

Misc

The Hungry Dragon

这题让你求龙吃了多少个糖和甜甜圈，初始文件是个 3D 建模文件：



观察一圈发现龙嘴巴里有东西：

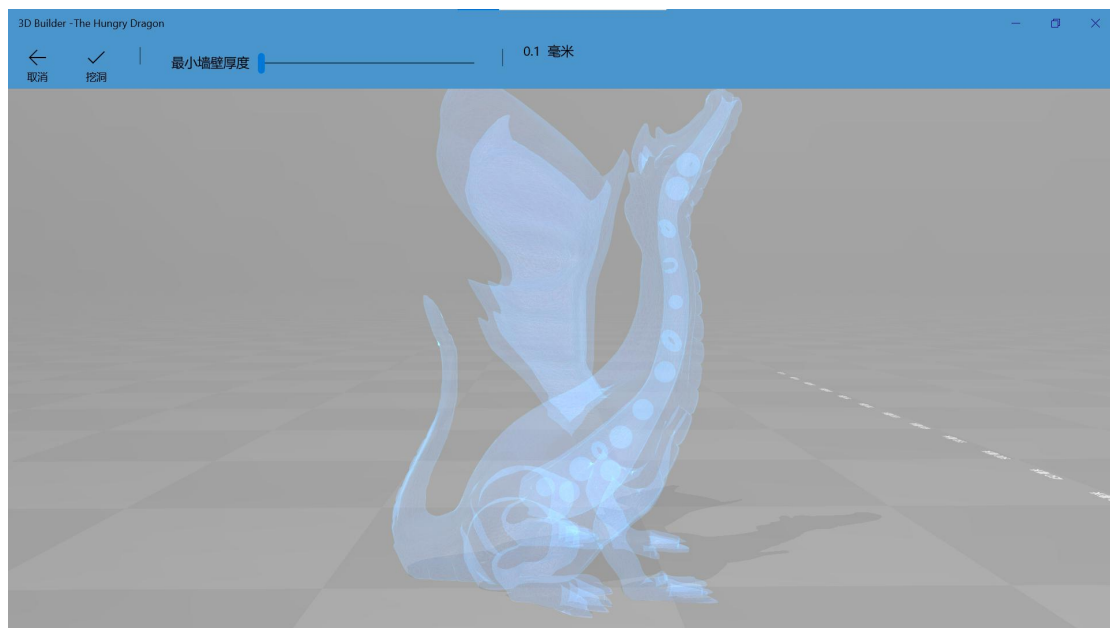


所以把这龙拆开应该就可以看到要找的东西。这里需要下载一个能够拆分模型
的软件，Windows 自带的 3D 画图没用。网上看了一圈发现 3D builder 挺合适。
接下来就是拆分这条龙，当时做的时候采用的是拆分功能（用一个剖面将物体拆

成两半)，效果如下：



这种方法不太好找剖面，因为这条龙肚子里的东西位置不是很对称，剖面找不好容易漏，后面写这个文档时又研究了一下，发现了另一个功能也挺好用，叫挖洞：



点进这个界面，啥不干就可以看到物体内部。

最后数一下就可以得出答案。

总结

这题估计考察的是处理新类型文件的能力和搜索资料的能力。难点在于怎样快速

上手一个没见过的玩意儿，大概只能在以后的练习里慢慢积累经验吧。

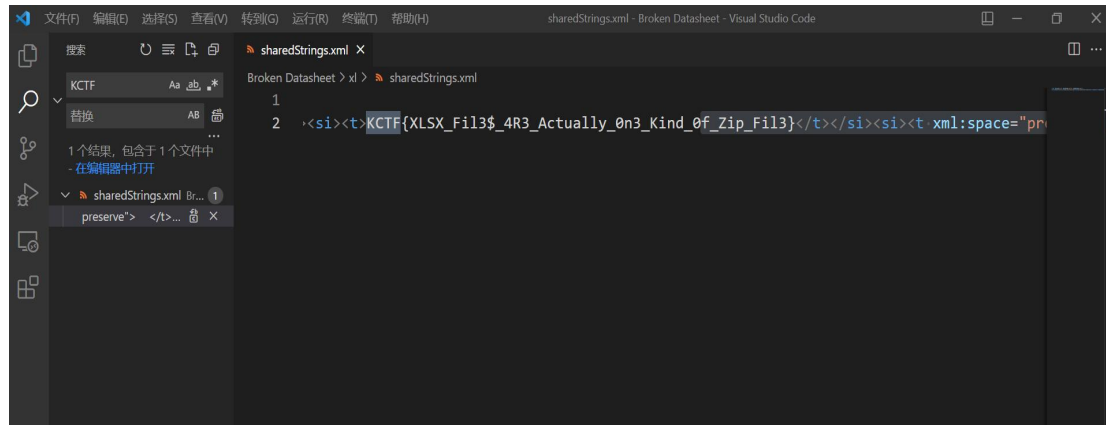
Broken Datasheet

这题让你修复一个损坏的 xlsx 文件（excel 表格）

先用 excel 自带的修复功能试试，果然没用。网上查了下资料发现 xlsx 可以用 winhex 修复，看了一眼教程发现及其复杂，涉及到 excel 文件结构和分盘之类的知识。看了半天没看懂，去偷偷瞄了一眼题解，原来根本不是这个方向。

