



# MoGua

## 母狗园 2.3.0.APK 分析报告



APP名称:

母狗园

包名: com.androidjks.aw.d1735030412293165332

域名线索: 20条

URL线索: 32条

邮箱线索: 4条

分析日期: 2025年10月2日

分析平台: [摸瓜APK反编译平台](#)

文件名: shishidh\_2.3.0\_30539743.apk  
文件大小: 40.4MB  
MD5值: 9268475e8b125fd1024674245be75bdd  
SHA1值: ae44a4e70d7d1975d3447265c3af40231cad9ebb  
SHA256值: c9a67930b0094eb92a9f1d183bcf35ab3c36b4d8d58759a0ac8e8a5b5f8fc0ff

# i APP 信息

App名称: 母狗园  
包名: com.androidjks.aw.d1735030412293165332  
主活动Activity: com.grass.mh.SplashActivity  
安卓版本名称: 2.3.0  
安卓版本: 230

## 🔍 域名线索

| 域名                       | 服务器信息                                                                                                                          |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| data.flurry.com          | IP: 98.136.147.17<br>所属国家: United States of America<br>地区: New York<br>城市: New York City<br>纬度: 40.731323<br>经度: -73.990089    |
| aw.vkdzygl0.xyz          | 没有服务器地理信息.                                                                                                                     |
| playready.directtaps.net | IP: 104.45.231.79<br>所属国家: United States of America<br>地区: California<br>城市: San Francisco<br>纬度: 37.774929<br>经度: -122.419418 |
|                          |                                                                                                                                |

|                                                    |                                                                                                                       |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| www.example.com                                    | IP: 173.222.245.18<br>所属国家: Italy<br>地区: Lazio<br>城市: Rome<br>纬度: 41.894253<br>经度: 12.484253                          |
| github.com                                         | IP: 20.205.243.166<br>所属国家: Singapore<br>地区: Singapore<br>城市: Singapore<br>纬度: 1.289987<br>经度: 103.850281             |
| www.sl4j.org                                       | IP: 127.0.0.1<br>所属国家: -<br>地区: -<br>城市: -<br>纬度: 0.000000<br>经度: 0.000000                                            |
| freemarker.org                                     | IP: 192.64.119.217<br>所属国家: United States of America<br>地区: Georgia<br>城市: Atlanta<br>纬度: 33.727291<br>经度: -84.425377 |
| tc-bj-alijs-1324672756.cos.ap-beijing.myqcloud.com | IP: 153.3.46.162<br>所属国家: China<br>地区: Jiangsu<br>城市: Nanjing<br>纬度: 32.061668<br>经度: 118.777992                      |
| freemarker.apache.org                              | IP: 151.101.2.132<br>所属国家: United States of America<br>地区: California<br>城市: San Francisco                            |

|                              |                                                                                                                                                                  |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | <b>纬度:</b> 37.775700<br><b>经度:</b> -122.395203                                                                                                                   |
| d56pev9tevmkv.cloudfront.net | IP: 3.169.8.196<br><b>所属国家:</b> United States of America<br><b>地区:</b> Washington<br><b>城市:</b> Seattle<br><b>纬度:</b> 47.627499<br><b>经度:</b> -122.346199        |
| schemas.android.com          | 没有服务器地理信息.                                                                                                                                                       |
| api.login.yahoo.com          | IP: 74.6.160.138<br><b>所属国家:</b> United States of America<br><b>地区:</b> New York<br><b>城市:</b> New York City<br><b>纬度:</b> 40.731323<br><b>经度:</b> -73.990089    |
| www.w3.org                   | IP: 104.18.23.19<br><b>所属国家:</b> United States of America<br><b>地区:</b> California<br><b>城市:</b> San Francisco<br><b>纬度:</b> 37.775700<br><b>经度:</b> -122.395203 |
| aw.vjgx0zd6.xyz              | 没有服务器地理信息.                                                                                                                                                       |
| aw.vekqdyjy.xyz              | 没有服务器地理信息.                                                                                                                                                       |
| schemas.microsoft.com        | IP: 13.107.246.73<br><b>所属国家:</b> United States of America<br><b>地区:</b> Washington<br><b>城市:</b> Redmond<br><b>纬度:</b> 47.682899<br><b>经度:</b> -122.120903      |
|                              | IP: 85.13.163.69                                                                                                                                                 |

