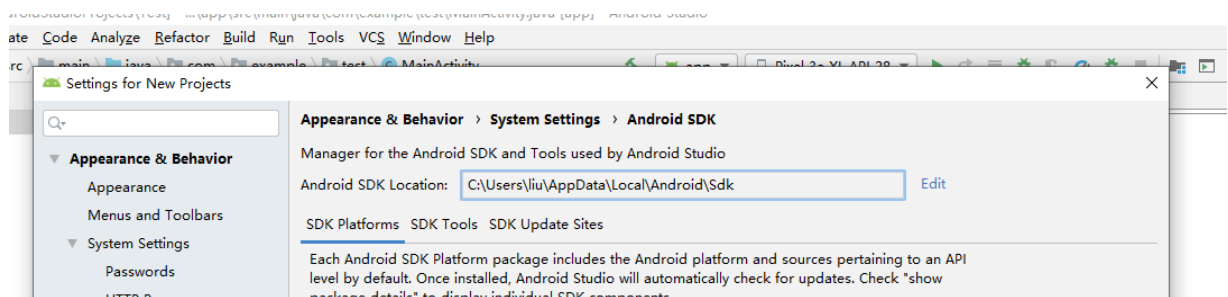


# 安卓渗透神器-Drozer的安装测试

- adb 的下载及安装

- 下载地址：<https://adbshell.com/downloads>（比较慢）。
- 下载下来直接解压应该就能用了。（我没测试，我以前装的有Android Studio,我用的是第二种办法）
- 若安装的有Android Studio 把SDK中platform-tools文件夹下的adb.exe加到环境变量中就行。在path中添加你的SDK路径\Sdk\platform-tools
- 在CMD中，用adb version测试一下。
- 若不知道SDK安装在哪，可通过Android Studio中的TOOL->SDKManager中查找，前提是SDK配置好。



- 结果

- 最后的效果应该是这样。

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.18362.900]
(c) 2019 Microsoft Corporation. 保留所有权利。

