第一届赣网杯网络安全大赛 2020GW-CTF Misc_Writeup

原创

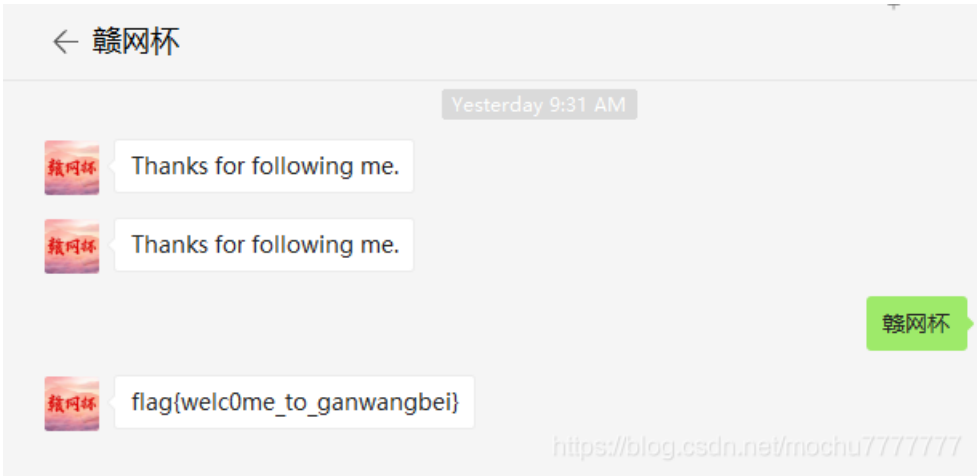
末 初 于 2020-11-07 17:03:38 发布 1650 收藏 11

分类专栏： CTF_MISC_Writeup

本文链接：https://blog.csdn.net/mochu7777777/article/details/109549446

目录

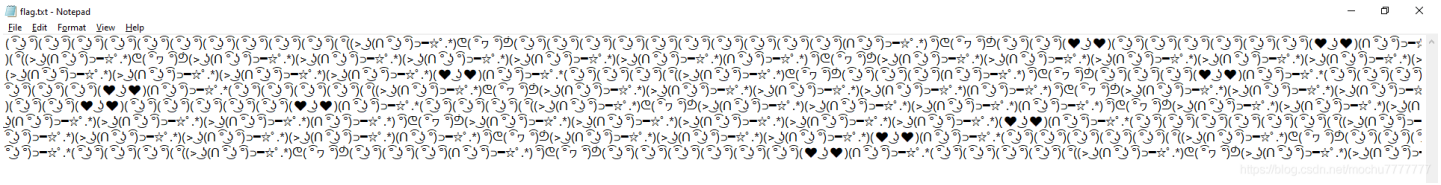
签到Checkin




```
flag{welc0me_to_ganwangbei}
```

face

`Lennyfuck interpreter`



https://github.com/Knorax/Lennyfuck_interpreter

Hi there (°ʖ°)

Hi! This project is a simple interpreter for the (°ʖ°)fuck esoteric language by ivancr72. My goal is to learn how to make interpreters and, eventually, compilers for some other esoteric language, because we obviously need it (~ʖ°). What to keep it mind during this project : it's all for that handsome Lenny. To execute your Lenny code, just call interpreter.py int the command prompt like : `python interpreter.py "pathToMyLennyCode"`

