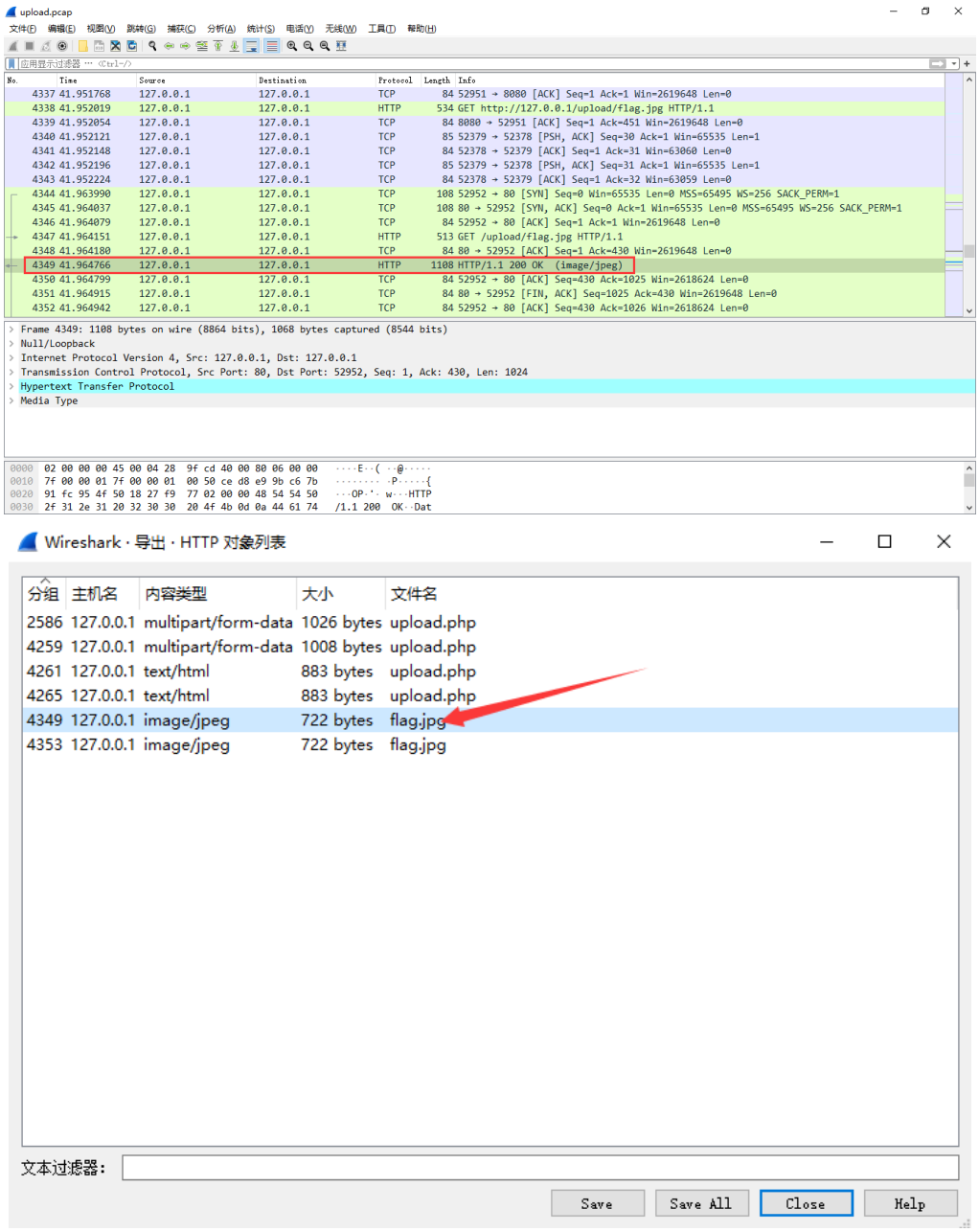
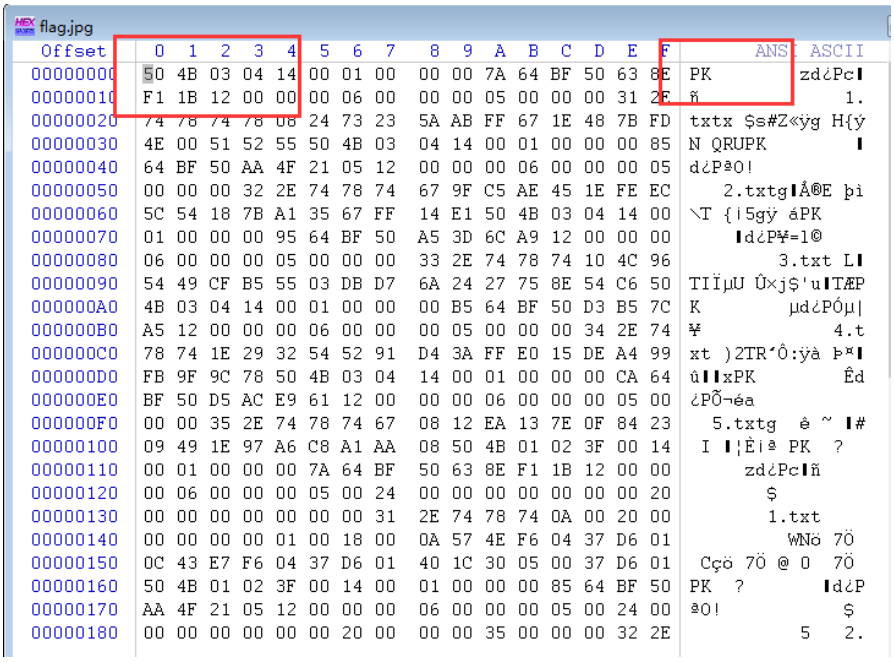
upload（难度：中）

