

Analyse Forensique de Smartphone Android

Mars 2023

Agenda

- Acquisition: difficultés et approches
- Android et sa sécurité
- Accès logique via ADB et ses limitations
- Arborescence Android et données importantes pour l'analyse forensique
- Utilisation d'un backup
- Accès root via l'émulateur
 - Extraction des mots de passe, SMS, ...
- Autres sources de données

Acquisition: problèmes possibles

- Effacement à distance
 - Passer en 'mode avion' ou travailler dans une cage de Faraday
- Protection du terminal
 - Mot de passe disponible ? Et pour un verrouillage biométrique ?
 - Chiffrement du stockage ?

Méthodes d'acquisition

- Acquisition manuelle
 - Utilise l'interface utilisateur
- Acquisition physique
 - Depuis la mémoire flash (chiffrement?)
- Acquisition logique
 - Via les APIs de synchronisation (backup dans le Cloud?). <http://developer.android.com/guide/topics/data/backup.html>
- Acquisition via le système de fichier
 - Root
 - Non root

Architecture Android



- Kernel Linux
 - Kernel 3.4 pour Android 4.2, 3.8 pour Android 4.4, 5.1 pour Android 13
- Code natif: bibliothèques (C ou C++)

Sécurité Android

- Basée sur Linux
 - Kernel + SELinux (\geq Android 4.3)
 - Groupes et utilisateurs Unix
 - Isolation des processus
 - ALSR, DEP, CFI
- Communication inter-processus (IPCs)
 - Binder. Pilote noyau qui arbitre les IPCs
- Niveau applicatif
 - Permissions déclarées par l'application, accordées par l'utilisateur à l'installation, puis à l'exécution
 - Niveau de permissions: normal, dangerous, signature, system

Sécurité Android (2)

- Niveau applicatif
 - Chaque application possède un UserID Unix unique, pour garantir l'isolation via l'OS
 - Application signée numériquement (par le développeur)
 - Application vérifiée automatiquement avant disponibilité sur Google Play (Protect)
 - La plupart des applications malveillantes proviennent de « Market » non officiels.
 - Google peut effacer/désinstaller à distance une application malicieuse sur les terminaux, de sa propre initiative
- Hardware
 - TEE (Trusted Execution Environment)
- Stockage chiffré par défaut depuis Android 5.0

Sécurité Android (3)

- Niveau applicatif
 - Jusqu'à Android 4.4: Dalvik VM(DVM), depuis 5.0: ART est le runtime par défaut, le code Dalvik est compilé à l'installation
- Sandboxing via droits Linux
 - Fichiers système: System ou root
 - Application: un UserID dédié
- SafetyNet/Droidguard
 - Vérification d'intégrité
 - [https://www.sstic.org/2022/presentation/droidguard a deep dive into safetynet/](https://www.sstic.org/2022/presentation/droidguard%20a%20deep%20dive%20into%20safetynet/)

Sécurité Android (4)

- Démarrage sécurisé
 - Chaine de confiance (binaire signés) depuis la ROM jusqu'aux applications
 - En détails:
 - BootROM
 - Bootloader (spécifique au constructeur)
 - Kernel
 - Init process
 - Zygote et Dalvik
 - Zygote gère les instances Dalvik et les ressources partagées
 - System server
 - Gère les accès à l'infrastructure applicative
- <https://source.android.com/devices/tech/security/verifiedboot/verified-boot.html>

Acquisition logique: requis

- Java JRE
 - <https://www.java.com/fr/download/>
- Android SDK
 - <https://developer.android.com/sdk/index.html#Other>
 - http://dl.google.com/android/installer_r24.3.4-windows.exe
- Utilisateur de Android Debug Bridge
 - Sur téléphone rooté (image émulateur du SDK)
 - Sur téléphone non rooté (téléphone personnel, en option)

Adb: installation

- Android SDK
 - Lancer 'Android SDK Manager'
 - Installer 'Tools/Android SDK Platform-Tools'
 - Installer 'Extra/Google USB driver'
- Activer 'USB debugging' sur le téléphone
- Connecter le téléphone (\geq Android 4.0)
- À partir de 4.2.2, il faut confirmer que l'ordinateur connecté est de confiance (authentification RSA)
- 'adb devices' pour tester

