



MoGua

91直播 2.0.1.APK 分析报告



APP名称:

91直播

包名:	xipg.xkvm.cftx.zcow
域名线索:	22条
URL线索:	17条
邮箱线索:	3条
分析日期:	2025年9月29日
分析平台:	摸瓜APK反编译平台

文件名: 91直播.apk
文件大小: 30.24MB
MD5值: aa143eb33df99da49f30bc7b9ccf46fc
SHA1值: e23c69a4ae6fbdadd5cdb6f0cd3f1077c3731103
SHA256值: ea8077460a2b0586efccc73afb576938da3a466bbb200459b7b466bccb17aa0e

i APP 信息

App名称: 91直播
包名: xipg.xkvm.cftx.zcow
主活动Activity: com.jj.live.audience.MainActivity
安卓版本名称: 2.0.1
安卓版本: 201

🔍 域名线索

域名	服务器信息
api.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
ptcc.in	IP: 162.125.6.1 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
rs.chat.agora.io	IP: 39.107.5.142 所属国家: China 地区: Zhejiang

	城市: Hangzhou 纬度: 30.293650 经度: 120.161423
flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
developer.android.com	IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
developer.mozilla.org	IP: 13.225.183.113 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696
www.ibm.com	IP: 104.71.149.203 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696
m.potato.im	IP: 104.244.43.229 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446

bak.jjzb7.live	IP: 104.21.52.68 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
ns.adobe.com	没有服务器地理信息.
dashif.org	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
www.openssl.org	IP: 104.71.138.221 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696
astat.bugly.cros.wr.pvp.net	IP: 170.106.135.32 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418
astat.bugly.qcloud.com	IP: 150.109.27.253 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067
	IP: 172.67.208.17 所属国家: United States of America

91zb.co	地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
10.10.20.131	IP: 10.10.20.131 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
github.com	IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
app1.jhuibp.work	IP: 104.18.14.68 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
android.bugly.qq.com	IP: 109.244.244.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

www.jsdelivr.com	IP: 92.223.84.84 所属国家: Germany 地区: Hessen 城市: Gallus 纬度: 50.100380 经度: 8.629500
rs.easemob.com	IP: 39.106.121.4 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423

 URL线索

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/PlatformPlugin.java
https://developer.android.com/reference/javax/net/ssl/SSLSocket	io/flutter/plugins/videoplayer/VideoPlayerPlugin.java
http://dashif.org/guidelines/last-segment-number	m1/d.java
http://dashif.org/guidelines/trickmode	m1/d.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	x3/e.java
http://ns.adobe.com/xap/1.0/	s0/a.java

http://www.w3.org/ns/ttml	x1/c.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/c.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/c.java
https://www.jsdelivr.com/using-sri-with-dynamic-files	Mogua Engine V2
https://github.com/apvarun/toastify-js	Mogua Engine V2
https://github.com/richttr/NoSleep.js/issues/15	Mogua Engine V2
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released	Mogua Engine V2
https://rs.easemob.com/easemob/server.json	lib/armeabi-v7a/libhyphenate.so
https://rs.chat.agora.io/easemob/server.json	lib/armeabi-v7a/libhyphenate.so
http://www.w3.org/XML/1998/namespace	lib/armeabi-v7a/libflutter.so
http://www.w3.org/2000/xmlns/	lib/armeabi-v7a/libflutter.so
<a)."="" href="https://www.w3.org/Style/CSS/Test/Fonts/Ahem/">https://www.w3.org/Style/CSS/Test/Fonts/Ahem/").	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues .	lib/armeabi-v7a/libflutter.so
https://91zb.co	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html	lib/armeabi-v7a/libapp.so
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
http://www.w3.org/2000/svg	lib/armeabi-v7a/libapp.so

https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues/new	lib/armeabi-v7a/libapp.so
https://github.com	lib/armeabi-v7a/libapp.so
http://10.10.20.131:9999	lib/armeabi-v7a/libapp.so
https://app1.jhuibp.work	lib/armeabi-v7a/libapp.so
https://bak.jjzb7.live	lib/armeabi-v7a/libapp.so
https://m.potato.im	lib/armeabi-v7a/libapp.so
https://ptcc.in/jiuyizb	lib/armeabi-v7a/libapp.so
http://www.w3.org/1998/Math/MathML	lib/armeabi-v7a/libapp.so
http://www.w3.org/2000/xmlns/	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android	lib/armeabi-v7a/libapp.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libqffmpeg.so

