图片隐写类简单思路介绍

原创

Deeeelete 于 2020-02-27 10:21:47 发布 717 收藏 3

分类专栏： ctf

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/Deeeelete/article/details/104529886

版权

ctf 专栏收录该内容

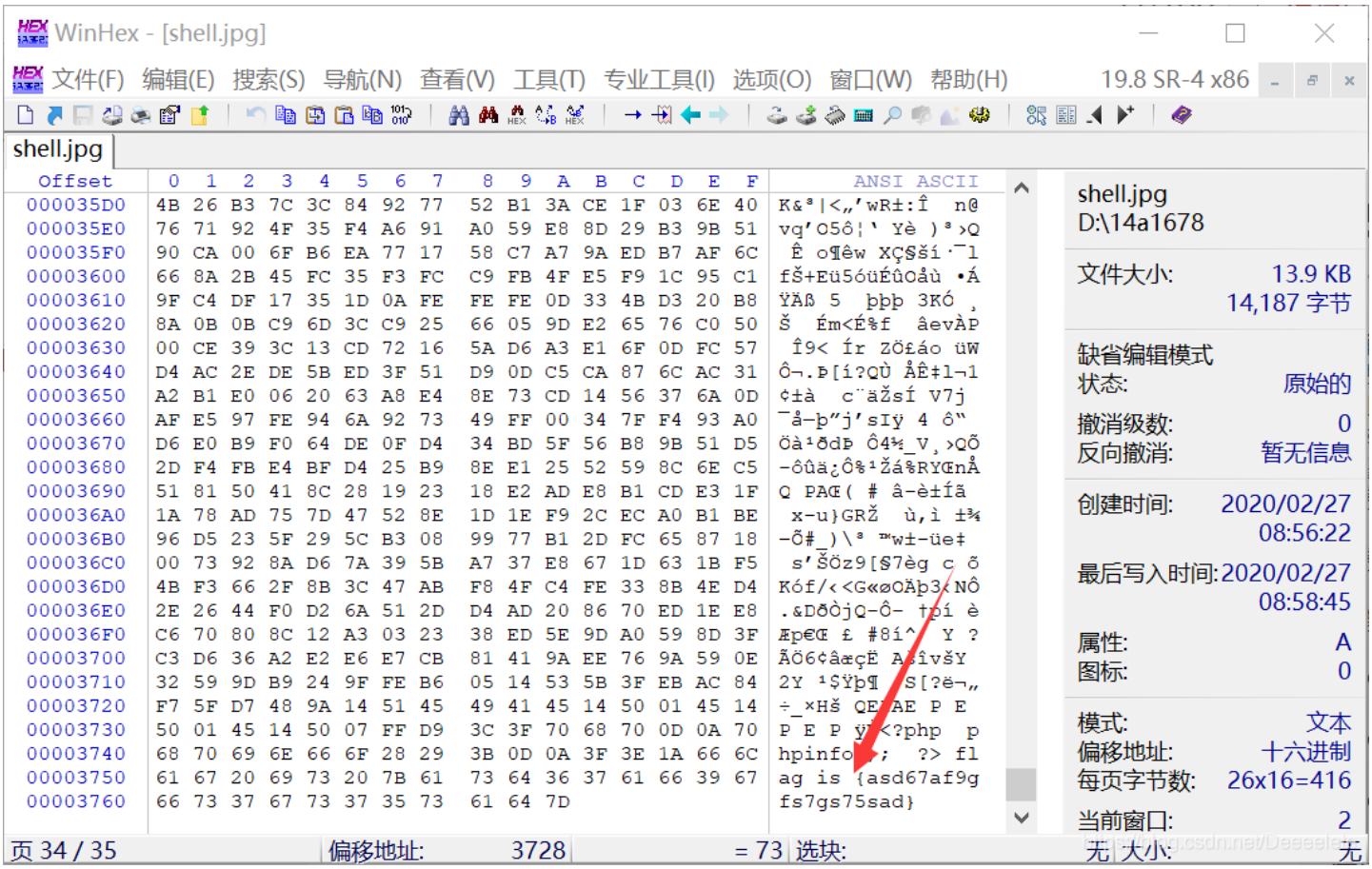
