00000133 00 00 04 81 00 00 00 0a 02 00 00 00 04 00 00 00 ........ ........

00000143 00 0b 32 38 36 37 33 30 31 2a 60 7d 4c 12 68 c1 ..286730 1\*`}L.h.

00000153 87 45 c0 3b 92 f0 73 9b f7 e2 bf ae 20 a1 9c c4 .E.;..s. .... ...

00000163 b5 a5 c4 cc b5 61 04 95 43 fc 86 f2 6c 53 2d fa .....a.. C...lS-.

00000173 86 e5 91 e6 79 70 dc ec 21 71 94 20 58 2d db 61 ....yp.. !q. X-.a

00000183 cb 20 aa 28 b8 2e 97 44 3b 61 c2 42 aa fc fa 13 . .(...D ;a.B....

00000193 58 b0 62 3a 07 9d 7a e7 07 6b dd f8 24 d8 4c 38 X.b:..z. .k..$.L8

000001A3 e4 70 6b a6 8a 17 47 6f f0 fb 32 93 94 f7 28 05 .pk...Go ..2...(.

000001B3 77 7c f0 23 e7 f9 e7 a0 51 4c 98 bc a2 f6 70 04 w|.#.... QL....p.

000001C3 f5 f5 15 c6 2e 3c 5c e8 ff 57 38 a3 61 43 8b db .....<\. .W8.aC..

000001D3 2d 49 60 29 7a 5c cd 9d 48 a4 d5 c0 93 4b d7 af -I`)z\.. H....K..

000001E3 d6 4b 0d f5 16 f8 97 02 85 4f 23 1d a3 fd b1 4f .K...... .O#....O

000001F3 7b 03 36 7e 5d fd c3 d9 1c 8b 9f bd 47 85 5d 0a {.6~]... ....G.].

00000203 1e 1f bc a9 ab 18 8e 8a 71 12 83 2a b3 94 c3 5f ........ q..\*...\_

00000213 dc a5 c1 75 58 e2 fd 2f 68 74 5e 58 28 3a b7 6b ...uX../ ht^X(:.k

00000223 27 aa c9 f2 eb 94 3d ce d4 fb 1f 92 82 5b ba 3b '.....=. .....[.;

00000233 29 b7 90 a2 bb 78 ab 99 97 2d 32 81 af c3 d6 bb )....x.. .-2.....

00000243 0b b6 ea be 8c 2e f4 54 f5 40 e2 e0 9b 29 6b a6 .......T .@...)k.

00000253 15 34 de 7d e8 30 19 19 2f 3f 47 6a fe 63 df e3 .4.}.0.. /?Gj.c..

00000263 ea e6 16 b9 6d e1 31 62 bb b7 d8 03 31 44 80 2c ....m.1b ....1D.,

00000273 37 89 09 86 42 3a 0b ea 14 01 19 c5 4b 67 9d c7 7...B:.. ....Kg..

00000283 3c 8f b8 a0 de 0e 67 ce 6b 11 de 63 0b 99 51 e7 <.....g. k..c..Q.

00000293 77 11 36 58 48 ee cf 88 09 4a d6 a1 02 df 61 33 w.6XH... .J....a3

000002A3 50 ab 63 45 c4 16 f7 04 0c bb 7c 9d bf 8f bf 55 P.cE.... ..|....U

000002B3 fd b9 16 3e 01 e0 6f 0d ca 75 0f 9c d3 d0 53 a4 ...>..o. .u....S.

000002C3 f1 19 96 73 33 75 74 b0 1e 82 62 e4 23 23 80 91 ...s3ut. ..b.##..

000002D3 20 52 60 e7 39 3d bb 2c 4a 93 90 32 49 75 54 96 R`.9=., J..2IuT.

000002E3 e6 c6 0b ad fc 4a b9 03 6a 9a 19 a9 6b b7 c7 e1 .....J.. j...k...

000002F3 9d 2d 73 1f ec 60 60 7c 7a b4 0a 37 59 d0 7c 36 .-s..``| z..7Y.|6

00000303 1a 98 e9 41 25 8c df f2 4c 41 53 f6 7d fb 7f 25 ...A%... LAS.}..%

00000313 5e 99 d8 0d 38 89 ac 38 e5 6b 50 bd 03 b3 0a 64 ^...8..8 .kP....d

00000323 2e b6 4d f5 ff ec 0e 69 55 fa a9 72 5c fb 87 21 ..M....i U..r\..!

