

论剑-writeup

因为很少人做出来，导致网上很少这个wp（找不到），所以我在这里记录下解题思路
打开题目

Challenge

19 Solves

×

论剑

100

剑客

十年磨一剑，霜刃未曾试。
今日把示君，谁有不平事。

lunjian.jpg

Flag

Submit

访问链接，把图片下载下来另存为



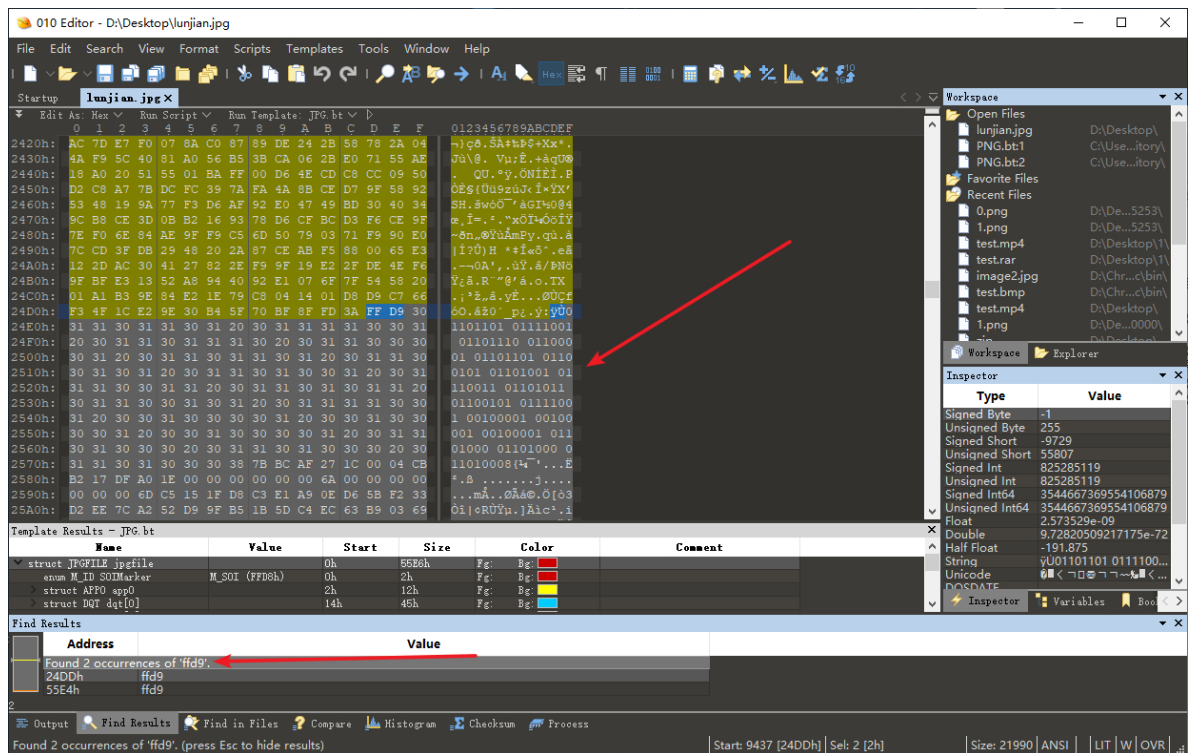
先把它丢进kali上binwalk扫描以下，发现有隐藏文件，foremost直接分离出来，得到两张图片



CTF_论剑场

CTF_论剑场

把图片都拿去二进制编辑工具查看下，在原图上搜索下FFD9（jpg的结束标识），发现有两个，以及一段二进制文件，很可疑
这段二进制拿去转ASCII码，得到mynameiskey!!!hhh 折腾了下，暂时先放着。



ASCII在线转换器-十六进制，十进制，二进制

ASCII转换到 ASCII (例: a b c)

m y n a m e i s k e y ! ! ! h h h

添加空格

删除空格

☐ 将空白字符转换

十六进制转换到 16进制(例:0x61或61或61/62) ☐ 删除 0x

0x6d 0x79 0x6e 0x61 0x6d 0x65 0x69 0x73 0x6b 0x65 0x79
0x21 0x21 0x21 0x68 0x68 0x68