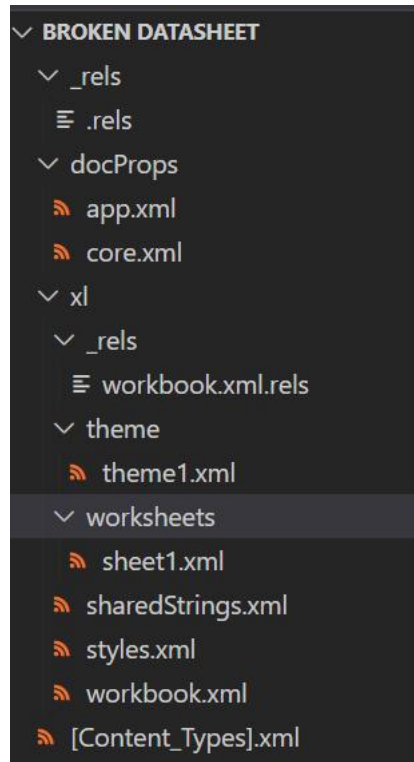
xlsx 文件和下面有道题中的 kra 文件类似，可以把后缀直接改为 zip 然后解压。解压后会发现 xlsx 由许多 xml 文件和几个 rels 文件组成。这道题里的 xlsx 解压出来后，文件夹里还有一个 xlsx，用同样的方法将其后缀改为 zip 再解压，解压后整个文件夹只剩 xml 和 rels 文件。

将此时的文件夹在 VS code 中打开，直接搜索 KCTF 即可：



总结

这道题主要考察 xlsx 的结构。当然用 winhex 修复文件还是要学一手，以后说不定用得到。一个 xlsx 文件的结构大致如下：



当然也存在xlsx里面还有xlsx的情况，这里只展示比较基本的结构。要解析数据一般只看以下几个文件：

xl/workbook.xml 包含表中的sheet数量名字和对应id

xl/_rels/workbook.xml.rels 通过上面xml的id找到对应的主xml

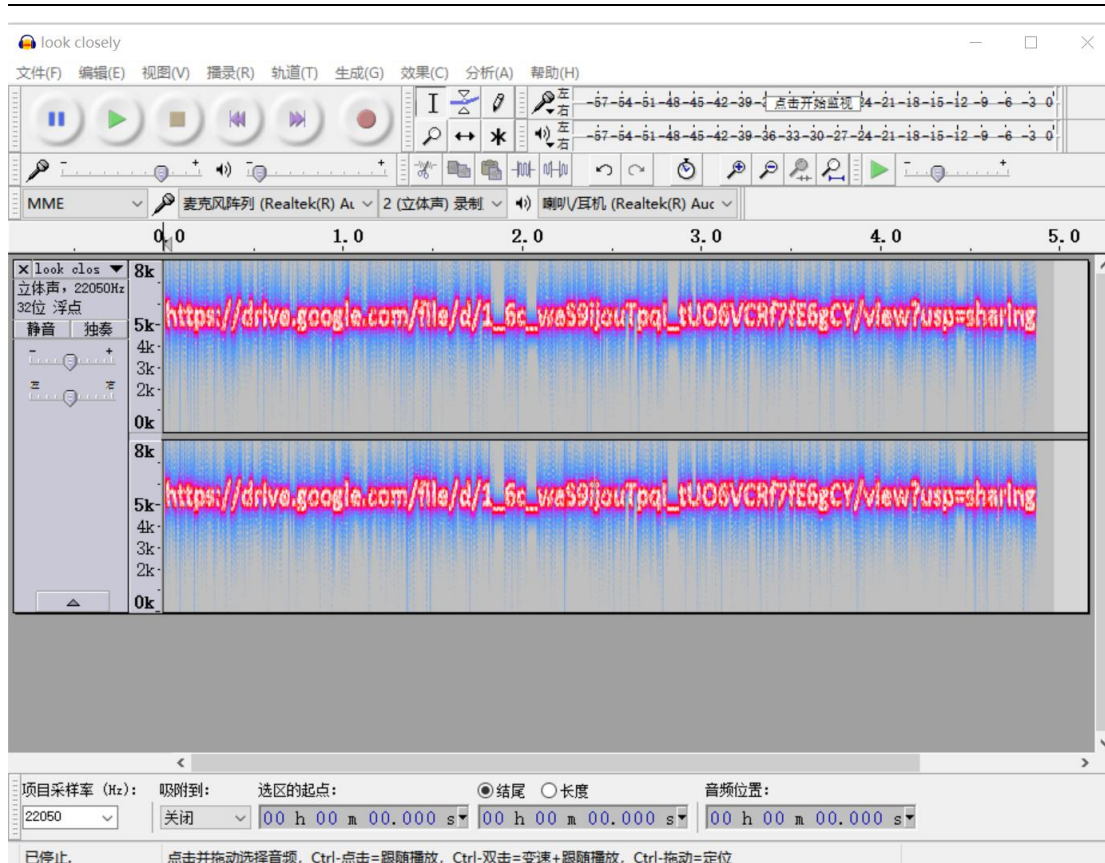
xl/worksheets/sheet{N}.xml 存储表中具体数据，只包含数字部分，文本内容根据索引到下面的xml中找

