第十五届CCFC计算机取证技术峰会暨展会

THE 15TH CHINA COMPUTER FORENSIC CONFERENCE & EXHIBITION

电子数据取证技术最新发展与应用

2019.11.5 -11.7

武汉市·荷田大酒店

安卓系统开机密码清除途径

河北阮咸科技有限公司
（三人行联合开发实验室）

李佳林

CONTENTS

1.Adb+root

2. 用户区FBE/FDE

3. MTK usb com/9008 读写内置存储

4.刷特定分区（清除脚本置入到boot/system）

5.后门程序

6.密码暴力破解

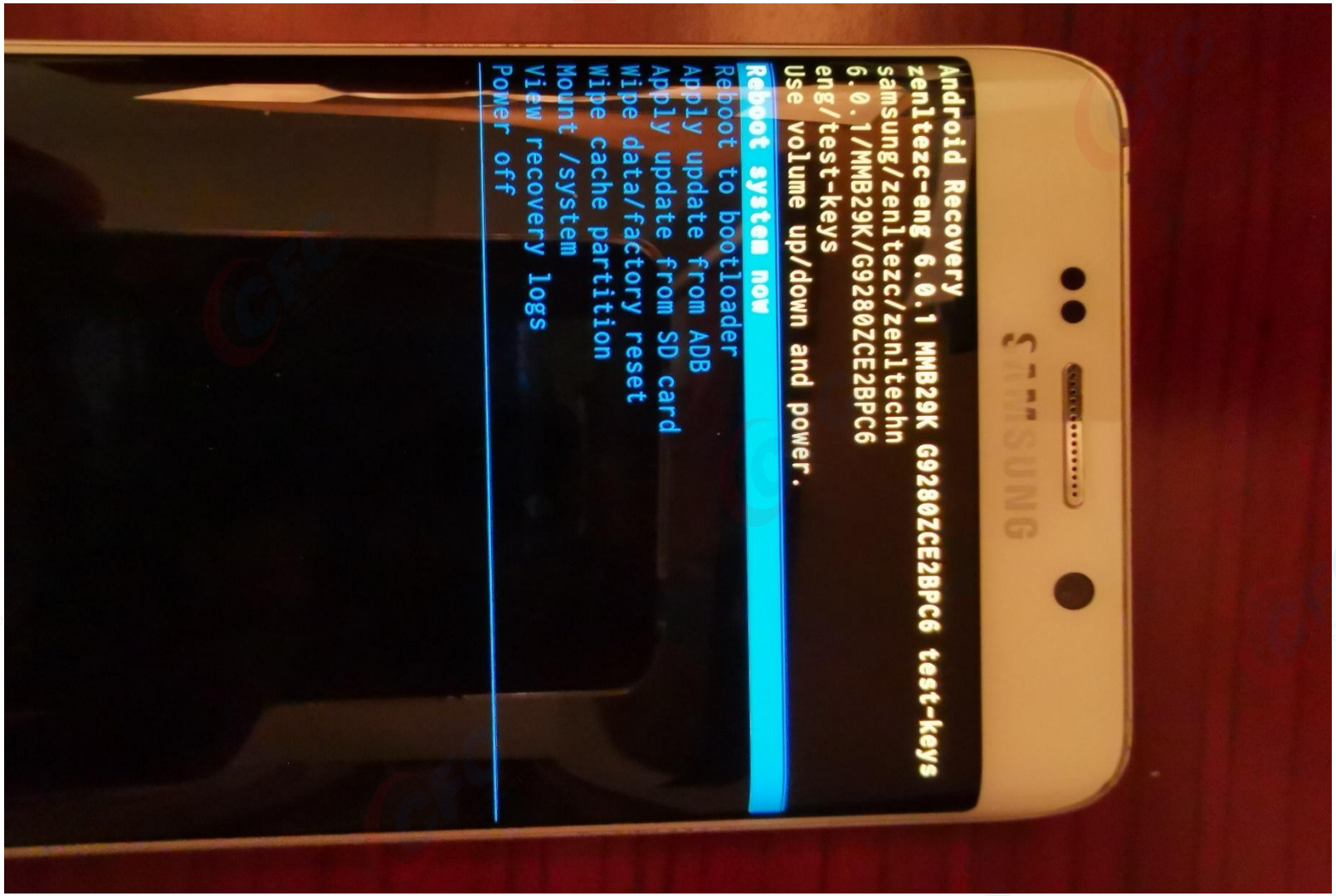
7.存储器外部处理

ADB/ROOT

ENG

工厂在对生产的手机进行测试时使用
1.拥有完整的ROOT权限用来测试每个硬件和软件。
2.默认开启adb用来记录测试结果

ADB/ROOT--ENG


Android Recovery
zenltezc-eng 6.0.1 MMB29K G9280ZCE2BPC6 test-keys
samsung/zenltezc/zenltechn
6.0.1/MMB29K/G9280ZCE2BPC6
eng/test-keys
Use volume up/down and power.
Reboot system now
Reboot to bootloader
Apply update from ADB
Apply update from SD card
Wipe data/factory reset
Wipe cache partition
Mount /system
View recovery logs
Power off
SAMSUNG

Adb/root--eng

```
root@zenltechn:/ # cd /data/data
cd /data/data
root@zenltechn:/data/data # ls
ls
com.alipay.security.mobile.authenticator
com.android.apps.tag
com.android.backupconfirm
com.android.bluetooth
com.android.bluetoothmidiservice
com.android.browser.provider
com.android.calendar
com.android.calllogbackup
com.android.captiveportallogin
com.android.carrierconfig
com.android.certinstaller
com.android.contacts
com.android.defcontainer
com.android.documentsui
com.android.dreams.basic
com.android.dreams.phototable
com.android.externalstorage
com.android.htmlviewer
com.android.incallui
com.android.inputdevices
```

