- 1. 按电源键+音量键-进入 fastboot 模式,音量键选择 BP Tools,然后电源键确认
- 2. 手机连接到电脑后需要安装"diag_mdm"的驱动

点中"diag_mdm"右键,选择"更新驱动程序软件" 然后选择"浏览计算机查找驱动程序软件"

▷ 谜語	
🔺 🌆 其他设备	
🔤 🦣 diag	
hadiaq md	
- modem	更新驱动程序软件(P)
Motorol	禁用(D)
	(し)
mmea	
🔤 🦣 RmNet	扫描检测硬件改动(A)
▷ 🎆 人体学输入设	
▷ 📢 声音、视频和	属性(R)
▶ 🖞 鼠标和其他指针设	옵 옵
🗼 🌡 通用串行总线控制	물목

		-		×
6	9	直更	更新驱动程序软件 - diag_mdm	
		您想	即何搜索驱动程序软件?	
		•	自动搜索更新的驱动程序软件(S) Windows 将在您的计算机和 Internet 上查找用于相关设备的最新驱动程序软件,除非在设备安装设备中禁用该功能。	
		•	浏览计算机以查找驱动程序软件(<u>R)</u> 手动查找并安装驱动程序软件。	
				取消

选择"从计算机的设备驱动程序列表中选取"

\bigcirc	更新驱动程序软件 - diag_mdm	
	浏览计算机上的驱动程序文件	
	在以下位置搜索驱动程序软件:	
	▼ 浏览(<u>R</u>)	
	☑ 包括子文件夹[]	
	→ 从计算机的设备驱动程序列表中选择(L) 此列表将显示与该设备兼容的已安装的驱动程序软件,以及与该设备处于同一类别下的 所有驱动程序软件。	
	下一步(N)	汉消

选择"显示所有设备"后,点"下一步"按钮。

		×
0	① 更新驱动程序软件 - diag_mdm	
8	从以下列表选择设备的类型。	
	常见硬件类型(H):	
	显示所有设备	
	🔮 61883 设备类	
	National Device	
	₩ AVC 设备	
	😣 Bluetooth 无线电收发器	
	all DVD/CD-ROM 驱动器	
	□ IDE ATA/ATAPI 控制器	
	HEEE 1284.4 兼容打印机	
	圖 IEEE 1284.4 设备	
	👹 IEEE 1394 和 SCSI 打印机	
	₩ IEEE 1394 总线主控制器	
	Sedia Center Extender	
	Im Microsoft Windows 举公共控制器	
	下一步(N)	取消

选择"从磁盘安装"

G	① 更新驱动程序软件 - diag_mdm	×
	选择要为此硬件安装的设备驱动程序	
	请选定硬件设备的厂商和型号,然后单击"下一步"。如果手头有包含要安装的驱动程序。	的磁
	(正在检索所有设备的列表)	
	从磁盘安装(日)
		取消

点"浏览"

ſ	-				23
G	<u></u> 更新骤	区动程序软件	- diag_mdm		
	选择要	为此硬件	安装的设备驱动程序		
	17	请选定硬件	&备的厂商和型号,然后单击"下一步"。如果手头 "从英央灾难"	有包含要安装的驱动程序的	白磁
		从磁盘安装			
	(正在检测	~	插入制造商的安装盘,然后确定已在下面选定正 确的驱动器。	<u>确定</u> 取消	
			制造商文件复制来源 (C):	浏览 (8)	
		_		从磁盘安装(H)	
				下一步(N) 取	消