00000333 e2 8f 60 7c af 0c 74 82 0c 11 e1 6d 0d 2c f2 d1 ..`|..t. ...m.,..

00000343 98 3a c3 d9 0a 23 79 c3 2f 7b f4 6f 5c 96 8b 8a .:...#y. /{.o\...

00000353 36 e1 0f c0 15 49 a6 79 cb a4 c0 d5 79 32 94 9a 6....I.y ....y2..

00000363 3f 08 69 02 f7 1b 03 00 de 6b 05 e8 fa 24 7e 33 ?.i..... .k...$~3

00000373 00 cd 33 a8 a2 56 91 b5 a7 19 0c 7a 12 0e 4a 0c ..3..V.. ...z..J.

00000383 54 0b 52 16 a4 e8 74 98 fd 6d 0d 0d d1 b1 9e a0 T.R...t. .m......

00000393 56 60 cf e8 cb 0a 68 9f bd c1 58 1a 36 a5 06 fa V`....h. ..X.6...

000003A3 b3 c3 af 7f bc f2 ea 6c 28 6f 3f 55 f9 e4 c6 5d .......l (o?U...]

000003B3 16 c5 ce e2 2f ee c0 47 7d 3c 40 54 e5 f2 d4 17 ..../..G }<@T....

000003C3 42 76 12 3b 1c c6 a8 04 da c1 69 ad fa 17 01 10 Bv.;.... ..i.....

000003D3 11 2d dd 78 70 9e 64 21 b7 98 fd 3c e8 1d b5 7a .-.xp.d! ...<...z

000003E3 3c 9a 7c 63 3f 71 50 58 bc 43 fc b6 63 08 2a 56 <.|c?qPX .C..c.\*V

000003F3 24 d8 74 05 73 19 5e a2 62 4b 6f 33 78 5a 00 da $.t.s.^. bKo3xZ..

00000403 41 44 e0 63 a4 07 94 57 f8 5e e0 0e 4b 01 8c 54 AD.c...W .^..K..T

00000413 83 a9 bd cd 6e 3c 18 2d ed de 4a 0d 3f 08 48 db ....n<.- ..J.?.H.

00000423 37 58 ac f6 9a 0c aa b4 11 8a e5 f2 45 f8 f1 8e 7X...... ....E...

00000433 04 20 f9 74 b9 6d b3 8e 8a b0 ed 77 08 93 a9 43 . .t.m.. ...w...C

00000443 f2 c8 93 61 5c 38 ac 3b 82 c0 a9 c2 80 6c a8 e3 ...a\8.; .....l..

00000453 be e9 a9 84 5d 1a 57 60 e4 21 87 f9 31 68 82 89 ....].W` .!..1h..

00000463 56 e9 5e 85 70 4f af cf de 49 ce 46 a8 87 a9 66 V.^.pO.. .I.F...f

00000473 57 93 b1 ea 84 e9 76 c6 a1 1e e7 e9 88 7a 40 7d W.....v. .....z@}

00000483 9a 1f dc 5f a8 ae 55 dd fe c7 5a 1d 91 f3 b6 7e ...\_..U. ..Z....~

00000493 cd 55 b6 26 02 77 f1 72 2e 97 43 b9 e1 91 4c d1 .U.&.w.r ..C...L.

000004A3 81 7d 60 2f 69 be 35 aa 44 b9 b9 cf fb f7 ef 6b .}`/i.5. D......k

000004B3 99 cf d2 a5 6f b7 c3 ab 62 c7 d3 3e ce 33 bd db ....o... b..>.3..

000004C3 f4 86 d0 87 51 99 7d 12 f6 bd de 38 c6 fe a7 a9 ....Q.}. ...8....

000004D3 07 53 63 5c 39 51 da cc d5 29 b4 68 9a 2f bd 8b .Sc\9Q.. .).h./..

000004E3 aa d2 b8 3d 19 c8 2a 98 f3 2a 9d 3d 61 9c 28 11 ...=..\*. .\*.=a.(.

000004F3 b2 bd 1a 39 5c 43 be a2 e4 10 59 6c 34 60 82 ca ...9\C.. ..Yl4`..