发现上传的图片并导出



图片实际上是一个压缩包，改文件后缀名。



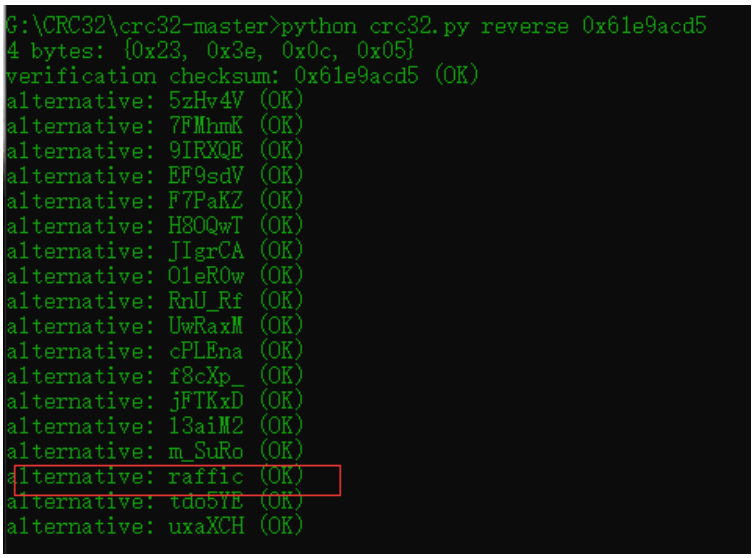
根据压所文件大小猜测 crc 暴破

```
G:\CRC32\crc32-master>python crc32.py reverse 0x1bf18e63
4 bytes: {0x3b, 0x24, 0xe9, 0x6a}
verification checksum: 0x1bf18e63 (OK)
alternative: 7worVu (OK)
alternative: 8x1sqb (OK)
alternative: ARXx7G (OK)
alternative: DwZXDq (OK)
alternative: Ie_WS7 (OK)
alternative: MaBVRT (OK)
alternative: R_wEiX (OK)
alternative: S_6trA (OK)
alternative: TF1JXj (OK)
alternative: W7XXwf (OK)
alternative: XTutT5 (OK)
alternative: Y8GhKh (OK)
alternative: can_U_ (OK)
alternative: ijlnh2 (OK)
alternative: jwvQCz (OK)
alternative: mnqoiQ (OK)
alternative: oRtqOL (OK)
alternative: uICBxv (OK)
alternative: w8kaLc (OK)
alternative: y7tQpm (OK)
```

```
G:\CRC32\crc32-master>python crc32.py reverse 0x05214faa
4 bytes: {0x4c, 0x63, 0x4f, 0x32}
verification checksum: 0x05214faa (OK)
alternative: 22Bt1V (OK)
alternative: 5fhwvu (OK)
alternative: 66_u05 (OK)
alternative: 8tmxa3 (OK)
alternative: KtXRs7 (OK)
alternative: OpESrT (OK)
alternative: QN1qRA (OK)
alternative: VW6Oxj (OK)
alternative: ZErqt5 (OK)
alternative: apiZu_ (OK)
alternative: dhz6n1 (OK)
alternative: fHOt68 (OK)
alternative: find_t (OK)
alternative: hfqIcz (OK)
alternative: if0exc (OK)
alternative: oc96HE (OK)
alternative: r0kZFH (OK)
alternative: wXDGXv (OK)
alternative: zJAHO0 (OK)
```

```
G:\CRC32\crc32-master>python crc32.py reverse 0xa96c3da5
4 bytes: {0xe1, 0x0f, 0x49, 0xb4}
verification checksum: 0xa96c3da5 (OK)
alternative: V8R_s1 (OK)
alternative: fjyYPk (OK)
alternative: gj8hKr (OK)
alternative: gvw4Jf (OK)
alternative: hefile (OK)
alternative: jYcw5x (OK)
alternative: t6u4yq (OK)
alternative: v7afH4 (OK)
alternative: yTLJkg (OK)
```