选择你驱动所在文件夹,选择"momdm"后点打开,然后确定

A 查找文件	-	×
查找范围 ①: 🌗 moto x qc diag interface - I 👻 🌘	3 🔊 📂 Ⅲ-	
	修改日期	类型
Domdm	2009/2/24 10:16	安装信息
Moser .	2009/2/24 10:18	安装信息
anotccgp	2010/6/18 15:37	安装信息
🗊 motmodem	2010/6/18 15:45	安装信息
🗊 motoandroid	2010/7/20 18:59	安装信息
i motodrv	2010/6/18 16:34	安装信息
🗊 motousbnet	2010/6/18 17:18	安装信息
i motport	2010/6/18 15:48	安装信息
motusbdevice	2010/6/18 16:37	安装信息
▲ []		•
文件名 (M): Mom dm	-	打开回
文件类型(I): 安装信息 (*.inf)		Tr (24

🕞 🛽 更新3	区动程序软件 - diag_mdm	23
选择要	为此硬件安装的设备驱动程序	
12	请选定硬件设备的厂商和型号,然后单击"下一步"。如果手头有包含要安装的驱动程序的磁力,连带于"以进去办法" 入磁盘安装	\$
(正在检验	↓ 插入制造商的安装盘,然后确定已在下面选定正 <u>确定</u> 确的驱动器。 取消	
	制造商文件复制来源 (C):]:\moto x qc diag interface - 64bit\moto → 浏览(B)	
	从磁盘安装(H)	
	下一步(N) 取消	

选择"Motorola USB Diagnostic Port"点"下一步"

			×
\bigcirc	更新驱动程序软件 - diag_mdm		
	选择要为此硬件安装的设备到	区动程序	
	请选定硬件设备的厂商和型。 盘,请单击"从磁盘安装"。	号,然后单击"下一步"。如果手头有包含要安装的驱动程序的	团截
	厂商	型号	*
	Motorola	🔄 Motorola USB BP Diagnostic Port	
	Motorola Inc	🔄 Motorola USB Composite Device	
		Motorola USB Device	
		🔄 Motorola USB Diagnostic Port	
		Motorola USB Linux Diagnostic Port	Ŧ
	🔄 这个驱动程序已经过数字签名。	从磁盘安装(日).	
	告诉我为什么驱动程序签名很重要		
		下—步(N) 取	消

出现警告点"是"

更新驱动程	i序警告 ×
4	不推荐安装这个设备驱动程序,因为 Windows 无法验证这个驱动程序 是否与硬件兼容。如果驱动程序不兼容,您的硬件将无法正常运行,计 算机可能会不稳定或完全停止运行。您想继续安装这个驱动程序吗?
	是(N) 香(N)

在设备管理器端口如下图显示就表明安装成功(注:端口号 com3 会有所不同)

· 当 设备管理器	
文件(F) 操作(A) 查看(V) 帮助(H)	
⊿ - الم zgm-PC	*
Android Device	
▷· 🛶 IDE ATA/ATAPI 控制器	
▶ 💼 磁曲驱动器	
▲·潭 端口 (COM 和 LPT)	
Motorola USB Diagnostic Port (COM3)	
□ 通信端 日 (COM1)	
▷····································	
	=
Managem	
▶	
▶ 刑 鼠标和其他指针设备	
▶ 🔮 网络适配器	-

