XCTF-MISC-新手区-功夫再高也怕菜刀

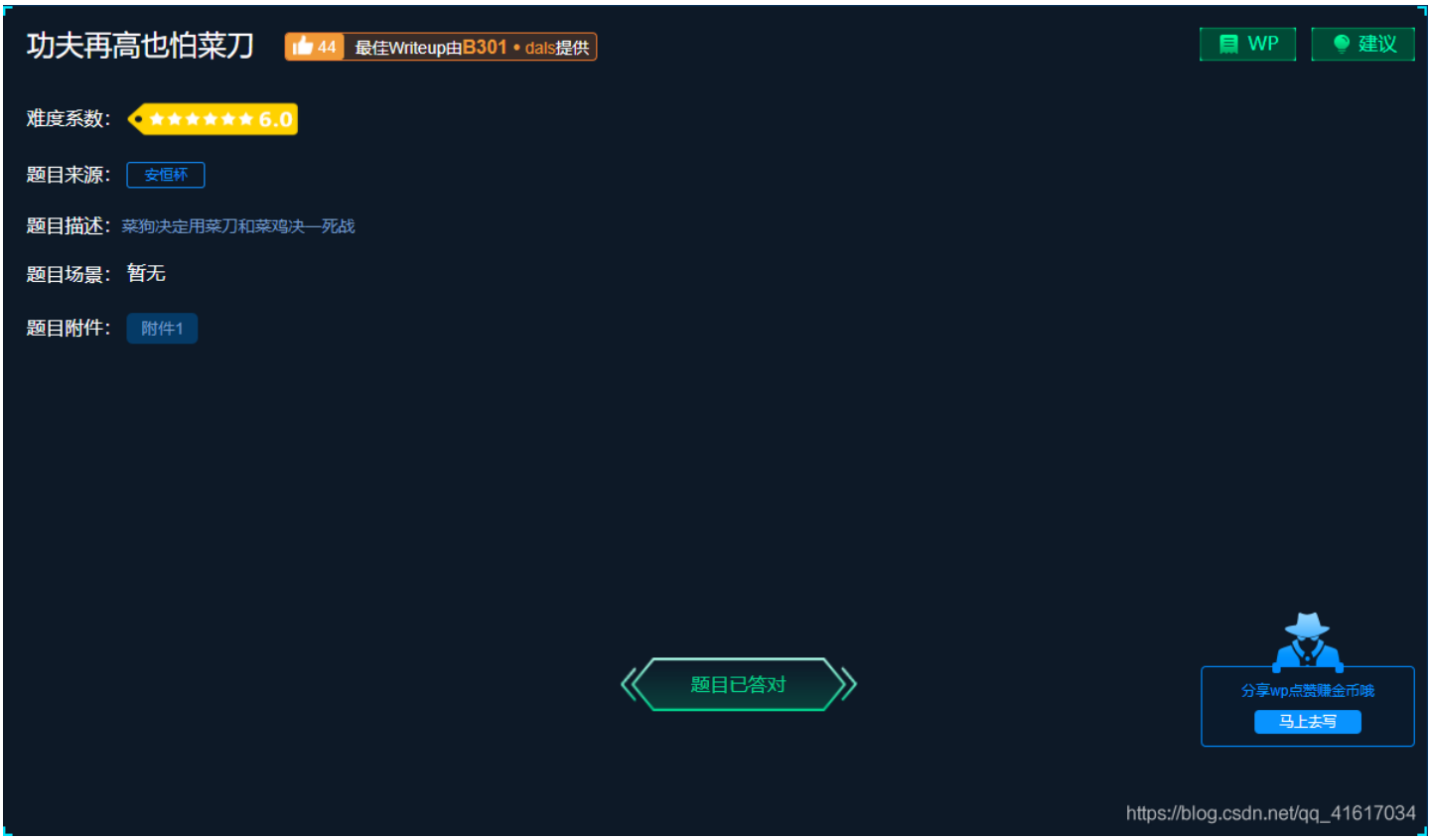
原创

1stPeak 于 2021-06-20 12:58:10 发布 105 收藏

分类专栏： CTF刷题 文章标签： XCTF

本文链接：https://blog.csdn.net/qq_41617034/article/details/118029442

题目



解题步骤

1、使用binwalk提取文件

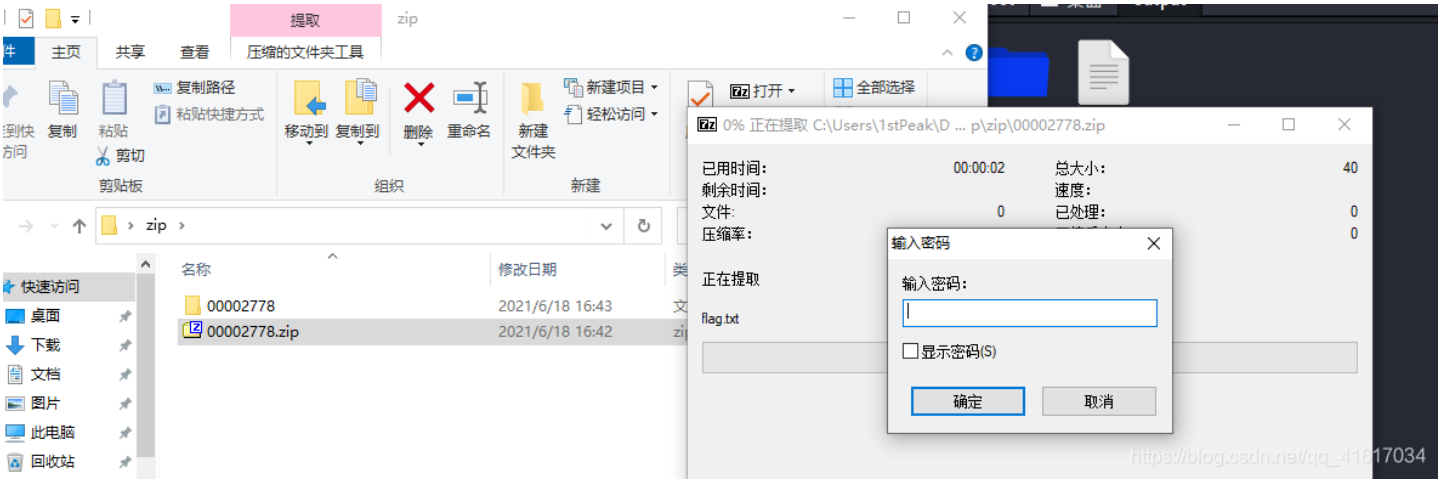
```
┌──(root💀kali)-[~/桌面]
└─# binwalk acfff53ce3fa4e2bbe8654284dfc18e1.pcapng

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
663085        0xA1E2D         xz compressed data
664045        0xA21ED         xz compressed data
812025        0xC63F9         xz compressed data
814001        0xC6BB1         xz compressed data
1238637       0x12E66D        xz compressed data
1240937       0x12EF69        xz compressed data
1391563       0x153BCB        xz compressed data
1393067       0x1541AB        xz compressed data
1406647       0x1576B7        xz compressed data
1412887       0x158F17        xz compressed data
1422689       0x15B561        Zip archive data, encrypted at least v2.0 to extract, compressed si
ze: 52, uncompressed size: 40, name: flag.txt
```