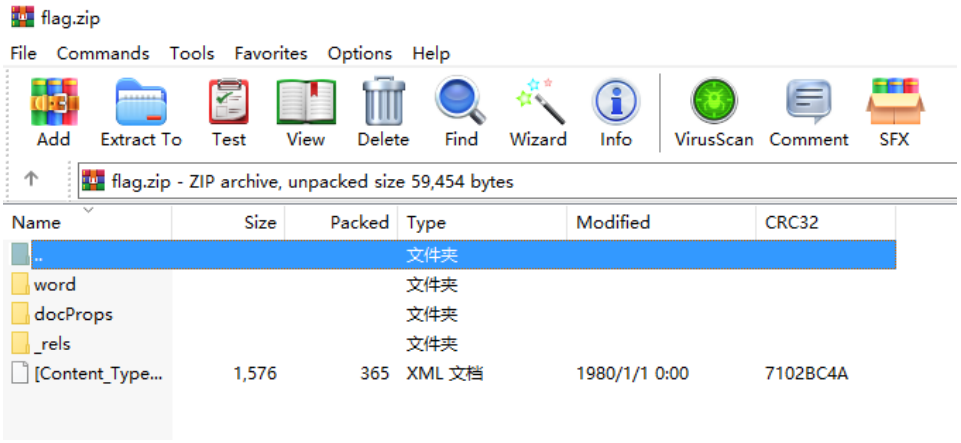
```
G:\CRC32\crc32-master>python crc32.py reverse 0xa57cb5d3
4 bytes: {0xa1, 0xa3, 0x2a, 0xb8}
verification checksum: 0xa57cb5d3 (OK)
alternative: 8o1qa3 (OK)
alternative: NwJ7hY (OK)
alternative: OkDZrT (OK)
alternative: PUqIIX (OK)
alternative: QUOxRA (OK)
alternative: VL7Fxj (OK)
alternative: WLvwcs (OK)
alternative: Yb7W61 (OK)
alternative: akhSu_ (OK)
alternative: from_t (OK)
alternative: nd6RRH (OK)
alternative: odwcIQ (OK)
alternative: u2mm1c (OK)
alternative: wCENXv (OK)
```



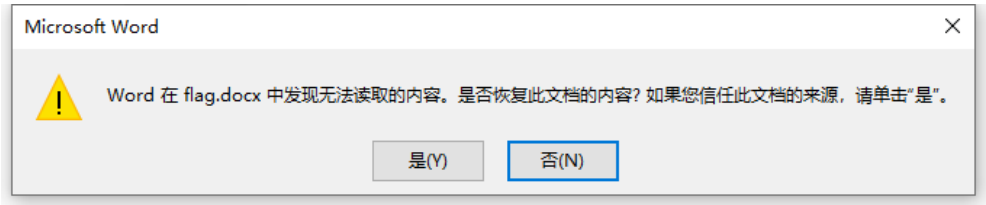
flag： Dozerctf{can_U_find_thefilefrom_traffic}