12 篇文章 0 订阅

订阅专栏

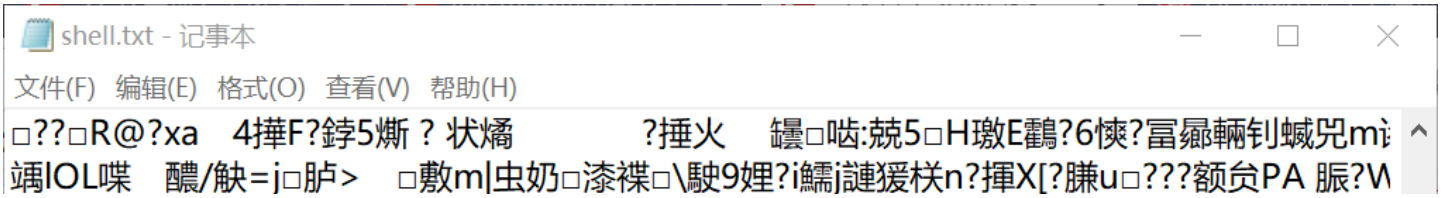
1.图片+文本隐写

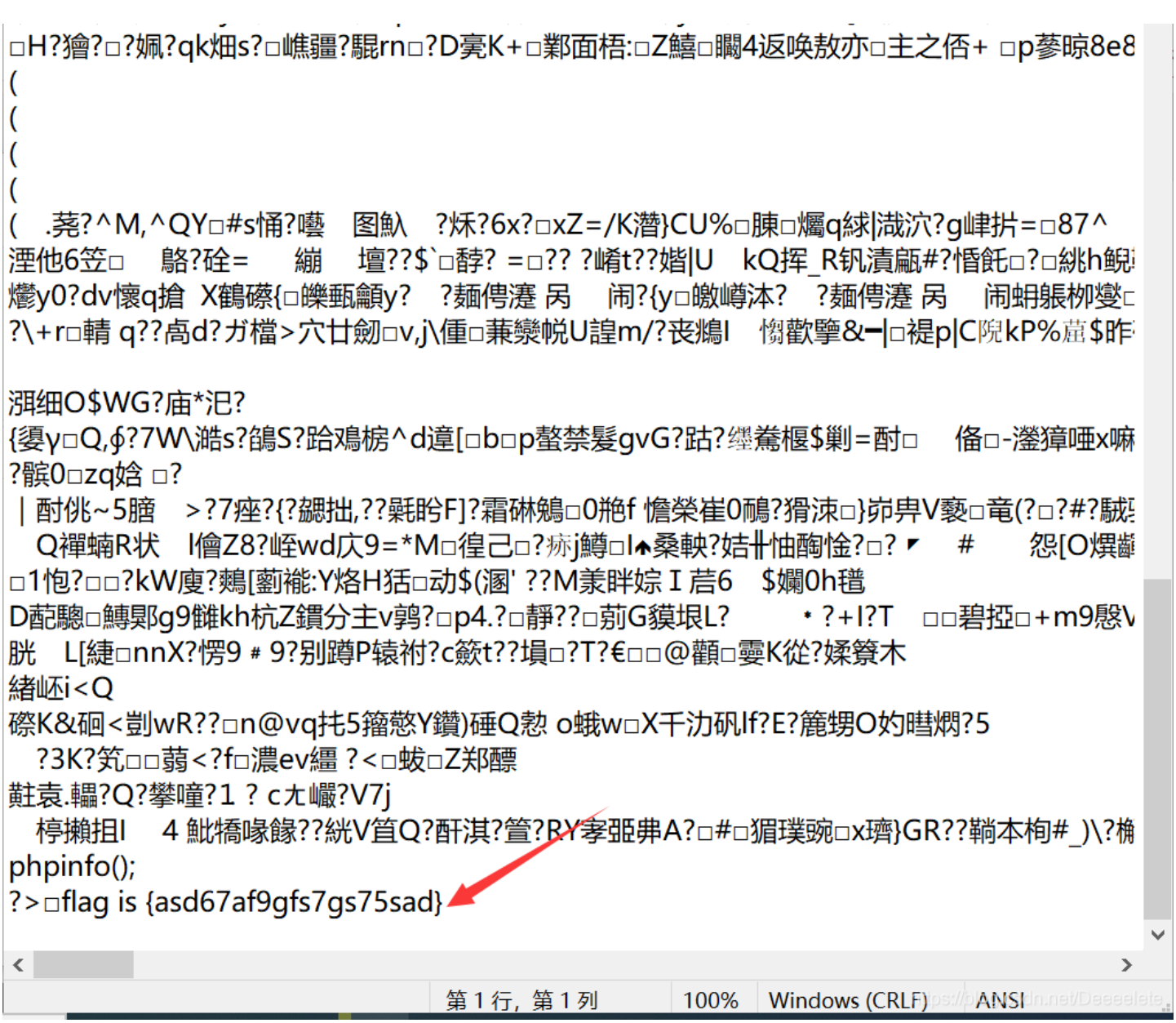
格式：内嵌着txt文本的jpg或者png图片

解决：直接winhex找，如果只是简单的txt文本嵌入，那应该能在最后的位置看到隐藏的明文信息。



或者直接把疑似的图片修改成txt格式，拉到最后就能找到。