Exploration de l'arborescence d'un Nexus 4 (5.1.1). Adb shell

```
shell@mako:/ $ df
```

Filesystem	Size	Used	Free	Blksize
/dev	917.9M	36.0K	917.8M	4096
/sys/fs/cgroup	917.9M	12.0K	917.9M	4096
/mnt/asec	917.9M	0.0K	917.9M	4096
/mnt/obb	917.9M	0.0K	917.9M	4096
/system	827.8M	815.3M	12.5M	4096
/cache	551.7M	11.2M	540.6M	4096
/data	12.9G	12.2G	691.1M	4096
/persist	15.8M	4.2M	11.6M	4096
/firmware	64.0M	44.4M	19.5M	16384
/mnt/shell/emulated	12.9G	12.2G	691.1M	4096

```
shell@mako:/ $ mount
```

```
/dev/block/platform/msm_sdcc.1/by-name/system /system ext4
    ro,seclabel,relatime,data=ordered 0 0
/dev/block/platform/msm_sdcc.1/by-name/cache /cache ext4
    rw,seclabel,nosuid,nodev,noatime,data=ordered 0 0
/dev/block/platform/msm_sdcc.1/by-name/userdata /data ext4
    rw,seclabel,nosuid,nodev,noatime,noauto_da_alloc,data=ordered 0 0
/dev/block/platform/msm_sdcc.1/by-name/persist /persist ext4
    rw,seclabel,nosuid,nodev,relatime,nodelalloc,data=ordered 0 0
/dev/block/platform/msm_sdcc.1/by-name/modem /firmware vfat
    ro,context=u:object_r:radio_efs_file:s0,relatime,uid=1000,gid=1000,fmask=0337,dmask
    =0227,codepage=cp437,iocharset=iso8859-1,shortname=mixed,errors=remount-ro 0 0
```

6 partitions
(dont 1 logique = emulated)

4 partitions ext4
1 partition vfat (modem)

Pixel5a (Android 13). Adb shell

```
barbet:/ $ df
Filesystem            1K-blocks    Used Available Use% Mounted on
/dev/block/dm-12      835228      832696        0 100% /
tmpfs                 2796164      1456    2794708   1% /dev
tmpfs                 2796164        0    2796164   0% /mnt
/dev/block/dm-13      356472     355392        0 100% /system_ext
/dev/block/dm-14      729020     726788        0 100% /vendor
/dev/block/dm-15      2417244    2409988        0 100% /product
tmpfs                 2796676        40    2796636   1% /apex
/dev/block/dm-44     114407404  73022280  41254052   64% /data
/dev/block/loop4       7872       7836        0 100% /apex/com.android.runtime@1
/dev/block/dm-40       8364      8332        0 100% /apex/com.android.tethering@331117000
/dev/block/dm-43        704        676       16   98% /apex/com.android.sdkext@331111000
/dev/block/dm-41        232        116      112   51% /apex/com.android.scheduling@330443040
/dev/block/dm-39       9668       9640        0 100% /apex/com.android.mediaprovider@331112050
/dev/block/dm-36       7024       6996        0 100% /apex/com.android.wifi@331112000
/dev/block/dm-35      19172     19144        0 100% /apex/com.android.media.swcodec@331116000
/dev/block/loop10     20116     20088        0 100% /apex/com.android.btservices@339990000
/dev/block/dm-34       6484       6452        0 100% /apex/com.android.adbd@331113122
/dev/block/dm-32        780        752       12   99% /apex/com.android.tzdata@331012050
/dev/block/dm-31       4792       4764        0 100% /apex/com.android.conscrypt@331115000
/dev/block/loop15     36808     36780        0 100% /apex/com.android.i18n@1
/dev/block/dm-25       1872       1844        0 100% /apex/com.android.os.statsd@331010010
/dev/block/dm-26       5840       5812        0 100% /apex/com.android.media@331115000
/dev/block/loop18     46504     46476        0 100% /apex/com.android.vndk.v33@1
/dev/block/dm-21       7384      7352        0 100% /apex/com.android.neuralnetworks@331113000
/dev/block/dm-18      17940     17912        0 100% /apex/com.android.adservices@331131000
/dev/block/dm-30       5860       5832        0 100% /apex/com.android.extservices@331112010
/dev/block/dm-22      14104     14076        0 100% /apex/com.android.cellbroadcast@331111030
/dev/block/dm-20        756        728       16   98% /apex/com.android.ipsec@331111030
/dev/block/dm-29       3016       2988        0 100% /apex/com.android.uwb@331115000
/dev/block/loop25      232        96      132  43% /apex/com.android.apex.cts.shim@1
/dev/block/dm-33      16372     16344        0 100% /apex/com.android.permission@331115020
/dev/block/dm-24       3908      3880        0 100% /apex/com.android.resolv@331114000
/dev/block/dm-17      50868     50832        0 100% /apex/com.android.art@331113000
/dev/block/loop29      1616      1588        0 100% /apex/com.google.mainline.primary.libs@331058000
/dev/block/dm-16       1616      1588        0 100% /apex/com.google.mainline.primary.libs@331148200
/dev/block/dm-23       3392      3360        0 100% /apex/com.android.appsearch@331011020
/dev/block/dm-38        232        88       140  39% /apex/com.android.ondevicepersonalization@330442000
/dev/fuse             114407404  73022280  41254052   64% /storage/emulated
```

