安卓MM6.6.9协议-登录发送包

# 

[TEA加密内容](#section=h.ypamc8p61gwz)

[MessageHead](#section=h.l02n1qbqc52j)

[SSOSeq](#section=h.kfragpfsmd6y)

[SubAppId](#section=h.li2fyphceecc)

[WxAppId](#section=h.v2n3fydccbhp)

[ExtBin](#section=h.ydp5ou7e7ucq)

[ServiceCmd](#section=h.3qaufa9ecpgf)

[MsgCookies](#section=h.4r9mxjyof8q0)

[IMEI](#section=h.hwqr82rg6lsh)

[ksid](#section=h.yj4lzamqmdml)

[Ver](#section=h.psfdx5gy8yqs)

[Buffer](#section=h.3ymwp6rn3w6r)

[密包，用ShareKey解包](#section=h.y5qhiyg3lzf4)

[Tlv包](#section=h.f4jbt6wucmwh)

[Tlv18](#section=h.f35kduyv9oku)

[Tlv106](#section=h.510gl3nvcyh)

[Tlv116](#section=h.scnjylmrbn69)

[Tlv100](#section=h.btq56cxecau3)

[Tlv107](#section=h.ibyo30njegog)

[Tlv108](#section=h.gsiyivhrfc5y)

[Tlv142](#section=h.93iql2bl19ho)

[Tlv144](#section=h.9hgx4vzfvux3)

[Tlv145](#section=h.h6hamyl7dwu1)

[Tlv147](#section=h.s0sta8o0c4y)

[Tlv154](#section=h.iuokrexth01p)

[Tlv141](#section=h.wh42gr1qrt8r)

[Tlv8](#section=h.1tag1u3372bh)

[Tlv511](#section=h.yugetkhx1xds)

[Tlv187](#section=h.wm5c2bjsuyf2)

[Tlv188](#section=h.4y2fqm9x5cj7)

[Tlv194](#section=h.emnsony9150i)

[Tlv191](#section=h.pqe0j9561xg3)

[Tlv202](#section=h.flltbrf9icf2)

[Tlv177](#section=h.g6krh4rog54d)

[Tlv516](#section=h.lzllg67z5p2p)

[Tlv521](#section=h.vtrtrwfh6yzs)

[Tlv525 //此包可不发或发送空包](#section=h.b3f2ahxqgy48)

**通信协议：tcp**

00 00 04 81 //包长度 1153

00 00 00 0a 02 00 00 00 04 00

00 00 00 0b //mm字节数+4

32 38 36 37 33 30 31 //mm[2867301]

# TEA加密内容

//下面Tea密包，16个0解密

****

//下面是16个0(TEA)解密后的包体

00 00 00 CC //本身4字节长度+数据长度=204

00 01 6A 91

20 02 BA 7A

20 02 BA 7A

01 00 00 00 00 00 00 00 00 00 00 00

00 00 00 4C

BB 69 1B 64 EC ED 72 3C C1 BF 19 F6 EF 36 EE BA 8D 1E 50 7D 24 80 54 F2 64 62 ED A8 DA 1B 69 20 EE 3F 8F 5D CD 49 F9 84 32 BD 88 DF 08 BE 34 9B B6 4B 64 C6 3F EF 59 7D 53 E2 34 1C 21 0D 15 14 10 FD 69 30 79 B0 F0 3E 00 00 00 11 77 74 6C 6F 67 69 6E 2E 6C 6F 67 69 6E 00 00 00 08 85 36 E7 17 00 00 00 13 38 36 34 33 39 34 30 31 30 31 36 30 39 39 34 00 00 00 14 C5 91 B0 F2 D4 51 BB 9A 5A 70 49 BF 3D 50 6E 1F 00 20 7C 34 36 30 30 37 31 36 30 39 39 31 35 35 30 39 7C 41 36 2E 36 2E 39 2E 32 35 37 32 39 35

