

Misc-登机牌[i春秋][150pt]

原创

将至将至 于 2018-09-02 15:26:00 发布 825 收藏 1

分类专栏: [CTF-Misc](#) 文章标签: [Misc Winhex](#)

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/Laurel_60/article/details/82315851

版权









[CTF-Misc 专栏收录该内容](#)

4 篇文章 1 订阅

订阅专栏

首先, 拿到的是这样的一张登机牌图片--

Ivan Boyko		June 5, 2016	 Lufthansa
LH 907 to Frankfurt	Boarding 9:10 AM	Seat A22	 Window
	Gate D10		Departing 9:40 AM 
		In Frankfurt take Sky Train to Terminal 1 <small>https://blog.csdn.net/Laurel_60</small>	

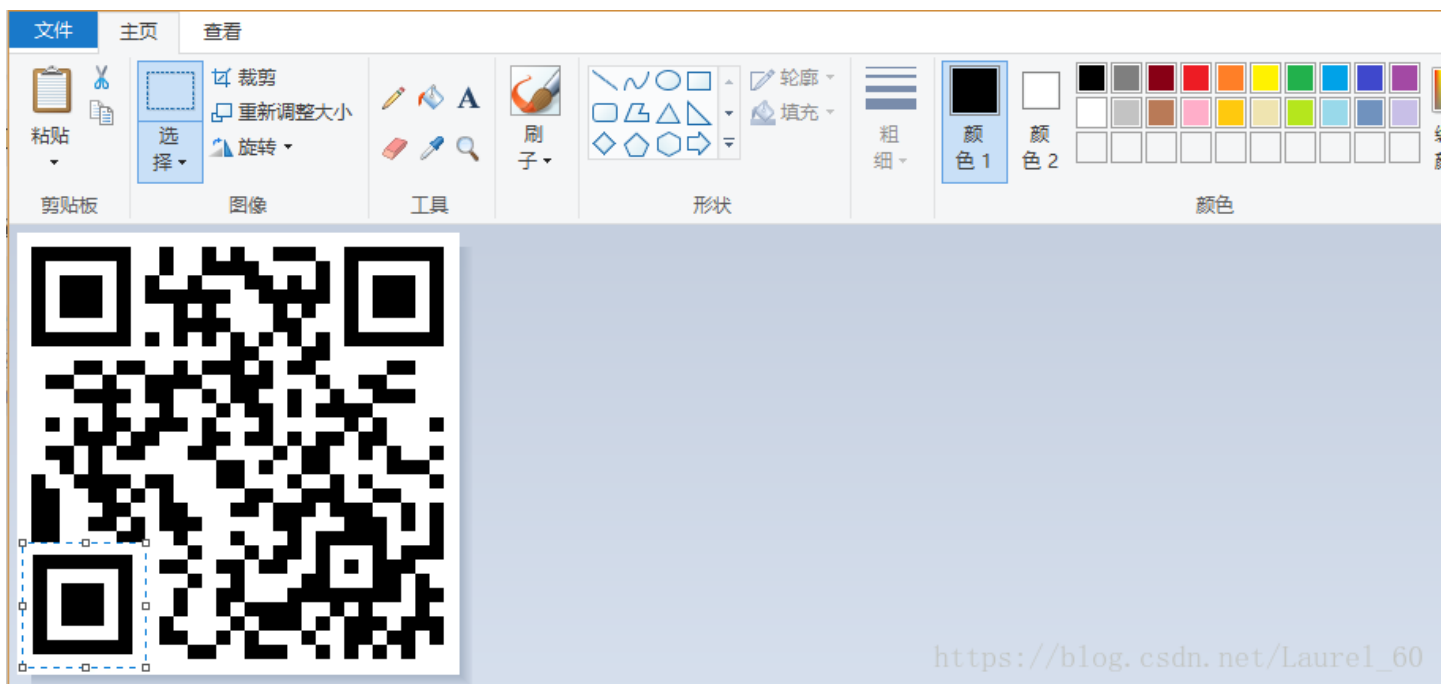
第一眼看到的就是图片中的二维码, 三个重要部位都被漂亮的小姐姐挡住了, 所以首先想到的就是把这个二维码还原。

