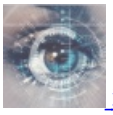
从CTF比赛真题中学习压缩包伪加密与图片隐写术，最新阿里P7技术体系

原创

开源Python 于 2022-03-21 14:08:28 发布 108 收藏

分类专栏： 程序员 文章标签： 面试 经验分享 开发语言

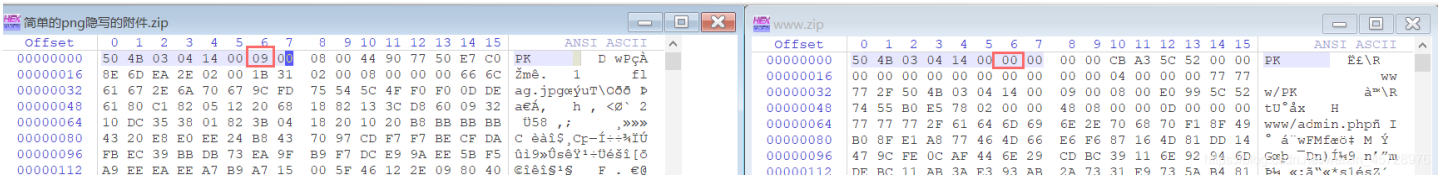
本文链接：https://blog.csdn.net/m0_68313184/article/details/123634326