xl/sharedStrings.xml 存储的是表中字符串的内容，与上面的文件对应组成完整数据。

后续我会进一步学习xlsx这类文件的相关知识。

Unzip me

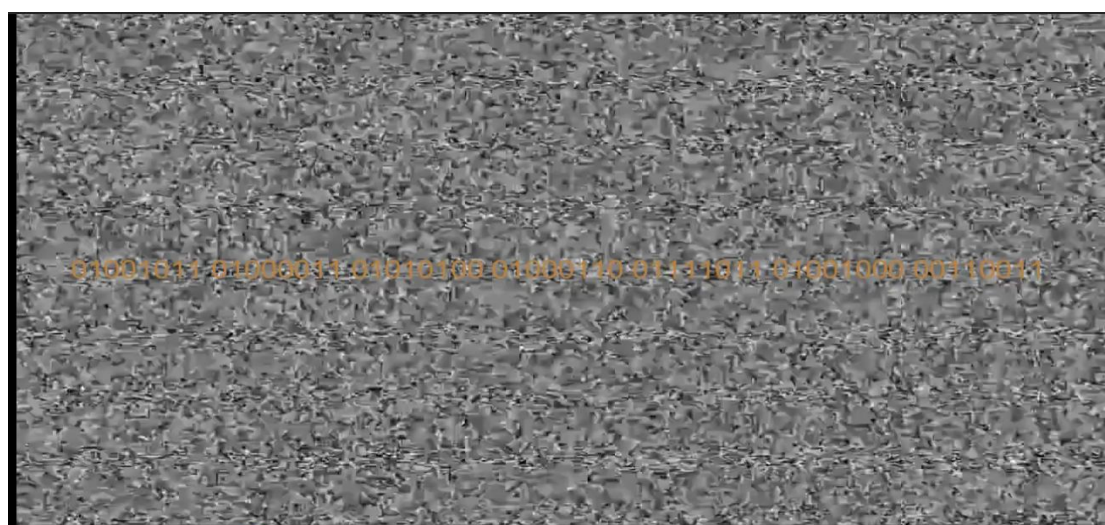
这题让你解压一个压缩包，我以为是设置了密码，让我暴力破解，结果直接解压就完事了，无事发生，解压出的文件夹里只有一个未知格式的文件。直接记事本伺候，打开是这样的：



很明显是个网址，输入网址即可。

输入网址时注意区分大写 i 和小写 l，即 l 和 l，在这个频谱里 i 和 l 其实也挺难分辨，最后经过枚举终于成功进入了网站。

网站是谷歌网盘，还得翻个墙，网盘里是一段视频，视频是长达一分钟的雪花，出这题的批人眼睛一定很好吧，第 13 秒处图像如下：



第 52 秒处图像如下：



仔细观察发现这串二进制数每隔 8 位有小小的间隙，因此以 8 位二进制数为一组进行分析，第一反应是 ASCII 码，查表后得到 flag。

总结：

这题属于音视频隐写，最大的感受是一定要准备好顺手的软件。好的工具非常重要（包括翻墙软件）。Ctfhub 和 ctfwiki 上都有对于各种工具的推荐，平时应当下载下来好好研究。

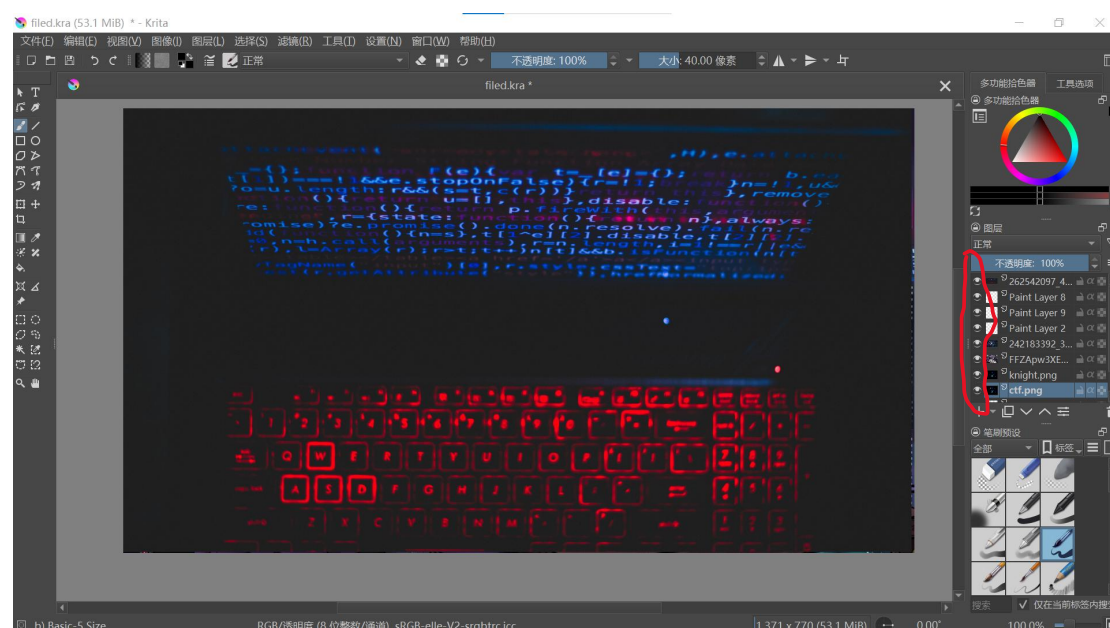
隐写是非常重要的题型，今后应当在此下大功夫。同时隐写也与解码紧密挂钩，需要进行一定的知识储备。

Steganography

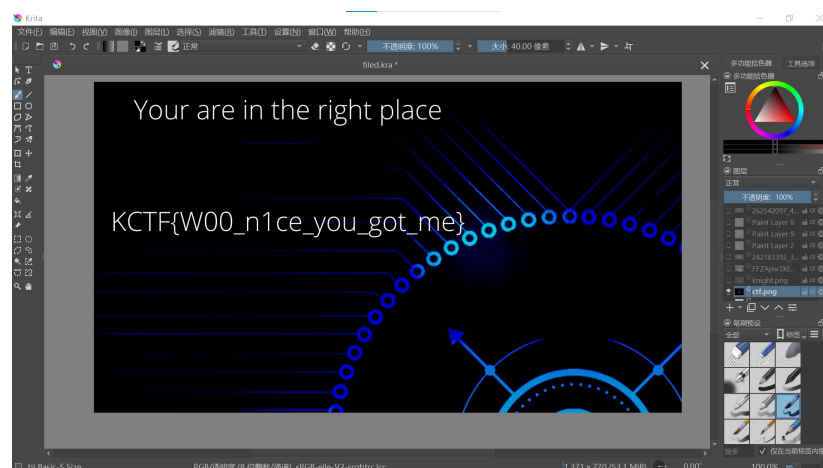
FileD

这题开始给了个 kra 文件，网上查了下发现是 Krita 软件产生的格式。这文件有意思的地方在于可以直接将 kra 后缀改为 zip，解压后可以看见源文件。但是这种方法找不到 flag，只能乖乖下载 krita。

