Module I Assignment: Introduction to Android APKs

Mobile Devices Security

Mobile devices security 2019-2020 (group 89)

Raúl Olmedo Checa (100346073)

Ignacio González Díaz-Tendero (100346133)

Tuesday, 25 February 2020

Table of Contents

2. Development of an Android application

This Android app can be divided into four main parts, the Activities, the classes interfacing with the repository, the database where we define our DB convenience methods and the model where we define our custom data objects.

Activities

Each one of them manages one of the screens requested in the lab report:

MainActivity uses a Recycler View component to show the current credentials stored in the SQLite database created for this app, each one of those Cards allows a detailed view when clicked on them, also, it contains a Floating Action Button that allows the user to add a local credential and a Menu Button in the Toolbar that allows the beginning of the import process.

NewRecordActivity allows the user to add a new credential into the local database by selecting as identifier one of the installed apps listed on the Spinner component, again there is a Floating Action Button to save the data and a back Button on the Toolbar that mimics the behavior of pressing the back physical button.

ImportActivity starts the process of importing a credential from the repository, once again the Spinner is populated with the ids of the credentials stored on it, obtained by using an AsyncTask that we will explain later, once the user has confirmed the operation, the data is sent back to the MainActivity by using methods putExtra and getExtra.

EditRecordActivity is started when one of the items in the Recycler View is clicked, revealing the contents of the credentials and a button to show/hide the password based on a 3 seconds timer (implemented using Threads as the WelcomeActivity timer), here we also have a Toolbar Button to export the credential to the external repo, once again using an AsyncTask defined later.

WelcomeActivity is shown the first time the user starts the app; it has an image and starts the MainActivity once 3 seconds have passed.

Repository related classes

In order to interact with the web server, we had to implement three Async Tasks to be run in a different Threads based on the code provided as example by the instructor, each one of them allows us to get a list of credentials, import and export them.

Database

In order to create a local database where we could store the credentials, we had to define our database (in DatabaseContract.class) and a database helper to manage the creation, update and deletion of our actual database file. Once set up, we followed the sqlite api documentation to insert and read entries from the database.

Model

Here we define our Credential custom object that manages the use of Credentials throughout the code

3. “CredHub” App Signing

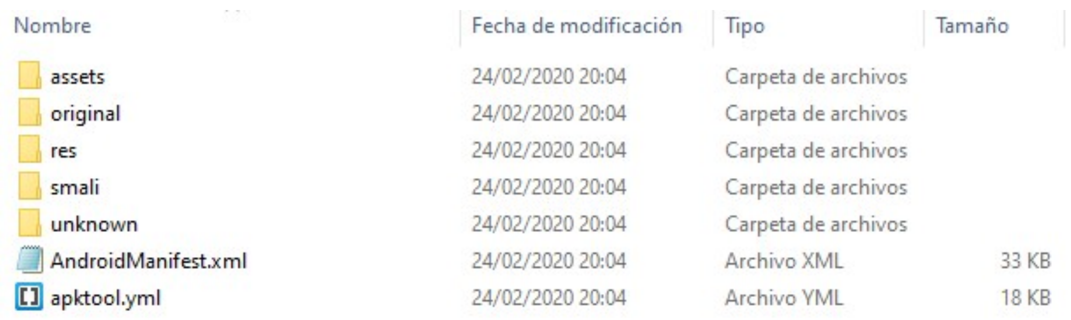
We simply created a keystore and a key by following the process in AndroidStudio to later generate the signed .apk required for the delivery.

4. Signature verification of the application kontaktos.apk

To carry out this section we have made use of apktool and the application kontaktos that has been provided.

Apktool is a utility that can be used for reverse engineering Android applications resources. With it we can decode APK resources to almost original form, we can modify the source code on the fly and rebuild the decoded resources back to APK.

Once we have de-compiled the application kontaktos.apk, we can find all the application structure and the Manifest.xml, in which we can analyze the basic configurations of our application.



Nombre	Fecha de modificación	Tipo	Tamaño
assets	24/02/2020 20:04	Carpeta de archivos	
original	24/02/2020 20:04	Carpeta de archivos	
res	24/02/2020 20:04	Carpeta de archivos	
smali	24/02/2020 20:04	Carpeta de archivos	
unknown	24/02/2020 20:04	Carpeta de archivos	
AndroidManifest.xml	24/02/2020 20:04	Archivo XML	33 KB
apktool.yml	24/02/2020 20:04	Archivo YML	18 KB

At this point, we are going to describe some manifest permissions exposed by the app:

1- <uses-permission android:name="android.permission.CALL_PHONE"/>

Allows an application to initiate a pone call without going through the Dialer user interface for the user to confirm the call.

2- <uses-permission android:name="android.permission.WAKE_LOCK"/>

Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.

3- <uses-permission android:name="android.permission.MODIFY_PHONE_STATE"/>

Allows modification of the telephony state - power on, mmi (Man Machine Interface), etc. This permission does not include making calls. Not for use by third-party applications.

4- <uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>

Allows applications to disable the element that locks the phone (PIN, pattern, default lockscreen, etc)

5- <uses-permission android:name="android.permission.READ_SYNC_SETTINGS"/>
Allows the app to read the “master” syncronization of the phone with all the services (google mail, synchronization of contacts, calendar, etc)

6- <uses-permission android:name="android.permission.WRITE_SYNC_SETTINGS"/>

Similarly to the above permission, this one allows the app to change the state of this syncronization services.

difference between permissions required at runtime and static permissions.

From Android 6.0 All applications must request access to the different elements of the mobile such as the microphone, location, contacts or access to the files of the mobile**.** What was once automatic, now is better controlled, separated and it is in our discretion to allow applications to have certain permissions.

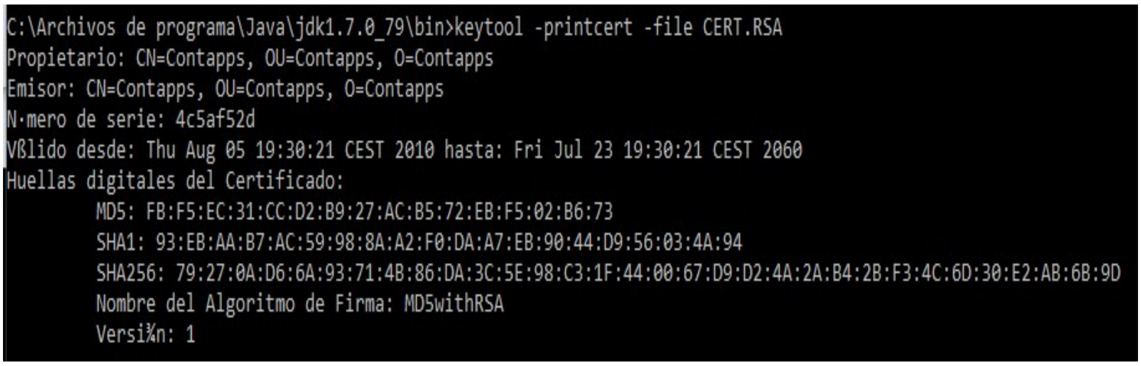
Permissions required at runtime are those in which users will be asked for permissions while the app is running. This way, a user is able to choose which permissions they should grant without affecting the application flow.