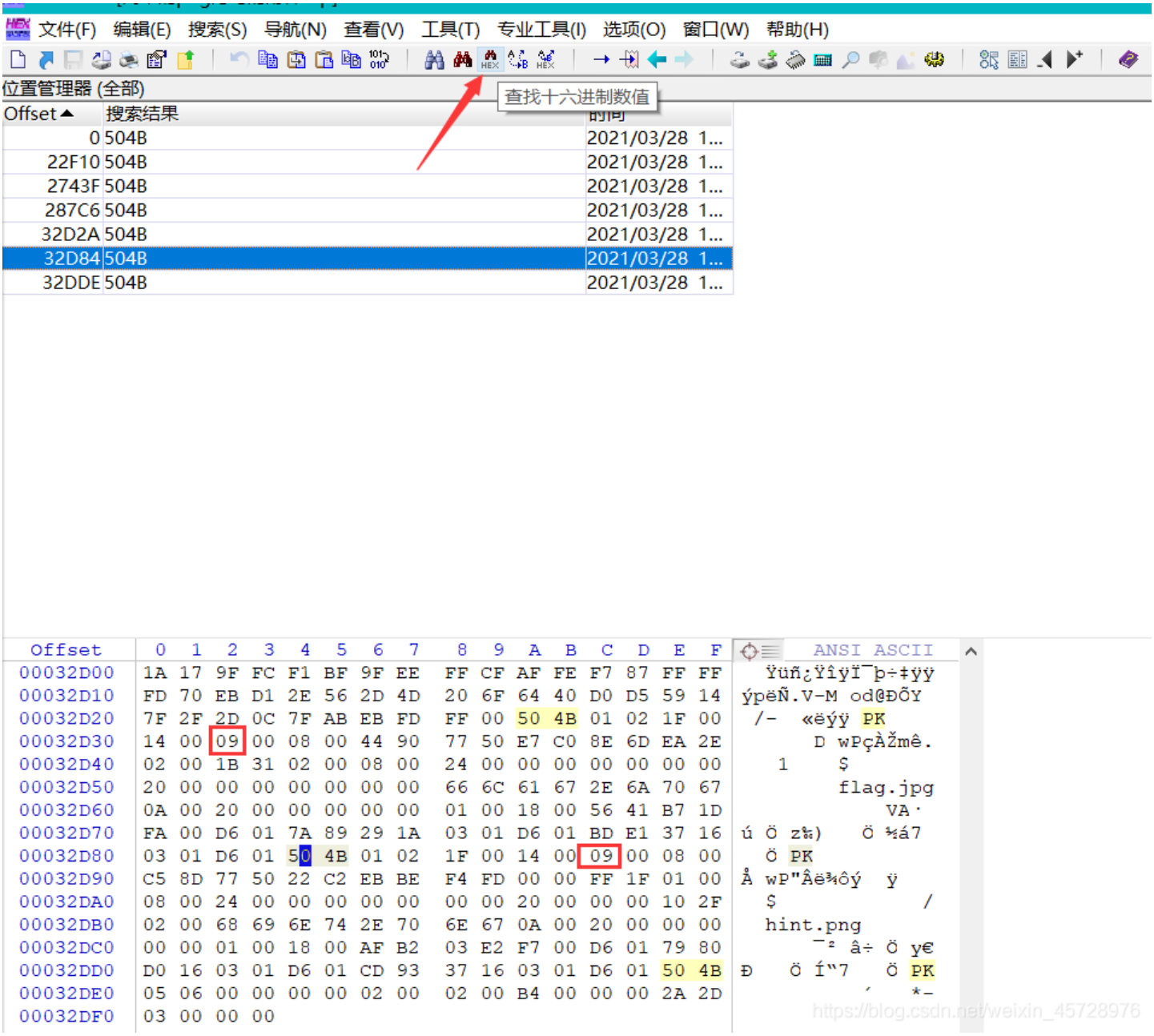
==========

如遇加密压缩包，在没有密码提示的情况下，先判断是不是伪加密

最简单的方法就是看十六进制数据，第一行如果有`09`多半就是了



点击查找十六进制数值搜索`504B`，最后如果有`09`那基本就是了，改为`00`完活

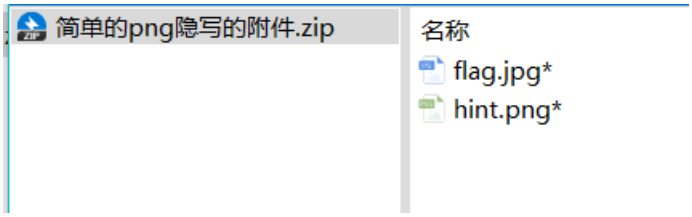


□(

)伪加密破解

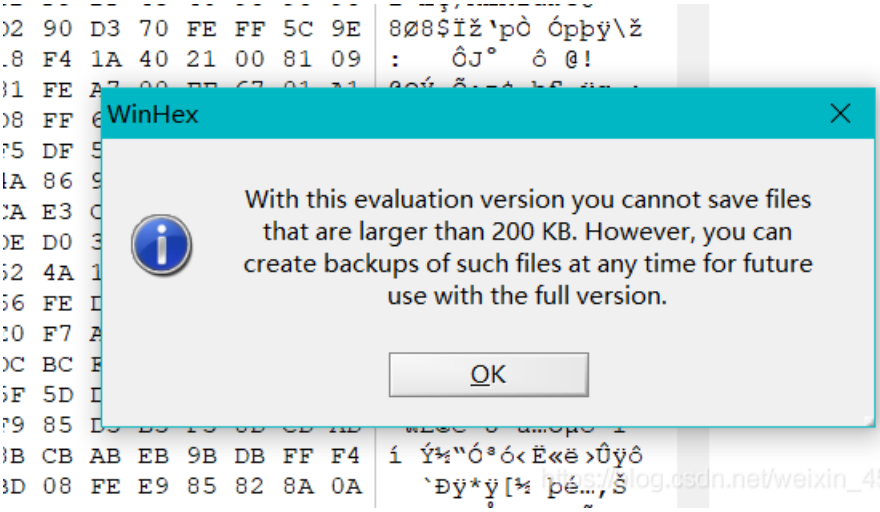
==========