[\[+\]Back](#)

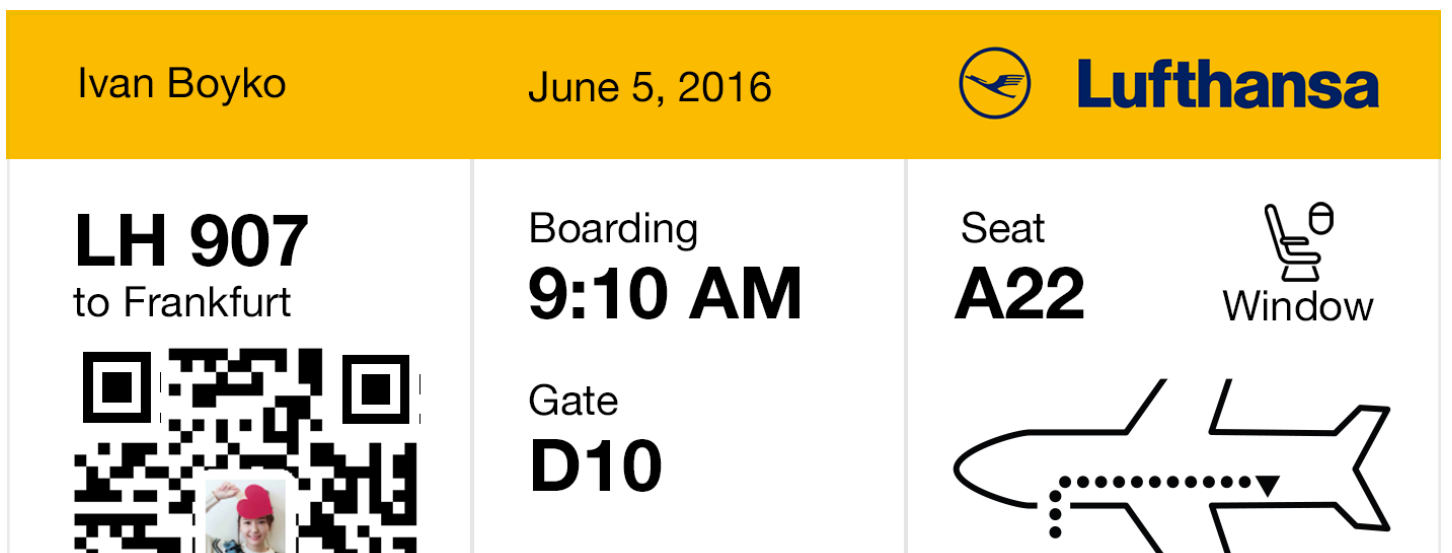
因为之前也刷过类似的二维码题目，名字是单身狗，当时给出的图片如下--



只需要用画图随便剪下一块粘贴过来，将狗狗覆盖就可以扫了，可以扫扫试试。。。



而我在还原这道题目的二维码时，先还原成了这个样子，死活扫不出来2333--






Boarding priority
1 2 **3** 4

Departing 9:40 AM ✈




In Frankfurt
take Sky Train to Terminal 1
https://blog.csdn.net/Laurel_60

对二维码的构造不是很了解，看多了就知道，三个大方块外面的黑边应该和中间内容的边是对齐的，如下所示--

Ivan Boyko June 5, 2016  **Lufthansa**

LH 907
to Frankfurt




Boarding
9:10 AM


Gate
D10

Boarding priority
1 2 **3** 4


Seat
A22



Window



Departing 9:40 AM ✈



In Frankfurt
take Sky Train to Terminal 1
https://blog.csdn.net/Laurel_60

颜值都变高了有木有。。。扫码后给的提示是，你咋不用binwalk？
好，那我们就用 *Binwalk* 分析看看！然鹅--

```
D:\Binwalk>binwalk ticket.png
* suggest: you'd better to input the parameters enclosed in double quotes.
* made by pcat

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          PNG image, 1416 x 833, 8-bit/color RGBA, non-interlaced
15164       0x3B3C       Zlib compressed data, best compression
https://blog.csdn.net/Laurel\_60
```

