

Week2

1. misc 所见即为假


下载压缩包根据对子 用 winhex 查看压缩包 发现为伪加密

```
55 CB 5D 8F AE 27 DB 5C 6D CB 02 76 06 FF 07 50
4B 01 02 1F 00 14 00 09 00 08 00 89 7B 34 50 1E
DF 09 47 FE 3E 10 00 80 4B 10 00 13 00 24 00 00
00 00 00 00 00 20 00 00 00 00 00 00 46 4C 41
47 5F 49 4E 5F 50 49 43 54 55 52 45 2E 6A 70 67
0A 00 20 00 00 00 00 00 01 00 18 00 D1 F9 81 2F
63 CF D5 01 7D 05 F7 12 64 CF D5 01 84 DE F6 12
64 CF D5 01 50 4B 05 06 00 00 00 00 01 00 01 00
65 00 00 00 2F 3F 10 00 18 00 46 35 20 6B 65 79
3A 20 4E 6C 6C 44 37 43 51 6F 6E 36 64 42 73 46
4C 72
```

修改后:

```
2E BD 6C 14 E1 70 E8 93 A8 47 47 8E F9 F9 C9 CA
55 CB 5D 8F AE 27 DB 5C 6D CB 02 76 06 FF 07 50
4B 01 02 1F 00 14 00 00 00 08 00 89 7B 34 50 1E
DF 09 47 FE 3E 10 00 80 4B 10 00 13 00 24 00 00
00 00 00 00 00 20 00 00 00 00 00 00 46 4C 41
47 5F 49 4E 5F 50 49 43 54 55 52 45 2E 6A 70 67
0A 00 20 00 00 00 00 00 01 00 18 00 D1 F9 81 2F
63 CF D5 01 7D 05 F7 12 64 CF D5 01 84 DE F6 12
64 CF D5 01 50 4B 05 06 00 00 00 00 01 00 01 00
65 00 00 00 2F 3F 10 00 18 00 46 35 20 6B 65 79
3A 20 4E 6C 6C 44 37 43 51 6F 6E 36 64 42 73 46
4C 72
```

后解压得 jpg 文件, 使用 steg binwalk 分析后无结果发现, 后从压缩包备注 得到提

示为 F5 隐写, 使用  F5-steganography 解密得到结果文件

得到一段

526172211A0701003392B5E50A01050600050101808000B9527AEA2402030BA70004A7
0020CB5BDC2D80000008666C61672E7478740A03029A9D6C65DFCED5016867616D65
7B343038375E7A236D737733344552746E46557971704B556B32646D4C505736307D1D
77565103050400 的代码

感觉像 16 进制转化文本

得到

```
526172211A0701003392B5E50A01050600050101808000B9527AEA2402030BA70004A70020CB5BDC2D800000086
66C61672E7478740A03029A9D6C65DFCED5016867616D657B343038375E7A236D737733344552746E465579717
04B556B32646D4C505736307D1D77565103050400
```



????????:

```
Rar!000030pâ
0000000000'Rz6$000$00$0 Ê[Ü-0000flag.txt
0000leßîÔ0hgane{4087*z#msw34ERtnFUyqpKUK2dmLPW60}0wVQ0000
```

2.