

## Week1的四道杂项题目

### 1、Base全家福

首先看到一串奇奇怪怪的字符，肯定是被加密过。用base64解码，解码后依旧是奇奇怪怪的字符，但有趣的是其中大写字母消失了，推测这个加密方式是base32，解码后发现居然还有一层base16。嗯flag找到了。

### 2、不起眼压缩包的养成的方法

打开网页后发现是一张图片，下载下来。先查看属性，没有什么特别的。用kali的binwalk命令发现这张图果然暗藏玄机。

```
kali@kali:~$ binwalk /home/kali/Desktop/1.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
30	0x1E	TIFF image data, big-endian, offset of first image directory: 8
4634	0x121A	Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"
629835	0x99C4B	Zip archive data, encrypted at least v2.0 to extract, compressed size: 129, uncompressed size: 117, name: NO PASSWORD.txt
630009	0x99CF9	Zip archive data, encrypted at least v2.0 to extract, compressed size: 835, uncompressed size: 823, name: plain.zip

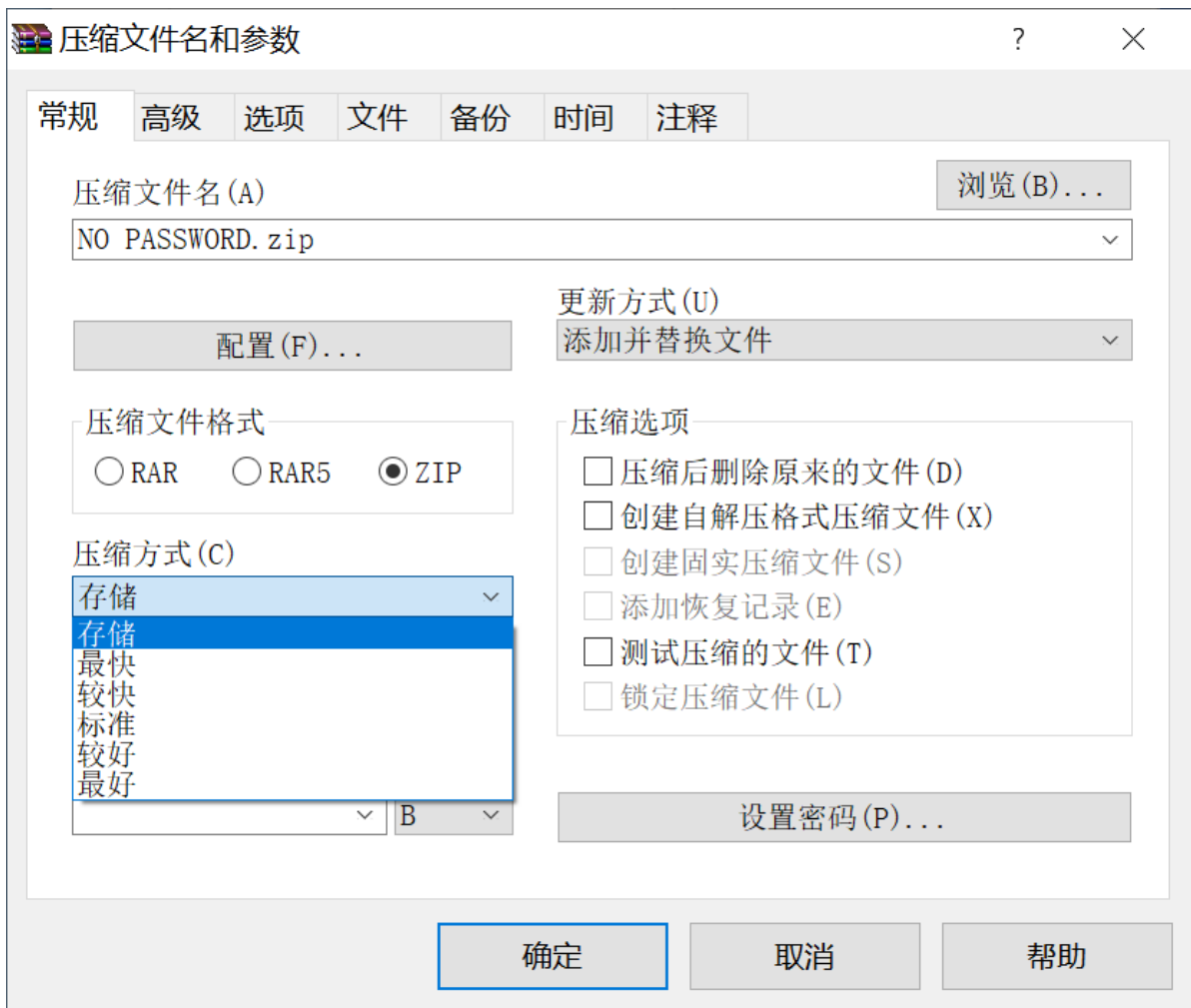
用binwalk分离后得到一个压缩包，压缩包里是两个有密码的文件。



用ziperello数字爆破后得到no password文档的密码。打开no password文档发现没有什么信息。而打开plain压缩文档，又发现两个新的文件。