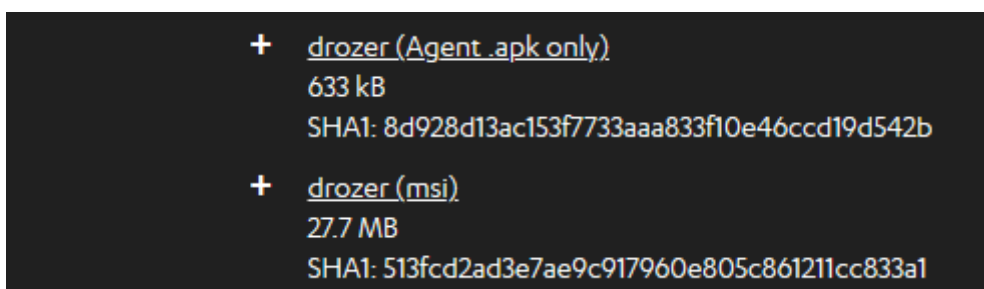
C:\Users\liu>adb version
Android Debug Bridge version 1.0.41
Version 29.0.5-5949299
Installed as C:\Users\liu\AppData\Local\Android\Sdk\platform-tools\adb.exe
```

- 参考博客：[https://blog.csdn.net/weixin\\_43927138/article/details/90477966](https://blog.csdn.net/weixin_43927138/article/details/90477966)

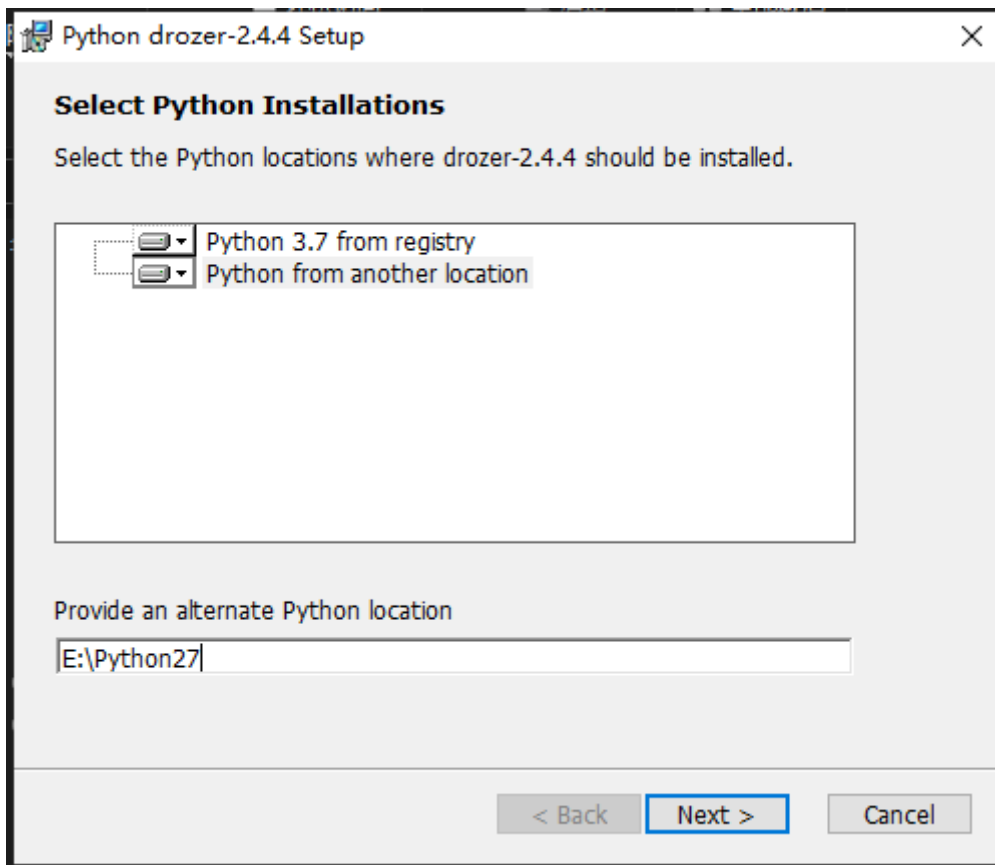
- Drozer电脑端安装

- 下载地址

- <https://labs.f-secure.com/tools/drozer/>
- 下载这两个，上面的是手机端，下面的是电脑端。

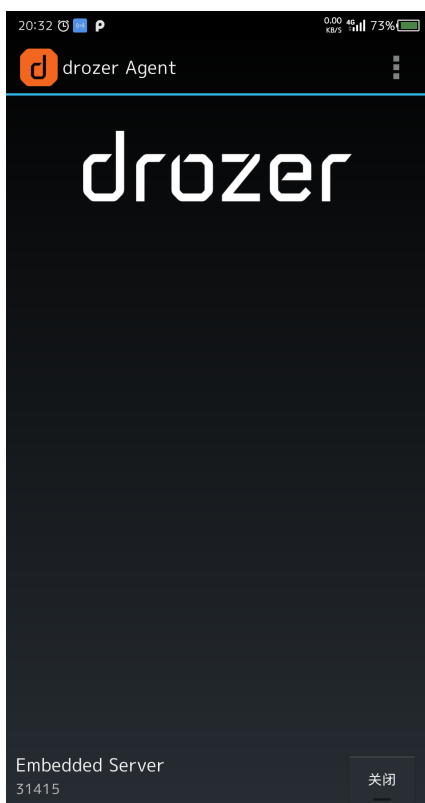


- 安装电脑端时，注意这一点，要手动选择python2的路径，让后一路下一步就行。



- Drozer手机端安装

- 我是直接下载好，通过手机QQ传到手机上，进行安装的。微信文件传输会自动更改后缀名，而且存储的位置不好找，看个人习惯。
- 手机上打开应该是这个样子。



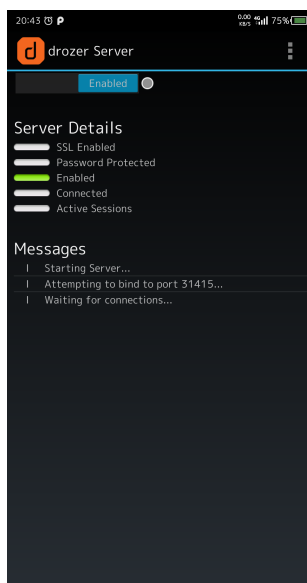
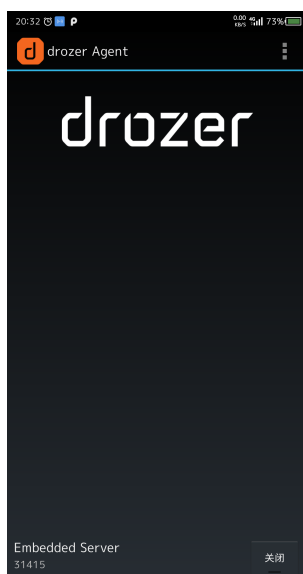
- 打开软件后，在PC上输入如下命令。这样就是已经进入到了手机的Shell。