2、使用foremost分离文件

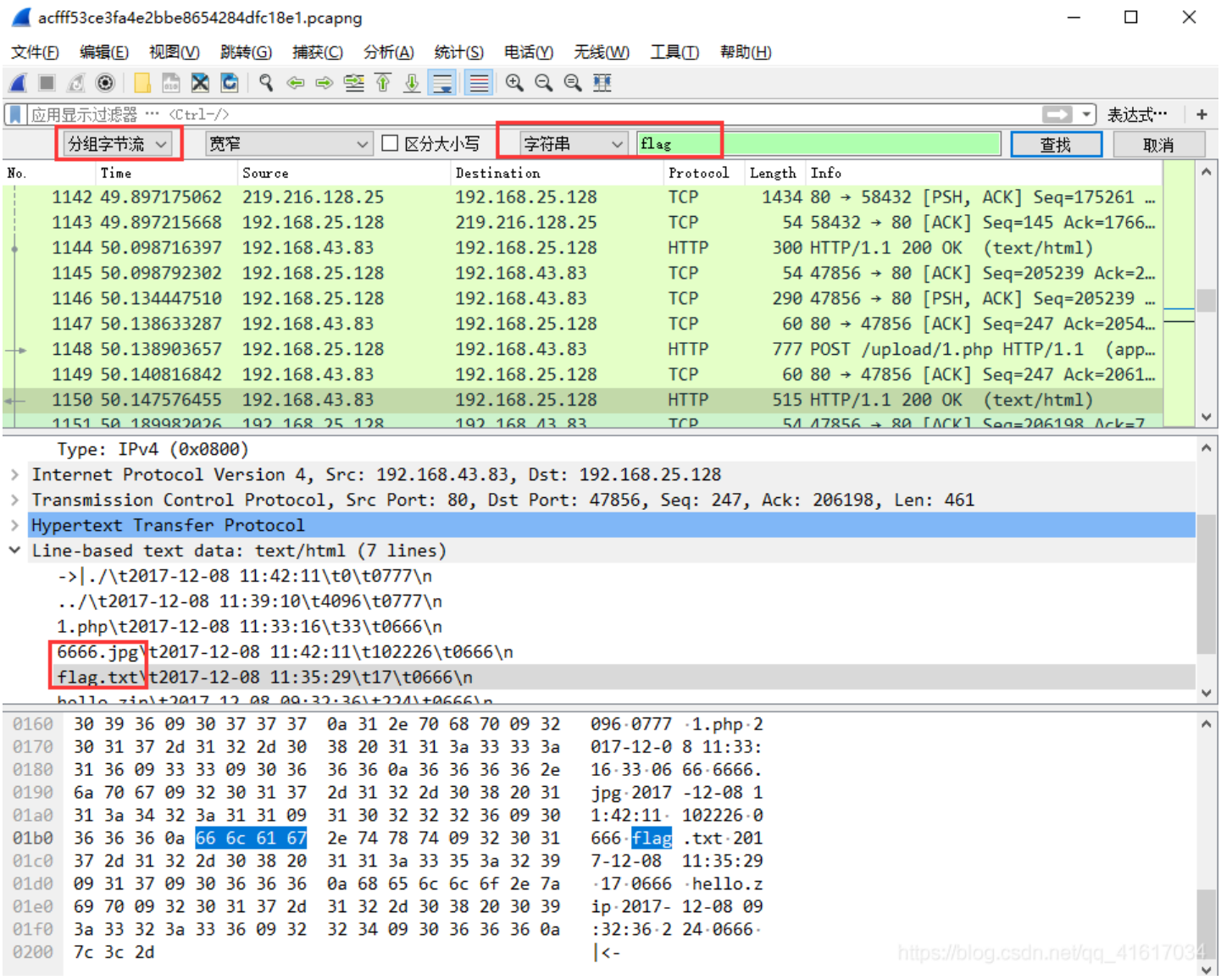
```
┌──(root💀kali)-[~/桌面]
└─# foremost acfff53ce3fa4e2bbe8654284dfc18e1.pcapng
Processing: acfff53ce3fa4e2bbe8654284dfc18e1.pcapng
|foundat=flag.txtC����cS���J��Ea�v�
                                ��&e$K��2%�$��,�=�J��1p��p46PK?
*|

┌──(root💀kali)-[~/桌面]
└─# ls
acfff53ce3fa4e2bbe8654284dfc18e1.pcapng  output
```

```
┌──(root💀kali)-[~/桌面/output]
└─# ls
audit.txt  zip
```