|                               |                                                                                                                                                                      |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| greenrobot.org                | <b>所属国家:</b> Germany<br><b>地区:</b> Thuringen<br><b>城市:</b> Friedersdorf<br><b>纬度:</b> 50.604919<br><b>经度:</b> 11.035770                                              |
| d12ilce452zs0c.cloudfront.net | <b>IP:</b> 18.65.214.130<br><b>所属国家:</b> Japan<br><b>地区:</b> Tokyo<br><b>城市:</b> Tokyo<br><b>纬度:</b> 35.689499<br><b>经度:</b> 139.692322                              |
| cfg.flurry.com                | <b>IP:</b> 69.147.80.12<br><b>所属国家:</b> United States of America<br><b>地区:</b> New York<br><b>城市:</b> New York City<br><b>纬度:</b> 40.731323<br><b>经度:</b> -73.990089 |
| clsp.fun                      | <b>IP:</b> 143.92.53.209<br><b>所属国家:</b> Hong Kong<br><b>地区:</b> Hong Kong<br><b>城市:</b> Hong Kong<br><b>纬度:</b> 22.285521<br><b>经度:</b> 114.157692                  |

 URL线索

| URL信息                                                                                                                           | Url所在文件                                  |
|---------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| <a href="https://github.com/danikula/AndroidVideoCache/issues/88">https://github.com/danikula/AndroidVideoCache/issues/88</a> . | com/danikula/mp3cache/HttpUrlSource.java |
| <a href="https://github.com/danikula/AndroidVideoCache/issues/43">https://github.com/danikula/AndroidVideoCache/issues/43</a> . | com/danikula/mp3cache/HttpUrlSource.java |
|                                                                                                                                 |                                          |

|                                                           |                                                   |
|-----------------------------------------------------------|---------------------------------------------------|
| https://github.com/danikula/AndroidVideoCache/issues.     | com/danikula/mp3cache/HttpUrlSource.java          |
| https://github.com/danikula/AndroidVideoCache/issues/134. | com/danikula/mp3cache/Pinger.java                 |
| http://%s:%d/%s                                           | com/danikula/mp3cache/Pinger.java                 |
| http://%s:%d/%s                                           | com/danikula/mp3cache/HttpProxyCacheServer.java   |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/videocache/HttpUrlSource.java        |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/danikula/videocache/HttpUrlSource.java        |
| https://github.com/danikula/AndroidVideoCache/issues.     | com/danikula/videocache/HttpUrlSource.java        |
| https://github.com/danikula/AndroidVideoCache/issues/134. | com/danikula/videocache/Pinger.java               |
| http://%s:%d/%s                                           | com/danikula/videocache/Pinger.java               |
| http://%s:%d/%s                                           | com/danikula/videocache/HttpProxyCacheServer.java |
| http://www.example.com                                    | com/flurry/sdk/ed.java                            |
| https://cfg.flurry.com/sdk/v1/config                      | com/flurry/sdk/cl.java                            |
| https://cfg.flurry.com/sdk/v1/config                      | com/flurry/sdk/by.java                            |
| https://data.flurry.com/v1/flr.do                         | com/flurry/sdk/br.java                            |
| https://api.login.yahoo.com/oauth2/device_session         | com/flurry/sdk/ef.java                            |
| https://aw.vekdyjy.xyz                                    | com/grass/mh/SplashActivity.java                  |
| https://aw.vjgx0zd6.xyz                                   | com/grass/mh/SplashActivity.java                  |
| https://aw.vkdzygl0.xyz                                   | com/grass/mh/SplashActivity.java                  |