On the other hand, before Android 6, the user granted all permissions while installing or updating the app, meaning less control over the specific tasks that required them and more tendency to exceed its intended usage.

5. Inspection of digital signatures and digital certificates of the application kontaktos.apk

1. Install the application kontaktos.apk.

2. Get the digital signature from the corresponding certificate of the app.



```
C:\Archivos de programa\Java\jdk1.7.0_79\bin>keytool -printcert -file CERT.RSA
Propietario: CN=Contapps, OU=Contapps, O=Contapps
Emisor: CN=Contapps, OU=Contapps, O=Contapps
N·mero de serie: 4c5af52d
Vßlido desde: Thu Aug 05 19:30:21 CEST 2010 hasta: Fri Jul 23 19:30:21 CEST 2060
Huellas digitales del Certificado:
         MD5: FB:F5:EC:31:CC:D2:B9:27:AC:B5:72:EB:F5:02:B6:73
         SHA1: 93:EB:AA:B7:AC:59:98:8A:A2:F0:DA:A7:EB:90:44:D9:56:03:4A:94
         SHA256: 79:27:0A:D6:6A:93:71:4B:86:DA:3C:5E:98:C3:1F:44:00:67:D9:D2:4A:2A:B4:2B:F3:4C:6D:30:E2:AB:6B:9D
         Nombre del Algoritmo de Firma: MD5withRSA
         Versi¾n: 1
```

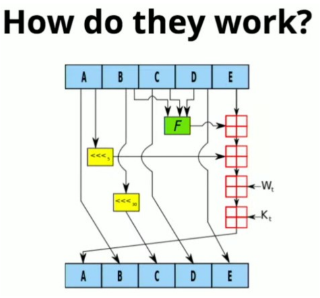
<u>3. Get the cryptographic hashes for the app´s logo and for at least three different image files with different density of pixels. Describe the algorithm used for the respective hash encoding.</u>

The cryptographic hash for the app’s logo:

Name: res/drawable-ldpi/icon.png

SHA1-Digest: VJIo9Ic2vADjDMcdEZ+VU0jNhds=

As we can see, it is making use of Secure Hash Algorithm, more specifically SHA-1 to hash both the logo and all the image files of the application.



How do they work?

SHA-1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest, typically rendered as a hexadecimal number, 40 digits long. In this case, we can see that the SHA-1 hash Digest has been encoded with base 64 but we can convert easily from base 64 to hexadecimal and vice versa.

SHA1-Digest base 64 (28 digits):

VJIo9Ic2vADjDMcdEZ+VU0jNhds=

SHA1-Digest hexadecimal number (40 digits):

54 92 28 f4 87 36 bc 00 e3 0c c7 1d 11 9f 95 53 48 cd 85 db

Here we will add the cryptographic hashes of some images according to their different pixel density:

- <u>ldpi</u>, resources for low-density (ldpi) screens (~120 dpi)

Name: res/drawable-ldpi/wizard_free_sms_pic.png

SHA1-Digest: iBswcLZoZPY+mWsnh2DlS+d6J4k=

- mdpi, resources for medium-density (mdpi) screens (~160dpi). (This is the baseline density.)

Name: res/drawable-mdpi/dialer_icon_pressed.png

SHA1-Digest: 6eKvpszPbR4COakBIS4t0236xMU=

- hdpi, resources for high-density (hdpi) screens (~240dpi) .

Name: res/drawable-xhdpi/icon_merger.png

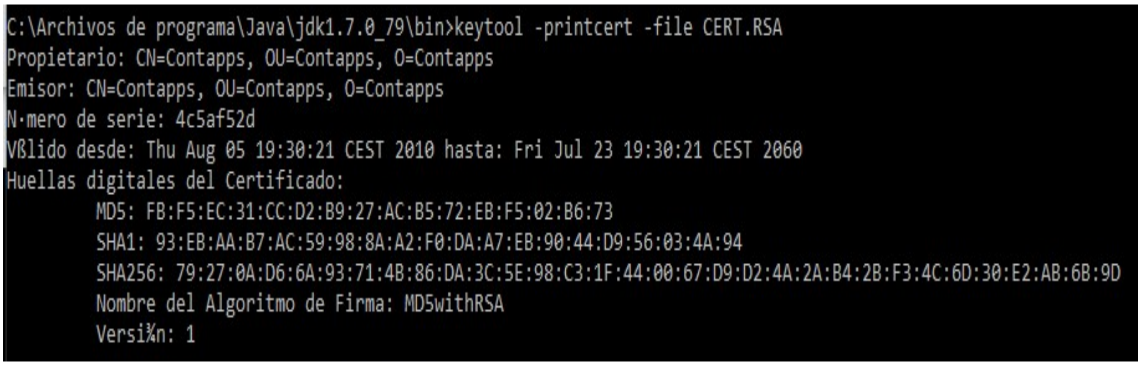
SHA1-Digest: bITJ43zfdZujDk/ncxm/Cf+r9kI=

- xhdpi, Resources for extra high-density (xhdpi) screens (~320dpi).

Name: res/drawable-hdpi/icon_call_log.png

SHA1-Digest: 1UWkf9hVMzxaQoxT4Z0Odi45hQw=

4. Describe each part of the CERT.RSA file of this app.



```
C:\Archivos de programa\Java\jdk1.7.0_79\bin>keytool -printcert -file CERT.RSA
Propietario: CN=Contapps, OU=Contapps, O=Contapps
Emisor: CN=Contapps, OU=Contapps, O=Contapps
N·mero de serie: 4c5af52d
Vßlido desde: Thu Aug 05 19:30:21 CEST 2010 hasta: Fri Jul 23 19:30:21 CEST 2060
Huellas digitales del Certificado:
         MD5: FB:F5:EC:31:CC:D2:B9:27:AC:B5:72:EB:F5:02:B6:73
         SHA1: 93:EB:AA:B7:AC:59:98:8A:A2:F0:DA:A7:EB:90:44:D9:56:03:4A:94
         SHA256: 79:27:0A:D6:6A:93:71:4B:86:DA:3C:5E:98:C3:1F:44:00:67:D9:D2:4A:2A:B4:2B:F3:4C:6D:30:E2:AB:6B:9D
         Nombre del Algoritmo de Firma: MD5withRSA
         Versi¾n: 1
```

The Fingerprints of the Certificate is composed of three parts:

1. MD5 (Message-Digest Algorithm 5) , It is a widely used 128-bit cryptographic reduction algorithm.
2. SHA-1 (Secure Hash Algorithm),
3. SHA-256 is a variation of SHA-2, the successor of SHA-1

The main differences that exist between them two are:

Algorithm	Output size (bits)	Internal state size	Block size (bits)	Max message	Rounds

		(bits)		size (bits)	
SHA-1	160 (5x32)	160	512	$2^{64} - 1$	80
SHA-256	256 (8x32)	256	512	$2^{64} - 1$	64

