

# 获取微信小程序的源码

## 方法一：直接抓包法

前提：手机上无该小程序的缓存文件，如果有，进行如下操作



删除小程序

## 操作步骤

- 1. 使用fiddler抓包，获取小程序下载链接

PS: burp也可以, 只是感觉fiddler抓手机包更快

#	Result	Protocol	Host	URL	Body	Caching
1	200	HTTP	Tunnel to gateway.abdcloud.com:443		0	
2	200	HTTP	Tunnel to gateway.abdcloud.com:443		0	
3	200	HTTP	Tunnel to open.weixin.qq.com:443		0	
4	4	HTTP	extxshort.weixin.qq.com	/jments/40c38f69	213	
5	200	HTTP	Tunnel to gateway.abdcloud.com:443		0	
6	200	HTTP	extxshort.weixin.qq.com	/jments/40c38f69	229	
7	200	HTTP	Tunnel to gateway.abdcloud.com:443		0	
8	200	HTTPS	open.weixin.qq.com	/jms/getexappinfo?appid=...	3,749	no-cache
9	200	HTTP	extxshort.weixin.qq.com	/jments/40c3190	229	
10	200	HTTP	Tunnel to gateway.abdcloud.com:443		0	
11	200	HTTPS	open.weixin.qq.com	/jms/launchapp?appid=...	438	no-cache
12	200	HTTP	extxshort.weixin.qq.com	/jments/40c63d3d	219	
13	200	HTTP	extxshort.weixin.qq.com	/jments/40c6564	213	
14	200	HTTP	extxshort.weixin.qq.com	/jments/40c6564	229	
15	200	HTTP	Tunnel to gateway.abdcloud.com:443		0	
16	200	HTTP	Tunnel to emp-mini.cn-bj.ufileos.com:443		0	
17	200	HTTP	extxshort.weixin.qq.com	/jments/40c7e00d	423	
18	200	HTTP	minshort.weixin.qq.com	/jments/40c7e00d	245	
19	200	HTTP	Tunnel to apikay.map.qq.com:443		0	
20	200	HTTP	Tunnel to oversectrl.map.qq.com:443		0	
21	200	HTTP	Tunnel to confinfo.map.qq.com:443		0	
22	200	HTTP	Tunnel to bs.map.qq.com:443		0	
23	200	HTTP	Tunnel to emp-api-ust-bj.ufileos.com:443		1,438	
24	200	HTTPS	emp-mini.cn-bj.ufileos.com	/new_ps_marker_2.png	1,086	
25	200	HTTP	Tunnel to emp-mini.cn-bj.ufileos.com:443		0	
26	200	HTTP	Tunnel to emp-mini.cn-bj.ufileos.com:443		0	
27	200	HTTPS	oversectrl.map.qq.com	/?apikey=4KXBZ-ICCHr-T...	33	
28	200	HTTPS	apikay.map.qq.com	/jkey/index.php?key=...	1,157	
29	200	HTTPS	confinfo.map.qq.com	/jkey/index.php?key=...	101	
30	200	HTTPS	bs.map.qq.com	/joc?c=18mrs=0&obs=2	155	
31	200	HTTP	Tunnel to bs.map.qq.com:443		0	
32	200	HTTP	emp-api-ust-bj.ufileos.com	/v1/standard/center/user...	213	
33	200	HTTPS	emp-mini.cn-bj.ufileos.com	/new_ps_marker_3.png	1,188	
34	200	HTTP	extxshort.weixin.qq.com	/jments/40c62d47	229	
35	200	HTTPS	emp-mini.cn-bj.ufileos.com	/new_ps_marker_2.png	1,086	
36	200	HTTP	Tunnel to vectorsdk.map.qq.com:443		0	
37	200	HTTPS	bs.map.qq.com	/joc?c=18mrs=1&obs=2	154	
38	200	HTTP	vectorsdk.map.qq.com	/fileupdate/files?dsvr=4...	102	
39	200	HTTP	extxshort.weixin.qq.com	/jments/40c3a3df	213	
40	200	HTTP	Tunnel to gateway.abdcloud.com:443		0	
41	200	HTTP	Tunnel to gateway.abdcloud.com:443		0	

```

GET https://open.weixin.qq.com/jms/launchapp?appid=wx656ad6eff1e0775224a61mHtHNTQm113&key=c388941a62c17530bc0b0244033de050ba429724ec1d0709256b480dd18377cos85cec9137bd9b0182f3b080eb6edfc206c204
Host: open.weixin.qq.com
Connect-Type: keep-alive
Accept: */*
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 13_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 MicroMessenger/7.0.8(0x170008020) NetType/WIFI Language/zh-CN
Referer: https://open.weixin.qq.com/getexappinfo?appid=wx656ad6eff1e0775224a61mHtHNTQm113&key=c388941a62c17530bc0b0244033de050ba429724ec1d0709256b480dd18377cos85cec9137bd9b0182f3b080eb6edfc206c204
Accept-Encoding: gzip, deflate, br