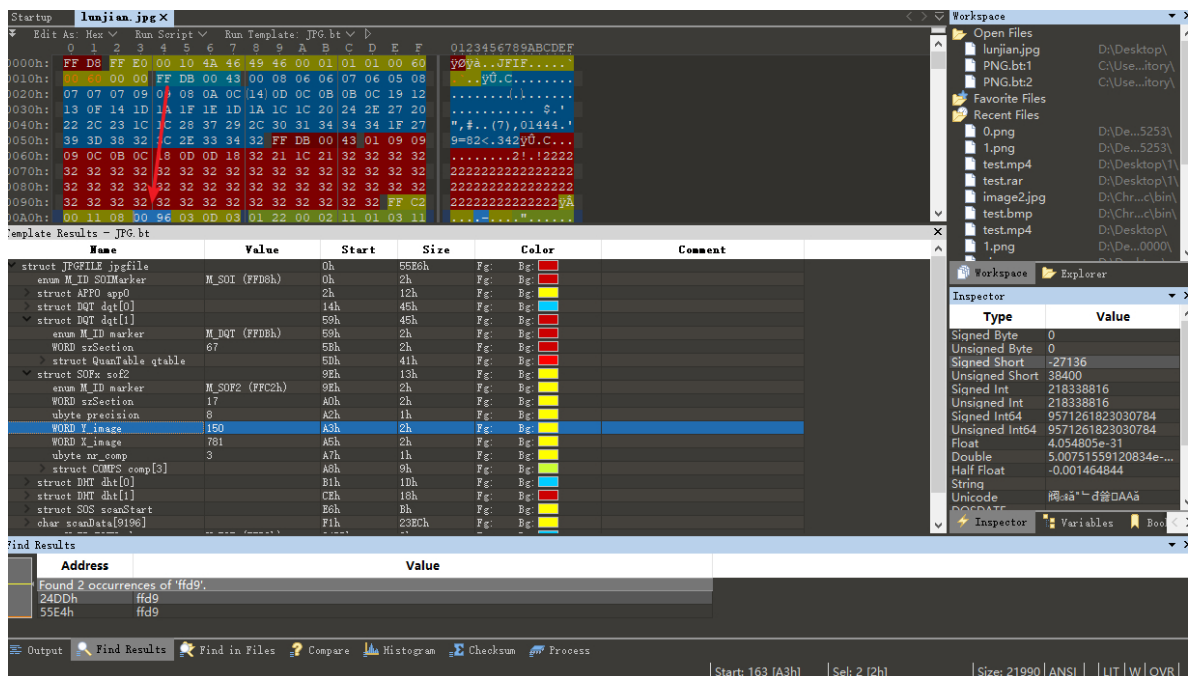
十进制转换到 10进制 (例: 97 98 99)

109 121 110 97 109 101 105 115 107 101 121 33 33 33 104
104 104

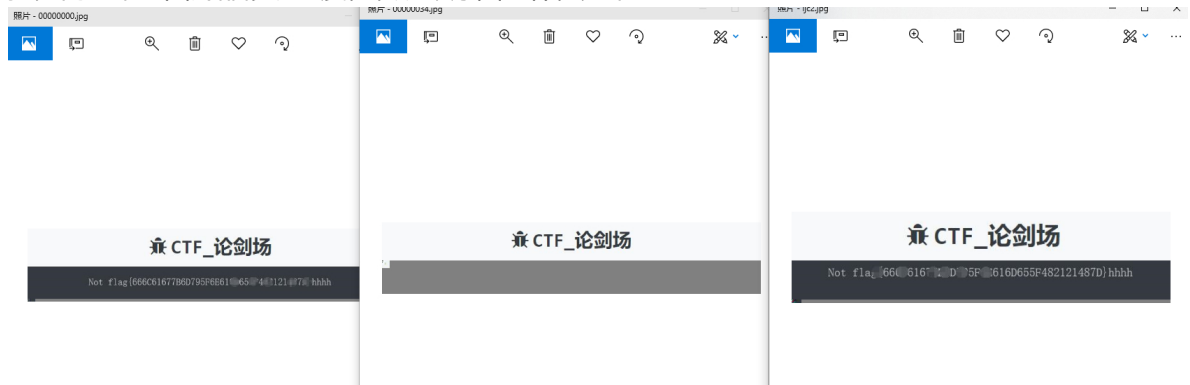
二进制转换到 2进制(例:01100001 01100010 01100011)