word（难度：简单）

打开文件发现是个 word 文档



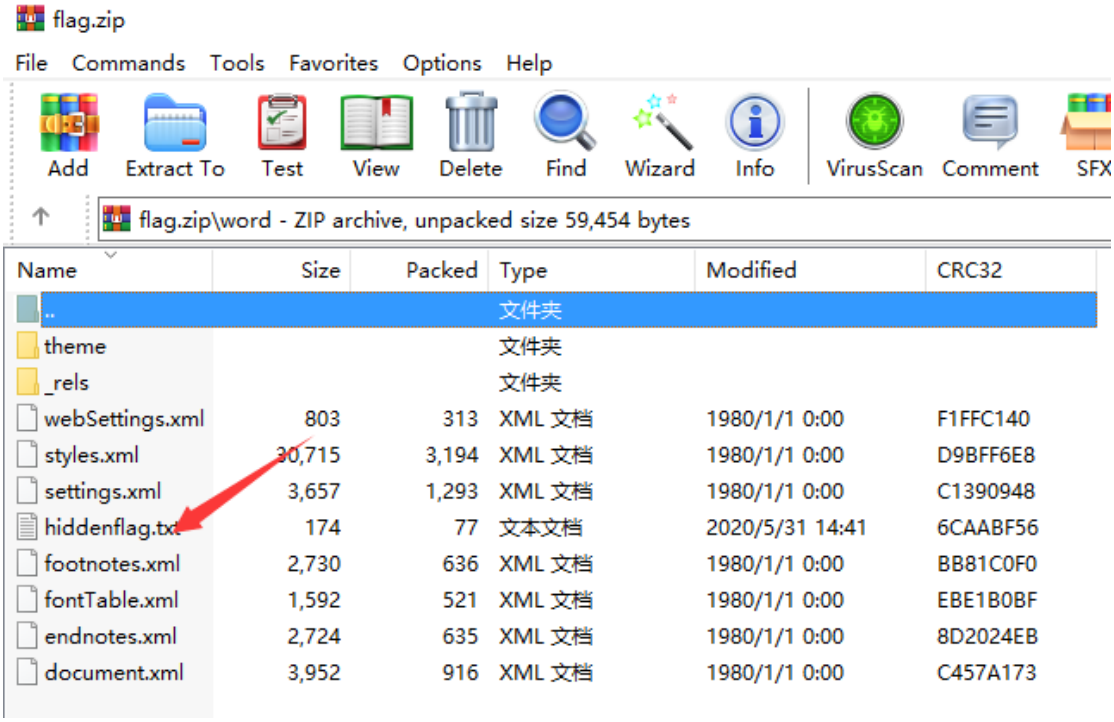
改后缀后打开发现隐藏文字且有报错



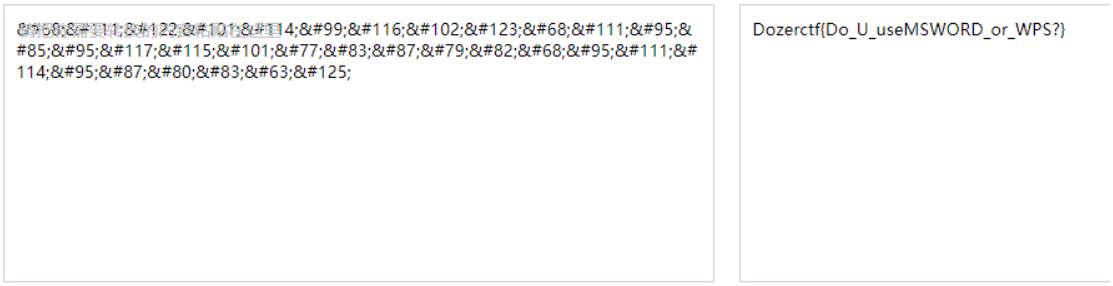
flag is here

it is not the flag you want

再次仔细检查 zip 发现 flag 文件



Unicode 解码



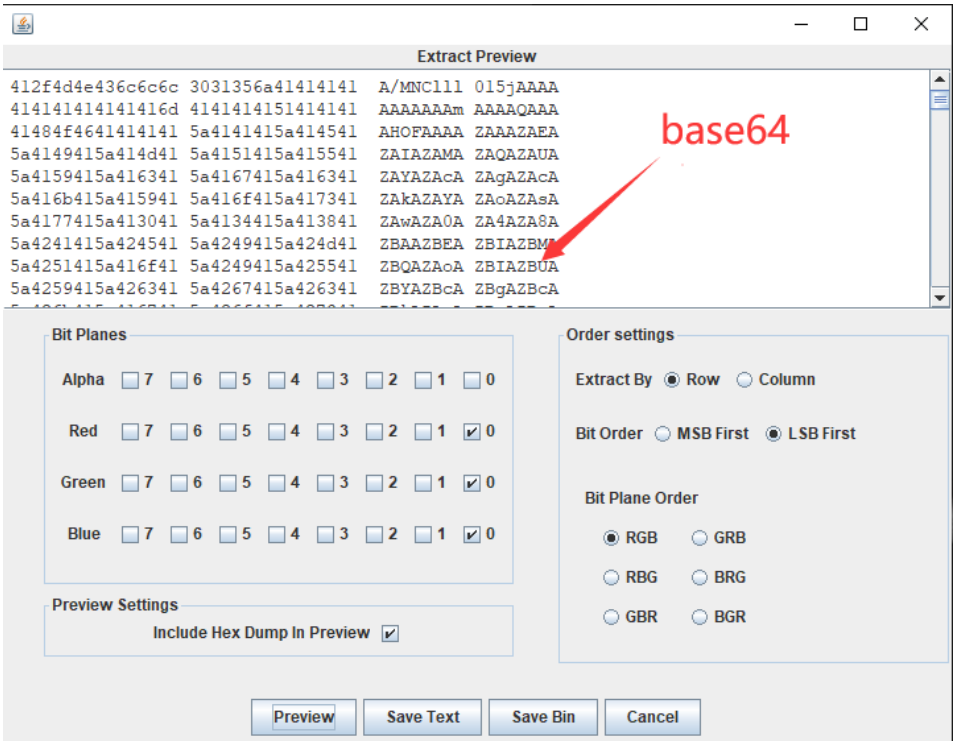
flag： Dozerctf{Do_U_useMSWORD_or_WPS?}

py 吗（难度：中）

修改图片高度

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	‰PNG IHDR
00000010	00	00	01	8E	00	00	01	8E	08	06	00	00	00	80	04	E4	Ž Ž ä
00000020	7C	00	01	00	00	49	44	41	54	78	9C	C4	FD	57	93	2D	| IDATxœÄýW"-
00000030	59	96	DF	89	FD	B6	70	75	64	E8	B8	22	45	55	56	96	Y–ß‰ý¶pudè¸"EUV–
00000040	68	74	37	AA	A1	05	39	63	80	0D	6C	40	33	7E	02	BE	ht7ª¡ 9c€ l@3~ ¾

lsb 隐写