|                                                                                                                                                     |                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| <a href="https://d56pev9tevmkv.cloudfront.net/aw.json">https://d56pev9tevmkv.cloudfront.net/aw.json</a>                                             | com/grass/mh/SplashActivity.java                             |
| <a href="https://tc-bj-alijs-1324672756.cos.ap-beijing.myqcloud.com/aw.json">https://tc-bj-alijs-1324672756.cos.ap-beijing.myqcloud.com/aw.json</a> | com/grass/mh/SplashActivity.java                             |
| <a href="https://d12ilce452zs0c.cloudfront.net/aw_ldy.json">https://d12ilce452zs0c.cloudfront.net/aw_ldy.json</a>                                   | com/grass/mh/SplashActivity.java                             |
| <a href="https://clsp.fun">https://clsp.fun</a>                                                                                                     | com/grass/mh/databinding/ActivityShareLayoutBindingImpl.java |
| <a href="https://freemarker.apache.org/docs/ref_builtins.html">https://freemarker.apache.org/docs/ref_builtins.html</a> ;                           | freemarker/core/BuiltIn.java                                 |
| <a href="http://freemarker.org/docs/ref_directive_list.html">http://freemarker.org/docs/ref_directive_list.html</a> ).                              | freemarker/core/FMParserTokenManager.java                    |
| <a href="http://freemarker.org/docs/ref_directive_alphaidx.html">http://freemarker.org/docs/ref_directive_alphaidx.html</a> ;                       | freemarker/core/FMParserTokenManager.java                    |
| <a href="https://github.com/ReactiveX/RxJava/wiki/Plugins">https://github.com/ReactiveX/RxJava/wiki/Plugins</a>                                     | io/reactivex/Completable.java                                |
| <a href="https://github.com/ReactiveX/RxJava/wiki/Plugins">https://github.com/ReactiveX/RxJava/wiki/Plugins</a>                                     | io/reactivex/Maybe.java                                      |
| <a href="https://github.com/ReactiveX/RxJava/wiki/Plugins">https://github.com/ReactiveX/RxJava/wiki/Plugins</a>                                     | io/reactivex/Single.java                                     |
| <a href="https://github.com/ReactiveX/RxJava/wiki/Plugins">https://github.com/ReactiveX/RxJava/wiki/Plugins</a>                                     | io/reactivex/Observable.java                                 |
| <a href="https://github.com/ReactiveX/RxJava/wiki/Plugins">https://github.com/ReactiveX/RxJava/wiki/Plugins</a>                                     | io/reactivex/Flowable.java                                   |
| <a href="https://github.com/ReactiveX/RxJava/wiki/Error-Handling">https://github.com/ReactiveX/RxJava/wiki/Error-Handling</a>                       | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| <a href="https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0">https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0</a>     | io/reactivex/exceptions/UndeliverableException.java          |
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>                                                 | org/dsq/library/widget/tablayout/SlidingTabLayout.java       |
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>                                                 | org/dsq/library/widget/tablayout/SegmentTabLayout.java       |
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>                                                 | org/dsq/library/widget/tablayout/CommonTabLayout.java        |
|                                                                                                                                                     |                                                              |

|                                                                                                                                                     |                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| <a href="https://greenrobot.org/greendao/documentation/database-encryption/">https://greenrobot.org/greendao/documentation/database-encryption/</a> | org/greenrobot/greendao/database/DatabaseOpenHelper.java               |
| <a href="http://www.slf4j.org/codes.html">http://www.slf4j.org/codes.html</a>                                                                       | org/slf4j/MDC.java                                                     |
| <a href="http://www.slf4j.org/codes.html">http://www.slf4j.org/codes.html</a>                                                                       | org/slf4j/LoggerFactory.java                                           |
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>                                                 | pl/droidsonroids/gif/GifViewUtils.java                                 |
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>                                                 | pl/droidsonroids/gif/GifTextureView.java                               |
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>                                                 | pl/droidsonroids/gif/GifTextView.java                                  |
| <a href="http://playready.directtaps.net/pr/svc/rightsmanager.asmx">http://playready.directtaps.net/pr/svc/rightsmanager.asmx</a>                   | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java |
| <a href="http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense">http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense</a>   | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java |

