# OJZ9008 Tool - How to manually grab the flash key

For some models, you need to grab the flash key to use the Ogazhen tool 9008 to flash the phone.

The key of each machine is different and can be used for a long time. Note: The process of grabbing the flashing key will clear all the keys in the phone.

If you have data, please back it up in advance.

1. Download and unzip a 9008 flash recovery package on your computer that can automatically 9008 without authorization (recommended

Go to Daxia Amu Download Station for free high-speed download:

https://yun.daxiaamu.com/OnePlus_Roms/). Install the flash driver

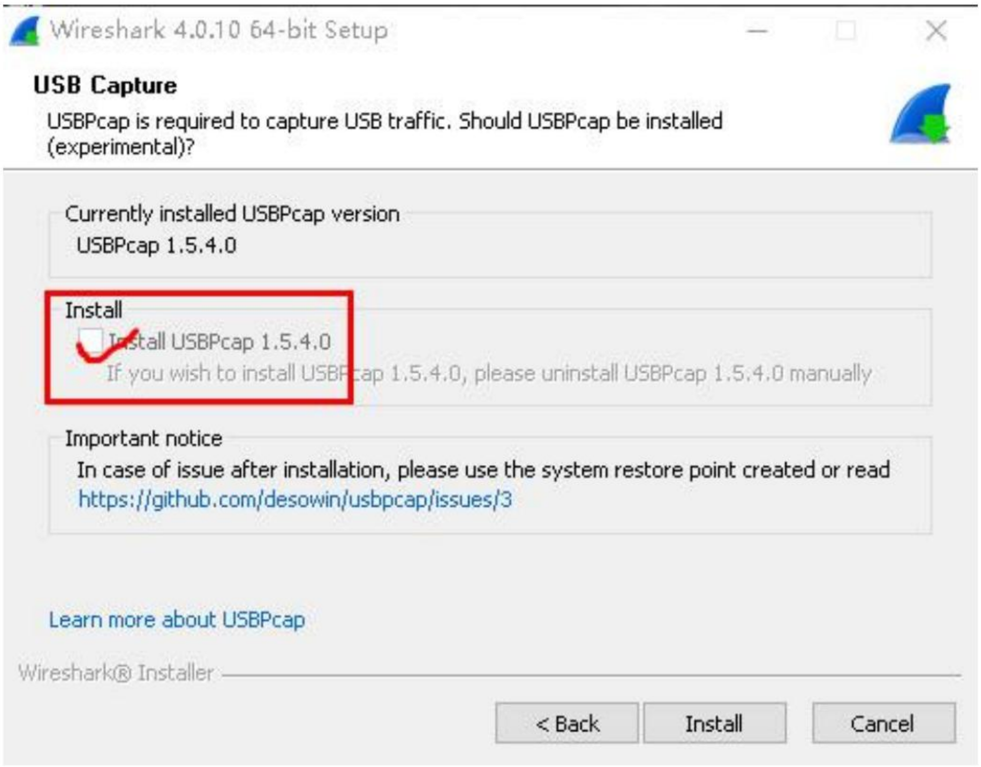
https://syxz.lanzoub.com/ifWQ313wmg5a. Download and unzip the latest version of Ogazhen

9008 tool https://syxz.lanzoub.com/b01fiq7sb (password: f65u ). Ou Jiazhen

The 9008 tool is made by Kuaian@ÿÿ and is completely free.

2. Download and install the packet capture software https://syxz.lanzoub.com/io4In1bzx8yd.

The other options are set to default, but Install USBPcap must be checked (not checked by default).



Wireshark 4.0.10 64-bit Setup

**USB Capture**

USBPcap is required to capture USB traffic. Should USBPcap be installed (experimental)?

Currently installed USBPcap version
USBPcap 1.5.4.0

Install
□ Install USBPcap 1.5.4.0
If you wish to install USBPcap 1.5.4.0, please uninstall USBPcap 1.5.4.0 manually

Important notice
In case of issue after installation, please use the system restore point created or read https://github.com/desowin/usbpcap/issues/3

Learn more about USBPcap

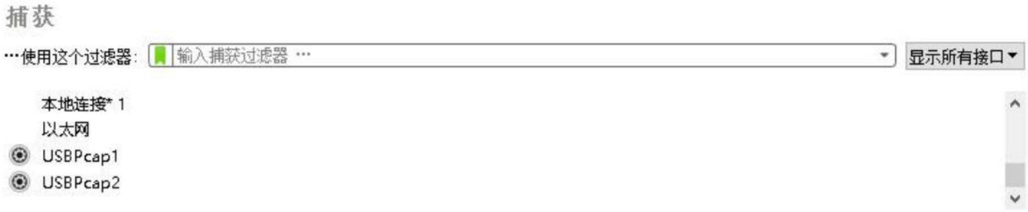
Wireshark® Installer

3. After the installation is complete, restart the computer as required (must be restarted).

4. After restarting, open the packet capture software and scroll down in the home page - "Capture" to see one or two

If there are two USBPcap ports, which one should be selected depends on the actual situation.

Choose 1 to catch it once, if you don't catch it try 2.