```

Find... (press Ctrl+Enter to highlight all)
View in Notepad

Transformer
Headers
Textview
Syntaxview
Imageview
Hexview
Webview
Auth
Caching
Cookies
Raw
JSON
XML

JSON

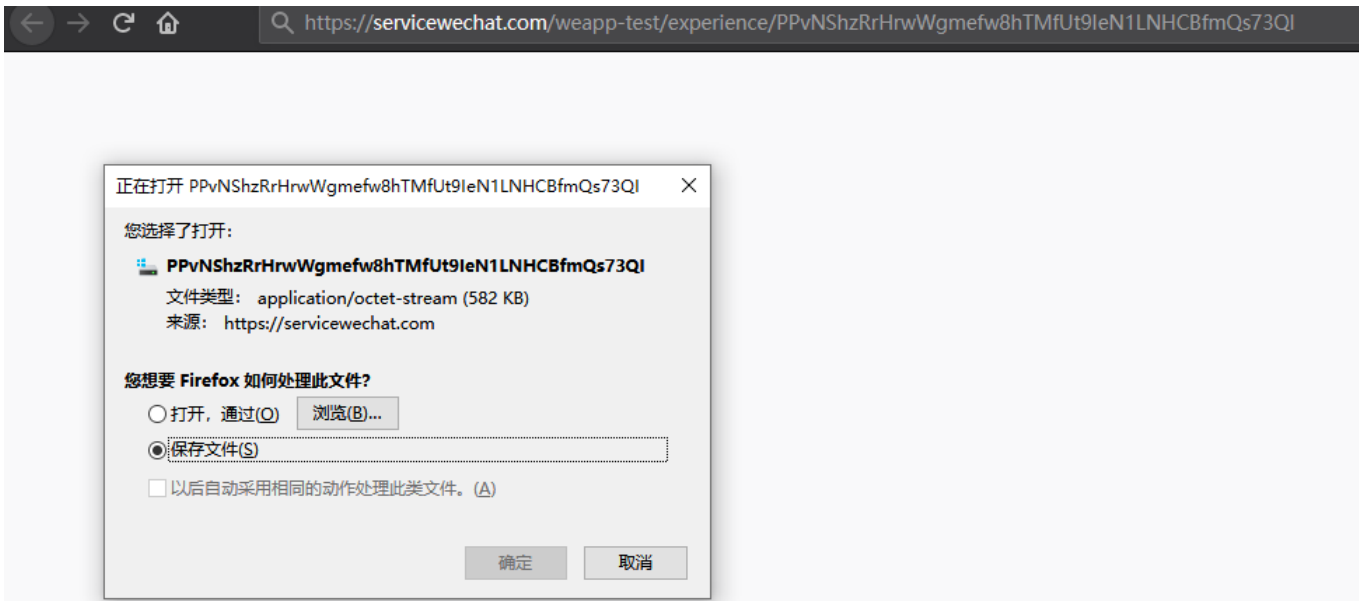
```

{
  "appid": "wx656ad6eff1e077522",
  "checkSumMds": "2c276c54c96b40356935fd262f216282",
  "downloadURL": "https://servicewechin.com/weapon-test/experience/PPvHnGzHrHwWtgmfeWkThMfHJN(e)1NHCHmQm7Q3Q",
  "extJsOnInfo": "[\"module_test-1\", \"device_ontestation\", \"loading_image_info-1\", \"data_type_declarations-1\", \"without_js_md5-1\", \"separated_plugin_test-1\"]",
  "openType": 2,
  "retcode": 0,
  "scene": 1001,
  "userName": "gh_4beccdd223f1aapp"
}

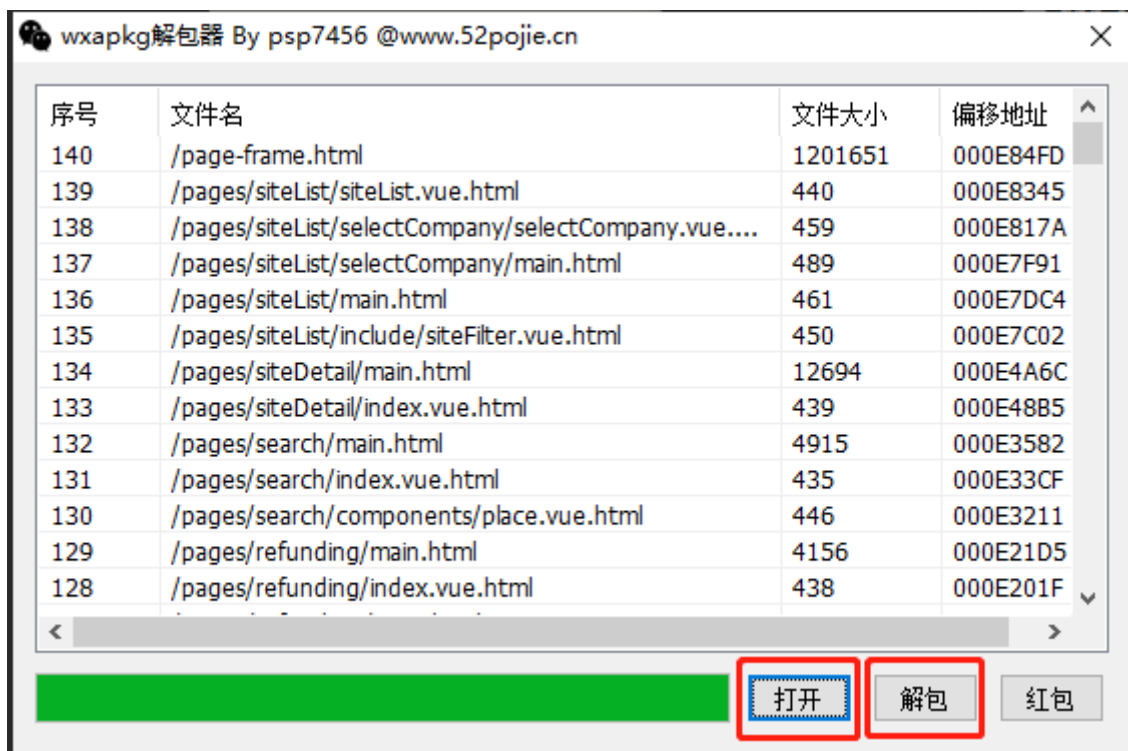
```

