

beautiful_sky(Bugku)

原创

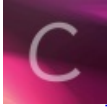
[一树梨花压小棠](#) 于 2022-04-22 17:28:55 发布 1345 收藏

分类专栏: [CTF misc](#) 文章标签: [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/AKAXPD/article/details/124350918>

版权



[CTF 同时被 2 个专栏收录](#)

6 篇文章 0 订阅

订阅专栏



[misc](#)

1 篇文章 0 订阅

订阅专栏

我的writeup被bugku管理员吞了, 去年11月份做出来的题快半年了wp都没过审核...

下载后解压提示压缩包加密

观察题目

描 述: 难道真的会有人不喜欢beautiful_sky么????? 我可太爱了

猜测密码为beautiful_sky

解压后得到一张图片

先观察图片, 除了打了doc encoded_by_we1的水印外没什么

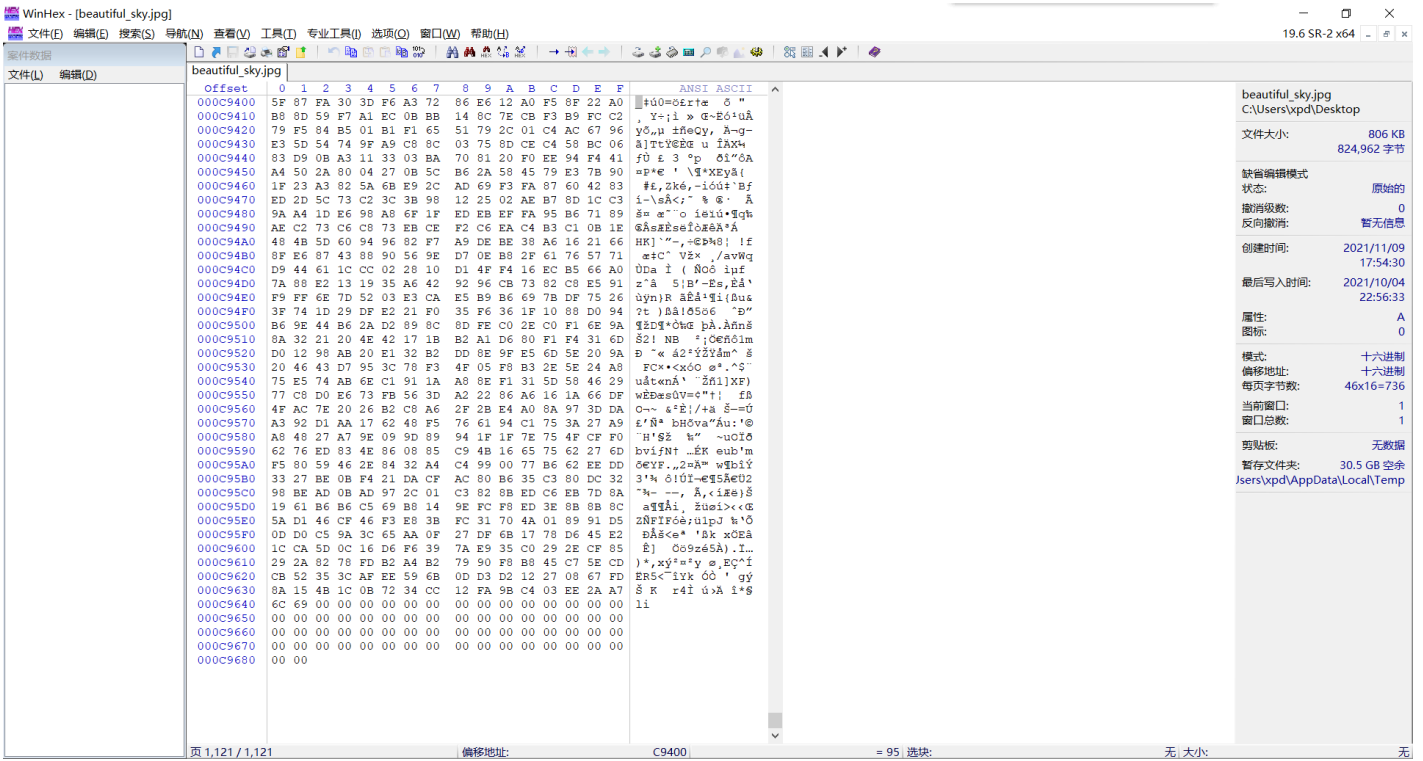
属性里提示了一句拉满了拉满了00000beautiful

暂时不明白是什么

把图片拖到winhex里看

发现一件事: jpg(JPEG)的文件尾的hex应该是FF D9

这里显然不是



首先想到了填充文件尾

但这个想法是不正确的

因为如果文件尾不全的话，一般会显示图片已损坏

这里猜测是做了两个文件的拼接

继续往上找

000C6680 FF D9 D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00 yÙÈÏ à;± á