00 00 00 04

### MessageHead

[

### SSOSeq

ssoSeq\_=92817

### SubAppId

(Sub)appId=537049722

### WxAppId

(Wx)appId=537049722

01 00 00 00 网络相关//固定

00 00 00 00 //固定

00 00 00 00 //固定

### ExtBin

extBin=

**BB 69 1B 64 EC ED 72 3C C1 BF 19 F6 EF 36 EE BA 8D 1E 50 7D 24 80 54 F2**

**64 62 ED A8 DA 1B 69 20 EE 3F 8F 5D CD 49 F9 84 32 BD 88 DF 08 BE 34 9B**

**B6 4B 64 C6 3F EF 59 7D 53 E2 34 1C 21 0D 15 14 10 FD 69 30 79 B0 F0 3E**

### ServiceCmd

serviceCmd=wtlogin.login //命令Login登录

### MsgCookies

msgCookies=85 36 E7 17

### IMEI

imei=38 36 34 33 39 34 30 31 30 31 36 30 39 39 34 //手机IMEI串号[864394010160994]

### ksid

ksid=C5 91 B0 F2 D4 51 BB 9A 5A 70 49 BF 3D 50 6E 1F

### Ver

ver=7C 34 36 30 30 37 31 36 30 39 39 31 35 35 30 39 7C 41 36 2E 36 2E 39 2E 32 35 37 32 39 35 //[|460071609915509|A6.6.9.257295] mm版本 6.6.9

]

## OicqRequestBuffer / wupBuffer

00 00 03 90 本身4字节+下面包长=912

02

03 8C //长度

1F 41 //固定 pc\_ver

08 10 //cmd

00 01 //sequence

00 2B C0 65 //[mm:2867301]

03 //固定

87 //4.5=0x00; 4.7=0x07; 6.6.9=0x87或0x45

00 //retry

00 00 00 02 //type 固定 default\_ext\_type

00 00 00 00 //no 固定 g\_client\_version **\_g**.\_app\_client\_version

00 00 00 00 //instance 固定 0 \_default\_ext\_instance

01 01 //rand key

22 36 10 B9 E9 07 A9 16 5A 6D 38 8E AE 3C 77 48 //随机16字节

01 02 //pub key

00 19 //下面包长 25字节

03 4B 6B 9F 22 CE C8 67 83 97 87 AA 32 06 7A E2 B3 BD 9D 57 8F 20 97 6D B4 //记得是Pub\_Key

## 密包，用ShareKey解包



//下面ShareKey解包后内容

## Tlv包

[

00 09 subcmd 9

00 18 //tlv个数

### Tlv18

00 18 //tlv18

00 16 //长度

00 01 //ping version

00 00 06 00 //ssoversion

00 00 00 10 //dwappid md5登录时为固定0x10

00 00 00 00 //client version

00 2B C0 65 //[mm:2867301]

00 00 //0

00 00 //0

**Tlv1**

00 01 //tlv1

00 14 //长度

00 01 //fixed

40 CE A3 26 //rand

00 2B C0 65 //[mm:2867301]

58 93 4A FD //登录时间

00 00 00 00 00 00

### Tlv106

01 06 //tlv106

00 78 //包长120

2A 2D 67 A5 CB 89 1C 8E 5E 3C 0B 7A 51 ED 22 31 C9 A7 7F 66 6E 88 63 B2 24 B1 38 62 74 A6 B2 41 B6 89 30 6B 38 FB 74 E5 CA 98 1C CC 4B 97 7C 23 B3 56 5A 9B 29 6B F3 B6 4C 42 5E 85 94 77 92 93 E2 E0 41 27 B2 EC 79 58 AA 6D 10 A4 C4 0F 18 E0 54 70 82 6B 58 BC 6E 6F 66 75 B1 5F 5D A4 F2 CC 26 07 61 B6 8B 90 AF 39 06 95 35 07 4E 94 85 0B 86 EE F6 6D ED 11 60 C7