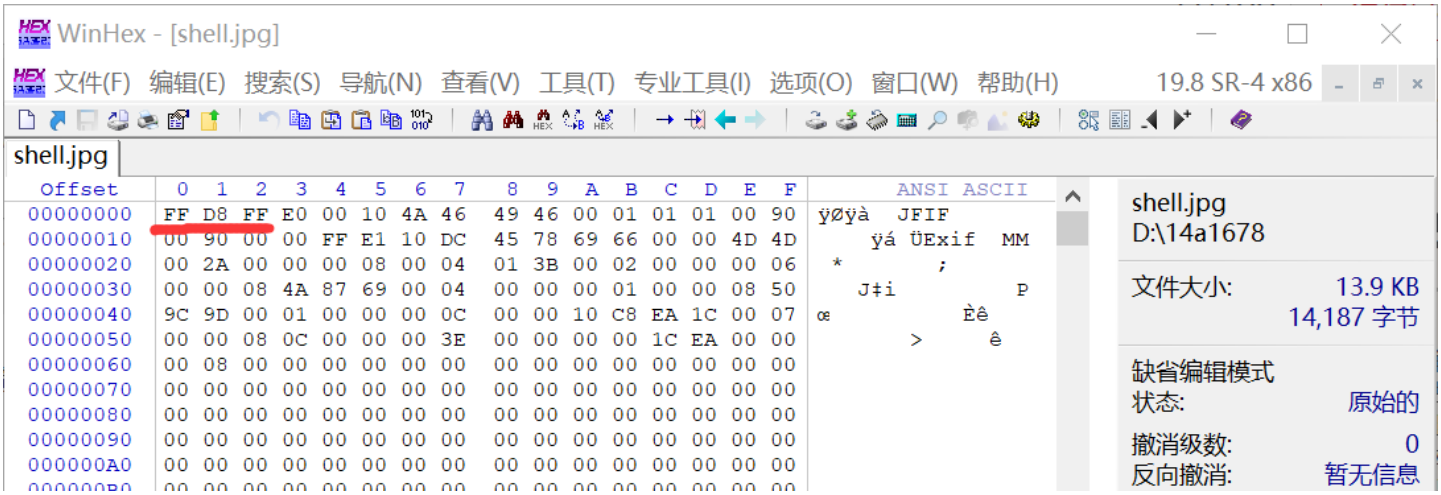


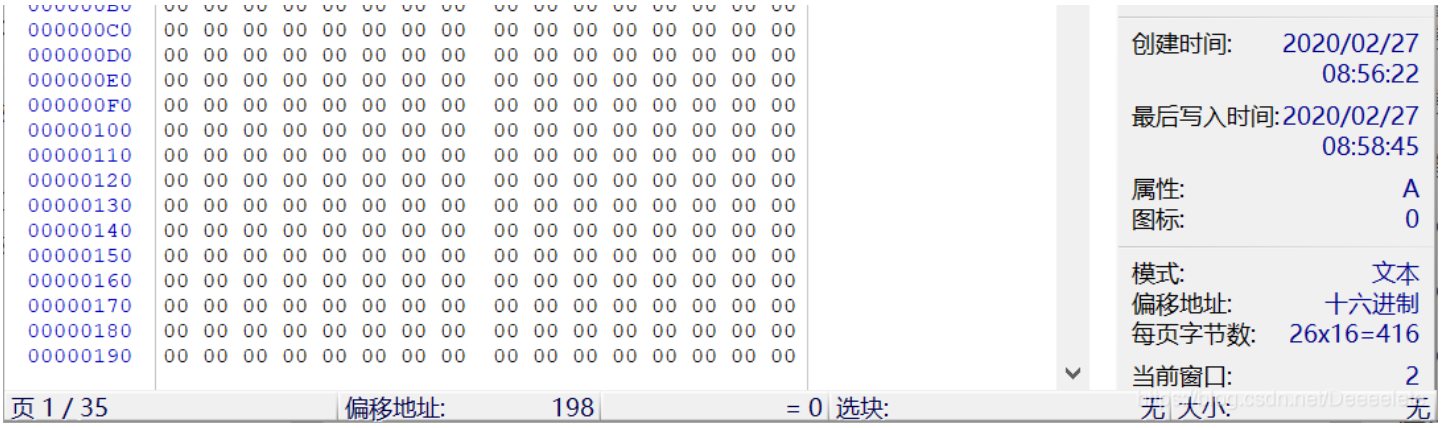


如果这两种方法都看不出明文，那也可以通过winhex简单查看一下该文件是否真的隐藏了信息。

(jpg) 文件头：FFD8FF　　文件尾：FF D9
(png) 文件头：89504E47　　文件尾：AE 42 60 82
(gif)　文件头：47494638　　文件尾：00 3B