这里不仅发现了jpg图片的尾

更发现了D0 CF 11 E0

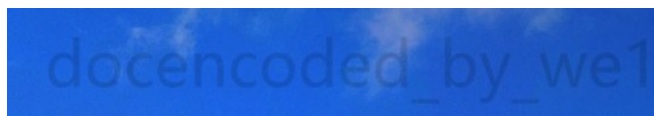
如果对文件头和尾的hex足够了解的朋友会知道这个是doc或xls的文件头

把D0 CF 11 E0之后的hex拿出来写到一个新的文件里并加上后缀.doc（之所以不修改为.xls的原因是改了之后会提示错误，大家改一下就知道了）

发现该.doc文件为加密文件

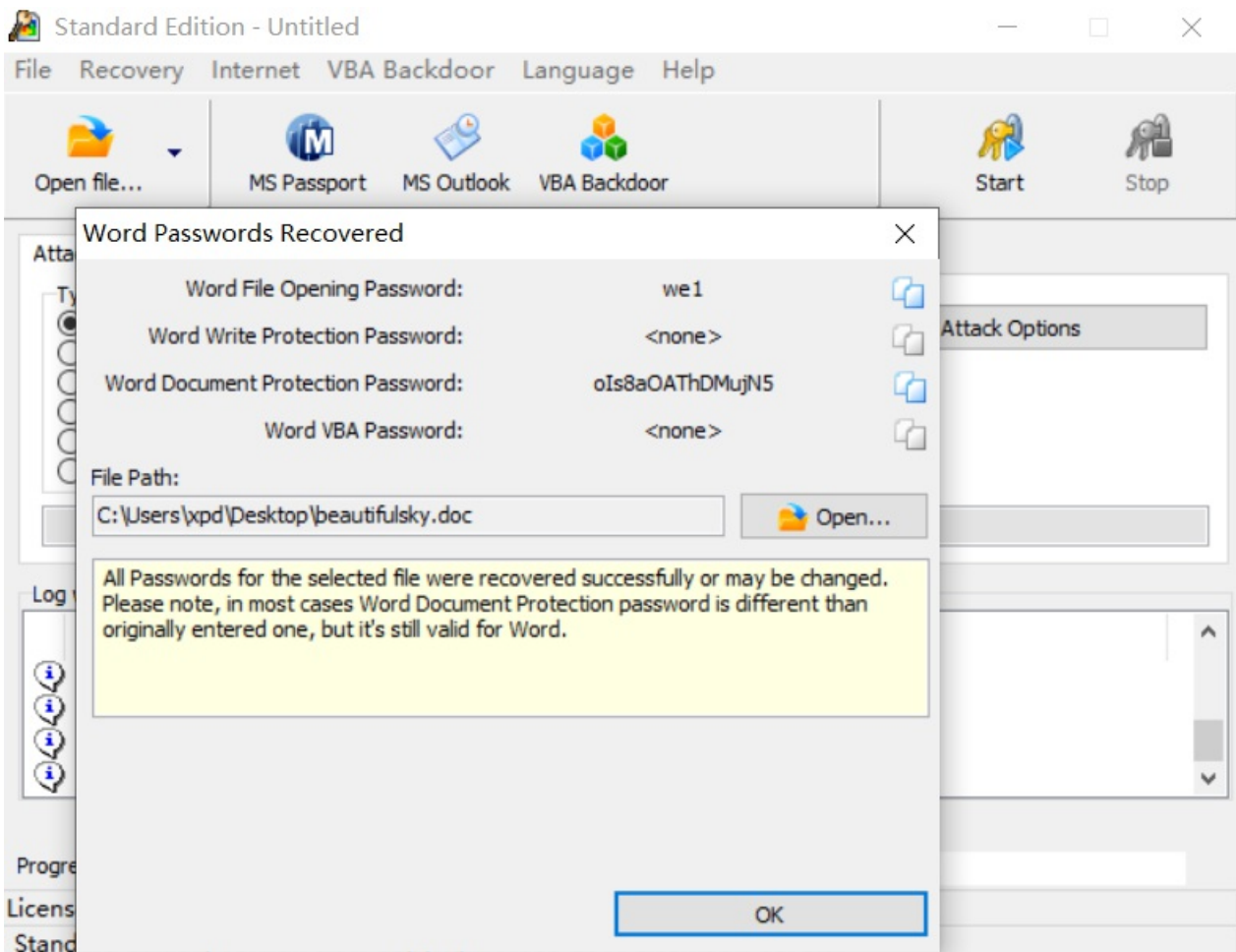
这里两种解决办法：

1.（推荐）仔细观察图片，上文我提到的水印这里就派上了用场



猜测密码为：we1

2.office password recovery直接爆破1秒搞定

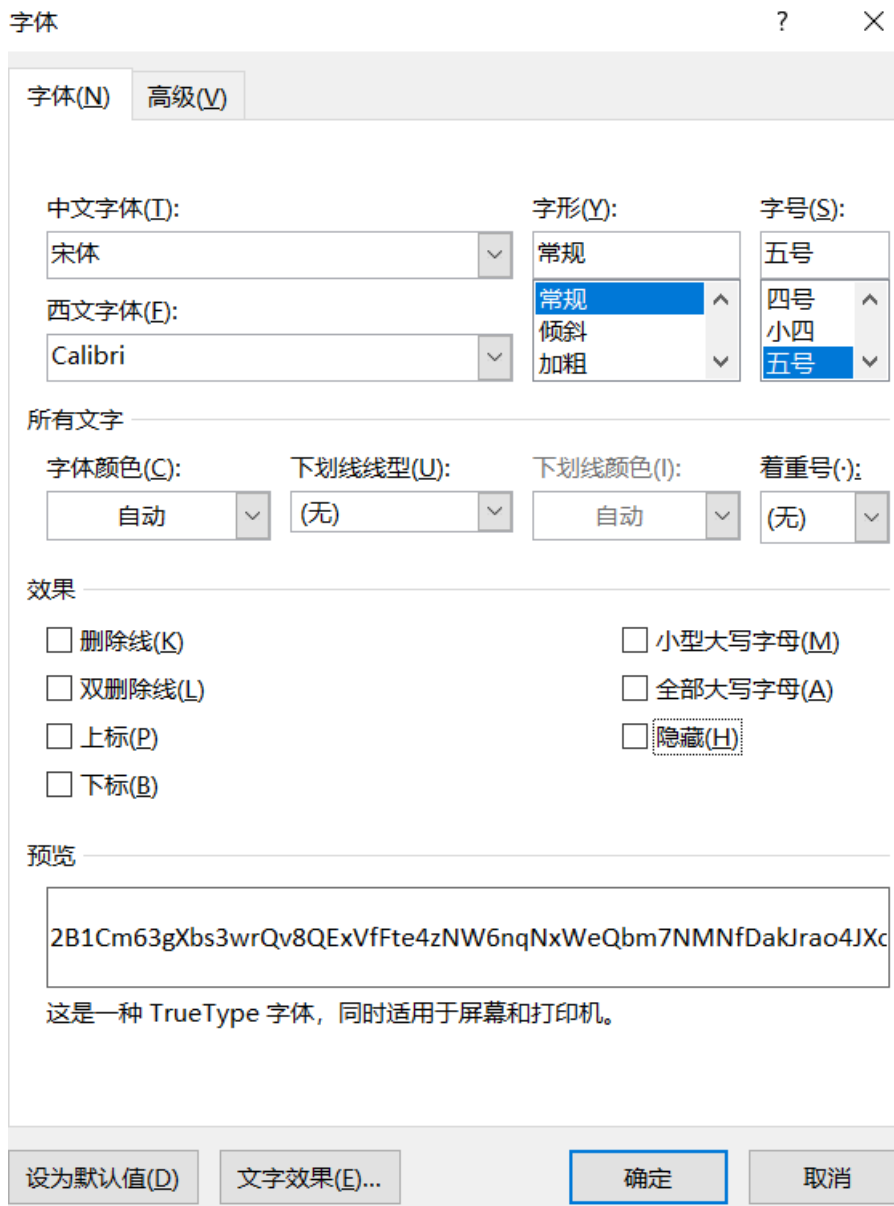


进入.doc文件后什么都看不到，但是很明显是有字的，将其改为黑色



2B1Cm63gXbs3wrQv8QExVffTe4zNW6nqNxWeQbm7NMNfDakJrao4JXoGQyp1JXuwVu9vgWjcwA
mGQRDUdXC8BQPfQoSrQz3wgD67nHx3QYttZMxXfgYXsRf9YkK9LT2NaMWFbEkVaYtM2B4JxPAeYj
wKLpimEHZLhfVzsw1tFVyoZfMTe7YYenK9eQS2iM6rJMwSgyChEBy9ZrjBr1t6hVvZvazph3i3Rbg2e8
Vvjar3J8GVudASDC9WSbMhu8wGwRa2MKnPEFkMj4VquNWj7NxBqjiFHAPRGNg4Xktogp1WCoDy
Q1nYSn3qEYdfPPAe5etmm8ugeFgWqXsGmJxZ7ijiaF8qrZhVxgEKsJY6PKq36KsUA5uRkwE6kr1oA5T
zUG9k69coGxvurDp99hcDuRYMscu3aFscfm7nbZ3APWcLaDxwVTGMFjxTaV3VYozK2VuRPgHWsJZ
7mFs18oRyD6thRWWFK2CETgE6CVUyqXgPowkun2tYELY48UhYs9zdbdWpVLBs28vTHSRRSD5rscD
UFUE665R2zCVk9B5PbfaC

这就完了吗？不不不



```
2B1Cm63gXbs3wrQv8QExVfFte4zNW6nqNxWeQbm7NMNfDakJrao4JXoGQyp1JXuwVu9vgWjcwA
mGQRDUdXC8BQPfQoSrqz3wgD67nHx3QYttZMxXfgYXsRf9YkK9LT2NaMWFbEkVaYtM2B4JxPAeYj
wKLpimEHZLhfVzsw1tFVyoZfMte7YYenK9eQS2iM6rJMwSgyCheBY9ZrjBr1t6hVvZvazph3i3Rbg2e8
Vvjar3J8GVudASDC9WSbMhu8wGwRa2MKnPEFkMj4VquNWj7NxBqjiFHAPRGNg4Xktogp1WCoDy
Q1nYSn3qEYdfPPAe5etmm8ugeFgWqXSgMJxZ7ijiaF8qrZhVxgEKsJY6PKq36KsUA5uRkwE6kr1oA5T
zUG9k69coGxvurDp99hcDuRYMscu3aFscfm7nbZ3APWcLaDxwVTGMFjxTaV3VYozK2VuRPgHWsJZ
7mFs18oRyD6thRWWFK2CETgE6CVUyqXgPowkun2tYELY48UhYs9zdbdWpvLbs28vTHSRRSD5rscD
