MoGua

——助手 2.3.5.8.APK 分析报告

APP名称: ——助手

包名:	com.wjmt.app
域名线索:	32条
URL线索:	41条
邮箱线索:	1条
分析日期:	2025年2月22日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 梦VS大师2358终极版.apk
文件大小: 16.63MB
MD5值: c869288ad09ec911f8b1d447e69ec098
SHA1值: 4c1ddfe8103e4f94acc0be1695e2af1c517c1f6b
SHA256值: e023427a8188a085456089782d3a82c322811a2a9552c26859fa1e326a685e3c

APP 信息

App名称: 一一助手
包名: com.wjmt.app
主活动Activity: com.mingning179.MainActivity
安卓版本名称: 2.3.5.8
安卓版本: 2358

域名线索

域名	服务器信息
www.android.com	**IP**: 142.250.217.78 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
app.navi.baidu.com	**IP**: 111.206.209.213 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
weibo.com	**IP**: 116.133.8.19 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397102
xerces.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api.cellocation.com	**IP**: 43.143.208.149 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
m.baidu.com	**IP**: 110.242.71.66 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
aweme.snssdk.com	**IP**: 123.125.216.228 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ofloc.map.baidu.com	**IP**: 111.206.209.193 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
image.cnamedomain.com	没有服务器地理信息.

43.163.3.132	**IP**: 43.163.3.132 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
api.map.baidu.com	**IP**: 111.206.208.72 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
oss-cn-.aliyuncs.comor	没有服务器地理信息.
loc.map.baidu.com	**IP**: 111.206.209.175 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
daohang.map.baidu.com	**IP**: 111.206.209.190 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
39.97.97.160	**IP**: 39.97.97.160 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
bbs.lbsyun.baidu.com	没有服务器地理信息.

127.0.0.1	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
203.107.1.1	**IP**: 203.107.1.1 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
map.baidu.com	**IP**: 111.206.208.32 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
169.254.169.254	**IP**: 169.254.169.254 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
itsdata.map.baidu.com	**IP**: 111.206.209.180 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
38.6.186.227	**IP**: 38.6.186.227 **所属国家**: United States of America **地区**: California **城市**: San Jose

	纬度: 37.333698 **经度**: -121.889297
obs-ysy-apks.obs.cn-south-1.myhuaweicloud.com	IP: 139.159.208.67 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
oss.aliyuncs.com	IP: 118.178.29.5 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
oss-cn-hangzhou.aliyuncs.com	IP: 118.31.219.189 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
www.slf4j.org	IP: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
xml.org	IP: 104.239.240.11 **所属国家**: United States of America **地区**: Texas **城市**: Windcrest **纬度**: 29.499678 **经度**: -98.399246
acs.amazonaws.com	没有服务器地理信息.

daup.map.baidu.com	**IP**: 110.242.69.98 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
192.168.0.100	**IP**: 192.168.0.100 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
schemas.android.com	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/a/e.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/a/e.java
http://oss-cn-hangzhou.aliyuncs.com	com/alibaba/sdk/android/a/b/c.java
http://203.107.1.1/181345/d?host=	com/alibaba/sdk/android/a/b/b/f.java

http://oss.aliyuncs.com	com/alibaba/sdk/android/a/d/f.java
http://127.0.0.1	com/alibaba/sdk/android/a/d/f.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/a/d/f.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/a/d/f.java
http://acs.amazonaws.com/groups/global/AllUsers	com/b/b/b/b.java
http://acs.amazonaws.com/groups/global/AuthenticatedUsers	com/b/b/b/b.java
http://acs.amazonaws.com/groups/s3/LogDelivery	com/b/b/b/b.java
http://acs.amazonaws.com/groups/global/AllUsers	com/b/b/b/t.java
http://acs.amazonaws.com/groups/global/AuthenticatedUsers	com/b/b/b/t.java
http://acs.amazonaws.com/groups/s3/LogDelivery	com/b/b/b/t.java
http://acs.amazonaws.com/groups/s3/LogDelivery	com/b/b/b/l.java
http://169.254.169.254	com/b/b/b/d/b.java
http://acs.amazonaws.com/groups/global/AllUsers	com/b/b/c/aw.java
http://acs.amazonaws.com/groups/global/AuthenticatedUsers	com/b/b/c/aw.java
http://acs.amazonaws.com/groups/s3/LogDelivery	com/b/b/c/aw.java
http://xml.org/sax/features/external-general-entities	com/b/c/a/a/a.java
http://xerces.apache.org/xerces-j/features.html	com/b/c/a/a/a.java

