制作证书绕过CA证书限制

【学习目标】

- 掌握模拟器使用
- 掌握安卓7.0抓包
- 掌握BurpSuite使用

安卓7.0以下抓包

> 环境：夜神模拟器、BurpSuite
>
> 物理机IP：192.168.141.1

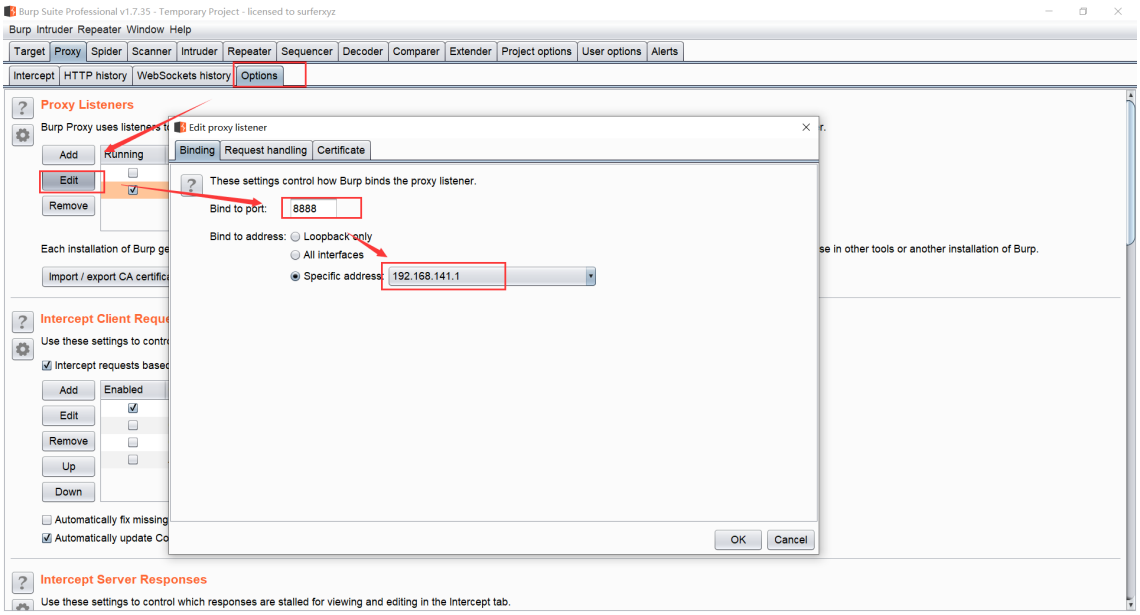
- 为了能够让系统校验公钥证书时认为证书是真实有效的，我们需要将抓包应用内置的CA证书手动安装到系统中，作为真正的证书发行商（CA），即洗白。这就是为什么，HTTPS抓包一定要先安装CA证书。
- 抓包应用内置的 CA 证书要洗白，必须安装到系统中。而 Android 系统将 CA 证书又分为两种：用户 CA 证书和系统 CA 证书。明显后者更真实有效