UFUE665R2zCVk9B5PbfaCWnWLry8FKGy9NpSGozwh8chuzmZztPJYyCGAxt1vbsuYJ8BqUzGXyBTJ
Nirueieq2qRsYzBR3fcyye59ezZZxcaGZxrBREyt1gKLSdHTv1xhkyWFpLEz4Ycvbkum3hKcMU96ubVf
N6w8dgVhTmPo1MBzmBAgLe4U8gXg9QZht2x6JrbJ8XrBVdZN8M1yN66vHaJv6qbg16gM5Bscx7ss
o9RbuifX4Jg9qFrgqyP58p7YLQrgwpD5EGGjS24SoUb3gBZFYRiCctT7giybEjtTKDDw2iUAuXJVASXZzp
L1eypbyVLZeEvP51iHfdVXqvDigG5CCxot1Yp2em6TYCTjL5aayj4MeaZHAz2LeNJADgEUo8k2ADe9vZ
Fwqz7dVTH9Mg5NpR9xRwbQEq1FnJJqo48DwhpYfJrB8Bu5t2pSL4D7rzNiA5gA9gKvvcx7R1rd7GCh
YKnbmqz6BjRxQv3NiVkv2Rj7GbuzhQmcCcR9JunpSi1bvJMs1fPGs1c5xvVzM2L3KQz4bKb2y6jfoqpF
R4cNAjNkfJSE6XFaU7yUbCH8nSm7EgApEr2parf4Fxinagsh5CdzRkRMuLad183P3a5DiMhohznAQj
X9fWbJWtW1zCV2Nezq98EUyEqprg4y11jAvvDAMfiHsmX3RiwRJRYUWHE54wYBxZQNAbvB8ALK
Xxqef1wwZ9fDS6jjqcWb9L1tx<
```

编码的后半部分被隐藏了，这才是完全的编码

首先base64跑一下发现不对，这里停住了没思路了

插个题外话：为什么你不去试试base32和base16

因为base32的数字范围是2~7而base16的字母范围是没有小写的

大家抽时间可以去了解一下base家族的组成，可以帮你在做misc的时候省下一些时间

当然如果你写base全家桶的脚本去跑就当我说

言归正传，仔细看，这段编码里是没有0的

锁定base58

在线解密

转换前:

um3hKcMu96ubVfN6w8dgVhTmPo1MBzmBAgLe4U8gXg9QZht2x6JrbJ8XrBVdZN8M1yN66vHaJv6qbg16gM5Bscx7sso9RbuifX4Jg9qFrgqyP58p7YLQrgwpD5EGGjSZ4SoUb3gBZFYRiCctT7giybEjtTKDDw2iUAuXJVASXZpL1eyppyVLZeEvP51iHfdVXqvDigG5CCxot1Yp2em6TYCTJL5aayj4MeaZHAZ2LeNJADgEUo8k2Ade9vZfwqz7dVTH9Mg5NpR9xRwbQEeq1FnJjqo48DwhpYfJrB8Bu5t2pSL4D7rzNIA5gA9gKvvcx7R1rd7GChYKnbmqz6BjRxQv3NiVkv2Rj7GbuzhQmcCcR9JunpSi1bvJMs1fPGs1c5xvVzML2L3KQz4bKb2y6jfoqpFR4cNAjNkfJSE6XFaU7yUbCH8nSm7EgApEr2parf4Fxinagsh5CdzRkRMuLad183P3a5DiMhohznAQyjX9fWbJWtW1zCV2Nezq98EUyEqprg4y11jAvvDAMfihHsmX3RiwRJRYUWHE54wYBxZQNAbvB8ALKXxqef1wwZ9fDS6jjqcWb9L1tx