Protection des répertoires (5.1.1)

```
shell@mako:/ $ id -a
uid=2000(shell) gid=2000(shell)
  groups=1003(graphics),1004(input),1007(log),1011(adb),1015(sdcard_rw),
  1028(sdcard_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats)
  context=u:r:shell:s0
```

```
shell@mako:/ $ mount
```

```
rootfs / rootfs ro,seclabel,relatime 0 0
tmpfs /dev tmpfs rw,seclabel,nosuid,relatime,mode=755 0 0
devpts /dev/pts devpts rw,seclabel,relatime,mode=600 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,seclabel,relatime 0 0
selinuxfs /sys/fs/selinux selinuxfs rw,relatime 0 0
debugfs /sys/kernel/debug debugfs rw,relatime 0 0
none /acct cgroup rw,relatime,cpuacct 0 0
none /sys/fs/cgroup tmpfs rw,seclabel,relatime,mode=750,gid=1000 0 0
tmpfs /mnt/asec tmpfs rw,seclabel,relatime,mode=755,gid=1000 0 0
tmpfs /mnt/obb tmpfs rw,seclabel,relatime,mode=755,gid=1000 0 0
none /dev/cpuctl cgroup rw,relatime,cpu 0 0
..
/dev/fuse /mnt/shell/emulated fuse
  rw,nosuid,nodev,noexec,relatime,user_id=1023,group_id=1023,default_permissions,allo
  w_other 0 0
```

Partitions montées avec
droits spécifiques et
GID=1000

Répertoire racine

```
shell@mako:/ $ ls -l
ls -l
drwxr-xr-x root      root      2015-08-27 08:05 acct
drwxrwx--- system    cache     2015-08-20 07:08 cache
lrwxrwxrwx root      root      1970-01-01 01:00 charger -> /sbin/healthd
dr-x----- root      root      2015-08-27 08:05 config
lrwxrwxrwx root      root      2015-08-27 08:05 d -> /sys/kernel/debug
drwxrwx--x system    system     2015-08-27 18:42 data
-rw-r--r-- root      root      341 1970-01-01 01:00 default.prop
drwxr-xr-x root      root      2015-08-27 08:30 dev
lrwxrwxrwx root      root      2015-08-27 08:05 etc -> /system/etc
-rw-r--r-- root      root      16760 1970-01-01 01:00 file_contexts
dr-xr-x--- system    system     1970-01-01 01:00 firmware
-rw-r----- root      root      2625 1970-01-01 01:00 fstab.mako
-rwxr-x--- root      root      301508 1970-01-01 01:00 init
-rwxr-x--- root      root      944 1970-01-01 01:00 init.envIRON.rc
-rwxr-x--- root      root      15304 1970-01-01 01:00 init.mako.rc
-rwxr-x--- root      root      5957 1970-01-01 01:00 init.mako.usb.rc
-rwxr-x--- root      root      21728 1970-01-01 01:00 init.rc
-rwxr-x--- root      root      1927 1970-01-01 01:00 init.trace.rc
-rwxr-x--- root      root      3885 1970-01-01 01:00 init.usb.rc
-rwxr-x--- root      root      301 1970-01-01 01:00 init.zygote32.rc
```