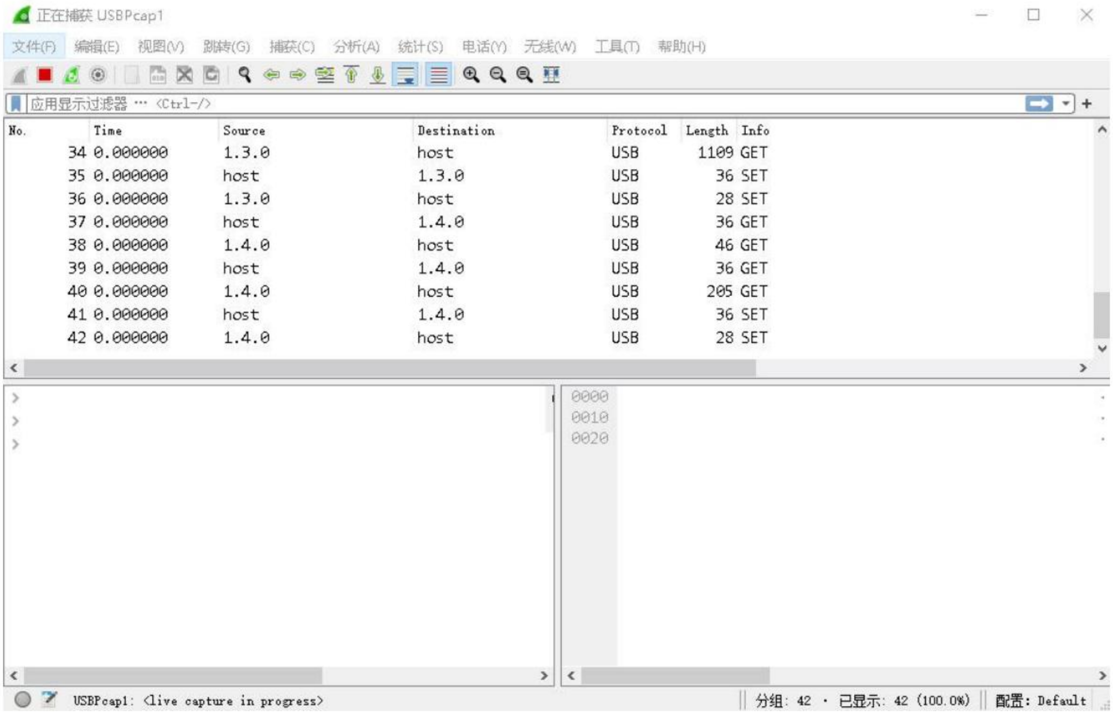


捕获

…使用这个过滤器: 输入捕获过滤器 …

本地连接* 1
以太网
USBPcap1
USBPcap2

5. Double-click the USBPcap port to start capturing packets.

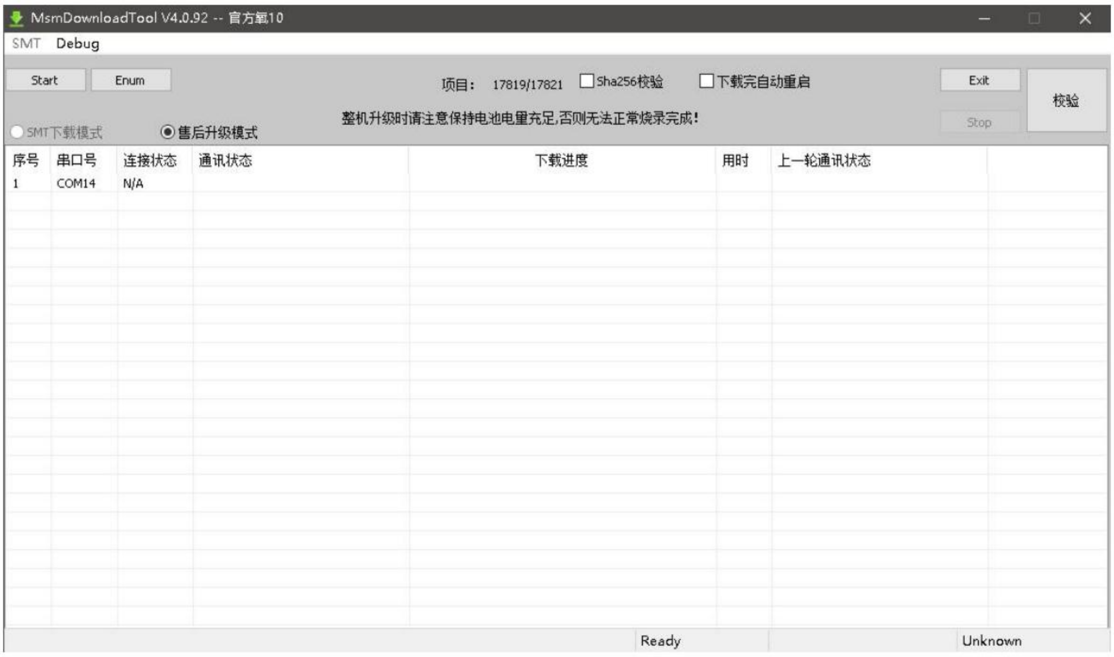


```
No.   Time      Source   Destination  Protocol  Length Info
  34 0.000000   1.3.0    host         USB        1109 GET
  35 0.000000   host     1.3.0        USB          36 SET
  36 0.000000   1.3.0    host         USB          28 SET
  37 0.000000   host     1.4.0        USB          36 GET
  38 0.000000   1.4.0    host         USB          46 GET
  39 0.000000   host     1.4.0        USB          36 GET
  40 0.000000   1.4.0    host         USB         205 GET
  41 0.000000   host     1.4.0        USB          36 SET
  42 0.000000   1.4.0    host         USB          28 SET
```

```
0000
0010
0020
```

USBPcap1: <live capture in progress>  分组: 42 · 已显示: 42 (100.0%)  配置: Default

6. Open the official package of MsmDownloadTool and click Start in the upper left corner to start flashing.


MsmDownloadTool V4.0.92 -- 官方氧10

项目: 17819/17821 □Sha256校验 □下载完自动重启

整机升级时请注意保持电池电量充足,否则无法正常烧录完成!

○SMT下载模式 ●售后升级模式

| 序号 | 串口号 | 连接状态 | 通讯状态 | 下载进度 | 用时 | 上一轮通讯状态 |
|---|---|---|---|---|---|---|
| 1 | COM14 | N/A | | | | |

Ready  Unknown

7. With the phone turned off, press and hold the volume up and down buttons at the same time, and then connect the phone to the computer via a data cable.