还有更多的文件头文件尾这里就不再一一列举了，而文件头文件尾的意思是，如果用winhex打开一个正常的jpg格式的文件，那文件的开头就会以FFD8FF作为开始。





然后以FFD9作为结束

shell.jpg | IMG_20200222_154046.jpg

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0021DA20	A5	65	65	53	4F	0D	AE	43	31	23	1E	A1	7D	FB	50	23	¥eeSO ®C1# ¡}ûP#
0021DA30	88	FE	28	44	16	23	93	CD	65	65	2E	A2	E6	2B	BA	66	ˆþ(D #"Íee.¢æ+°f
0021DA40	EC	6E	8C	00	C7	A5	1E	19	7C	D6	12	85	0B	74	C7	F4	ìnŒ Ç¥ |Ö … tÇô
0021DA50	AC	AC	AD	A6	13	D4	6B	DA	E7	6C	90	C0	ED	28	EB	97	¬¬-¦ ÔkÚçl Àí(ë—
0021DA60	36	A7	42	A2	E2	CB	61	85	9A	B2	B2	92	F9	25	72	6C	6§B¢âËa…š²²'ù%rl
0021DA70	DA	5B	2C	61	6F	90	37	1B	F4	A8	0E	B8	AA	86	8A	FB	Ú[,ao 7 ô¨ ¸ª†Šû
0021DA80	F2	0E	F5	95	94	D5	9E	24	FA	82	E9	95	96	E7	D6	A3	ò õ•"Õž$ú,é•–çÖ£
0021DA90	9F	AA	AD	22	2C	C4	59	58	A7	7B	EE	2B	2B	2A	69	9A	Ÿª-",ÄYX§{î++*iš
0021DAA0	A8	C5	26	B2	DC	0D	C1	EF	57	30	8B	69	B1	11	A0	05	¨Å&²Ü ÁïW0‹i±
0021DAB0	41	27	FA	7E	D5	95	94	2B	5E	79	95	4A	BC	69	2C	BE	A'ú~Õ•"+^y•J¼i,¾
0021DAC0	54	09	60	C0	80	7A	D3	F5	5A	D6	63	23	C2	02	5F	D3	T `À€zÓõZÖc#Â _Ó
0021DAD0	61	B5	65	65	07	03	4F	A7	93	30	48	56	25	4D	C9	3C	aµee O§"0HV%MÉ<
0021DAE0	55	5E	A1	D2	2D	A4	8B	2D	ED	B5	65	65	6D	72	E7	45	U^¡Ò-¤‹-íµeemrçE
0021DAF0	8F	50	C6	73	1B	FA	87	01	BA	8A	B8	B3	65	E5	B1	C0	PÆs ú‡ °Š¸³eå±À
0021DB00	05	BD	EB	2B	2A	EA	52	56	7A	5F	13	29	8E	95	55	99	½ë+*êRVz_)Ž•U™
0021DB10	95	6F	90	EB	55	FA	CD	43	6A	9E	54	50	C1	76	B9	CB	•o ëUúÍCjžTPÁv¹Ë
0021DB20	7A	CA	CA	9D	D9	33	CA	AA	31	28	66	5C	AF	DB	DA	8A	zÊÊ Ù3Ê ª1(f\¯ÛÚŠ
0021DB30	59	53	EA	24	0F	DE	B2	B2	A7	3C	E4	D7	C3	FF	D9		YSê$ Þ²²§<ä×ÃÿÙ

https://blog.csdn.net/Deeeelete

如果发现

在文件尾后面还有内容，那说明该文件可能夹带私货。