1. 新建模拟器

- 选择安卓5版本（超过5版本会有证书校验）

2. Burp设置代理

- 设置Burp代理



3. 夜神模拟器设置代理

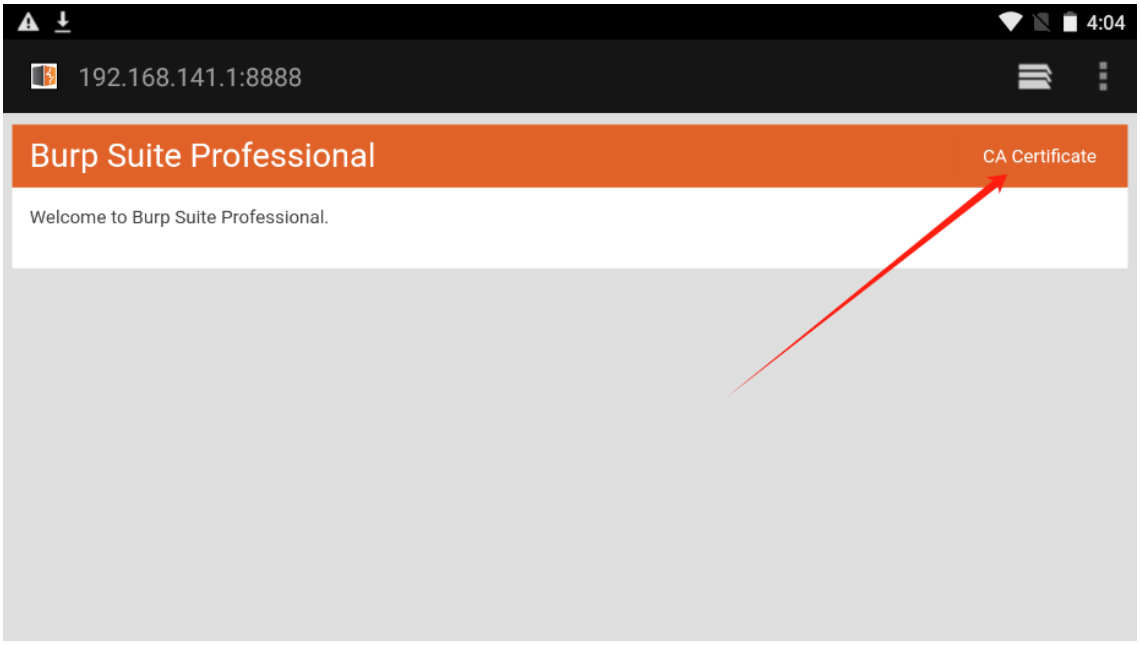
- 设置>WLAN>长按WiredSSID>修改网络

- 设置手动代理模式，IP和端口要和Burp保持一致

- 这个时候只能抓http的包，需要安装证书，才能抓https的包。

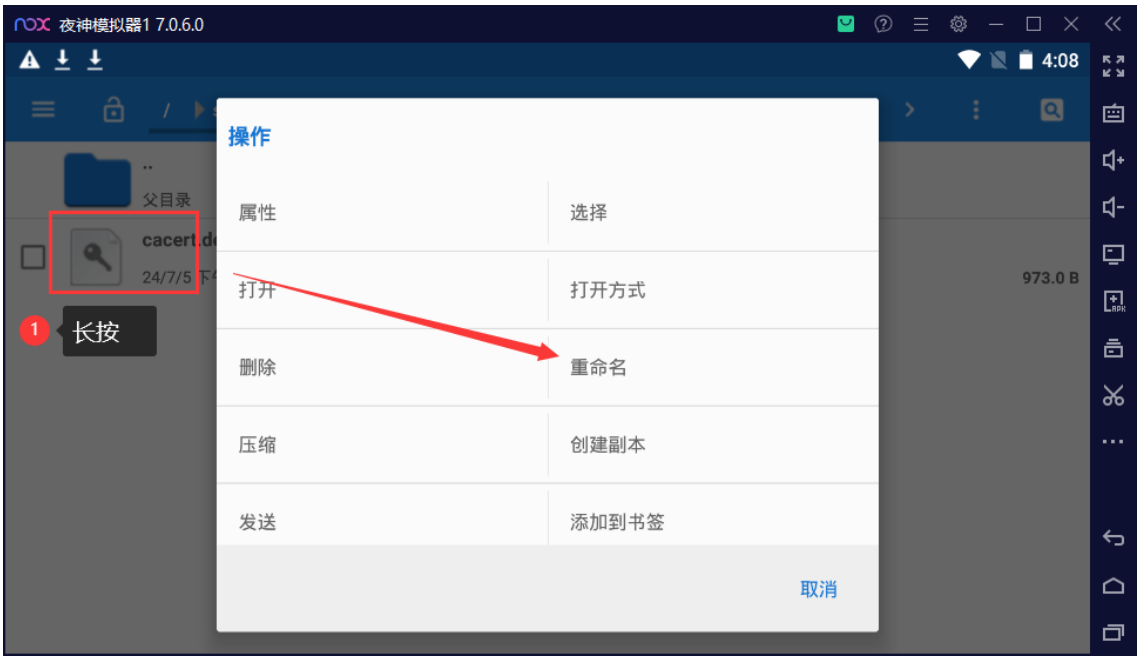
4. 下载证书

- 模拟器中，浏览器访问http://192.168.141.1:8888/下载证书

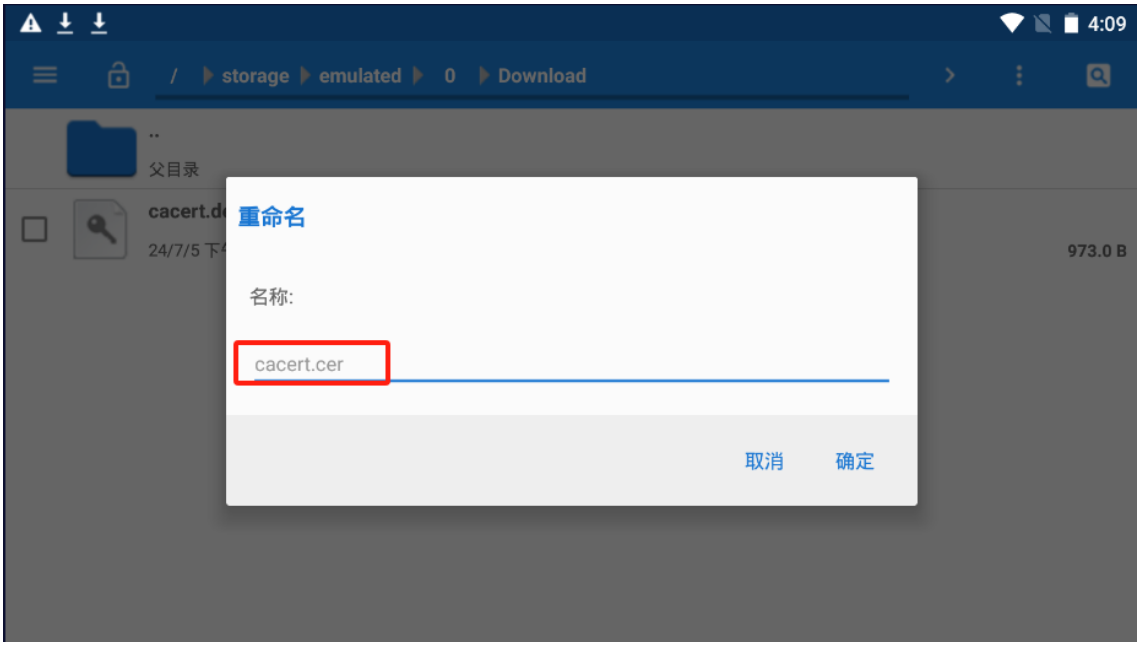