Krita 是个画图软件，打开题目给的文件，效果如下：



刚打开人直接麻了，好在是个 25 分的题大概不会刁难人。仔细观察发现这个文件图层很多，flag 可能隐藏在某个图层里。经过一通操作发现上图红色圆圈位置的按钮可以隐藏图层，隐藏几个图层后果然发现了 flag：



总结

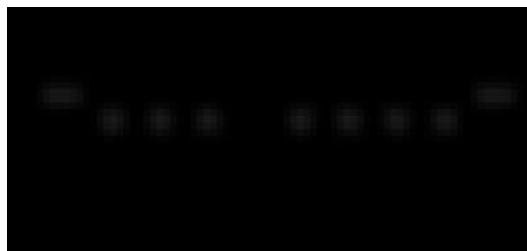
这题类似于那个 hungry dragon, 考察对于新事物的上手能力, 想到图层里藏 flag
属于生活经验, 没啥可总结的。

Follow The White Rabbit

一上来给了张图:



放大之后隐隐约约看见有些点:



直接掏出无敌的 PS 对其进行一波渐变处理:



这个有长有短的估计是摩斯电码, 翻译结果如下:

LOOK B4 Y0U L34P

LOOK B4 U LEAP

按照意思拆分了一下，发现怎么填都不对，加下划线也没用，懵了

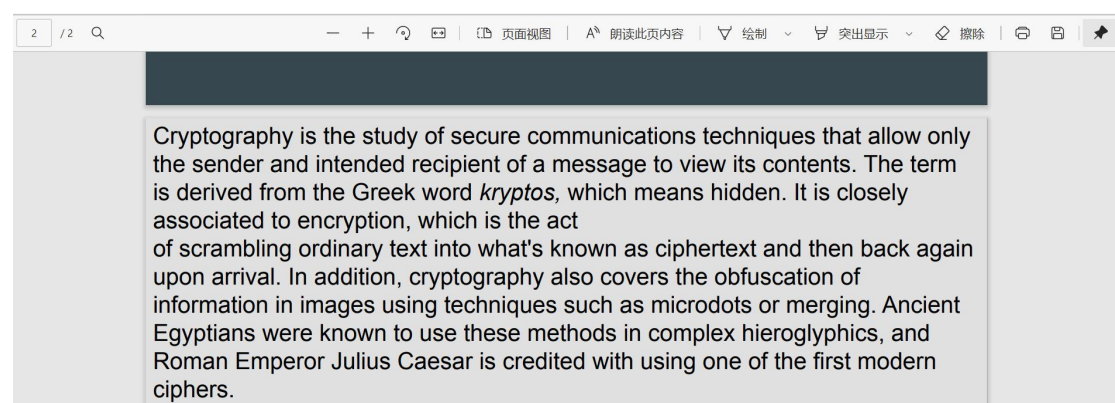
看了眼题解，噯，不用按意思拆，flag 是 KCTF{LOOKB4Y0UL34P}，下面那行没用，那没事了。

总结：

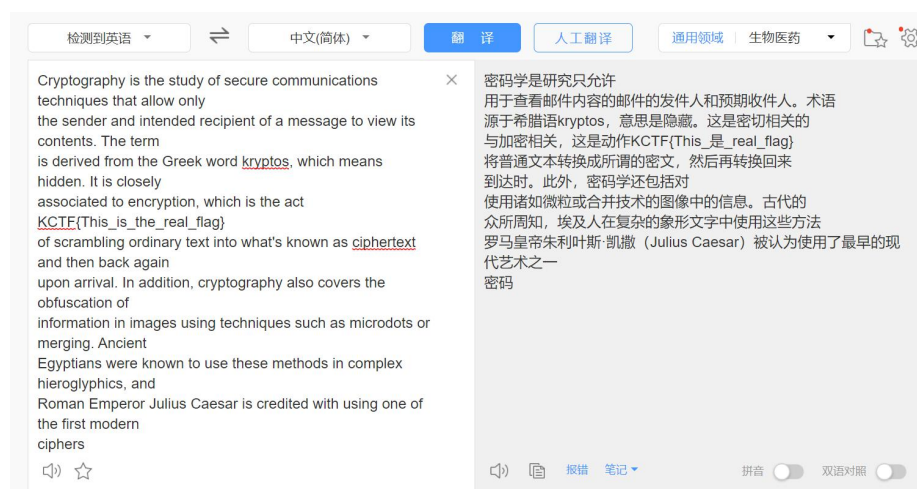
图片隐写有可能在明暗上做文章，以后需要积累点图片处理的技巧。

Follow

一上来给了个 pdf：



由于鄙人英文较差，所以先复制到百度翻译：



呃，百度翻译，我滴超人！

总结：

这题其实挺明显，act 和 of 之间那么大个空，多半有问题，只是没想到直接复制就能出来 $\backslash(\text{---}, \text{---})\text{厂}$

QR Code From The Future

这题一打开是一个不断闪烁的二维码???

用看图软件打开发现是一个由 48 张二维码组成的 gif???

