【picoCTF2022】Misc部分

原创

Sparks_Pion 已于 2022-03-27 22:18:29 修改 4763 收藏 1

分类专栏： CTF训练 文章标签： 经验分享 python 网络安全

于 2022-03-27 15:15:45 首次发布

Enhance!

```
:e:0.00352781px;line-height:1.25;fill:#ffffff;stroke-width:0.26458332;"
5">c </tspan><tspan
:"line"
'
'
:e:0.00352781px;line-height:1.25;fill:#ffffff;stroke-width:0.26458332;"
3">o </tspan><tspan
:"line"
'
'
:e:0.00352781px;line-height:1.25;fill:#ffffff;stroke-width:0.26458332;"
)">C </tspan><tspan
:"line"
'
'
:e:0.00352781px;line-height:1.25;fill:#ffffff;stroke-width:0.26458332;"
2">T </tspan><tspan
:"line"
'
'
:e:0.00352781px;line-height:1.25;fill:#ffffff;stroke-width:0.26458332;"
4">F { 3 n h 4 n </tspan><tspan
:"line"
'
'
:e:0.00352781px;line-height:1.25;fill:#ffffff;stroke-width:0.26458332;"
2">c 3 d _ 5 6 e 8 7 c 9 6 }</tspan></text>
```

File types

```
┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ binwalk Flag.pdf

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Executable script, shebang: "/bin/sh"
168           0xA8            Executable script, shebang: "/bin/sh' line above, then type 'sh FILE'."
3029          0xBD5           uuencoded data, file name: "flag", file permissions: "600"
```

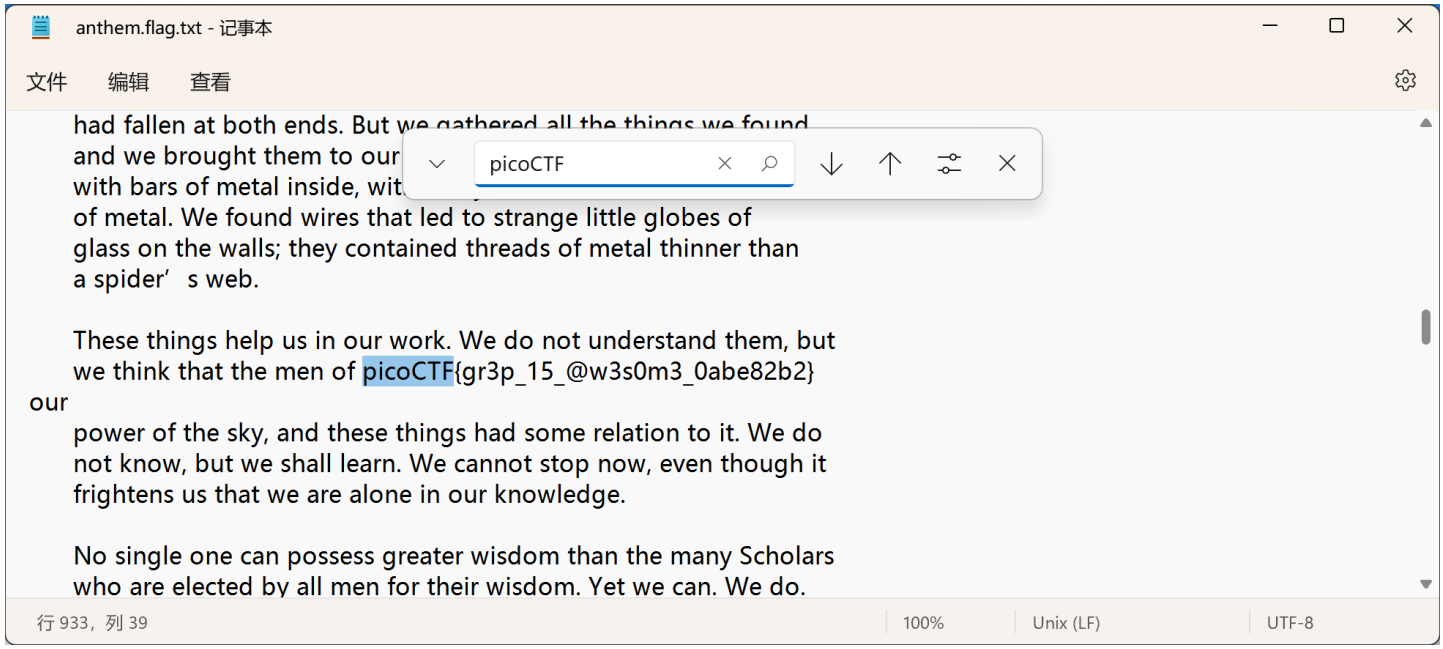
去掉 `.pdf` 是一个 shell 脚本，运行时用到了 uudecode，需要 `sudo apt install sharutils`