5. 修改证书后缀

- 文件管理>download>修改证书后缀为cer

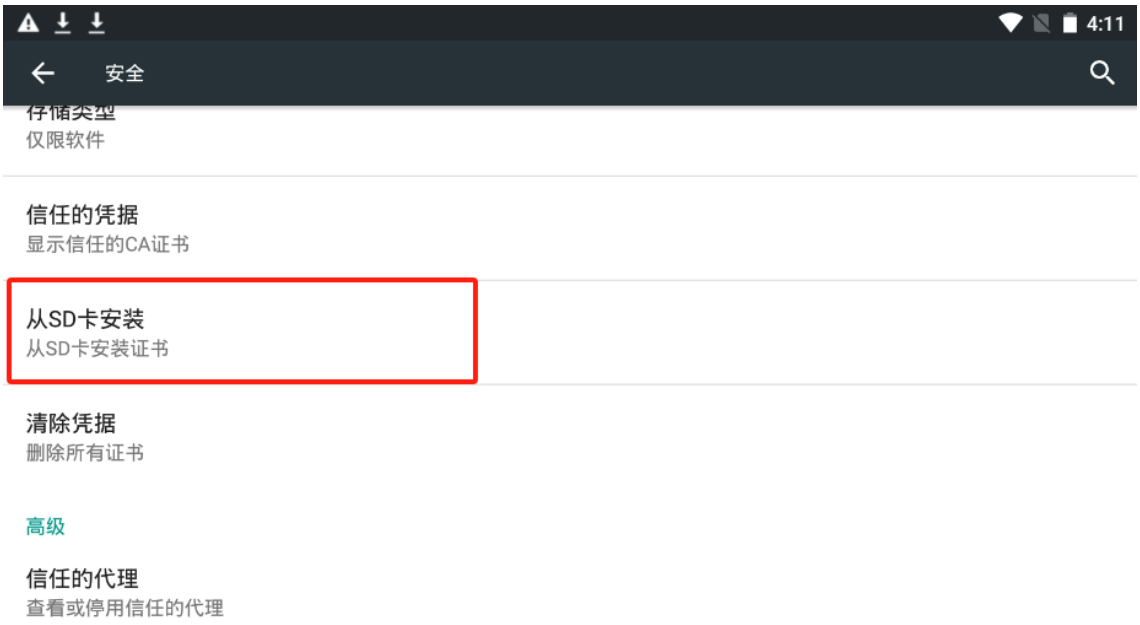


- 修改后缀

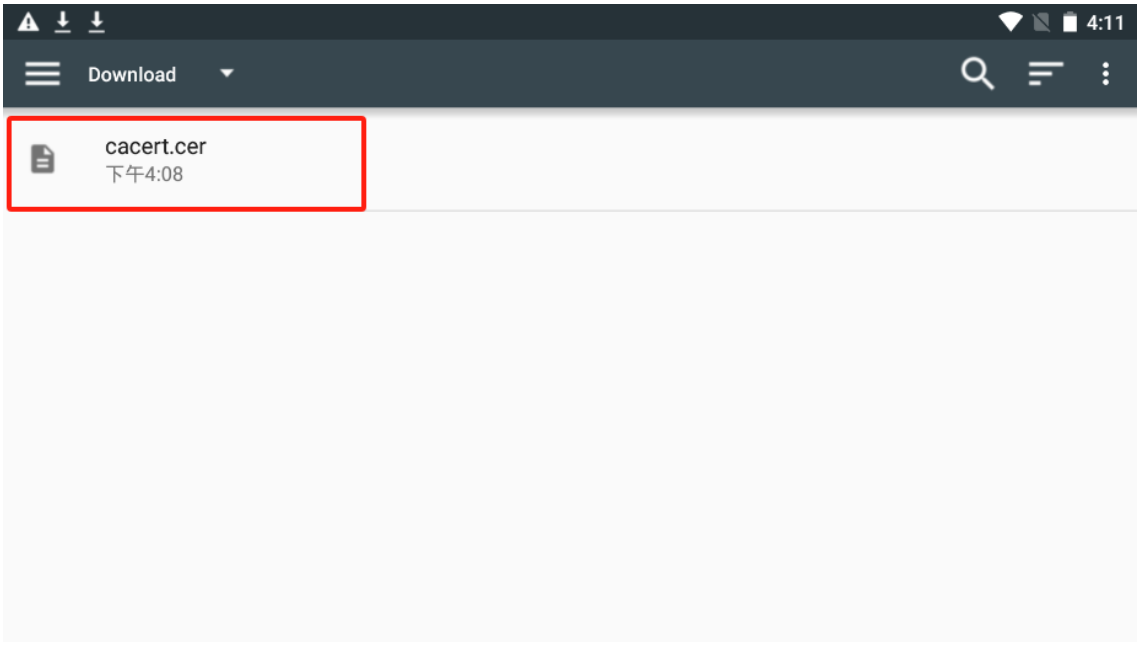


6. 安装证书

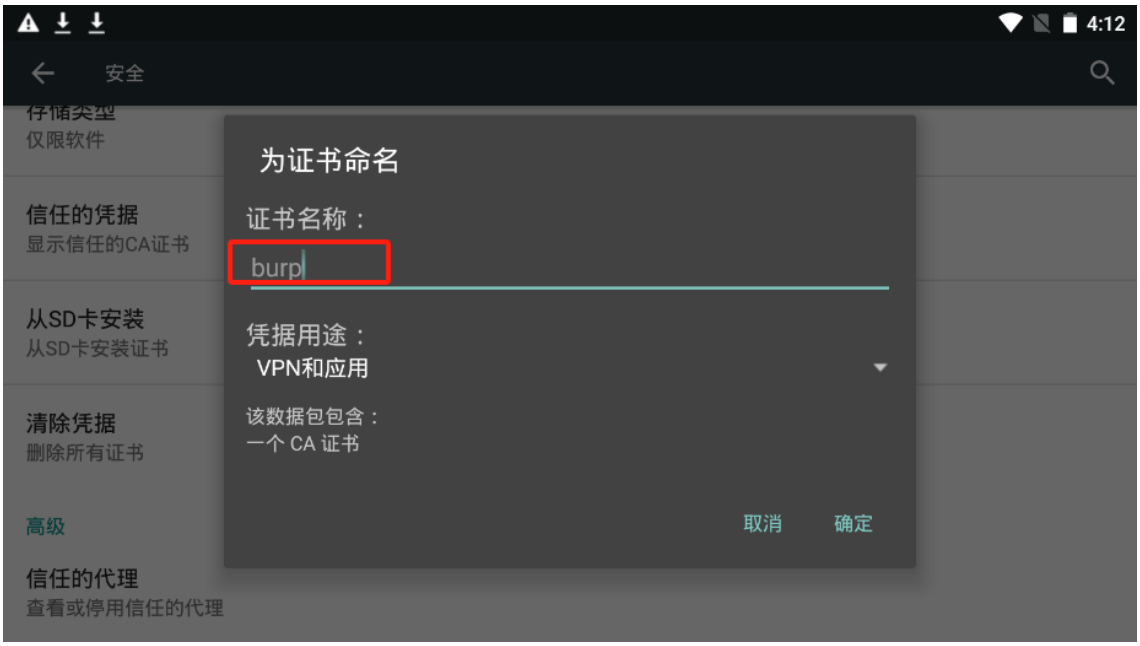
- 设置>安全>从SD卡安装>


4:11
安全
仅限软件
信任的凭据
显示信任的CA证书
从SD卡安装
从SD卡安装证书
清除凭据
删除所有证书
高级
信任的代理
查看或停用信任的代理

- 找到证书文件


4:11
Download
cacert.cer
下午4:08

- 命名任意