shell.jpg

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
000035D0	4B	26	B3	7C	3C	84	92	77	52	B1	3A	CE	1F	03	6E	40
000035E0	76	71	92	4F	35	F4	A6	91	A0	59	E8	8D	29	B3	9B	51
000035F0	90	CA	00	6F	B6	EA	77	17	58	C7	A7	9A	ED	B7	AF	6C
00003600	66	8A	2B	45	FC	35	F3	FC	C9	FB	4F	E5	F9	1C	95	C1
00003610	9F	C4	DF	17	35	1D	0A	FE	FE	FE	0D	33	4B	D3	20	B8
00003620	8A	0B	0B	C9	6D	3C	C9	25	66	05	9D	E2	65	76	C0	50
00003630	00	CE	39	3C	13	CD	72	16	5A	D6	A3	E1	6F	0D	FC	57
00003640	D4	AC	2E	DE	5B	ED	3F	51	D9	0D	C5	CA	87	6C	AC	31
00003650	A2	B1	E0	06	20	63	A8	E4	8E	73	CD	14	56	37	6A	0D
00003660	AF	E5	97	FE	94	6A	92	73	49	FF	00	34	7F	F4	93	A0
00003670	D6	E0	B9	F0	64	DE	0F	D4	34	BD	5F	56	B8	9B	51	D5
00003680	2D	F4	FB	E4	BF	D4	25	B9	8E	E1	25	52	59	8C	6E	C5
00003690	51	81	50	41	8C	28	19	23	18	E2	AD	E8	B1	CD	E3	1F
000036A0	1A	78	AD	75	7D	47	52	8E	1D	1E	F9	2C	EC	A0	B1	BE
000036B0	96	D5	23	5F	29	5C	B3	08	99	77	B1	2D	FC	65	87	18
000036C0	00	73	92	8A	D6	7A	39	5B	A7	37	E8	67	1D	63	1B	F5

```
000036D0  4B F3 66 2F 8B 3C 47 AB  F8 4F C4 FE 33 8B 4E D4
000036E0  2E 26 44 F0 D2 6A 51 2D  D4 AD 20 86 70 ED 1E E8
000036F0  C6 70 80 8C 12 A3 03 23  38 ED 5E 9D A0 59 8D 3F
00003700  C3 D6 36 A2 E2 E6 E7 CB  81 41 9A EE 76 9A 59 0E
00003710  32 59 9D B9 24 9F FE B6  05 14 53 5B 3F EB AC 84
00003720  F7 5F D7 48 9A 14 51 45  49 41 45 14 50 01 45 14
00003730  50 01 45 14 50 07 FF D9  3C 3F 70 68 70 0D 0A 70
00003740  68 70 69 6E 66 6F 28 29  3B 0D 0A 3F 3E 1A 66 6C
00003750  61 67 20 69 73 20 7B 61  73 64 36 37 61 66 39 67
00003760  66 73 37 67 73 37 35 73  61 64 7D
```