自制 adb+root

修改手机官方固件并且刷入手机中，在有开机密码的前提下，开启adb默认配对并且获取ROOT权限。

Adb/root--华为MATE9 安卓9.0版本通过软件自制ROOT

Adb无ROOT

仅仅能够打开并且配对adb通道，无ROOT权限，也可以清除开机密码

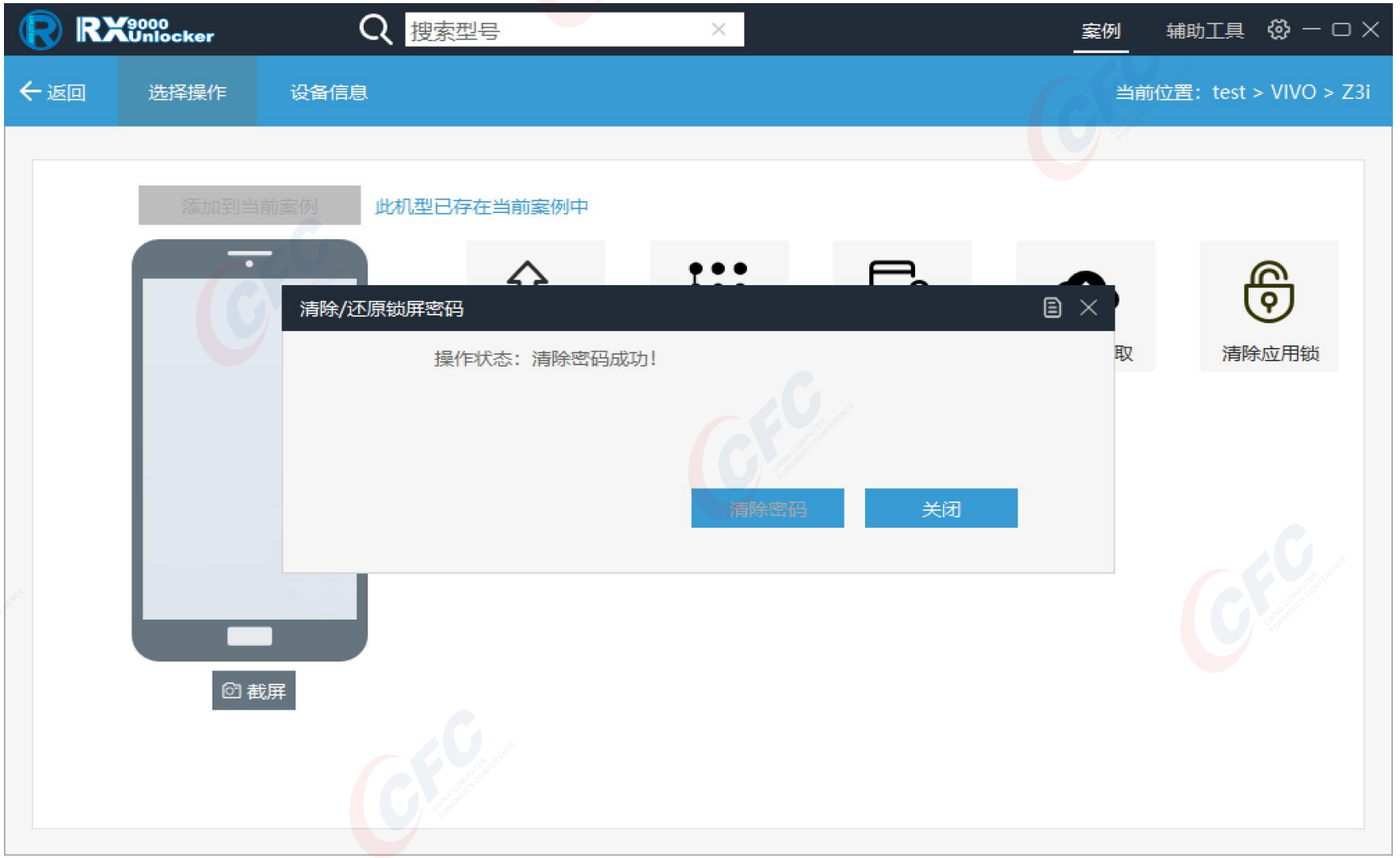
Adb无root--VIVO Z3i通过adb清除开机密码

Adb无root--VIVO Z3i通过adb清除开机密码

VIVO Z3I（安卓8.1）官方recovery可以强制开启adb并且默认配对，但是并无root权限。可以通过adb通道干掉密码附着进程

```
C:\Program Files (x86)\RX-Unlocker\bin>adb shell
PD1813E:/ $ su
su
/system/bin/sh: su: not found
127|PD1813E:/ $
```