 邮箱线索

邮箱地址	所在文件
bg_mall@3x.png icon_has_vehicle@3x.png icon_turntable@3x.png icon_turntable_high@3x.png	

icon_vehicle_play@3x.png
bg_anchor_rank@3x.png
bg_user_rank@3x.png
empty_game_maintain@3x.png
empty_game_no1@3x.png
empty_game_no2@3x.png
empty_game_no@3x.png
empty_member@3x.png
empty_noanchor@3x.png
empty_noanchor_black@3x.png
empty_nosignal@3x.png
empty_record_no@3x.png
game_jiantou@3x.png
game_jiantou_xiao@3x.png
game_kjil_normal@3x.png
game_kjil_select@3x.png
game_tzjl_normal@3x.png
game_tzjl_select@3x.png
game_wfsm@3x.png
icon_back_white@3x.png
icon_close@3x.png
icon_cm_big_1@3x.png
icon_cm_big_2@3x.png
icon_cm_big_3@3x.png
icon_cm_big_4@3x.png
icon_cm_big_5@3x.png
icon_cm_big_6@3x.png
icon_cm_big_7@3x.png
icon_cm_big_8@3x.png
on_inputdelect_white@3x.png
icon_shaizi_1@3x.png
icon_shaizi_1_big@3x.png
icon_shaizi_2@3x.png
icon_shaizi_2_big@3x.png
icon_shaizi_3@3x.png
icon_shaizi_3_big@3x.png
icon_shaizi_4@3x.png
icon_shaizi_4_big@3x.png

icon_shaizi_5@3x.png
icon_shaizi_5_big@3x.png
icon_shaizi_6@3x.png
icon_shaizi_6_big@3x.png

num_0@3x.png
num_1@3x.png
num_2@3x.png
num_3@3x.png
num_4@3x.png
num_5@3x.png
num_6@3x.png
num_7@3x.png
num_8@3x.png
num_9@3x.png
game_left_normal@3x.png
game_left_selected@3x.png
guard_help_header@3x.png
guard_help_power@3x.png
guard_help_title@3x.png
guard_help_type@3x.png
guard_icon_avatar@3x.png
d_icon_avatar_center@3x.png
guard_icon_coin@3x.png
guard_icon_help@3x.png
ard_icon_power_enter@3x.png
_power_enter_disable@3x.png
_icon_power_fighting@3x.png
wer_fighting_disable@3x.png
uard_icon_power_gift@3x.png
n_power_gift_disable@3x.png
rd_icon_power_people@3x.png
power_people_disable@3x.png
_icon_power_selected@3x.png
icon_addimg@3x.png
icon_anchor_tg@3x.png
icon_anchor_potato@3x.png
icon_arrowright@3x.png
icon_back@3x.png
icon_eggsipping@3x.png
on_game_gold_refresh@3x.png
icon_home_hot@3x.png
icon_hot@3x.png

icon_indicator@3x.png
icon_inputdelect@3x.png
icon_inputsearch@3x.png
icon_officialnotice@3x.png

icon_popclose@3x.png
icon_ranking@3x.png
icon_search@3x.png
key_icon@3x.png
like_icon@3x.png
icon_doublehit_open@3x.png
icon_eggskiping2@3x.png
icon_pop_turntable@3x.png
op_turntable_pointer@3x.png
icon_voice@3x.png
20icon_bianji@3x.png
_icon_chat_album@3x.png
_icon_chat_send@3x.png
_icon_notice@2x.png
_icon_selected@2x.png
_icon_service@2x.png
anchor_rz_img@3x.png
anchor_rz_success@3x.png
del_icon@3x.png
gf_icon@3x.png
icon_addcard@2x.png
icon_anchor_grade@3x.png
icon_another_service@3x.png
icon_arrowdown@3x.png
icon_game_service@3x.png
icon_income@3x.png
icon_living@3x.png
icon_loading@3x.png
icon_news@2x.png
icon_phone_login@3x.png
icon_receivegift@3x.png
con_recharge_service@3x.png
icon_safe_login@3x.png
icon_sartlive@3x.png
icon_select_ok@3x.png
icon_upload_pic@3x.png
icon_upload_potato@3x.png
icon_upload_type@3x.png

icon_upload_video@3x.png
icon_x@3x.png
noble_service@3x.png
rank@3x.png

Mogua Engine V2

help-icon@3x.png
noble-bg@3x.png
pop_rocket@3x.png
icon_bangding@3x.png
icon_fangan@3x.png
icon_guanli@3x.png
icon_mingxi@3x.png
icon_shangxiaji@3x.png
icon_tuiguang@3x.png
icon_crown_copper@3x.png
icon_crown_gold@3x.png
icon_crown_silver@3x.png
icon_hidden@3x.png
icon_hidden_avatar@3x.png
icon_hidden_state@3x.png
icon_living_da@3x.png
icon_rank_1@3x.png
icon_rank_2@3x.png
icon_rank_3@3x.png
user_tx_default@3x.png
game_theme_recharge@3x.png
game_theme_record@3x.png
game_theme_withdraw@3x.png
icon_contribute@2x.png
icon_gamerecord@2x.png
icon_incomedetail@2x.png
icon_mine_agent@2x.png
icon_mine_apply@2x.png
icon_mine_beginshow@2x.png
icon_mine_grade@2x.png
icon_mine_jiazguanli@2x.png
icon_mine_potato@2x.png
icon_mine_setting@2x.png
icon_noble@2x.png
icon_spread@2x.png
icon_wallet@2x.png
icon_withdrawal@2x.png
icon_gender_female@3x.png