之后就是各种压缩包的嵌套了，QAQ

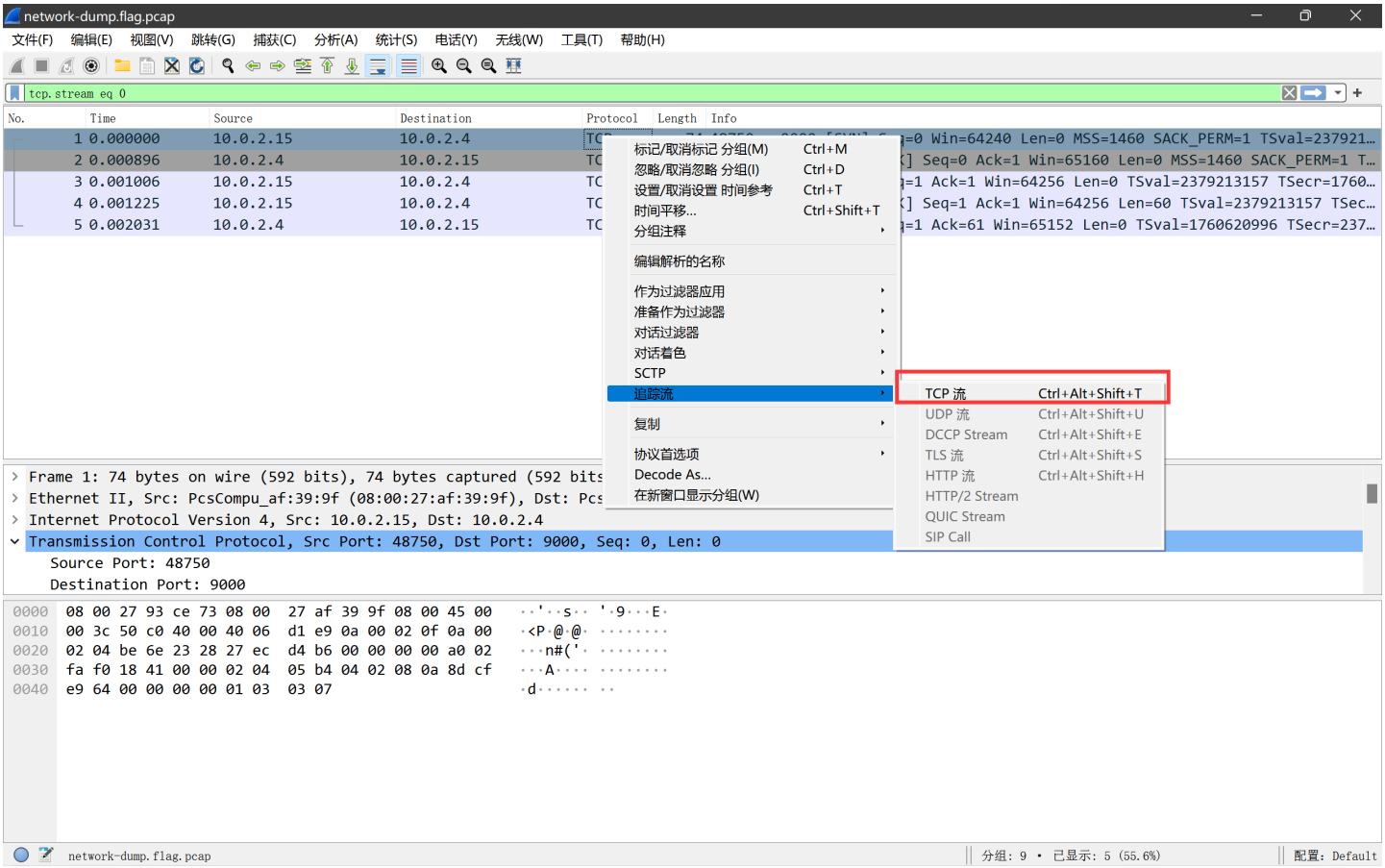
```
┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ file Flag
Flag: current ar archive

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ ar -p Flag > flag1

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ file flag1
flag1: cpio archive

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ cpio -idmv < flag1
flag
2 blocks

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ file flag
flag: bzip2 compressed data, block size = 900k

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ bunzip2 flag
bunzip2: Can't guess original name for flag -- using flag.out

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ file flag.out
flag.out: gzip compressed data, was "flag", last modified: Tue Mar 15 06:50:49 2022, from Unix, original size mo
dulo 2^32 326

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ gzip -d flag.out

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ file flag.out
flag.out: lzip compressed data, version: 1

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ unzip flag.out

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ file flag
flag: LZ4 compressed data (v1.4+)

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ lz4 -d flag.lz4
Decoding file flag
flag.lz4             : decoded 263 bytes

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ file flag
flag: LZMA compressed data, non-streamed, size 252

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ lzma -d flag.lzma

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ file flag
flag: lzop compressed data - version 1.040, LZO1X-1, os: Unix
```

