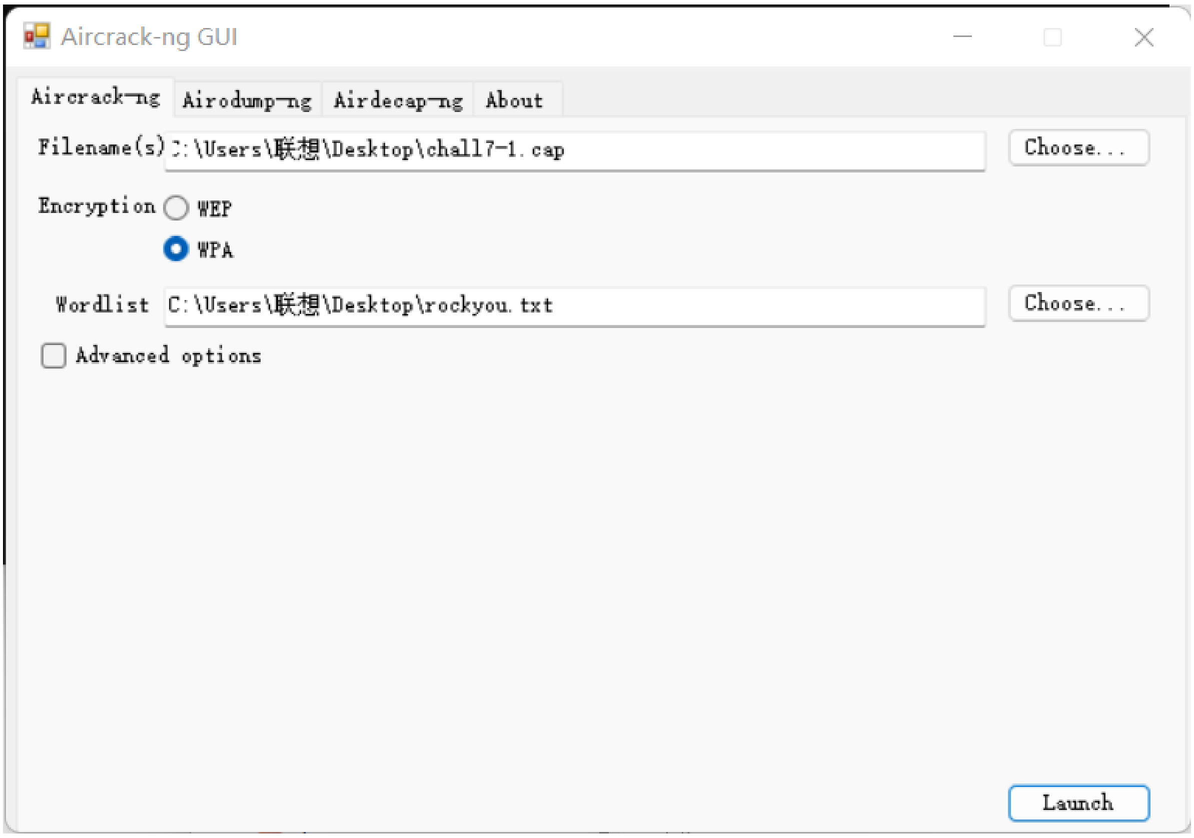
CTF1：

```
flag{aee19bb57a15b1821d4abdf7c89d4a27}
```

use **aircrack-ng** with **rockyou.txt** to find the password:

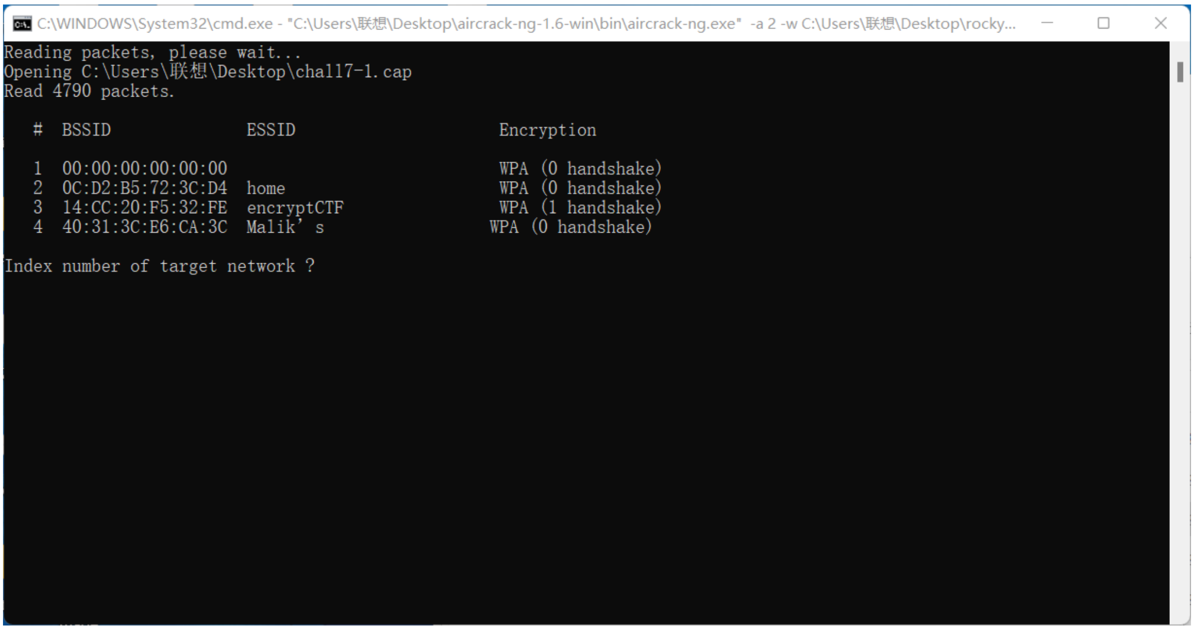


Filename(s) C:\Users\联想\Desktop\chall7-1.cap

Encryption ○ WEP ● WPA

Wordlist C:\Users\联想\Desktop\rockyou.txt

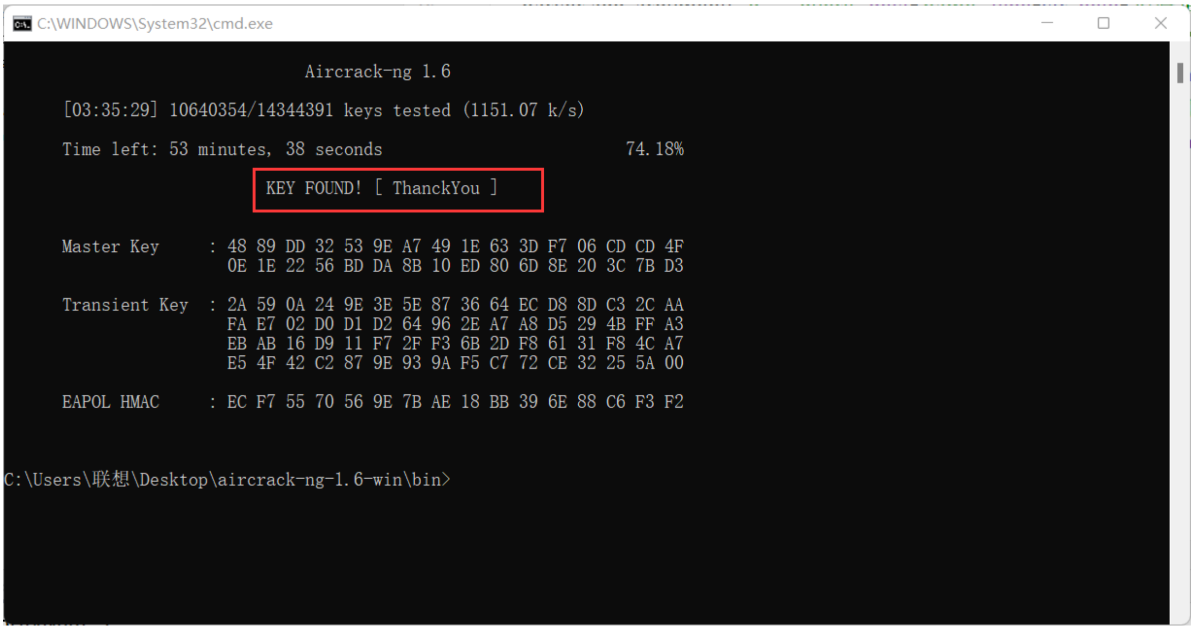
□ Advanced options



C:\WINDOWS\System32\cmd.exe - "C:\Users\联想\Desktop\aircrack-ng-1.6-win\bin\aircrack-ng.exe" -a 2 -w C:\Users\联想\Desktop\rocky...