 邮箱线索

| 邮箱地址                | 所在文件                                       |
|---------------------|--------------------------------------------|
| danikula@gmail.com  | com/danikula/mp3cache/HttpUrlSource.java   |
| danikula@gmail.com  | com/danikula/videocache/HttpUrlSource.java |
| aw666me01@gmail.com | com/grass/mh/SplashActivity.java           |
| aw666me01@gmail.com | 摸瓜V1引擎                                     |

 手机线索

| 手机号         | 所在文件                                          |
|-------------|-----------------------------------------------|
| 17179869185 | freemarker/core/FMParserTokenManager.java     |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |

## 🌸 签名证书

APK已签名  
v1 签名: True  
v2 签名: True  
v3 签名: False  
找到 1 个唯一证书  
主题: C=86, ST=Hainan, L=Haikou, O=wujikeji, OU=CHN, CN=ChenXiaopeng  
签名算法: rsassa\_pkcs1v15  
有效期自: 2024-07-08 03:53:48+00:00  
有效期至: 2049-07-02 03:53:48+00:00  
发行人: C=86, ST=Hainan, L=Haikou, O=wujikeji, OU=CHN, CN=ChenXiaopeng  
序列号: 0x1d9272ce  
哈希算法: sha256  
md5值: 6611eaf74372fd774c2e0599ebb2c5b3  
sha1值: a735159e80a7445642fd7f8f506780d21e50f4a4  
sha256值: ec46082daea84aac1dd4c81bb2b30d5f42bf332edd75bf9a0e577b6371c39363  
sha512值: d4323dd601f8b2d81906a885b2ea5aa0e8311a90e05426430ceb88b20dd440c979ad5872f742516359e635b2028079748dd697e97865dc3f78517d31520747b5  
公钥算法: rsa  
密钥长度: 2048  
指纹: 9bd3fbcbf530ffe3d8d5456295aa7f20e1535a2e2bc53d729056f38ba85ad51a

## 🔑 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.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                     |
| 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.REQUEST_INSTALL_PACKAGES | 危险   | 允许应用程序请求安装包。   | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。      |
| android.permission.CAMERA                   | 危险   | 拍照和录像          | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
|                                             |      |                |                                   |

|                                                |    |                    |                                                               |
|------------------------------------------------|----|--------------------|---------------------------------------------------------------|
| android.permission.FOREGROUND_SERVICE          | 正常 |                    | 允许常规应用程序使用 Service.startForeground。                           |
| android.permission.WAKE_LOCK                   | 正常 | 防止手机睡眠             | 允许应用程序防止手机进入睡眠状态                                              |
| 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.READ_PHONE_STATE            | 危险 | 读取电话状态和身份          | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| android.permission.MOUNT_UNMOUNT_FILESYSTEMS   | 危险 | 装载和卸载文件系统          | 允许应用程序为可移动存储安装和卸载文件系统                                         |
| android.permission.SYSTEM_ALERT_WINDOW         | 危险 | 显示系统级警报            | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕                              |
| android.permission.SYSTEM_OVERLAY_WINDOW       | 未知 | Unknown permission | Unknown permission from android reference                     |
| android.permission.ACCESS_FINE_LOCATION        | 危险 | 精细定位 (GPS)         | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量     |
| android.permission.READ_PRIVILEGED_PHONE_STATE | 未知 | Unknown permission | Unknown permission from android reference                     |



应用内通信