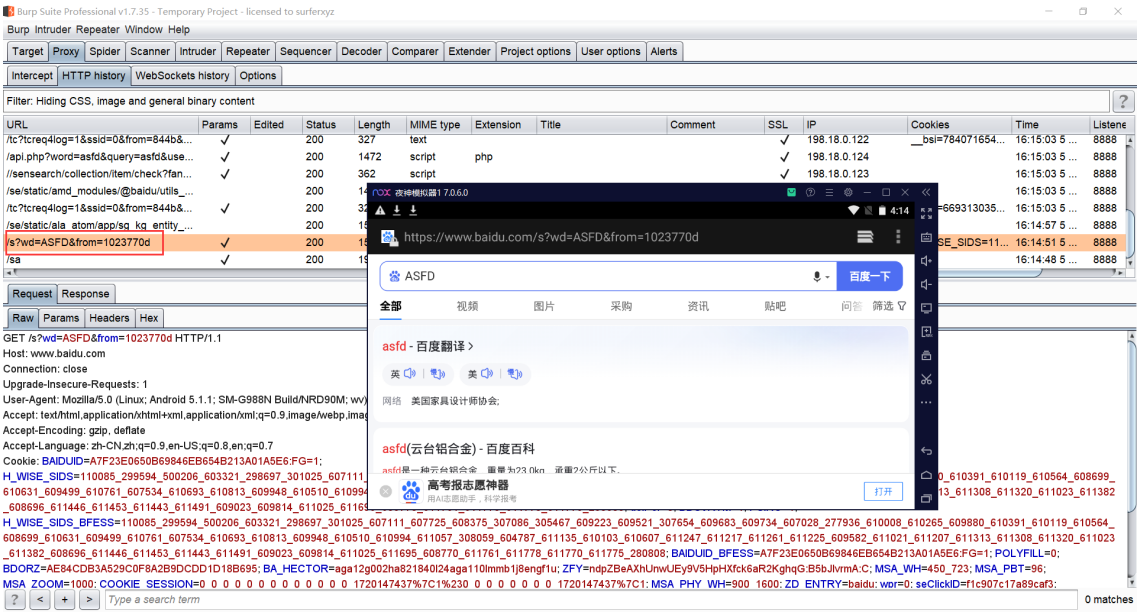


7. 设置PIN码

- 安装证书的过程需要设置密码，密码1234即可

8. 正常抓包

- 测试即可正常抓包



安卓7.0以上抓包

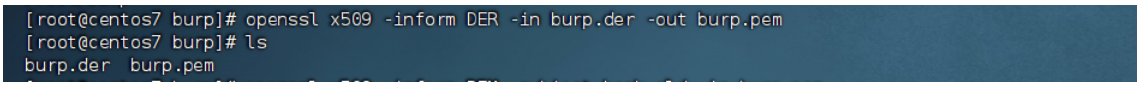
- 安卓5.1版本过低，有的时候不能满足我们的测试需求。
- Android 自 7.0 版本开始，系统不再信任用户 CA 证书（应用 targetSdkVersion >= 24 时生效，如果 targetSdkVersion < 24 即使系统是 7.0+ 依然会信任），也就是说即使安装了用户 CA 证书，应用的HTTPS包依然抓不了，会弹框证书不受信任。