编码Base58>

解码Base58>

转换后:

NTA0QjAzMDQxNDAwMDkwMDYzMDAxQUIxNDQ1M0M1NTYxRTBDOUYwMDAwMDAxNzAyMDAwMDA4MDAwQjAwNjY2QzYxNjcyRtC0Nzg3NDAXOTkwNzAwMDEwMDQxNDUwMzA4MDAyMQQxMDEyNjM1M0NGRTdDNjFEQ0VCMTBCQjkwQjI2Qjk2RkUyQU1zQ0E4OURFRENGQjNEOUNEMDNDMTJCMzY4MzMzMTBQkU5MTY0MjA0QTBDOThBNDZBMkJDNTkwMzQ4OUMwRkM5MTA2Mz1CNENBMDIxN0FCMTE3RTdBQjI1NjFjMzJCNUNBRTVGOTICQzc3Q0NEMDhFMzE5REVBOTM3QjI1OEYyN0Y2NThDNzBGNDMxMEUyMzMQ0JCNDRERTFGOEU4QUE1MDA5MDMwNTE2ODQzRkYyM0QyOUE5QjIzNjYzI2NkM2NDQxQkJKCQTKzNkRDODRDNTgyNjg1RDBCOENGQkQ2NjAxMUNCQTA50TM0RUZGMURGRUJERjQ4MkZDOEVGRj1GQzE5ODMxMDdBOE11MT1BOU4REZCRTQ1MDRCMDcwOEM1NTYxRTBDOUYwMDAwMDAxNzAyMDAwMDUwNEIwMTAyMUyMDEOMDAwOTAwNjMwMDFBQjE0NDUzQzU1NjFFMEM5RjAwMDAwMDE3MDIwMDAwMDgwMDJGMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwNjY2QzYxNjcyRtC0Nzg3NDBBMDAyMDAwMDAwMDAwMTAwMTgwMDVFNEM1RTVDMj1COUQ3MDE1RTRDNUU1QzI5QjI1ENzAxMTI1REZBMzUyOU15RDcwMTAxOTkwNzAwMDEwMDQxNDUwMzA4MDA1MDRCMDUwNjAwMDAwMDAwMDEwMDAxMDA2NTAwMDAwMEUwMDAwMDAwMDAwMA==

发现解密完后是一段base64

继续

DQxNDUwMzA4MDAyMQQxMDEyNjM1M0NGRTdDNjFEQ0VCMTBCQjkwQjI2Qjk2RkUyQU1zQ0E4OURFRENGQjNEOUNEMDNDMTJCMzY4MzMzMTBQkU5MTY0MjA0QTBDOThBNDZBMkJDNTkwMzQ4OUMwRkM5MTA2Mz1CNENBMDIxN0FCMTE3RTdBQjI1NjFjMzJCNUNBRTVGOTICQzc3Q0NEMDhFMzE5REVBOTM3QjI1OEYyN0Y2NThDNzBGNDMxMEUyMzMQ0JCNDRERTFGOEU4QUE1MDA5MDMwNTE2ODQzRkYyM0QyOUE5QjIzNjYzI2NkM2NDQxQkJKCQTKzNkRDODRDNTgyNjg1RDBCOENGQkQ2NjAxMUNCQTA50TM0RUZGMURGRUJERjQ4MkZDOEVGRj1GQzE5ODMxMDdBOE11MT1BOU4REZCRTQ1MDRCMDcwOEM1NTYxRTBDOUYwMDAwMDAxNzAyMDAwMDUwNEIwMTAyMUyMDEOMDAwOTAwNjMwMDFBQjE0NDUzQzU1NjFFMEM5RjAwMDAwMDE3MDIwMDAwMDgwMDJGMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwNjY2QzYxNjcyRtC0Nzg3NDBBMDAyMDAwMDAwMDAwMTAwMTgwMDVFNEM1RTVDMj1COUQ3MDE1RTRDNUU1QzI5QjI1ENzAxMTI1REZBMzUyOU15RDcwMTAxOTkwNzAwMDEwMDQxNDUwMzA4MDA1MDRCMDUwNjAwMDAwMDAwMDEwMDAxMDA2NTAwMDAwMEUwMDAwMDAwMDAwMA==

清空 加密 解密 解密为UTF-8字节流

504B03041400090063001AB14453C5561E0C9F0000001702000008000B00666C61672E747874019907000100414503080023D10126353CFE7C61DCBB10BB90B26B96FE2CB3CA89DEDCFB3D9CD03C12B36833314ABE9164204A0C98A46A2BC5903489C0FC910639B4CA0217AB117E7AB2561A32B5CAE5F99BC77CCD08E319DEA937B258F27F658C70F4310E2337CBB44DEF8E8AA5009030516843FF23D29A9B23622C266C6441BBBA936DC84C582685D0B8CFBD66011CBA09934EFF1DFEBDF482FC8EFF9FC1983107ASB519A9E8DFBE4504B0708C5561E0C9F000000170200000504B01021F001400090063001AB14453C5561E0C9F0000001702000008002F000000000000020000000000000000666C61672E7478740A00200000000000010018005E4C5E5C29B9D7015E4C5E5C29B9D701125DFA3529B9D7010199070001004145030800504B050600000000100010065000000E00000000000

复制

Base编码系列: [Base64](#) [Base32](#) [Base16](#)

Base64编码是使用64个可打印ASCII字符 (A-Z、a-z、0-9、+、/) 将任意字节序列数据编码成ASCII字符串, 另有 "=" 符号用作后缀用途。

Base64 索引表

数值	字符	数值	字符	数值	字符	数值	字符
----	----	----	----	----	----	----	----

解出来是一段hex

50 4B 03 04真是太令人开心了, 一看就是压缩包的头, 把这些写进winhex里

这里再插一句题外话

了解文件的格式对于misc手来讲很重要!!!