可见，压缩包里就是我们想要找的flag。而这两个文档依旧是需要密码的，因为其中的no password文档是已知的，可用明文解密。值得注意的一点是，压缩文档的时候要注意选择压缩方式（如图），否则明文解密压根就无法进行。



解密后就可以分离出我们想要的flag.txt文档。但这个文档依旧是需要密码的，用notepad++可以发现，这是伪加密，修改50 4b后第7个字符的十六进制为00后即可打开文档得到flag值

### 3、Galaxy

用wireshark打开下载好的pcapng文档，对其进行协议分级统计。

Wireshark · 协议分级统计 · 2

协议	按分组百分比	分组	按字节百分比	字节	比特/秒	End Pa
Frame	100.0	2864	100.0	7960873	3486 k	0
Ethernet	100.0	2864	0.5	40096	17 k	0
Internet Protocol Version 4	99.8	2858	0.7	57160	25 k	0
User Datagram Protocol	1.9	53	0.0	424	185	0
Simple Service Discovery Protocol	0.3	8	0.0	1380	604	8
Session Traversal Utilities for NAT	0.1	4	0.0	80	35	4
Domain Name System	1.4	41	0.0	3251	1423	41
Transmission Control Protocol	97.9	2805	98.7	7856472	3440 k	2054
Secure Sockets Layer	29.0	831	40.3	3205465	1403 k	728
Malformed Packet	0.6	17	0.0	0	0	17
Hypertext Transfer Protocol	0.2	6	59.7	4752340	2081 k	3
Portable Network Graphics	0.0	1	59.7	4748771	2079 k	1
Line-based text data	0.1	2	0.0	345	151	2
