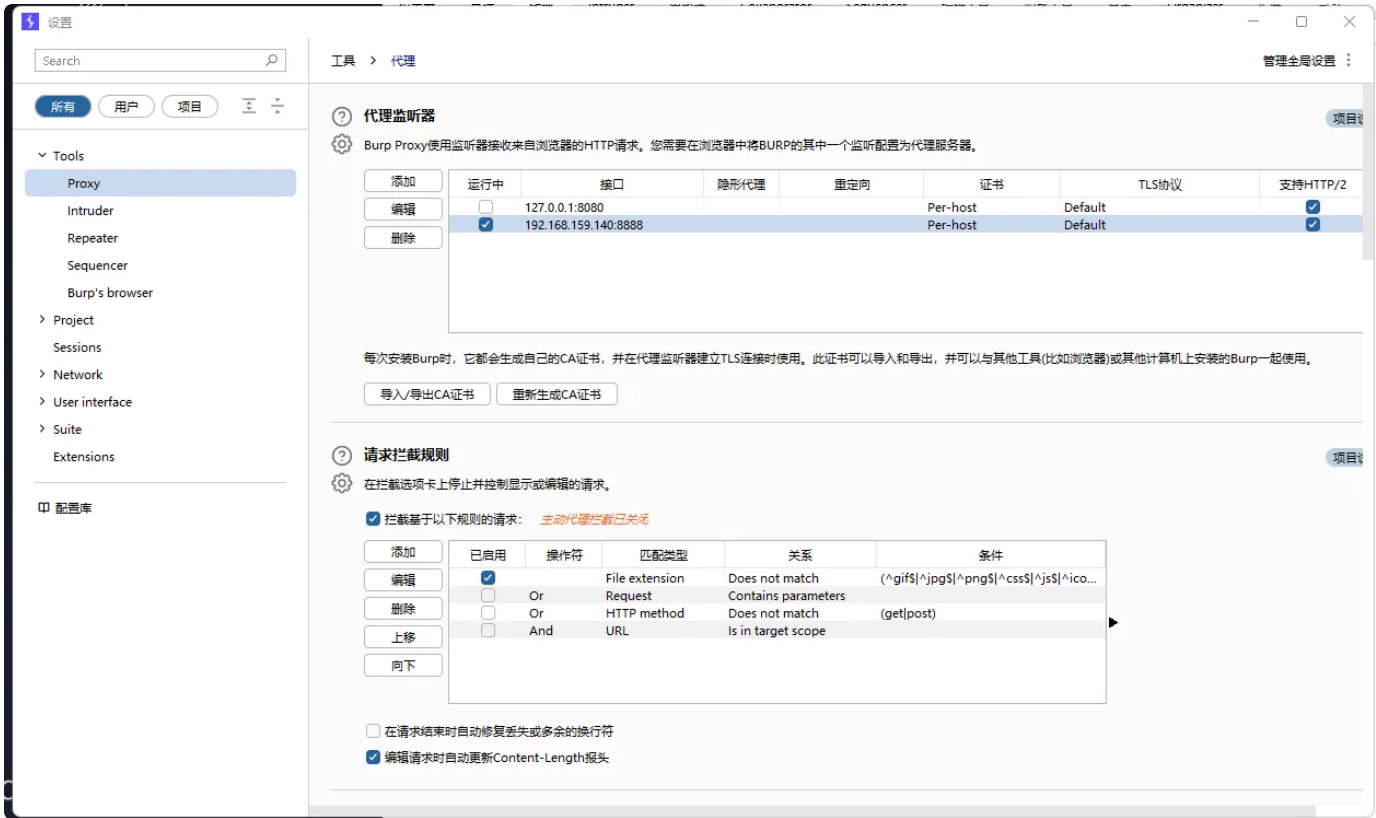


4、app抓包检测

- 1、设置burp代理
- 2、模拟器设置代理
- 3、导出CA证书

1、设置burp代理

注意IP是本机下的ip



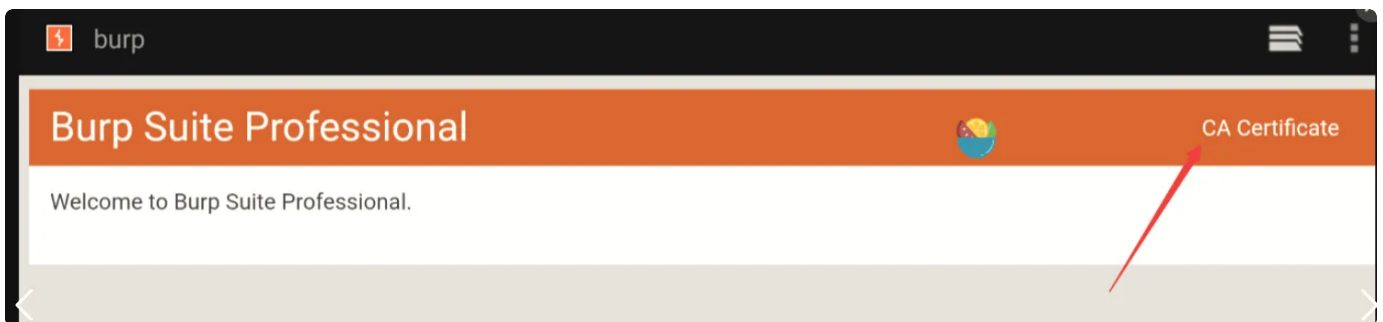
2、模拟器设置代理

点击wifi长按鼠标修改网络



3、导出CA证书