导出的 base64 根据提示猜测为 py 或 pyc 文件

```
1  import base64
2
3  fin=open("py.txt","r")
4  fout=open('2.pyc',"wb")
5  base64.decode(fin,fout)
6  fin.close()
7  fout.close()
```

将 pyc 文件反编译得到加密脚本

请选择pyc文件进行解密。支持所有Python版本

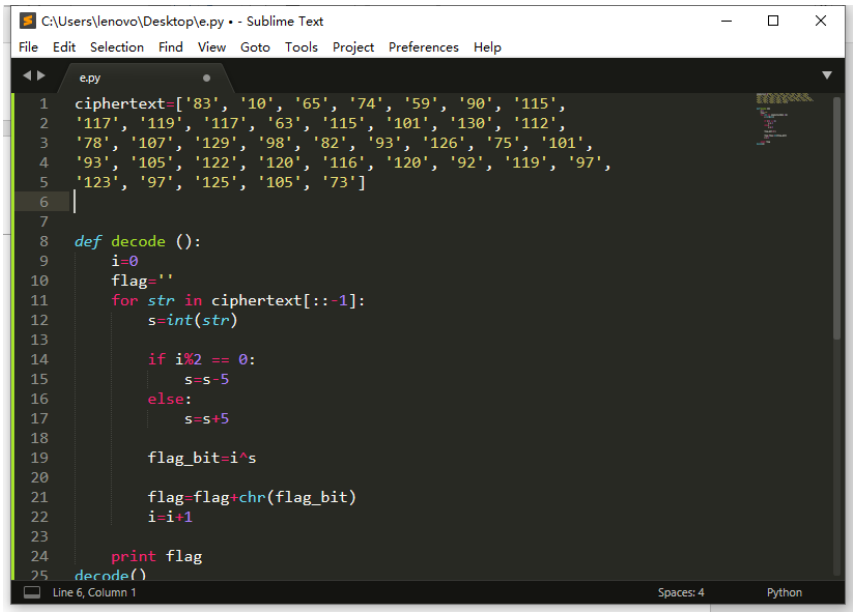
选择文件 未选择任何文件

```
    '97',
    '125',
    '105',
    '73']

def encode():
    flag = 'Dozerctf{python_is_the_best_language!}'
    ciphertext = []
    for i in range(len(flag)):
        s = chr(i ^ ord(flag[i]))
        if i % 2 == 0:
            s = ord(s) + 5
        else:
            s = ord(s) - 5
        ciphertext.append(str(s))

    print ciphertext[::-1]
```

写出对应揭秘脚本得到 flag



flag： Dozerctf{python_is_the_best_language!}