### 获取下载链接

- 2.下载小程序



- 3.使用 `WxApkgUnpacker.exe` 反编译wxapkg获取源文件



获取源码

## 结果

```
10442 | serverAppid: "13f97b4017e84d19a85918715ba64588",
10443 | serverTitle: "邦驰新能源"
10444 | },
10445 | wxcf486f4bc524ebaa: {
10446 |   serverAppid: "c94e5eb2252e418b999f52315fdcb128",
10447 |   serverTitle: "首星充峰"
10448 | },
10449 | wxa56ad6ff1e0f7522: {
10450 |   serverAppid: "9069020f87be48c8bdca6a230614582e",
10451 |   serverTitle: "碧辟充电"
10452 | },
10453 | dev: {
10454 |   baseUrl: "http://ps-internal.chargerhere.net:1111/emsp/v1"
10455 | },
10456 | test: {
10457 |   baseUrl: "https://emsp-api-uat-bp.chargerhere.net/v1"
10458 | },
10459 | pro: {
10460 |   baseUrl: "https://emsp-api.chargerhere.net/v1"
10461 | }
10462 | };
10463 | e.a = o()({}, i, i[i.active], i[i.wxAppId])
10464 | }, function(t, e, n) {
10465 |   var r = n(17);
10466 |   t.exports = function(t) {
```

