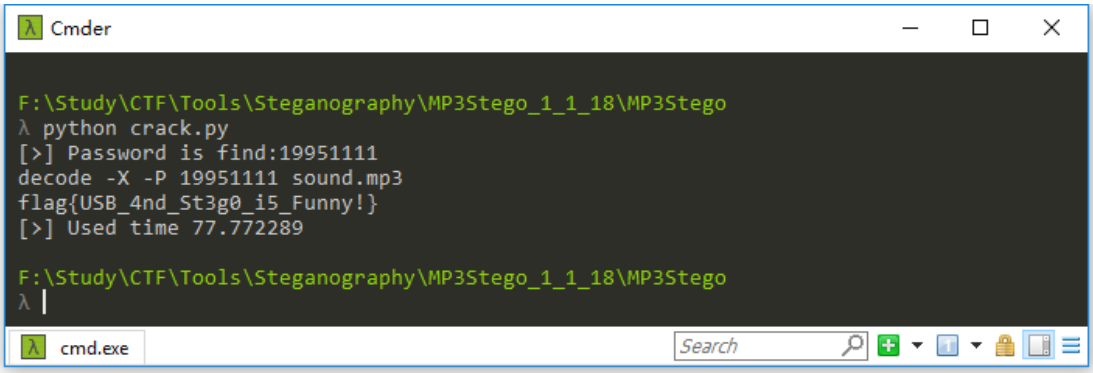


3、编写脚本穷举自动穷举密码提取 flag

提示是 mp3stego，而密码提示是生日，范围在 19951101 到 19951231 于是编写脚本穷举密码获取 flag。

```
#coding=utf-8
#!/usr/bin/python
#crack.py

import os
import subprocess
import time

def password_crack(password):
    command='decode -X -P %s sound.mp3 '% password
    # print command
    p = subprocess.Popen(command, stdin = subprocess.PIPE,
    stdout = subprocess.PIPE, stderr = subprocess.PIPE, shell = True)
    if "unexpected end of cipher message."not in p.communicate()[1]:
        print '[>] Password is find:%s' %password
        print command
        flag = open('sound.mp3.txt')
        print flag.read()
        return True

def generate_birthday():
    start = time.clock()
    year = '1995'
    for month in xrange(11,13):
        month = str(month)
```

```
        for day in xrange(1,32):
            day = str(day).zfill(2)
            birthday = year + month + day
            password_find = password_crack(birthday)
            if password_find is True:
                end = time.clock()
                print '[>] Used time %f' %(end - start)
                exit()

    print '[>] Used time %f' %(end - start)

def main():
    generate_birthday()

if __name__ == '__main__':
    main()
```



最终得到 flag：flag{USB_4nd_St3g0_i5_Funny!}