00000503 94 40 27 3c fc e5 11 6d 60 52 1b a0 bb c6 37 04 .@'<...m `R....7.

00000513 90 80 2a 56 64 19 6f bf 71 4e a5 72 bd 06 df e8 ..\*Vd.o. qN.r....

00000523 e1 e8 1a 8d eb ae 55 2c 07 12 67 c6 28 76 f7 96 ......U, ..g.(v..

00000533 e9 fb 61 05 bf 73 38 fb aa 6a 83 b6 6a c5 46 60 ..a..s8. .j..j.F`

00000543 45 2d 15 ae 42 6c f4 e8 ad a2 43 0e 79 ad 61 91 E-..Bl.. ..C.y.a.

00000553 ab bf d4 97 cf bb 6d ec 02 86 d1 a9 b1 c0 a4 6e ......m. .......n

00000563 be e8 70 88 39 37 db a3 41 19 8d e5 c4 87 7e b0 ..p.97.. A.....~.

00000573 3b 63 2f 51 8c 26 a8 4d ff 25 88 33 c7 e6 12 8d ;c/Q.&.M .%.3....

00000583 3f 98 a4 e7 65 d2 a0 84 10 8d 94 28 44 a4 f8 5f ?...e... ...(D..\_

00000593 71 d4 50 30 c6 9f bd 28 65 f7 e6 30 1e 86 b9 23 q.P0...( e..0...#

000005A3 82 74 ca f2 12 56 32 1d 0c 60 cd 19 1a e8 77 1d .t...V2. .`....w.

000005B3 a1 .

00 00 04 81 //包长度 1153

00 00 00 0a 02 00 00 00 04 00 00 00

00 0b //QQ字节数+4

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

0[16]tea解密

00 00 00 CC //长度204

00 01 85 49 //ssoSeq

20 02 BA 7A //subapp

05 4C 4D 8A //wxappid（好像不是，跟下面的不一样）

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

00 00 00 4C //extbin

97 1D 2F B6 53 4F 0A 8C 09 32 C4 A9 D8 31 D8 EF C9 8B 6D 9C 1D C7 0D 61 DA 41 88 39 C9 B5 10 AD 2A C9 77 D9 CD D7 29 D6 89 BC 98 7C 96 BD F8 FB 12 90 7D D3 34 F8 8F 47 59 7E 21 BD E1 B3 13 59 C9 05 06 7A FA C1 DD 94

00 00 00 11

77 74 6C 6F 67 69 6E 2E 6C 6F 67 69 6E //"wtlogin.login"

00 00 00 08

5A 74 58 DF

00 00 00 13

38 36 34 33 39 34 30 31 30 31 36 30 39 39 34 //imei "864394010160994"

00 00 00 14 //ksid\_len

9F 26 8A 6B 52 1B 52 33 DA BF F5 AF 8B E5 19 45 //ksid

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 // "|460071609915509|A6.6.9.257295"

00 00 00 04

00 00 03 90

02

03 8C

1F 41

08 10 //cmd

00 01 //seq

00 2B C0 65 //uin

03 87

00

00 00 00 02 00 00 00 00 00 00 00 00

01 01

66 6F 55 BC 4D 6B 3A 34 6C F4 B0 B1 B4 B9 6C A9 //randkey

01 02

00 19 //len25

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 //pubkey



用sharekey（7d1ffc96239d17a236f122d2b497a300）解包[

00 09 //subcmd

00 18 //num

00 18 //tlv\_t18

00 16 //len

00 01 //\_ping\_version

00 00 06 00 //\_sso\_version

00 00 00 10 //appid

00 00 00 00 //client\_version

00 2B C0 65 //uin

00 00 //rc

00 00 //0

00 01 //tlv\_t1

00 14 //len

00 01 //\_ip\_ver

75 FF 00 EF //rand

00 2B C0 65 //uin

58 98 1E 89 //server\_cur\_time 2017-2-6 14:58:17

00 00 00 00 //client\_ip

00 00 //0

01 06 //tlv\_t106

00 78 //len

C2 11 24 08 7B 4E 9F 0B 61 FF 3C 0F 54 6A 30 A7 51 2F 1B 11 BB E9 D9 50 C4 F8 2D 43 66 3F 14 0F B3 79 BD 7F E7 F5 B5 8C CB 43 3F 26 1B B1 96 79 BD 28 E6 B7 AB 28 24 30 41 BB BF 82 23 88 65 0D ED 5F E3 48 EE 3D 8E 58 96 DA 15 CF 9C DD BE 77 A0 AA 85 7A 37 26 CE 69 64 11 66 78 A6 1D 75 6C EC 5E FF 9A 19 A9 D5 D7 D9 C8 DA AF CA BE 72 22 86 15 E9 9E 72 C4 EF 42