icon_gender_male@3x.png
icon_level_1_big@2x.png
icon_level_1_big@3x.png
icon_level_2_big@2x.png

icon_level_2_big@3x.png icon_level_3_big@2x.png icon_level_3_big@3x.png icon_level_4_big@2x.png icon_level_4_big@3x.png icon_level_5_big@2x.png icon_level_5_big@3x.png bg_balance@3x.png bg_goldcoin@3x.png empty_record@3x.png icon_addcard@3x.png icon_coin@3x.png icon_recharge@3x.png icon_withdraw_alipay@3x.png icon_withdraw_bank@3x.png icon_withdraw_usdt@3x.png icon_withdrawway@3x.png	
storationinformation@867124995.fromserial _httpparser@13463476.responsepa anchor_rz_success@3x.png icon_crown_copper@3x.png icon_cm_big_7@3x.png icon_shangxiaji@3x.png icon_mine_grade@2x.png power_people_disable@3x.png game_kjil_select@3x.png _future@4048458.immediate _growablelist@0150898._literal icon_mine_agent@2x.png guard_help_type@3x.png icon_tuiguang@3x.png n_power_gift_disable@3x.png _link@14069316.fromrawpat _icon_chat_album@3x.png c_growablelist@0150898.withcapaci _receiveportimpl@1026248.fromrawrec noble_service@3x.png rank@3x.png empty_noanchor@3x.png m_growablelist@0150898._literal2 g_bigintimpl@0150898.from	

_list@0150898.empty
icon_ranking@3x.png
on_game_gold_refresh@3x.png
icon_incomedetail@2x.png
icon_sartlive@3x.png
icon_cm_big_2@3x.png
bg_anchor_rank@3x.png
_directory@14069316.fromrawpat
icon_withdraw_usdt@3x.png
icon_mine_setting@2x.png
_big@3x.png
icon_eggsleeping2@3x.png
icon_bianji@3x.png
_colorfilter@16065589.srgbtoline
op_turntable_pointer@3x.png
icon_level_3_big@2x.png
empty_nosignal@3x.png
_icon_selected@2x.png
icon_recharge@3x.png
anchor_rz_img@3x.png
lectiontoolbarbutton@591113492.text
d_icon_avatar_center@3x.png
q_imagefilter@16065589.blur
_growablelist@0150898._literal4
bg_balance@3x.png
icon_level_5_big@3x.png
x_growablelist@0150898.of
k_colorfilter@16065589.lineartosr
_icon_service@2x.png
_list@0150898.of
_list@0150898.generate
icon_withdrawal@2x.png
n_typeerror@0150898._create
_list@0150898._ofgrowabl
empty_game_no1@3x.png
_list@0150898._ofefficie
icon_cm_big_3@3x.png
_growablelist@0150898._ofarray

icon_mine_beginshow@2x.png
icon_withdraw_bank@3x.png
_power_enter_disable@3x.png
game_theme_recharge@3x.png

rd_icon_power_people@3x.png
icon_arrowright@3x.png
_icon_chat_send@3x.png
game_tzjl_normal@3x.png
icon_crown_silver@3x.png
pop_rocket@3x.png
icon_home_hot@3x.png
_icon_notice@2x.png
con_recharge_service@3x.png
icon_upload_potato@3x.png
_list@0150898._ofother
eo_bytebuffer@7027147._new
icon_wallet@2x.png
game_tzjl_select@3x.png
icon_game_service@3x.png
icon_select_ok@3x.png
icon_cm_big_8@3x.png
help-icon@3x.png
av_nativesocket@14069316.normal
game_kjil_normal@3x.png
icon_loading@3x.png
e@audio.onerror
icon_mine_jiazguanli@2x.png
icon_addcard@3x.png
guard_icon_coin@3x.png
empty_member@3x.png
icon_gamerecord@2x.png
icon_arrowdown@3x.png
icon_contribute@2x.png
icon_cm_big_5@3x.png
qd_growablelist@0150898._literal8
icon_cm_big_1@3x.png
guard_icon_avatar@3x.png
icon_officialnotice@3x.png
_future@4048458.zonevalue
icon_crown_gold@3x.png
ard_icon_power_enter@3x.png
icon_gender_male@3x.png

empty_record_no@3x.png
icon_back@3x.png
icon_news@2x.png
erflowindicatormixxin@764204652.mixin

