

记2021年春秋杯秋季赛勇者山峰赛道 Misc两题

原创

Mr.水函263 于 2021-11-28 01:30:00 发布 343 收藏 1

文章标签: 安全 python 其他

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_56229685/article/details/121583644

版权

Helloshark

拖进010,发现一个pcapng

名称	值	开始	大小	颜色	注释
struct BITMAPFILEHEAD...	0h	Eh	Fg:	Bg:	
struct BITMAPINFOHEAD...	Eh	28h	Fg:	Bg:	

CSDN @Mr.水函263

需要密码, 使用zsteg -a 得到密码

```

dell@kali: ~
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)

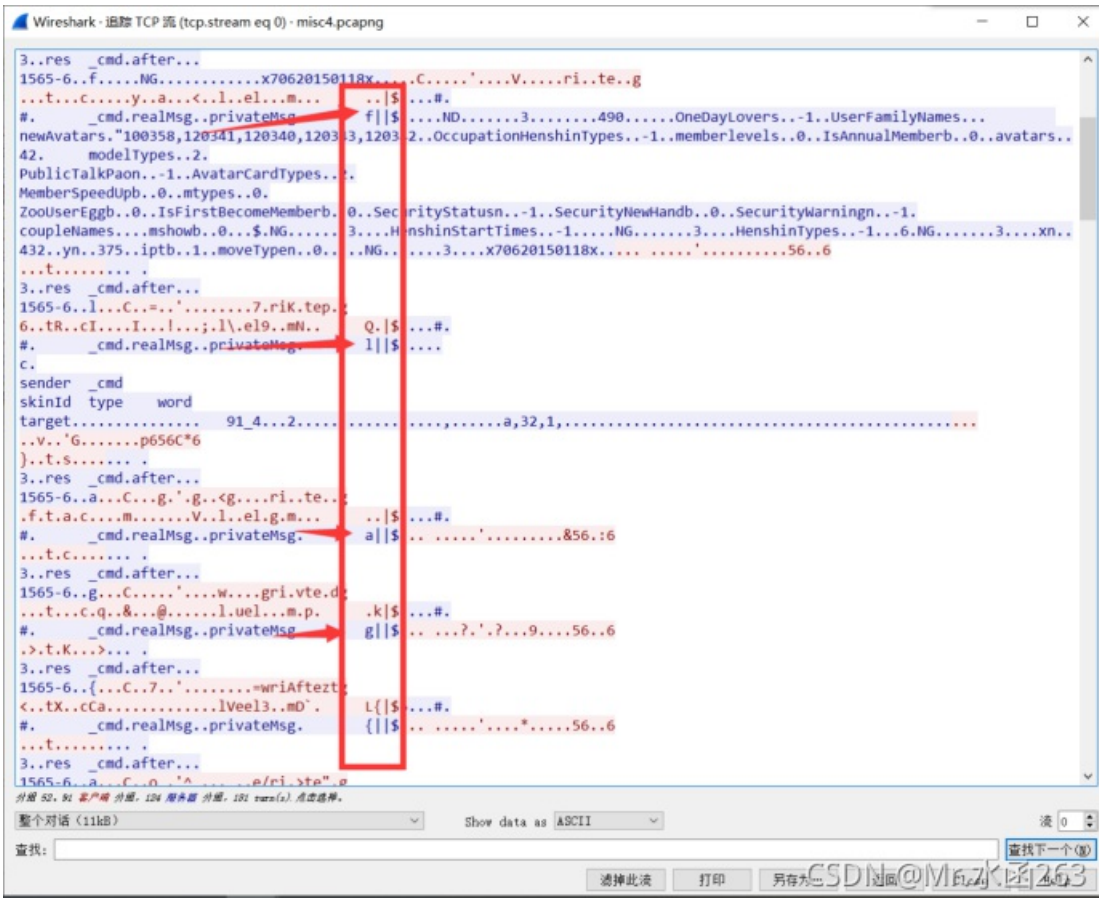
00000010: 18 0a 6b 25 09 00 14 a6 0b 00 0c 00 0b 00 6d 69 ..k%.....mi
00000020: 73 63 34 2e 70 63 61 70 6e 67 01 99 07 00 01 00 sc4.pcapng.....
00000030: 41 45 03 08 00 b6 a1 88 63 05 61 fd 77 74 1b cf AE.....c.a.wt..
00000040: 43 fc 35 5e 5d 90 cf 98 4d 44 00 ec 2d de 32 e8 C.5^]...MD..-.2.
00000050: c1 38 0c a9 61 4b 88 3f b9 06 87 ef 48 51 1f 71 .8..aK?...HQ.q
00000060: 6a c3 20 1c c5 02 6a 83 b3 9a 85 e4 42 2e 4b 31 j. ...j.....B.K1
00000070: fa 52 69 86 d5 19 11 1f ad 9d ad df e5 32 68 11 .Ri.....2h.
00000080: e4 b8 7f df 84 7a f4 a1 09 b0 a3 9b 19 8b b7 96 .....z.....
00000090: 63 7d 68 3d c0 86 55 35 84 af cc f6 51 34 2b 4f c}h=..U5...Q4+0
000000a0: 08 25 2c f8 95 88 31 ff 7d 99 86 29 12 ee 28 f6 .%, ...1.}..)..(
