MISC - 高度隐写

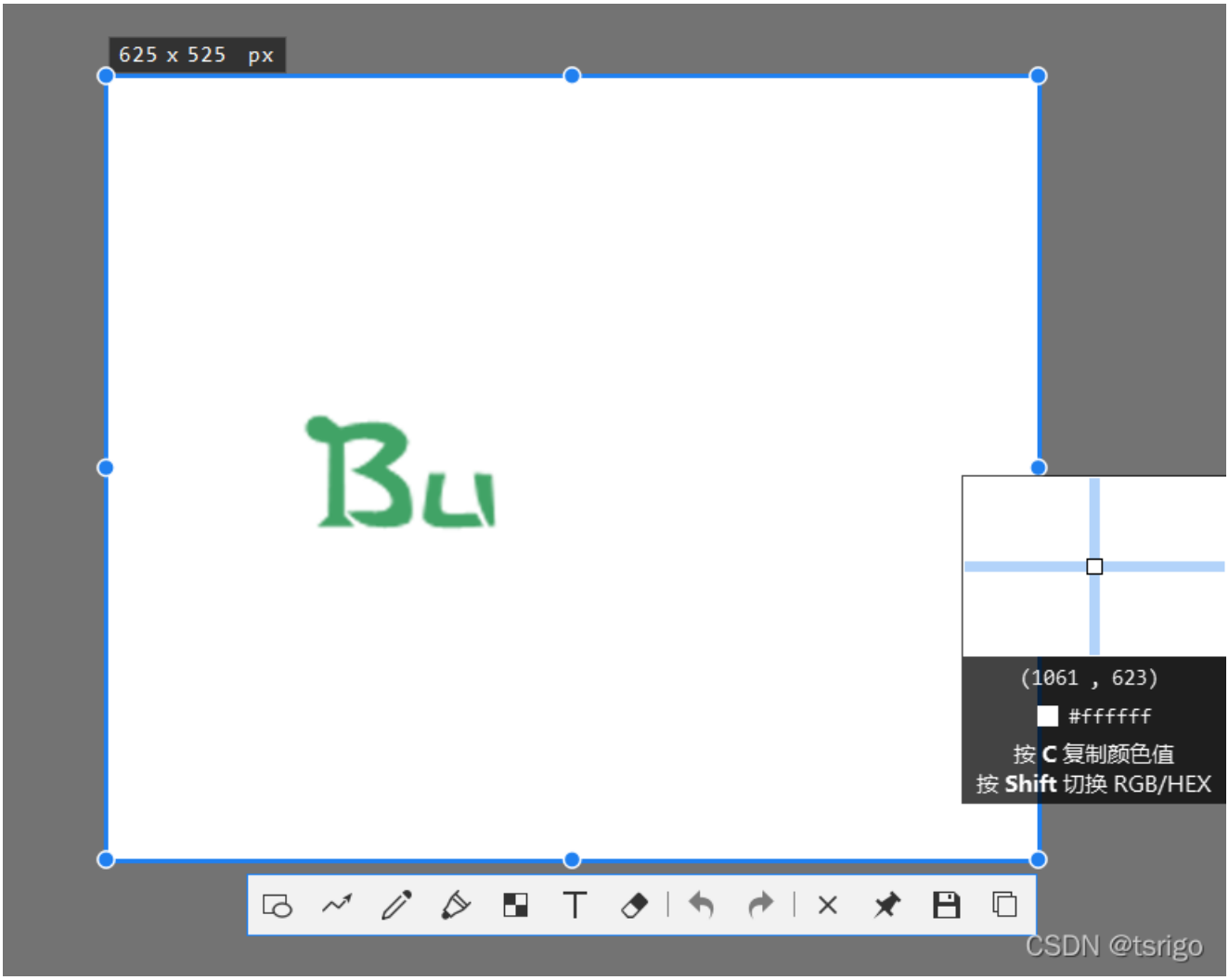
原创

tsrigo 已于 2022-03-20 13:37:43 修改 452 收藏

文章标签： python 经验分享

于 2022-03-20 13:32:03 首次发布

本文链接：https://blog.csdn.net/weixin_45574854/article/details/123611452

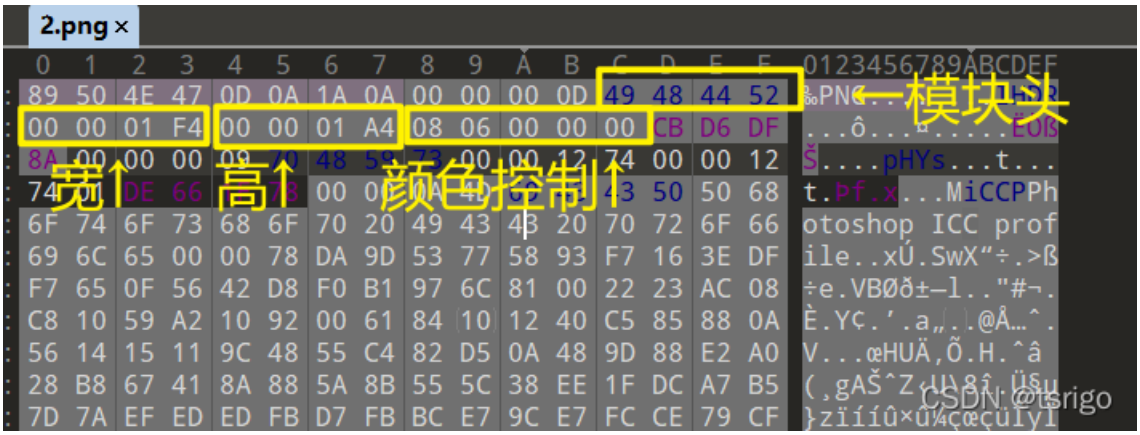


下载题目，解压缩，得到一张图片

但是在Kali环境下无法正常打开，说明修改了图片高度，通常宽不会被修改，否则window下将无法打开图片，准备进行爆破

利用pngcheck得到正确的CRC值：cbd6df8a

```
D:\CTF\chapter4-隐写\图片隐写\16 PNG IDAT>pngcheck.exe -v D:\CTF\Exp\2.png
File: D:\CTF\Exp\2.png (17675 bytes)
  chunk IHDR at offset 0x0000c, length 13
    500 x 420 image, 32-bit RGB+alpha, non-interlaced
  CRC error in chunk IHDR (computed c758d77d, expected cbd6df8a)
ERRORS DETECTED in D:\CTF\Exp\2.png
```



运行以下脚本（python2）

https://c.runoob.com/compile/6/

```
# -*- conding: utf-8 -*-
import binascii
import struct
crc32key = 0xcbd6df8a
for i in range(0, 65535):
    height = struct.pack('>i', i)
    data = '\x49\x48\x44\x52' + '\x00\x00\x01\xF4' + height + '\x08\x06\x00\x00\x00'
    crc32result = binascii.crc32(data) & 0xffffffff
    if (crc32result == crc32key):
        print(''.join(map(lambda c : "%02x" % ord(c), height)))
```