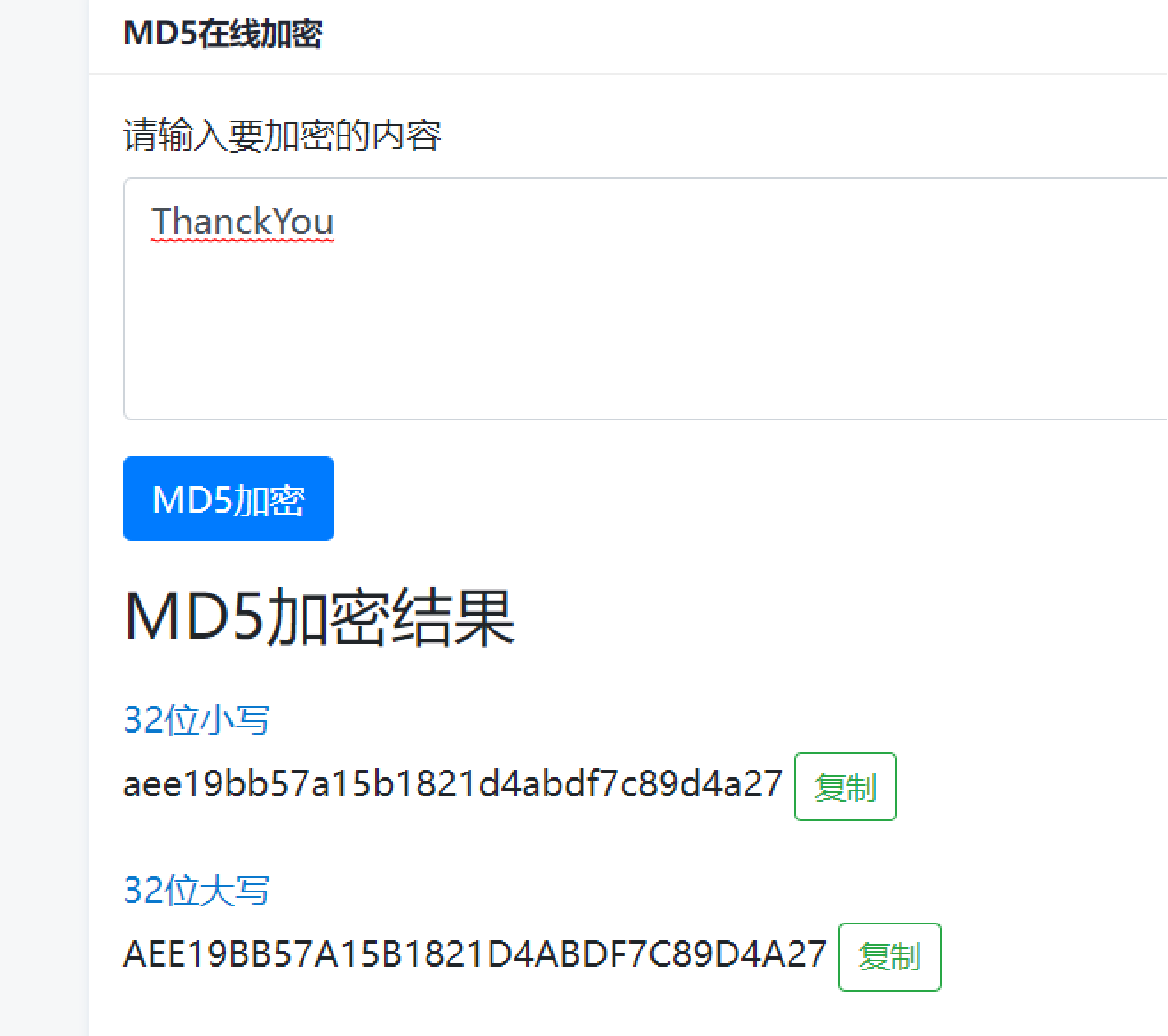
```
Reading packets, please wait...
Opening C:\Users\联想\Desktop\chall7-1.cap
Read 4790 packets.

   #  BSSID              ESSID                     Encryption

   1  00:00:00:00:00:00                            WPA (0 handshake)
   2  0C:D2:B5:72:3C:D4  home                      WPA (0 handshake)
   3  14:CC:20:F5:32:FE  encryptCTF                WPA (1 handshake)
   4  40:31:3C:E6:CA:3C  Malik’ s                 WPA (0 handshake)

Index number of target network ?
```

Finally find the answer:



C:\WINDOWS\System32\cmd.exe

```
                               Aircrack-ng 1.6

      [03:35:29] 10640354/14344391 keys tested (1151.07 k/s)

      Time left: 53 minutes, 38 seconds                          74.18%

                          KEY FOUND! [ ThanckYou ]


      Master Key     : 48 89 DD 32 53 9E A7 49 1E 63 3D F7 06 CD CD 4F
                       0E 1E 22 56 BD DA 8B 10 ED 80 6D 8E 20 3C 7B D3

      Transient Key  : 2A 59 0A 24 9E 3E 5E 87 36 64 EC D8 8D C3 2C AA
                       FA E7 02 D0 D1 D2 64 96 2E A7 A8 D5 29 4B FF A3
                       EB AB 16 D9 11 F7 2F F3 6B 2D F8 61 31 F8 4C A7
                       E5 4F 42 C2 87 9E 93 9A F5 C7 72 CE 32 25 5A 00

      EAPOL HMAC     : EC F7 55 70 56 9E 7B AE 18 BB 39 6E 88 C6 F3 F2


C:\Users\联想\Desktop\aircrack-ng-1.6-win\bin>
```



MD5在线加密

请输入要加密的内容

ThanckYou

MD5加密结果

32位小写

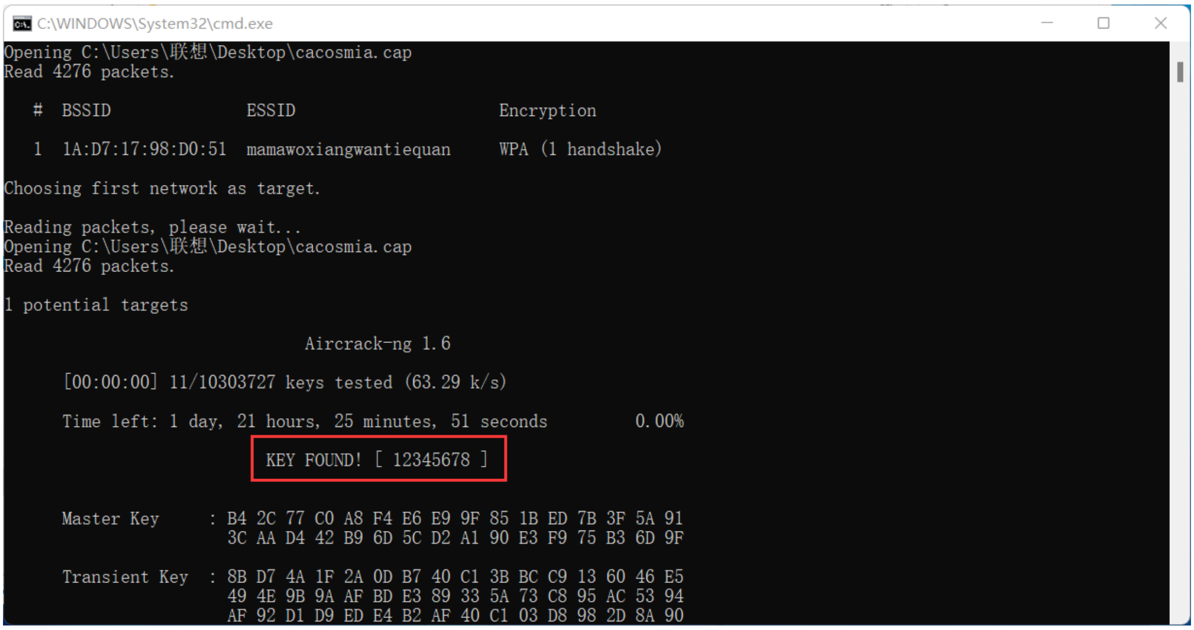
aee19bb57a15b1821d4abdf7c89d4a27

32位大写

AEE19BB57A15B1821D4ABDF7C89D4A27

CTF2:

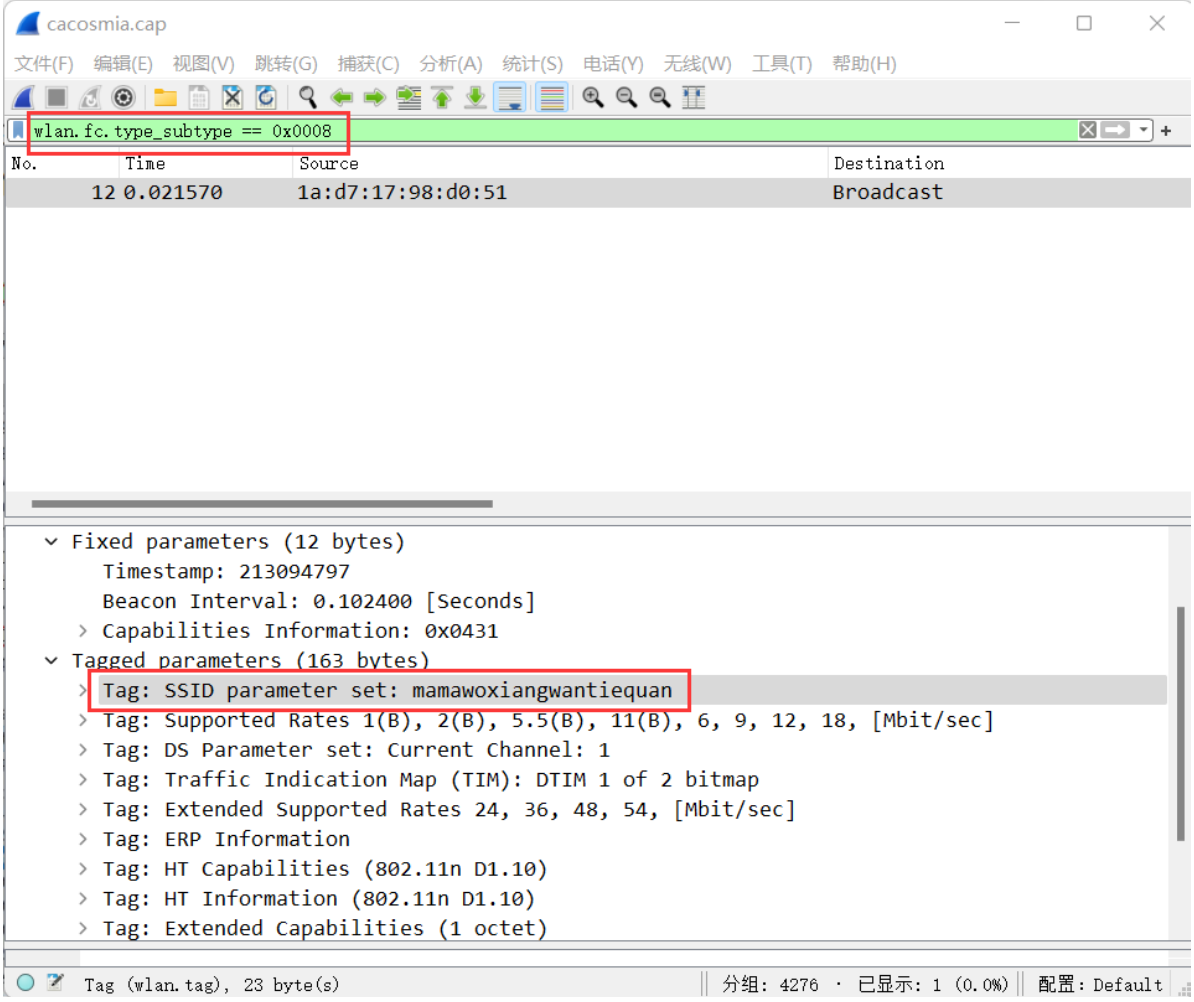
crack to get the word:



```
Opening C:\Users\联想\Desktop\cacosmia.cap
Read 4276 packets.

   #  BSSID              ESSID                     Encryption

   1  1A:D7:17:98:D0:51  mamawoxiangwantiequan     WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening C:\Users\联想\Desktop\cacosmia.cap
Read 4276 packets.

1 potential targets

                               Aircrack-ng 1.6

      [00:00:00] 11/10303727 keys tested (63.29 k/s)

      Time left: 1 day, 21 hours, 25 minutes, 51 seconds         0.00%

                         KEY FOUND! [ 12345678 ]


      Master Key     : B4 2C 77 C0 A8 F4 E6 E9 9F 85 1B ED 7B 3F 5A 91
                       3C AA D4 42 B9 6D 5C D2 A1 90 E3 F9 75 B3 6D 9F

      Transient Key  : 8B D7 4A 1F 2A 0D B7 40 C1 3B BC C9 13 60 46 E5
                       49 4E 9B 9A AF BD E3 89 33 5A 73 C8 95 AC 53 94
                       AF 92 D1 D9 ED E4 B2 AF 40 C1 03 D8 98 2D 8A 90
```

Decrypted packet:

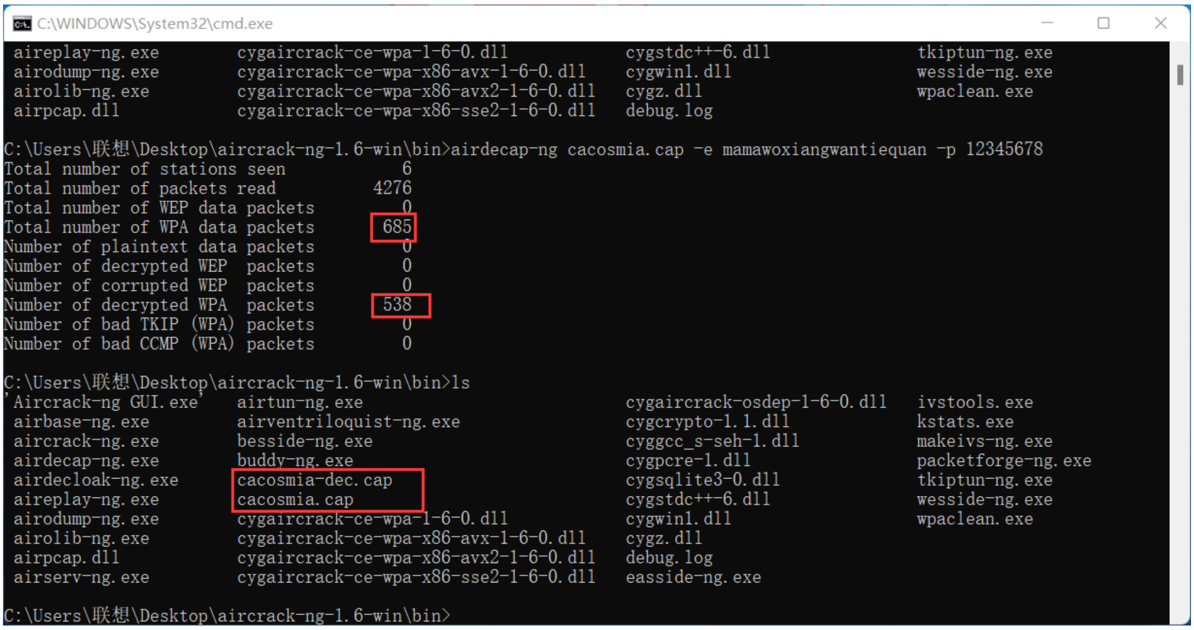
1.get SSID name:



cacosmia.cap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

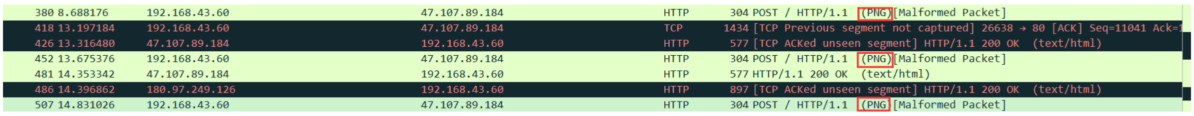
```
wlan.fc.type_subtype == 0x0008

No.  Time        Source              Destination
  12 0.021570    1a:d7:17:98:d0:51   Broadcast

 ⌄ Fixed parameters (12 bytes)
     Timestamp: 213094797
     Beacon Interval: 0.102400 [Seconds]
   › Capabilities Information: 0x0431
 ⌄ Tagged parameters (163 bytes)
   › Tag: SSID parameter set: mamawoxiangwantiequan
   › Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
   › Tag: DS Parameter set: Current Channel: 1
   › Tag: Traffic Indication Map (TIM): DTIM 1 of 2 bitmap
   › Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
   › Tag: ERP Information
   › Tag: HT Capabilities (802.11n D1.10)
   › Tag: HT Information (802.11n D1.10)
   › Tag: Extended Capabilities (1 octet)

Tag (wlan.tag), 23 byte(s)    分组: 4276 · 已显示: 1 (0.0%)    配置: Default
```

2.decrypt it:

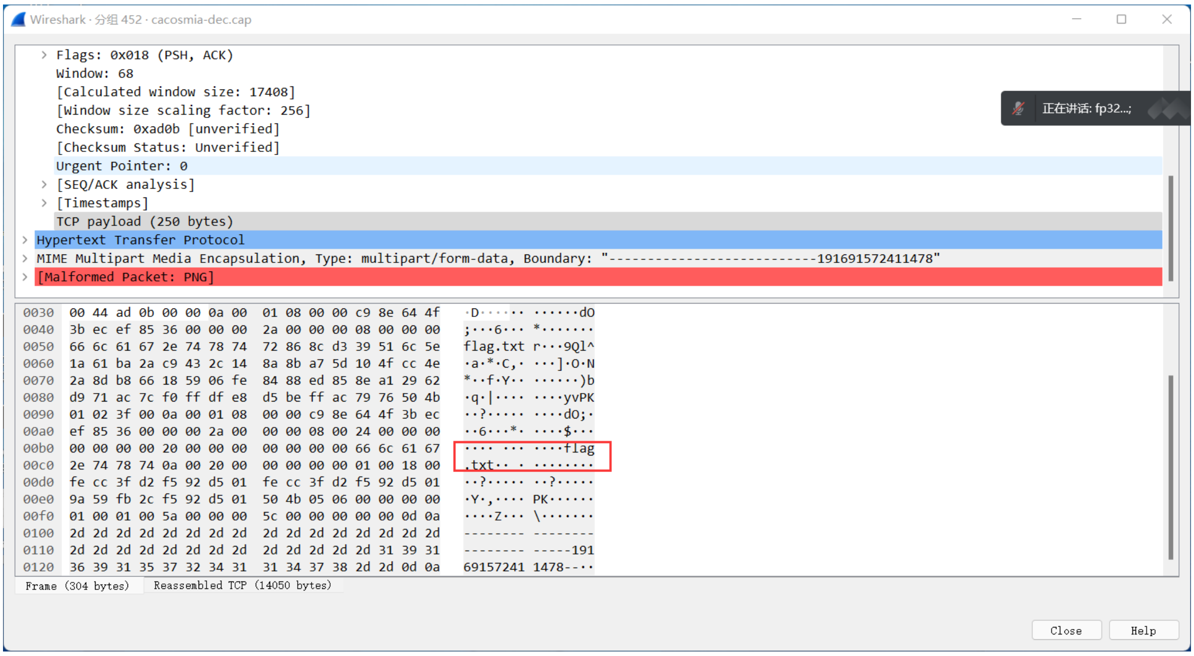


```
 aireplay-ng.exe        cygaircrack-ce-wpa-1-6-0.dll                cygstdc++-6.dll          tkiptun-ng.exe
 airodump-ng.exe        cygaircrack-ce-wpa-x86-avx-1-6-0.dll        cygwin1.dll              wesside-ng.exe
 airolib-ng.exe         cygaircrack-ce-wpa-x86-avx2-1-6-0.dll       cygz.dll                 wpaclean.exe
 airpcap.dll            cygaircrack-ce-wpa-x86-sse2-1-6-0.dll       debug.log

C:\Users\联想\Desktop\aircrack-ng-1.6-win\bin>airdecap-ng cacosmia.cap -e mamawoxiangwantiequan -p 12345678
Total number of stations seen            6
Total number of packets read          4276
Total number of WEP data packets         0
Total number of WPA data packets       685
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets       538
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0

C:\Users\联想\Desktop\aircrack-ng-1.6-win\bin>ls
'Aircrack-ng GUI.exe'   airtun-ng.exe                               cygaircrack-osdep-1-6-0.dll   ivstools.exe
 airbase-ng.exe         airventriloquist-ng.exe                     cygcrypto-1.1.dll             kstats.exe
 aircrack-ng.exe        besside-ng.exe                              cyggcc_s-seh-1.dll            makeivs-ng.exe
 airdecap-ng.exe        buddy-ng.exe                                cygpcre-1.dll                 packetforge-ng.exe
 airdecloak-ng.exe      cacosmia-dec.cap                            cygsqlite3-0.dll              tkiptun-ng.exe
 aireplay-ng.exe        cacosmia.cap                                cygstdc++-6.dll               wesside-ng.exe
 airodump-ng.exe        cygaircrack-ce-wpa-1-6-0.dll                cygwin1.dll                   wpaclean.exe
 airolib-ng.exe         cygaircrack-ce-wpa-x86-avx-1-6-0.dll        cygz.dll
 airpcap.dll            cygaircrack-ce-wpa-x86-avx2-1-6-0.dll       debug.log
 airserv-ng.exe         cygaircrack-ce-wpa-x86-sse2-1-6-0.dll       easside-ng.exe

C:\Users\联想\Desktop\aircrack-ng-1.6-win\bin>
```

Analyse the package:



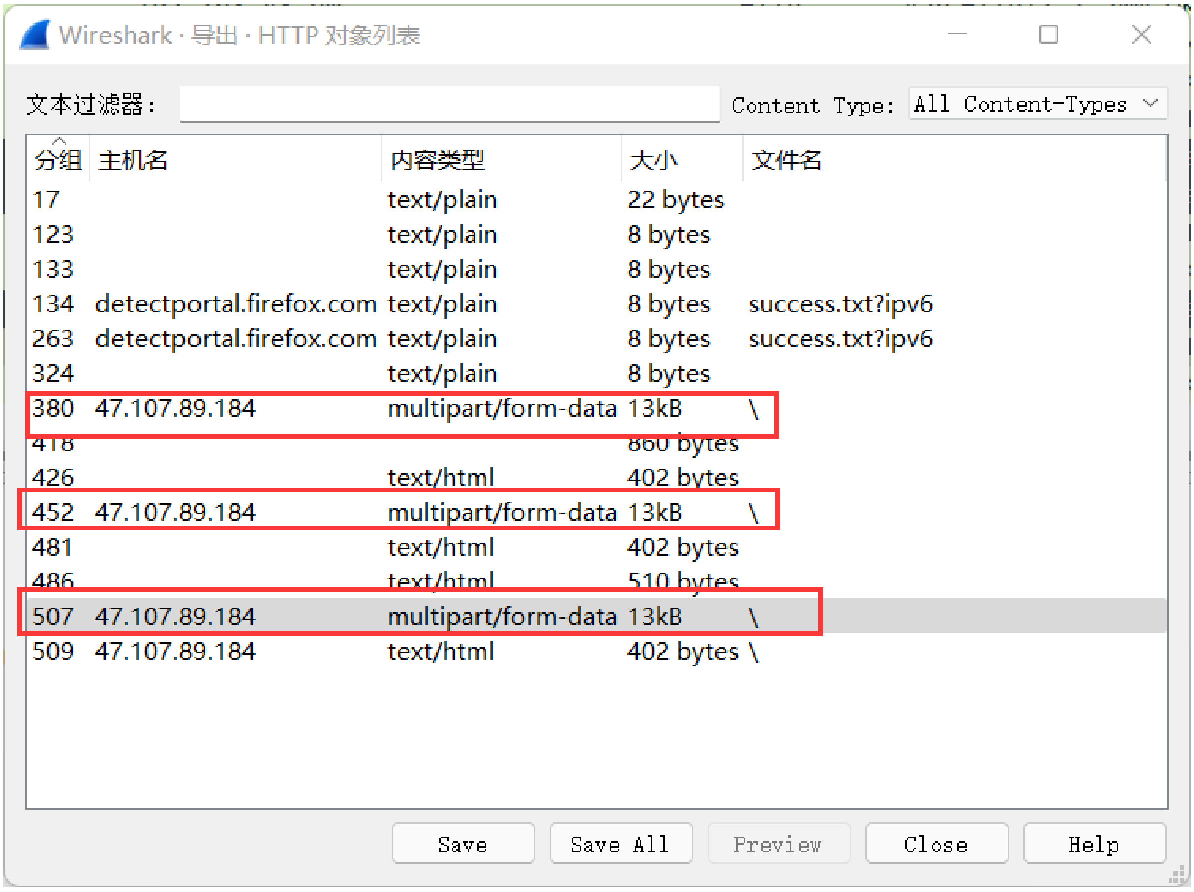
```
380 8.688176    192.168.43.60     47.107.89.184    HTTP   304 POST / HTTP/1.1  (PNG)[Malformed Packet]
418 13.197184   192.168.43.60     47.107.89.184    TCP   1434 [TCP Previous segment not captured] 26638 → 80 [ACK] Seq=11041 Ack=1
426 13.316480   47.107.89.184     192.168.43.60    HTTP   577 [TCP ACKed unseen segment] HTTP/1.1 200 OK  (text/html)
452 13.675376   192.168.43.60     47.107.89.184    HTTP   304 POST / HTTP/1.1  (PNG)[Malformed Packet]
481 14.353342   47.107.89.184     192.168.43.60    HTTP   577 HTTP/1.1 200 OK  (text/html)
486 14.396862   180.97.249.126    192.168.43.60    HTTP   897 [TCP ACKed unseen segment] HTTP/1.1 200 OK  (text/html)
507 14.831026   192.168.43.60     47.107.89.184    HTTP   304 POST / HTTP/1.1  (PNG)[Malformed Packet]
```



```
  > Flags: 0x018 (PSH, ACK)
    Window: 68
    [Calculated window size: 17408]
    [Window size scaling factor: 256]
    Checksum: 0xad0b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (250 bytes)
> Hypertext Transfer Protocol
> MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "---------------------------191691572411478"
> [Malformed Packet: PNG]

0030  00 44 ad 0b 00 00 0a 00  01 08 00 00 c9 8e 64 4f   ·D······ ······dO
0040  3b ec ef 85 36 00 00 00  2a 00 00 00 08 00 00 00   ;···6··· *·······
0050  66 6c 61 67 2e 74 78 74  72 86 8c d3 39 51 6c 5e   flag.txt r···9Ql^
0060  1a 61 ba 2a c9 43 2c 14  8a 8b a7 5d 10 4f cc 4e   ·a·*·C,· ···]·O·N
0070  2a 8d b8 66 18 59 06 fe  84 88 ed 85 8e a1 29 62   *··f·Y·· ······)b
0080  d9 71 ac 7c f0 ff df e8  d5 be ff ac 79 76 50 4b   ·q·|···· ····yvPK
0090  01 02 3f 00 0a 00 01 08  00 00 c9 8e 64 4f 3b ec   ··?····· ····dO;·
00a0  ef 85 36 00 00 00 2a 00  00 00 08 00 24 00 00 00   ··6···*· ····$···
00b0  00 00 00 00 20 00 00 00  00 00 00 00 66 6c 61 67   ········ ····flag
00c0  2e 74 78 74 0a 00 20 00  00 00 00 00 01 00 18 00   .txt·· · ········
00d0  fe cc 3f d2 f5 92 d5 01  fe cc 3f d2 f5 92 d5 01   ··?····· ··?·····
00e0  9a 59 fb 2c f5 92 d5 01  50 4b 05 06 00 00 00 00   ·Y·,···· PK······
00f0  01 00 01 00 5a 00 00 00  5c 00 00 00 00 00 0d 0a   ····Z··· \·······
0100  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0110  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 31 39 31   -------- -----191
0120  36 39 31 35 37 32 34 31  31 34 37 38 2d 2d 0d 0a   69157241 1478--··

Frame (304 bytes)   Reassembled TCP (14050 bytes)
```