\*\*\* md5(md5(pwd)+uin[8]) decrypted\*\*\*

00 04 //tgtgt ver

58 04 97 e1 //rand

00 00 00 05 //sso ver

00 00 00 10 //dwappid md5登录时为固定0x10

00 00 00 00 //client ver

00 00 00 00

00 2b c0 65 //uin 2867301

58 93 4a fd //init time

00 00 00 00 //$client\_ip

01 //$seve\_pwd

25 f9 e7 94 32 3b 45 38 85 f5 18 1f 1b 62 4d 0b //md5(pwd)

2d 1a 25 bc 4c 96 9d 65 8b b6 ee 62 26 30 86 42 //tgtgt

00 00 00 00 //fix 0

01 //imei flag

d1 61 60 d5 b3 56 a0 a5 4f b9 93 24 a3 63 28 6b [网络环境md5]

20 02 ba 7a //subapp=537049722

00 00 00 01 //fix 1

00 07 [字符串mm号(长度)]

32 38 36 37 33 30 31 //到文本mm2867301

00 00

### Tlv116

01 16 //tlv116

00 0E //包长度14

00

00 57 FF 7C bitmap

00 01 04 00 //get\_sig

01 //count

5F 5E 10 E2

### Tlv100

01 00 //tlv100

00 16 //包长度22

00 01 //db\_buf\_ver

00 00 00 05 sso ver

00 00 00 10 //dwappid

20 02 BA 7A //[(wx)Appid:537049722]

00 00 00 00 //client ver

02 16 10 E0 getsig

### Tlv107

01 07 //tlv107

00 06 //包长度6

00 00 //pic\_type

00 //cap type

00 00 //pic size

01

### Tlv108

01 08 //tlv108

00 10 //包长度16

C5 91 B0 F2 D4 51 BB 9A 5A 70 49 BF 3D 50 6E 1F ksid

### Tlv142

01 42 //tlv142

00 18 //包长度24

00 00 00 14

63 6F 6D 2E 74 65 6E 63 65 6E 74 2E 6D 6F 62 69 6C 65 71 71 //固定[com.tencent.mobilemm]

### Tlv144

01 44 //tlv144

00 80 //包长度128

**87 4B 33 00 B3 12 B9 4D 37 70 CC 96 F0 21 E8 C1 B3 5E 94 2A D9 67 F2 CB E4 C3 8F 95 B6 E9 36 66 70 4F AE FD E0 ED B9 74 59 C9 4A 4E 1D 59 C3 87 78 A5 D5 84 04 79 57 51 F8 36 1A 45 CE 46 3A 95 5D 2E B0 E0 7A D8 98 14 6D 12 69 CB 4A 23 4A 6A B4 13 F7 50 FE 1C 08 FB 69 5C 25 A0 2A 64 64 7B A2 03 52 B4 87 66 89 CE 48 E8 13 7B 6A FF D6 74 07 ED F5 0A AA 89 FF 52 88 FA 79 59 18 D4 6F C7**

**tgtgt 解**

00 04 //count

//sub TLV

01 09 //tlv109

00 10 //16字节

b1 37 85 10 0c d5 0d b5 11 50 6a b3 66 d5 40 a3 //网络环境md5

//sub TLV

01 24 //tlv124

00 20 //包长度

00 07//系统类型长度

61 6e 64 72 6f 69 64 //android

00 05//系统版本长度

34 2e 34 2e 32//[Android4.4.2]

00 02 //nettype[01=移动数据，02=Wifi网络]

00 04 //netdetail

43 4d 43 43 //[CMCC]

00 00 addr

00 04 网络类型长度4

77 69 66 69 //wifi

//sub TLV

01 28 //tlv128

00 2c //包长度

00 00 //fixed

00

01

00

01 00 00 00 //flag

00 07 //手机型号长度

4d 49 20 34 4c 54 45 //[MI 4LTE]

00 10 //guid

d1 61 60 d5 b3 56 a0 a5 4f b9 93 24 a3 63 28 6b

00 06 //手机品牌长度

58 69 61 6f 6d 69 //[Xiaomi]

//sub TLV

01 6e //tlv16e

00 07 //手机型号长度

4d 49 20 34 4c 54 45 //手机型号[MI 4LTE]

### Tlv145

01 45 //tlv145

00 10 //包长度16

D1 61 60 D5 B3 56 A0 A5 4F B9 93 24 A3 63 28 6B //网络环境md5

### Tlv147

01 47 //tlv147

00 1D //包长度29

00 00 00 10 //固定

00 05 //len5

36 2E 36 2E 39 //6.6.9 apk\_v

00 10 //len16

A6 B7 45 BF 24 A2 C2 77 52 77 16 F6 F3 6E B6 8D //据说是apk\_sig.