01101101 01111001 01101110 01100001 01101101 01100101
01101001 01110011 01101011 01100101 01111001 00100001
00100001 00100001 01101000 01101000 01101000

什么详细信息、备注都毫无hint，想着修改图片高度看下，发现新大陆，但是隐藏了一部分-_-!



把分离出来的图片都修改高度，发现跟原图一样，无果



天坑，这里想打si作者的环节，在分离出来的两张图片，以及这段二进制狂下功夫，xor、盲水印、色道分析..折腾了一段时间并没有什么用

查看二进制那段信息发现，看到BC AF 27 1C好熟悉，好像特征码给改过，尝试修改,修复文件头

```
23F0h: E5 9B 66 EA BB 29 83 6D 3A D4 30 C9 AE 96 10 AC  Å>f&»)fm:00E0~-.~
2400h: 08 16 13 BC 7C FC 85 AA 16 93 78 D4 4F BC D0 04  ...&|d...".x0C+@.
2410h: 41 4C 75 6D 7C DF F9 C3 4D 46 74 01 11 FF 00 67  ALum|BùÅMft..y.g
2420h: AC 7D E7 F0 07 8A C0 87 89 DE 24 2B 58 78 2A 04  ~)çð.ŠÅ+±B$+Xx*.
2430h: 4A F9 5C 40 81 A0 56 B5 3B CA 06 2B E0 71 55 AE  Jù\@. Vù;È.+àqU@
2440h: 18 A0 20 51 55 01 BA FF 00 D6 4E CD C8 CC 09 50  . QU.*ý.ÖNİÈİ.P
2450h: D2 C8 A7 7B DC FC 39 7A FA 4A 8B CE D7 9F 58 92  ÒÈ§(Üu9zúJ<İ×YX'
2460h: 53 48 19 9A 77 F3 D6 AF 92 E0 47 49 BD 30 40 34  SH.šwóÖ' àGI+0@4
2470h: 9C B8 CE 3D 0B B2 16 93 78 D6 CF BC D3 F6 CE 9F  æ.İ=.*. "xÖİ+0öİY
2480h: 7E F0 6E 84 AE 9F F9 C5 6D 50 79 03 71 F9 90 E0  ~ðn,øYùÅmPy.qù.à
2490h: 7C CD 3F DB 29 48 20 2A 87 CE AB F5 88 00 65 E3  (İ?Ü)H *+İ«ö'.eä
24A0h: 12 2D AC 30 41 27 82 2E F9 9F 19 E2 2F DE 4E F6  .-→0A',.üY.ä/BNö
24B0h: 9F BF E3 13 52 A8 94 40 92 E1 07 6F 7F 54 58 20  Y¿ä.R'"@'á.o.TX
24C0h: 01 A1 B3 9E 84 E2 1E 79 C8 04 14 01 D8 D9 C7 66  .;³ž..ä.yÈ...öÜçf
24D0h: F3 4F 1C E2 9E 30 B4 5F 70 BF 8F 7D 3A FF D9 30  60.äž0' _p¿.ý:yü0
24E0h: 31 31 30 31 31 30 31 20 30 31 31 31 31 30 30 31  1101101 01111001
24F0h: 20 30 31 31 30 31 31 31 30 20 30 31 31 30 30 30  01101110 011000
2500h: 30 31 20 30 31 31 30 31 31 30 31 20 30 31 31 30  01 01101101 0110
2510h: 30 31 30 31 20 30 31 31 30 31 30 30 31 20 30 31  0101 01101001 01
2520h: 31 31 30 30 31 31 20 30 31 31 30 31 30 31 31 20  110011 01101011
2530h: 30 31 31 30 30 31 30 31 20 30 31 31 31 31 30 30  01100101 0111100
2540h: 31 20 30 30 31 30 30 30 30 31 20 30 30 31 30 30  1 00100001 00100
2550h: 30 30 31 20 30 30 31 30 30 30 30 31 20 30 31 31  001 00 000001 011
2560h: 30 31 30 30 30 20 30 31 31 30 31 30 30 30 20 30  01000 01101000 0
2570h: 31 31 30 31 30 30 30 37 7A BC AF 27 1C 00 04 CB  11010007z&"....È
2580h: B2 17 DF A0 1E 00 00 00 00 00 00 00 6A 00 00 00 00  ".B .....j....
2590h: 00 00 00 6D C5 15 1F D8 C3 E1 A9 0E D6 5B F2 33  ...mÄ..øÄá@.Ö[ð3
25A0h: D2 EE 7C A2 52 D9 9F B5 1B 5D C4 EC 63 B9 03 69  Òi|øRÜÿu.]Älc³.i
25B0h: DE 43 75 48 4A AE EE 35 5E 1E D0 3F 3E 0B C4 E5  pCuHJøi5^.ð?>.Ää
25C0h: 24 F9 62 19 10 C0 05 81 1F 88 D1 A7 C4 2D D0 17  Šùb..Ä...^NšÄ-ð.
25D0h: 1A 6F A7 78 25 D2 D1 EB E9 18 22 FD EB FA 4E 37  .o$x%ÖNëe."yèúN7
```