Adb无root--VIVO Z3i通过adb清除开机密码

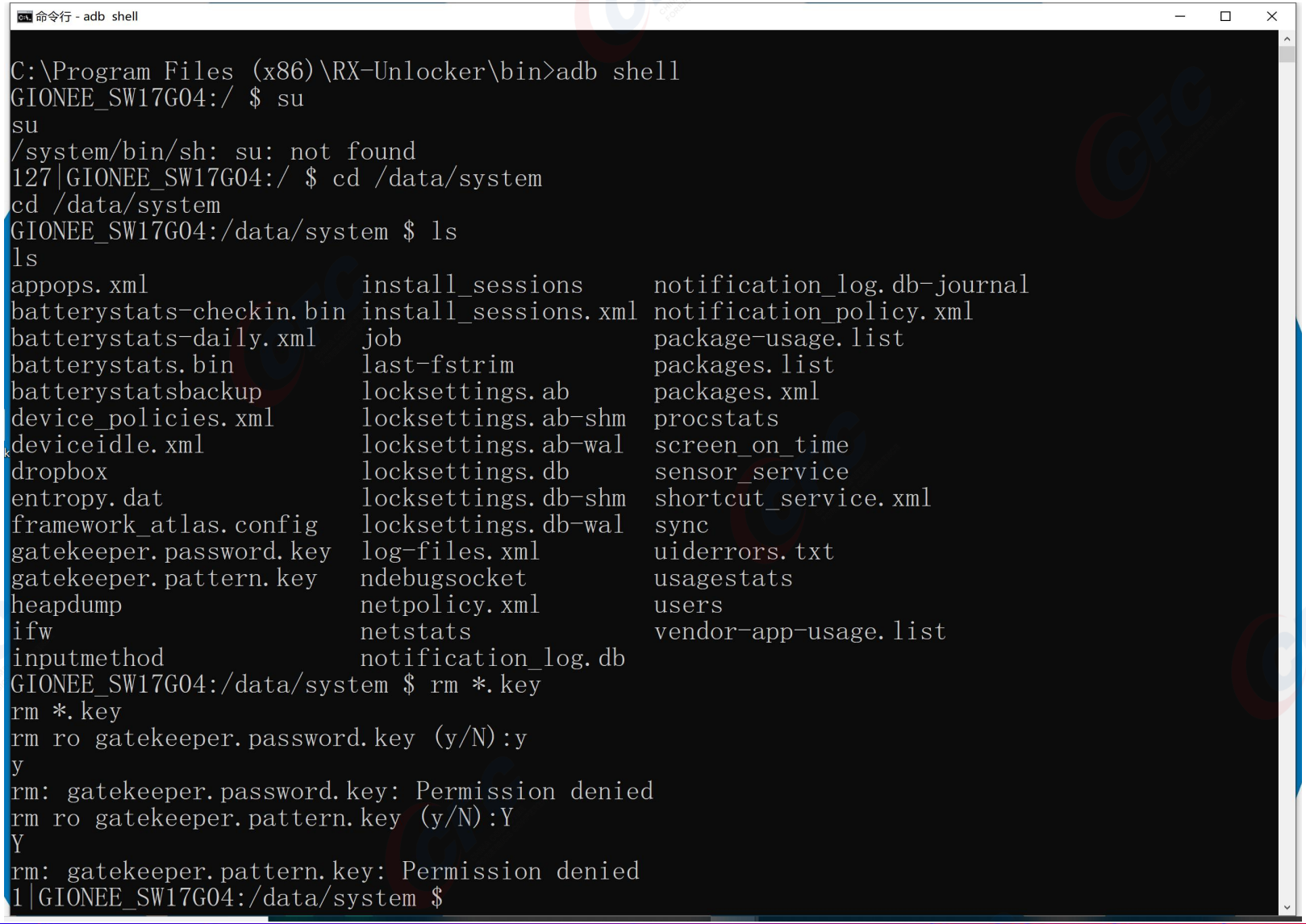


Adb无root--VIVO Z3i通过adb清除开机密码

ADB无ROOT，金立S10通过漏洞权限进行清除开机密码

金立S10手机在recovery下拥有adb默认配对，但是并无root权限，我们可以访问但是无法删除开机密码，所以我们可以利用漏洞去提权获取暂时的ROOT权限然后利用root权限清除开机密码

ADB无ROOT，金立S10通过漏洞权限进行清除开机密码



ADB无ROOT，金立S10通过漏洞权限进行清除开机密码

```
C:\Program Files (x86)\RX-Unlocker\bin>adb push C:\Users\57066\Desktop\rx-unlocker /data/l
ocal/tmp
10405 KB/s (42832 bytes in 0.004s)

C:\Program Files (x86)\RX-Unlocker\bin>adb shell
GIONEE_SW17G04:/ $ su
su
/system/bin/sh: su: not found
127|GIONEE_SW17G04:/ $ cd /data/local/tmp
cd /data/local/tmp
GIONEE_SW17G04:/data/local/tmp $ chmod 777 rx-unlocker
chmod 777 rx-unlocker
GIONEE_SW17G04:/data/local/tmp $ ./rx-unlocker
./rx-unlocker
UID: 0  cap: 3fffffffff  selinux: permissive
GIONEE_SW17G04:/data/local/tmp # cd /data/system
cd /data/system
GIONEE_SW17G04:/data/system # ls
ls
appops.xml                 install_sessions      notification_log.db-journal
batterystats-checkin.bin   install_sessions.xml  notification_policy.xml
batterystats-daily.xml     job                   package-usage.list
batterystats.bin           last-fstrim           packages.list
batterystatsbackup         locksettings.ab       packages.xml
device_policies.xml        locksettings.ab-shm   procstats
deviceidle.xml             locksettings.ab-wal   screen_on_time
dropbox                    locksettings.db       sensor_service
entropy.dat                locksettings.db-shm   shortcut_service.xml
framework_atlas.config     locksettings.db-wal   sync
gatekeeper.password.key    log-files.xml         uiderrors.txt
gatekeeper.pattern.key     ndebugsocket          usagestats
heapdump                   netpolicy.xml         users
ifw                        netstats              vendor-app-usage.list
```

ADB无ROOT，金立S10通过漏洞权限进行清除开机密码

```
batterystats-checkin.bin  install_sessions.xml  notification_policy.xml
batterystats-daily.xml    job                   package-usage.list
batterystats.bin          last-fstrim           packages.list
batterystatsbackup        locksettings.ab       packages.xml
device_policies.xml       locksettings.ab-shm   procstats
deviceidle.xml            locksettings.ab-wal   screen_on_time
dropbox                   locksettings.db       sensor_service
entropy.dat               locksettings.db-shm   shortcut_service.xml
framework_atlas.config    locksettings.db-wal   sync
gatekeeper.password.key   log-files.xml         uiderrors.txt
gatekeeper.pattern.key    ndebugsocket          usagestats
heapdump                  netpolicy.xml         users
ifw                       netstats              vendor-app-usage.list
inputmethod               notification_log.db
GIONEE_SW17G04:/data/system # rm *.key
rm *.key
GIONEE_SW17G04:/data/system # ls
ls
appops.xml                install_sessions.xml  notification_log.db-journal
batterystats-checkin.bin  job                   notification_policy.xml
batterystats-daily.xml    last-fstrim           package-usage.list
batterystats.bin          locksettings.ab       packages.list
batterystatsbackup        locksettings.ab-shm   packages.xml
device_policies.xml       locksettings.ab-wal   procstats
deviceidle.xml            locksettings.db       screen_on_time
dropbox                   locksettings.db-shm   sensor_service
entropy.dat               locksettings.db-wal   shortcut_service.xml
framework_atlas.config    log-files.xml         sync
heapdump                  ndebugsocket          uiderrors.txt
ifw                       netpolicy.xml         usagestats
inputmethod               netstats              users
install_sessions          notification_log.db   vendor-app-usage.list
GIONEE_SW17G04:/data/system # _
```