lib/armeabi-v7a/libapp.so

icon_withdraway@3x.png
icon_another_service@3x.png
icon_level_4_big@2x.png
icon_level_5_big@2x.png
icon_vehicle_play@3x.png
icon_level_1_big@2x.png
_double@0150898.fromintege
game_jiantou_xiao@3x.png
_growablelist@0150898._literal6
icon_level_2_big@3x.png
icon_upload_video@3x.png
-_list@0150898._ofarray
z_timer@1026248.periodic
icon_gender_female@3x.png
icon_mine_apply@2x.png
empty_game_maintain@3x.png
icon_addcard@2x.png
game_left_selected@3x.png
guard_help_title@3x.png
_icon_power_selected@3x.png
icon_level_2_big@2x.png
user_tx_default@3x.png
_casterror@0150898._create
icon_level_4_big@3x.png
l_invocationmirror@0150898._withtype
icon_addimg@3x.png
_colorfilter@16065589.mode
del_icon@3x.png
icon_anchor_tg@3x.png
icon_hidden_avatar@3x.png
icon_turntable@3x.png
icon_cm_big_4@3x.png
icon_level_3_big@3x.png
_growablelist@0150898._literal1
4_uri@0150898.file
icon_close@3x.png
icon_receivegift@3x.png
guard_help_header@3x.png

icon_withdraw_alipay@3x.png
bb_growablelist@0150898._ofgrowabl
game_theme_record@3x.png
icon_voice@3x.png

guard_icon_help@3x.png
icon_pop_turntable@3x.png
_cookie@13463476.fromsetcoo
authenticationscheme@13463476.fromstring
icon_mine_potato@2x.png
icon_hidden_state@3x.png
empty_record@3x.png
icon_turntable_high@3x.png
icon_safe_login@3x.png
icon_x@3x.png
icon_popclose@3x.png
like_icon@3x.png
bg_user_rank@3x.png
_growablelist@0150898._literal3
wer_fighting_disable@3x.png
u_growablelist@0150898._ofother
icon_upload_type@3x.png
game_theme_withdraw@3x.png
noble-bg@3x.png
_timer@1026248._internal
_growablelist@0150898._literal5
empty_game_no2@3x.png
icon_guanli@3x.png
icon_phone_login@3x.png
empty_game_no@3x.png
game_wfsm@3x.png
icon_upload_pic@3x.png
icon_cm_big_6@3x.png
on_inputdelect_white@3x.png
guard_help_power@3x.png
icon_spread@2x.png
lectiontoolbarbutton@476392285.text
ngstreamsubscription@4048458.zoned
_assertionerror@0150898._create
icon_back_white@3x.png
bg_goldcoin@3x.png
uard_icon_power_gift@3x.png
icon_fangan@3x.png

_uri@0150898.directory
icon_has_vehicle@3x.png
icon_mingxi@3x.png
v_file@14069316.fromrawpat

_icon_power_fighting@3x.png icon_level_1_big@3x.png gf_icon@3x.png empty_noanchor_black@3x.png icon_anchor_potato@3x.png icon_bangding@3x.png icon_anchor_grade@3x.png gh_growablelist@0150898.generate _uri@0150898.notsimple 7u_growablelist@0150898._literal7 icon_search@3x.png _growablelist@0150898._ofefficie _future@4048458.immediatee	
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libfqplayer.so

手机线索

手机号	所在文件
17512775099	h2/a.java
17179869184	com/tomato/ijk/media/player/IjkMediaMeta.java
18221338086	Mogua Engine V2
19163324438	lib/armeabi-v7a/libapp.so

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=zxc, ST=asd, L=qwe, O=aqwe, OU=asdasd, CN=sdasd
签名算法: rsassa_pkcs1v15
有效期自: 2023-01-15 09:53:34+00:00
有效期至: 2122-12-22 09:53:34+00:00
发行人: C=zxc, ST=asd, L=qwe, O=aqwe, OU=asdasd, CN=sdasd
序列号: 0x6bf41ab7
哈希算法: sha256
md5值: f74132b03a0ad9fcc9fd944f973460ba
sha1值: 3598cfa0a35ce2e6e423b0faa7588f7e5c7307b2
sha256值: a839f78cf781d5dfbdb0102d364235a8b2580acbfccd4963764ecbed2bb781b4
sha512值: 3582a0f670ab8a25477fa3d86365c6f8590852299080706a055b2567229a466cf819425638712b570e3d4a7b679002d170bc704fdbe79150b965ae65f7f3613f
公钥算法: rsa
密钥长度: 2048
指纹: a866704943f10ccf53862f72cc0a1401944108a2a61f5a9736b7e1b65fdbd4e9

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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.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.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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
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。
	正常		

android.permission.SCHEDULE_EXACT_ALARM	异常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.jj.live.audience.MainActivity	Schemes: rtgy0bb7://,

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。