find it post 3 pngs and txt was hiden inside.

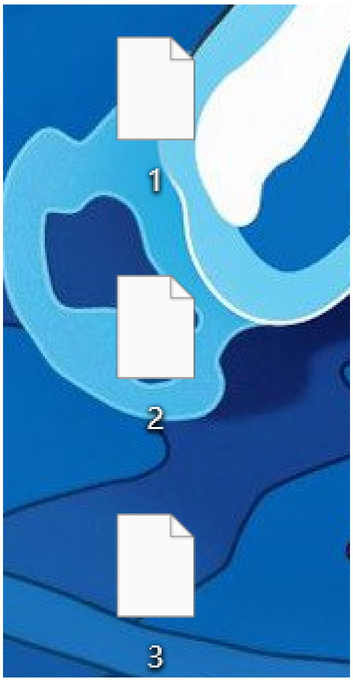
export it and rename it to zip.

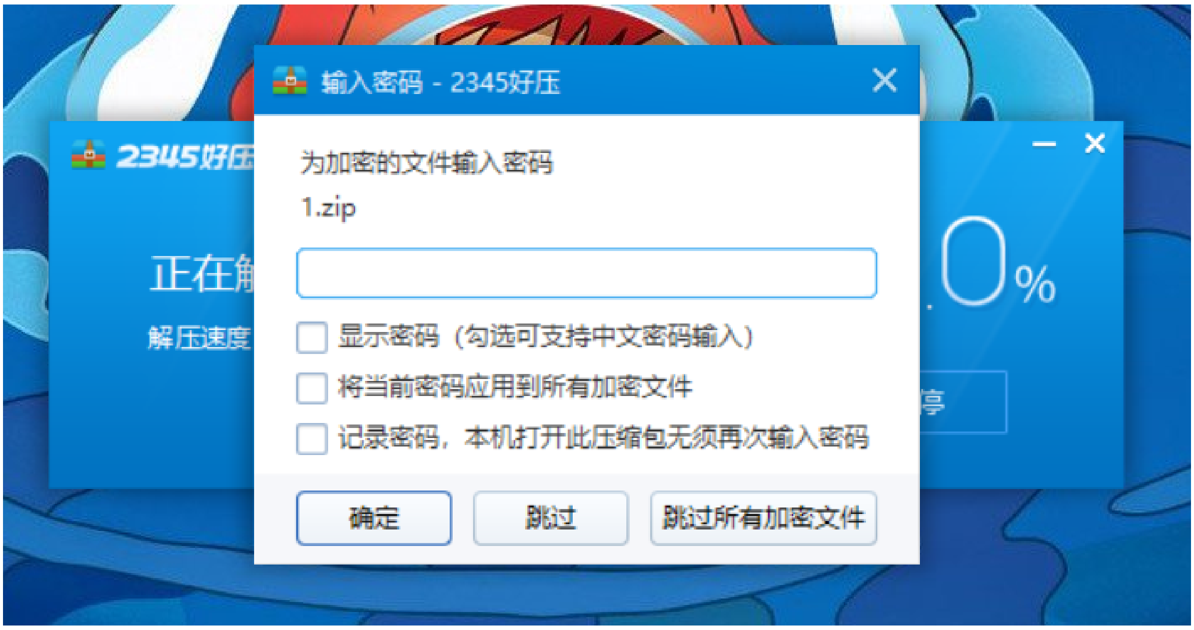


Wireshark · 导出 · HTTP 对象列表

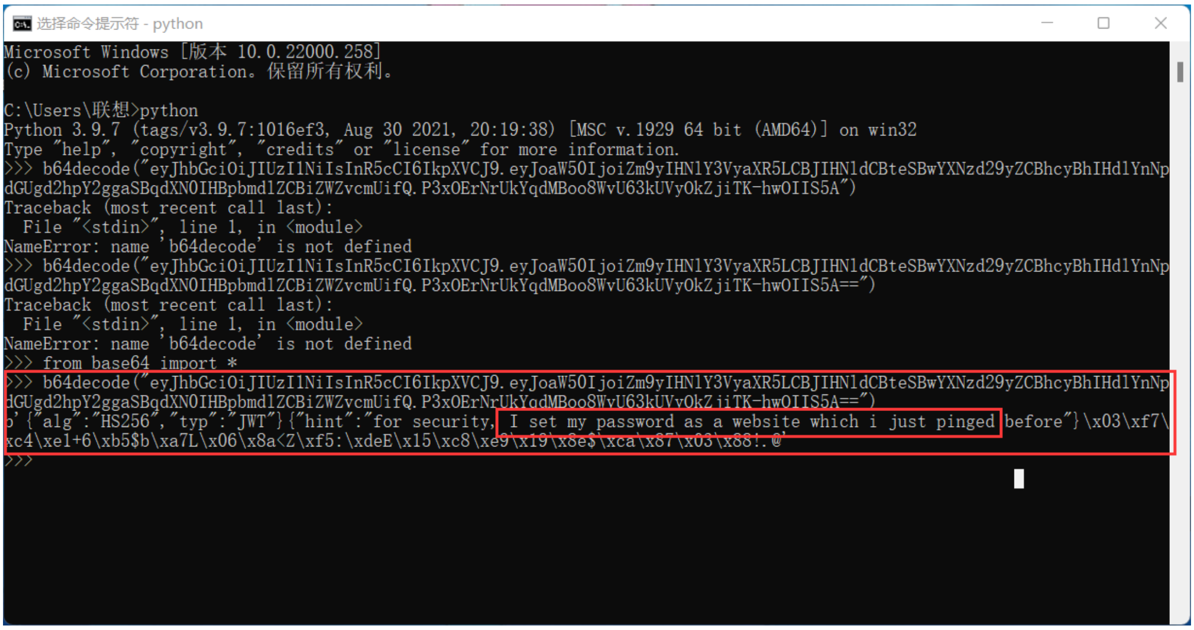
文本过滤器： Content Type: All Content-Types

分组	主机名	内容类型	大小	文件名
17		text/plain	22 bytes	
123		text/plain	8 bytes	
133		text/plain	8 bytes	
134	detectportal.firefox.com	text/plain	8 bytes	success.txt?ipv6
263	detectportal.firefox.com	text/plain	8 bytes	success.txt?ipv6
324		text/plain	8 bytes	
380	47.107.89.184	multipart/form-data	13kB	\
418			860 bytes	
426		text/html	402 bytes	
452	47.107.89.184	multipart/form-data	13kB	\
481		text/html	402 bytes	
486		text/html	510 bytes	
507	47.107.89.184	multipart/form-data	13kB	\
509	47.107.89.184	text/html	402 bytes	\