1. 制作证书

- 获取有效的系统证书文件名，使用openssl 将.der格式转换成pem格式，命令如下

```
[root@centos7 burp]# openssl x509 -inform DER -in burp.der -out burp.pem
[root@centos7 burp]# ls
burp.der  burp.pem
```

执行完以后将在目录中生成burp.pem文件

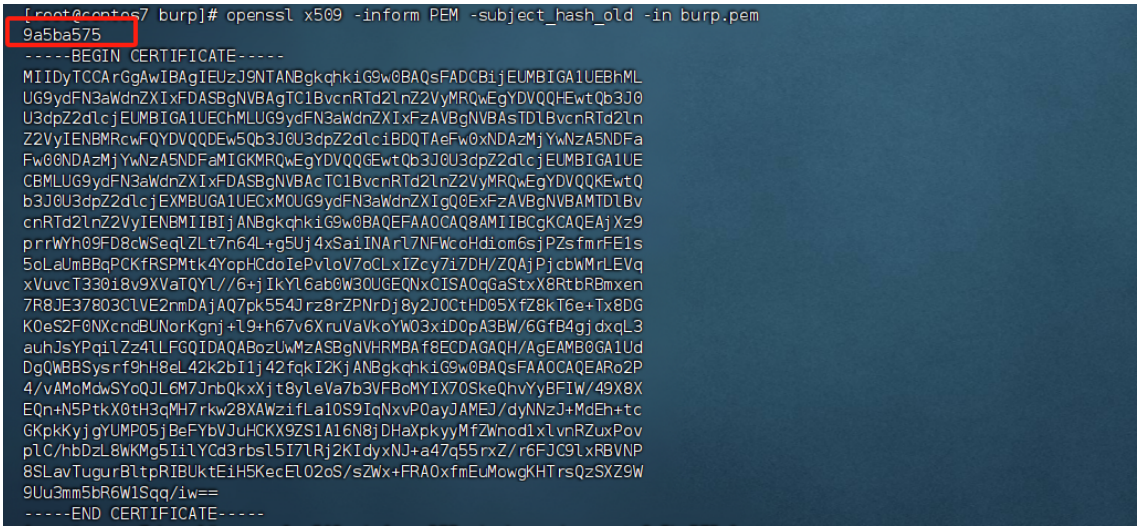


- 使用openssl 获取有效的系统证书文件名，命令如下

```
[root@centos7 burp]# openssl x509 -inform PEM -subject_hash_old -in burp.pem
9a5ba575
-----BEGIN CERTIFICATE-----
MIIDyTCCArGgAwIBAgIEUzJ9NTANBgkqhkiG9w0BAQsFADCBijEUMBIGA1UEBhML
UG9ydFN3aWdnZXIxFDASBgNVBAgTC1BvcnRTd2lnZ2VyMRQwEgYDVQQHEwtQb3J0
U3dpZ2dlcjEUMBIGA1UEChMLUG9ydFN3aWdnZXIxFzAVBgNVBAsTDlBvcnRTd2ln
Z2VyIENBMRcwFQYDVQQDEw5Qb3J0U3dpZ2dlciBDQTAeFw0xNDAzMjYwNzA5NDFa
Fw00NDAzMjYwNzA5NDFaMIGKMRQwEgYDVQQGEwtQb3J0U3dpZ2dlcjEUMBIGA1UE
CBMLUG9ydFN3aWdnZXIxFDASBgNVBAcTC1BvcnRTd2lnZ2VyMRQwEgYDVQQKEwtQ
b3J0U3dpZ2dlcjEXMBUGA1UECxMOUG9ydFN3aWdnZXIgQ0ExFzAVBgNVBAMTDlBv
cnRTd2lnZ2VyIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAjXz9
prrWYhO9FD8cWSeqlZLt7n64L+g5Uj4xSaiINArl7NFWcoHdiom6sjPZsfmrFE1s
5oLaUmBBqPCKfRSPMtk4YopHCdoIePvloV7oCLxIZcy7i7DH/ZQAjPjcbWMrLEVq
xVuvcT33Oi8v9XVaTQYl//6+jIkYl6abOw3OUGEQNxCISAOqGaStxX8RtbRBmxen
```

```
7R8JE378O3ClVE2nmDAjAQ7pk554Jrz8rZPNrDj8y2JOCtHD05XfZ8kT6e+Tx8DG
KOeS2F0NXcndBUNorKgnj+l9+h67v6XruVaVkoYWO3xiDOpA3BW/6GfB4gjdxqL3
auhJsYPqilZz4lLFGQIDAQABozUwMzASBgNVHRMBAf8ECDAGAQH/AgEAMB0GA1Ud
DgQWBBSysrf9hH8eL42k2bI1j42fqkI2KjANBgkqhkiG9w0BAQsFAAOCAQEARo2P
4/vAMoMdwSYoQJL6M7JnbQkxXjt8yleVa7b3VFBoMYIX7OSkeQhvYyBFIW/49X8X
EQn+N5PtkX0tH3qMH7rkw28XAWzifLa1OS9IqNxvPOayJAMEJ/dyNNzJ+MdEh+tc
GKpkKyjgYUMPO5jBeFYbVJuHCKX9ZS1A16N8jDHaXpkyyMfZWnod1xlvnRZuxPov
plC/hbDzL8WKMg5IilYCd3rbsl5I7lRj2KIdyxNJ+a47q55rxZ/r6FJC9lxRBVNP
8SLavTugurBltpRIBUktEiH5KecElO2oS/sZWx+FRAOxfmEuMowgKHTrsQzSXZ9W
9Uu3mm5bR6W1Sqq/iw==
-----END CERTIFICATE-----
```