漏洞权限

1.三星S8,S8+安卓7.0—安卓9.0，可以利用漏洞权限提取整个data/data目录（包含微信分身）

2.OPPO R15，A9X，RanoZ等安卓8.1-9.0，可以利用漏洞权限镜像或者提取整个data/data目录（包含微信分身）

3.酷派，小米，金立，美图，oppo，360等上百个品牌，2000余款机型可以利用漏洞提权方式进行密码破解，数据镜像，app分身数据提取。

两种用户区加密方式：FDE/FBE

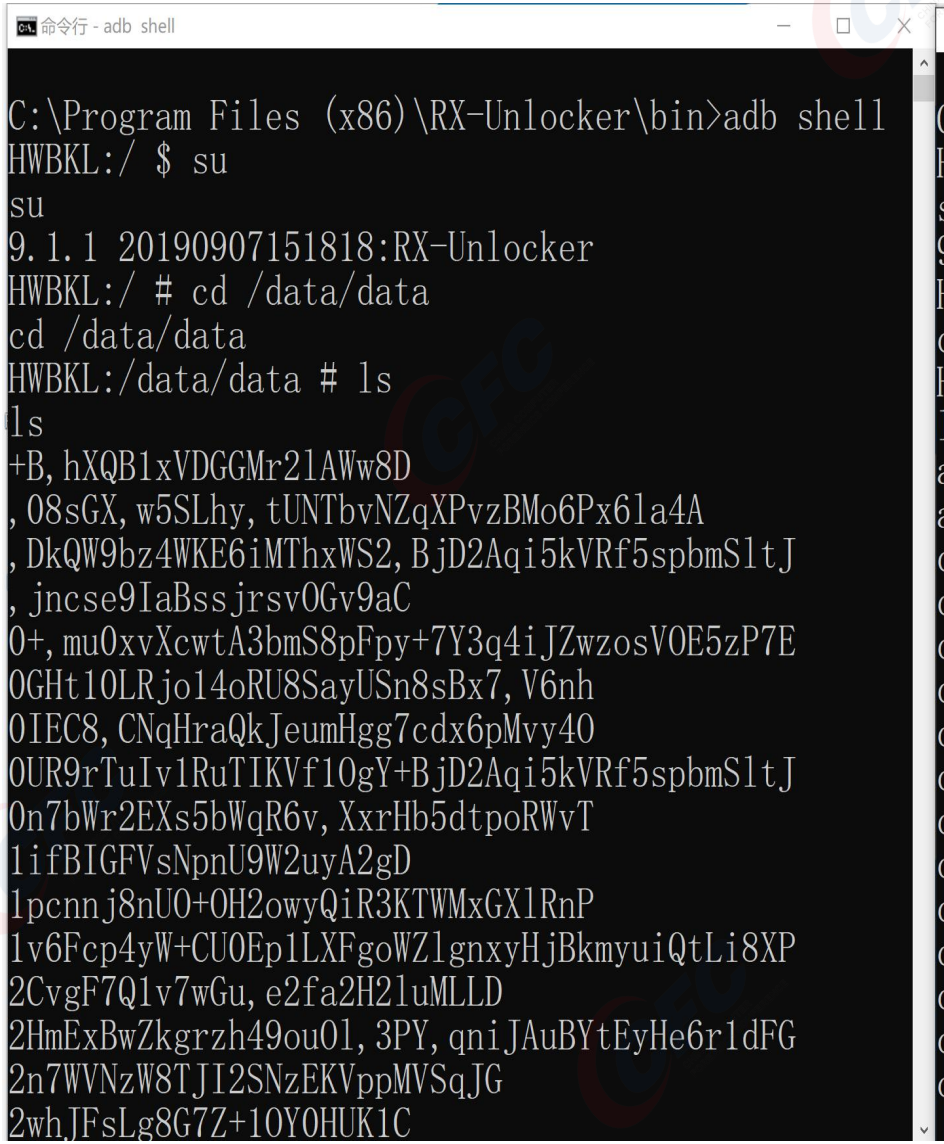
FDE是从安卓4.4开始引入，并在安卓6.0系统开始大面积使用的用户区加密方式。表现为整个用户区域整体加密，未解密情况下，不能解析任何分区结构和数据结构

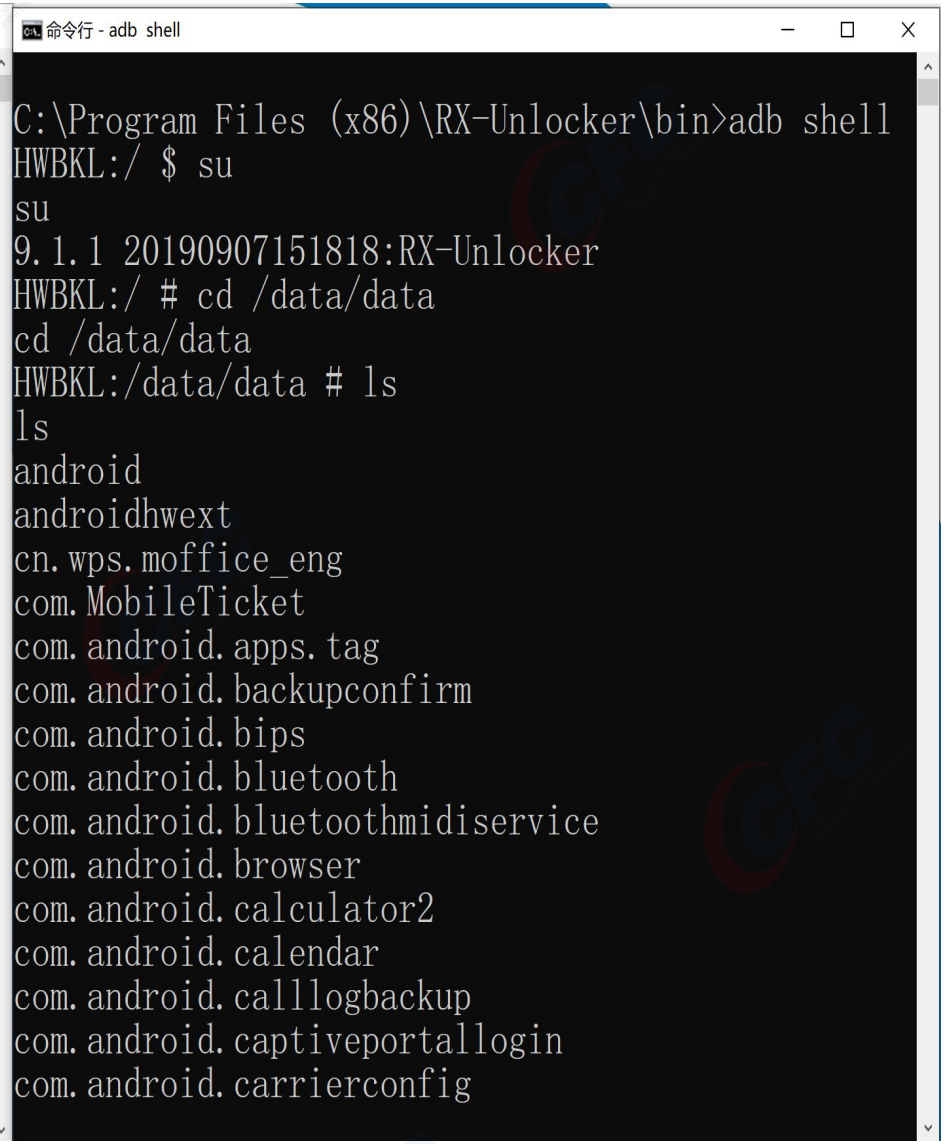
FBE是从安卓7.0开始引入，并在安卓8.0系统开始大面积普及使用的用户区加密方式。变现为用户区域可以在未解密状态下解析到分区结构和数据结构，但是分区内文件被逐一加密不能解析。