5. Give a brief description and the values obtained from these app certificate elements:

a. Serial Number

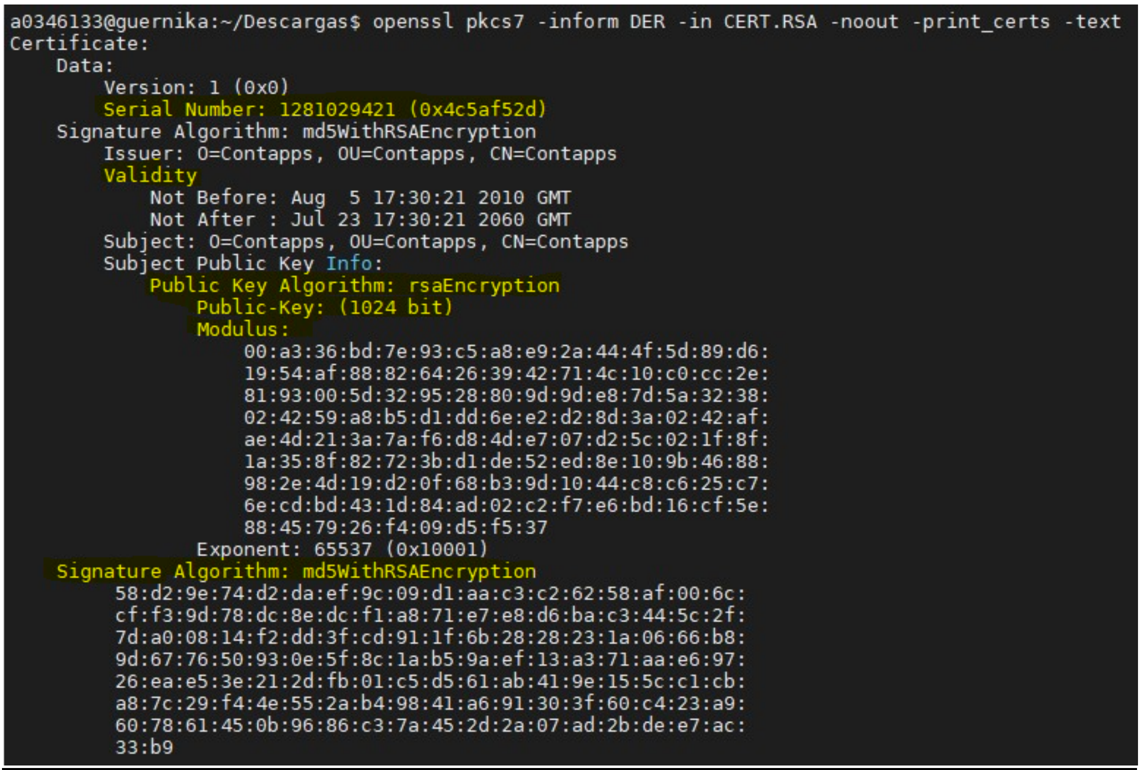
b. Validity

c. Coding algorithm used for public key

d. Size of the public key

e. Modulus

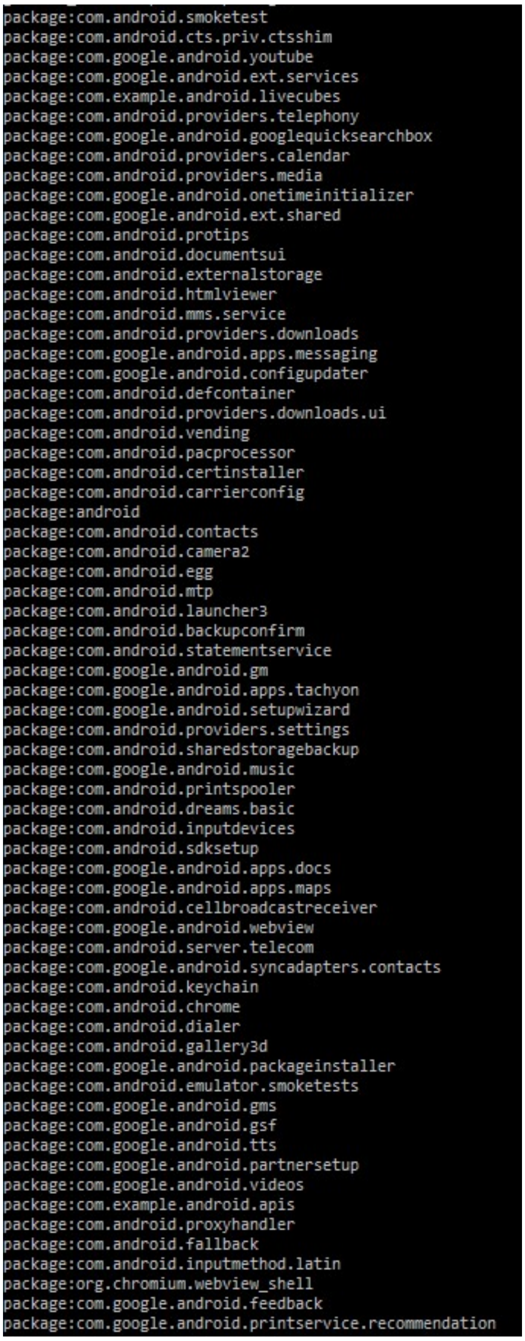
f. Signature algorithm



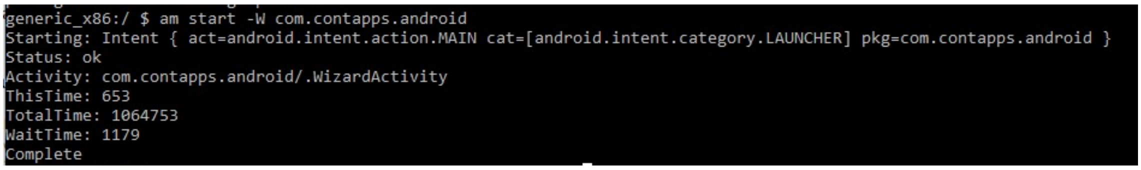
```
a0346133@guernika:~/Descargas$ openssl pkcs7 -inform DER -in CERT.RSA -noout -print_certs -text
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 1281029421 (0x4c5af52d)
    Signature Algorithm: md5WithRSAEncryption
        Issuer: O=Contapps, OU=Contapps, CN=Contapps
        Validity
            Not Before: Aug  5 17:30:21 2010 GMT
            Not After : Jul 23 17:30:21 2060 GMT
        Subject: O=Contapps, OU=Contapps, CN=Contapps
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:a3:36:bd:7e:93:c5:a8:e9:2a:44:4f:5d:89:d6:
                    19:54:af:88:82:64:26:39:42:71:4c:10:c0:cc:2e:
                    81:93:00:5d:32:95:28:80:9d:9d:e8:7d:5a:32:38:
                    02:42:59:a8:b5:d1:dd:6e:e2:d2:8d:3a:02:42:af:
                    ae:4d:21:3a:7a:f6:d8:4d:e7:07:d2:5c:02:1f:8f:
                    1a:35:8f:82:72:3b:d1:de:52:ed:8e:10:9b:46:88:
                    98:2e:4d:19:d2:0f:68:b3:9d:10:44:c8:c6:25:c7:
                    6e:cd:bd:43:1d:84:ad:02:c2:f7:e6:bd:16:cf:5e:
                    88:45:79:26:f4:09:d5:f5:37
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
         58:d2:9e:74:d2:da:ef:9c:09:d1:aa:c3:c2:62:58:af:00:6c:
         cf:f3:9d:78:dc:8e:dc:f1:a8:71:e7:e8:d6:ba:c3:44:5c:2f:
         7d:a0:08:14:f2:dd:3f:cd:91:1f:6b:28:28:23:1a:06:66:b8:
         9d:67:76:50:93:0e:5f:8c:1a:b5:9a:ef:13:a3:71:aa:e6:97:
         26:ea:e5:3e:21:2d:fb:01:c5:d5:61:ab:41:9e:15:5c:c1:cb:
         a8:7c:29:f4:4e:55:2a:b4:98:41:a6:91:30:3f:60:c4:23:a9:
         60:78:61:45:0b:96:86:c3:7a:45:2d:2a:07:ad:2b:de:e7:ac:
         33:b9
```