exo me? 好像没什么特别的，把它分开之后看了几遍也没找到有用信息。
刷wp说里面藏有压缩包，那再用 *Winhex* 打开看看。
搜索 *rar*，就可以看到--

```
00201680 08 82 20 08 82 20 08 82 20 08 82 B8 40 21 81 98  , , , , , @! ~
00201696 20 08 82 20 08 82 20 08 82 20 08 82 20 08 E2 02  , , , , ,  a
00201712 85 04 62 82 20 08 82 20 08 82 20 08 82 20 08 82  ... b, , , , ,
00201728 20 88 08 14 12 88 09 82 20 08 82 20 08 82 20 08  ^
00201744 82 20 08 82 20 2E 50 FE FF 01 00 2F 44 C0 0F 3C  , , , .Ppy /DÅ <
00201760 29 D0 B0 00 00 00 00 49 45 4E 44 AE 42 60 82 52  )D° IEND&B`,R
00201776 41 52 21 1A 07 00 CF 80 73 00 00 0D 00 00 00 00  a! t e
```

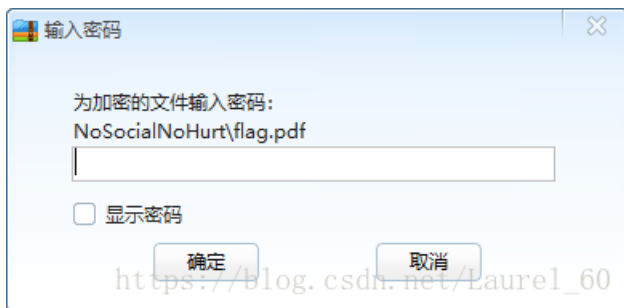

骚年

来包卫龙冷静一下吧



https://blog.csdn.net/Laurel_60

终于! --



密码在哪里找? 回到原来的登机牌, 咱们还有一个条形码没有处理过--

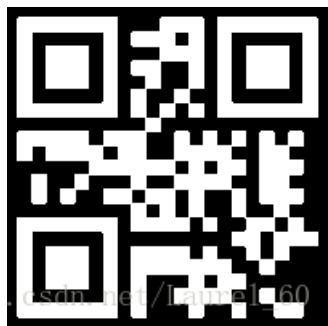


这码看着怪怪的, 扫不出东西, 跟普通的条形码一对比, 嗯原来是反相了, 那我们就反回来吧--



[+]Back

曾经也遇到过反相的二维码，原图是这样--



扫不出来，二维码不标准，反相一下--



常识啊，都是常识！

回到原来的题目，拿在线网站扫描一波--

解码结果：

Key1921070120171018

https://blog.csdn.net/Laurel_60

顺便附上扫码网站-- <http://jiema.wwei.cn/>

拿到key之后就可以去解压缩包了,解开之后是这样滴--



The screenshot shows a Baidu search interface. The search bar contains the text "乱晒登机牌的危害". Below the search bar, there are navigation tabs for "网页", "新闻", "贴吧", "知道", "音乐", "图片", "视频", "地图", "文库", and "更多". The search results section shows "百度为您找到相关结果约2,390个" and a search tool icon. The first result is titled "太恐怖!千万不要在朋友圈晒登机牌 - 站长之家". It includes a small image of a person holding a boarding pass, a text snippet: "2016年12月30日 - 朋友圈晒旅行的方式有很多种,有晒当地美景的,有晒当地美食的,还有一种,是晒登机牌的。很多人喜欢在出行时拍下登机牌晒到朋友圈,殊不知,你的一大...", and a link to "www.chinaz.com/news/20...". To the right of the link is the text "百度快照" and a URL "https://blog.csdn.net/Laurel_60".

在文章的末尾可以看到flag -

flag{Car3_Y0ur_Secret}

https://blog.csdn.net/Laurel_60

所以, 这道题告诉了我们--

不要乱晒登机牌



OVER—