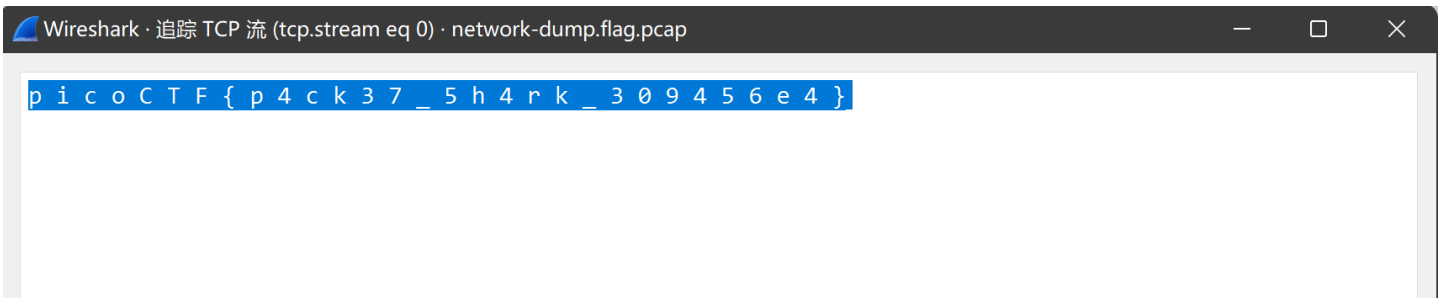
```
flag: lzop compressed data   version 1.040, LZO1X-1, os: Unix

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ lzop -dv flag.lzo
decompressing flag.lzo into flag

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ file flag
flag: lzip compressed data, version: 1

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ unzip flag.out

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ file flag
flag: XZ compressed data, checksum CRC64

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ xz -d flag.xz

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ file flag
flag: ASCII text

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ cat flag
7069636f4354467b66316c656e406d335f6d406e3170756c407431306e5f
6630725f3062326375723137795f37353137353362307d0a

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/File types]
└─$ cat flag | hex --decode
picoCTF{f1len@m3_m@n1pul@t10n_f0r_0b2cur17y_751753b0}
```