Répertoire racine (2)

```
...
drwxrwxr-x root      system      2015-08-27 08:05 mnt
lstat './persist' failed: Permission denied
dr-xr-xr-x root      root          1970-01-01 01:00 proc
-rw-r--r-- root      root          2870 1970-01-01 01:00 property_contexts
drwxr-xr-x root      root          1970-01-01 01:00 res
drwx----- root      root          2015-07-09 01:24 root
drwxr-x--- root      root          1970-01-01 01:00 sbin
lrwxrwxrwx root      root          2015-08-27 08:05 sdcard ->
    /storage/emulated/legacy
-rw-r--r-- root      root          471 1970-01-01 01:00 seapp_contexts
-rw-r--r-- root      root           52 1970-01-01 01:00 selinux_version
-rw-r--r-- root      root      129888 1970-01-01 01:00 sepolicy
-rw-r--r-- root      root          9438 1970-01-01 01:00 service_contexts
drwxr-x--x root      sdcard_r      2015-08-27 08:05 storage
dr-xr-xr-x root      root          2015-08-27 08:05 sys
drwxr-xr-x root      root          2015-08-20 07:07 system
-rw-r--r-- root      root          2342 1970-01-01 01:00 ueventd.mako.rc
-rw-r--r-- root      root          4464 1970-01-01 01:00 ueventd.rc
lrwxrwxrwx root      root          2015-08-27 08:05 vendor -> /system/vendor
```


Android 13

```
barbet:/ $ ls -l
total 68
drwxr-xr-x  2 root  root    4096 2009-01-01 01:00 acct
drwxr-xr-x 60 root  root   1260 2023-02-19 16:08 apex
lrw-r--r--  1 root  root    11 2009-01-01 01:00 bin -> /system/bin
lrw-r--r--  1 root  root    50 2009-01-01 01:00 bugreports -> /data/user_de/0/com.android.shell/files/bugreports
l????????  ? ?    ?        ?      ? cache -> ?
drwxr-xr-x  3 root  root     0 1970-01-01 01:00 config
lrw-r--r--  1 root  root    17 2009-01-01 01:00 d -> /sys/kernel/debug
drwxrwx--x 50 system system 4096 2023-02-16 07:34 data
d????????  ? ?    ?        ?      ? data_mirror
drwxr-xr-x  2 root  root   4096 2009-01-01 01:00 debug_ramdisk
drwxr-xr-x 25 root  root   4600 2023-02-16 10:11 dev
lrw-r--r--  1 root  root    15 2009-01-01 01:00 dsp -> /vendor/lib/dsp
lrw-r--r--  1 root  root    11 2009-01-01 01:00 etc -> /system/etc
l????????  ? ?    ?        ?      ? init -> ?
-????????  ? ?    ?        ?      ? init.environ.rc
d????????  ? ?    ?        ?      ? linkerconfig
drwx----- 2 root  root  16384 2009-01-01 01:00 lost+found
d????????  ? ?    ?        ?      ? metadata
drwxr-xr-x 15 root  system  320 1970-01-18 16:42 mnt
drwxr-xr-x  2 root  root   4096 2009-01-01 01:00 odm
drwxr-xr-x  2 root  root   4096 2009-01-01 01:00 odm_dkkm
drwxr-xr-x  2 root  root   4096 2009-01-01 01:00 oem
l????????  ? ?    ?        ?      ? persist -> ?
d????????  ? ?    ?        ?      ? postinstall
dr-xr-xr-x 849 root  root     0 1970-01-01 01:00 proc
drwxr-xr-x 13 root  root   4096 2009-01-01 01:00 product
lrw-r--r--  1 root  root    21 2009-01-01 01:00 sdcard -> /storage/self/primary
drwxr-xr-x  2 root  root   4096 2009-01-01 01:00 second_stage_resources
drwx--x---  4 shell everybody 80 1970-01-18 16:42 storage
dr-xr-xr-x 12 root  root     0 1970-01-01 01:00 sys
drwxr-xr-x 13 root  root   4096 2009-01-01 01:00 system
d????????  ? ?    ?        ?      ? system_dkkm
drwxr-xr-x  9 root  root   4096 2009-01-01 01:00 system_ext
drwxr-xr-x 21 root  shell   4096 2009-01-01 01:00 vendor
drwxr-xr-x  2 root  root   4096 2009-01-01 01:00 vendor_dkkm
```