beautiful_sky.jpg		1.zip																ANSI ASCII																																																																																		
Offset		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F																																																																																			
00000000	50 4B 03 04 14 00 09 00 63 00 1A B1 44 53 C5 56	PK	c	±DSÅV	00000010	1E 0C 9F 00 00 00 17 02 00 00 08 00 0B 00 66 6C	ÿ		fl	00000020	61 67 2E 74 78 74 01 99 07 00 01 00 41 45 03 08	ag.txt	™	AE	00000030	00 23 D1 01 26 35 3C FE 7C 61 DC EB 10 BB 90 B2	#Ñ	&5<p aüë	» °	00000040	6B 96 FE 2C B3 CA 89 DE DC FB 3D 9C D0 3C 12 B3	k-p,	°Ê%PÜú=œÐ<	°	00000050	68 33 31 4A BE 91 64 20 4A 0C 98 A4 6A 2B C5 90	h3lJ¾'	d J ~mj+Å	00000060	34 89 C0 FC 91 06 39 B4 CA 02 17 AB 11 7E 7A B2	4%Àü'	9'Ê « ~z°	00000070	56 1A 32 B5 CA E5 F9 9B C7 7C CD 08 E3 19 DE A9	V 2µÊâù>	Ç Í ä B@	00000080	37 B2 58 F2 7F 65 8C 70 F4 31 0E 23 37 CB B4 4D	7°Xò e@pôl	#7Ë'M	00000090	E1 F8 E8 AA 50 09 03 05 16 84 3F F2 3D 29 A9 B2	áòè°P	„?ò=)@°	000000A0	36 22 C2 66 C6 44 1B BB A9 36 DC 84 C5 82 68 5D	6"ÁfÆD	»@6Ü,,Å,h]	000000B0	0B 8C FB D6 60 11 CB A0 99 34 EF F1 DF EB DF 48	ûÖ`	Ë °4iñßèßH	000000C0	2F C8 EF F9 FC 19 83 10 7A 8B 51 9A 9E 8D FB E4	/Èiùù	f z<Qšž ûä	000000D0	50 4B 07 08 C5 56 1E 0C 9F 00 00 00 17 02 00 00	PK	ÅV ÿ	000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à	
00000020	61 67 2E 74 78 74 01 99 07 00 01 00 41 45 03 08	ag.txt	™	AE	00000030	00 23 D1 01 26 35 3C FE 7C 61 DC EB 10 BB 90 B2	#Ñ	&5<p aüë	» °	00000040	6B 96 FE 2C B3 CA 89 DE DC FB 3D 9C D0 3C 12 B3	k-p,	°Ê%PÜú=œÐ<	°	00000050	68 33 31 4A BE 91 64 20 4A 0C 98 A4 6A 2B C5 90	h3lJ¾'	d J ~mj+Å	00000060	34 89 C0 FC 91 06 39 B4 CA 02 17 AB 11 7E 7A B2	4%Àü'	9'Ê « ~z°	00000070	56 1A 32 B5 CA E5 F9 9B C7 7C CD 08 E3 19 DE A9	V 2µÊâù>	Ç Í ä B@	00000080	37 B2 58 F2 7F 65 8C 70 F4 31 0E 23 37 CB B4 4D	7°Xò e@pôl	#7Ë'M	00000090	E1 F8 E8 AA 50 09 03 05 16 84 3F F2 3D 29 A9 B2	áòè°P	„?ò=)@°	000000A0	36 22 C2 66 C6 44 1B BB A9 36 DC 84 C5 82 68 5D	6"ÁfÆD	»@6Ü,,Å,h]	000000B0	0B 8C FB D6 60 11 CB A0 99 34 EF F1 DF EB DF 48	ûÖ`	Ë °4iñßèßH	000000C0	2F C8 EF F9 FC 19 83 10 7A 8B 51 9A 9E 8D FB E4	/Èiùù	f z<Qšž ûä	000000D0	50 4B 07 08 C5 56 1E 0C 9F 00 00 00 17 02 00 00	PK	ÅV ÿ	000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à											
00000030	00 23 D1 01 26 35 3C FE 7C 61 DC EB 10 BB 90 B2	#Ñ	&5<p aüë	» °	00000040	6B 96 FE 2C B3 CA 89 DE DC FB 3D 9C D0 3C 12 B3	k-p,	°Ê%PÜú=œÐ<	°	00000050	68 33 31 4A BE 91 64 20 4A 0C 98 A4 6A 2B C5 90	h3lJ¾'	d J ~mj+Å	00000060	34 89 C0 FC 91 06 39 B4 CA 02 17 AB 11 7E 7A B2	4%Àü'	9'Ê « ~z°	00000070	56 1A 32 B5 CA E5 F9 9B C7 7C CD 08 E3 19 DE A9	V 2µÊâù>	Ç Í ä B@	00000080	37 B2 58 F2 7F 65 8C 70 F4 31 0E 23 37 CB B4 4D	7°Xò e@pôl	#7Ë'M	00000090	E1 F8 E8 AA 50 09 03 05 16 84 3F F2 3D 29 A9 B2	áòè°P	„?ò=)@°	000000A0	36 22 C2 66 C6 44 1B BB A9 36 DC 84 C5 82 68 5D	6"ÁfÆD	»@6Ü,,Å,h]	000000B0	0B 8C FB D6 60 11 CB A0 99 34 EF F1 DF EB DF 48	ûÖ`	Ë °4iñßèßH	000000C0	2F C8 EF F9 FC 19 83 10 7A 8B 51 9A 9E 8D FB E4	/Èiùù	f z<Qšž ûä	000000D0	50 4B 07 08 C5 56 1E 0C 9F 00 00 00 17 02 00 00	PK	ÅV ÿ	000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																
00000040	6B 96 FE 2C B3 CA 89 DE DC FB 3D 9C D0 3C 12 B3	k-p,	°Ê%PÜú=œÐ<	°	00000050	68 33 31 4A BE 91 64 20 4A 0C 98 A4 6A 2B C5 90	h3lJ¾'	d J ~mj+Å	00000060	34 89 C0 FC 91 06 39 B4 CA 02 17 AB 11 7E 7A B2	4%Àü'	9'Ê « ~z°	00000070	56 1A 32 B5 CA E5 F9 9B C7 7C CD 08 E3 19 DE A9	V 2µÊâù>	Ç Í ä B@	00000080	37 B2 58 F2 7F 65 8C 70 F4 31 0E 23 37 CB B4 4D	7°Xò e@pôl	#7Ë'M	00000090	E1 F8 E8 AA 50 09 03 05 16 84 3F F2 3D 29 A9 B2	áòè°P	„?ò=)@°	000000A0	36 22 C2 66 C6 44 1B BB A9 36 DC 84 C5 82 68 5D	6"ÁfÆD	»@6Ü,,Å,h]	000000B0	0B 8C FB D6 60 11 CB A0 99 34 EF F1 DF EB DF 48	ûÖ`	Ë °4iñßèßH	000000C0	2F C8 EF F9 FC 19 83 10 7A 8B 51 9A 9E 8D FB E4	/Èiùù	f z<Qšž ûä	000000D0	50 4B 07 08 C5 56 1E 0C 9F 00 00 00 17 02 00 00	PK	ÅV ÿ	000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																					
00000050	68 33 31 4A BE 91 64 20 4A 0C 98 A4 6A 2B C5 90	h3lJ¾'	d J ~mj+Å	00000060	34 89 C0 FC 91 06 39 B4 CA 02 17 AB 11 7E 7A B2	4%Àü'	9'Ê « ~z°	00000070	56 1A 32 B5 CA E5 F9 9B C7 7C CD 08 E3 19 DE A9	V 2µÊâù>	Ç Í ä B@	00000080	37 B2 58 F2 7F 65 8C 70 F4 31 0E 23 37 CB B4 4D	7°Xò e@pôl	#7Ë'M	00000090	E1 F8 E8 AA 50 09 03 05 16 84 3F F2 3D 29 A9 B2	áòè°P	„?ò=)@°	000000A0	36 22 C2 66 C6 44 1B BB A9 36 DC 84 C5 82 68 5D	6"ÁfÆD	»@6Ü,,Å,h]	000000B0	0B 8C FB D6 60 11 CB A0 99 34 EF F1 DF EB DF 48	ûÖ`	Ë °4iñßèßH	000000C0	2F C8 EF F9 FC 19 83 10 7A 8B 51 9A 9E 8D FB E4	/Èiùù	f z<Qšž ûä	000000D0	50 4B 07 08 C5 56 1E 0C 9F 00 00 00 17 02 00 00	PK	ÅV ÿ	000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																										
