Ditf 攻防世界

题目描述

题目是一个图片

解题

`binwalk` 分析文件，发现有一个压缩包。

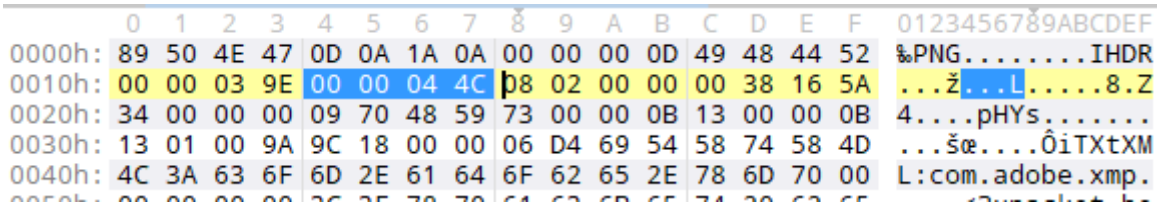
```
root@ubuntu:/home/ams/ws# binwalk e02c9de40be145dba6baa80ef1d270ba.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 926 x 1100, 8-bit/color RGB, non-interlaced
274           0x112           Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rd
f:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="htt
p
1822          0x71E           Zlib compressed data, default compression
989714        0xF1A12         RAR archive data, first volume type: MAIN_HEAD
```

`foremost` 分离文件。

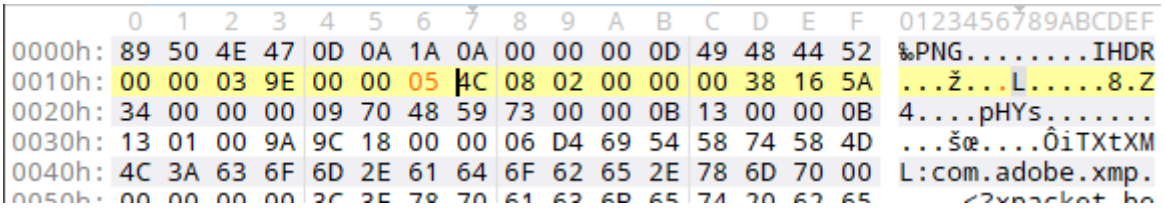
```
root@ubuntu:/home/ams/ws# foremost e02c9de40be145dba6baa80ef1d270ba.png
Processing: e02c9de40be145dba6baa80ef1d270ba.png
|*|
root@ubuntu:/home/ams/ws# cd output/;ls
audit.txt  png  rar
```