Répertoires intéressants pour l'analyse forensique (1)

/cache	Cache système des applications.
/data	Données pour chaque application. La plupart des données utilisateurs y sont stockées
/data/dalvik-cache	Contient une version optimisée (.odex) des applications
/data/data	Données privées des applications (“stockage interne”)
/proc	Comme sous Linux
/root	Homedir de l'utilisateur root
/misc	Contient des données de configuration
/sdcard	“stockage externe”, même si celui-ci est non amovible
/sdcard/DCIM	Photos et films capturés par le téléphone
/sdcard/download	téléchargements

Répertoires intéressants pour l'analyse forensique (2)

/system	Bibliothèques et binaires du système et les applications pré-installées
/system/app	Applications systèmes et pré-installées

Protection du répertoire /data

drwxrwx--x system system

2015-08-27 18:42 data

```
shell@mako:/ $ ls /data
opendir failed, Permission denied
shell@mako:/data $ cd data
shell@mako:/data/data $ ls
opendir failed, Permission denied
255|shell@mako:/data $ cd /data/dalvik-cache
shell@mako:/data/dalvik-cache $ ls
opendir failed, Permission denied
1|shell@mako:/ $ cd /data/app
shell@mako:/data/app $ ls
opendir failed, Permission denied
```

Propriétés de compilation

/system/build.prop

```
shell@mako:/ $ cat /system/build.prop
# begin build properties
# autogenerated by buildinfo.sh
ro.build.id=LMY48M
ro.build.display.id=LMY48M
ro.build.version.incremental=2167285
ro.build.version.sdk=22
ro.build.version.codename=REL
ro.build.version.all_codenames=REL
ro.build.version.release=5.1.1
ro.build.date=Fri Aug 14 03:15:32 UTC 2015
ro.build.date.utc=1439522132
ro.build.type=user
ro.build.user=android-build
ro.build.host=vpec4.mtv.corp.google.com
ro.build.tags=release-keys
ro.build.flavor=occam-user
ro.product.model=Nexus 4
```

Android 13

```
cat /system/build.prop:
Permission denied
```

Données à récupérer

Données personnelles:

- SMS, MMS, Messagerie Instantanée, Sauvegarde, emails, journal des appels, contacts, images, vidéos, historique Internet, données GPS, fichiers téléchargés,
- Données applicatives (Facebook, Skype, Twitter, Instagram, Snapchat...), entrée du calendrier...

Données système:

- Code PIN, « Gesture key », points d'accès visités...

Adb backup: utilisation

Dans `c:\Users\lclevy\AppData\Local\Android\android-sdk\platform-tools>`
si installé pour l'utilisateur seulement

Syntaxe:

```
adb backup -apk -shared -all -f backup.ab
```

Options:

Apk = les applications

Shared = carte mémoire

Conseil: uniquement `-all`

Extraction du backup

https://github.com/lclevy/ab_decrypt

ab_decrypt.py

v 1.1

Introduction

An educational python tool to decrypt Android backups (created using "adb backup").

Not memory optimized, as decryption and decompression are done in memory !

The tricky thing is to prepare the PBKDF2 secret value for password verification, as Java/Android implementation does byte to UTF16BE char to UTF8 strange conversions!

References documents:

- [Unpacking android backups](#), Nikolay Elenkov, 8th June 2012
- [BackupManagerService.java](#), Android code source
- [Java Widening and Narrowing Primitive Conversion](#), Java specification

Requirements : PyCryptoDome 3.9.0, Python 3.7.3. Tested with Android 5.1, 7.0 and 8.1 backups.