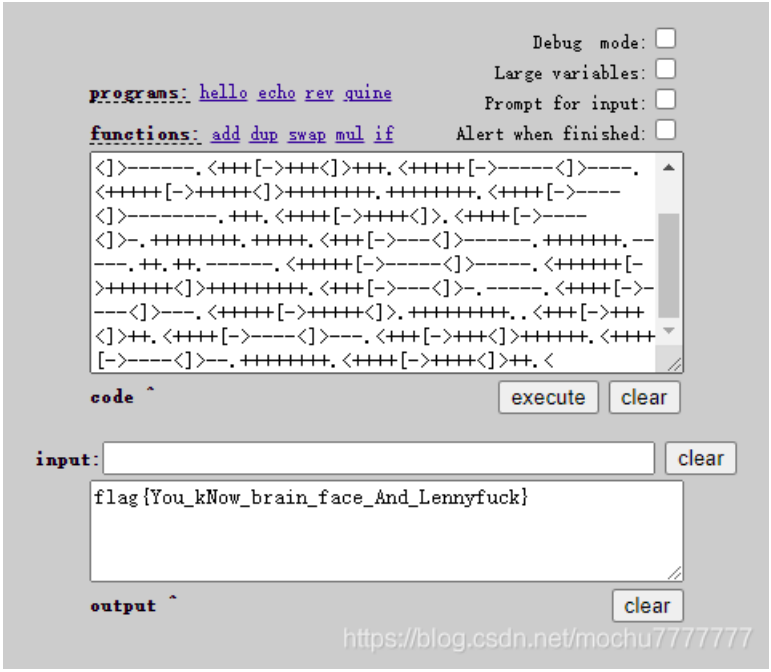
Opcodes

Lenny Command	Brainfuck+3 Command	Description
(°ʖ°)	+	Increment the memory cell under the pointer
(>ʖ<)	-	Decrement the memory cell under the pointer
(♥ʖ♥)	.	Output the character signified by the cell at the pointer
ᕕ(°ʖ°)ᕗ	,	Input a character and store it in the cell at the pointer
(∩°ʖ°)⊃━☆゚.*	<	Move the pointer to the left
ᘿ(°ヮ°)ᕤ	>	Move the pointer to the right
ᘿ(°ʖ°)ᕤ	^	Move the pointer up
(°□ل͜°)	v	Move the pointer down
ಠ_ಠ	x	Exit program.
(°(	[	Jump past the matching] if the cell under the pointer is 0
)°)	]	Jump back to the matching [if the cell under the pointer is nonzero

跟着对照表替换即可

```
++++++++++[->++++++++++<]>++.++++++.<+++[->---<]>--.++++++.<++++[->++++<]>++++.<+++++[->-----<]>---------.<++++[
->++++<]>++++++.++++++.<++++[->----<]>-------.<+++[->+++<]>+++.<+++++[->-----<]>----.<+++++[->+++++<]>++++++++.++
++++++.<++++[->----<]>---------.+++.<++++[->++++<]>.<++++[->----<]>-.++++++++.+++++.<+++[->---<]>------.+++++++.-
----.++.++.-------.<+++++[->-----<]>-----.<++++++[->++++++<]>+++++++++.<+++[->---<]>-.------.<++++[->----<]>---.<+
++++[->+++++<]>.+++++++++..<+++[->+++<]>++.<++++[->----<]>---.<+++[->+++<]>++++++.<++++[->----<]>--.++++++++.<++
++[->++++<]>++.<
```

