10、隐写2



34 篇文章 1 订阅 订阅专栏

0x01、题目: 隐写2



0x02、WP

1、右键链接,点击新建标签页打开链接,保存该jpg图片



2、好了,又开始了,图片隐写的套路

①、打开该图片,发现宽高和颜色没什么特别的,略过(就是图太jian了。。。。。)





想拿到flag?心の中ないいくつかB数かの?

https://blog.csdn.net/qq_45555226

②、右键图片,查看属性的详细信息,没什么特别的,略过

Nelcome_jpg 唐性	×
常规 安全 详细信息 以前的版本	
屋性 值	^
说明	
标题 hint:	
主题 网络安全工作室在哪	
分级 ☆☆☆☆☆	
标记	
备 注	
来源	
作者	
拍摄日期	
程序名称	
获取日期	
版权	
图像	
图像 ID	
分辨率 581 x 533	
宽度 581 像素	
高度 533 像素	
水平分辨率 120 dpi	
垂直分辨率 120 dpi	
位深度 24	*
删除属性和个人信息	
确宪st//blog.es.取消.lai/gc_4或限。	% 226

③、记事本打开该图片,ctrl+f搜索: flag、fl@g、PK、rar等字符,并且拖到最下面查看有没有特殊字符

查找		x
查找 替换 文件查找 标记		
查找目标(E): flag	~ 查找下一个	
	□ 选取范围内① 计数①	
	查找所有打开文件(2)	y図 📕 00000310.jpg区 🔚 Welcomejpg 3.気石の RDBNAK ~8_轵^i~ DDB iビt(
□反向查找 □全词匹配(W)	在当前文件中查找	¥Y庈 xB30C3 xE6 XE9 NUD STX XE9 N - If [US XDB3鯰 聍陆 SP貉 旒u i- 欺 XBD ' 叭h 鬘 XE1 % XA20)
 □ 匹配大小与(C) □ 循环查找(P) 	取消	128>EM疠渧SUBn焞沚袺1匭転鍓& 1 XB7:骞tXDCEM用UCXC9SOSTX
查找模式 ●普通(N) ○ 扩展(N) (n,)r,)t, (n,)x, ()	 ✓ 透明度(Y) ● 失去焦点后 ○ 始终 	33。嚵怜) S0家 AND 7 ANS ' 创馿焻瞍 DAD 0 現都 BS 菴 bJ ANS ' UT) j CAN (村 AND AND AND SI S. AF CAN AND SI S . AF CAN AND SI S . AF CAN AND SI S . AF
		图挡绛。绕ECAB6000 CCCCC2EC011 鰕D鋈妖嫩 聋咏倔NAKCSCC2/襙厂
	又怕策J既静。 ————————————————————————————————————	

IR 福 u次 ' ' XCD VD r US 蚁 檔 介 穡 剔 b 罐 9 US XD3 ETX X X P (想 X39 (X39 K X 20 V D) r US 蚁 檔 介 穡 M 0 b 僅 9 US XD3 ETX X X 20 (速 X 20) 様 X 20) ' X 20 V D) c E C 2 N UD Q E

;掺n002202.t冬p4< 拥@ 姗礒233& 篰綍2070000023503652解盕<搑zp"221003'k'咢V2204eXd鴉a笻263'G0023雅莉 |臨'鲤d疏251惍 珜経0001怍鈲蛟|晩輔C>賀#289353 閹絆XG280/劑D鈥腐喚q覗/_鍲禱昿2336501毮[237\$VI氧]?WER2 值p 髸22285愈獚貏碉迳2瀊醯卤N銟|<渡t y呕'苚2820048膨焜K80L蕏6556n200885 驫2551斈橋頤娌5溺碖V+N52004

艾|佤:T貶x4崇涉嗒至ACDIDAED5壢DID7ETNQ烟&S湾噴=H0摶\盔30+B3D#奴|BMW 2 2339/ADBETX [, e堑遡TSODHSD B2CAN 哥澱c桮12p_0圖DC9j 2D9ETNc 2B3+M搾?闕2034 醉T龁DC82D3=2C31DC3鰞 BS CANk NAX2E3 239SD ;z灻DC2汹m33(WD5澍)絡3NAXN2E76SOD1篶肥H2AB#2B2 SgACX店ざ!agP鯫DC9唹艓X2EDSO223=跺佁J父臂ZA9SOXK(