000000b0: eb 33 c5 5c 75 58 9f 46 4e 31 81 68 58 1b 27 52 .3.\uX.FN1.hX.'R
000000c0: fe dc e6 de 54 9a 77 b7 22 1f 00 eb 19 f9 a6 2f ....T.w."...../
000000d0: 68 ea c7 84 48 ee a8 29 3e ed cd d3 2c 22 01 27 h...H..)>...,".'
000000e0: fa bd e1 66 61 8b 26 e2 c8 69 be 13 80 51 60 42 ...fa.6..i...Q`B
000000f0: 1a 92 c7 b1 06 fd e1 3e 6a e2 ad bb b0 49 48 a5 .....>j....IH.

imagedata .. text: ":ff:::~::~:f::"
b1,r,msb,xy .. file: Big-endian UTF-16 Unicode text, with very long lines, with no
terminators
b8,rgb,msb,xy .. file: RDI Acoustic Doppler Current Profiler (ADCP)
b1,r,lsb,yx .. text: "password:091902AF23C#276C2FC7EAC615739CC7C0"
b4,rgb,msb,yx .. text: ["w" repeated 12 times]
b8,rgb,msb,yx .. file: RDI Acoustic Doppler Current Profiler (ADCP)
b2,rgb,lsb,yx,prime .. file: MPEG ADTS, layer III, v1, 160 kbps, 32 kHz, 2x Monoaural
b3,r,lsb,yx,prime .. file: very old 16-bit-int big-endian archive
b5,r,lsb,yx,prime .. file: MPEG ADTS, layer II, v1, 384 kbps, JntStereo
b8,r,msb,yx,prime .. file: ddis/ddif
b1,r,msb,Yx .. text: "0C7CC937516CAE7CF2C672#C32FA20919@:drowssap"
b2,r,msb,Yx .. text: "_w_W_}_uWuwu"
b1,r,lsb,Yx,prime .. file: AIX core file fulldump
b4,rgb,msb,Yx,prime .. text: ["w" repeated 10 times]
dell@kali:~$