http://xerces.apache.org/xerces2-j/features.html	com/b/c/a/a/a.java
http://xml.org/sax/features/external-parameter-entities	com/b/c/a/a/a.java
https://loc.map.baidu.com/cc.php	com/baidu/location/b/g.java
https://ofloc.map.baidu.com/locnu	com/baidu/location/b/ab.java
https://itsdata.map.baidu.com/long-conn-gps/sdk.php	com/baidu/location/b/i.java
https://loc.map.baidu.com/cfgs/loc/commcfgs	com/baidu/location/b/a.java
https://daup.map.baidu.com/cltr/rcvr	com/baidu/location/b/ac.java
http://loc.map.baidu.com/sdk.php	com/baidu/location/e/l.java
https://loc.map.baidu.com/sdk_ep.php	com/baidu/location/e/l.java
http://loc.map.baidu.com/user_err.php	com/baidu/location/e/l.java
http://loc.map.baidu.com/oqur.php	com/baidu/location/e/l.java
https://loc.map.baidu.com/tcu.php	com/baidu/location/e/l.java
http://loc.map.baidu.com/rtbu.php	com/baidu/location/e/l.java
http://loc.map.baidu.com/iofd.php	com/baidu/location/e/l.java
http://loc.map.baidu.com/wloc	com/baidu/location/e/l.java
https://loc.map.baidu.com/sdk.php	com/baidu/location/e/l.java
https://daup.map.baidu.com/cltr/rcvr	com/baidu/location/e/l.java
http://app.navi.baidu.com/mobile/	com/baidu/mapapi/navi/BaiduMapNavigation.java

http://daohang.map.baidu.com/mobile/	com/baidu/mapapi/navi/BaiduMapNavigation.java
http://map.baidu.com/zt/client/index/?fr=sdk_[	com/baidu/mapapi/utils/OpenClientUtil.java
http://api.map.baidu.com/place/detail?uid=	com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java
http://api.map.baidu.com/place/search?	com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java
http://api.map.baidu.com/direction?	com/baidu/mapapi/utils/route/BaiduMapRoutePlan.java
http://bbs.lbsyun.baidu.com/forum.php?mod=viewthread&tid=106461\n==========\n	com/baidu/mapsdkplatform/comapi/util/PermissionCheck.java
https://api.map.baidu.com/lbs_sdkcc/report	com/baidu/mapsdkplatform/comapi/b/a/c.java
https://api.map.baidu.com/sdkcs/verify	com/baidu/lbsapi/auth/LBSAuthManager.java
http://xml.org/sax/properties/lexical-handler	com/caverock/androidsvg/h.java
http://38.6.186.227	com/mingning179/data/AliyunOssUtil.java
https://obs-ysy-apks.obs.cn-south-1.myhuaweicloud.com:443/configFiles%2F1a2b3511e8de426092d9e83a29e87ff3	com/mingning179/commonutils/ConversionUtil.java
http://api.cellocation.com:81/	com/mingning179/networkapi/request/RecellInfoRequest.java
http://api.cellocation.com:81/	com/mingning179/networkapi/request/RewifiInfoRequest.java
http://43.163.3.132:80/api/	com/mingning179/a/a.java
http://39.97.97.160:80/	com/mingning179/a/a.java
http://api.cellocation.com:81/	com/mingning179/a/a.java
https://obs-ysy-apks.obs.cn-south-1.myhuaweicloud.com:443/	com/mingning179/http/GetBackUpFile.java

https://weibo.com/signup/v5/formcheck?type=mobilesea&zone=0086&value=	com/mingning179/http/controller/DetectionWeiboAccountCtrl.java
https://weibo.com/signup/signup.php	com/mingning179/http/controller/DetectionWeiboAccountCtrl.java
http://m.baidu.com	com/mingning179/http/controller/StartSettingCtrl.java
https://aweme.snssdk.com/aweme/v1/user/profile/other/?user_id=	com/ss/android/ugc/aweme/ContextHelper.java
http://192.168.0.100:8088/test/testaa	com/lt/km.java
http://www.slf4j.org/codes.html	org/e/e.java
http://www.slf4j.org/codes.html	org/e/d.java
http://www.android.com/	org/e/d.java
http://api.map.baidu.com/geocoding/v3/?address=	kxj/newgjforsystem/activity/MapActivity.java
http://127.0.0.1:	kxj/newgjforsystem/activity/GJpartner.java
http://43.163.3.132/api/appCollectInfo/getGaiJiPartnerInfo?token=false&phoneId=	kxj/newgjforsystem/activity/GJpartner.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/n.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java

邮箱线索

邮箱地址	所在文件

javamail@sun.com	com/e/b/d/e.java

手机线索

手机号	所在文件
18345352118	com/baidu/mapsdkplatform/comapi/util/b.java
17179869184	com/caverock/androidsvg/d.java
17179869184	com/caverock/androidsvg/h.java
17179869184	com/caverock/androidsvg/e.java

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-04-15 22:40:50+00:00
有效期至: 2035-09-01 22:40:50+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0xb3998086d056cffa
哈希算法: md5
md5值: 8ddb342f2da5408402d7568af21e29f9
sha1值: 27196e386b875e76adf700e7ea84e4c6eee33dfa
sha256值: c8a2e9bccf597c2fb6dc66bee293fc13f2fc47ec77bc6b2b0d52c11f51192ab8
sha512值: 5d802f24d6ac76c708a8e7afe28fd97e038f888cef6665fb9b4a92234c311d6ff42127ccb2eb5a898f4e7e4e553f6ef602d43d1a2ebae9f002a6598e72fd2d83

公钥算法: rsa
密钥长度: 2048
指纹: 65ba0830722d5767f8779e37d0d9c67562f03ec63a2889af655ee9c59effb434

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息

android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取

应用内通信