FDE加密机型输入开机密码前后数据状态

```
C:\Program Files (x86)\RX-Unlocker\C:\Program Files (x86)\RX-Unlocker\bin>adb shell
HWCAZ:/ $ su                                HWCAZ:/ $ su
su                                          su
2.1.0 20190509224837:RX-Unlocker            2.1.0 20190509224837:RX-Unlocker
HWCAZ:/ # ls /data/data                     HWCAZ:/ # ls /data/data
ls /data/data                               ls /data/data
android                                     android
androidhwext                                androidhwext
cn.wps.moffice_eng                          cn.wps.moffice_eng
com.Qunar                                   com.Qunar
com.achievo.vipshop                         com.achievo.vipshop
com.amap.android.ams                        com.amap.android.ams
com.android.apps.tag                        com.android.apps.tag
com.android.backupconfirm                   com.android.backupconfirm
com.android.bluetooth                       com.android.bluetooth
com.android.bluetoothmidiservice            com.android.bluetoothmidiservice
com.android.browser                         com.android.browser
com.android.calculator2                     com.android.calculator2
com.android.calendar                        com.android.calendar
com.android.calllogbackup                   com.android.calllogbackup
com.android.captiveportallogin              com.android.captiveportallogin
com.android.carrierconfig                   com.android.carrierconfig
com.android.certinstaller                   com.android.certinstaller
com.android.contacts                        com.android.contacts
com.android.cts.ctsshim                     com.android.cts.ctsshim
```

FBE加密机型输入开机密码前后数据状态





两种用户区加密方式：FDE/FBE

总结：

1.FDE加密的机型内部数据在完成开机后自动解密，开机密码并不影响数据解密。

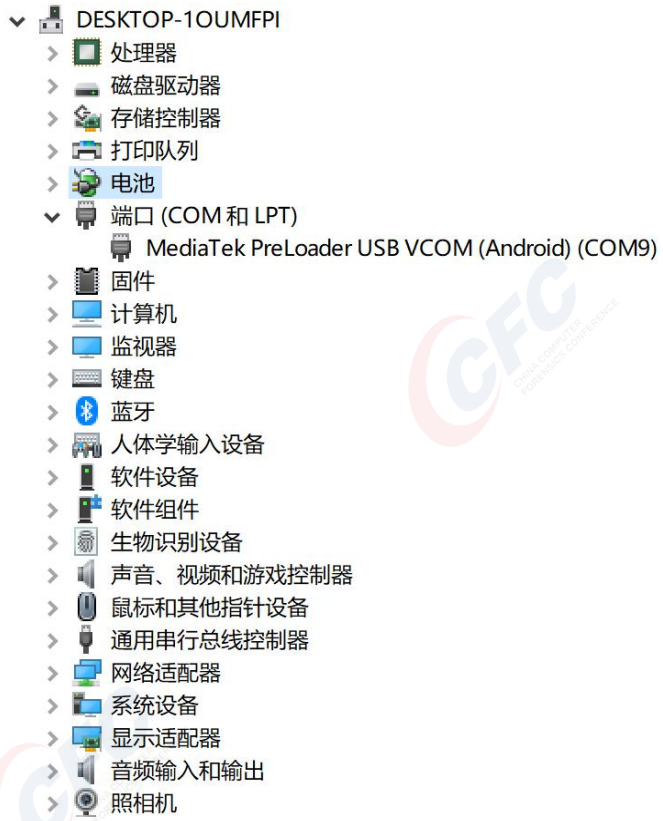
2.FBE加密的机型内部数据要通过开机密码的介入完成解密。

Mtk usb com/9008

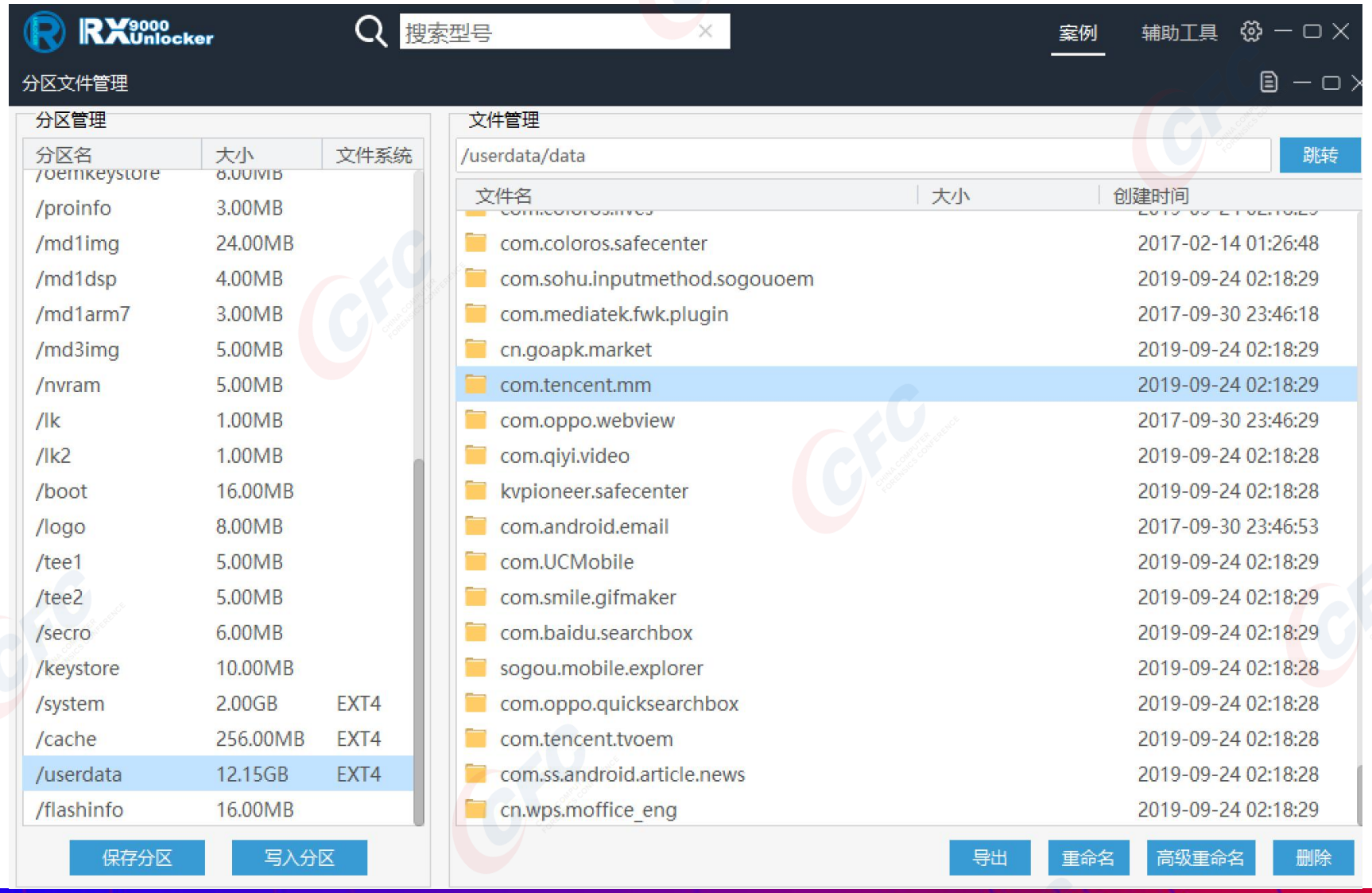
1.普遍存在的一种手机端口，通过USB实现，不依赖手机系统。手机厂商用此端口进行批量写入系统固件，售后进行软件维修使用。

