

1.社交网络

A记录

感觉自己的脑洞还是太小,一开始没有想到Birthday是什么意思,后来想到生日应该是8位数字,于是重新爆破。在这个过程中 大胆猜测社交网络上的人生日应该在1900年之后,于是从这个数字开始爆破。

SOS

绕

理查德

http://blog.csdn.net/FunkyPants

Snake

🏼 KRyLack Z	IP Password Recovery		0 0
<u>File Action</u>	<u>T</u> ools <u>H</u> elp		
Start	Stop Open S	Save Settings Help About	<u>E</u> xit
- Encrypted ZI	P Archive:	Recovery Type:	
E:\chrome_do	ownload\Birthday.zip Browse	● Brute-force ○ Mask ○ Dicti	ionary
Charset:		Start Options	
🔲 Latin	Password Recovered!		
E Caps	KRyLack ZIP Password Recovery has	successfully recovered the password!	Clear
✓ Digits			
Custo	Password: 19971028	Copy Sa <u>v</u> e	Liear
0123456	E:\chrome_download	l\Birthday.zip	
	Format: ZIP Archive		Bro <u>w</u> se
Priority:	RyLack		
Low		Close Help	
Background	work	File format:	
	Minimize to <u>T</u> ray	Time Elapsed: Average Speed:	
Recovery stopp	bed		
KRy	Lack ZJ	P Password Recove	ľy kvPants

00000850	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000860	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000870	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000880	00	00	00	00	00	00	00	00	00	00	00	00	53	4F	4E	59					SONY	
00000890	00	00	32	30	31	35	ЗA	31	30	ЗA	32	38	20	31	36	ЗA	2	015	5:10	:28	3 16:	
000008A0	30 3	39	ЗА	32	36	00	66	6C	61	67	7B	68	69	5F	6D	79	09:	26	fla	g{1	hi_my	
000008B0	5F	66	72	69	33	6E	64	7Å	7D	00	00	05	90	03	00	02	_fr	i3r	ndz}			
00000800	00	00	00	14	00	00	10	A6	90	04	00	02	00	00	00	14			1			
000008D0	00	00	10	92	92	91	00	02	00	00	00	03	36	32	00	00		· · ·			62	
000008E0	92	92	00	02	00	00	00	03	36	32	00	00	EA	1C	00	07	· ·		6	2	ê	
000008F0	00	00	07	В4	00	00	08	DE	00	00	00	00	1C	EÀ	00	00		1	Þ		ê	
00000900	00	08	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000910	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000920	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
00000930	00	00	00	00	00	00	00	00	00	00	00	00	00	0,0	00	00						
00000940	00	00	00	00	00	00	00	00	00	00	00	00	iqo:	00	00	00	csd	n. 1	net	/F	`unkyl	Pants
00000050		nn	nn.	$\cap \cap$	$\cap \cap$	$\cap \cap$	$\cap \cap$	00	00	$\cap \cap$	00											

2.有趣的文件

看了大佬的writeup之后有了思路,于是自己手动写了一个脚本解密,但是其中走了很多弯路……

N

直接复制前面8个十六进制字符去搜索的话,会发现这很像7z压缩包的文件头,但是每两个字节之间需要换下位置(我之前并不知道7z的格式是什么样的......)。图一是错误的格式,图二是正确的格式

	国际版						
fbc 1	c27						م
顶	图片	视频	学术	词典	地图		
太 会潮底	到版論 \ 73	कर्फ स्ट्रांस	田協到国际世	62 烟苗立约	4里雨丰宫雨准确	×	
122,023		CX / MORVA	20196001#41P070	R : 1999.244		· ·	
,690 条	结果 时间	间不限 🔻					
7-Zip	o / Disc	ussion	/ Help:	Error: C	Can not ope	en file as 📱	11年此页
2012-10	413 · Error: Col 1 kog oor	Can not op הההה ההחר	pen file as a LOOOO OO3d	rchive he nana nana	xdump head 0000	1000 7 a37 <mark>afbc 1 c27</mark>	0300 83e2

7-Zip / Discussion / Help:Multi-part issue 翻译此页

sourceforge.net/p/sevenzip/discussion/45797/thread/5a6e0f6a -

顶 图,	片 视频	学术 词典	地图	
検測剤療 输	入了英文,试试切	换到国际版?搜英文约	吉果更丰富更准确)	
52,000 条结果	₹ 时间不限 ▼			

sourceforge.net/p/sevenzip/discussion/45798/thread/c0838d18 -

377a bcaf 271c 0004 9b97 92e0 0a2f 0000 0000 0000 ... 翻译此页

377a bcaf 271c 0004 9b97 92e0 0a2f 0000. 0000 0000 5a00 0000 0000 0000 4624 bf06. e08e b42f 025d 003d e18c d2e2 bb89 d288. f2b7 e69c 654f 5a88 945a 1b67 b56e 18e0; //blog.csdn.net/FunkyPants https://pastebin.com/1BUJαZ0v マ