[

00 04 //\_TGTGTVer

2B 72 0F 1D //rand

00 00 00 05 //\_SSoVer

00 00 00 10 //appid

00 00 00 00 //client\_ver

00 00 00 00 00 2B C0 65 //uin

58 98 1E 89 //init\_time 2017-2-6 14:58:17

00 00 00 00 //client\_ip

01 //seve\_pwd

1E 1B 28 D6 9E BB 95 FD 04 06 24 BC E5 2B 68 3C //md5

B9 09 8A A6 8F 53 95 95 12 56 DC D0 57 DF C7 DF //TGTGT

00 00 00 00 //0

01 //readflg

D1 61 60 D5 B3 56 A0 A5 4F B9 93 24 A3 63 28 6B //guid

20 02 BA 7A //subapp

00 00 00 01 //0x01

00 07 //uin\_str\_len

32 38 36 37 33 30 31 //uin\_str

00 00 //0

]

01 16 //tlv\_t116

00 0E //len

00 //\_ver

00 57 FF 7C //bitmap

00 01 04 00 //get\_sig

01 //tappid.length

5F 5E 10 E2 //tappid

01 00 //tlv\_t100

00 16 //len

00 01 //\_db\_buf\_ver

00 00 00 05 //\_sso\_ver

00 00 00 10 //appid

20 02 BA 7A //wxappid

00 00 00 00 //client\_ver

02 16 10 E0 //getsig

01 07 //tlv\_t107

00 06 //len

00 00 //pic\_type

00 //cap\_type

00 00 //pic\_size

01 //ret\_type

01 08 //tlv\_t108

00 10 //len

9F 26 8A 6B 52 1B 52 33 DA BF F5 AF 8B E5 19 45 //ksid

01 42 //tlv\_t142

00 18 //len

00 00 //\_version

00 14 //id.length

63 6F 6D 2E 74 65 6E 63 65 6E 74 2E 6D 6F 62 69 6C 65 71 71 //id

01 44 //tlv\_t144

00 80 //len

68 27 FA BA B9 0C 0C AE 7B 55 92 CA 03 B1 73 63 01 29 38 D3 CB 64 5E 6B E9 1C EF 9A 8A 32 E5 C7 15 0D 03 BD 53 A3 B9 46 C9 1B 36 B7 FB E5 01 5D A0 21 73 91 2C D3 D8 60 D1 8B F8 8A 19 4A AA 4F 48 29 43 5F 7B F5 DB 93 4F 1A 24 2B F5 D0 37 46 C0 9B 93 70 E6 20 0E 38 9B D1 30 72 90 CF 9C 89 28 E8 6D EC FC 98 F5 5A 11 2E FA 1E F1 46 D3 6A EB 2E 48 33 5C 16 DF 87 12 E7 46 6D D7 55 F0 1F

TGTGT解密[

00 04 //count

01 09 //tlv\_t109

00 10 //len

B1 37 85 10 0C D5 0D B5 11 50 6A B3 66 D5 40 A3 //IMEI[16]（网络环境md5）

01 24 //tlv\_t124

00 20 //len

00 07 //ostype\_len[2](16)

61 6E 64 72 6F 69 64 //ostype

00 05 //osver\_len[2](16)

34 2E 34 2E 32 //osver

00 02 //nettype[2]

00 04 //netdetail\_len[2](16)

43 4D 43 43 //netdetail "CMCC"

00 00 //0[2]

00 04 //addr\_len[2](32)

77 69 66 69 //addr

01 28 //tlv\_t128

00 2C //len

00 00 //0[2]

00 //newins[1]

01 //readguid[1]

00 //guidchg[1]

01 00 00 00 //flag[4]

00 07 //devicetype\_len[2](32)

4D 49 20 34 4C 54 45 //devicetype "MI 4LTE"

00 10 //guid\_len[2](16)