2.拥有完整的读/写协议，可以通过该协议对手机内部存储进行分区镜像/分区写入/文件提取/文件删除等操作。

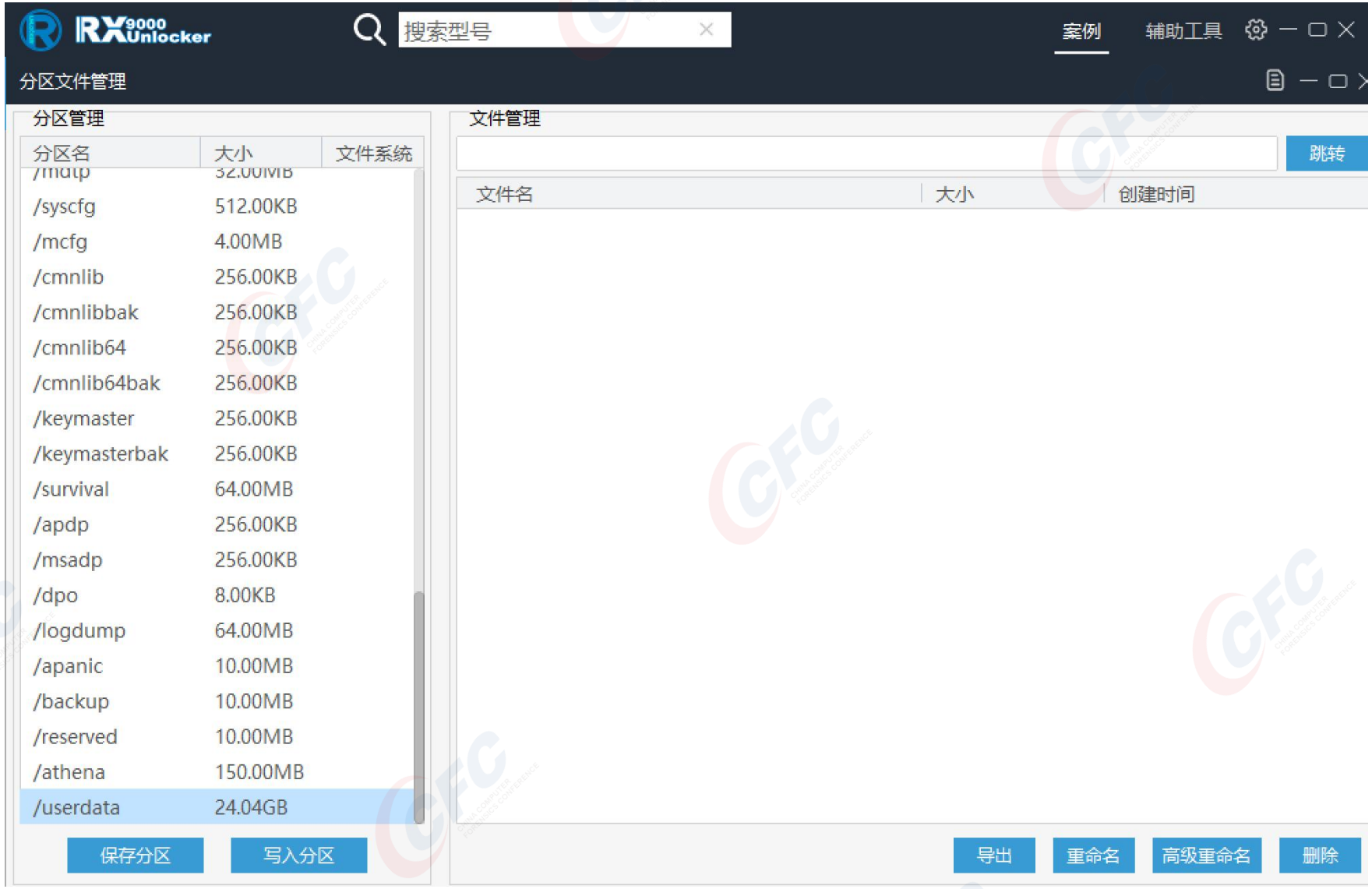
Mtk usb com/9008



未加密机型通过串口分区文件管理访问分区数据



加密机型通过串口分区文件管理访问分区数据



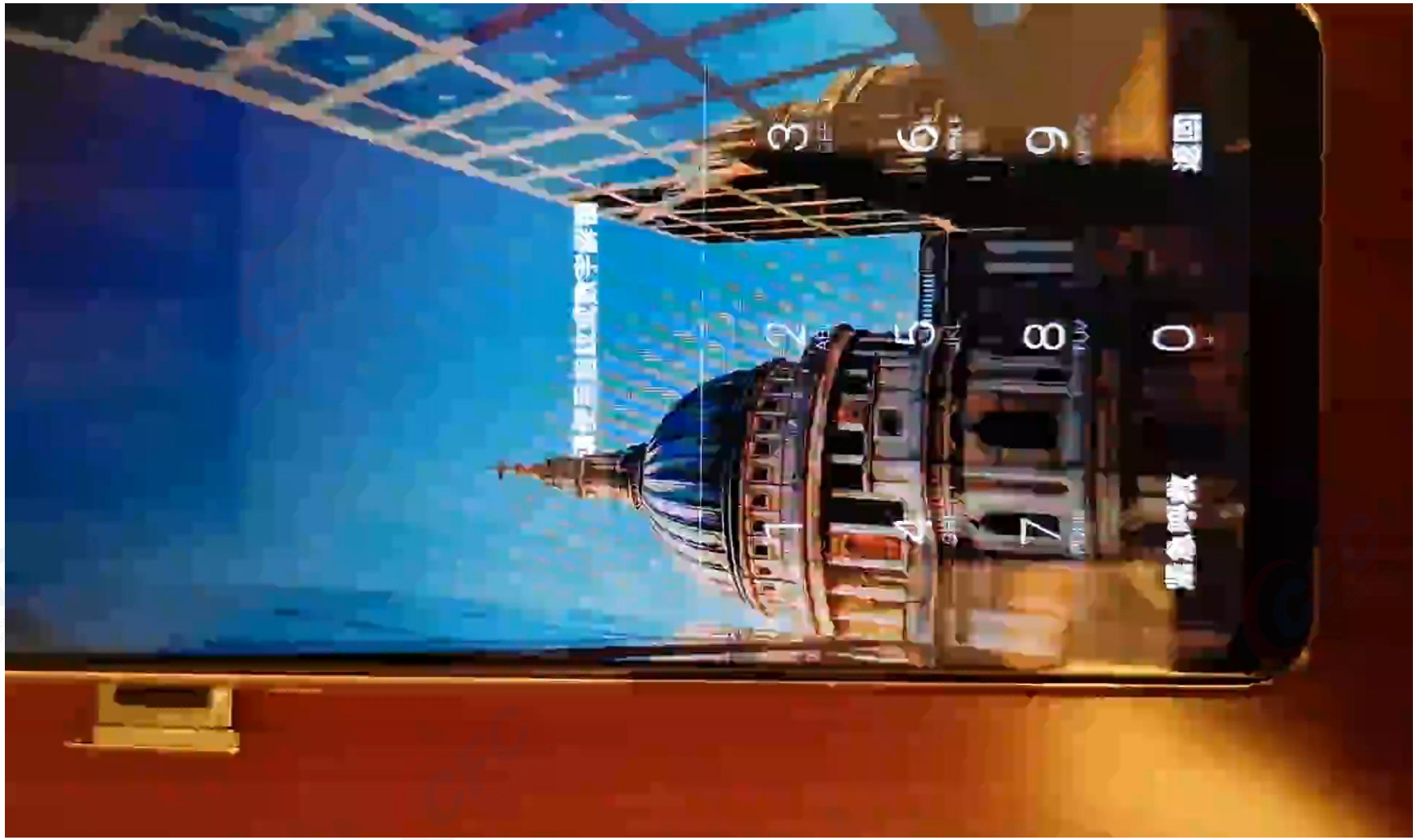