- 执行完以后将输出有效的**系统证书文件名**，如下所示

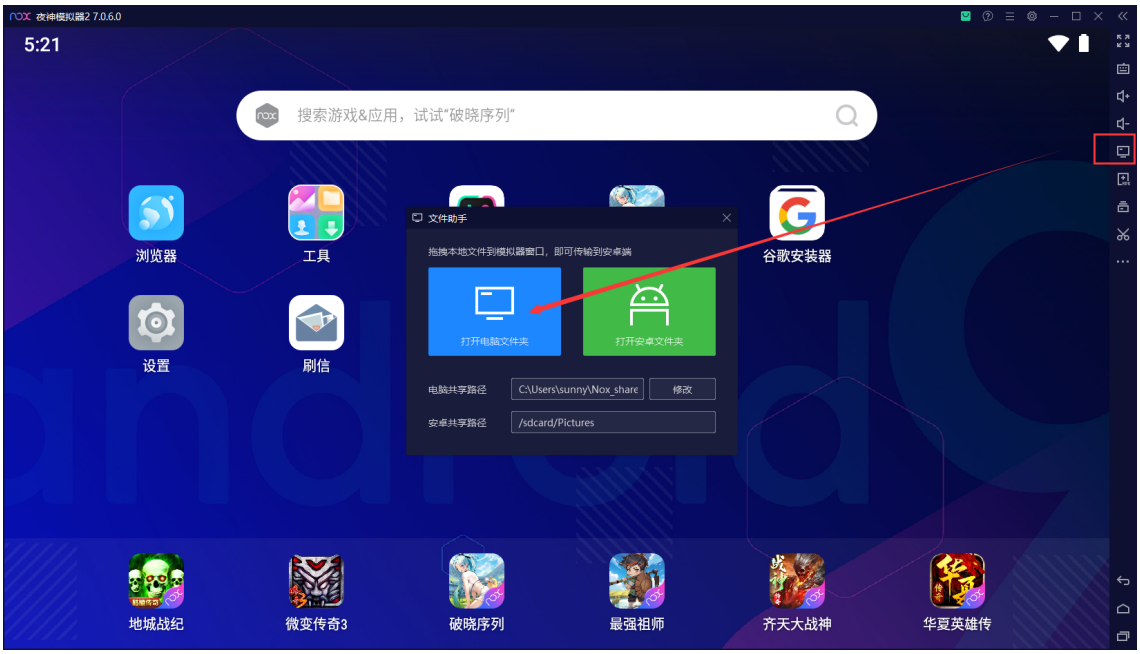


- 使用openssl 将证书文件转换为有效的系统证书文件，也就是文件名改为上面输出的系统证书文件名加上".0"，具体命令如下所示

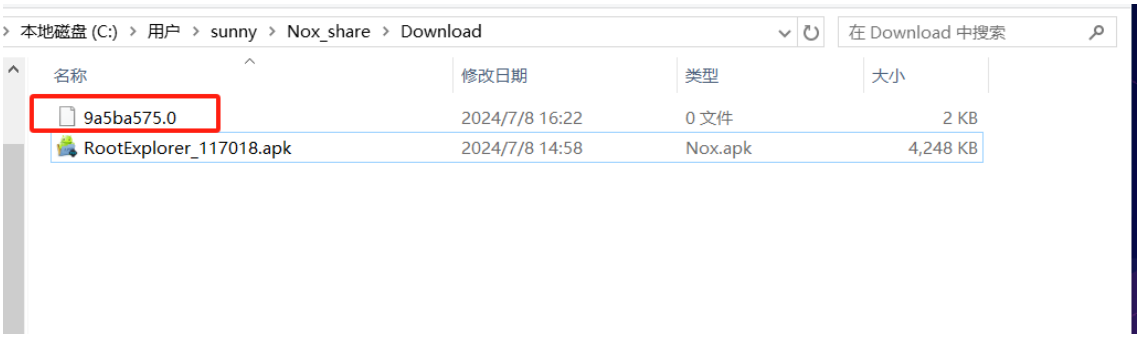
```
[root@centos7 burp]# openssl x509 -inform DER -in burp.der -out 9a5ba575.0
[root@centos7 burp]# ll
总用量 12
-rw-r--r-- 1 root root 1375 7月   8 16:08 9a5ba575.0
-rw-r--r-- 1 root root  973 7月   8 16:06 burp.der
-rw-r--r-- 1 root root 1375 7月   8 16:06 burp.pem
```