比如这道misc题，结合了压缩包伪加密与图片隐写技术，我们就以它为例学习一下这两种常见技术的解决方法



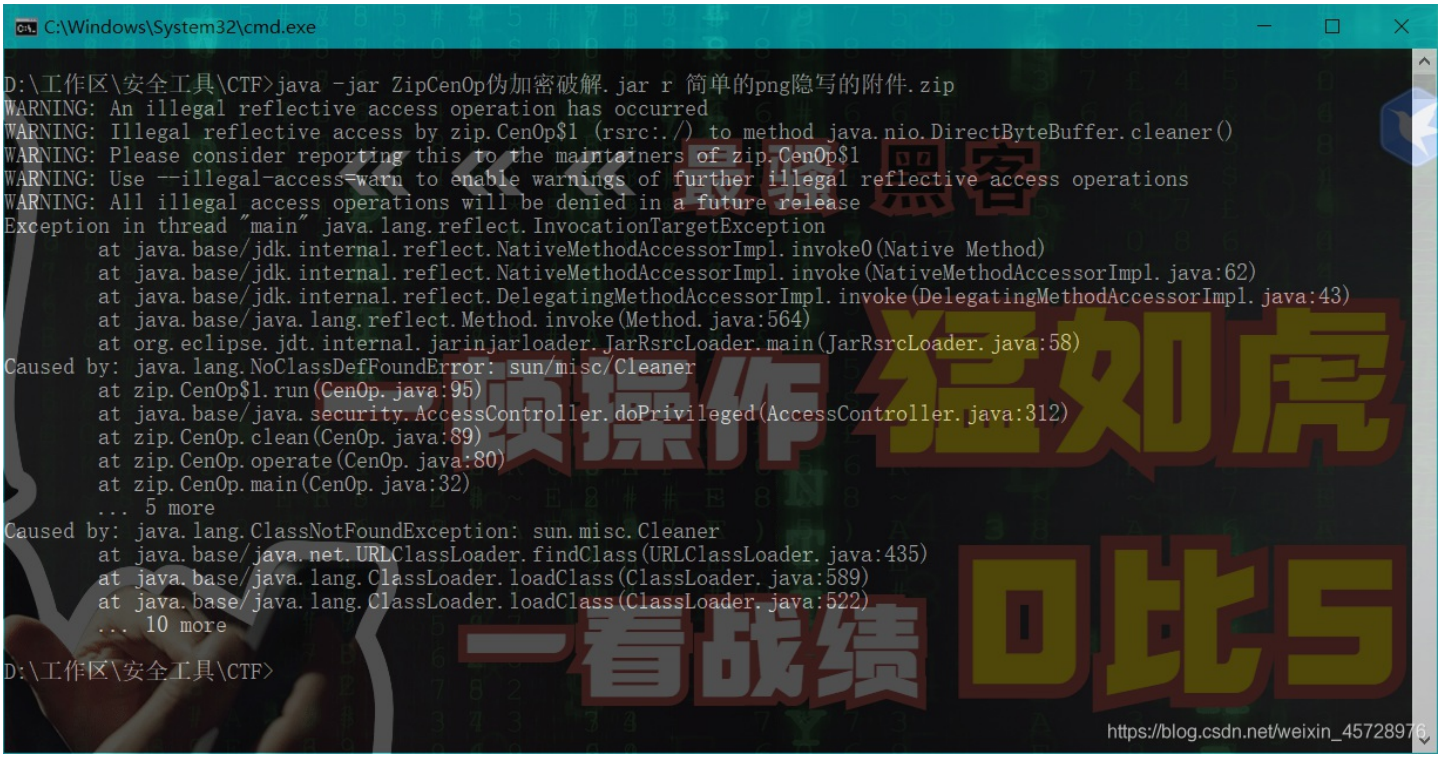
就是这个压缩文件，后面带`*`说明需要密码，但是题中没有任何密码提示，ctf中不可能让你无脑爆破，因为时间是有限的，但也有可能是弱口令，反正无从下手先爆破一下试试呗

当时我也想到了伪加密，用`WinHex`打开压缩包，将全局方位标记中的`09`改为`00`保存即可解除密码限制，这里有两个文件所以要改两处，但提示我试用版超过200kb不能保存，怎么回事，我记得是破解的啊