下面是破解电信 3G

按电源键+音量键-进入 fastboot 模式,音量键选择 BP Tools,然后电源键确认

1, 打开 DFS, 首先点 Ports 按钮, 打开添加设备的界面, 选择你的设备端口, 在 devices online 有显示以链接的设备

2, 返回主界面, 点解 spc 解锁设备

FS CDMA Tool v.13.9.29.0			
ESN: 806B1A38 MIN: 6251768450 www.cdmato	ol.com: Account not exist	Port Rate: 115200 BS GPS Time: 2015/1/20 8:52:46 China Unio	om CDMA
🚓 Ports 🕺 Motorola USB Diagnostic Port (COI	14) 🔹	▼ 🖨 Abort DM NotUse ▼ 🖪 Log 🛞 About	Account
SPC 00000 Automatic -	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	▼ ByteCS ▼	🍰 Reset 🔻
Equipment Programming NV EFS Memory 1	ownload Modem Test call EQF	Settings	
EQF:	Status: IS95 ESN 80681A38 MIN 6251768450762517 Channel 283 SID/NID 1383176 RF mode: Sleep RX state: Pagino: Shapping Channel Shapping Abound COMA and Shapping Shapping Mission Shapping Band Class SID/NID 1383176 Band Class 800 MHz Cellular P REV BS: Silor TIS2000 RF Mode: Step Band Class Stop Stop Band Class 800 MHz Cellular Fixor Minal: Column: Column: Stapping Stop Band Class 800 MHz Cellular Fixor Column: Stop Stop Band Class 800 MHz Cellular Entry Normal: CDMA operatic Channel: 283 Stop/NID Stop/NID 1383176 Stop <th>Di agnostic: Version Number SCM 0x3A MSM ver UxF507 Compile Nov 7.20115.06:27 Release Sep 25.2014 17:00:00 Ver. dir. TAARANAZ Model Test SURF OSC 6055 NOR Extended Build ID Version OT 20 HVR MSM rev 0x7F53 Mob model 0x0FF7 Mob SW rev MPS5.D14.0::300118:M9625TAARANAZM-1 Model efer TAG RX-rac -20.248 dBm TX adj 138.248 dBm RX/TX rate Blanked / Blanked Analyzer</th> <th></th>	Di agnostic: Version Number SCM 0x3A MSM ver UxF507 Compile Nov 7.20115.06:27 Release Sep 25.2014 17:00:00 Ver. dir. TAARANAZ Model Test SURF OSC 6055 NOR Extended Build ID Version OT 20 HVR MSM rev 0x7F53 Mob model 0x0FF7 Mob SW rev MPS5.D14.0::300118:M9625TAARANAZM-1 Model efer TAG RX-rac -20.248 dBm TX adj 138.248 dBm RX/TX rate Blanked / Blanked Analyzer	

3, 点"Programming"->"Data"标签,首先点"Read"读取配置。

DFS CDMA Tool v.13.9.29.0			
ESN: 806B1A38 MIN: 6251768450 www.cdmatool.co	m: Account not exist Port Rate	115200 BS GPS Time: 2015/1/	20 8:55:09 China Unicom CDMA
🏶 Ports 🛛 🚿 Motorola USB Diagnostic Port (COM4)	•	Abort DM NotUse 🔻	💌 Log 🕡 About 🛛 🧟 Account
SPC 000000 Automatic 👻 💿 Pwd FFFI	FFFFFFFFFFF OCMD	▼ ByteCS ▼	🤹 Reset 🔻
Equipment Programming NV 1 EFS Memory Downl	oad Modem Test call EQF Settings		
Write changes UseNam1 - Provisioning			
General NAM Data Mobile IP Customize			
Account settings:	MODE:	Data config:	EVDO SCP option:
PAP	HDR SCP force AT config:	 QNC enabled 	I01 Sub2 PL
	HDR SCP force release 0 config:	✓ PPP detection	■ [1] EC CH ■
0	Hybrid preferred mode:	SCRM enabled	
Pwd D 0	Data MDR (HSPD) mode:	Pe pet disturb	■ /3/EF/CH ■
PPP	Duran in the state of the state	EMAC DBC Gation	
SIP NAI 0	Data service option:	Lup Unsolicited	In the table
UID:0		Pre CC Cycle Enabled	1 I /7/Gen M-M
Pwd L		RUP Override	BCMCS [0]
HDR AN		EVDO Antenna RX C	ontrol 🔲 App Sub MFPA 🔳
NAI: 0		CDMA Antenna RX C	iontrol
Pwd D 0		Dial string:	
HDR AN Long			
UID: 0		SCP Session:	
Pwd D 0			•
HDR AN PPP		DNS primary/second	Jary: Active config
0		000.000.000	Paulo Days
Pwd LL 0		000,000,000,000	Rev 0
Authentification require password encryption	Read Write	3	Rev A