6. Interacting with the Activity Manager via ADB

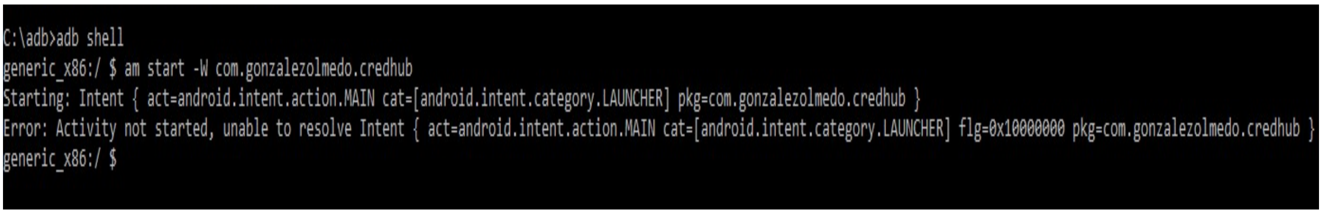
Get a screenshot of the partial list of applications installed on the emulator used for development, showing the package corresponding to kontaktos.apk application and the application created by you (CredHub).



```
package:com.android.smoketest
package:com.android.cts.priv.ctsshim
package:com.google.android.youtube
package:com.google.android.ext.services
package:com.example.android.livecubes
package:com.android.providers.telephony
package:com.google.android.googlequicksearchbox
package:com.android.providers.calendar
package:com.android.providers.media
package:com.google.android.onetimeinitializer
package:com.google.android.ext.shared
package:com.android.protips
package:com.android.documentsui
package:com.android.externalstorage
package:com.android.htmlviewer
package:com.android.mms.service
package:com.android.providers.downloads
package:com.google.android.apps.messaging
package:com.google.android.configupdater
package:com.android.defcontainer
package:com.android.providers.downloads.ui
package:com.android.vending
package:com.android.pacprocessor
package:com.android.certinstaller
package:com.android.carrierconfig
package:android
package:com.android.contacts
package:com.android.camera2
package:com.android.egg
package:com.android.mtp
package:com.android.launcher3
package:com.android.backupconfirm
package:com.android.statementservice
package:com.google.android.gm
package:com.google.android.apps.tachyon
package:com.google.android.setupwizard
package:com.android.providers.settings
package:com.android.sharedstoragebackup
package:com.google.android.music
package:com.android.printspooler
package:com.android.dreams.basic
package:com.android.inputdevices
package:com.android.sdksetup
package:com.google.android.apps.docs
package:com.google.android.apps.maps
package:com.android.cellbroadcastreceiver
package:com.google.android.webview
package:com.android.server.telecom
package:com.google.android.syncadapters.contacts
package:com.android.keychain
package:com.android.chrome
package:com.android.dialer
package:com.android.gallery3d
package:com.google.android.packageinstaller
package:com.android.emulator.smoketests
package:com.google.android.gms
package:com.google.android.gsf
package:com.google.android.tts
package:com.google.android.partnersetup
package:com.google.android.videos
package:com.example.android.apis
package:com.android.proxyhandler
package:com.android.fallback
package:com.android.inputmethod.latin
package:org.chromium.webview_shell
package:com.google.android.feedback
package:com.google.android.printservice.recommendation
```



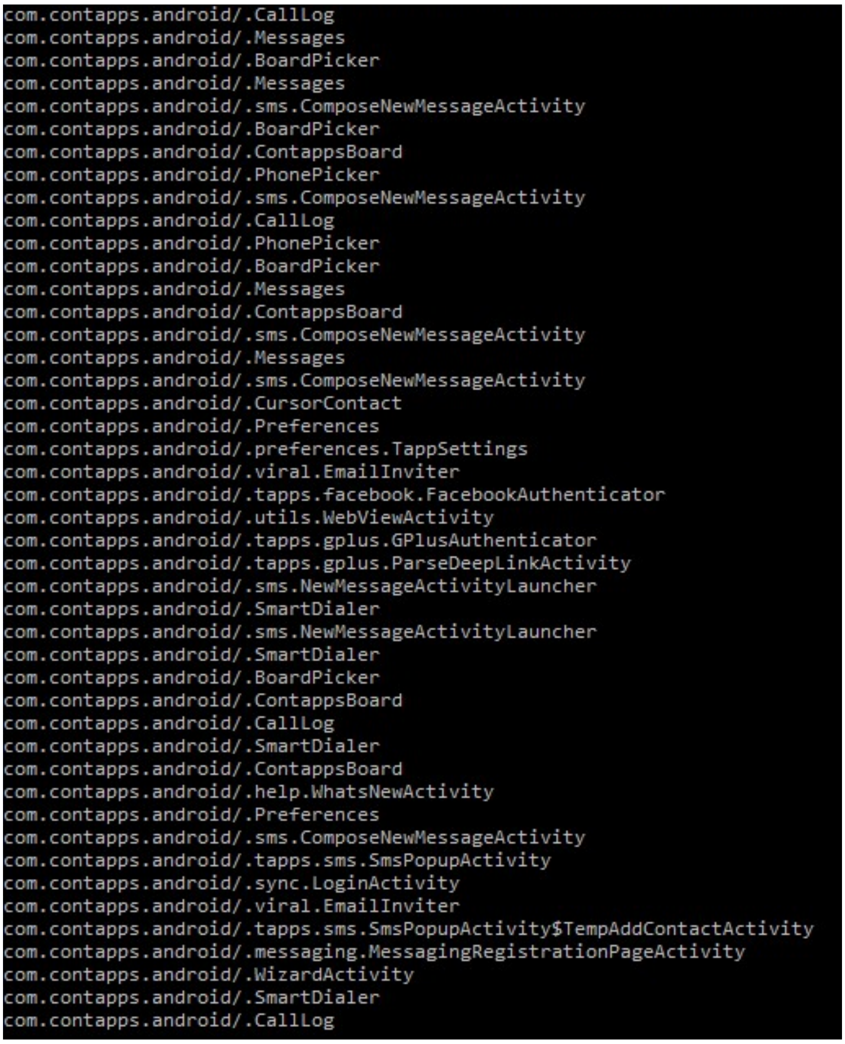
```
generic_x86:/ $ am start -W com.contapps.android
Starting: Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] pkg=com.contapps.android }
Status: ok
Activity: com.contapps.android/.WizardActivity
ThisTime: 653
TotalTime: 1064753
WaitTime: 1179
Complete
```



```
C:\adb>adb shell
generic_x86:/ $ am start -W com.gonzalezolmedo.credhub
Starting: Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] pkg=com.gonzalezolmedo.credhub }
Error: Activity not started, unable to resolve Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] flg=0x10000000 pkg=com.gonzalezolmedo.credhub }
generic_x86:/ $
```