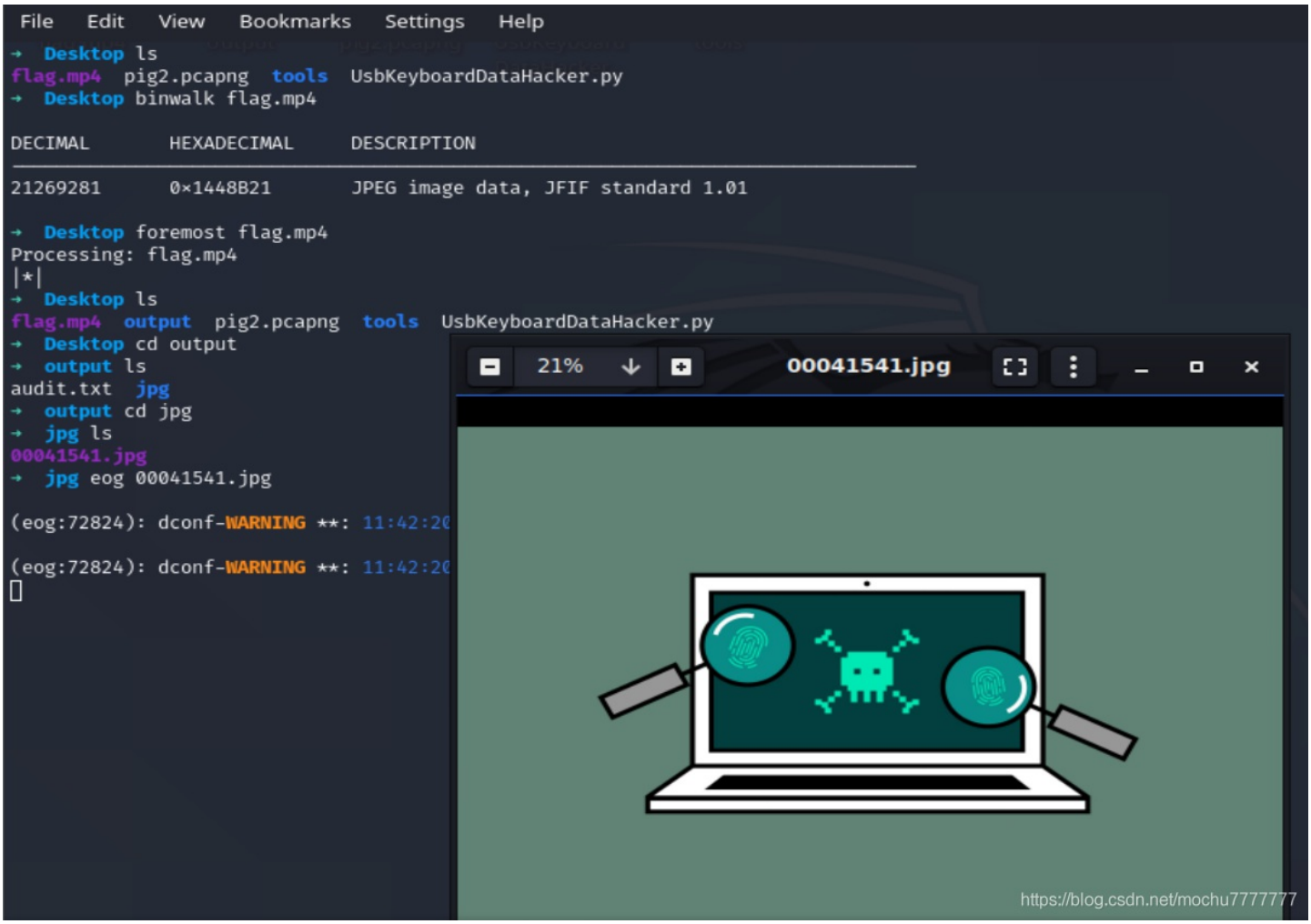
在线解释网站：https://sange.fi/esoteric/brainfuck/impl/interp/i.html



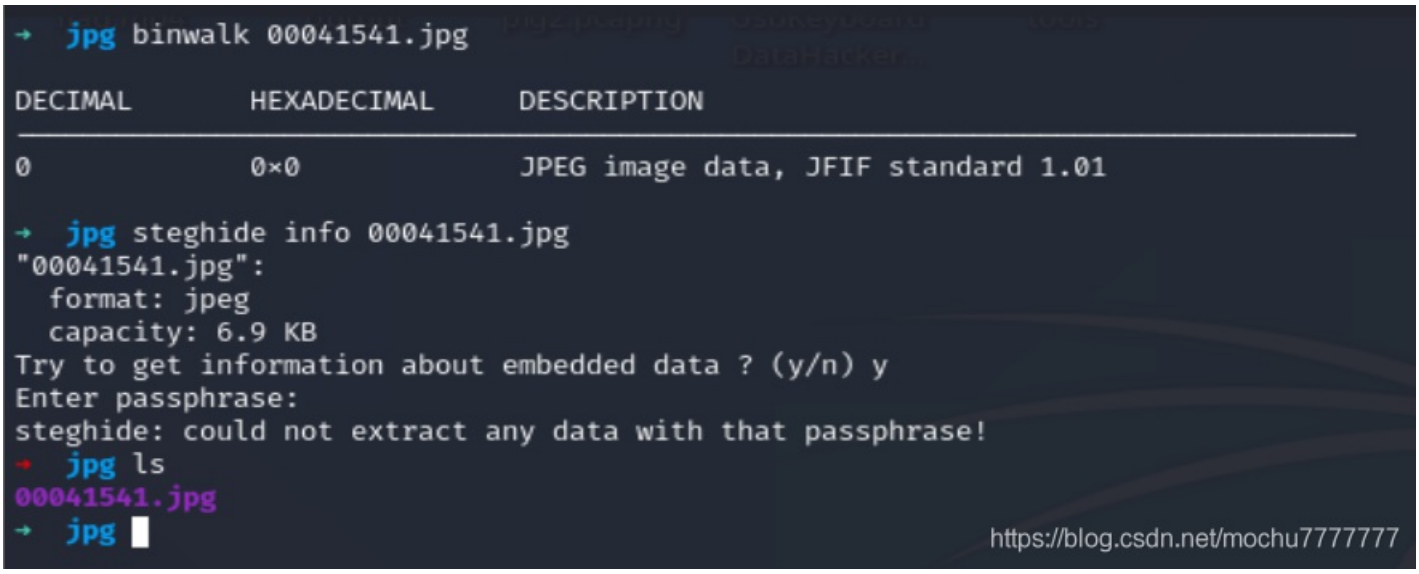

```
flag{You_kNow_brain_face_And_Lennyfuck}
```