https://blog.csdn.net/Deeeelete

2.图片+图片隐写

格式：多图片复合，而且用winhex查看也是正常的文件头文件尾

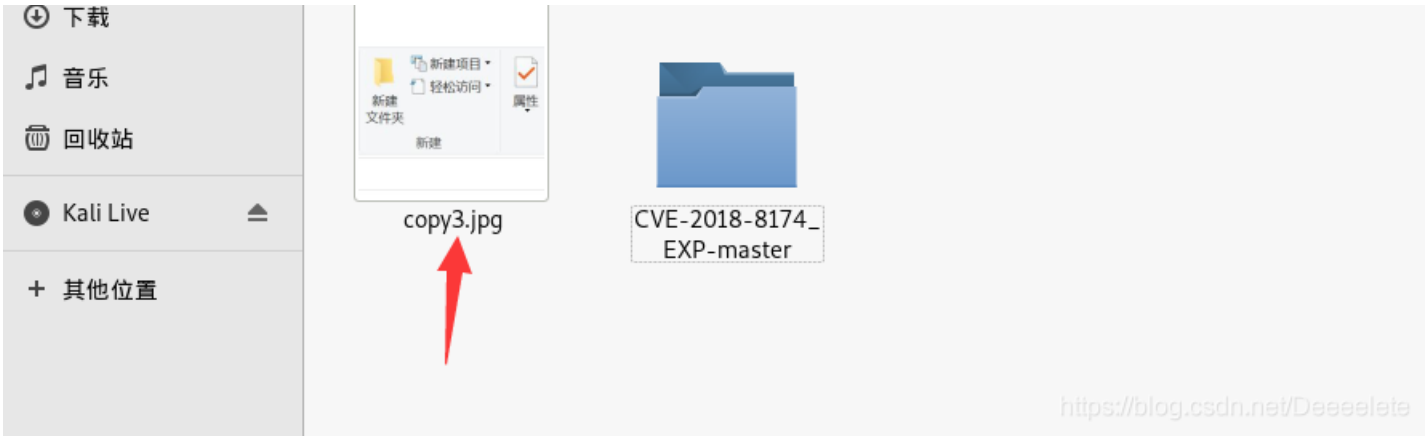
解决：利用kali下的Foremost，但使用之前需要先装一下

```
apt-get install foremost
```

```
root@kali2019:~# apt-get install foremost
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
下列软件包将被升级：
  foremost
升级了 1 个软件包，新安装了 0 个软件包，要卸载 0 个软件包，有 2057 个软件包未被升级。
需要下载 0 B/42.1 kB 的归档。
解压缩后会消耗 1,024 B 的额外空间。
读取变更记录(changelogs)... 完成
(正在读取数据库 ... 系统当前共安装有 374674 个文件和目录。)
准备解压 .../foremost_1.5.7-9+b1_amd64.deb  ...
正在解压 foremost (1.5.7-9+b1) 并覆盖 (1.5.7-8) ...
正在设置 foremost (1.5.7-9+b1) ...
正在处理用于 man-db (2.8.5-1) 的触发器 ...
root@kali2019:~#
```