常见的文件头:

7z

文件头标识: 37 7A BC AF 27 1C

JPEG/JPG

文件头标识: ff, d8 (SOI) (JPEG 文件标识)

文件结束标识: ff, d9 (EOI)

PNG

文件头标识: 89 50 4E 47 0D 0A 1A 0A

GIF

文件头标识: 47 49 46 38 39(37) 61--- GIF89(7)a

BMP

文件头标识: 42 4D--- BM

HTML (html)

文件头标识: 68746D6C3E

ZIP Archive (zip)

文件头标识: 504B0304 --- PK

RAR Archive (rar)

文件头标识: 52617221

等等..

丢回kali用binwalk分析，发现多了一个压缩包，分离，注意使用foremost分离不出来，利用dd分离出来

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# binwalk lunjian.jpg

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0            0x0           JPEG image data, JFIF standard 1.01
9591         0x2577        7-zip archive data, version 0.4
17569        0x44A1        JPEG image data, JFIF standard 1.01

root@kali:~/Desktop# dd if=lunjian.jpg of=1.7z bs=1 skip=9591
12399+0 records in
12399+0 records out
12399 bytes (12 kB, 12 KiB) copied, 0.0237755 s, 522 kB/s
root@kali:~/Desktop# ls
1.7z  lunjian.jpg  mount-shared-folders  restart-vm-tools
root@kali:~/Desktop#
```

使用dd命令分离文件，如：

```
dd if=hehe.jpg of=hehe1.zip bs=1 skip=54163
```

if=file（源文件）

of=file（输出文件）

bs=bytes（一次性转换bytes个字节，及转换缓冲区大小）

skip=blocks（输入文件开头跳过blocks个块再开始复制--通俗点讲就是从哪开始）

进行解压，需要密码，用二进制转的ASCII码进行解密，得到一张图片，修改高度，得到另一部分的flag，进行拼接
最终得到一个的密文



这个不是md5，是一个base16密文，进行base16解密，得到flag

```
666C61677B6D795F6E616D655F482121487D
```

编码 解码

```
flag(my_name_H!!H)
```