00000060	34 89 C0 FC 91 06 39 B4 CA 02 17 AB 11 7E 7A B2	4%Àü'	9'Ê « ~z°	00000070	56 1A 32 B5 CA E5 F9 9B C7 7C CD 08 E3 19 DE A9	V 2µÊâù>	Ç Í ä B@	00000080	37 B2 58 F2 7F 65 8C 70 F4 31 0E 23 37 CB B4 4D	7°Xò e@pôl	#7Ë'M	00000090	E1 F8 E8 AA 50 09 03 05 16 84 3F F2 3D 29 A9 B2	áòè°P	„?ò=)@°	000000A0	36 22 C2 66 C6 44 1B BB A9 36 DC 84 C5 82 68 5D	6"ÁfÆD	»@6Ü,,Å,h]	000000B0	0B 8C FB D6 60 11 CB A0 99 34 EF F1 DF EB DF 48	ûÖ`	Ë °4iñßèßH	000000C0	2F C8 EF F9 FC 19 83 10 7A 8B 51 9A 9E 8D FB E4	/Èiùù	f z<Qšž ûä	000000D0	50 4B 07 08 C5 56 1E 0C 9F 00 00 00 17 02 00 00	PK	ÅV ÿ	000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																														
00000070	56 1A 32 B5 CA E5 F9 9B C7 7C CD 08 E3 19 DE A9	V 2µÊâù>	Ç Í ä B@	00000080	37 B2 58 F2 7F 65 8C 70 F4 31 0E 23 37 CB B4 4D	7°Xò e@pôl	#7Ë'M	00000090	E1 F8 E8 AA 50 09 03 05 16 84 3F F2 3D 29 A9 B2	áòè°P	„?ò=)@°	000000A0	36 22 C2 66 C6 44 1B BB A9 36 DC 84 C5 82 68 5D	6"ÁfÆD	»@6Ü,,Å,h]	000000B0	0B 8C FB D6 60 11 CB A0 99 34 EF F1 DF EB DF 48	ûÖ`	Ë °4iñßèßH	000000C0	2F C8 EF F9 FC 19 83 10 7A 8B 51 9A 9E 8D FB E4	/Èiùù	f z<Qšž ûä	000000D0	50 4B 07 08 C5 56 1E 0C 9F 00 00 00 17 02 00 00	PK	ÅV ÿ	000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																		
00000080	37 B2 58 F2 7F 65 8C 70 F4 31 0E 23 37 CB B4 4D	7°Xò e@pôl	#7Ë'M	00000090	E1 F8 E8 AA 50 09 03 05 16 84 3F F2 3D 29 A9 B2	áòè°P	„?ò=)@°	000000A0	36 22 C2 66 C6 44 1B BB A9 36 DC 84 C5 82 68 5D	6"ÁfÆD	»@6Ü,,Å,h]	000000B0	0B 8C FB D6 60 11 CB A0 99 34 EF F1 DF EB DF 48	ûÖ`	Ë °4iñßèßH	000000C0	2F C8 EF F9 FC 19 83 10 7A 8B 51 9A 9E 8D FB E4	/Èiùù	f z<Qšž ûä	000000D0	50 4B 07 08 C5 56 1E 0C 9F 00 00 00 17 02 00 00	PK	ÅV ÿ	000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																						
00000090	E1 F8 E8 AA 50 09 03 05 16 84 3F F2 3D 29 A9 B2	áòè°P	„?ò=)@°	000000A0	36 22 C2 66 C6 44 1B BB A9 36 DC 84 C5 82 68 5D	6"ÁfÆD	»@6Ü,,Å,h]	000000B0	0B 8C FB D6 60 11 CB A0 99 34 EF F1 DF EB DF 48	ûÖ`	Ë °4iñßèßH	000000C0	2F C8 EF F9 FC 19 83 10 7A 8B 51 9A 9E 8D FB E4	/Èiùù	f z<Qšž ûä	000000D0	50 4B 07 08 C5 56 1E 0C 9F 00 00 00 17 02 00 00	PK	ÅV ÿ	000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																										
000000A0	36 22 C2 66 C6 44 1B BB A9 36 DC 84 C5 82 68 5D	6"ÁfÆD	»@6Ü,,Å,h]	000000B0	0B 8C FB D6 60 11 CB A0 99 34 EF F1 DF EB DF 48	ûÖ`	Ë °4iñßèßH	000000C0	2F C8 EF F9 FC 19 83 10 7A 8B 51 9A 9E 8D FB E4	/Èiùù	f z<Qšž ûä	000000D0	50 4B 07 08 C5 56 1E 0C 9F 00 00 00 17 02 00 00	PK	ÅV ÿ	000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																														
000000B0	0B 8C FB D6 60 11 CB A0 99 34 EF F1 DF EB DF 48	ûÖ`	Ë °4iñßèßH	000000C0	2F C8 EF F9 FC 19 83 10 7A 8B 51 9A 9E 8D FB E4	/Èiùù	f z<Qšž ûä	000000D0	50 4B 07 08 C5 56 1E 0C 9F 00 00 00 17 02 00 00	PK	ÅV ÿ	000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																																		
000000C0	2F C8 EF F9 FC 19 83 10 7A 8B 51 9A 9E 8D FB E4	/Èiùù	f z<Qšž ûä	000000D0	50 4B 07 08 C5 56 1E 0C 9F 00 00 00 17 02 00 00	PK	ÅV ÿ	000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																																						
000000D0	50 4B 07 08 C5 56 1E 0C 9F 00 00 00 17 02 00 00	PK	ÅV ÿ	000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																																										
000000E0	50 4B 01 02 1F 00 14 00 09 00 63 00 1A B1 44 53	PK	c	±DS	000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																																														
000000F0	C5 56 1E 0C 9F 00 00 00 17 02 00 00 08 00 2F 00	ÅV ÿ		/	00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																																																			
00000100	00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C			fl	00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																																																								
00000110	61 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00	ag.txt			00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																																																													
00000120	18 00 5E 4C 5E 5C 29 B9 D7 01 5E 4C 5E 5C 29 B9	^L^`)	¹x ^L^`)	¹	00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																																																																		
00000130	D7 01 12 5D FA 35 29 B9 D7 01 01 99 07 00 01 00	x]ú5)	¹x	™	00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																																																																							
00000140	41 45 03 08 00 50 4B 05 06 00 00 00 00 01 00 01	AE	PK		00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																																																																												
00000150	00 65 00 00 00 E0 00 00 00 00 00 00 00 00 00 00	e	à																																																																																																	