D1 61 60 D5 B3 56 A0 A5 4F B9 93 24 A3 63 28 6B //guid

00 06 //devicebrand\_len[2]

58 69 61 6F 6D 69 //devicebrand "Xiaomi"

01 6E //tlv\_t16e

00 07 //len

4D 49 20 34 4C 54 45 //devicetype "MI 4LTE"

]

01 45 //tlv\_t145

00 10 //len

D1 61 60 D5 B3 56 A0 A5 4F B9 93 24 A3 63 28 6B //guid[16]

01 47 //tlv\_t147

00 1D //len

00 00 00 10 //appVerID[4]

00 05 //appVer\_len[2](32)

36 2E 36 2E 39 //appVer "6.6.9"

00 10 //appSign\_len[2](32)

A6 B7 45 BF 24 A2 C2 77 52 77 16 F6 F3 6E B6 8D //appSign

01 54 //tlv\_t154

00 04 //len

00 01 85 49 //ssoSeq[4]

01 41 //tlv\_t141

00 10 //len

00 01 //\_version[2]

00 04 //operator\_name.length[2]

43 4D 43 43 //operator\_name "CMCC"

00 02 //network\_type[2]

00 04 //apn.length[2]

77 69 66 69 //apn "wifi"

00 08 //tlv\_t8

00 08 //len

00 00 //0[2]

00 00 08 04 //localid[4]

00 00 //0[2]

05 11 //tlv\_t511

00 67 //len

00 07 //uri\_num[2]

01 //0x01[1]

00 0A //url\_len[2]

74 65 6E 70 61 79 2E 63 6F 6D //url "tenpay.com"

01

00 0C

71 7A 6F 6E 65 2E 71 71 2E 63 6F 6D //url "qzone.qq.com"

01

00 0A

71 75 6E 2E 71 71 2E 63 6F 6D //url "qun.qq.com"

01

00 0B

6D 61 69 6C 2E 71 71 2E 63 6F 6D //url "mail.qq.com"

01

00 11

6F 70 65 6E 6D 6F 62 69 6C 65 2E 71 71 2E 63 6F 6D //url "openmobile.qq.com"

01

00 09

71 7A 6F 6E 65 2E 63 6F 6D //url "qzone.com"

01

00 0B

67 61 6D 65 2E 71 71 2E 63 6F 6D //url "game.qq.com"

01 87 //tlv\_t187

00 10 //len

A3 13 8A 8D D1 7E E1 A5 84 63 D7 56 83 18 0E 87 //md5[16](mac)

01 88 //tlv\_t188

00 10 //len

90 06 AF 4D 14 8C 18 22 88 1F 7E FE 8E 6D F2 39 //md5[16](androidID)

01 94 //tlv\_t194

00 10 //len

5F 64 AA B8 ED A2 E7 73 CA 1D 79 5D E6 19 19 68 //md5[16](IMSI)

01 91 //tlv\_t191

00 01 //len

01 //bool[1](CanWebVerify)

02 02 //tlv\_t202

00 1D //len

00 10 //md5\_bssid\_len[2]

FA DB FA D6 6E F7 15 71 BD 7B 99 2D 9D 9C 5D B7 //md5[16](bssid)

00 09 //WifiSSID\_len[2]

41 6E 64 72 6F 69 64 41 50 //WifiSSID "AndroidAP"

01 77 //tlv\_t177

00 11 //len

01 //0x01[1]

58 63 52 B2 //0x586352b2

00 0A //len[2]

36 2E 33 2E 31 2E 31 39 39 33 // "6.3.1.1993"

05 16 //tlv\_t516

00 04 //len

00 00 00 00 //0[4]

05 21 //tlv\_t521

00 06 //len

00 00 00 00 00 00 //0[6]

05 25 //tlv\_t525

00 44 //len

00 01 //count[2]

05 22 //tlv\_t522

00 3E //len

01

3C //len

00 00 00 00 00 2B C0 65

01 5A AC 05 //ip "1.90.172.5"

58 97 F1 39 //time 2017-2-6 11:44:57

20 02 BA 7A //mversion

00 00 00 00 00 2B C0 65

01 5A AC 05

58 97 F1 47

20 02 BA 7A

00 00 00 00 00 2B C0 65

01 5A AC 05

58 97 F3 29

20 02 BA 7A

]

03