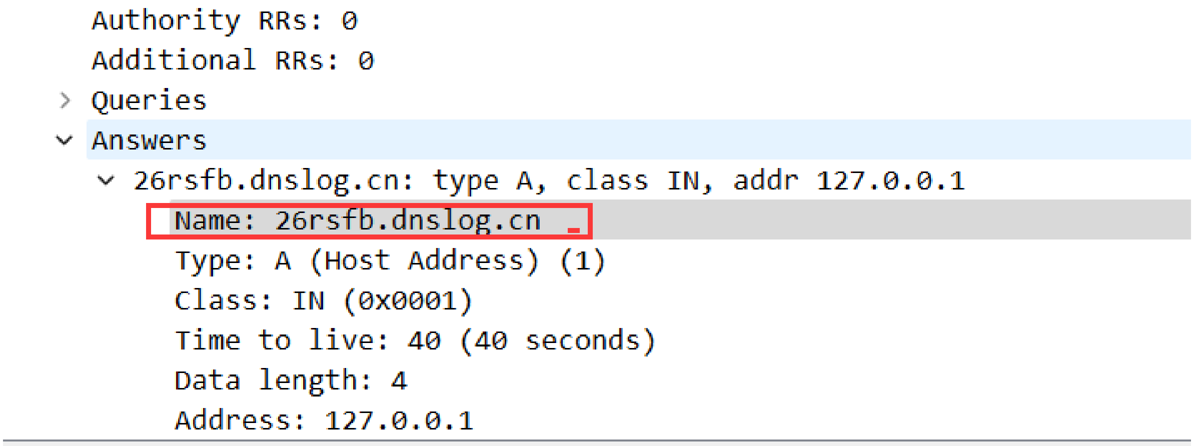

2345好压
正在解
解压速度
0%
停
输入密码 - 2345好压
为加密的文件输入密码
1.zip
□ 显示密码（勾选可支持中文密码输入）
□ 将当前密码应用到所有加密文件
□ 记录密码，本机打开此压缩包无须再次输入密码
确定
跳过
跳过所有加密文件

Find the password for unzip, get hint from cookie:



```
Microsoft Windows [版本 10.0.22000.258]
(c) Microsoft Corporation。保留所有权利。

C:\Users\联想>python
Python 3.9.7 (tags/v3.9.7:1016ef3, Aug 30 2021, 20:19:38) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> b64decode("eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJoaW50IjoiZm9yIHNlY3VyaXR5LCBJIHNldCBteSBwYXNzd29yZCBhcyBhIHdlYnNp
dGUgd2hpY2ggaSBqdXN0IHBpbmdlZCBiZWZvcmUifQ.P3xOErNrUkYqdMBoo8WvU63kUVyOkZjiTK-hwOIIS5A")
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'b64decode' is not defined
>>> b64decode("eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJoaW50IjoiZm9yIHNlY3VyaXR5LCBJIHNldCBteSBwYXNzd29yZCBhcyBhIHdlYnNp
dGUgd2hpY2ggaSBqdXN0IHBpbmdlZCBiZWZvcmUifQ.P3xOErNrUkYqdMBoo8WvU63kUVyOkZjiTK-hwOIIS5A==")
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'b64decode' is not defined
>>> from base64 import *
>>> b64decode("eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJoaW50IjoiZm9yIHNlY3VyaXR5LCBJIHNldCBteSBwYXNzd29yZCBhcyBhIHdlYnNp
dGUgd2hpY2ggaSBqdXN0IHBpbmdlZCBiZWZvcmUifQ.P3xOErNrUkYqdMBoo8WvU63kUVyOkZjiTK-hwOIIS5A==")
b'{"alg":"HS256","typ":"JWT"}{"hint":"for security, I set my password as a website which i just pinged before"}\x03\xf7\
xc4\xe1+6\xb5$b\xa7L\x06\x8a<Z\xf5:\xdeE\x15\xc8\xe9\x19\x8e$\xca\x87\x03\x88!.@'
>>>
```

Find the webite through DNS record:



```
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  ∨ Answers
    ∨ 26rsfb.dnslog.cn: type A, class IN, addr 127.0.0.1
        Name: 26rsfb.dnslog.cn
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 40 (40 seconds)
        Data length: 4
        Address: 127.0.0.1
```

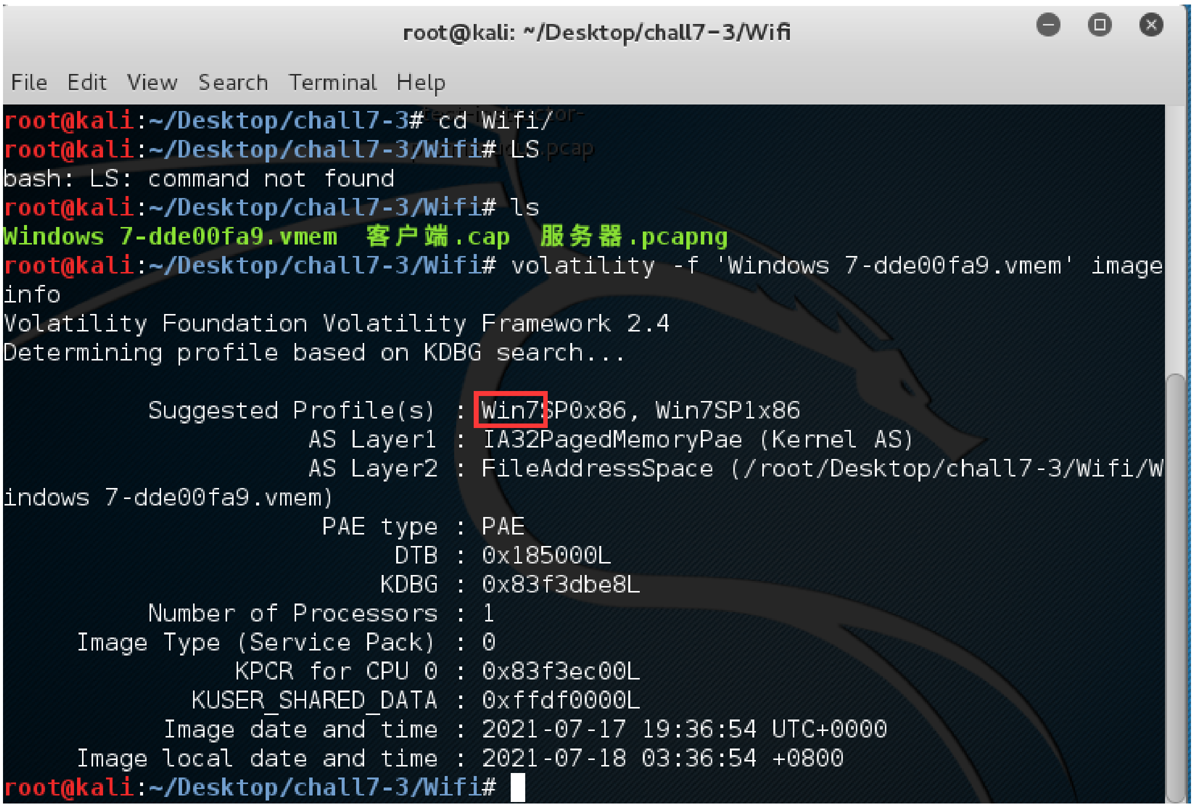
Then unzip it and get the flag.

```
flag{f14376d0-793e-4e20-9eab-af23f3fdc158}
```

CTF3:

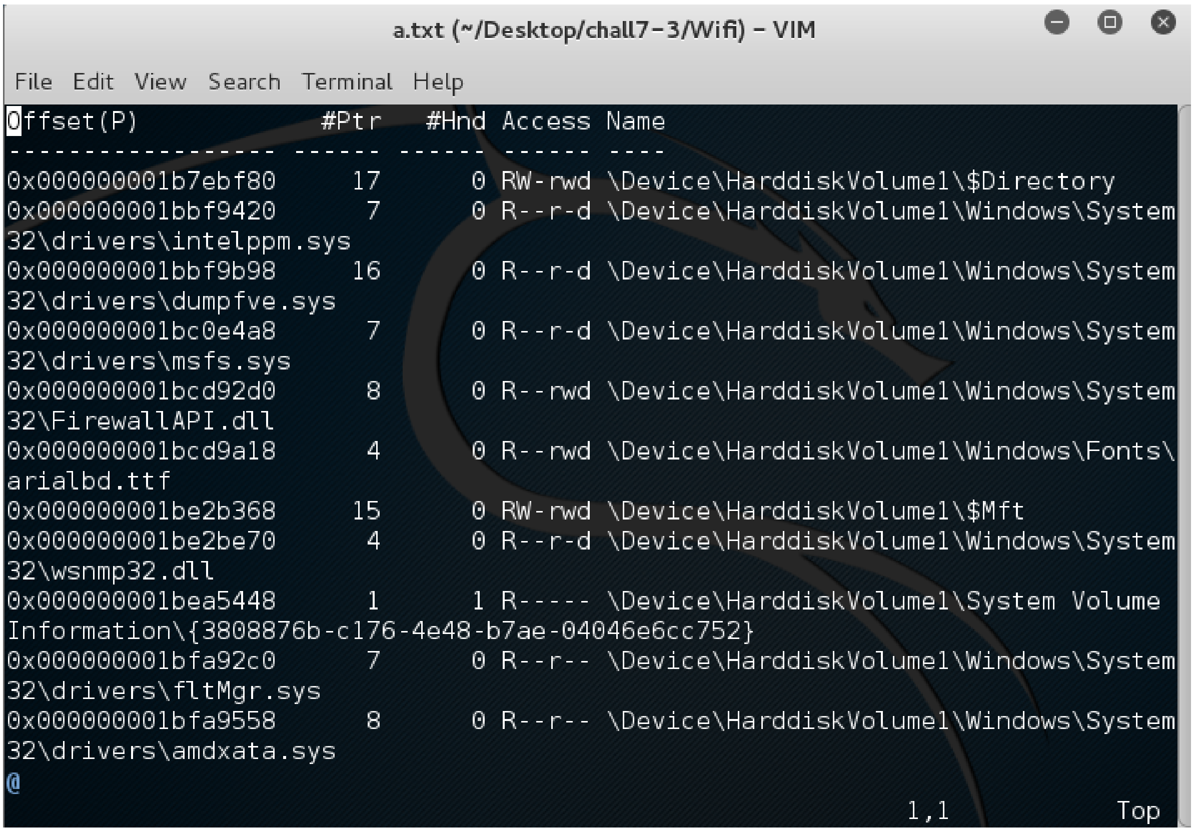
```
flag{5db5b7b0bb74babb66e1522f3a6b1b12}
```