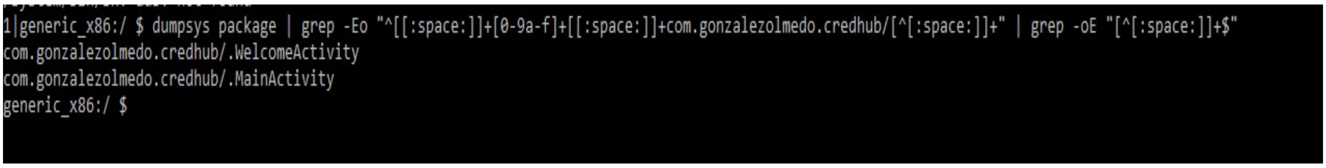
Get a list of all installed activities on kontaktos.apk and on CredHub

kontaktos.apk:



```
com.contapps.android/.CallLog
com.contapps.android/.Messages
com.contapps.android/.BoardPicker
com.contapps.android/.Messages
com.contapps.android/.sms.ComposeNewMessageActivity
com.contapps.android/.BoardPicker
com.contapps.android/.ContappsBoard
com.contapps.android/.PhonePicker
com.contapps.android/.sms.ComposeNewMessageActivity
com.contapps.android/.CallLog
com.contapps.android/.PhonePicker
com.contapps.android/.BoardPicker
com.contapps.android/.Messages
com.contapps.android/.ContappsBoard
com.contapps.android/.sms.ComposeNewMessageActivity
com.contapps.android/.Messages
com.contapps.android/.sms.ComposeNewMessageActivity
com.contapps.android/.CursorContact
com.contapps.android/.Preferences
com.contapps.android/.preferences.TappSettings
com.contapps.android/.viral.EmailInviter
com.contapps.android/.tapps.facebook.FacebookAuthenticator
com.contapps.android/.utils.WebViewActivity
com.contapps.android/.tapps.gplus.GPlusAuthenticator
com.contapps.android/.tapps.gplus.ParseDeepLinkActivity
com.contapps.android/.sms.NewMessageActivityLauncher
com.contapps.android/.SmartDialer
com.contapps.android/.sms.NewMessageActivityLauncher
com.contapps.android/.SmartDialer
com.contapps.android/.BoardPicker
com.contapps.android/.ContappsBoard
com.contapps.android/.CallLog
com.contapps.android/.SmartDialer
com.contapps.android/.ContappsBoard
com.contapps.android/.help.WhatsNewActivity
com.contapps.android/.Preferences
com.contapps.android/.sms.ComposeNewMessageActivity
com.contapps.android/.tapps.sms.SmsPopupActivity
com.contapps.android/.sync.LoginActivity
com.contapps.android/.viral.EmailInviter
com.contapps.android/.tapps.sms.SmsPopupActivity$TempAddContactActivity
com.contapps.android/.messaging.MessagingRegistrationPageActivity
com.contapps.android/.WizardActivity
com.contapps.android/.SmartDialer
com.contapps.android/.CallLog
```

Credhub:



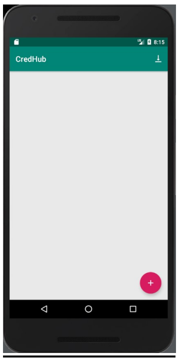
```
1|generic_x86:/ $ dumpsys package | grep -Eo "^[[:space:]]+[0-9a-f]+[[:space:]]+com.gonzalezolmedo.credhub/[^[:space:]]+" | grep -oE "[^[:space:]]+$"
com.gonzalezolmedo.credhub/.WelcomeActivity
com.gonzalezolmedo.credhub/.MainActivity
generic_x86:/ $
```

Pick an activity from CredHub and run it via ADB: describe the obtained results.

Depending on the activity we execute:

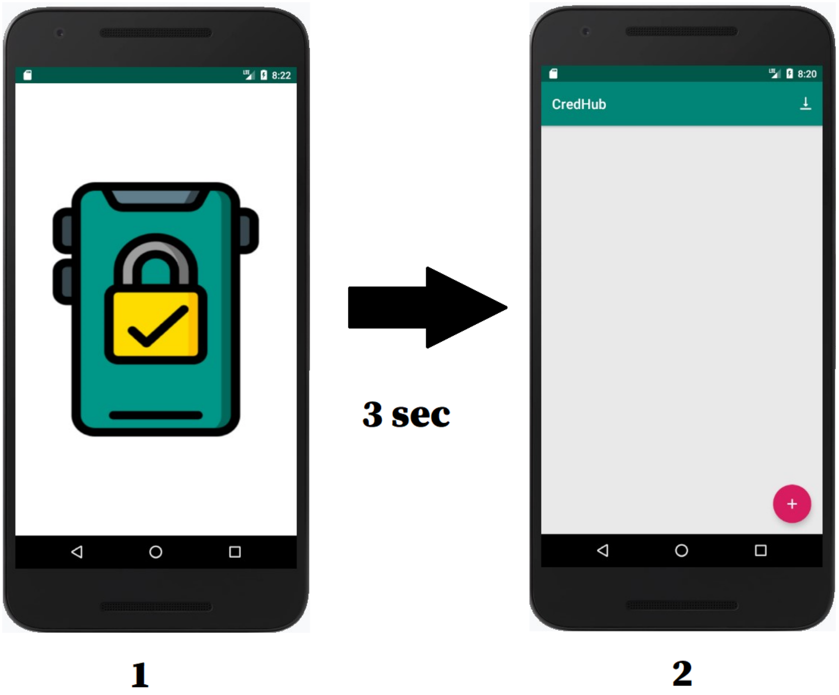
1-If we execute MainActivity we arrive directly at the following window:

am start -n com.gonzalezolmedo.credhub/.MainActivity



2- On the contrary, if we execute the activity WelcomeActivity, we arrive at the welcome window and after 3 seconds we obtain the same window as before.

am start -n com.gonzalezolmedo.credhub/.WelcomeActivity



<u>*Pick a service from kontaktos.apk and run it via ADB: please describe briefly*</u>

In order to get the services that are running we have used the command: *dumpsys -l*