Accès root avec l'émulateur

```
root@android:/ # id
uid=0(root) gid=0(root)
root@android:/ # mount
rootfs / rootfs ro 0 0
tmpfs /dev tmpfs rw,nosuid,mode=755 0 0
devpts /dev/pts devpts rw,mode=600 0 0
proc /proc proc rw 0 0
sysfs /sys sysfs rw 0 0
none /acct cgroup rw,cpuacct 0 0
tmpfs /mnt/secure tmpfs rw,mode=700 0 0
tmpfs /mnt/asec tmpfs rw,mode=755,gid=1000 0 0
tmpfs /mnt/obb tmpfs rw,mode=755,gid=1000 0 0
none /dev/cpuctl cgroup rw,cpu 0 0
/dev/block/mtdblock0 /system yaffs2 ro 0 0
/dev/block/mtdblock1 /data yaffs2 rw,nosuid,nodev 0 0
/dev/block/mtdblock2 /cache yaffs2 rw,nosuid,nodev 0 0
```

Données applicatives internes

/data/data/

```
root@android:/ # ls -l /data/data/
drwxr-x--x u0_a35    u0_a35    2015-09-01 08:27 com.android.backupconfirm
drwxr-x--x u0_a33    u0_a33    2015-09-03 12:18 com.android.browser
drwxr-x--x u0_a18    u0_a18    2015-08-30 21:01 com.android.calculator2
drwxr-x--x u0_a4     u0_a4     2015-08-30 21:04 com.android.calendar
drwxr-x--x u0_a37    u0_a37    2015-09-03 12:17 com.android.camera
drwxr-x--x u0_a9     u0_a9     2015-08-30 21:01 com.android.certinstaller
drwxr-x--x u0_a1     u0_a1     2015-09-01 12:14 com.android.contacts
...
drwxr-x--x u0_a0     u0_a0     2015-08-30 21:01 com.android.gallery
drwxr-x--x u0_a41    u0_a41    2015-09-03 13:41 com.android.gesture.builder
drwxr-x--x u0_a24    u0_a24    2015-08-30 21:01 com.android.htmlviewer
drwxr-x--x system    system    2015-08-30 21:01 com.android.inputdevices
drwxr-x--x u0_a10    u0_a10    2015-08-30 21:03 com.android.inputmethod.latin
drwxr-x--x u0_a14    u0_a14    2015-08-30 21:01
com.android.inputmethod.pinyin
drwxr-x--x system    system    2015-08-30 21:01 com.android.keychain
drwxr-x--x u0_a20    u0_a20    2015-08-30 21:03 com.android.launcher
...
```

Configuration système

/data/system/

```
root@android:/ # ls -l /data/system/
-rw----- system system 13124 2015-09-20 15:32 batterystats.bin
drwxrwx--x system system      2015-09-02 11:42 cache
-rw----- system system 284 2015-08-30 21:02 called_pre_boots.dat
-rw----- system system 206 2015-09-03 13:30 device_policies.xml
drwx----- system system      2015-09-20 15:33 dropbox
-rw----- system system 4096 2015-09-20 15:32 entropy.dat
-rw----- system system 0 2015-09-01 11:35 gesture.key
drwx----- system system      2015-09-20 15:32 inputmethod
-rw-rw---- system system 4096 2015-08-30 21:02 locksettings.db
-rw----- system system 32768 2015-09-20 15:32 locksettings.db-shm
-rw----- system system 164832 2015-09-01 11:35 locksettings.db-wal
drwx----- system system      2015-08-30 21:02 netstats
-rw-rw---- system system 3810 2015-09-20 15:32 packages.list
-rw-rw---- system system 55165 2015-09-20 15:32 packages.xml
-rw----- system system 72 2015-09-01 11:35 password.key
drwxrwx--x system system      2015-08-30 21:03 registered_services
drwxrwx--x system system      2015-09-01 12:41 shared_prefs
drwx----- system system      2015-09-20 15:32 sync
drwx----- system system      2015-08-30 21:04 throttle
-rwxrwxr-- system system 58 2015-08-30 21:01 uiderrors.txt
drwx----- system system      2015-09-20 15:32 usagestats
drwxrwxr-x system system      2015-09-20 15:32 users
```