比赛结束后我才找到破解伪加密的工具——`ZipCenOp`

命令`java -jar ZipCenOp伪加密破解.jar r 简单的png隐写的附件.zip`



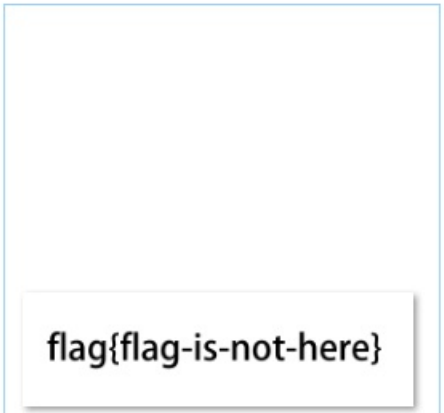
)(

)图片隐写破解

==========

图片隐写的方式很多样，用到的工具也多，文件名已经提示的很明显了，是png隐写，所以朝着这方面想就行了

flag.jpg



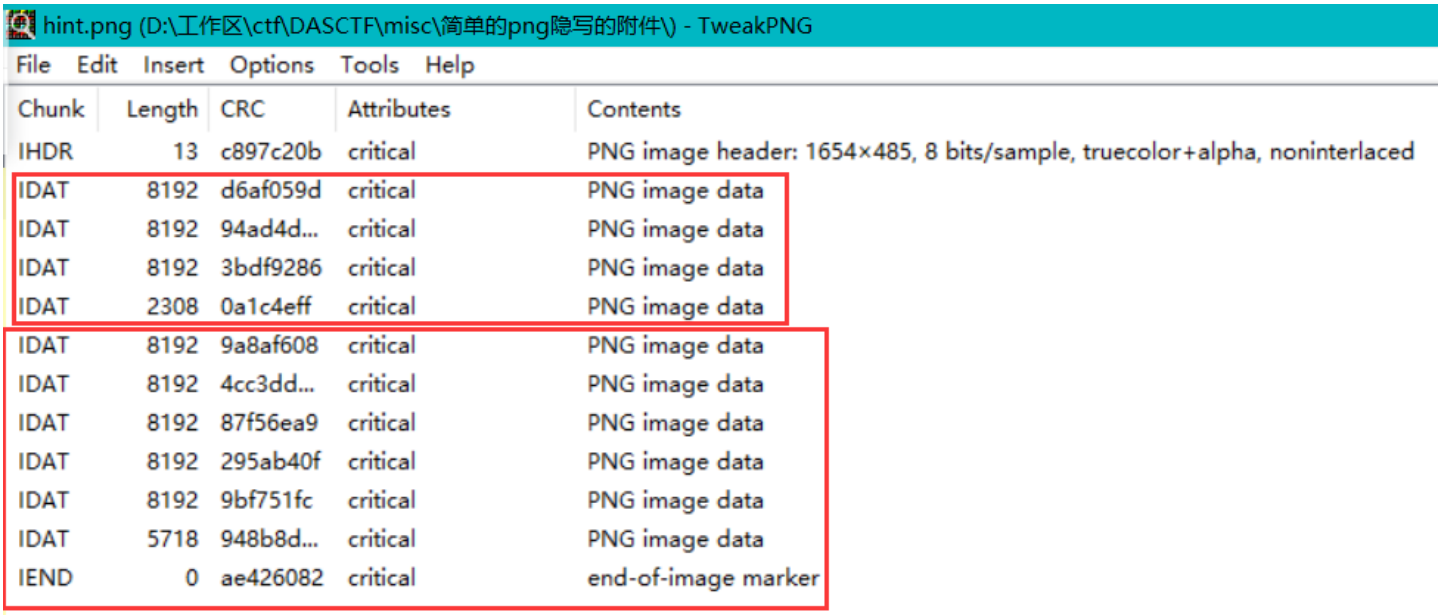
hint.png

`binwalk` 和 `Stegsolve` 都没能找到什么有用的东西

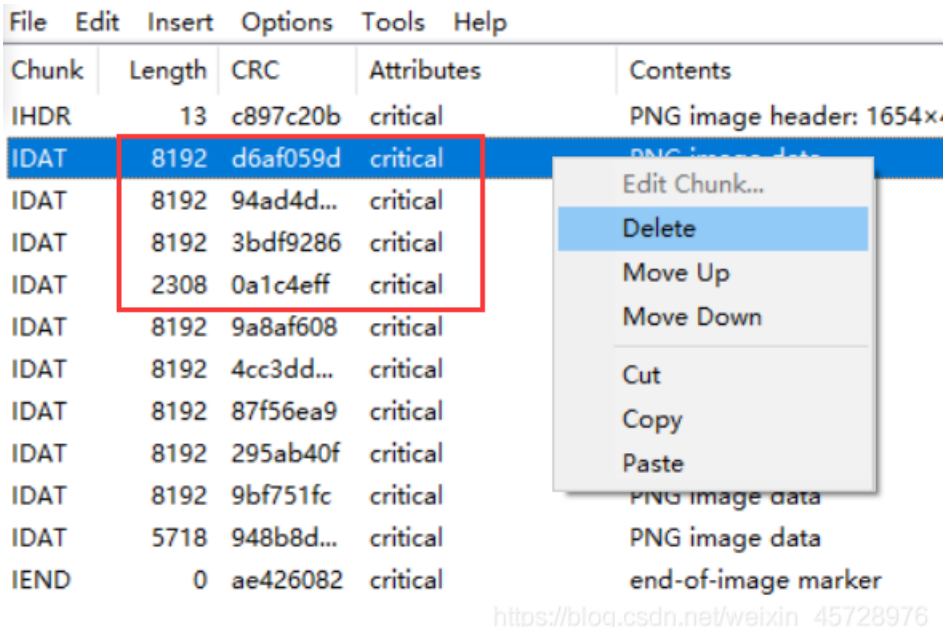
所以百度一下，当当当，学到两个新工具`pngcheck`和`TweakPNG`

它们的功能是差不多的，只不过一个是命令行模式一个是图形化界面，但`pngcheck`可以识别多个图像类型，而另一个只能是`png格式`

复制一张`hint.png`然后用`TweakPNG`打开，可以看到两个`IDAT块`，正常的图片应该只有一条IDAT数据不同，而这里有两条不一样的，可以判断是两张图片



右键将上面四条`Delete`，然后`Ctrl+s`保存