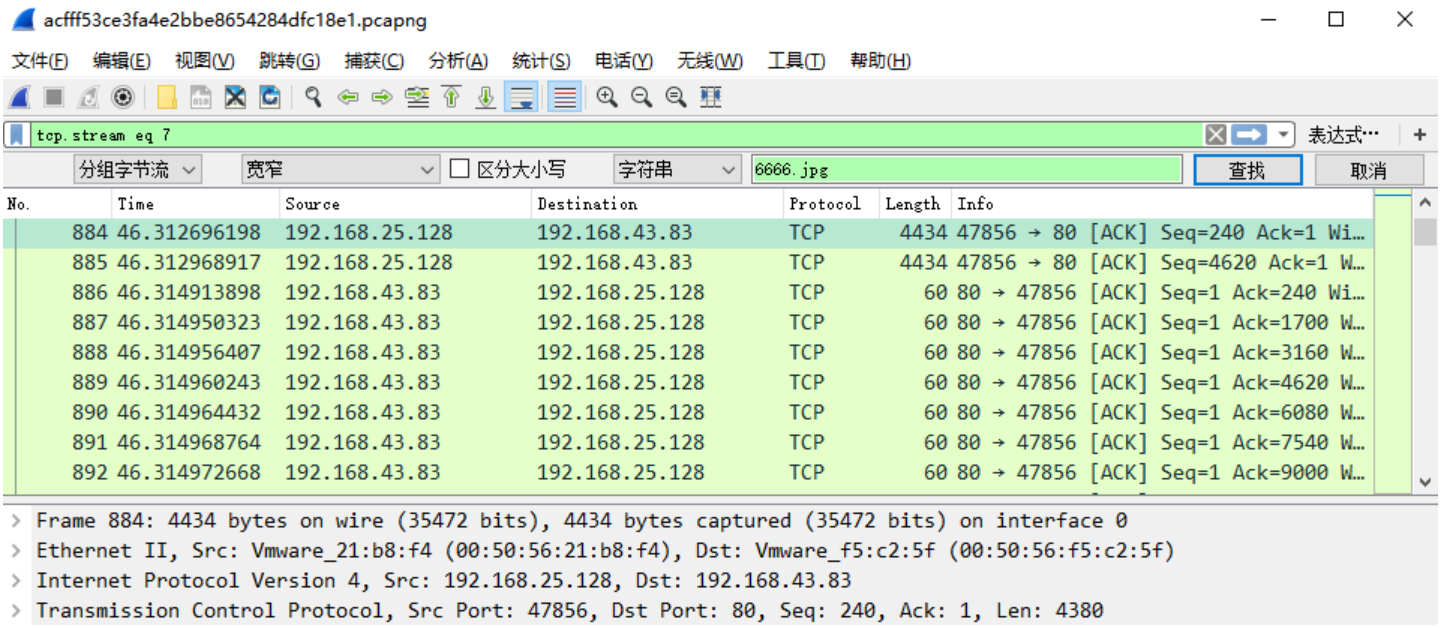
3、该压缩包解压需要密码



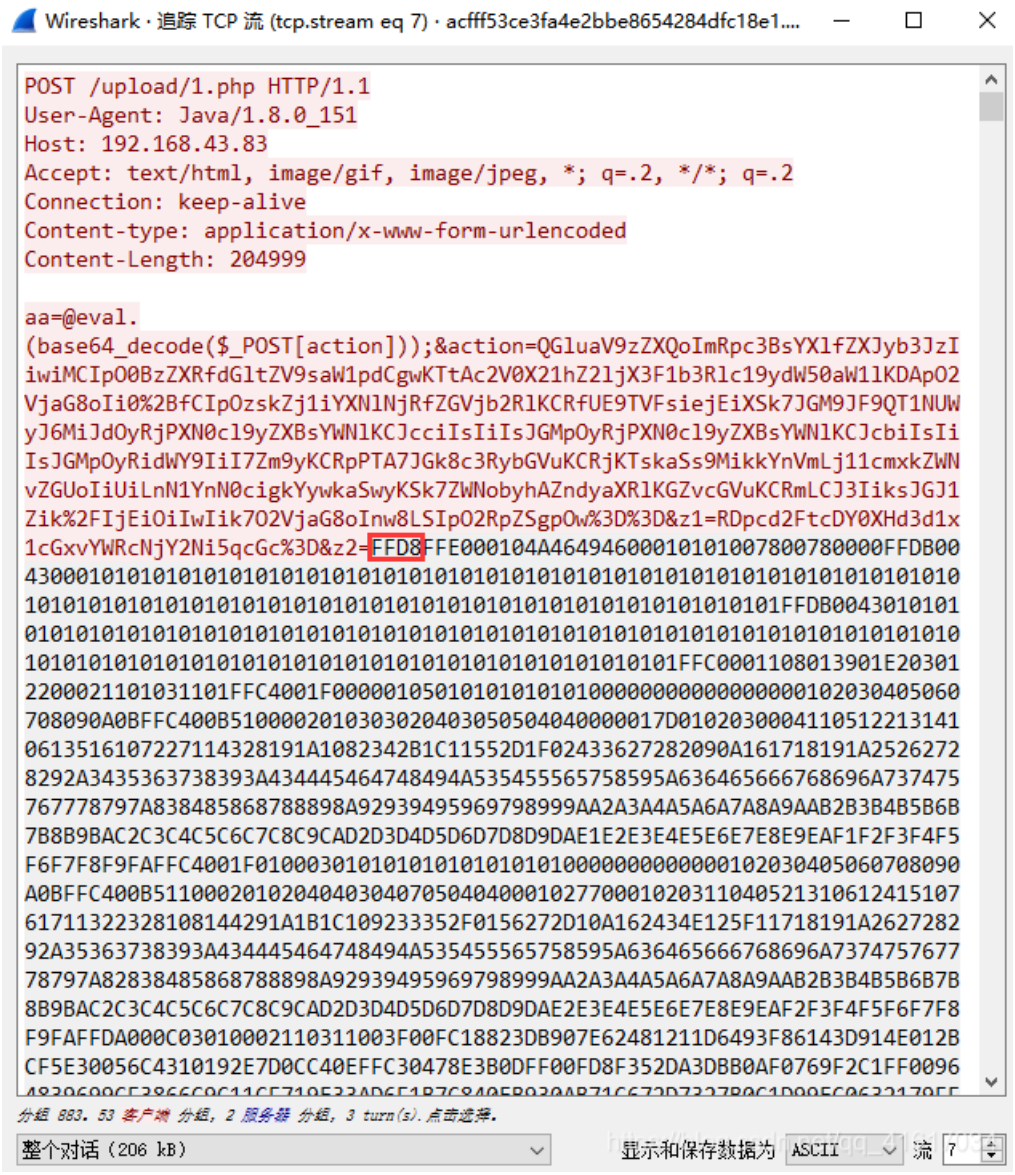
4、使用wireshark分析该数据包，搜索flag，找到6666.jpg


acfff53ce3fa4e2bbe8654284dfc18e1.pcapng
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)
应用显示过滤器 … <Ctrl-/>
表达式…
分组字节流
宽窄
区分大小写
字符串
flag
查找
取消
No. Time Source Destination Protocol Length Info
1142 49.897175062 219.216.128.25 192.168.25.128 TCP 1434 80 → 58432 [PSH, ACK] Seq=175261 …
1143 49.897215668 192.168.25.128 219.216.128.25 TCP 54 58432 → 80 [ACK] Seq=145 Ack=1766…
1144 50.098716397 192.168.43.83 192.168.25.128 HTTP 300 HTTP/1.1 200 OK (text/html)
1145 50.098792302 192.168.25.128 192.168.43.83 TCP 54 47856 → 80 [ACK] Seq=205239 Ack=2…
1146 50.134447510 192.168.25.128 192.168.43.83 TCP 290 47856 → 80 [PSH, ACK] Seq=205239 …
1147 50.138633287 192.168.43.83 192.168.25.128 TCP 60 80 → 47856 [ACK] Seq=247 Ack=2054…
1148 50.138903657 192.168.25.128 192.168.43.83 HTTP 777 POST /upload/1.php HTTP/1.1 (app…
1149 50.140816842 192.168.43.83 192.168.25.128 TCP 60 80 → 47856 [ACK] Seq=247 Ack=2061…
1150 50.147576455 192.168.43.83 192.168.25.128 HTTP 515 HTTP/1.1 200 OK (text/html)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.43.83, Dst: 192.168.25.128