门锁理论/通过分区植入脚本清除开机密码

华为NOVA通过分区植入脚本清除开机密码

后门程序

手机厂商为了更方便的处理手机售后问题，会故意在系统当中添加清除开机密码的程序，我们仅仅需要激活该程序即可清除密码

后门程序



后门程序

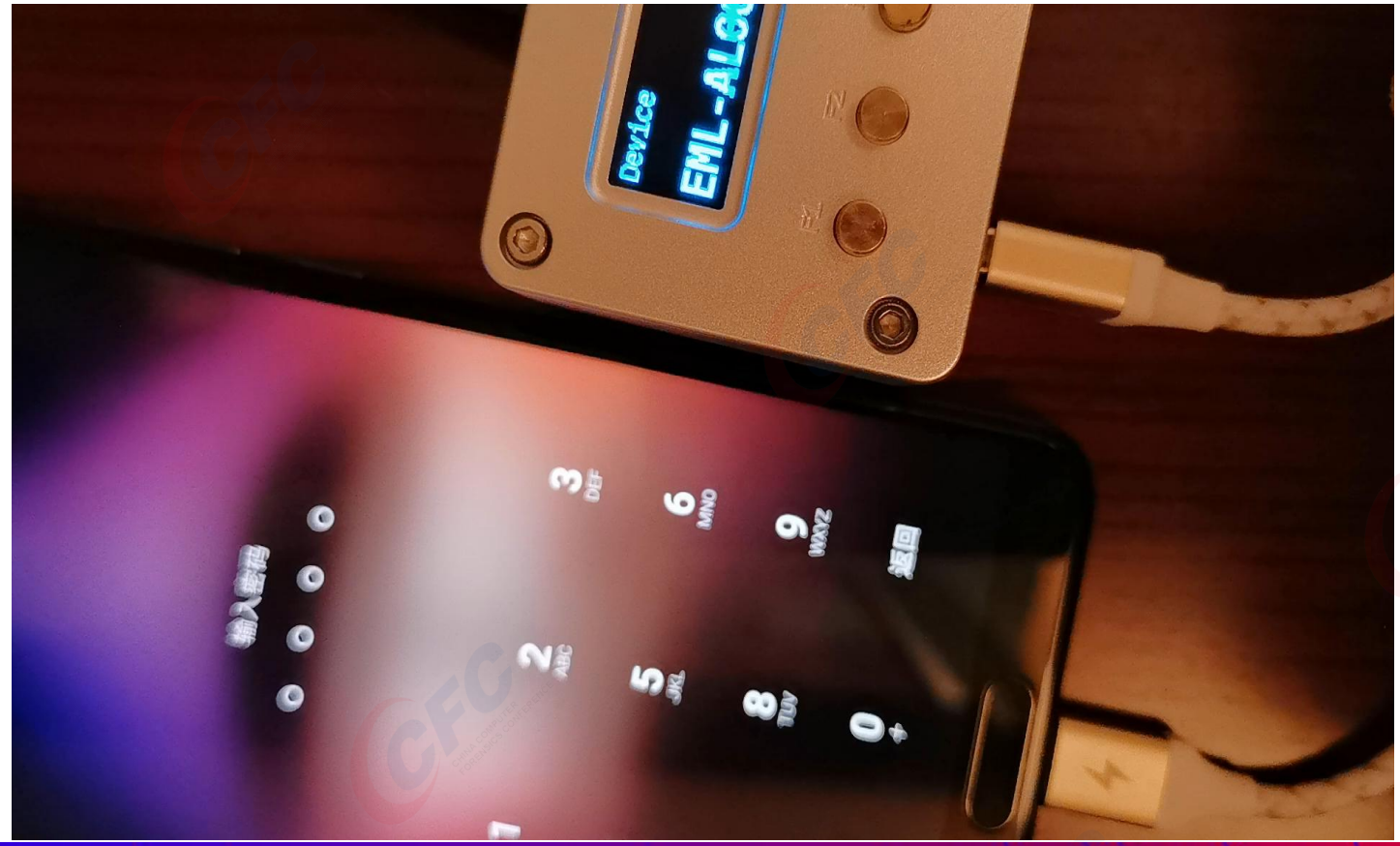
VIVO 全系列FDE机型拥有后门程序，可以通过开启密码清除进程自动清除开机密码（包括S1 X23）。