这样隐藏的图片就出来了，这句意思是`你可以用89504E猜出旗子在哪里`

hint - 副本.png

hint.png

`89504E`应该是个密码，而需要密码解图片隐写的工具有很多，如：`steghide`和`stegpy`，然而都没用，看了大佬的wp才知道用的是`outguess`，又学了一个工具

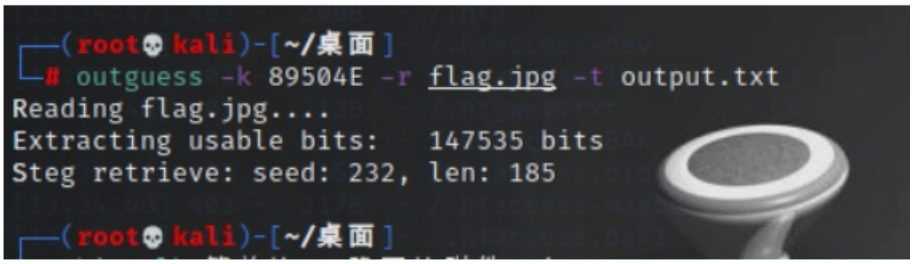
```
┌──(root💀kali)-[~/桌面]
└─# steghide extract -sf flag.jpg -p 89504E
steghide: could not extract any data with that passphrase!

┌──(root💀kali)-[~/桌面]
└─# stegpy flag.jpg -p 89504E
Enter password (will not be echoed):
Wrong password.
```

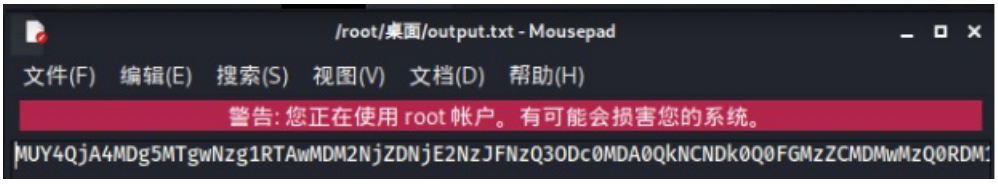
这个kali里是没有的，输

入`apt install outguess`安装即可

用命令`outguess -k 89504E -r flag.jpg -t output.txt`导出加密内容



里面有一行编码字符，看着像`Base64`



()