get the data in the vm:


root@kali: ~/Desktop/chall7-3/Wifi
File Edit View Search Terminal Help

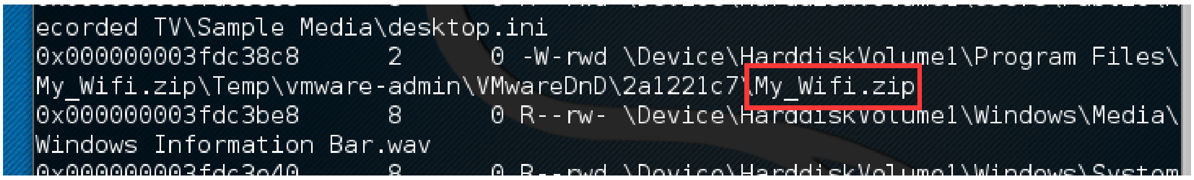
```
root@kali:~/Desktop/chall7-3# cd Wifi/
root@kali:~/Desktop/chall7-3/Wifi# LS
bash: LS: command not found
root@kali:~/Desktop/chall7-3/Wifi# ls
Windows 7-dde00fa9.vmem  客户端.cap  服务器.pcapng
root@kali:~/Desktop/chall7-3/Wifi# volatility -f 'Windows 7-dde00fa9.vmem' image
info
Volatility Foundation Volatility Framework 2.4
Determining profile based on KDBG search...

          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Desktop/chall7-3/Wifi/W
indows 7-dde00fa9.vmem)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x83f3dbe8L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x83f3ec00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2021-07-17 19:36:54 UTC+0000
     Image local date and time : 2021-07-18 03:36:54 +0800
root@kali:~/Desktop/chall7-3/Wifi#
```

get file dir:


a.txt (~/Desktop/chall7-3/Wifi) - VIM
File Edit View Search Terminal Help

```
Offset(P)            #Ptr   #Hnd Access Name
------------------ ------ ------ ------ ----
0x000000001b7ebf80     17      0 RW-rwd \Device\HarddiskVolume1\$Directory
0x000000001bbf9420      7      0 R--r-d \Device\HarddiskVolume1\Windows\System
32\drivers\intelppm.sys
0x000000001bbf9b98     16      0 R--r-d \Device\HarddiskVolume1\Windows\System
32\drivers\dumpfve.sys
0x000000001bc0e4a8      7      0 R--r-d \Device\HarddiskVolume1\Windows\System
32\drivers\msfs.sys
0x000000001bcd92d0      8      0 R--rwd \Device\HarddiskVolume1\Windows\System
32\FirewallAPI.dll
0x000000001bcd9a18      4      0 R--rwd \Device\HarddiskVolume1\Windows\Fonts\
arialbd.ttf
0x000000001be2b368     15      0 RW-rwd \Device\HarddiskVolume1\$Mft
0x000000001be2be70      4      0 R--r-d \Device\HarddiskVolume1\Windows\System
32\wsnmp32.dll
0x000000001bea5448      1      1 R----- \Device\HarddiskVolume1\System Volume
Information\{3808876b-c176-4e48-b7ae-04046e6cc752}
0x000000001bfa92c0      7      0 R--r-- \Device\HarddiskVolume1\Windows\System
32\drivers\fltMgr.sys
0x000000001bfa9558      8      0 R--r-- \Device\HarddiskVolume1\Windows\System
32\drivers\amdxata.sys
@
                                                            1,1           Top
```

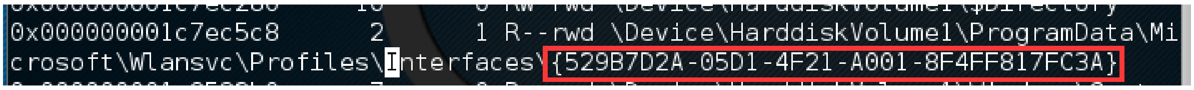
Find zip file:



```
ecorded TV\Sample Media\desktop.ini
0x000000003fdc38c8      2       0 -W-rwd \Device\HarddiskVolume1\Program Files\
My_Wifi.zip\Temp\vmware-admin\VMwareDnD\2a1221c7\My_Wifi.zip
0x000000003fdc3be8      8       0 R--rw- \Device\HarddiskVolume1\Windows\Media\
Windows Information Bar.wav
0x000000003fdc3c40      8       0 R--rwd \Device\HarddiskVolume1\Windows\System
```

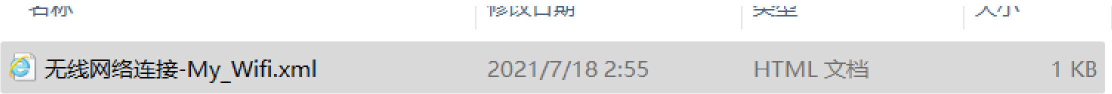
to unzip it need password:

search interface and find it:s

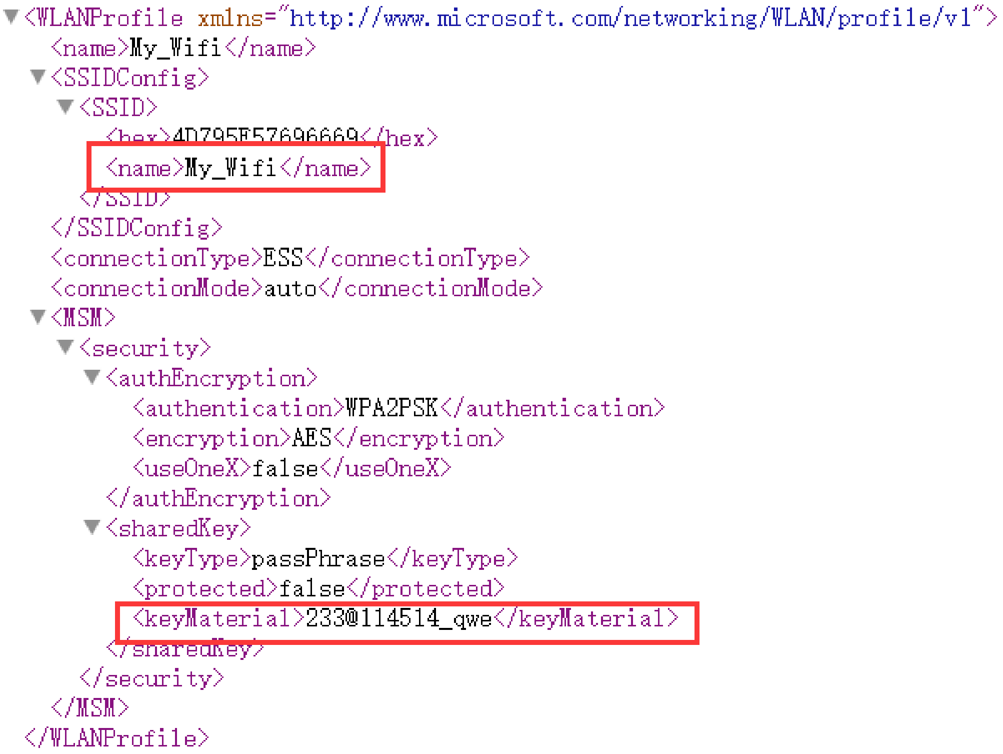


```
0x000000001c7ec2b0     10       0 Rw-rwd \Device\HarddiskVolume1\$Directory
0x000000001c7ec5c8      2       1 R--rwd \Device\HarddiskVolume1\ProgramData\Mi
crosoft\Wlansvc\Profiles\Interfaces\{529B7D2A-05D1-4F21-A001-8F4FF817FC3A}
```