DestroyJava

下载附件是`mp4`文件，视频内容是关于销毁JAVA的，并没什么线索，`binwalk`分析，发现有图片隐写在`mp4`文件中，使用`foremost`分离



得到一张`jpg`的图片，`steghide info`探测到`jpg`中隐写了文件



使用脚本爆破密码，

```python
# -*- coding: utf8 -*-
#python2
from subprocess import *

def foo():
    stegoFile='flag.jpg'#这里填图片名称
    extractFile='output.txt'#输出从图片中得到的隐藏内容
    passFile='password.txt'#密码字典

    errors=['could not extract','steghide --help','Syntax error']
    cmdFormat='steghide extract -sf "%s" -xf "%s" -p "%s"'
    f=open(passFile,'r')

    for line in f.readlines():
        cmd=cmdFormat %(stegoFile,extractFile,line.strip())
        p=Popen(cmd,shell=True,stdout=PIPE,stderr=STDOUT)
        content=unicode(p.stdout.read(),'gbk')
        for err in errors:
            if err in content:
                break
        else:
            print content,
            print 'the passphrase is %s' %(line.strip())
            f.close()
            return

if __name__ == '__main__':
    foo()
    print 'ok'
    pass
```

```
→  jpg ls
brute.py  flag.jpg  password.txt
→  jpg python brute.py
wrote extracted data to "hide.txt".
the passphrase is password
ok
→  jpg ls
brute.py  flag.jpg  hide.txt  password.txt
→  jpg cat hide.txt
W^7?+drDz;VP7$GUvy|?Ut&dbbYE;iZfA92XJub$ZeLVrWnXu1a%^OM
→  jpg python3
Python 3.8.5 (default, Aug  2 2020, 15:09:07)
[GCC 10.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import base64
>>> base64.b85decode('W^7?+drDz;VP7$GUvy|?Ut&dbbYE;iZfA92XJub$ZeLVrWnXu1a%^OM')
b'flag{Java_1s_the_bEst_lAnguage_in_The_world}'
>>>
```

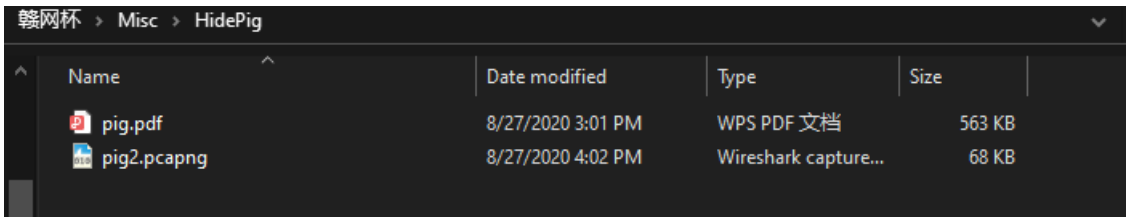

得到密码为：`password`，并且得到隐写的文件`hide.txt`，查看内容发现特征类似`base85`

```
W^7?+drDz;VP7$GUvy|?Ut&dbbYE;iZfA92XJub$ZeLVrWnXu1a%^OM
```