Enter 9008 deep flashing mode (black screen), MsmDownloadTool automatically starts flashing.

8. Observe whether the packet capture software interface captures a large amount of data reading and writing. If not, it means that the port is selected incorrectly.

Please refer to the following tutorial to restart packet capture.

9. You don't have to capture all the packets. When you see MsmDownloadTool is writing the partition image (for example,

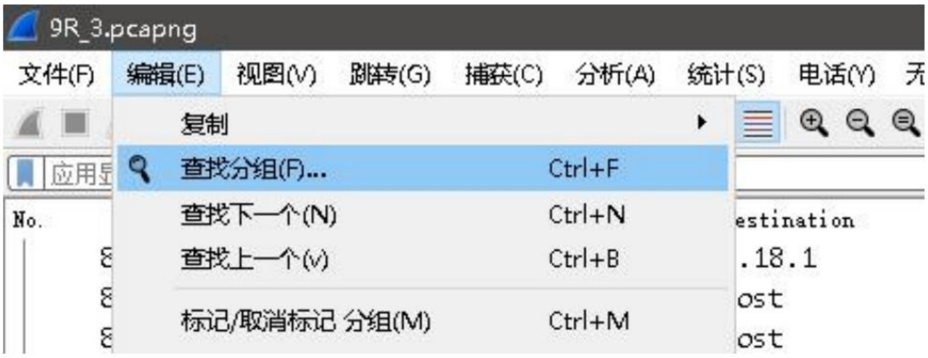
When there are too many packets, such as system, super, etc., you can stop capturing packets. Capturing too many packets will not be conducive to subsequent analysis.

Then close the packet capture software and save the packet capture file.

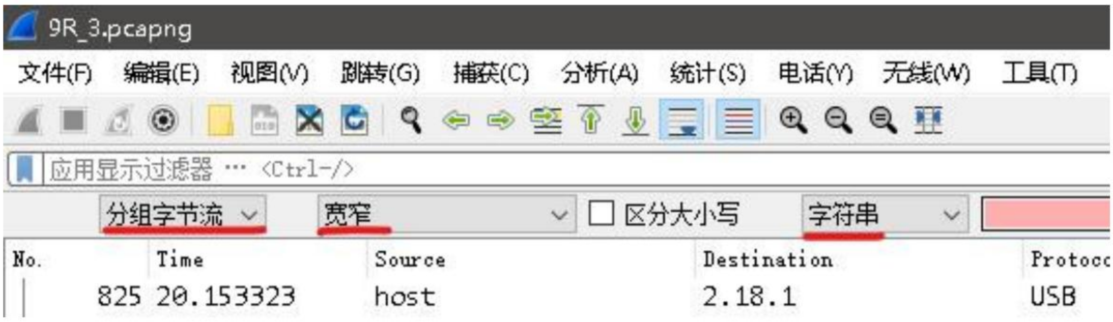
10. You will get a file with the suffix .pcapn. Double-click to open it. We need to search for

3 sets (6 pieces) of flashing keys.

Click Edit-Find Group in the menu bar.



Adjust the settings as shown below.

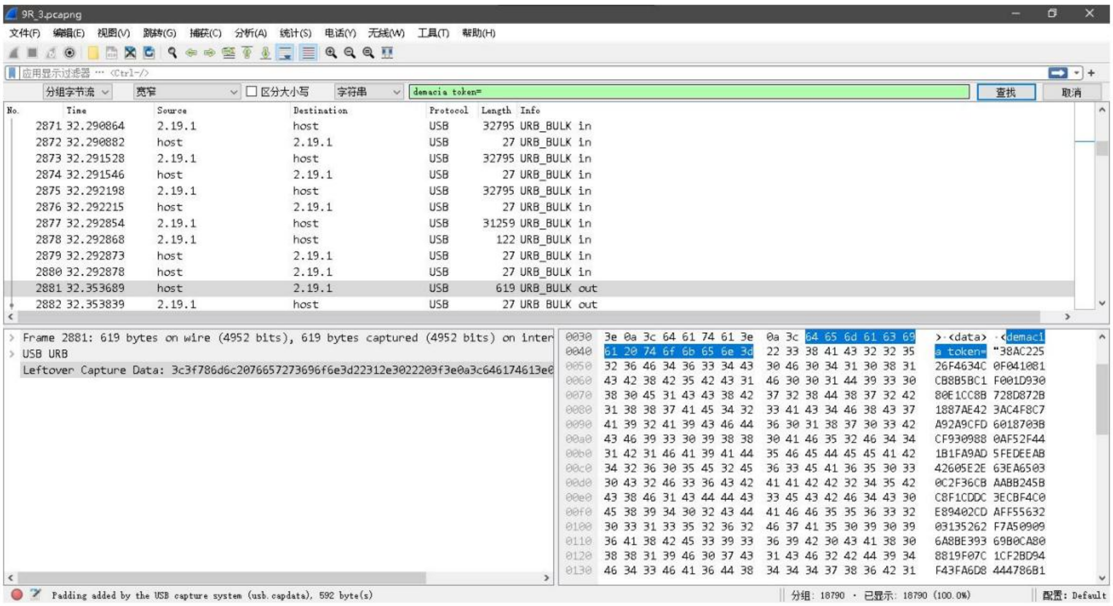


分组字节流 | 宽窄 | □ 区分大小写 | 字符串

| No. | Time | Source | Destination | Protoco |
|---|---|---|---|---|
| 825 | 20.153323 | host | 2.18.1 | USB |

11. Then search for the first set of keys. In the search box on the right, enter the keyword: demacia token=[redacted]

Click Find.