我硬生生用微信扫了 48 下码，得出来这个：

`XPGS{DE_pbqr_tbg_ribyirq_sebz_fgngvp_gb_qlanzvp}`

根据 flag 格式，猜测 KCTF 和 XPGS 对应，不难根据此规律得出其余字母意思：

`KCTF{QR_code_got_evolved_from_static_to_dynamic}`

总结：

解这题最费时间的反而是扫码，以后可能得找点针对性的工具。只能说这题确实逆天。

Bangladesh

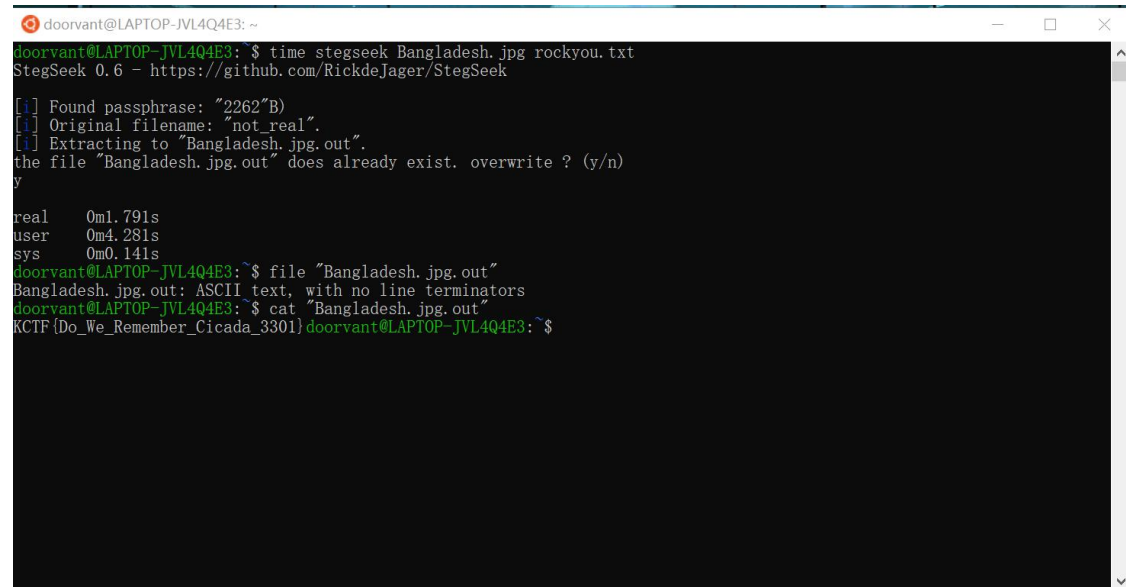


题中给的提示是：3 个数字之和等于 game-changer。

谷歌识图出来发现这地方叫 lalbagh fort，然后线索就断了。

找到题解了，好耶！果断进行一波题解的看，果然方向一来就错了。。。

按大佬的题解，下载了个 stegseek，运行如下命令，结束。



```
doorvant@LAPTOP-JVL4Q4E3: ~  
doorvant@LAPTOP-JVL4Q4E3:~$ time stegseek Bangladesh.jpg rockyou.txt  
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek  
[!] Found passphrase: "2262'B"  
[!] Original filename: "not_real".  
[!] Extracting to "Bangladesh.jpg.out".  
the file "Bangladesh.jpg.out" does already exist. overwrite ? (y/n)  
y  
real    0m1.791s  
user    0m4.281s  
sys     0m0.141s  
doorvant@LAPTOP-JVL4Q4E3:~$ file "Bangladesh.jpg.out"  
Bangladesh.jpg.out: ASCII text, with no line terminators  
doorvant@LAPTOP-JVL4Q4E3:~$ cat "Bangladesh.jpg.out"  
KCTF{Do_We_Remember_Cicada_3301}doorvant@LAPTOP-JVL4Q4E3:~$
```

至于 330 这个提示到底有啥用，由于这个软件属于暴力破解，所以也就不得而知了。

总结：

多看看大佬的题解，了解一些好用的工具，暴力破解有时还是挺管用。

Canada Server

这题让你查询 NS TechValley 在加拿大的服务器的 IP 地址。

先谷歌一下 NS TechValley，找到他们官网的域名 nstechvalley.com，然后先 DNS 查询：

当前位置： [站长工具](#) > [Dns查询](#) 广告 集团高品质产品

[Ping检测](#) [国内测速](#) [国际测速](#) [网站速度对比](#) **DNS查询** [路由器追踪](#) [DNS污染检测](#)

A类型

nstechvalley.com

×

检测

选填:如果要针对固定DNS服务器可填此项(限IP地址) *(选填限IP地址)

DNS所在地	响应IP	TTL值
广东[电信]	192.99.167.83 [加拿大魁北克博阿努瓦 OVH]	14400
贵州[电信]	-	-
安徽[电信]	192.99.167.83 [加拿大魁北克博阿努瓦 OVH]	14400
云南[电信]	192.99.167.83 [加拿大魁北克博阿努瓦 OVH]	3600
山东[联通]	-	-
吉林[联通]	-	-
江苏[联通]	-	-

发现这个响应 IP 就是加拿大的，因此 192.99.167.83 即为所求 IP。

后续看题解时发现一个更秀的解法，linux 下用 host 命令可以直接查询 ip：

```
doorvant@LAPTOP-JVL4Q4E3:~$ host nstechvalley.com
nstechvalley.com has address 192.99.167.83
```

总结

本题需要一定的计网知识以及一点点查询 ip 的手段。平时还得多看看大佬的题解，学习一些先进的操作。

Explosion In Front Of Bank Of Spain

这题让你找下面这个地方的坐标：



Google 这个图片发现是网剧《纸钞屋》里的一个镜头，往下翻了一会儿发现全是营销号：

<https://www.lpls.net> › ent ▼

豆瓣9.5，网飞牛剧，季季封神！!!! - 隆平联社！!!!