Lookey here

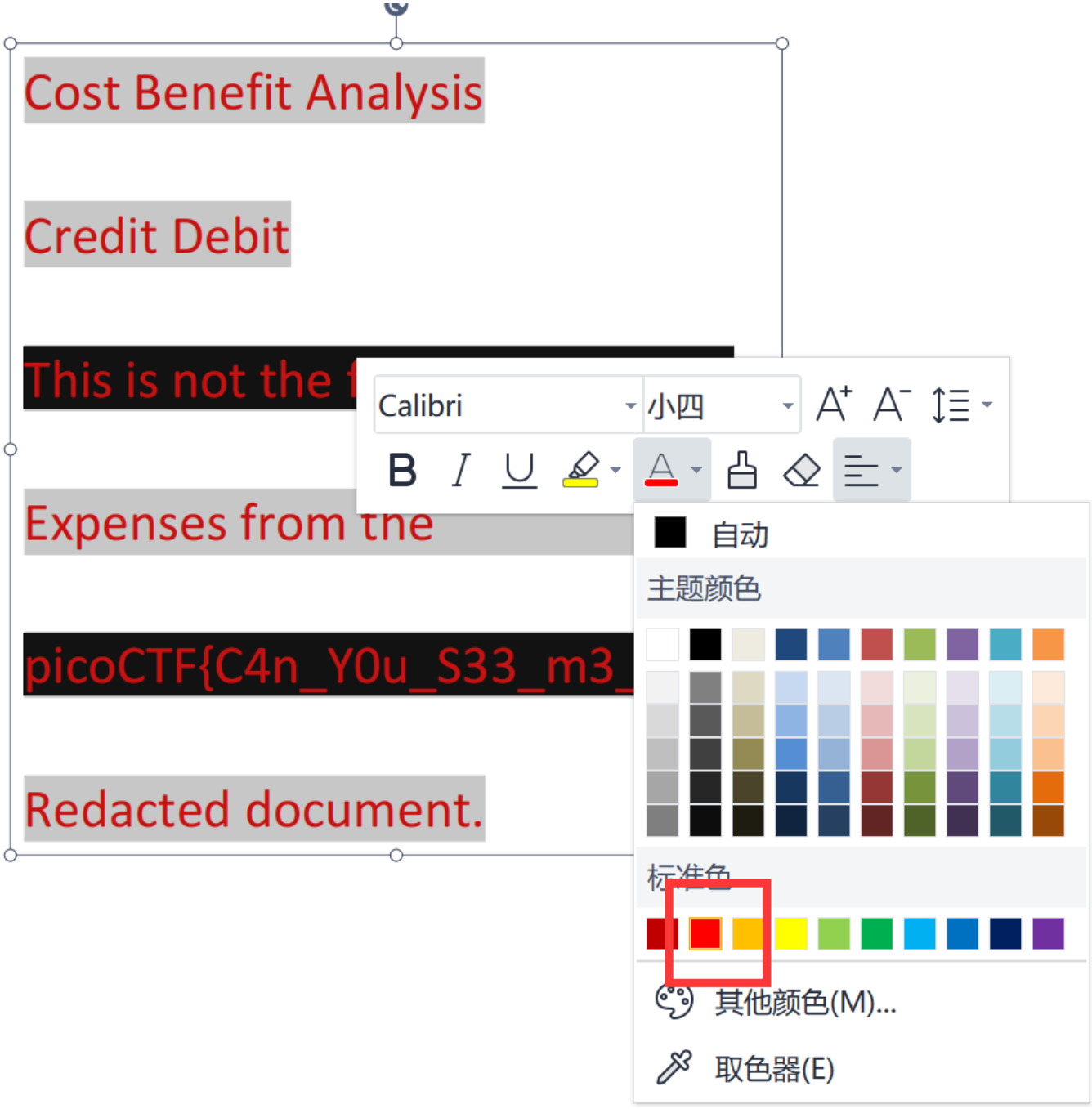


Packets Primer





Redaction gone wrong

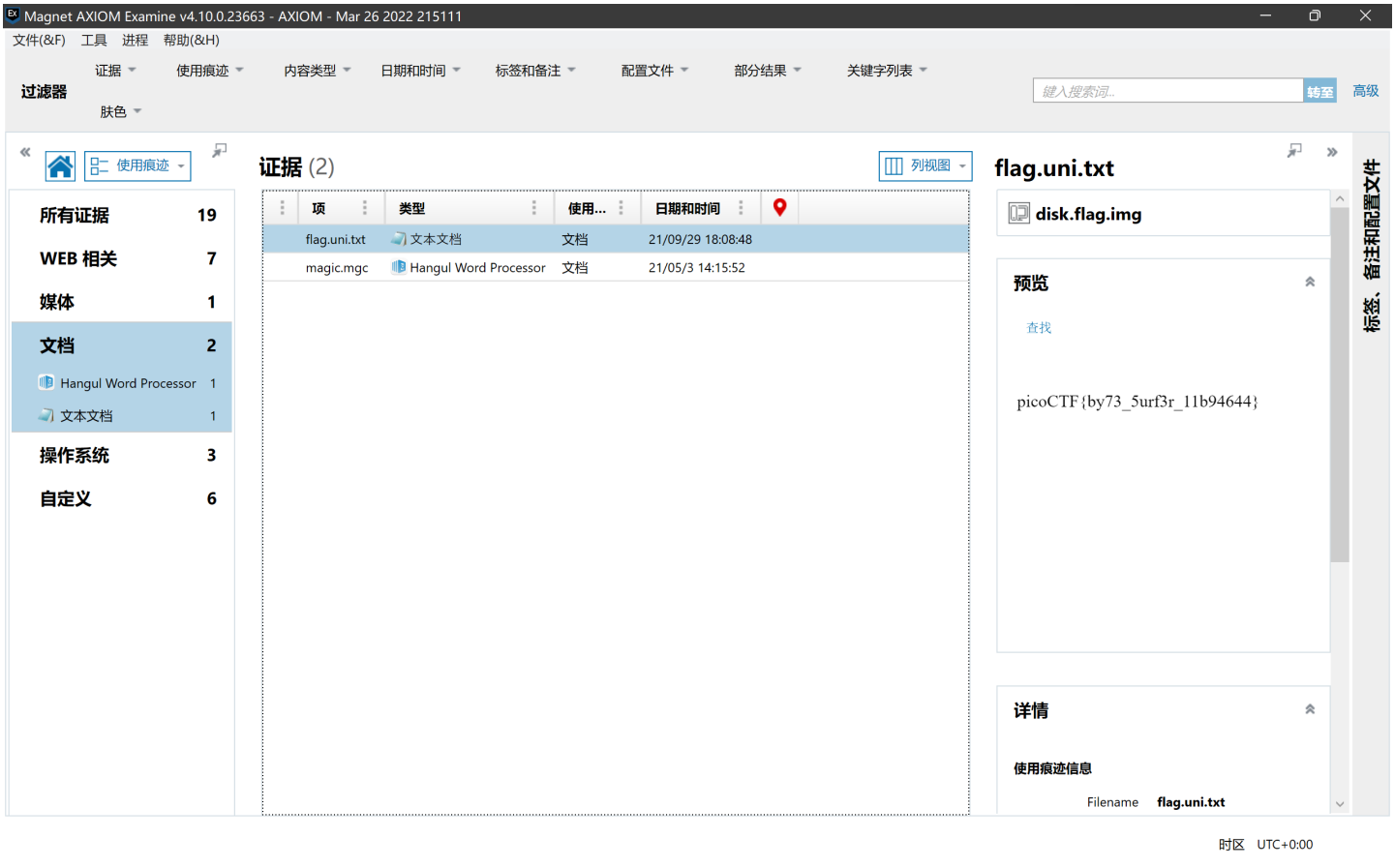


Sleuthkit Intro

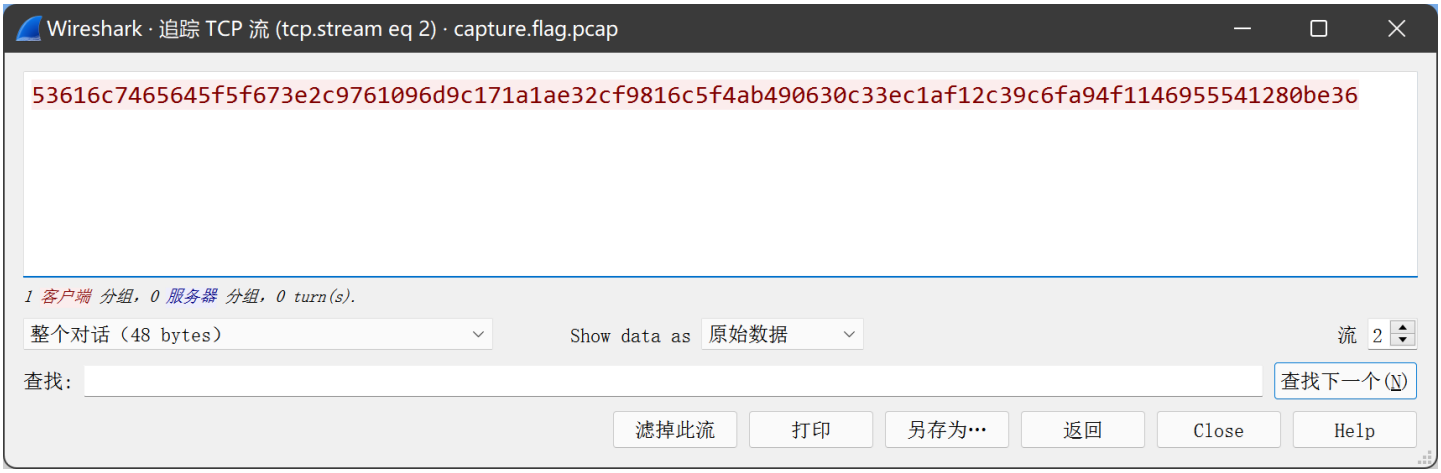
```
┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/Sleuthkit Intro]
└─$ mmls -B disk.img
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Size    Description
000:  Meta      0000000000   0000000000   0000000001   0512B   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   1024K   Unallocated
002:  000:000   0000002048   0000204799   0000202752   0099M   Linux (0x83)

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/Sleuthkit Intro]
└─$ nc saturn.picoctf.net 52279
What is the size of the Linux partition in the given disk image?
Length in sectors: 202752
202752
Great work!
picoCTF{mm15_f7w!}
```