)十六进制数据还原文件

==========

解密得到一串好像十六进制的东西

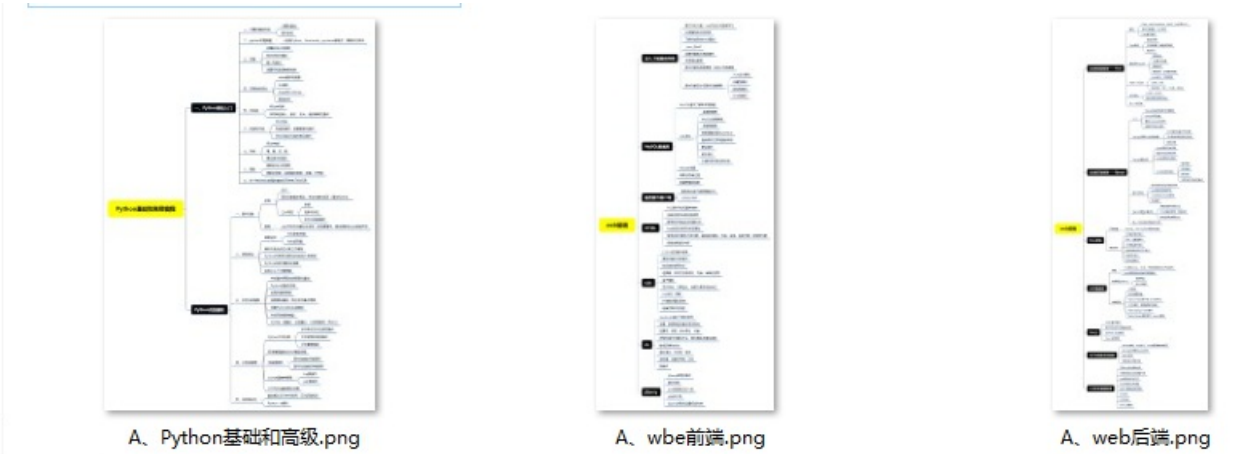
十六进制再转字符串发现有个`flag.txt`字样，有经验的已经想到了，这可能是个压缩文件，那怎样将十六进制数据变成文件呢？大神用的Python导出成文件，那咱这种菜鸡不会，只能用笨办法喽

最后

Python崛起并且风靡，因为优点多、应用领域广、被大牛们认可。学习 Python 门槛很低，但它的晋级路线很多，通过它你能进入机器学习、数据挖掘、大数据，CS等更加高级的领域。Python可以做网络应用，可以做科学计算，数据分析，可以做网络爬虫，可以做机器学习、自然语言处理、可以写游戏、可以做桌面应用…Python可以做的很多，你需要学好基础，再选择明确的方向。这里给大家分享一份全套的 Python 学习资料，给那些想学习 Python 的小伙伴们一点帮助！