9R_3.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
分组字节流
宽窄
☐ 区分大小写
字符串
demacia token=
查找
取消

```
No.   Time       Source   Destination  Protocol  Length Info
 2871 32.290864  2.19.1   host         USB        32795 URB_BULK in
 2872 32.290882  host     2.19.1       USB           27 URB_BULK in
 2873 32.291528  2.19.1   host         USB        32795 URB_BULK in
 2874 32.291546  host     2.19.1       USB           27 URB_BULK in
 2875 32.292198  2.19.1   host         USB        32795 URB_BULK in
 2876 32.292215  host     2.19.1       USB           27 URB_BULK in
 2877 32.292854  2.19.1   host         USB        31259 URB_BULK in
 2878 32.292868  2.19.1   host         USB          122 URB_BULK in
 2879 32.292873  host     2.19.1       USB           27 URB_BULK in
 2880 32.292878  host     2.19.1       USB           27 URB_BULK in
 2881 32.353689  host     2.19.1       USB          619 URB_BULK out
 2882 32.353839  2.19.1   host         USB           27 URB BULK out
```

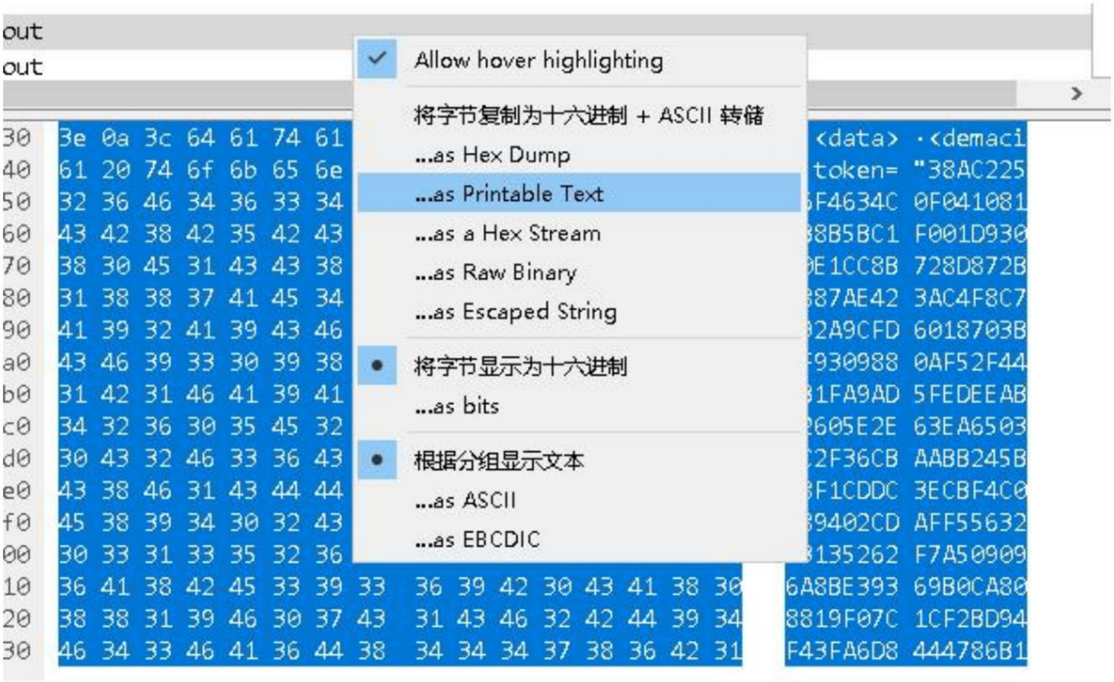
```
> Frame 2881: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on inter
> USB URB
  Leftover Capture Data: 3c3f786d6c2076657273696f6e3d22312e3022203f3e0a3c646174613e0
```

```
0030  3e 0a 3c 64 61 74 61 3e  0a 3c 64 65 6d 61 63 69   >·<data> ·<demaci
0040  61 20 74 6f 6b 65 6e 3d  22 33 38 41 43 32 32 35   a token= "38AC225
0050  32 36 46 34 36 33 34 43  30 46 30 34 31 30 38 31   26F4634C 0F041081
0060  43 42 38 42 35 42 43 31  46 30 30 31 44 39 33 30   CB8B5BC1 F001D930
0070  38 30 45 31 43 43 38 42  37 32 38 44 38 37 32 42   80E1CC8B 728D872B
0080  31 38 38 37 41 45 34 32  33 41 43 34 46 38 43 37   1887AE42 3AC4F8C7
0090  41 39 32 41 39 43 46 44  36 30 31 38 37 30 33 42   A92A9CFD 6018703B
00a0  43 46 39 33 30 39 38 38  30 41 46 35 32 46 34 34   CF930988 0AF52F44
00b0  31 42 31 46 41 39 41 44  35 46 45 44 45 45 41 42   1B1FA9AD 5FEDEEAB
00c0  34 32 36 30 35 45 32 45  36 33 45 41 36 35 30 33   42605E2E 63EA6503
00d0  30 43 32 46 33 36 43 42  41 41 42 42 32 34 35 42   0C2F36CB AABB245B
00e0  43 38 46 31 43 44 44 43  33 45 43 42 46 34 43 30   C8F1CDDC 3ECBF4C0
00f0  45 38 39 34 30 32 43 44  41 46 46 35 35 36 33 32   E89402CD AFF55632
0100  30 33 31 33 35 32 36 32  46 37 41 35 30 39 30 39   03135262 F7A50909
0110  36 41 38 42 45 33 39 33  36 39 42 30 43 41 38 30   6A8BE393 69B0CA80
0120  38 38 31 39 46 30 37 43  31 43 46 32 42 44 39 34   8819F07C 1CF2BD94
0130  46 34 33 46 41 36 44 38  34 34 34 37 38 36 42 31   F43FA6D8 444786B1
```

```
Padding added by the USB capture system (usb.capdata), 592 byte(s)    分组: 18790 · 已显示: 18790 (100.0%)    配置: Default
```