https://blog.csdn.net/Deeeelete

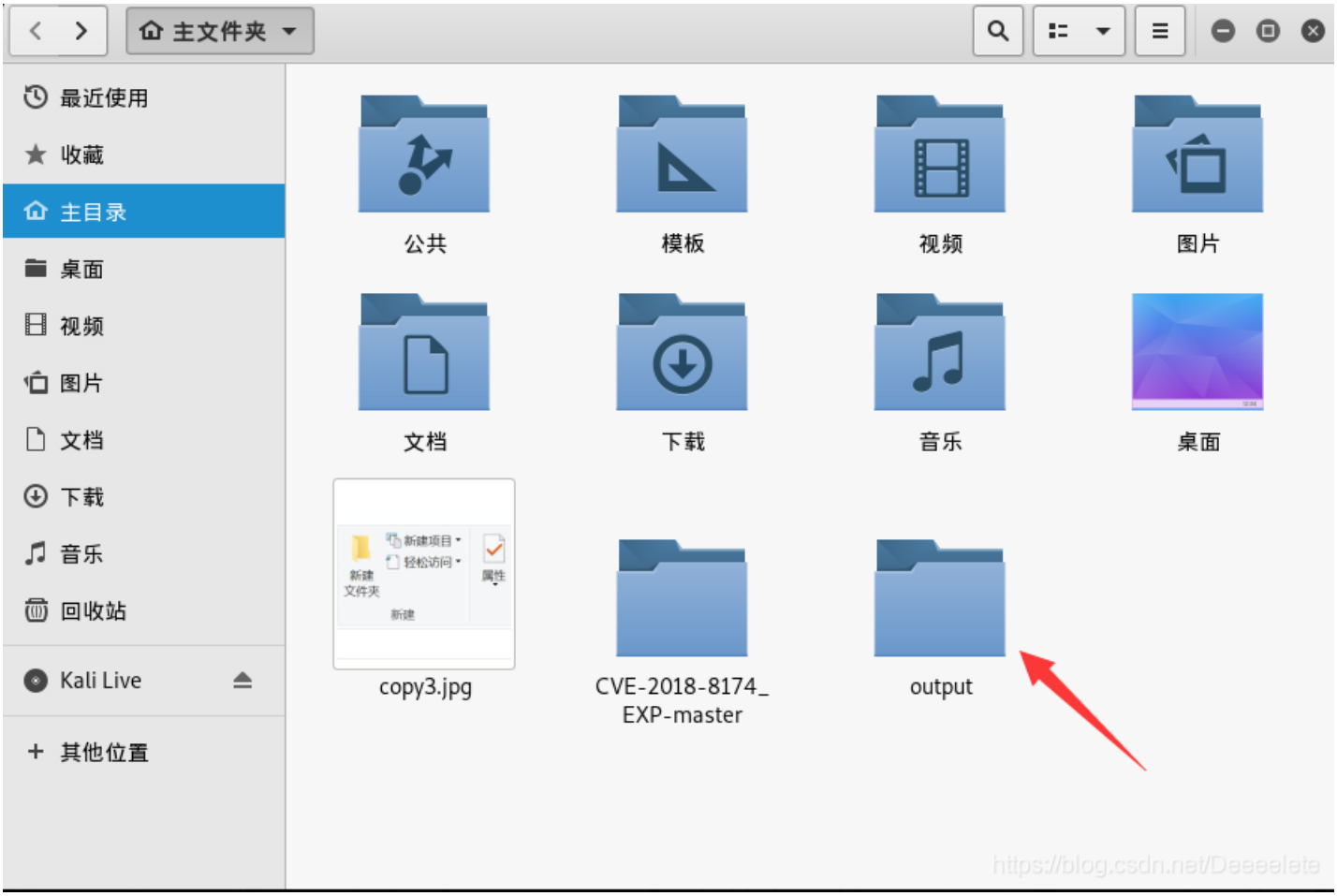
然后就是把我们需要的文件拖进kali



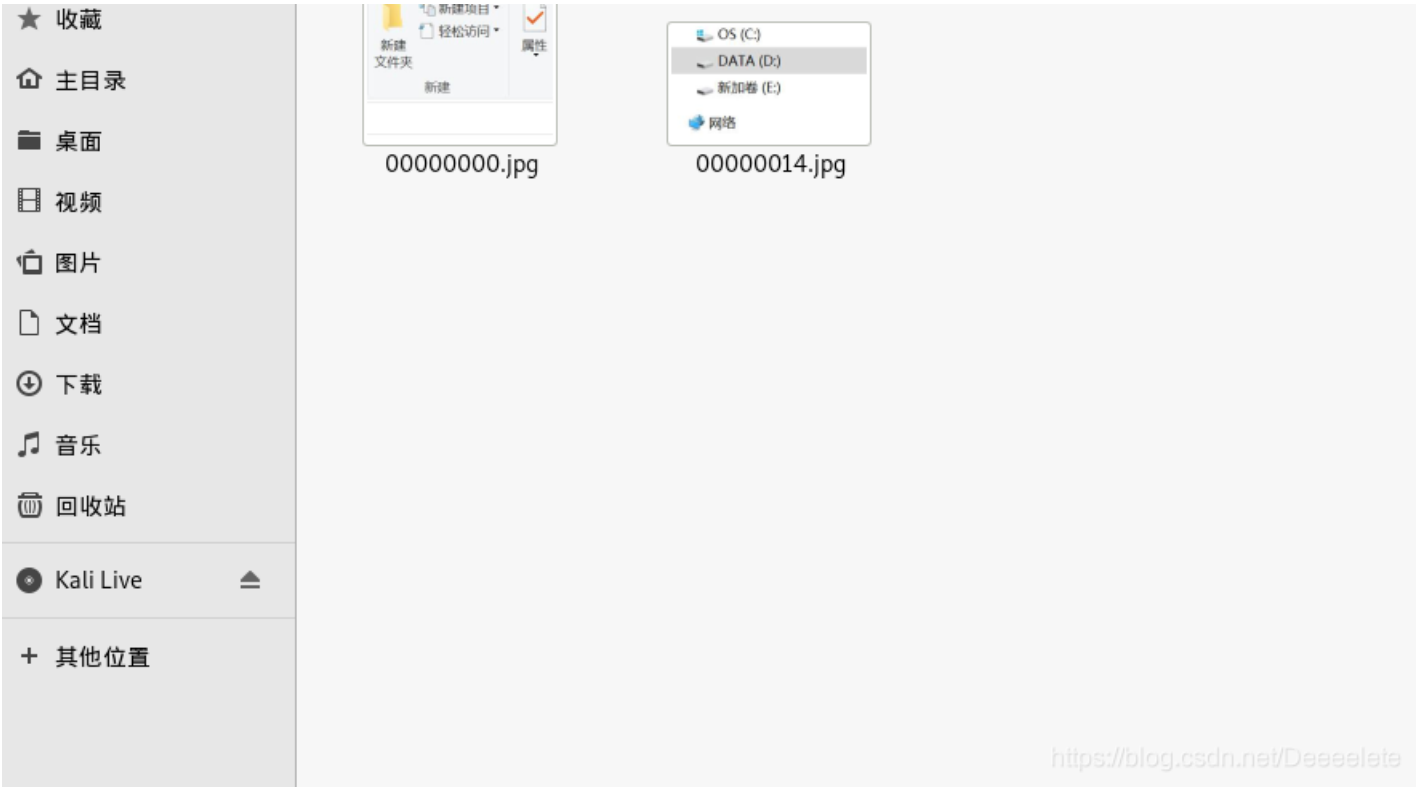
空白处右击在终端打开

输入命令 `foremost -i copy3.jpg` (-i参数后指定自己的文件名)

然后回到我们保存copy3图片的界面，发现多给了一个output文件夹



这个文件夹里就保存着我们分离出来的图片了。



3.GIF帧隐藏

格式：往往是动态图在播放的时候忽然有一帧异样的图片闪过，但闪过的太快无法彻底看清。

解决：ps

（ps这里就不多讲了，直接打开扔进去在图层里找就行。）