553 × 311 · 2021年9月17日 — 《纸钞屋》系列五季的剧情只讲了两季抢劫事件：. 前两季抢劫了西班牙皇家印钞厂，劫匪团自己印刷了10亿欧元 ...



<https://www.lpls.net> › read ▼

豆瓣9.5，网飞牛剧，季季封神！!!!

553 × 311 · 2021年9月17日 — 《纸钞屋》系列五季的剧情只讲了两季抢劫事件：. 前两季抢劫了西班牙皇家印钞厂，劫匪团自己印刷了10亿欧元 ...



<http://www.ywei.net> › ent ▼

豆瓣9.5，网飞牛剧，季季封神！!!! - 悦薇网

553 × 311 · 2021年9月17日 — 《纸钞屋》系列五季的剧情只讲了两季抢劫事件：. 前两季抢劫了西班牙皇家印钞厂，劫匪团自己印刷了10亿欧元 ...



<https://sunnews.cc> › entertainment ▼

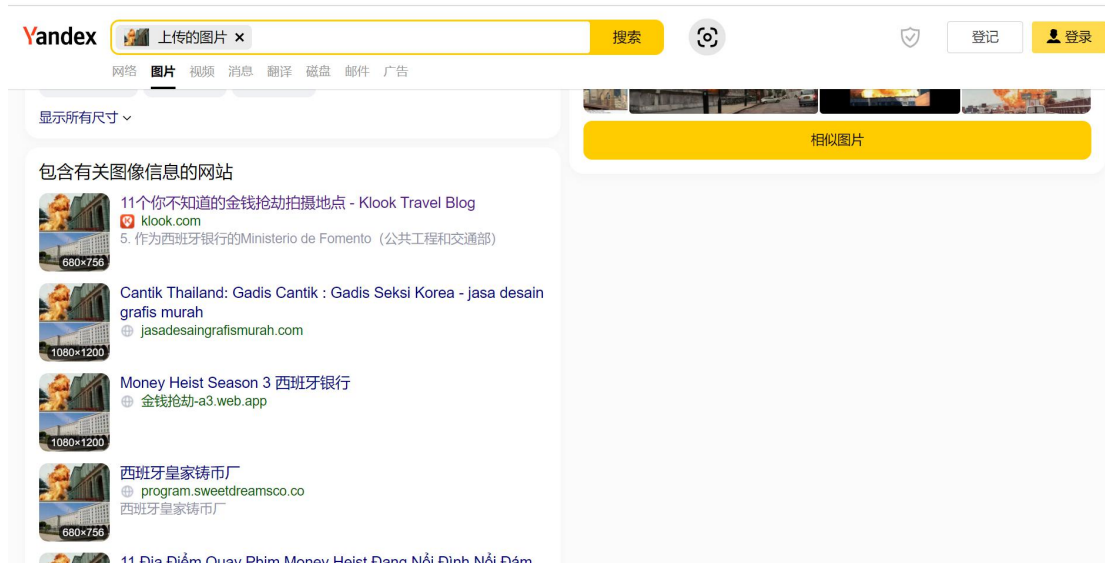
豆瓣9.5，网飞牛剧，季季封神！ - 全网搜

553 × 311 · 2021年9月17日 — 《纸钞屋》是网飞旗下最成功的海外剧，2017年推出第一季后，收视热潮席卷全球，“纸钞屋元素”甚至还成为了一种流行文化现象。