```
C:\Users\liu>adb devices
* daemon not running; starting now at tcp:5037
* daemon started successfully
List of devices attached
5fd7e32b      unauthorized

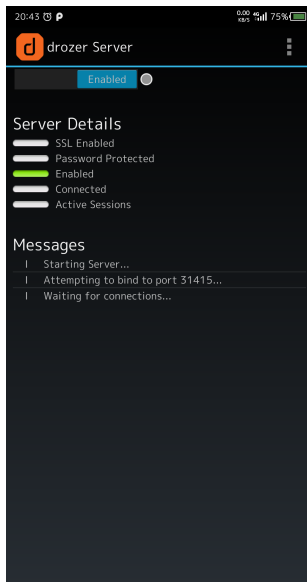
C:\Users\liu>adb shell
NX609J:/ $
```

- 疑难杂症

- 手机连接要配置成USB调试模式。
- cmd默认编码是简体中文GBK 936，连接终端的时候会乱码，无法连接，所以开始前我们临时更改一下cmd的编码：改为UTF-8 65001。命令 chcp 65001。
- 手机开启Drozer。界面如下



- 点击左下角，进入如下界面，点击Disable，开启。



- PC端命令行进入python27的script目录下

```
C:\Users\liu> D:
D:\>E:
E:\Python27\Scripts>_
```

- 设置端口转发，命令如下 adb forward tcp:31415 tcp:31415

```
E:\Python27\Scripts>adb forward tcp:31415 tcp:31415
31415
```

TCP	127.0.0.1:31415	0.0.0.0:0	LISTENING
TCP	127.0.0.1:31415	127.0.0.1:64515	ESTABLISHED

- 启动drozer 命令：drozer console connect

```
C:\Users\liu>drozer console connect
Selecting a635be76438140e4 (nubia NX609J 9)
```

```
..
..o..
..a..
ro..idsnemesisisand..pr
.otectorandroidsneme.
.,sisandprotectorandroids+.
..nemesisisandprotectorandroidsn:.
.emesisandprotectorandroidsnemes..
..isandp,..,rotectorandro,..,idsnem.
.isisandp..rotectorandroid..snemisis.
, andprotectorandroidsnemisisandprotec.
.torandroidsnemesisandprotectorandroid.
.snemisisandprotectorandroidsnemesisan:
.dprotectorandroidsnemesisandprotector.
```

```
drozer Console (v2.4.4)
dz>
```

- 至此Drozer连接真机成功。
- 在中途安装过程中可能因为大家安装的有python3和python2两个版本，在最后一步可能会出现报错，这是因为Drozer是在Py't'hon2的基础上进行开发的。所以要切换到

Python2。

- 若提示缺少protobuf等模块，就直接pip install 模块名安装上就行。

```
D:\Python27>pip install protobuf
Collecting protobuf
  Retrying (Retry(total=4, connect=None, read=None, redirect=None, status=None)) after connection broken by 'ConnectTime
outError(<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x0000000005084710>, 'Connection to files.pyt
honhosted.org timed out. (connect timeout=15)')': /packages/47/90/27eac528bb6871336e86ed8bcb72a9b412a4020bf69bb7be71d40
e5eab0/protobuf-3.12.2-py2.py3-none-any.whl
  Downloading https://files.pythonhosted.org/packages/47/90/27eac528bb6871336e86ed8bcb72a9b412a4020bf69bb7be71d40e5eab0
/protobuf-3.12.2-py2.py3-none-any.whl (443kB)
    27% |#####| 122kB 10kB/s eta 0:00:32
```

- 若提示pip也有问题。。。就自行百度吧！若还是不行的话，就重装python2吧。。（我是这么做的。。。）
- 若是pip install openssl的时候出现无法下载，或者没办法解压的情况，试试 pip install pyopenssl这个命令。
- 若有别的疑问的话或者模拟器的安装办法，就请参考  
<https://mp.weixin.qq.com/s/A51TaOOxpxzcAU3vUHXg>