app-server.js

## 方法二：本地缓存文件读取法

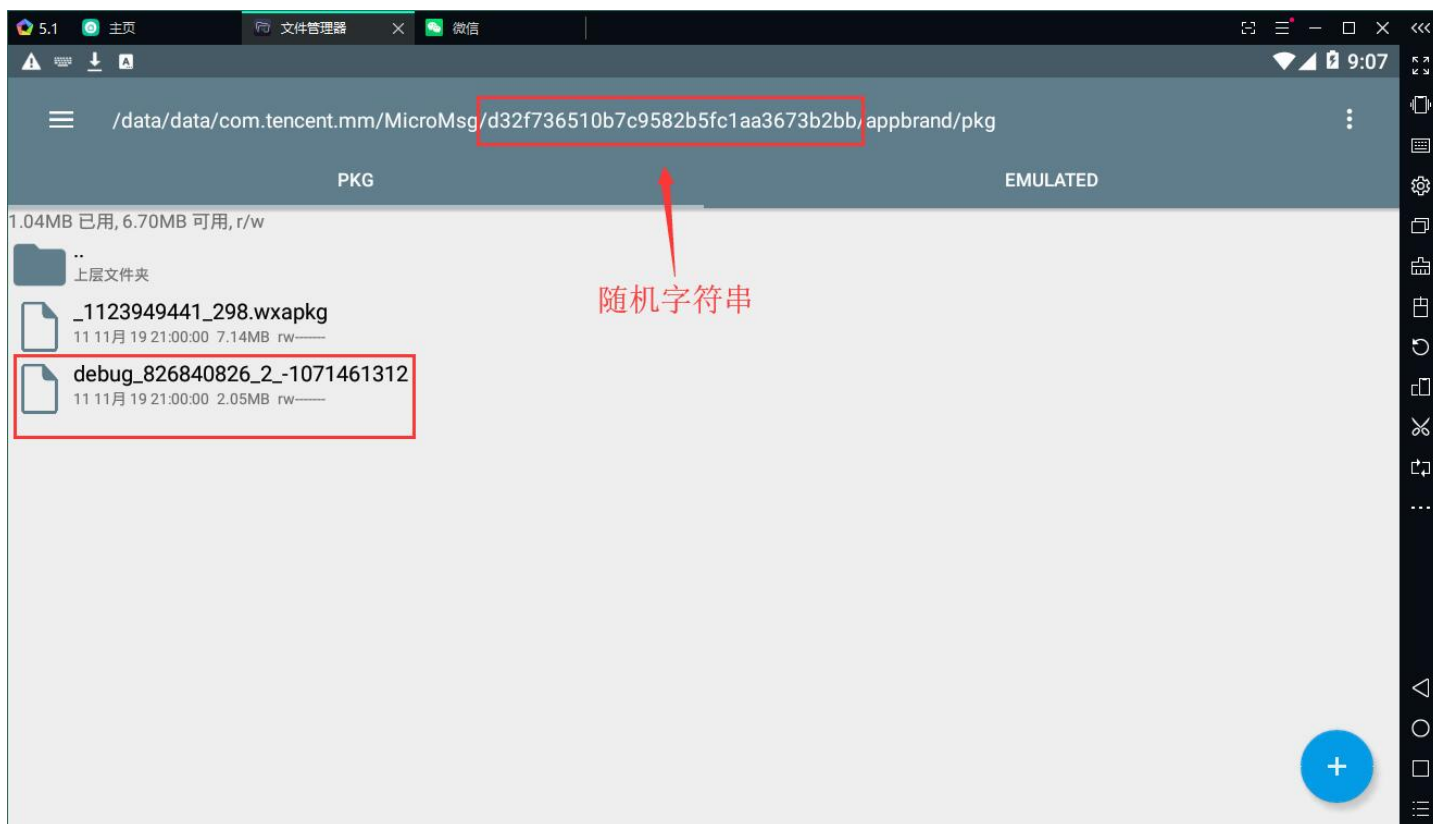
前提：

- 手机root
- 手机已经访问过小程序，在系统中存在缓存

- 安装[RE文件管理器](#)