模拟器中进入http://burp页面，点击黄色的地方下载



下载证书，可以选择本地下载下来然后移到模拟器里面一般下载路径在download

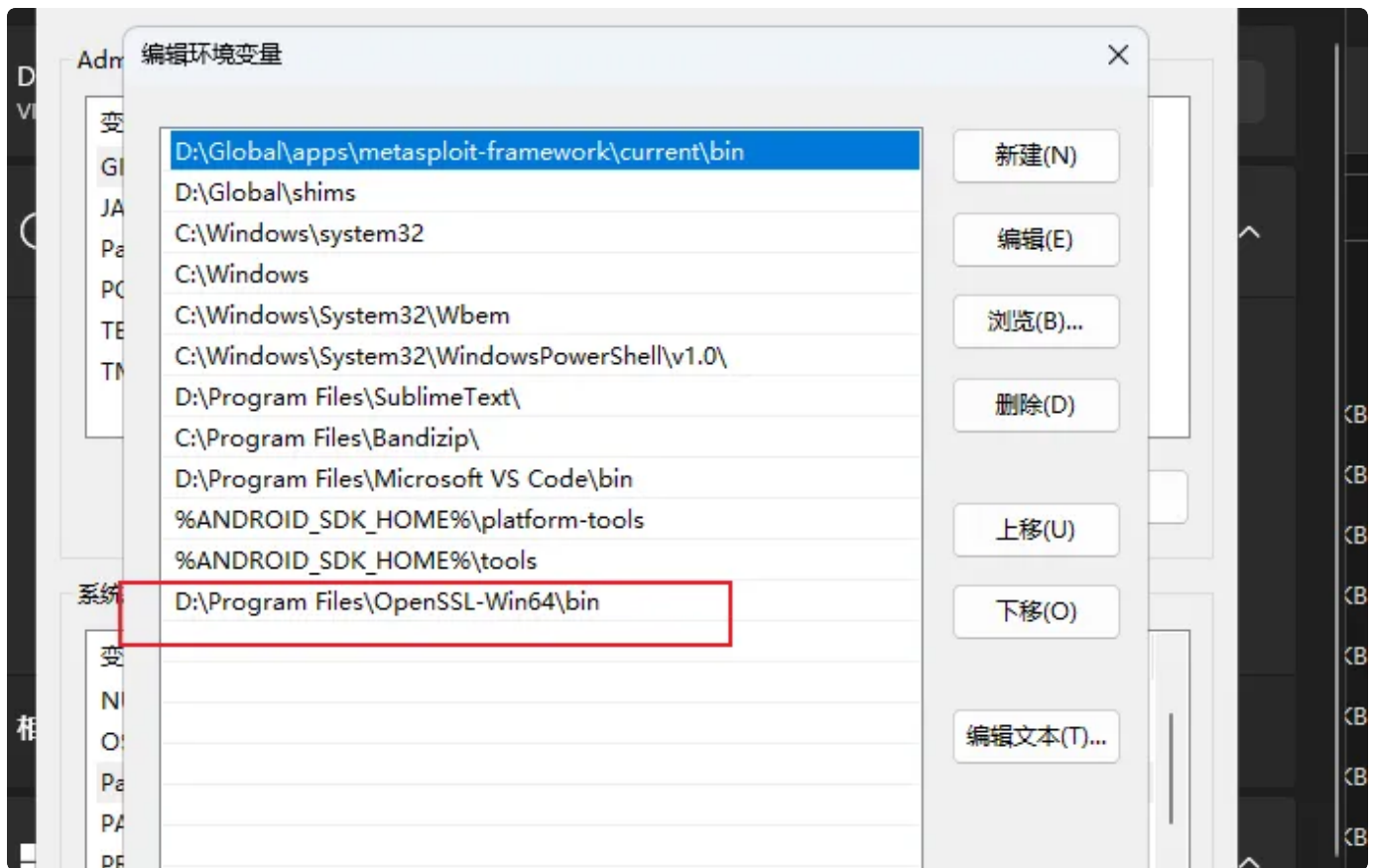
安装openssl

<https://slproweb.com/products/Win32OpenSSL.html>

根据自己电脑的配置选择需要的版本

无脑安装然后记住安装路径