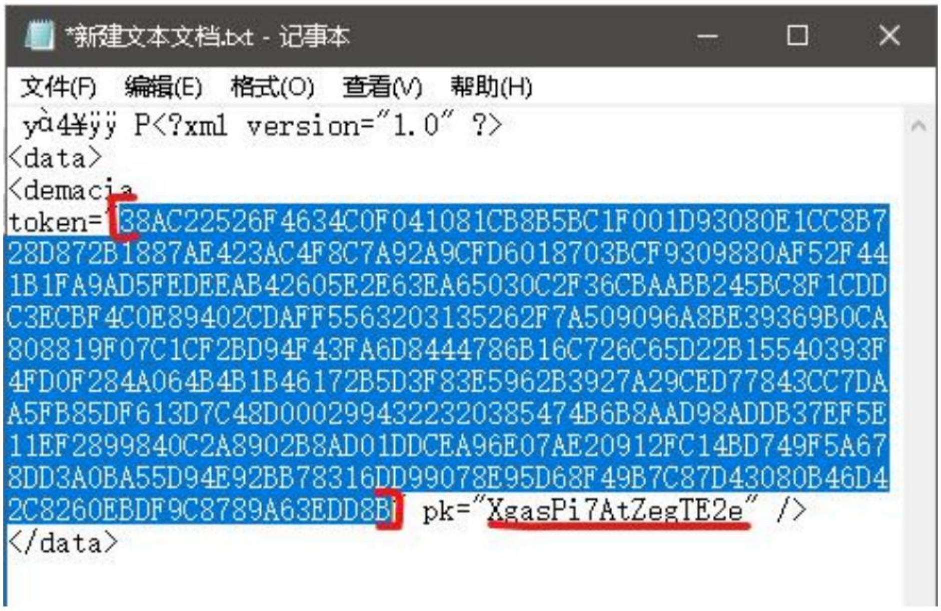
12, you can see the corresponding results found in the lower right corner. If not found, please refer to the following text to re-capture

Right-click on the result and select Copy as Printable Text.



```
30  3e 0a 3c 64 61 74 61                                    <data> ·<demaci
40  61 20 74 6f 6b 65 6e                                    token= "38AC225
50  32 36 46 34 36 33 34                                    F4634C 0F041081
60  43 42 38 42 35 42 43                                    8B5BC1 F001D930
70  38 30 45 31 43 43 38                                    E1CC8B 728D872B
80  31 38 38 37 41 45 34                                    87AE42 3AC4F8C7
90  41 39 32 41 39 43 46                                    2A9CFD 6018703B
a0  43 46 39 33 30 39 38                                    930988 0AF52F44
b0  31 42 31 46 41 39 41                                    1FA9AD 5FEDEEAB
c0  34 32 36 30 35 45 32                                    605E2E 63EA6503
d0  30 43 32 46 33 36 43                                    2F36CB AABB245B
e0  43 38 46 31 43 44 44                                    F1CDDC 3ECBF4C0
f0  45 38 39 34 30 32 43                                    9402CD AFF55632
00  30 33 31 33 35 32 36                                    135262 F7A50909
10  36 41 38 42 45 33 39 33  36 39 42 30 43 41 38 30   6A8BE393 69B0CA80
20  38 38 31 39 46 30 37 43  31 43 46 32 42 44 39 34   8819F07C 1CF2BD94
30  46 34 33 46 41 36 44 38  34 34 34 37 38 36 42 31   F43FA6D8 444786B1
```

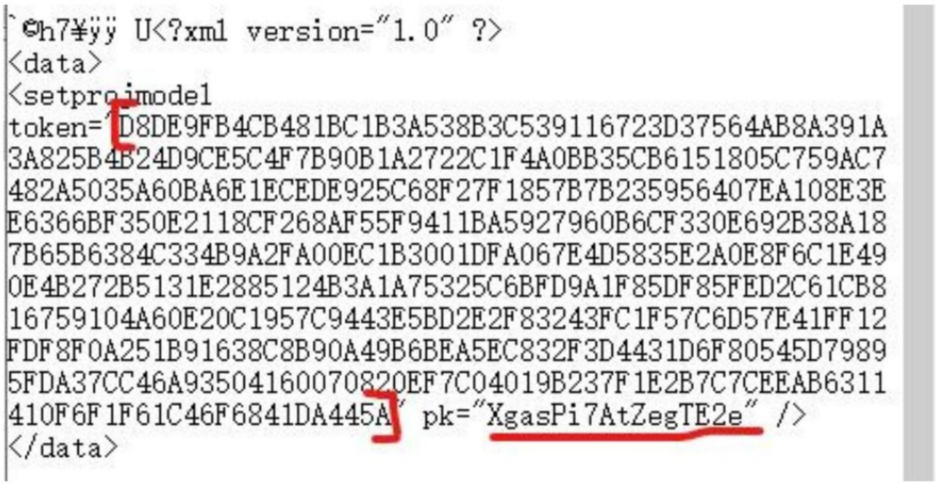
13. Find a text file and paste it into it, and we will get the demacia_token and demacia_pk A set of keys.



```
 yà4¥ÿÿ P<?xml version="1.0" ?>
<data>
<demacia
token="38AC22526F4634C0F041081CB8B5BC1F001D93080E1CC8B7
28D872B1887AE423AC4F8C7A92A9CFD6018703BCF9309880AF52F44
1B1FA9AD5FEDEEAB42605E2E63EA65030C2F36CBAABB245BC8F1CDD
C3ECBF4C0E89402CDAFF5563203135262F7A509096A8BE39369B0CA
808819F07C1CF2BD94F43FA6D8444786B16C726C65D22B15540393F
4FD0F284A064B4B1B46172B5D3F83E5962B3927A29CED77843CC7DA
A5FB85DF613D7C48D00029943223203854 74B6B8AAD98ADDB37EF5E
11EF2899840C2A8902B8AD01DDCEA96E07AE20912FC14BD749F5A67
8DD3A0BA55D94E92BB78316DD99078E95D68F49B7C87D43080B46D4
2C8260EBDF9C8789A63EDD8B" pk="XgasPi7AtZegTE2e" />
</data>
```