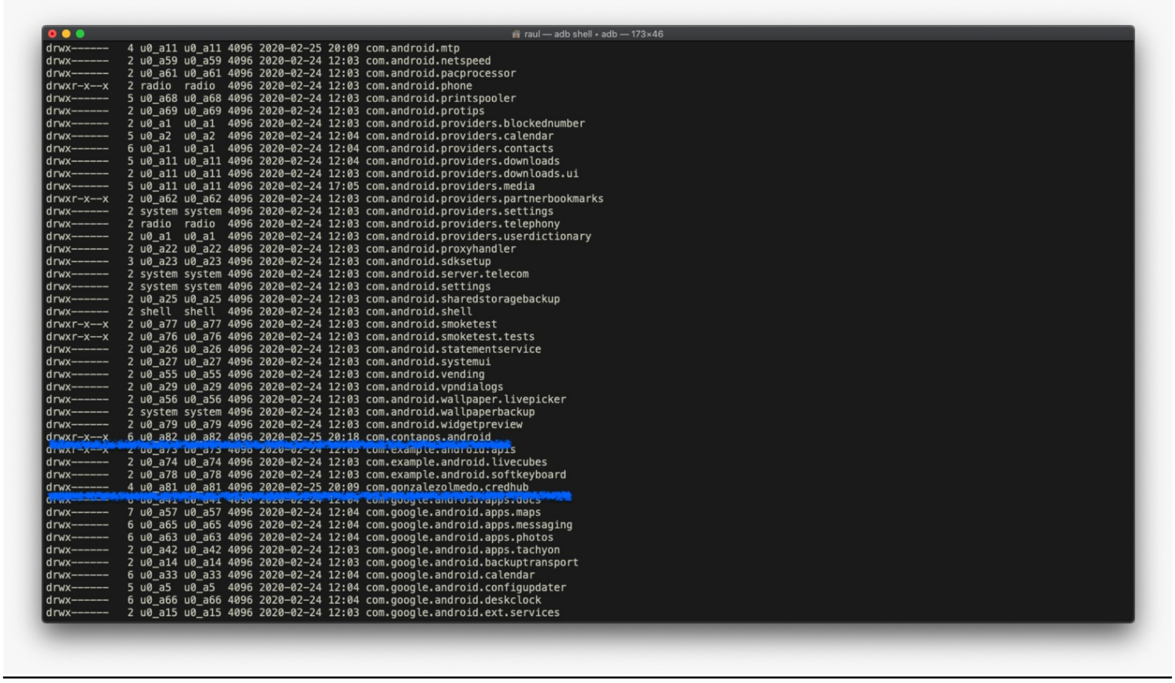
Dumpsys is a tool built into the Android OS, generally used for development purposes to show the status of services running on the device. *Dumpsys* does not require root access, but like all ADB commands, it does require USB Debugging to be enabled on the device and Secure USB Debugging to be bypassed.

ServiceInfo: AuthenticatorDescription {type=com.contapps.android.sync.account}, ComponentInfo{com.contapps.android/com.contapps.android.sync.AccountAuthenticatorService}, uid 10082