2. 导入证书

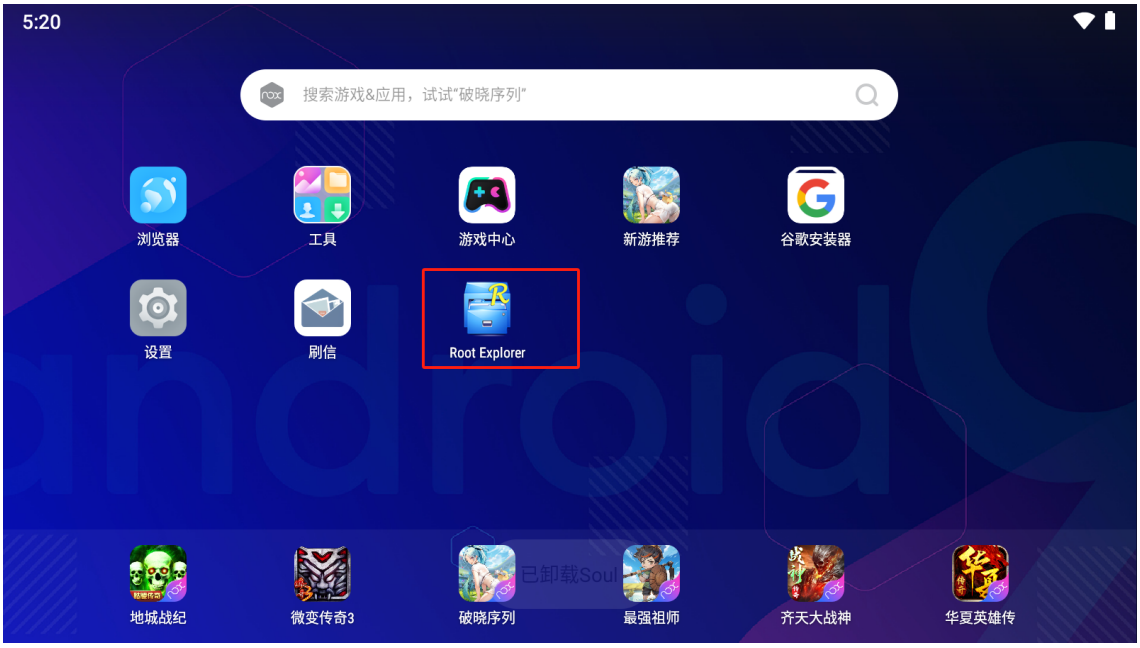
- 将生成的证书放入模拟器



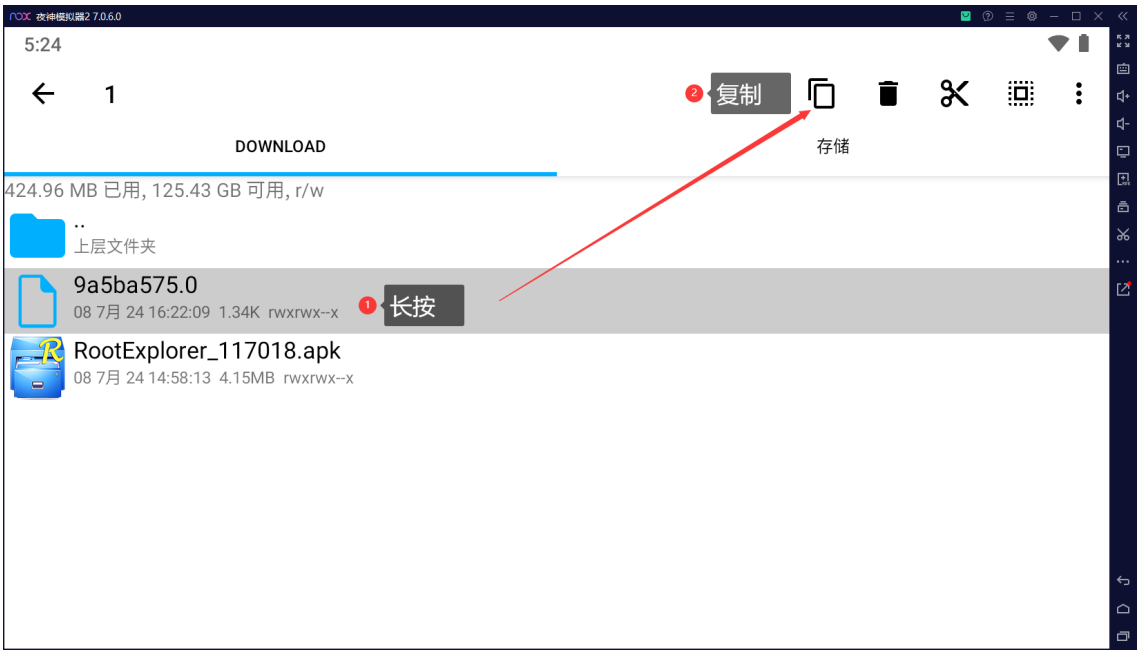
- 放到download目录下

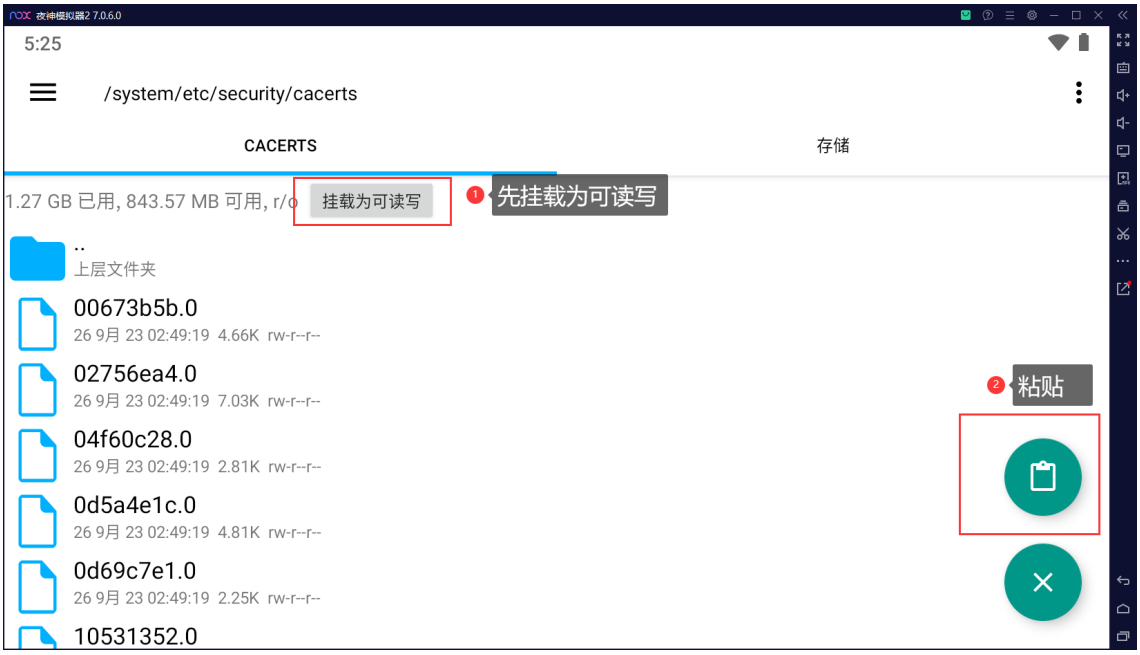


- 下载re文件管理器



- 将 `/storage/emulated/0/Download` 下的证书，复制到 `/system/etc/security/cacerts` 下