4, 按照截图修改一下,修改后点"Write"按钮写入配置

穿 DFS CDMA Tool v.13.9.29.0		
ESN: 806B1A38 MIN: 6251768450 www.cdmatoo	Account not exist Port Rate: 115200 B	S GPS Time: 2015/1/20 8:58:25 China Unicom CDMA
🇠 Ports 🛛 🚿 Motorola USB Diagnostic Port (CON	14) 🔻 🖨 Abort 🛛 [DM NotUse 👻 💌 Log 🕢 About 🛛 🕺 Account
SPC 000000 Automatic - OPwd	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	▼ ByteCS ▼ Seset ▼
Equipment Programming NV EFS Memory D	ownload Modem Test call EQF Settings	
Write changes UseNam1 - Provisioning		
General NAM Data Mobile IP Customize		
Account settings: PAP UID: Pwd PP SIP NAI UID: Pwd HDR AN NAI: 460036251768450@mycdma.cn Pwd	MODE: RevA_MFPA_EMPA HDR SCP force AT config: EVD0_RevA HDR SCP force release 0 config: EVD0_RevA Hybrid preferred mode: Enable Data MDR (HSPD) mode: MDR_Only Data service option: IS707	Data config: EVDO SCP option: Q NG enabled Q I/I Sub2 PL III NPP detection III EC CH III EC CH CRM enabled Q IZ EA CH III ET CH HPP detection III ET CH III ET CH HRD enabled I SI EFT CH III ET CH MAC DRG Gating IS Sub I RT III III CH Luo Unsolicited ISI Ehr Idle III ET CH HPC Overide III EN CN III EN CN EVDO Antenna RX Control App Sub MFPA IIII CDM Antenna RX Control Dial string: IIII EN CONTROL IIII EN CONTROL
HDR AN Long UID: 460036251768450@mycdma.cn Pwd	25 0 0 0 0 Bead Write	#777 SCP Session: Active DNS primary/secondary: 0.0.0 Rev fill Rev A

5,切换到**"Mobile IP"**标签,不要点**"Read"**按钮,直接修改**"DS QcMIP"**为**"SimpleIP"**;然后修改**"Retries interval"**为**"ms2000"**,最后点**"Write"**按钮写入

FIS CDMA Tool v.13.9.29.0	
ESN: 806B1A38 MIN: 6251768450 www.cdmatool.com: Account not exist Port Rate: 115200 BS GPS Time: 2015/1/20 9):02:12 China Unicom CDMA
🗢 Ports 🖉 Motorola USB Diagnostic Port (COM4) 🔹 🗣 🤤 Abort 🛛 DM 🛛 NotUse 💌 🛤	Log 🕡 About 🛛 🚨 Account
SPC 000000 Automatic V Pwd FFFFFFFFFF OCMD V ByteCS V	🤣 Reset 🔻
Equipment Programming NV EFS Memory Download Modem Test call EQF Settings	
Write changes UseNam1	
General NAM Data Mobile IP Customize	
Mabile -IP main sottings: Current User Profile DS QcMIP offer SimpleIP offer Profile settings: offer Active profile offer Number of profiles offer Registration settings: offer Retries count 1 Preveg timeout 30 Preveg timeout 000 Retries interval ms2000 Stringer offer Ashared Secret Erter value in HEX HA Shared Secret Erter value in HEX	
Domant handoff Image: Constraint of the set of	

完成后重启手机

下面是破解 4G

按电源键+音量键-进入 fastboot 模式,音量键选择 BP Tools,然后电源键确 打开 QPST configuration 先点 Ports 标签,选择所显示的设备,然后点下面"remove" 出现提示窗口点"yes"

🚯 QPST Configuration (zgm-pc)				
File Server	Start Clients V	Window Help		
Active Phones	Ports Activ	ve Clients IP Server		
Port	State	Label	Phone	Link
Д СОМ3	Waiting	COM3 (Auto add)	N/A	N/A
Enable	Disable	Remove		Add New Port
0 Phones 0	Ports 1 (Clients Server Runn	ning	