com.contapps.android.sync.AccountAuthenticatorService

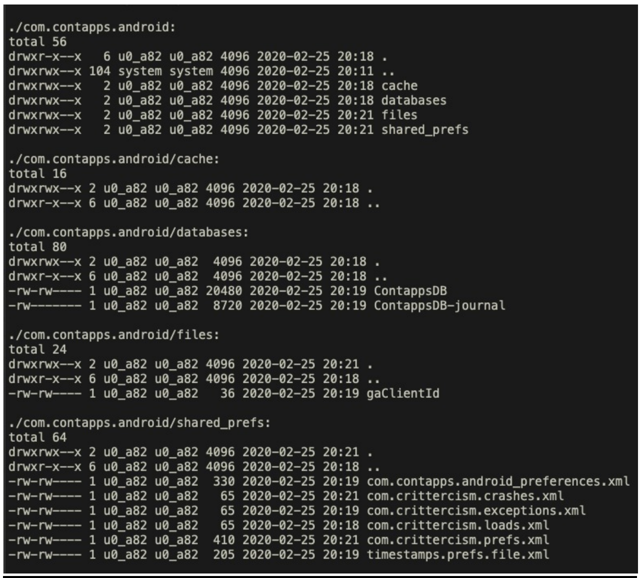
7. Extracting an app via ADB

Get a list of all permissions and creation dates for CredHub and kontaktos.apk

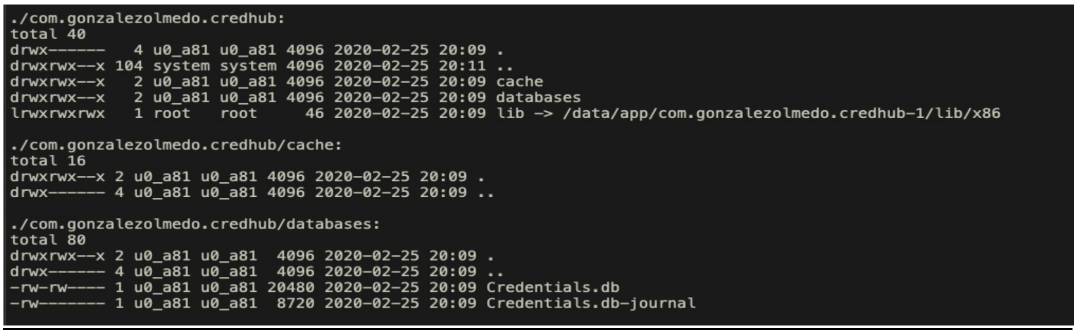


```
drwx------   4 u0_a11 u0_a11 4096 2020-02-25 20:09 com.android.mtp
drwx------   2 u0_a59 u0_a59 4096 2020-02-24 12:03 com.android.netspeed
drwx------   2 u0_a61 u0_a61 4096 2020-02-24 12:03 com.android.pacprocessor
drwxr-x--x   2 radio  radio  4096 2020-02-24 12:03 com.android.phone
drwx------   5 u0_a68 u0_a68 4096 2020-02-24 12:03 com.android.printspooler
drwx------   2 u0_a69 u0_a69 4096 2020-02-24 12:03 com.android.protips
drwx------   2 u0_a1  u0_a1  4096 2020-02-24 12:03 com.android.providers.blockednumber
drwx------   5 u0_a2  u0_a2  4096 2020-02-24 12:04 com.android.providers.calendar
drwx------   6 u0_a1  u0_a1  4096 2020-02-24 12:04 com.android.providers.contacts
drwx------   5 u0_a11 u0_a11 4096 2020-02-24 12:04 com.android.providers.downloads
drwx------   2 u0_a11 u0_a11 4096 2020-02-24 12:03 com.android.providers.downloads.ui
drwx------   5 u0_a11 u0_a11 4096 2020-02-24 17:05 com.android.providers.media
drwxr-x--x   2 u0_a62 u0_a62 4096 2020-02-24 12:03 com.android.providers.partnerbookmarks
drwx------   2 system system 4096 2020-02-24 12:03 com.android.providers.settings
drwx------   2 radio  radio  4096 2020-02-24 12:03 com.android.providers.telephony
drwx------   2 u0_a1  u0_a1  4096 2020-02-24 12:03 com.android.providers.userdictionary
drwx------   2 u0_a22 u0_a22 4096 2020-02-24 12:03 com.android.proxyhandler
drwx------   3 u0_a23 u0_a23 4096 2020-02-24 12:03 com.android.sdksetup
drwx------   2 system system 4096 2020-02-24 12:03 com.android.server.telecom
drwx------   2 system system 4096 2020-02-24 12:03 com.android.settings
drwx------   2 u0_a25 u0_a25 4096 2020-02-24 12:03 com.android.sharedstoragebackup
drwx------   2 shell  shell  4096 2020-02-24 12:03 com.android.shell
drwxr-x--x   2 u0_a77 u0_a77 4096 2020-02-24 12:03 com.android.smoketest
drwxr-x--x   2 u0_a76 u0_a76 4096 2020-02-24 12:03 com.android.smoketest.tests
drwx------   2 u0_a26 u0_a26 4096 2020-02-24 12:03 com.android.statementservice
drwx------   2 u0_a27 u0_a27 4096 2020-02-24 12:03 com.android.systemui
drwx------   2 u0_a55 u0_a55 4096 2020-02-24 12:03 com.android.vending
drwx------   2 u0_a29 u0_a29 4096 2020-02-24 12:03 com.android.vpndialogs
drwx------   2 u0_a56 u0_a56 4096 2020-02-24 12:03 com.android.wallpaper.livepicker
drwx------   2 system system 4096 2020-02-24 12:03 com.android.wallpaperbackup
drwx------   2 u0_a79 u0_a79 4096 2020-02-24 12:03 com.android.widgetpreview
drwxr-x--x   6 u0_a82 u0_a82 4096 2020-02-25 20:18 com.contapps.android
[redacted]
drwx------   2 u0_a74 u0_a74 4096 2020-02-24 12:03 com.example.android.livecubes
drwx------   2 u0_a78 u0_a78 4096 2020-02-24 12:03 com.example.android.softkeyboard
drwx------   4 u0_a81 u0_a81 4096 2020-02-25 20:09 com.gonzalezolmedo.credhub
[redacted]
drwx------   7 u0_a57 u0_a57 4096 2020-02-24 12:04 com.google.android.apps.maps
drwx------   6 u0_a65 u0_a65 4096 2020-02-24 12:04 com.google.android.apps.messaging
drwx------   6 u0_a63 u0_a63 4096 2020-02-24 12:04 com.google.android.apps.photos
drwx------   2 u0_a42 u0_a42 4096 2020-02-24 12:03 com.google.android.apps.tachyon
drwx------   2 u0_a14 u0_a14 4096 2020-02-24 12:03 com.google.android.backuptransport
drwx------   6 u0_a33 u0_a33 4096 2020-02-24 12:04 com.google.android.calendar
drwx------   5 u0_a5  u0_a5  4096 2020-02-24 12:04 com.google.android.configupdater
drwx------   6 u0_a66 u0_a66 4096 2020-02-24 12:04 com.google.android.deskclock
drwx------   2 u0_a15 u0_a15 4096 2020-02-24 12:03 com.google.android.ext.services
```

Get a list of all application resources for CredHub and kontaktos.apk, as well as their metadata.

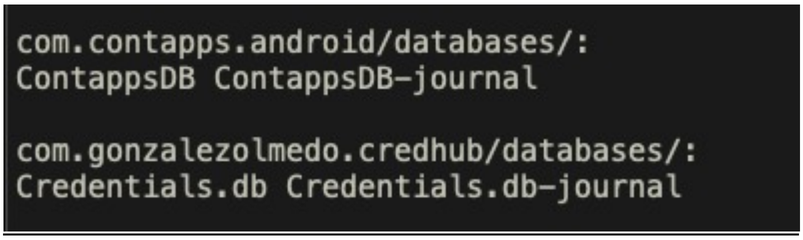


```
./com.contapps.android:
total 56
drwxr-x--x   6 u0_a82 u0_a82 4096 2020-02-25 20:18 .
drwxrwx--x 104 system system 4096 2020-02-25 20:11 ..
drwxrwx--x   2 u0_a82 u0_a82 4096 2020-02-25 20:18 cache
drwxrwx--x   2 u0_a82 u0_a82 4096 2020-02-25 20:18 databases
drwxrwx--x   2 u0_a82 u0_a82 4096 2020-02-25 20:21 files
drwxrwx--x   2 u0_a82 u0_a82 4096 2020-02-25 20:21 shared_prefs

./com.contapps.android/cache:
total 16
drwxrwx--x 2 u0_a82 u0_a82 4096 2020-02-25 20:18 .
drwxr-x--x 6 u0_a82 u0_a82 4096 2020-02-25 20:18 ..

./com.contapps.android/databases:
total 80
drwxrwx--x 2 u0_a82 u0_a82  4096 2020-02-25 20:18 .
drwxr-x--x 6 u0_a82 u0_a82  4096 2020-02-25 20:18 ..
-rw-rw---- 1 u0_a82 u0_a82 20480 2020-02-25 20:19 ContappsDB
-rw------- 1 u0_a82 u0_a82  8720 2020-02-25 20:19 ContappsDB-journal

./com.contapps.android/files:
total 24
drwxrwx--x 2 u0_a82 u0_a82 4096 2020-02-25 20:21 .
drwxr-x--x 6 u0_a82 u0_a82 4096 2020-02-25 20:18 ..
-rw-rw---- 1 u0_a82 u0_a82   36 2020-02-25 20:19 gaClientId

./com.contapps.android/shared_prefs:
total 64
drwxrwx--x 2 u0_a82 u0_a82 4096 2020-02-25 20:21 .
drwxr-x--x 6 u0_a82 u0_a82 4096 2020-02-25 20:18 ..
-rw-rw---- 1 u0_a82 u0_a82  330 2020-02-25 20:19 com.contapps.android_preferences.xml
-rw-rw---- 1 u0_a82 u0_a82   65 2020-02-25 20:21 com.crittercism.crashes.xml
-rw-rw---- 1 u0_a82 u0_a82   65 2020-02-25 20:19 com.crittercism.exceptions.xml
-rw-rw---- 1 u0_a82 u0_a82   65 2020-02-25 20:18 com.crittercism.loads.xml
-rw-rw---- 1 u0_a82 u0_a82  410 2020-02-25 20:21 com.crittercism.prefs.xml
-rw-rw---- 1 u0_a82 u0_a82  205 2020-02-25 20:19 timestamps.prefs.file.xml
```