Then we get wifi password:

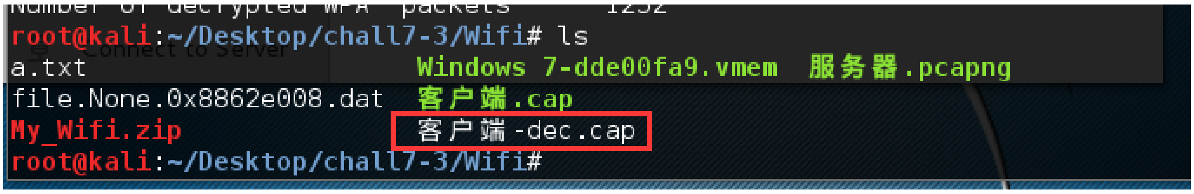


名称	修改日期	类型	大小
无线网络连接-My_Wifi.xml	2021/7/18 2:55	HTML 文档	1 KB



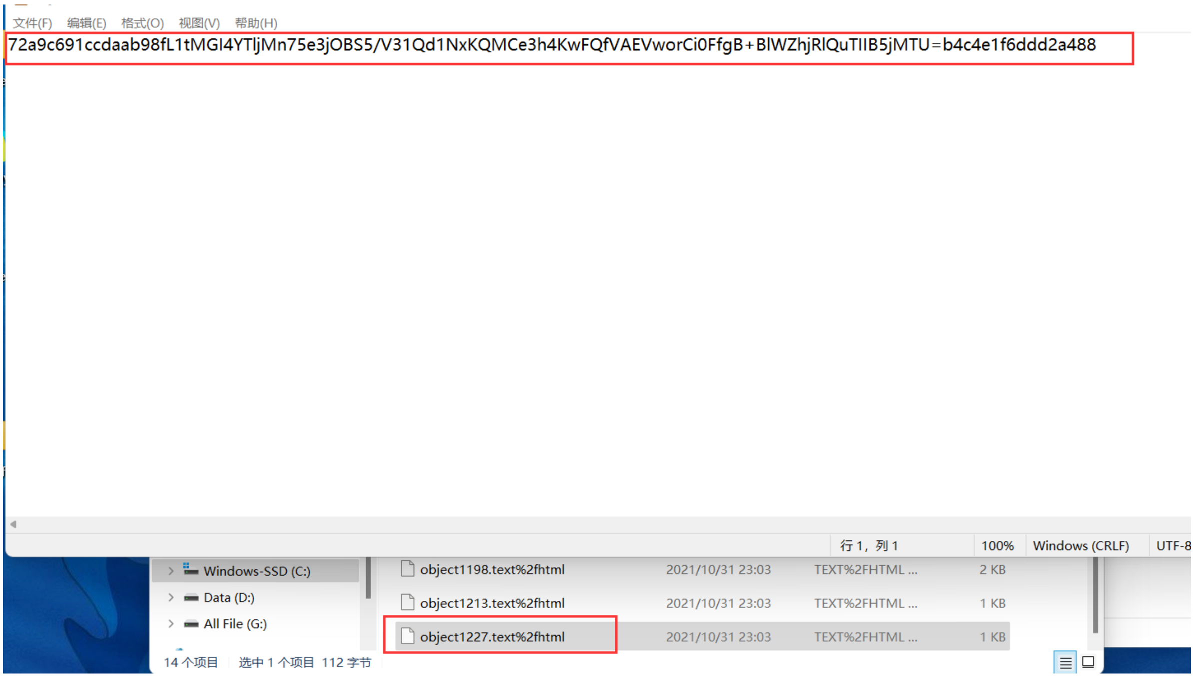
```
▼<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
   <name>My_Wifi</name>
 ▼<SSIDConfig>
   ▼<SSID>
      <hex>4D795F57696669</hex>
      <name>My_Wifi</name>
    </SSID>
   </SSIDConfig>
   <connectionType>ESS</connectionType>
   <connectionMode>auto</connectionMode>
 ▼<MSM>
   ▼<security>
     ▼<authEncryption>
        <authentication>WPA2PSK</authentication>
        <encryption>AES</encryption>
        <useOneX>false</useOneX>
      </authEncryption>
     ▼<sharedKey>
        <keyType>passPhrase</keyType>
        <protected>false</protected>
        <keyMaterial>233@114514_qwe</keyMaterial>
      </sharedKey>
    </security>
   </MSM>
</WLANProfile>
```

decrept 客户端.cap



```
Number of decrypted WPA packets      1232
root@kali:~/Desktop/chall7-3/Wifi# ls
a.txt                   Windows 7-dde00fa9.vmem  服务器.pcapng
file.None.0x8862e008.dat  客户端.cap
My_Wifi.zip             客户端-dec.cap
root@kali:~/Desktop/chall7-3/Wifi#
```

export HTTP object and get the last object:

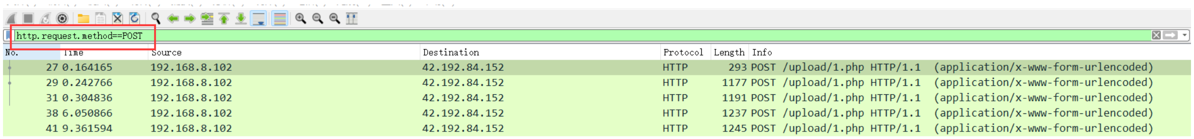


```
72a9c691ccdaab98fL1tMGI4YTljMn75e3jOBS5/V31Qd1NxKQMCe3h4KwFQfVAEVworCi0FfgB+BlWZhjRlQuTIIB5jMTU=b4c4e1f6ddd2a488
```

```
object1198.text%2fhtml    2021/10/31 23:03    TEXT%2FHTML ...    2 KB
object1213.text%2fhtml    2021/10/31 23:03    TEXT%2FHTML ...    1 KB
object1227.text%2fhtml    2021/10/31 23:03    TEXT%2FHTML ...    1 KB
```

And we need to decrpt it:

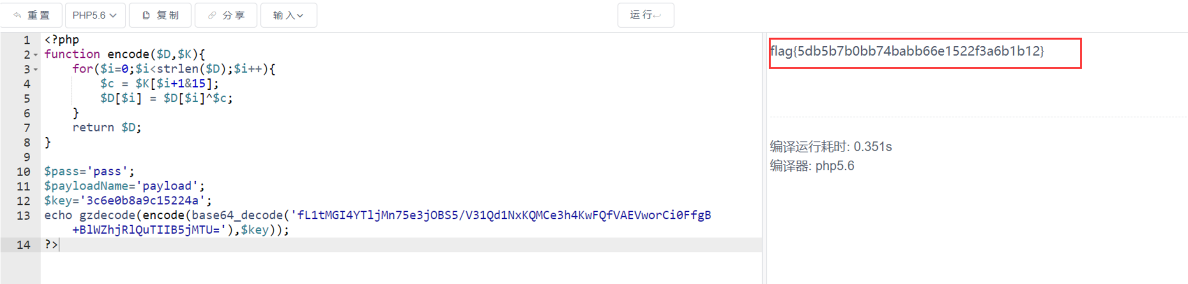
We find php script in the 服务器.pcap:



```
http.request.method==POST
```

```
No.  Time      Source         Destination    Protocol Length Info
  27 0.164165  192.168.8.102  42.192.84.152  HTTP      293 POST /upload/1.php HTTP/1.1  (application/x-www-form-urlencoded)
  29 0.242766  192.168.8.102  42.192.84.152  HTTP     1177 POST /upload/1.php HTTP/1.1  (application/x-www-form-urlencoded)
  31 0.304836  192.168.8.102  42.192.84.152  HTTP     1191 POST /upload/1.php HTTP/1.1  (application/x-www-form-urlencoded)
  38 6.050866  192.168.8.102  42.192.84.152  HTTP     1237 POST /upload/1.php HTTP/1.1  (application/x-www-form-urlencoded)
  41 9.361594  192.168.8.102  42.192.84.152  HTTP     1245 POST /upload/1.php HTTP/1.1  (application/x-www-form-urlencoded)
```

Finally by a script, we decrypt it:



```php
<?php
function encode($D,$K){
    for($i=0;$i<strlen($D);$i++){
        $c = $K[$i+1&15];
        $D[$i] = $D[$i]^$c;
    }
    return $D;
}

$pass='pass';
$payloadName='payload';
$key='3c6e0b8a9c15224a';
echo gzdecode(encode(base64_decode('fL1tMGI4YTljMn75e3jOBS5/V31Qd1NxKQMCe3h4KwFQfVAEVworCi0FfgB
    +BlWZhjRlQuTIIB5jMTU='),$key));
?>
```

```
flag{5db5b7b0bb74babb66e1522f3a6b1b12}

编译运行耗时: 0.351s
编译器: php5.6
```