```

CSDN @Mr.水函263

流量里追踪tcp流



储为txt, 写脚本提取

```

s) Dell / Desktop / 春秋 / 1 / get.py
get_snake_flag.py 1 import re
2 with open("1.txt", "r", encoding="utf-8") as f:
3     lines=f.readlines()
4     str=''
5     for i_line in enumerate(lines):
6         if "cmd.realMsg.privateMsg." in line:
7             tmp=line.split("||")
8             str+=tmp[0][-1]
9     print(str)

get x
C:\Users\Dell\AppData\Local\Programs\Python\Python37\python.exe C:/Users/Dell/Desktop/春秋/1/get.py
dtflag{a4e0a418-fced-4b2d-9d76-fdc9053d69a1}s

Process finished with exit code 0

```

CSDN @Mr.水函263

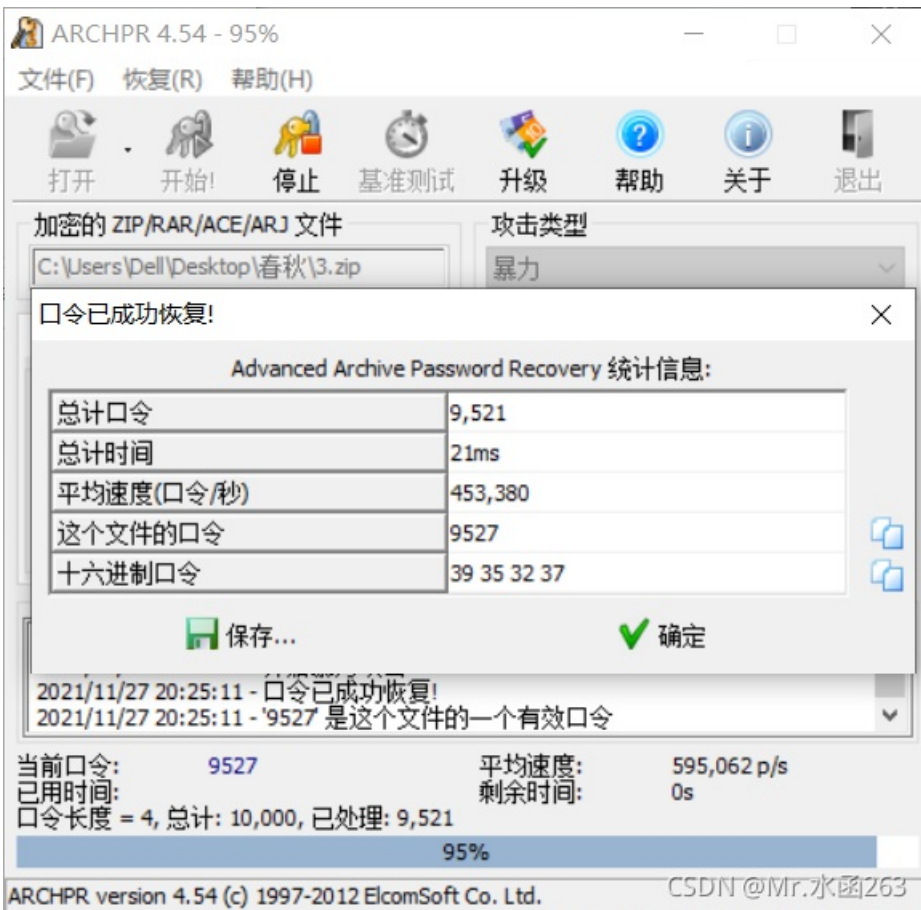
secret_chart

拿到图片，还是010，分解出zip

名称	值	开始	大小	颜色	注释
struct PNG_SIGNATURE ...		0h	8h	Fg: Bg:	
struct PNG_CHUNK chunk IHDR (Critic...		8h	19h	Fg: Bg:	
struct PNG_CHUNK chunk IDAT (Critic...		21h	6E97h	Fg: Bg:	
struct PNG_CHUNK chunk IEND (Critic...		0EB8h	Ch	Fg: Bg:	
struct PNG_CHUNK chunk ...		6EC4h	0h	Fg: Bg:	