Address Resolution Protocol	0.2	6	0.0	168	73	6

无显示过滤器。

Close 复制 Help

发现占比最多的是其中的png，重要信息大概率在这个png文件里面，导出

Wireshark · 导出 · HTTP 对象列表

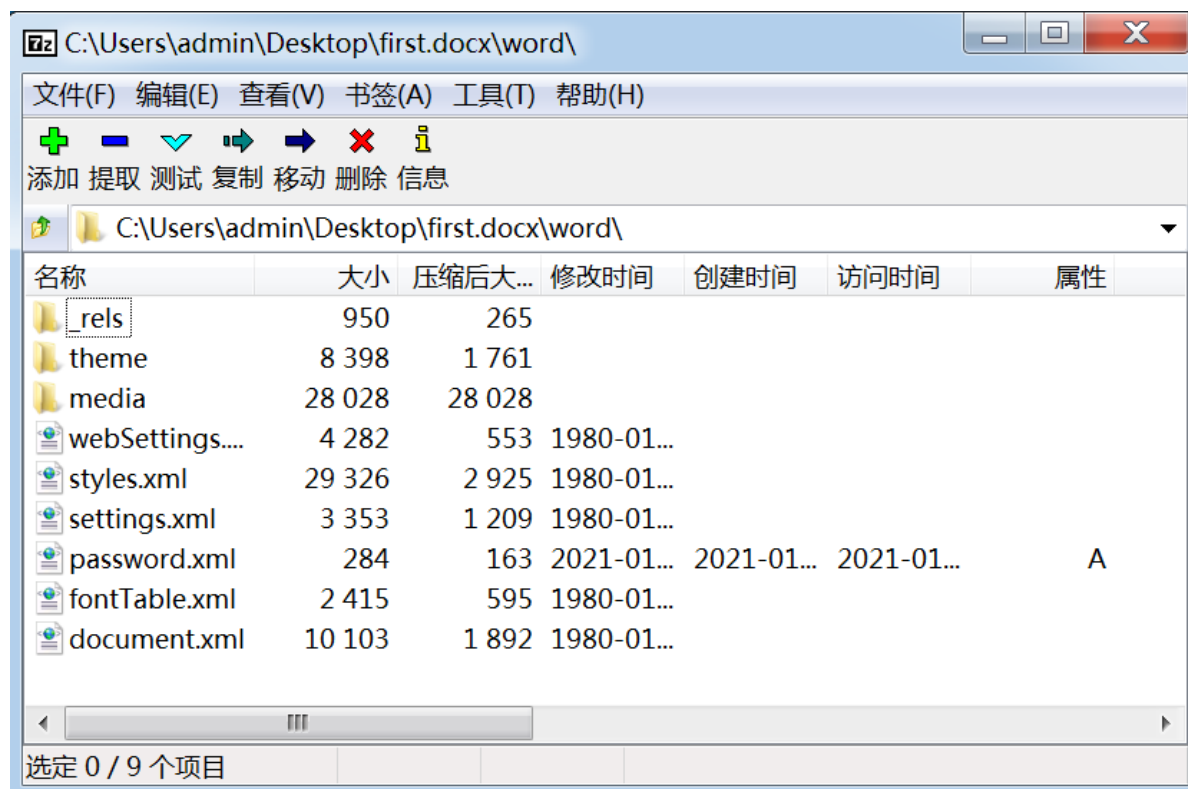
分组	主机名	内容类型	大小	文件名
1149	192.168.43.146	image/png	4748 kB	galaxy.png
1630	image.baidu.com	text/html	167 bytes	i?tn=baiduimage&ps=1&ct=201326
1638	image.baidu.com	text/html	178 bytes	index?tn=baiduimage&ps=1&ct=20

Save Save All Close Help

得到一张星空的图片。把他放到kali里面，用binwalk发现里面没有包含的文件。但发现kali打不开这张图片，大概率是这张图片的长或者宽不太对，隐藏了一部分东西。在windows里面用notepad++打开，编辑图片使他的宽变长一点，在图片下半部分得到flag。

#### 4、Word RE:MASTER

解压后发现两个word文档，查看属性发现，maimai文档的密码在first文档中，打开first文档，找不到有用的信息。于是把first文档用压缩包的方式打开，发现其中有含有password字样的文档



用记事本打开后，发现里面的字符被加密了，符号都是由< + - . , [ ]来组成，是Brainfuck加密算法，解密之后得到maimai.txt的密码。打开maimai文档后，发现文档中有隐藏的符号。

### 始终在屏幕上显示这些格式标记

- ☒ 制表符(T) →
- ☒ 空格(S) ...
- ☒ 段落标记(M) ↵
- ☒ 隐藏文字(D) 🔒
- ☒ 可选连字符(Y) ~
- ☒ 对象位置(C) 📍
- ☒ 可选分隔符(O) 📏

把这些都选中以后，得到这样的一串字符