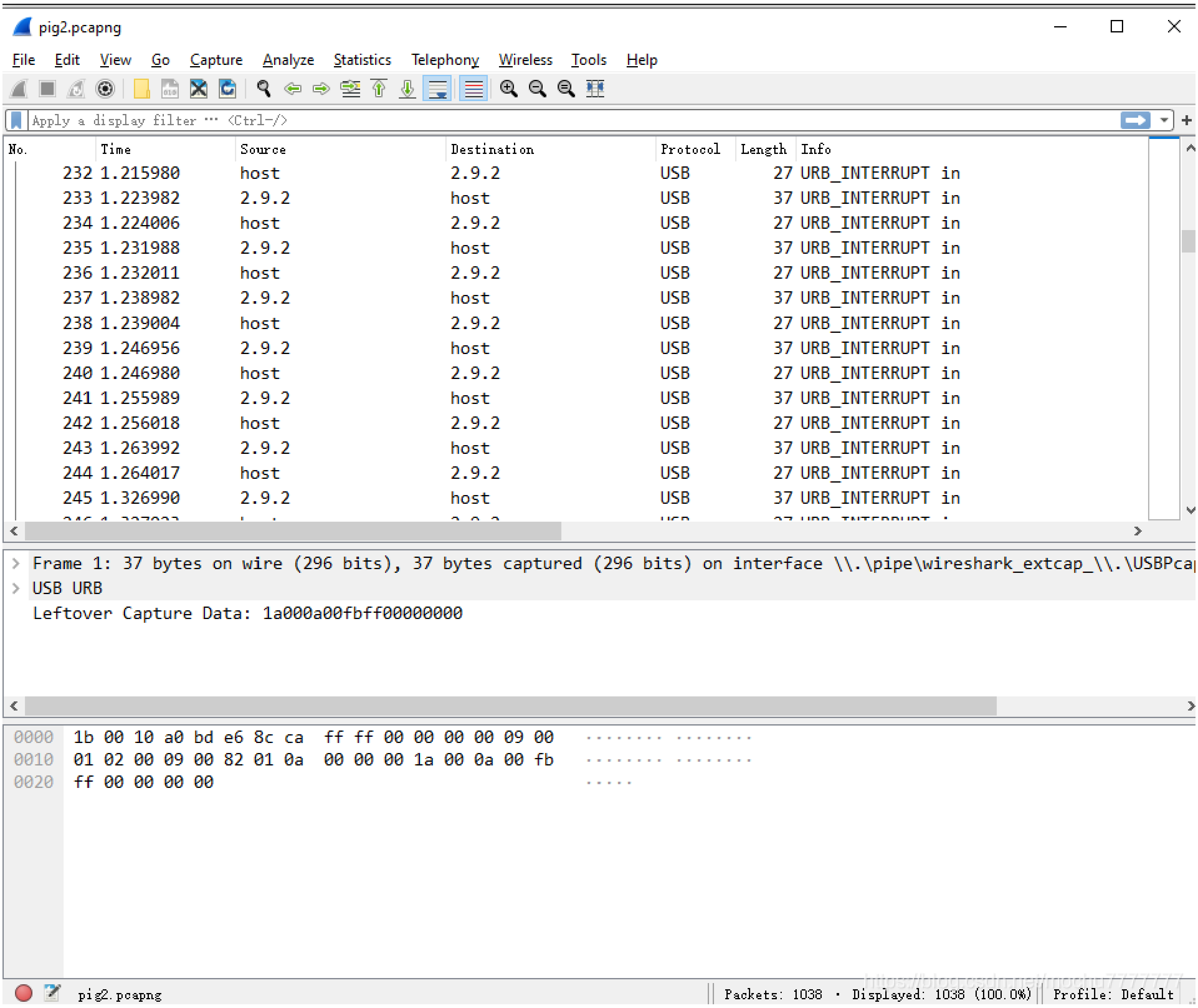
网上的bse85在线解密站好像解不出来，使用python base64模版解决base85解密得到flag

```
flag{Java_1s_the_bEst_lAnguage_in_The_world}
```

Hidepig



`pig.pdf`是母猪的产后护理的资料，猜测应该是`pdf隐写`，使用`wbStego4open`，但是需要输入密码，猜测密码就在`pig2.pcapng`，使用wireshark打开，USB流量分析