## 操作步骤

- 1.首先访问如下目录 `/data/data/com.tencent.mm/MicroMsg/` , 找到 `wxapkg` 文件



获取源码

- 2.拖到电脑（此处我用的adb，也可以使用模拟器的共享文件夹等）

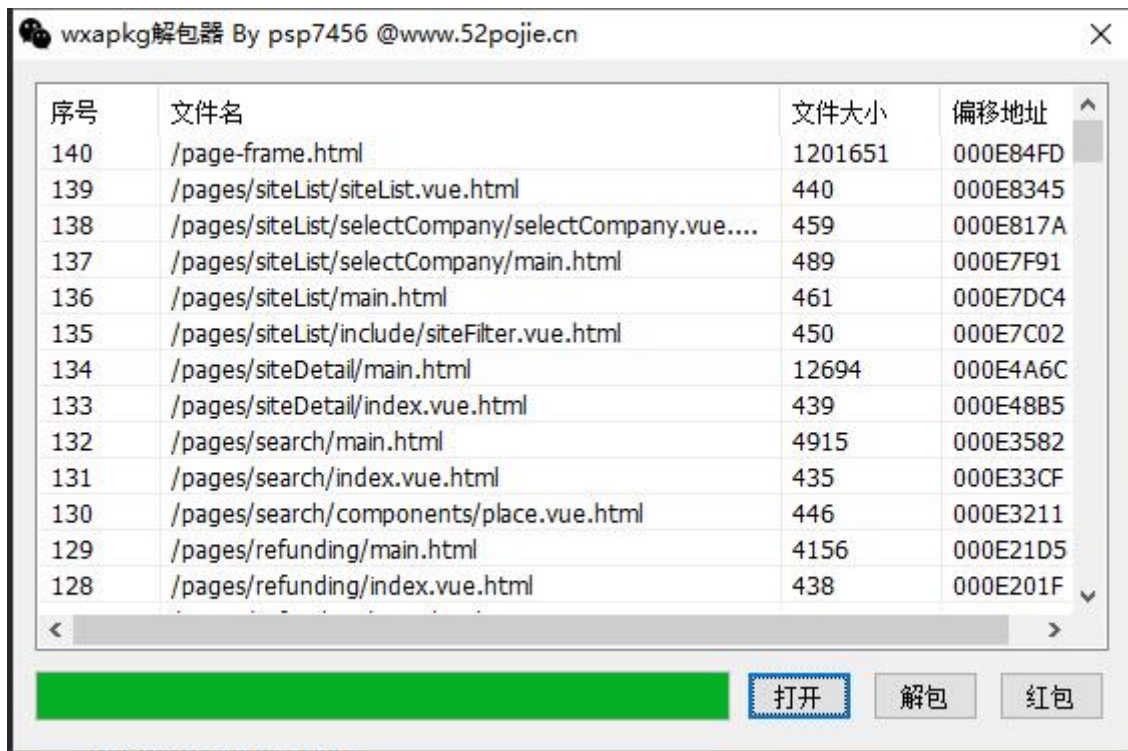
adb命令：

```
adb pull
/data/data/com.tencent.mm/MicroMsg/d32f736510b7c9582b5fc1aa3673b2bb/appbrand/
pkg/debug_826840826_2_-1071461312
```

```
E:\x>"D:\Program Files\Microvirt\MEmu\adb.exe" pull /data/data/com.tencent.mm/MicroMsg/d32f736510b7c9582b5fc1aa3673b2bb/a
ppbrand/pkg/debug_826840826_2_-1071461312
1586 KB/s (2153200 bytes in 1.325s)
```

下载到电脑

- 3.使用 `WxApkgUnpacker.exe` 反编译wxapkg获取源文件



获取源码

结果

```
10545     }).a
10546   })
10547 }, function(t, e, n) {
10548   e.a = function() {
10549     return new o.a(function(t, e) {
10550       var n = {
10551         clientId: "0410aba5abd143f09de7c20b3f642f27",
10552         appId: i.a.wxAppId
10553       };
10554       wx.login({
10555         success: function(r) {
10556           var o = r.code;
10557           n.code = o, Object(s.a)({
10558             url: "/standard/ucenter/user/login",
10559             data: n,
10560             notNeedLoad: !0,
10561             notToken: !0
10562           }).then(function(e) {
10563             var n = e.accessToken,
10564               r = e.openid;
10565             a.a.setToken(n), a.a.setOpenid(r), t(e)
10566           }).catch(function(t) {
10567             c.a.showToast(t.msg), e(t)
10568           })
10569         },
10570         fail: function() {
10571           e(0)
10572         }
10573       })
10574     })
10575   }
10576 }
```

app-server.js

# 其他

除了 `WxApkgUnpacker.exe` 外，也可以用Github上开源的 [wxappUnpacker](#) 去还原小程序的源码

wxappUnpacker参考文章

- <https://www.jianshu.com/p/8a0280d0afd8>
- <https://blog.csdn.net/as66708/article/details/80618978>

---

Repetition by [qulc@knownsec.com](#)