解压rar需要输入密码。

尝试修改原的图片分辨率。根据 文件结构 ，第二行第5~8个字节为图片高度。



将其修改为 `00 00 05 4C`

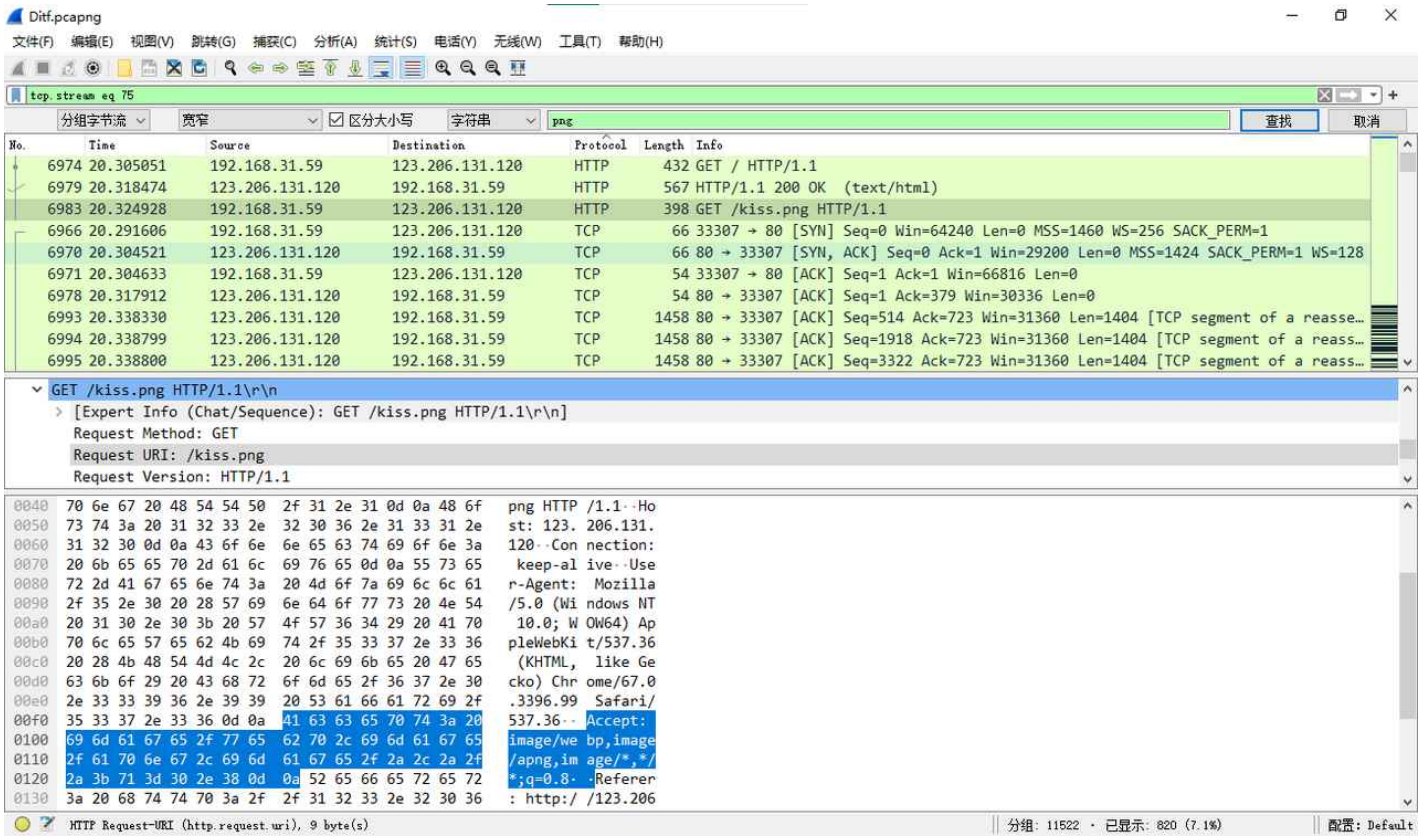


再查看图片，可得解压密码

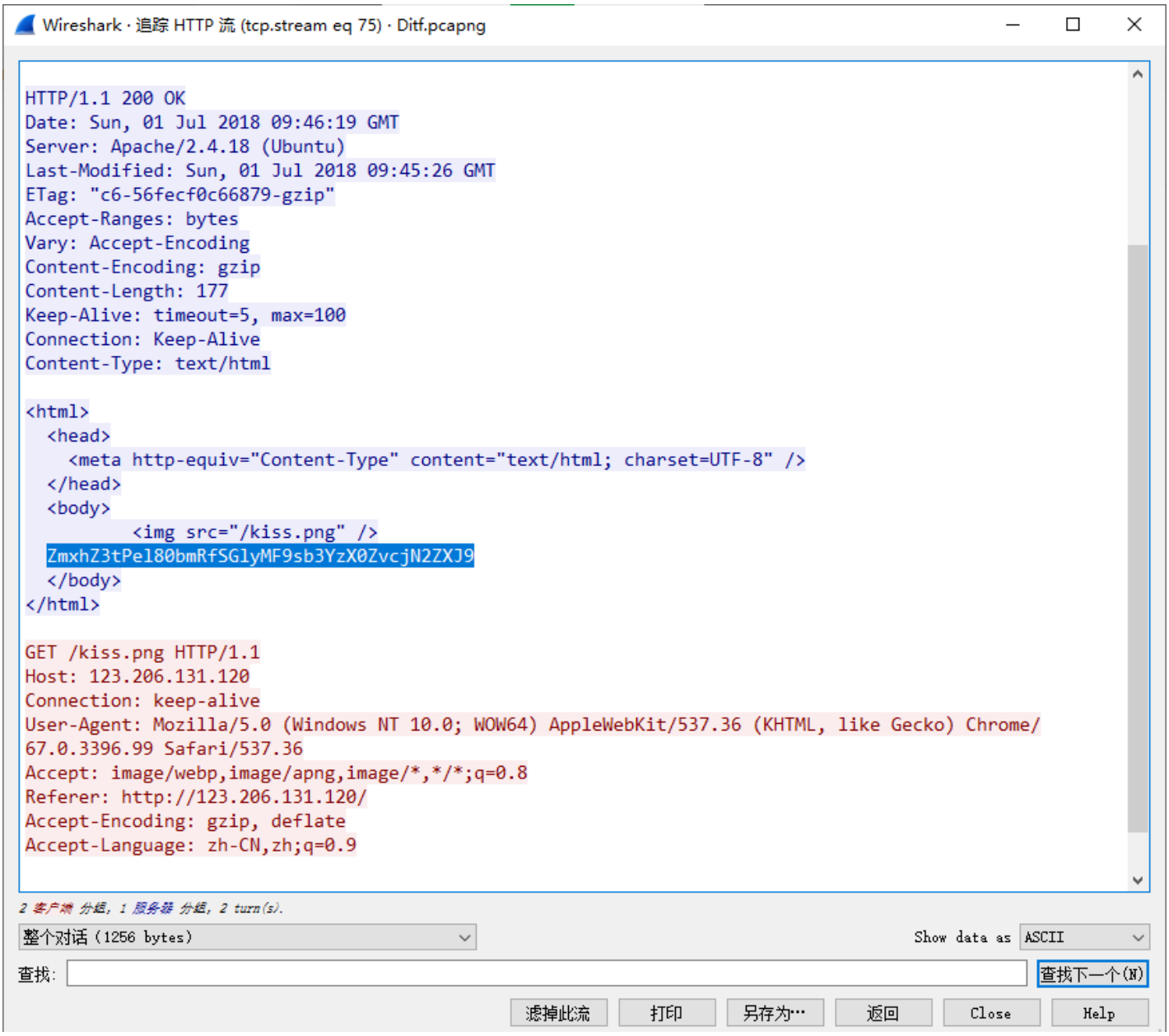
StRe1izia

解压后是一个 `pacpng` 文件，用 `wireshark` 分析。

查找 `png` 关键字，发现一个向服务器发送的HTTP GET请求


Ditf.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)
tcp.stream eq 75
分组字节流 宽窄 区分大小写 字符串 png 查找 取消
No. Time Source Destination Protocol Length Info
6974 20.305051 192.168.31.59 123.206.131.120 HTTP 432 GET / HTTP/1.1
6979 20.318474 123.206.131.120 192.168.31.59 HTTP 567 HTTP/1.1 200 OK (text/html)
6983 20.324928 192.168.31.59 123.206.131.120 HTTP 398 GET /kiss.png HTTP/1.1
6966 20.291606 192.168.31.59 123.206.131.120 TCP 66 33307 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6970 20.304521 123.206.131.120 192.168.31.59 TCP 66 80 → 33307 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1424 SACK_PERM=1 WS=128
6971 20.304633 192.168.31.59 123.206.131.120 TCP 54 33307 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
6978 20.317912 123.206.131.120 192.168.31.59 TCP 54 80 → 33307 [ACK] Seq=1 Ack=379 Win=30336 Len=0
6993 20.338330 123.206.131.120 192.168.31.59 TCP 1458 80 → 33307 [ACK] Seq=514 Ack=723 Win=31360 Len=1404 [TCP segment of a reasse…
6994 20.338799 123.206.131.120 192.168.31.59 TCP 1458 80 → 33307 [ACK] Seq=1918 Ack=723 Win=31360 Len=1404 [TCP segment of a reass…
6995 20.338800 123.206.131.120 192.168.31.59 TCP 1458 80 → 33307 [ACK] Seq=3322 Ack=723 Win=31360 Len=1404 [TCP segment of a reass…