看到了flag.txt的字样

赶紧解压

提示需要密码

看了眼评论区作者自己的评论



R0se64 1天前

jpg属性里的字符如果解不出来就试试下面这个吧

KZDTCMCUNMYXGUTKLJMGCMMKKKBMVIQLXMVLFM5DDI5YE4YL2KZ4FM3CSJ5KDEVTTMEZ
WQVKXJBEOVKGIU4VAUJ5HU=====

回复 0

经典base32转base64再转base64

如果你没有判断出来的话也可以写个脚本跑一下：

```
import base64
```

```
str1='
```

```
KZDTCMCUNMYXGUTKLJMGCMMKKKBMVIQLXMVLFM5DDI5YE4YL2KZ4FM3CSJ5KDEVTTMEZWQVKXJB
```

```
print base64.b64decode(str1)
```

```
print base64.b32decode(str1)
```

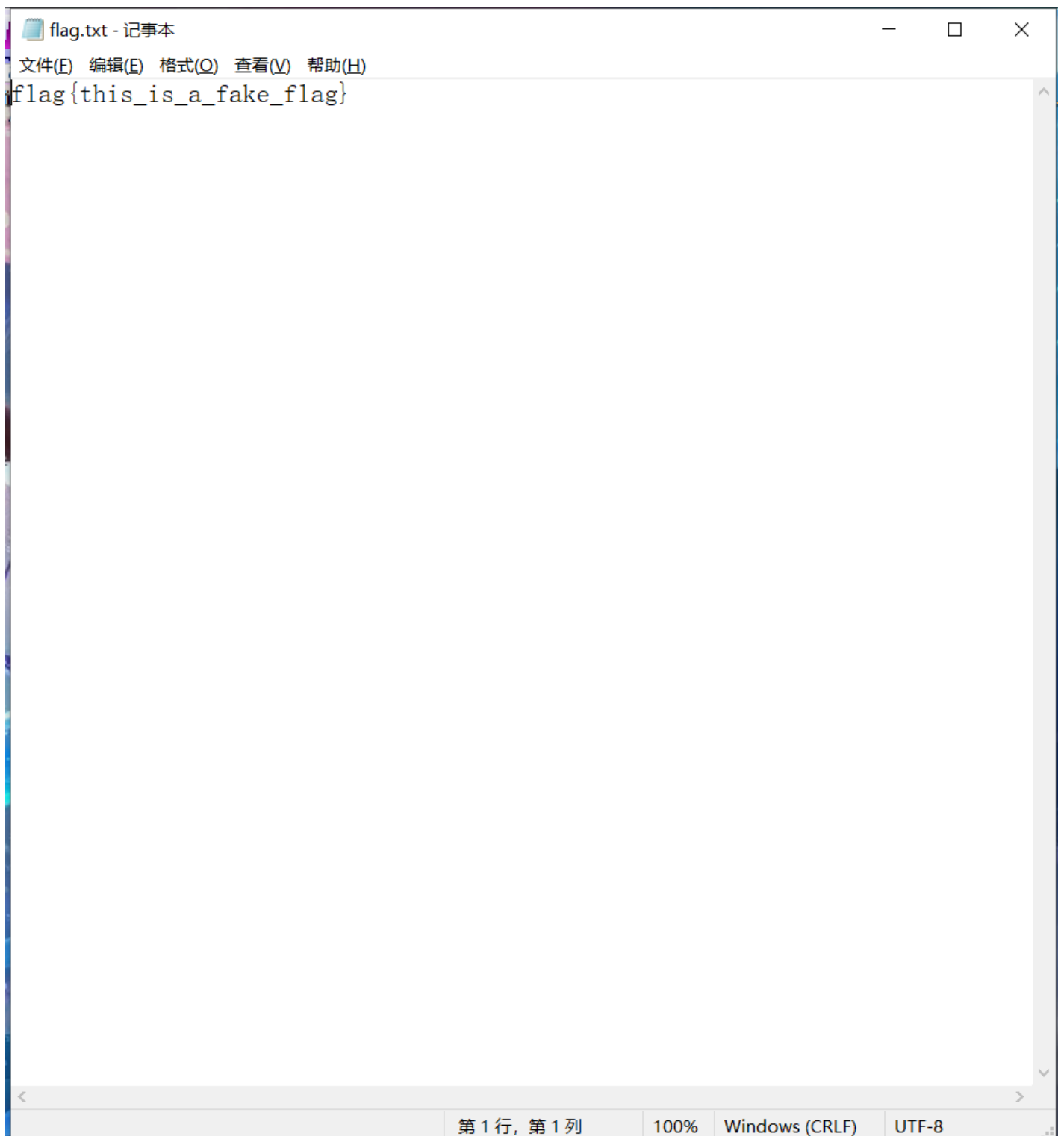
```
print base64.b16decode(str1)
```

解得: llllove1

.....不予评价

用它去解密压缩包

得到flag.txt



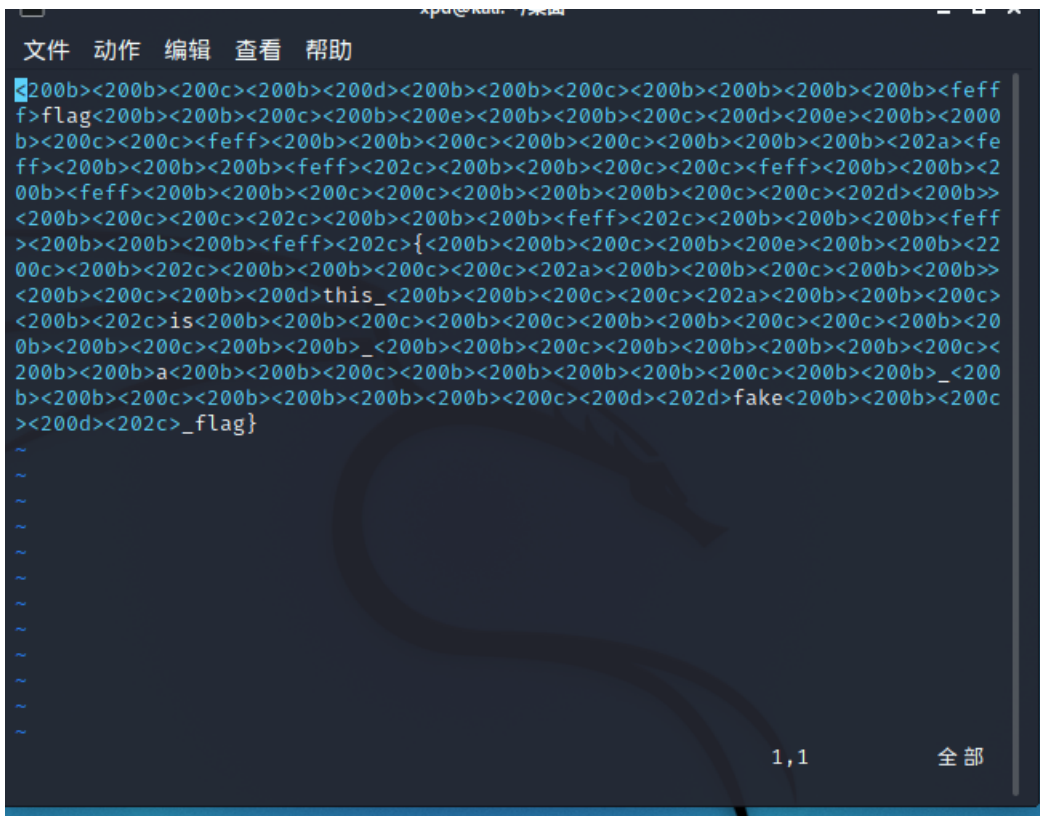
```
flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag{this_is_a_fake_flag}
第 1 行, 第 1 列 100% Windows (CRLF) UTF-8
```

额 看来还没完我们继续

仔细观察属性，发现这个文本文档明明只有一句话我们却看到了518个字节

初步怀疑是0宽度字符隐写，拖到kali里看一下

vim flag.txt



是它没跑了，在线工具跑一下

Unicode Steganography with Zero-Width Characters

这里我还很耐心的看了一下都有什么，结果还是没跑出来

Zero Width Characters for Steganography:

- U+200B ZERO WIDTH SPACE
- U+200C ZERO WIDTH NON-JOINER
- U+200D ZERO WIDTH JOINER
- U+200E LEFT-TO-RIGHT MARK
- U+202A LEFT-TO-RIGHT EMBEDDING