Transmission Control Protocol, Src Port: 80, Dst Port: 47856, Seq: 247, Ack: 206198, Len: 461
Hypertext Transfer Protocol
Line-based text data: text/html (7 lines)
->|./\t2017-12-08 11:42:11\t0\t0777\n
../\t2017-12-08 11:39:10\t4096\t0777\n
1.php\t2017-12-08 11:33:16\t33\t0666\n
6666.jpg\t2017-12-08 11:42:11\t102226\t0666\n
flag.txt\t2017-12-08 11:35:29\t17\t0666\n
0160 30 39 36 09 30 37 37 37 0a 31 2e 70 68 70 09 32 096·0777 ·1.php·2
0170 30 31 37 2d 31 32 2d 30 38 20 31 31 3a 33 33 3a 017-12-0 8 11:33:
0180 31 36 09 33 33 09 30 36 36 36 0a 36 36 36 36 2e 16·33·06 66·6666.
0190 6a 70 67 09 32 30 31 37 2d 31 32 2d 30 38 20 31 jpg·2017 -12-08 1
01a0 31 3a 34 32 3a 31 31 09 31 30 32 32 32 36 09 30 1:42:11· 102226·0
01b0 36 36 36 0a 66 6c 61 67 2e 74 78 74 09 32 30 31 666·flag .txt·201
01c0 37 2d 31 32 2d 30 38 20 31 31 3a 33 35 3a 32 39 7-12-08 11:35:29
01d0 09 31 37 09 30 36 36 36 0a 68 65 6c 6c 6f 2e 7a ·17·0666 ·hello.z
01e0 69 70 09 32 30 31 37 2d 31 32 2d 30 38 20 30 39 ip·2017- 12-08 09
01f0 3a 33 32 3a 33 36 09 32 32 34 09 30 36 36 36 0a :32:36·2 24·0666·
0200 7c 3c 2d |<-