■+嚭鰭僸C羶禮STXuL罍 X97EMXC5+'XD6

及模5xx*v<xxx0: 榨魷肌腐的Marka纓!3xxx10xxxx高Max2概题的Brakx30A3A xxx15xMax0051%前 Kom秋客x20"C 錄

④、把图片拖进010edit,搜索504b 0304;并且拉到最下面看看有没有特殊的字符

如图所示,发现了三处504b 0304,那我们就很不方便手动截取了,我们只能用kali的binwalk+foremost了

:	6	_					_	~	1				-W		1 4	· ·		👞 💼 : 👞 : 👡 🛁 = 🏍 🕡 == mmr : 🕯
Start	up	x	Tel	com	e j	pg	x											
∓ Ed	lit	As:	Hex		Ru	n Sc	ript	Ψ.	Rur	. Теп	plat	e 🔻						
		0	1	2	3	4	5	6	7	8	9	A	В	C	D	E	F	0123456789ABCDEF
CCEOh	:	00	51	45	14	00	51	45	14	00	51	45	14	00	51	45	14	.QEQEQE.
CCFOh	:	00	51	45	14	00	51	45	14	00	51	45	14	00	51	45	14	.QEQEQE.
CD00h	:	00	51	45	14	00	51	45	14	00	51	45	14	00	51	8A	28	.QEQEQEQŠ(
CD10h	: 3	A 0	02	8A	28	AU	02	0A	20	AU	02	8A	28	A0	02	8A	28	.š <mark></mark> Š(.Š(
CD20h	:	A 0	0F	FF	D9	50	4B	03	04	0A	00	00	08	00	00	38	7E	.ÿ <mark>J</mark> PK8~
CD30h	:	6E	4B	B 3	46	27	45	40	12	90	00	±C	LА	00	00	00	00	nV3
CD40h	:	00	00	66	6C	61	67	2E	72	61	72	50	4B	03	04	14	00	flag.rarPK
CD50h	:	01	08	08	00	7C	7D	6E	4B	26	F1	20	10	BC	19	00	00	···· ; ; !!Kall, .*•
CD60h	:	71	1A	00	00	05	00	00	00	33	2E	6A	70	67	43	41	D3	q3.jpgCAÓ
CD70h	:	ЗA	6C	B 0	FB	54	2A	E5	EC	61	7D	81	EB	EF	34	FO	32	:l°ûT*åìa}.ëï4ð2
CD80h	:	9C	E7	16	3C	C2	38	59	E7	4C	49	D2	7B	1E	F3	2D	F5	œç.<Â8YçLIÒ{.ó-õ
CD90h	:	67	CD	C2	25	95	73	94	5D	51	4F	B2	AB	A 5	D1	86	9D	gÍÄ%•s″]QO°«¥Ñ†.
CDAOh	:	41	92	C3	7F	91	17	ЗA	88	09	92	65	52	31	B2	5F	BE	A'A.\.:^.'eRl*_%
CDB0h	:	0E	03	Β7	83	CA	E2	03	BA	1A	13	8A	27	49	DA	7E	4C	fÊâ.°Š'IÚ~L
CDCOh	:	3B	F2	9C	15	14	2E	F1	87	9D	25	2E	6C	00	85	99	7A	;òœñ‡.%.l™z
CDD0h	:	F7	48	C9	A 8	3C	51	17	54	40	35	AB	54	D6	65	29	4E	+HE ^{**} <q.t@5«töe)n< td=""></q.t@5«töe)n<>
Output																		
		۵d	dree														Val	
		110 24b	3 00	cum	centro 50	as o Mh	030	46 U	304	•		_	_	_	_	_	_	
	CD4	4Ah			50	04b	0304	1										
	E79	6h			50	04b	0304	1										
+																		

⑤、kali的binwalk、foremost命令提取隐写在内的文件

如下图所示: binwalk 图片,发现了有压缩包的存在

		₩ binwalk Welcomejpg
DECIMAL	HEXADECIMAL	DESCRIPTION
0 30 ectory: 8 52516 size: 6732, 0	0x0 0x1E 0xCD24 uncompressed size	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image dir Zip crchive data, at least v1.0 to extract, compressed e: 6732, name: flag.rar
9264 47852	0xE780 0x2418C	End of Zip archive, footer length: 22 End of Zip archive, footer hengy/biog2csdn.net/qq_45555226