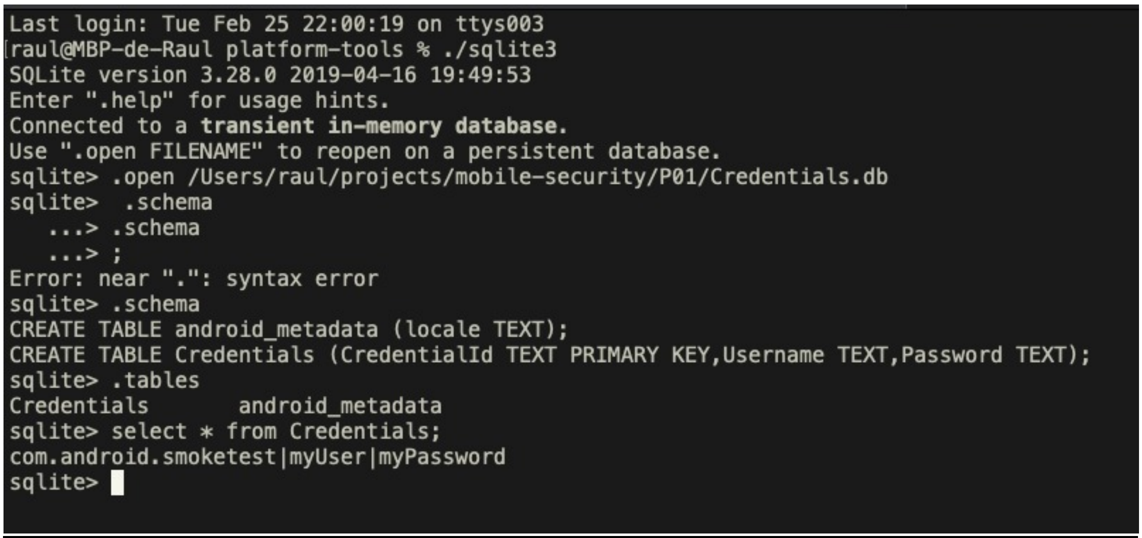
```
./com.gonzalezolmedo.credhub:
total 40
drwx------   4 u0_a81 u0_a81 4096 2020-02-25 20:09 .
drwxrwx--x 104 system system 4096 2020-02-25 20:11 ..
drwxrwx--x   2 u0_a81 u0_a81 4096 2020-02-25 20:09 cache
drwxrwx--x   2 u0_a81 u0_a81 4096 2020-02-25 20:09 databases
lrwxrwxrwx   1 root   root     46 2020-02-25 20:09 lib -> /data/app/com.gonzalezolmedo.credhub-1/lib/x86

./com.gonzalezolmedo.credhub/cache:
total 16
drwxrwx--x 2 u0_a81 u0_a81 4096 2020-02-25 20:09 .
drwx------ 4 u0_a81 u0_a81 4096 2020-02-25 20:09 ..

./com.gonzalezolmedo.credhub/databases:
total 80
drwxrwx--x 2 u0_a81 u0_a81  4096 2020-02-25 20:09 .
drwx------ 4 u0_a81 u0_a81  4096 2020-02-25 20:09 ..
-rw-rw---- 1 u0_a81 u0_a81 20480 2020-02-25 20:09 Credentials.db
-rw------- 1 u0_a81 u0_a81  8720 2020-02-25 20:09 Credentials.db-journal
```

Get a list of all the databases for CredHub and kontaktos.apk.



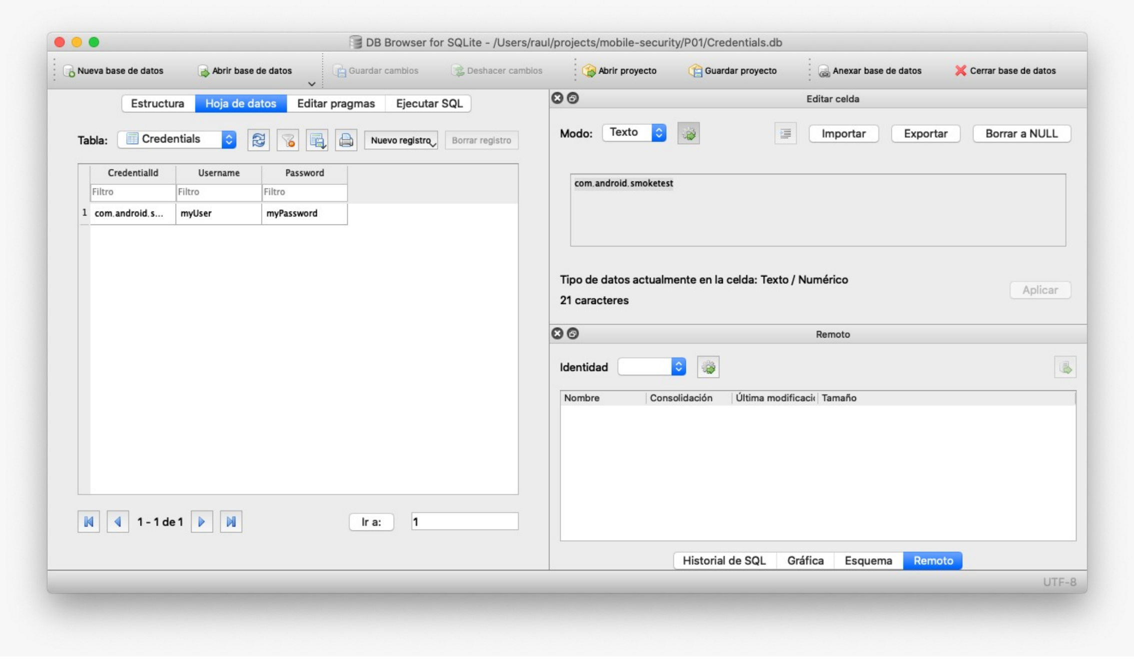
```
com.contapps.android/databases/:
ContappsDB ContappsDB-journal

com.gonzalezolmedo.credhub/databases/:
Credentials.db Credentials.db-journal
```

Get a description of the tables and columns in the database of CredHub.



```
Last login: Tue Feb 25 22:00:19 on ttys003
[raul@MBP-de-Raul platform-tools % ./sqlite3
SQLite version 3.28.0 2019-04-16 19:49:53
Enter ".help" for usage hints.
Connected to a transient in-memory database.
Use ".open FILENAME" to reopen on a persistent database.
sqlite> .open /Users/raul/projects/mobile-security/P01/Credentials.db
sqlite>  .schema
   ...> .schema
   ...> ;
Error: near ".": syntax error
sqlite> .schema
CREATE TABLE android_metadata (locale TEXT);
CREATE TABLE Credentials (CredentialId TEXT PRIMARY KEY,Username TEXT,Password TEXT);
sqlite> .tables
Credentials       android_metadata
sqlite> select * from Credentials;
com.android.smoketest|myUser|myPassword
sqlite> 
```

Extract all credentials stored inside the CredHub database file by using the “DB Browser for SQLite” tool.



DB Browser for SQLite - /Users/raul/projects/mobile-security/P01/Credentials.db

Tabla: Credentials

	CredentialId	Username	Password
	Filtro	Filtro	Filtro
1	com.android.s...	myUser	myPassword

Modo: Texto

com.android.smoketest

Tipo de datos actualmente en la celda: Texto / Numérico
21 caracteres