于是我写了一个脚本,去除行号,去除换行符,并且在4个字符中1号2号位置的字符和3号4号位置字符交换位置。最终得到了正确的十六进制数据。



但是因为我不知道怎么把十六进制数据写入文件并让它也存储为十六进制数据,所以在得到十六进制的数据后,使用winhex来帮 我完成接下来的工作。

新建一个txt文档,直接拖入winhex中准备写入数据。

Offset	0	1	2	3	- 4	- 5	6	7	8	9	A	в	С	D	Е	F		ANSI	ASCII	
00000000																				_
																	_			
										- 1			- A -					/=	. D	
										h	tt	p:/	/b.	log	;. C		h. net	/Fun	kyPan	ts

复制上个程序中得到的十六进制数据

[flag.t	xt - 记寻	缽																			_	٢	נ	×
文	(牛(F)	编辑(E)	格式(0) 査	看(\∕)	帮助 (H))																		
c6	5795	08ac	bbae	f229	bd31	f598	11ab	2144	4ba9	4ffd	158e	f297	e311	d47f	344f	e659	788d	5dad	0e4e	a6ab	11df	ca9f	eab9	4cf6	6 ^
39	65d9	ad87	9846	fde2	941d	df09	06bd	b5ce	333d	d87d	1783	1004	c231	fd4d	72eb	814a	Of9c	70e1	c5ad	93b8	4c28	133c	e56c	e28b	6
61	9345	062b	ad34	260a	7e2e	2272	c124	9259	1540	9691	c36d	ec55	3c02	fca5	fc49	0d61	76cc	665b	e3cd	bb1b	573c	5007	de47	c5b5	4
f4	e700	d8e9	394f	d249	2948	b234	cef2	7040	_c36c	Obda	41bd	7599	9fcf	e23e	aa91	7607	4987	5be9	Obbd	0532	20de	5cc4	347e	84f6	6
47	8611	5488	2cd0	4e3b	b03c	b2ce	ff85	e7cd	9eab	1d04	6cef	11a6	8976	7aa2	2ce3	42a4	6d92	ald0	1b43	1a94	da2f	6efd	ff13	b538	2
b۵.	526a	6561	ea9a	2db9	bc18	6693	7729	blfc	beaf	f410	1036	2620	05f2	c35a	9343	e09f	ed51	ac35	4a40	clfa	f80f	1081	96aa	d4fa	5
ăc.	dc4d	1267	9628	1/b/	543d	e808	be3d	2660	e814	25b3	e887	64e5	bcd/	bebc	6655	d017	b463	dae2	db85	4e8b	67f1	dbc8	5890	becc	9
45	1819	Saab	e3fd	6070	9e3a	9e08	Idbb	899e	Uda/	9ad9	bcfU	d4e5	241d	b8e/	(ede	504f	3291	3240	ba87	2ee9	157c	3684	2a28	6C65	4
81	e62d	65d1	8653	64/f	8c4f	8725	0625	6650	3064	21ba	eU2b	924c	bdfa	CU18	CUCI	Ucbe	d/fd	dleU	05a4	a4d3	9779	66Uc	e256	6936	8
(3 44	52ca	dded	690I	1291	4012	0774	CD3a	0000	(180	0654	diau	3740	2376	SSec.	2752	8341	3284	dddb	40.0	1010	baye	23Ie	DCD (0000	C
44 00	1dbc	duxe	alle	30dc	7254	104b	a504	2898	1210	597e	a(23	e414	CJEE	305a	977a	e942	9811	000	4880	8072	SDD1	UI14	1002	a4b1	1
20	DDIA	0019	9983 440-	0110	5258	DIDZ	CCC7	4190	1190	100-9	edau	100e	3a9a	93ab	4600	(0eŏ	acib	45-0	2000 A 30-	93eZ	0-61	ba∪a ⊒77-	0744	5123	ک د
0Z.	01-1	84ea	448e	bdae	alec	5001	5802	1229	a040	0088	39ae	A000	- C/aa - ⊒7	3000	E010	ezap	abo3	40.0	4080	ODGE	2001 2071	170-	9/14	C114 7002	α
4a 0-	ZICD	DOCD	200	ab25	a80a	071-1	JO02	abcb	ae72	a090	100%	1298	1074	-711	2018	9CZa	1500	1902	9082	9200	137D	-70E	dola Aran	1843	a 1
90	00ac	1023	Jaen	0241	-00a1	-900L	1440	949Z	4076	0570	1000	E040	DZ(4)	155-	02-4	2009	0002	2031	dese anar	0000	720-	#77a	41UD	2045 1-641-	1
90	Vofo	16Ca	1724	-CIED 	1440	uo48	4040 076a	1100	4010	9010	15-0	7-01	0054	100C	-02au	-204	4040	0970	200-	2000 4£44	14-0	hEe0	0440	14ee	a
06.	5-60	0014	1000	059A	50fa	- auso - 2650	-950	0405	fdo7	2447	foedf	1001 140	2001	2600	+20~	0.504	1614	7hah	500a	6hQa	2-10	567a	ouuo o0do	14ae 44b9	0
90 90	0405	702a	Noaf	6625	7492	5675	2032	- 31 a.J - 325 c	7144	offed	7£43	2090	5264	f5ec	4825	6492	5433	10-9	a541	59K4	4040	2014 2290	225a	094b	
03	6609	2221	20f7	h720	47fa	171a	0402	2000	-66h3	3270	3747	ha52	4765	1686	-1020 	c10e	45hQ	4505	6244	7175	47.46	a072	2222	1hal	ă
24 84	8670	5694	7a6b	lehf	7622	=014	co41	014	662a	Qhao	465d	4684	9444	2222	- K979	9696	Qofa	0197	a18b	5-04	£973	Rdod	6bbc	7270	ž.
aĤ	34dc	9cdb	0652	71fa	3353	5048	191a	Neeh	_999A	3ec0	h217	08af	2000	Scef	7269	8f88	6267		8266	4bd5	7649	4068	fa51	4068	h
32	1477	5acf	fb0b	7370	f73a	9f7a	761f	8bb1	aba6	e843	e7bc	97f2	16b1	8c44	6e95	70be	9fab	d2ff	e9b8	aSca	3527	ae98	9140	2a0c	4
f3.	95ce	h5f9	35cd	a8f2	dd97	b1bc	8650	1a7e	ffic8	8642	6b1e	a49f	85.44	f9ac	5af0	2eab	f18f	b18e	hf7f	h7ch	dd44	1804	ca7a	32f7	0
1c	108a	d6ad	a20e	066c	f8a7	1568	0bo0	bf84	5e61	28aa	0ed7	c44b	4adc	a23c	2932	4568	ъ357	36ь1	2.487	bacc	ed53	6766	24e9	caf5	č
2ъ	5245	255e	5f93	4987	b2b4	81e7	7570	4ecd	d082	14d7	3c05	3a3c	c0ba	5bd5	9a7c	646f	c03c	4eff	aeee	648e	2e38	8749	1a23	579f	5
72	2e00	6a00	7000	6700	0000	140a	0100	0f8e	a288	4450	d101	1506	0100	2000	0000	0000									~
<																									>
																		ttp:	//b]	1行,	第1列	net/i			ts "