Sleuthkit Apprentice

取证题，搞半天，用了 AXIOM Process



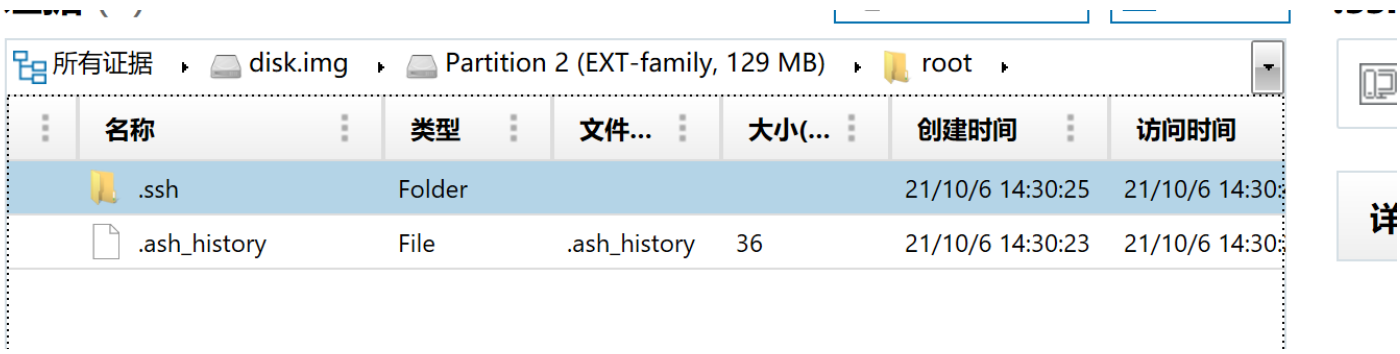
Eavesdrop




```
┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/Eavesdrop]
└─$ openssl des3 -d -salt -in file.des3 -out file.txt -k supersecretpassword123
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/Eavesdrop]
└─$ cat file.txt
picoCTF{nc_73115_411_aefc6100}
```

Operation Oni

先提取出.ssh 文件



加入到本地，尝试连接

```
┌──(sparks㉿LAPTOP-Sparks)-[~/.ssh]
└─$ ssh -i key_file -p 57455 ctf-player@saturn.picoctf.net
Warning: Identity file key_file not accessible: No such file or directory.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for '/home/sparks/.ssh/id_ed25519' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "/home/sparks/.ssh/id_ed25519": bad permissions
ctf-player@saturn.picoctf.net's password:
```

更改权限后再次尝试

```
┌──(sparks㉿LAPTOP-Sparks)-[~/.ssh]
└─$ sudo chmod 600 id_ed25519

┌──(sparks㉿LAPTOP-Sparks)-[~/.ssh]
└─$ sudo chmod 600 id_ed25519.pub

┌──(sparks㉿LAPTOP-Sparks)-[~/.ssh]
└─$ ssh -i key_file -p 57455 ctf-player@saturn.picoctf.net
Warning: Identity file key_file not accessible: No such file or directory.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-1017-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ctf-player@challenge:~$ ll
-bash: ll: command not found
ctf-player@challenge:~$ ls
flag.txt
ctf-player@challenge:~$ cat flag.txt
picoCTF{k3y_5l3u7h_d6570e30}
```

补充一下 `mnt` 下的不能改权限

```
┌──(root㉿LAPTOP-Sparks)-[/mnt/…/pico2022/Misc/Operation Oni/已保存文件]
└─# sudo chmod 600 id_ed25519.pub

┌──(root㉿LAPTOP-Sparks)-[/mnt/…/pico2022/Misc/Operation Oni/已保存文件]
└─# ll
total 0
-rwxrwxrwx 1 sparks sparks 111 Mar 27 22:02 id_ed25519.pub
```