服了，看来谷歌比百度好不到哪里去

果断打开题解，看见大佬用的是 yandex 这个搜索引擎，好像 osint 里图片识别用这个的比较多：

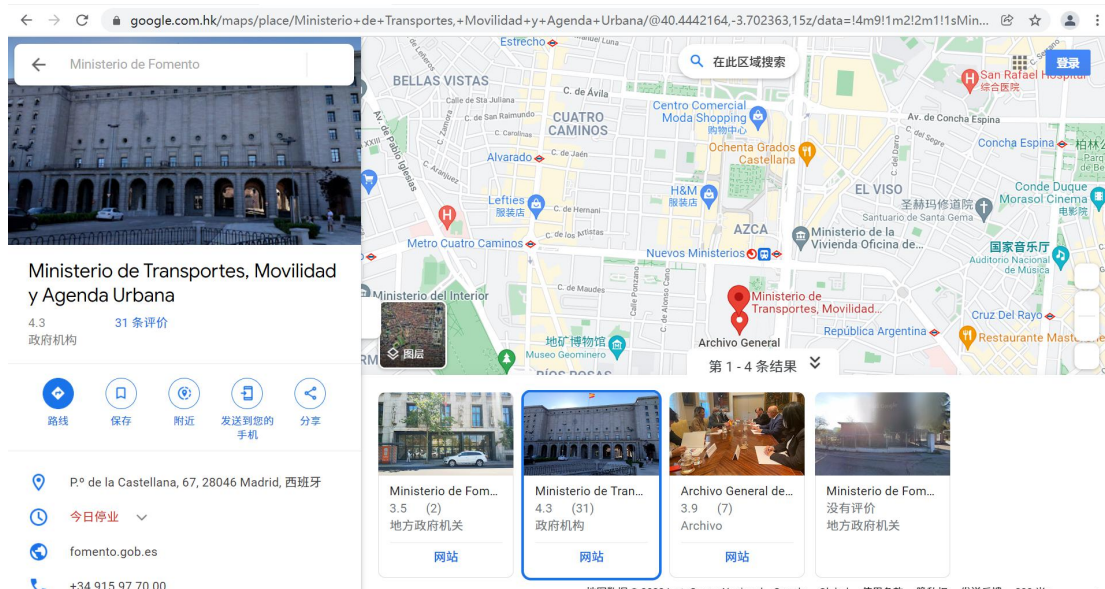


点开第一篇文章：

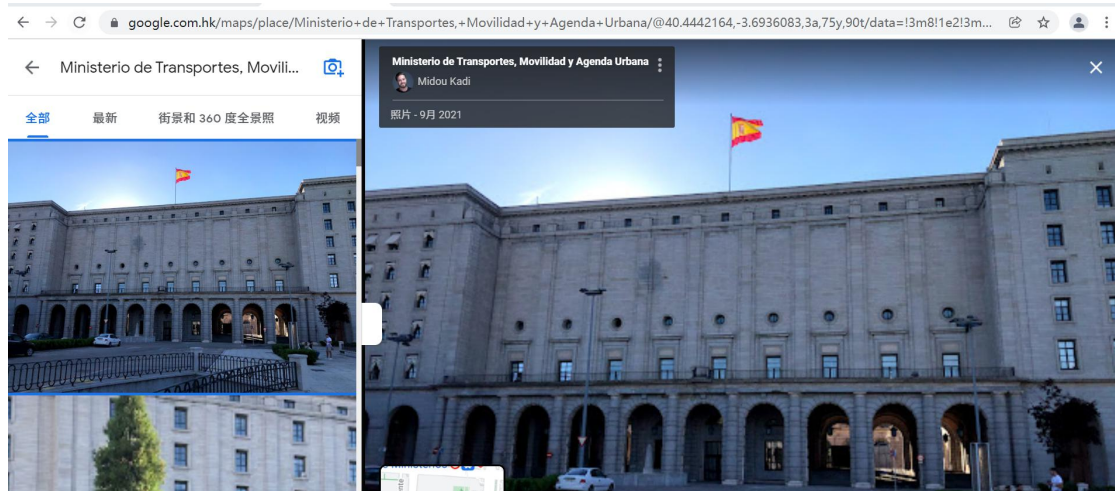
5. 作为西班牙银行的Ministerio de Fomento（公共工程和交通部）



Google 地图里输入上面那个名字，找了半天发现一个更像拍摄地的：



这还不算完，要获取这地方的准确坐标，你必须点网页左上角的图片：



进入这个页面，复制 url 里的坐标即可（40.4442164,-3.6936083），注意，一定要点进这个页面，否则坐标可能有误。

总结

靠谱的识图引擎是必要的，否则对于这种电视剧里的场景，搜出来的多半是营销号。在以后的练习里需要更加熟练 google 地图的用法。我特意拿百度地图试了下这道题，发现百度地图的坐标和 google 的大不相同，所以能用 google 还是尽量用 google。

Find The Camera

这道题让你找拍照的相机的制造商和型号，图长这样：



先搜索图片上的 JenCh012 试试看：

Google

jench012

×

🔍

🔍 全部

🖼️ 图片

📍 地图

📺 视频

📰 新闻

⋮ 更多

🛠️ 工具

找到约 6 条结果 (用时 0.36 秒)

https://fotobus.msk.ru › vehicle

Luxembourg, bus # 19

Author: [JenCh012](#) · 167 KB, 2. 195. Interior, view to back. Sunday, September 18, 2011.


Author: [JenCh012](#) ... Author: [JenCh012](#).

https://fotobus.msk.ru › vehicle

Luxembourg, bus # 232

Author: [JenCh012](#) · Region: Luxembourg. Location: Lëtzebuerg – Lëtzebuerg ... Author: [JenCh012](#) · 157 KB, 101. Luxembourg-ville.

🖼️ jench012的图片搜索结果



提供反馈

看见一张熟悉的照片，一路点进去看看：

Statistics

Published 17.05.2010 20:56 MSK
Views — 500

Detailed info

Voting

Rating: +43

Евгений Хонгуров

+1

Щукин Д.

+1

Макс И

+1

yarem4uk.r

+1

Ozzi

+1

saveliy

+1

Скоробогатых Илья

+1

Maksim

+1

Станислав Богомолов

+1

Дмитрий Халимов

+1

Kot_Beluga

+1

DimonPV

+1

Владимир М.

+1

PPS

+1

vladislav_izh

+1

Александров Николай

+1

Костя

+1

Alexeum

+1

Штык

+1

Артём Веселов

+1

Camera Settings

Make/Manufacturer:	SONY
Model:	DSC-S980
Software or Firmware:	Adobe Photoshop Elements 2.0
Date and Time:	15.05.2010 15:51
Exposure Time:	1/320 sec
Aperture Value:	5.6
ISO Speed:	100
Focal Length:	23.2 mm
Flash:	Flash did not fire, auto mode
Metering Mode:	Pattern
Shooting Mode:	Program

Your comment

You need to [log in](#) to write comments.