粘贴到winhex中,选择ASCII hex模式粘贴(这里的图没截到……)

之后保存文件,手动将文件后缀改为7z,可以打开压缩包,将里面的阿狸图片再拖到winhex中可以看到base64编码的flag。

🔇 新建	文本文档	(2).7z - E	3 andizip	6.10					_		\times
文件(F)	编辑(E)	查找(l)	选项(0)) 视图(V)	帮助(H)						
[→ ±177	-	し 解压		し よ 新建	下 十 添加			。 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			
🏫 新建	文本文档 (2) . 7z		名称		Ý		压缩后大小	厦	融大小	类型
				■ 阿狸.jp	g			100,994	1	00,010	JPG 文4
				/				_			
							http://k	 文件: 1, 文件夹	: 0, 压缩色	四大小: 98	7 KB

3.Paint&Scan

因为对于图片隐写有一定的基础,看到点的坐标时就知道这个题目需要我们通过点的坐标画图还原FLAG,一开始还以为可以直接得到FLAG字符串的,结果还需要扫个二维码……

Python的PIL库简单易用(在Python3中对应库为Pillow),在网上随便找了篇画图教程之后就知道了其原理,个人觉得稍难一点的 地方是还需要调用这个库去新建一个图片。可以参考官方文档: http://www.effbot.org/imagingbook/image.htm 最终的代码如下:



得到结果如下图所示,扫码可得FLAG。



因为这个题目做完之后没及时写Writeup,所以忘了截图。

打开所给GIF图片后不能显示,放到winhex里面发现文件头错误,修改文件头为GIF89a,可以看到一张19帧的活蹦乱跳的小黄人GIF,放入逐帧分解的软件中(我用的PS),可以看到每一帧中小黄人的位置,将小黄人对应位置用六十四卦幻方配数图对应为相应数字,再用Base64索引表解码得到base64字符串Q1RGe2FiY19kZWZfZ30,解码得flag(这两种编码方法是结合题目名称64在网上搜索到的)。

5.异性相吸

下载后得到一个明文和一个密文,并且都是32位的,同时题目难度为"易",猜测可能是进行了一些简单的位运算,又因为题目名称为"异性相吸",猜测可能是进行了异或,使用以下Python脚本解密



这个程序打印出来的结果提交后并不正确,展开脑洞把后面都写成biubiubiu后成功.....