得到正确的高值：000001f4

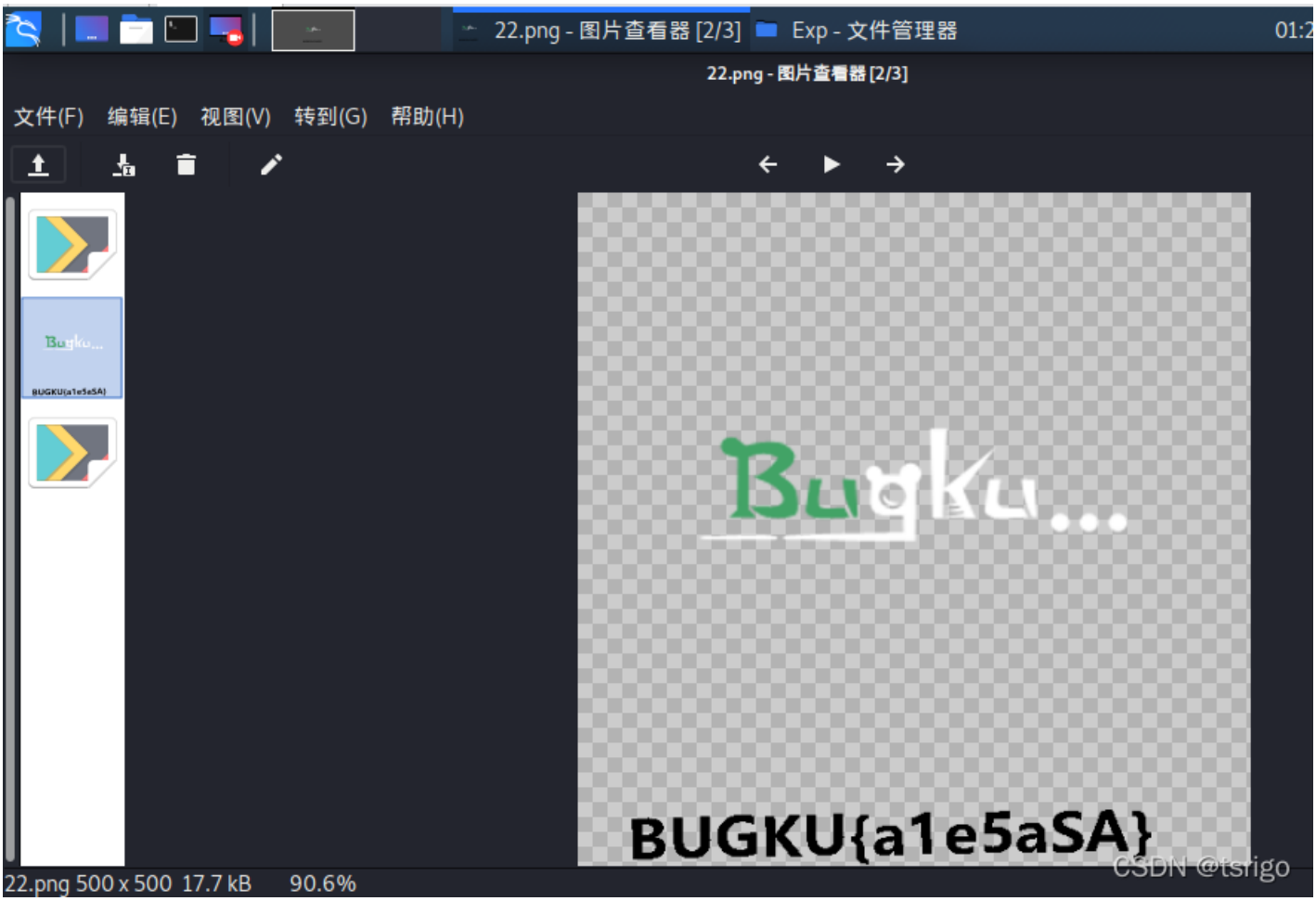
点击运行 | Python2 在线工具 | 复制 | 清空 | 邮件反馈

```python
# -*- conding: utf-8 -*-
import binascii
import struct
crc32key = 0xcbd6df8a
for i in range(0, 65535):
    height = struct.pack('>i', i)
    data = '\x49\x48\x44\x52' + '\x00\x00\x01\xF4' + height + '\x08\x06\x00\x00\x00'
    crc32result = binascii.crc32(data) & 0xffffffff
    if (crc32result == crc32key):
        print(''.join(map(lambda c : "%02x" % ord(c), height)))
```

000001f4

CSDN @tsrigo

使用010editior进行修改，得到正确的图片与flag



值得注意的是，原图长宽相当接近，一开始可以尝试将高修改为宽，效率将更高。

思路，代码来源：《CTF安全竞赛入门》