14. In the same way, continue to search for setprojmodel token= and get

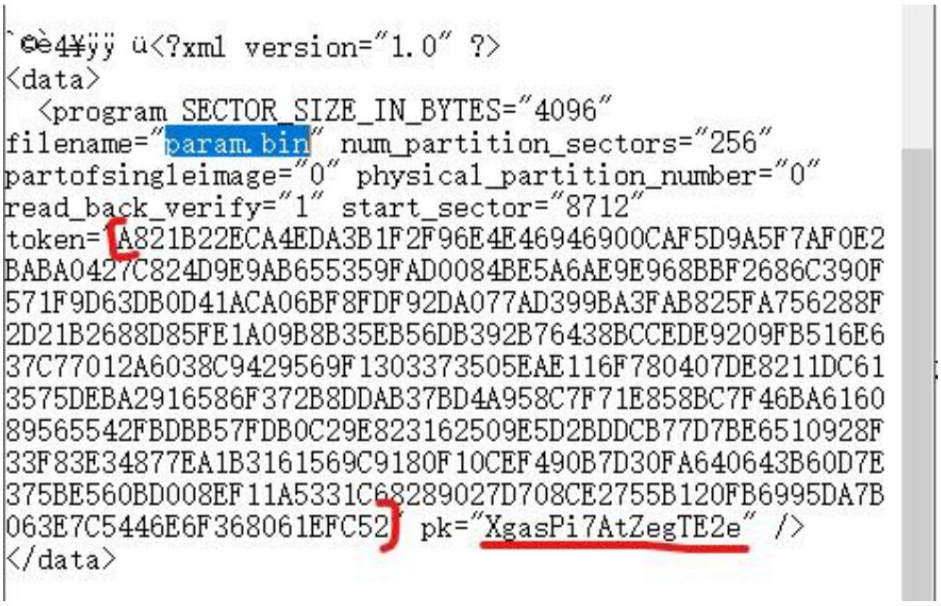
setprojmodel_token and setprojmodel_pk A set of keys.



```
`©h7¥ÿÿ U<?xml version="1.0" ?>
<data>
<setprojmodel
token="D8DE9FB4CB481BC1B3A538B3C539116723D37564AB8A391A
3A825B4B24D9CE5C4F7B90B1A2722C1F4A0BB35CB6151805C759AC7
482A5035A60BA6E1ECEDE925C68F27F1857B7B235956407EA108E3E
E6366BF350E2118CF268AF55F9411BA5927960B6CF330E692B38A18
7B65B6384C334B9A2FA00EC1B3001DFA067E4D5835E2A0E8F6C1E49
0E4B272B5131E2885124B3A1A75325C6BFD9A1F85DF85FED2C61CB8
16759104A60E20C1957C9443E5BD2E2F83243FC1F57C6D57E41FF12
FDF8F0A251B91638C8B90A49B6BEA5EC832F3D4431D6F80545D7989
5FDA37CC46A93504160070820EF7C04019B237F1E2B7C7CEEAB6311
410F6F1F61C46F6841DA445A" pk="XgasPi7AtZegTE2e" />
</data>
```