3. 夜神模拟器设置代理

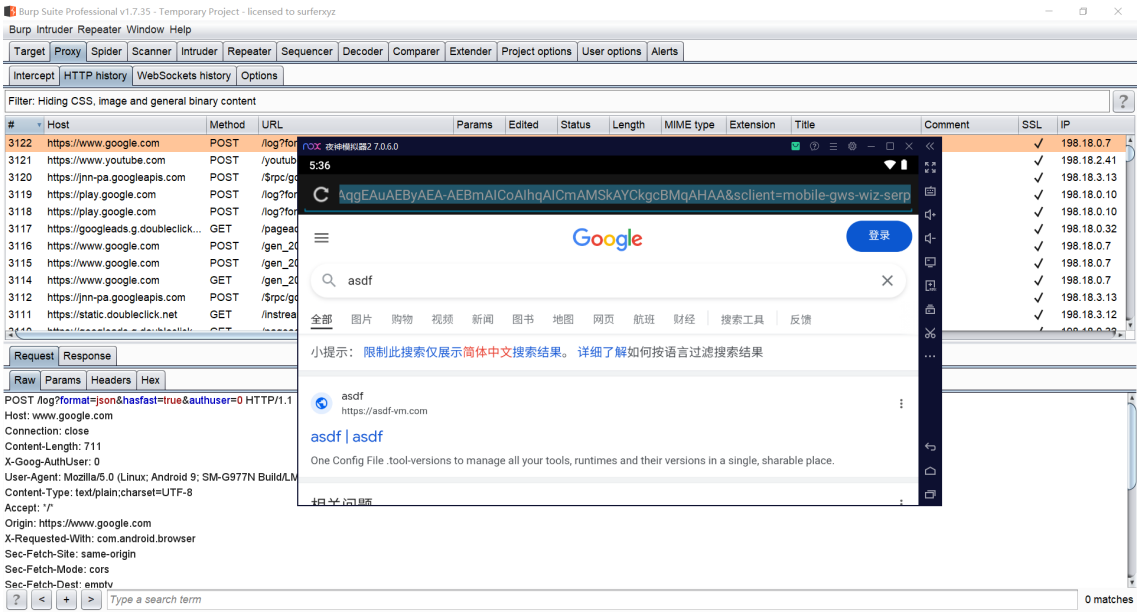
- 同上

4. Burp设置代理

- 同上

5. 正常抓包

- 测试即可正常抓包



6. 浏览器出现安全告警

- 出现以下告警，一直点击继续，直到告警消失

- 然后点击右上角三个点>设置>隐私和安全>取消显示安全告警选项

问题

- 添加模拟器时，解锁失败
  - 解决方法：将base5-disk复制到nox/bin目录下，替换掉源文件