`-i` 参数应该后面接私钥文件的，之前是歪打正着了□

下面是正确用法

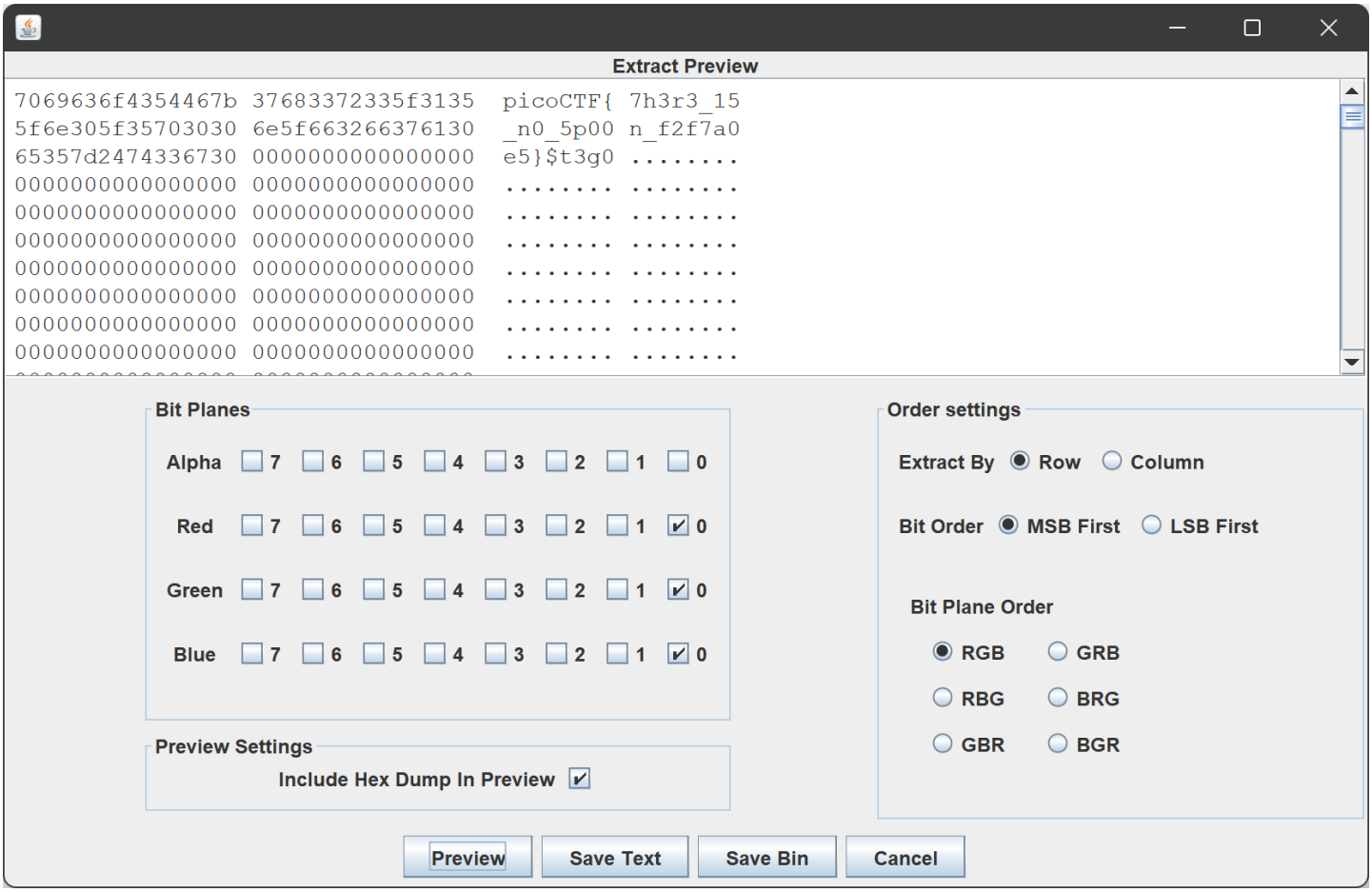
```
┌──(root㉿LAPTOP-Sparks)-[/tmp]
└─# chmod 600 sshkey

┌──(root㉿LAPTOP-Sparks)-[/tmp]
└─# ssh -i sshkey -p 55145 ctf-player@saturn.picoctf.net
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-1017-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Mar 27 14:12:00 2022 from 127.0.0.1
ctf-player@challenge:~$
```