15. In the same way, continue to search param.bin and get a set of flash_token and flash_pk

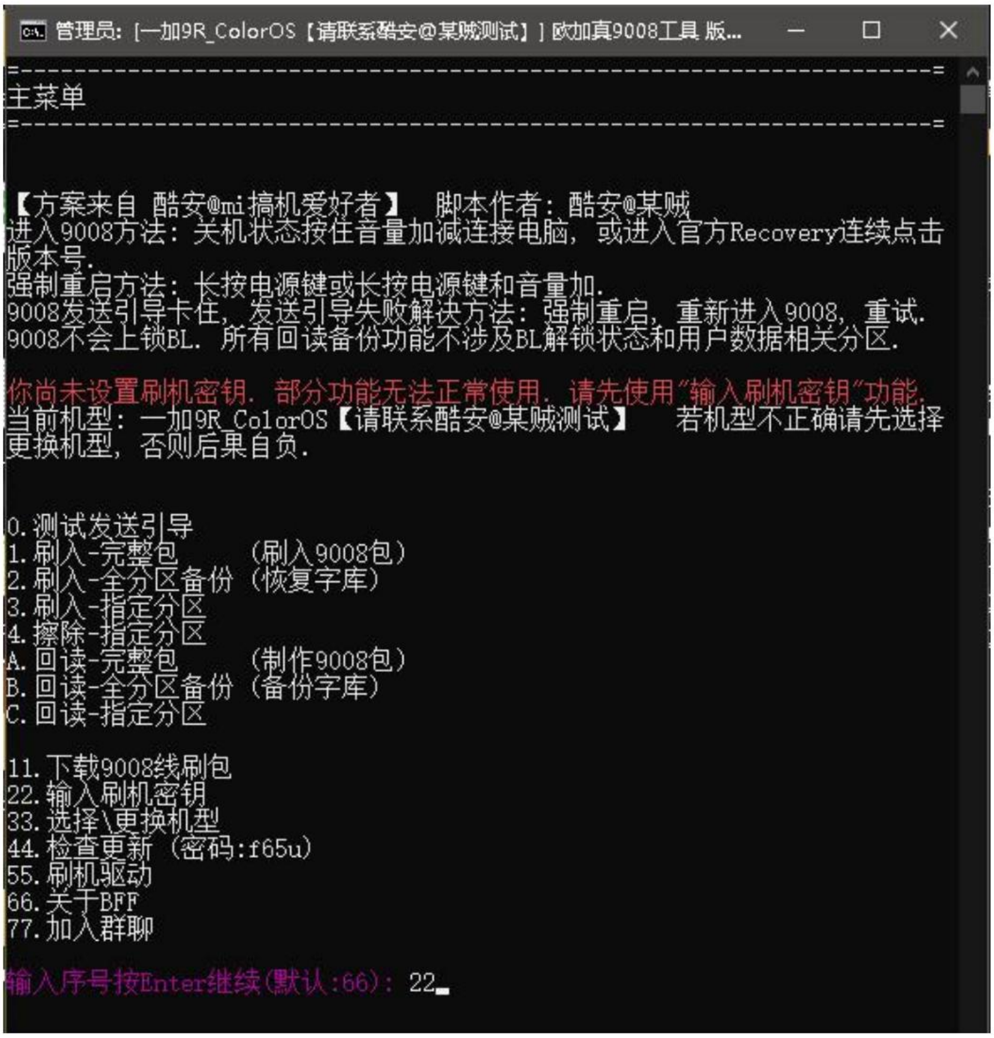
Key.



```
`©è4¥ÿÿ ü<?xml version="1.0" ?>
<data>
  <program SECTOR_SIZE_IN_BYTES="4096"
filename="param.bin" num_partition_sectors="256"
partofsingleimage="0" physical_partition_number="0"
read_back_verify="1" start_sector="8712"
token=A821B22ECA4EDA3B1F2F96E4E46946900CAF5D9A5F7AF0E2
BABA0427C824D9E9AB655359FAD0084BE5A6AE9E968BBF2686C390F
571F9D63DB0D41ACA06BF8FDF92DA077AD399BA3FAB825FA756288F
2D21B2688D85FE1A09B8B35EB56DB392B76438BCCEDE9209FB516E6
37C77012A6038C9429569F1303373505EAE116F780407DE8211DC61
3575DEBA2916586F372B8DDAB37BD4A958C7F71E858BC7F46BA6160
89565542FBDBB57FDB0C29E823162509E5D2BDDCB77D7BE6510928F
33F83E34877EA1B3161569C9180F10CEF490B7D30FA640643B60D7E
375BE560BD008EF11A5331C68289027D708CE2755B120FB6995DA7B
063E7C5446E6F368061EFC52" pk="XgasPi7AtZegTE2e" />
</data>
```

Generally speaking, the three pks should be the same.

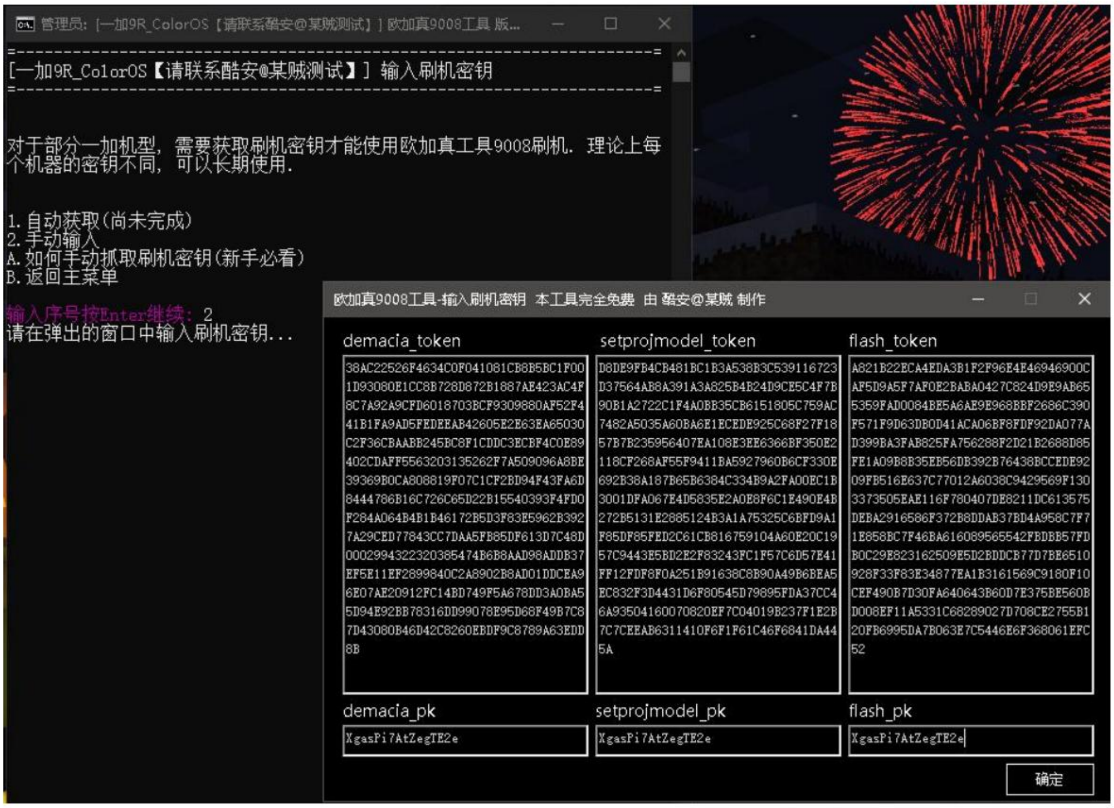
16. Open the Ogazhen 9008 tool, select and enter the flash key, and press Enter to confirm.