配置环境变量path



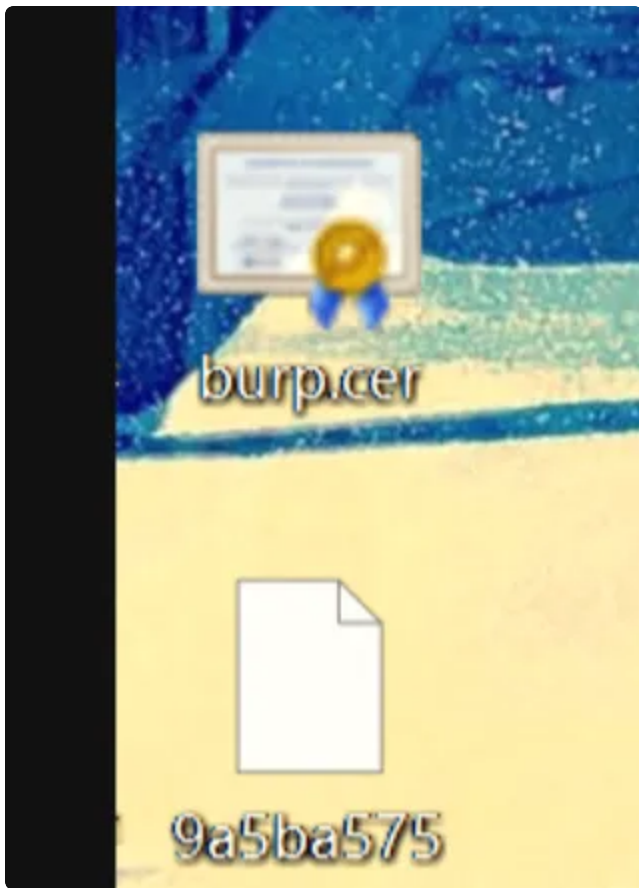
安装成功

安装openssl是用来进行证书格式转换

可以将上面的burp下载好的证书的移动到桌面，打开cmd，输入命令

```
cd Desktop
```

```
openssl x509 -inform der -in cacert.der -out burp.pem
```