□Python所有方向的学习路线□

Python所有方向的技术点做的整理，形成各个领域的知识点汇总，它的用处就在于，你可以按照上面的知识点去找对应的学习资源，保证自己学得较为全面。

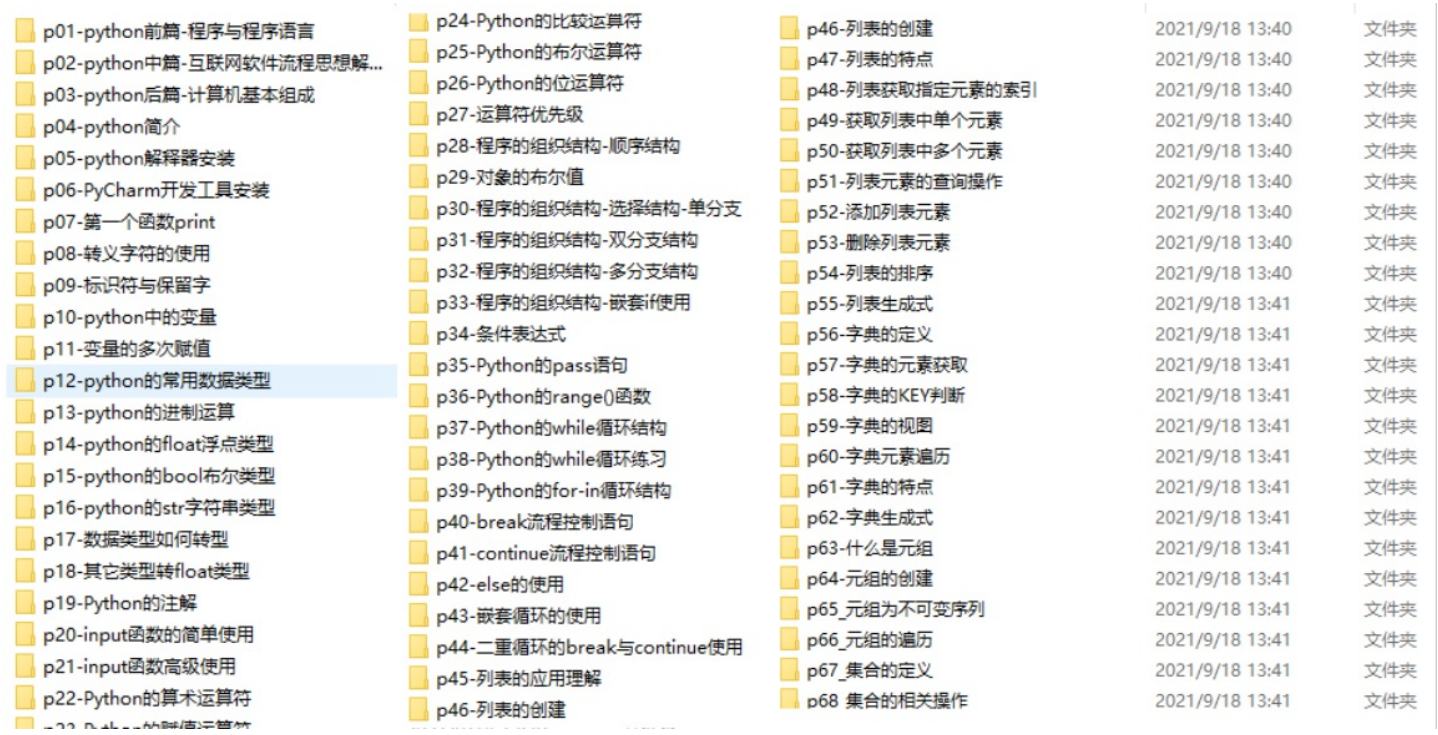


□Python必备开发工具□

工欲善其事必先利其器。学习Python常用的开发软件都在这里了，给大家节省了很多时间。

□Python全套学习视频□

我们在看视频学习的时候，不能光动眼动脑不动手，比较科学的学习方法是在理解之后运用它们，这时候练手项目就很适合了。



□实战案例□

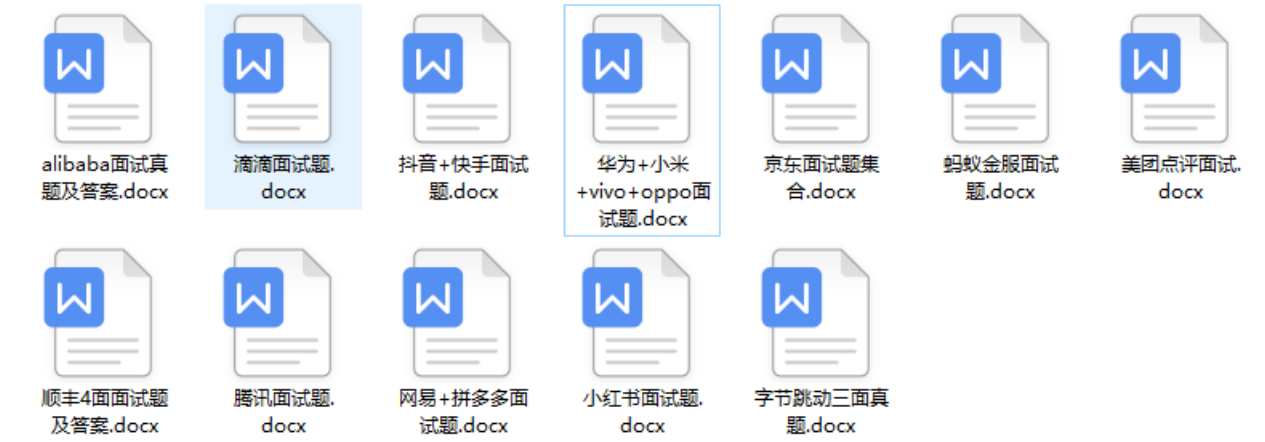
学python就与学数学一样，是不能只看书不做题的，直接看步骤和答案会让人误以为自己全都掌握了，但是碰到生题的时候还是会一筹莫展。