点"Add New Prot"

G QPST Con File Server	nfiguration (zgm r Start Clients nes Ports Ac	1-pc) Window Help tive Clients IP	Server	
Port	State	Label	Phone	Link
Enable	e Disab	le Remov	e	Add New Port
0 Phones	0 Ports	1 Clients Sen	ver Running	

点选下面与你 bp 驱动,然后点"OK"按钮

d New Port	- Sant Charles Minds		×
Serial/USB Ports Outgoing II	^o Connections		
Please enter port to be moni	tored by the QPST Server		
COM1 - Serial (通信端口)			
COM3 - USB/QC Diagnost	ic (Motorola USB Diagnostic F	ort, ZX1G2255VS)	
📝 Show Serial and USB/Q	C Diagnostic ports only		
	B .	20110	
	Port:	COM3	
	Port Label:	СОМЗ	
Note: The baud rate for the	port will be set to 38400 bps		
ОК			Cancel
			Cancer

点"Start Client"菜单中的"EFS Explorer"选项,然后点"OK"

G QPST Configuration (zgm-	pc)		
File Server Start Clients	Window Help		
Active Phone Active Phone	er Sert	ver	
Port Service Pro	gramming	Phone	Link
COM3 Software Do	ownload	MDM9x25 (806B1A	384
Enable Disable	Remove		Add New Port
1 Phones 1 Ports 1	Clients Server I	Running	

ESN	Phone Number	Banner	Port
806B1A	(625) 176-8450	MSM8626	COM3 (COM3)
	ESN 806B1A	806B1A (625) 176-8450	806B1A (625) 176-8450 MSM8626

连接上手机后,在 EFS 根目录创建 policyman 目录,点"/"然后右键选择"new"-"directory"

Reference of the second	M9x25			
File View Phone Help				
	8 8			
	NI	Size Type	Modified	Attribu. 🛆
New •	File	Directory		=
Delete	Directory	Directory		
cert	Link	Directory		
CGPS_ME	CGPS_SM	Directory		
CGPS_PE	SUPL	Directory		
CGPS_SM	apn_throttle	Directory		
client-cert	🚞 cert	Directory		
client-key	🗀 client-cert	Directory		
data	← _!! !	D!		
For Help, press F1				COM3 (COM3)

输入 policyman

QPST EFS Explorer - 1	MDM9x25	
File View Phone He	elp	
📋 🖬 🗛 🖻 📘		
	Create Directory Please enter the directory to create (57 chars max) /policyman OK Cancel	Attribu. Attribu.
⊡ data ⊕⊡ ds	client-cert Directory	
For Help, press F1		COM3 (COM3)

把 carrier_policy.xml 拖进 policyman 目录中

QPST EFS Explorer - MDM9x25					
File View Phone Help					
- 📄 ims 🔺	Name	Size	Туре	Modified	Attribu
- 🖉 mmgsdi	carrier_policy.x	5,357 bytes	File	Wed Jan 21 08:30:5	-AD
⊞… 🧰 mmode					
🖉 mot_hob					
i±…≦ nv	•				
🛛 🖉 nvm 🖳					
pdp_profiles					
🛁 policyman 🍧					
🗄 💼 rfc 📃					
💼 rpm					
🛛 🧭 safe 🛛 👻	•	111			۱.
For Help, press F1 QQ COM3 (COM3)				OM3)	

完成后重启手机

设置 apn

使用 adb 及 fastboot 组件输入以下命令进行设置(请用 adb 版本为 1.0.31 进行)

adb shell am start -ncom.android.settings/.Settings\\$ApnSettingsActivity

名称	ctlte
接入点名称	ctlte
用户名	ctnet@mycdma.cn
密码	vnet.mobi

注:我在新建的时候 MCC/MNC 是自动生成的