GET /kiss.png HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /kiss.png HTTP/1.1\r\n]
Request Method: GET
Request URI: /kiss.png
Request Version: HTTP/1.1
0040 70 6e 67 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f png HTTP /1.1··Ho
0050 73 74 3a 20 31 32 33 2e 32 30 36 2e 31 33 31 2e st: 123. 206.131.
0060 31 32 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 120··Con nection:
0070 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 73 65 keep-al ive··Use
0080 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
0090 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 /5.0 (Wi ndows NT
00a0 20 31 30 2e 30 3b 20 57 4f 57 36 34 29 20 41 70 10.0; W OW64) Ap
00b0 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 pleWebKi t/537.36
00c0 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 (KHTML, like Ge
00d0 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 36 37 2e 30 cko) Chr ome/67.0
00e0 2e 33 33 39 36 2e 39 39 20 53 61 66 61 72 69 2f .3396.99 Safari/
00f0 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 3a 20 537.36·· Accept:
0100 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d 61 67 65 image/we bp,image
0110 2f 61 70 6e 67 2c 69 6d 61 67 65 2f 2a 2c 2a 2f /apng,im age/*,*/
0120 2a 3b 71 3d 30 2e 38 0d 0a 52 65 66 65 72 65 72 *;q=0.8· ·Referer
0130 3a 20 68 74 74 70 3a 2f 2f 31 32 33 2e 32 30 36 : http:/ /123.206
HTTP Request-URI (http.request.uri), 9 byte(s)
分组: 11522 · 已显示: 820 (7.1%)
配置: Default

追踪该HTTP流



发现一个惹人注目的字符串

`ZmxhZ3tPel80bmRfSGlyMF9sb3YzX0ZvcjN2ZXJ9`

base64解码可得flag。