管理员: [一加9R_ColorOS【请联系酷安@某贼测试】] 欧加真9008工具 版...

```
=------------------------------------------------------------------------=
主菜单
=------------------------------------------------------------------------=


【方案来自 酷安@mi搞机爱好者】  脚本作者: 酷安@某贼
进入9008方法: 关机状态按住音量加减连接电脑, 或进入官方Recovery连续点击
版本号.
强制重启方法: 长按电源键或长按电源键和音量加.
9008发送引导卡住, 发送引导失败解决方法: 强制重启, 重新进入9008, 重试.
9008不会上锁BL. 所有回读备份功能不涉及BL解锁状态和用户数据相关分区.

你尚未设置刷机密钥. 部分功能无法正常使用. 请先使用"输入刷机密钥"功能.
当前机型: 一加9R_ColorOS【请联系酷安@某贼测试】    若机型不正确请先选择
更换机型, 否则后果自负.


0.测试发送引导
1.刷入-完整包      (刷入9008包)
2.刷入-全分区备份  (恢复字库)
3.刷入-指定分区
4.擦除-指定分区
A.回读-完整包      (制作9008包)
B.回读-全分区备份  (备份字库)
C.回读-指定分区

11.下载9008线刷包
22.输入刷机密钥
33.选择\更换机型
44.检查更新 (密码:f65u)
55.刷机驱动
66.关于BFF
77.加入群聊

输入序号按Enter继续(默认:66): 22_
```

Select Manual Input. Click OK after input.



```
管理员: [一加9R_ColorOS【请联系酷安@某贼测试】] 欧加真9008工具 版...
=-----------------------------------------------------------------------=
[一加9R_ColorOS【请联系酷安@某贼测试】] 输入刷机密钥
=-----------------------------------------------------------------------=


对于部分一加机型, 需要获取刷机密钥才能使用欧加真工具9008刷机. 理论上每
个机器的密钥不同, 可以长期使用.


1. 自动获取(尚未完成)
2. 手动输入
A. 如何手动抓取刷机密钥(新手必看)
B. 返回主菜单

输入序号按Enter继续: 2
请在弹出的窗口中输入刷机密钥...
```

欧加真9008工具-输入刷机密钥 本工具完全免费 由 酷安@某贼 制作

demacia_token

```
38AC22526F4634C0F041081CB8B5BC1F00
1D93080E1CC8B728D872B1887AE423AC4F
8C7A92A9CFD6018703BCF9309880AF52F4
41B1FA9AD5FEDEEAB42605E2E63EA65030
C2F36CBAABB245BC8F1CDDC3ECBF4C0E89
402CDAFF5563203135262F7A509096A8BE
39369B0CA808819F07C1CF2BD94F43FA6D
8444786B16C726C65D22B15540393F4FD0
F284A064B4B1B46172B5D3F83E5962B392
7A29CED77843CC7DAA5FB85DF613D7C48D
00029943223203854 74B6B8AAD98ADDB37
EF5E11EF2899840C2A8902B8AD01DDCEA9
6E07AE20912FC14BD749F5A678DD3A0BA5
5D94E92BB78316DD99078E95D68F49B7C8
7D43080B46D42C8260EBDF9C8789A63EDD
8B
```

setprojmodel_token

```
D8DE9FB4CB481BC1B3A538B3C539116723
D37564AB8A391A3A825B4B24D9CE5C4F7B
90B1A2722C1F4A0BB35CB6151805C759AC
7482A5035A60BA6E1ECEDE925C68F27F18
57B7B235956407EA108E3EE6366BF350E2
118CF268AF55F9411BA5927960B6CF330E
692B38A187B65B6384C334B9A2FA00EC1B
3001DFA067E4D5835E2A0E8F6C1E490E4B
272B5131E2885124B3A1A75325C6BFD9A1
F85DF85FED2C61CB816759104A60E20C19
57C9443E5BD2E2F83243FC1F57C6D57E41
FF12FDF8F0A251B91638C8B90A49B6BEA5
EC832F3D4431D6F80545D79895FDA37CC4
6A93504160070820EF7C04019B237F1E2B
7C7CEEAB6311410F6F1F61C46F6841DA44
5A
```

flash_token

```
A821B22ECA4EDA3B1F2F96E4E46946900C
AF5D9A5F7AF0E2BABA0427C824D9E9AB65
5359FAD0084BE5A6AE9E968BBF2686C390
F571F9D63DB0D41ACA06BF8FDF92DA077A
D399BA3FAB825FA756288F2D21B2688D85
FE1A09B8B35EB56DB392B76438BCCEDE92
09FB516E637C77012A6038C9429569F130
3373505EAE116F780407DE8211DC613575
DEBA2916586F372B8DDAB37BD4A958C7F7
1E858BC7F46BA616089565542FBDBB57FD
B0C29E823162509E5D2BDDCB77D7BE6510
928F33F83E34877EA1B3161569C9180F10
CEF490B7D30FA640643B60D7E375BE560B
D008EF11A5331C68289027D708CE2755B1
20FB6995DA7B063E7C5446E6F368061EFC
52
```

demacia_pk: XgasPi7AtZegTE2e

setprojmodel_pk: XgasPi7AtZegTE2e

flash_pk: XgasPi7AtZegTE2e

Wait a moment and it will be written automatically.

17. After writing, you can realize free reading and writing of 9008. Note: The key of each machine is different.

The same machine can be used for a long time, but it is not universal between different machines.

# How to re-grab the key

If the key fails to be downloaded, you need to download it again. First, stop flashing, exit MsmDownloadTool, close

Close the packet capture software, unplug the phone, long-press the power button and volume up button to restart, and then go through the packet capture process again.

If the phone cannot be turned off, you can try to enter Recovery mode to turn it off, or press and hold the power button and volume up button.

Restart, release the power button when the screen goes black, hold down the volume up and down, insert the data cable, and you can enter 9008.