⑥、根据以上解压出的文件,有一个提示图片和一个加密了的压缩包

告诉你们一个秘密,密码是3个数哦。

查理曼:

查理曼, 法兰克王国国王, 征服了西欧与中欧大部分 土地, 具有了至高无上的权威, 下令全国人民信仰基 督教, 查理重振了西罗马帝国。 雅典娜: 女神帕拉斯·雅典娜, 是希腊神话中的女战神也是智慧 女神, 雅典是以她命名的。 兰斯洛特, 英格兰传说中的人物, 是亚瑟王圆桌骑士团中的一 员。看上去就是一个清秀年轻的帅小伙儿, 由于传说 中他是一名出色的箭手, 因此梅花J手持箭支。兰斯洛 特与王后的恋爱导致了他与亚瑟王之间的战争。 **Hint: 其实斗地主挺好玩的。**

https://blog.csdn.net/gq_45555226

👔 Ziperello		– 🗆 X
zip password recover	y tool	帮助 关于 退出
当前密码长度 当前密码 当前速度 0% 逝去时间: 00:00:00	3 信息 × 密码: 871 确定 开始	步骤 4 准备就绪,请点击 [开始] 按钮 注意:搜索进度条 (%) 及剩余时间字段显示的信息与当 前的密码效验长度相关。 破解 AES 算法加密的密码可能 耗时较长。
	步骤 4 / 4: 破解密码.Go	https://blog.csdn.ne /qष⊑≭500002

⑦、解压后得到一张图片:



https://blog.csdn.net/qq_45555226

又开始了图片隐写的套路。。。。

第一步:宽高和颜色没特殊的问题,略过

第二步:详细信息没特殊字符,略过

第三步:记事本打开,搜索结果和查看最下面的有无特殊字符

如下图所示: 搜索到最下面有flag: f1@g{eTB1lEFyZSBhlGhAY2tlciE=} //很明显是base64加密,我们解密即可得到: flag{y0u Are a h@cker!}

<u> <u> </u> <u> </u></u>	★ III - IIIk - III + II + II + II + II +	■ FRAm ▼ ・ 炉×邦・PQSOBEED2 EXQ^高端 涨娱EXD 茶JEOD 核MEDIEED SOBECOD;薄 蜗星<開e7 YO KEB<差(DE3 開<廠4斧<笙 KEB KESD SOBECOD;薄 蜗星<開e7 YO KEB<差(DE3 開 $SOBECOD;薄 蜗星<開e7 YO KEB<差(DE3 開SOBECOD;薄 蜗星<開e7 YO KEB<差(DE3 DE3 KEBSOBECOD;薄 蜗星<開e7 YO KEB SOBECOD;薄 蜗星<開き(SOBECD;7),第 SOBECOD;SOBECOD;500SO$
查找模式 ● 普通(い) ○ 扩展(2) (\n, \r, \t, \0, \x) ○ 正则表达式(G) □ 。匹配新行	 ✓ 透明度() ● 失去焦点后 ○ 始终 	h[F 2327)+2C3 EOT) 铤P232230001*絝吪 CCSUB澻62213:"F叟^詰切B\$B緣]4甯亏账菏糮 倭23380009j0Su92333B333CAN涂

刑 飜A用 059;细9*\$733次泣@MNk鞙s\卓概Dt永2737000>2336001登蟉@M222033;22504225573×233987820大腾 201057238,23495733凄‡ 63鞅 呜J2荒23390008枱驾程槽±刳508739;9355,Q2342796633躏p0340脓搧虹W早&惠*漲503 5733\\$D235

195/q嬴眸 20132 { \$ 漶 S 6013 夜 P 7 7207 (53繙 1220) 许杯 8 1000 鳖 in 2013 1021 1 糜 \$ n 0020 爱 i k A # 紱 2013 1213 1203

fl@g{eTBlIEFyZSBhIGhAY2tlciE=}

Base64:	(
eTB1IEFyZSBhIGhAY2ttciE=	用#223 Base64
解密Base64:	
y0u Are a h@cker!	

0x03、Flag

flag{y0u Are a h@cker!}