St3g0

binwalk 没有发现什么东西，有 Zlib 是正常现象

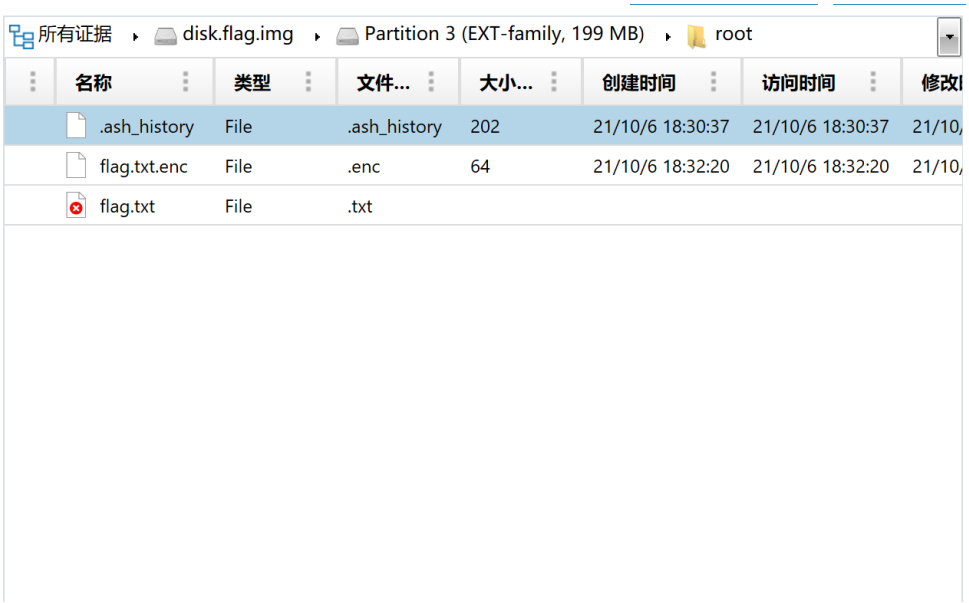
```
┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/St3g0]
└─$ file pico.flag.png
pico.flag.png: PNG image data, 585 x 172, 8-bit/color RGBA, non-interlaced
┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/St3g0]
└─$ binwalk pico.flag.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 585 x 172, 8-bit/color RGBA, non-interlaced
41            0x29            Zlib compressed data, default compression
```

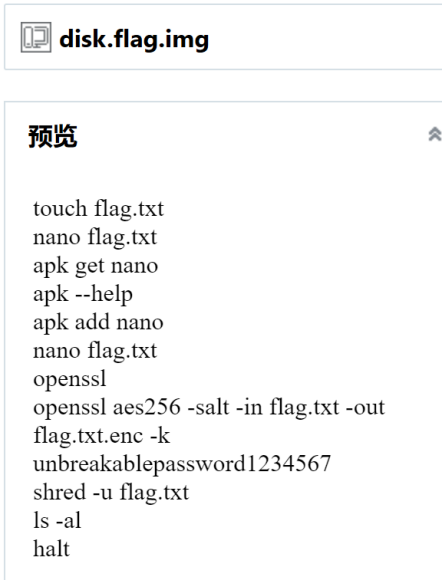
然后使用 Stegsolve，发现发现 flag，原理不清楚



好像是LSB，找时间学一下

Operation Orchid





```
┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/pico2022/Misc/Operation Orchid/已保存文件]
└─$ openssl aes256 -d -in flag.txt.enc -out flag.txt
enter aes-256-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bad decrypt
140269673760128:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:../crypto/evp/evp_enc.c
:615:

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/pico2022/Misc/Operation Orchid/已保存文件]
└─$ cat flag.txt
picoCTF{h4un71ng_p457_186cf0da}
```

SideChannel

时间测信道攻击，比较 pin 时是一个字符一个字符比较的，可以比较时间获取 pin

```
┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/SideChannel]
└─$ time (echo 48390513 | ./pin_checker)
Please enter your 8-digit PIN code:
8
Checking PIN...
Access granted. You may use your PIN to log into the master server.

real    1.15s
user    1.06s
sys     0.02s
cpu     94%

┌──(sparks㉿LAPTOP-Sparks)-[/mnt/…/CTF/pico2022/Misc/SideChannel]
└─$ time (echo 00000000 | ./pin_checker)
Please enter your 8-digit PIN code:
8
Checking PIN...
Access denied.

real    0.23s
user    0.14s
sys     0.00s
cpu     62%
```

真密码 `48390513` 的用时，比假密码要大 `00000000` ，本人不才，用手调出来的，不会 Shell 交互，时间比较总是莫名其妙的出问题，不懂了。。。

代码来了

```python
import subprocess
import time

ans = "00000000"
# character = '0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz'
character = '0123456789'
for index in range(8):

    minTime = 0
    anschar = ''

    for ch in character:
        ans = ans[:index] + ch + ans[index + 1:]
        command = 'echo {} | ./pin_checker'.format(ans)
        start = time.time()
        for i in range(1):
            ex = subprocess.Popen(command,
                                  shell=True,
                                  executable='zsh',
                                  stdin=subprocess.PIPE,
                                  stdout=subprocess.PIPE,
                                  stderr=subprocess.STDOUT)
            ex.communicate()
            ex.wait()
        end = time.time()
        if (end - start) > minTime:
            minTime = (end - start)
            anschar = ch

    ans = ans[:index] + anschar + ans[index + 1:]
    print(ans[:index + 1])

# 48390513
```

Torrent Analyze

未完待续。。。