海信安卓6.0-8.1版本绝大部分拥有后门程序，通过外置存储卡清除开机密码。

OPPO 所有安卓8.1版本机型拥有ROOT后门，轻松开启ADB+ROOT（包括 R17 FIND X）

开机密码暴力破解-在线式

华为从安卓7.0开始引入用户区fbe加密，fbe加密机型破解开机密码主要通过暴力破解实现，诸如Mate10，Mate20

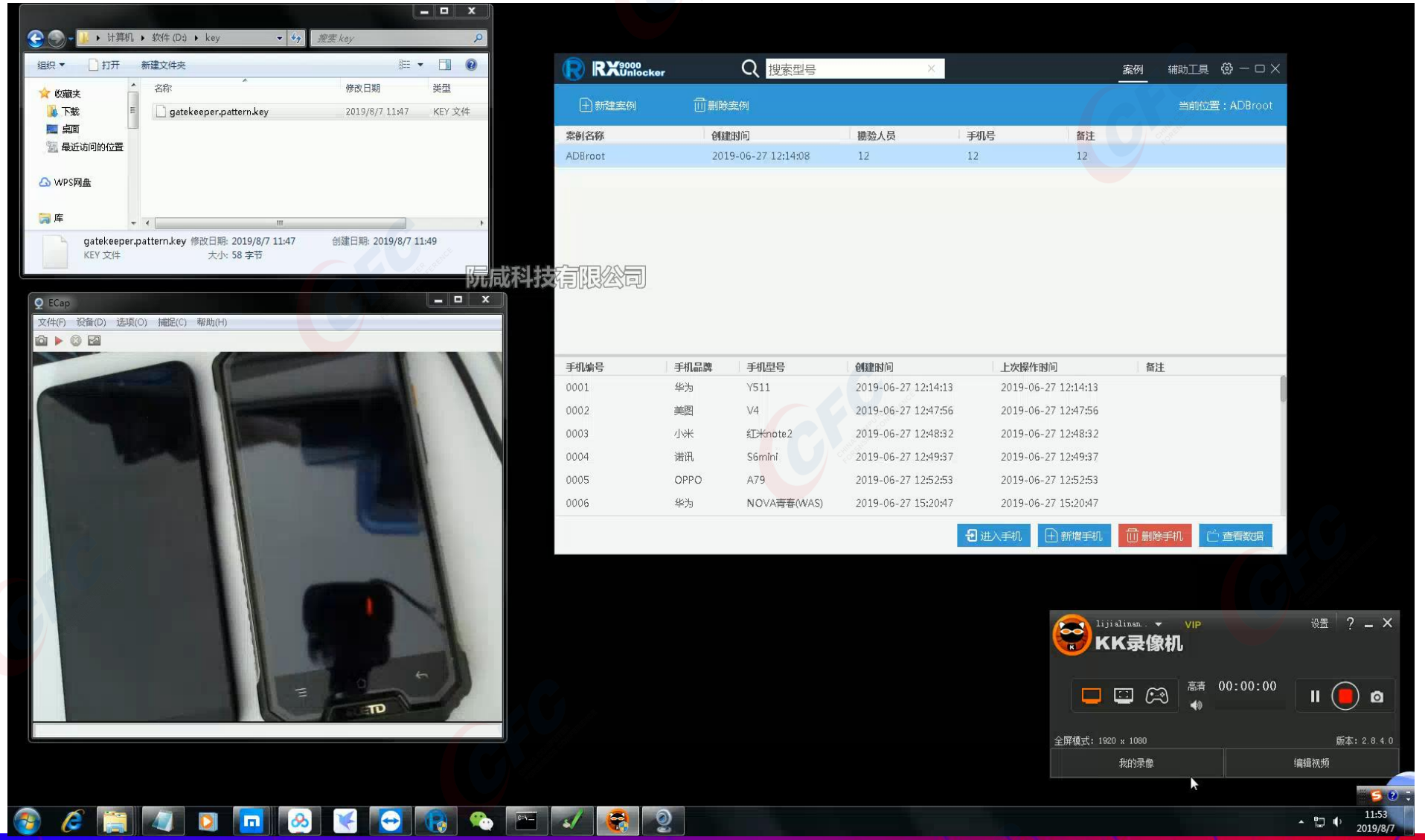


开机密码暴力破解-离线式

1.安卓2.X—5.1版本对password.key; gesture.key进行爆破

2.安卓6.0-8.0版本针对gatekeeper.password.key gatekeeper.pattern.key 进行爆破（部分品牌和机型）

开机密码暴力破解-离线式



阮威科技有限公司

存储器外部处理

有些机器如果无法通过usb通信进行密码清除，那么只能通过line out 或者chip off的方式进行破解

比如R15X,R15梦境，R17,FIND X等

存储器外部处理—OPPO R15X 通过飞线方式清除开机密码

感谢倾听

河北阮咸科技有限公司-三人行实验室