Stockage des SMS

```
root@android:/ # ls -l
/data/data/com.android.providers.telephony/databases/
-rw-rw----  radio      radio      102400 2015-09-01 14:00 mmssms.db
-rw-----  radio      radio      33344 2015-09-01 14:00 mmssms.db-journal
```

Structure de la base de données

Parcourir les données

Éditer les Pragma

Exécuter le SQL

Table : sms

Nouvel Enregistrement

Supprimer l'enregistrement

	_id	thread_id	address	person	date	date_sent	protocol	read	status	type
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	1	+33 6 23 23 23 23	NULL	1441116021290	0	NULL	1	-1	2



	_id	index_text	source_id	table_to_use
1	1	Hello	1	1

Source:

http://az4n6.blogspot.fr/2013/02/finding-and-reverse-engineering-deleted_1865.html

Contacts

```
/data/data/com.android.providers.contacts/databases/contacts2.db
```

Table : data   Nouvel Enregistrement Supprimer l'enregistrement

	page_id	mimetype_id	raw_contact_id	read_or	is_primar	is_super_primary	data_version	data1	data2	data3	data4
		Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1		5	1	0	0	0	1	+33 6 91 19 11 00	2	NULL	+33691191100
2		8	1	0	0	0	0	Cyber Maison De Retraite	1	NULL	Cyber Maison ...
3		1	1	0	0	0	0	mum@family.org	1	NULL	NULL
4		7	1	0	0	0	0	Mum	Mum	NULL	NULL

Autres sources de données

SMS et MMS	/data/data/com.android.providers.telephony/databases/mmssms.db
Contacts synchronisés (user #0)	/data/system/users/0/accounts.db
Contacts téléphoniques et historique des appels	/data/data/com.android.providers.contacts/databases/contacts2.db
Mot de passe du Browser	/data/data/com.android.browser/databases/webview.db
Historique de navigation Internet	/data/data/com.android.browser/databases/browser2.db
Facebook Messenger messages	/data/data/com.facebook.orca/databases/threads_db2
Skype messages / calls	/data/data/com.skype.raider/files/<account_name>/main.db

Samsung SmartSwitch

<https://www.samsung.com/us/support/owners/app/smart-switch>

Mais le backup est chiffré

Il faut acheter ce papier

<https://www.sciencedirect.com/science/article/abs/pii/S2666281721002353>

... et reverser l'application PC et Android



Forensic Science International: Digital
Investigation

Volume 39, December 2021, 301310



Methods for decrypting the data encrypted by
the latest Samsung smartphone backup
programs in Windows and macOS

Soojin Kang^a ✉, Giyeon Kim^a ✉, Myungseo Park^a ✉, Jongsung Kim^{a, b} ✉

Show more ▼

+ Add to Mendeley ✉ Share 📄 Cite

<https://doi.org/10.1016/j.fsidi.2021.301310>

[Get rights and content >](#)

Highlights

- Smart Switch provides basic backup and PIN-based backup methods, and encryption methods applied to each backup are different.
- The PIN used for PIN-based backup is verified using the authenticator contained in the backup data.
- We analyzed the latest version of Smart Switch in Windows and macOS environments, and decrypted all encrypted backup files.

ALEAPP

Android Logs Events And Protobuf Parser

<https://github.com/abrignoni/ALEAPP>

Open source!

Beaucoup d'artefacts analysés:

<https://github.com/abrignoni/ALEAPP/tree/main/scripts/artifacts>

Gmail, WhatsApp, Firefox, Smsmms, teams, Snapchat, Skype, protonVPN, Chrome, Downloads, Bluetooth, CallLog...

Utilisable sous Autopsy

https://sleuthkit.org/autopsy/docs/user-docs_fr/4.19.0/aleapp_page.html

Logiciels commerciaux

Cellebrite

<https://cellebrite.com/en/glossary/mobile-forensics/>

Oxygen Forensic Detective

<https://oxygenforensics.com/en/products/oxygen-forensic-detective/>