- U+202C POP DIRECTIONAL FORMATTING
- U+202D LEFT-TO-RIGHT OVERRIDE
- U+2062 INVISIBLE TIMES
- U+2063 INVISIBLE SEPARATOR
- U+FEFF ZERO WIDTH NO-BREAK SPACE

这里回到上文，图片的属性里有一句

备注 | 拉满了拉满了00000beautiful

直接全部拉满

(Extension must be modified)

Zero Width Characters for Steganography:

- U+200B ZERO WIDTH SPACE
- U+200C ZERO WIDTH NON-JOINER
- U+200D ZERO WIDTH JOINER
- U+200E LEFT-TO-RIGHT MARK
- U+202A LEFT-TO-RIGHT EMBEDDING
- U+202C POP DIRECTIONAL FORMATTING
- U+202D LEFT-TO-RIGHT OVERRIDE
- U+2062 INVISIBLE TIMES
- U+2063 INVISIBLE SEPARATOR
- U+FEFF ZERO WIDTH NO-BREAK SPACE

Text in Text Steganography Sample

Original Text: <input type="button" value="Clear"/> (length: 25) flag{this_is_a_fake_flag}		Steganography Text: <input type="button" value="Clear"/> (length: 195) flag{this_is_a_fake_flag}
Hidden Text: <input type="button" value="Clear"/> (length: 34) flag{we1_wants_a_girlfriendeddd~}	<input type="button" value="Encode »"/> <input type="button" value="« Decode"/>	<input type="button" value="Download Stego Text as File"/>

得到flag

PS:有关压缩包的密码那件事，这道题的作者和我进行了讨论，应该是平台在上传题目的时候弄错了。