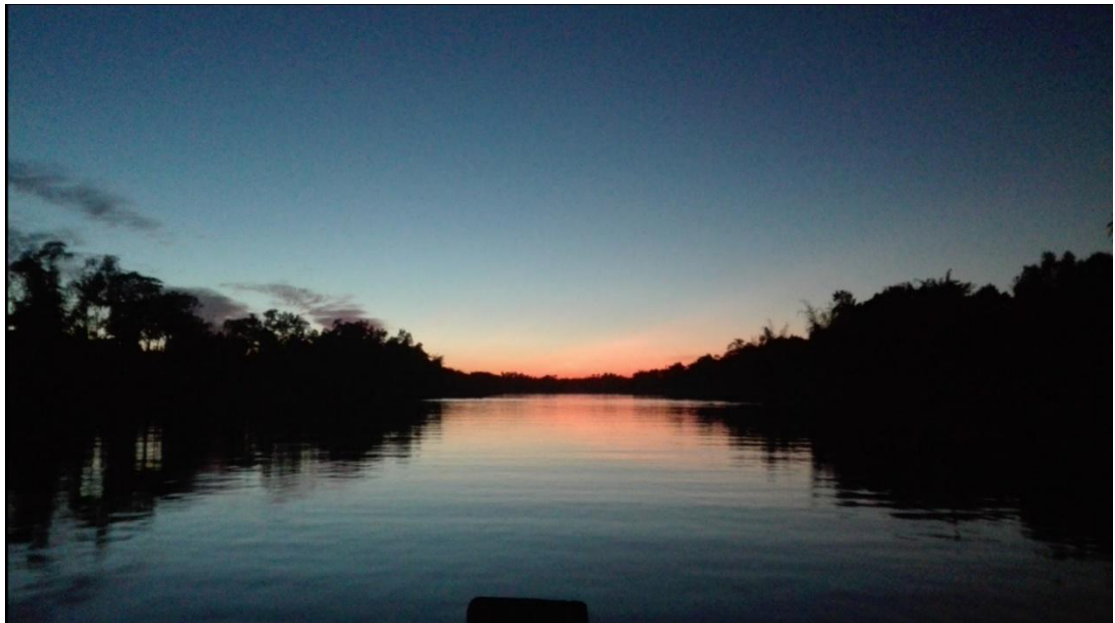
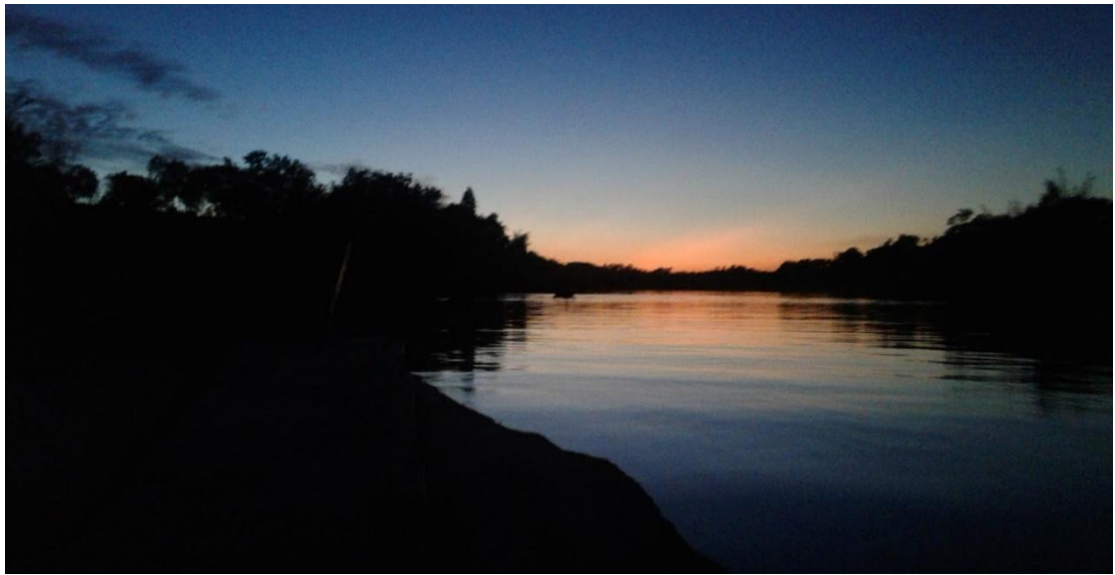
是 SONY DSC-S980，搞定。

总结：

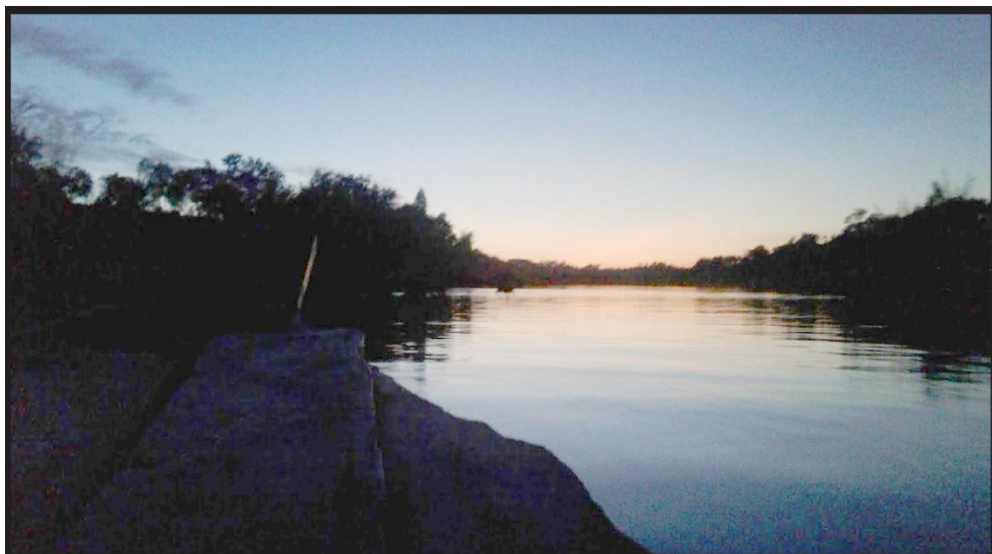
用仅有的信息一路往下搜索即可。用图片搜应该也能找到答案。

Find The Hacker

这题给了两张图片，让你找出图片里是孟加拉国北部的啥地方：



用 PS 对第一张图进行一下处理：



拿处理过后的图在网上搜了半天，没啥显著效果，没辙了

寄！