**在该目录下打开cmd输入命令(该端口是夜神模拟器的端口，各模拟器可能有所不同 逍遥模拟器端口:21503)

adb connect 127.0.0.1:62001 连接

adb root 查看root

adb remount 写入权限

openssl x509 -subject_hash_old -in burp.pem 获取hash结果里证书的名称

Could not open file or uri for loading certificate from cacert.der.cer: No su

👤 Administrator on 📁 ~/Desktop

🔥 # openssl x509 -inform der -in cacert.der -out burp.pem

👤 Administrator on 📁 ~/Desktop

🔥 # openssl x509 -subject_hash_old -in burp.pem

9a5ba575

-----BEGIN CERTIFICATE-----

MIIDqDCCApCgAwIBAgIFAJJ52r0wDQYJKoZIhvcNAQELBQAwYoxFDASBgNVBAYT
C1BvcnRTd2lnZ2VyMRQwEgYDVQQIEwtQb3J0U3dpZ2dldjEUMBIGA1UEBxMLUG9y
dFN3aWdnZXIxFDASBgNVBAoTC1BvcnRTd2lnZ2VyMRcwFQYDVQQLEw5Qb3J0U3dp
Z2dldjEiBDQTEKMBUGA1UEAxM0UG9ydFN3aWdnZXIgc0EwHhcNMTQxMTA3MDYxMjU4
WhcNMzIxMTA3MDYxMjU4WjCBiEUMBIGA1UEBhMLUG9ydFN3aWdnZXIxFDASBgNV
BAGTC1BvcnRTd2lnZ2VyMRQwEgYDVQQHEwtQb3J0U3dpZ2dldjEUMBIGA1UEChML
UG9ydFN3aWdnZXIxFzAVBgNVBAsTDlBvcnRTd2lnZ2VyIENBMRCwFQYDVQQDEw5Q
b3J0U3dpZ2dldjEiBDQTEKCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAlE
PMvoXbdRtvSRKkEsaqwkAW0ELPWqHqo6imlvGDVmtLd0bI6RmHDniL9EZhxHIA/
N5RGjuum3u44rEFDuNdx9UIU+ysxszjCeQ67A+cPkxtBaYbMZCwFS6W00NfJcKGT
HSGw+ys3XdhQPnCiQJ0uB3HZzVnodaPrMKyTA54rSCzeYpvtCCyswxTZU8joGUU2r
PuunnmdyIM4saA74q3GhSht41US027UVXm7MX/Wjsn9aJqw0BM70VfqKEp0Vj70c
55NTyf3wwyFr1a/9eaU+WvmwaRWLd92mf1PtRzqA6M4QnW0goQb1C7P60gvL0ub1
cUCKk2rbGIrCxa9GfvcCAwEAAAMTMBEwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG
9w0BAQsFAA0CAQEAPn+LI0Cm0djV0AjeSGVhBv7mrhl98T/0qhTaAetdw2VXTVS
BX3xDBZeg0jj/gd07Q36FQSGn5vZho1KxIMmtdzrzqedMr0+M6vuNwT2FUNmUxLR
B3HUfLMG9HbfEDlFHFJbEb7iGAxqLDhUmPKHR45Xhs6SuGmSn60R/qsrKadPYLxa
AJSrwWyIaIjkdureNXfNiIekHhngi7WKqIansv3deUM3EwaGjWRUR0eo/quy+Sno
JL7gGnErGoaI6WES/aAB2wrXlMp4sAHXbbwRt08jpVxAobTbUu05v7ipC+VfafWU
q0rH6iz2yXbmB1m+T9kGK0B95+PSdVuhf7CEww==

▼

Python |

```
1 adb push 9a5ba575.0 /system/etc/security/cacerts/
```

我们最后到模拟器中查看是否安装成功

设置 安全 找到 信任任凭



设备管理器

查看或停用设备管理器

未知来源

允许安装来自未知来源的应用

凭据存储

存储类型

硬件支持

信任的凭据

显示信任的CA证书

用户凭据

查看和修改存储的凭据



拦截HTTP历史记录WebSocket历史记录代理设置

过滤: 隐藏CSS, 图片, 一般二进制文件

#	Host	方法	URL	参数	已编辑	状态码	长度	MIME类型	扩展
379	https://bi.yeshen.com	POST	/sa	✓		200	194	text	
380	https://newservice.d.com.cn	POST	/	✓		200	9597	JSON	
382	https://newservice.d.com.cn	POST	/	✓		200	445	JSON	
383	https://newservice.d.com.cn	POST	/	✓		200	2386	JSON	
384	https://newservice.d.com.cn	POST	/	✓		200	1057	JSON	
385	https://bi.yeshen.com	POST	/sa	✓		200	194	text	
387	https://newservice.d.com.cn	POST	/	✓		200	448	JSON	
388	https://bi.yeshen.com	POST	/sa	✓		200	194	text	
389	https://bi.yeshen.com	POST	/sa	✓		200	194	text	
390	https://bi.yeshen.com	POST	/sa	✓		200	194	text	

请求

美化RawHex

1 POST / HTTP/1.1

2 Content-Type: application/x-www-form-urlencoded; charset=UTF-8

3 User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.1.2; SM-G9810 Build/QP1A.190711.020)

4 Host: newservice.d.com.cn

5 Connection: close

6 Accept-Encoding: gzip, deflate

7 Content-Length: 233

8

9 notice_token=8294fa7338c5150c&_cmd=app_notice&device_width=720&_deviceid=8294fa7338c5150c&device_os=7.1.2¬iceflag=1&_client=ANDROID&version=4.2.6&channel=mime&device_height=1280&_sign=3e4fca17c3ab568dbe7db1f585358c27&_token=

响应

美化RawHex页面渲染

1 HTTP/1.1 200 OK

2 Server: nginx

3 Date: Wed, 18 Sep 2024 08:32:28 GMT

4 Content-Type: application/json; charset=utf8

5 Connection: close

6 Set-Cookie: PHPSESSID=1a7g6rci6od6pplorci3ed9gul; path=/; domain=.d.com.cn

7 Expires: Thu, 19 Nov 1981 08:52:00 GMT

8 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

9 Pragma: no-cache

10 Content-Length: 77

11

12 {

13 "code": "0",

14 "msg": "",

15 "data": {

16 "msg": "appToken"

17 },

18 "time": 1726648345

19 }

<https://blog.csdn.net/liamin416100569/article/details/129176916>