USB键盘流量包取证脚本：https://github.com/WangYihang/UsbKeyboardDataHacker

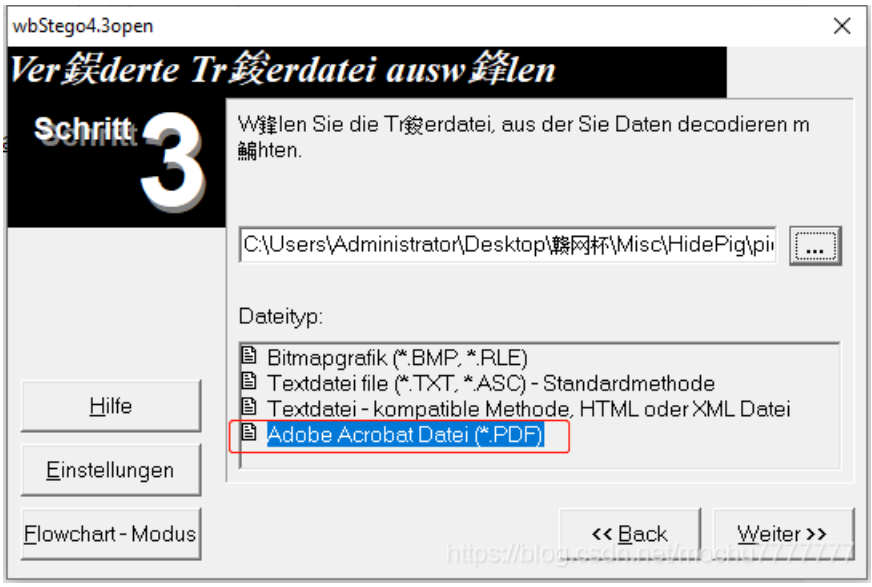
按做法运行一下即可

```
tshark -r ./example.pcap -T fields -e usb.capdata

python UsbKeyboardDataHacker.py ./pig2.pcapng
```

然后使用`wbStego4open`，提取pdf隐藏的文件`

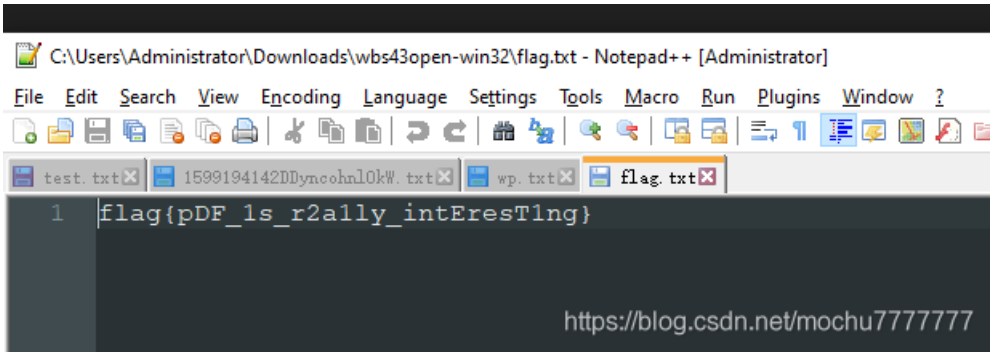
wbStego4open下载地址：http://www.bailer.at/wbstego/fs_download.html


wbStego4.3open
Schritt 3
W鐘len Sie die Tr鍐erdatei, aus der Sie Daten decodieren m
鯆hten.
C:\Users\Administrator\Desktop\鶱冈杯\Misc\HidePig\pi
...
Dateityp:
Bitmapgrafik (*.BMP, *.RLE)
Textdatei file (*.TXT, *.ASC) - Standardmethode
Textdatei - kompatible Methode, HTML oder XML Datei
Adobe Acrobat Datei (*.PDF)
Hilfe
Einstellungen
Flowchart - Modus
<< Back
Weiter >>

填如密码


wbStego4.3open
Schritt 4
Bitte geben Sie das Pa遷ort an, das 慵
die Verschl匱selung der Daten verwendet
wurde.
Wenn keine Verschl匱selung verwendet
wurde, lassen Sie das Eingabefeld leer.
Hilfe
Einstellungen
Flowchart - Modus
<< Back
Weiter >>

选择输出文件




```
flag{pDF_1s_r2a1ly_intEresT1ng}
```