因此在学习python的过程中一定要记得多动手写代码，教程只需要看一两遍即可。

实例43_批量发送不同内容的邮件给不同的收件人	2021-09-12 10:43	文件夹	-
实例45_用Python分析文本数据的词频	2021-09-12 10:43	文件夹	-
实例46_Python文本数据可视化之“词云”图	2021-09-12 10:43	文件夹	-
实例47_Python替换不了word中的文字？	2021-09-12 10:43	文件夹	-
实例48_批量修改word文件中的段落格式	2021-09-12 10:43	文件夹	-
实例50_Python一键提取PDF中的表格到Excel	2021-09-12 10:43	文件夹	-
实例51_5行代码，Python给孩子出数学练习题	2021-09-12 10:43	文件夹	-
实例52_Pandas提取指定数据并保存在原Excel工作簿中	2021-09-12 10:43	文件夹	-
实例53_Python从原Excel表中抽出数据存入同一文件的新...	2021-09-12 10:43	文件夹	-
实例54_Python指挥打印机批量打印文件	2021-09-12 10:43	文件夹	-
实例55_看你怎么作弊抄答案？Python出题，每个学生的...	2021-09-12 10:43	文件夹	-
实例56_Python从多路径多Excel表中获取数据并存入新表	2021-09-12 10:43	文件夹	-
实例57_Python爬虫爬取会计师协会网站的指定文章	2021-09-12 10:43	文件夹	-
实例58_Python爬虫~已爬取目标网站所有文章，后续如...	2021-09-12 10:43	文件夹	-
实例59_Python检查word文件中的特殊标记词是否与文...	2021-09-12 10:43	文件夹	-
实例60_Python汇总各单位Excel档领料记录并加总每日领...	2021-09-12 10:43	文件夹	-
实例61_Python制作图形用户界面(GUI)让操作可视化	2021-09-12 10:43	文件夹	-
实例62_将Python程序打包成安装文件分享给小伙伴	2021-09-12 10:43	文件夹	-
实例63_Tkinter制作Python程序的图形用户界面(GUI)，...	2021-09-12 10:43	文件夹	-
实例64_Python分块拆分txt文件中的数据	2021-09-12 10:43	文件夹	-
实例65_Python识别加密的word文件并移动到单独文件夹	2021-09-12 10:43	文件夹	-
实例66_Python一键更新Excel档“生产订单周报”的图表	2021-09-12 10:43	文件夹	-
实例67_Python爬取博客的所有文章并存为带目录的wor...	2021-09-12 10:43	文件夹	-
实例68_Python批量新建文件夹并保存日志信息	2021-09-12 10:43	文件夹	-
实例69_Python保留格式复制多个excel工作表到汇总表并...	2021-09-12 10:43	文件夹	-
实例70_Python批量将公号文章保留原格式下载为PDF	2021-09-12 10:43	文件夹	-
实例71_Python从Excel表中批量复制粘贴数据到新表	2021-09-12 10:43	文件夹	-

□大厂面试真题□

我们学习Python必然是为了找到高薪的工作，下面这些面试题是来自阿里、腾讯、字节等一线互联网大厂最新的面试资料，并且有阿里大佬给出了权威的解答，刷完这一套面试资料相信大家都能找到满意的工作。



学习Python必然是为了找到高薪的工作，下面这些面试题是来自阿里、腾讯、字节等一线互联网大厂最新的面试资料，并且有阿里大佬给出了权威的解答，刷完这一套面试资料相信大家都能找到满意的工作。