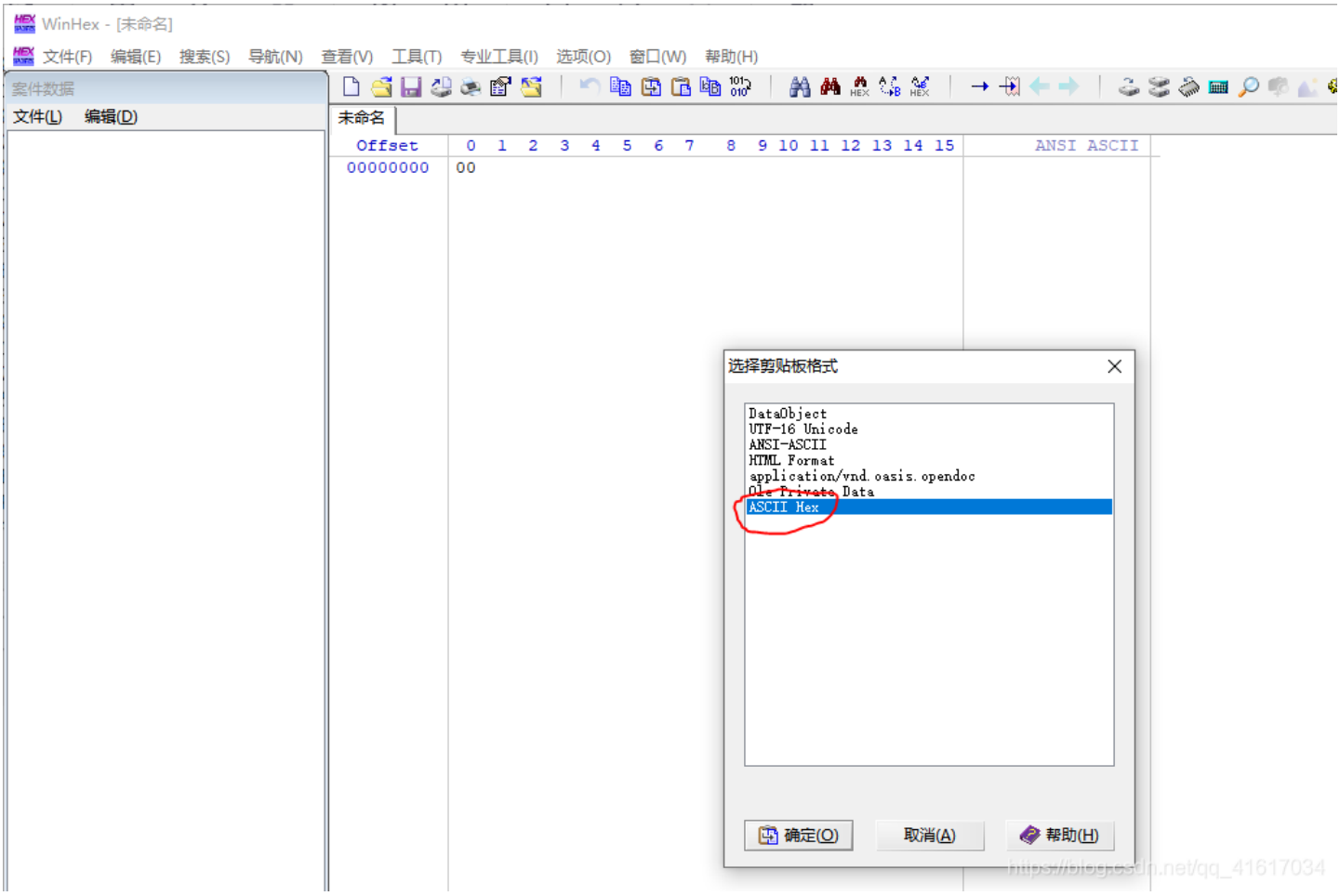
5、查找6666.jpg

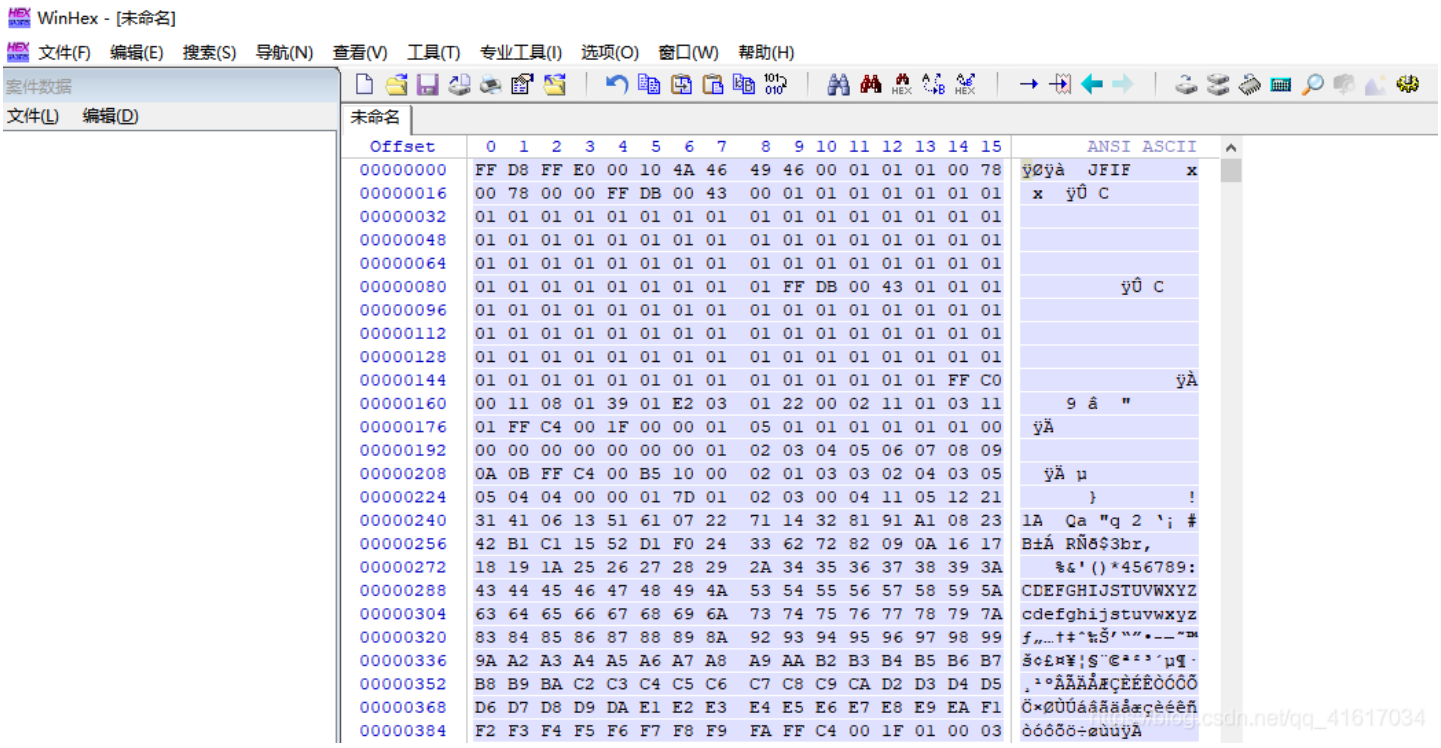


6、追踪TCP流，并将FFD8至FFD9的所有内容复制到010Editor或Winhex中，保存为xx.jpg

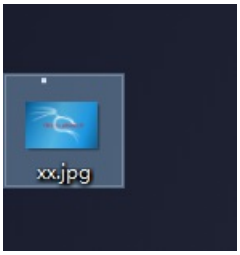


7、复制粘贴选择ASCII Hex

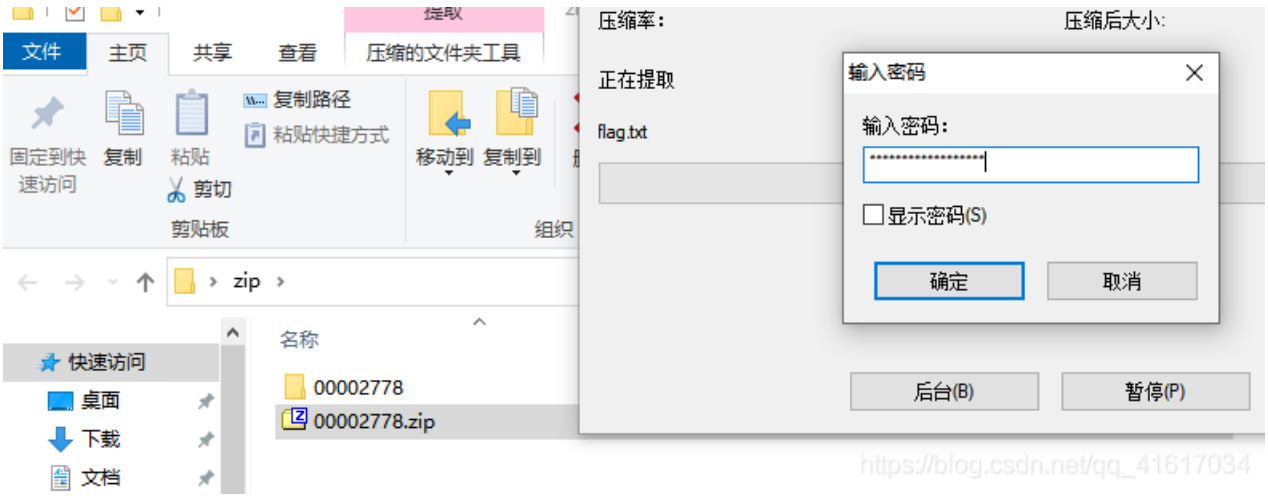

WinHex - [未命名]
文件(F) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H)
案件数据
文件(L) 编辑(D)
未命名
Offset 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ANSI ASCII
00000000 00
选择剪贴板格式
DataObject
UTF-16 Unicode
ANSI-ASCII
HTML Format
application/vnd.oasis.opendoc
Ole Private Data
ASCII Hex
确定(O)
取消(A)
帮助(H)


WinHex - [未命名]
文件(F) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H)
案件数据
文件(L) 编辑(D)
未命名
Offset 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ANSI ASCII
00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 78 ÿØÿà JFIF x
00000016 00 78 00 00 FF DB 00 43 00 01 01 01 01 01 01 01 x ÿÛ C