### Tlv154

01 54 //tlv154

00 04 //包长度4

00 01 6A 91 //92817(SSOSeq)

### Tlv141

01 41 //tlv141

00 10 //包长度16

00 01 //this.\_version=1 固定

00 04 //4字节

43 4D 43 43 //[中国移动-CMCC]

00 02 network\_type 01数据网络 02wifi

00 04 //4字节

77 69 66 69//[wifi环境]

### Tlv8

00 08 //tlv008

00 08 //包长8字节

00 00

00 00 08 04 //localid

00 00

### Tlv511

05 11 //tlv511

00 67 //包长103

00 07 //下面的网址数量，7个

01 //固定

00 0A //10字节

74 65 6E 70 61 79 2E 63 6F 6D [tenpay.com]

01//固定

00 0C //12字节

71 7A 6F 6E 65 2E 71 71 2E 63 6F 6D [qzone.mm.com]

01 //固定

00 0A //10字节

71 75 6E 2E 71 71 2E 63 6F 6D [qun.mm.com]

01 //固定

00 0B //11字节

6D 61 69 6C 2E 71 71 2E 63 6F 6D [mail.mm.com]

01 //固定

00 11 //17字节

6F 70 65 6E 6D 6F 62 69 6C 65 2E 71 71 2E 63 6F 6D [openmobile.mm.com]

01 //固定

00 09 //9字节

71 7A 6F 6E 65 2E 63 6F 6D [qzone.com]

01 //固定

00 0B //11字节

67 61 6D 65 2E 71 71 2E 63 6F 6D [game.mm.com]

### Tlv187

01 87 //tlv187

00 10 //16字节

A3 13 8A 8D D1 7E E1 A5 84 63 D7 56 83 18 0E 87 md5(mac)

### Tlv188

01 88 //tlv188

00 10 //16字节

90 06 AF 4D 14 8C 18 22 88 1F 7E FE 8E 6D F2 39 md5(androidID)

### Tlv194

01 94 //tlv194

00 10 //16字节

5F 64 AA B8 ED A2 E7 73 CA 1D 79 5D E6 19 19 68 md5(IMSI)

### Tlv191

01 91 //tlv191

00 01 //1字节

01

### Tlv202

02 02 //tlv202

00 1D //包长29字节

00 10 //16字节

FA DB FA D6 6E F7 15 71 BD 7B 99 2D 9D 9C 5D B7 //md5(bssid)

00 09 //9字节

41 6E 64 72 6F 69 64 41 50//[WifiSSID：AndroidAP]

### Tlv177

01 77 //tlv177

00 11 //17字节

01

58 63 52 B2 //固定 [时间：2016-12-28 13:50:42]

00 0A //长度10字节

36 2E 33 2E 31 2E 31 39 39 33 //[6.3.1.1993]

### Tlv516

05 16 //tlv516

00 04 //4字节

00 00 00 00

### Tlv521

05 21 //tlv521

00 06 //6字节

00 00 00 00 00 00

### Tlv525 //此包可不发或发送空包

登录历史

05 25 //tlv525

00 44 //68字节

00 01 //count

Sub Tlv

05 22 Tlv LoginExtraData

00 3E //length

01 //固定

3C //length

00 00 00 00 00 2B C0 65

01 5A AC 05 //ip

58 93 20 69 //time

20 02 BA 7A //mversion

00 00 00 00 00 2B C0 65

01 5A AC 05

58 93 1D 28

20 02 BA 7A

00 00 00 00 00 2B C0 65

01 5A AC 05

58 93 20 69

20 02 BA 7A

]

03 //包尾]