CSDN @Mr.水函263

爆破zip得到密码

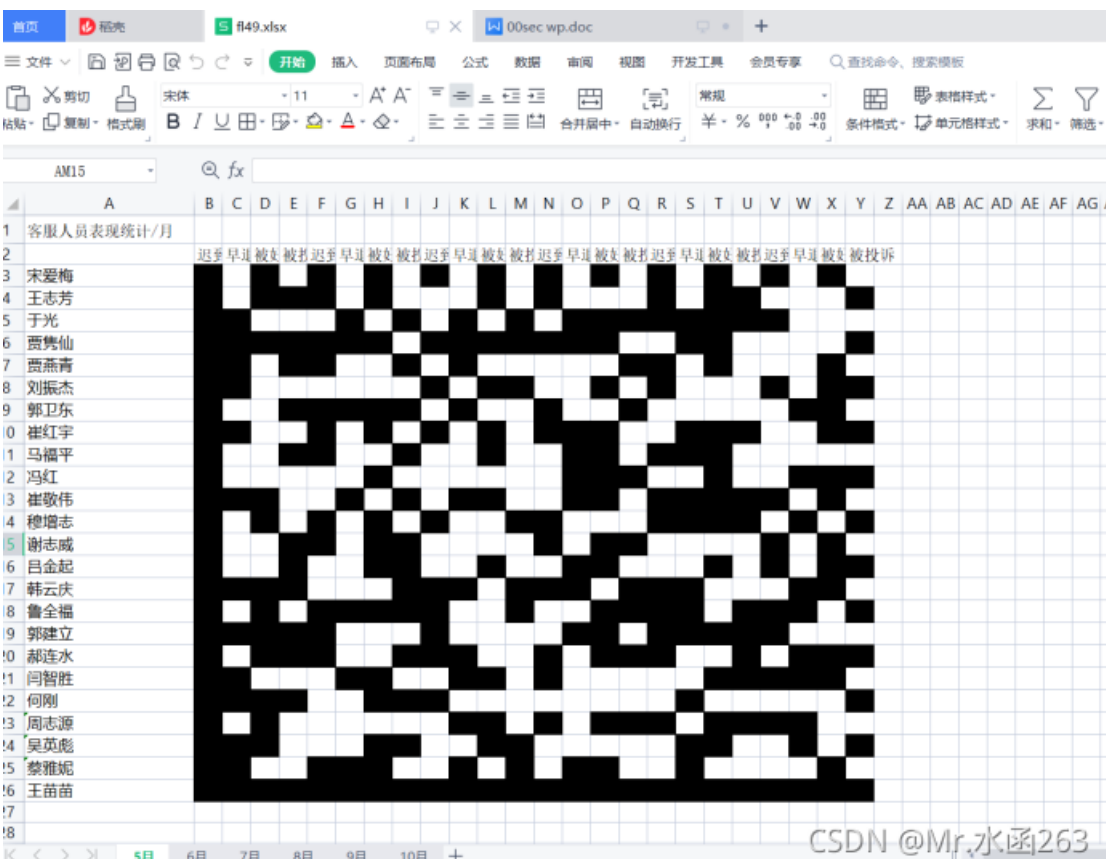


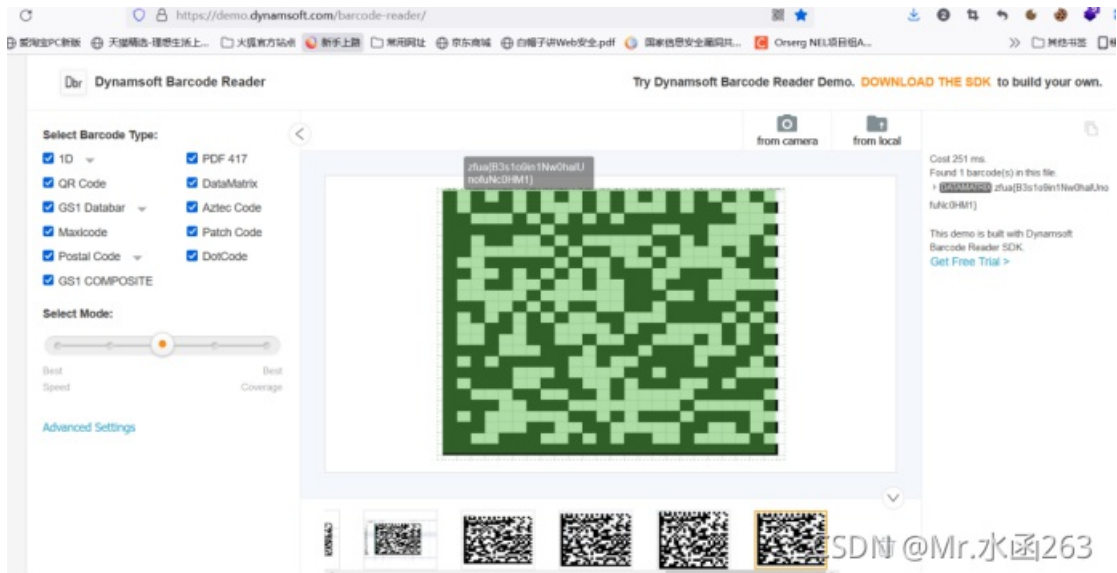
打开excel

类似于dasctf之前的一道题目

将1替换为黑色色块

多个表单的数据拼起来就可以得到barcode





凯撒一把梭