00000032 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
00000048 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
00000064 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
00000080 01 01 01 01 01 01 01 01 01 FF DB 00 43 01 01 01 ÿÛ C
00000096 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
00000112 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
00000128 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
00000144 01 01 01 01 01 01 01 01 01 01 01 01 01 01 FF C0 ÿÀ
00000160 00 11 08 01 39 01 E2 03 01 22 00 02 11 01 03 11 9 â "
00000176 01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 00 ÿÄ
00000192 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09
00000208 0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 03 05 ÿÄ µ
00000224 05 04 04 00 00 01 7D 01 02 03 00 04 11 05 12 21 } !
00000240 31 41 06 13 51 61 07 22 71 14 32 81 91 A1 08 23 1A Qa "q 2 ¡ #
00000256 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17 B±Á RÑð$3br,
00000272 18 19 1A 25 26 27 28 29 2A 34 35 36 37 38 39 3A %&'()*456789:
00000288 43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A CDEFGHIJSTUVWXYZ
00000304 63 64 65 66 67 68 69 6A 73 74 75 76 77 78 79 7A cdefghijstuvwxyz
00000320 83 84 85 86 87 88 89 8A 92 93 94 95 96 97 98 99 ƒ„…†‡ˆ‰Š'""•–—˜™
00000336 9A A2 A3 A4 A5 A6 A7 A8 A9 AA B2 B3 B4 B5 B6 B7 š¢£¤¥¦§¨©ª²³´µ¶·
00000352 B8 B9 BA C2 C3 C4 C5 C6 C7 C8 C9 CA D2 D3 D4 D5 ¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕ
00000368 D6 D7 D8 D9 DA E1 E2 E3 E4 E5 E6 E7 E8 E9 EA F1 Ö×ØÙÚáâãäåæçèéêñ
00000384 F2 F3 F4 F5 F6 F7 F8 F9 FA FF C4 00 1F 01 00 03 òóôõö÷øùúÿÄ

8、解压密码在图片中



9、使用解压密码解密zip文件



10、解压后的文件中找到flag.txt